Collaboration Asks:
Call IT?

Deploying Cisco Jabber on Mobile Devices

Seongho Hong, Technical Marketing Engineer

BRKCOL-2344

Cisco live!

Session Agenda

- Cisco Jabber & Architecture Overview

- Configuring User, Device & Services for Cisco Jabber

- Flexible JID & Multiple IM Address Domain

- File Transfer

- SAMLv2 Single Sign-On (SSO)

- Security Features

- Considerations for Wireless LAN

- Distributing Cisco Jabber for Mobile

- Closing Thoughts

Overview of Cisco Jabber for Mobile

Introducing Cisco Jabber for Mobile

- The client application turning mobile devices into business-class collaboration endpoints

- Instant access to UC workloads on-premises or in the cloud

- Works over public/home Wi-Fi, wireless LAN or mobile data network

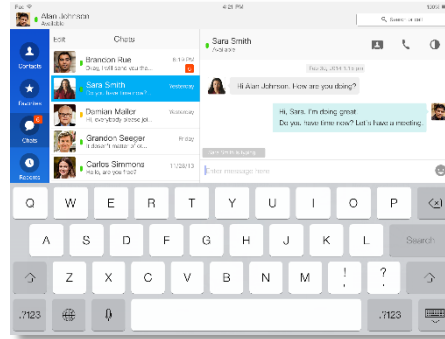- Supports smartphones & tablets running Apple iOS or Android
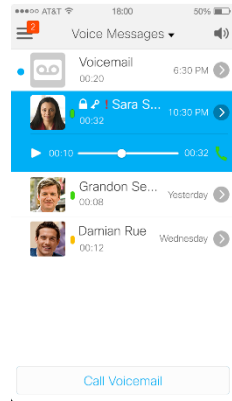
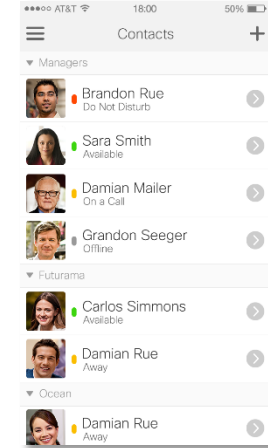# Core Features of Cisco Jabber for Mobile

Voice/Video

IM/Chat

Directory Search/ Contact Management

Web Conferencing & Desktop Sharing

Visual Voicemail
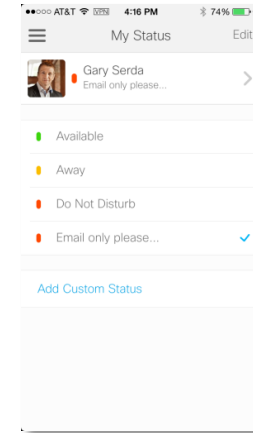
Presence

A Few Highlights in Jabber 10.6 for Mobile

- SAMLv2 SSO over Cisco Expressway

- Flexible Jabber ID (JID) & multiple IM address domain support

- File transfer with 3rd party cloud storage system integration

- BFCP-based desktop sharing

- Real-time audio/video statistics

- Answer without unlocking on Apple iOS

What's Coming in Jabber 11.0 for Mobile

Available SOON

- New meeting integration
  - Personal Room feature
  - Collaboration Meeting Rooms
  - Video conference bridge escalation

- Contact & chat management
  - AD Distribution Group support
  - Contact groups & group chat creation

- Voice & video features
  - Far End Camera Control (FECC)
  - DTMF digit management
  - G722 & Opus codec support

- Security enhancements
  - Encrypted TFTP access
  - Server certificate validation handling

- URI handler alignments

- App configuration via EMM

- More smartphones & tablets
  - Sonim XP7 ultra-rugged Android phone

Look for this sign throughout the remaining slides!

New in 11.0

Cisco Jabber Solution Architecture

Cisco Jabber On-Premises Deployment
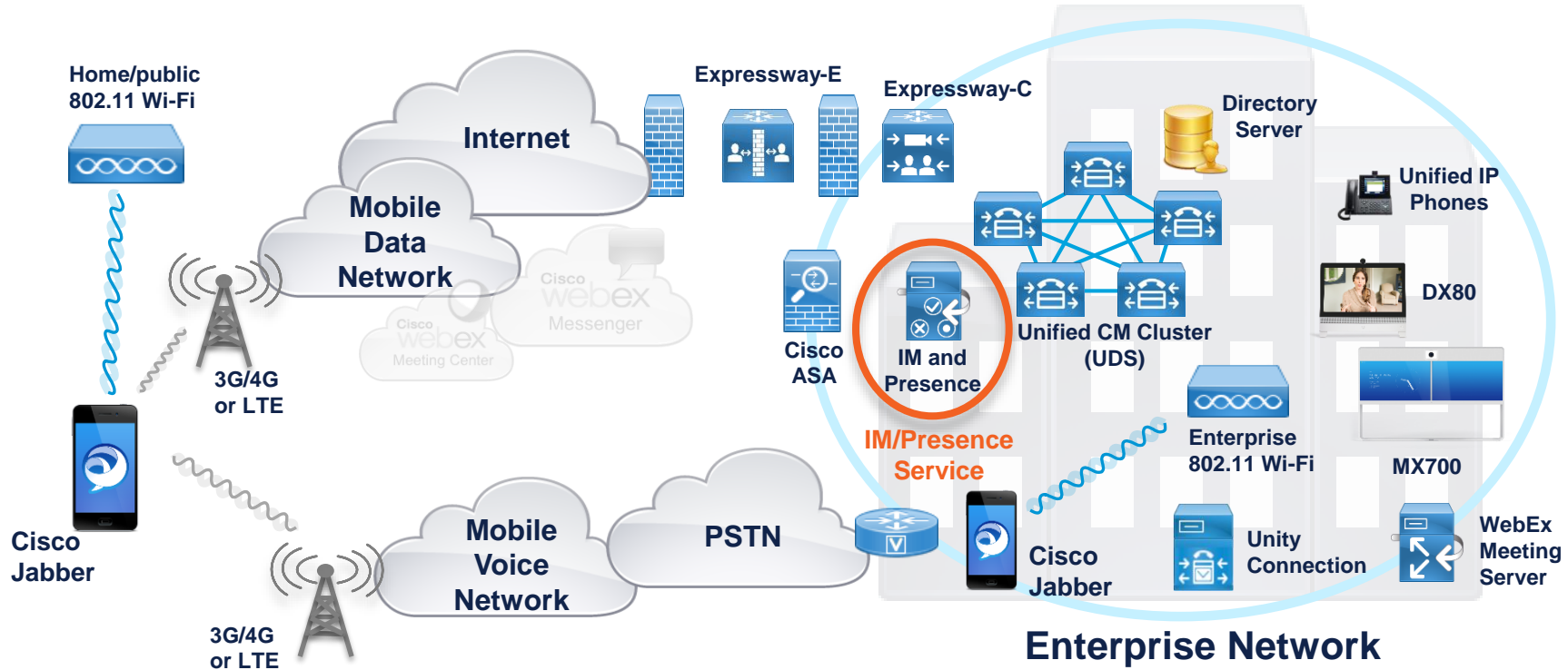
Cisco Jabber Cloud (or Hybrid) Deployment
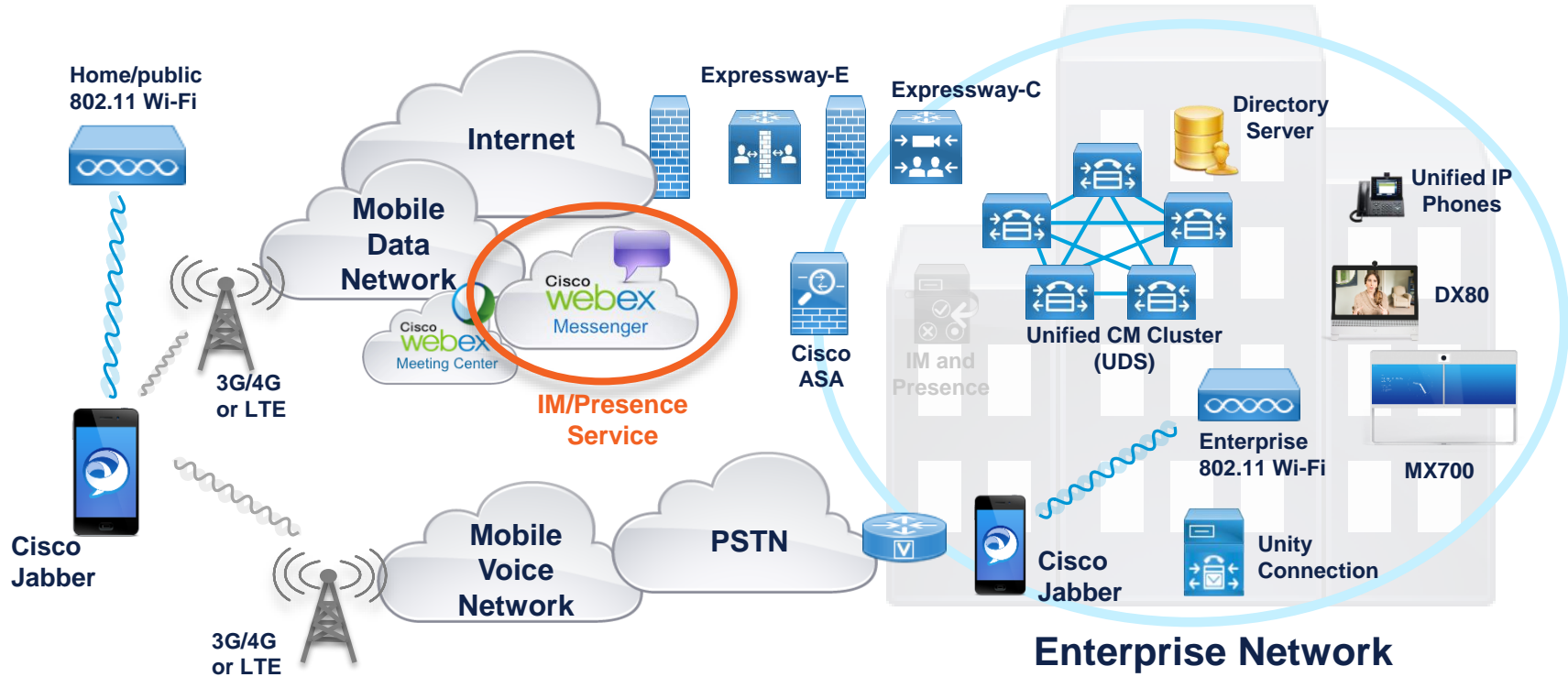
Cisco Jabber – Three Modes of Operation

Full UC Mode **Phone-Only Mode** **IM-Only Mode**

Planning for A Successful Jabber Deployment

- ✓ Deployment model
- ✓ Operating mode
- ✓ User & device
- ✓ Authentication
- ✓ Remote access
- ✓ Distribution & installation
- ✓ Wireless network

Planned Deployment **=** Successful Deployment

User & Device

Cisco Jabber – User Centric Architecture

IM & Presence Profile
Directory Profile
CTI Profile
Voicemail Profile
Conferencing Profile

Service Profile

Policy Items
Policy Items
UC Setting

Policies & UC Settings

Unified CM Home Cluster

Devices

Directory Number or SIP URI

Permissions – Groups & Roles

Jabber User
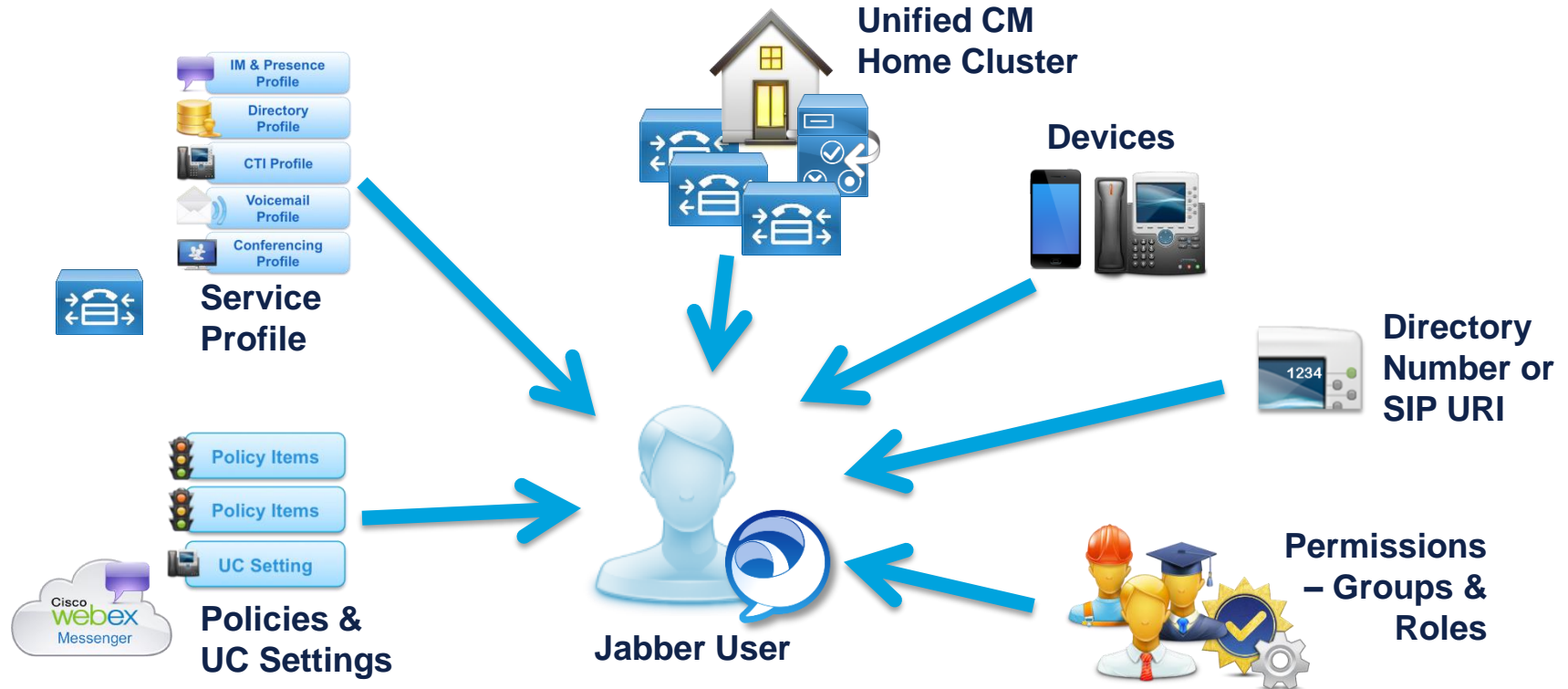
What is User?

- User is …
  - Person who carries devices

- Logical entity in:
  - Unified CM (& IM and Presence)
  - WebEx Messenger service

User must exist regardless which mode of operation!
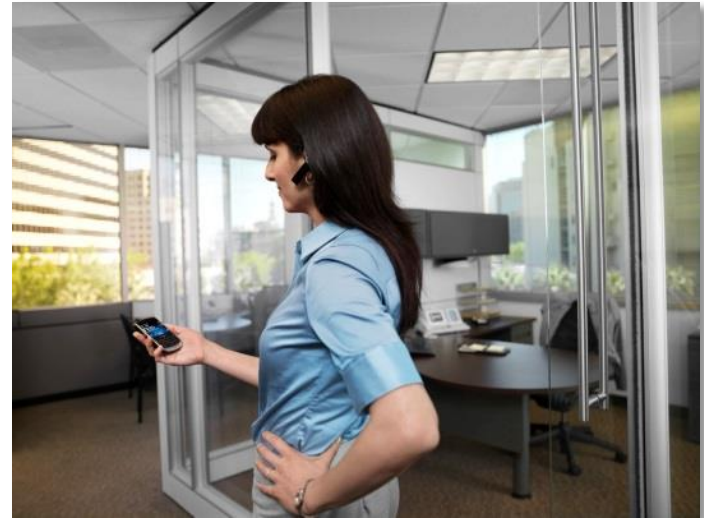
Adding User in Unified CM & IM and Presence

IM and Presence

Unified CM Call Control

Directory Server

User Authentication

DB Sync

LDAP Sync

Jabber User

Jabber User

Highly recommended

User

Jabber ID (JID)

User Fields (UserID & Directory URI)

LDAP Attributes
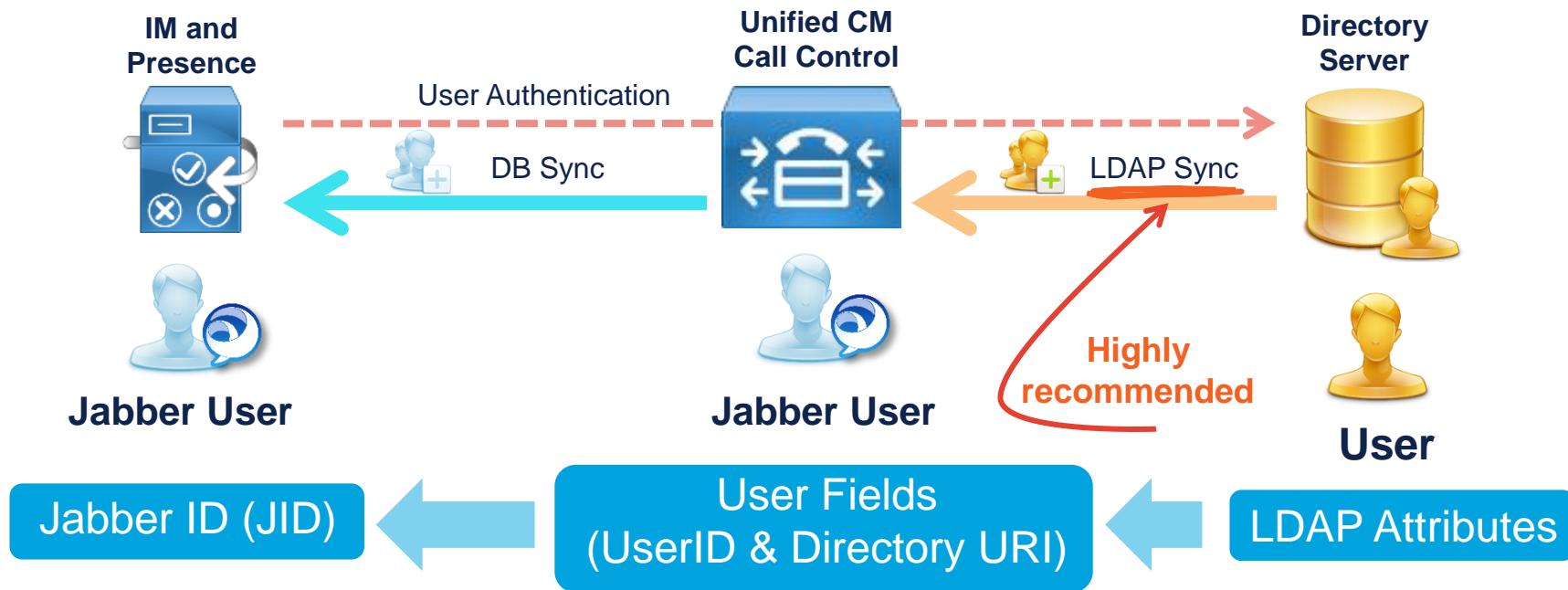
Enterprise Groups Support

New in 11.0

IM and Presence
11.0 or higher

Unified CM
11.0 or higher

Active
Directory

DB Sync

LDAP Sync

Backstage_Team

Desktop_Team

Endpoints_Team

Backstage_Team

Desktop_Team

Endpoints_Team

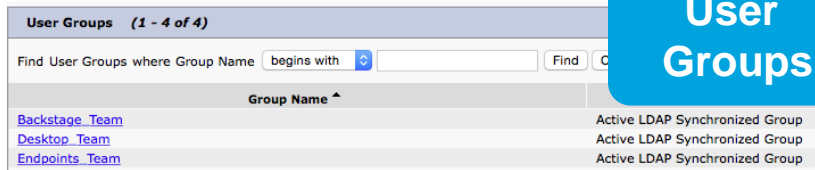**Backstage_Team**

Desktop_Team

Endpoints_Team

User Groups

User Groups (1 - 4 of 4)	

Find User Groups where Group Name [begins with ▾] [Find] [C]

Group Name ▲	
Backstage_Team	Active LDAP Synchronized Group
Desktop_Team	Active LDAP Synchronized Group
Endpoints_Team	Active LDAP Synchronized Group

Distribution Groups

Backstage_Team Properties   [?][X]

Object	Security	Attrib
General	Members	Member Of

Backstage_Team

Group name (pre-Windows 2000): [Backstage_Team]

Description: [Backstage Support Team]

E-mail: [   ]

Group scope
- ○ Domain local
- ◉ Global
- ○ Universal

Group type
- ○ Security
- ◉ Distribution

Cisco live!

Synchronizing/Searching for Enterprise Groups

New in 11.0

- Requires Unified CM & IM and Presence 11.0 or higher
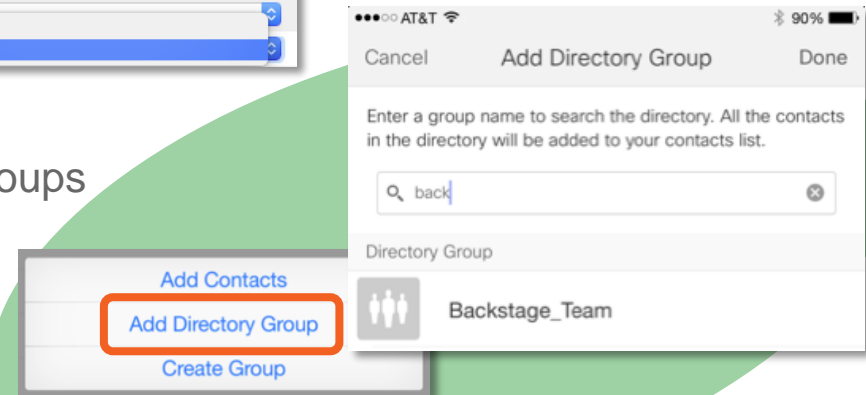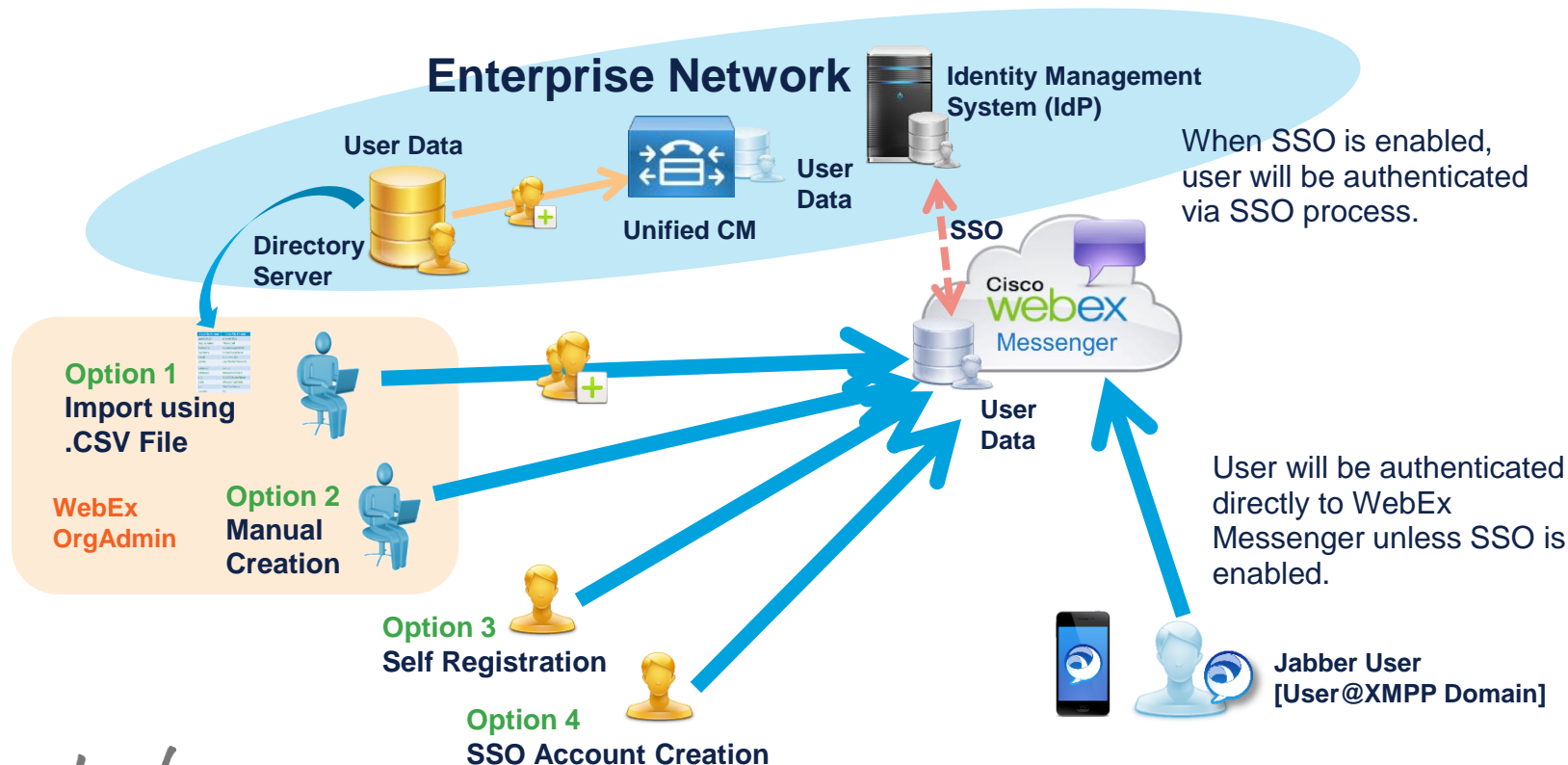 - An Enterprise Parameter is enabled (disabled by default)

User Management Parameters

Effective Access Privileges For Overlapping User Groups and roles *	Maximum
Allow non-super user to grant access to administrative web pages *	True
User Assignment Mode for Presence Server *	Balanced
Directory Group Operations on Cisco IM and Presence *	✓ Enabled / Disabled

- LDAP synchronized for both Users and Groups

Synchronize *   ○ Users Only   ● Users and Groups

Add Directory Group

Cancel   Add Directory Group   Done

Enter a group name to search the directory. All the contacts in the directory will be added to your contacts list.

🔍 back

Directory Group
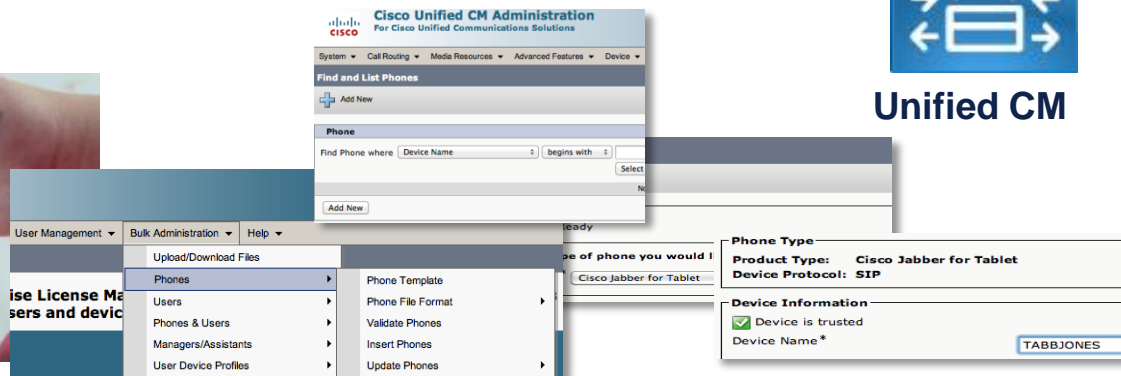
👥 Backstage_Team

Add Contacts

Add Directory Group

Create Group

Jabber user can search/add/delete enterprise groups in his contacts list.

Adding User in WebEx Messenger Service

Enterprise Network

Identity Management System (IdP)

User Data

Directory Server

User Data

Unified CM

SSO

When SSO is enabled, user will be authenticated via SSO process.

Option 1
Import using .CSV File

WebEx OrgAdmin

Option 2
Manual Creation

User Data

Option 3
Self Registration

Option 4
SSO Account Creation

User will be authenticated directly to WebEx Messenger unless SSO is enabled.

Jabber User [User@XMPP Domain]

What is Device?

- Device is…
  - What user carries
  - Where Cisco Jabber runs

- A logical entity in Unified CM
  - Required only when voice/video is needed
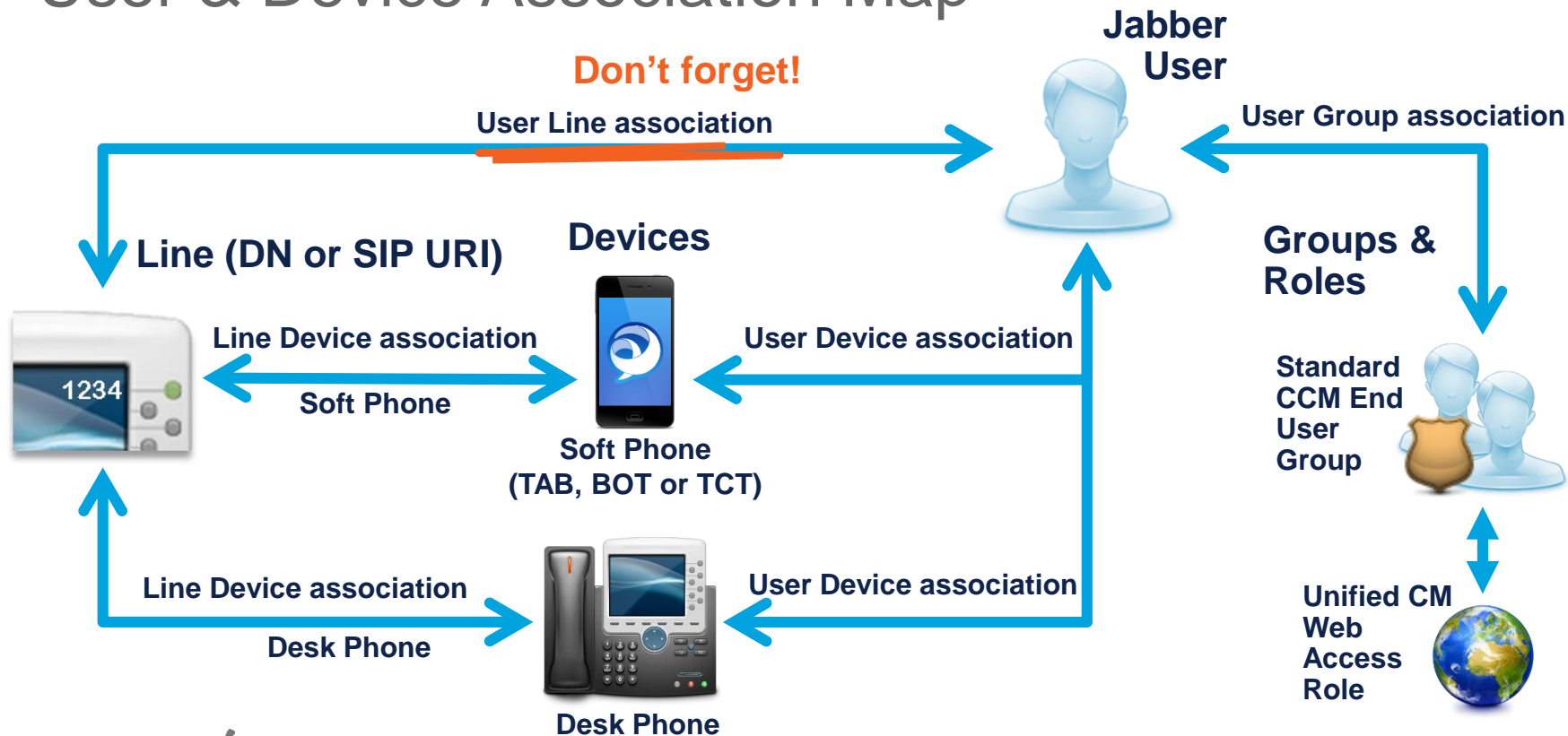 - Can be added via Admin GUI or via BAT

Jabber User

seongho@cisco.com

408-555-1234

Unified CM

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

CISCO

System Call Routing Media Resources Advanced Features Device

Find and List Phones

Add New

Phone

Find Phone where Device Name begins with

Select

Add New

User Management Bulk Administration Help

Upload/Download Files

ise License Ma   Phones   Phone Template
sers and devic   Users   Phone File Format
                      Phones & Users Validate Phones
                      Managers/Assistants Insert Phones
                      User Device Profiles Update Phones

Phone Type
Product Type: Cisco Jabber for Tablet
Device Protocol: SIP

Device Information
☑ Device is trusted
Device Name*   TABBJONES

Cisco Jabber for Tablet

Cisco live!

Device Type in Unified CM

	iPad & Android Tablet without Cellular Voice Capability	Android Smartphone & Tablet with Cellular Voice Capability	iPhone
Product Type (Device Type)	Cisco Jabber for Tablet	Cisco Dual Mode for Android	Cisco Dual Mode for iPhone
Device Protocol	SIP	SIP	SIP
Device Name	**TAB**<USERID> e.g. TABKJONES	**BOT**<USERID> e.g. BOTKJONES	**TCT**<USERID> e.g. TCTKJONES

New in 11.0

With Jabber 11.0, Android tablets with the cellular voice capability can be registered as TAB.

User & Device Association Map

Jabber User

Don't forget!

User Line association

User Group association

Line (DN or SIP URI)

Devices

Groups & Roles

Line Device association

Soft Phone

User Device association

1234

**Soft Phone
(TAB, BOT or TCT)**

Standard CCM End User Group

Line Device association

Desk Phone

User Device association

Unified CM Web Access Role

Desk Phone

Flexible JID & Multiple IM Address Domain

Formatting Jabber ID (JID) with Flexible JID Structure

Jabber ID (JID)   **User Fields**   **LDAP Attributes**

DB Sync

LDAP Sync

IM and Presence

Unified CM

LDAP

Jabber User (JID)

Jabber ID (JID)	User Fields	LDAP Attributes
		sAMAccountName
		mail
UserID@PresenceDomain	UserID	employeeNumber
		telephoneNumber
		userPrincipleName
Directory URI	Directory URI	mail
		msRTCSIP-PrimaryUserAddress

Cisco live!
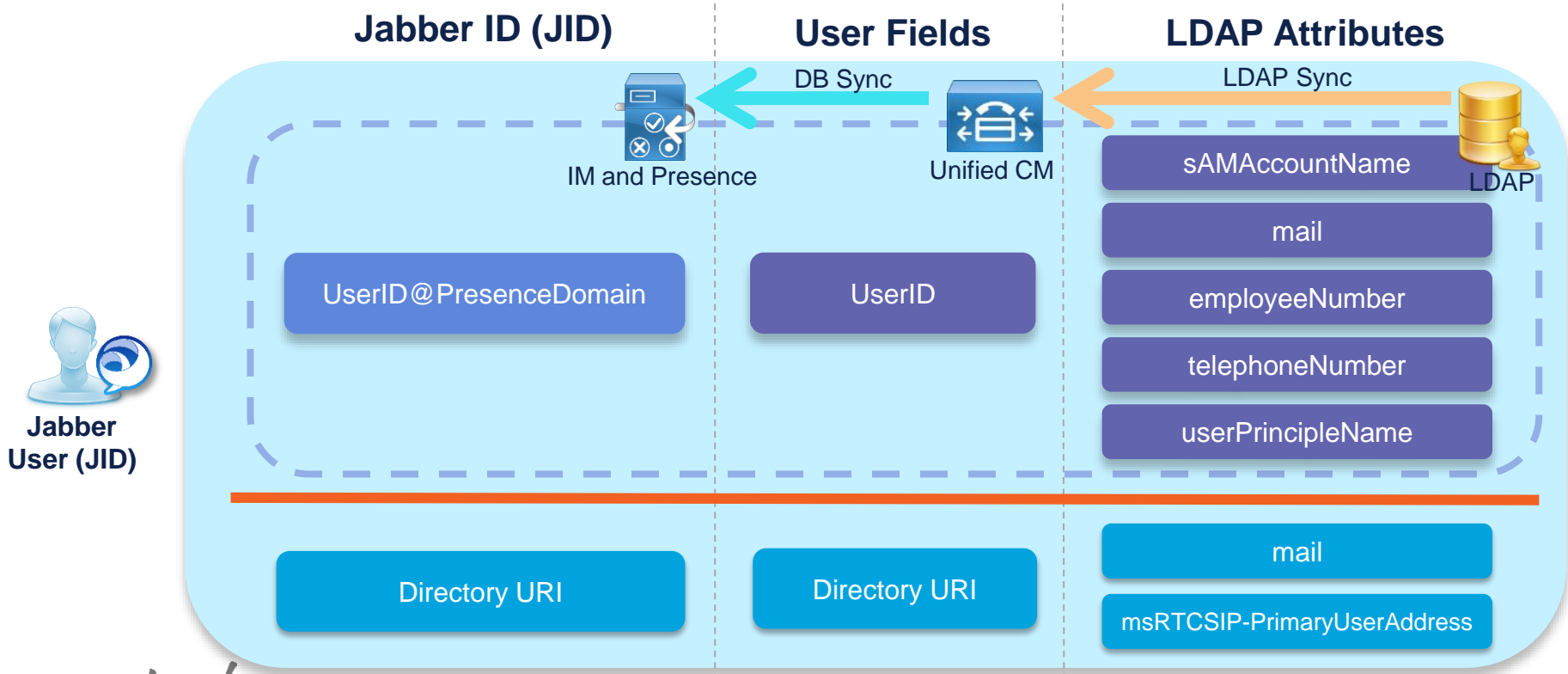
Flexible JID Structure Example

Without Flexible JID, Sue's JID would have been: '**smiller@example.com**'.

UserID (UID): smiller
JID: sue.miller@example.com

Jabber User (Sue Miller)

Jabber-config.xml
<BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts><BDISipUri>**mail**</BDISipUri>

Standard User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName
Middle Name	middleName
Manager ID	manager
Phone Number	telephoneNumber
Title	title
Mobile Number	mcBTSFIP primaryusera
Directory URI	✓ mail

Unified CM LDAP Directory Settings

IM and Presence
Default Domain: example.com

DB Sync

JID = Directory URI:
sue.miller@example.com

Unified CM

LDAP Sync

UserID: smiller
URI: sue.miller@example.com

Directory

Sue Miller
sAMAccountName=smiller
mail=sue.miller@example.com

○ Do not change Default Domain or IM Address scheme
○ Default Domain*
● IM Address Scheme*

Directory URI ▼
UserID@[Default Domain]
Directory URI

Advanced Presence Settings

Multiple IM Address Domain Support

- Allows JIDs with different domains in a single IM/presence deployment
  - e.g. seongho@cisco.com, sally.kim@webex.com & bobcook@meraki.cisco.com

- Automatically turned on when:
  - Flexible JID is enabled (i.e. IM Address Scheme = Directory URI)
  - Directory URI contains multiple domains

Important Requirements:
- All IM and Presence nodes must be on 10.0 or higher
- All Jabber clients must be on 10.6 or higher
- Jabber-config.xml must be updated with the keys to support the multiple IM address domain

- **Everything at once**
- **ALL or Nothing**
- **No reverting back**

Creation of Multiple IM Address Domains

- Domains get added in the database by:
  - IM/Presence Service which parses the domain in each active user's Directory URI
  - System admin who manually adds the domains

Administrator Managed Domains:
Domains with no associated users

System Managed Domains:
Domains with associated users

Administrator Managed Domains (1 - 3 of 3)		
Find Administrator Managed Domains where Domain		Clear Filter ➕ ➖
☐	**Domain ▲**	**Configured on Local Cluster**
☐	cisco.com	✔
☐	meraki.cisco.com	✔
	webex.com	✔

Select All   Clear All   Delete Selected

System Managed Domains (1)	
Domain	**In use on Local Cluster**
jabber.lab	✔

Integrating with Contact Source

Selecting Contact Source for Cisco Jabber

Contact source is a MUST in every Jabber deployment!

LDAP based Contact Source (On Prem Default)
Active Directory by default or other LDAP directory environments

HTTPS/REST based Contact Source (Expressway Default or On Prem Alternative)
UDS built into Unified CM 8.6(2)+

WebEx Messenger Contact Source (Cloud Default)
WebEx Messenger service database

Phone's Local Contacts
Search only; cannot be added as Jabber's contact unless in phone-only mode

User Data Service (UDS)* as Jabber's Contact Source

Directory Server

Unified CM Clusters

Sync

AD

UDS

UDS

UDS
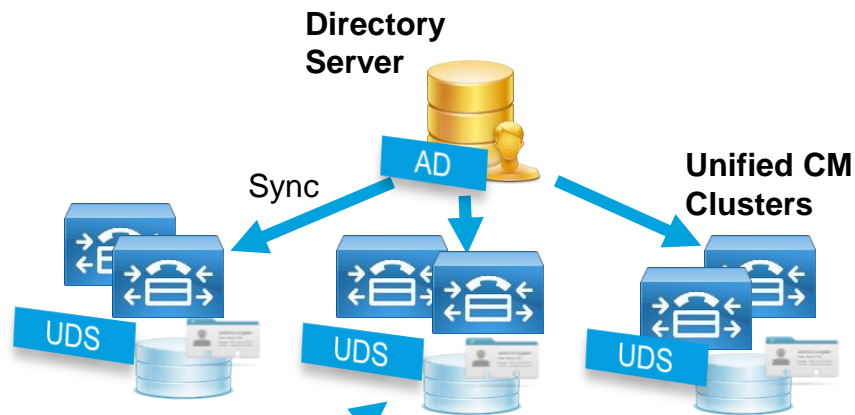
*Resolve ssmith@example.com
Sara Smith
555-325-1010*

Jabber resolves contact lookups against UDS

- Recommend that UDS get synced from corporate directory

- Unified CM 9.1(2) or higher is required to use UDS as Jabber's contact source

- jabber-config.xml is a must

- Jabber supports only UDS when connected via Cisco Expressway

* UDS is a web service on Unified CM providing RESTful API for clients such as Jabber to display or manage user's data or preference settings.

What is jabber-config.xml?

- Global configuration file for Jabber clients

- Admin creates & uploads to TFTP server

- Jabber downloads as its user signs in

- A group configuration file can be assigned to a group of devices

Keep it as **SIMPLE** as possible.
Add **ONLY** what you need!

TFTP restart is not required!

TFTP

jabber-config.xml

group_configuration_file_iphone.xml

Product Specific Configuration Layout

Cisco Support Field   configurationfile=group_configuration_file_iphone.xml
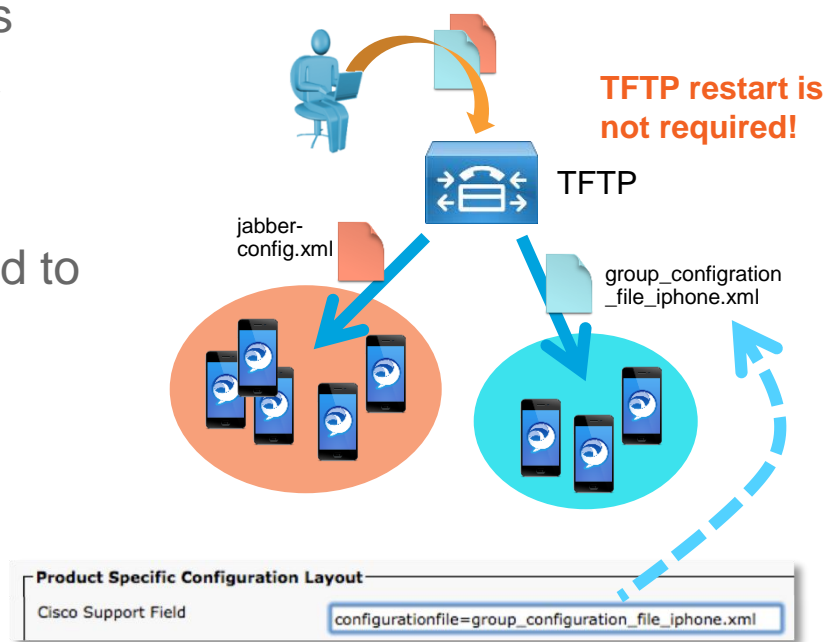
Enabling UC Services for User

Where Does Cisco Jabber Get Configuration?

Device Configuration

jabber-config.xml

IM & Presence

On-Premises Deployment

URL Configuration

Hybrid Deployment

UC Service Profile

End User Input

Local Cache

jabber-config.xml

Cisco Webex Messenger

UC Cluster Settings in OrgAdmin

Device Configuration
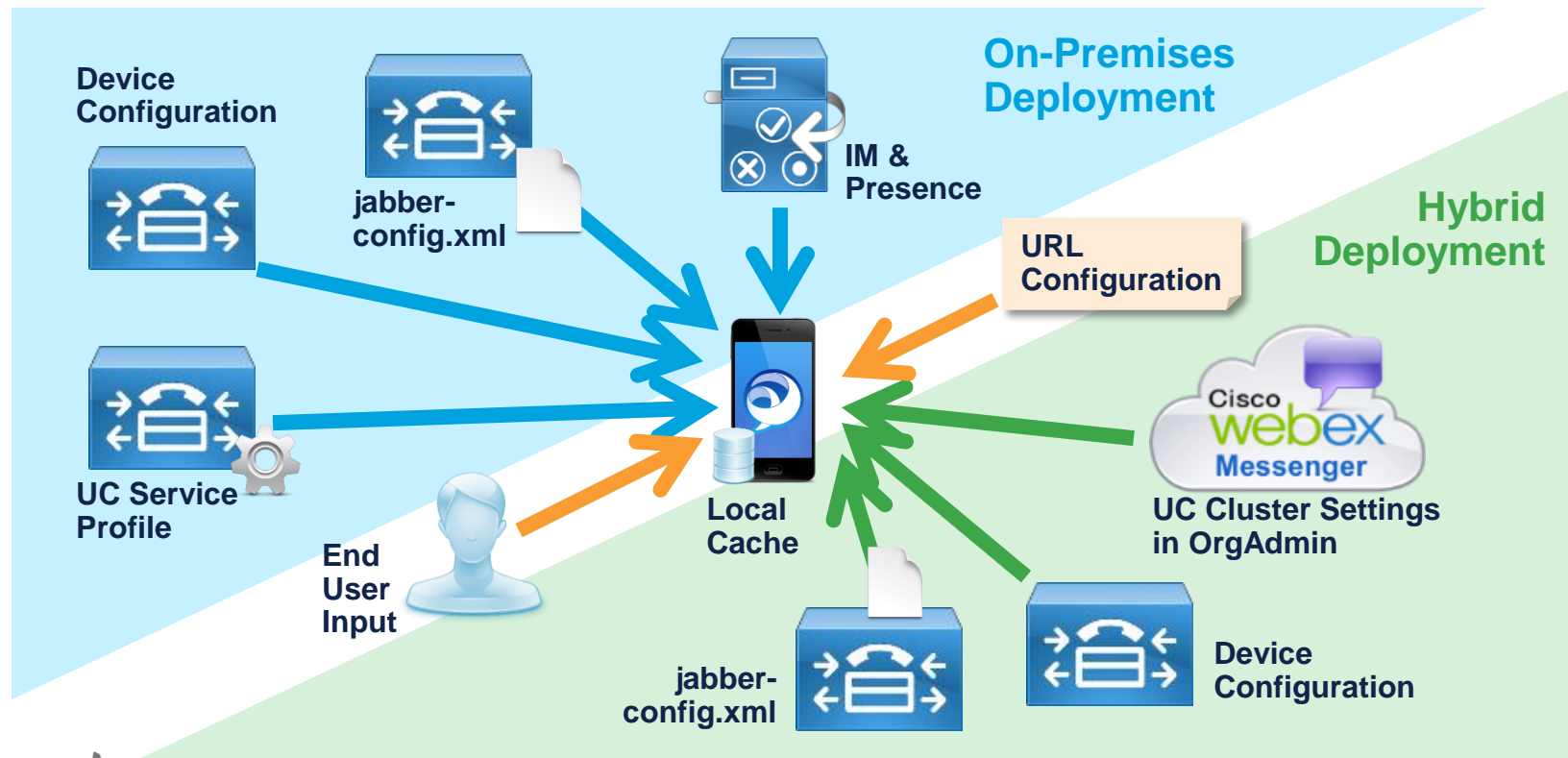
UC Services & Service Profile in Unified CM

Unified CM 9.x or higher

Jabber User ←→ **Service Profile**

IM & Presence Profile

CTI Profile*

Voicemail Profile

Conferencing Profile

Directory Profile

UC Services in Service Profile
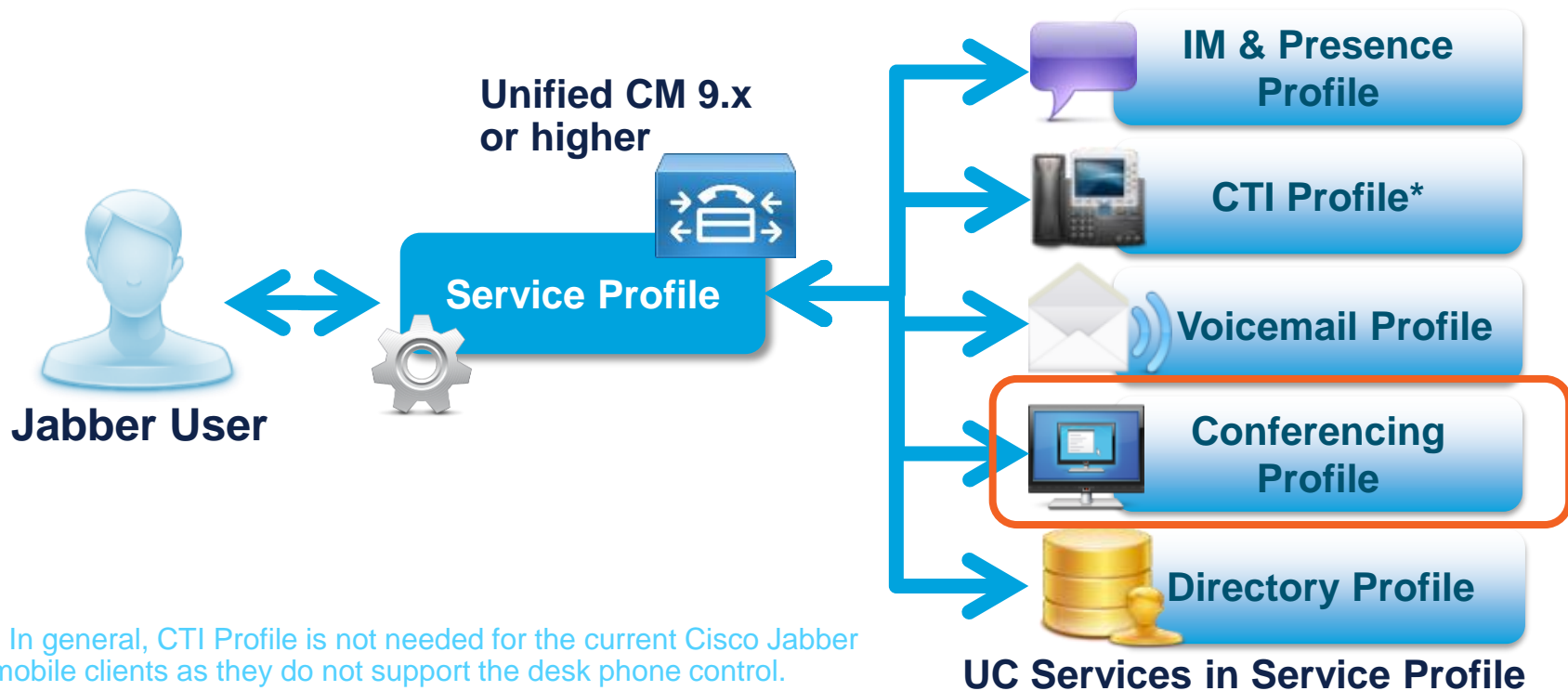
* In general, CTI Profile is not needed for the current Cisco Jabber mobile clients as they do not support the desk phone control.

User & Admin Configuration for Meeting Integration

UC Service Profile in Unified CM
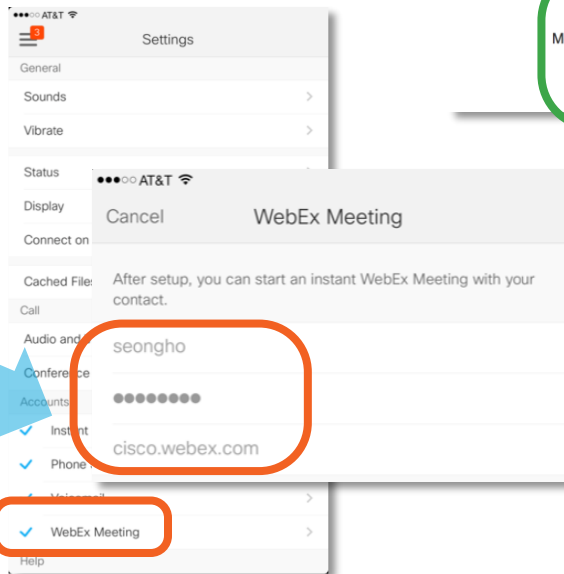
Admin configures the meeting site that can be either **WebEx Meeting Center** or **Collaboration Meeting Rooms (CMR).**

Jabber user can decide whether or not **Personal Room** is used for meeting integration.

Starting/Joining Meeting with WebEx Meeting Center
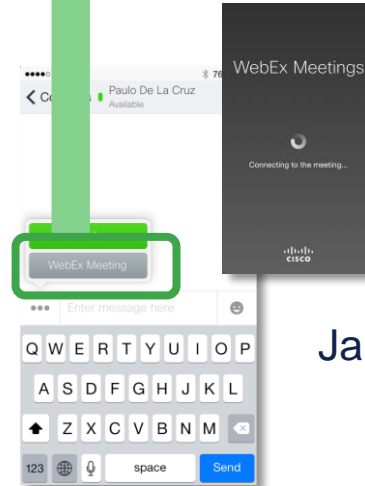
New in 11.0

The meeting starts in Jabber user's **Personal Room** if it's enabled by user.

Cross-launch WebEx Meetings app

Cross-launch WebEx Meetings app
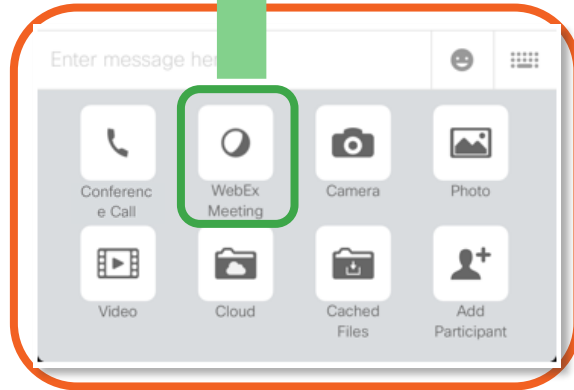
Jabber 11.0

Jabber 10.6

Starting/Joining Meeting with CMR Cloud

New in 11.0

The meeting starts in Jabber user's **Personal Room** if enabled.

Cross-launch WebEx Meetings app to start a CMR meeting

OR

Join a CMR meeting as video endpoint

Jabber 11.0

Collaboration Meeting Rooms

Enabling UC Services for User in Unified CM

- Assign Unified CM home cluster

- Enable IM and Presence service

- Assign a UC Service Profile

Unified CM Home Cluster

IM & Presence Profile

Directory Profile

CTI Profile

Voicemail Profile

Conferencing Profile

Device ▾ Application ▾ User Management ▾
Application Us
End User
User/Phone Add

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)

UC Service Profile   Master Profile   ⬍ View Details

UC Service Profile (e.g. Master Profile)

Enabling UC Services for User in WebEx Messenger

- Create Cluster(s) in Unified Communications menu
  - Voicemail needs to be defined before Cluster(s) gets added

- Assign the Cluster(s) to User in Add or Edit User configuration page

Deploying Jabber in Phone-Only Mode

- IM and Presence service must be disabled

- **User** must exist in Unified CM
  - Sign-in with DeviceID is not supported

- Registers to Unified CM as a SIP device
  - Via service discovery or manual sign in
  - BOT, TCT or TAB associated with user
  - DN or SIP URI (voice & video)

- Supports directory integration
  - LDAP or UDS (search & add)
  - Phone native contacts (pre-populate)
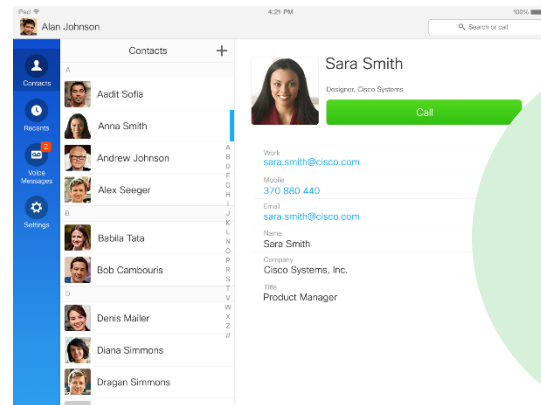
- Works over Cisco Expressway

IM-Only Mode with Unified CM IM and Presence

- End user must be enabled for IM and Presence in Unified CM

Service Settings

☑ Home Cluster

☑ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)
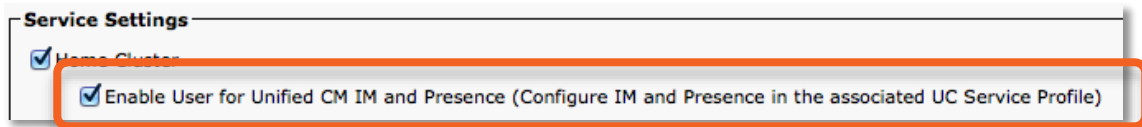
- Device association is not required

- Parameters to hide telephony UE components on Jabber
  - URL configuration string
    ciscojabber://provision?ServicesDomain=cisco.com&Telephony_Enabled=False
  - Key in jabber-config.xml
    <Telephony_Enabled>false</Telephony_Enabled>   ← **Higher priority than URL Config String**

File Transfer

File Transfer in Cisco Jabber for Mobile

- Users can share photos, files & screen captures

- In a 1:1 chat or a group chat*

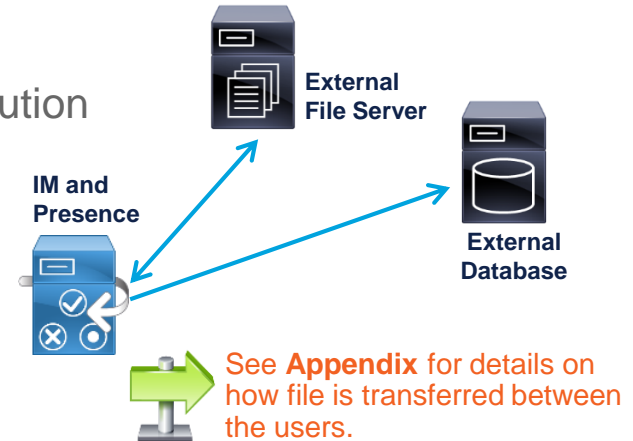- Integration with 3rd party cloud file storages

- Save received files on mobile devices
  - Android – received files in SD card
  - iOS – sent/received files in Jabber app folder

- Events can be logged for compliance purpose*

* File transfer in group chats & compliance logging require Managed File Transfer turned on.

Managed File Transfer (MFT) Support

- Only for Unified CM IM and Presence 10.5(2)+ running XCP File Transfer Manager

- Allows file transfer in a group chat

- Enables event logging for compliance & audit purposes

- Requires external database & external file server
  - PostgreSQL or Oracle external database server
  - Linux (CentOS) file server providing file storage & distribution

External File Server

External Database

IM and Presence

See **Appendix** for details on how file is transferred between the users.
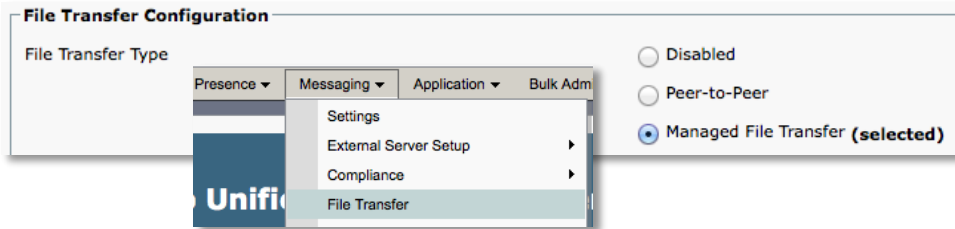
File Transfer Policies & Settings

WebEx Messenger

Unified CM IM and Presence

Action Editor

Action Tag Name:

External File Transfer
Internal File Transfer
External IM
External VOIP
Internal VOIP

Save   Cancel

Cisco webex Connect Administration Tool

User | Configuration | Policy Editor | Group | Report | About | Help

System Settings
- Organization Information
- Domain(s)
- Resource Management
- URL Configuration
- Security Settings
- Password Settings
- Email Templates
- User Provisioning

Connect Client
- General IM
- Contact List
- Profile Settings
- **IM Block Settings**
- XMPP IM Clients

IM Block Settings ?

Blocked File Types: Separated multiple values with semicolon, e.g. zip;.exe

.exe;.zip

Blocked URLs: Separated multiple URLs with semicolon

In jabber-config.xml,

    File_Transfer_Enabled

    Disallowed_File_Transfer_Types (file extension such as .exe)

    Diasallow_FileTransfer_On_Mobile

    P2P_File_Transfer_MaxSize_KB

In IM and Presence Admin GUI,
File Transfer Type :
    Disabled
    Peer-to-Peer
    Managed File Transfer
Managed File Transfer Configuration :
    Maximum File Size

Enabling MFT (system-wide)

SAMLv2 Single Sign-On (SSO)

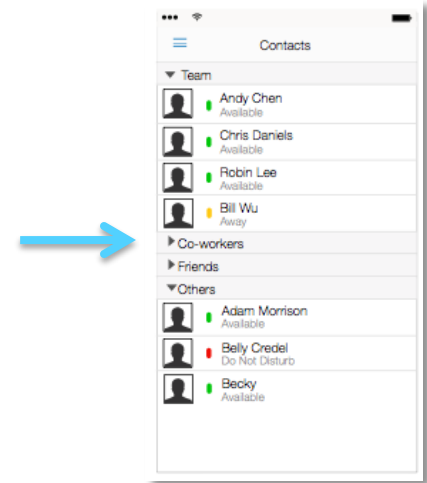# SSO User Experience Design Concept for Jabber

Jabber starts & continues the service discovery process.
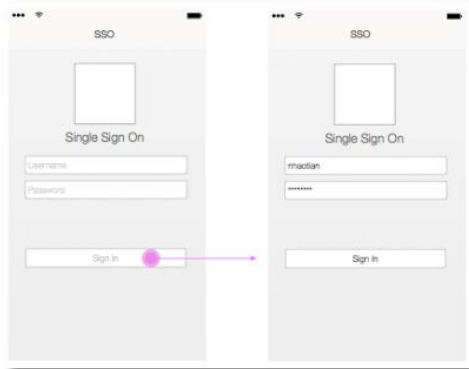
Jabber will display **embedded browser** page to get login credentials from user.

Jabber signs in; no additional credentials is requested.

Signed in for all provisioned UC services; no need to enter additional credentials for the UC services.

SAMLv2 SSO Architecture for On-Premises Deployment

Cisco Jabber on Mobile

Corporate DMZ

Identity Management

Ping Identity
OpenAM
Active Directory Federation Services 2.0 RTW

3rd Party Identity Provider

Directory

SAMLv2

OAuth

SAMLv2

LDAP Sync

UCM 10.5   IM/P 10.5   CWMS 2.5   CUC 10.5

SSO Enabled On-Prem UC Services
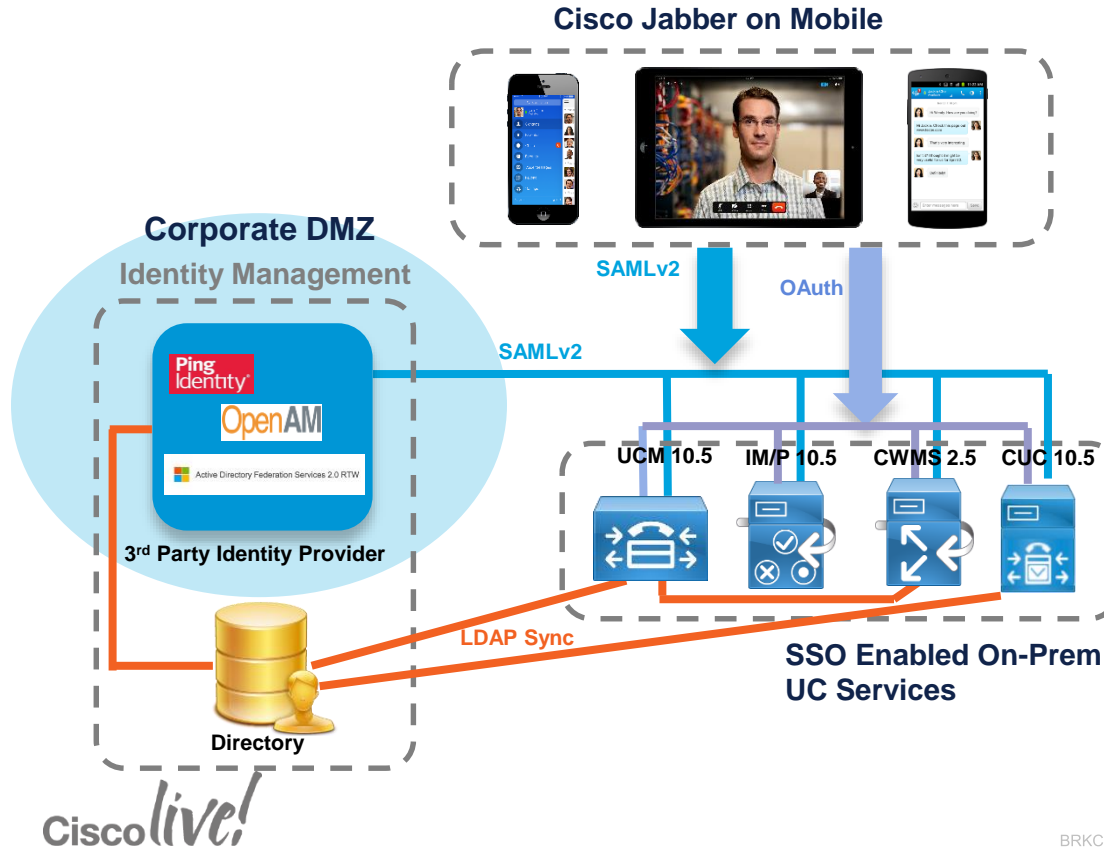
- Single credentials for all SSO enabled UC services

- UC services will directly integrate with IdP via SAMLv2

- Cisco Expressway or AnyConnect is required from the outside of enterprise network

UCM: Cisco Unified CM
IM/P: Cisco Unified CM IM and Presence
CWMS: Cisco WebEx Meeting Server
CUC: Cisco Unity Connection

SAMLv2 SSO Architecture for Hybrid Deployment

Cisco Jabber on Mobile

- Jabber with WebEx Messenger using the same IdP should be able to login to SSO enabled on-premises UC services using same credentials

- Cisco Expressway or AnyConnect is required to access on-premises UC servers from the outside of enterprise network

Corporate DMZ

Identity Management

SAMLv2

OAuth

SAMLv2

PingIdentity
OpenAM
Active Directory Federation Services 2.0 RTW

3rd Party Identity Provider

SAMLv2

UCM 10.5

CUC 10.5

SAMLv2

SSO Enabled On-Prem UC Services

LDAP Sync

Directory

.cvs

FTP

Messenger

Meeting Center

Cisco WEBEX

WebEx Cloud Services
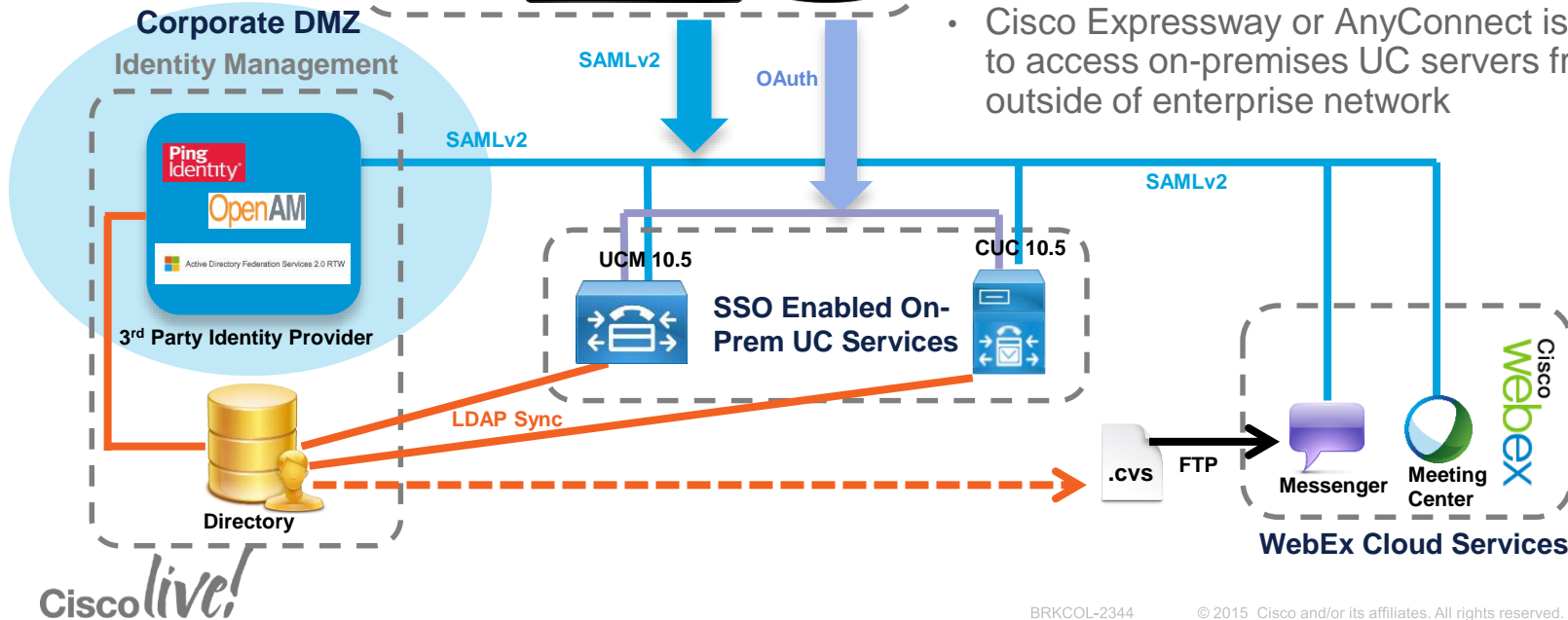
SAMLv2 SSO Support over Cisco Expressway

- Requires at minimum:
  - Cisco Expressway X8.5
  - Unified CM 10.5(2)
  - Jabber 10.6

- Supports Jabber on-premises & hybrid deployment models

See **Appendix** for details on how SAMLv2 SSO works over Cisco Expressway.

SAML 2.0
Security Assertions Markup Language

Jabber 10.5 or later with SSO Enabled

SSO enabled Cisco UC Applications

Internet

Jabber 10.6 or later with SSO Enabled

IdP (Identity Provider)
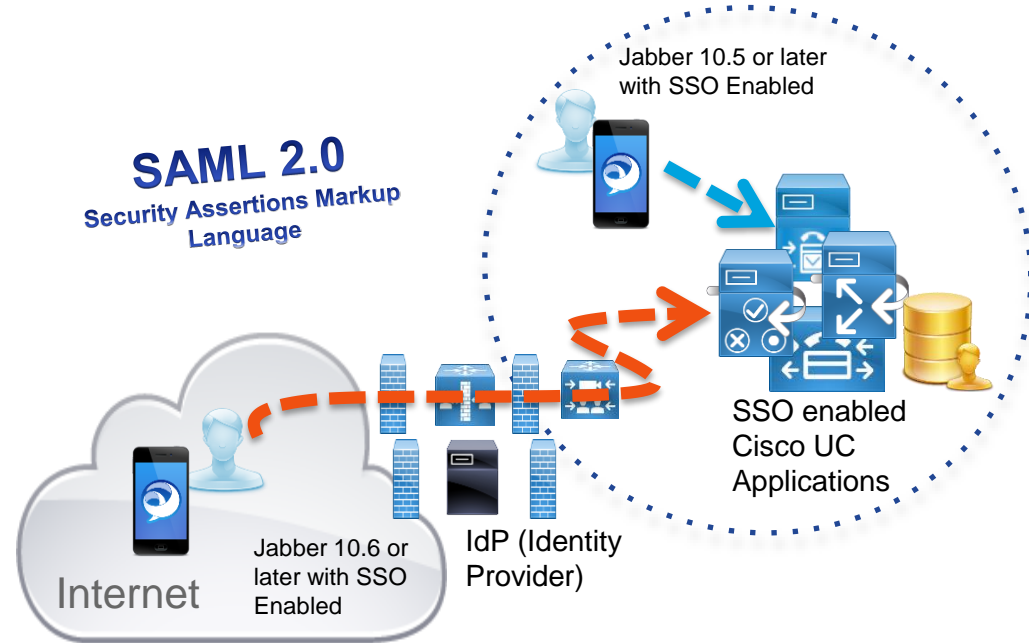
Security in Cisco Jabber

Secure Communications with UC Services

Web Server for Contact Photos

Active Directory or LDAP Server

Voice or Video

Cisco Unified CM

LDAPS

sRTP

SIP over TLS

HTTP

HTTPS

Cisco Unified CM UDS Server

HTTPS*

New in 11.0

Cisco Unified CM TFTP Server

Requires Jabber 11.0 & UCM 11.0 or higher.

Cisco Unity Connection

VMREST/HTTPS

XMPP HTTPS (SOAP)

Cisco Unified CM IM and Presence

HTTPS

Cross launch WebEx Meetings app

Cisco Jabber

Cisco
webex
Meeting Center

Cisco live!

Signaling & Media Encryption over Expressway

SIP (or SIP over TLS)
Secure RTP
XMPP (or XMPP over TLS)

SIP line side (not trunk)

Expressway-E

Firewall

Expressway-C

Unified CM (Mixed Mode)

Cisco Jabber

🔒 Encrypted

🔒 Encrypted only when Unified CM is Mixed Mode; Jabber requires CAPF enrollment

IM and Presence
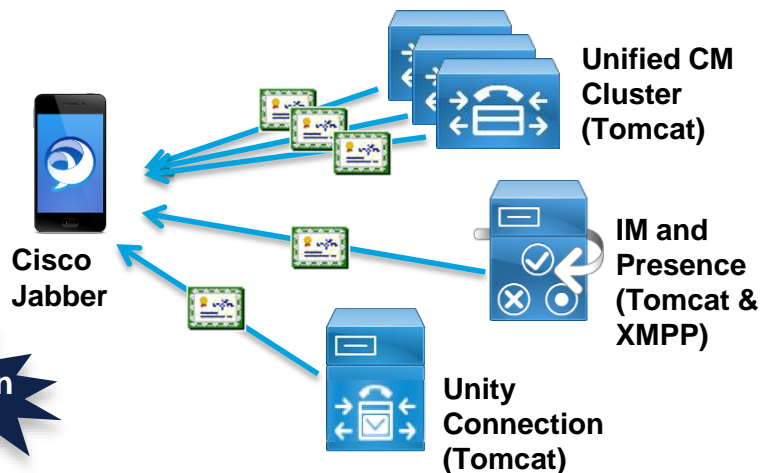
Cisco Jabber

Cisco IP Phone
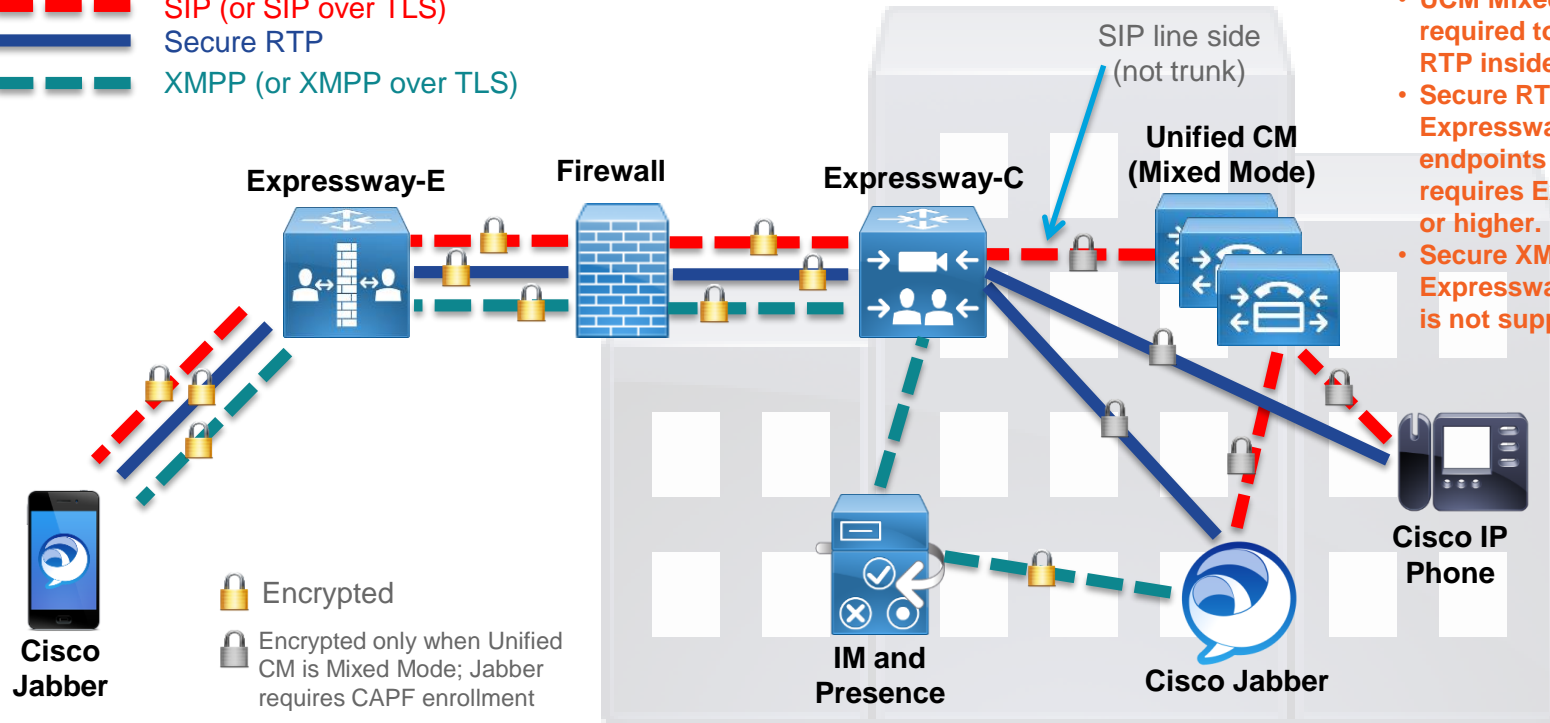
- **UCM Mixed Mode is required to secure SIP & RTP inside the network.**
- **Secure RTP between Expressway-C and endpoints including Jabber requires Expressway X8.2 or higher.**
- **Secure XMPP between Expressway-C & UCM IM/P is not supported.**

UC Server Certificate Validation

- Jabber validates the certificates from UC application servers

- Validation fails when the certificate is:
  - Invalid (e.g. self signed certificate) AND
  - Not matching with one in cache

- Admin can control how the invalid certificate is handled by the end user
  - Default – End user is prompted to either accept or decline (when accepted, the certificate gets stored)
  - Prompt per session – End user is prompted to either accept or decline (the certificate is not stored)
  - Reject & notify – End user is prompted but cannot accept invalid certificates

New in 11.0

Cisco Jabber

Unified CM Cluster (Tomcat)
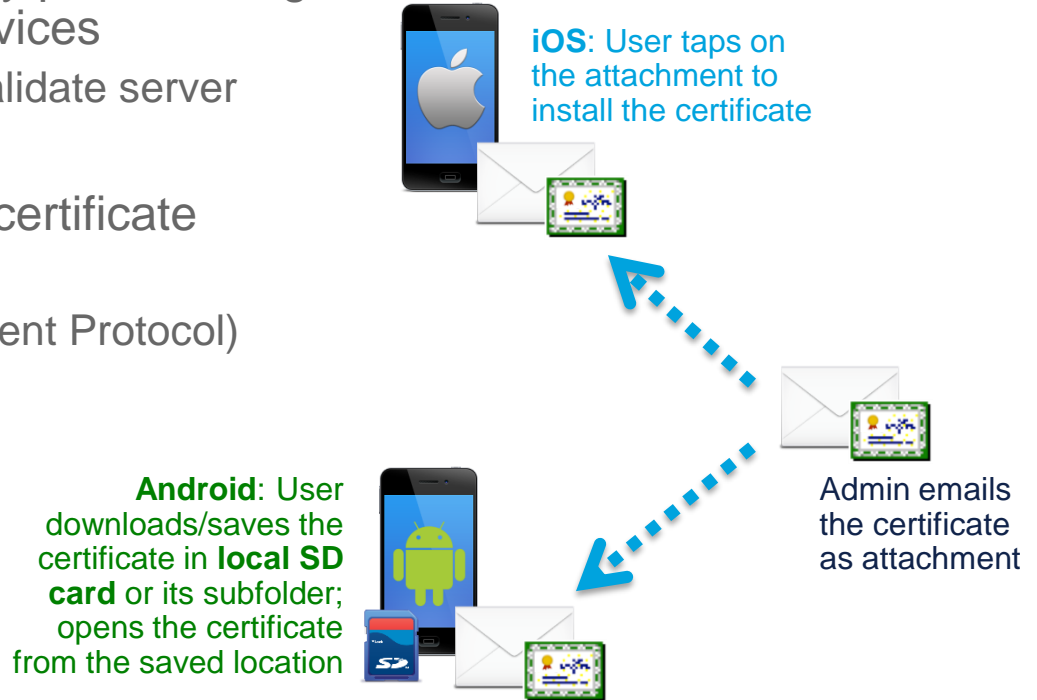
IM and Presence (Tomcat & XMPP)
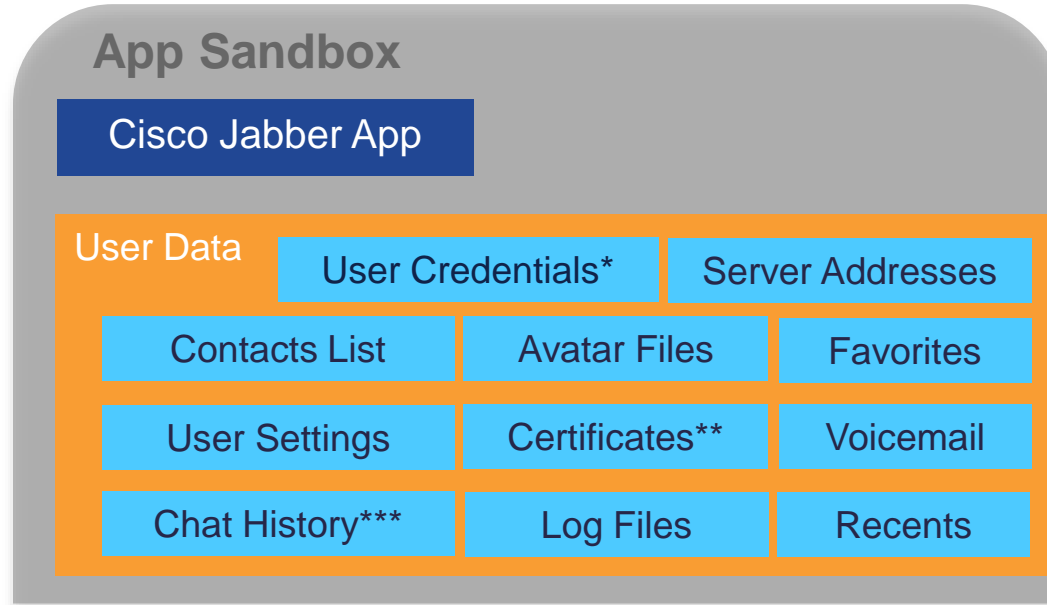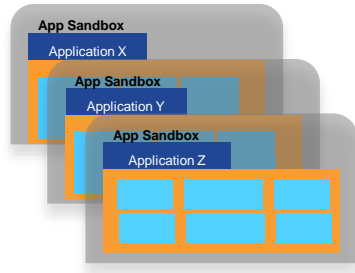
Unity Connection (Tomcat)

A new configuration key, **InvalidCertificateBehavior**, via either MAM app configuration or configuration URL:

ciscojabber://provision?
InvalidCertificateBehavior=RejectAndNotify

Pre-installing Root CA Certificate

- Enhance end user experience by pre-installing root CA certificate on mobile devices
  - Cisco Jabber will not prompt to validate server certificates

- Options for distributing root CA certificate
  - As an attachment in email
  - SCEP (Simple Certificate Enrollment Protocol)

iOS: User taps on the attachment to install the certificate

Admin emails the certificate as attachment

Android: User downloads/saves the certificate in **local SD card** or its subfolder; opens the certificate from the saved location

Cisco Jabber for Mobile in App Sandbox

App Sandbox
Application X

App Sandbox
Application Y

App Sandbox
Application Z

App Sandbox

Cisco Jabber App

User Data

User Credentials*		Server Addresses
Contacts List	Avatar Files	Favorites
User Settings	Certificates**	Voicemail
Chat History***	Log Files	Recents

Jabber app & user data get sandboxed unencrypted.

Everything in the app sandbox will be removed when user uninstalls Jabber.

* On Android, user credentials are encrypted using AES-128 before they get stored in the sandbox.
  On iOS, user credentials are stored only in the iOS Keychain (encrypted container), not in the sandbox.
** Accepted server certificates are stored encrypted on iOS; stored unencrypted on Android.
*** Chat history gets stored only when enabled by the system admin.

Considerations for Wireless LAN

Common Complaints from Jabber for Mobile Users

- Common complaints
  - Poor audio/video quality
  - Call drops (especially while moving)

- Potential root causes
  - Weak signal power
  - Interference/noise
 - Low capacity
  - Slow roaming
  - Quality of Service (QoS)

WiFi™

Wireless Characteristics
- Shared media
- Coverage
- Security
- Battery life
- Roaming

Optimizing RF Coverage

- Cell design
  - 20% overlap & -67 dBm at the cell edge
  - Channel utilization < 50%
  - 5GHz spectrum whenever possible
- AP (Access Point) placement
  - Roughly one AP for every 2,500 – 3,000 square feet
  - Avoid highly reflective/obstructive objects near by
  - Places you never thought people would be…
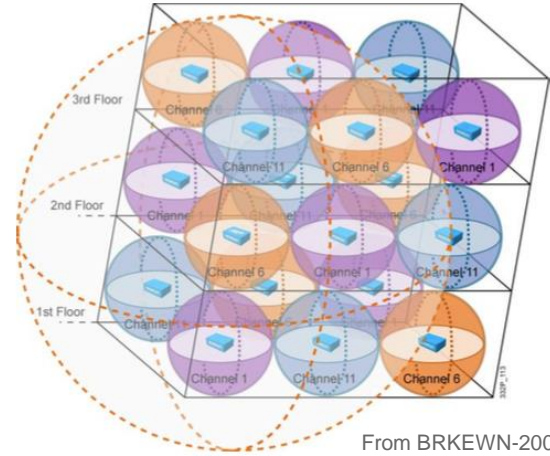
From BRKEWN-2000 Design and Deployment of Wireless LANs for Voice and Video

Ensuring Fast & Reliable Roaming

- Transition AP
  - Allow enough time to scan for neighboring APs
- Fast transition via 802.11r*
  - Key caching for client association & re-authentication
- Fast neighbor scanning via 802.11k*
  - Provide neighbor AP lists based on client location
- Better wireless network management via 802.11v*

* 80211r, 11k & 11v work only with mobile devices such as smartphones & tablets.

Enabling End to End QoS

- Set WLAN QoS to Platinum (voice)
  - To allow the highest DSCP value into CAPWAP packet

- Allow WMM (Wi-Fi Multimedia)*
  - To enable 802.11e User Priority (UP)

- Enable AVC (Application Visibility & Control)
  - For better reporting & restriction on bad traffic

- Add switch port QoS configuration for APs & WLCs
  - To ensure the wired/switch side honor the QoS tagging
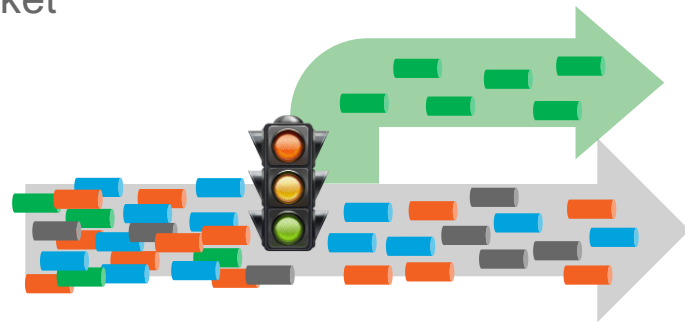
* Ensure to assign the lowest QoS profile to Non-WMM clients.

QoS Marking Example for Voice Call (Downstream)

11e UP	DSCP	Payload
0		

DSCP	CAPWAP Encapsulated		
0	802.11	DSCP **46**	Payload

802.1p	DSCP	Payload
	46	

DSCP 46 gets marked down to 0, UP marked to 0 (Best Efforts)

QoS:Silver

WLAN Controller

CAPWAP Tunnel

AP

802.1Q Trunk

Ethernet Switch

QoS:Platinum

11e UP	DSCP	Payload
6		

DSCP	CAPWAP Encapsulated		
46	802.11	DSCP **46**	Payload

802.1p	DSCP	Payload
	46	
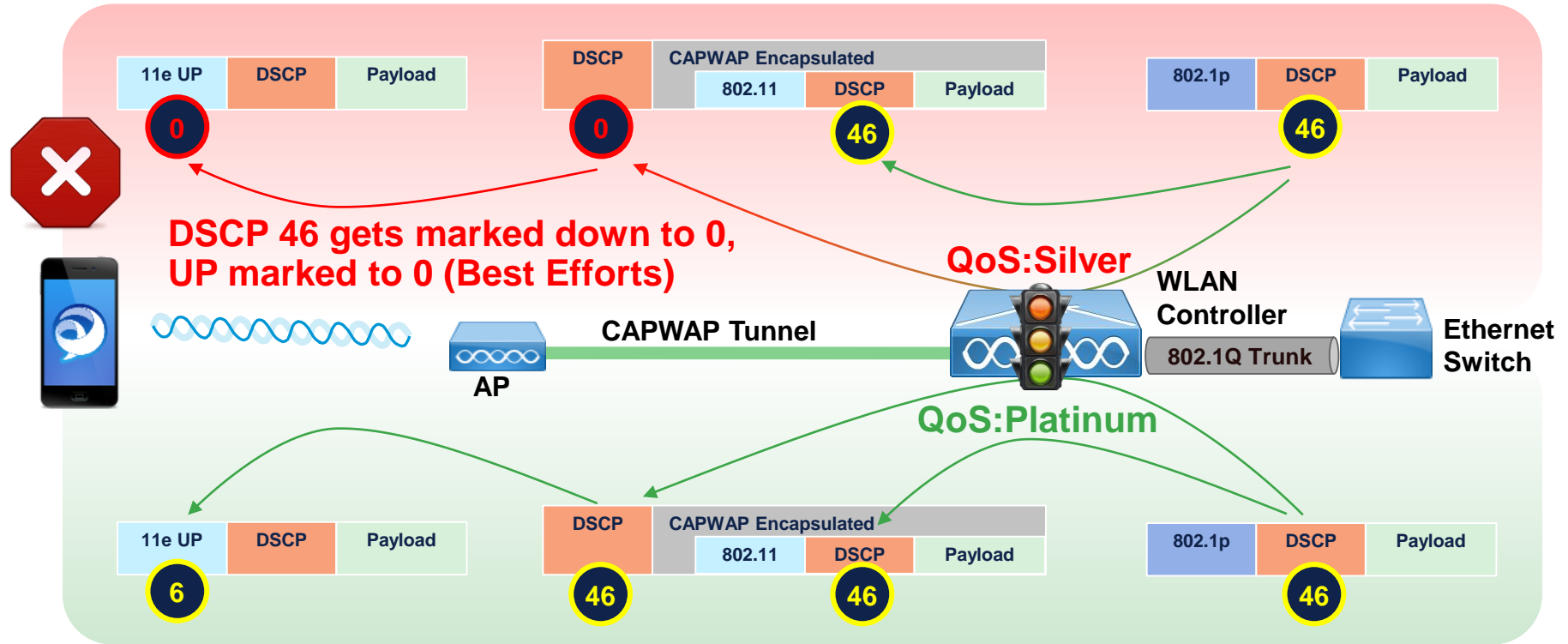
You, the Jabber guru

What do you want? I don't like it when you're smiling…
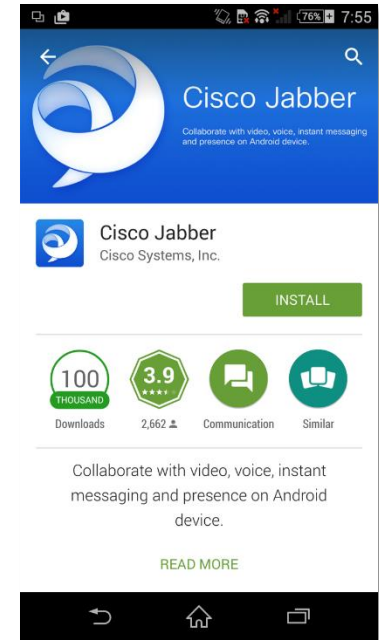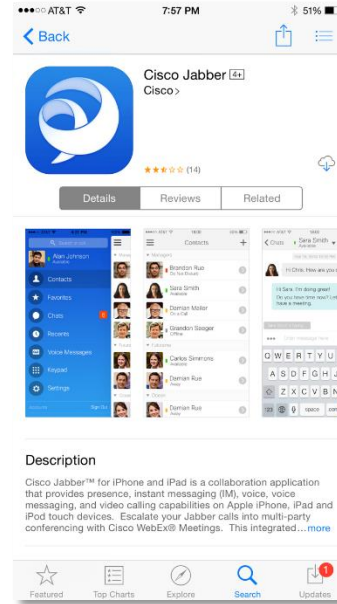
Your wireless guy

Distributing Cisco Jabber for Mobile

Where to Find the Latest Jabber Clients

- Cisco Jabber is an public app with free download

- Recommend that end users download/upgrade directly from App Store or Google Play

- 3rd party EMM* solution can be used to configure/distribute Jabber within an organization

* EMM (Enterprise Mobility Management)

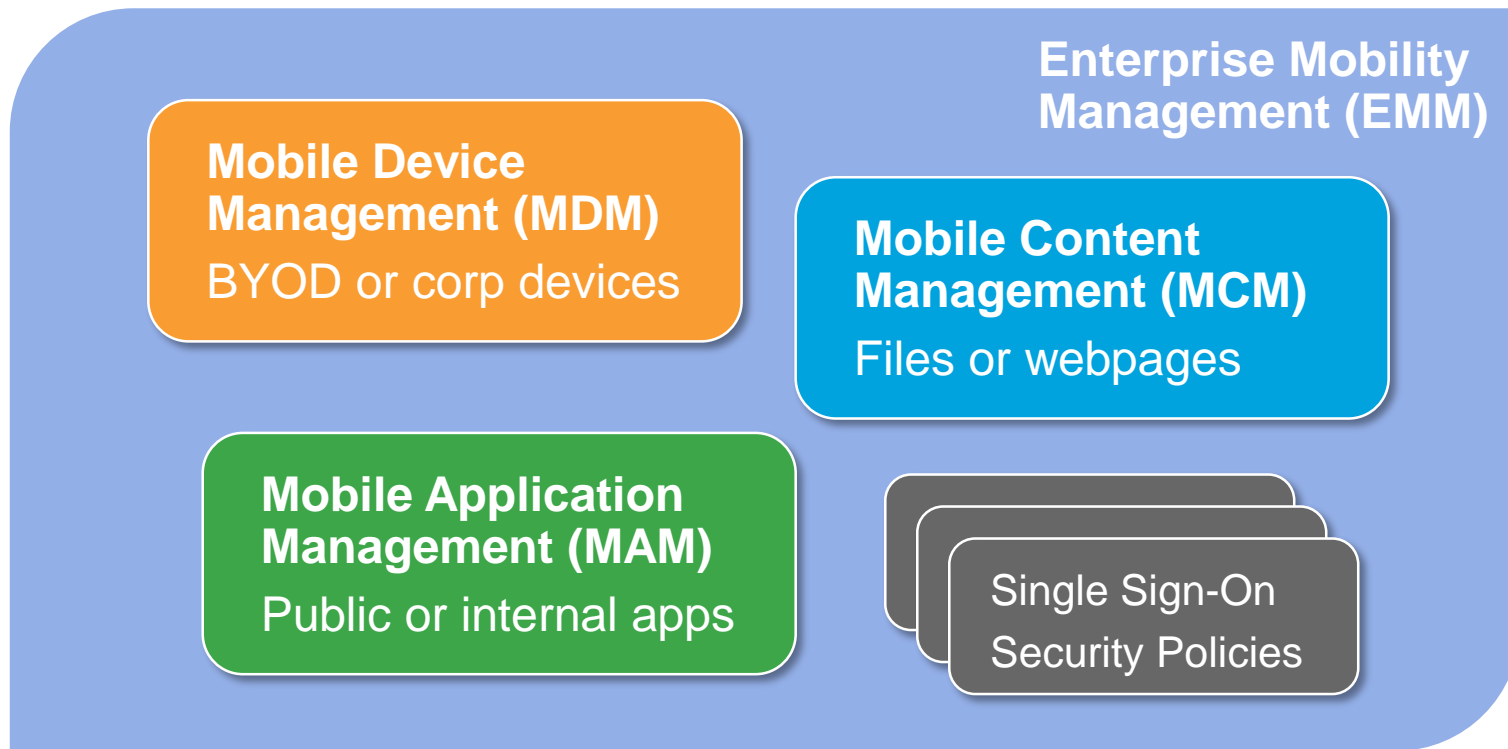# Common Questions from Jabber Customers

Does Jabber support MDM? If so which MDM vendor?

Does/will Jabber work with the MDM my company has?

Can I distribute Jabber using my MDM console?

Can I manage Jabber using the MDM I have deployed?

What is MDM, MAM, EMM or M&M?

Enterprise Mobility Management (EMM)

Mobile Device Management (MDM)
BYOD or corp devices

Mobile Content Management (MCM)
Files or webpages

Mobile Application Management (MAM)
Public or internal apps

Single Sign-On
Security Policies

What is MDM, MAM, EMM or M&M?

Enterprise Mobility Management (EMM)

Mobile Device Management (MDM)
BYOD or corp devices

Mobile Content Management (MCM)
s or webpages

Mobile Application Management (MAM)
Public or internal apps

Single Sign-On
Security Policies

Different Ways to Manage Apps via MAM

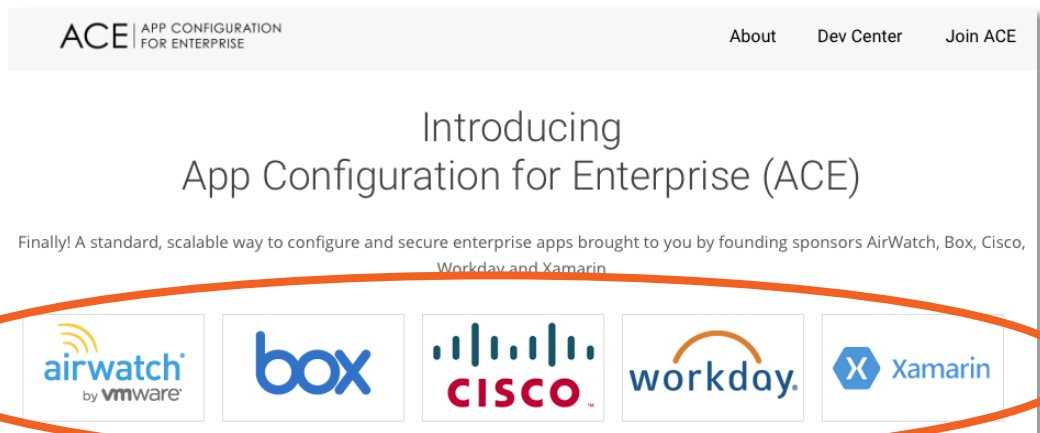| App Wrapping	SDK	API
• Wrapping tool provided by each MAM vendor	• SDK provided by each MAM vendor	• Standard APIs available for mobile native OS
• No code change on app (as long as compatible)	• SDK must be imported into app (per vendor)	• Small code change on app
• Internal distribution only (not on public app store)	• Multiple versions on public app store	• Only single version on public app store
• Compatibility or update issues	• Potential feature gaps with public app	

Most economical & scalable approach

Introducing App Configuration for Enterprise (ACE)

- Standard way for enterprise apps to interpret configurations & policies from EMM to provide:
  - App configuration
  - Enterprise connectivity
  - SSO & access control
  - Security policies

http://AppConfigForEnterprise.org

ACE | APP CONFIGURATION FOR ENTERPRISE   About   Dev Center   Join ACE

Introducing
App Configuration for Enterprise (ACE)

Finally! A standard, scalable way to configure and secure enterprise apps brought to you by founding sponsors AirWatch, Box, Cisco, Workday and Xamarin

Initial Founding Members

airwatch by vmware   box   cisco   workday.   X Xamarin

Jabber & App Configuration via EMM

New in 11.0

Managed Jabber 11.0

EMM Platform

iOS "Managed Configurations" NSUserDefaults API

"App Restrictions" get/setRestrictions API

Managed Device

Deploying Jabber with configuration

APPLICATION CONFIGURATION

Enter Key-Value pairs to configure applications for users:

Configuration Key	Value Type	Configuration Value	
ServicesDomain	String	example.com	✚ Insert Lookup Value
VoiceServicesDomain	String	voice.example.com	✚ Insert Lookup Value
ForceLaunchBrowser	String	true	✚ Insert Lookup Value

✚ Add

Configuration Key Definition*

* Captured from AirWatch Console

What's Supported in Jabber 11.0?

Key values that can be configured via standard APIs in Jabber 11.0

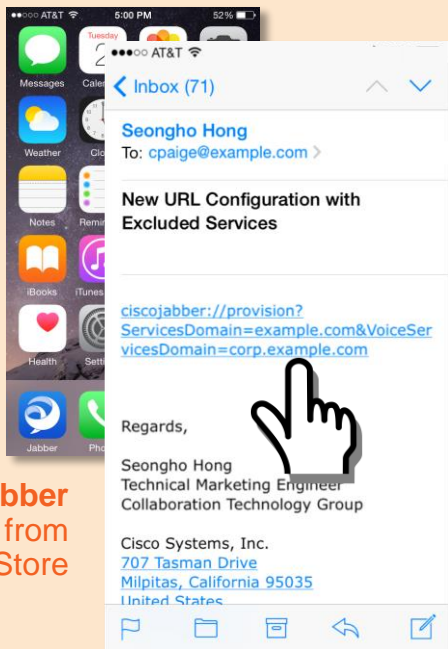New in 11.0

| Keys in Configuration URL	Keys in jabber-config.xml
• InvalidCertificateBehavior • ServicesDomain • VoiceServicesDomain • ForceLaunchBrowser • ServicesDomainSsoEmailPrompt • Telephony_Enabled • ServiceDiscoveryExcludedServices • TelemetryEnabled • Meetings_Enabled • Telephony_P2P_Enabled	• EnableTelProtocol • EnableCiscoTelProtocol • EnableClickToCallProtocol • EnableSIPProtocol • EnableIMProtocol • EnableXMPPProtocol • EnableCiscoIMProtocol • EnableProvisionProtocol • EnableShareProtocol • EnableCiscoChatProtocol • EnableStatusProtocol • EnableProfileProtocol

Two Options to Distribute Jabber

New in 11.0

URL Configuration

Jabber
downloaded from
App Store
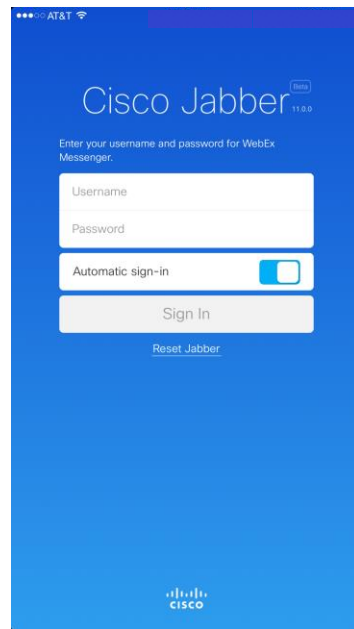
App Configuration
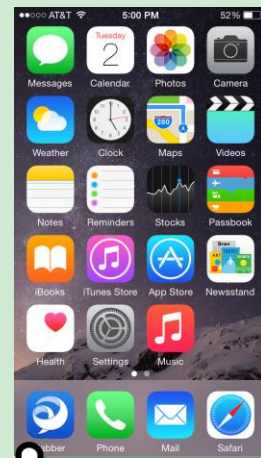
Managed Jabber
pushed from EMM

Requirements for Jabber App Configuration

New in 11.0

Jabber for Mobile	Device OS	MAM
• 11.0 or higher • Managed app only*	• iOS 8.0 or higher • Android L (5.0) or higher	• Supports standard APIs defined in ACE**

* Jabber downloaded directly from App Store or Google Play will not support app configuration via MAM.

** Jabber 11.0 has been tested with AirWatch for app configuration.

Closing Thoughts

Key Takeaways

- A well-planned deployment is a successful deployment

- Make sure that the wireless network is ready for Jabber

- Integrate Jabber with Collaboration Meeting Rooms for better meeting experience

- Encourage your MAM vendor to participate in ACE

Participate in the "My Favorite Speaker" Contest

Promote Your Favorite Speaker and You Could Be a Winner

- Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)

- Send a tweet and include
  - Your favorite speaker's Twitter handle
  - Two hashtags: #CLUS #MyFavoriteSpeaker

- You can submit an entry for more than one of your "favorite" speakers

- Don't forget to follow @CiscoLive and @CiscoPress

- View the official rules at http://bit.ly/CLUSwin

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

- Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.

Don't forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

• Demos in the Cisco campus

• Table Topics

• Meet the Engineer 1:1 meetings

• Related sessions

Collaboration Cisco Education Offerings

Course	Description	Cisco Certification
CCIE Collaboration Advanced Workshop (CIEC)	Gain expert-level skills to integrate, configure, and troubleshoot complex collaboration networks	CCIE® Collaboration
Implementing Cisco Collaboration Applications (CAPPS)	Understand how to implement the full suite of Cisco collaboration applications including Jabber, Cisco Unified IM and Presence, and Cisco Unity Connection.	CCNP® Collaboration
Implementing Cisco IP Telephony and Video Part 1 (CIPTV1) Implementing Cisco IP Telephony and Video Part 2 (CIPTV2) Troubleshooting Cisco IP Telephony and Video (CTCOLLAB)	Learn how to implement Cisco Unified Communications Manager, CUBE, and audio and videoconferences in a single-site voice and video network. Obtain the skills to implement Cisco Unified Communications Manager in a modern, multisite collaboration environment. Troubleshoot complex integrated voice and video infrastructures	CCNP® Collaboration
Implementing Cisco Collaboration Devices (CICD) Implementing Cisco Video Network Devices (CIVND)	Acquire a basic understanding of collaboration technologies like Cisco Call Manager and Cisco Unified Communications Manager. Learn how to evaluate requirements for video deployments, and implement Cisco Collaboration endpoints in converged Cisco infrastructures.	CCNA® Collaboration

For more details, please visit: http://learningnetwork.cisco.com
Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
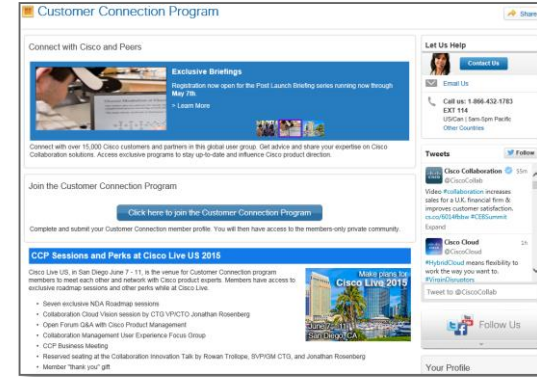
Cisco Customer Connection Program
Connect with Cisco & Peers

17,000+ Members

- Influence Collaboration **product direction**

- Access to **early adopter & beta trials**

- Contribute to **advisory groups**

- Monthly technical & roadmap briefings

- Exclusive **perks at Cisco Live**
  - Collaboration Cloud Fusion: Vision & Architecture (speaker: Jonathan Rosenberg, VP/CTO CTG)
  - 5 NDA Roadmap Sessions + Microsoft Interop
  - Q&A Open Forum with Product Management
  - Reserved seats at *Work Human* Innovation Talk (Wed. 3:30 – 4:30)

Visit the Customer Connection Program - Collaboration zone in the Cisco Campus
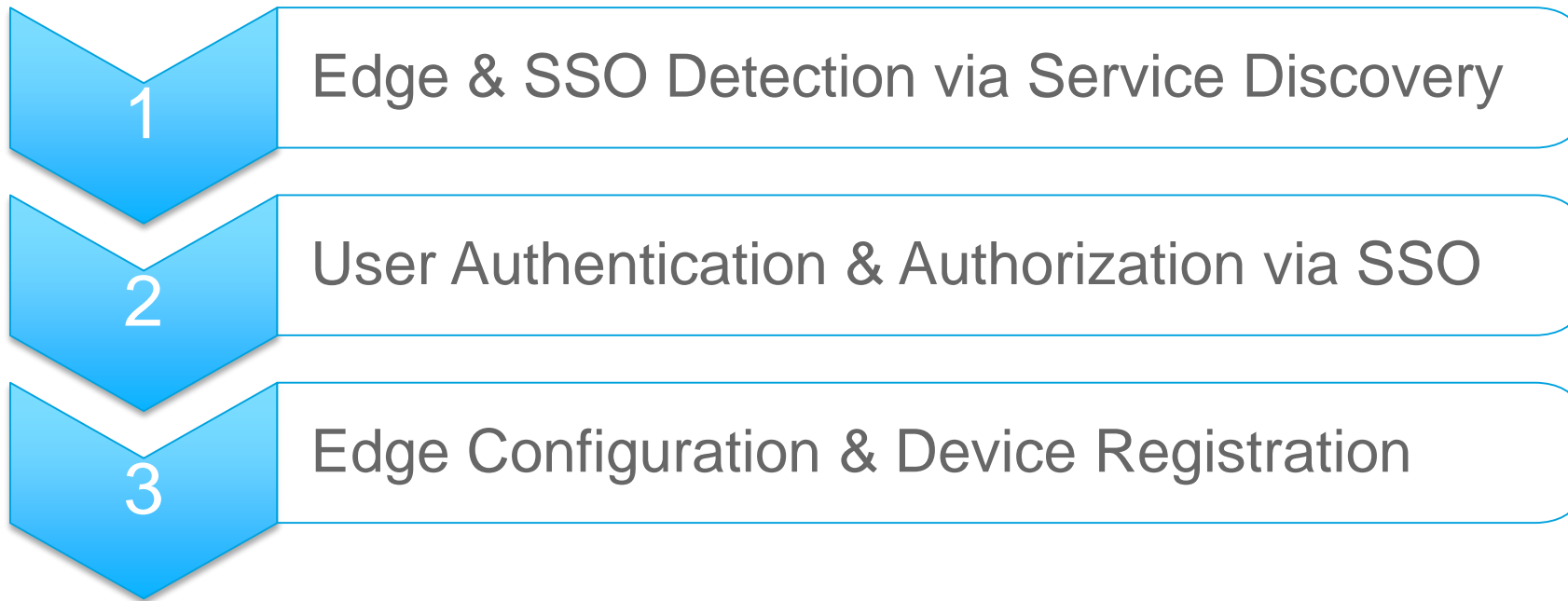
➤ Join the Customer Connection program
➤ Explore the Collaboration community
➤ New CCP members get a thank-you gift

Cisco *live!*

Thank you

Cisco *live!*

Appendix

Jabber SSO Flow over Expressway Summary

1 Edge & SSO Detection via Service Discovery

2 User Authentication & Authorization via SSO

3 Edge Configuration & Device Registration

Edge Detection & SSO Check

Jabber   **DNS**   **IdP**   **Exp-E**   **Exp-C**   **UDS**   **Authz**   **UCM**

Web

1. Determine if outside

2. Ask if SSO is enabled

3. Find home cluster

4. Find if SSO is enabled

5. SSO is enabled; where to send authorization request
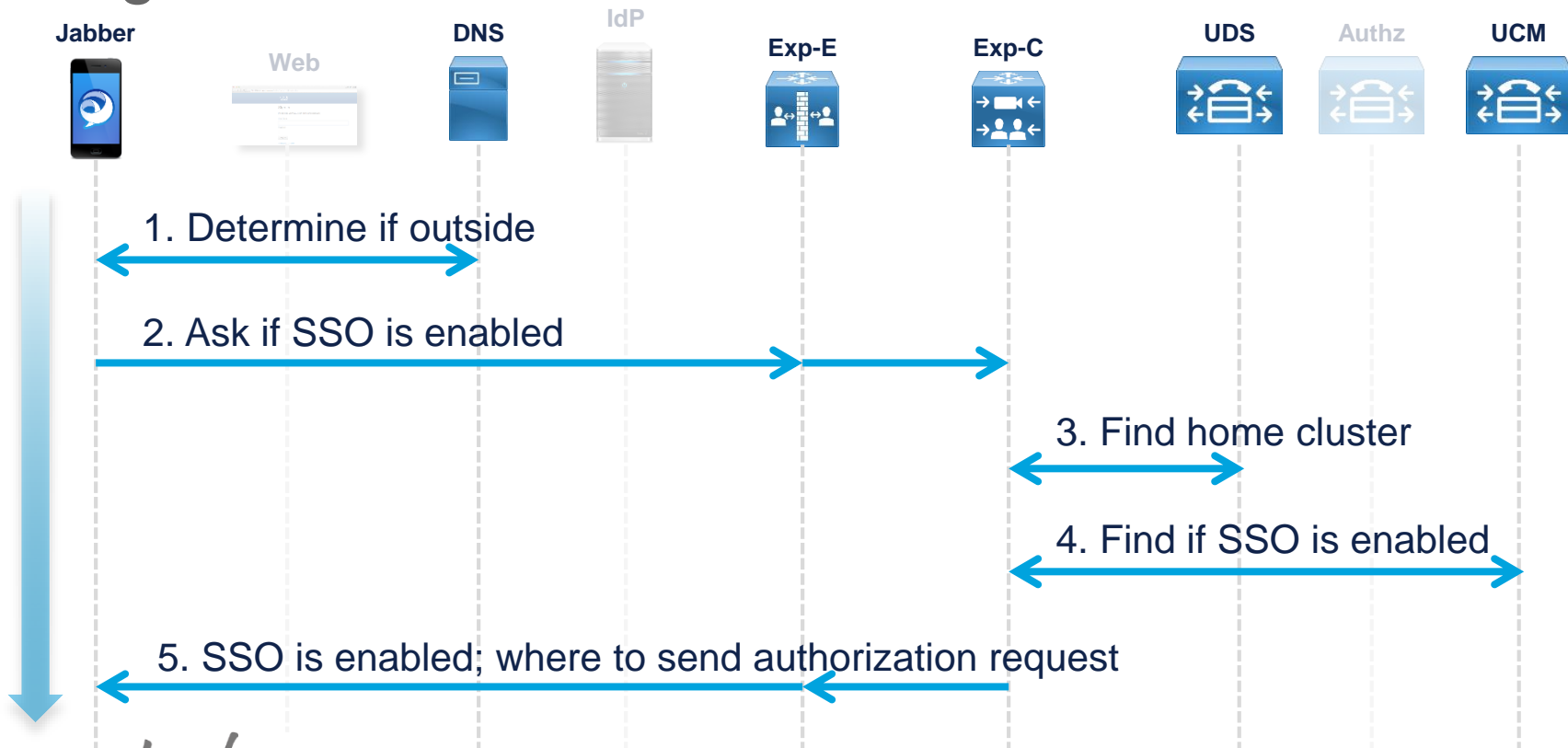
Authenticated & Authorized via SSO

Jabber   Web   DNS   IdP   Exp-E   Exp-C   UDS   Authz   UCM

1. Request for authorization

2. Redirected to IdP with SAML Request

3. Authenticated & get SAML Assertion

4. Ask for access token with SAML Assertion

5. Swap SAML Assertion with access token

6. Jabber gets access token
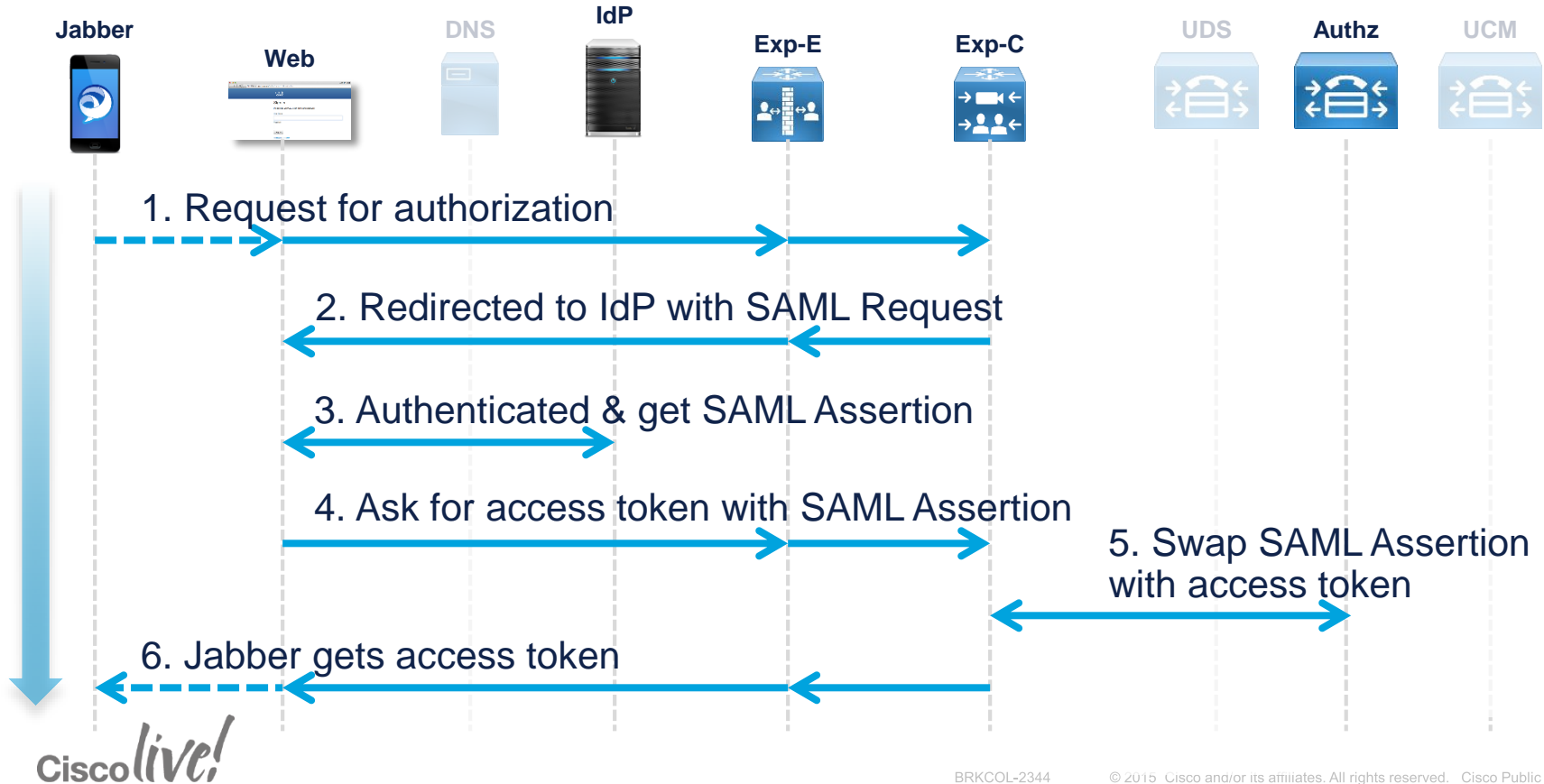
Getting Edge Configuration & Registering Device

Jabber   **Web**   **DNS**   **IdP**   **Exp-E**   **Exp-C**   **UDS**   **Authz**   **UCM**

1. Request for edge configuration

2. Receive edge configuration

3. Request for UDS access to get device data

4. Validate token

5. Receive device data
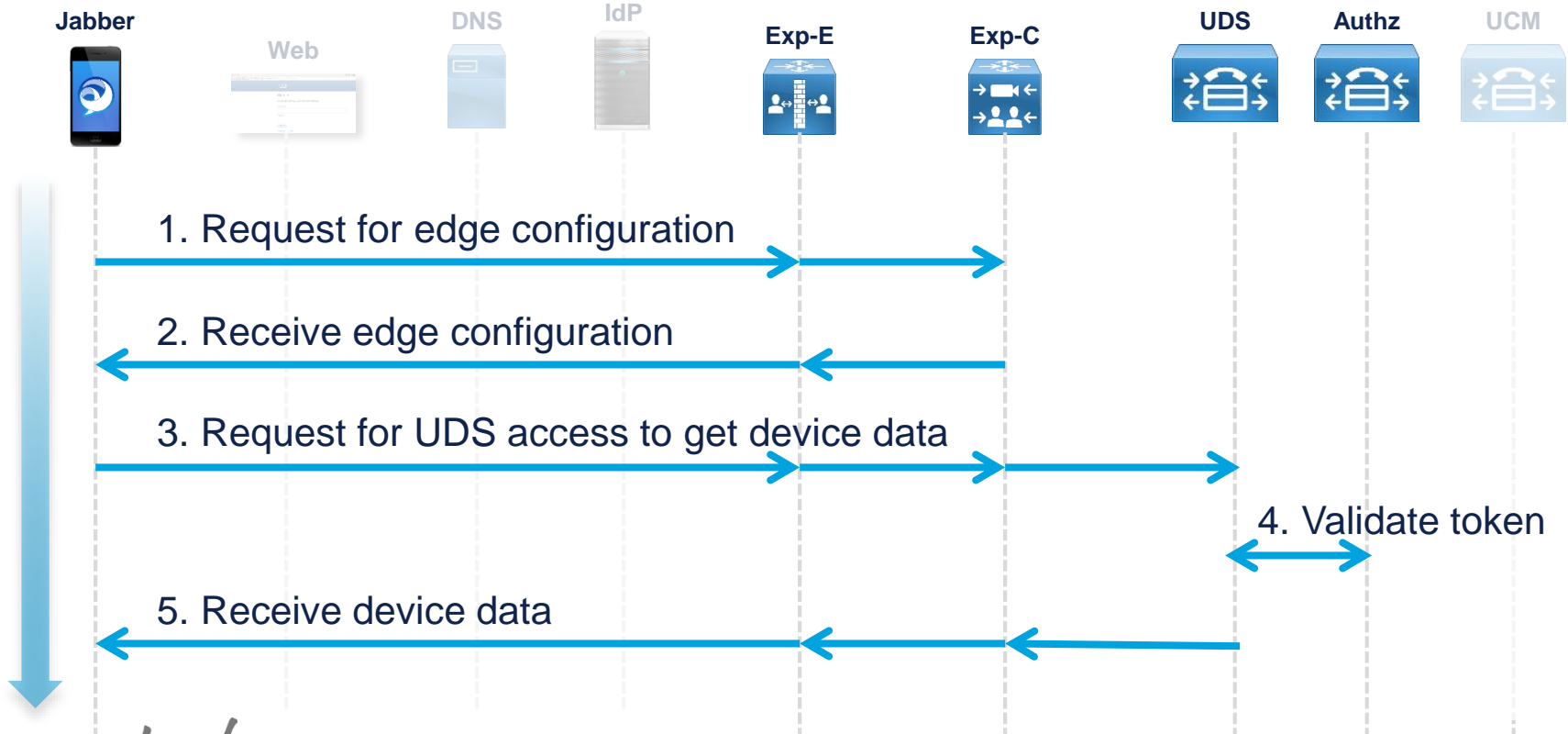
Requirements for SAMLv2 SSO

- Cisco Jabber 10.5 or higher*

- 3rd Party Identity Providers
  - Microsoft AD Federation Services 2.0
  - OpenAM 10.1
  - Ping Federate 6.10.0.4

- On-Premises UC Services
  - Unified CM & IM and Presence 10.5*
  - Unity Connection 10.5*
  - WebEx Meeting Server 2.5

- WebEx Cloud Services
  - WebEx Messenger Service
  - WebEx Meeting Center

- The following is also required:
  - NTP server
  - DNS server
  - Directory server (AD or LDAP based)

- Cisco Expressway X8.5 or higher*

> * To support SAMLv2 **SSO over Cisco Expressway**, the following is required:
> Jabber 10.6 or higher
> Unified CM & IM and Presence 10.5(2) or higher
> Cisco Expressway X8.5 or higher

Jabber File Transfer Flow with MFT Enabled

Jabber - Sender   **Jabber - Receiver**   **IM and Presence**   **External File Server**   **External Database**

1. Upload via HTTP

2. File storage

3. Audit log

4. URI of file

5. IM with URI

6. Request via HTTP

7. File retrieve

8. Audit log

9. Download via HTTP