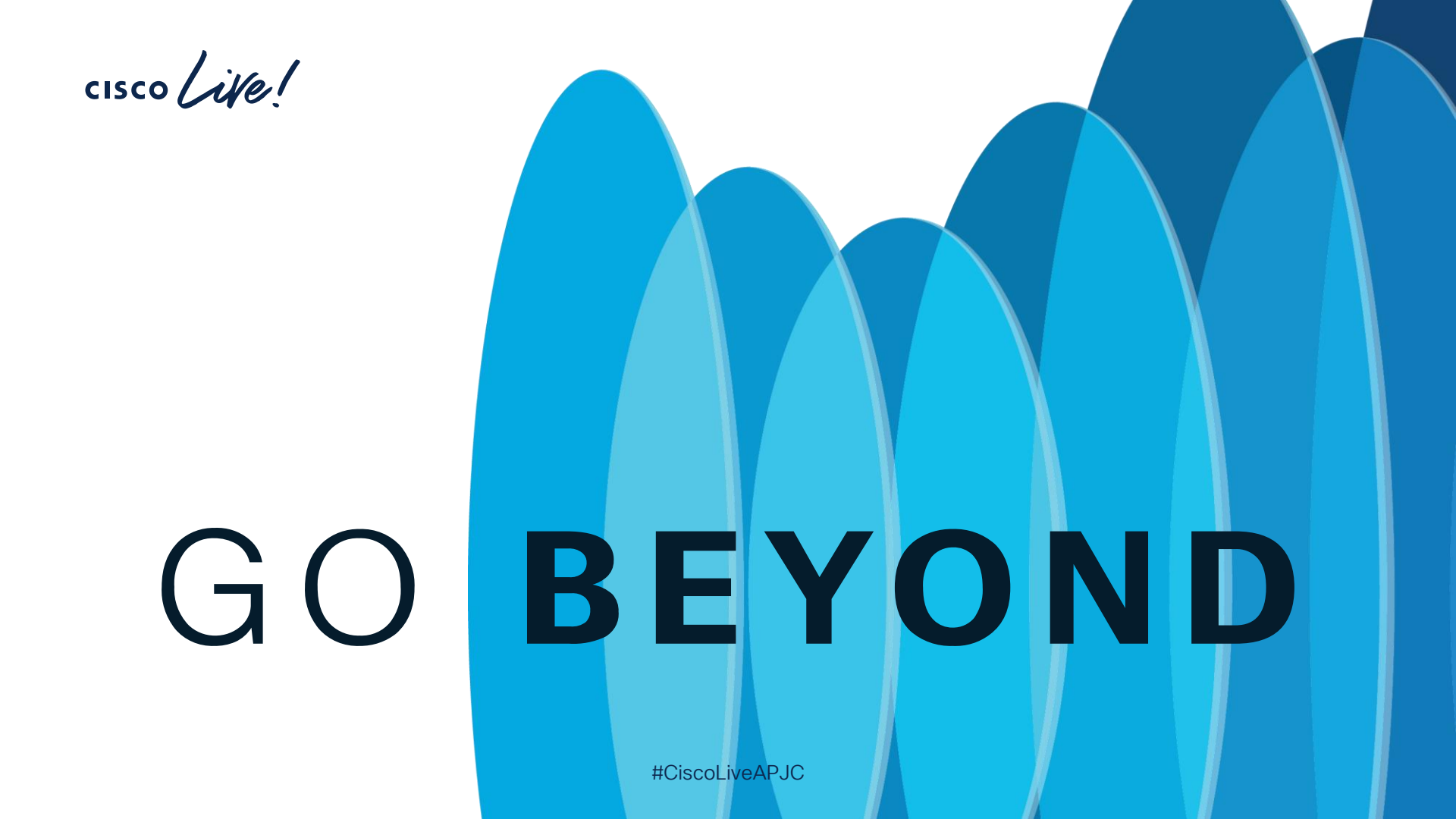

cisco Live!
GO BEYOND
#CiscoLiveAPJC

"Reconciliation"- Dustin Koa Art

Troubleshooting Collaboration

Johannes Krohn
Principal Technical Marketing Engineer
BRKCOL-3531

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-3531

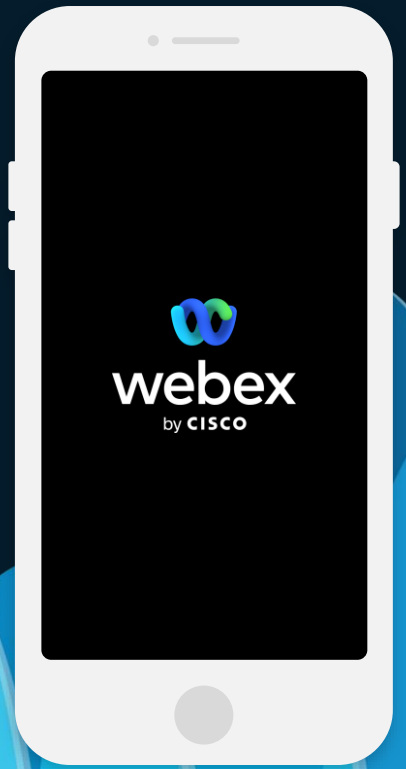
Questions?

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

How

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

Webex spaces will be moderated by the speaker until November 15, 2024.



cisco Live!

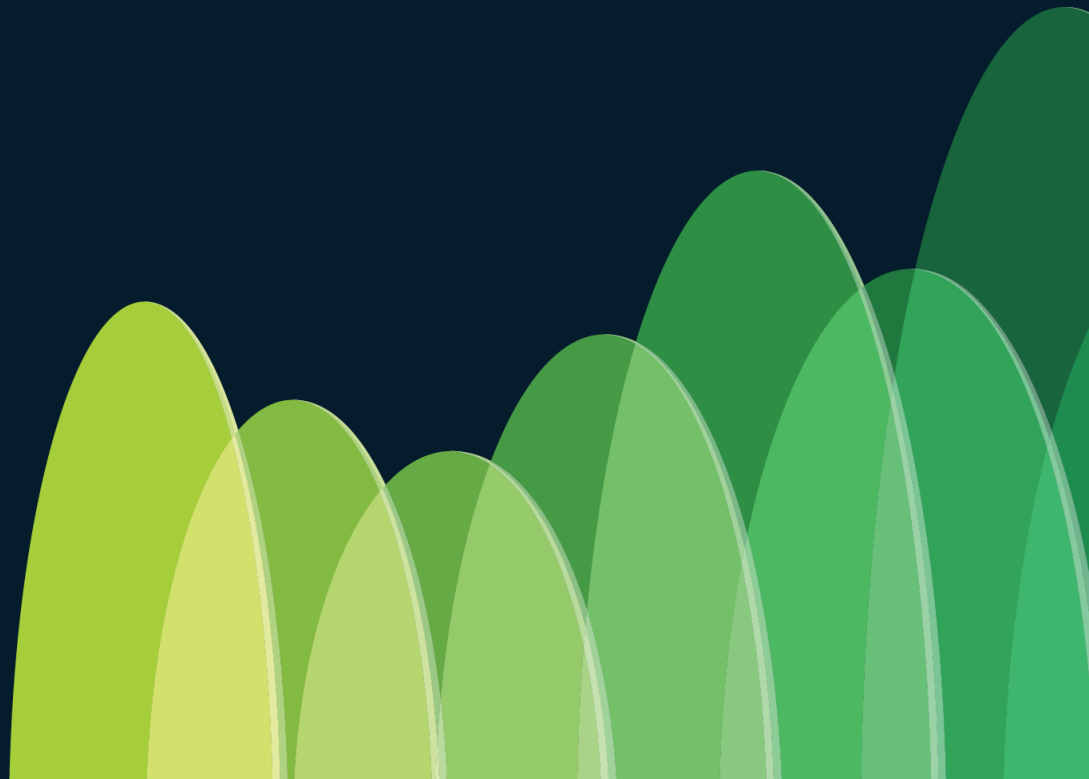
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Web debugging
- User Provisioning
  - Direct
  - Director Connector
  - Extra ID Wizard
- Authentication
  - SSO
- Call Routing

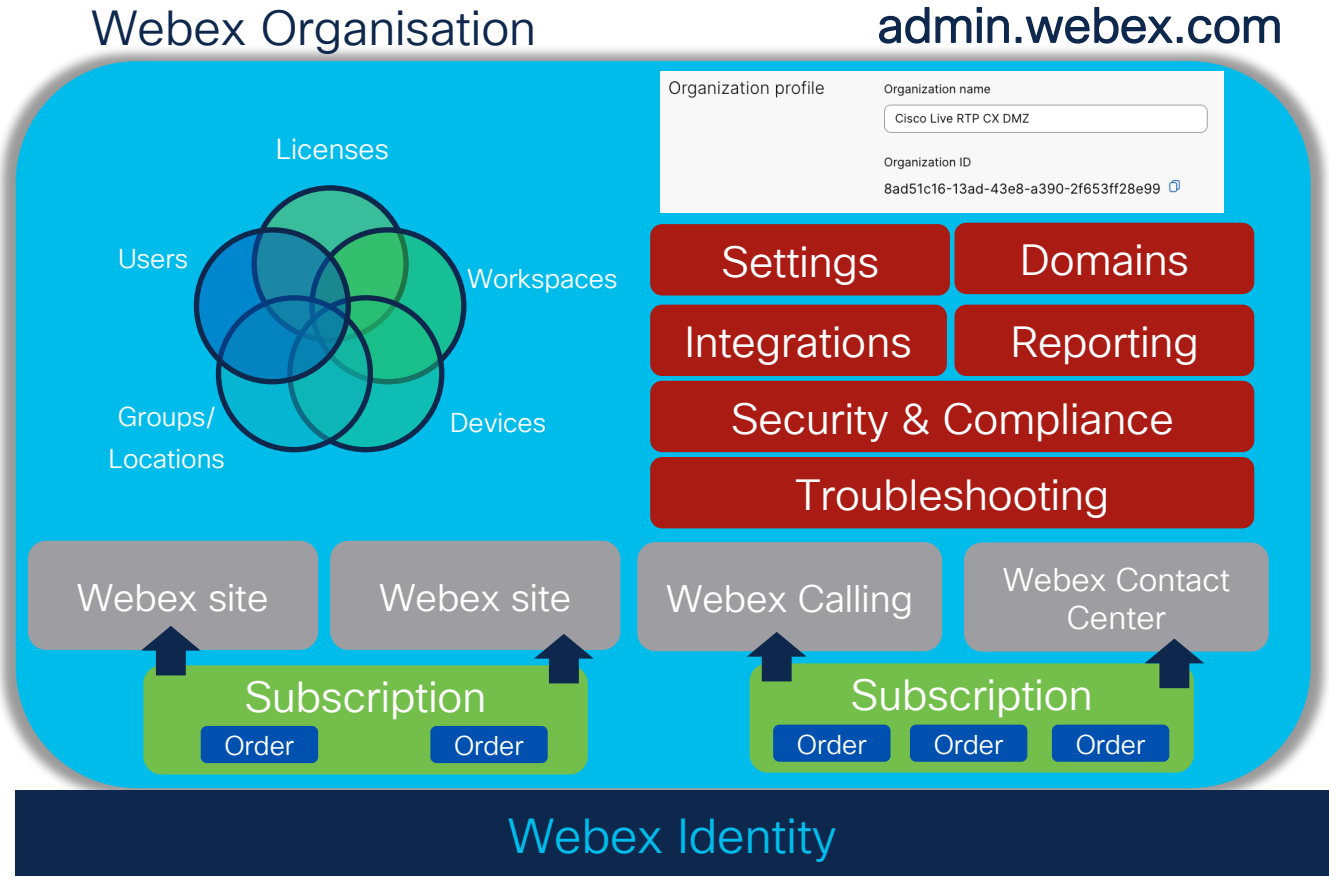
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introduction



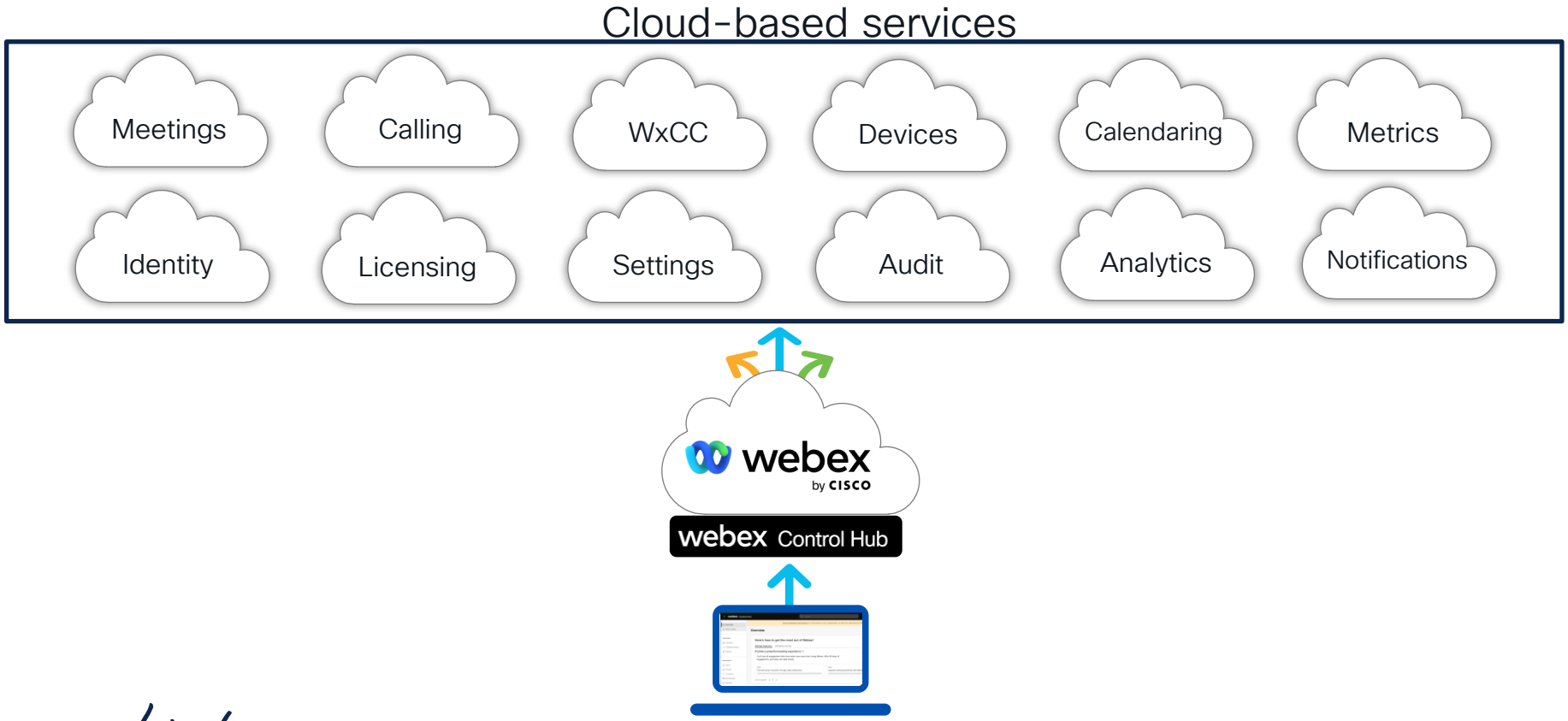
What is a Webex Organisation?

An organisation is a logical management construct for a customer in the Webex platform which allows them to manage their Webex collaboration services for a set of users & devices



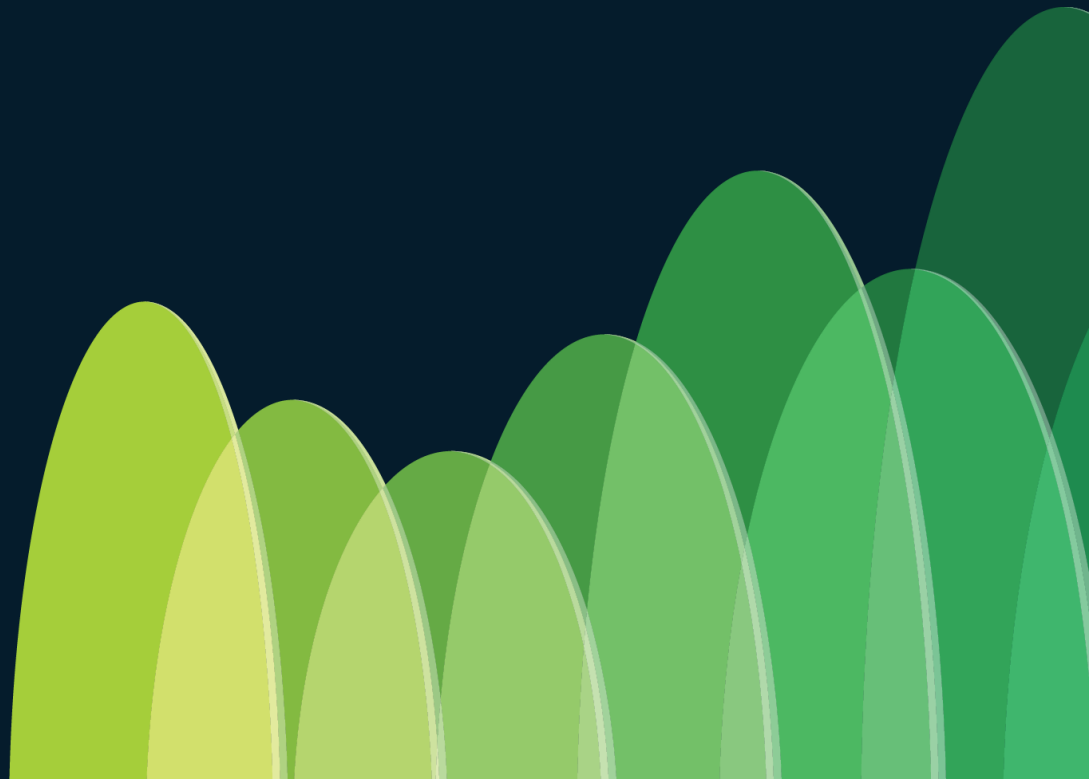
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Hub: Window into the World



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

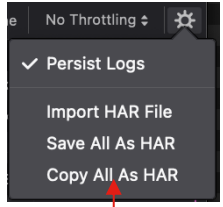
Web debugging basics



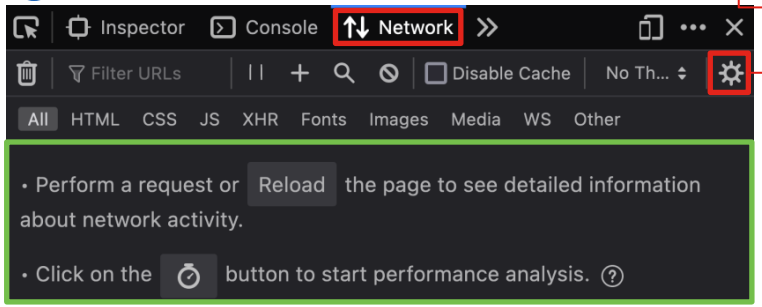
cisco Live!

Troubleshooting Control Hub Errors

Collecting a Browser Trace

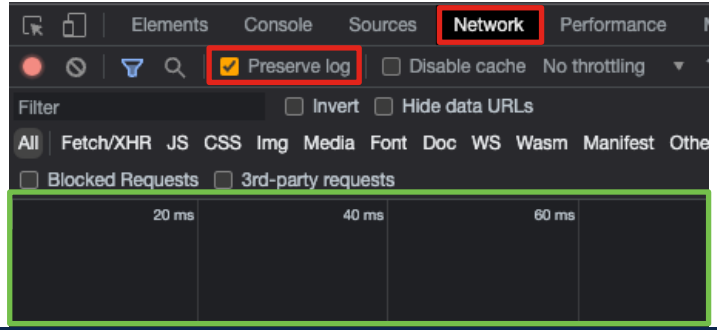


TIP [Collecting a browser trace]



Firefox

1. Right-click > **Inspect**
2. Select Network
3. Load page



Chrome

1. Right-click > Inspect
2. Select Network
3. Check Preserve Log
4. Load page

Many tools such as Proxyman or Google's HAR Analyzer allow you to read the HAR file more easily.

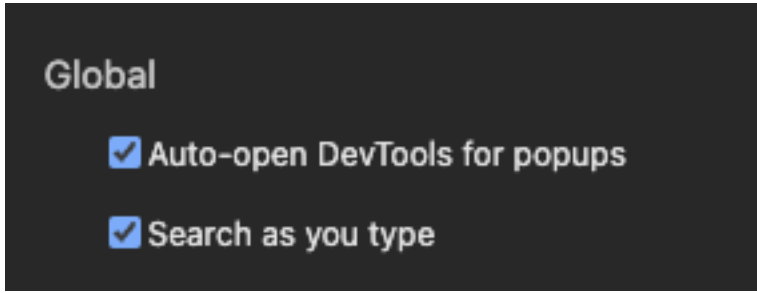
features include text search, filter by HTTP status code, and message color coding

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Web debugging Tips & Tricks

Chrome: Continue debugging on popups

- In Partner Hub if you launch into a Customer organisation it will open a new tab
- By default, the cross-launch **isn't captured by a browser trace**
- To adjust this, from a browser trace:
  - Click the gear icon ⚙
  - Navigate to the Global section
  - Check the box for **Auto-open DevTools for popups**



Firefox requires add-on support to deliver the same capability

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

HTTP Request Types

RFC 2616

DELETE	Requests the origin server delete the resource identified by
GET	Retrieve whatever information is identified by the Request-URI
OPTIONS	A request for information about the communication options available on the request/response chain
POST	Creates a new resource or appends data an existing resource
PUT	Updates an existing resource or creates one if it is not present
PATCH	Used to make a partial update on a resource

Most used Request Types in Control Hub

Does not represent the full list!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

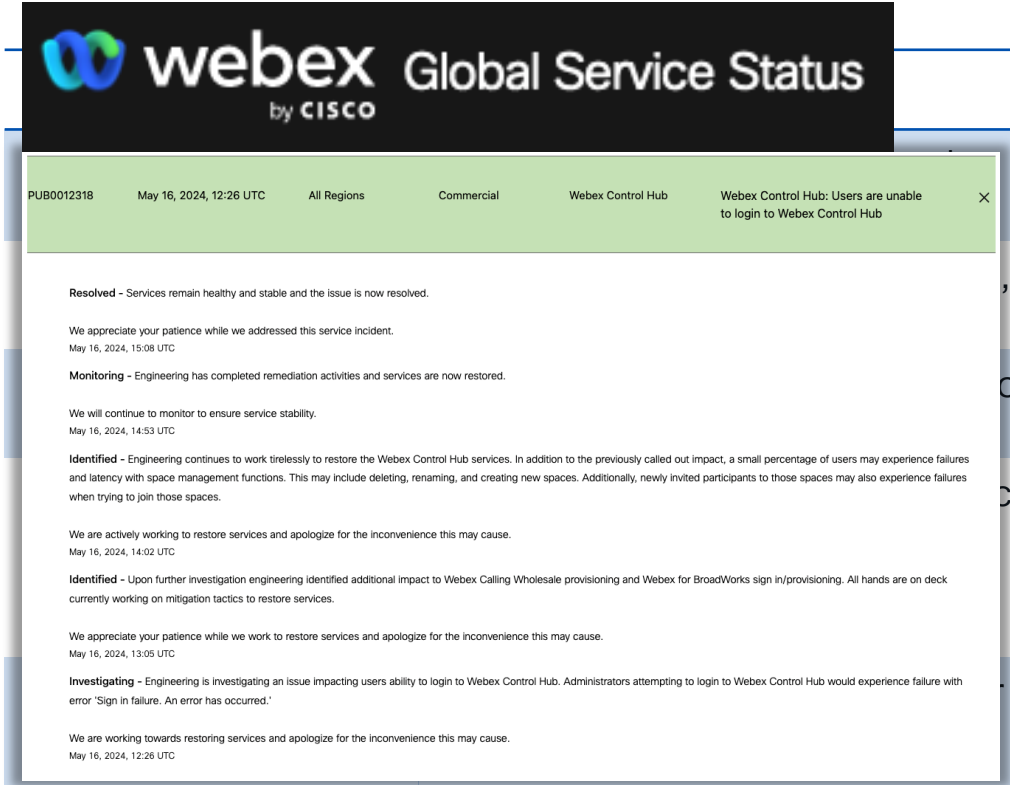
Common HTTP Responses

Code	Definition	Example
1xx – Info Response	The request was received and understood	100 Continue
2xx – Success	Action was received, understood, and accepted	200 OK 201 Created
3xx – Redirection	Client requires additional action to complete request	302 Found 307 Temporary Redirect
4xx – Client error	Error that is likely caused by the client that is making the request	400 Bad Request 401 Unauthorized 403 Forbidden 404 Not Found 429 Too Many Requests
5xx – Server error	Error that is caused by the server performing the request	500 Internal Server Error 503 Service Unavailable 504 Gateway Timeout

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Common HTTP Responses

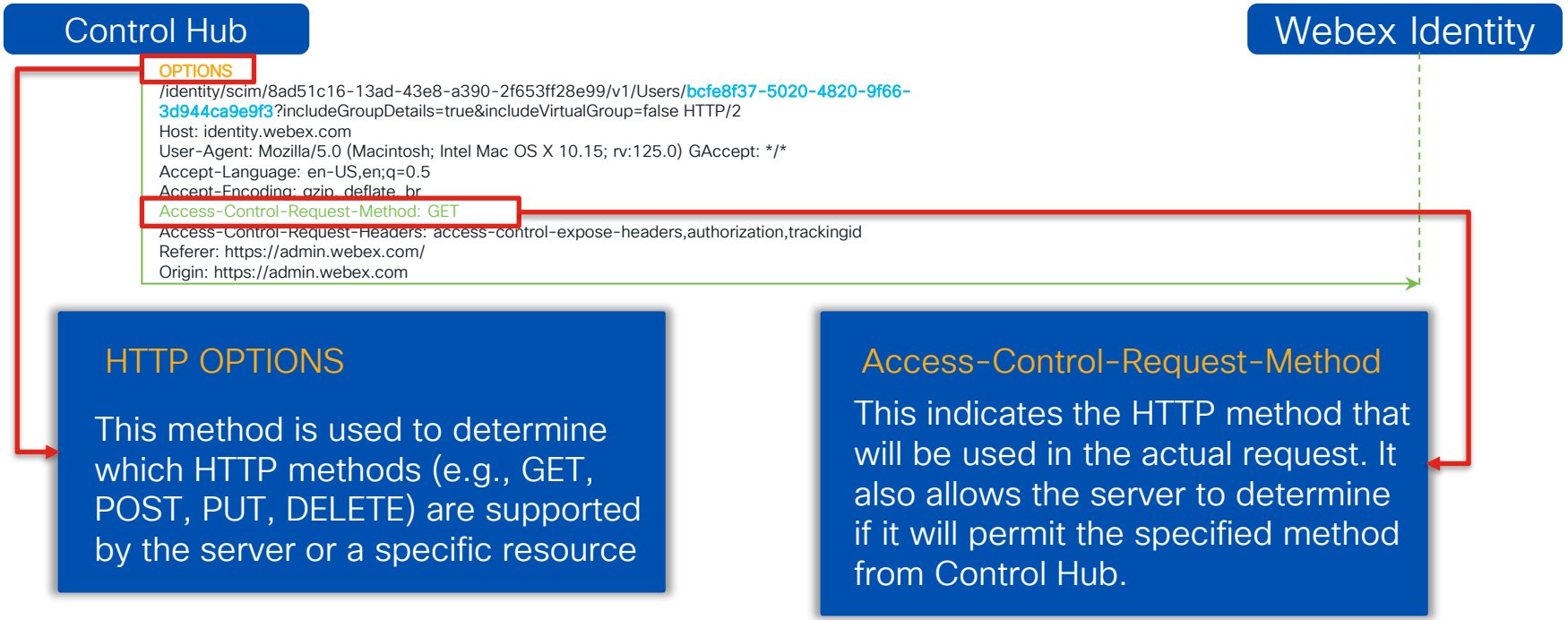
https://status.webex.com



	Example
	100 Continue
, and	200 OK 201 Created
o	302 Found 307 Temporary Redirect
client	400 Bad Request 401 Unauthorized 403 Forbidden 429 Too Many Requests
	500 Internal Server Error 503 Service Unavailable 504 Gateway Timeout

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Web Debugging shows up in Control Hub



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

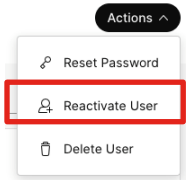
How Web Debugging shows up in Control Hub

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Web Debugging shows up in Control Hub

Control Hub

Webex Identity



Response header

PATCH
/identity/scim/8ad51c16-13ad-43e8-a390-2f653ff28e99/v1/Users/c5f551f5-f116-4ca4-9a67-c3f64c7bd25d HTTP/2
Host: identity.webex.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/json, text/plain, */*
Authorization: Bearer <token>
TrackingID: ATLAS_52ad16f8-6960-4954-be4f-ab4682bbafca_24
Content-Type: application/json
Content-Length: 109

Request body

{"schemas":["urn:scim:schemas:core:1.0","urn:scim:schemas:extension:cisco:commonidentity:1.0"],"active":true}

HTTP/2 200
trackingid: ATLAS_52ad16f8-6960-4954-be4f-ab4682bbafca_24
datacenter: prod-achm
location: https://identity.webex.com/identity/scim/8ad51c16-13ad-43e8-a390-2f653ff28e99/v1/Users/c5f551f5-f116-4ca4-9a67-c3f64c7bd25d
content-type: application/json;charset=UTF-8
date: Wed, 24 Apr 2024 18:15:15 GMT

{"schemas":["urn:scim:schemas:core:1.0","urn:scim:schemas:extension:cisco:commonidentity:1.0"],"userName":"freeuser@thestoj.com","emails":[{"primary":true,"type":"work","value":"freeuser@thestoj.com"}],"name":{"givenName":"Paul","familyName":"Stojanovski"},"entitlements":["spark-test-account","basic-meeting","basic-message","cloudmeetings","screen-share","spark","squared-call-initiation","webex-squared"],"cisSyncSource":"SCIM","userStatus":"active","id":"c5f551f5-f116-4ca4-9a67-c3f64c7bd25d","meta":{"created":"2023-12-22T13:51:08.338Z","lastModified":"2024-04-24T18:15:15.043Z","lastLoginTime":"2024-03-12T20:11:57.726Z","version":"W/\"14987552451\"","location":"https://identity.webex.com/identity/scim/8ad51c16-13ad-43e8-a390-2f653ff28e99/v1/Users/c5f551f5-f116-4ca4-9a67-c3f64c7bd25d","organizationID":"8ad51c16-13ad-43e8-a390-2f653ff28e99","userClaimTime":"2023-12-22T13:51:07.875Z"},"displayName":"Paul Stojanovski","active":true,"accountStatus":["active"],"licenseID":["WXSFREE_c1f9f2e1-b4ae-41bd-b405-2634a46b930e_ciscolivecx-converged.webex.com"sipAddresses":[{"type":"cloud-calling","value":"freeuser@ciscolive.calls.webex.com","primary":true}],"trainSiteNames":["ciscolivecx-converged.webex.com","userType":"user","sensitive":false}

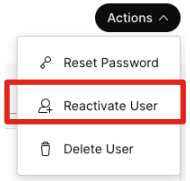
200 OK

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Web Debugging shows up in Control Hub

Control Hub

Webex Identity



Response header

```
PATCH
/identity/scim/8ad51c16-13ad-43e8-a390-2f653ff28e99/v1/Users/c5f551f5-f116-4ca4-9a67-c3f64c7bd25d HTTP/2
Host: identity.webex.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/json, text/plain, */*
Authorization: Bearer <token>
TrackingID: ATLAS_52ad16f8-6960-4954-be4f-ab4682bbafca_24
Content-Type: application/json
Content-Length: 109

{"schemas":["urn:scim:schemas:core:1.0","urn:scim:schemas:extension:cisco:commonidentity:1.0"],"active":true}
```

Webex Identity – Active state

Determines if the user is Active or Inactive in Control Hub.

PATCH (RFC 5789 – Patch Method for HTTP)

- Used when making an update to an existing resource
- No values are being completely replaced or removed

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Web Debugging shows up in Control Hub

Control Hub

License Service

Request header

POST
/license/api/v1/organization/8ad51c16-13ad-43e8-a390-2f653ff28e99/users/onboard HTTP/2
Host: license-a.wbx2.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/json, text/plain, */*
Authorization: Bearer <token>
Access-Control-Expose-Headers: TrackingID
Content-Type: application/json
Content-Length: 535

Request body

[{"email":"demo_user@thestoj.com","licenses":[id":"EE_a8e7d08d-5966-46c7-a1c2-e4173b0e0f78_ciscolivecx.webex.com","idOperation":"ADD","properties":{}}],"extendedSiteAccounts":[],"onboardMethod":"MANUAL","name":{"givenName":"Demo","familyName":"User"},"displayName":"Demo User","entitlements":[]}]

HTTP/2 200
vary: origin,accept-encoding
access-control-allow-origin: https://admin.webex.com
access-control-allow-credentials: true
access-control-expose-headers: TrackingId, Link, Retry-After
timing-allow-origin: https://admin.webex.com
x-content-type-options: nosniff
trackingid: ATLAS_acc3db0d-0181-4a6d-914c-90678e88018b_44
content-encoding: gzip
content-type: application/json
date: Tue, 21 May 2024 17:05:56 GMT

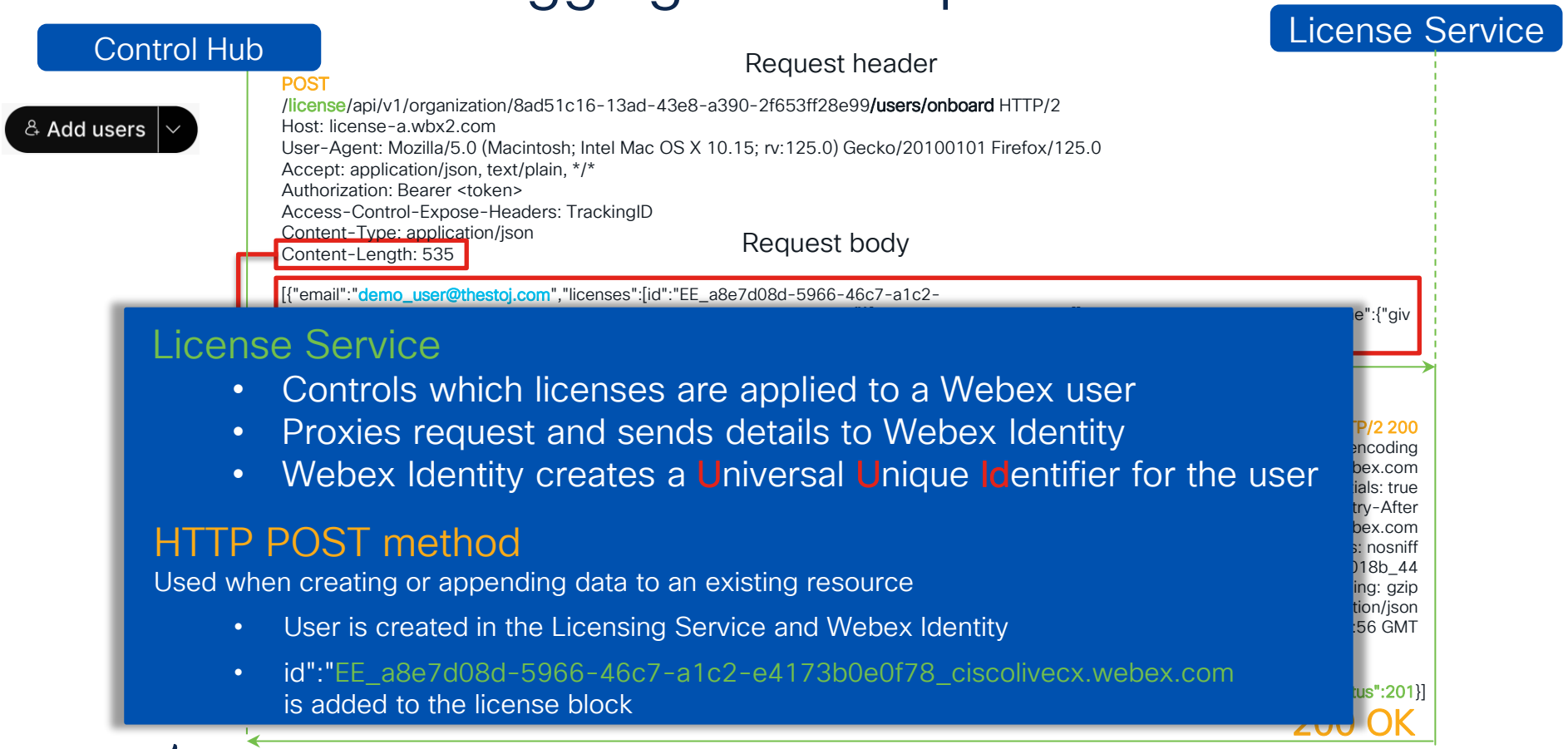
Response body

[{"email":"demo_user@thestoj.com","uuid":"a9605af8-169b-485e-8f6c-4a5caef07a21","status":201}]

200 OK

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Web Debugging shows up in Control Hub



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Hub – Network Issues

Yes, blame it on the network!

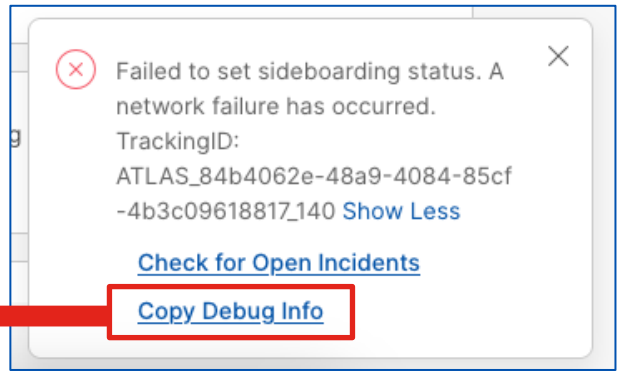
- **Status 0** indicates a network failure occurred when making an HTTP Request to Control Hub
- Common causes is network connection failure (ex: loss of Wi-Fi), proxy blocking traffic, outbound routing

Troubleshoot must begin by debugging common network failures

Referrer: Control Hub notification toaster-links
Browser URL: https://admin.webex.com/settings
Control Hub Build: 20240423-46f592f
View Org ID: 8ad51c16-13ad-43e8-a390-2f653ff28e99
Logged-in User ID: bcfe8f37-5020-4820-9f66-3d944ca9e9f3
Logged-in User Org ID: 8ad51c16-13ad-43e8-a390-2f653ff28e99
Logged-in User Clock UTC: Tue, 30 Apr 2024 18:11:11 GMT
Customer Type: Enterprise

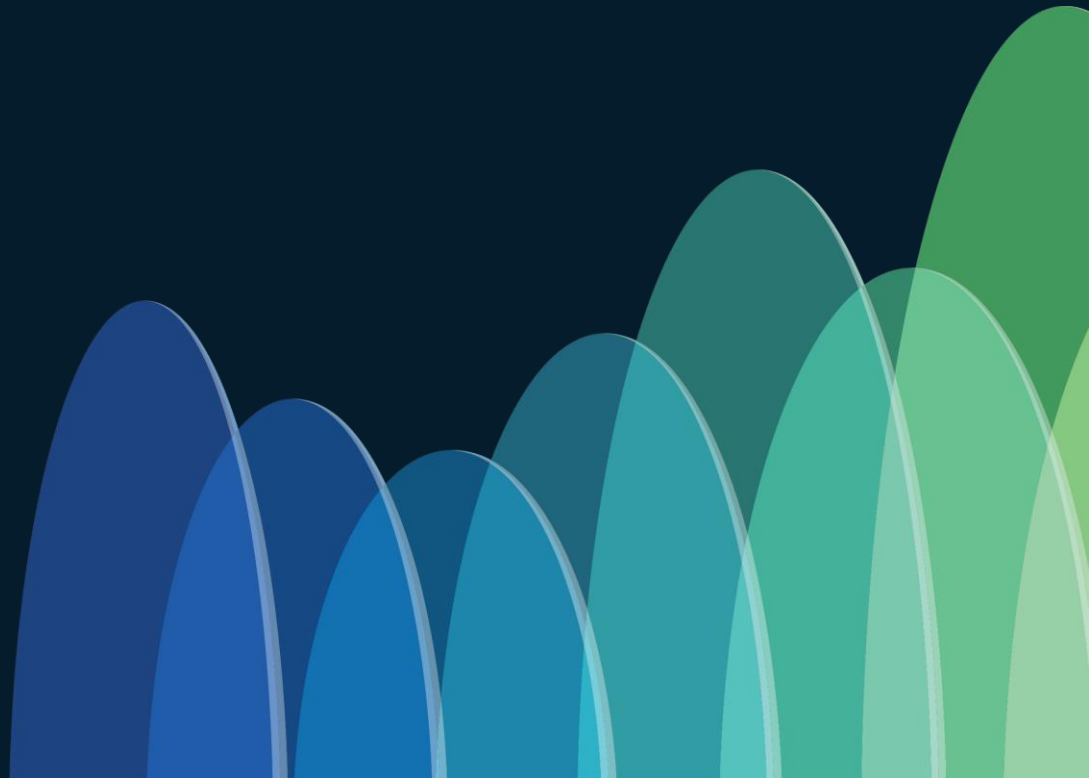
Status: 0
Status Text: Unknown Error
URL: https://atlas-a.wbx2.com/admin/api/v1/organizations/8ad51c16-13ad-43e8-a390-2f653ff28e99?selfSubscribe=false
Tracking ID: ATLAS_84b4062e-48a9-4084-85cf-4b3c09618817_140
Error: {
  "isTrusted": true
}

Message: Failed to set sideboarding status. A network failure has occurred.
TrackingID: ATLAS_84b4062e-48a9-4084-85cf-4b3c09618817_140



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting User Provisioning



cisco Live!

Why is this topic so important?

First impressions are critical.... especially for user adoption

What percentage of Control Hub-related TAC cases does user management account for?

What is Cisco's most common Google-search related to technical issues?

50-55%

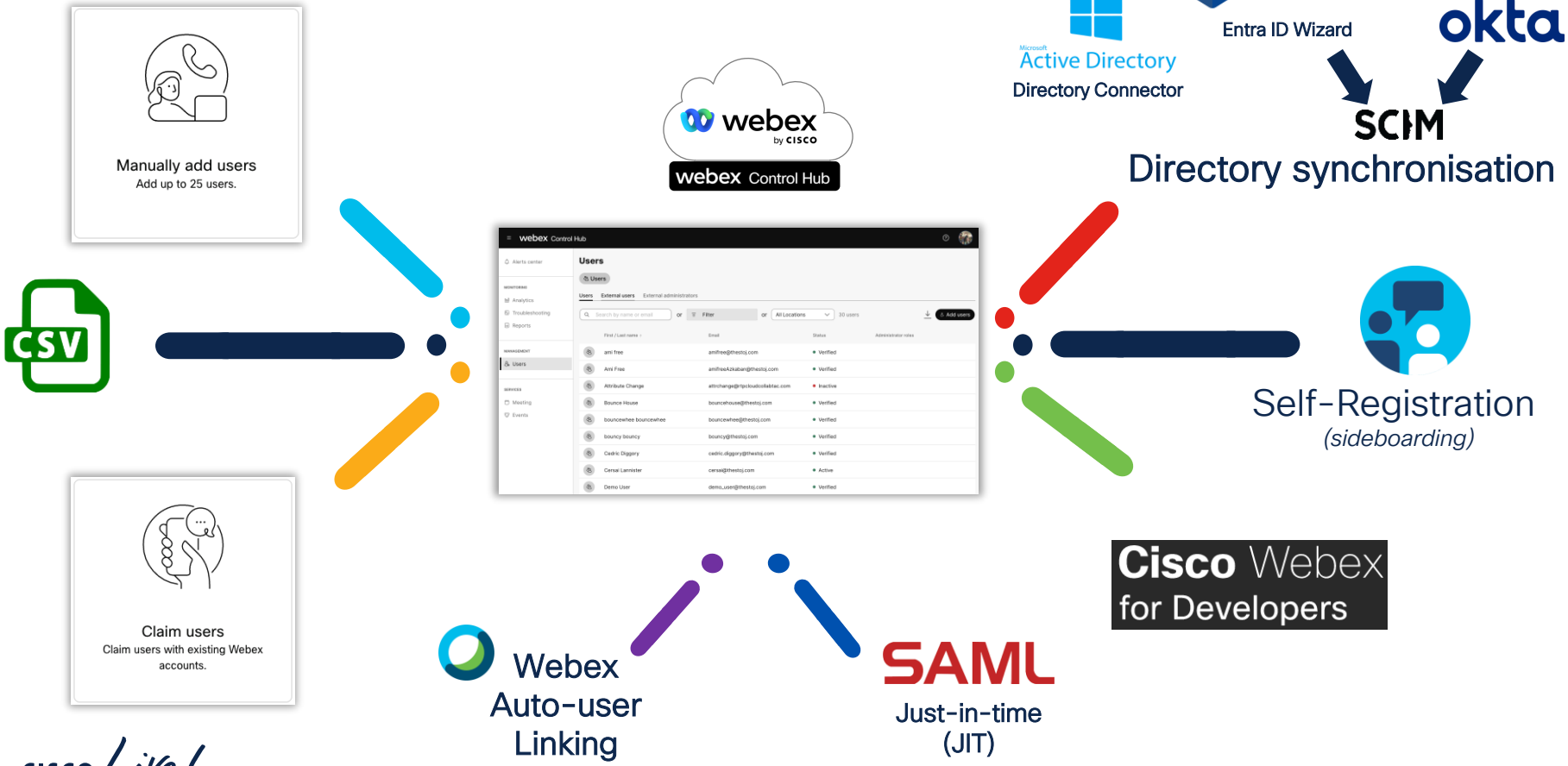
Unable to login to Webex

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Direct Provisioning

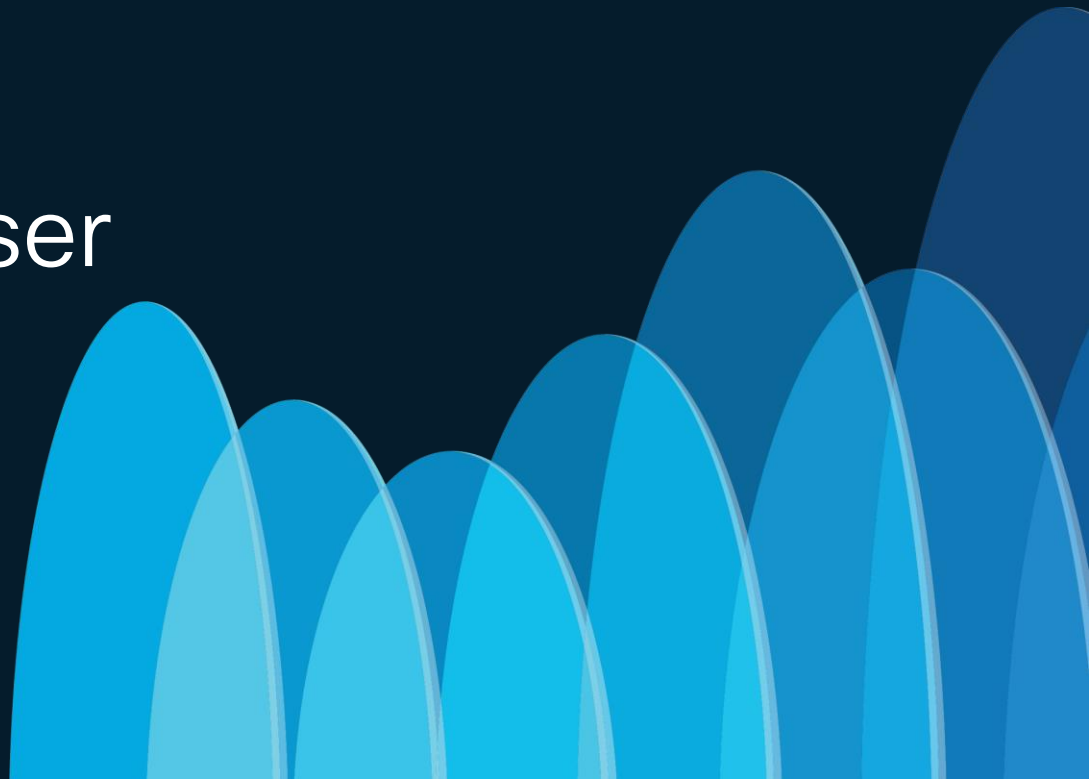
cisco Live!

Control Hub User Add Methods



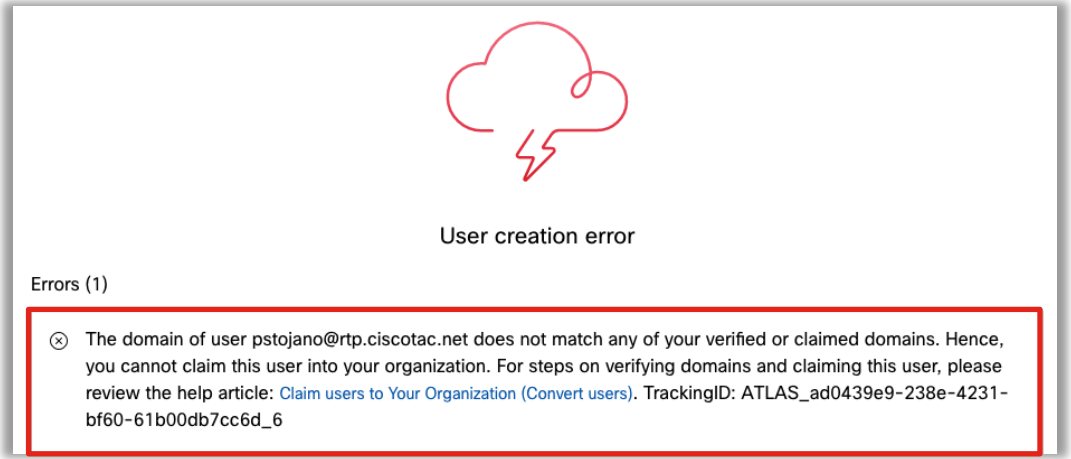
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unable to add user



Unable to Add User

- By far the **largest** “add user error” issue **observed in TAC**
- Nearly **half of all TAC user management cases** are due to this condition



Error is triggered when the user exists in Webex Identity outside of your organisation AND your organisation does not have the email domain verified

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Understanding the add user logic

Webex Admin

Action: Add user

pstojano@rtp.ciscotac.net

User Found
Domain not verified

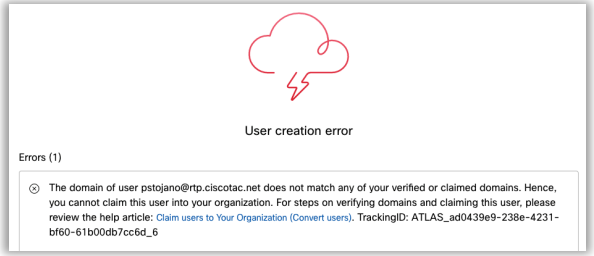
webex by CISCO

webex Control Hub

Check Webex Identity for existing user

user1@thestoj.com
user2@thestoj.com
user3@thestoj.com

Verified Domain:
thestoj.com



webex by CISCO
Enterprise Org

webex by CISCO
Webex.com Org

webex by CISCO
Webex Free Org

pstojano@rtp.ciscotac.net

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Looking beyond Control Hub Provisioning

Active Directory

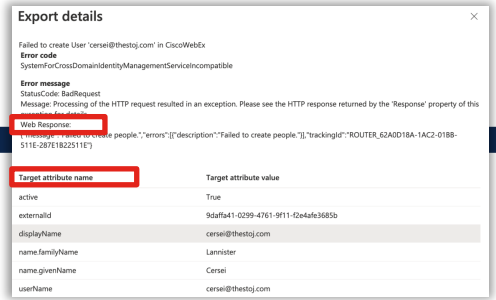
Directory Connector

Windows Event Logs / Sync Report

[sessionId: 608d0e38-d3fb-41f1-ad20-81233b98b365] There is a naming conflicts for CN=Test User,OU=IT,OU=Winterfell,DC=rtpcloudcollabtac,DC=com with an existing cloud entry with name testuser@rtpcloudcollabtac.com of type user. See https://cisco.com/go/troubleshoot-directory-connector#reference_DCB41087FC7309F241284A1424D9695B

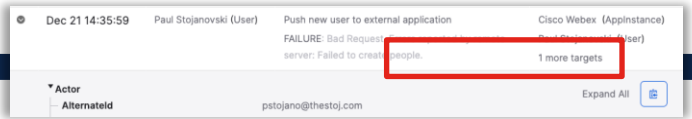
webex by CISCO

Microsoft Entra ID



webex by CISCO

okta



webex by CISCO

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Add User Remediation

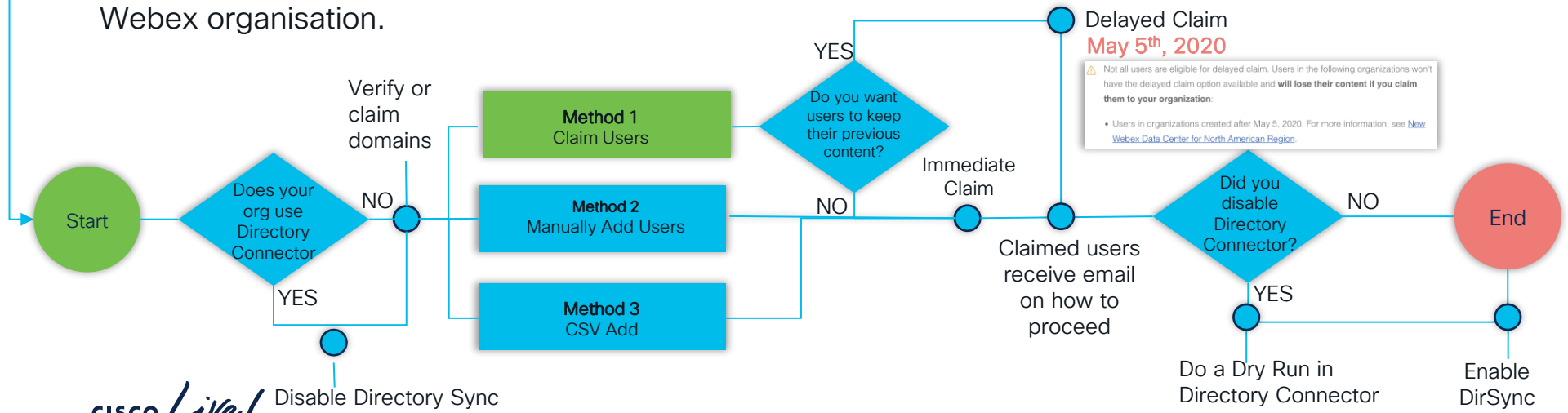
If user exists in a Webex Enterprise or Webex.com organisation the admin of the org must delete them.

1. Verify your domain (Webex best practice)

By verifying your domain, you will be allowed to claim (add) any users who have signed up for a Webex account with your company email domain outside of your Webex organisation.

2. Delete the free user -> settings.webex.com

We do not recommend this approach because there could be additional users you want to add who use your company email domain and have signed up for a Webex account outside of your Webex organisation.

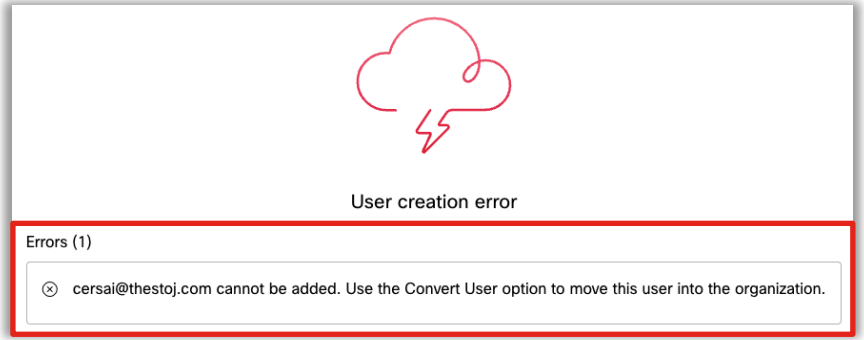


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Factors that impact ability to claim users

There are several Webex organisation configurations that could prevent a user from being added **despite your Webex organisation having a** verified domain.

1. Directory Connector enabled
2. The Webex organisation has the same domain verified
3. Single Sign-On enabled

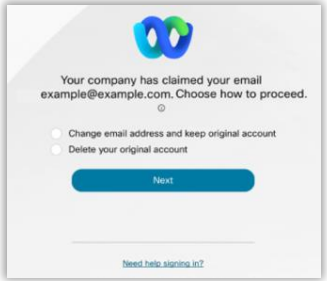


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

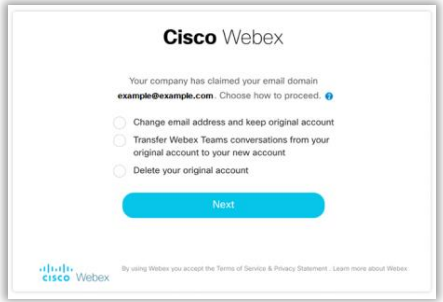
User Claim FAQ

- Do claimed users consume a license?
  - Yes
- Can you undo/retract a user claim?
  - Yes, if the user has not signed in and 14 days have not passed.
- Can the organisation that I'm claiming a user from retract a claim that my organisation made?
  - No, only the organisation that initiated the claiming process can retract the claim.
- Do all claimed users show up as Active in my organization?
  - Claimed users match the status they had in their previous organisation. For example, if a user was Not Verified in their previous organisation, then they'll show up as Not Verified when claimed in your organisation.
- What is the experience for a claimed user?

IMMEDIATE



DELAYED



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Immediate User Claim Process Flow

1 User creates a Free account

username: pleasesaveme@thestoj.com

id: 6e6be6ae-64b1-42d8-83f2-3032ee601875

created: 2021-10-11T15:27:32.885Z

orgId: a2846766-4793-4366-afe1-303099abecc2

orgName: Webex Free Org

2 Enterprise admin claims Free user

From Control Hub

- Add Users > Claim users

This process kicks off two events described in 3a & 3b

3b New user created in Enterprise org

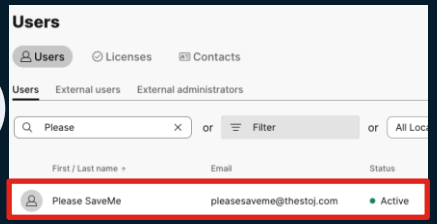
userName: pleasesaveme@thestoj.com

id: 071467f9-51ab-474e-a09c-d627e899079b

created: 2024-05-01T14:42:34.718Z

organizationID: 8ad51c16-13ad-43e8-a390-2f653ff28e99

accountStatus: active



3a Free user email remapped

New email: pleasesaveme@thestoj.com.convert-user.local

Old email: pleasesaveme@thestoj.com

id: 6e6be6ae-64b1-42d8-83f2-3032ee601875

created: 2021-10-11T15:27:32.885Z

orgId: a2846766-4793-4366-afe1-303099abecc2

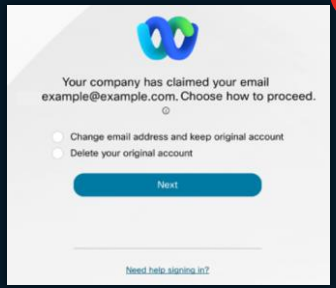
orgName: Webex Free Org

accountStatus: pending

4 Free user attempts to login

Free user must act and choose:

1) **Change email to personal address**
2) Delete free account



5 Email changed to personal

1) Free user logs in with personal address
2) All message history preserved

username: personal_email@gmail.com

id: 6e6be6ae-64b1-42d8-83f2-3032ee601875

created: 2021-10-11T15:27:32.885Z

orgId: a2846766-4793-4366-afe1-303099abecc2

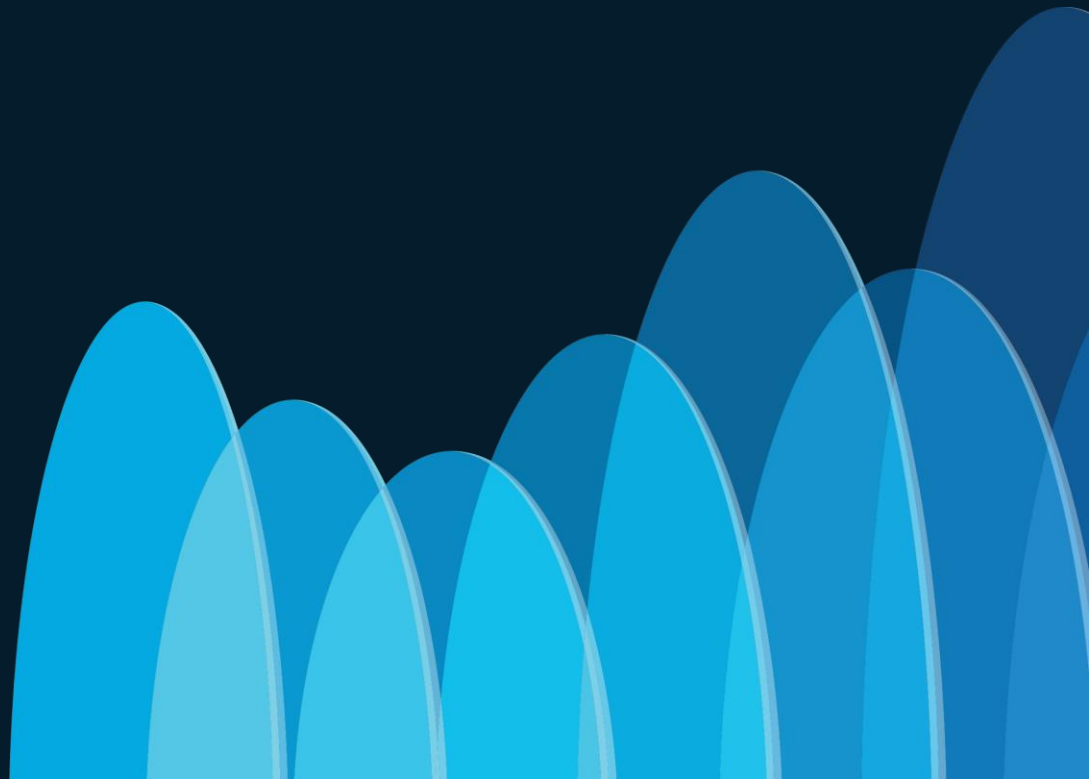
orgName: Webex Free Org

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

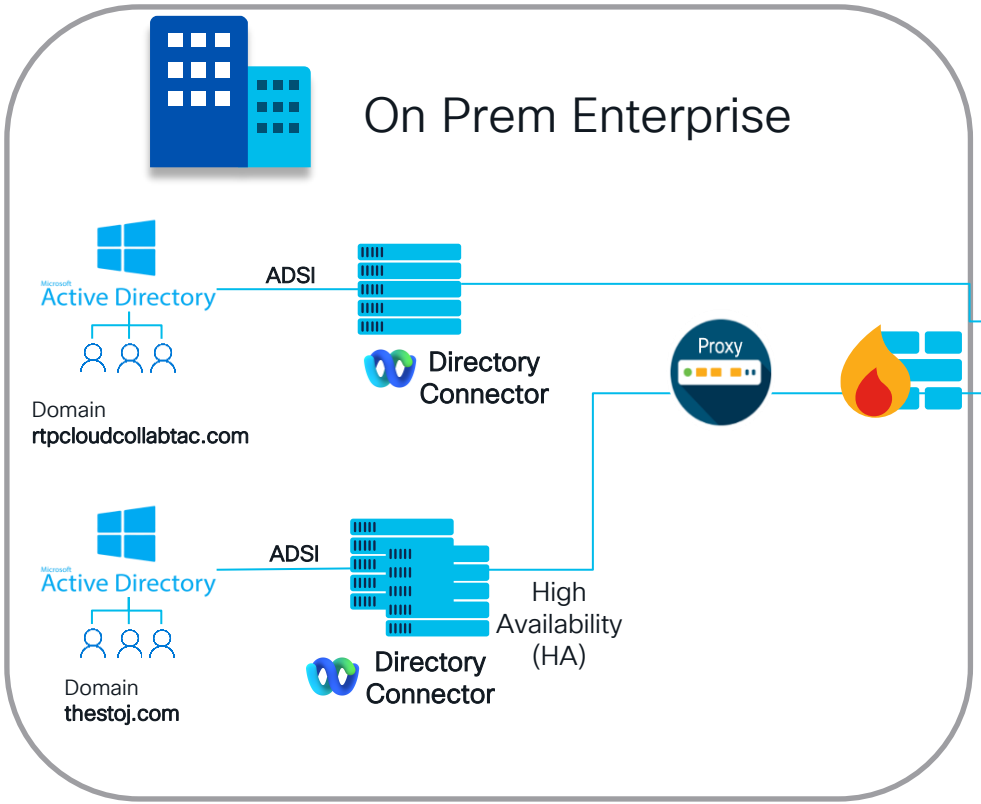
Troubleshooting Directory Connector Provisioning

cisco Live!

Overview



Architecture Overview



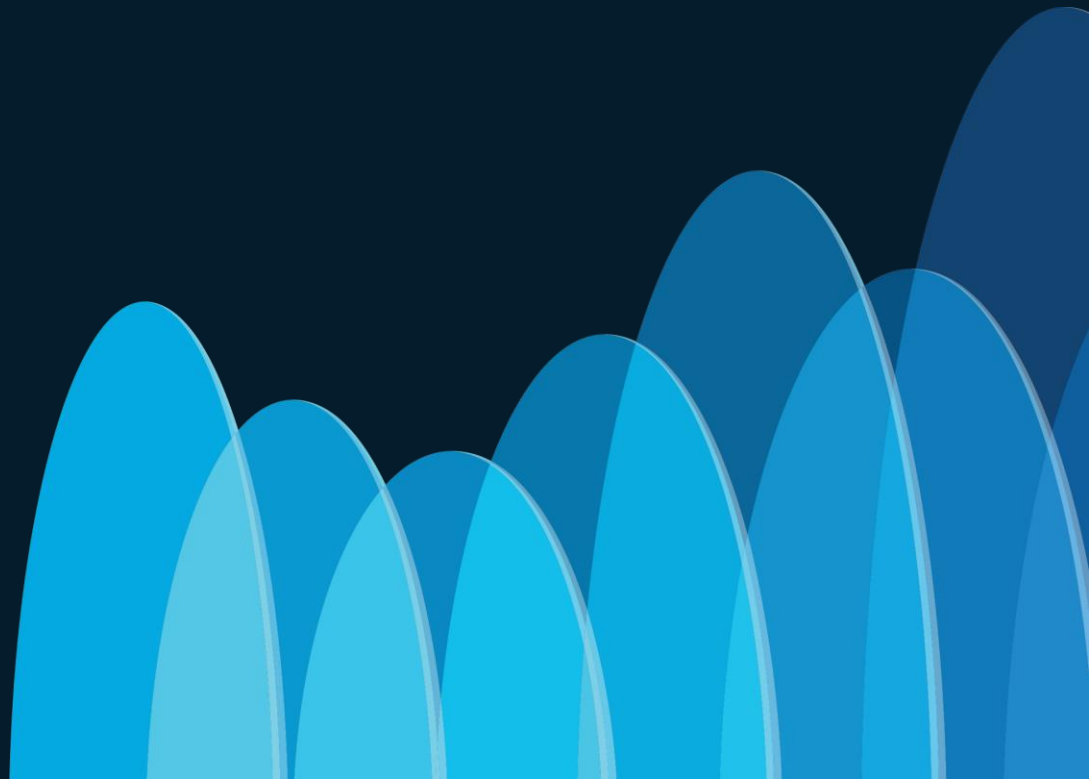
Additional considerations:

- Directory Connector is supported on 2012 R2, 2012, 2008 R2 and 2003 Windows Server 2022, 2019, 2016,
- Directory Connector traffic can route through a proxy & will use default system proxy settings.
- When Directory Connector is enabled, it is the **single source of truth** for user provisioning and no other user provisioning will work.

Note: URL can change depending on your Webex org cluster location
ex: idbroker-b-us.webex.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tools & Log Collection



Understanding your toolbox

Microsoft Entra ID

Easy

Ease of understanding

Difficult

Reports

- Sync Dry Run
- Synchronisation Reports

Tools

- Directory Connector Diagnostic Tool

Logs

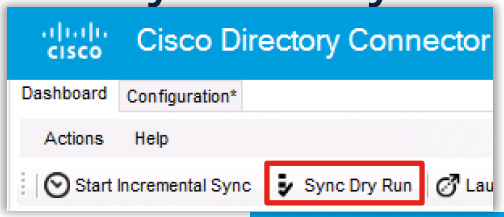
- Directory Connector logs

  <Install_DIR>\Cisco Systems\Cisco Directory Connector\Logs

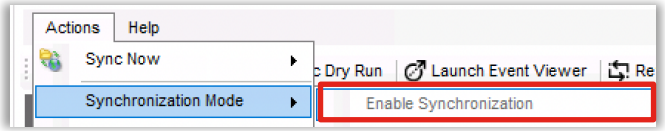
- Windows Event logs

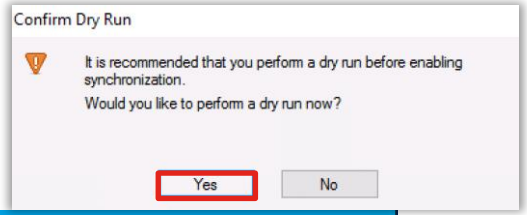
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

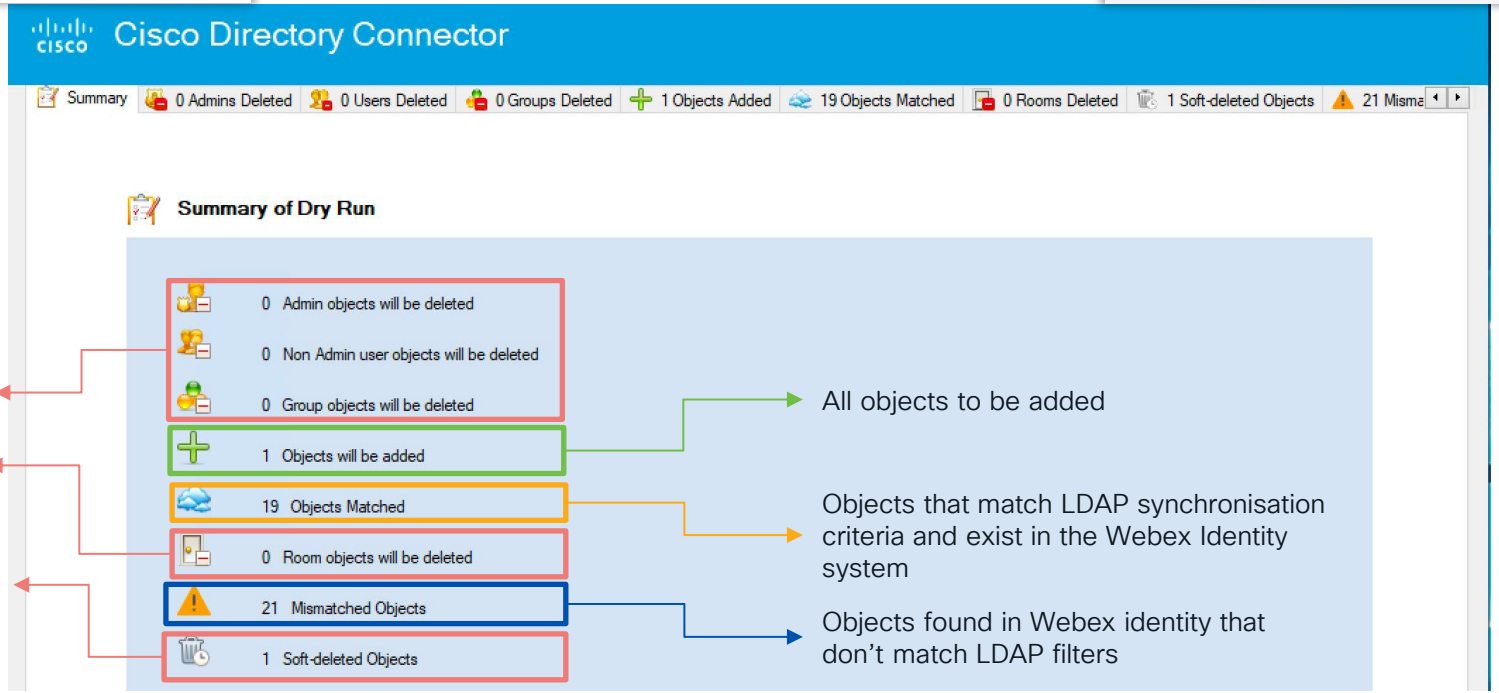
Sync Dry Run: Analysing



OR







Displays Users, Admins, Groups, and Rooms that will be deleted

Provides a mechanism to permanently delete users immediately

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reasons why a user is inactive

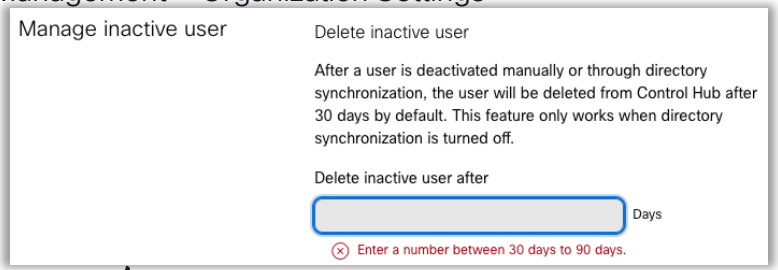
Source	Reason	Retention
Control Hub	Administratively deactivated	30 days
Control Hub	Claimed into organisation and does not match a Directory synchronisation LDAP filter (Directory Connector)	30 days
Site Admin	User created via auto user linking and user was deactivated in Site Administration	30 days
Directory Connector	Administratively deactivated in Active Directory *Applies to other SCIM integration (Okta/Azure) deactivate actions as well*	Indefinite
Directory Connector	Originally synced and no longer included in the Directory synchronisation filter	7 days

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Customizing User Inactive Duration

Source	Reason	Retention
Control Hub	Administratively deactivated	30 days
Control Hub	Claimed into organization and does not match a Directory synchronization LDAP filter (Directory Connector)	30 days
Site Admin	User created via auto user linking and user was deactivated in Site Administration	30 days

Management > Organization Settings

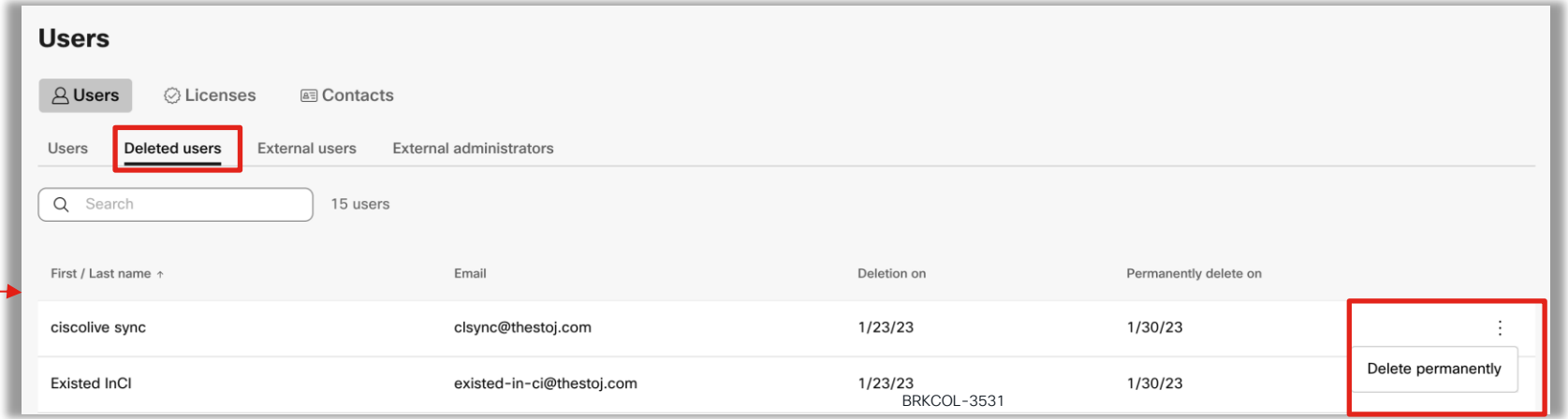


Non-Directory Connector provisioned users can now be retained for up to 90 days

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

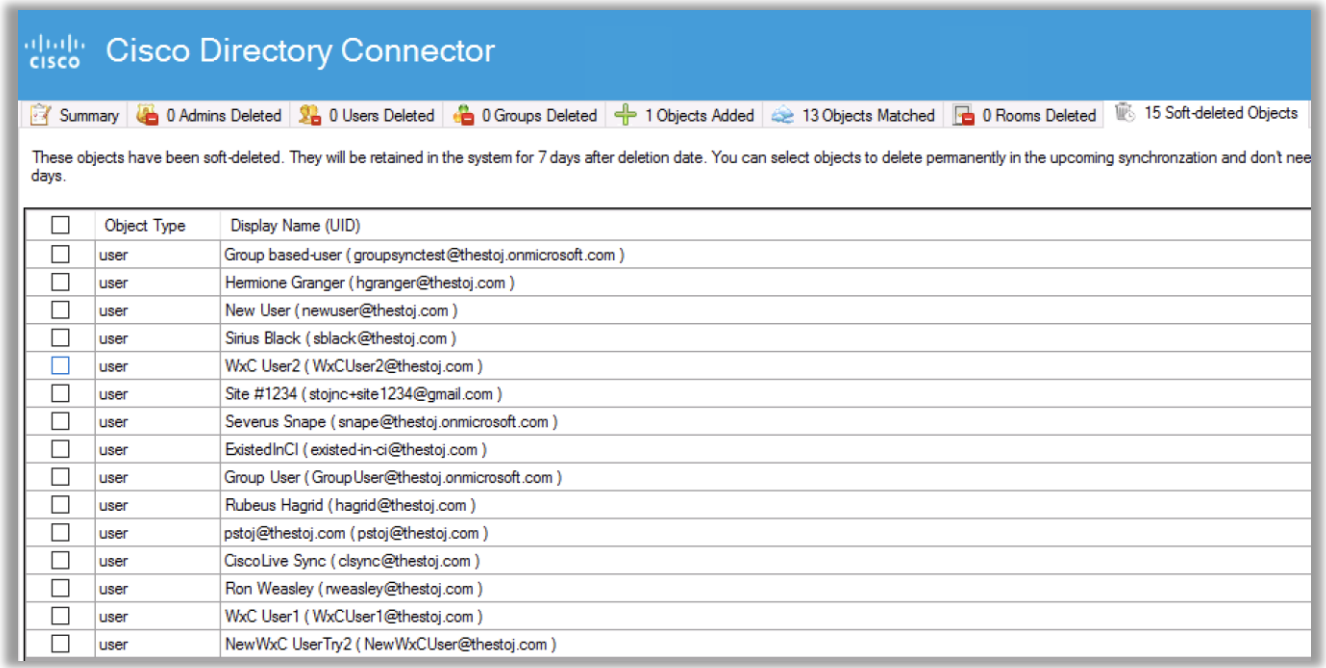
Control Hub: Soft-deleted AD synced

- Existing Control Hub users not matching an LDAP filter/OU are marked as **Inactive**
- These users remain in an Inactive state for **7 days** then are purged
  - This timeframe is not configurable
- Delete users feature allows you to permanently delete Inactive users



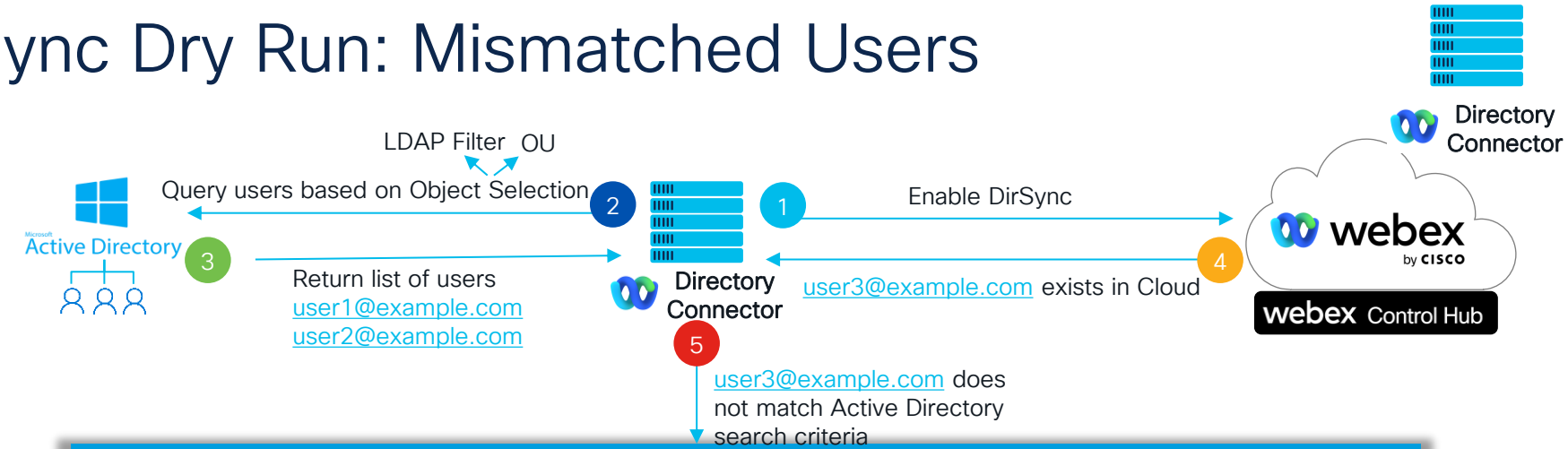
Directory Connector: Soft-deleted AD synced

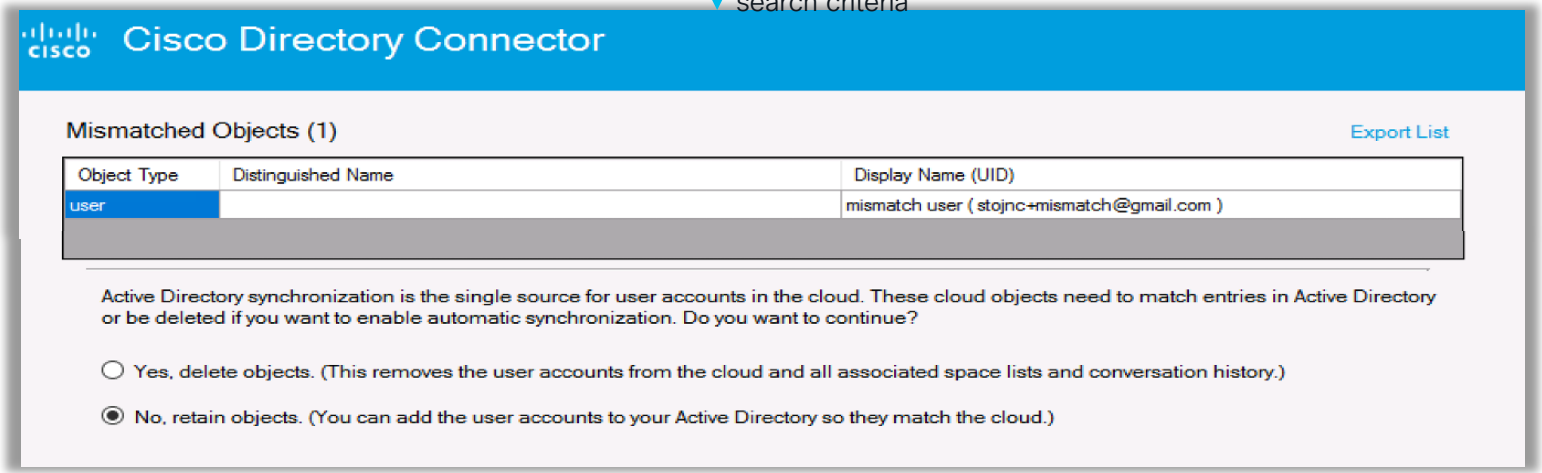
- Select users to be purged
- Deletion occurs upon next sync
- You may force sync by choosing Incremental or Full sync



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Sync Dry Run: Mismatched Users

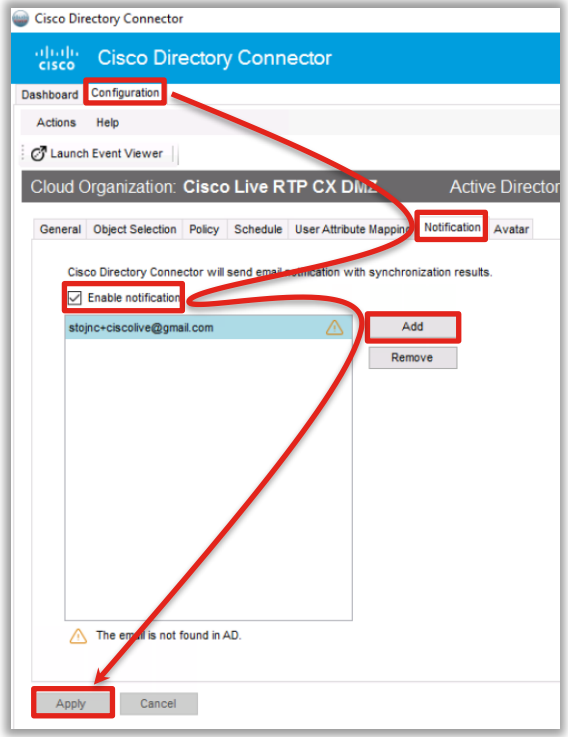




© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Synchronization Report

CONFIG



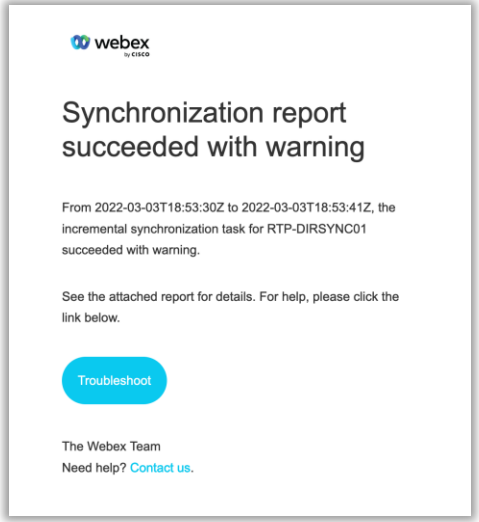
OUTPUT

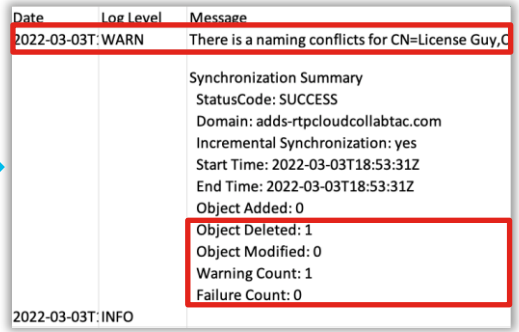
from: noreply@cisco.com

to: your_email@domain.com

date: Mar 3, 2022, 1:53 PM

subject: Synchronization Report for **Cisco Live RTP CX DMZ**: Task Succeeded with Warning

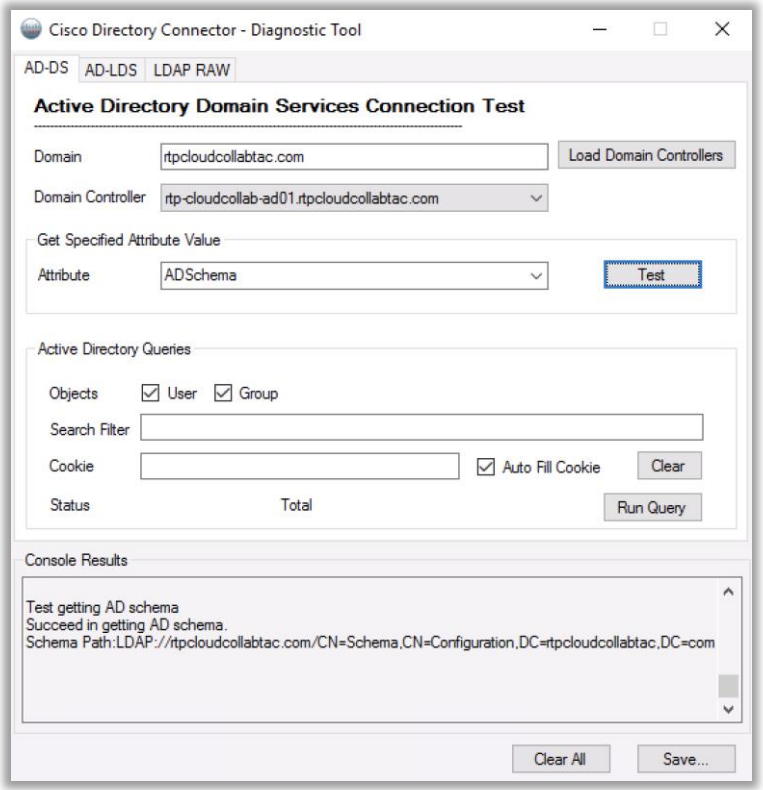




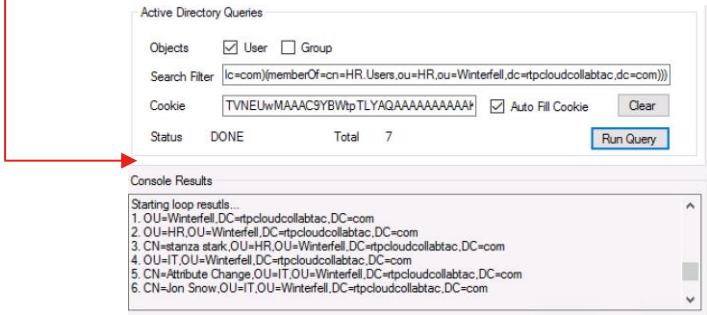
Note: Report sent every 4 hours when an issue is detected.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Directory Connector Diagnostic Tool



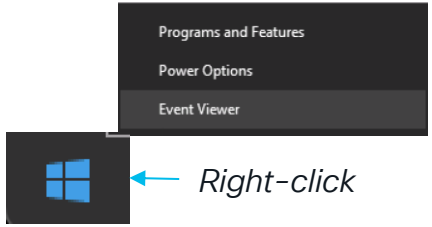
- Available after Directory Connector 3.4
- Bundled with install
- Supports AD-DS, AD-LDS, LDAP RAW
- Capable of testing:
  - LDAP Connection
  - LDAP User / Group filters



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Logging Options

Windows Event Logs



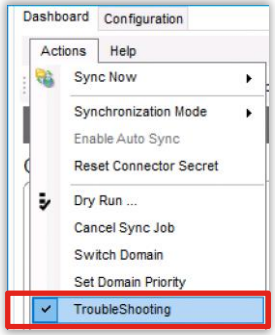
Data location

Right-click

Directory Connector Local Logging

<Install_DIR>\Cisco Systems\Cisco Directory Connector\Logs

- EventLog.DirSyncService.exe
- Network.DirSyncService.exe
- EventLog.CloudConnectorManager.exe
- Network.CloudConnectorManager.exe



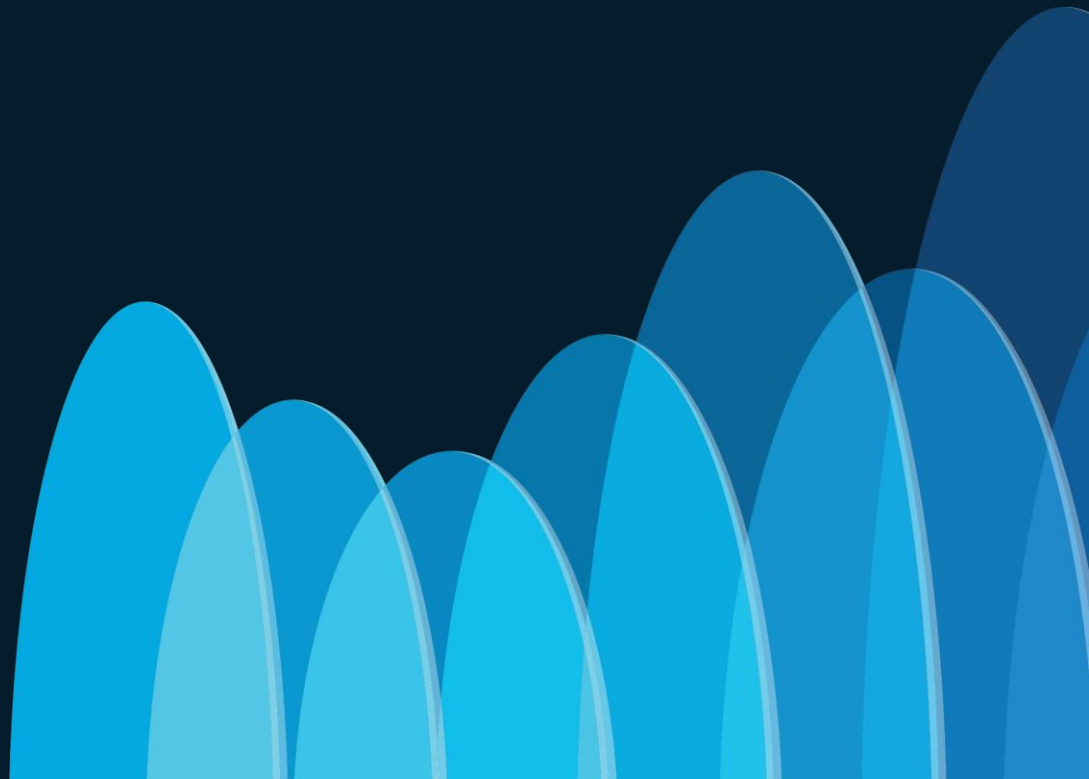
Enabled by default	✓	✗
High-level sync errors	✓	✓ EventLog.DirSyncService.exe
HTTPS communication	✗	✓ Network.DirSyncService.exe Network.CloudConnectorManager.exe
Includes sync communication detail	✗	✓ EventLog.DirSyncService.exe

[DirSyncWorker ReportEvent] ServiceMessage:
taskId: 46a5d9c1-24cd-4b40-941a-f0e5905d4c74
attribute: preferredLanguage groupType telephoneNumber mail displayName postalCode description title objectclass employeeNumber objectguid objectGUID member sn userAccountControl st physicalDeliveryOfficeName c manager ou givenName mobile facsimileTelephoneNumber cn l o employeeType streetAddress departmentNumber
base: dc=rtpcloudcollabtac,dc=com
filter:
(|(&(objectClass=Group)(!(isCriticalSystemObject=TRUE))((&(objectclass=Group)(|(cn=IT Users)(cn=HR.Users)(cn=Finance Users)))))(&(objectClass=User)(!(ObjectClass=Computer))((&(objectClass=person)(|(memberOf=cn="IT Users",ou=IT,ou=Winterfell,dc=rtpcloudcollabtac,dc=com)(memberOf=cn=HR.Users,ou=HR,ou=Winterfell,dc=rtpcloudcollabtac,dc=com))))))
deleteThreshold: 20
syncBases: OU=Winterfell,DC=rtpcloudcollabtac,DC=com
preferredHost: rtp-cloudcollab-ad01.rtpcloudcollabtac.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Common Issues

What drives TAC cases



Top issues observed by TAC

Hidden Slide

Syncing

1. LDAP Filter Issues
2. Mandatory attribute mapping not defined for user in Active Directory
3. User exists in another organisation
4. Duplicate on premise object ID
5. Delete threshold has been triggered
6. User within multiple domains

Login

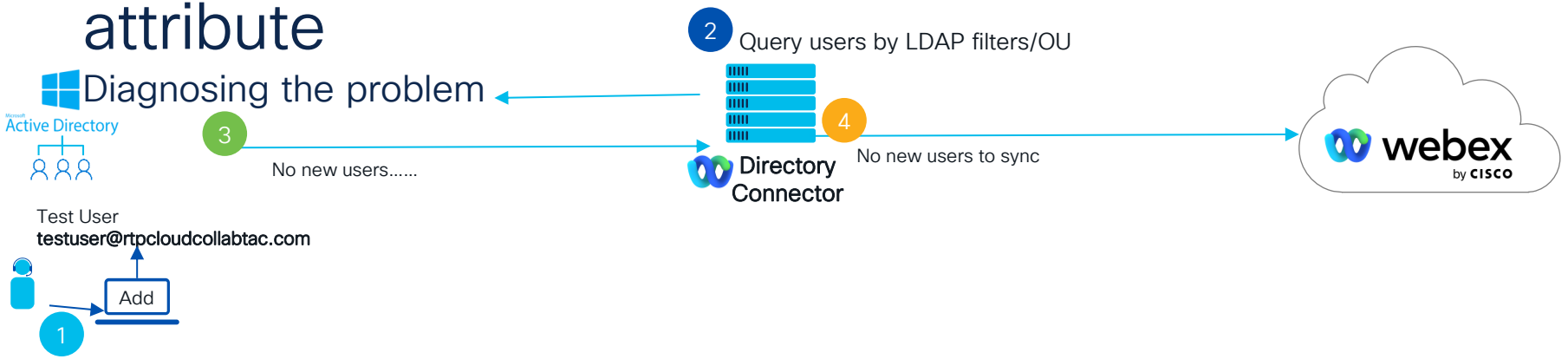
7. Directory Connector page cannot be displayed
8. Webex cloud connection issues

Installation/LDAP Binding

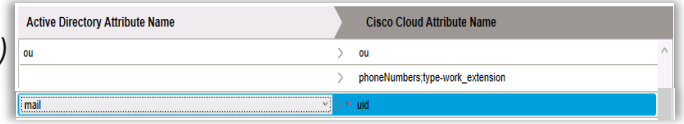
9. .NET Framework not installed
10. No Permission to LDAP

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

1 & 2 LDAP Filters and missing mandatory attribute



1. Verify the required cloud uid attribute you are syncing *(mail, userPrincipleName)*
2. Determine if that value is present in the user's Active Directory configuration
3. Verify if you are syncing based on OUs (On Premise Base DNs), LDAP filters, or both
4. Determine if the user is in the correct OU or matches the LDAP filter *(if applicable)*
5. Use the Directory Connector Diagnostic Tool to check LDAP connectivity and filter logic.



Get-AdUser -Filter 'mail -eq "testuser@rtpcloudcollabtac.com"' -Properties *

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Deconstructing Object Selection

User filter

Allows you to further scope which users you want to consider within your directory structure. It's common to include members who belong to a specific security group.

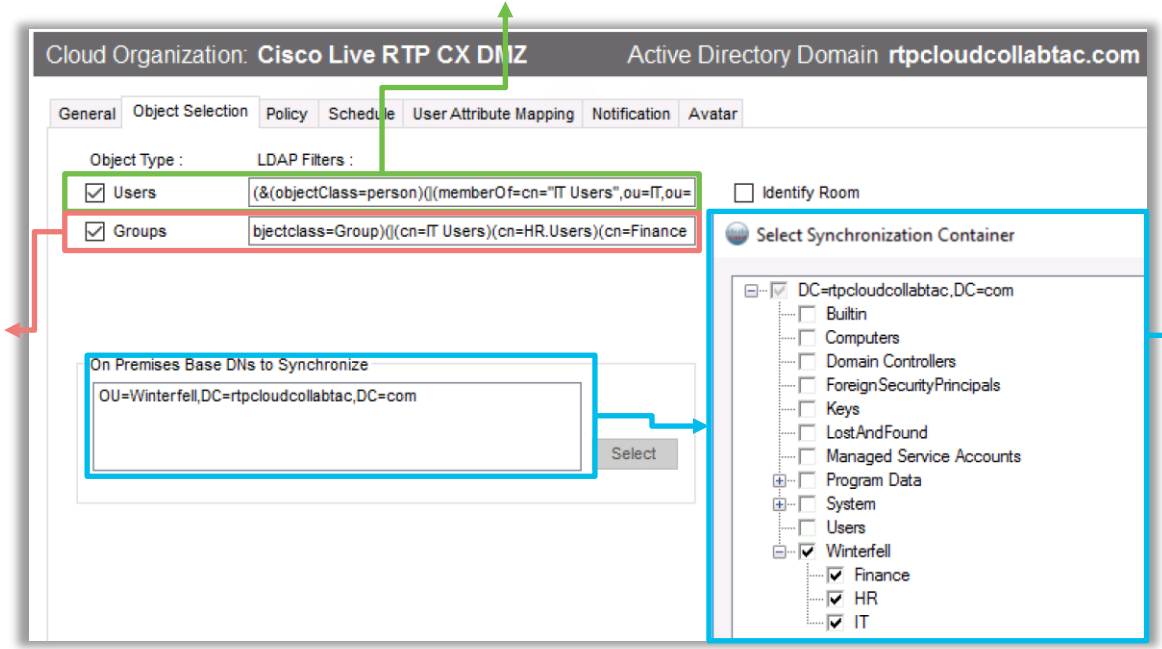
Can be used in conjunction with the On Premises Base DNs to synchronise

Groups filter

Allows you to sync Groups that can be used for **Automatic License Assignment** in Control Hub

Does NOT sync users in the Group

Can be used in conjunction with the On Premises Base DNs to synchronise



On Premises Base DNs to Sync

Allows you to specify which **OUs** should be synced

Optionally you could sync the entire directory and rely on User and Group filtering

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

1 LDAP Filters 101

PowerShell command provides all available user attributes

*Get-AdUser -Filter 'mail -eq "user@example.com"' -Properties **

RFC 4515 – LDAP: String Representation of Search Filters

Search Criteria

Search criteria is not limited to only the table on the right. Full definition of search attributes can be found in RFC 4515.

Criteria Logic	Description	Example
=	Value is equal to…	(mail=user@example.com)
! =	Value is not equal to..	(!(mail=user@example.com))
*	Any value present accepted	(mail=*) or (mail=*@*)
! *	Any value present is not accepted	(!(mail=*))

Operators

Operators are placed at the beginning of the statement and can be nested together.

Operator	Description	Example
&	AND	(&(objectclass=user)(mail=user@example.com))
|	OR	(|(memberOf=cn=IT,ou=users,dc=example,dc=com)(memberOf=cn=HR,ou=users,dc=example,dc=com))
Nested	AND + OR	(|(&(<CriteriaA>)(<CriteriaB>))(&(<CriteriaC>)(CriteriaD>)))

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

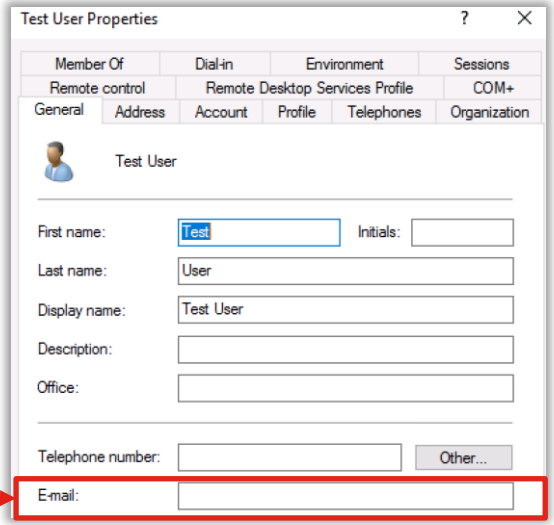
2 Missing required AD Attribute

Windows Event Logs or Synchronisation Report:

[sessionId: ed159bc0-01b5-4e9d-829a-8cdc7fef97e5] Missing naming attribute mail when adding on-premise entry CN=Test User,OU=IT,OU=Winterfell,DC=rtpcloudcollabtac,DC=com. The entry will not be created in the cloud until naming attribute have a value.

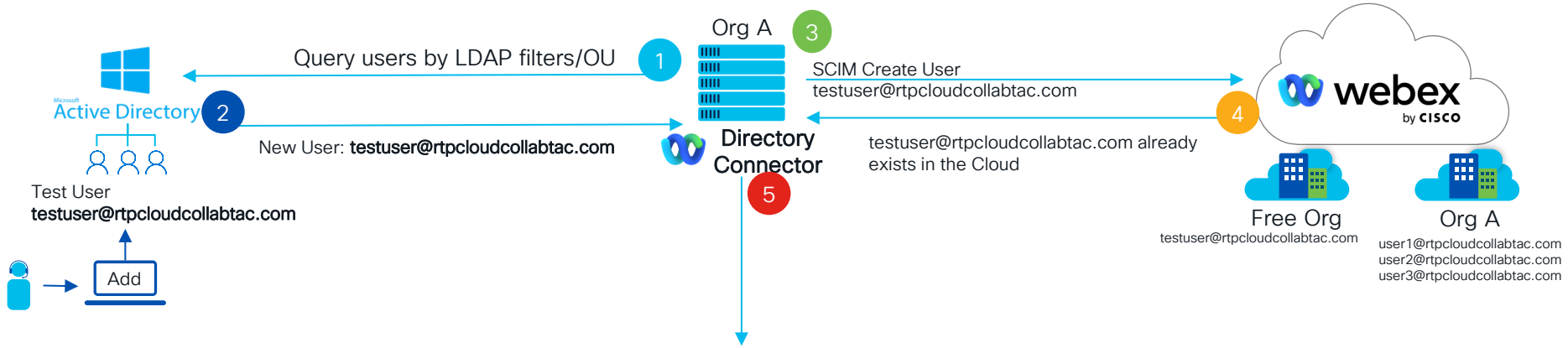
Directory Connector: User Attribute Mapping

Active Directory Attribute Name	Cisco Cloud Attribute Name
ou	ou
	phoneNumbers;type-work_extension
physicalDeliveryOfficeName	physicalDeliveryOfficeName
postalCode	postalCode
preferredLanguage	preferredLanguage
	sipAddresses;type-enterprise
sn	sn
st	st
streetAddress	street
telephoneNumber	telephoneNumber
	timezone
title	title
mail	* uid



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

3 Conflict with existing cloud entry



Windows Event Logs / Sync Report

[sessionId: 608d0e38-d3fb-41f1-ad20-81233b98b365] There is a naming conflicts for CN=Test User,OU=IT,OU=Winterfell,DC=rtpcloudcollabtac,DC=com with an existing cloud entry with name testuser@rtpcloudcollabtac.com of type user. See https://cisco.com/go/troubleshoot-directory-connector#reference_DCB41087FC7309F241284A1424D9695B

Note: In rare circumstances this condition could be met if:
1) *Another Webex organization has claimed the domain of the user you're attempting to add.*
2) *You have deleted and re-created a user account in Active Directory that was already synced to the Cloud.*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

3 Conflict with existing cloud entry

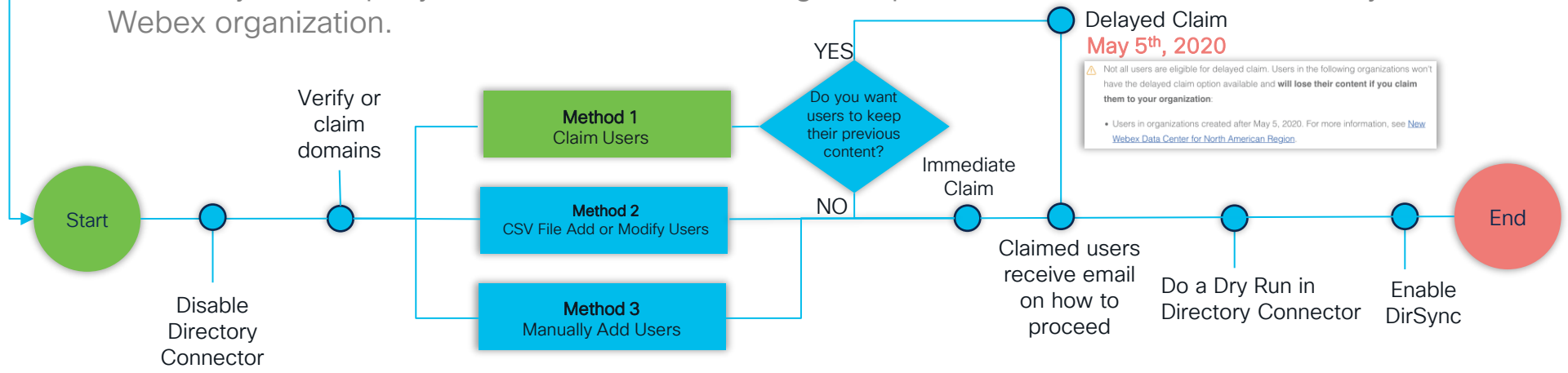
If user exists in a Webex Enterprise or Webex.com organization the admin of the org must delete them.

1. Verify your domain (Webex best practice)

By verifying your domain, you will be allowed to claim (add) any users who have signed up for a Webex account with your company email domain outside of your Webex organization.

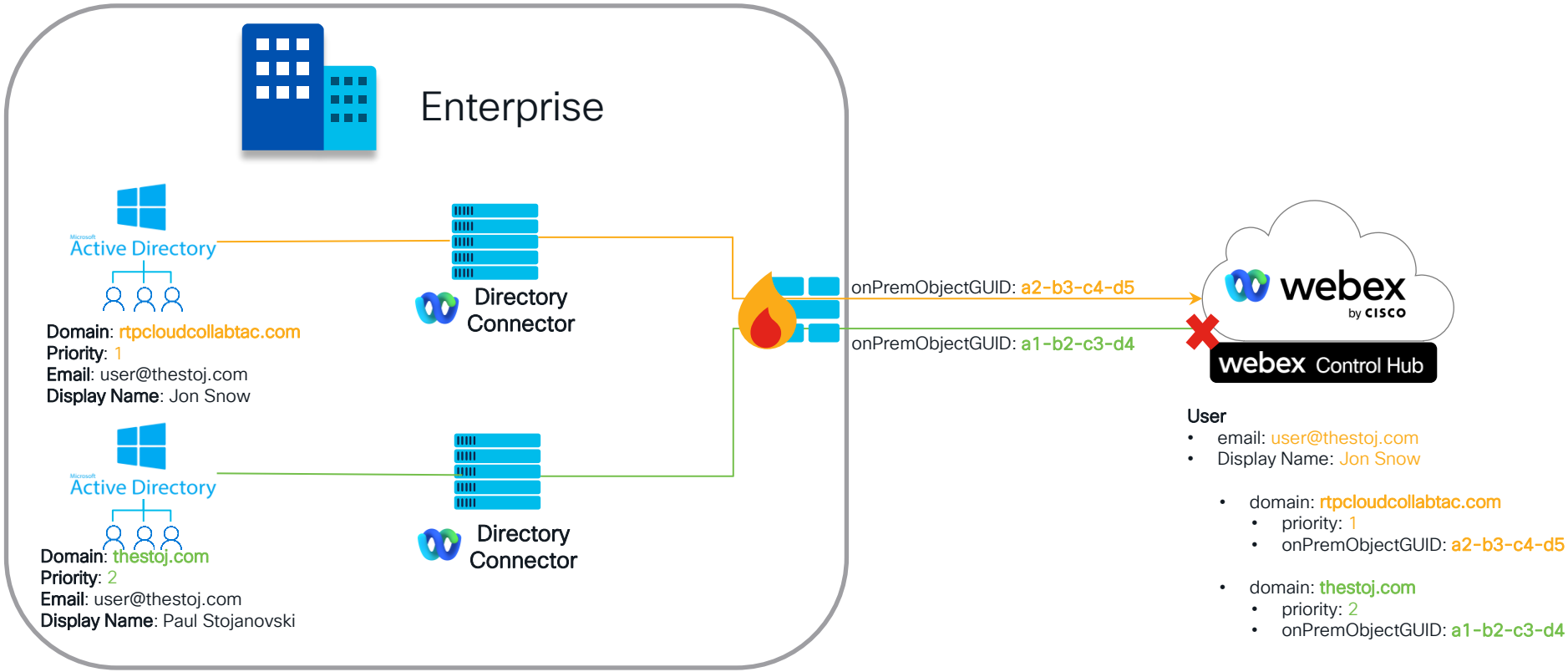
2. Delete the free user -> settings.webex.com

We do not recommend this approach because there could be additional users you want to add who use your company email domain and have signed up for a Webex account outside of your Webex organization.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

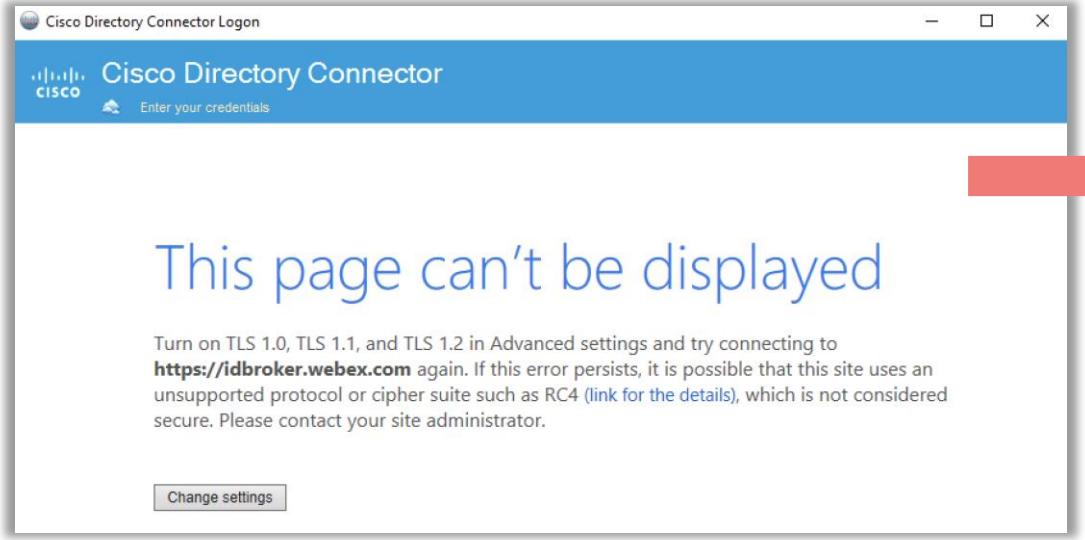
6 User exists in multiple domain

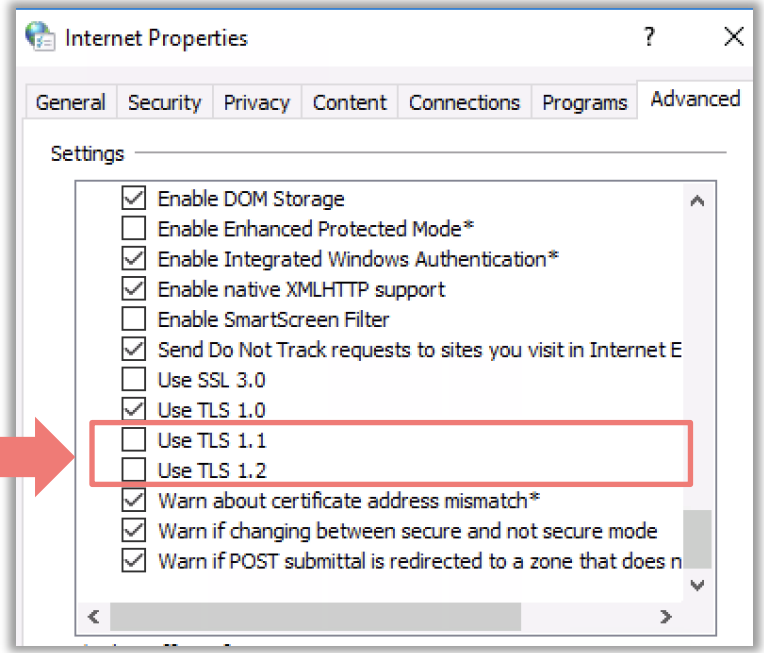


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

7 Login page not displayed

Error upon Directory Connector authentication





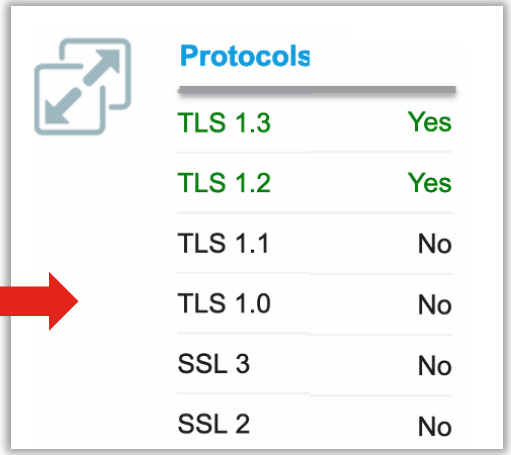
Use TLS 1.1 and 1.2 must be enabled

- Control Panel
  - Internet Options
    - Advanced
      - Security Settings

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

7 Login page not displayed

- If Use TLS 1.1 or 1.2 is checked further inspection is required
- Trust, but verify the Webex Cloud using SSL Report
- Determine the Cipher Family the Server is using



Group Policy	Computer Configuration > Administrative Templates > Network > SSL Configuration Settings
Registry	HKLM:\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002

- Leverage PowerShell to ensure one of the following Ciphers are available
  - Get-TLSCipherSuite
  - Set-TLSCipherSuite *(will set the value if missing)*

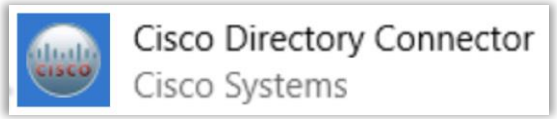
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

8 Webex cloud connectivity

Error progression

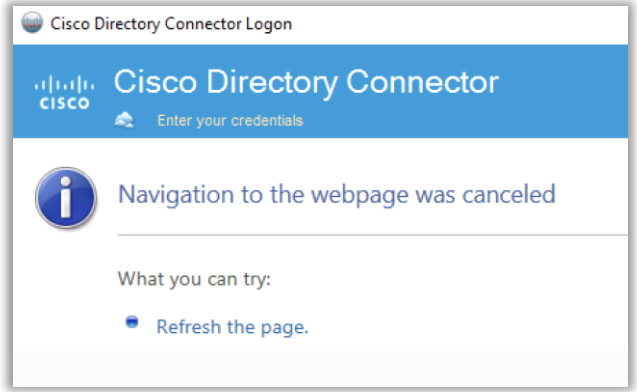
Launch Directory Connector



Webex Identity URL blocked

identity.webex.com
identity-b-us.webex.com
identity-eu.webex.com
identity-ca.webex.com

EXPECTED EXPERIENCE →

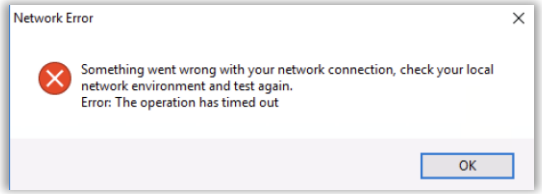


1 → 2 → 3

Cloud Connector URL blocked

cloudconnector.webex.com
cloudconnector-b-us.webex.com
cloudconnector-eu.webex.com
cloudconnector-ca.webex.com

EXPECTED EXPERIENCE



OR

Result of proxy rejecting traffic

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

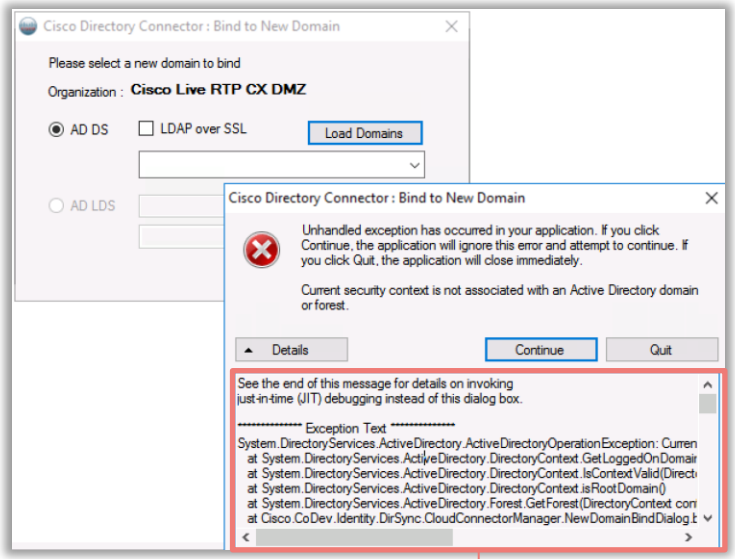
8 Webex cloud connectivity
Debugging

1. Can you get to the Directory Connector cloud-based URL:
   - https://cloudconnector.webex.com/SynchronizationService-v1_0/?orgId=GLOBAL
2. Take a packet capture and determine the following:
   - Does cloudconnector.webex.com or idbroker.webex.com resolve? *(European customers URL contains -eu)*
   - Can the server establish a TCP connection to either resolved IP?
   - Does the SSL handshake fail?
3. If TCP connection is failing attempt a traceroute to determine how far the packet makes it
4. If Troubleshooting enabled review **Network.CloudConnectorManager.exe** logs
5. Check status.webex.com for an open service incident

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

10 No permission to LDAP

Condition occurs when the logged-in user does not have permission to the LDAP tree structure




```
********** Exception Text **********
System.DirectoryServices.ActiveDirectory.ActiveDirectoryOperationException: Current security context is not associated with an Active Directory domain or forest.
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Directory Connector FAQ & Limitations

Why do deleted users show as inactive in Control Hub?

- This is expected behavior called “soft delete”. It’s a protective measure that guards against accidental deletion. Users deleted through Directory Connector are in a soft delete state for 7 days. After 7 days they are purged.

- Will users marked as inactive in Control Hub *(by disabling them in Active Directory)* be deleted after 7 days?
  - **No**, the soft delete capability does not apply in this condition.
- Do inactive users consume a license?
  - **Yes**, if they were assigned a license
- Can users change their profile settings (First and last name, Display name, or Profile picture) when Directory Connector is enabled?
  - No, these options in Control Hub are disabled when Directory Connector is enabled.
- Does Directory Connect sync passwords?
  - No

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Directory Connector FAQ & Limitations (cont)

- Why is my primary Directory Connector taking so long to failover when service is down?
  - The failover time is determined by the Failover Interval time configured on the Directory Connector under Configuration > Schedule > Failover interval. The default is 300 minutes (5 hours)
- Can Directory Connector be setup to run with a Managed Service Account (MSA) or Group Managed Service Account (gMSA)?
  - These accounts are currently not supported with Directory Connector.
- Can I assign a role to all users associated with a specific synced Group?
  - This role assignment is not possible today. It is a feature that's in the Backlog and being developed as part of a larger initiative for role based access control (RBAC)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Entra ID Wizard Provisioning

cisco Live!

Microsoft Branding Clarification

Old Name

Azure Active Directory

New Name

Microsoft Entra ID

Azure AD is becoming Microsoft Entra ID

Published date: July 11, 2023

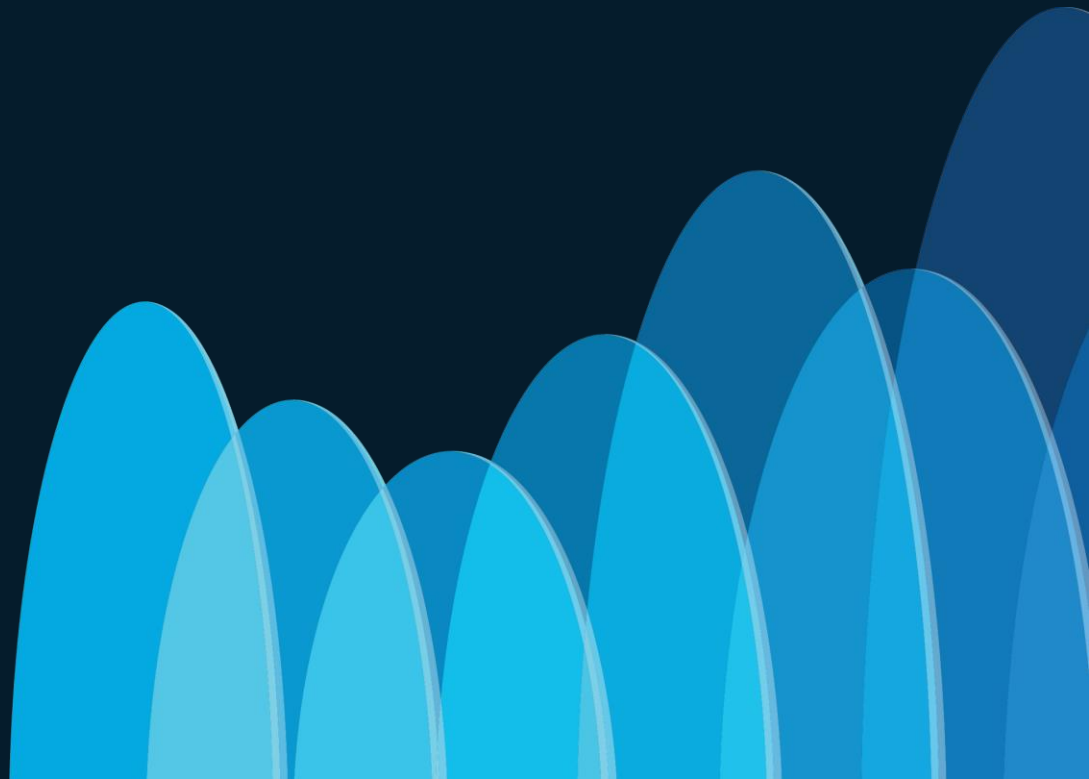
Microsoft Entra ID is the new name for Azure Active Directory (Azure AD). **No action is required from you.**

The name change to Microsoft Entra ID represents the evolution and unification of the Microsoft Entra product family, and a commitment to simplify secure access experiences for everyone.

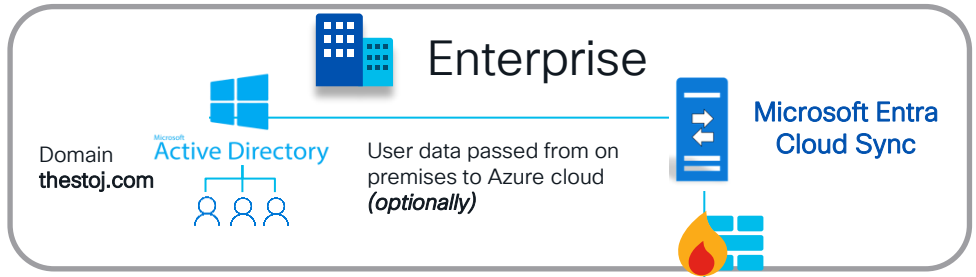
Note: Not all Cisco Webex documentation and Control Hub UX has been updated to reflect these changes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Overview



Architecture Overview



webex by CISCO

webex API

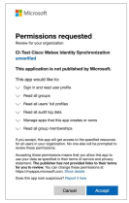
webex Control Hub

webex Identity

5

OAuth 2

4 Cisco Webex Identity Synchronisation
Enterprise application created to access Graph API



Microsoft Entra ID

Cisco Webex Identity

Cisco Webex Identity Synchronisation

Azure Active Directory admin center

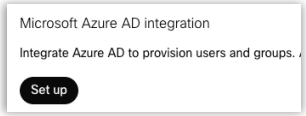
Creating sync/provisioning Enterprise App

Microsoft Graph API

3 Configuration data sent Webex identity system

7 SCIM creates or updates **users**

6 User, group, avatar provisioning data sent to Webex



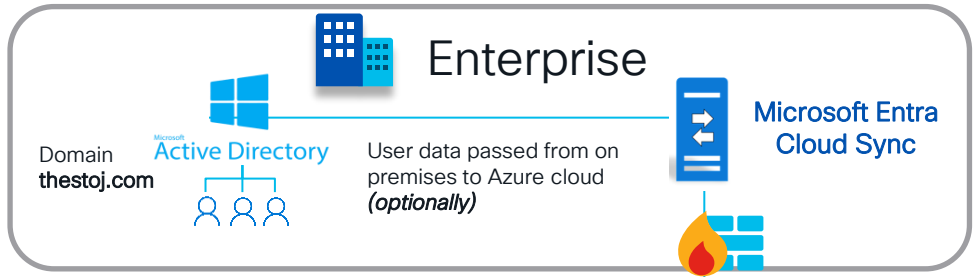
2 Configure the Azure AD Wizard to sync users.

Webex organisation admin

1 Configure users, groups, avatars, and domains that you wish to sync

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Architecture Overview



- User synchronisation occurs every 40 minutes
- Manager and Avatar mappings are 12 hours
- The Entra ID Wizard **is not** a single source of truth for user provisioning.....yet

webex Control Hub

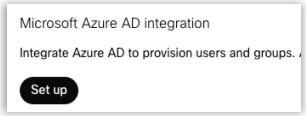
Cisco Webex Identity Synchronisation

Active Directory admin center

3 Configuration data … Webex identity system

7 … updates **users**

6 User, group, avatar provisioning data sent to Webex



2 Configure the Azure AD Wizard to sync users.

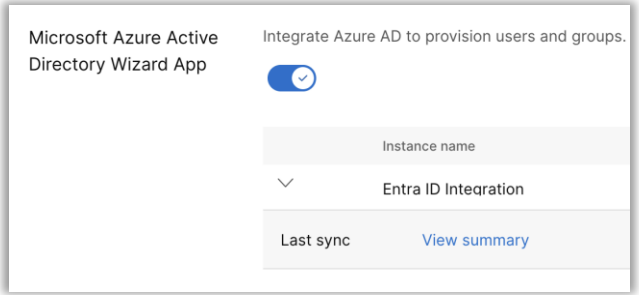
Webex organisation admin

1 Configure users, groups, avatars, and domains that you wish to sync

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID Wizard and Webex Microsoft Gallery App

Entra ID Wizard



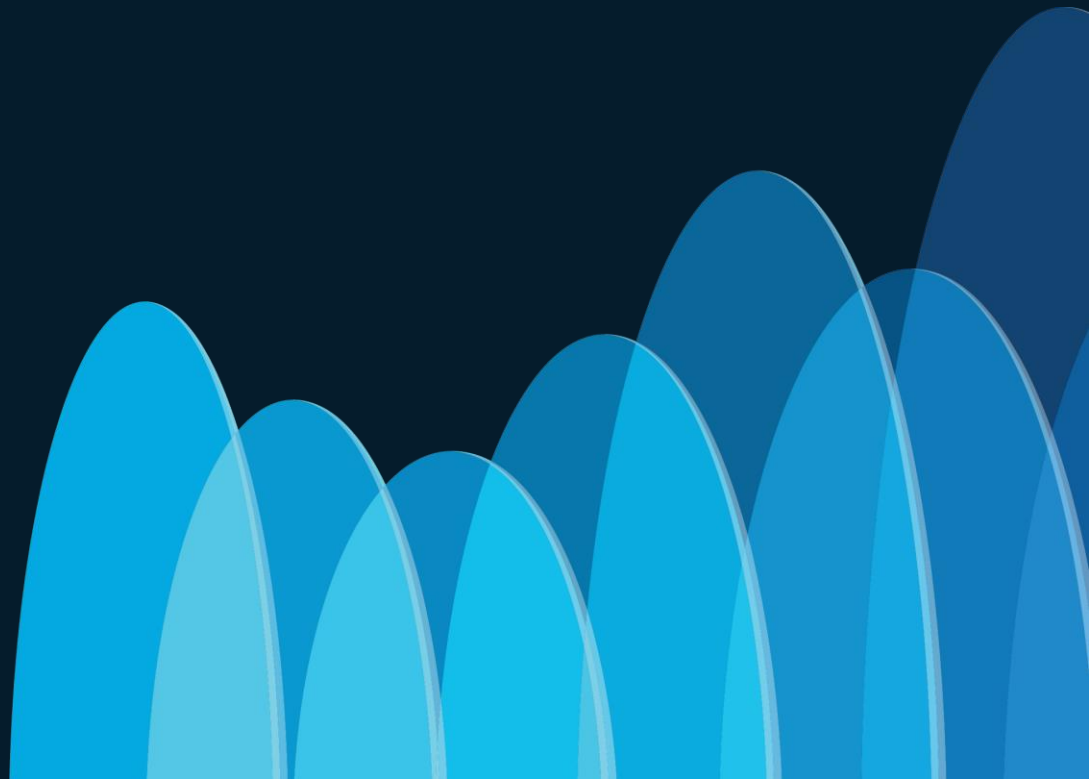
- Preferred Entra ID integration
- Setup is included in Webex Control Hub
- Provides easy to use wizard
- Allows for Group-based provisioning
- Can only be used with a single Entra tenant

Entra ID Gallery App

- Deployment is not preferred
- Setup resides in Entra ID Gallery Apps
- Does not support Avatars or Rooms
- Allows for Group-based provisioning
- Can be used with multiple Entra tenants

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tools & Log Collection

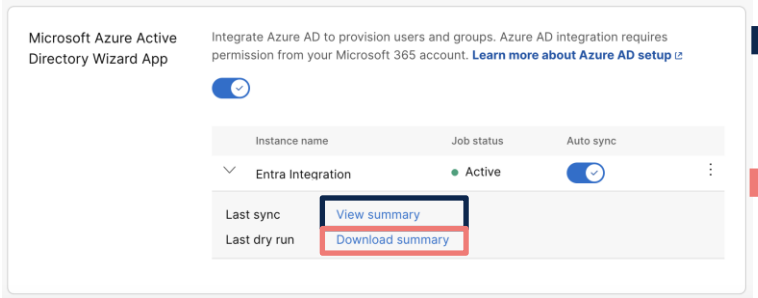


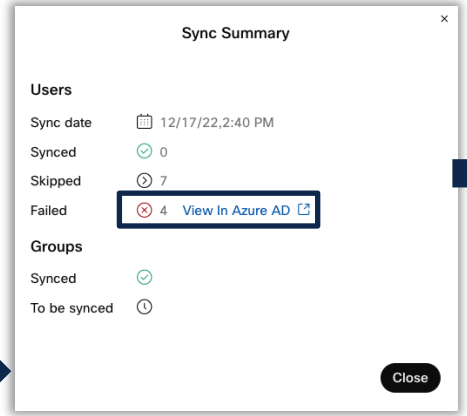
Entra ID Wizard Logs and Tools

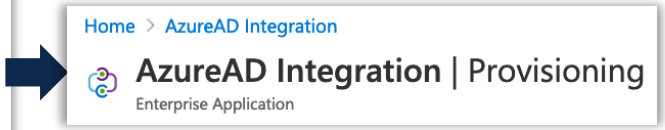
Control Hub

webex by cisco

webex Control Hub







CSV

Organization Settings > Microsoft Azure Active Directory Wizard App

Object Type	Action Type	Azure Id	Azure Name	Webex Name	Reason
User	Matched	ba0f1e65-df8	pstoj@thest	pstoj@thestoj.com(pstoj@thestoj.com)	
User	Add	9cba217a-cc	CiscoLive Sync(clsync@thestoj.com)		
User	Deactive			Paul Test(sav	The user - paul@thestoj.com is possible deleted in Azure AD
User	Mismatch			Hermione Granger(hgranger@thestoj.com)	
Group	Matched	dbcb8aca-10	SyncToContr	SyncToControlHub	

cisco Live!

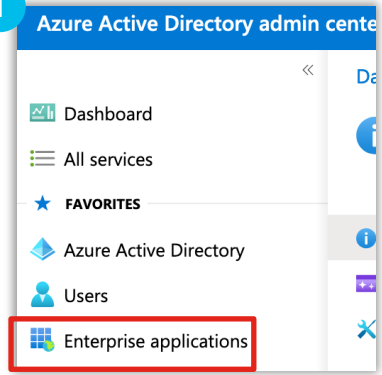
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Analysing Entra ID Sync Logging

Microsoft Entra ID

aad.portal.azure.com

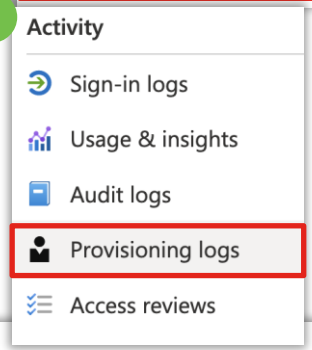
1



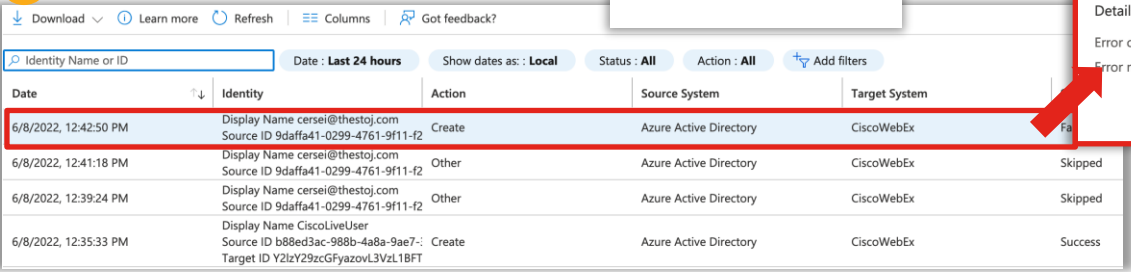
2

Name	Object ID	Application ID	Homepage URL	Created on
Cisco Webex Ident...	1fe72dc3-c299-41f7-a4f9...	90db942a-c1eb-4e8d-82e...	http://webex.com	12/22/2022
Cisco Webex Ident...	2df3e4bf-ee7d-4a2e-901...	04d7bd61-acac-424b-8d4...	https://idbroker.webex.co...	12/22/2022
AzureAD Integration	3bfe4c53-0534-4ea3-ade...	2020a6d1-8ba7-46d5-a8...	https://idbroker.webex.co...	1/4/2023

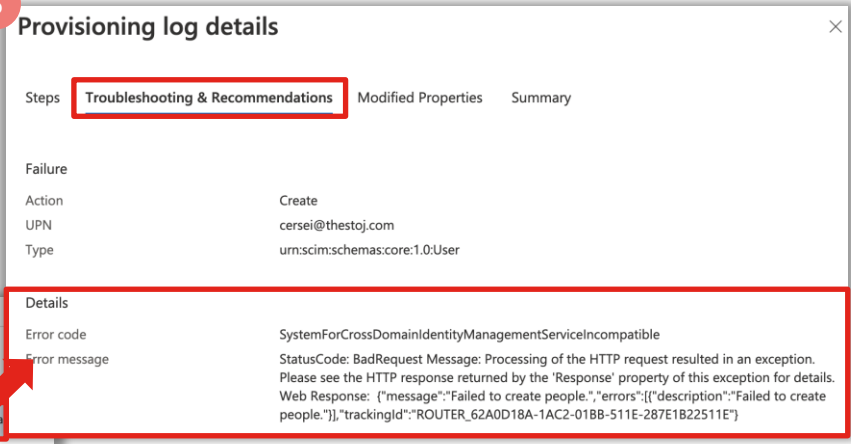
3



4

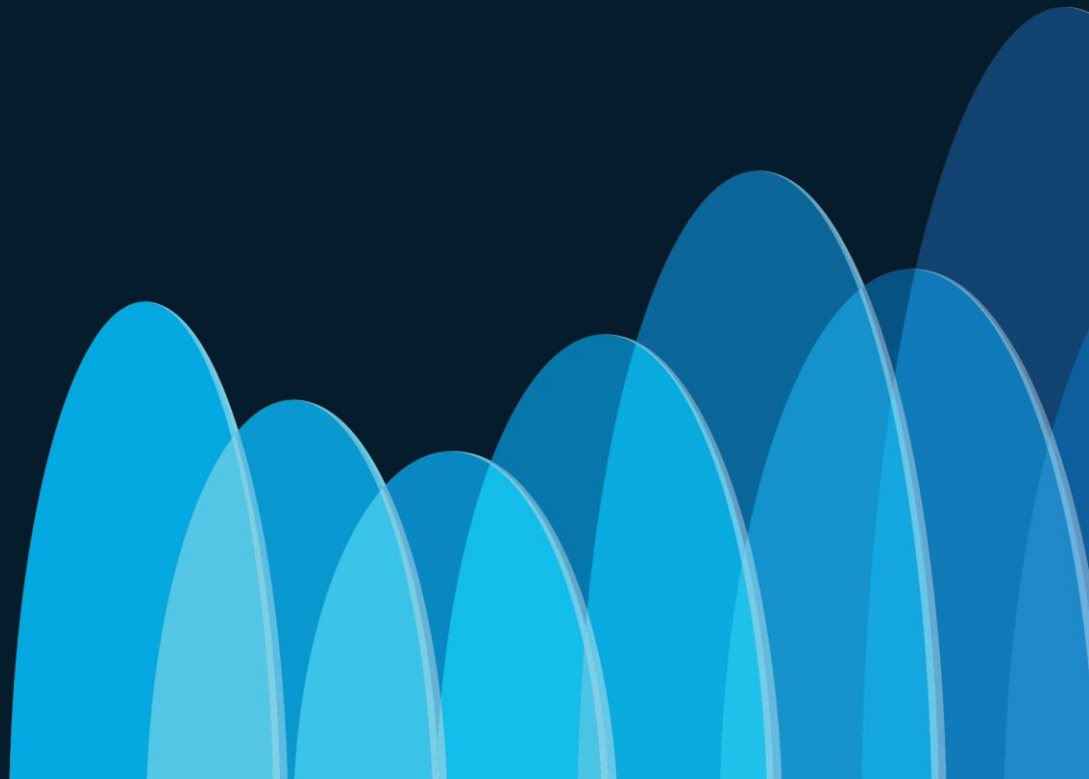


5



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Most Common Issues

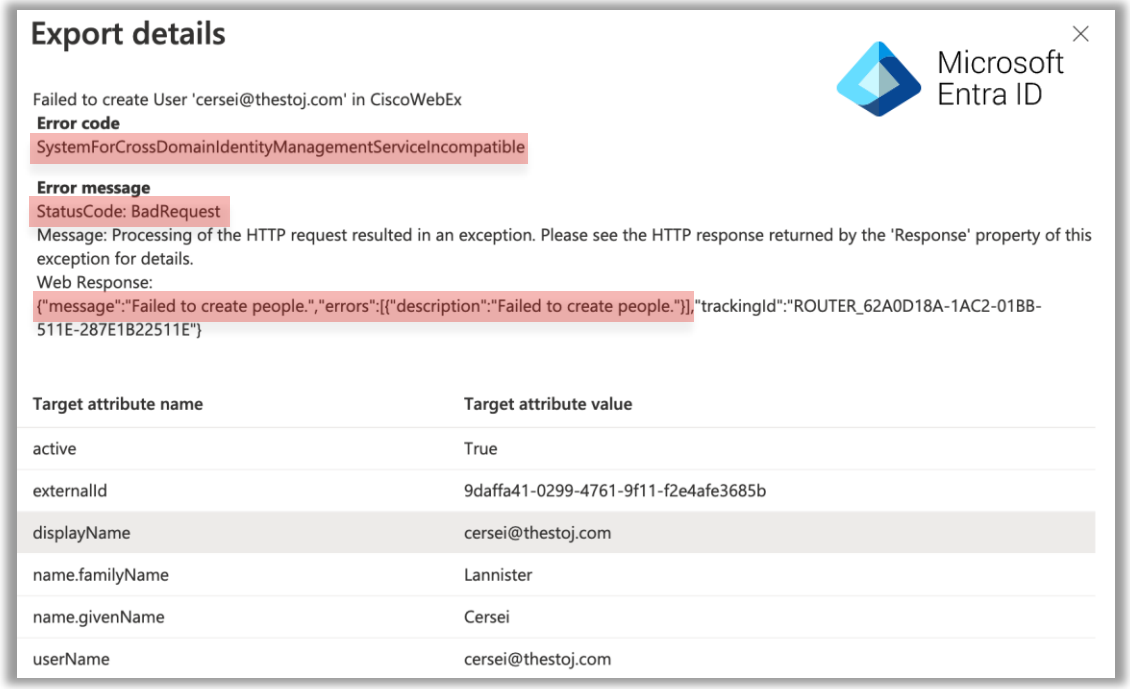


TAC Most Common Issues

1. User exists in another Webex org
2. Country value mismatch
3. Entra ID App deployment failures

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Failed to create people?



Export details

Microsoft Entra ID

Failed to create User 'cersei@thestoj.com' in CiscoWebEx

Error code

SystemForCrossDomainIdentityManagementServiceIncompatible

Error message

StatusCode: BadRequest

Message: Processing of the HTTP request resulted in an exception. Please see the HTTP response returned by the 'Response' property of this exception for details.

Web Response:

{"message":"Failed to create people.","errors":[{"description":"Failed to create people."}],"trackingId":"ROUTER_62A0D18A-1AC2-01BB-511E-287E1B22511E"}

Target attribute name	Target attribute value
active	True
externalId	9daffa41-0299-4761-9f11-f2e4afe3685b
displayName	cersei@thestoj.com
name.familyName	Lannister
name.givenName	Cersei
userName	cersei@thestoj.com

ISSUE

Triggered when the user exists in another Webex organization

REMEDIATION

1. Verify domain and claim user

OR

2. Instruct user to have their account deleted

Note: Free users can delete their accounts through settings.webex.com. Webex organization administrators must delete users associated to a paid organization.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Provisioning/Update Failure: Country Bad Request

StatusCode: BadRequest

Message: Processing of the HTTP request resulted in an exception. Please see the HTTP response returned by the 'Response' property of this exception for details.

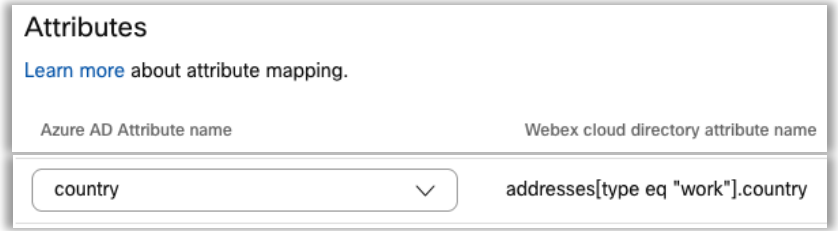
Web Response: {"message":"PATCH failed: HTTP/1.1 400 Bad Request (url = https://identity.webex.com/identity/scim/8ad51c16-13ad-43e8-a390-2f653ff28e99/v1/Users/36ecd61b-90bf-4a34-bf7b-190d58b2fcf1, request/response TrackingId = ROUTER_63B5B6ED-15C2-01BB-0123-287E1B200123, error = 'addresses.country United States of America is not in the legal value list;code=400;errorCode=100008;trackingId=ROUTER_63B5B6ED-15C2-01BB-0123-287E1B200123')"

Entra ID: *Enterprise Applications > Cisco Webex Identity > Provisioning Logs*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Provisioning/Update Failure: Country Bad Request

- Determine which Entra ID attribute is being mapped to **addresses[type eq "work"].country**



- Determine value configured on user's profile in Entra ID

SCIM

RFC 7643

country

The country name component. When specified, the value **MUST** be in ISO 3166-1 **"alpha-2" code format** [ISO3166]; e.g., the United States and Sweden are "US" and "SE", respectively.

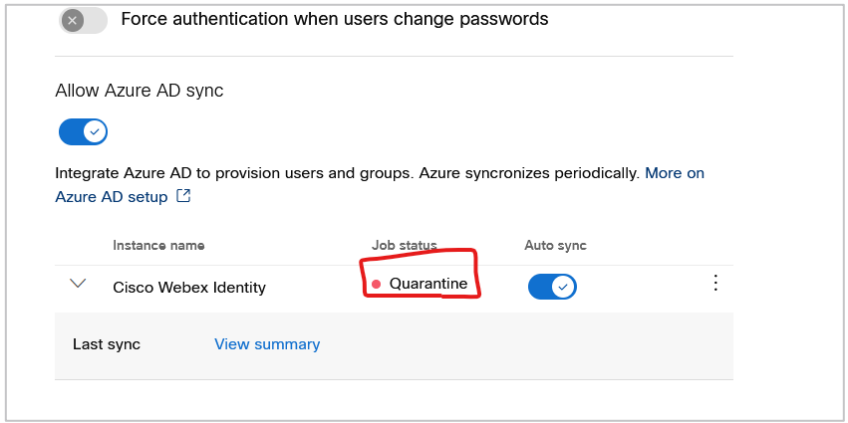
Recommendation: Map country to Entra ID Attribute: usageLocation

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

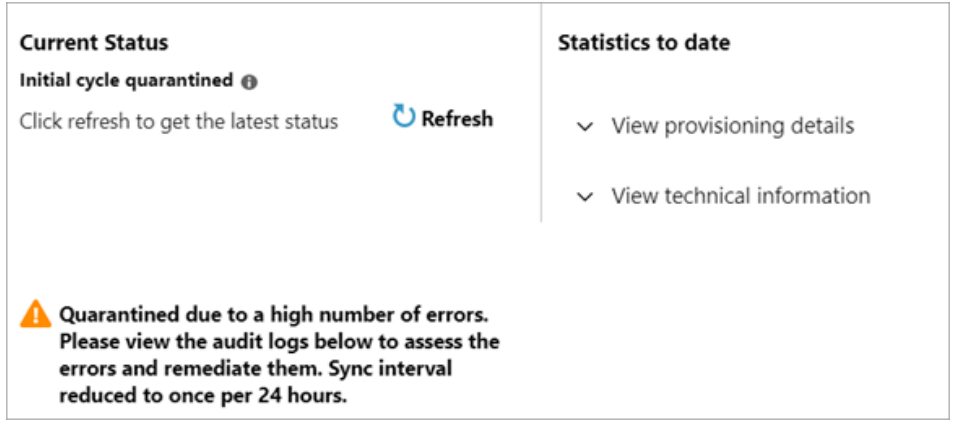
Entra ID (Azure) Integration Quarantined

webex by CISCO

webex Control Hub



Microsoft Entra ID



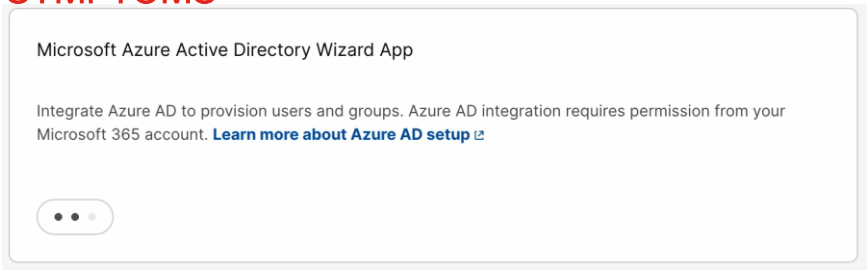
- Typically, the result of large-scale failure provisioning failure events - Microsoft quarantine rules
- Review *Entra ID > Enterprise Apps > Audit logs* for **Activity: Quarantine**

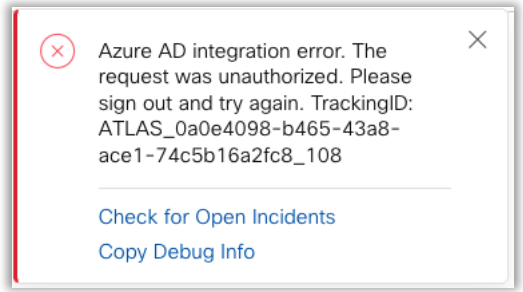
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID Integration Error

TIP [Collecting a browser trace](#)
details also on next (hidden) slide

SYMPTOMS





webex Control Hub

webex Identity

HTTP REQUEST

GET https://identity.webex.com/extIntegration/azureAD/8ad51c16-13ad-43e8-a390-2f653ff28e99/v1/WebexApplications/status

HTTP RESPONSE

```
"error":{
 "key": "401",
 "message":[{"code": "701018","description": "Request unauthorized. client-request-id: 03766b11-0cd5-4910-b380-50b2afe28a03"}]
```

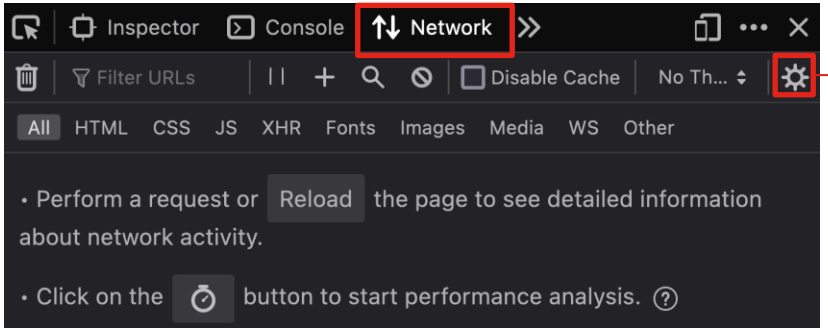

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Control Hub User Errors

Collection a Browser Trace

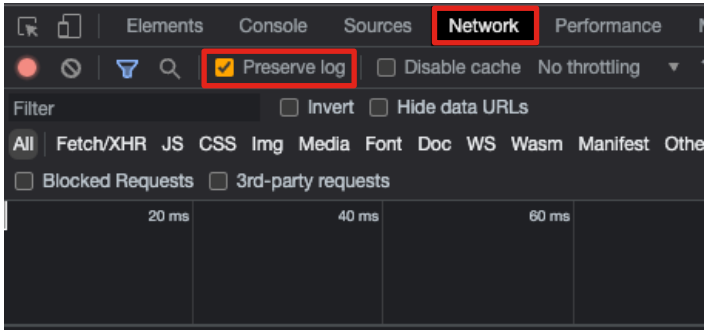
Firefox

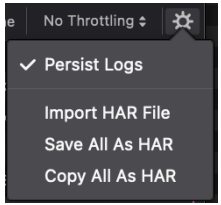
1. Right-click > **Inspect**
2. Select Network
3. Load page



Chrome

1. Right-click > Inspect
2. Select Network
3. Check Preserve Log
4. Load page





Many tools such as Proxyman or Google's HAR Analyzer allow you to read the HAR file more easily.

features include text search, filter by HTTP status code, and message color coding

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID Integration Error

Problem Isolation

Cisco Webex Identity Synchronization Enterprise application **was deleted by an Administrator**

1. Login to Entra ID
2. Select Enterprise applications

EXPECTED

Name	Object ID	Application ID	Homepage URL	Created on
Cisco Webex Identity Synchronization	1fe72dc3-c299-41f7-...	90db942a-c1eb-4e8d...	http://webex.com	12/22/2022
Cisco Webex Identity	2df3e4bf-ee7d-4a2e-...	04d7bd61-acac-424b...	https://idbroker.web...	12/22/2022
AzureAD Integration	3bfe4c53-0534-4ea3...	2020a6d1-8ba7-46d5...	https://idbroker.web...	1/4/2023

Original Microsoft SCIM solution

OBSERVED

Name	Object ID	Application ID	Homepage URL	Created on
Cisco Webex Identity	2df3e4bf-ee7d-4a2e-...	04d7bd61-acac-424b...	https://idbroker.web...	12/22/2022
AzureAD Integration	3bfe4c53-0534-4ea3...	2020a6d1-8ba7-46d5...	https://idbroker.web...	1/4/2023

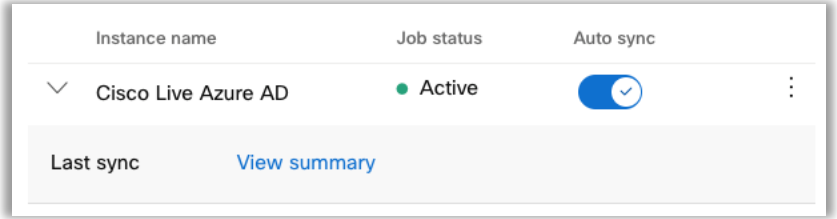
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID Integration Error

Remediation

Cisco Webex Identity Synchronization Enterprise App

- Cisco Webex Identity Synchronization can be rebuilt by providing admin consent
  - https://login.microsoftonline.com/common/adminconsent?client_id=90db942a-c1eb-4e8d-82e4-eebf64a7e2ae
- Enterprise App will display within one minute after granting consent
- If only Cisco Webex Identity Synchronization was deleted, then original configuration will be restored

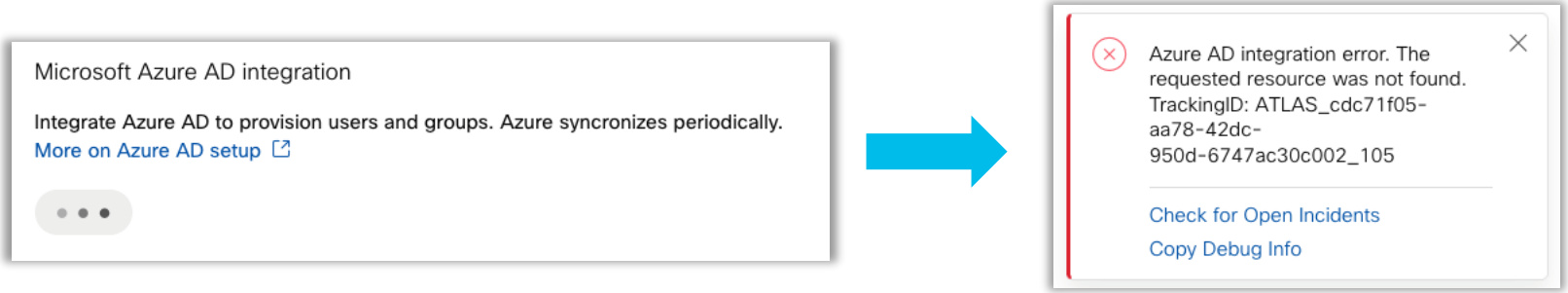


Step–by-step Troubleshooting instructions

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID Integration Error

Similar though different



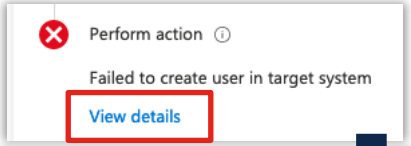
- This condition occurs **when only** the Enterprise app used for provisioning is deleted
  - Default name: **Cisco Webex Identity**
- Since the Enterprise app configuration remains in the Webex Identity system, a TAC case is required to clear it

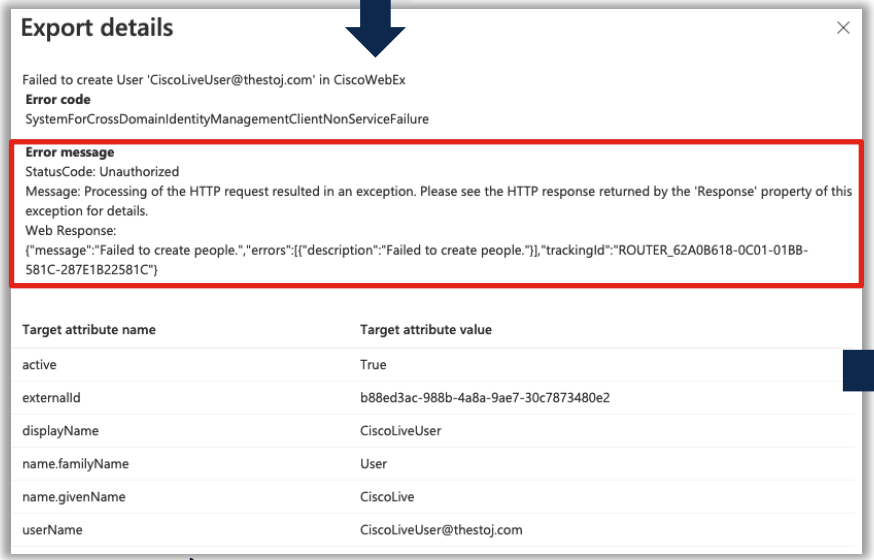
Support Case Manager

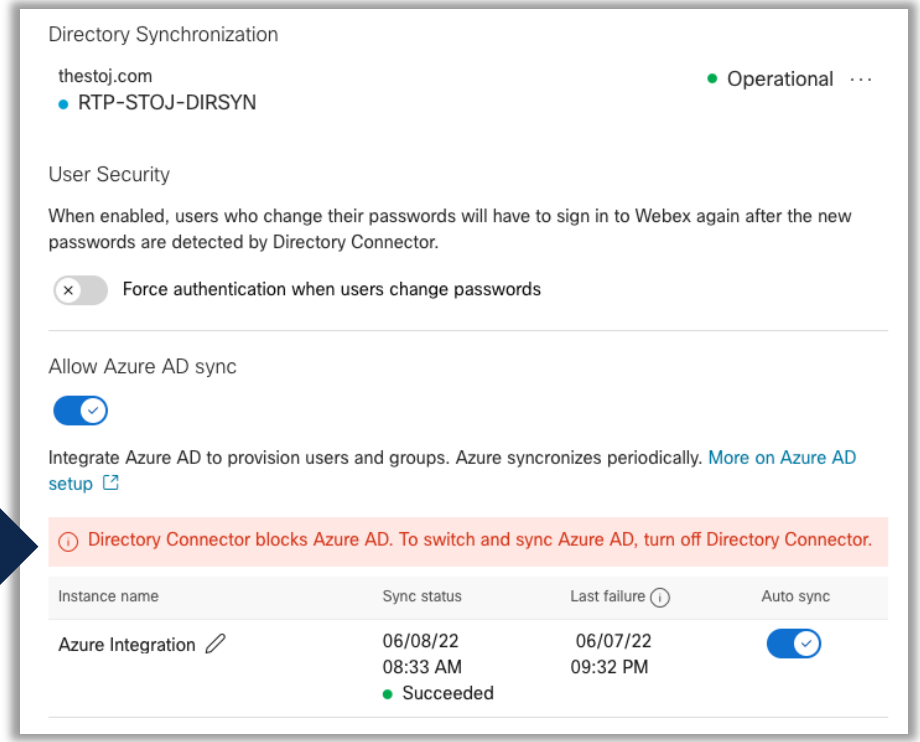
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Directory Connector + Entra ID Wizard

Not Supported

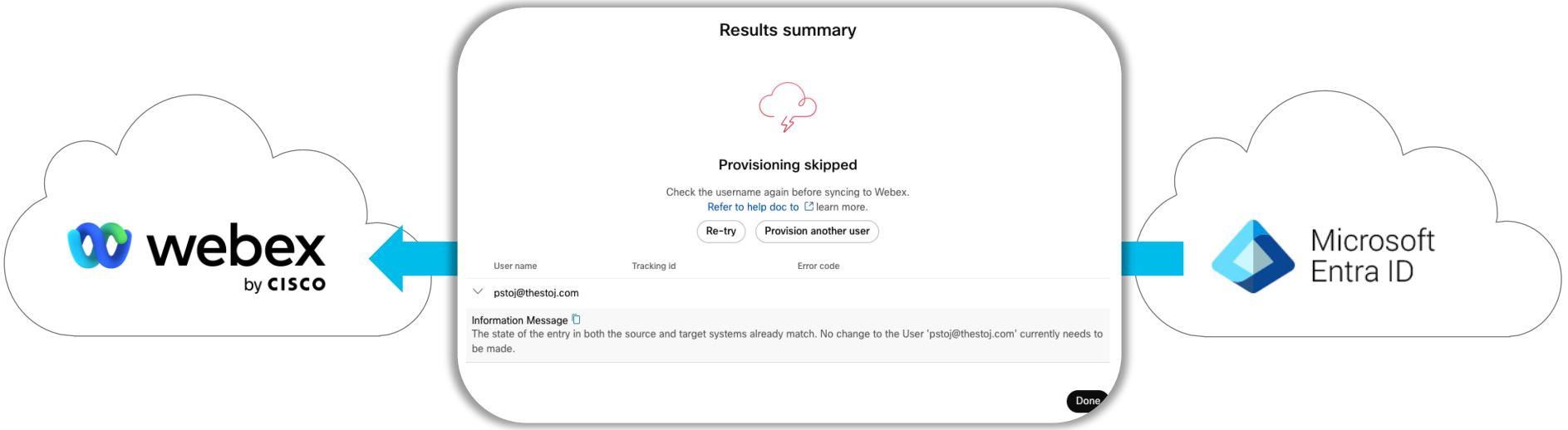






© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

On Demand Provisioning – Skipped



- You can expect to see Provisioning skipped when you attempt to provision a user on demand and this user exists in Webex
- This is the equivalent of a “**Matched**” user in a Sync Dry Run

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID FAQ

- Is the feature "Force authentication when users change password" valid for Entra ID synced users?
  - No. The Wizard App cannot detect users changing password in Entra ID. This feature will be coming
- Will there eventually be support for multiple Entra ID tenants?
  - Yes. It is in the backlog
- What happens to my existing Webex users if they aren't included in the Entra ID sync?
  - The current design of the Entra ID Wizard doesn't lock provisioning down to only users who come through the Entra ID Wizard. In the future Control Hub will offer the ability to lock provisioning down to the Entra ID Wizard so it can be marked as a single source of truth.
- What will happen if a user is moved out from a synced group?
  - The user will be deactivated and show inactive state in Control Hub. The users will be purged once the Manage inactive user window expires. (Default: 30 days)
- What will happen if a user is deleted in Entra ID and the user was in the sync scope?
  - The user will be removed from sync scope automatically. It is managed by Entra ID framework. After a periodic sync, the user will be deactivated and show inactive state in Control Hub. The users will be purged once the Manage inactive user window expires. (Default: 30 days)
- Do Entra ID synced groups show up under Webex groups or Synchronized groups in Control Hub?
  - Entra ID synced users will show as Synchronized groups. When the solution was originally released, they showed under Webex groups.
- Does Entra ID support expression-based attribute mappings?
  - No, this is not supported natively in the Entra ID app. This can be done from the Entra perspective by editing that Attribute mapping directly from the Entra ID portal. See this article to learn more about Entra ID expression mappings.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID FAQ

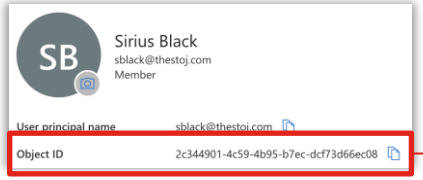
- Can you sync Entra ID users to two different Webex organizations?
  - Yes, this is possible. You'll have to carefully manage the users or Groups you want to sync. Turning off Auto-sync can help with this

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting

- Groups
- Migrations to Entra ID

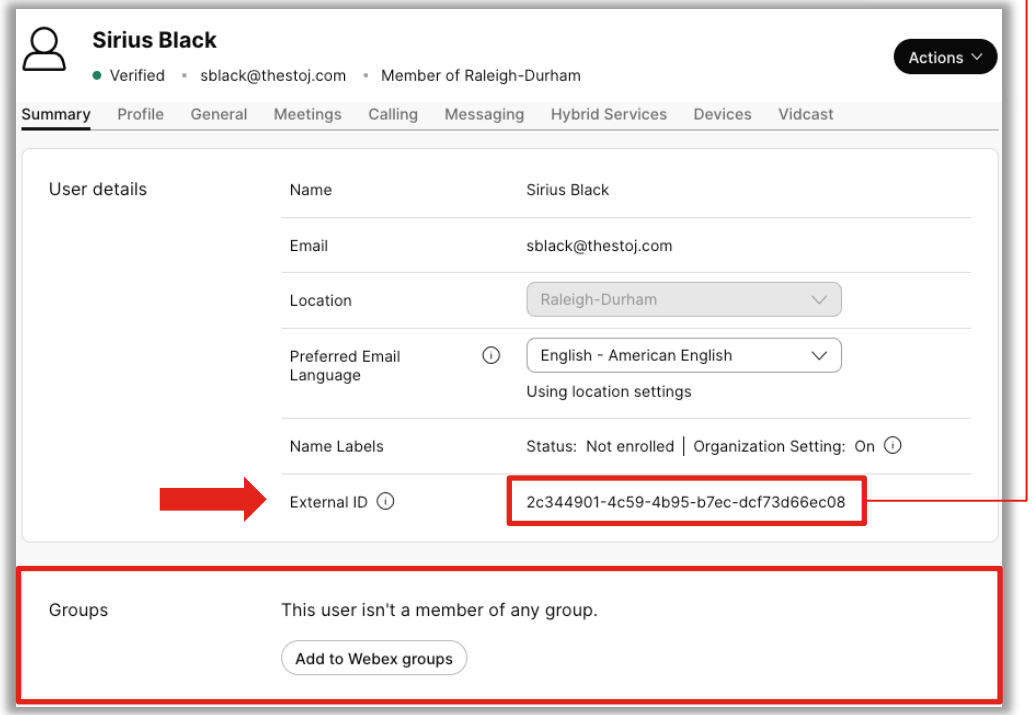
Group Configuration Issues



My Entra ID **Groups are not syncing** even though users are?

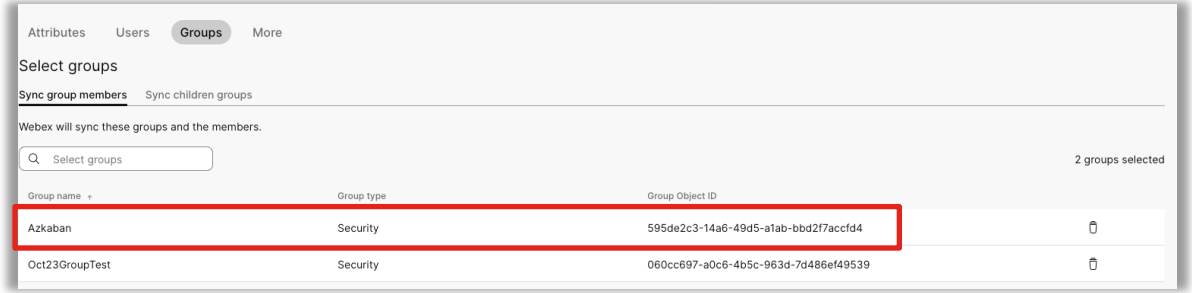
A few things to know

- External ID specifies the user was created through synchronization
  - Matches user's Object ID in Entra ID
- Webex Identity allows you to sync users from Groups (and children groups)
- Syncing users from a Group **does not sync the Group**

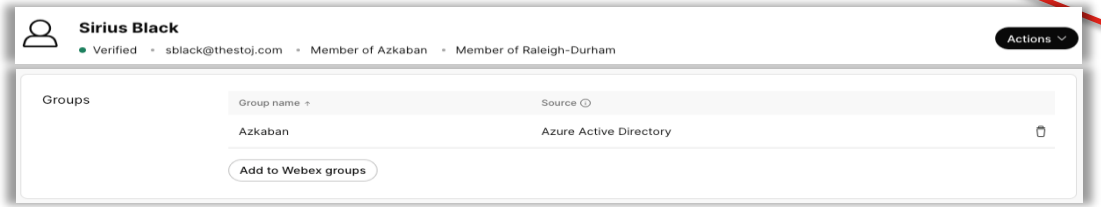


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Group Configuration Issues

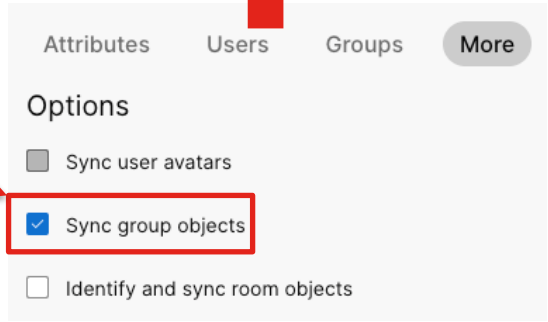


- To sync Groups explicitly:
  - Org Settings > Entra ID config > Click ⋮ > Choose Edit
  - Select More
  - Check the **Sync group object** option
- Upon next group synchronization



Webex Identity Config

data": {"avatarSync": false,
+
"directoryInfo": { ... },
"displayName": "Entra Integration",
"enableAutoSync": false,
"groupSync": true,
"id": "db684e5d-6794-41c9-936d-70a0d6c7a828",
+
"msTokenInfo": { ... },
+
"objectMappings": { ... },
"oidcSSOEnabled": false,
"roomSync": false,
"ssoEnabled": true,
+
"syncScope": { ... },
"totalUsers": 23
}

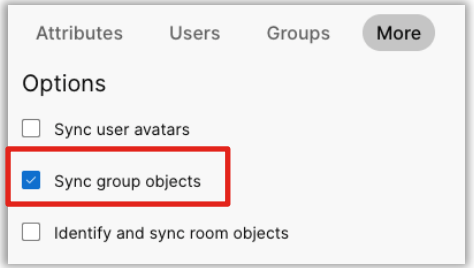


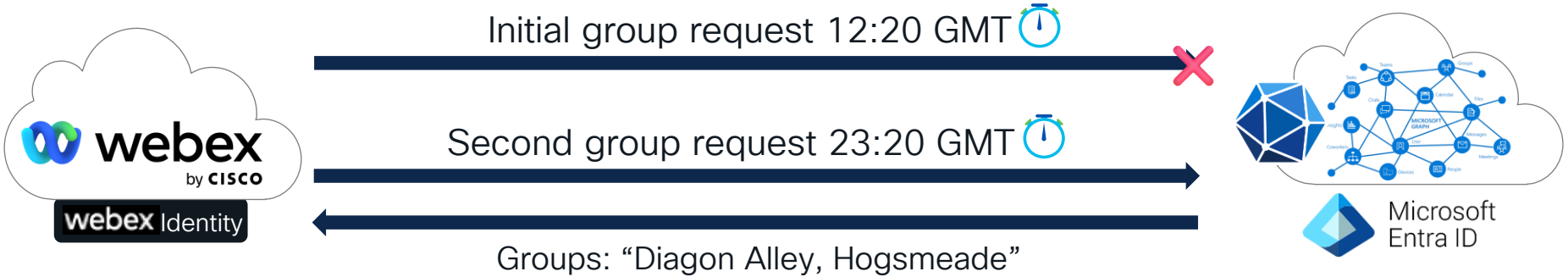
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Entra ID Group sync delays

How long will it take for my groups to sync to Control Hub?

- Group synchronisation is **not handled through SCIM**
- Webex Identity leverages the **Graph API** to request Groups
- Troubleshooting tip: Group sync can be forced by toggling the **Sync group objects** setting





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unable to Delete Synchronized Groups

CSCwd97988

Symptom: Webex organization administrators are **unable to delete groups** from Control Hub.

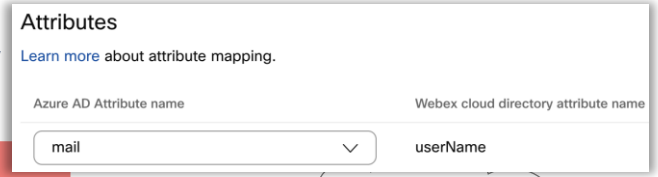
Conditions: This occurs if you are syncing Groups from Directory sources like Entra ID or Directory Connector.

Workaround: Before disabling a sync source, remove the groups from the sync, and run a full sync from Entra ID or Directory Connector.

- Open a TAC case to have the groups removed

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What about Migrating to Entra ID?



Recommendations:
1. Mapped attributes should match **(Cloud attribute is critical!)**
2. Directory information *should* match (users, groups, avatars)

Microsoft Entra ID

Microsoft Graph API

Enterprise

Active Directory

Domain
rtpcloudcollabtac.com

Directory Connector

FAQ: Disabling Directory Connector **still preserves users** in Control Hub

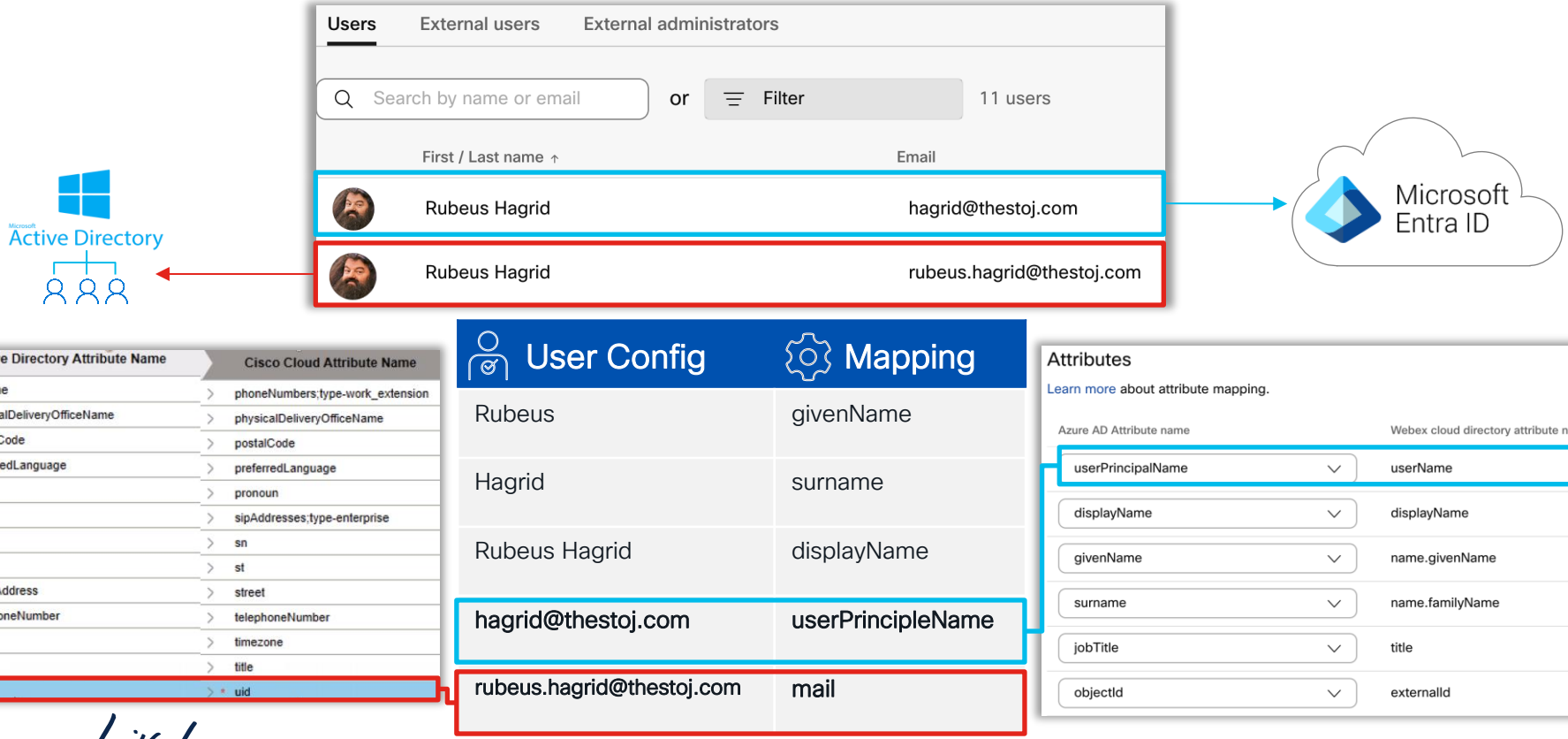
webex by CISCO

webex Control Hub

Requirements:
1. Disable or Block Directory Connector
2. Invoke the Entra ID Wizard
3. Setup configuration to match existing LDAP Users, Groups, Avatars

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duplicate identities after migrating



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Missing attributes

Aha!

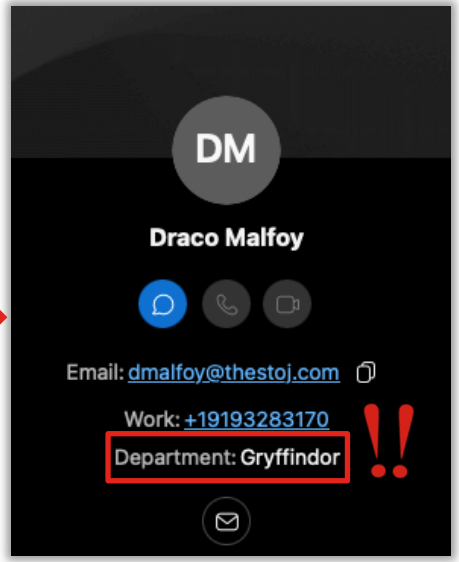
WXCUST-I-4352

Attributes will be added in 2024

- After migration you may experience unavailable attributes
  - Most commonly reported are:
    - departmentNumber *(can be mapped to AD department)*
    - ipPhone
    - employeeId

- departmentNumber changes won't reflect in the Webex App contact card

Workaround: Use the *Admin API* > *Update a Person*



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

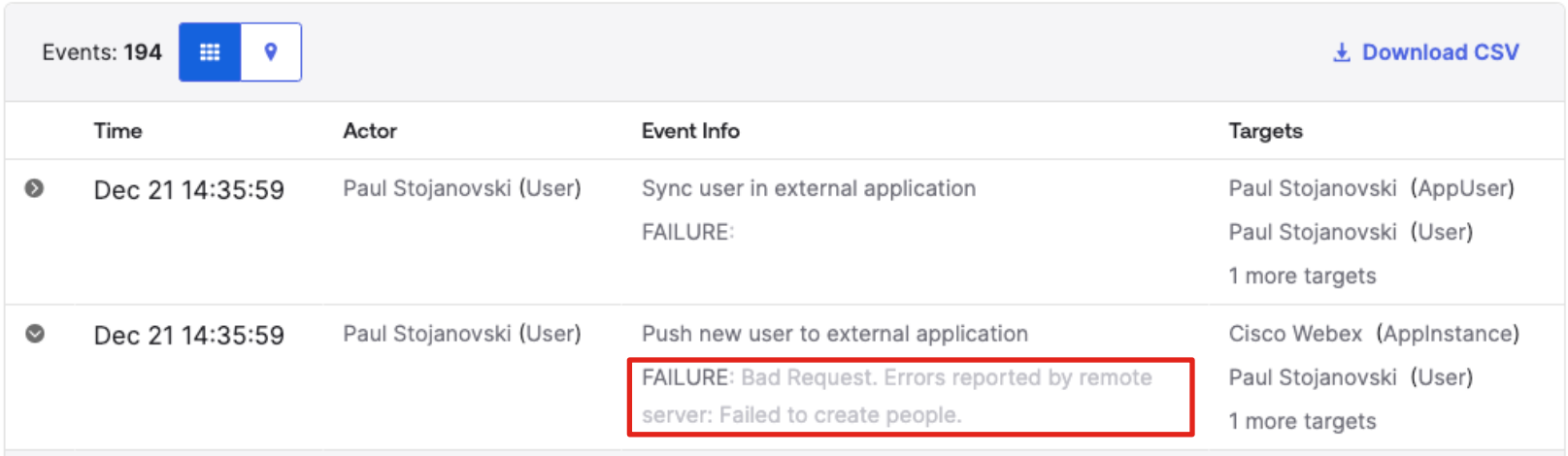
Groups and Entra ID Migration FAQ

- What is the max user size of a synchronized Group?
  - 250,000
- Can Directory Connector synchronize Distribution groups?
  - No, these are not eligible for synchronization because Distribution groups are used for mass communication whereas security groups are used for granting permissions.
- Is Group synchronization supported for Okta?
  - No, we do not support synchronizing groups from Okta with your Webex organization.
- What happens if a user is added to two different groups which have different licenses? (One for Meetings, one for Calling)
  - The licenses in this situation are combined so the user will be licensed for Meetings and Calling
- How do I license users if they are added to a Group before the licensing template is applied?
  - First, add the license to the group. Second, in the Apply scope section, check the box to apply the template to Existing Users

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

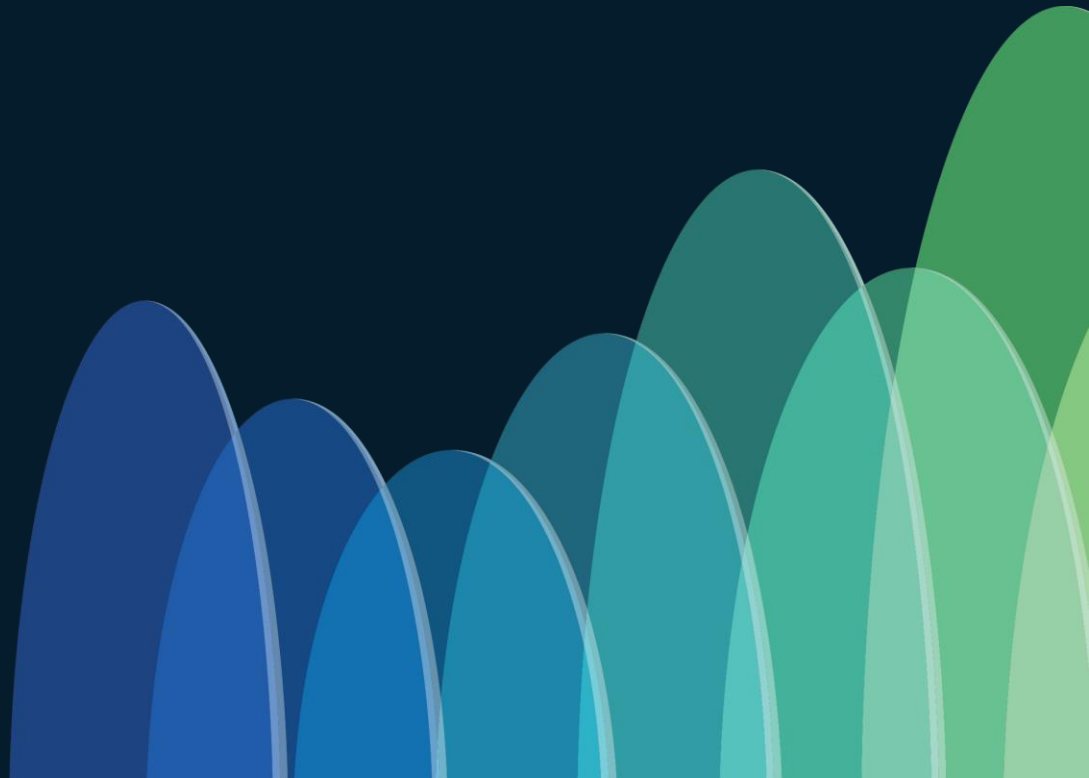
Okta User Provisioning Failure

- Okta and SCIM based integration logging is minimal
- Bad Request + Failed to create people
  - Common condition when adding a user that exists in another Webex org



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Authentication

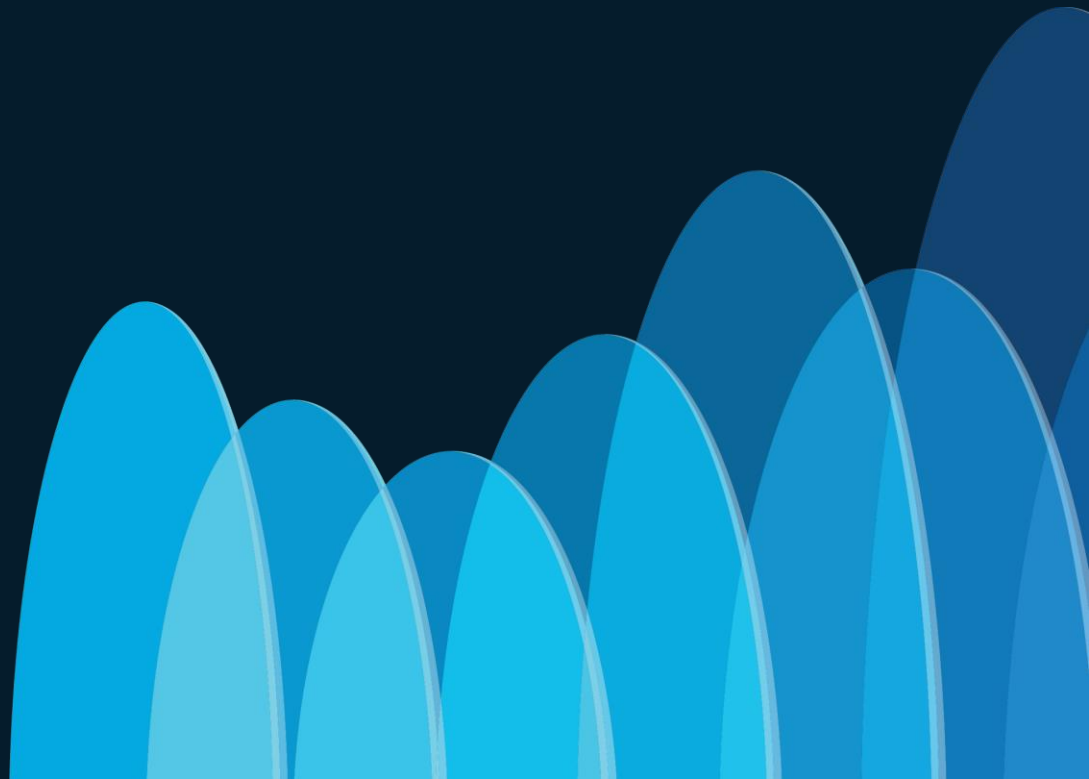


cisco Live!

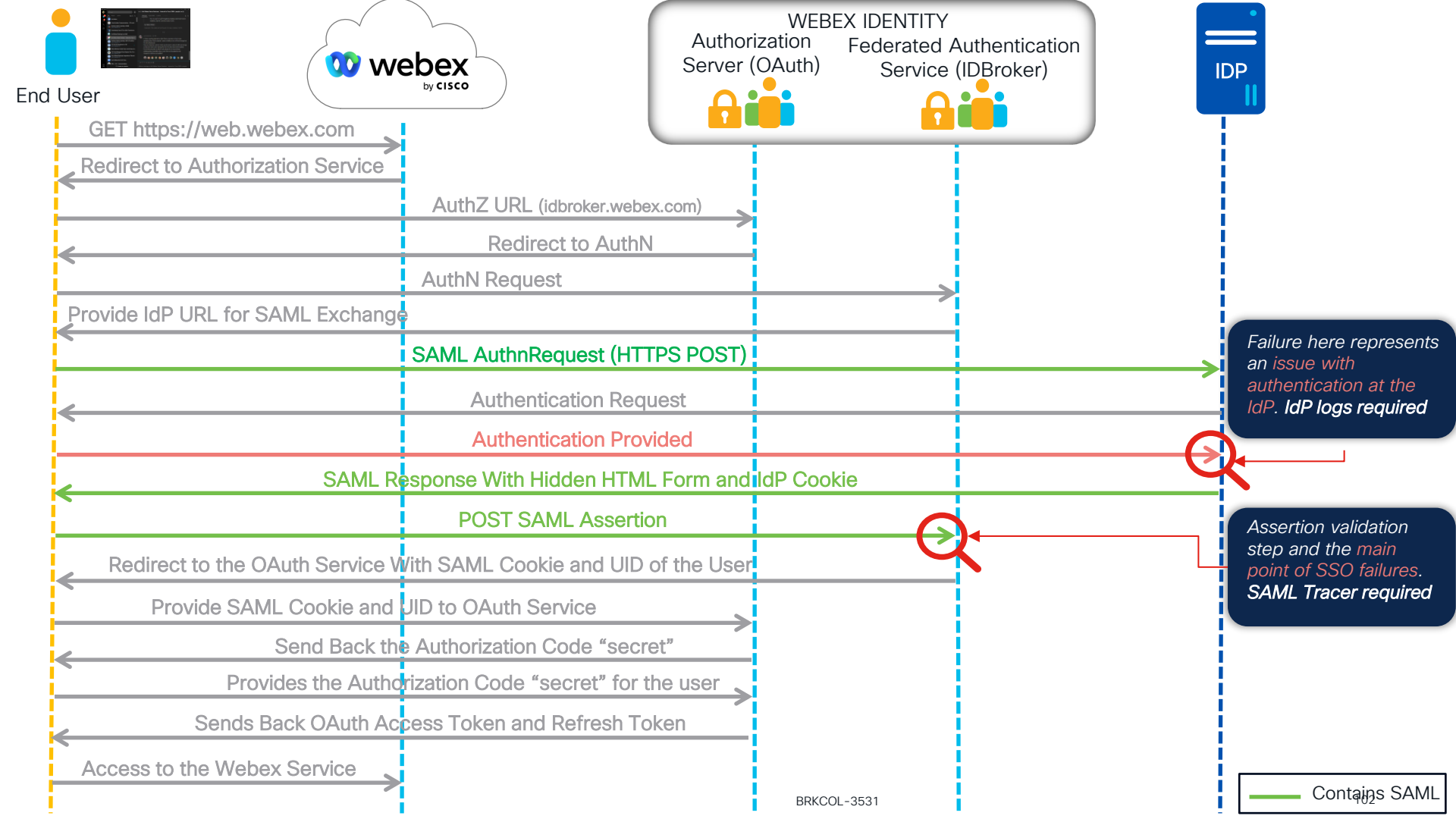
Troubleshooting Single sign-on Authentication

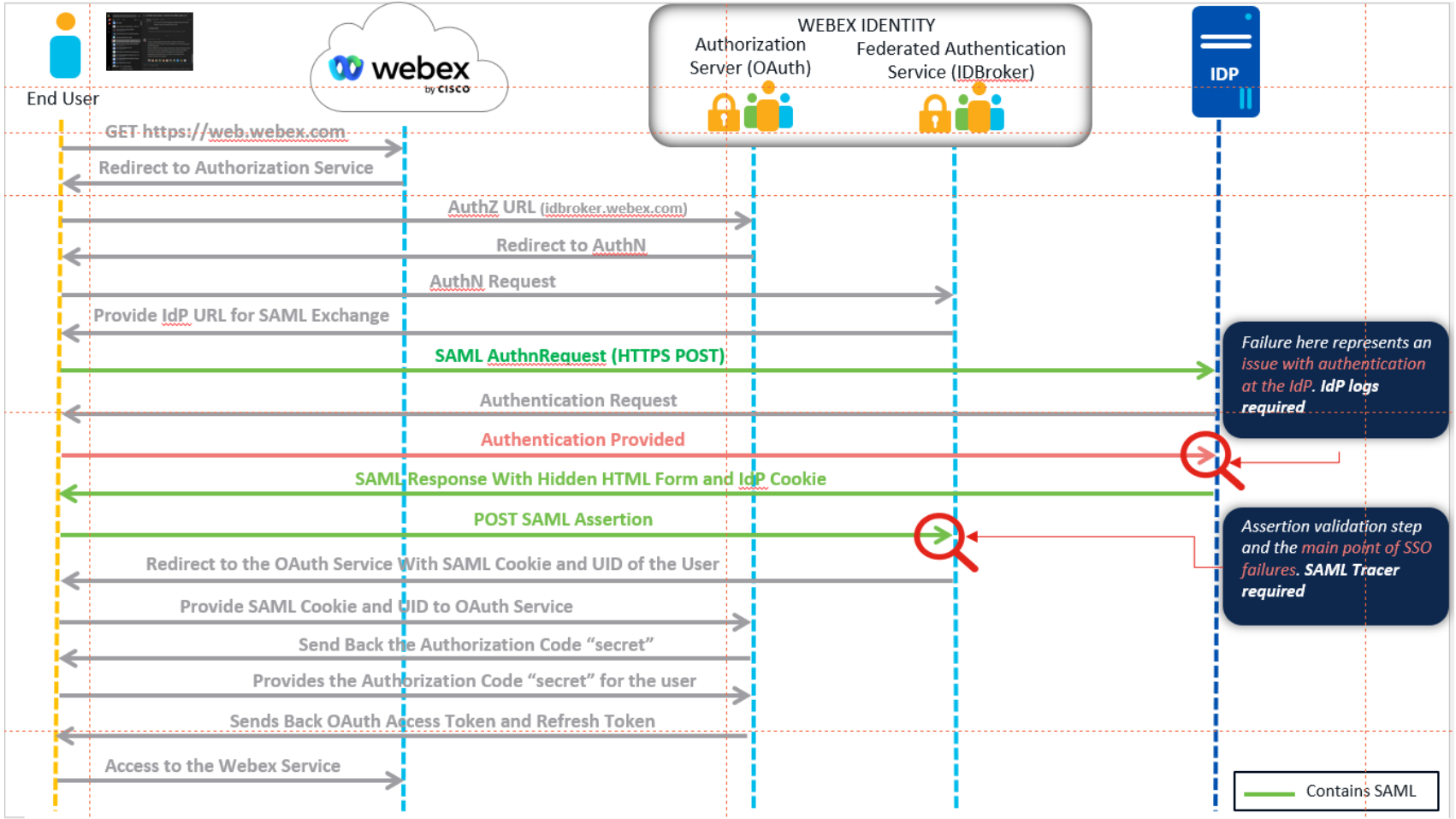
cisco Live!

Quick SAML Bootcamp



cisco Live!


End User
webex by cisco
WEBEX IDENTITY
Authorization Server (OAuth)
Federated Authentication Service (IDBroker)
IDP
GET https://web.webex.com
Redirect to Authorization Service
AuthZ URL (idbroker.webex.com)
Redirect to AuthN
AuthN Request
Provide IdP URL for SAML Exchange
SAML AuthnRequest (HTTPS POST)
Authentication Request
Authentication Provided
SAML Response With Hidden HTML Form and IdP Cookie
POST SAML Assertion
Redirect to the OAuth Service With SAML Cookie and UID of the User
Provide SAML Cookie and UID to OAuth Service
Send Back the Authorization Code "secret"
Provides the Authorization Code "secret" for the user
Sends Back OAuth Access Token and Refresh Token
Access to the Webex Service
Failure here represents an issue with authentication at the IdP. IdP logs required
Assertion validation step and the main point of SSO failures. SAML Tracer required
Contains SAML



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAML AuthnRequest Breakdown
SAML AUTHNREQUEST (HTTP POST) -> idp.example.com

```
<samlp:AuthnRequest
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="s2a69bda9b2e9a5c46e5ec3777cce54811c30b9003" Version="2.0" IssueInstant="2022-04-08T18:44:24Z" Destination="https://adfs01.thestoj.com/adfs/ls/" ForceAuthn="false" IsPassive="false" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" AssertionConsumerServiceURL="https://idbroker.webex.com/idb/Consumer/metaAlias/8ad51c16-13ad-43e8-a390-2f653ff28e99/sp" >
        <saml:Issuer
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99
        </saml:Issuer>
        <samlp:NameIDPolicy
                xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" SPNameQualifier="https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99" AllowCreate="true" />
        </samlp:AuthnRequest>
```

Destination

A **URI reference indicating the address to which this request has been sent**. This is useful to prevent malicious forwarding of requests to unintended recipients, a protection that is required by some protocol bindings.

ACS URL

Specifies by value the **location to which the <Response> message MUST be returned** to the requester.

SPNameQualifier

Further qualifies a name with the **name of a service provider or affiliation of providers**. This attribute provides an additional means to federate names on the basis of the relying party or parties.

Format

A URI reference representing the **classification of string-based identifier information**.

SAML 2.0

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAML Assertion Breakdown (cont)

SAML RESPONSE (HTTP POST) –> idbroker.webex.com

```
<samlp:Response ID="_6cd9c53d-c3ac-4b01-8232-72f2328bb129" Version="2.0" IssueInstant="2022-04-08T18:49:58.218Z"
Destination="https://idbroker.webex.com/idb/Consumer/metaAlias/8ad51c16-13ad-43e8-a390-2f653ff28e99/sp"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="s2a69bda9b2e9a5c46e5ec3777cce54811c30b9003"
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" >
        <Issuer
                xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://ADFS01.thestoj.com/adfs/services/trust
        </Issuer>
        <samlp:Status>
                <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
```

SAML 2.0 – 3.2.2 Complex Type StatusResponseType

A subordinate status code that provides more specific information on an error condition. Note that responders MAY omit subordinate status codes in order to prevent attacks that seek to probe for additional information by intentionally presenting erroneous requests.

Sample responses:
Success
The request succeeded. Additional information MAY be returned in the <StatusMessage> and/or <StatusDetail> elements.

InvalidNameIDPolicy
The responding provider cannot or will not support the requested name identifier policy.

SAML 2.0 – 5.4.5 KeyInfo

XML Signature defines usage of the <ds:KeyInfo> element. SAML does not require the use of <ds:KeyInfo>, nor does it impose any restrictions on its use. Therefore, <ds:KeyInfo> MAY be absent.

Contains x509 Certificate information

```
<ds:Signature
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
                <ds:Reference URI="#_fcc3db6e-865e-4386-8be1-90dd9c478413">
                        <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                        <ds:DigestValue>WvsompKbJ8b7cebxTzl+KXX2DRSrszsljfnfK2BXxxk=</ds:DigestValue>
                </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>%SIG_DATA%</ds:SignatureValue>
        <KeyInfo
                xmlns="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                        <ds:X509Certificate>%CERT_DATA%</ds:X509Certificate>
                </ds:X509Data>
        </KeyInfo>
</ds:Signature>
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAML Assertion Breakdown (cont)

SAML RESPONSE (HTTP POST) –> idbroker.webex.com

8.3 Name Identifier Format Identifiers

Webex supports NameID format:

- 8.3.1 – unspecified
- 8.3.2 – emailAddress
- 8.3.8 – transient

2.5 Conditions

- ***2.5.1.2 Attributes NotBefore and NotOnOrAfter***

The **NotBefore** and **NotOnOrAfter** attributes specify time limits on the validity of the assertion within the context of its profile(s) of use. They do not guarantee that the statements in the assertion will be correct or accurate throughout the validity period.

```
<Subject>
        <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://ADFS01.thestoj.com/adfs/services/trust"
SPNameQualifier="https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99" >THESTOJAD\pstojano</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <SubjectConfirmationData InResponseTo="s2a69bda9b2e9a5c46e5ec3777cce54811c30b9003" NotOnOrAfter="2022-04-
08T18:54:58.218Z" Recipient="https://idbroker.webex.com/idb/Consumer/metaAlias/8ad51c16-13ad-43e8-a390-2f653ff28e99/sp" />
        </SubjectConfirmation>
</Subject>
<Conditions NotBefore="2022-04-08T18:49:58.218Z" NotOnOrAfter="2022-04-08T19:49:58.218Z" >
        <AudienceRestriction>
                <Audience>https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99</Audience>
        </AudienceRestriction>
</Conditions>
<AttributeStatement>
        <Attribute Name="uid">
                <AttributeValue>pstojano@thestoj.com</AttributeValue>
        </Attribute>
</AttributeStatement>
```

2.7.3.1.1 Element <AttributeValue>

The <AttributeValue> element supplies the value of a specified SAML attribute. It is of the xs:anyType type, which allows any well-formed XML to appear as the content of the element. If the data content of an <AttributeValue> element is of an XML Schema simple type (such as xs:integer or xs:string), the datatype MAY be declared explicitly by means of an xsi:type declaration in the <AttributeValue> element. If the attribute value contains structured data, the necessary data elements MAY be defined in an extension schema.

2.5.1.4 Elements <AudienceRestriction> and <Audience>

A URI reference that identifies an intended audience. The URI reference MAY identify a document that describes the terms and conditions of audience membership. It MAY also contain the unique identifier URI from a SAML name identifier that describes a system entity (see Section 8.3.6).

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Understanding Webex SSO Security Certificates

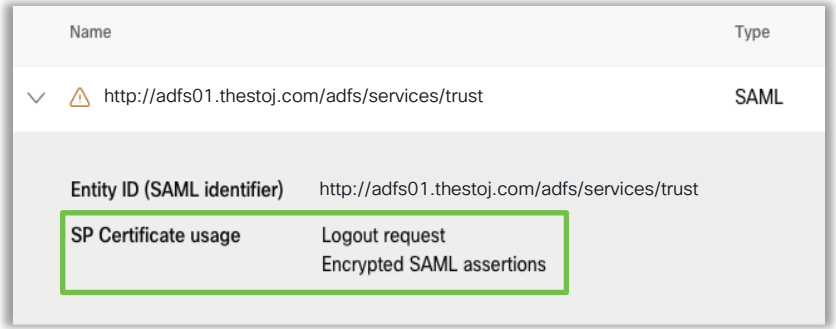
Two types of certificates are used with Webex Single Sign-on

1. IdP Certificate
2. Webex SP Certificate

Certificates are used for both Signing and Encrypting

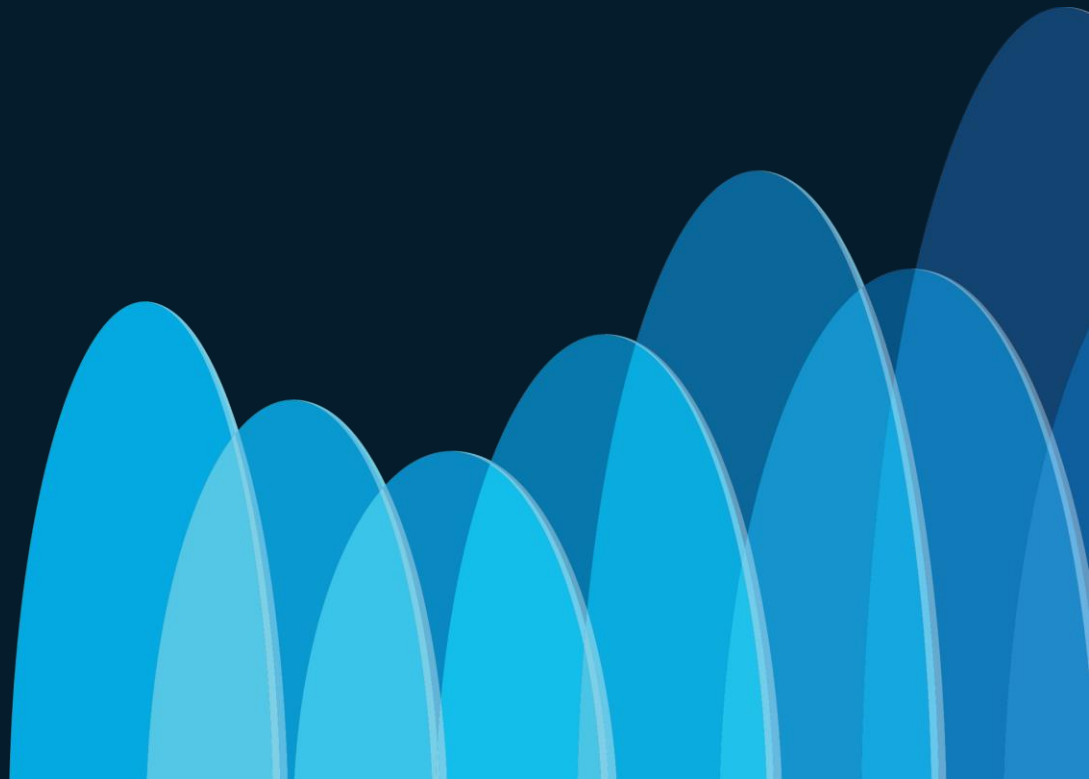
- Encrypting means the IdP will use **the Webex SP public key** to write a message and Webex will use **its private key** to read it.
- Signing means the IdP will use **its own private key** to write the message signature and the Webex SP will use **the IdP public key** to check if it is really the IdP.

Organization Settings > Authentication > Manage SSO and IdPs



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

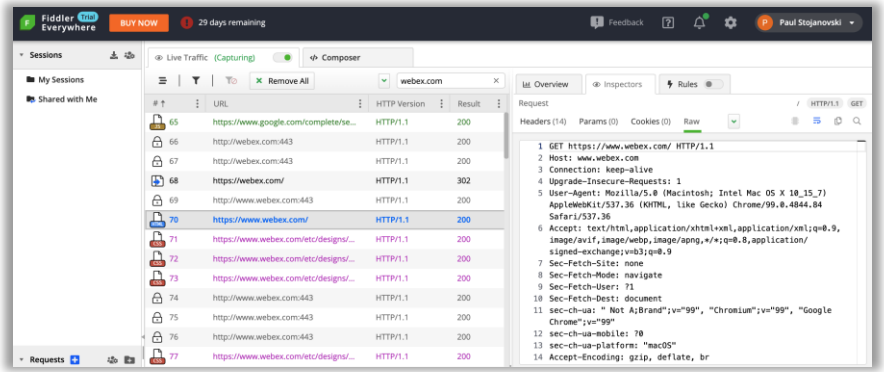
Tools & Log Collection



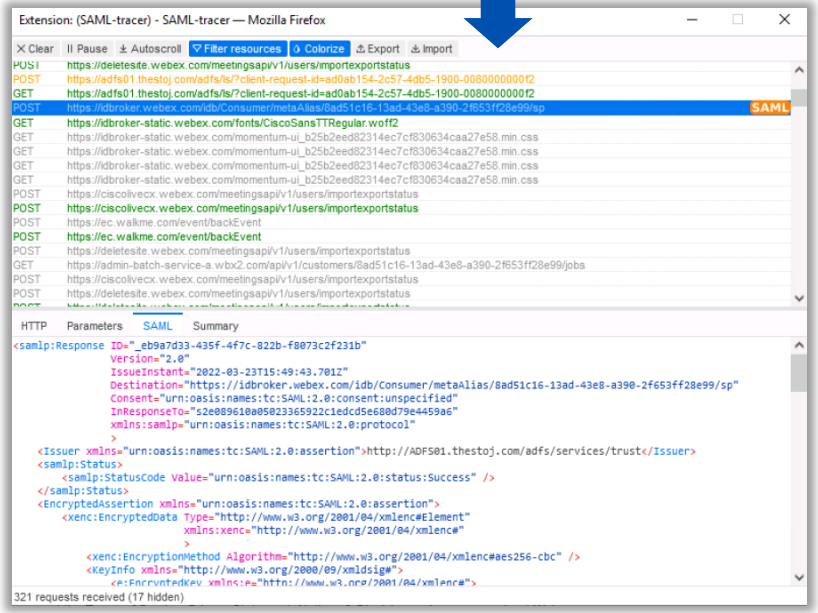
Single Sign-On Troubleshooting Tools

1. **SAML Tracer** – Available for Chrome and Firefox

2. Fiddler



3. Browser Inspection Trace

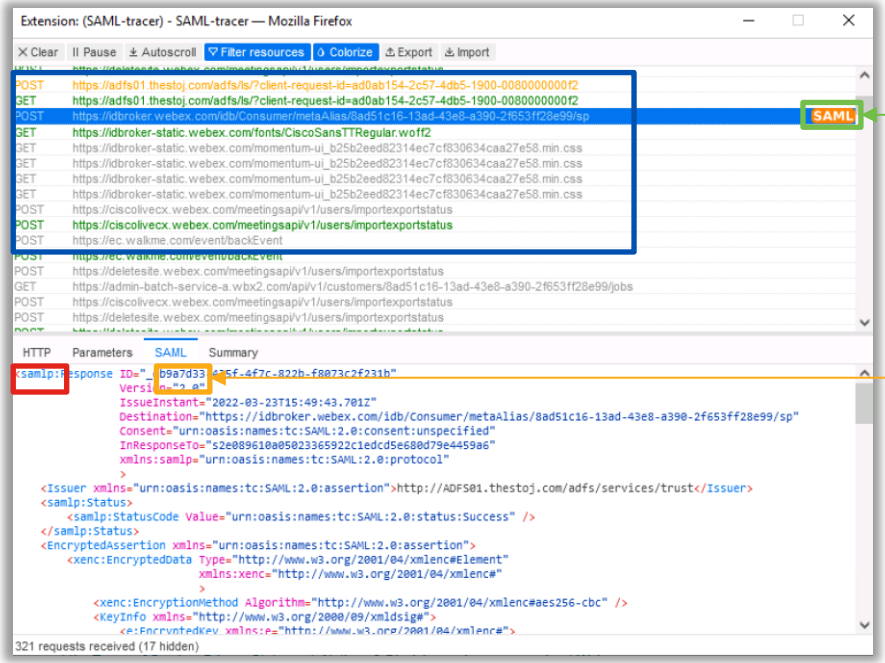


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAML Tracer

SAML-tracer is a Firefox/Chrome extension that aims to make debugging of SAML- and WS-Federation-communication between websites easier. It is a request logger that in addition to showing normal requests, also highlights and decodes SAML messages that are transmitted.

Each HTTP request/response is recorded with method type and full URL



Messages including SAML data are marked with a SAML logo

Request and response headers captured

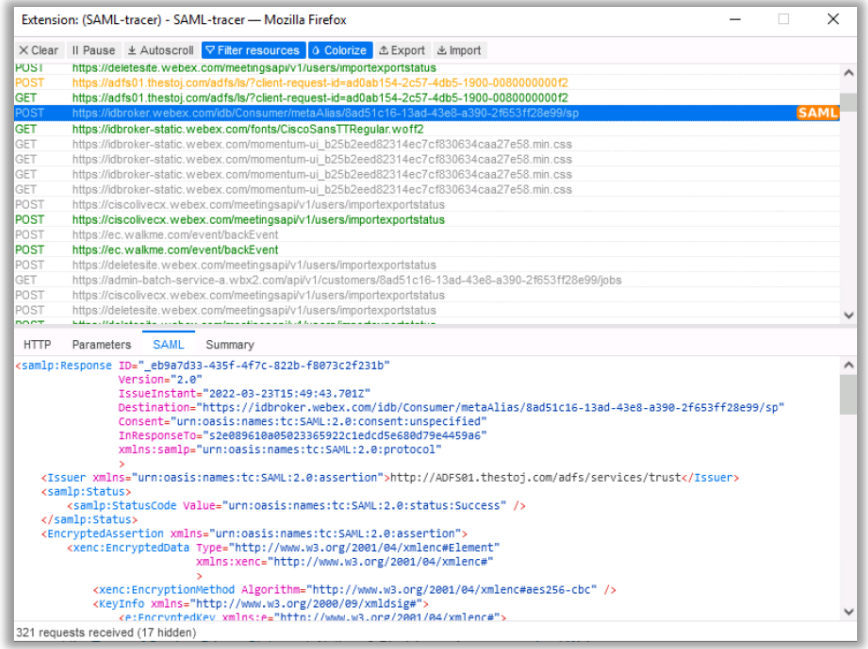
Full SAML response included in body

*Note: **Does not** work for **Webex App**-based authentication issues*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Handling Encrypted SAML Assertions

- Troubleshooting may require you to temporarily decrypt the SAML assertion
- Refer to your IdP documentation for instructions on how to accomplish this

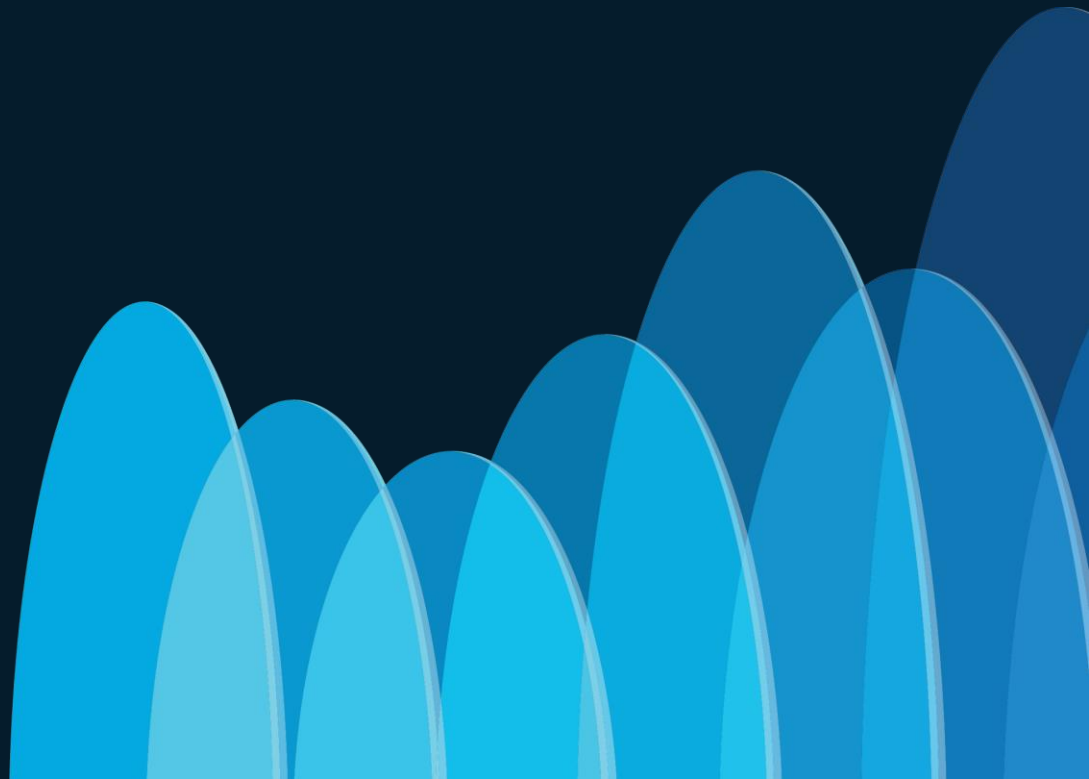


On ADFS Server, have ADFS admin run this command
Set-ADFSRelyingPartyTrust -TargetIdentifier SPEntityID (get from Metadata) -EncryptClaims $False

Example - Set-ADFSRelyingPartyTrust -TargetIdentifier https://idbroker.webex.com/bd1db2d6-dfe3-4a8f-8082-3dc26deee307 -EncryptClaims $False (get from Metadata)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single sign-on Common Issues



Top issues observed by TAC

= Hidden Slide

Configuration (SAML Assertion)

1. Attribute value is mismatched
2. Identity Provider NTP is out of sync
3. NameID format not supported by IdP
4. User inactive in Control Hub
5. User not permitted for authentication
6. Single Logout incorrectly/not configured

Certificates

7. Identity Provider Certificate Expiration
8. Webex SP Certificate Expiration
9. Failed to decrypt SAML Assertion
10. ADFS CRL Check Failing

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Invalid Status code in Response

IdP-driven error response

okta | Microsoft Entra ID | ADFS | PingIdentity | DUO | f5

Cisco Webex

Single Sign On failed.
Invalid Status code in Response.

TrackingID: NA_874dad91-aeff-4a38-8e4e-5439af83ebe0

SAML RESPONSE

```
<samlp:Status> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:
Responder"> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:
RequestDenied" /> </samlp:StatusCode>
</samlp:Status>
```

`urn:oasis:names:tc:SAML:2.0:status:Responder`

The request could not be performed due to an error on the part of the SAML responder or SAML authority.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Invalid Status code in Response

IdP-driven error response

okta | Microsoft Entra ID | ADFS | PingIdentity | DUO | F5

SAML RESPONSE

```
<samlp:Status> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:
Responder"> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:
RequestDenied" /> </samlp:StatusCode>
</samlp:Status>
```

- Issue is originated from the Identity Provider
- Identity Provider logs are required for troubleshooting
- There isn't one specific configuration that elicits this response

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Invalid Status code in Response

Log collection

PingIdentity

- PingFederate supports a wide range of logging.
  - Security audit logging
    - Activities from SSO, SLO, OAuth, WS-Trust STS, and SCIM inbound provisioning transactions are recorded in the security audit log, the audit.log file, located in the **<pf_install>/pingfederate/log**
  - Server logging
    - When configured to log DEBUG messages (for troubleshooting purpose), it records all runtime and administrative events, including status and error messages that can be used for troubleshooting, in the **<pf_install>/pingfederate/log/server.log** file

Full list of logging option can be found here

ADFS

- Login to your ADFS server
- Open the Window Event Viewer
- Under the *Applications and Services logs > ADFS* folder select **Admin**

Microsoft ADFS documentation for Admin logs

okta

- Login to the Okta admin portal
- Select *Applications > Applications* then choose **Cisco Webex**
- Select **View Logs**

Okta documentation for System Logs

Microsoft Entra ID

- Login to the Entra admin portal
- Select **Azure Active Directory** from the *Azure services* menu
- Under *Monitoring* select **Sign-in logs**

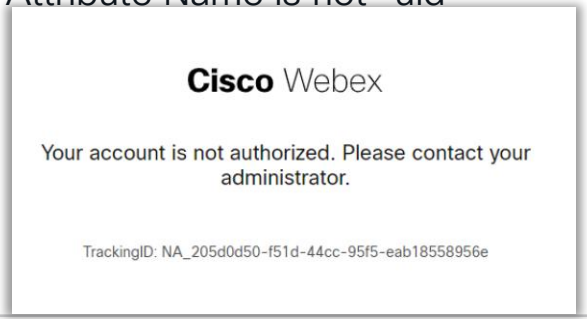
Microsoft Azure documentation for Sign-in logs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

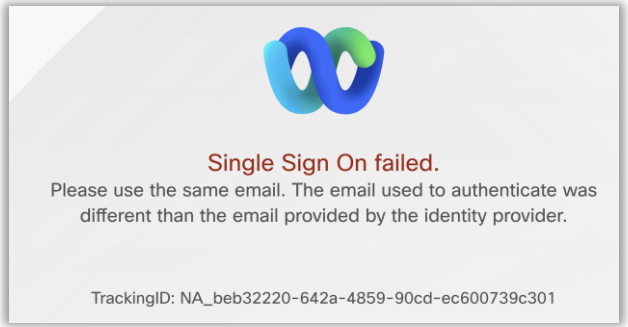
1 Attribute Value Mismatch

This issue can be cause be several possible conditions:

- Attribute Value passed is not an email
- No Attribute Value is passed at all
- Attribute Name is not “uid”



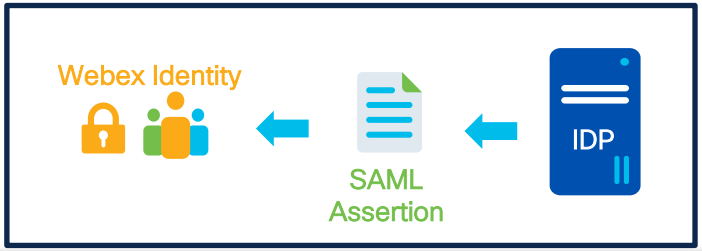
- Email address does not match Webex Identity



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

1 Attribute Value Mismatch

Attribute Value does not match



SAMPLE BAD ASSERTIONS

1

```
<AttributeStatement>
        <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
                <AttributeValue>pstojano@thestoj.com</AttributeValue>
        </Attribute>
</AttributeStatement>
```

Attribute Name not passed as “uid”

2

```
<AttributeStatement>
        <Attribute Name="uid">
                <AttributeValue>Paul Stojanovski</AttributeValue>
        </Attribute>
</AttributeStatement>
```

Email address not passed as a AttributeValue

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

2 NTP Out of Sync

REMEDIATION

1. Check the clock on the IdP
2. Check connectivity to NTP source
3. Choose different NTP source

ACTUAL TIME
= 02-08-2022 @ 18:40:30 GMT

Webex Identity

SAML Assertion

IDP

```
<Subject>
        <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://ADFS01.thestoj.com/adfs/services/trust"
SPNameQualifier="https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99" >THESTOJAD\pstojano</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <SubjectConfirmationData InResponseTo="s2a69bda9b2e9a5c46e5ec3777cce54811c30b9003" NotOnOrAfter="2022-04-
08T18:54:58.218Z" Recipient="https://idbroker.webex.com/idb/Consumer/metaAlias/8ad51c16-13ad-43e8-a390-2f653ff28e99/sp" />
        </SubjectConfirmation>
</Subject>
<Conditions NotBefore="2022-04-08T18:49:58.218Z" NotOnOrAfter="2022-04-08T19:49:58.218Z" >
                <Audience>https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99</Audience>
        </AudienceRestriction>
</Conditions>
<AttributeStatement>
        <Attribute Name="uid">
                <AttributeValue>pstojano@thestoj.com</AttributeValue>
        </Attribute>
</AttributeStatement>
```

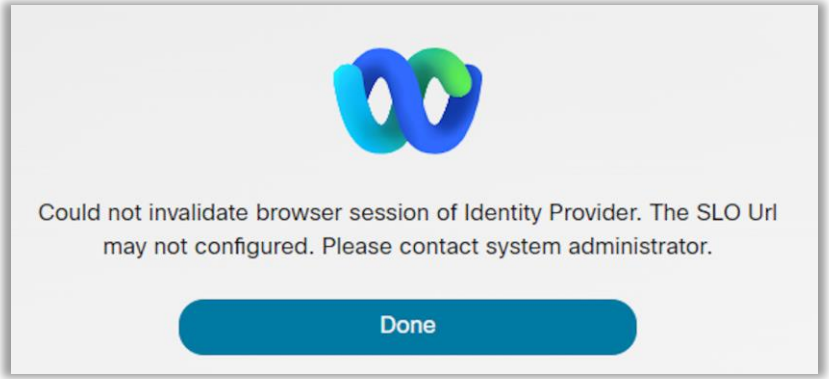
2.5 Conditions

- *2.5.1.2 Attributes NotBefore and NotOnOrAfter*

The **NotBefore** and **NotOnOrAfter** attributes specify time limits on the validity of the assertion within the context of its profile(s) of use. They do not guarantee that the statements in the assertion will be correct or accurate throughout the validity period.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

6 Single Logout Failure



- Condition occurs when **no SLO request** is made to the IdP
- Requires inspection of the IdP metadata file
  - *This can be downloaded directly from your IdP*

```
<?xml version="1.0" encoding="windows-1252"?>
<md:EntityDescriptor entityID="http://www.okta.com/exk4g4480fVW60QhS5d7"
                     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
                     <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
                                          <md:KeyDescriptor use="signing">
                                                               <ds:KeyInfo
                                                                                    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                                                                    <ds:X509Data>
                                                                                                         <ds:X509Certificate>%CERT_DATA%ds:X509Certificate>
                                                                                    </ds:X509Data>
                                                               </ds:KeyInfo>
                                          </md:KeyDescriptor>
                                          <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
                                          <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
                                          <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev-3877412.okta.com/app/ciscocommonidentity/exk4g4480fVW60QhS5d7/sso/saml"/>
                                          <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://dev-3877412.okta.com/app/ciscocommonidentity/exk4g4480fVW60QhS5d7/sso/saml"/>
                     </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

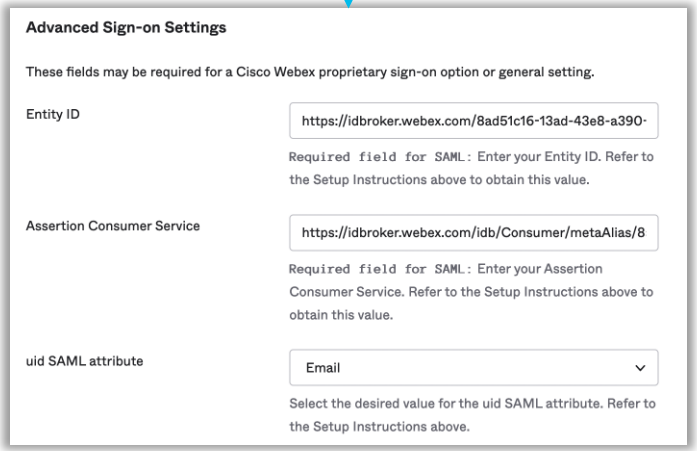
No SLO statement

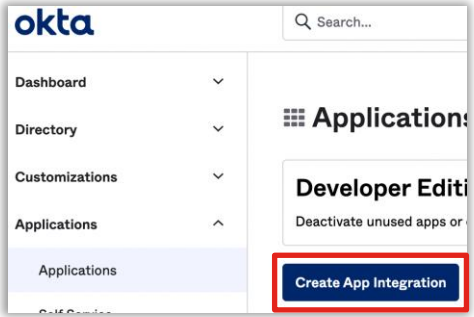
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single Logout Failure

The okta use case

- Okta offers a Cisco Webex app integration
- App covers basic Single sign-on features
  - App integration DOES NOT include SLO
- To leverage SLO you must build the integration using the Create App Integration option



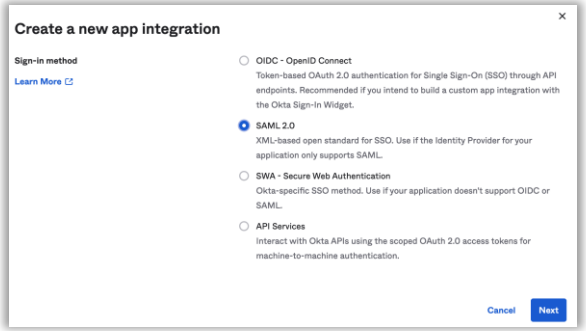


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single Logout Failure

The okta use case

1. Provide the integration a name (Webex)
2. Configure the SAML attributes (defined below)



Setting	Description	Example
Single sign on URL	The location where the SAML assertion is sent with a HTTP POST. This is often referred to as the SAML Assertion Consumer Service (ACS) URL for your application.	https://idbroker.webex.com/idb/Consumer/metaAlias/8ad51c16-13ad-43e8-a390-2f653ff28e99/sp
Audience URI (SP Entity ID):	The application-defined unique identifier that is the intended audience of the SAML assertion. This is most often the SP Entity ID of your application.	https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99
NameID format	Identifies the SAML processing rules and constraints for the assertion's subject statement. Use the default value of 'Unspecified' unless the application explicitly requires a specific format.	Unspecified
Enable Single Logout	Enable SAML Single Logout.	Allow application to initiate Single Logout
Single Logout URL	The location where the logout response will be sent.	https://idbroker.webex.com/idb/SPSloRedirect/metaAlias/8ad51c16-13ad-43e8-a390-2f653ff28e99/sp
SP Issuer	The location where the logout response will be sent.	https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99
Signature Certificate	Determines the public key certificate used to verify the digital signatures.	Either the Cisco self-sign or IdenTrust certificate

Note: Okta does not sign out web applications – Okta SLO documentation

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single Logout Success
Expected REQUEST / RESPONSE

SAML TRACER

POST	https://dev-3877412.okta.com/app/dev-3877412_webex_1/exk4iigu1q8bXRnlv5d7/slo/saml	SAML
GET	https://ok12static.oktacdn.com/assets/img/icons/favicons/favicon-96x96.de988286141a33ca04fcfaa07679f345.png	
GET	https://ok12static.oktacdn.com/assets/img/icons/favicons/favicon-32x32.99bc356b6e293b927f9e3a2b69761c26.png	
GET	https://ok12static.oktacdn.com/assets/img/ui/indicators/interstitial-dark-blue-brand.d4ca51b5579d1772af159f12276beb72.gif	
POST	https://idbroker.webex.com/idb/SPSloRedirect/metaAlias/8ad51c16-13ad-43e8-a390-2f653ff28e99/sp	SAML

SLO REQUEST

```
<samlp:LogoutRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://dev-3877412.okta.com/app/dev-
3877412_webex_1/exk4iigu1q8bXRnlv5d7/slo/saml" ID="s298f7858cad33d4c8999810f6eadbb34079172c50" IssueInstant="2022-04-
04T12:43:16Z" Version="2.0" >
    <saml:Issuer
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99
    </saml:Issuer>
    <ds:Signature
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference URI="#s298f7858cad33d4c8999810f6eadbb34079172c50">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>5VZDlg98hczB8UDwV+uiC4mJbz6El3hCoSUYJ0ghpO8=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue> %SIG_DATA%</ds:SignatureValue>
    </ds:Signature>
    <saml:NameID
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
>pstojano@thestoj.com
    </saml:NameID>
    <samlp:SessionIndex
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">s2b6705e2c9c2587dec57b2d4017c7634f0e381509
    </samlp:SessionIndex>
</samlp:LogoutRequest>
```

SLO RESPONSE

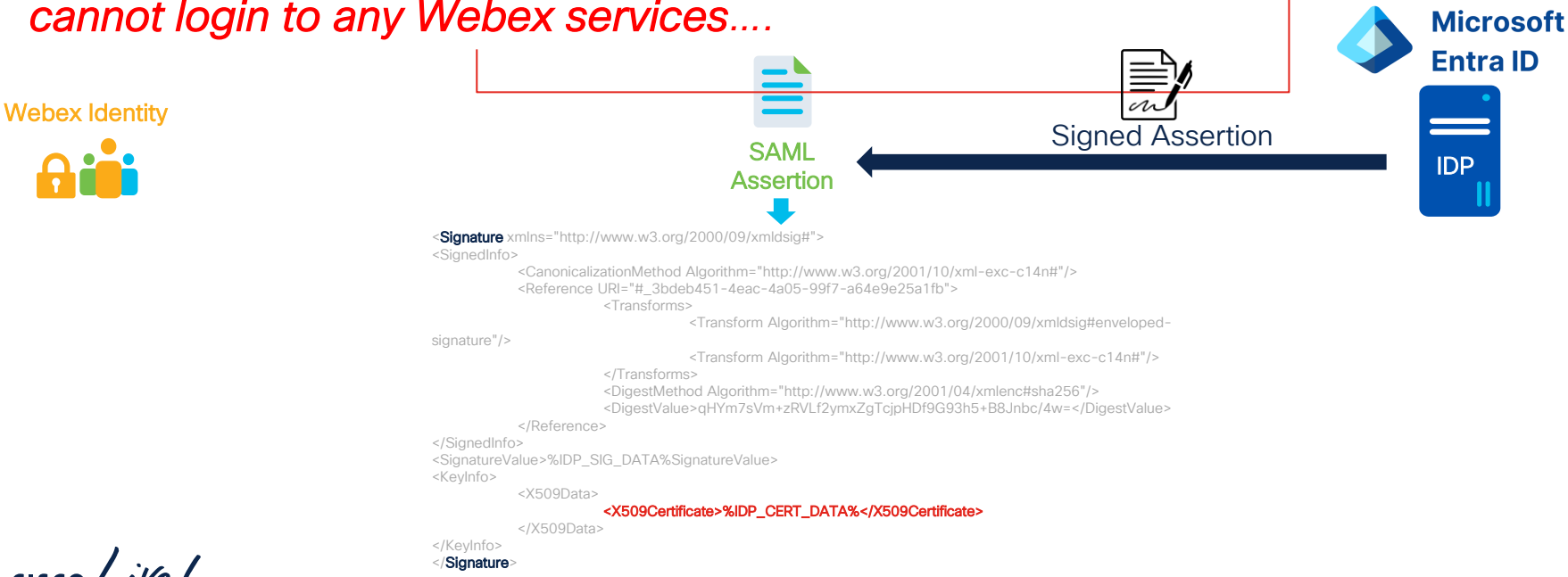
```
<saml2p:LogoutResponse Destination="https://idbroker.webex.com/idb/SPSloRedirect/metaAlias/8ad51c16-13ad-43e8-a390-
2f653ff28e99/sp"
                ID="id307356314219421958997O5"
                InResponseTo="s298f7858cad33d4c8999810f6eadbb34079172c50"
                IssueInstant="2022-04-04T12:43:16.667Z"
                Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
                 <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
                                xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
            >http://www.okta.com/exk4iigu1q8bXRnlv5d7
                </saml2:Issuer>
                <ds:Signature
                                xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <ds:SignedInfo>
                                                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                                                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
/>
                                                <ds:Reference URI="#id307356314219421958997O5">
                                                                <ds:Transforms>
                                                                                <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                                                                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                                                                </ds:Transforms>
                                                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>
                <ds:DigestValue>HBVHE8eU1uFFV09+Xg2SdDmlX8rq+Ve+ATT/RW6c5h4=</ds:DigestValue>
                                                </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue>%SIGNATURE_DATA%</ds:SignatureValue>
                                <ds:KeyInfo>
                                                <ds:X509Data>
                                                                <ds:X509Certificate>%CERT_DATA%ds:X509Certificate>
                                                </ds:X509Data>
                                </ds:KeyInfo>
                </ds:Signature>
                <saml2p:Status
                                xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
                                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
                </saml2p:Status>
</saml2p:LogoutResponse>
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

7 Invalid digital signature

Identity Provider Cert (IdP)

*Your company is about to **present on a major acquisition** and the CEO reports that **they cannot login to any Webex services....***



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Signing means the IdP will use its own private key to write the message signature and the Webex SP will use the IdP public key to check if it is really the IdP.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

7 Invalid digital signature

Identity Provider Cert (IdP)

*Your company is about to **present on a major acquisition** and the CEO reports that **they cannot login to any Webex services....***

Microsoft Entra ID

IDP

Signed Assertion

SAML Assertion

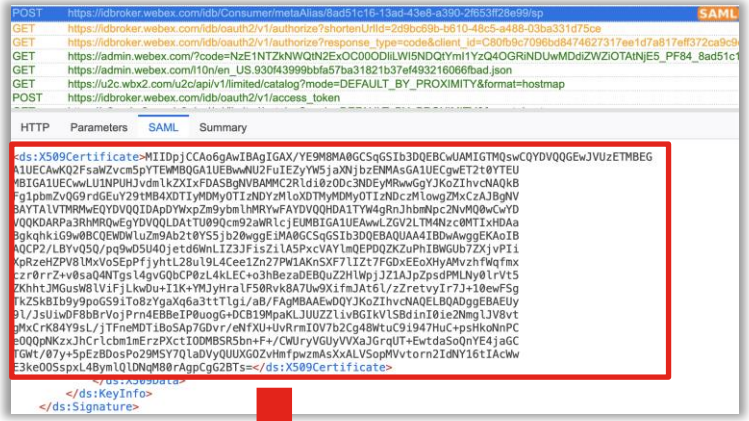
Webex Identity

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <Reference URI="#_3bdeb451-4eac-4a05-99f7-a64e9e25a1fb">
                <Transforms>
                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <DigestValue>qHYm7sVm+zRVLf2ymxZgTcjpHDf9G93h5+B8Jnbc/4w=</DigestValue>
        </Reference>
</SignedInfo>
<SignatureValue>%IDP_SIG_DATA%SignatureValue>
<KeyInfo>
        <X509Data>
                <X509Certificate>%IDP_CERT_DATA%</X509Certificate>
        </X509Data>
</KeyInfo>
</Signature>
```

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extracting Certificate from SAML Tracer

1. Launch SAML Tracer
2. Attempt authentication with user
3. In SAML Tracer, click on HTTP POST to idbroker.webex.com containing the SAML assertion
4. Click the SAML tab and locate **X509Certificate** raw certificate detail
5. Copy raw cert data into a notepad file encasing it with BEGIN and END CERTIFICATE statements
6. Save with .cer file extension then open the file



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IdP Expired Certificate Exception

Trust Anchors

*IdP cert will show updated in Control Hub **with no renewal warning if trust anchors are used***

If the Subject Name and Issuer Name match in both certificates *(IdP metadata and SAML Assertion)*, a trust anchor is established, and authentication succeeds.

webex by CISCO

webex Control Hub

Authentication
idbroker.webex.com

IdP Metadata

My Company Certificate

Subject Name
Common Name: mycompany.example.com

Serial Number: A1 B2 C3 D4 E5 F6 G7 H8

Issuer Name
Common Name: ca.caprovider.com

Not Valid Before: Thursday, March 21st, 2019
Not Valid After: Monday, March 21st, 2022

TRUST ANCHOR ESTABLISHED

SAML Assertion

IDP

My Company Certificate

Subject Name
Common Name: mycompany.example.com

Serial Number: H8 G7 F6 E5 D4 C3 B2 A1

Issuer Name
Common Name: ca.caprovider.com

Not Valid Before: Thursday, March 21st, 2022
Not Valid After: Monday, March 21st, 2024

IdP Metadata never updated in Control Hub

Certificate upgraded on day of expiration

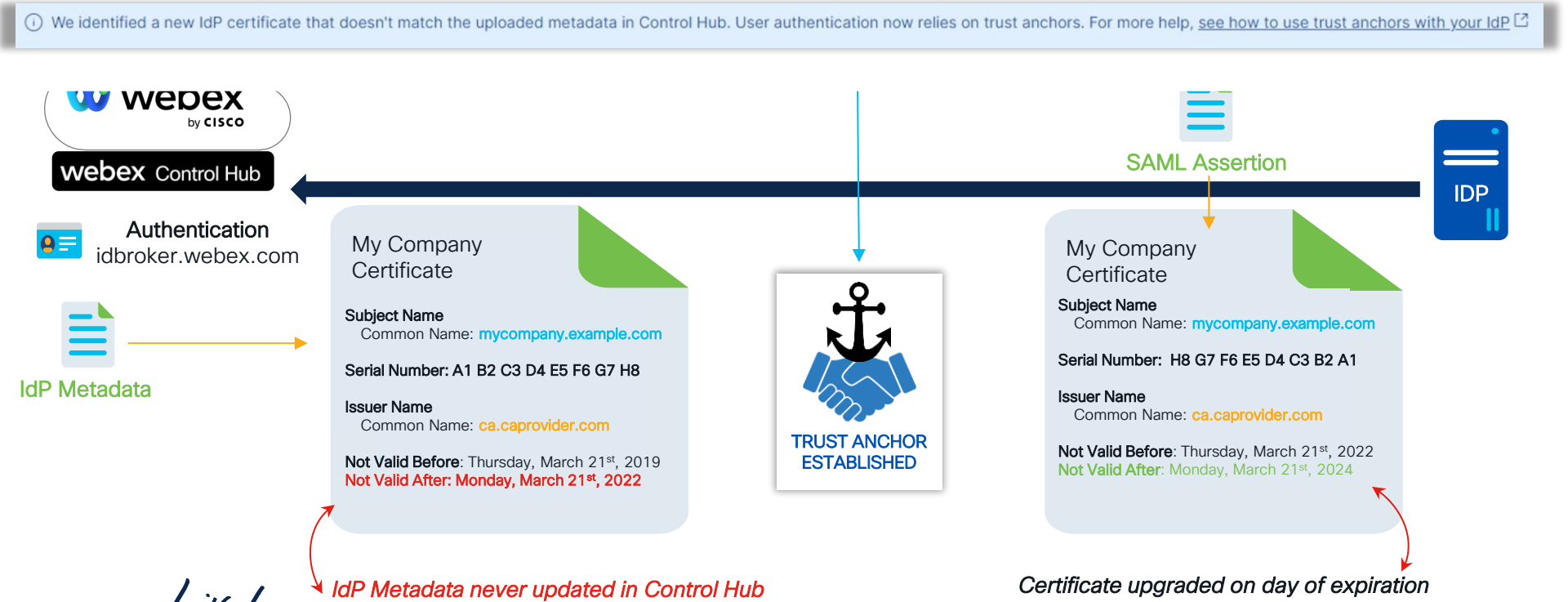
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IdP Expired Certificate Exception

Trust Anchors

*IdP cert will show updated in Control Hub **with no renewal warning if trust anchors are used***

If the Subject Name and Issuer Name match in both



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

8 Missing Assertion in Response

Webex (SP) Certificate Expired

*Your company is on the verge of **presenting their Q4 financials** and the CFO reports that they cannot login to any Webex services....*

```
<EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
   <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
         <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
            <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
               <X509Data>
                  <X509Certificate>%WEBEX_SP_CERT_DATA%</X509Certificate>
               </X509Data>
            </KeyInfo>
         </EncryptedKey>
      </KeyInfo>
   </EncryptedData>
</EncryptedAssertion>
```

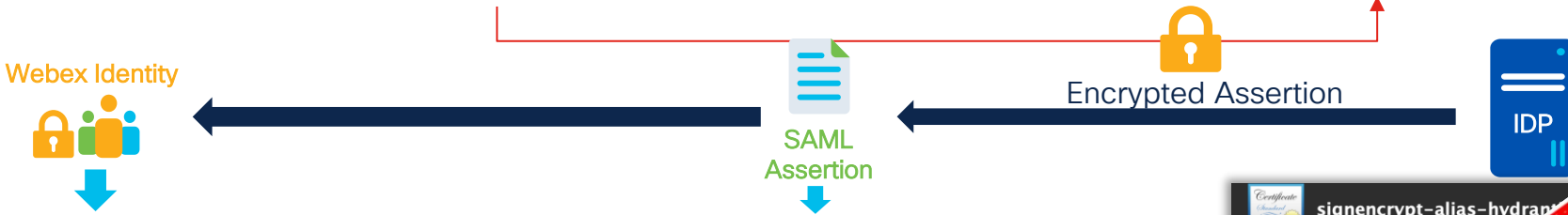

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Encrypting means the IdP will use the Webex SP public key to write a message and the Webex SP will use its private key to read it.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

8 Missing Assertion in Response
Webex (SP) Certificate Expired

*Your company is on the verge of **presenting their Q4 financials** and the CFO reports that **they cannot login to any Webex services....***

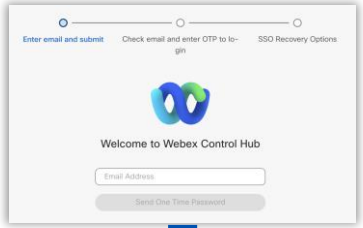


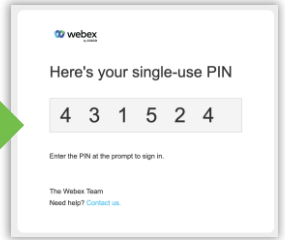
```
<EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
    <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <X509Data>
            <X509Certificate>%WEBEX_SP_CERT_DATA%</X509Certificate>
          </X509Data>
        </KeyInfo>
      </EncryptedKey>
    </KeyInfo>
  </EncryptedData>
</EncryptedAssertion>
```

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Remediation for “Expired” Certificate

No Access to the Control Hub





Video-based instructions

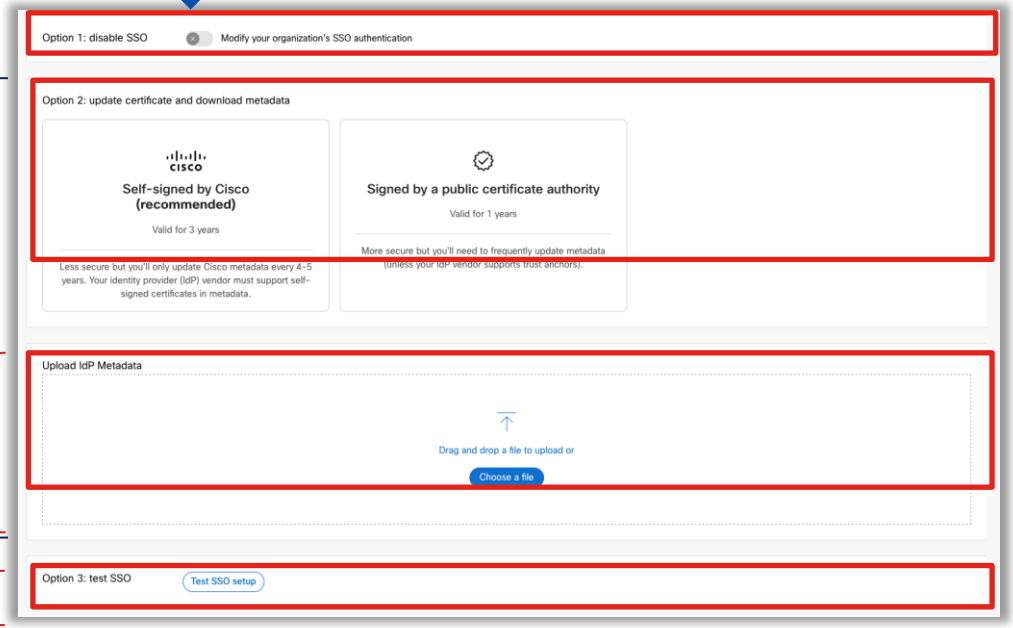
STEP 1

1. Request a One Time Password from https://admin.webex.com/manage-sso
2. Retrieve and Enter OTP

STEP 2

Click the option to Disable SSO

Restores access to Control Hub allowing you to renew the impacted certificate directly in Control Hub



STEP 3

Used for SP certificate expiration remediation

1. Download the latest Webex SP certificate
2. Upload certificate to the Identity provider

STEP 4

Used for IdP certificate expiration remediation

1. Renew certificate on Identity Provider
2. Download latest Identity Provider metadata file
3. Upload IdP Metadata file

Test new certificate configuration changes

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Hub: Remediation for “Expiring” Certificate

UPDATE IDP CERTIFICATE

⚠ https://sts.windows.net/<TenantID>/ is expiring soon.

1. Update IdP Cert on the Identity Provider
2. Generate a new IdP metadata file
3. Login to Control Hub
   - Organization Settings > Authentication > Manage SSO & IdPs
   - Upload IdP metadata and select the IdP metadata file generated from the IdP
   - Test your SSO configuration

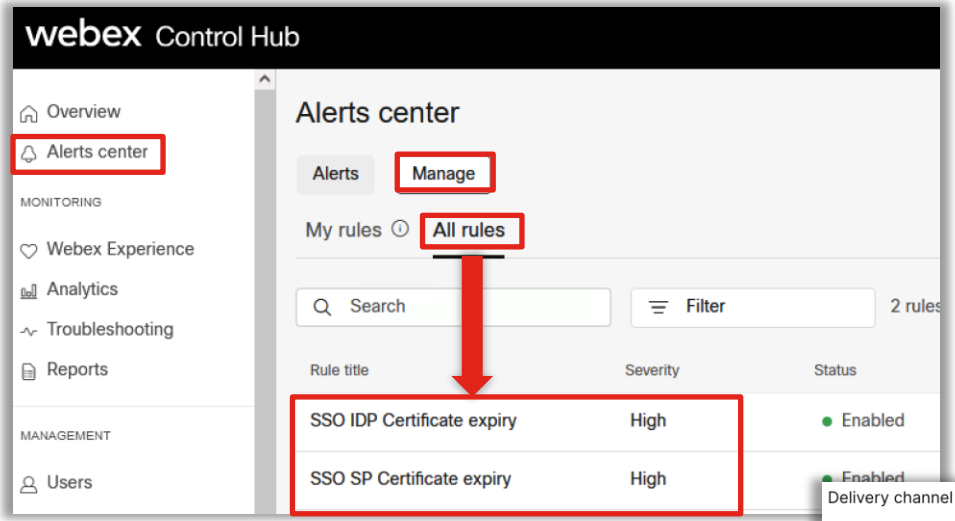
UPDATE SP CERTIFICATE

⚠ SP certificate is expiring soon.

1. Login to Control Hub
   - Organization Settings > Authentication
   - Next to the SP cert warning choose, **Renew certificate**
2. Download new Webex Metadata file
3. Import Webex Metadata file on your IdP
4. Return to Control Hub and choose **Updated all the IdPs** and select **Next**
5. Choose **Finish renewal**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

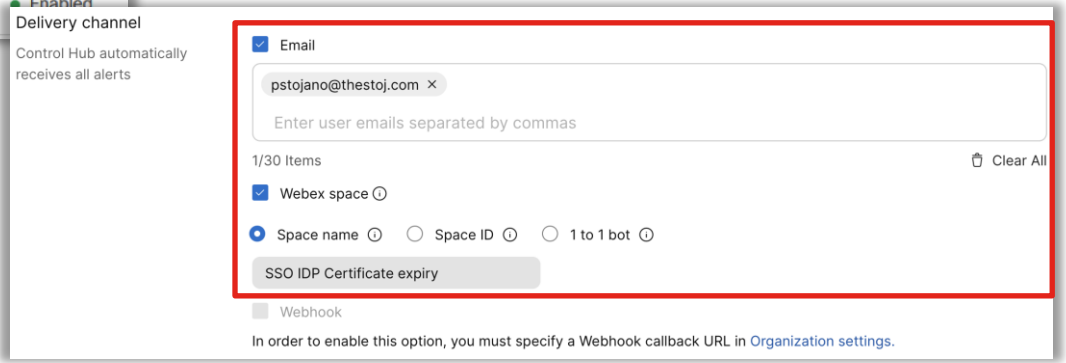
Certificate Expiration Prevention



One rule is configured per certificate type

DELIVERY CHANNEL

- Combination of Email or Webex space can be selected
- Initial reminder sent 60 days from expiration
- Email supports distribution lists and non-Webex Identity email addresses



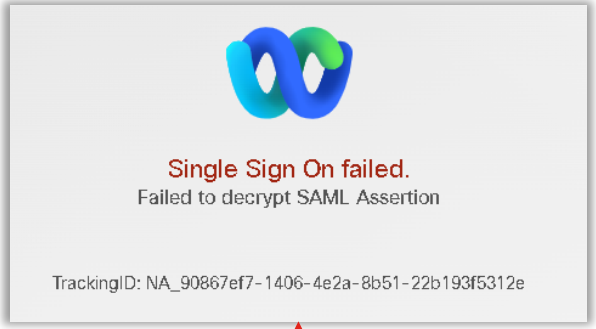
Partner Alert: Organization Name/ID is not present in the notification

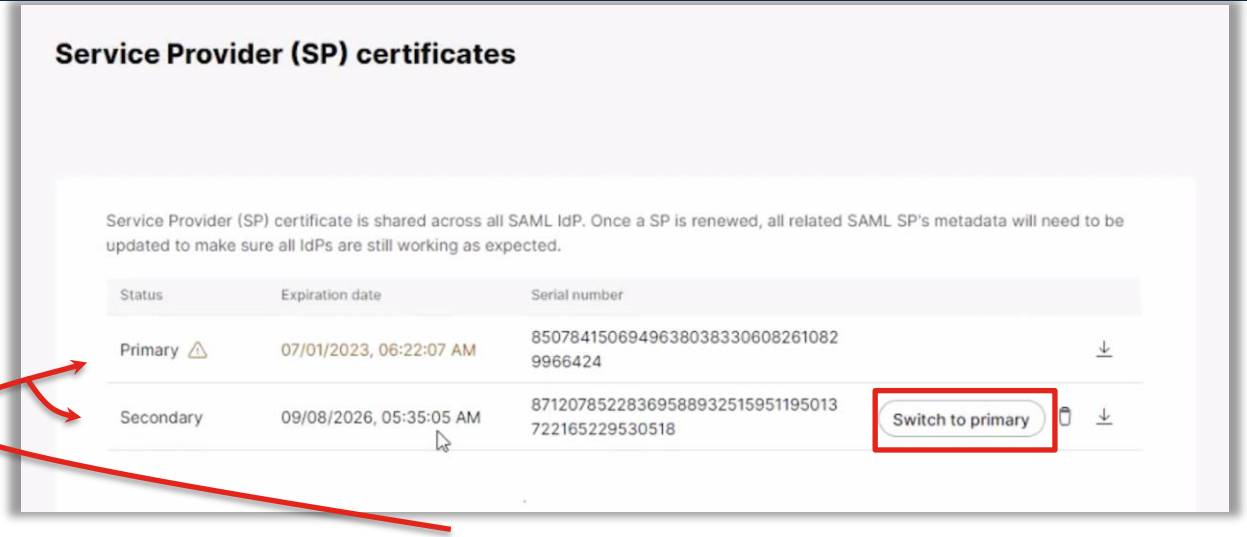
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

9 Failed to decrypt SAML Assertion

What are customers telling TAC?

I've updated my Webex SP certificate and now I'm no longer able to login!





If your IdP supports **multiple certificates** you will see two certificates in the table. The updated certificate will be listed as the **secondary certificate**.

Complete the certificate renewal process by selecting **Switch to primary** then choose Finish renewal

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

10 Invalid Response
CRL Check

Symptom:

I've just updated the Cisco Webex SP certificate and suddenly I'm unable to login. What's wrong with the Webex certificate?

ADFS LOGS

An error occurred during an attempt to build the certificate chain for the relying party trust 'https://idbroker.webex.com/8ad51c16-13ad-43e8-a390-2f653ff28e99' certificate identified by thumbprint '9C97C7321FA1C2B941981EEF50E4888FA0D97340'. **Possible causes are that the certificate has been revoked, the certificate chain could not be verified as specified by the relying party trust's encryption certificate revocation settings or certificate is not within its validity period.**

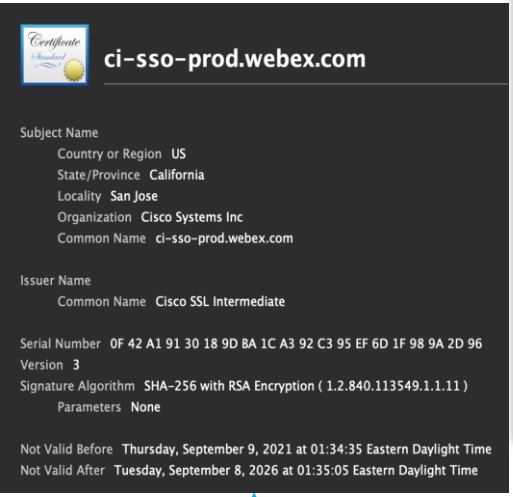
You can use Windows PowerShell commands in ADFS to configure the revocation settings for the relying party encryption certificate.

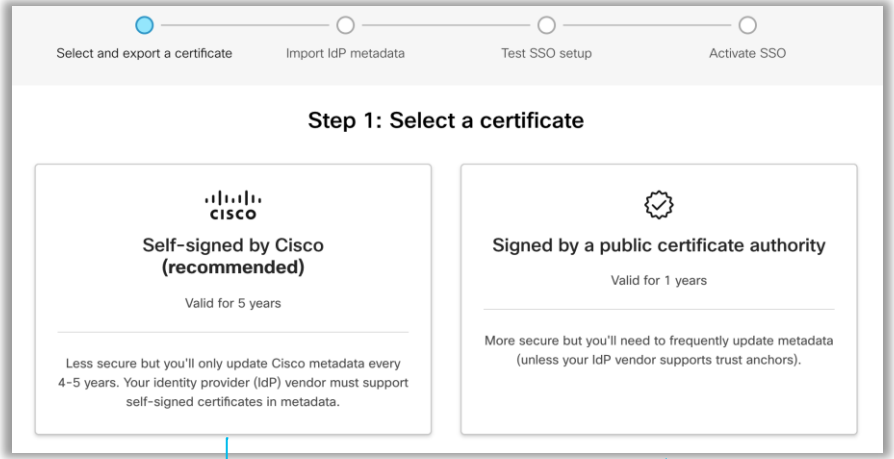
Relying party trust's encryption certificate revocation settings: CheckChainExcludeRoot

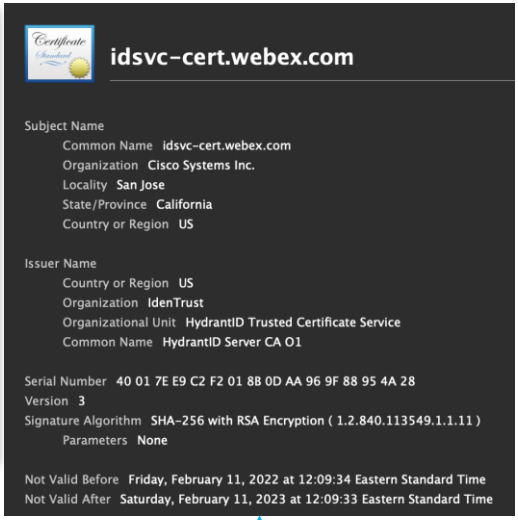
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

10 Single Sign-On Certificate Selection

CRL Check







Cert does not include CRL

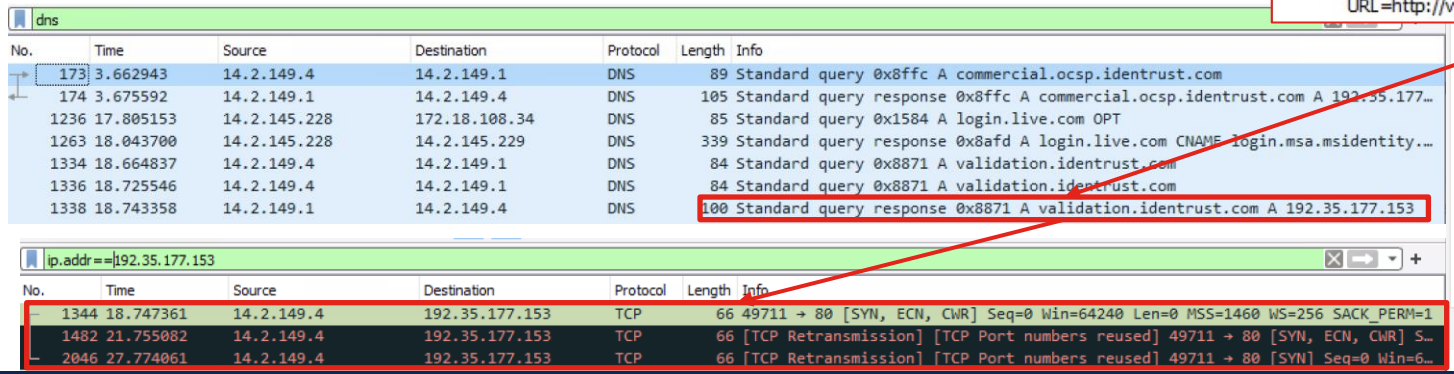
Cert includes a CRL

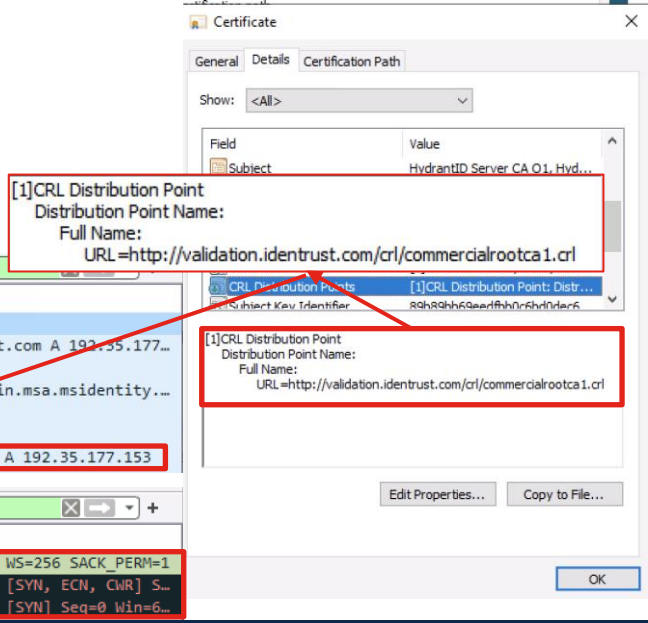
Extension=CRL Distribution Points (2.5.29.31)
Critical=NO
URI=http://validation.identrust.com/crl/hydrantidcao1.crl

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

10 ADFS Analysis and Root Cause

CRL Check





By default, ADFS performs Certificate Revocation checking

- For Webex self-signed cert no CRL is available so checking must be disabled.

```
Set-ADFSRelyingPartyTrust -TargetIdentifier https://idbroker.webex.com/<orgID> -EncryptionCertificateRevocationCheck None
```

- For Webex CA-signed cert communication TCP/80 must be opened to identrust.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Audience attribute not set

```
<AudienceRestriction>
    <Audience>https://idbroker.webex.com/
458d5400-5fc5-43aa-a77c-e5bcaef3de36
    </Audience>
</AudienceRestriction>
```

CSCwb36235

Audience is associated with the Condition element of SAML Assertion and that tells under which security conditions or context, the assertion is valid and provide some terms and conditions relating to such validity (like time validity of assertion, who can consume the assertion, etc). Typically, Audience will the EntityID of SP.

2.5.1.4 Elements <AudienceRestriction> and <Audience>

The `<AudienceRestriction>` element specifies that the assertion is addressed to one or more specific audiences identified by `<Audience>` elements. Although a SAML relying party that is outside the audiences specified is capable of drawing conclusions from an assertion, the SAML asserting party explicitly makes no representation as to accuracy or trustworthiness to such a party. It contains the following element:

`<Audience>`

A URI reference that identifies an intended audience. The URI reference MAY identify a document that describes the terms and conditions of audience membership. It MAY also contain the unique identifier URI from a SAML name identifier that describes a system entity (see Section 8.3.6).

The audience restriction condition evaluates to ***Valid*** if and only if the SAML relying party is a member of one or more of the audiences specified.

The SAML asserting party cannot prevent a party to whom the assertion is disclosed from taking action on the basis of the information provided. However, the `<AudienceRestriction>` element allows the SAML asserting party to state explicitly that no warranty is provided to such a party in a machine- and human-readable form. While there can be no guarantee that a court would uphold such a warranty exclusion in every circumstance, the probability of upholding the warranty exclusion is considerably improved.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single Sign-On FAQ & Limitations

- Why does authentication succeed when running the SSO Test in Control Hub but fails after turning SSO on?
  - This is often occurring because the test is using an existing authentication cookie. We recommend copying the authentication URL from the SSO Wizard into a private web browser to run the test.
- If a Control Hub linked Webex site is SSO integrated with Site Admin and the customer deploys the Webex App will authentication work against Control Hub or the SSO configured in Site Admin.
  - Authentication in this situation will be based on the SSO configuration in Site Admin. If the site decides to convert to Control Hub managed, then we require Control Hub to be setup for SSO.
- Does modifying the Single Sign-On configuration in Control Hub revoke end users OAuth tokens?
  - **No**, existing end user OAuth tokens are still valid.
- Can Single sign-on be enabled if my Webex organisation does not use Directory synchronization?
  - Yes. SSO and Directory solutions (DirSync, Entra ID) are independent from each other.
- What Identity Providers does Webex Control Hub support?
  - The full list of IdPs Webex has tested against is listed here. If your IdP is not listed, SSO can still be configured if the IdP uses SAML 2.0
- Will enabling Multi-Factor Authentication enable it for Control Hub, the Webex site, and Webex App?
  - Yes, if you choose the Allow mandatory MFA mandatory MFA for organization option.

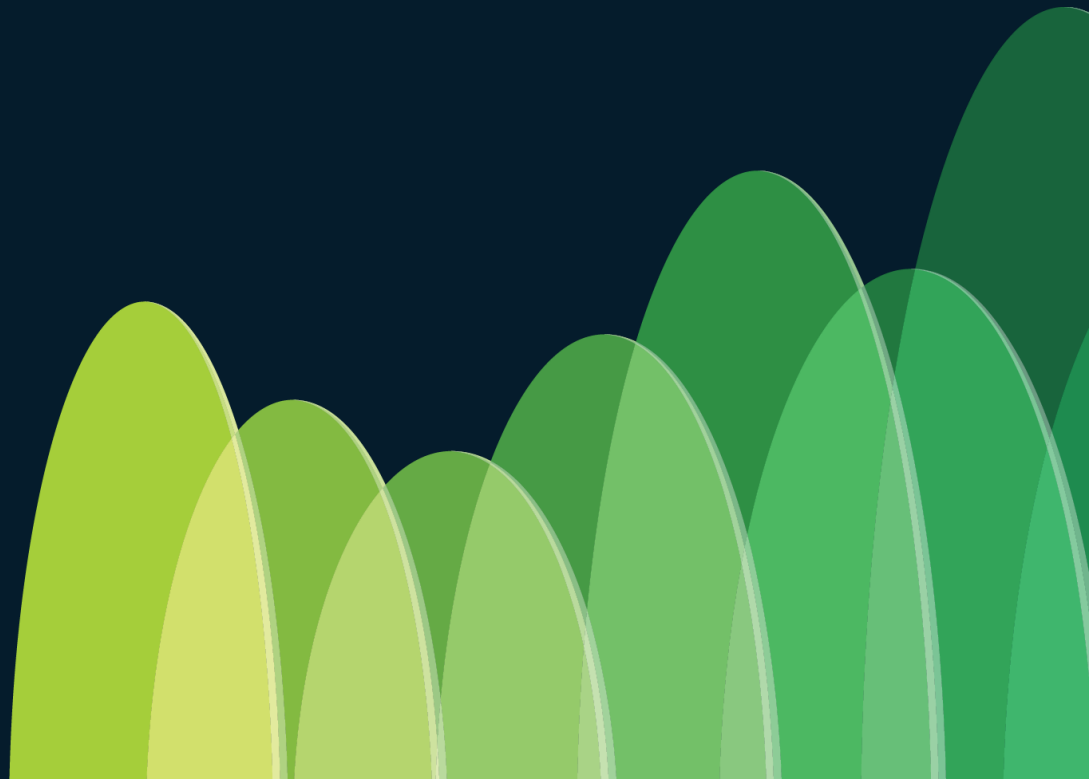
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single Sign-On FAQ & Limitations

- How does enabling Single Sign-on impact existing users, meetings, or devices?
  - There is no functionality impact. The only impact is where they are directed for authentication.
- Will Single-Sign-on synchronization overwrite local users in Control Hub?
  - When SSO is enabled, users are not synchronized to Control Hub unless JIT provisioning is configured. This will only configure new users
- Will Single-Sign-on synchronization overwrite local users in Control Hub?
  - When SSO is enabled, users are not synchronized to Control Hub unless JIT provisioning is configured. This will only configure new users
- Can we leverage the Multi-IdP feature to have a single user use different Identity Providers based on if they are on their PC (on-prem) versus Mobile (off-prem)
  - No, this is not possible today. Your identity strategy should be defined at the Identity Provider, not in Control Hub through this feature. If you do not want PCs to have access to the network off-prem then your Identity Provider should build policies to prevent that from occurring.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Call Routing



cisco Live!

Webex Calling Call Routing

- Three phases
  - Source classification
    - Type of call: user, premises, external
  - Destination selection
    - Where to send the call to: user, premises, PSTN, …
  - Screening and routing
    - Is this call allowed?

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

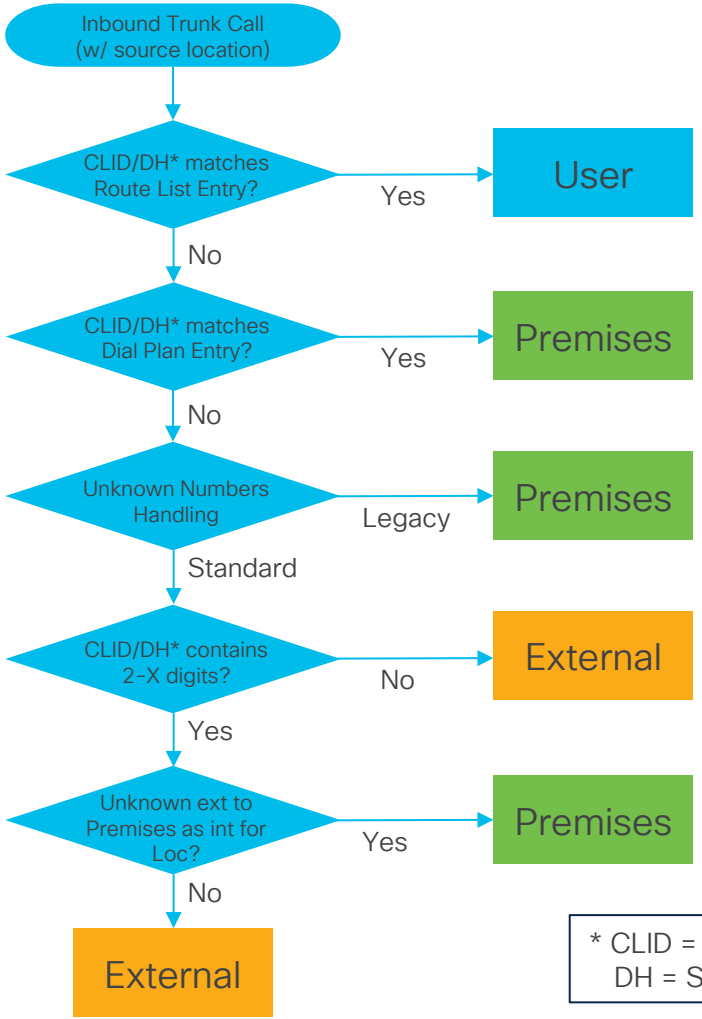
Call from	Classified as
Room devices, MPP, Webex app	User
Cloud PSTN (Cisco Calling Plan or Cloud Connect for Webex Calling)	External (PSTN)
Trunk (Local GW)	Premises or External*
Webex Calling Dedicated instance	User or External*

*based on calling party number (or diversion header if present) and configuration settings
→ see following slides

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

Calls from Local Gateway or Webex Calling DI



* CLID = Calling Party ID
DH = SIP Diversion Header

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

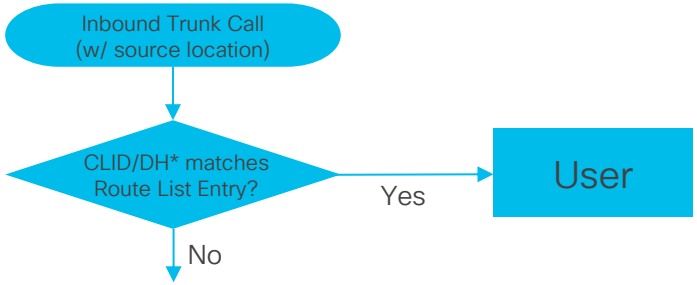
Calls from Local Gateway or Webex Calling DI

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

Calls from Local Gateway or Webex Calling DI

Match only considers route lists that use the incoming trunk as destination (via route group)



Number in Diversion header used if present, if not number in From header is used

```
INVITE sip:89943702@peering3.us.sipconnect.bcld.webex.com:5062 SIP/2.0
Via: SIP/2.0/TLS 64.102.250.137:5061;branch=z9hG4bK8BF831C1E
From: <sip:+19194766200@64.102.250.137>;tag=FD340CF9-200D
To: <sip:89943702@peering3.us.sipconnect.bcld.webex.com>
Call-ID: 2EB7BD48-EF7111ED-B8429147-F554AD62@64.102.250.137
Supported: timer,resource-priority,replaces
Min-SE:  1800
User-Agent: Cisco-SIPGateway/IOS-17.10.1a
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Contact: <sip:+19194766200@svs-rtp-dmz-cube9a.cube.ecatslab.com:5061;transport=tls>
Diversion: <sip:89915678@svs-rtp-dmz-cube9a.cube.ecatslab.com>
Expires: 180
Max-Forwards: 68
… snip …
```

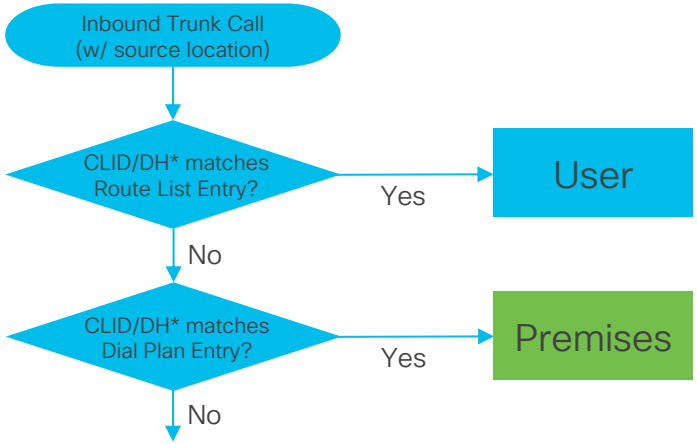
* CLID = Calling Party ID
  DH = SIP Diversion Header

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

Calls from Local Gateway or Webex Calling DI

Match only considers dial plans that use the inbound trunk as destination (directly or via route group).



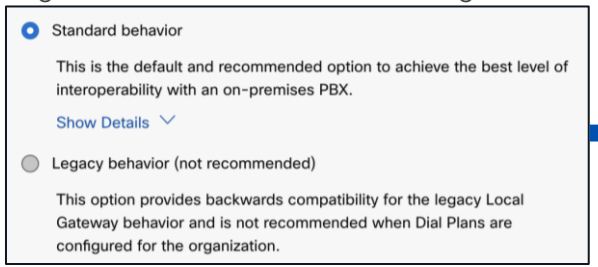
* CLID = Calling Party ID
DH = SIP Diversion Header

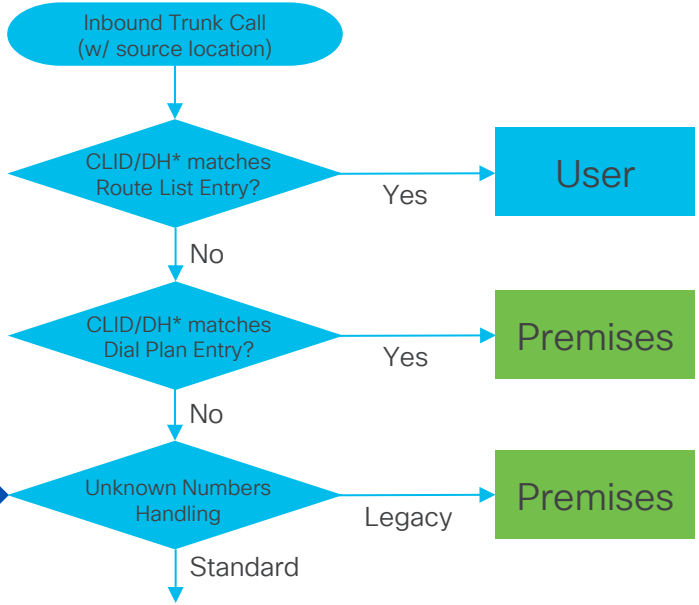
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

Calls from Local Gateway or Webex Calling DI

Org-wide unknown number handling



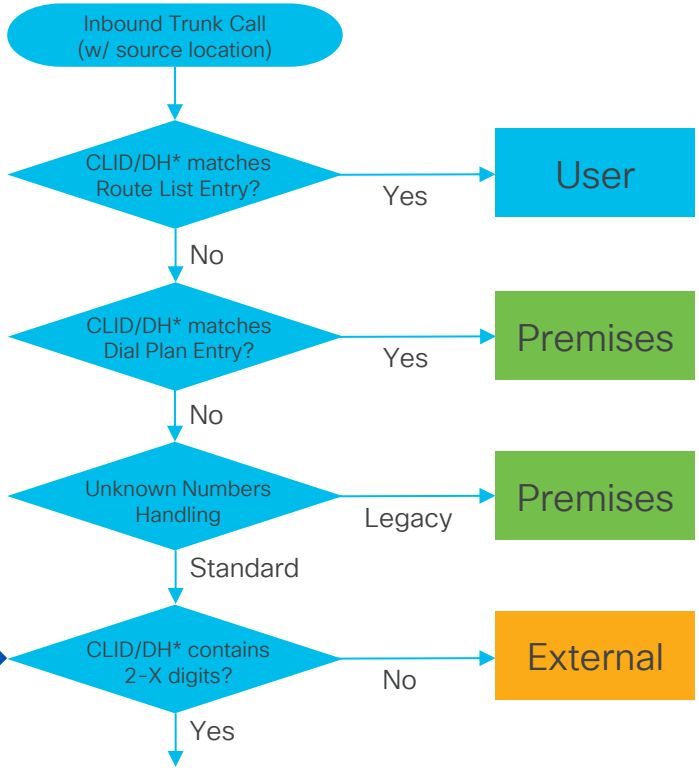


* CLID = Calling Party ID
DH = SIP Diversion Header

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

Calls from Local Gateway or Webex Calling DI



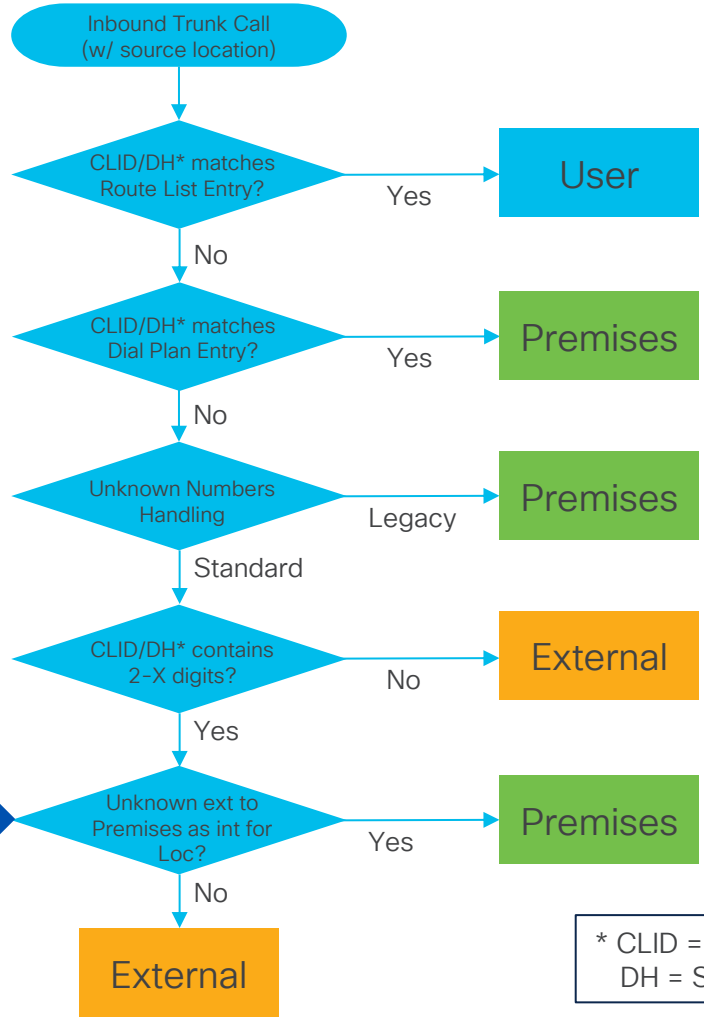
Org-wide unknown extension length

* CLID = Calling Party ID
DH = SIP Diversion Header

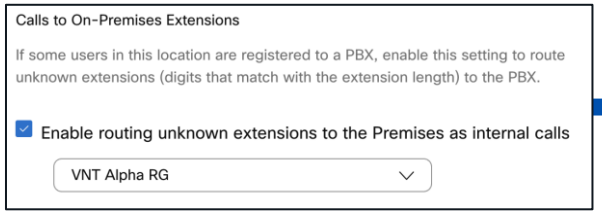
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

Calls from Local Gateway or Webex Calling DI



Trunk Location Configuration



Inbound trunk is destination for unknown extensions

* CLID = Calling Party ID
DH = SIP Diversion Header

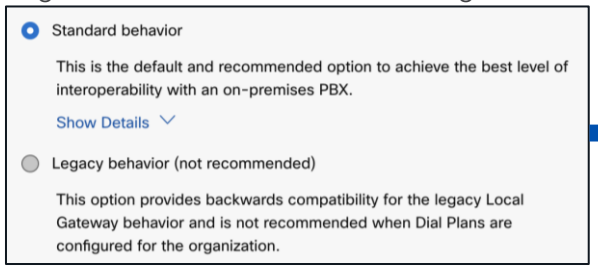
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

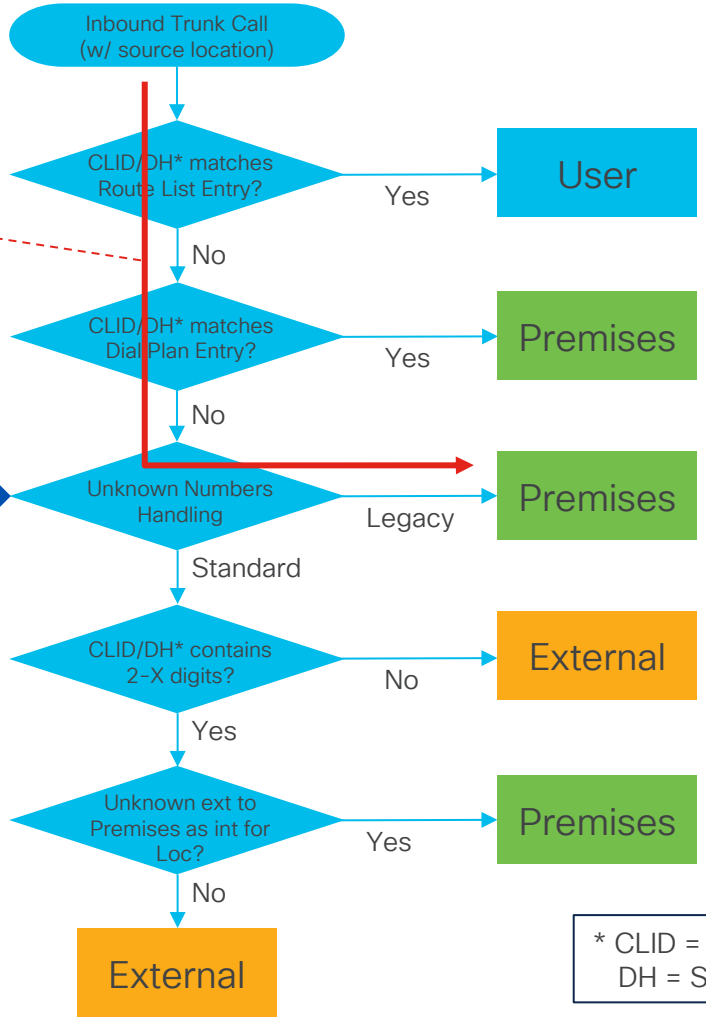
Source Classification

Calls from Local Gateway or Webex Calling DI

With “legacy behavior” incoming calls will never get classified as ”External”! Breaks features that rely on call types.

Org-wide unknown number handling





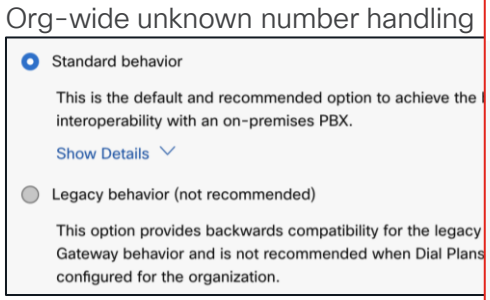
* CLID = Calling Party ID
DH = SIP Diversion Header

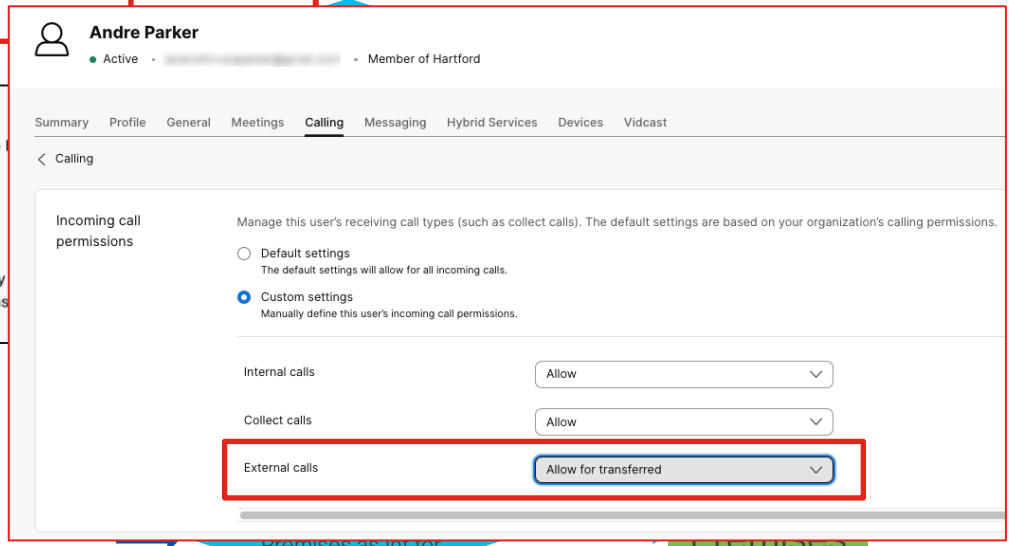
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source Classification

Calls from Local Gateway or Webex Calling DI

With “legacy behavior” incoming calls will never get classified as ”External”! Breaks features that rely on call types.

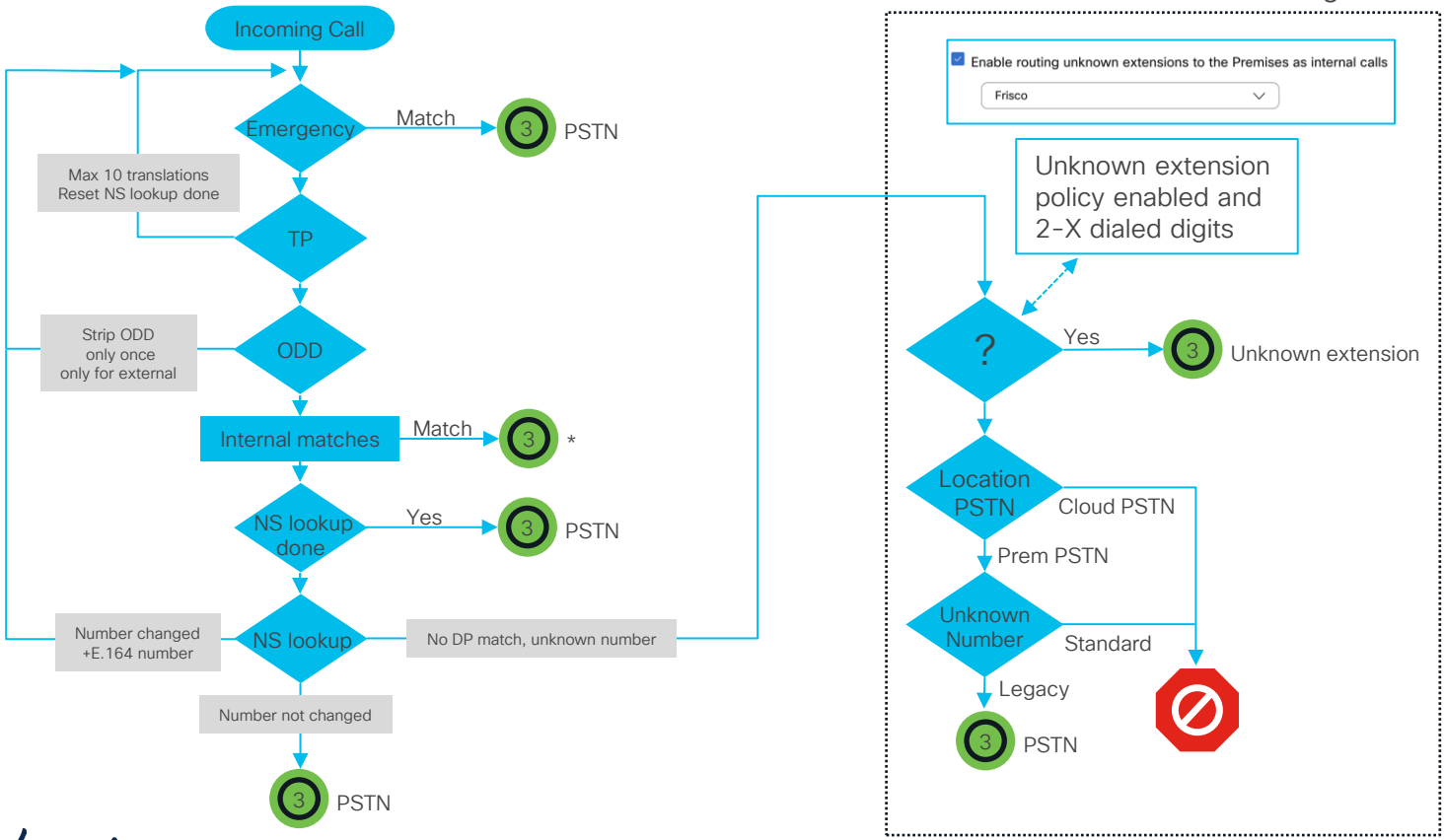




* CLID = Calling Party ID
DH = SIP Diversion Header

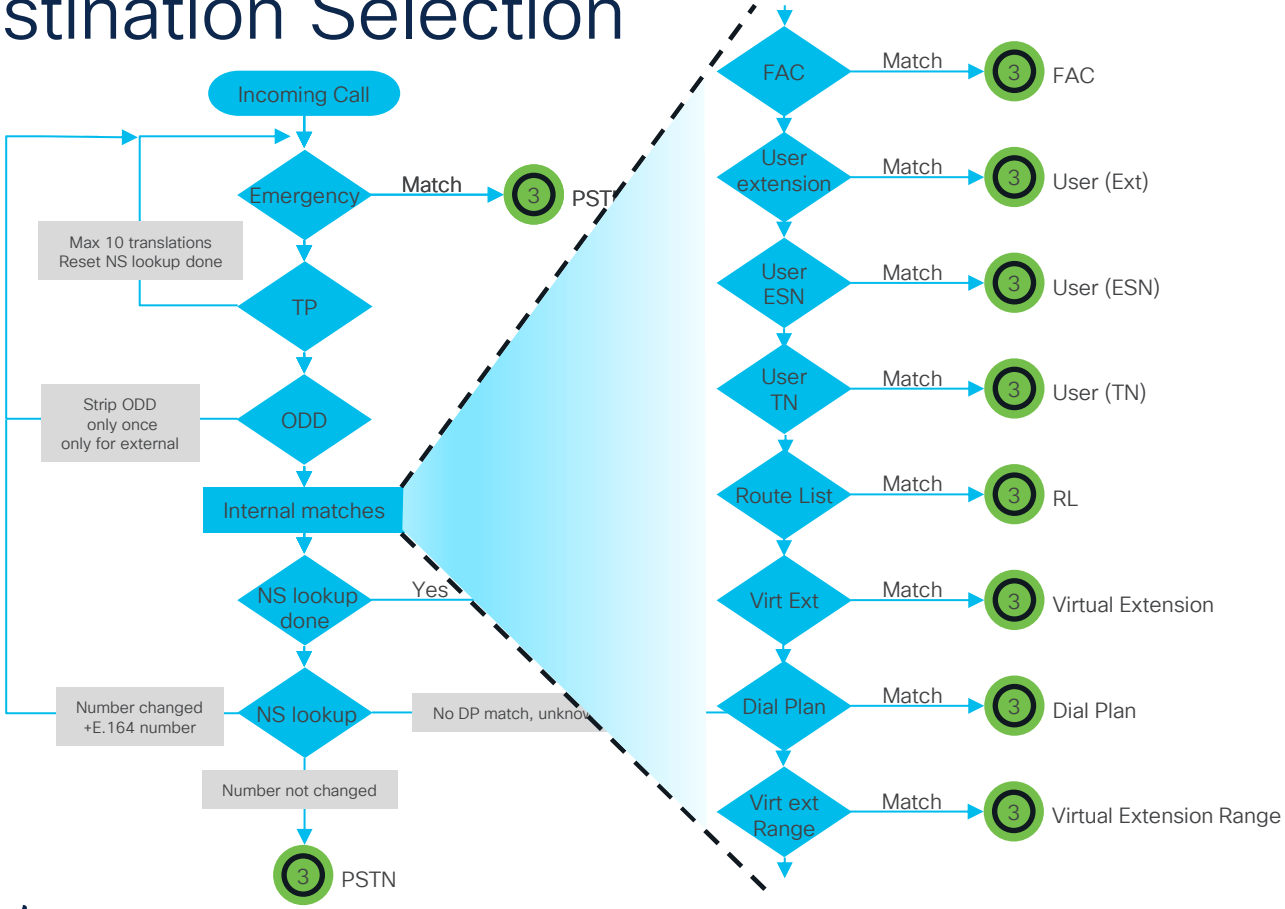
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



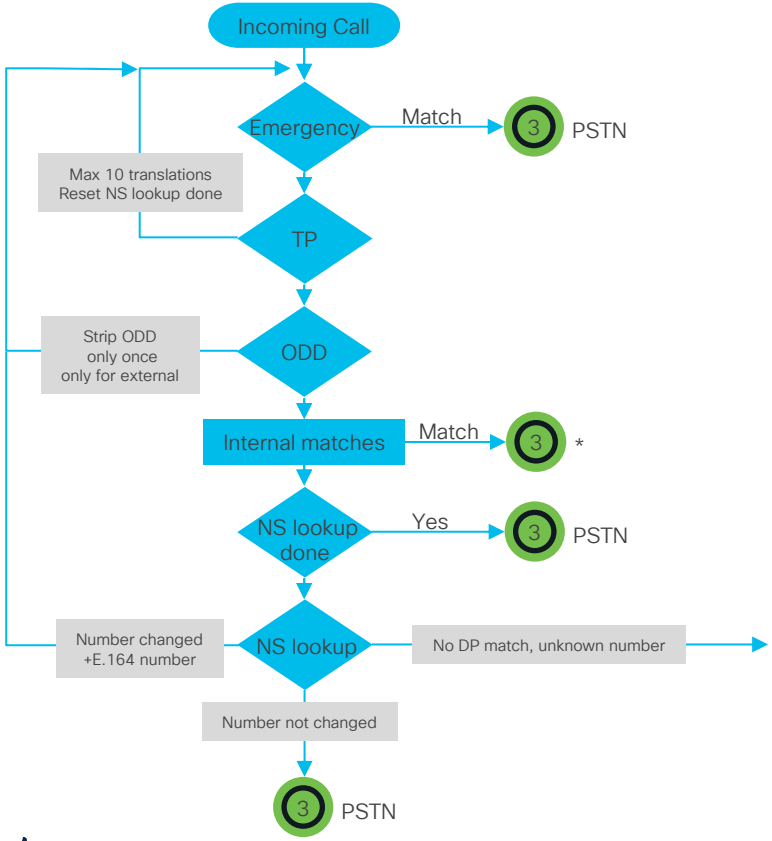
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



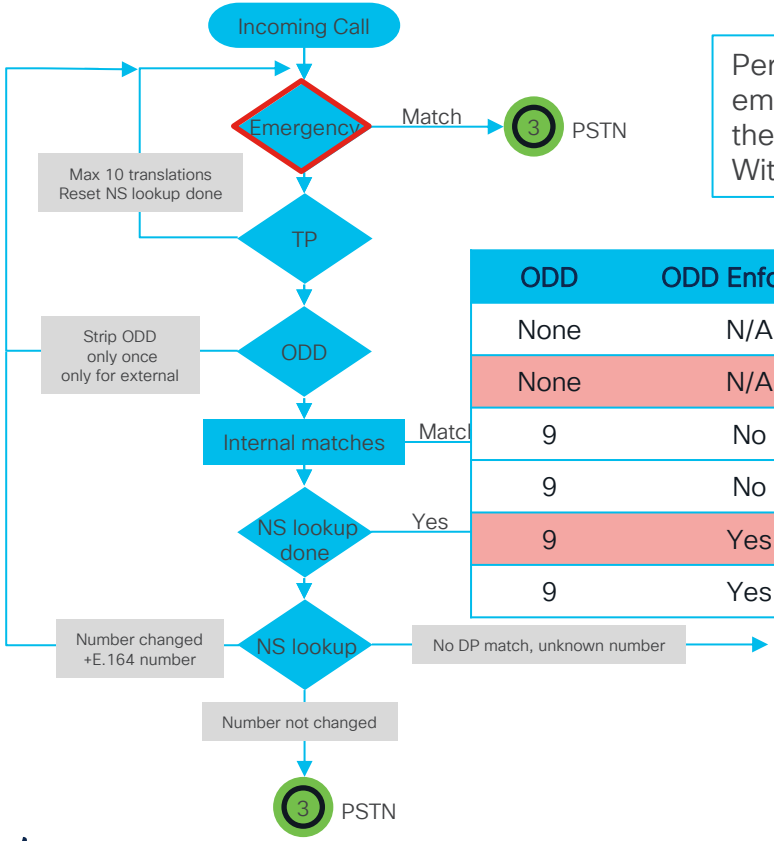
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



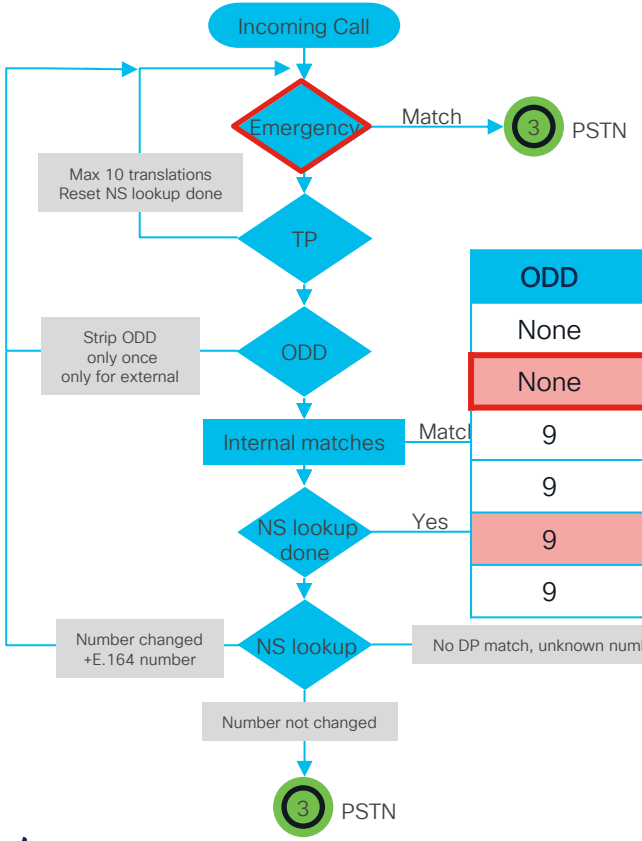
Permissive match: If dial string doesn't match emergency pattern and starts with a configured ODD then try to match with ODD removed.
With ODD 9 both 911 and 9911 work.

ODD	ODD Enforced	Dial String	Result
None	N/A	911	Emergency Call
None	N/A	9911	Unknown Extension (if enabled)
9	No	911	Emergency Call
9	No	9911	Emergency Call
9	Yes	911	Emergency Call
9	Yes	9911	Emergency Call

Note: same behavior for above variations of 933 dialing
Exception: 1911 supported (inherited for backward compatibility) but 1933 isn't

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



Permissive match: If dial string doesn't match emergency pattern and starts with a configured ODD then try to match with ODD removed.
With ODD 9 both 911 and 9911 work.

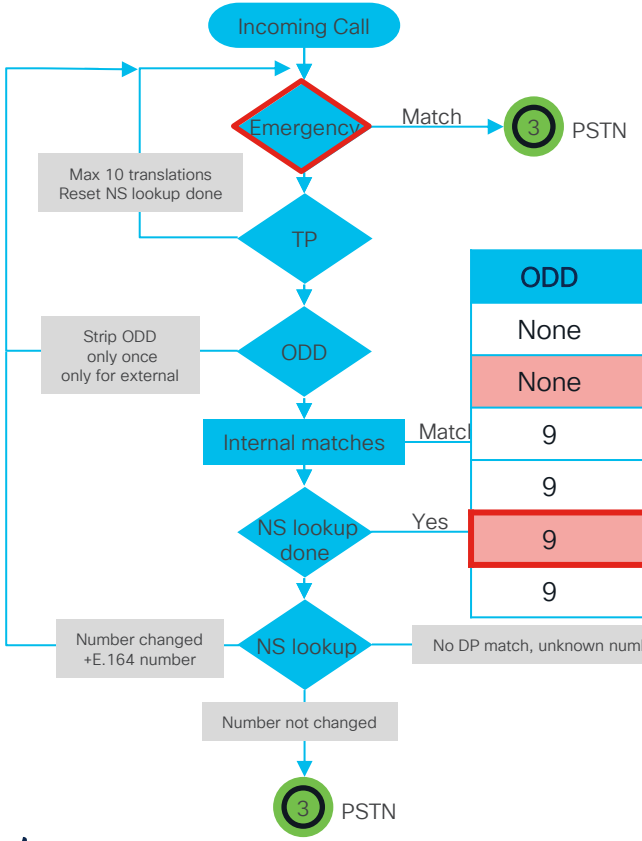
ODD	ODD Enforced	Dial String	Result
None	N/A	911	Emergency Call
None	N/A	9911	Unknown Extension (if enabled)
9	No	911	Emergency Call
9	No	9911	Emergency Call
9	Yes	911	Emergency Call
9	Yes	9911	Emergency Call

9911 only routed as emergency w/ ODD "9"

Note: same behavior for above variations of 933 dialing
Exception: 1911 supported (inherited for backward compatibility) but 1933 isn't

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



Permissive match: If dial string doesn't match emergency pattern and starts with a configured ODD then try to match with ODD removed.
With ODD 9 both 911 and 9911 work.

ODD	ODD Enforced	Dial String	Result
None	N/A	911	Emergency Call
None	N/A	9911	Unknown Extension (if enabled)
9	No	911	Emergency Call
9	No	9911	Emergency Call
9	Yes	911	Emergency Call
9	Yes	9911	Emergency Call

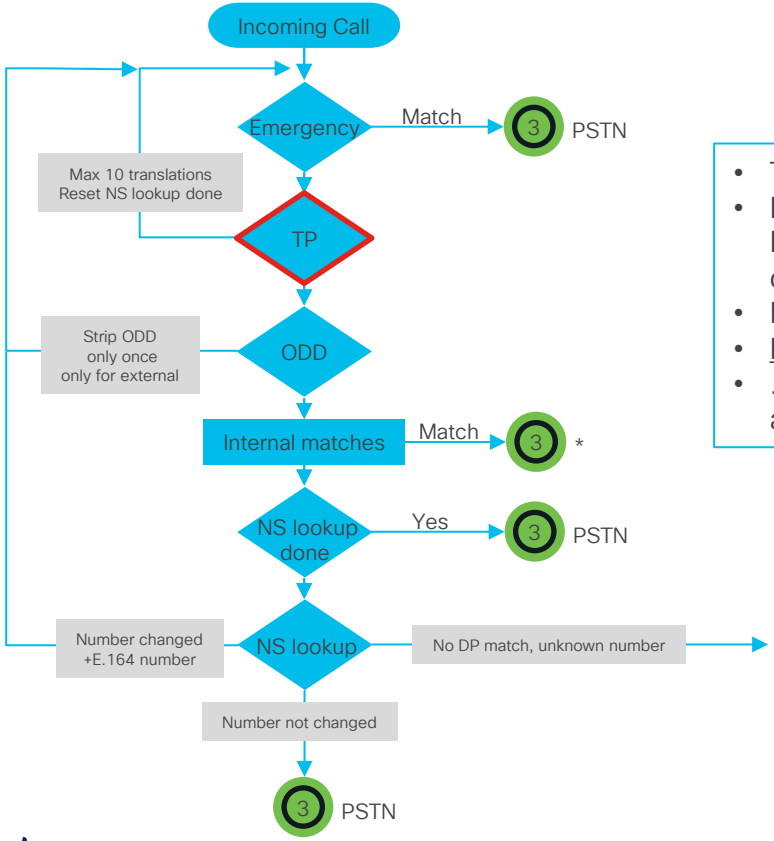
9911 only routed as emergency w/ ODD "9"

911 routed as emergency even w/ mandatory ODD "9"

Note: same behavior for above variations of 933 dialing
Exception: 1911 supported (inherited for backward compatibility) but 1933 isn't

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

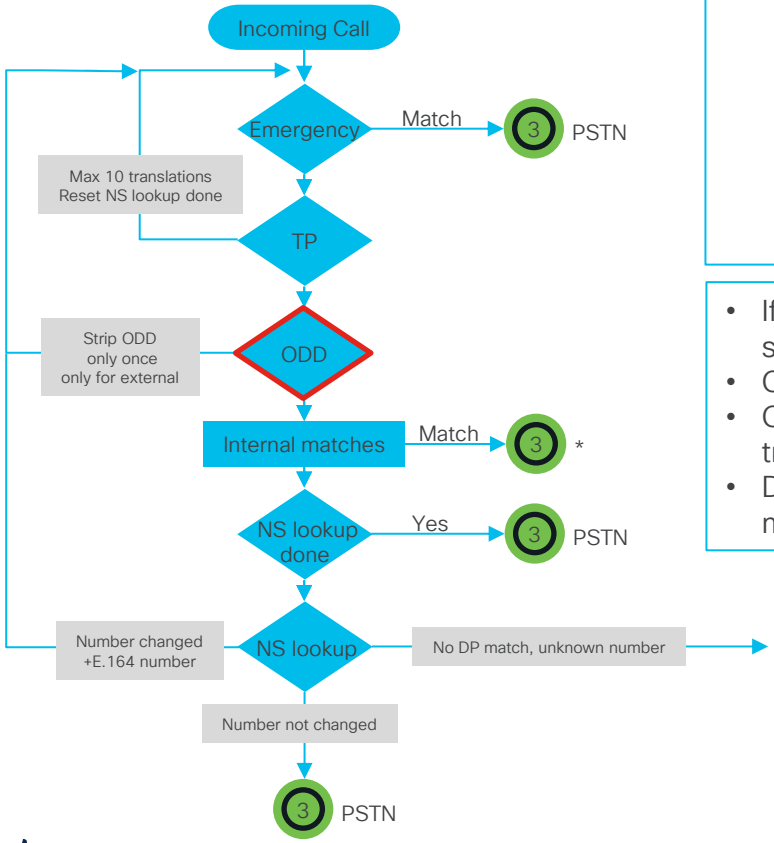
Destination Selection

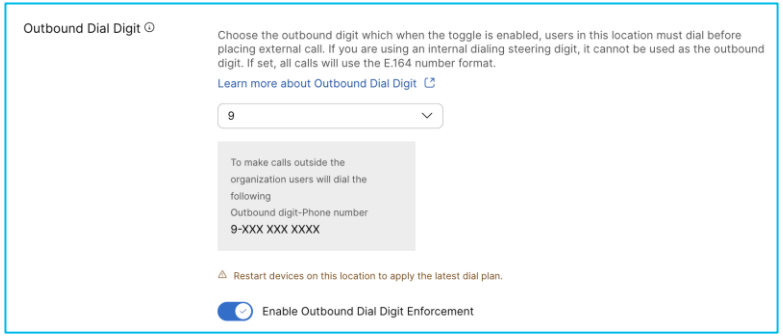


- Try to match translation patterns
- Loop back if the dial string actually changes
  For example: 6432 hitting TP (6XXX → 6432) is not changing the dial string
- Max 10 translations in total per call leg
- Don't check TPs if ODD was removed earlier
- .. Unless NS lookup transformed number to +E.164 and we came back here

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection

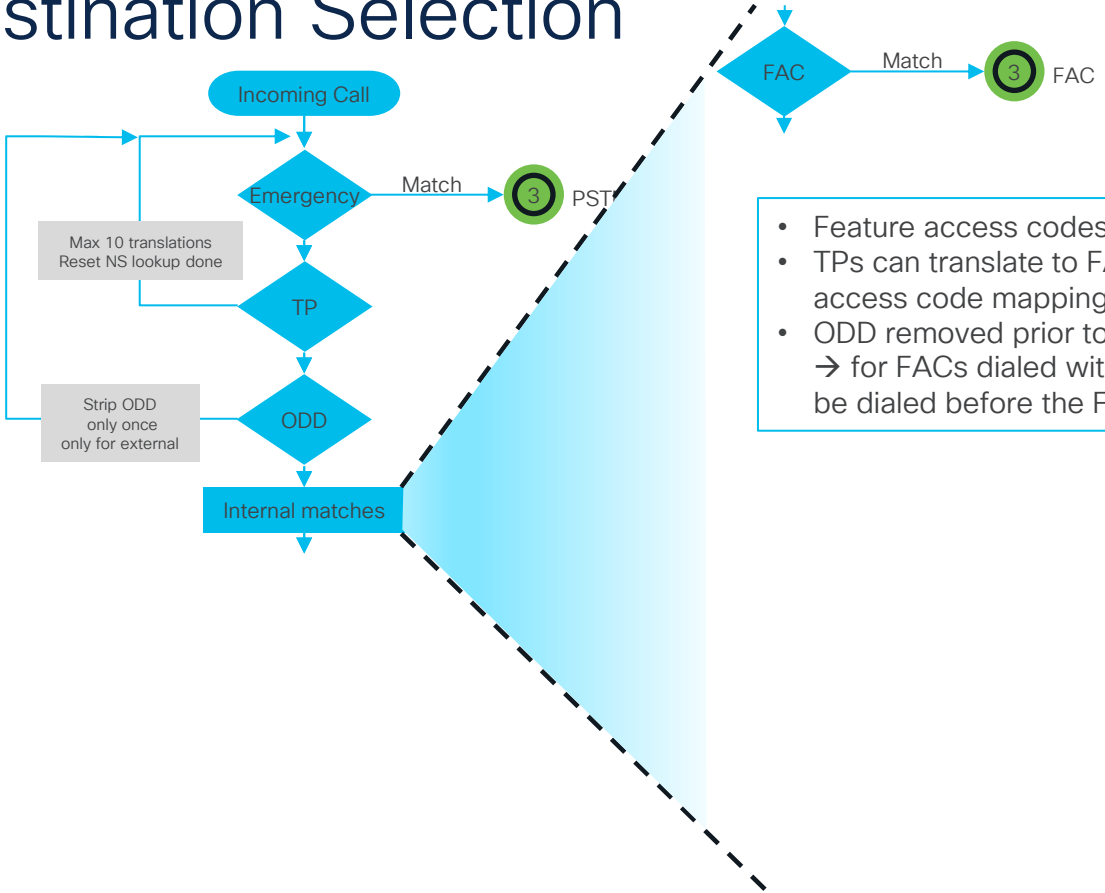




- If dial string starts with outside dial digit (e.g. “9“) then start lookups again w/ ODD removed
- ODD enforcement policy setting is irrelevant here
- ODD is only stripped once: be careful with TPs translating to dial strings starting with ODD
- Dial string w/ ODD removed is not used for internal matches (next step)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

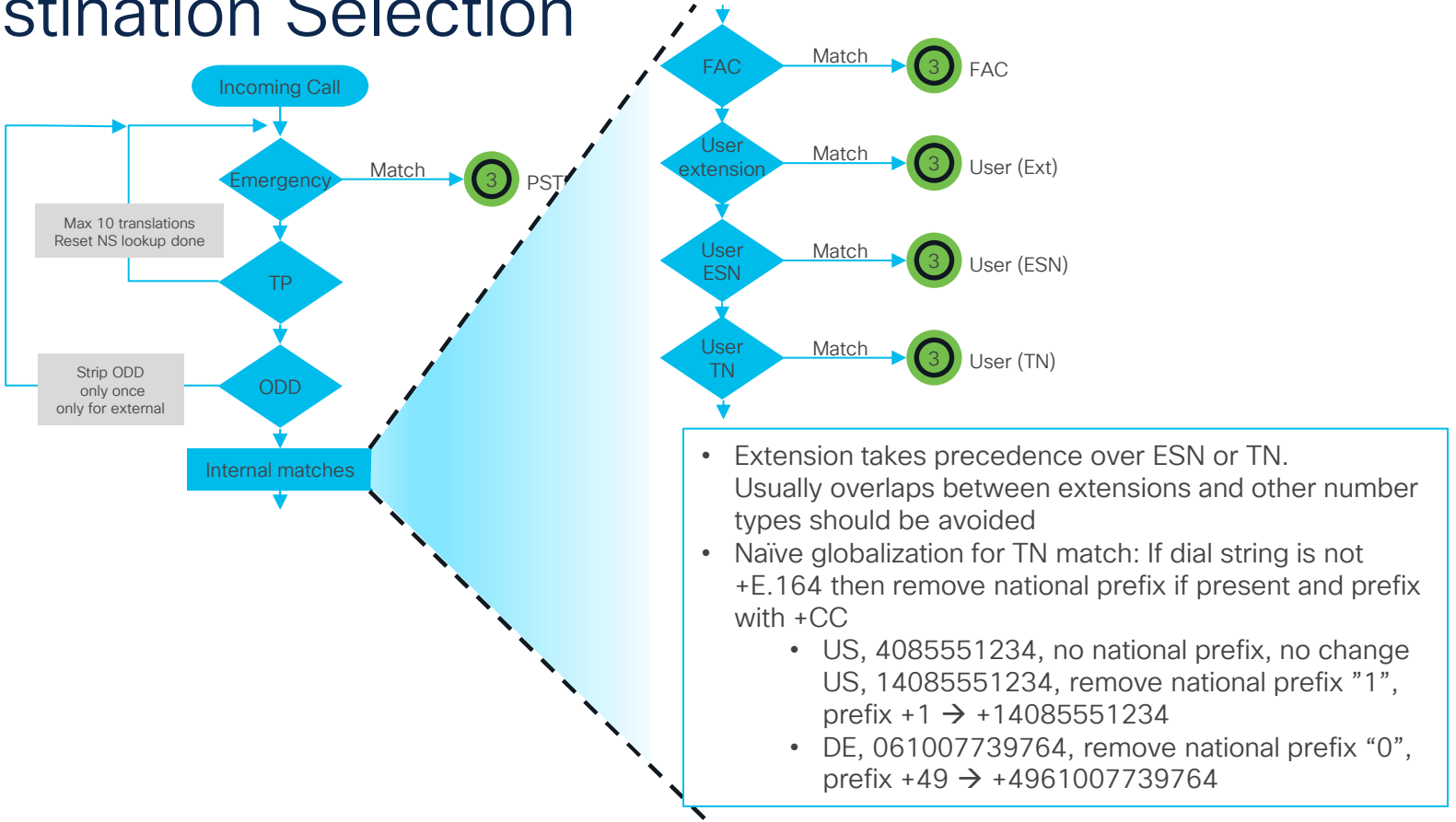
Destination Selection



- Feature access codes handled after TPs
- TPs can translate to FACs to create custom feature access code mappings
- ODD removed prior to FAC match
  → for FACs dialed with a phone number the ODD can be dialed before the FAC

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

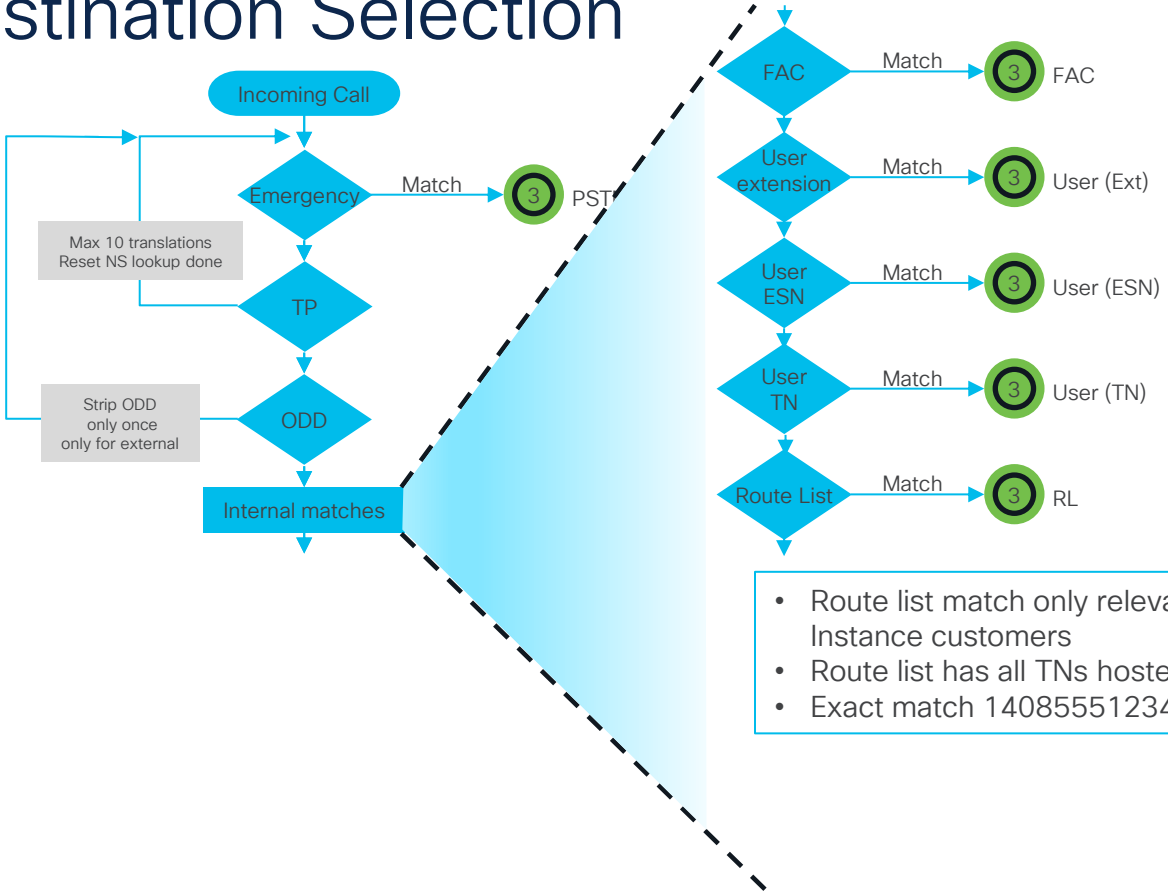
Destination Selection



- Extension takes precedence over ESN or TN.
  Usually overlaps between extensions and other number types should be avoided
- Naïve globalization for TN match: If dial string is not +E.164 then remove national prefix if present and prefix with +CC
  - US, 4085551234, no national prefix, no change
    US, 14085551234, remove national prefix ”1”, prefix +1 → +14085551234
  - DE, 061007739764, remove national prefix “0”, prefix +49 → +4961007739764

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

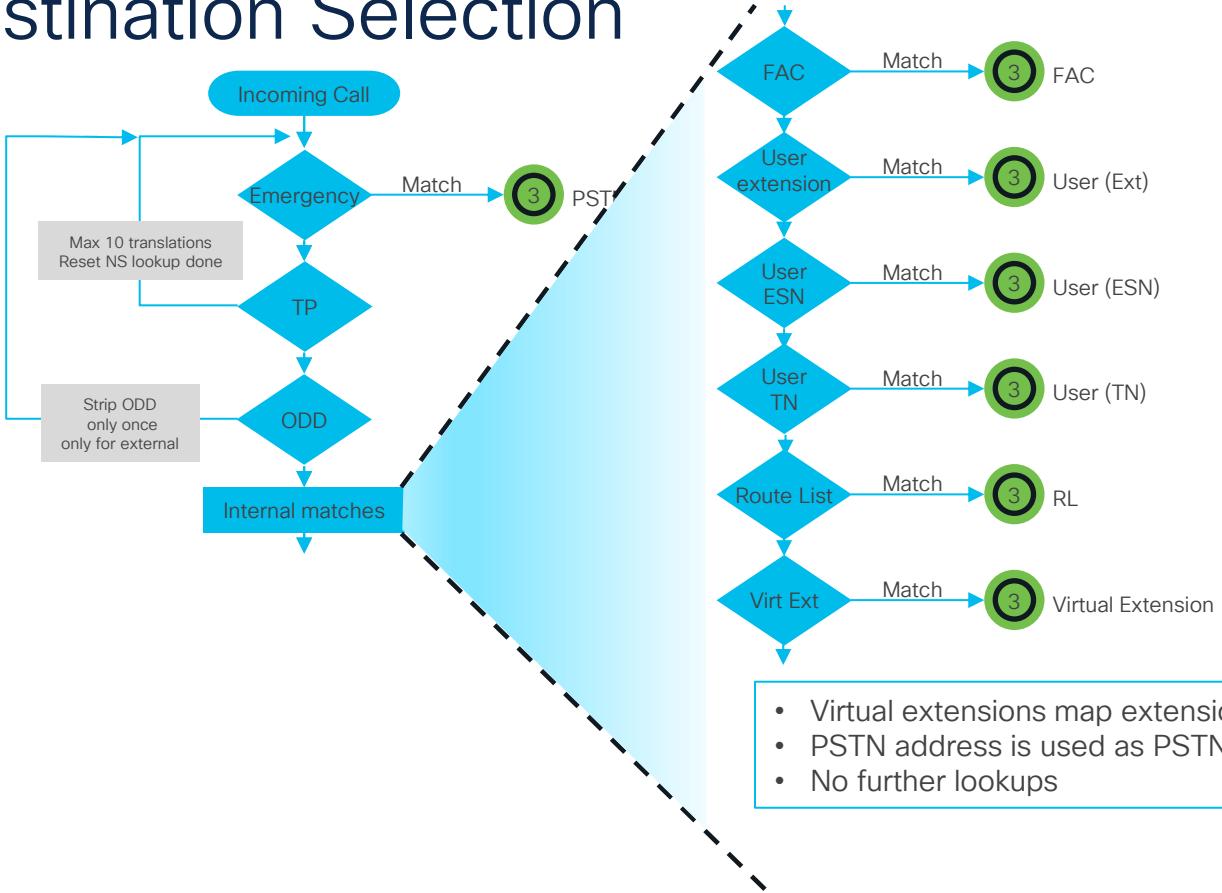
Destination Selection



- Route list match only relevant for Webex Calling Dedicated Instance customers
- Route list has all TNs hosted on Dedicated Instance
- Exact match 14085551234 doesn't match +14085551234

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

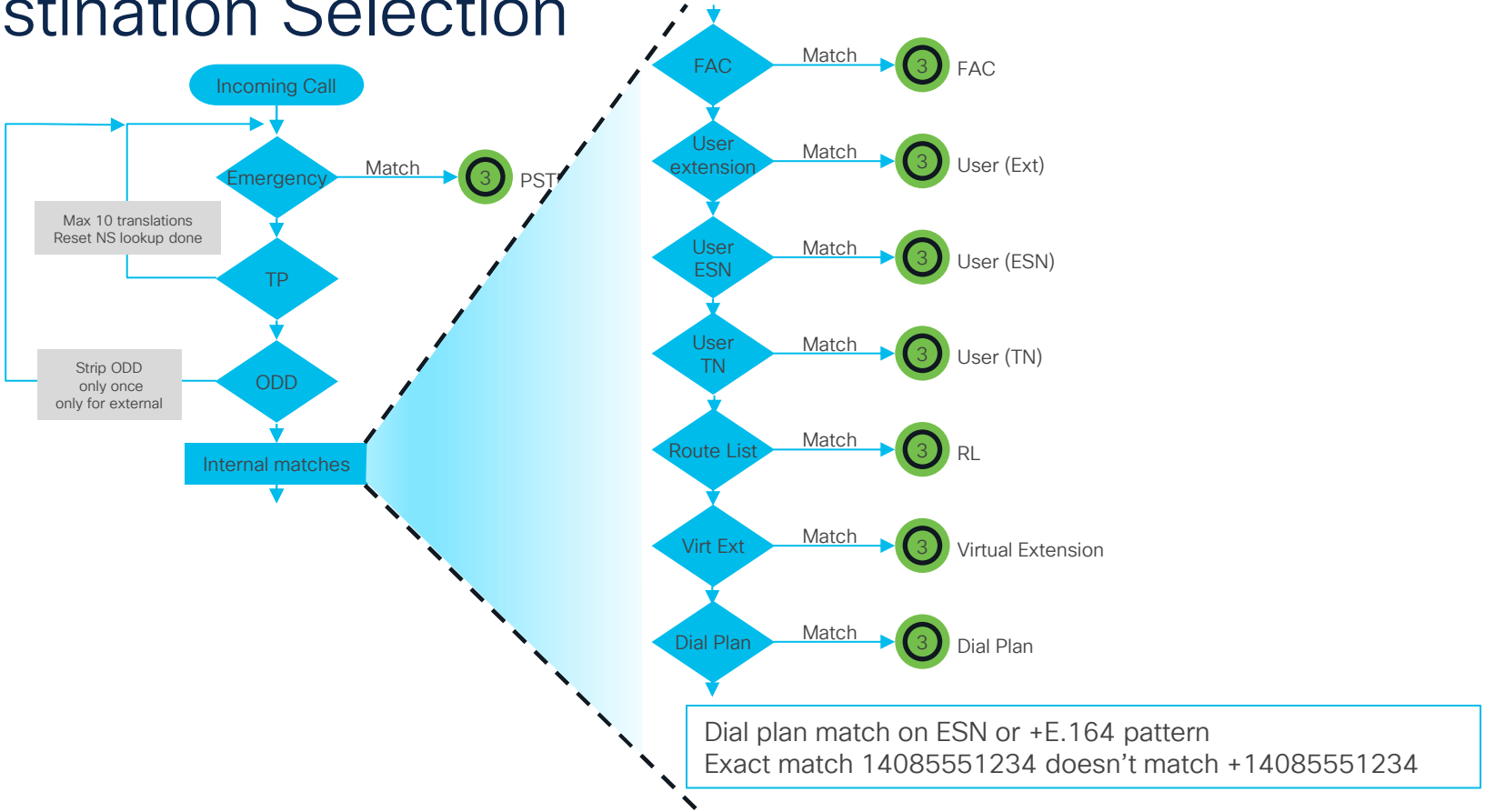
Destination Selection



- Virtual extensions map extensions to PSTN address
- PSTN address is used as PSTN destination directly
- No further lookups

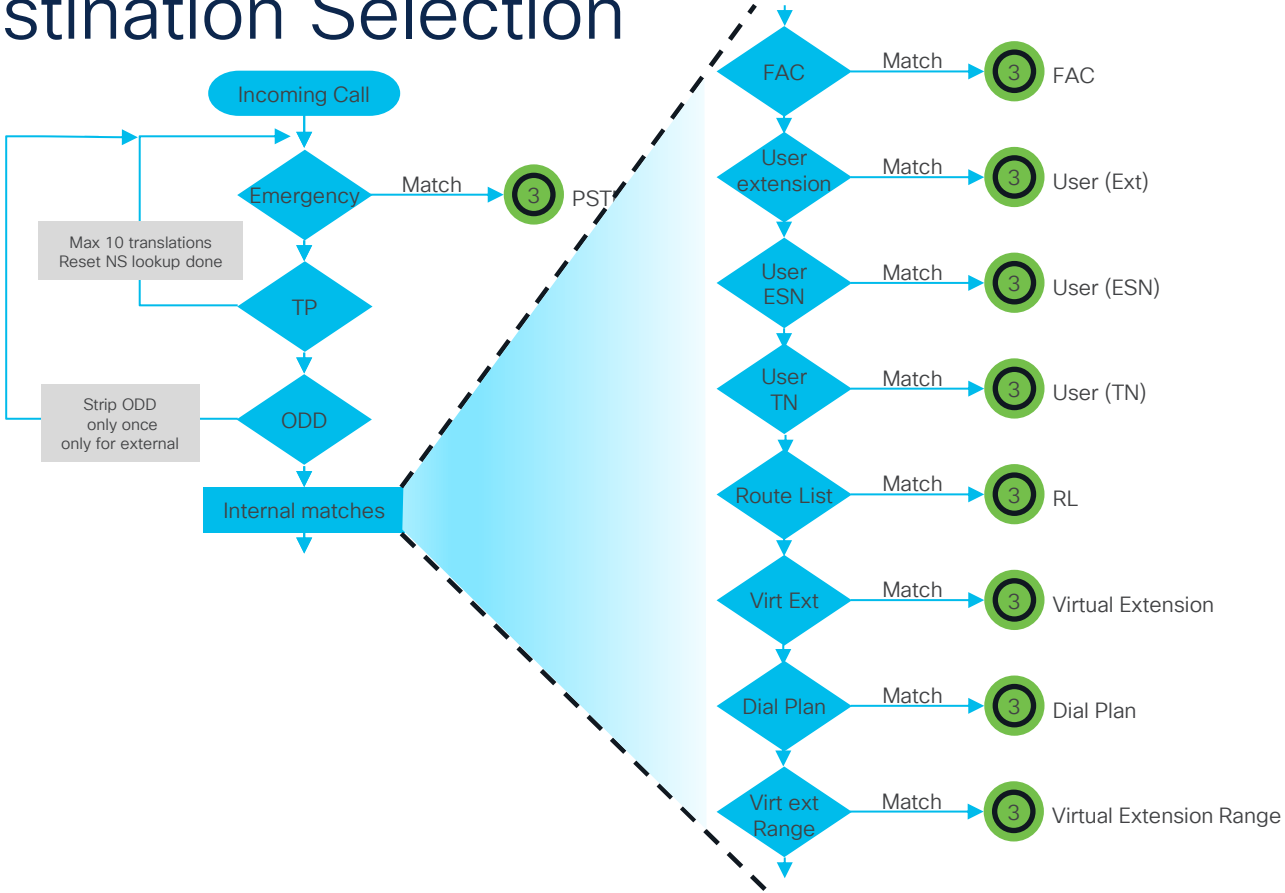
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

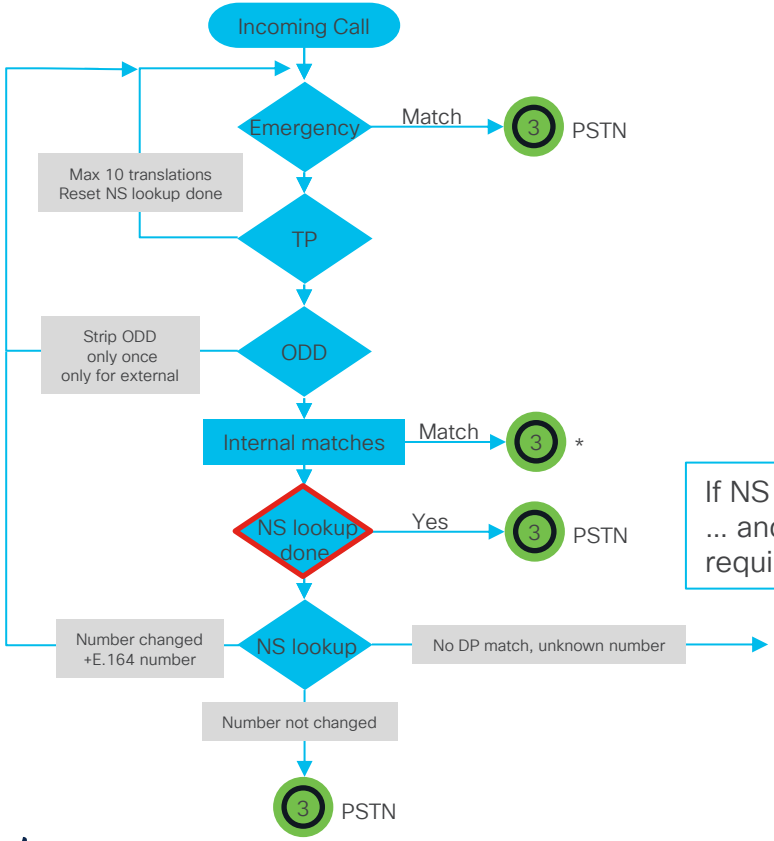
Destination Selection



Same as Virtual Extension, but based on ranges

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

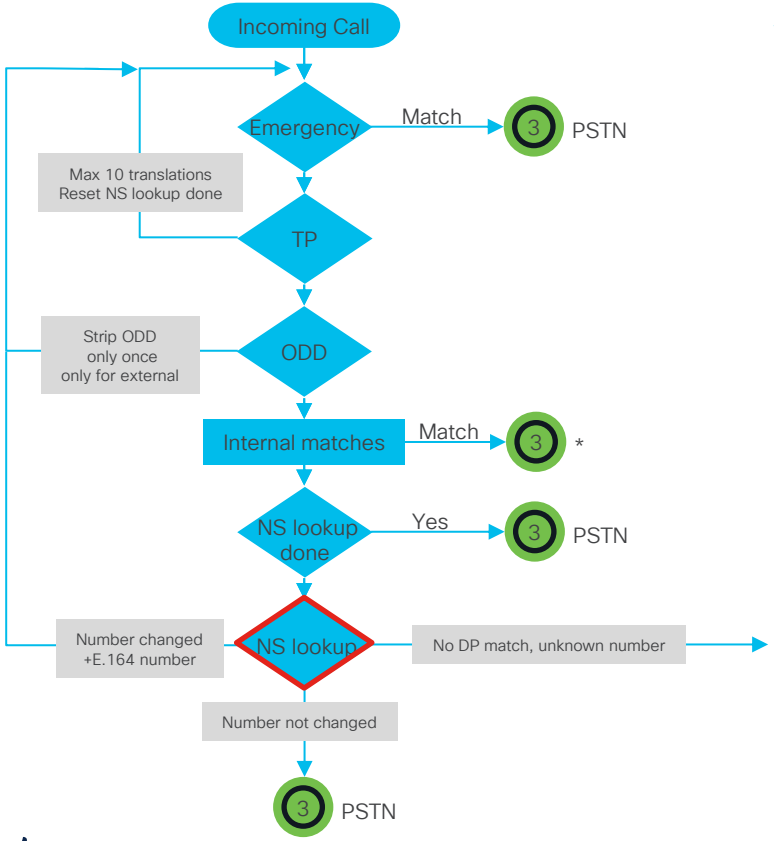
Destination Selection



If NS lookup was already done
… and no TP was applied after that then no new lookup is required b/c the lookup result would be the same

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



https://help.webex.com/en-us/article/757iyo/Dial-plans-by-country

Netherlands

Outbound calling plan

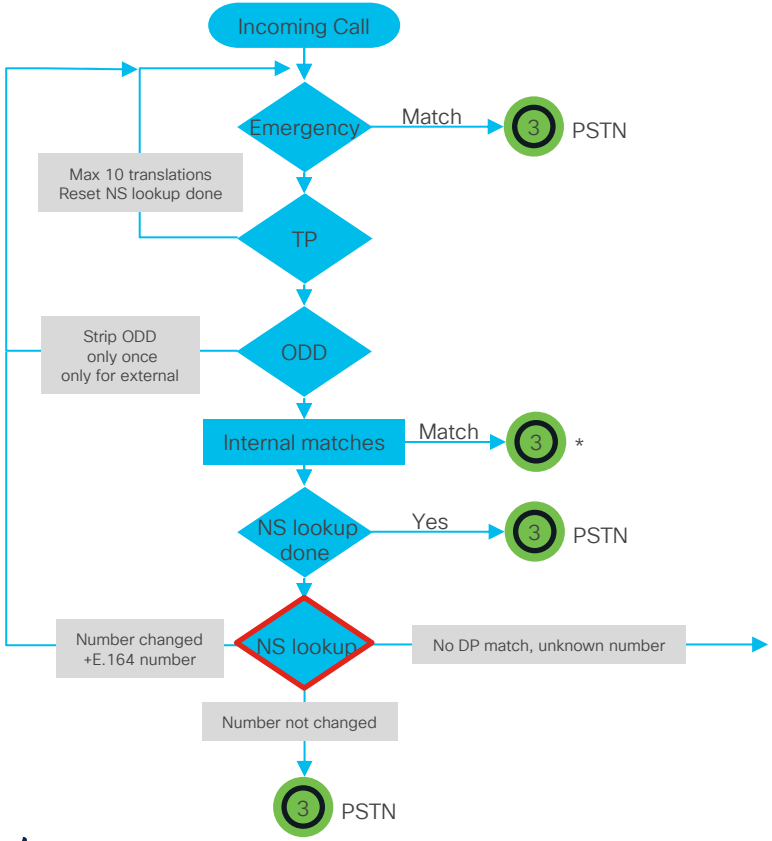
Table 185. Netherlands outbound calling plan

Country code	Digit map	Call type	Description
31	18xx	Chargeable Directory Assistance	Directory Assistance
31	116xxx	Chargeable Directory Assistance	European Harmonized Services
31	00xxxxx.	International	International Destinations
31	xxxxxx	Local	Local Calls
31	xxxxxxx	Local	Local Calls
31	084xxxxxxx	Premium Services I	Personal Assistant Services

- NS lookup considers dialed ODD and ODD enforcement
- NS lookup uses national calling plan for the country of the Location
- Call Type tagging used for call restrictions (covered later)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection

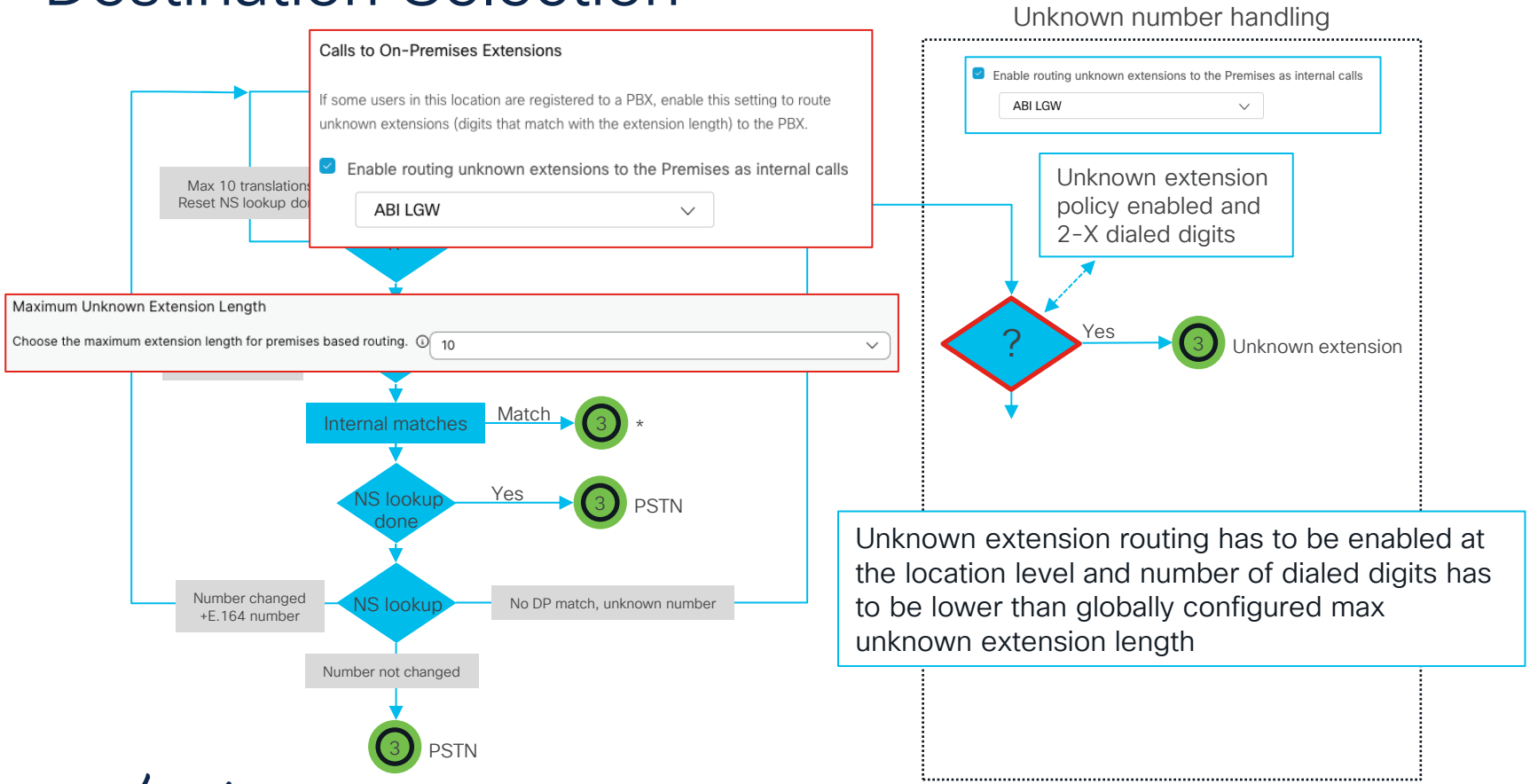


- Three possible outcomes of NS lookup:
  - Unknown number (no dial plan match)
  - Found a match, no change
  - Number changed (typically to +E.164) → loop
    Example: 9011496100123 → +496100123
- Loop enables:
  - +E.164 TN matches
  - +E.164 TP matches
  - +E.164 Route list and dial plan matches
  - …

- Dial string also considered not a match (unknown) if:
  - Dial string matches NS pattern
  - ODD configured
  - ODD enforcement enabled
  - ODD not dialed
- This is to make sure that unknown extensions that overlap with NS patterns can be treated as unknown extensions
  - example: unknown 7D extension in US or 5D extension in DE

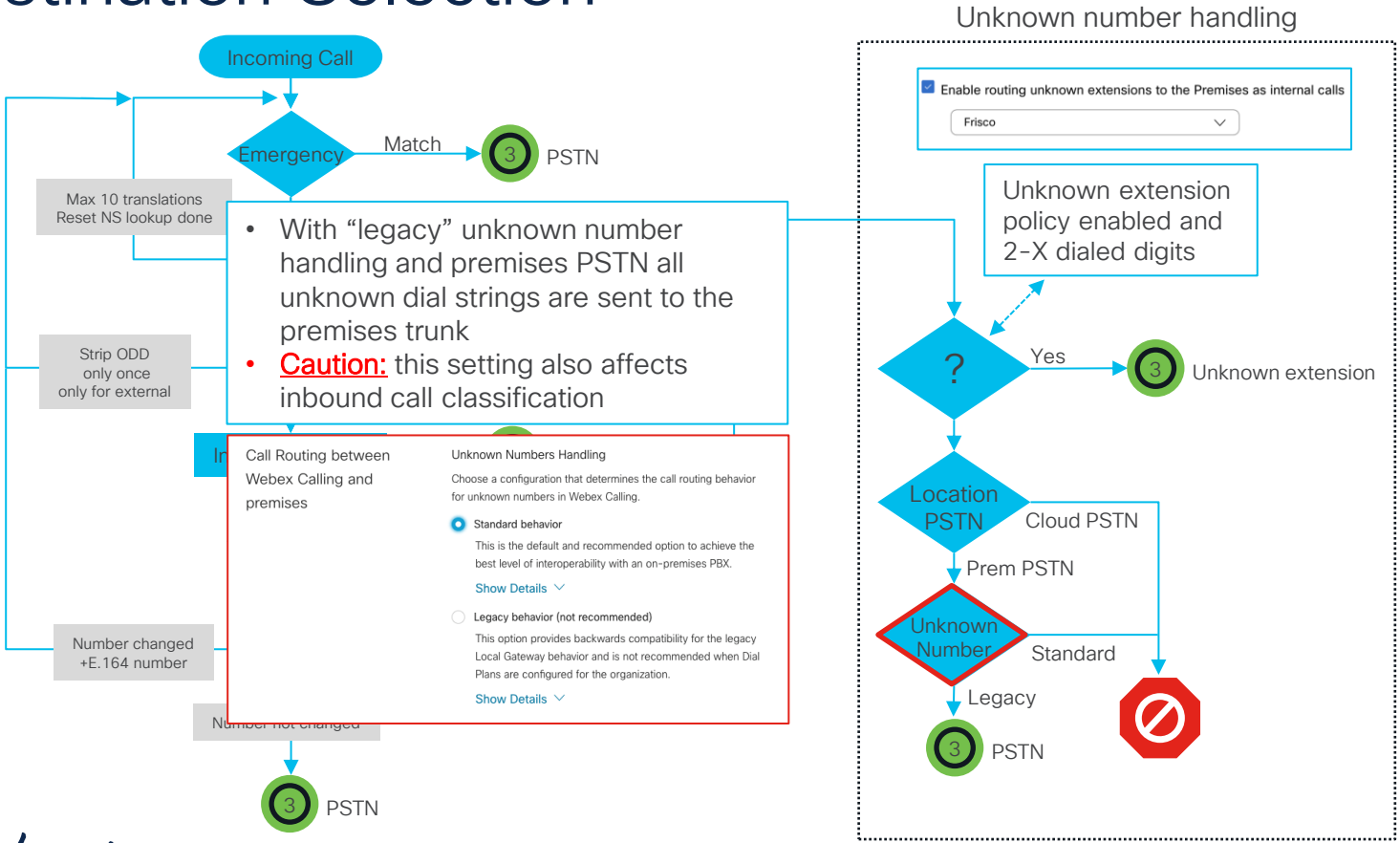
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



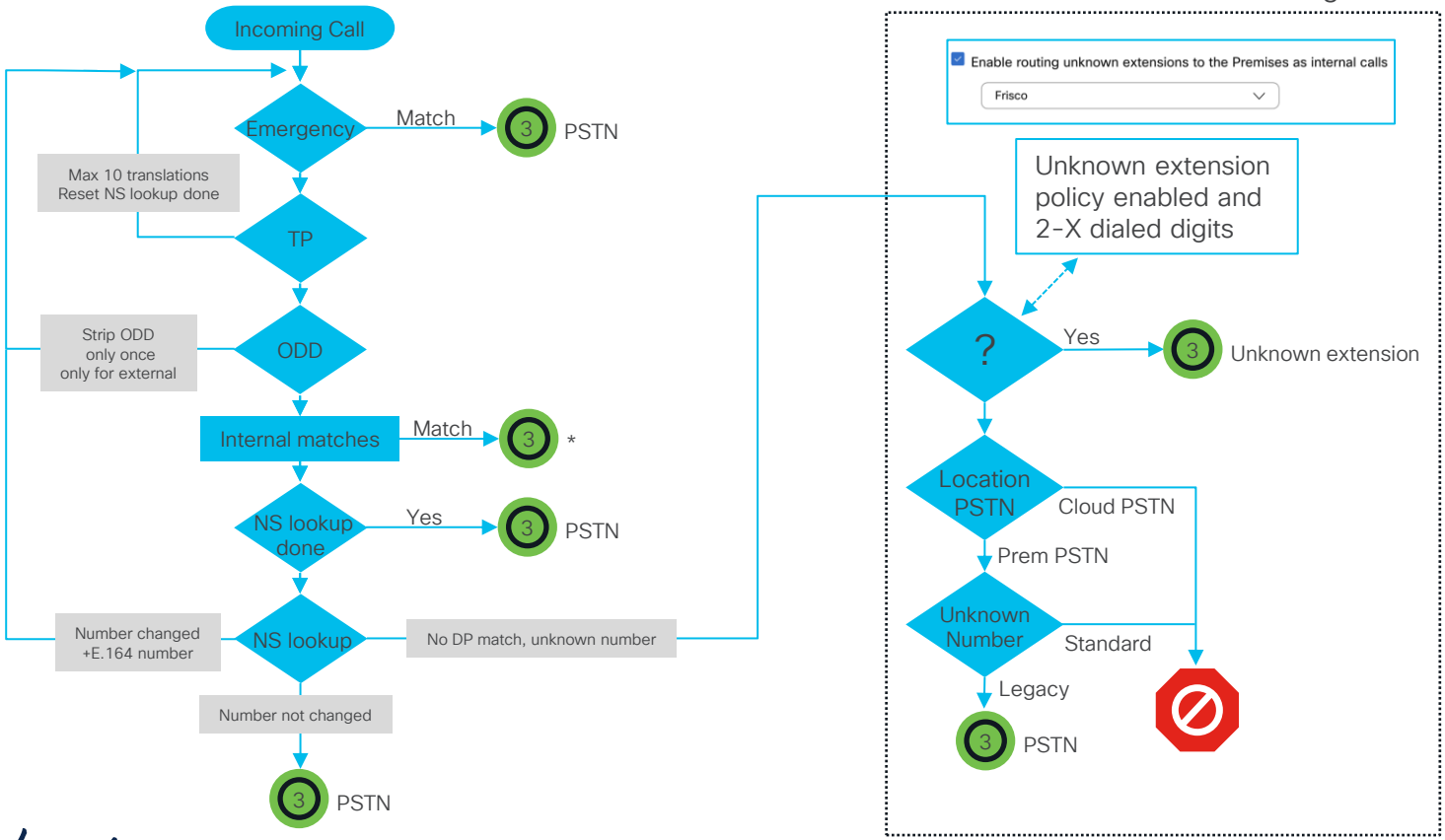
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Destination Selection



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

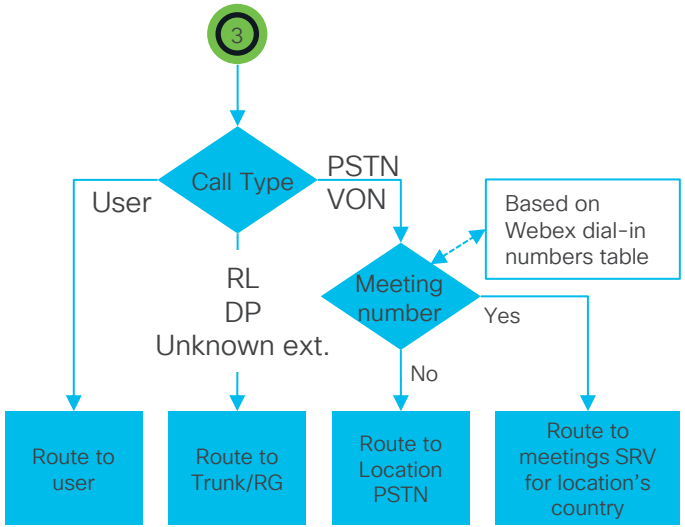
Destination Selection



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Screening and Routing

Block or allow based on calling permissions and route



- Webex dial-in is checked for all PSTN destinations
- Webex Calling dial plan elements like TPs and VONs can point to Webex dial-in numbers and the calls will be optimized

Call Routing for Webex Meetings Dial-in calls (Integrated Audio)

- (●) Optimized On-net
  This is the default and recommended option to achieve PSTN cost savings and optimized call routing.
- ( ) PSTN (not recommended)
  This option disables the on-net routing optimization for Webex Meetings dial-in calls.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Screening and Routing

From \ To	User (TN)	User (ESN/Ext)	Trunk (RL)	Trunk (DP or unknown ext)	PSTN / VON
User	✓	✓	✓	✓	✓
Premises	✓	✓	✓	✓	✗
External	✓	✗	✓	✗	✗

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Screening and Routing

From \ To	User (TN)	User (ESN/Ext)	Trunk (RL)	Trunk (DP or unknown ext)	PSTN / VON
User	✓	✓	✓	✓	✓
Premises	✓	✓	✓	✓	✗
External	✓	✗	✓	✗	✗

- Calls from Webex Calling users (including DI users) can be routed anywhere

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Screening and Routing

From \ To	User (TN)	User (ESN/Ext)	Trunk (RL)	Trunk (DP or unknown ext)	PSTN / VON
User	✓	✓	✓	✓	✓
Premises	✓	✓	✓	✓	✗
External	✓	✗	✓	✗	✗

- Calls from On-Premises Users can be routed anywhere except for the PSTN

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Screening and Routing

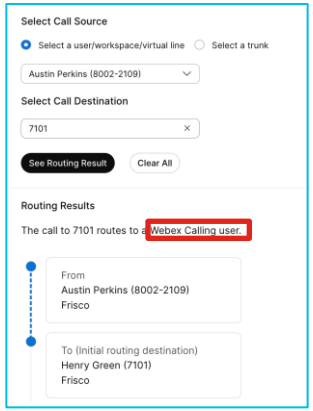
From \ To	User (TN)	User (ESN/Ext)	Trunk (RL)	Trunk (DP or unknown ext)	PSTN / VON
User	✓	✓	✓	✓	✓
Premises	✓	✓	✓	✓	✗
External	✓	✗	✓	✗	✗

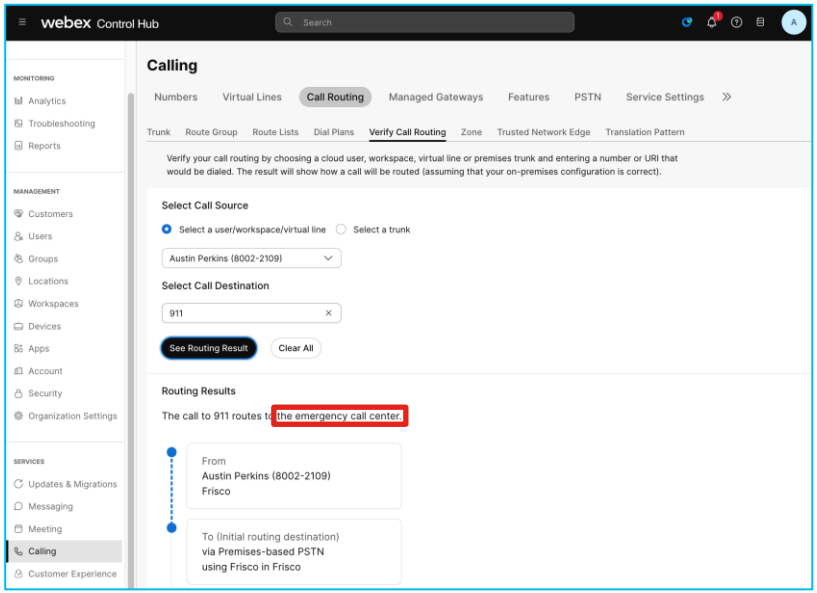
- Calls from PSTN can only route to User TN's (including DI users). Calls from PSTN cannot call ESN / Extension.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verify Call Routing Tool (VCR)

- VCR allows to troubleshoot call routing decisions for user calls
  - Calls from Webex Calling users
  - Trunk calls classified as “premises” or “user”

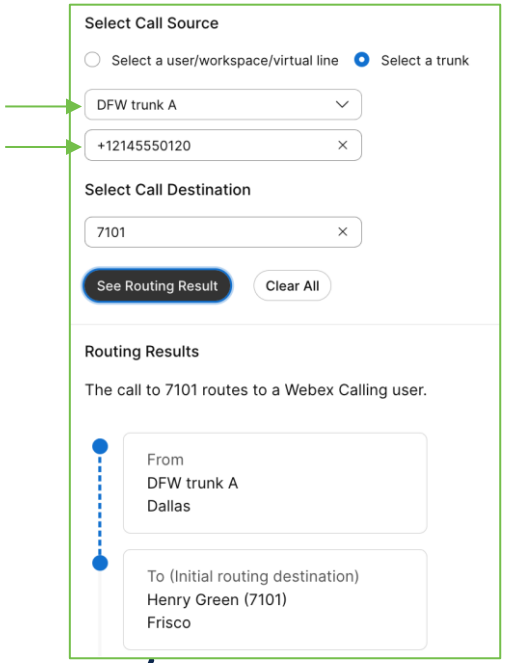


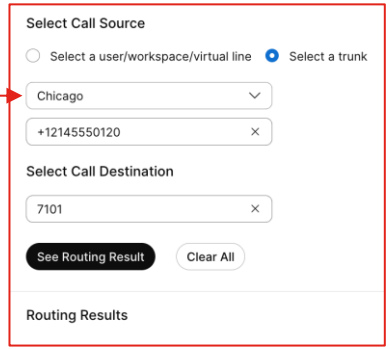


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

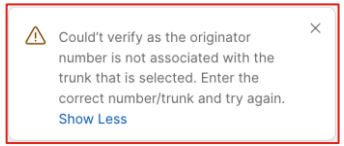
Trunk Calls and Dial Plan Match

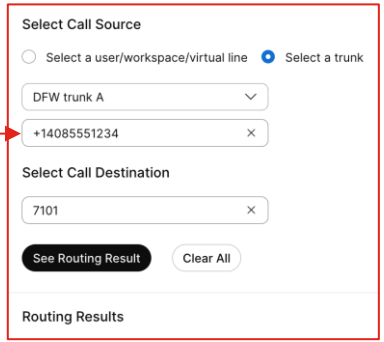
- Call from trunk to extension fails if call is not classified as “premises” or “user”



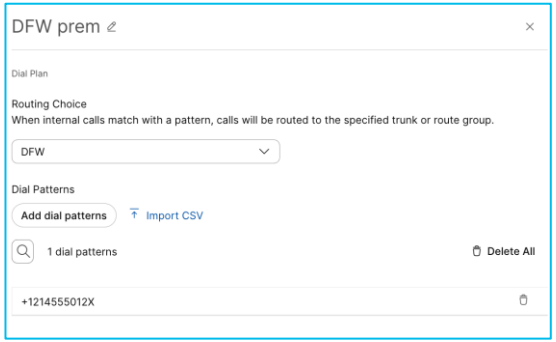


Caller ID does not match an EDP pattern .. of a dial plan pointing to the right trunk





Caller ID does not match an EDP pattern

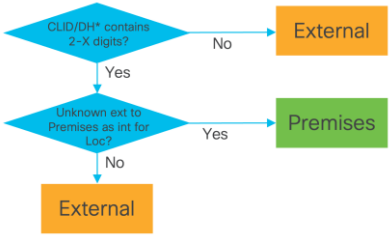


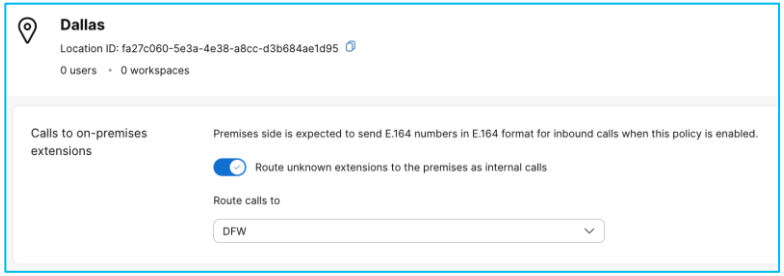
Note: Cisco recommends to use +E.164 caller ID on trunks except for calls from extension only users

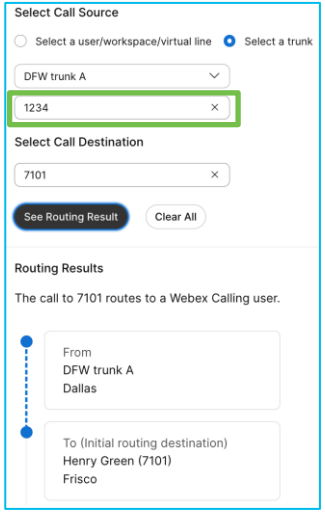
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

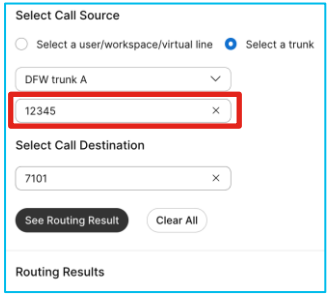
Trunk Calls and Extensions as Caller Id

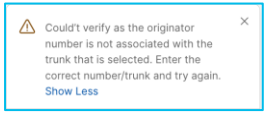
Calls with extension caller id are classified as user calls only if unknown extension dialing is enabled and the caller id length matches







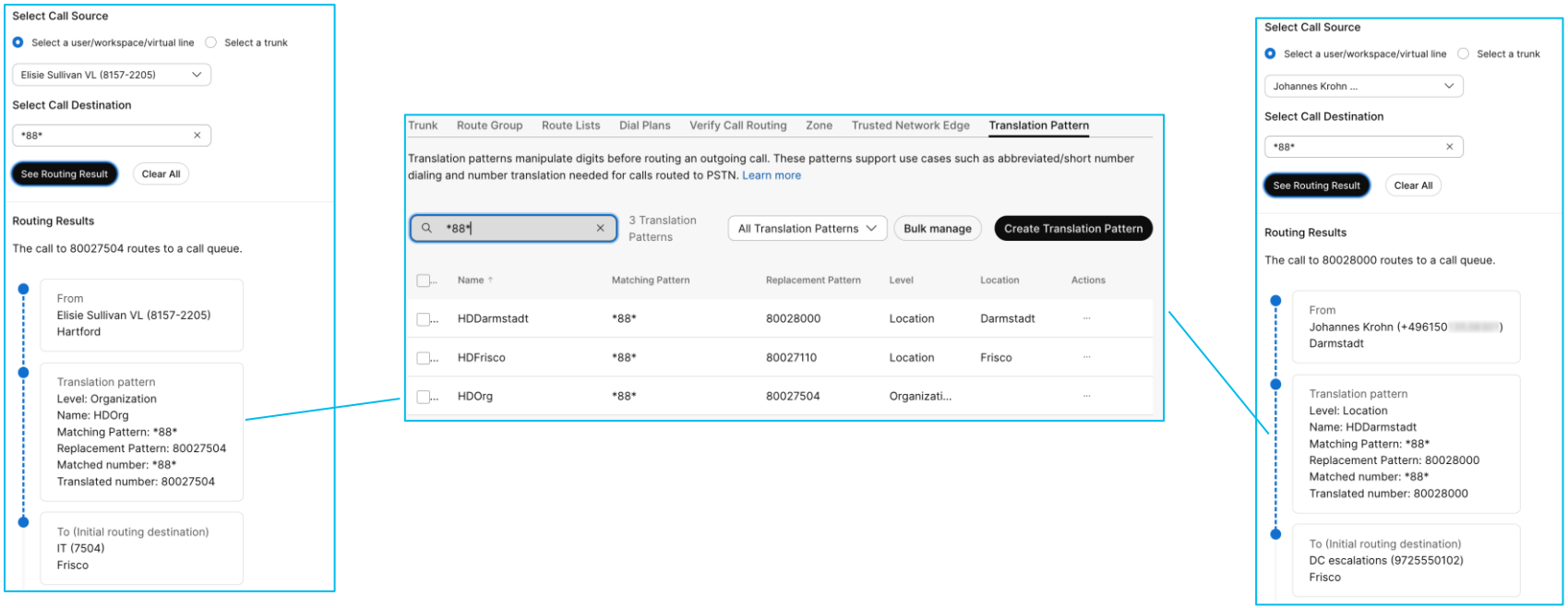




© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Translation Patterns

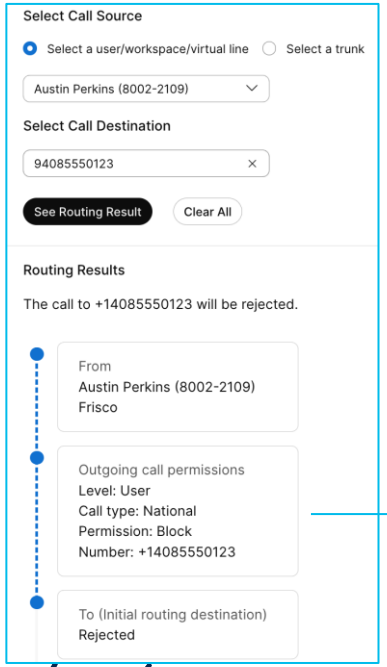
- VCR shows intermediate translations

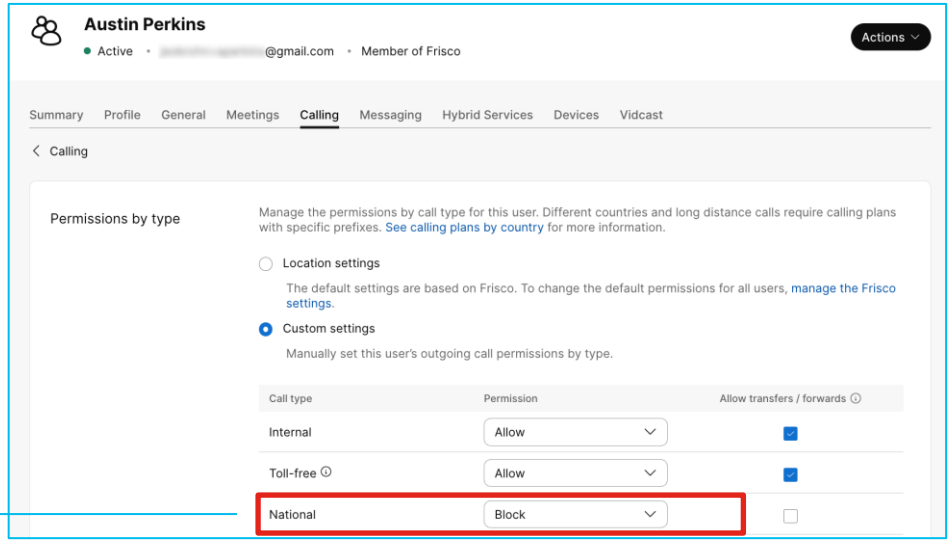


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Outgoing Call Permissions

- VCR shows outgoing call permissions

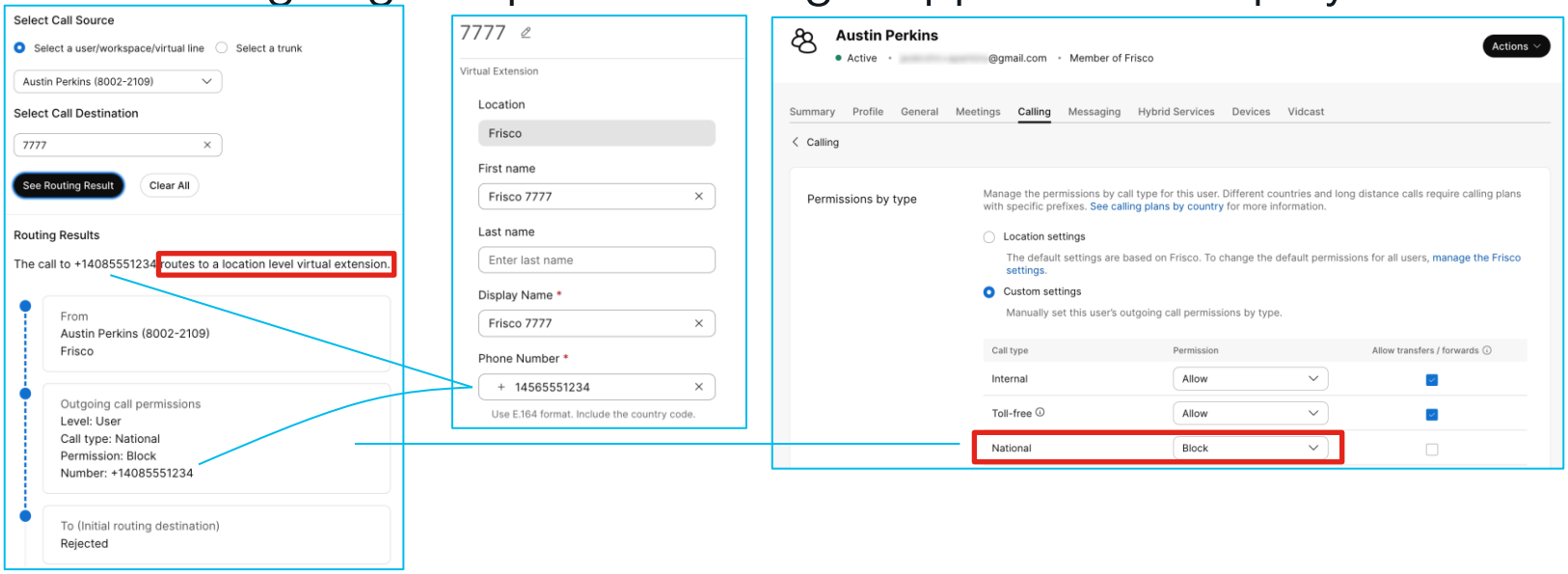




© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Virtual Extensions

- VCR does show virtual extension mapping
- … and outgoing call permissions get applied and displayed



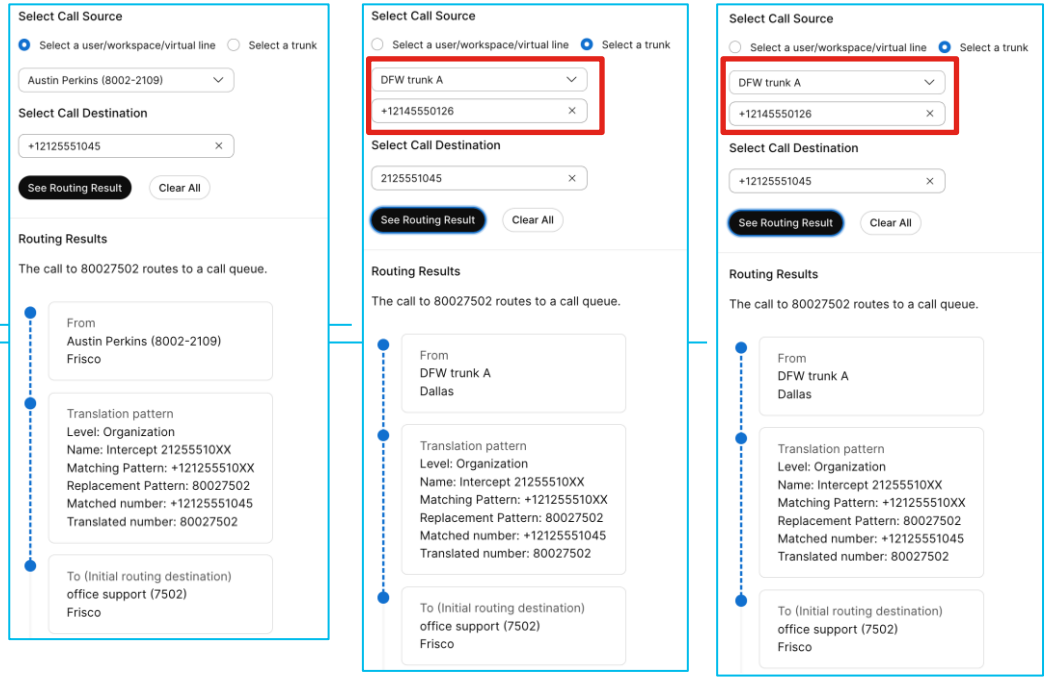
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Another Translation Pattern Example

Name	Matching Pattern	Replacement Pattern	Level
Intercept 21255510XX	+121255510XX	80027502	Organization

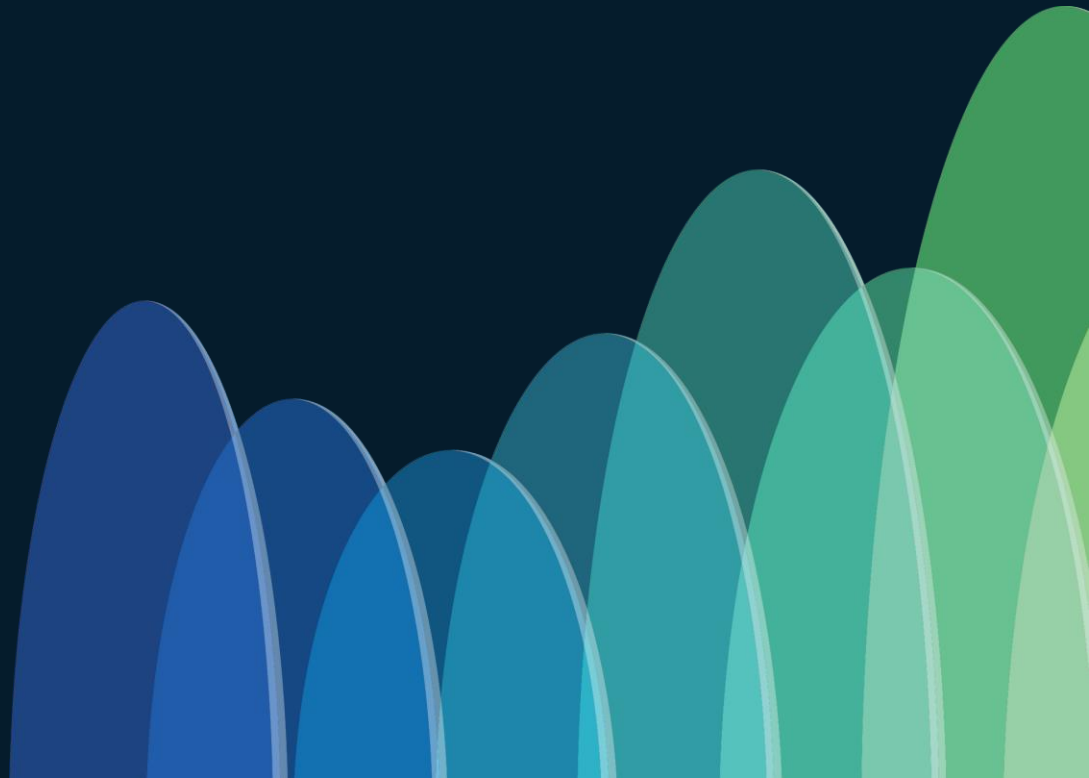
Calls to given range get redirected to some on-net destination (CQ)

Translation patterns get applied to user calls ..
.. and that includes trunk calls classified as “premises” or “user”
This example also shows that 10D gets normalized to +E.164 inbound on trunks



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Closing



Recap

- Web debugging
- User Provisioning
  - Direct
  - Director Connector
  - Extra ID Wizard
- Authentication
  - SSO
- Call Routing

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

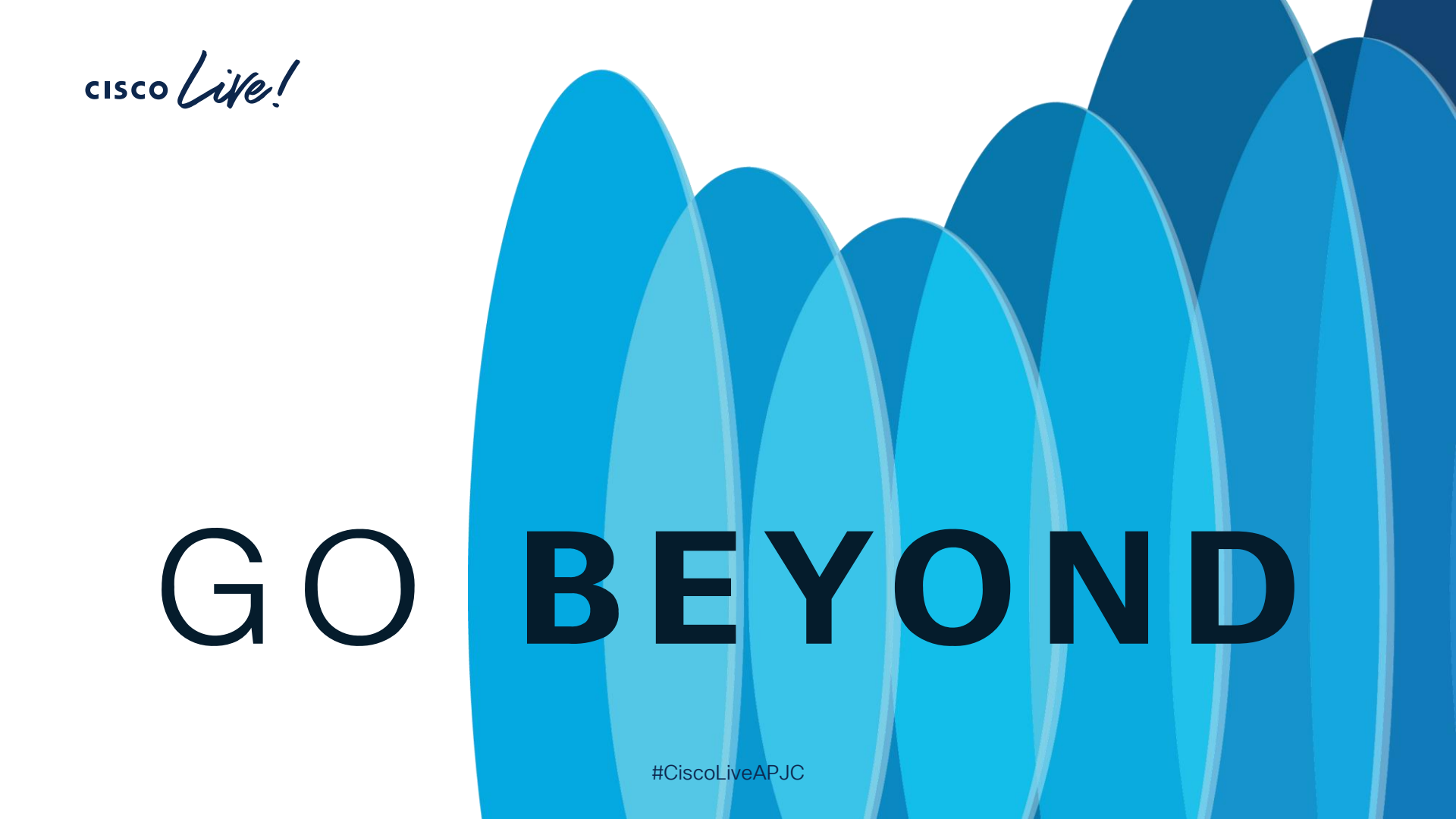
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC