cisco

You make **possible**

Best Practice on enterprise grade Deployment for Cisco Jabber

Malte Kostewicz
Technical Solutions Architect - Collaboration

BRKCOL-3392

Barcelona | January 27-31, 2020

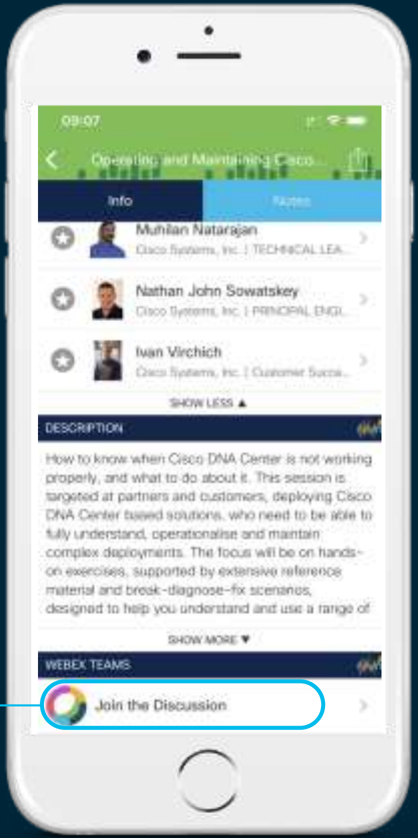
Cisco Webex Teams

Questions?

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

How

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



Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Best Practice on enterprise grade Deployment for Cisco Jabber

Cisco Jabber continues to be the pillar for Cisco`s on premise Collaboration solution. This session will cover various aspects of expanding your existing Jabber deployment to leverage the full enterprise feature set.

Integrating Cisco Jabber into your company's Single-Sign-On Solution will greatly enhance the login/start-up experience for your end-users. Adding MFA on top of that will provide an extra level of security and delight your Chief Security Officer. We will have a closer look into the deployment options and login flows in the context of **Authentication**, Authorization, oAuth, SSO and MFA and outline the new or enhanced functionalities in Cisco Jabber.

Management of **Jabber clients** in a **mobile** and connected world is complex. As the support for MS Intune and Blackberry MAM as mobile device management solution is planned for early CY2020, we are looking into all options of management for Jabber mobile.

Compliance and data-loss prevention tools are gaining relevance in today's world of cloud applications. Have you actually considered to integrate similar capabilities into your existing On-Premise deployments of Cisco Jabber? In-line compliance, ethical walls or file-sharing controls are just a few examples for possible integrations. We will review and provide you with some best practices. We will also take a look on other aspect of being compliant like the ability of storing chats locally.

Centralized IM/P deployments are growing and usecases are enhancing. We will review it focusing on it's potential for additional service aggregation like federation or Webex hybrid message service.

TOP JABBER CHARTS

TOP #4 Jabber Charts

#   Jabber Authentication

#   Jabber Mobile Management

#   Jabber compliance

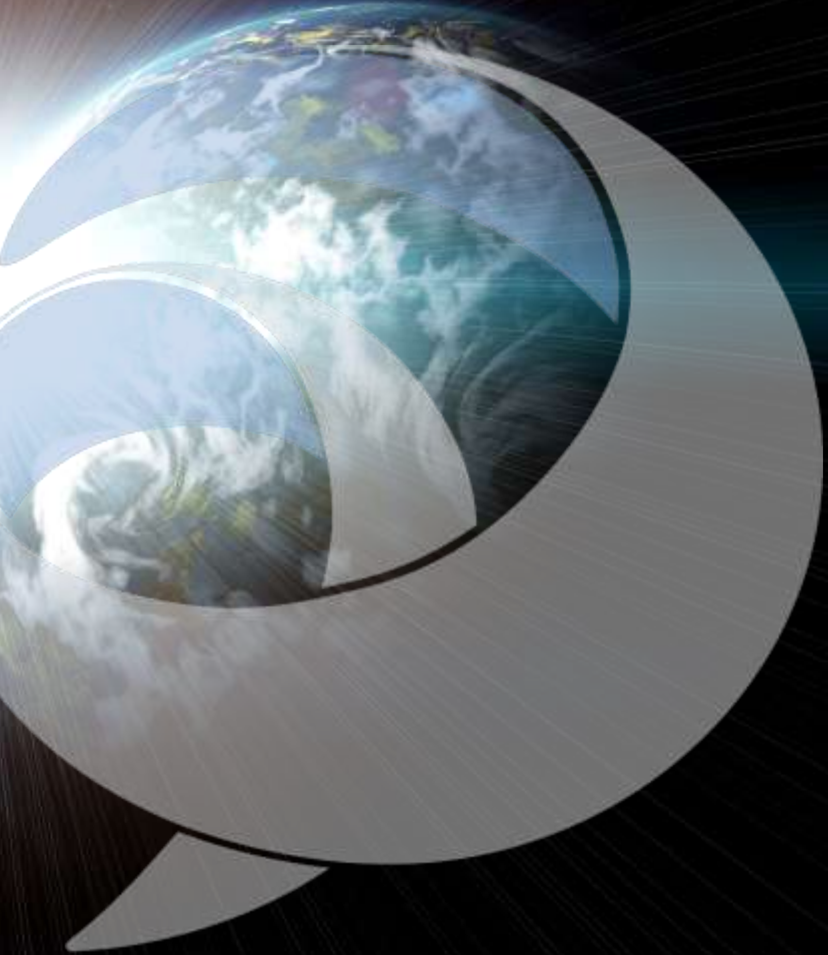
#   Centralized IM&P Deployment

TOP #5 → BRKCOL-2602

Friday 09:00am
Hall 8.0, D137

Migrating your existing Jabber deployment to the Cisco Collaboration Cloud

- Migration
- Federation – XMPP Federation, Hybrid Message
- Jabber team messaging mode
- Webex Teams CUCM calling
- Cloud Calling
- General infrastructure recommendations



This presentation assumes:

Jabber On-Premise Deployment

Jabber Client 12.8

UC Manager 12.5

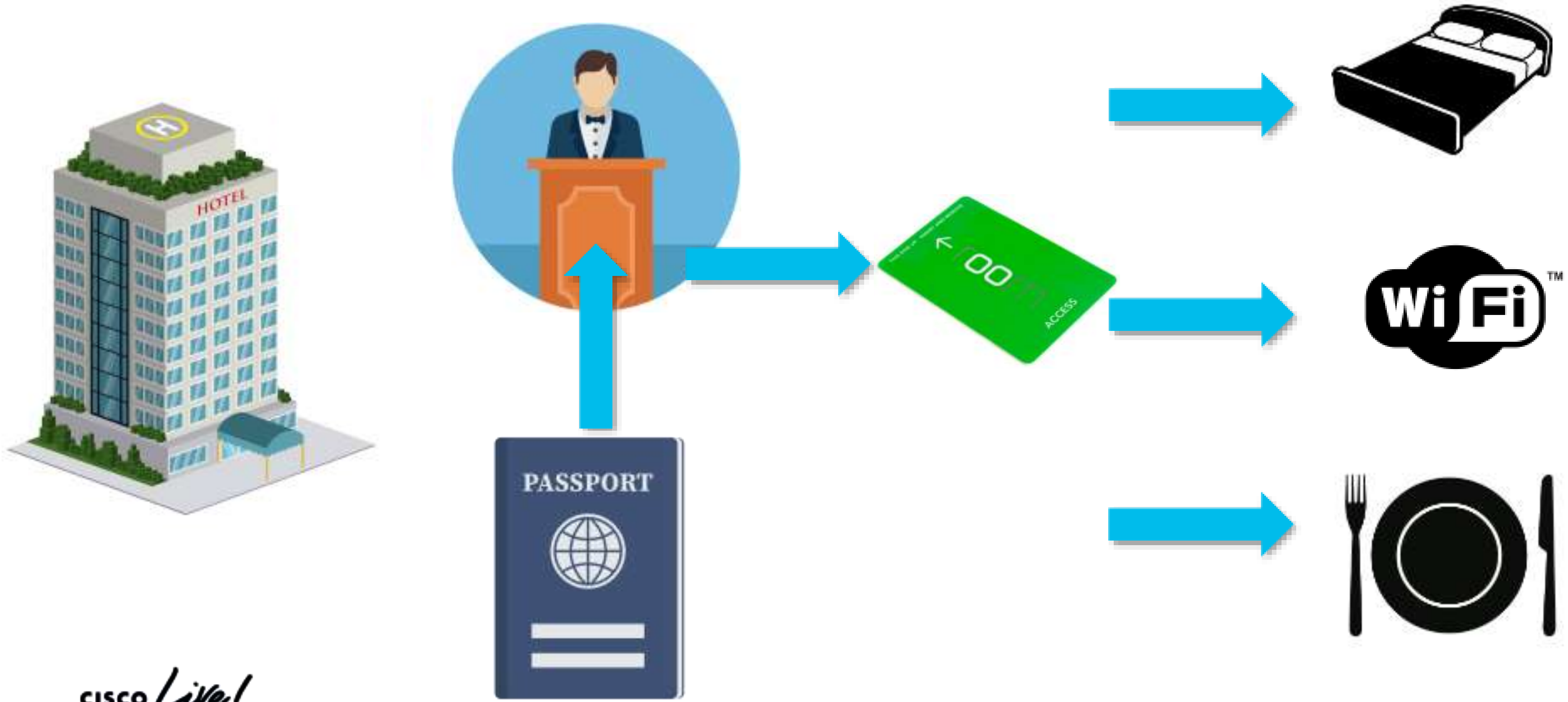
TOP

#4 Jabber Authentication

CHARTS

Jabber Authentication

Jabber Authentication flow



Jabber Authentication

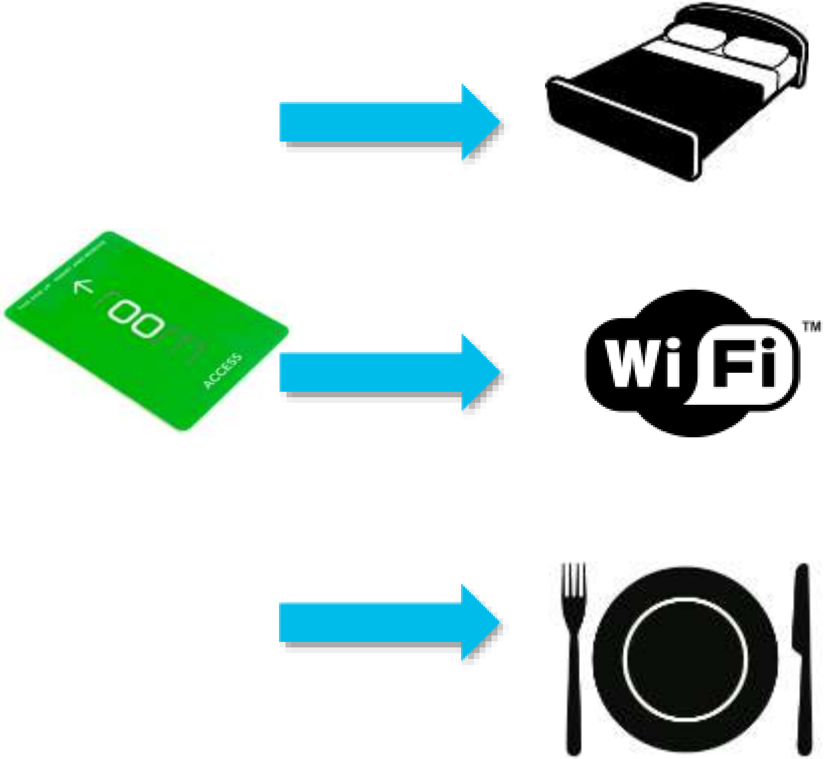
Jabber Authentication flow

AUTHENTICATION:
Verification that "you are, who you say you are"

Jabber Authentication

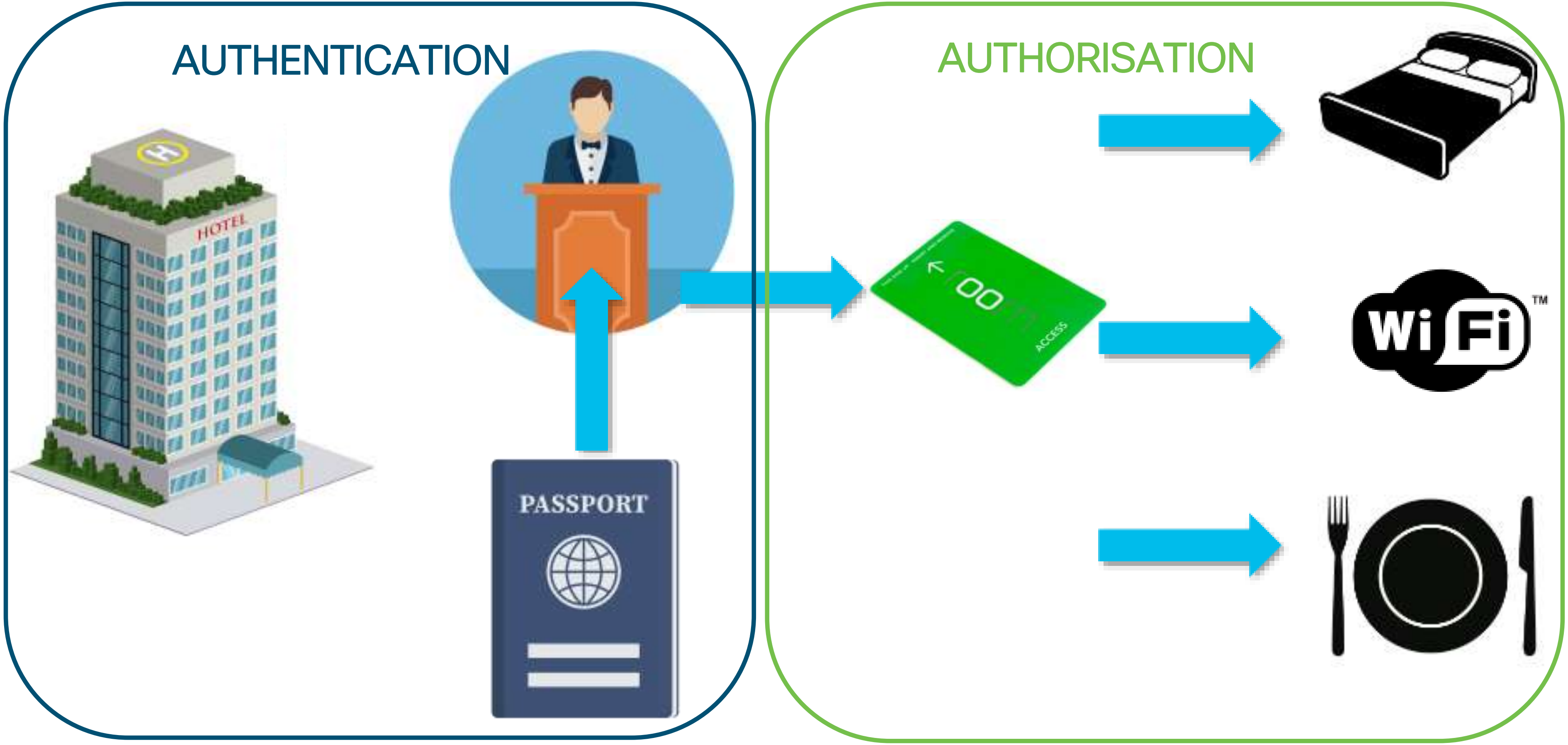
Jabber Authorisation

AUTHORISATION:
is the process of verifying that "you are permitted to do what you are trying to do".



Jabber Authentication

Jabber Authentication flow

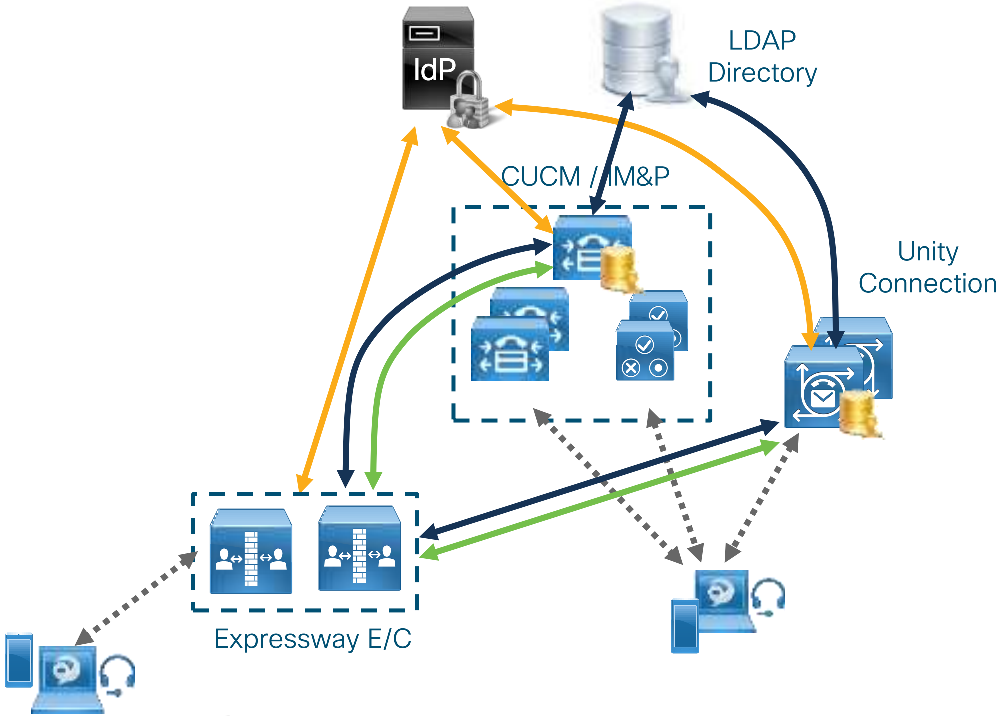


AUTHENTICATION

AUTHORISATION

Jabber Authentication

Authentication Options



1 **Local Authentication :**

- Built-in user databases in CUCM / IM&P and Unity Connection

2 **LDAP Authentication:**

- CUCM / IM&P and Unity Connection use LDAP bind to authenticate end-users against external directory

3 **Single Sign On (SAML based):**

- CUCM / IM&P, Unity Connection and Expressway set up SAML agreements with IdP
- End-user authentication is delegated to the IdP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Authentication

Single Sign on - SSO

A session/user authentication process that enables a user to provide credentials **only once** in order to access multiple applications.

The process authenticates the user for all the applications they have been given rights to without further prompts when they switch applications during the session.

Jabber Authentication

Single Sign On based on SAML 2.0

REFERENCE

- SAML - Security Assertion Markup Language → open Standard

  http://www.oasis-open.org/committees/security

- SAML v2.0 is current version (not backward-compatible with v1.0/1.1)

- Defines a framework for exchanging security and identity information between different systems.

Jabber Authentication

SSO – Requirements

REFERENCE

Cisco supports any IdP vendor that is compliant with the **SAML v2.0** OASIS Standard.

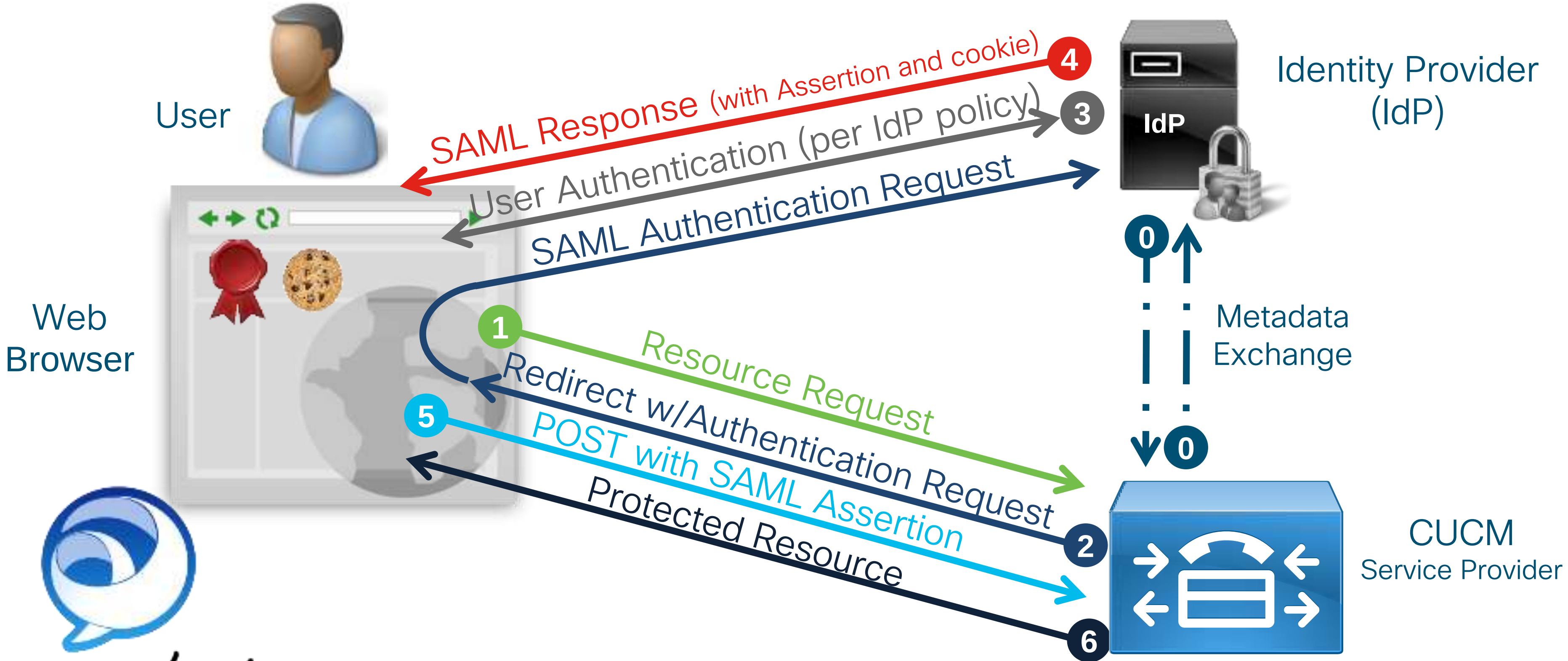
Internally in our development test cycles, we test our products against selected authentication methods of the following IdP's :

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIG-IP 11.6.0
- Okta 2017.38

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

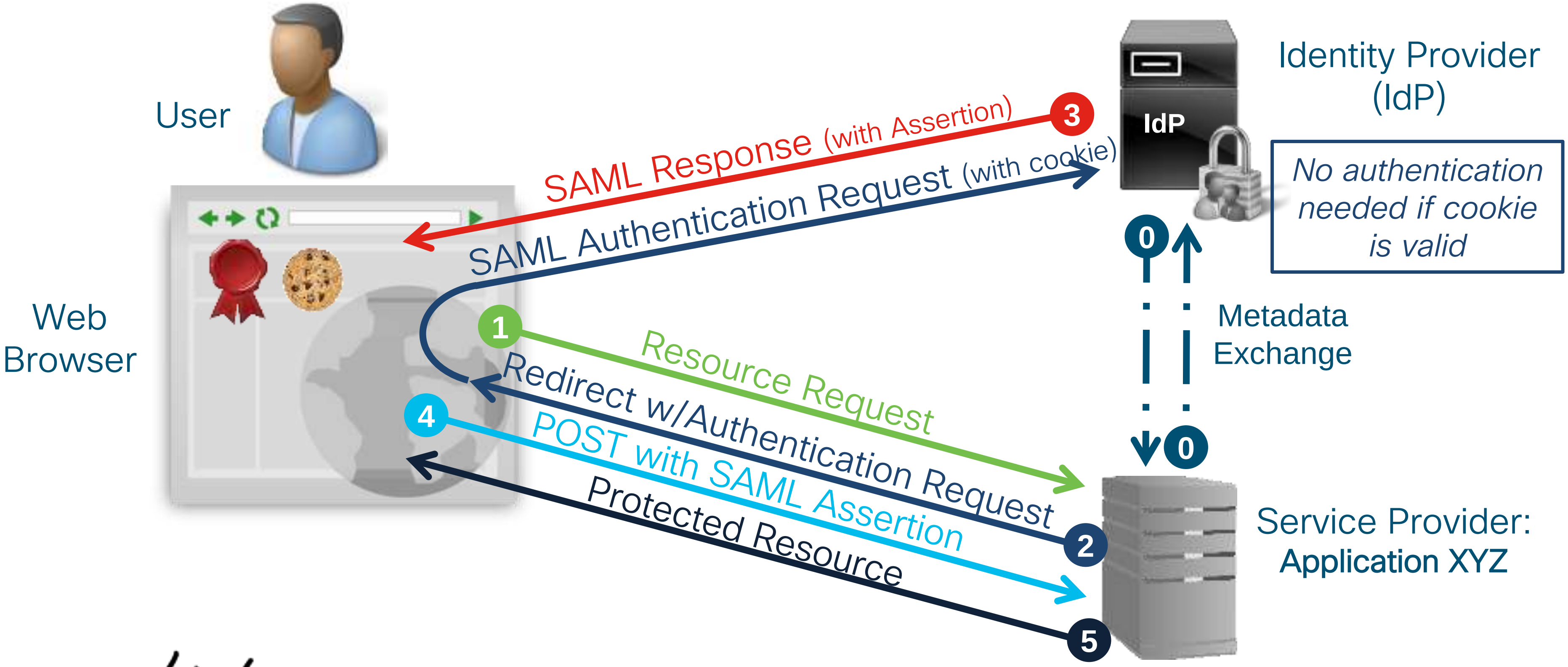
Jabber Authentication

Single Sign On - SAML 2.0



Jabber Authentication

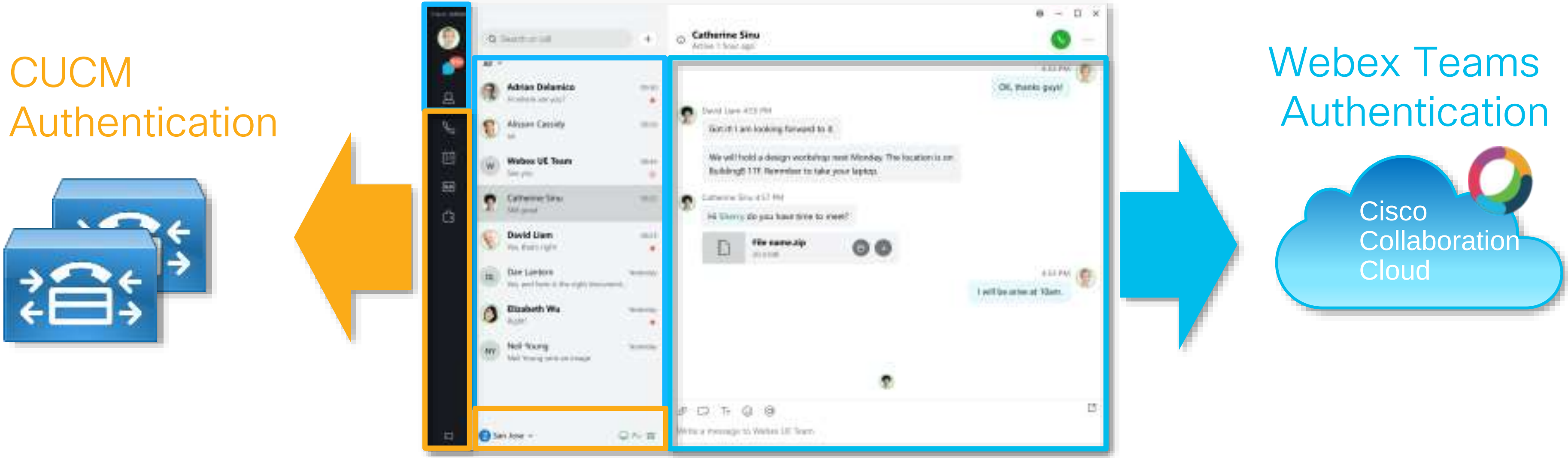
SAML SSO – avoid Re-Authentication


User
Web Browser
Identity Provider (IdP)
IdP
No authentication needed if cookie is valid
0
0
Metadata Exchange
Service Provider: Application XYZ
1 Resource Request
2 Redirect w/Authentication Request
SAML Authentication Request (with cookie)
3 SAML Response (with Assertion)
4 POST with SAML Assertion
5 Protected Resource

Jabber Authentication

Jabber in team messaging mode → SSO

AD Passwords will never be synchronized to the Webex cloud



OK, thanks guys!

Got it! I am looking forward to it.

We will hold a design workshop next Monday. The location is on Building8 11F. Remember to take your laptop.

Hi Sherry do you have time to meet?

I will be arrive at 10am.

Jabber Authentication

Multi Factor Authentication - MFA

AUTHENTICATION:
Verification that "you are, who you say you are"

HOTEL
PASSPORT

Jabber Authentication

Multi Factor Authentication - MFA

Authentication method where a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

Something you know:

- Password
- Security Question

Something you have:

- SMS
- Push
- Phone Call
- Token (HW/SW)
- Wearables
- U2F

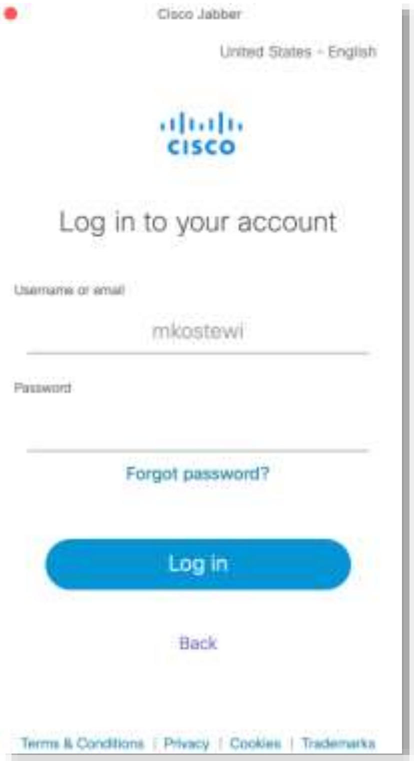
Something you are:

- Fingerprint
- Iris Scan

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Authentication

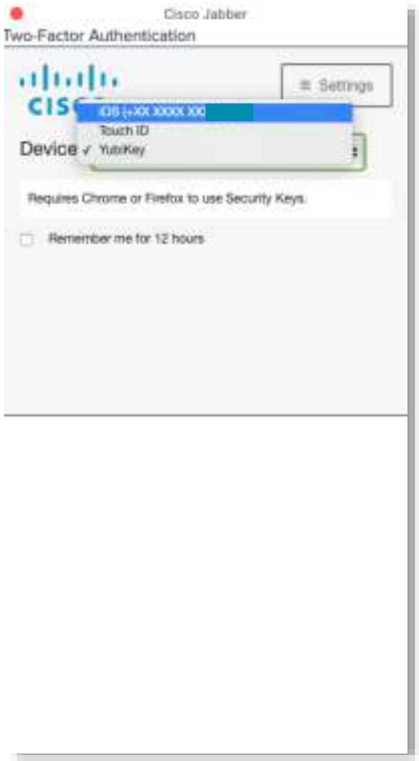
Multi Factor Authentication - MFA



Log in to your account

Username or email: mkostewi

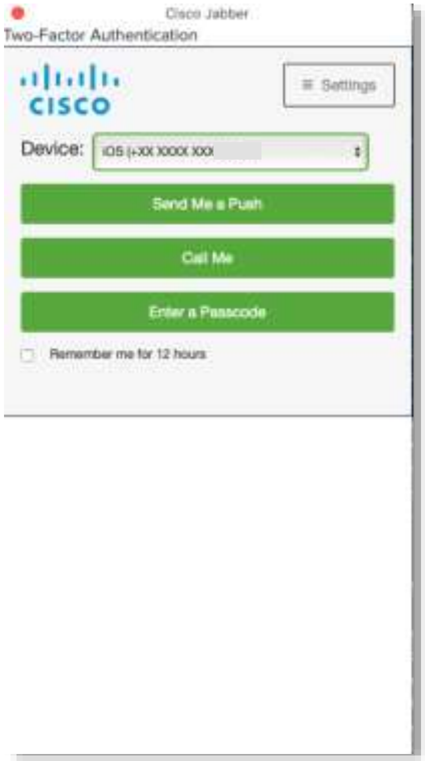
Password:



Device: ✓ YubiKey

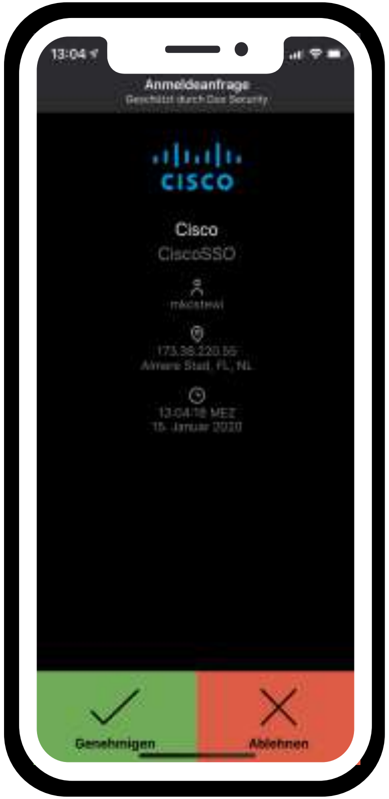
Requires Chrome or Firefox to use Security Keys.

□ Remember me for 12 hours



Device: iOS (+XX XXXX XXX

□ Remember me for 12 hours



Cisco
CiscoSSO
mkostewi
173.38.220.55
Almere Stad, FL, NL
13:04:18 MEZ
15. Januar 2020

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Authentication

Open Authorization – oAuth 2.0

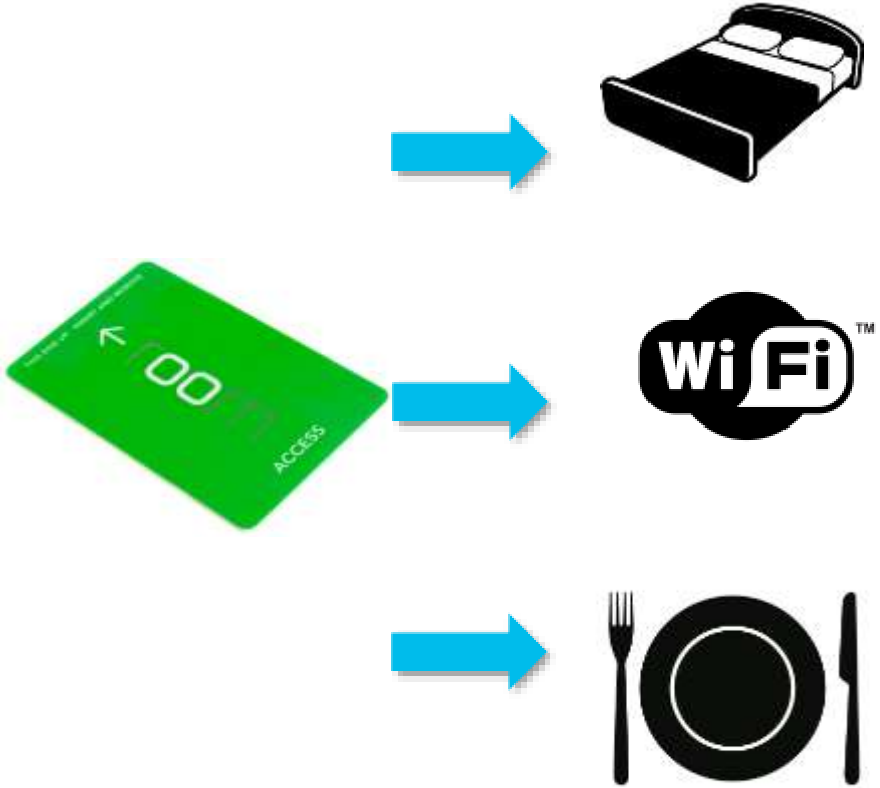
- Open Standard for Access Delegation (RFC 6749)
- OAuth provides to clients a "secure delegated access" to server resources on behalf of a resource owner – without sharing their credentials
- Authorization Code Grant based on:
  - **Access Token**: Authorizes the user to access a protected resource
  - **Refresh Token**: Allows a user to request a new access token once its expires

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Authentication

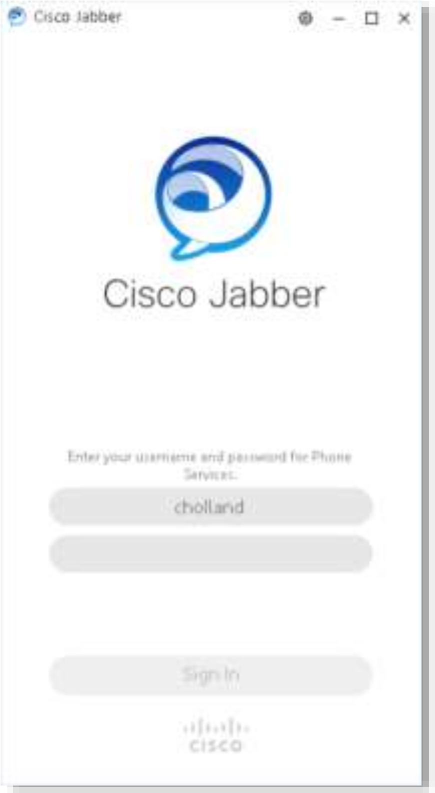
Open Authorization – oAuth 2.0

- Open Standard for Access Delegation (RFC 6749)
- OAuth provides to clients a "secure delegated access" to server resources on behalf of a resource owner – without sharing their credentials
- Authorization Code Grant based on:
  - **Access Token**: Authorizes the user to access a protected resource
  - **Refresh Token**: Allows a user to request a new access token once its expires



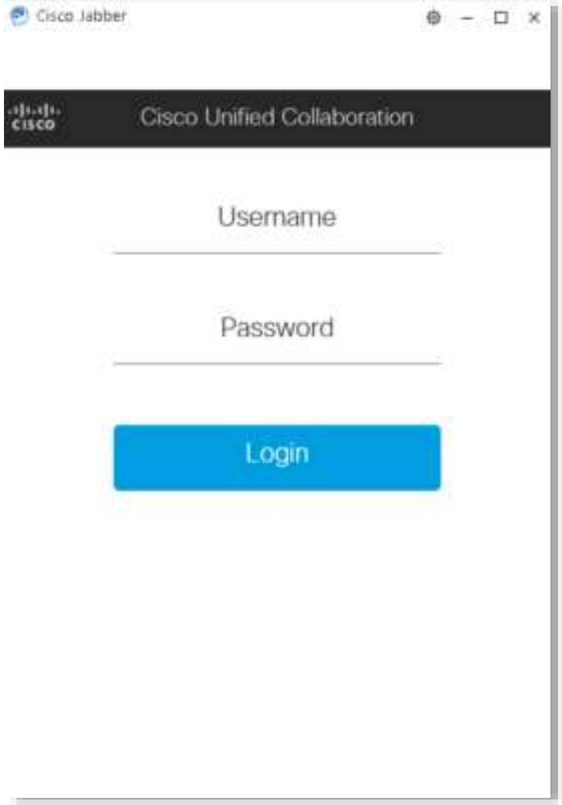
Jabber Authentication

Which Jabber LogIn is oAuth enabled?



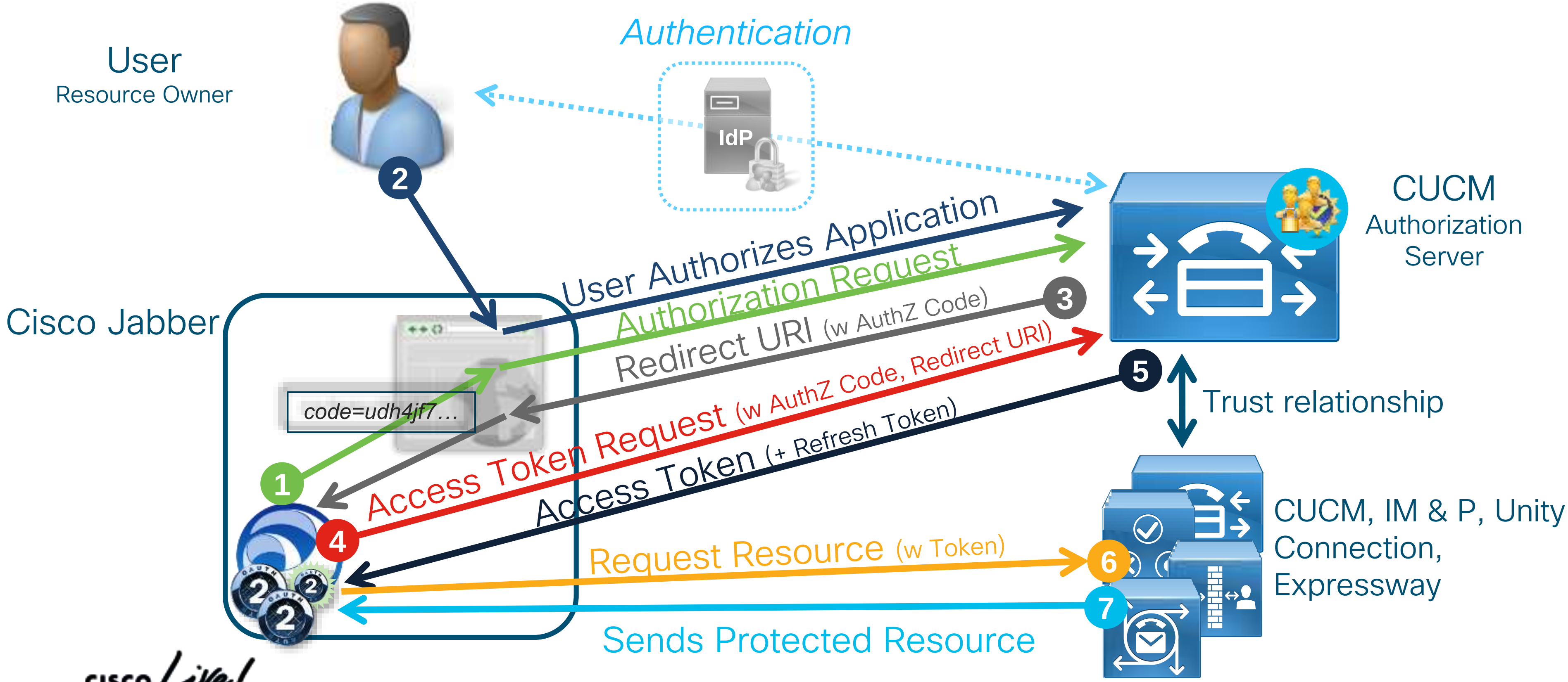
Enter your username and password for Phone Services.

cholland



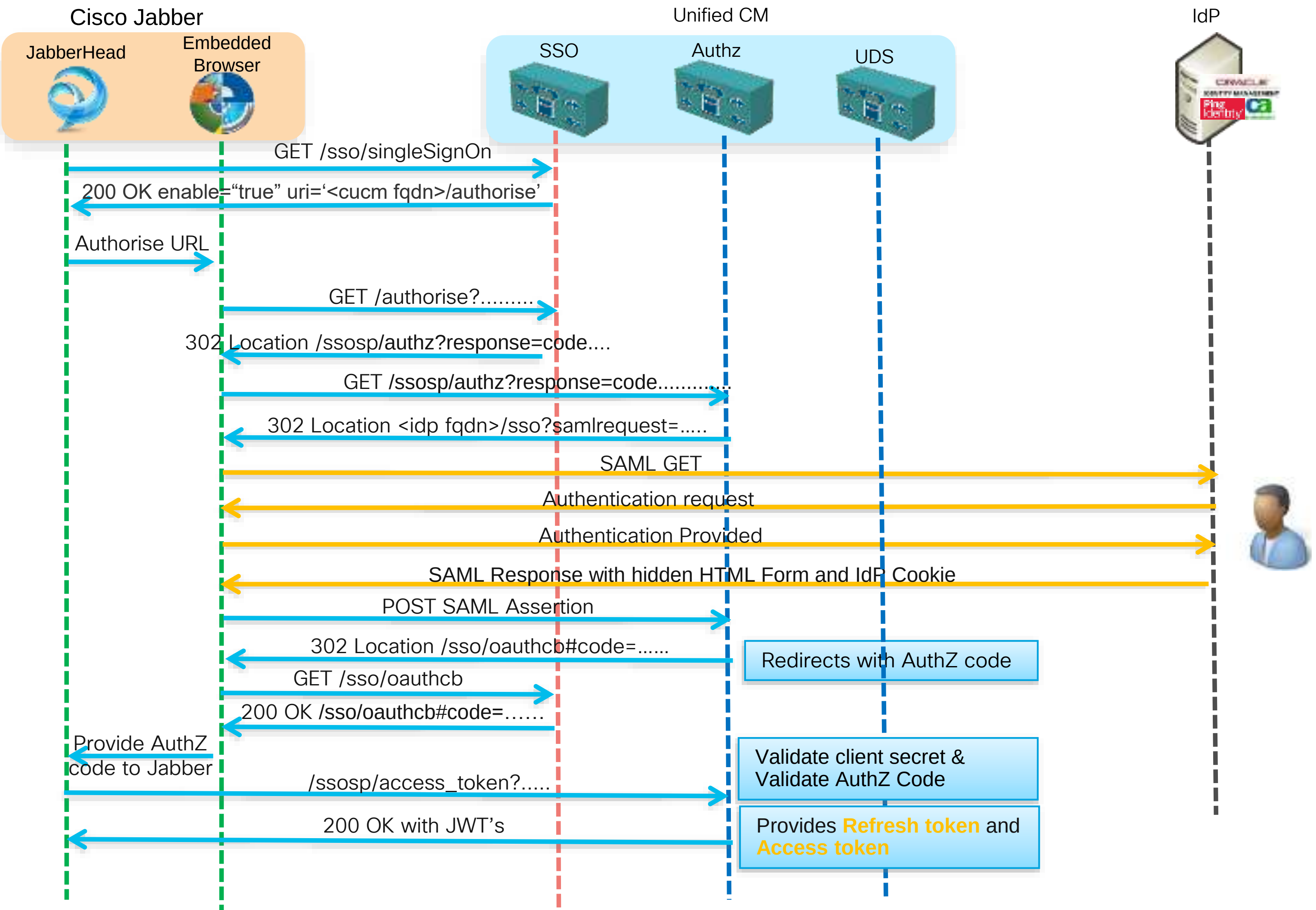
Jabber Authentication

oAuth based LogIn flow



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SAML & New OAuth flow @first AuthZ or when Refresh tokens expires



Cisco Jabber

JabberHead

Embedded Browser

Unified CM

SSO

Authz

UDS

IdP

GET /sso/singleSignOn

200 OK enable="true" uri='<cucm fqdn>/authorise'

Authorise URL

GET /authorise?.........

302 Location /ssosp/authz?response=code....

GET /ssosp/authz?response=code..........

302 Location <idp fqdn>/sso?samlrequest=.....

SAML GET

Authentication request

Authentication Provided

SAML Response with hidden HTML Form and IdP Cookie

POST SAML Assertion

302 Location /sso/oauthcb#code=......

Redirects with AuthZ code

GET /sso/oauthcb

200 OK /sso/oauthcb#code=……

Provide AuthZ code to Jabber

/ssosp/access_token?.....

Validate client secret & Validate AuthZ Code

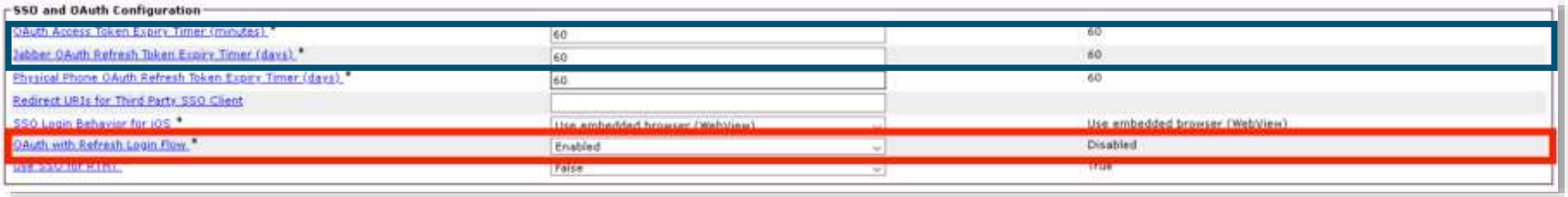
200 OK with JWT's

Provides Refresh token and Access token

Jabber Authentication

oAuth based Authentication flow

REFERENCE



SSO and OAuth Configuration

OAuth Access Token Expiry Timer (minutes) *	60	60
Jabber OAuth Refresh Token Expiry Timer (days) *	60	60
Physical Phone OAuth Refresh Token Expiry Timer (days) *	60	60
Redirect URIs for Third Party SSO Client		
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled	Disabled
Use SSO for RTMT	False	True

CUCM Admin > System > Enterprise Parameters:

Access Token default validity: **60 minutes**
(configurable: 1 minute → 24 hours)

Refresh Token default validity: **60 days**
(configurable: 1 day → 5 years)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Authentication

oAuth - Revoke CUCM Token

REFERENCE

- To revoke a Refresh Token for an active user and force them to re-authenticate (e.g., if one of their devices got lost), use the following REST-based API on CUCM (needs AXL admin credentials):

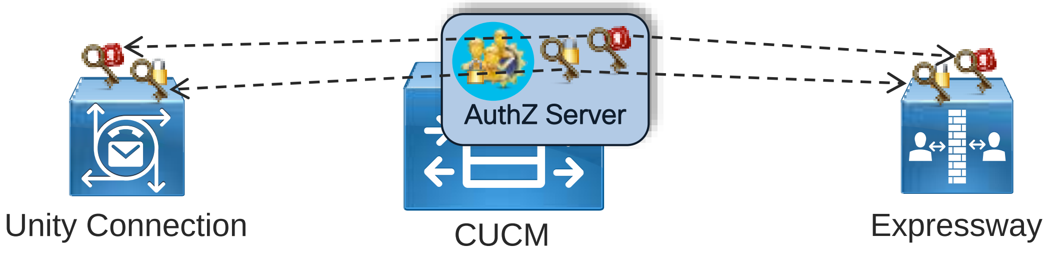
  https://<CUCMaddress>:8443/ssosp/token/revoke?user_id=<end_user>

- Changing the Refresh Token expiry timer Enteprise parameter automatically revokes all Refresh Tokens issued by that CUCM cluster
- Even if a Jabber client presents a valid access or refresh token to the UDS service on CUCM, the user must be "active" in the CUCM user database to be authenticated
  - Perform a manual LDAP sync or delete the user from the database to immediately prevent a user from using Jabber

Jabber Authentication

Authorization Key Management

REFERENCE



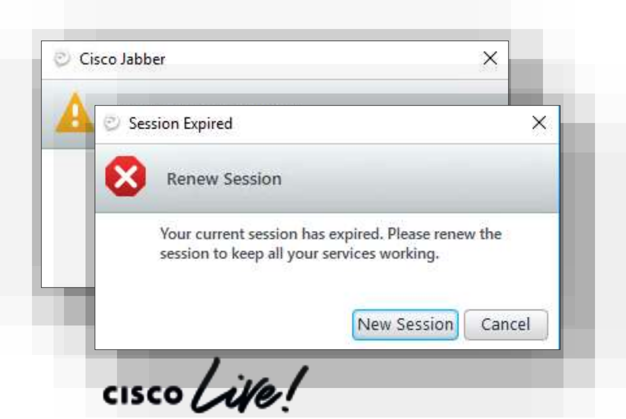
- CUCM generates a **signing key** and an **encryption key**, used to issue tokens
  - If needed (e.g., suspected compromise), keys can be regenerated through CUCM CLI commands:
    `set key regen authz signing` and **`set key regen authz encryption`**
  - Note: issuing these commands invalidates all previously-issued tokens
- A configuration "refresh" is needed in Expressway and Unity Connection after a CUCM upgrade, cluster change or keys re-generation, so that the new keys can be synchronized

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Authentication
SSO & oAuth based LogIn flow

- If OAuth token reaches 75% (by default 45 min) Jabber uses Refresh Token to get a new Access Token

- Same during lifetime of Refresh Token (by default 60 days)

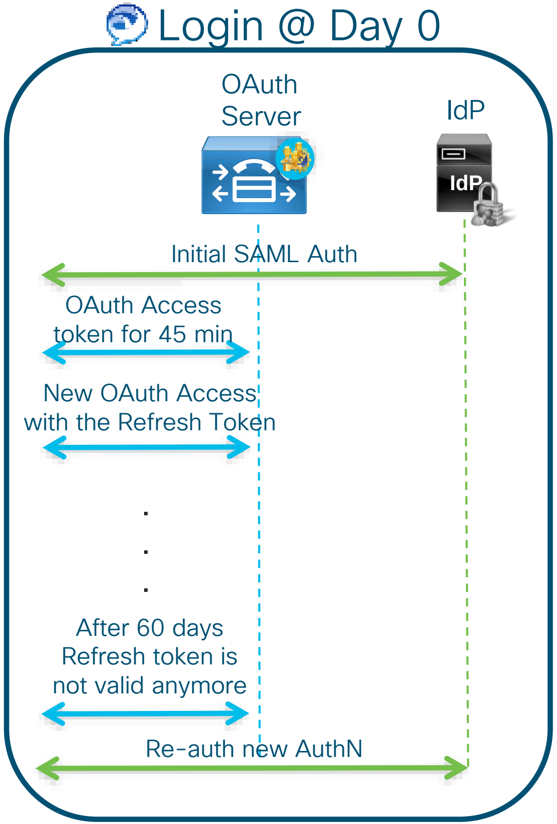


Cisco Jabber

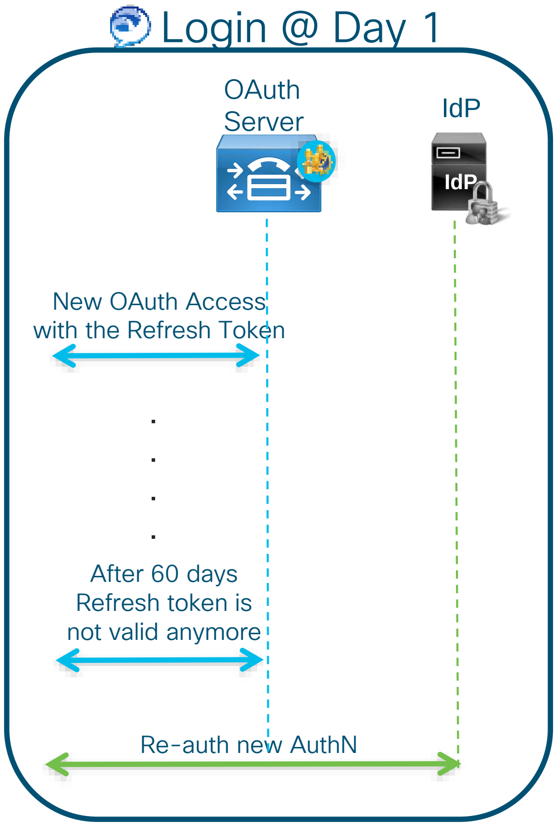
Session Expired

Renew Session

Your current session has expired. Please renew the session to keep all your services working.



Login @ Day 0
OAuth Server
IdP
IdP
Initial SAML Auth
OAuth Access token for 45 min
New OAuth Access with the Refresh Token
. . .
After 60 days Refresh token is not valid anymore
Re-auth new AuthN

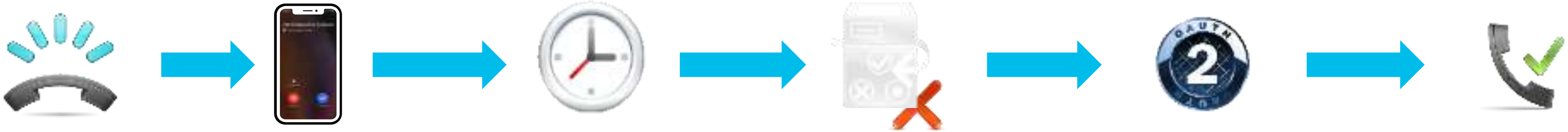


Login @ Day 1
OAuth Server
IdP
IdP
New OAuth Access with the Refresh Token
. . . .
After 60 days Refresh token is not valid anymore
Re-auth new AuthN

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Authentication

Why Jabber Login with New Flow…?



Push Notification
alerts Jabber of incoming chat/call

Fast Login
Client uses cached config for quick service reconnect

Off-line Login
allows the client to by-pass unavailable services

OAuth
allows Jabber to quickly access authorised UC services

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

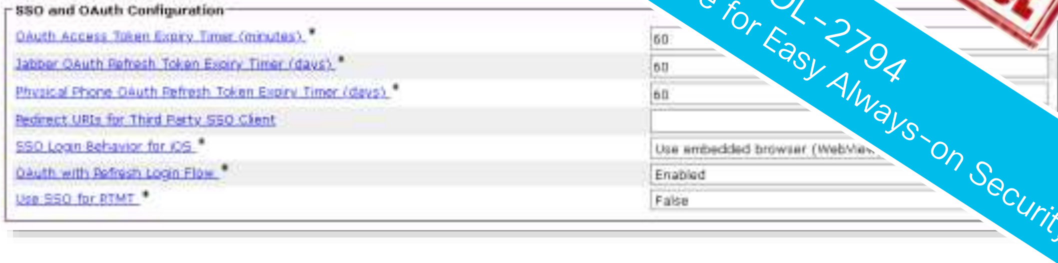
Jabber Authentication

Jabber and oAuth configuration

A New Architecture for Easy Always-on Security BRKCOL-2794

REFERENCE

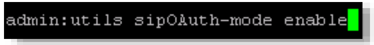
- oAuth based Authentication



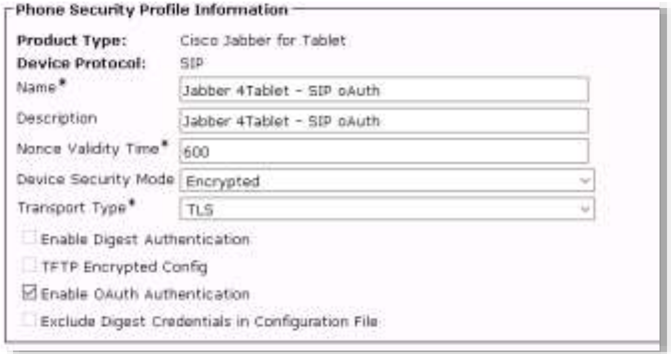
SSO and OAuth Configuration

OAuth Access Token Expiry Timer (minutes) *	60
Jabber OAuth Refresh Token Expiry Timer (days) *	60
Physical Phone OAuth Refresh Token Expiry Timer (days) *	60
Redirect URIs for Third Party SSO Client	
SSO Login Behavior for iOS *	Use embedded browser (WebView
OAuth with Refresh Login Flow *	Enabled
Use SSO for RTMT *	False

- SIP oAuth
  - Simple Encrypted Jabber clients
  - No longer require UCM mixed mode, CTL, LSCs, or CAPF enrollment
  - Enables ICE Media Path Optimization
  - Active Control (iX) can be negotiated in more call flows with CMS or Webex conferencing



```
admin:utils sipOAuth-mode enable
```



Phone Security Profile Information

Product Type:	Cisco Jabber for Tablet
Device Protocol:	SIP
Name*	Jabber 4Tablet - SIP oAuth
Description	Jabber 4Tablet - SIP oAuth
Nonce Validity Time*	600
Device Security Mode	Encrypted
Transport Type*	TLS

□ Enable Digest Authentication

□ TFTP Encrypted Config

☑ Enable OAuth Authentication

□ Exclude Digest Credentials in Configuration File

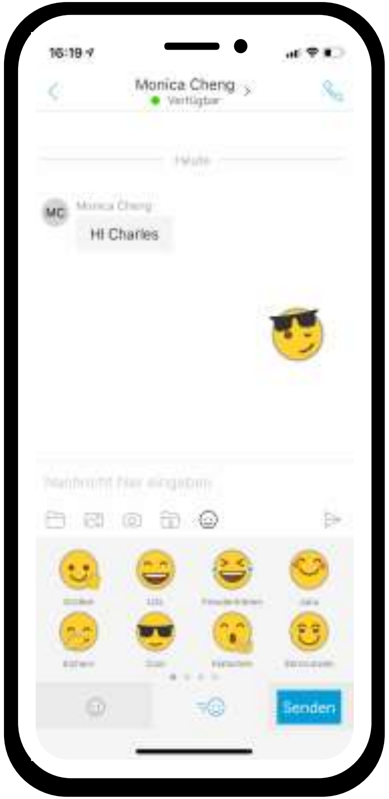
TOP

#3 Jabber Mobile Management

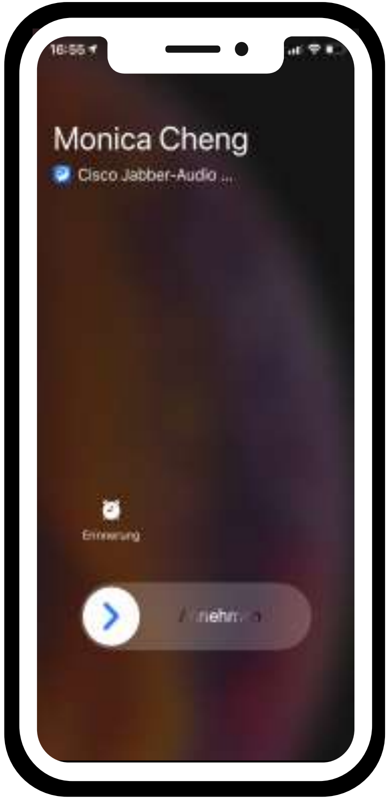
CHARTS

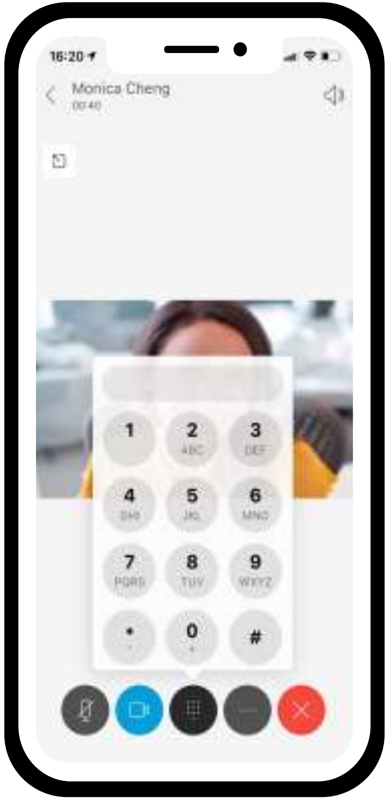
Jabber Mobile Management

Objective



HI Charles

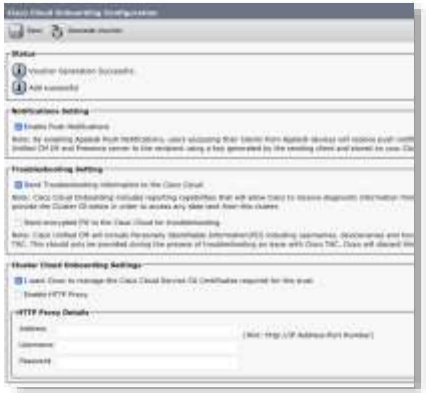




Jabber Mobile Management

Apple Push Notification

- Apple announced to change iOS API`s which will change Jabber notification behavior
- Apple Push Notifications support:
  - Jabber 11.9
  - CUCM and IM/P 11.5(1)SU3
  - Cisco Expressway X8.10.1 for optional MRA



Cisco Cloud Onboarding Configuration

Save Generate Voucher

Status

Voucher Generation Successful

Add successful

Notifications Setting

☑ Enable Push Notifications

Note: [illegible]

Troubleshooting Setting

☑ Send Troubleshooting information to the Cisco Cloud

Note: [illegible]

□ Send encrypted PII to the Cisco Cloud for troubleshooting

Note: [illegible]

Cluster Cloud Onboarding Settings

☑ I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust

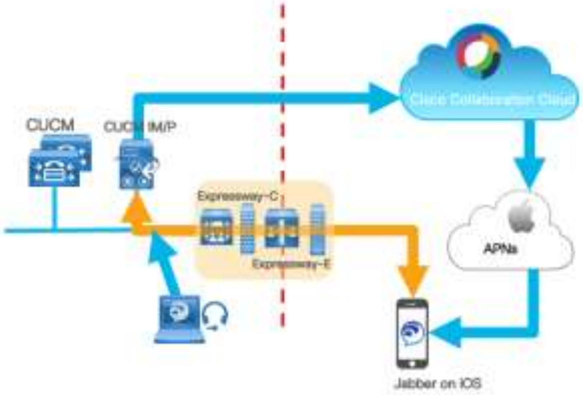
□ Enable HTTP Proxy

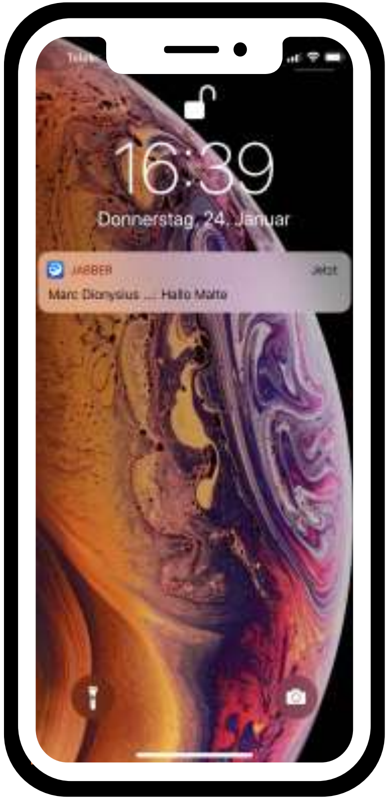
HTTP Proxy Details

Address (Hint : http://IP Address:Port Number)

Username

Password





Telekom

16:39

Donnerstag, 24. Januar

JABBER Jetzt

Marc Dionysius ... Hallo Malte

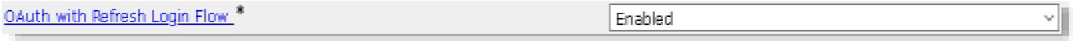
Details on APNs @BRKCOL3392 CLEUR 2019
https://www.ciscolive.com/global/on-demand-library.html?search=BRKCOL-3392#/session/1530899267184001gP3c

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Mobile Management

MRA Policies

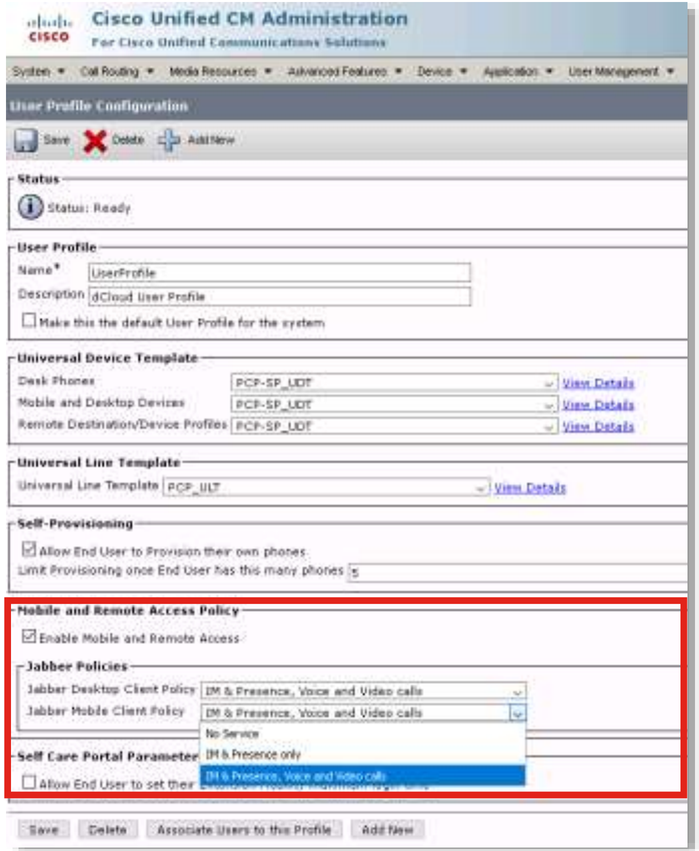
- CUCM provides policy based access for MRA connection:
  - No Service
  - IM & Presence only
  - IM & Presence, Voice and Video Calls
- Based on oAuth
- Requires CUCM 12.0+ Jabber 12.0+



OAuth with Refresh Login Flow * | Enabled

System → Enterprise Parameter

User Management → User Settings → User Profile



Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾

User Profile Configuration

Status

Status: Ready

User Profile

Name* UserProfile

Description dCloud User Profile

□ Make this the default User Profile for the system

Universal Device Template

Desk Phones PCP-SP_UDT View Details

Mobile and Desktop Devices PCP-SP_UDT View Details

Remote Destination/Device Profiles PCP-SP_UDT View Details

Universal Line Template

Universal Line Template PCP_ULT View Details

Self-Provisioning

☑ Allow End User to Provision their own phones

Limit Provisioning once End User has this many phones 5

Mobile and Remote Access Policy

☑ Enable Mobile and Remote Access

Jabber Policies

Jabber Desktop Client Policy IM & Presence, Voice and Video calls

Jabber Mobile Client Policy IM & Presence, Voice and Video calls

No Service

IM & Presence only

IM & Presence, Voice and Video calls

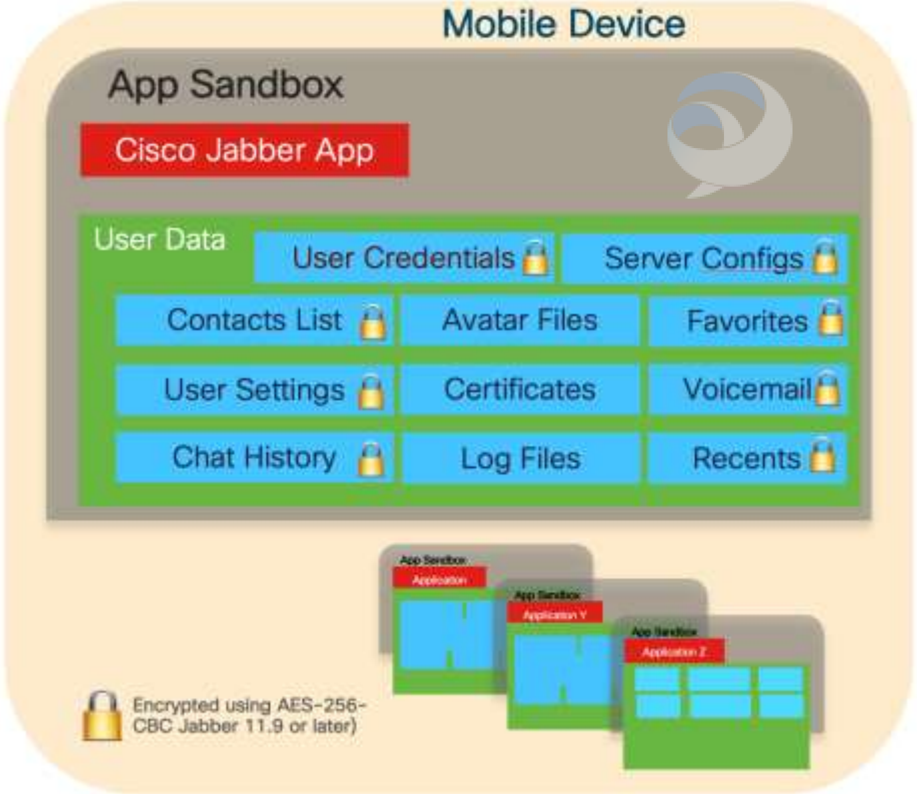
Self Care Portal Parameter

□ Allow End User to set their

Jabber Mobile Management

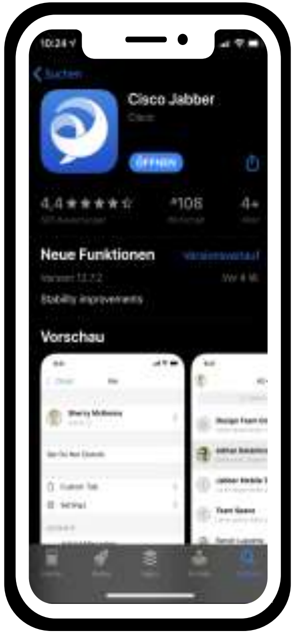
App Sandbox

- Jabber (11.9+) encrypts most cache and configuration files before it stores them on the user's device
- AES-256-CBC with self-generated encryption keys
- The encryption keys are stored only locally on the user's device in:
  - Keychain in iOS/Mac
  - KeyStore on Android
  - User profile directory in Windows
- Uninstallation of the App deletes all the data



Jabber Mobile Management

Option 1: Manually from Appstore



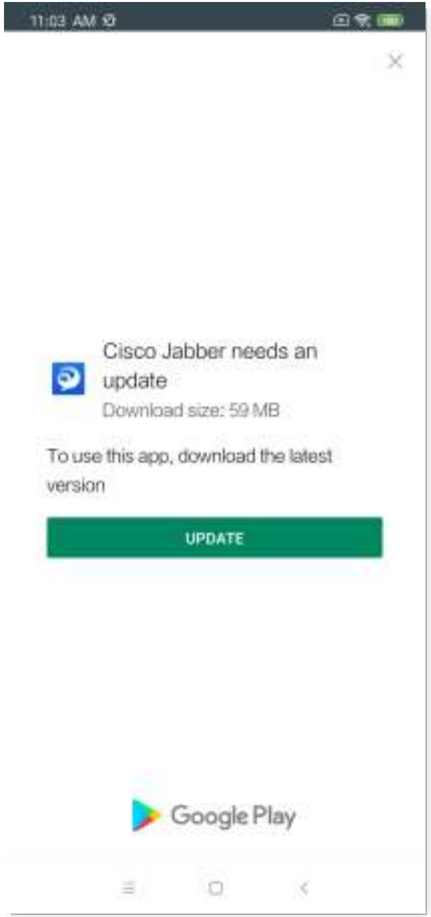
- Download manually from Appstore
- Sign In with Jabber credentials
  - Service discovery (recommended) or enter Service domain
  - MRA recommended
- Update manually

Jabber Mobile Management

Force Upgrading

- **Android only (**Android 5.0 (API level 21) or higher)
- **Jabber 12.8+**
  - Use Android native **'Immediate in-app update'**
  - **Immediate:** A full screen user upgrade experience that blocks the use of App, handled mostly by Google Play.
  - Jabber will pop up the update screen constantly once signed in, in order to push users to upgrade

```
<ForceUpgradingOnMobile >true</ForceUpgradingOnMobile >
```



Cisco Jabber needs an update

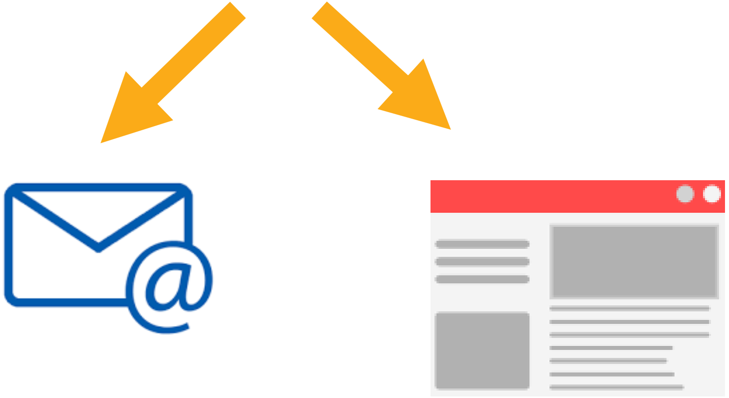
Download size: 59 MB

To use this app, download the latest version

Jabber Mobile Management

Option 2: URL config

- Download and update manually from Appstore
- Use Provision URL to apply Jabber config



https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_7/cjab_b_deploy-jabber-team-messaging-mode127/cjab_b_deploy-jabber-team-messaging-mode127_chapter_01001.html#reference_773264F416A93B5905F8312214CB7355

Jabber Mobile Management

Option 2: URL config

REFERENCE

Provision Service discovery Information directly to the user by URL config:

- Webex - _cisco-uds / _cuplogin / _collab-edge
- CUCM - _cuplogin / _collab-edge
- CUP - _cisco-uds / _collab-edge
- ServicesDomainSsoEmailPrompt – ON / OFF
- InvalidCertificateBehavior – RejectAndNotify / PromptPerSession
- PRTCertificateUrl
- Telephony_Enabled – Ture / Flase
- ForceLaunchBrowser – True / False
- AllowTeamsUseEmbeddedSafari – True / False

Examples:

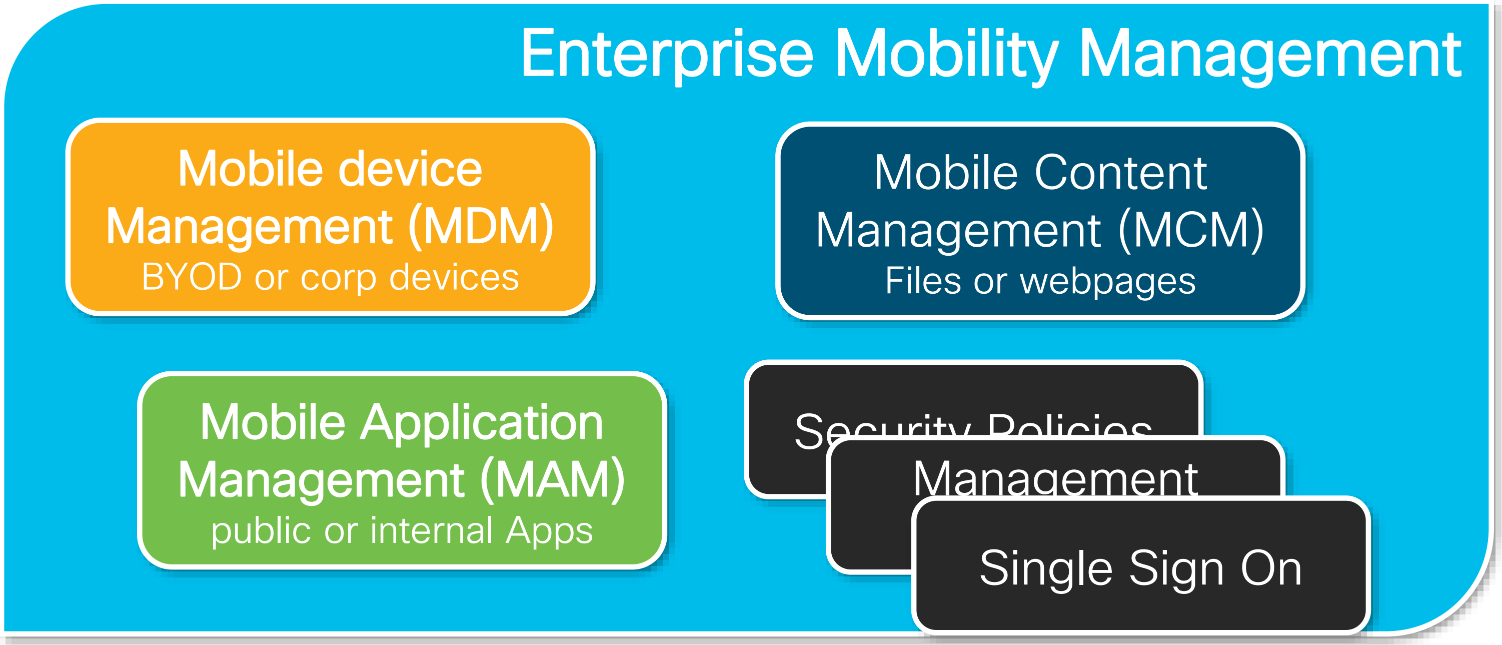
```
ciscojabber://provision?ServicesDomain=cisco.com
ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com
ciscojabber://provision?ServicesDomain=service_domain&VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX
ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP
ciscojabber://provision?ServicesDomain=cisco.com&VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP
&ServicesDomainSsoEmailPrompt=OFF
```

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_7/cjab_b_deploy-jabber-team-messaging-mode127/cjab_b_deploy-jabber-team-messaging-mode127_chapter_01001.html#reference_773264F416A93B5905F8312214CB7355

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Mobile Management

What is EMM, MDM, MAM….?



Enterprise Mobility Management

Mobile device Management (MDM)
BYOD or corp devices

Mobile Content Management (MCM)
Files or webpages

Mobile Application Management (MAM)
public or internal Apps

Security Policies

Management

Single Sign On

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Mobile Management

Option 3: EMM Provisioning

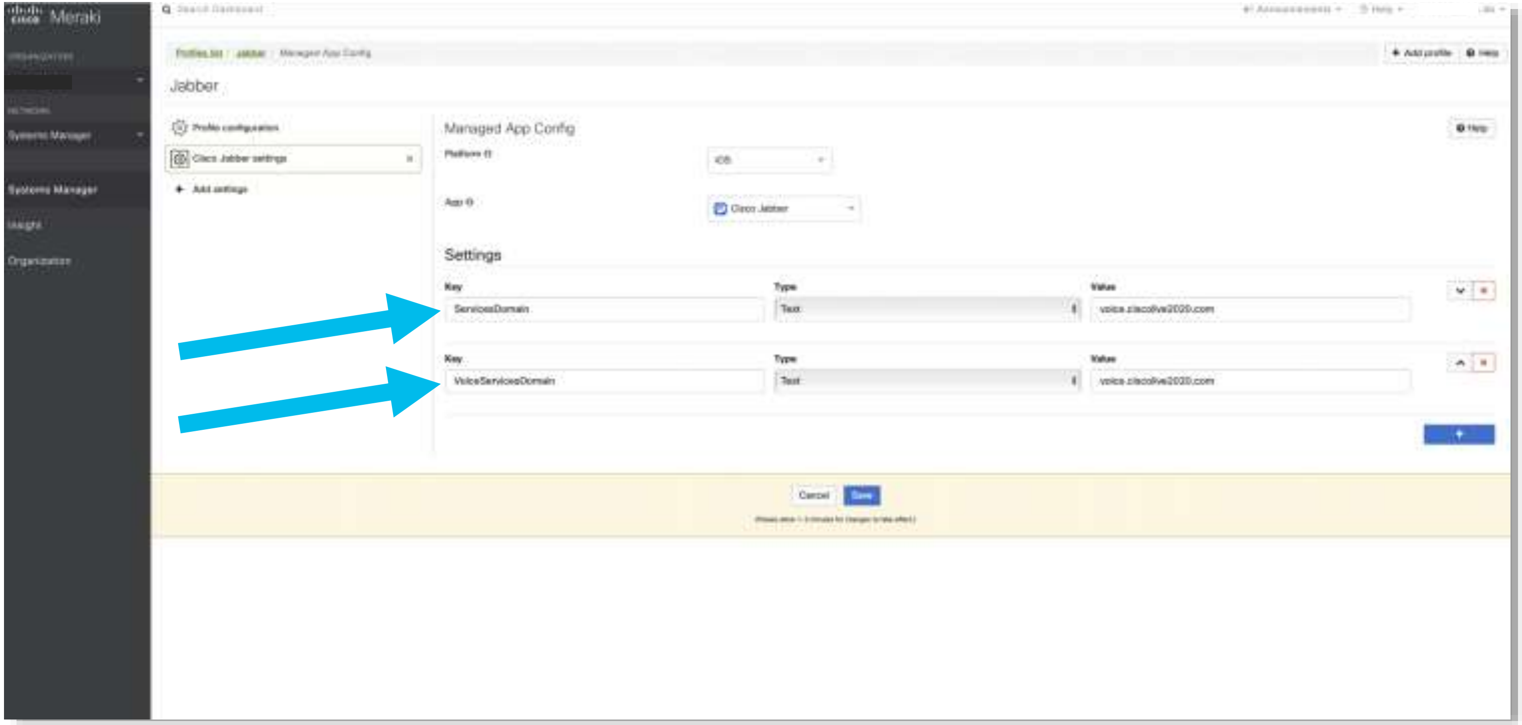
- Distribution and configuration of Jabber via EMM
- Uses the native mobile APIs of Jabber mobile
- Supported by several EMM vendors: appconfig.org
- Deployment mechanisms use:

Apple: “Managed App Configuration”

Google: “Android for Work”
requires devices running Android 5 and later

Jabber Mobile Management

Option 3: EMM Provisioning



Managed App Config

Platform: iOS

App: Cisco Jabber

Settings

Key	Type	Value
ServicesDomain	Text	voice.ciscolive2020.com
VoiceServicesDomain	Text	voice.ciscolive2020.com

Meraki EMM

Jabber Mobile Management

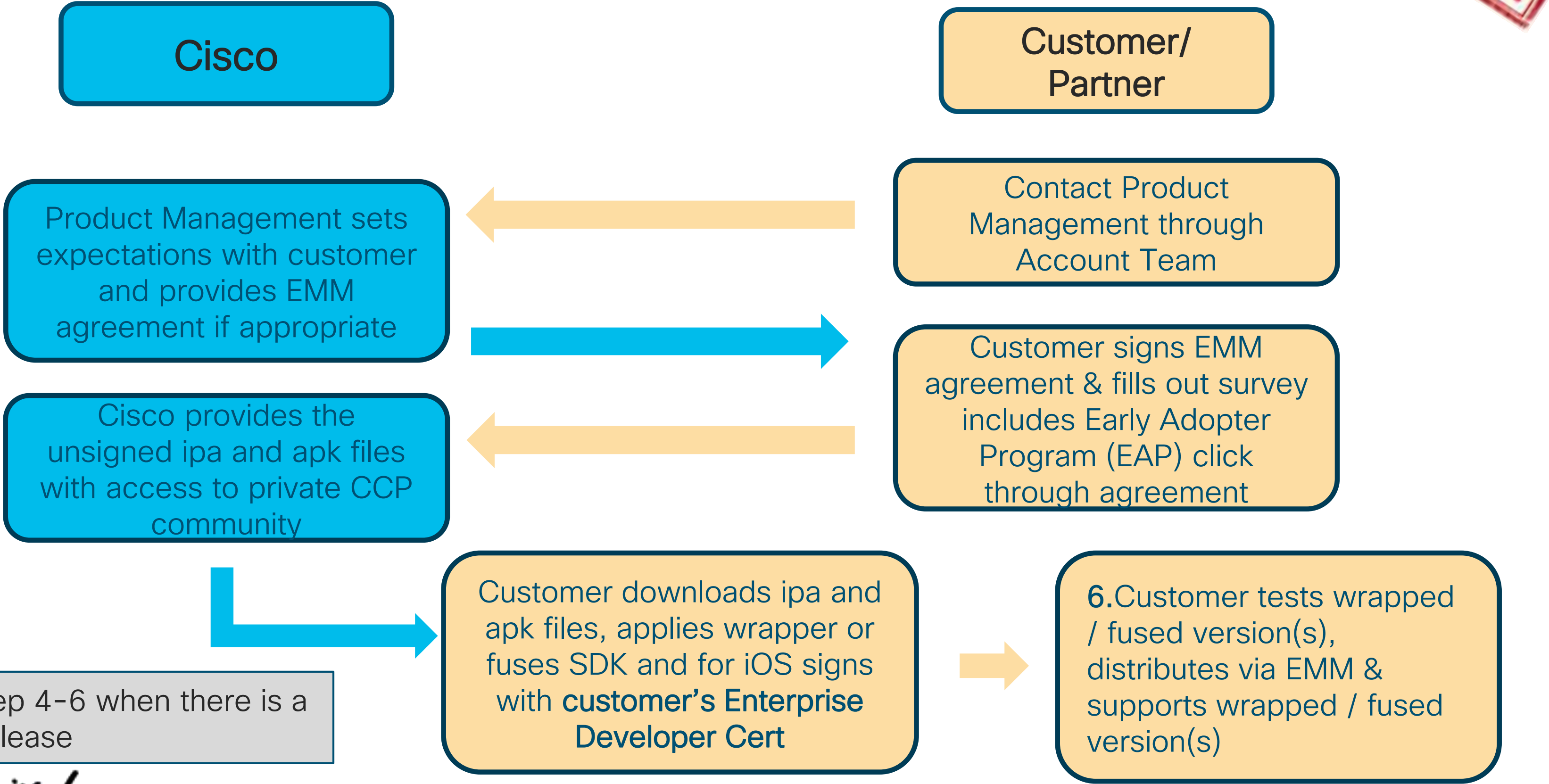
Option 4a: EMM Wrapping or fusing

- **Customer** or **Partner** Supported – TAC **will NOT troubleshoot integration**
- App wrapping performed by customer or partner, and signed with customer’s enterprise certificate
- App fusing with SDK performed by customer or partner, and signed with customer’s enterprise certificate
- Apple Push Notifications **will not** work
- Updates & new Releases needs to integrated manually

Jabber Mobile Management

Option 4a: EMM Wrapping or fusing process

REFERENCE



Cisco

Customer/ Partner

Contact Product Management through Account Team

Product Management sets expectations with customer and provides EMM agreement if appropriate

Customer signs EMM agreement & fills out survey includes Early Adopter Program (EAP) click through agreement

Cisco provides the unsigned ipa and apk files with access to private CCP community

Customer downloads ipa and apk files, applies wrapper or fuses SDK and for iOS signs with **customer's Enterprise Developer Cert**

6.Customer tests wrapped / fused version(s), distributes via EMM & supports wrapped / fused version(s)

Note: Redo step 4-6 when there is a new Jabber release

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Mobile Management

Option 4b: EMM Wrapping or fusing by Cisco Advanced Service

```
<link rel="stylesheet" href="http://localhost/css.css" type="text/css"
<script type="text/javascript" src="http://localhost/javascript.js"></script>
<script type="text/javascript">
  (function(){
    onLoaded: function(request) {
      if (request.name == 'log_error') return;
      log.trace("Ajax.Request: " + (request.name || request.url.substr(0, 3
        )) + "...");

    },
    onComplete: function(request) {
      if (request.name == 'log_error') return;

    },
    onException: function(request, e) {
      if (request.name == 'log_error') return;
      log.fatal(request.url
        .stack);
```

- **Customer** or **Partner** Supported – TAC **will NOT troubleshoot integration**
- App wrapping performed by Cisco AS Team, and signed with Cisco`s certificate
- App fusing with SDK performed by Cisco AS Team, and signed with Cisco`s certificate
- Apple Push Notifications **will** work
- Updates & new Releases needs to integrated manually

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Mobile Management

Option 5: Jabber for EMM

Microsoft Intune

BlackBerry Dynamics

- Jabber (12.8+) built on top of MS Intune SDK(preferred) and BlackBerry Dynamics.
- Users can get these two App from Apple’s App Store and Google Play Store.
  - Jabber for Intune
  - Jabber for Blackberry Dynamics
- Cisco Jabber for MAM will have different release cycles
- It will support the following functions:
  - Jailbreak/Root detection
  - Disable Copy-Paste outside the app
  - Disable “open in” and “share with” 3rd party apps
  - Enforce minimum app version
  - Enforce minimum OS version
  - Apple Push Notifications(iOS)
  - Remote wipe app data
  - Block standard Jabber

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

TOP

#2 Compliance

CHARTS

Jabber Compliance

Overview

Jabber Compliance

Message Archiver

- Logging of all IM traffic (sender & recipient information, timestamp, and the message body)
- single cluster, intercluster or federated network
- Point to point & group chats
- inbound only or in and outbound IM traffic
- External database required (for storing of achieved messages)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

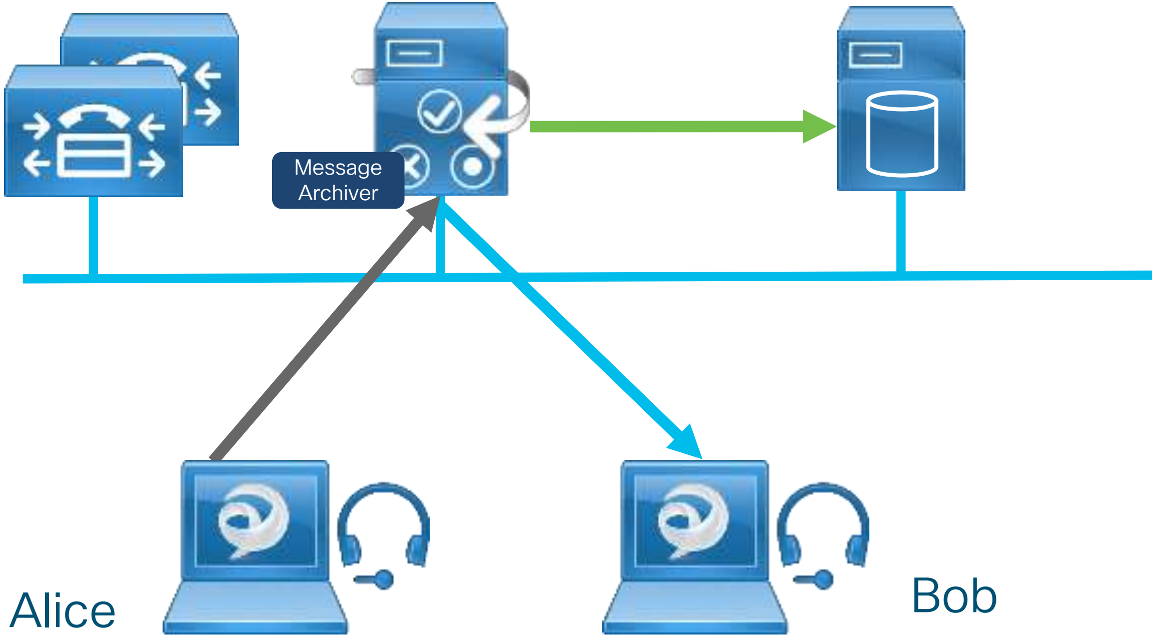
Jabber Compliance

Message Archiver

Alice sends Bob a Message, passing through IM & P Server

IM & P Server passes Message to Bob

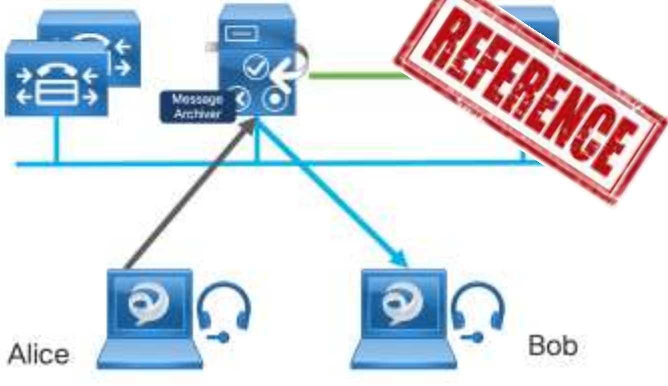
Message is being achieved to external database including Alice and Bobs information, timestamp and message body



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Compliance

Message Archiver



REFERENCE

Encryption supported (SHA2 with AES256)

- Information stored encrypted on DB (key by IM&P)

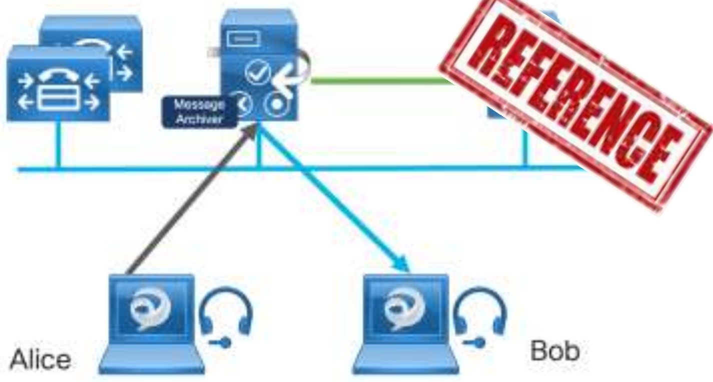
External Databases required – can be shared with persistent group chat and managed file transfer as each feature uses separate data tables. This is dependent on the capacity of the database instance.

- PostgreSQL
- Oracle SQL
- Microsoft SQL Server

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

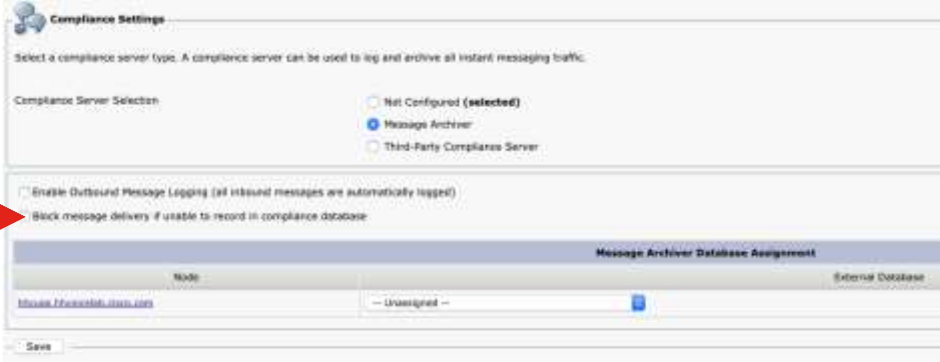
Jabber Compliance

Message Archiver



REFERENCE

- Configure Compliance Settings
- Activate the Cisco XCP Message Archiver
- Restart Cisco XCP Router
- Configure Alarms for IM Compliance (Cisco XCP Message Archiver) (optional)
- Configure Encryption (optional)



Compliance Settings

Select a compliance server type. A compliance server can be used to log and archive all instant messaging traffic.

Compliance Server Selection
○ Not Configured **(selected)**
● Message Archiver
○ Third-Party Compliance Server

□ Enable Outbound Message Logging (all inbound messages are automatically logged)
□ Block message delivery if unable to record in compliance database

Message Archiver Database Assignment	
Node	External Database
[illegible]	-- Unassigned --

Messaging → Compliance → Compliance Settings

Jabber Compliance

3-rd Party Compliance Server

Enhanced compliance functions (Logging or ethical wall)

- IM & P uses Event Broker component to send events to 3rd Party compliance server:
  - User login/ out,
  - presence sharing
  - IM exchange
  - group chat activity
- Events set by policy:
  - filter certain users, groups,
  - block/modify content depending on originator or recipient
- Potential risk of performance delays in network based on volume of events
- All IM&P server will redirect events to configured 3rd Party Compliance server
- Supported clients – Jabber, 3rd Party XMPP clients
- No secure connection (TLS/SSL) between IM & P and 3rd Party compliance server

Jabber Compliance

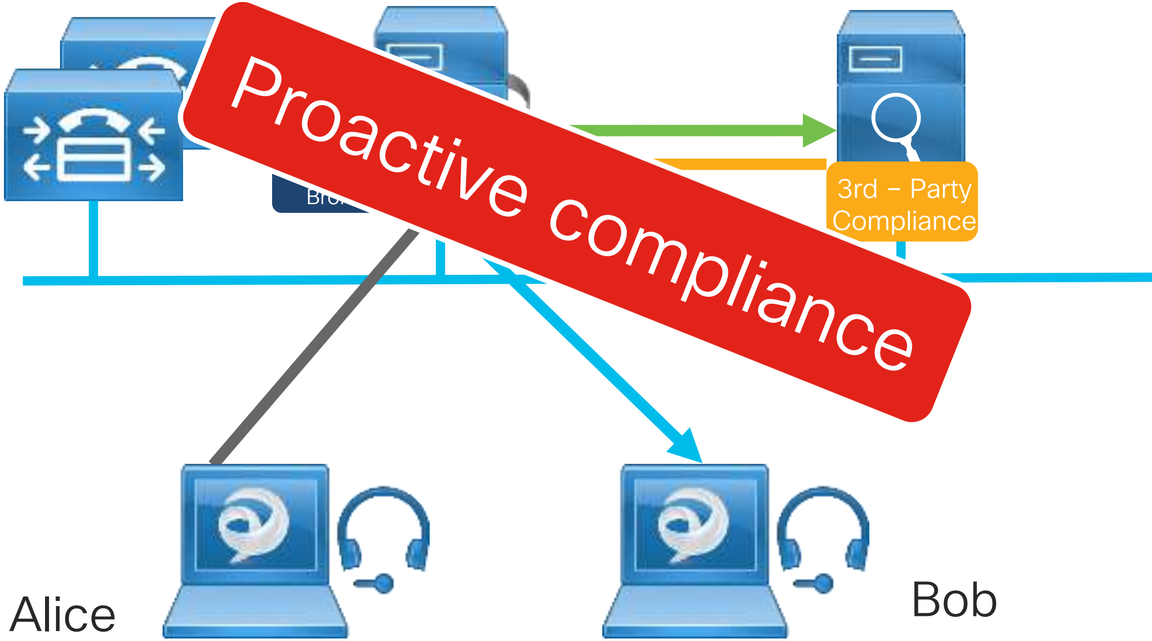
3-rd Party Compliance Server

Alice sends Bob a Message, passing through IM/P Server

IM/P Server passes Message to 3rd Party Compliance server via IM, using Event Broker

3rd Party Compliance server may apply rule/ filtering based on policy and passes the IM back to IM & P

IM & P passes (modified) IM to Bob



Jabber Compliance

Compliance Profiles

Event Broker

REFERENCE

- Profiles based on Jabber Session Manager (JSM) and/or Text Conferencing (TC) event
  - Defined events will be logged to compliance Server
  - Handling definition of compliance server:
    - Error responses
    - Waiting for response
    - No response

- Jabber Session Manager (JSM) Event and Parameter:
  - User related XMPP traffic, maintains user state, manages rosters and privacy

- Text Conferencing (TC) Event and Parameter:
  - Manages chat rooms (ad-hoc & persistent)

Profile Parameters:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/im_compliance/12_5_1/cup0_b_im-compliance-guide-1251/cup0_b_im-compliance-guide-1251_chapter_010.html

Jabber Compliance

Compliance Profiles

Jabber Session Manager (JSM) Events

Event Broker

REFERENCE

Event	Description
e_SESSION	Packets sent during login, which is the creation of a new session.
e_OFFLINE	Packets sent to users who are offline. Offline users are users who do not have an active session.
e_SERVER	Packets sent directly to the server for internal handling.
e_DELIVER	The first event for packets coming in from another server; the second event for packets coming in from a user on the same server. (The first event for packets coming in from the same server is es_IN.)
e_AUTH	IQ packets sent during authentication.
e_REGISTER	Packets generated during registration of a new account by a user.
e_STATS	Packets sent periodically that contain server statistics.
e_DISCOFEAT	Triggered when a user sends a disco#info query.
e_PRISESSION	Determines a user's primary or default session when the user has more than one session. An EventBroker component may dictate the choice of a user's primary session.
es_IN	Generated when a stanza is about to be received by a user's session.
es_OUT	Generated when a stanza is sent from a user's session.
es_END	Packets generated when a user logs out.

Jabber Compliance

Compliance Profiles

REFERENCE

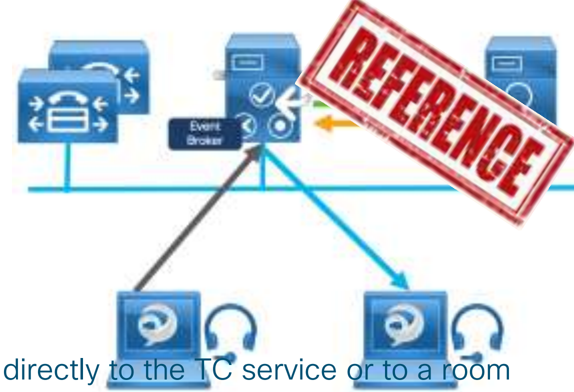
Jabber Session Manager (JSM) Parameter

Parameter	Description
Packet Type	•Select one of the following XMPP packet types: all - All packets •iq - Packets used during info-query functions •message - Packets containing standard IM or group chat messages •presence - Packets containing presence information •subscription - Packets sent when subscribing to another user's presence
Handling	Select bounce if errors returned from the compliance server should be bounced back to the originating party or component Select pass if they should be discarded.
Fire and Forget	Leave the check box unchecked if the IM and Presence Service node must wait for a response from the compliance server before it continues to process the event. Check the check box if the IM and Presence Service node does not require a response from the compliance server before it continues to process the event further.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Compliance

Compliance Profiles



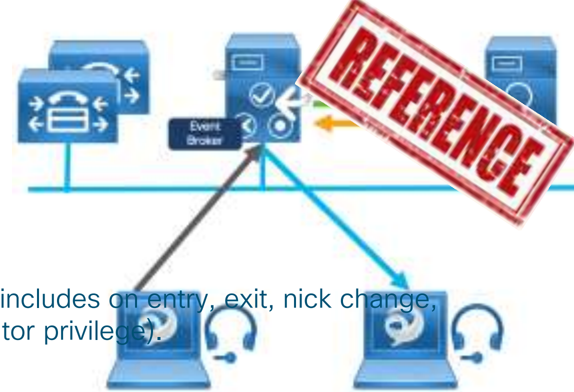
Text Conferencing (TC) Events (1/2)

Event	Description
onServicePacket	The system receives a packet from the router that is either addressed directly to the TC service or to a room that does not currently exist on the system.
onBeforeRoomCreate	A gear is attempting to create a room on the system.
onAfterRoomCreate	A room has been successfully created on the system. The only valid response is PASS with no modification to the original stanza.
onServiceDiscoInfo	An entity has sent a disco#info packet to the TC service. The only valid response is PASS.
onServiceReconfig	The TC service receives a signal to reconfigure itself. The only valid response is PASS. This is a notification event only. The XDB packet will be of a type="set". The external component should not respond to this packet.
onDestroy	A room owner closes a room. The only valid response is PASS.
onClose	A gear requests to close a room.
onPacket	A new XML stanza is directed at a room, or participant within a room.
onMetaInfoGet	Room configuration information is available. The only valid response is PASS.
onBeforeMetaInfoSet	A room configuration is about to be modified by a user.
onAfterMetaInfoSet	A room configuration has been modified by a user. The only valid response is PASS with nothing in it.
onExamineRoom	A Jabber entity requests information, either by browse or disco, from a room. The only valid response is PASS.

Jabber Compliance

Compliance Profiles

Text Conferencing (TC) Events (2/2)



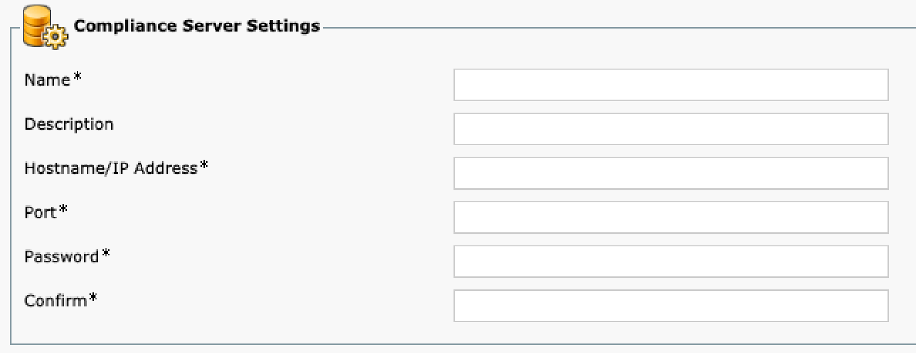
Event	Description
onBeforeChangeUser	A change has been requested of a user role, nickname, or presence. This includes on entry, exit, nick change, availability change, or any role change (granting or revoking voice, moderator privilege).
onAfterChangeUser	A user has changed. The only valid response is PASS with nothing in it.
onBeforeChangeAffiliation	A user affiliation is about to change.
onAfterChangeAffiliation	A user affiliation has changed. The only valid response is PASS with nothing in it.
onBeforeRemoveAffiliation	A user affiliation is about to be removed.
onAfterRemoveAffiliation	A user affiliation has been removed. The only valid response is PASS with no modification to the original stanza.
onBeforeJoin	A user is about to join a room.
onAfterJoin	A user has joined a room. The only valid response is PASS with nothing in it.
onLeave	A user has left a room. The only valid response is PASS.
onBeforeSubject	A room subject is about to change.
onAfterSubject	A room subject has changed. The only valid response is PASS with nothing in it.
onBeforeInvite	A user is about to be invited to a room.
onAfterInvite	A user has been invited to a room. The only valid response is PASS with nothing in it.
onHistory	A room's history has been requested. The only valid response is PASS.
onBeforeSend	A message is about to be sent in a room.
onBeforeBroadcast	A message is about to be broadcast in a room.

Jabber Compliance

Configuration of 3rd Party Compliance

REFERENCE

- Add 3rd Party Compliance Server



Compliance Server Settings

Name*

Description

Hostname/IP Address*

Port*

Password*

Confirm*

Messaging → External Server Setup → Third-Party Compliance Servers

cisco Live!

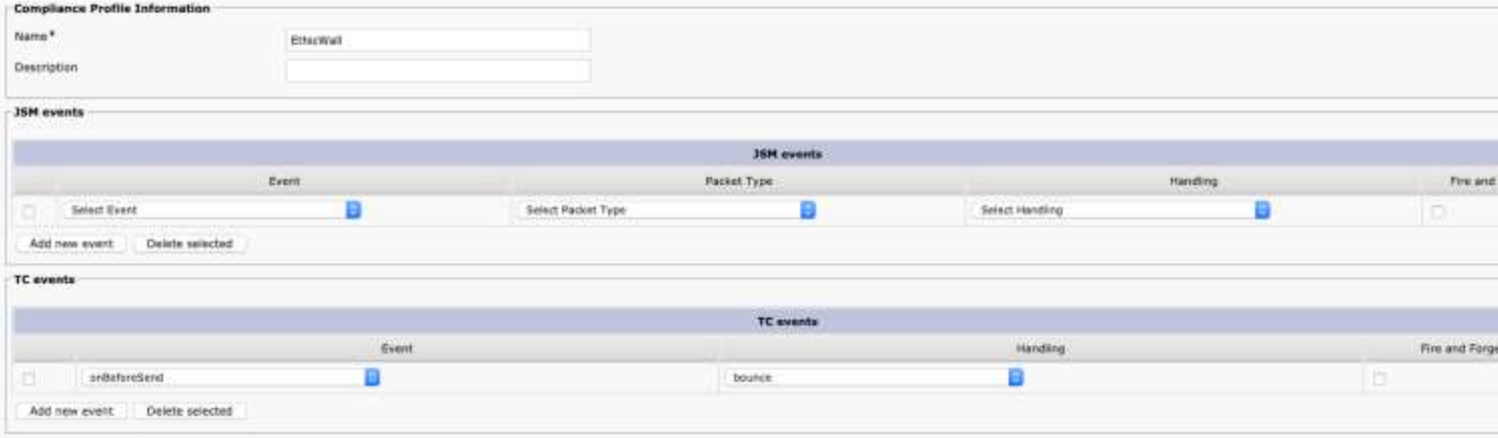
Jabber Compliance

Configuration of 3rd Party Compliance

REFERENCE

- Add 3rd Party Compliance Server
- Configure Compliance Profiles

Messaging → Compliance → Compliance Profiles



Compliance Profile Information

Name*	EthicWall
Description	

JSM events

	Event	Packet Type	Handling	Fire and
□	Select Event	Select Packet Type	Select Handling	□

Add new event | Delete selected

TC events

	Event	Handling	Fire and Forge
□	onBeforeSend	bounce	□

Add new event | Delete selected

Reference List of available configurable events:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/im_compliance/12_5_1/cup0_b_im-compliance-guide-1251/cup0_b_im-compliance-guide-1251_chapter_010.html#CUP0_TP_C28F57D7_00

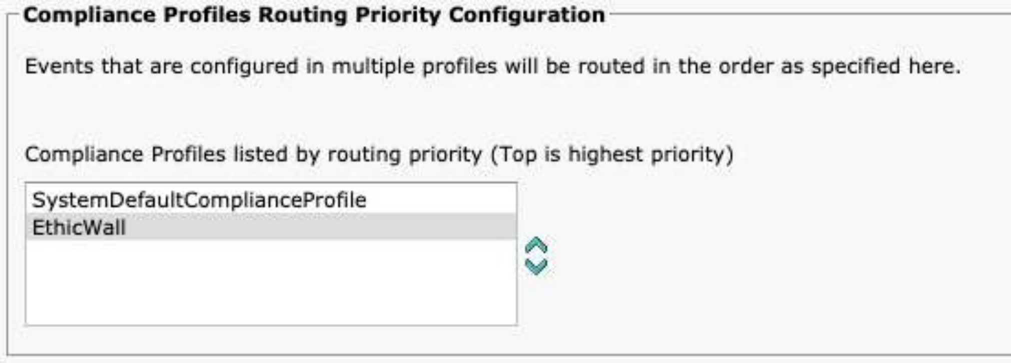
Jabber Compliance

Configuration of 3rd Party Compliance

REFERENCE

- Add 3rd Party Compliance Server
- Configure Compliance Profiles
- Configure Profile Priority

Messaging → Compliance → Compliance Profiles Routing Priority



Compliance Profiles Routing Priority Configuration

Events that are configured in multiple profiles will be routed in the order as specified here.

Compliance Profiles listed by routing priority (Top is highest priority)

SystemDefaultComplianceProfile
EthicWall

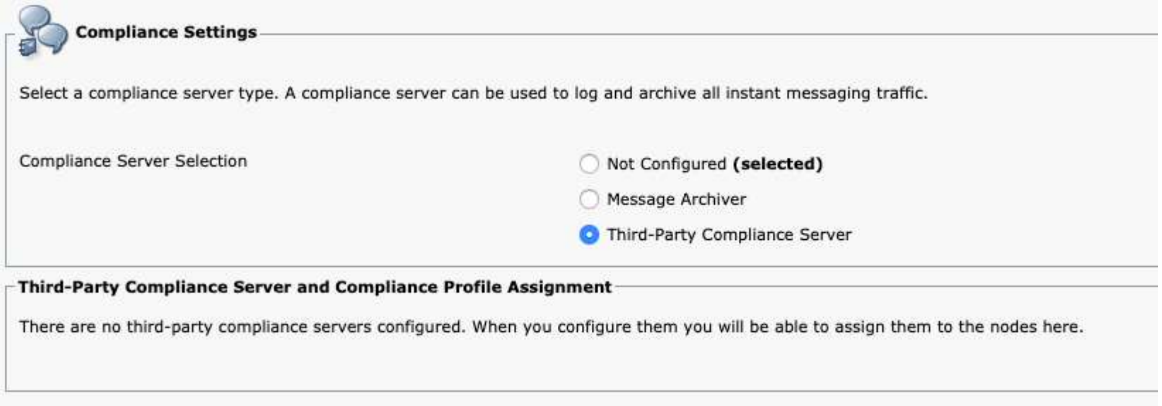
Jabber Compliance

Configuration of 3rd Party Compliance

REFERENCE

- Add 3rd Party Compliance Server
- Configure Compliance Profiles
- Configure Profile Priority
- Assign Compliance Server (restart Cisco XCP Router & enable Alarmsetting)

Messaging → Compliance → Compliance Settings



Compliance Settings

Select a compliance server type. A compliance server can be used to log and archive all instant messaging traffic.

Compliance Server Selection

○ Not Configured **(selected)**

○ Message Archiver

● Third-Party Compliance Server

Third-Party Compliance Server and Compliance Profile Assignment

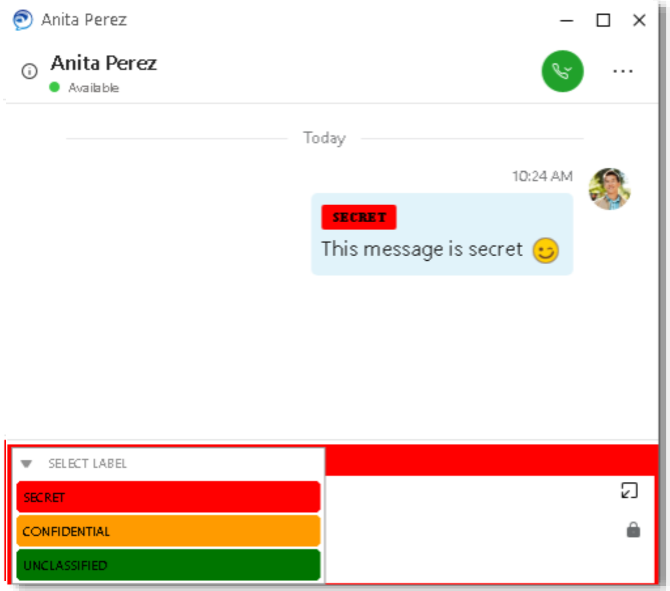
There are no third-party compliance servers configured. When you configure them you will be able to assign them to the nodes here.

cisco Live!

Jabber Compliance

XMPP Security Labels

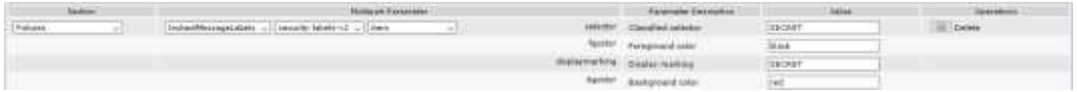
- Admin defines a catalogue of Labels (→17)
- User must apply Label before typing
- Jabber for Windows & Jabber Softphone for VDI only
- XEP-0258 label headers
- Control of labeled chats need to be done by compliance server



This message is secret 😉

Jabber-config.xml

```
<InstantMessageLabels>
  <item selector="Classified|SECRET">
    <securitylabel xmlns='urn:xmpp: sec-label:0'>
     <displaymarking fgcolor='black' bgcolor='red'>SECRET </displaymarking>
      <label>
       <edhAttrs xmlns="https://www.surevine.com/protocol/xmpp/edh">
       <specification>2.0.2</specification>
       <version>XXXX:1.0.0</version>
       <policyRef></policyRef>
       <originator>Acme</originator>
       <custodian>Acme</custodian>
       <classification>A</classification>
       <nationalities>Acme</nationalities>
       <organisations>Acme</organisations>
       </edhAttrs>
      </label>
    </securitylabel>
  </item>
<item...> ... </item>
</InstantMessageLabels>
```



Section	Multipart Parameter				Parameter Description	Value	Operations
Policies	InstantMessageLabels	security-labels-v2	item	selector	Classified selector	SECRET	Delete
				fgcolor	Foreground color	black	
				displaymarking	Display marking	SECRET	
				bgcolor	Background color	red	

Jabber Compliance

Jabber chat history

IM History

- Specifies if Jabber retains chat history after closing window (until Jabber reset)
- Displays the last 200 messages
- Jabber 11.8 + / onPrem only

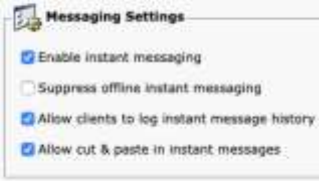
Jabber-config.xml

- Disable_IM_History
  - True → Client does not retain the chat history after participants close the chat window.
  - false (default) → Client retains the chat history.
- For persistent chat users, key must be false (defaultvalue) – It will affects the @mention feature in persistent chat rooms

```
<Disable_IM_History>true</Disable_IM_History
>
```

Serverside

- CUCM IM & P
  - Allow clients to log message history
- For persistent chat users, key must be false (defaultvalue) – It will affects the @mention feature in persistent chat rooms



Messaging Settings

☑ Enable instant messaging

□ Suppress offline instant messaging

☑ Allow clients to log instant message history

☑ Allow cut & paste in instant messages

Jabber Compliance

Saving of Jabber chat history

REFERENCE

RestoreChatOnLogin

- Cisco Jabber for desktops
- Specifies if *Remember my open conversations* checkbox is checked when users sign in for the first time.
  - True → *Remember my open conversations* checkbox is checked
  - false (default) → Rem*ember my open conversations* checkbox is not checked
- If chat history is not enabled, then the restoredchat windowsare empty.
- Example:<RestoreChatOnLogin>false</RestoreChatOnLogin>

Jabber Configuration Reference Guide:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_7/cjab_b_parameter-reference-guide-jabber-127.pdf

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Jabber Compliance

Saving of Jabber chat history

Enable Autosave

REFERENCE

- Cisco Jabber for desktops
- Users must have a CUCM account
- Users must be enabled for local archiving
- Specifies whether users can save IMs to an HTML file automatically, each time they close a conversation (The file persists even the user signs out or resets Jabber).
- Enable the option in the client:
  - Windows–File>Options>Chats>Autosavechat sessionto
  - Mac–Jabber>Preferences>Chats>Save chat archives to:▪
    - True → Thecheckbox is available.▪
    - false (default) → Thecheckbox is unavailable
- Example:<EnableAutosave>true</EnableAutosave>

Jabber Configuration Reference Guide:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_7/cjab_b_parameter-reference-guide-jabber-127.pdf

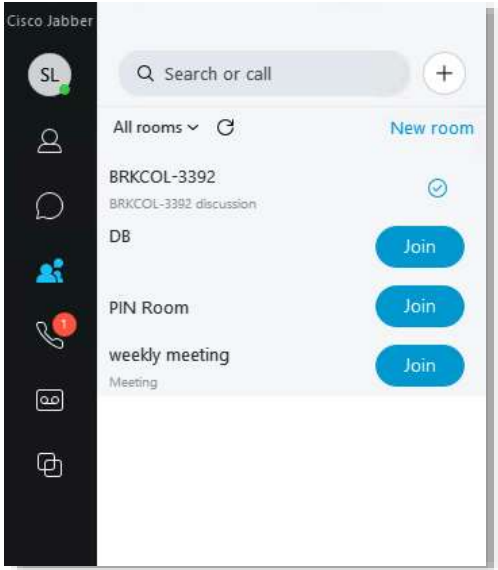
Jabber Compliance

Persistent Chat

XMPP persistent text chat function by the Cisco Unified IM & Presence server

- External Database required
- CUCM IM/P 10.x
- CUCM IM/P 11.5 for HA of persistent Chat

```
Jabber-config.xml
        <Persistent_Chat_Enabled>
        <Persistent_Chat_Mobile_Enabled>
```



Details on Persistent Chat @BRKCOL3392 CLEUR 2019
https://www.ciscolive.com/global/on-demand-library.html?search=BRKCOL-3392#/session/1530899267184001gP3c

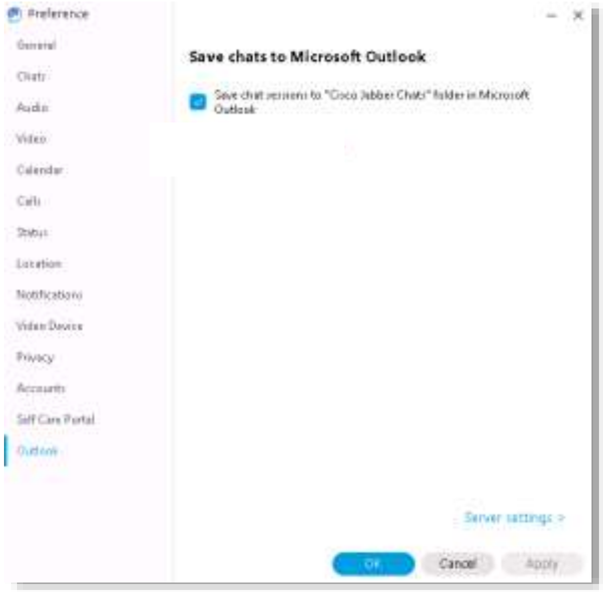
Jabber Compliance

Save Jabber chat history

Save Chat to Outlook

Saving Jabber chat history automatically to Jabber Chat`s folder in Microsoft Outlook

- Jabber Desktop only
- Exchange onPrem & O365



Save chats to Microsoft Outlook

☑ Save chat sessions to "Cisco Jabber Chats" folder in Microsoft Outlook

```
Jabber-config.xml
<EnableSaveChatHistoryToExchange>true</EnableSaveChatHistoryToExchange>
```

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

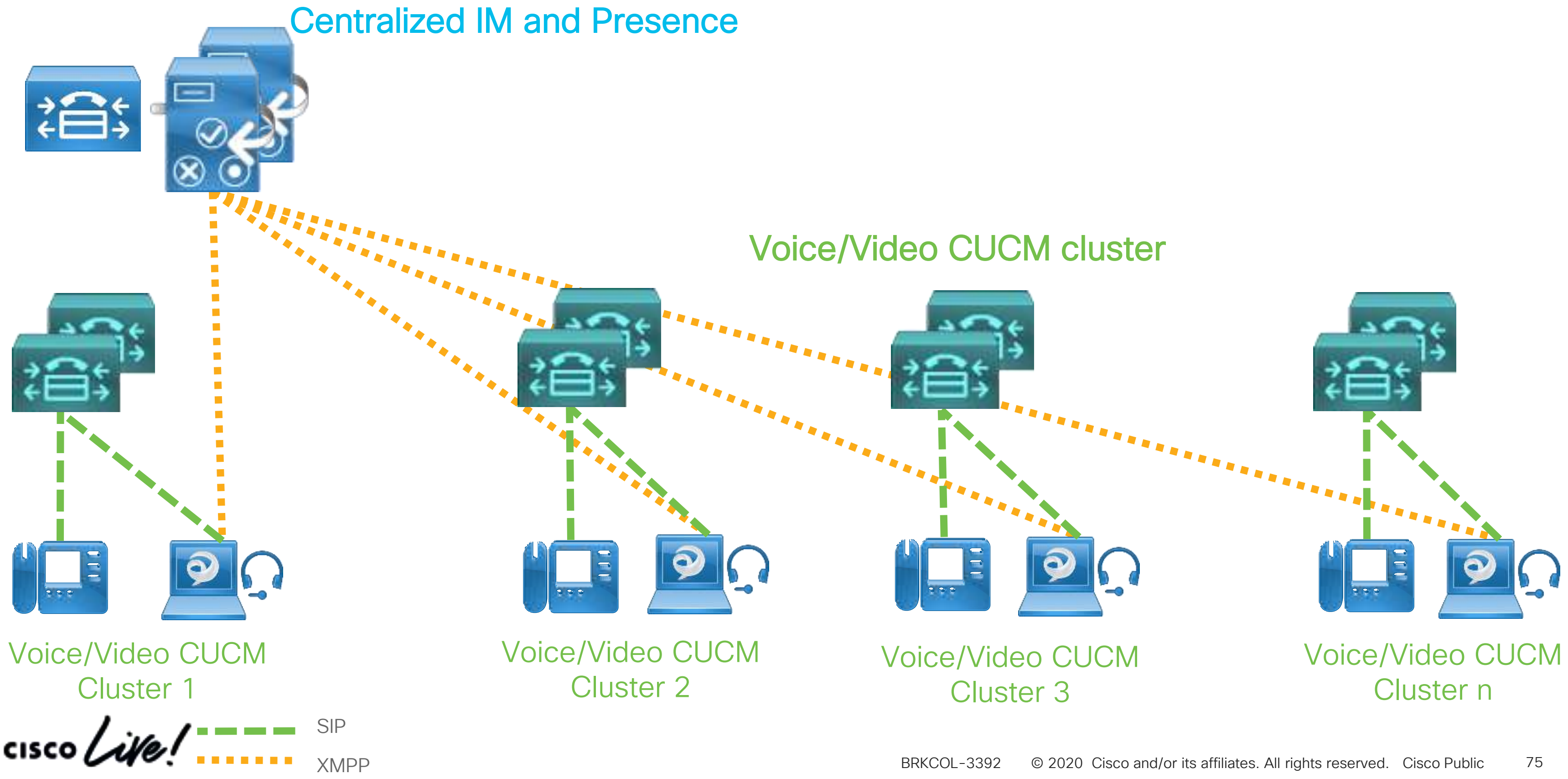
TOP

#1 Centralized IM/P Deployment

CHARTS

Components

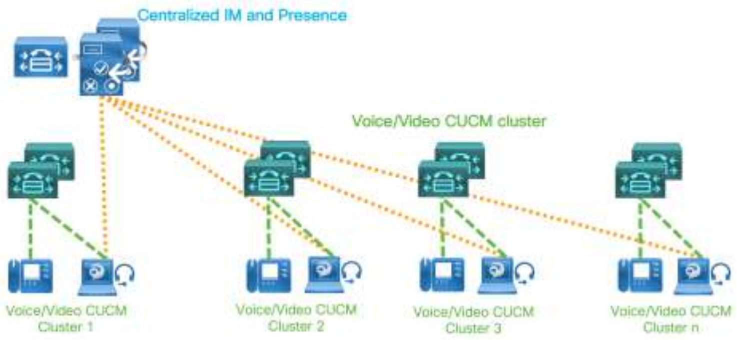
Centralized IM/P Deployment


Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized IM/P Deployment

Why?


Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n

Designed for High cluster count

- No 1x1 ratio of telephony clusters to IM & P clusters – scalability
- Full mesh topology is not required for the IM and Presence Service
- Version independent from telephony cluster
- Manage IM and Presence upgrades and settings from the central cluster
- No additional licensing

*Feature limitation:

No telephony presence if Jabber is offline. As of no SIP trunk between centralized IM & P and Voice/Video CUCM

Service Aggregation

- Central Federation
- Central external databases

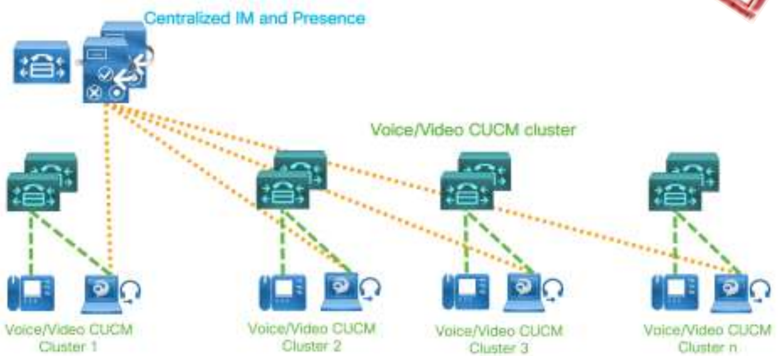
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized IM/P Deployment

Requirements

REFERENCE

- Centralized CUCM & CUCM IM/P 11.5(1)SU4
- Voice/Video CUCM 10.5(2)
- Cisco Jabber 11.9



Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n

APNS support for IM Push (based on central IM/P)*
APNS support for voice* – Voice/Video CUCM 11.5(1)SU4

OAuth Refresh Logins support* - Voice/Video CUCM 11.5(1)SU4

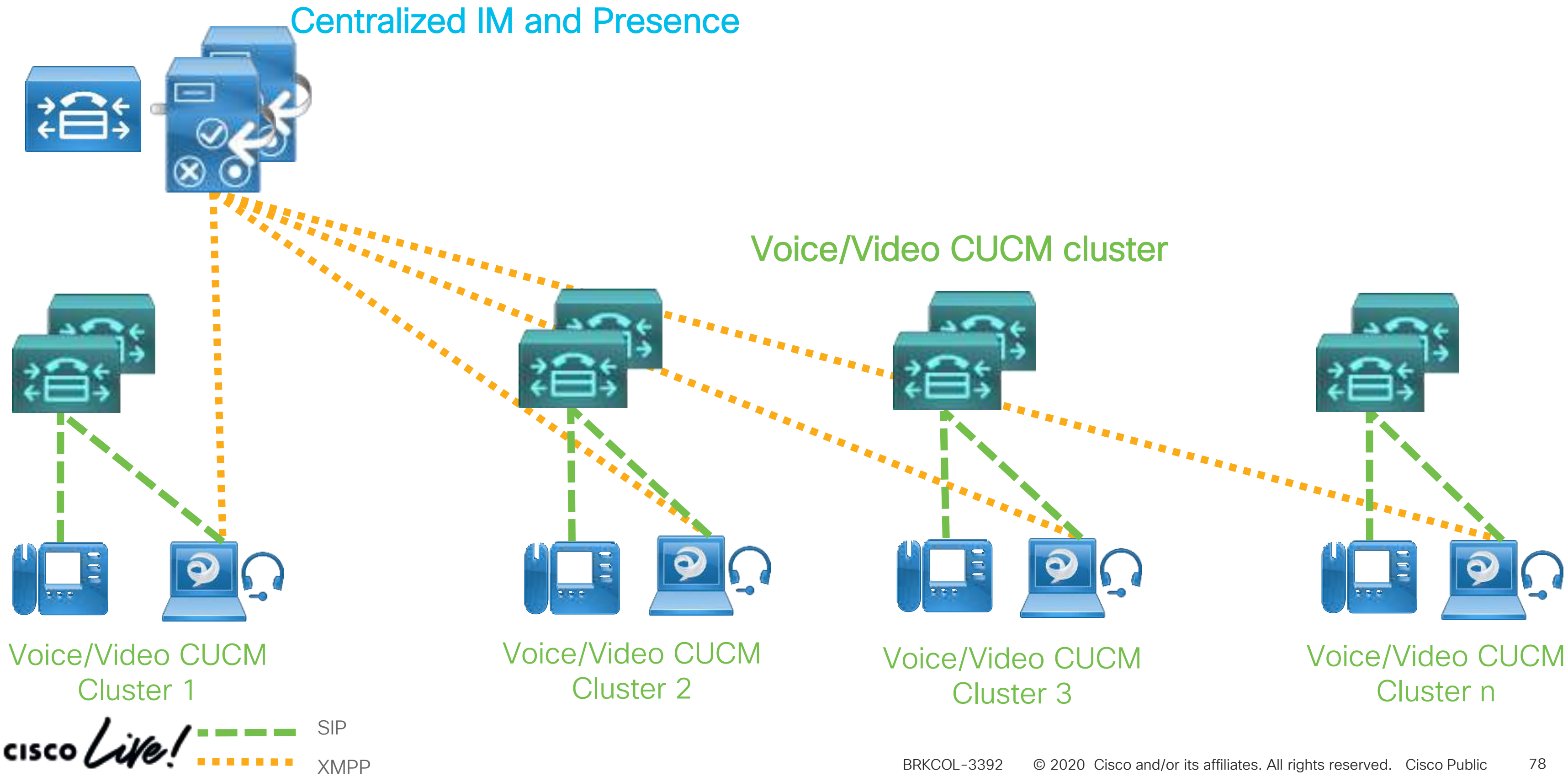
SAML SSO* - Voice/Video CUCM 11.5(1)SU4

*optional

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

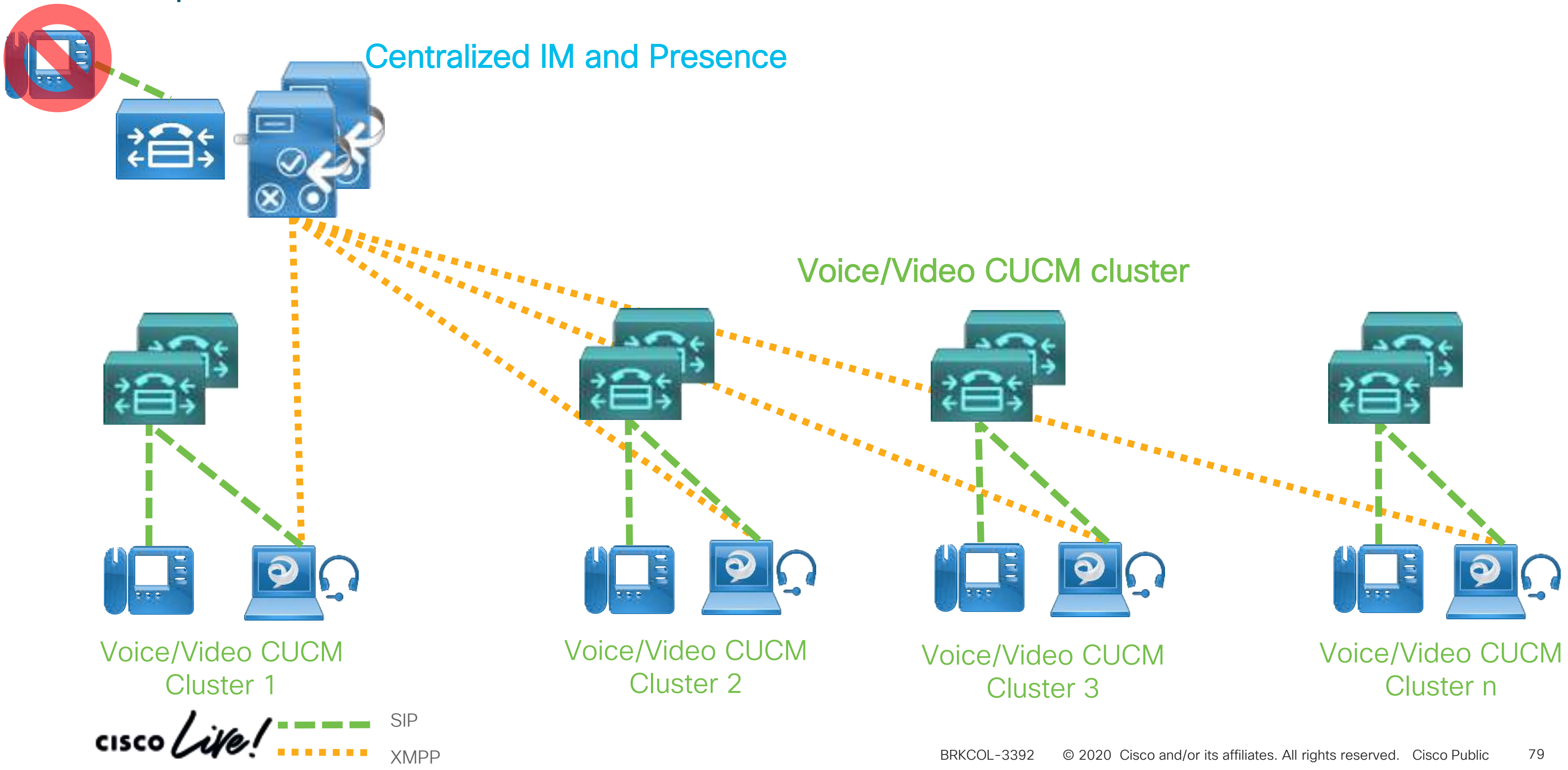
Centralized IM/P Deployment

Components


Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

Centralized IM/P Deployment

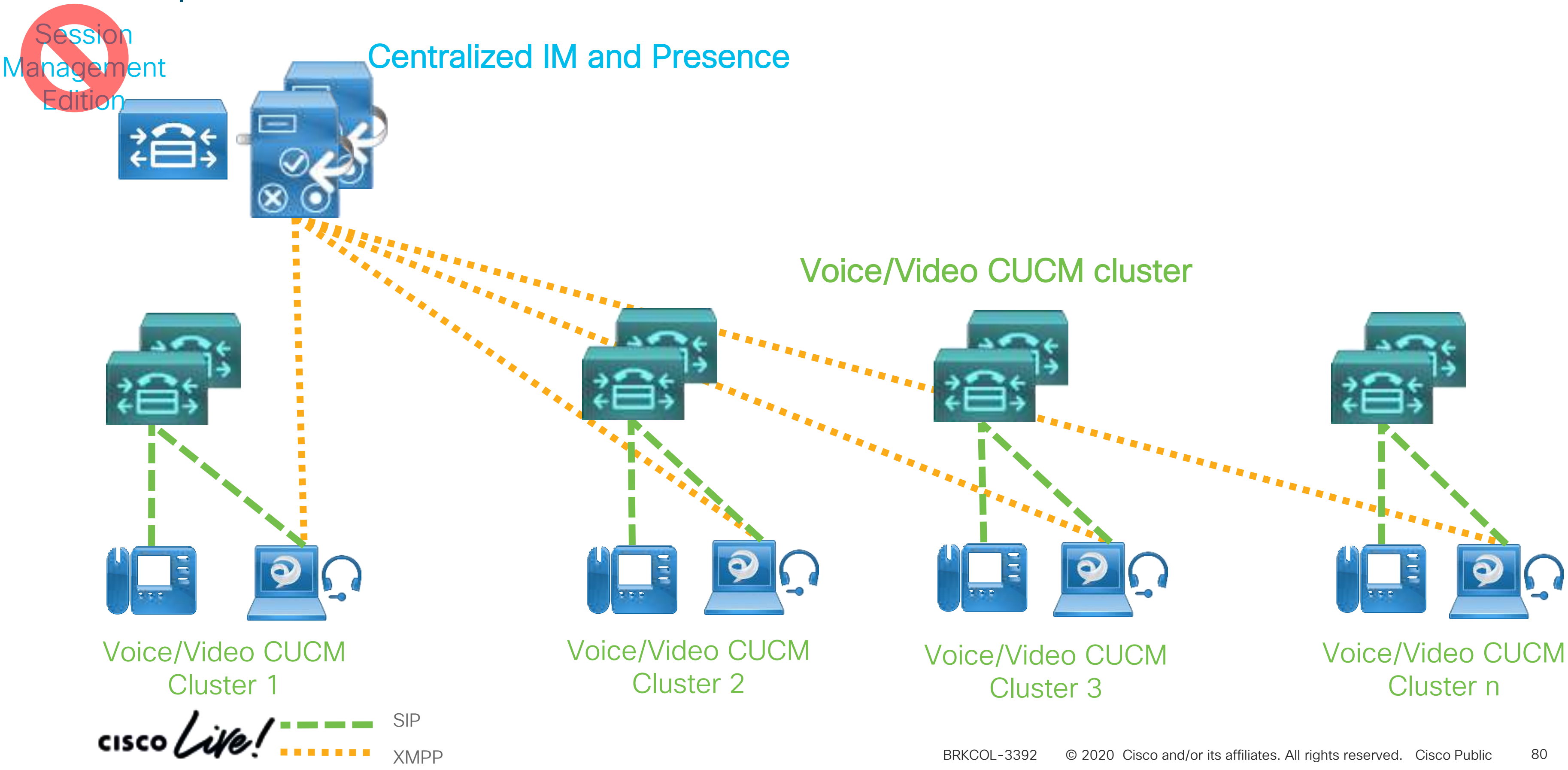
Components


Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized IM/P Deployment

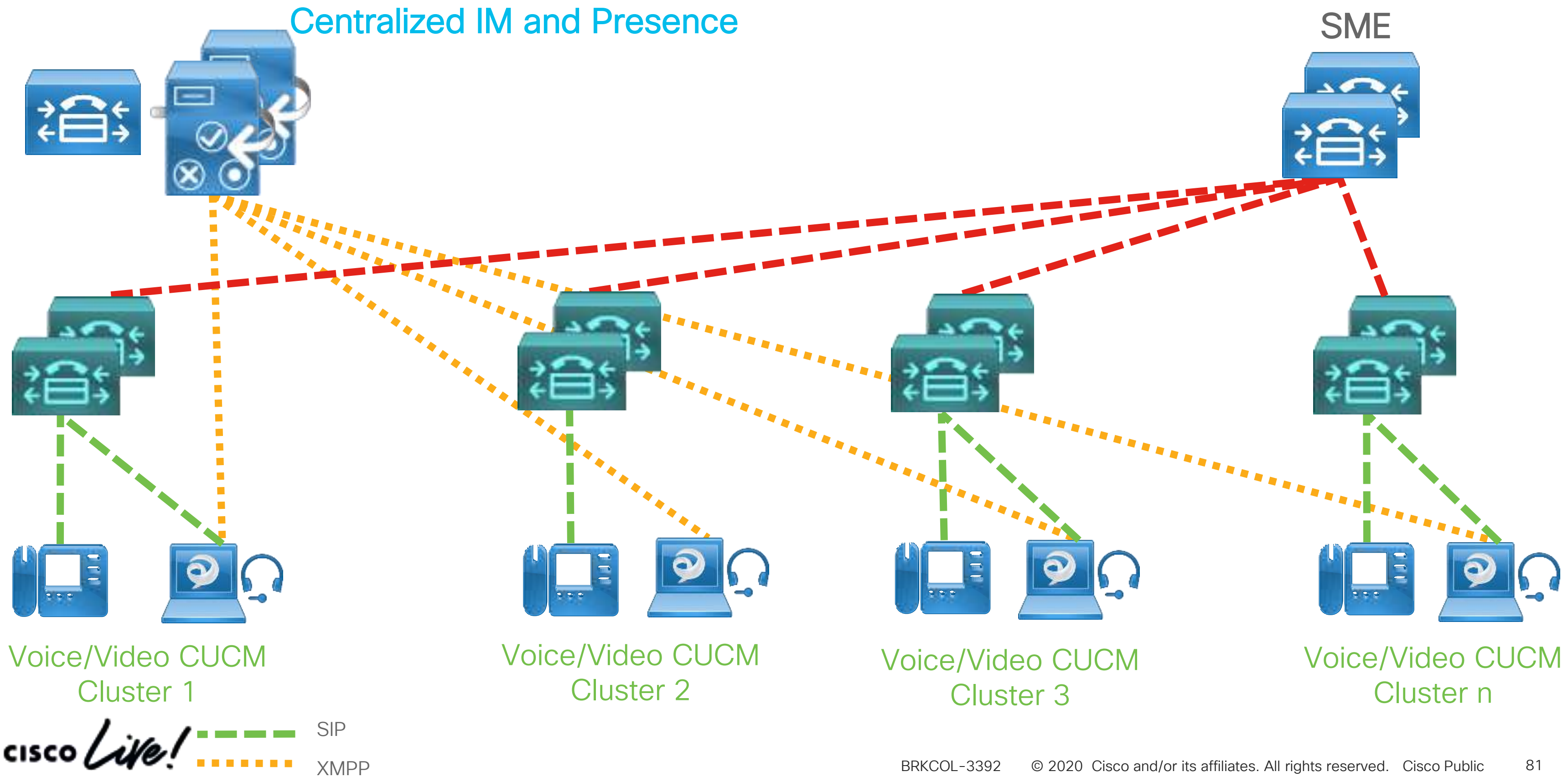
Components


Session Management Edition
Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized IM/P Deployment

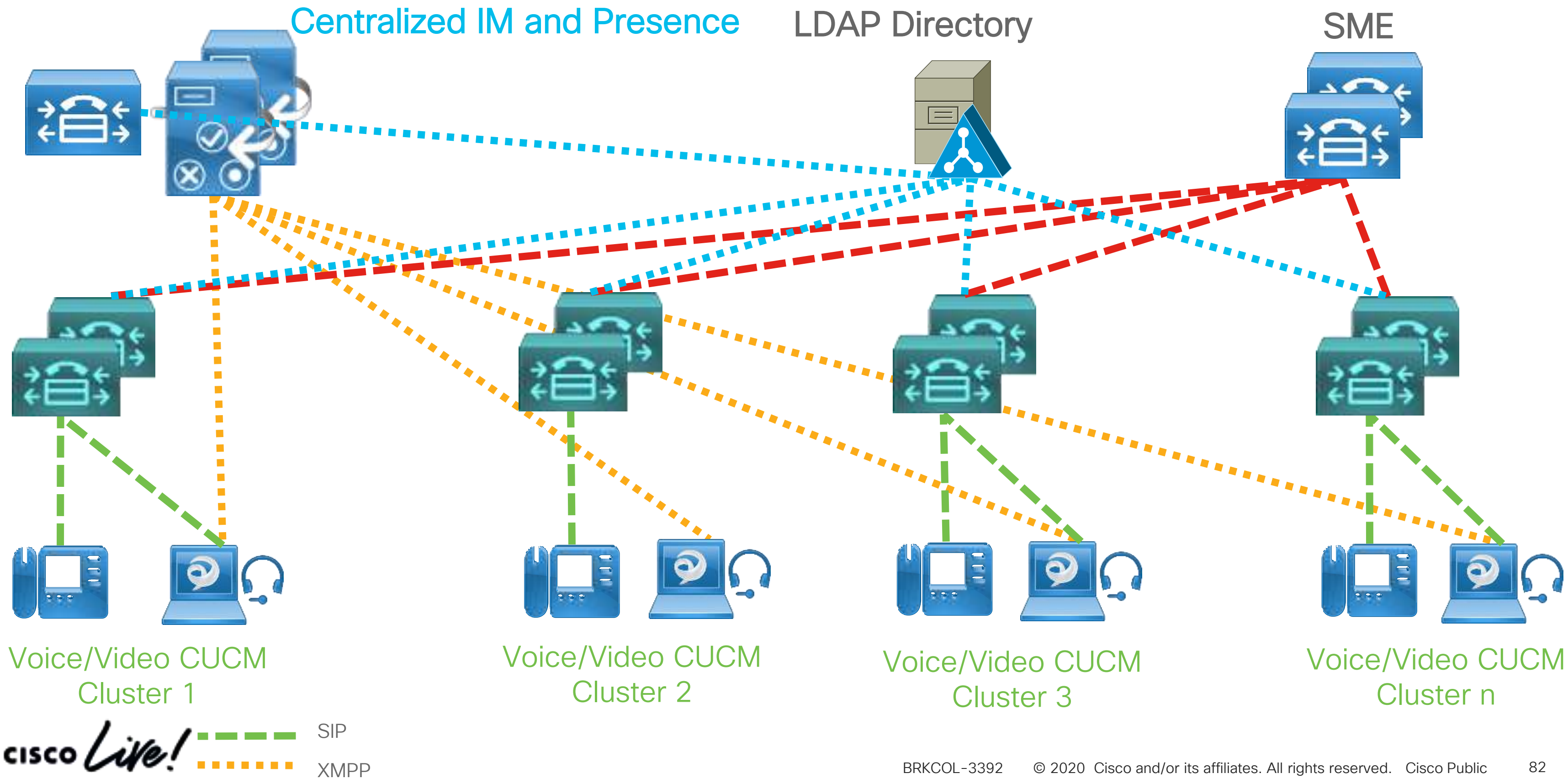
Components


Centralized IM and Presence
SME
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized IM/P Deployment

Components


Centralized IM and Presence
LDAP Directory
SME
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

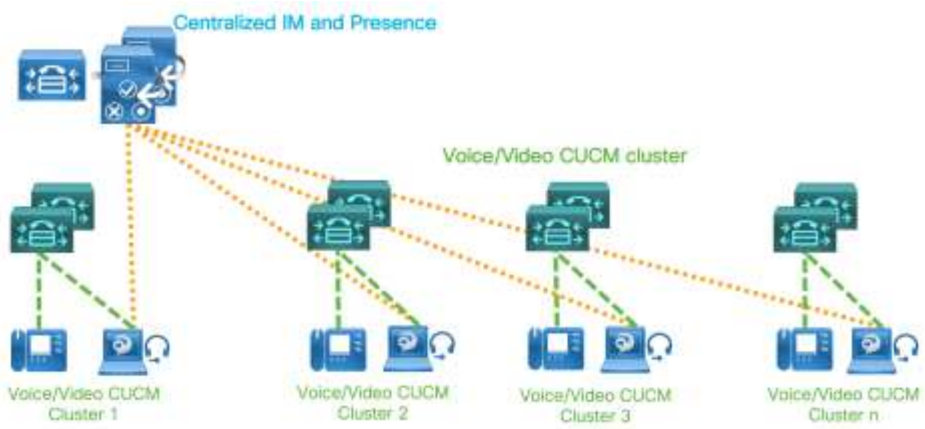
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design considerations for high cluster count

Centralized IM/P Deployment

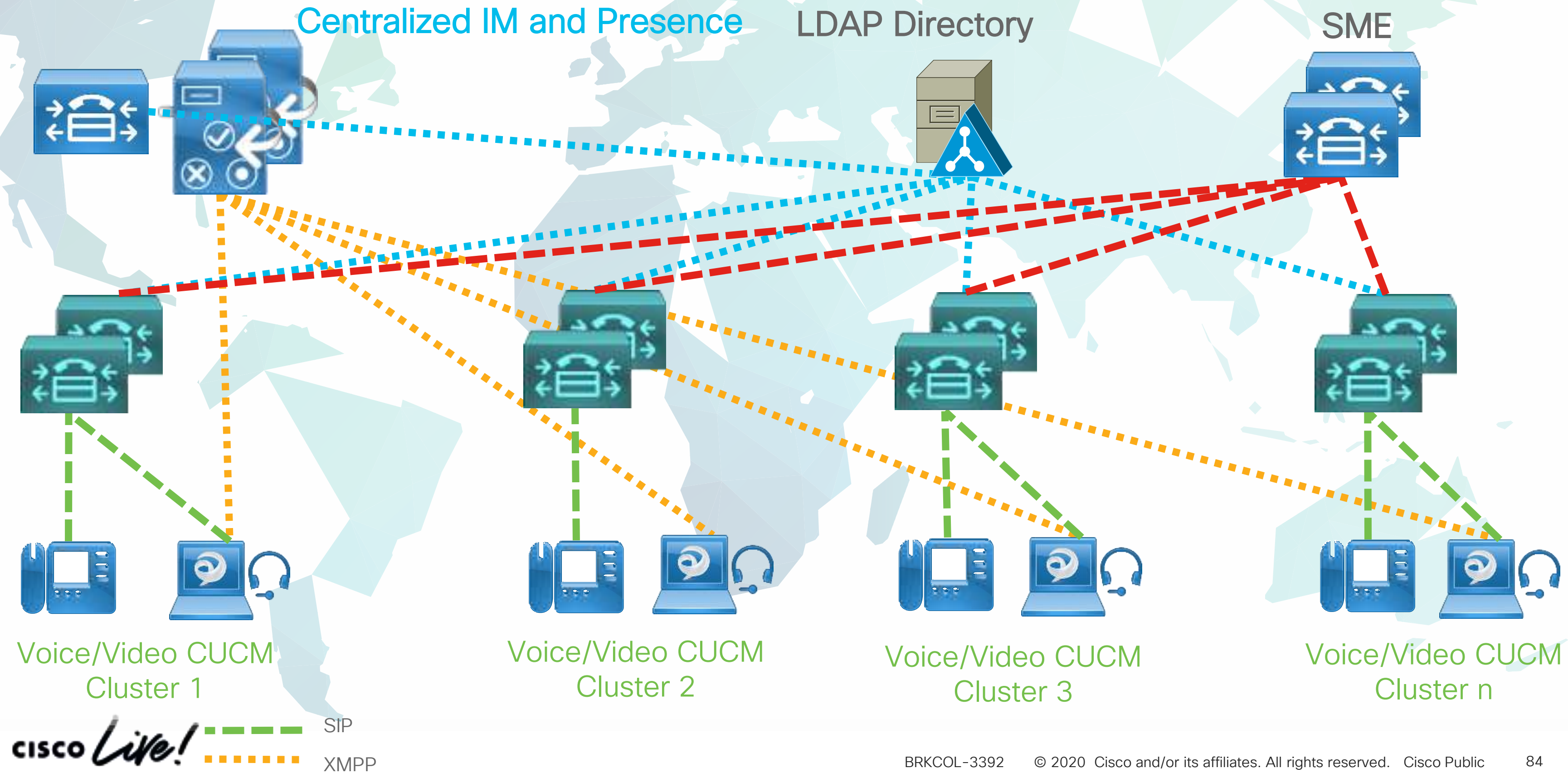
Centralized IM&P

- No database synchronization between centralized IM/P and Voice/Video CUCM
- No significant bandwidth requirements between centralized IM/P and Voice/Video CUCM. Only initial key sync when configured.
- 75.000 clients per cluster – 6 nodes (@ 25k ova)
- Interclustering is supported for centralized IM/P


Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n

Centralized IM/P Deployment

Worldwide Deployment


Centralized IM and Presence
LDAP Directory
SME
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

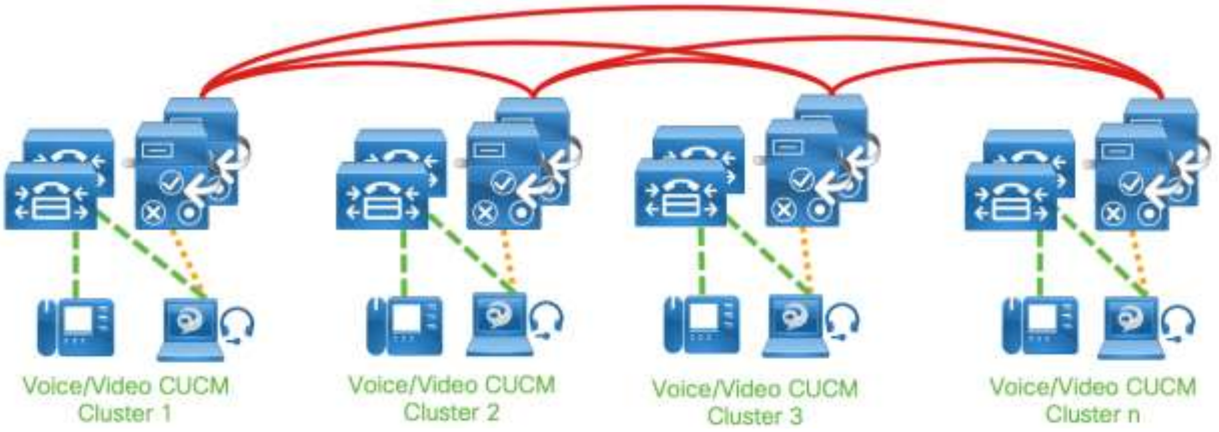
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design considerations for high cluster count

Centralized IM/P Deployment

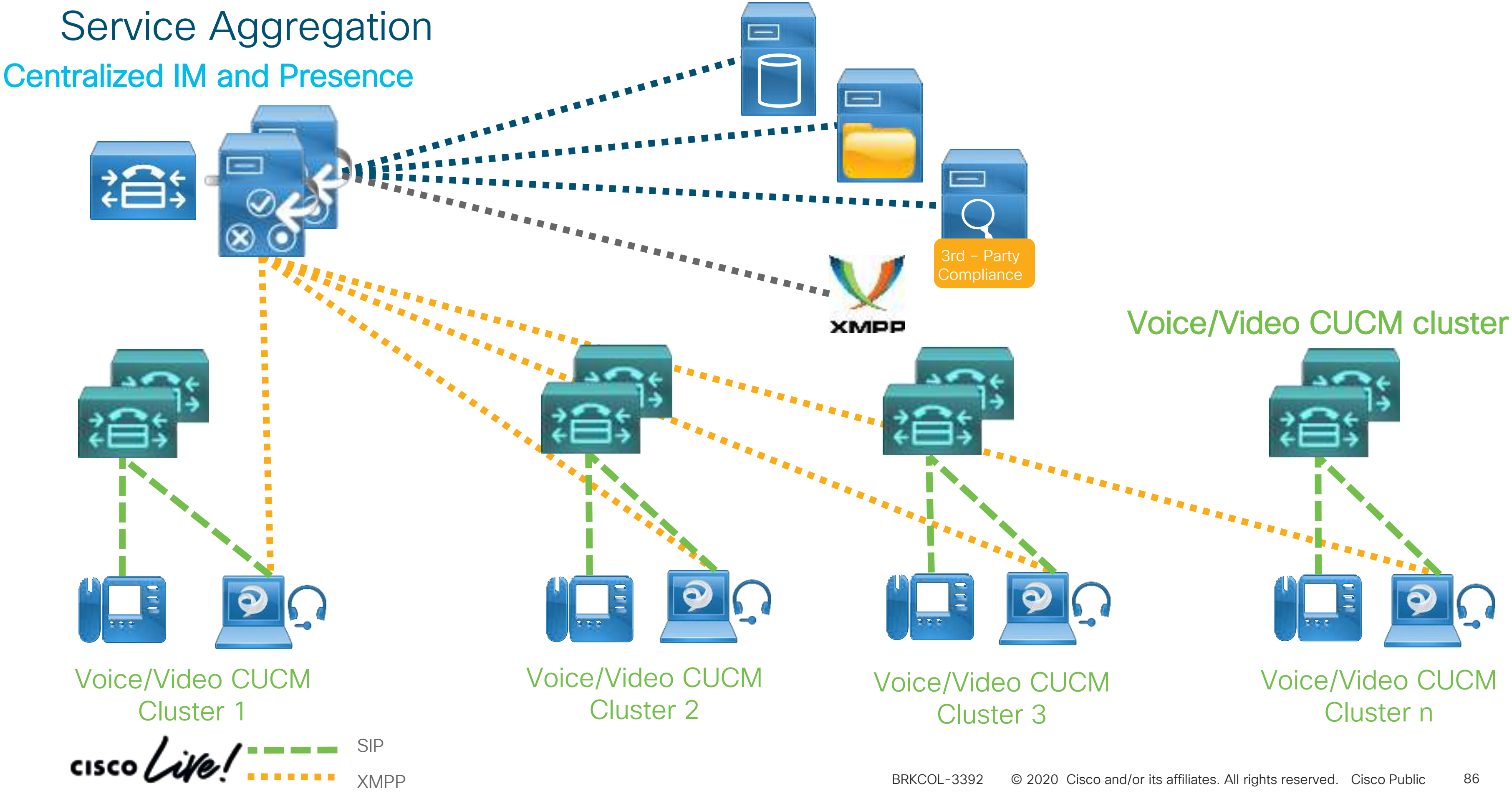
Alternative – Inter Clustering

- 5Mbps / 80ms rtt
- Each additional cluster requires additional 5Mbps / 80ms rtt
- Full mesh topology – server side
- Min 15k ova
- Not supported on BE6k


Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n

Centralized IM/P Deployment

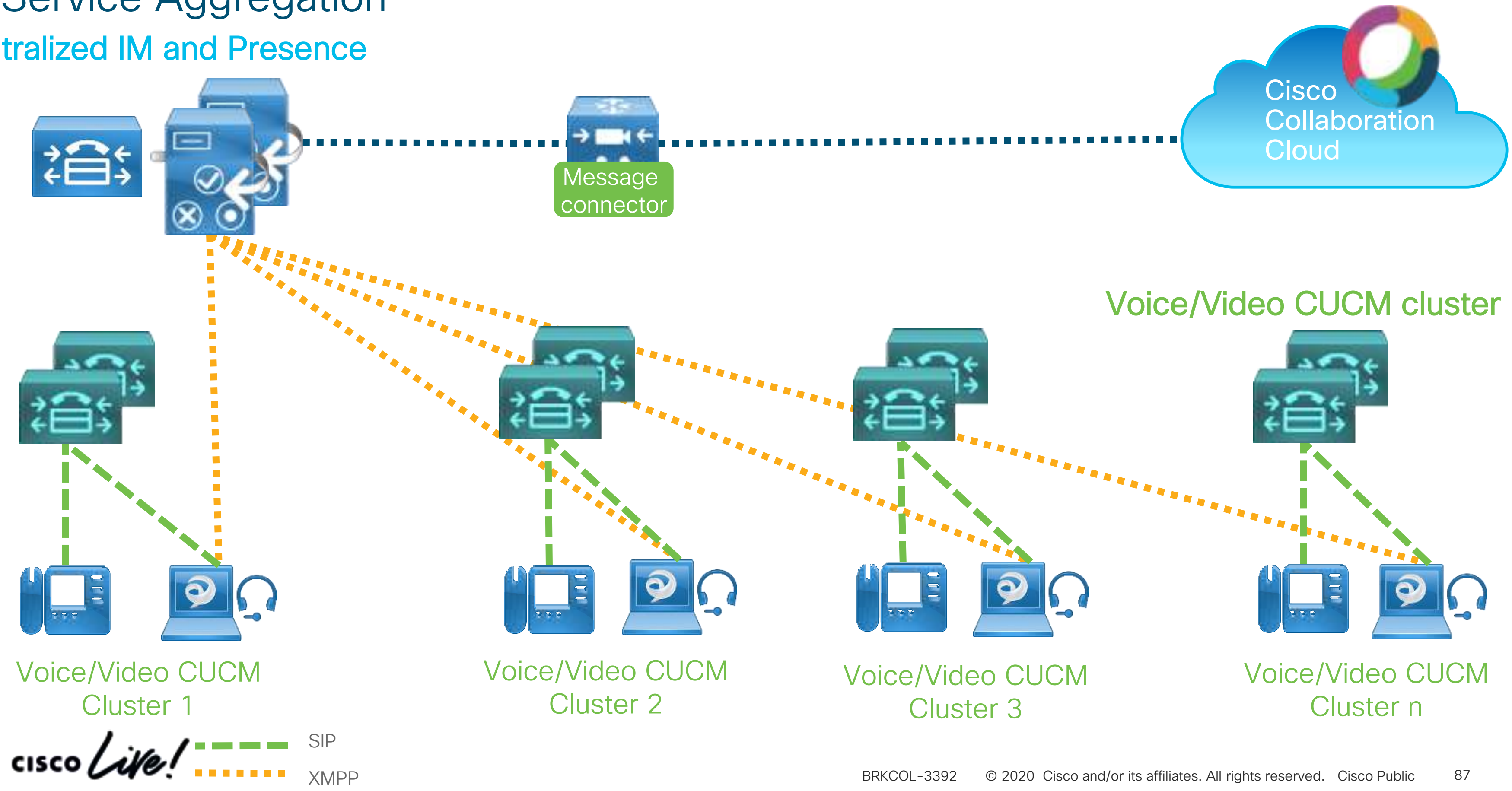
Service Aggregation



Centralized IM and Presence
3rd – Party Compliance
XMPP
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

Centralized IM/P Deployment

Service Aggregation


Centralized IM and Presence
Message connector
Cisco Collaboration Cloud
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n
SIP
XMPP

Centralized IM/P Deployment

Design considerations for high cluster count

REFERENCE

Centralized IM/P

- No database transaction
- No significant bandwidth requirements between Centralized IM&P and Voice/Video. Only initial key sync when configured.
- 75.000 clients per cluster - 6 nodes (@ 25k ova)
- Intercluster support for centralized IM/P

Inter/Intra clustering

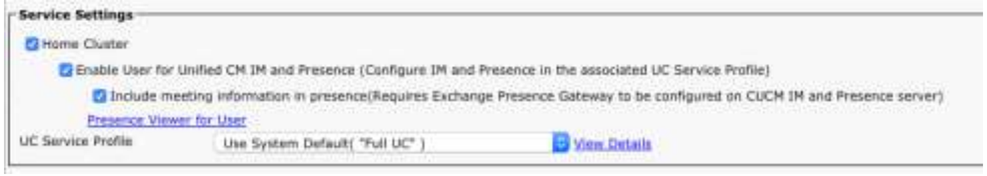
- 5Mbps / 80ms rtt
- Each additional cluster requires additional 5Mbps / 80ms rtt
- Full mesh topology - server side
- 5k ova
- No BE6k

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized IM/P Deployment

Configuration

- Centralized IM/P enable end users for IM and Presence
  - Individually, bulk and/or “Feature Group Template”



Service Settings

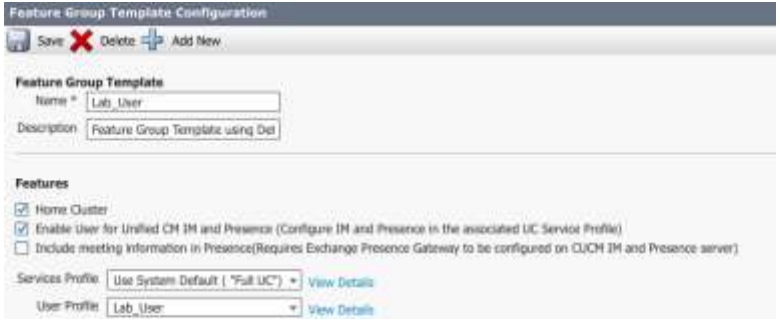
☑ Home Cluster

☑ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

☑ Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

Presence Viewer for User

UC Service Profile: Use System Default("Full UC") View Details



Feature Group Template Configuration

Feature Group Template

Name *: Lab_User

Description: Feature Group Template using Def

Features

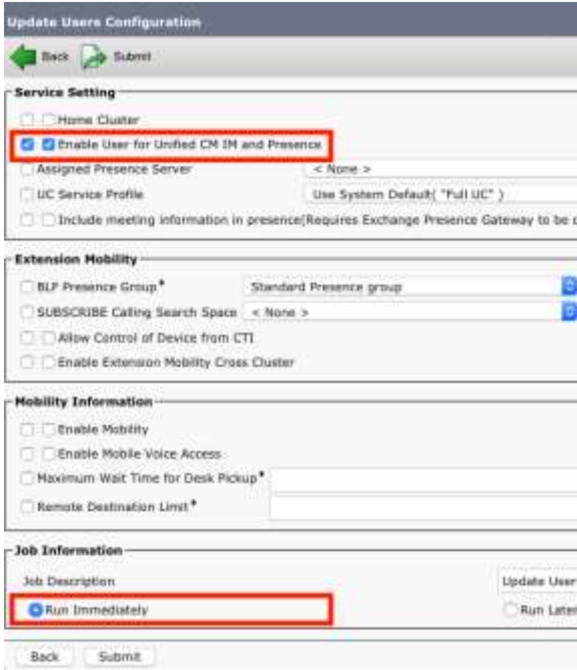
☑ Home Cluster

☑ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

☐ Include meeting information in Presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

Services Profile: Use System Default ("Full UC") View Details

User Profile: Lab_User View Details



Update Users Configuration

Service Setting

☐ ☐ Home Cluster

☑ ☑ Enable User for Unified CM IM and Presence

☐ Assigned Presence Server: < None >

☐ UC Service Profile: Use System Default("Full UC")

☐ ☐ Include meeting information in presence(Requires Exchange Presence Gateway to be c

Extension Mobility

☐ BLF Presence Group*: Standard Presence group

☐ SUBSCRIBE Calling Search Space: < None >

☐ ☐ Allow Control of Device from CTI

☐ ☐ Enable Extension Mobility Cross Cluster

Mobility Information

☐ ☐ Enable Mobility

☐ ☐ Enable Mobile Voice Access

☐ Maximum Wait Time for Desk Pickup*

☐ Remote Destination Limit*

Job Information

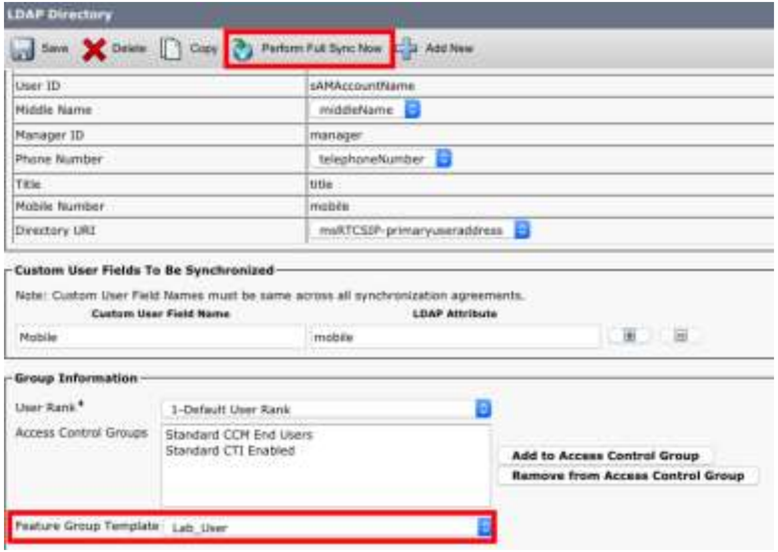
Job Description: Update User

● Run Immediately ○ Run Later

Centralized IM/P Deployment

Configuration

- Centralized IM/P – enable end users for IM and Presence
- Centralized IM/P – LDAP sync



User ID	sAMAccountName
Middle Name	middleName
Manager ID	manager
Phone Number	telephoneNumber
Title	title
Mobile Number	mobile
Directory URI	msRTCSIP-primaryuseraddress

Custom User Fields To Be Synchronized

Note: Custom User Field Names must be same across all synchronization agreements.

Custom User Field Name	LDAP Attribute
Mobile	mobile

Group Information

User Rank* 1-Default User Rank

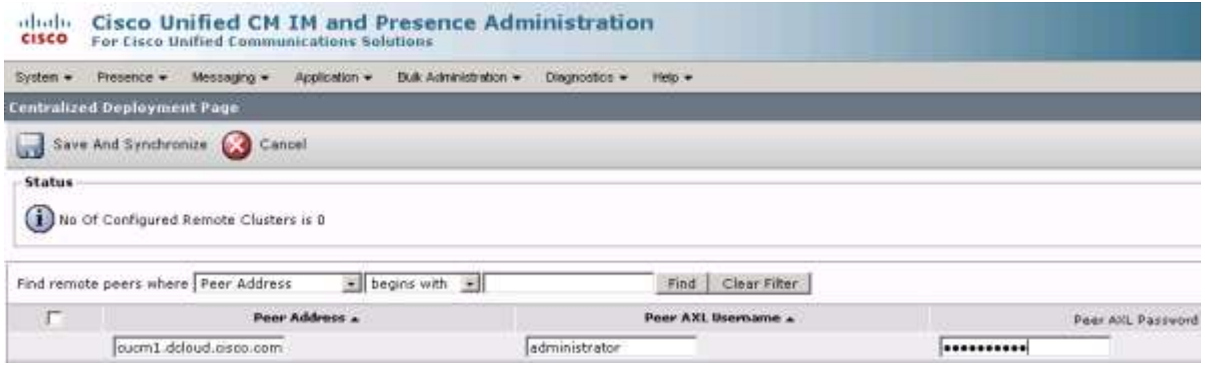
Access Control Groups
Standard CCM End Users
Standard CTI Enabled

Feature Group Template Lab_User

Centralized IM/P Deployment

Configuration

- Centralized IM/P – enable end users for IM and Presence
- Centralized IM/P – LDAP sync
- Centralized IM/P – add remote telephony clusters peers



Centralized Deployment Page

Status

No Of Configured Remote Clusters is 0

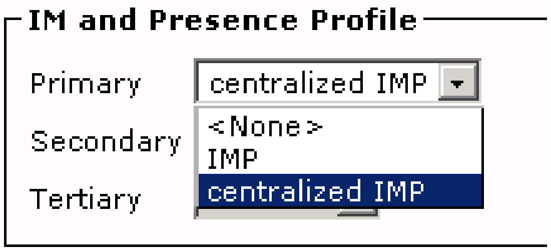
Find remote peers where Peer Address begins with

□	Peer Address ▲	Peer AXL Username ▲	Peer AXL Password
	cucm1.dcloud.cisco.com	administrator	●●●●●●●●●●●

Centralized IM/P Deployment

Configuration

- Centralized IM/P – enable end users for IM and Presence
- Centralized IM/P – LDAP sync
- Centralized IM/P – add remote telephony clusters peers
- Voice/Video clusters – new UC Service for IM and Presence that points to centralized IM/P, update Service Profile and Feature Group Template



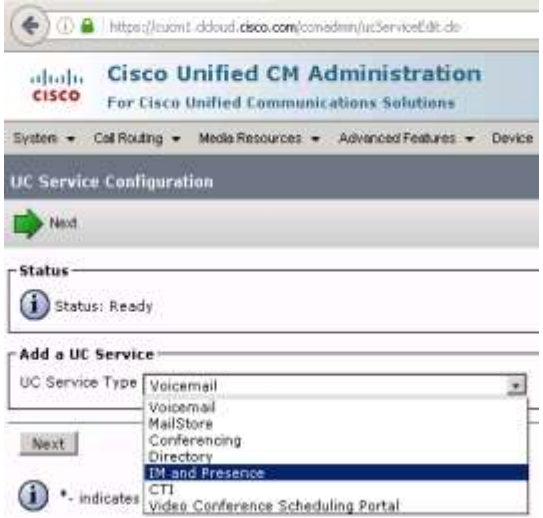
IM and Presence Profile

Primary: centralized IMP

Secondary

Tertiary

<None>
IMP
centralized IMP



https://cucm1.dcloud.cisco.com/ccmadmin/ucServiceEdit.do

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

UC Service Configuration

Status

Status: Ready

Add a UC Service

UC Service Type: Voicemail

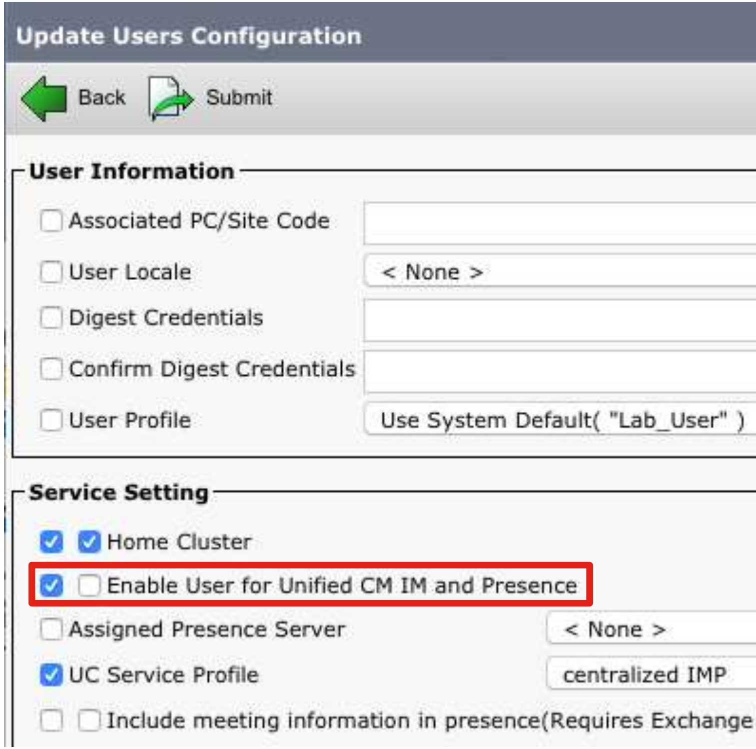
Voicemail
MailStore
Conferencing
Directory
IM and Presence
CTI
Video Conference Scheduling Portal

*- indicates

Centralized IM/P Deployment

Configuration

- Centralized IM/P – enable end users for IM and Presence
- Centralized IM/P – LDAP sync
- Centralized IM/P – add remote telephony clusters peers
- Voice/Video clusters – new UC Service for IM and Presence that points to centralized IM/P, update Service Profile and Feature Group Template
- Voice/Video clusters– disable end users for IM and Presence and update UC Service profile



Update Users Configuration

User Information

□ Associated PC/Site Code

□ User Locale: < None >

□ Digest Credentials

□ Confirm Digest Credentials

□ User Profile: Use System Default("Lab_User")

Service Setting

☑ ☑ Home Cluster

☑ □ Enable User for Unified CM IM and Presence

□ Assigned Presence Server: < None >

☑ UC Service Profile: centralized IMP

□ □ Include meeting information in presence(Requires Exchange

Centralized IM/P Deployment

Configuration

- Centralized IM/P - enable end users for IM and Presence
- Centralized IM/P – LDAP sync
- Centralized IM/P - add remote telephony clusters peers
- Voice/Video clusters – new UC Service for IM and Presence that points to centralized IM/P, update Service Profile and Feature Group Template
- Voice/Video clusters– disable end users for IM and Presence and update UC Service profile

- No Presence Gateway required
- No SIP Publish trunk required
- No Service Profile on the centralized IM/P → the Service Profile is configured on Voice/Video clusters

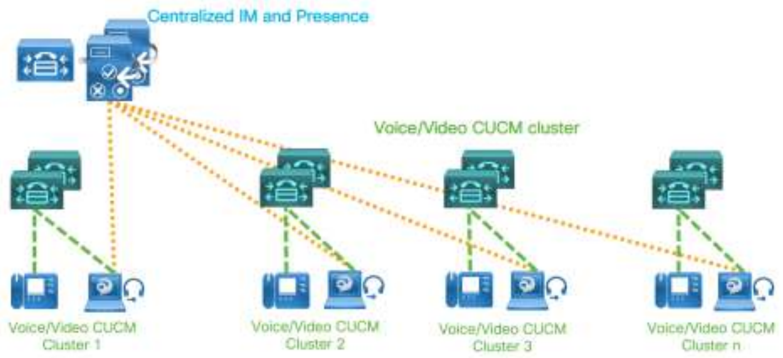
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Centralized IM/P Deployment

Considerations for Migration

Migration from “standard” design to Centralized IM/P Deployment

- Jabber Contact list is stored on locally IM/P
  → exported and reimported to centralized IM/P
- Jabber uses certificates from local IM/P
  → distribute centralized IM/P certificates
- Verify and migrate local and infrastructure services
  - Federation Services
  - Persistent Chat database
  - Managed File Transfer


Centralized IM and Presence
Voice/Video CUCM cluster
Voice/Video CUCM Cluster 1
Voice/Video CUCM Cluster 2
Voice/Video CUCM Cluster 3
Voice/Video CUCM Cluster n

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

© 2020 Cisco and/or its affiliates. All rights reserved.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

You make **possible**