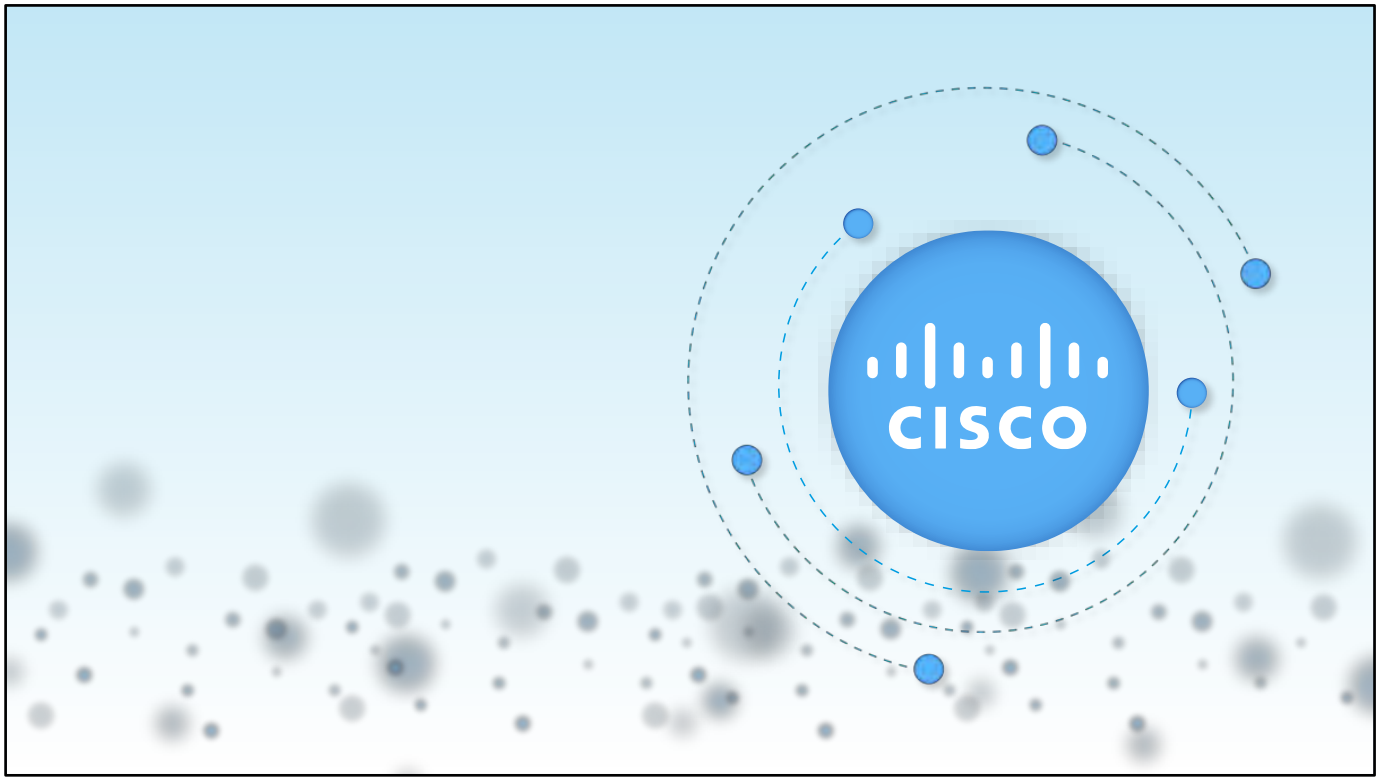
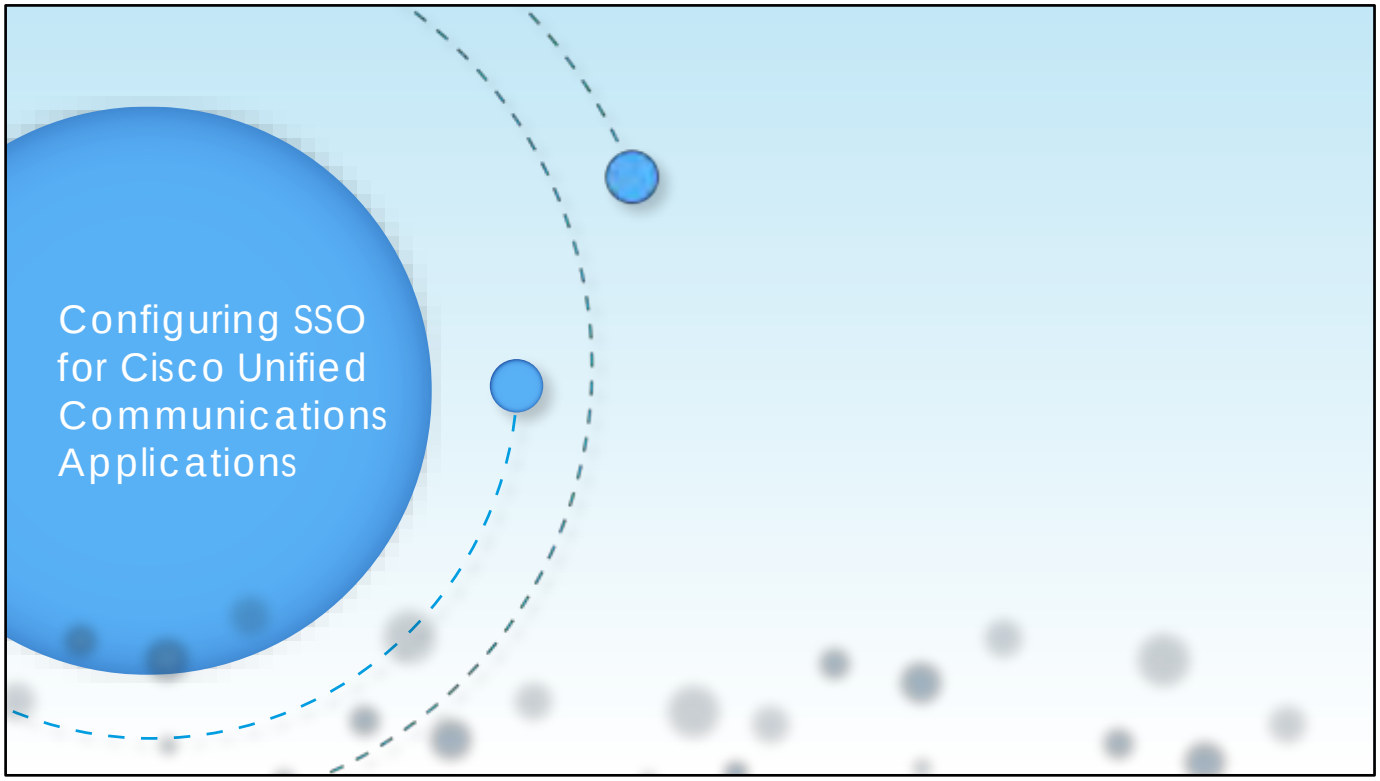
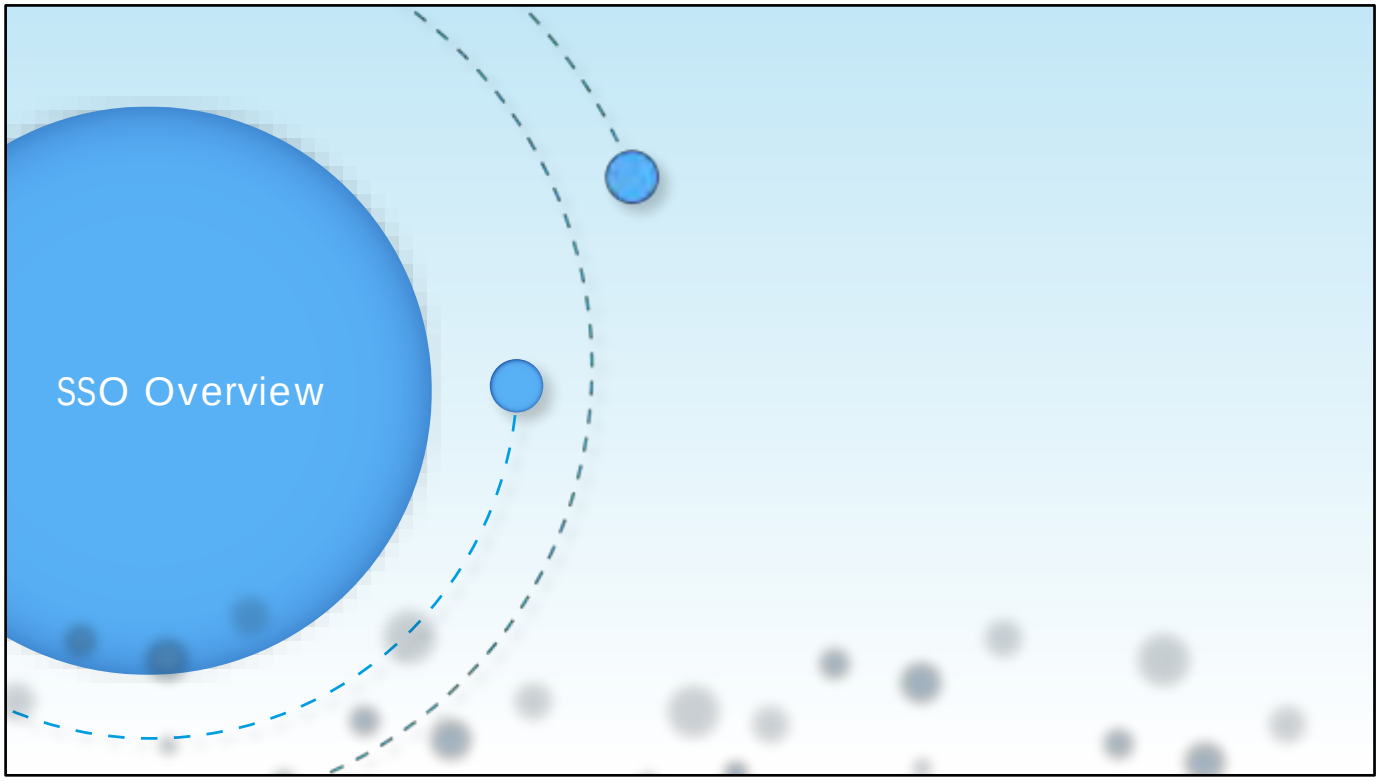
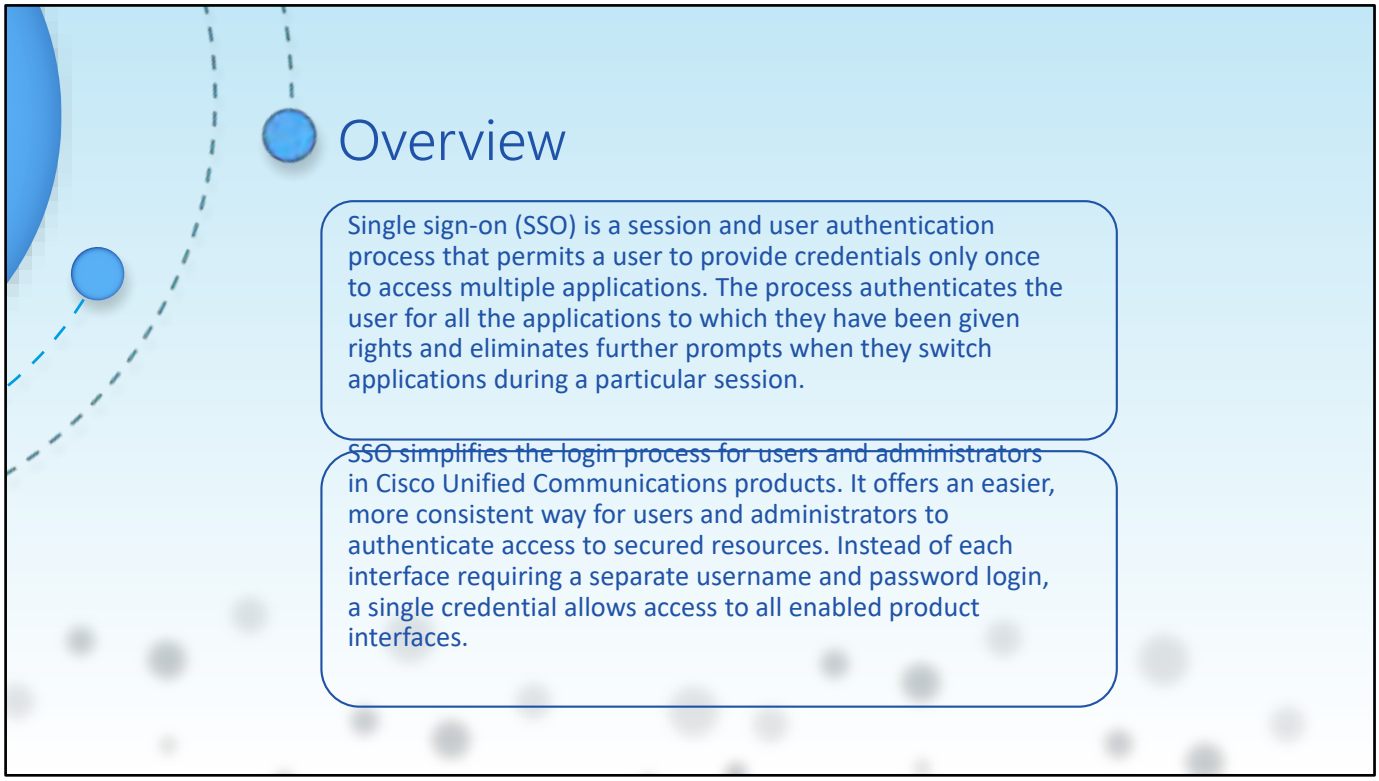
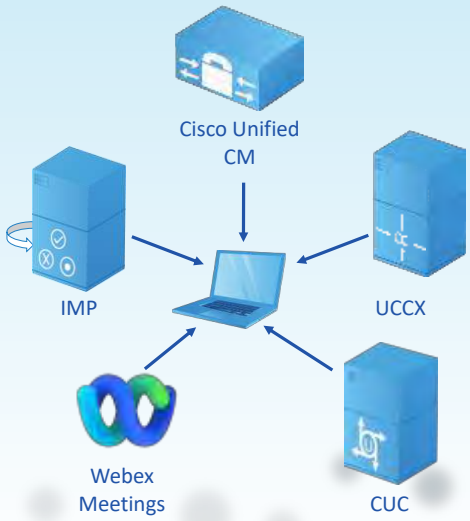




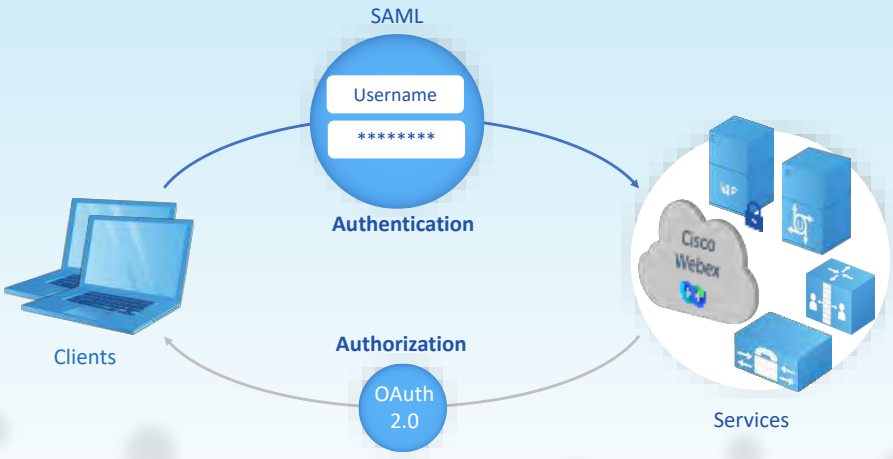




Cisco SSO Overview

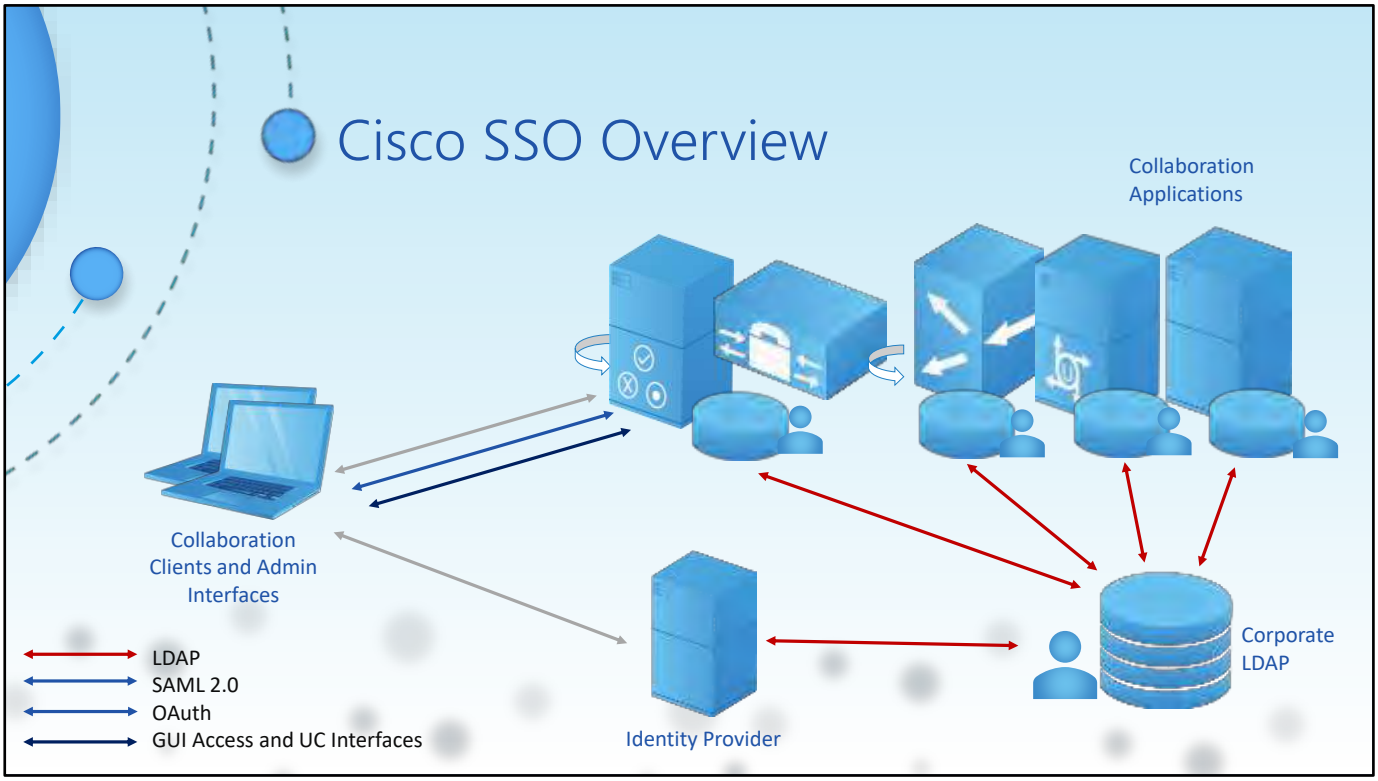


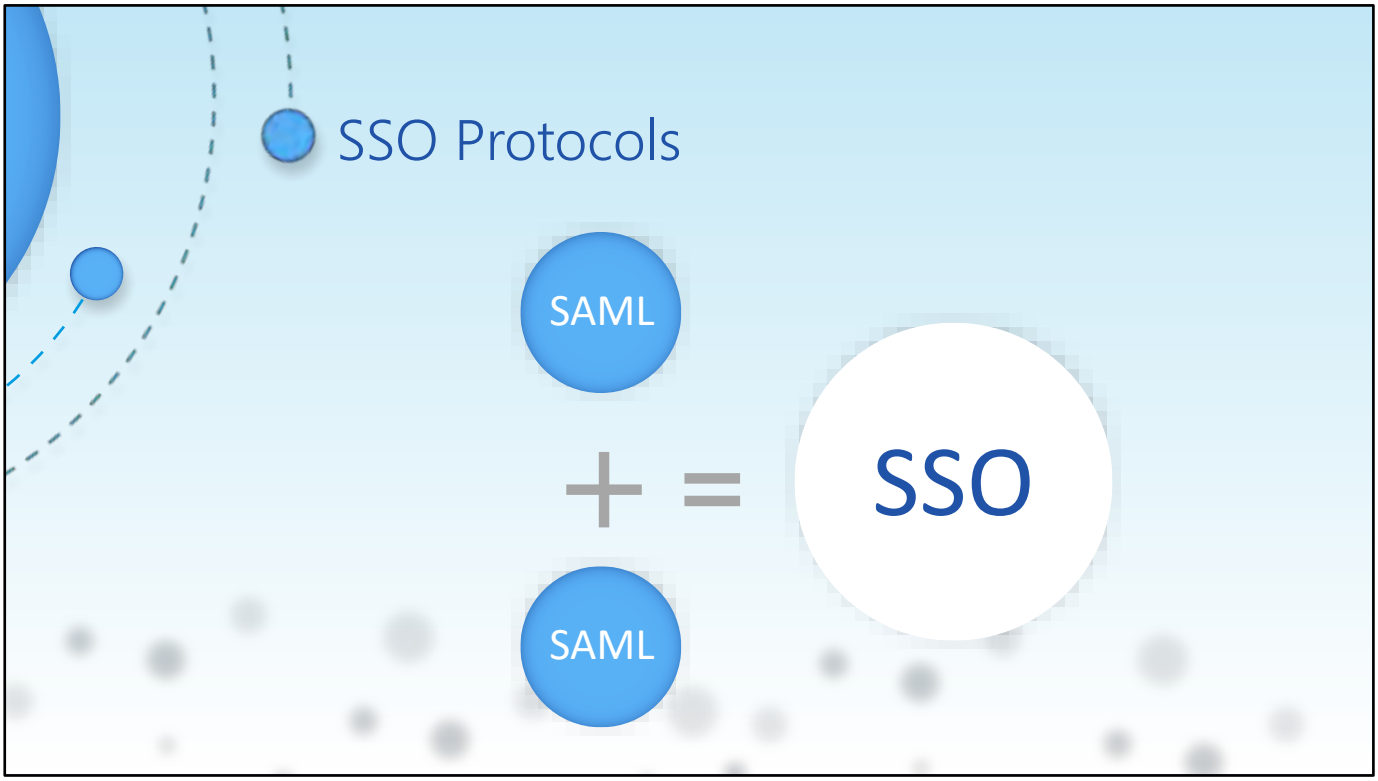
Cisco SSO Overview

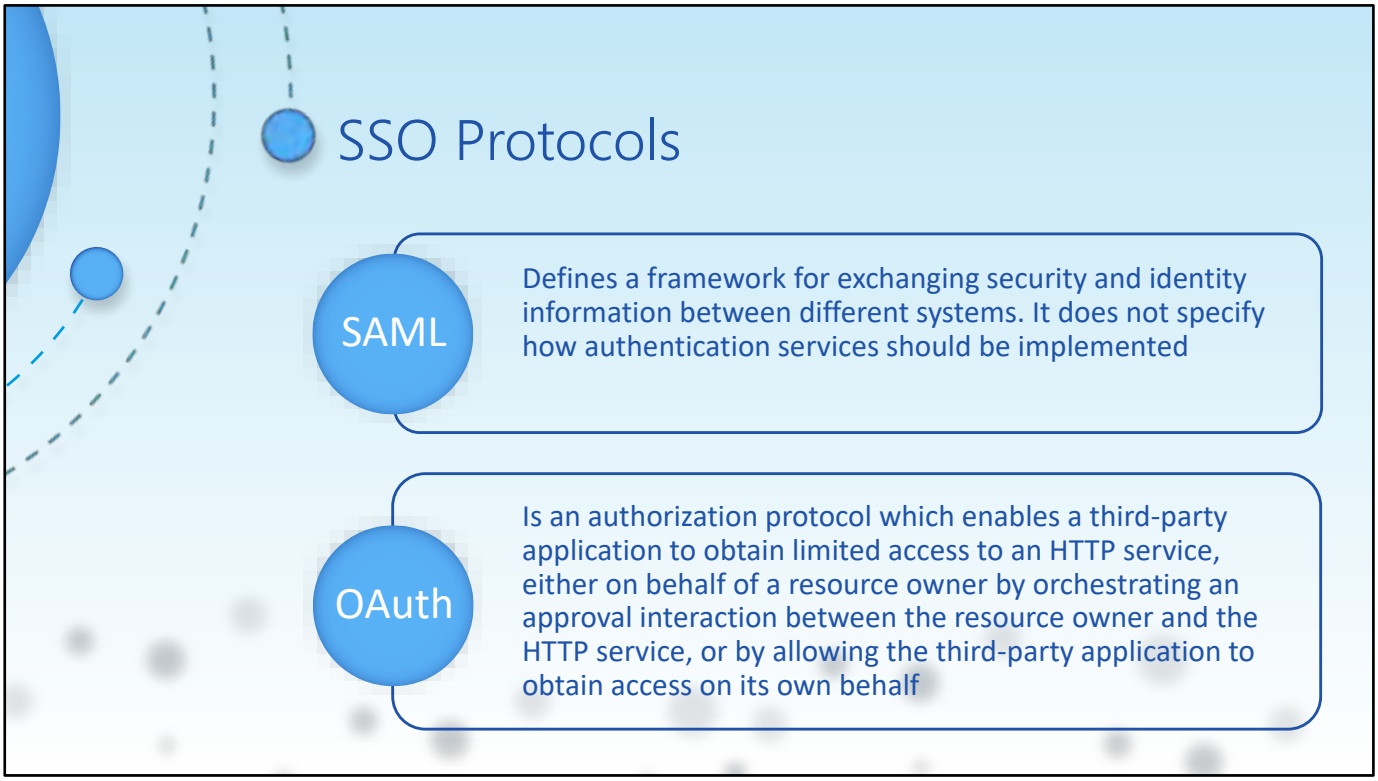


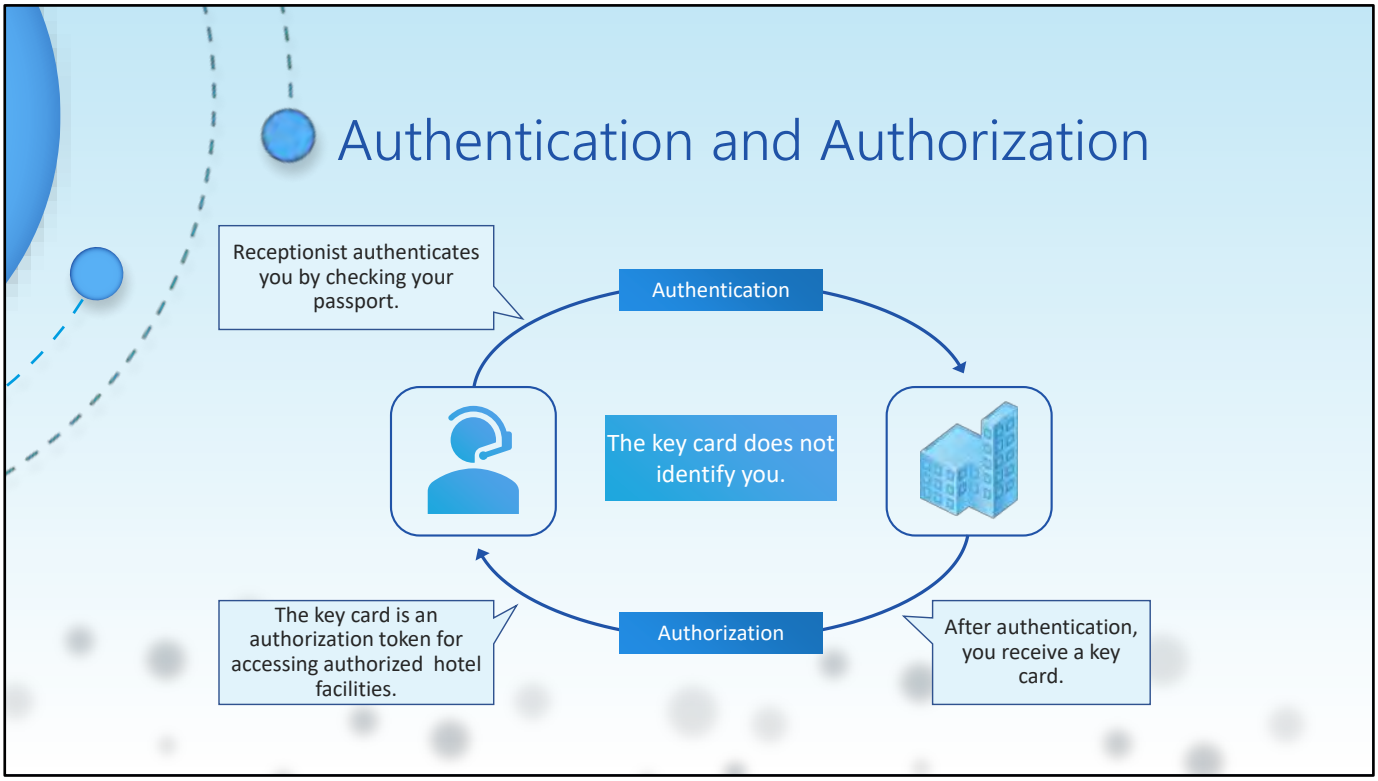
Authentication – verifies who you say you are

Authorization – verifies that you are permitted to do what you are trying to do









Authentication

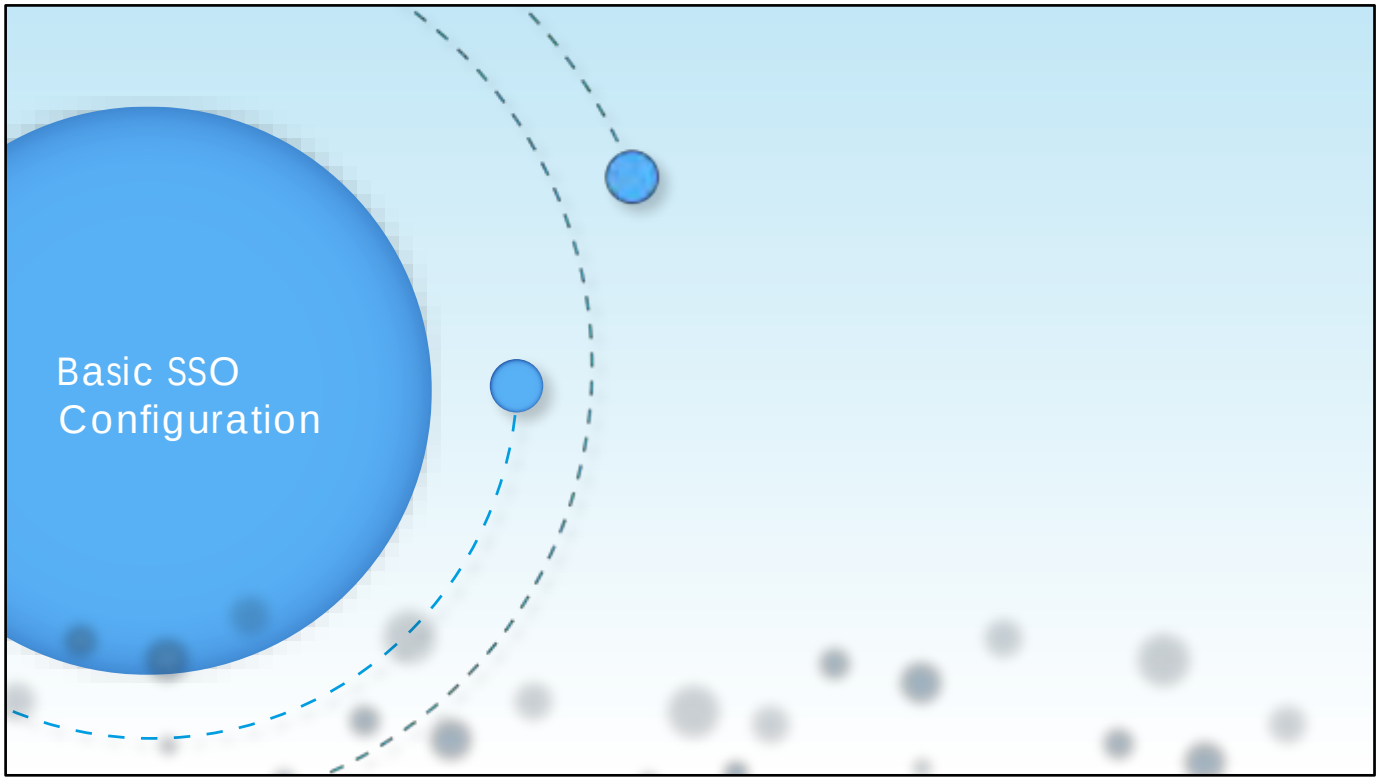
Strong authentication strengthens identity and access security by combining two or more identifiable elements:

Authentication

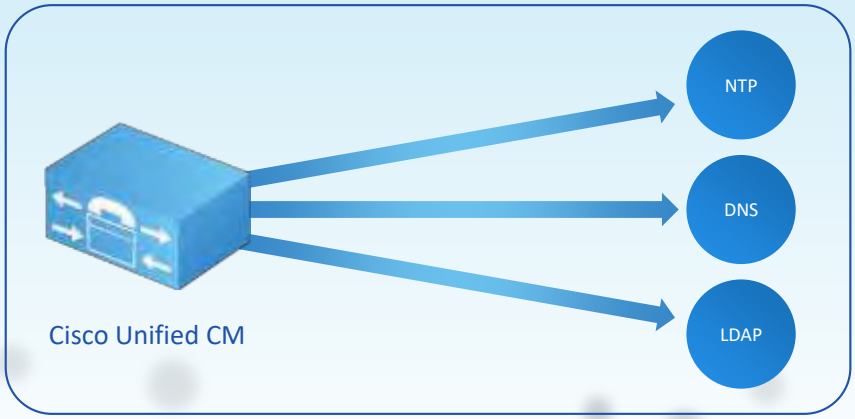
Strong authentication strengthens identity and access security by combining two or more identifiable elements:

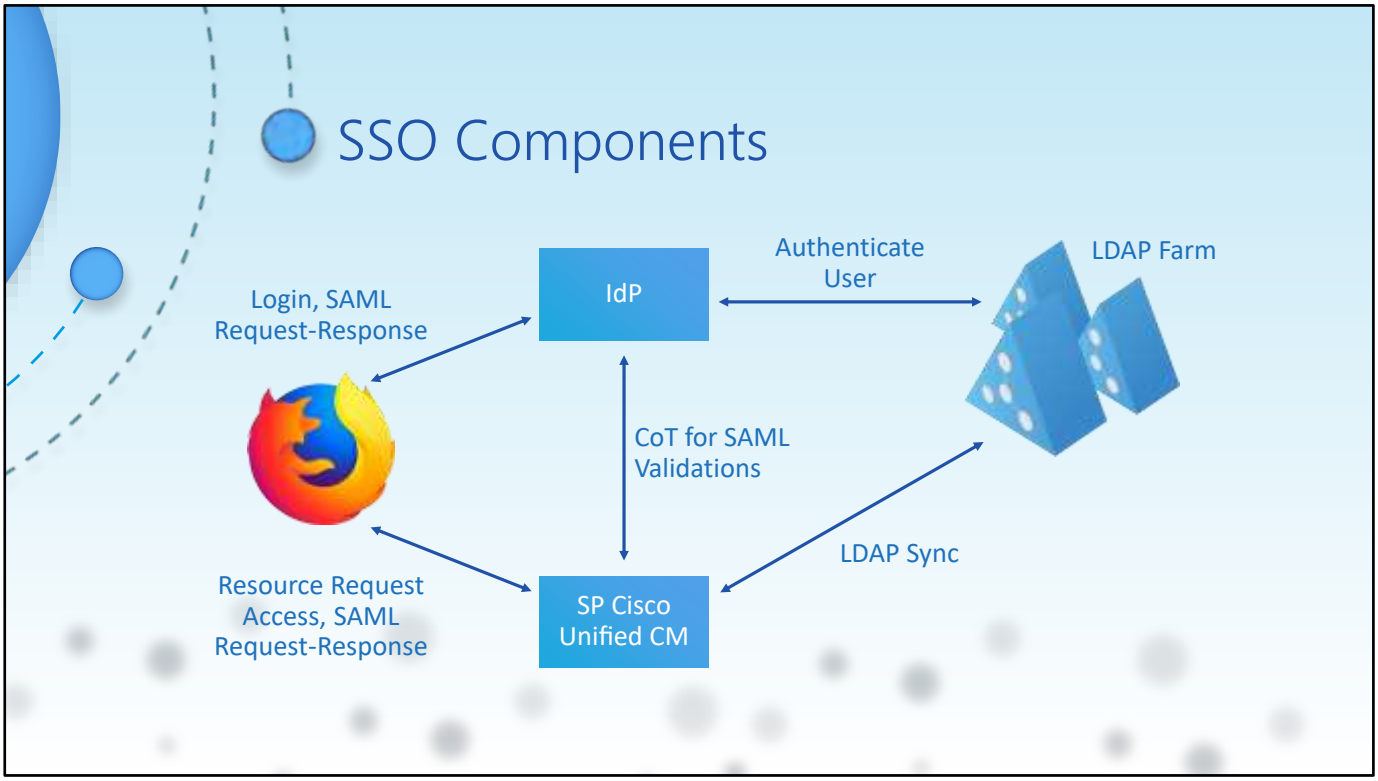
Authorization

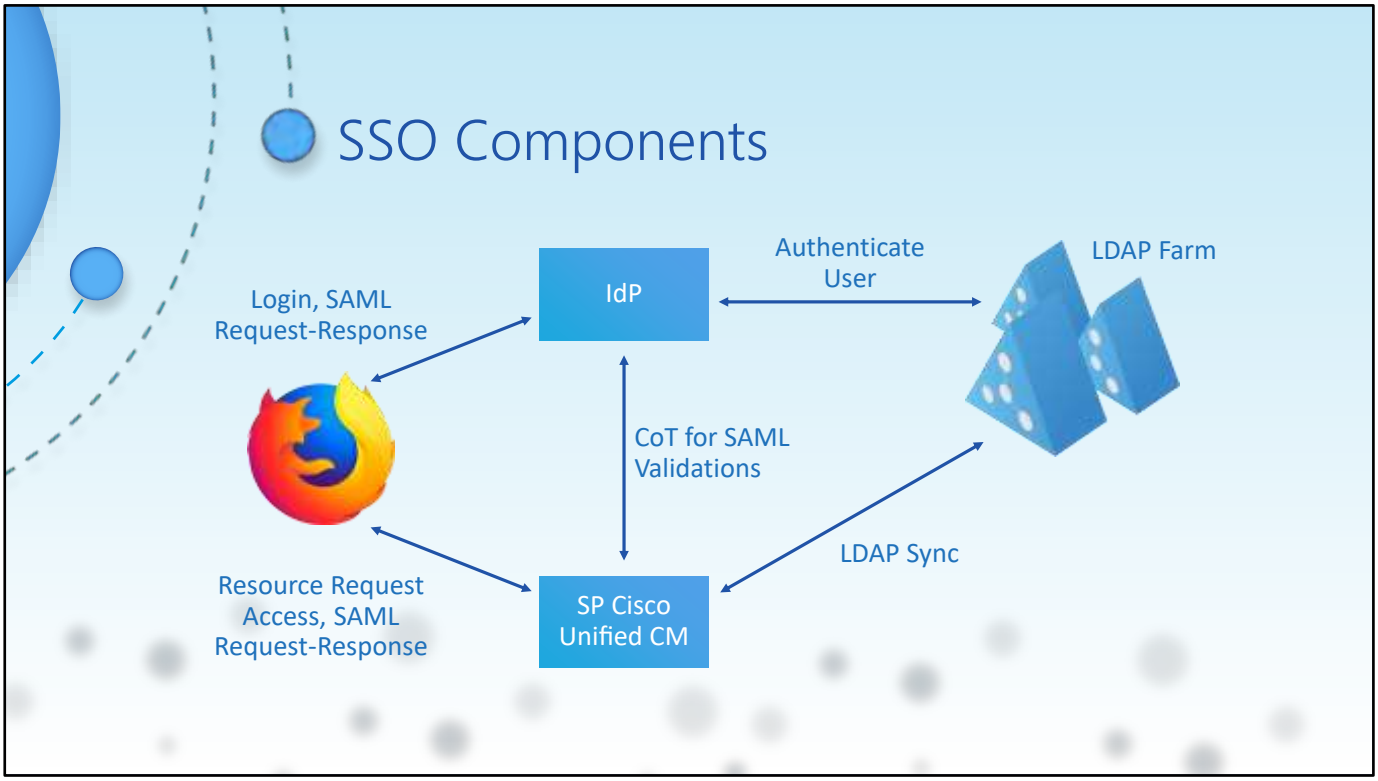
Authorization verifies that
"you are permitted to do what you are trying to do"

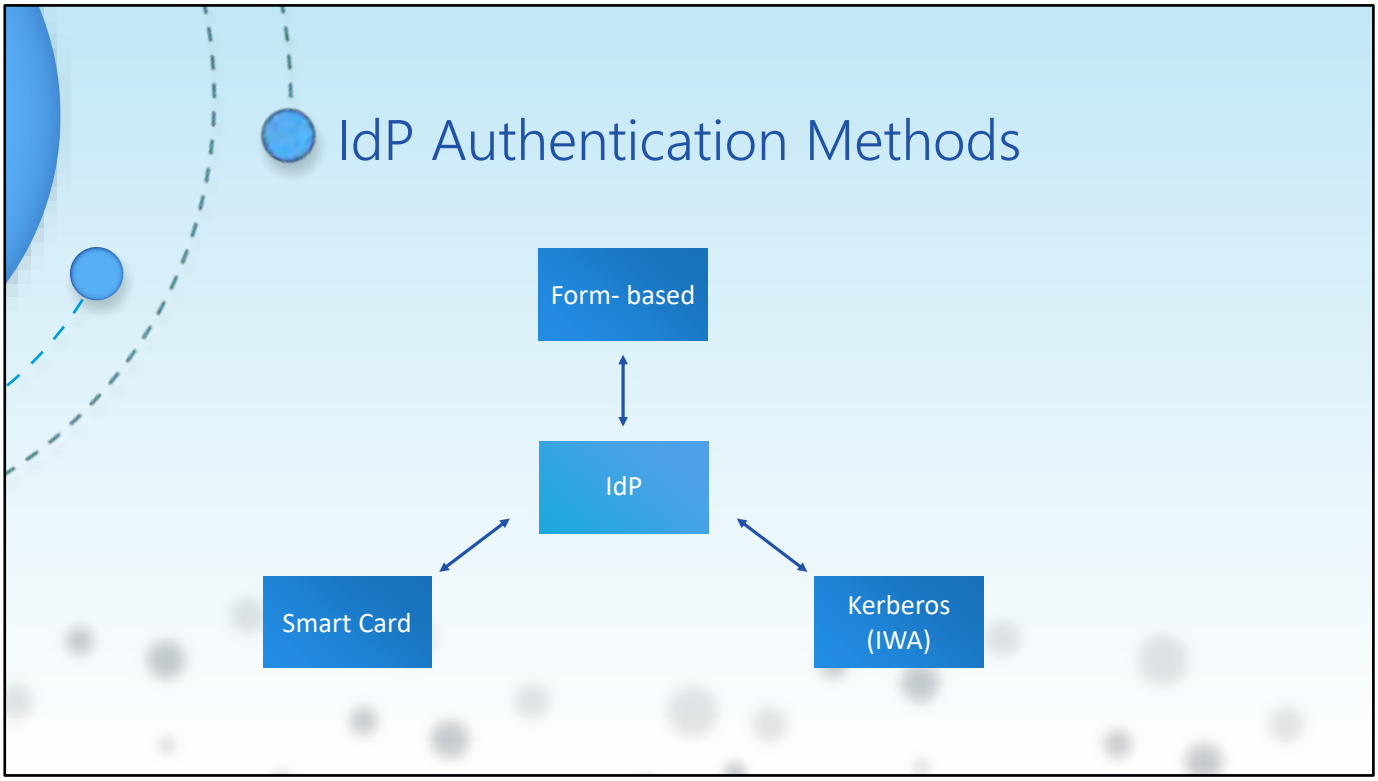


SSO Prerequisites







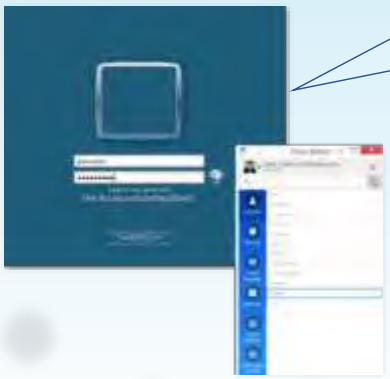


Form-Based Authentication

Cross Launch

Supported on all Devices and Operating Systems

Kerberos for IWA



Magic Credentials

Changing Active Directory credentials has no impact on the logic process

Limitations:

- Supported on Cisco Jabber for Windows, Mac, or iOs
- Not supported outside firewall
- Need to be logged into devices that are part of Active Directory domain

Smart Card Authentication

- Most secure way of providing authentication
- Two-factor authentication
- Changing Active Directory credentials has no impact on the login process.

Trust Metadata File

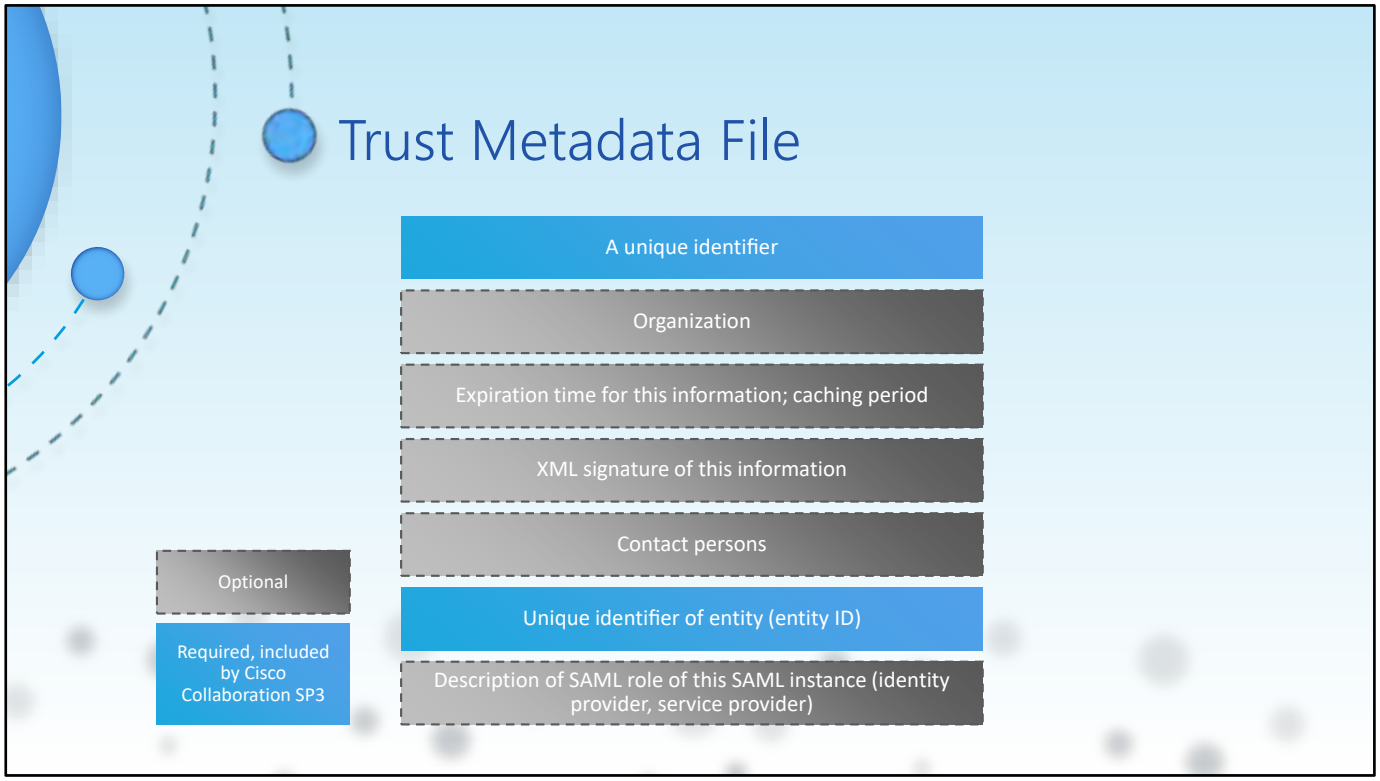
The SAML metadata standard belongs to the family of XML-based standards published by the Organization for the Advancement of Structured Information Standards (OASIS) in 2005.

Introduction to SAML Metadata

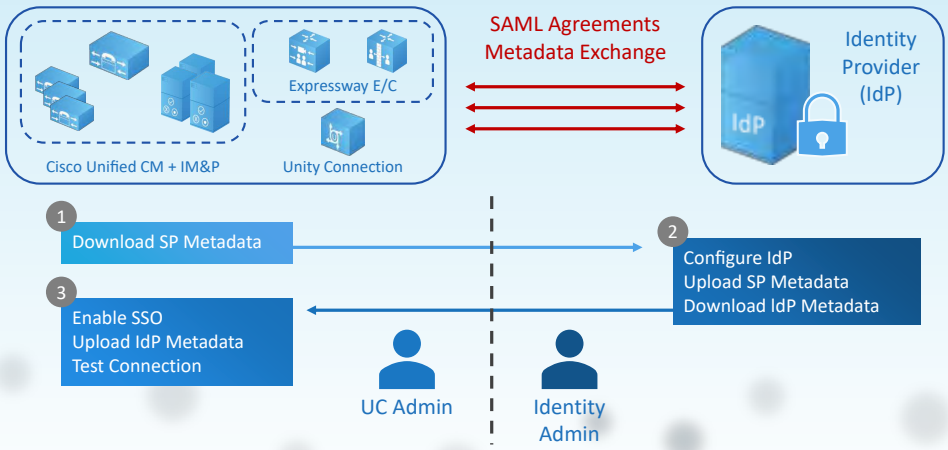
Before SAML authentication can occur, a trust relationship between the service providers and the IdP must be established. This relationship is established by exchanging metadata between the service providers and the IdP.

To securely interoperate, partners share metadata in whatever form and by whatever means possible.

Trust Metadata File



Metadata Exchange



Step 1: Download SP Metadata

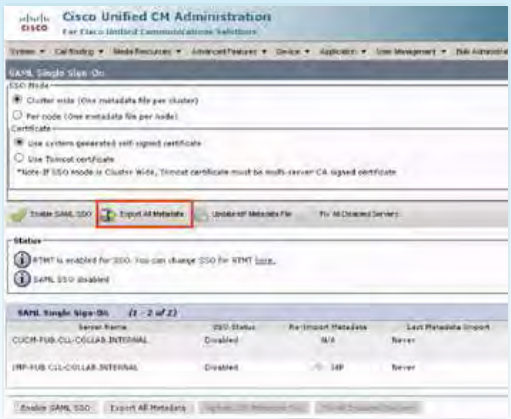
An example is shown for Cisco Unified CM

Download **<hostname>- single-agreement.xml**

SP Medatada contains:

- ID, entityID
- AuthnRequestSigned
- WantAssertionsSigned
- Encryption key and signing key
- nameIDFormat
- AssertionConsumerService

UC Admin



Step 1: Download SP Metadata

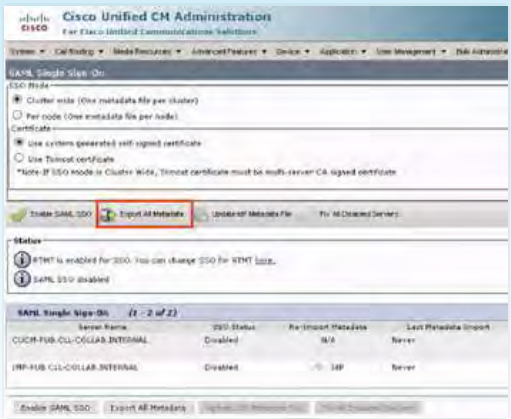
An example is shown for Cisco Unified CM

Download **<hostname>- single-agreement.xml**

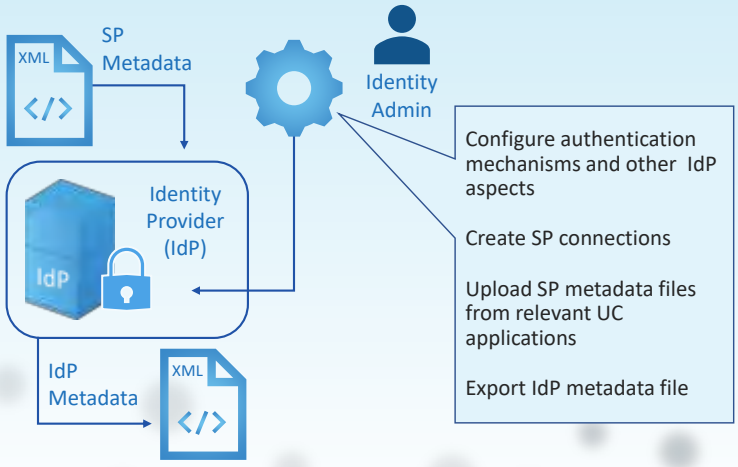
SP Medatada contains:

- ID, entityID
- AuthnRequestSigned
- WantAssertionsSigned
- Encryption key and signing key
- nameIDFormat
- AssertionConsumerService

UC Admin



Step 2: Configure the IdP

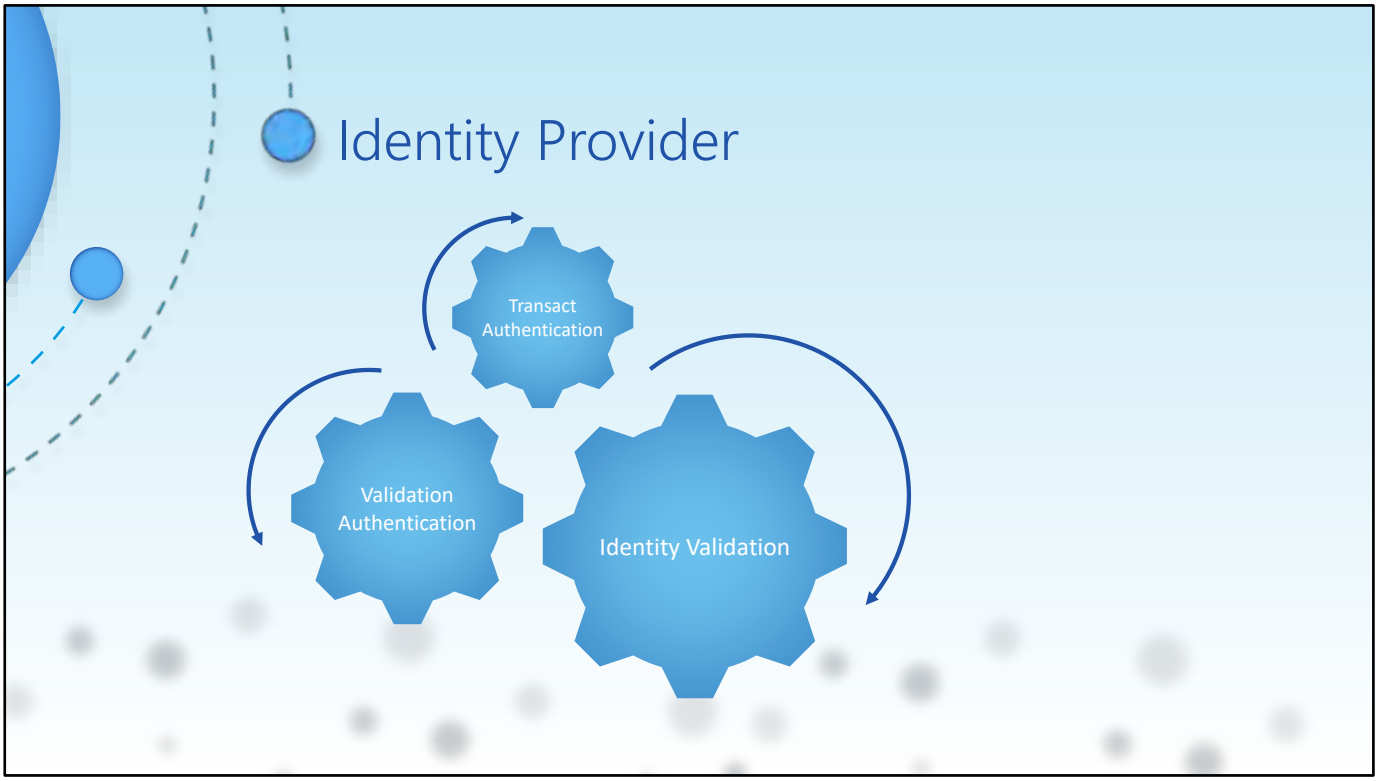


Step 3: Upload the IdP Metadata

Cisco Expressway

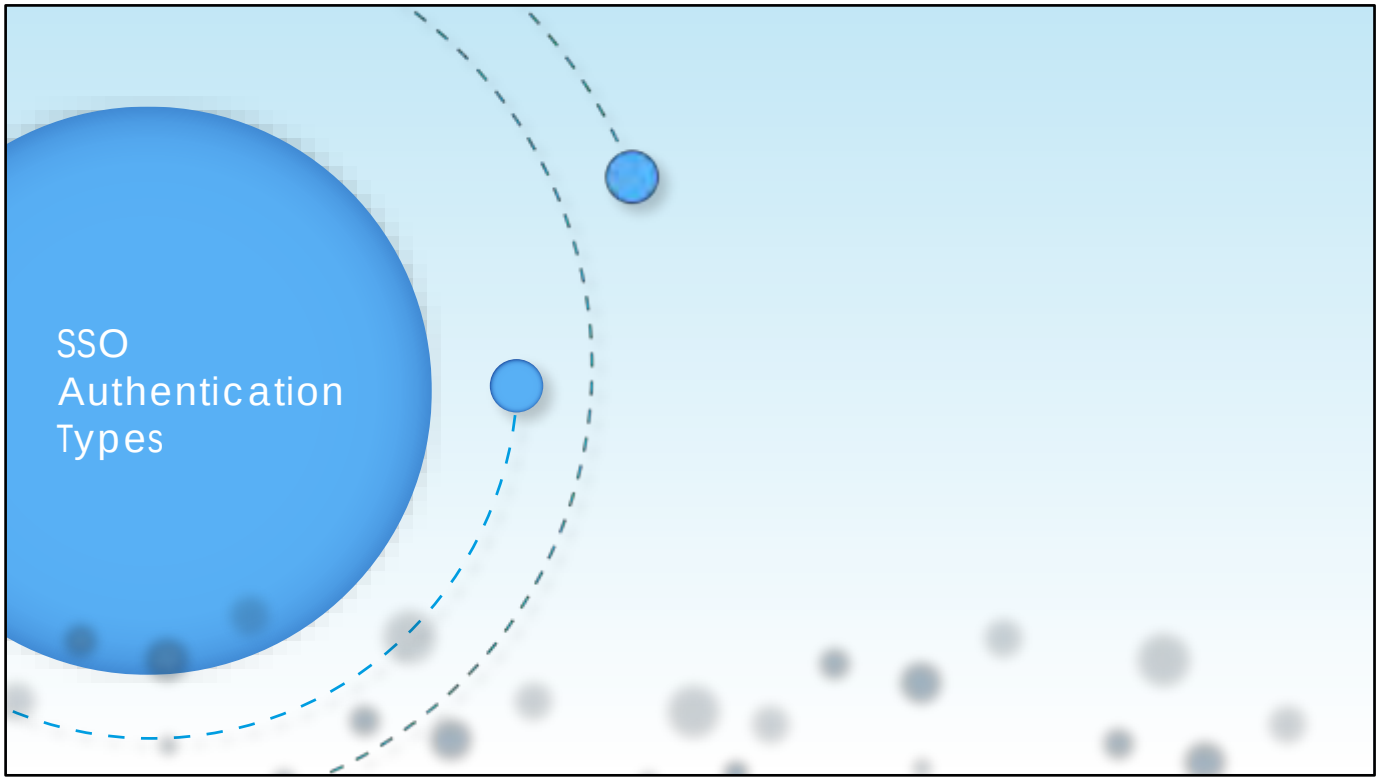
Cisco Unified CM

Cisco Webex

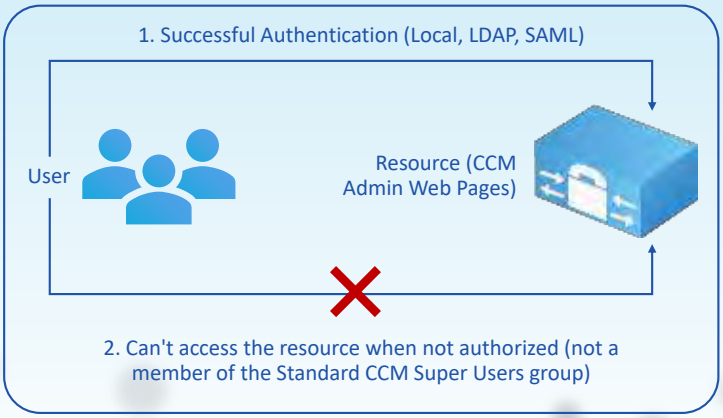


IdPs Supported by Cisco

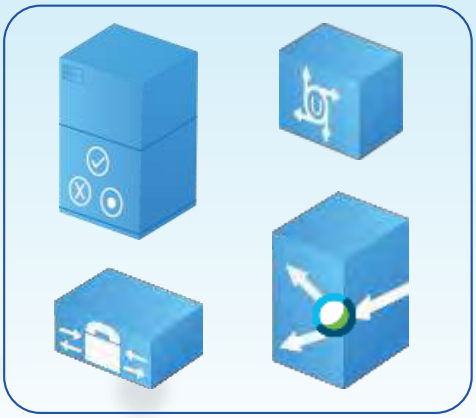
The IdP can be any IdP that is available on the market that complies with the SAML 2.0 specification



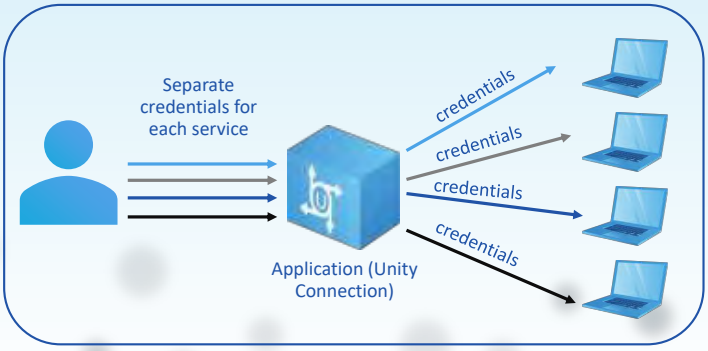
OAuth



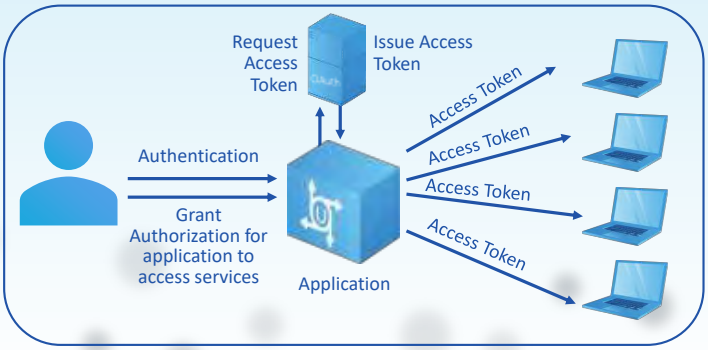
OAuth



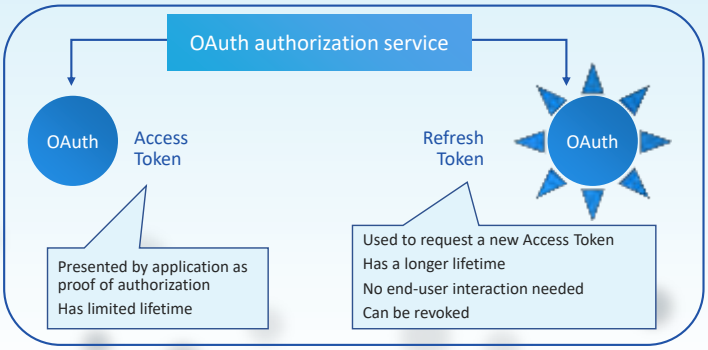
OAuth 2.0 Overview

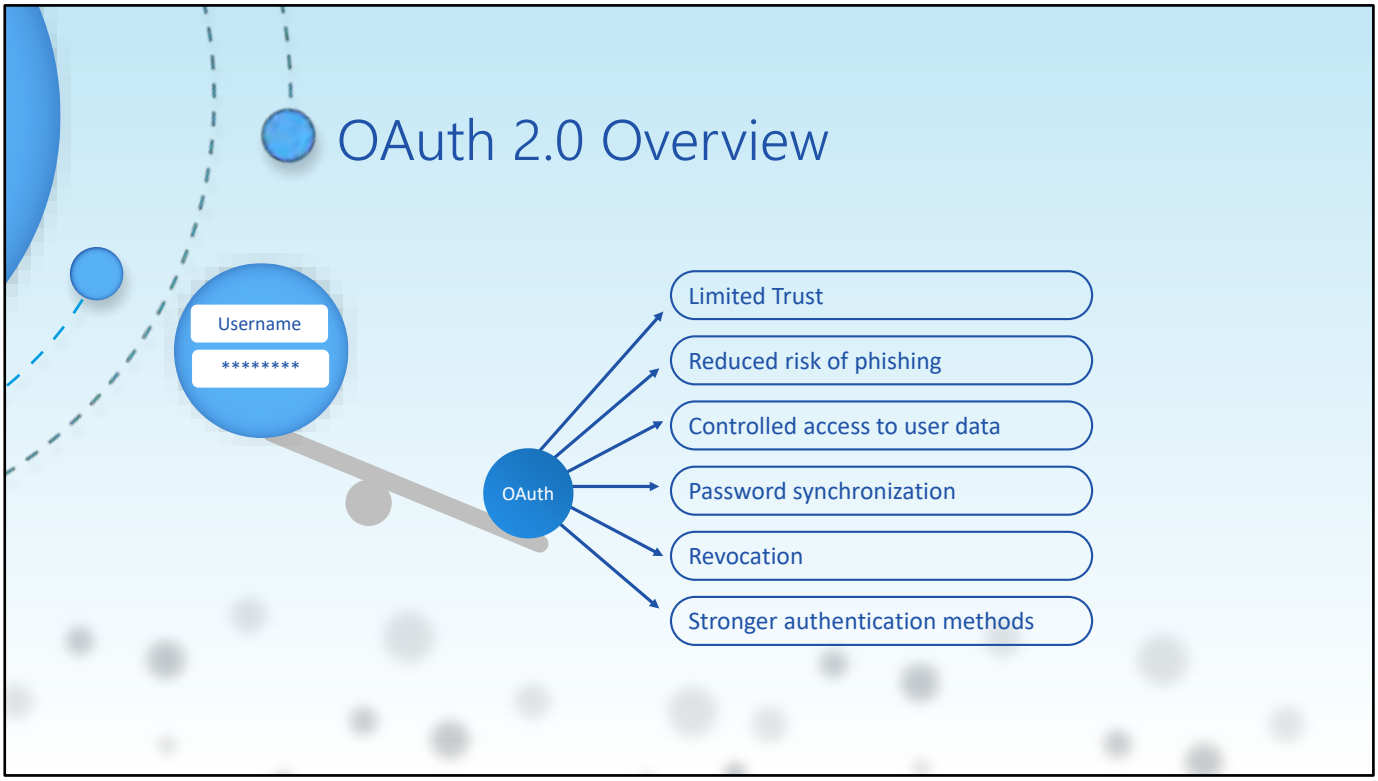


OAuth 2.0 Overview

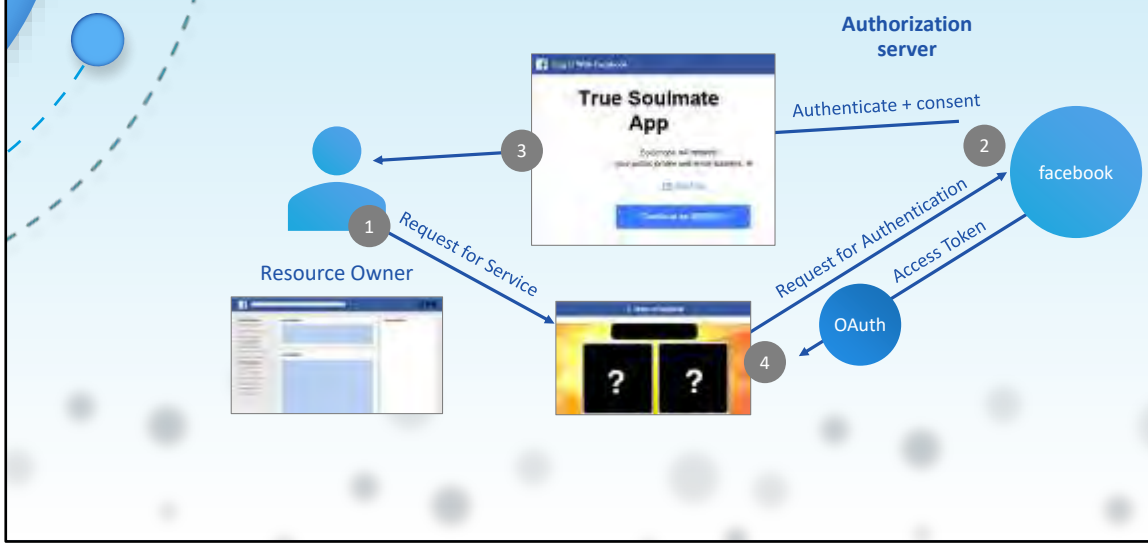


OAuth 2.0 Overview





OAuth 2.0 Overview



OAuth 2.0 Overview

OAuth is commonly used by various services on the Internet. Instead of building authorization logic into their own web applications, some services delegate responsibility to the OAuth authorization service of sites such as Facebook, Google, and Twitter. On the main website of the service, the user clicks the icon for the OAuth authorization link with, for example, Facebook

(1). The main website (client) will then initiate the OAuth authorization flow, which in turn redirects the end-user agent (web browser) to the authorization server (for example, Facebook)

(2). The end user authenticates against the authorization server using their credentials, and the authorization prompts the user for authorization of the level of access (scope) that the client requested via the flow (for example, access to the user email address)

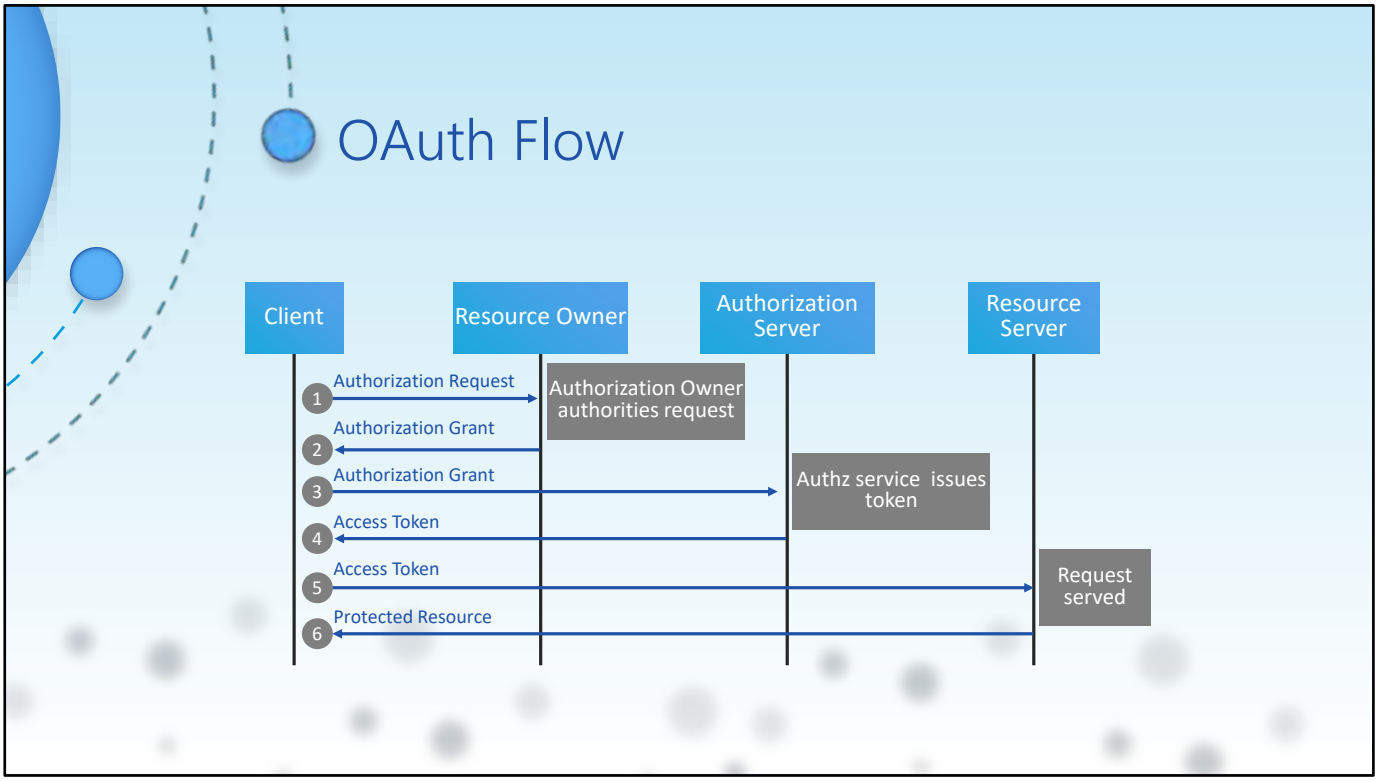
(3). When the user responds, the authorization server grants access, and an access token is issued to the client that is requesting access

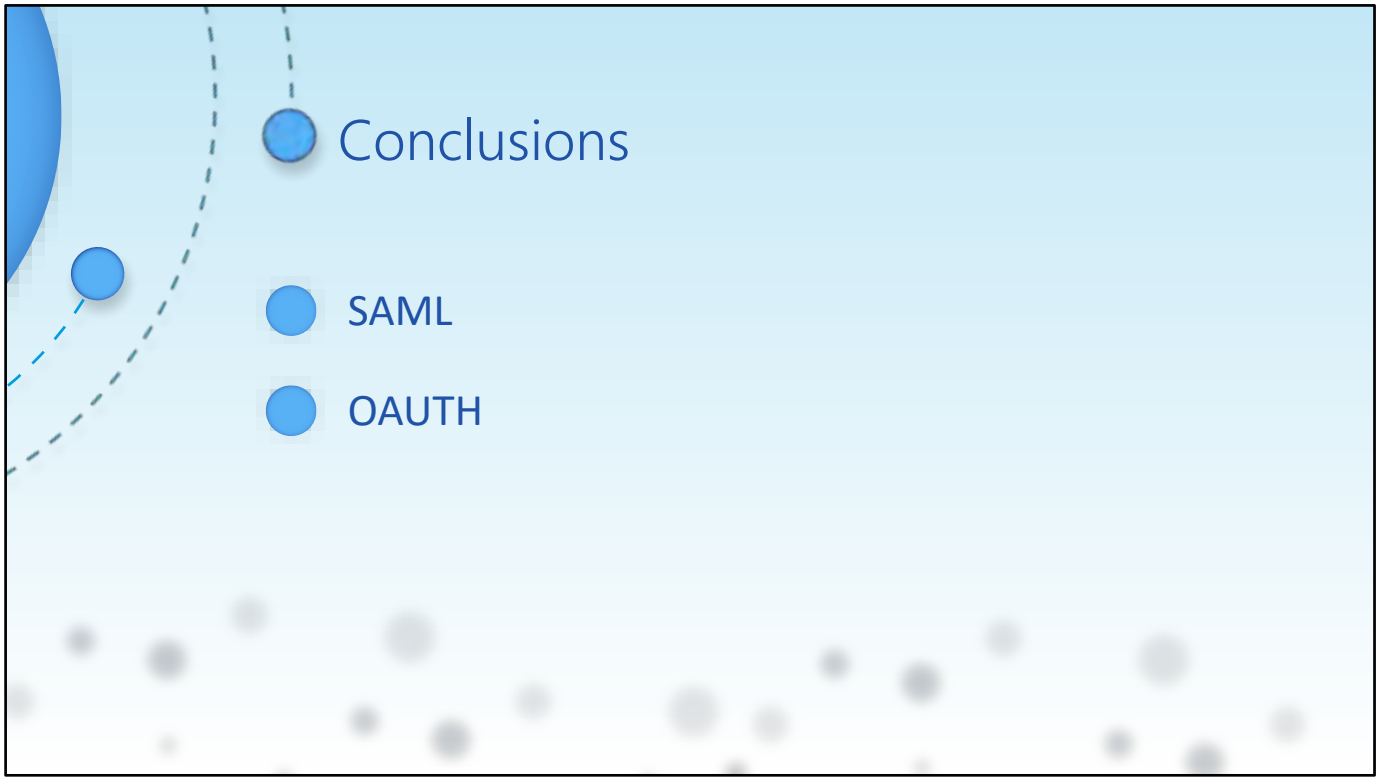
(4). The actual process by which the client obtains the access token depends on the type of OAuth authorization flow that the client uses.

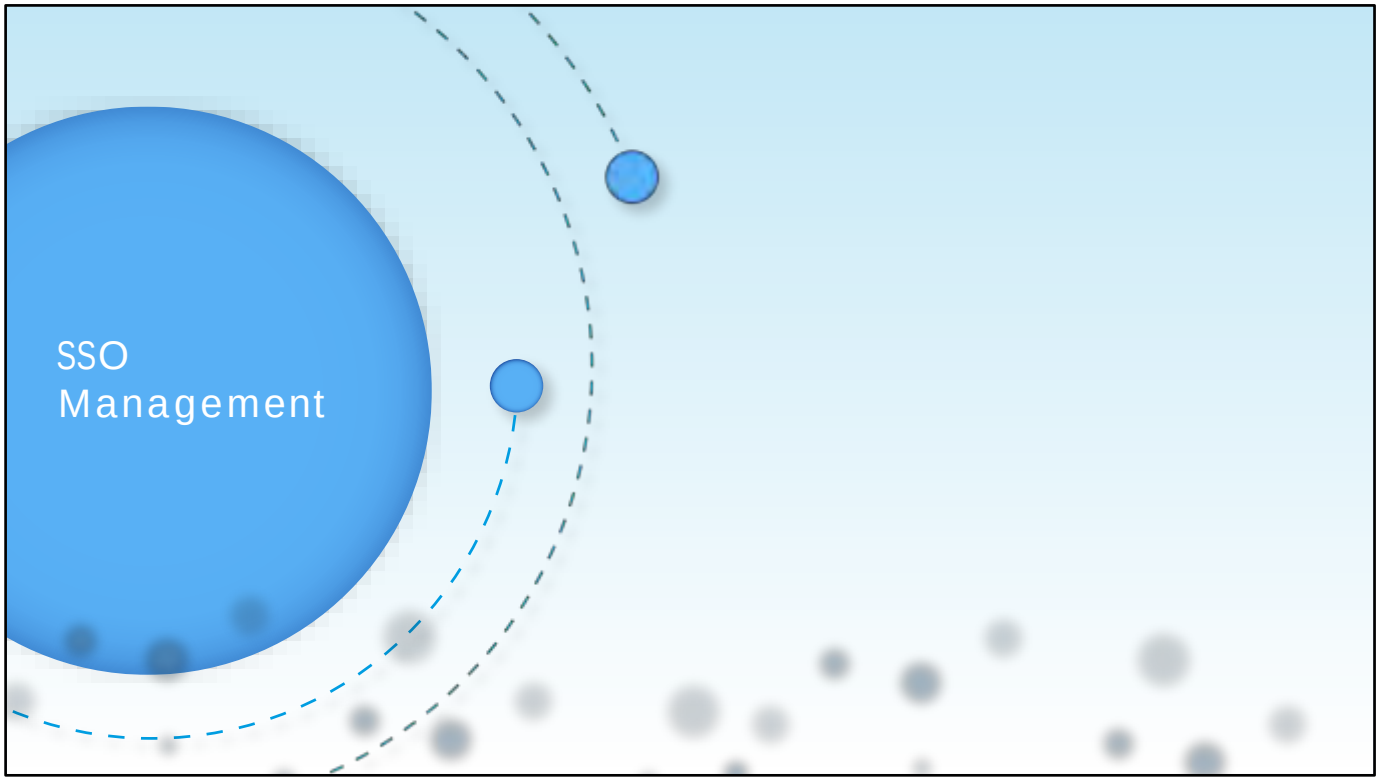
OAuth Roles

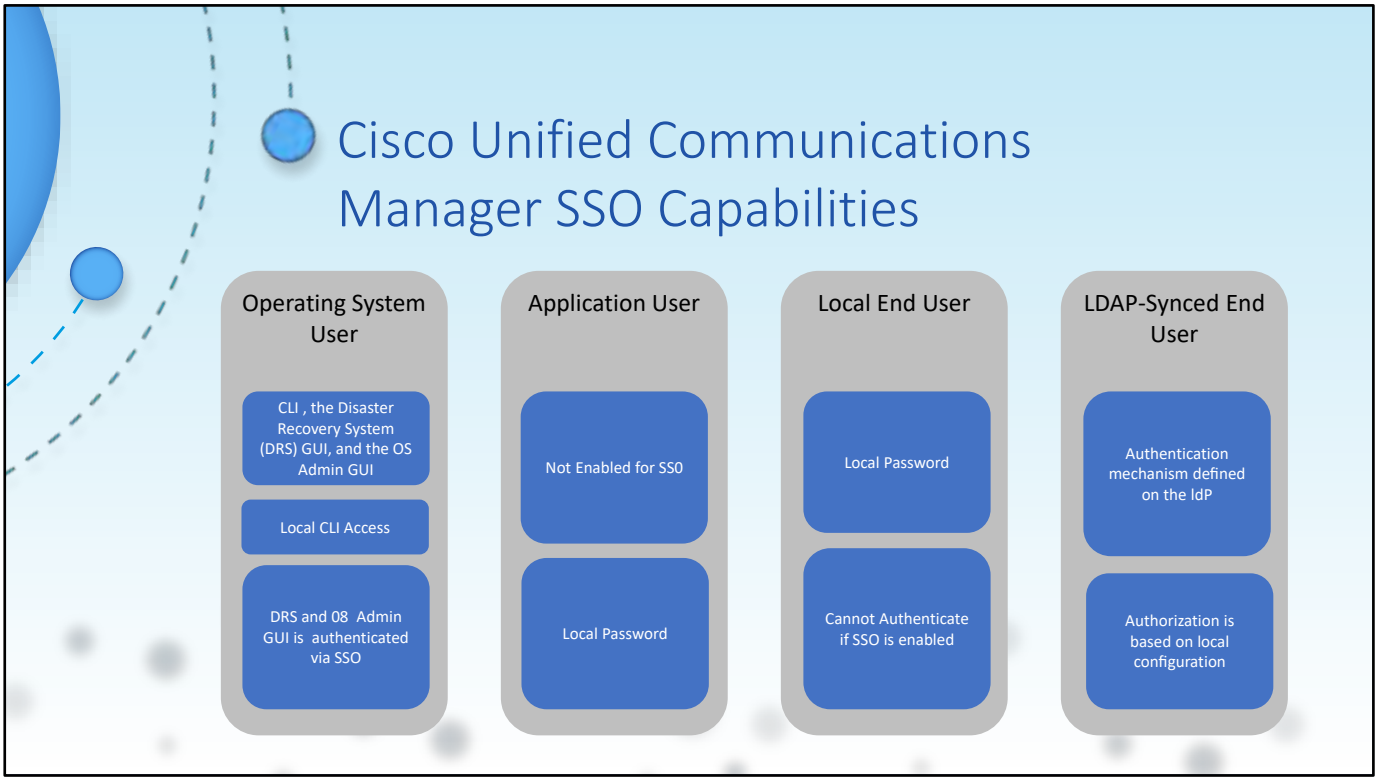
The OAuth framework has multiple components to address authorization challenges in SSO environments.

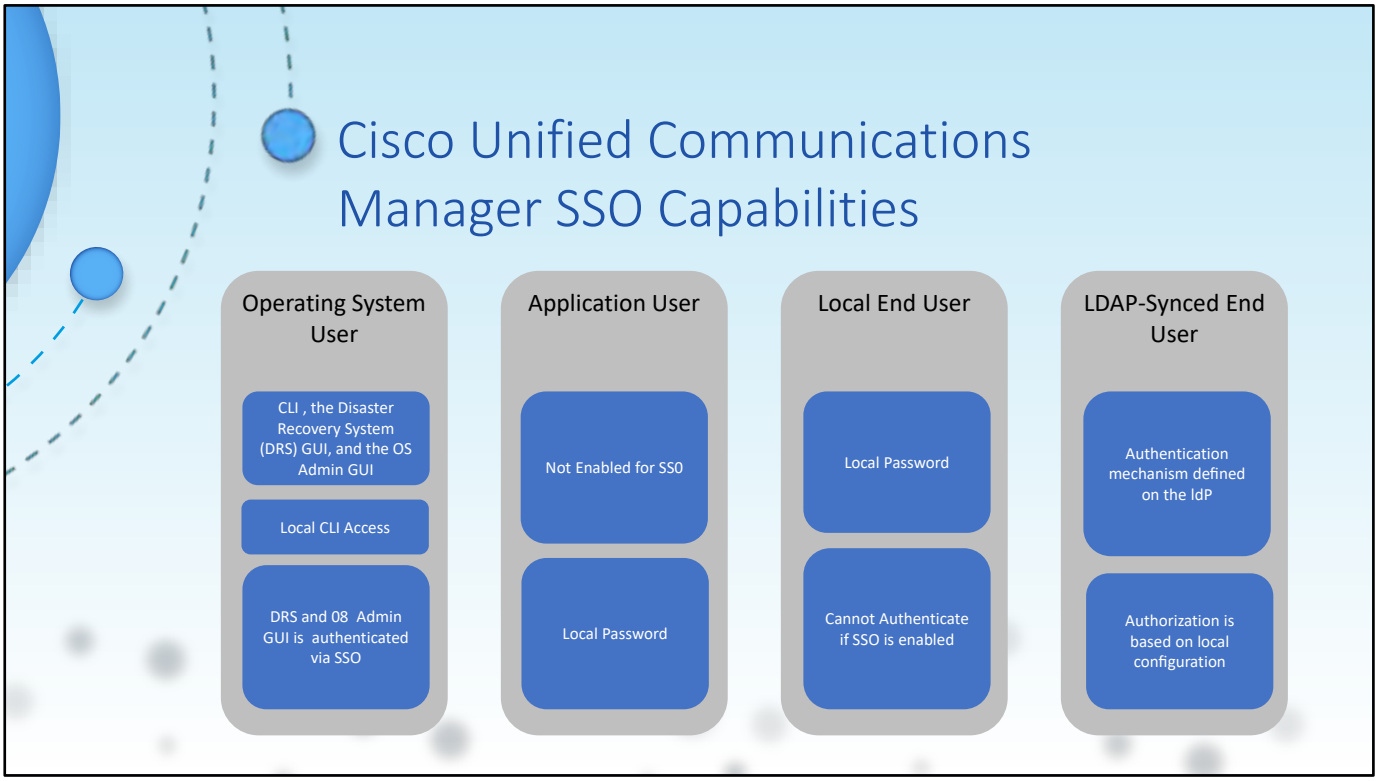
Resource Owner	Resource Server	Client	Authorization Server
End User	UDS Cisco Unity Connection VMRest And so on	Cisco Collaboration Service (e.g. Expressway- E) End User Client (e.g. Cisco Jabber) Each client has client_id	Issues Access Tokens Can be collocated with Resource Server











SSO-Enabled Collaboration Web Interfaces

Cisco Unified Commutations Manger, Cisco Unity Connection, and Cisco Unified CM IM and Presence servers support access to different web interfaces using SSO.

SSO-Enabled Collaboration Web Interfaces

The following web services are enabled for SSO based on SAML IdP redirects:

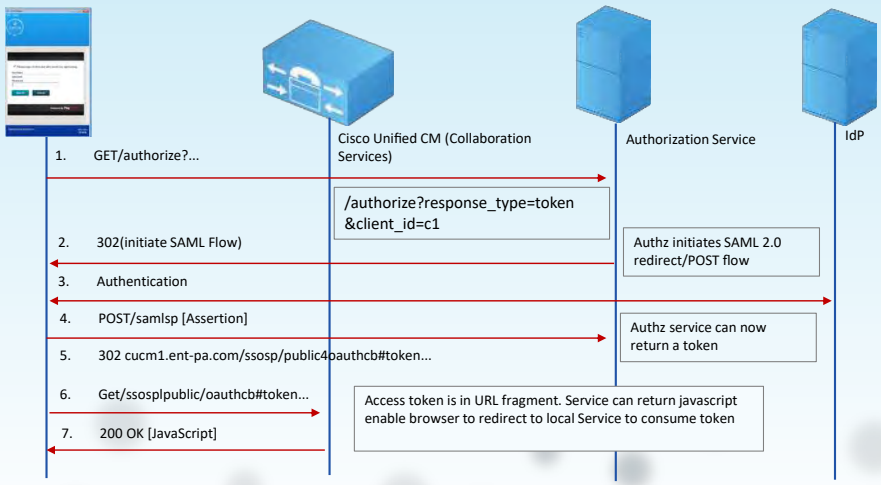
- Cisco Unified Communications Manager Administration GUI
- Cisco Unified Communications Manager Self-Care Portal
- Cisco Unified Communications Manager Serviceability GUI
- Cisco Unified Communications Manager Reporting Tool GUI
- Cisco Unified Communications Manager Platform Administration GUI
- Cisco Unified Communications Manager Disaster Recovery GUI
- Cisco Unified Communications Manager IM and Presence Administration GUI
- Cisco Unified Communications Manager IM and Presence Platform Administration GUI
- Cisco Unity Connection Administration GUI
- Cisco Unity Connection Platform Administration GUI
- Cisco Unified Personal Communicator Assistant
- Cisco Unity Connection Web InBox

Even after enabling SSO in the Cisco Collaboration application, you can still use the administration pages with the initial application user

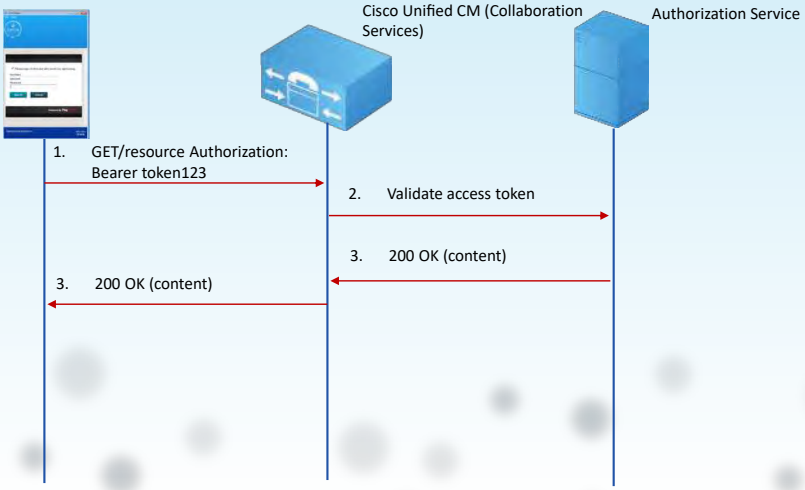
SSO-Enabled Collaboration Web Interfaces

OS	Windows	MAC	iOS	Android
Browser Control API	Iweb Browser2	Webview	UIWebView	Webview
Underlying browser technology	IE	Safari	WebKit	WebKit
Control shares cookies with native OS browser	Yes	Yes	No	No

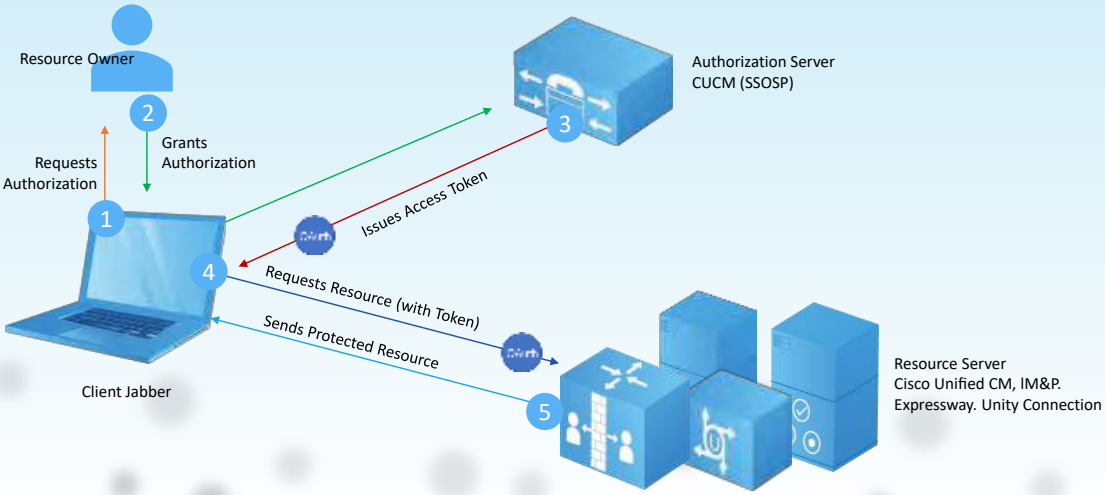
OAuth Implicit Grant Flow



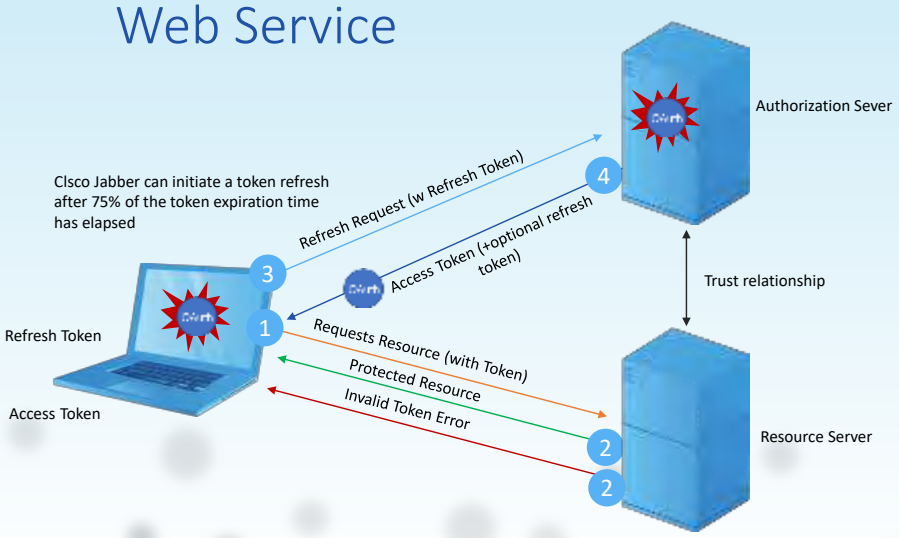
Using an OAuth Token to Authenticate to a Web Service

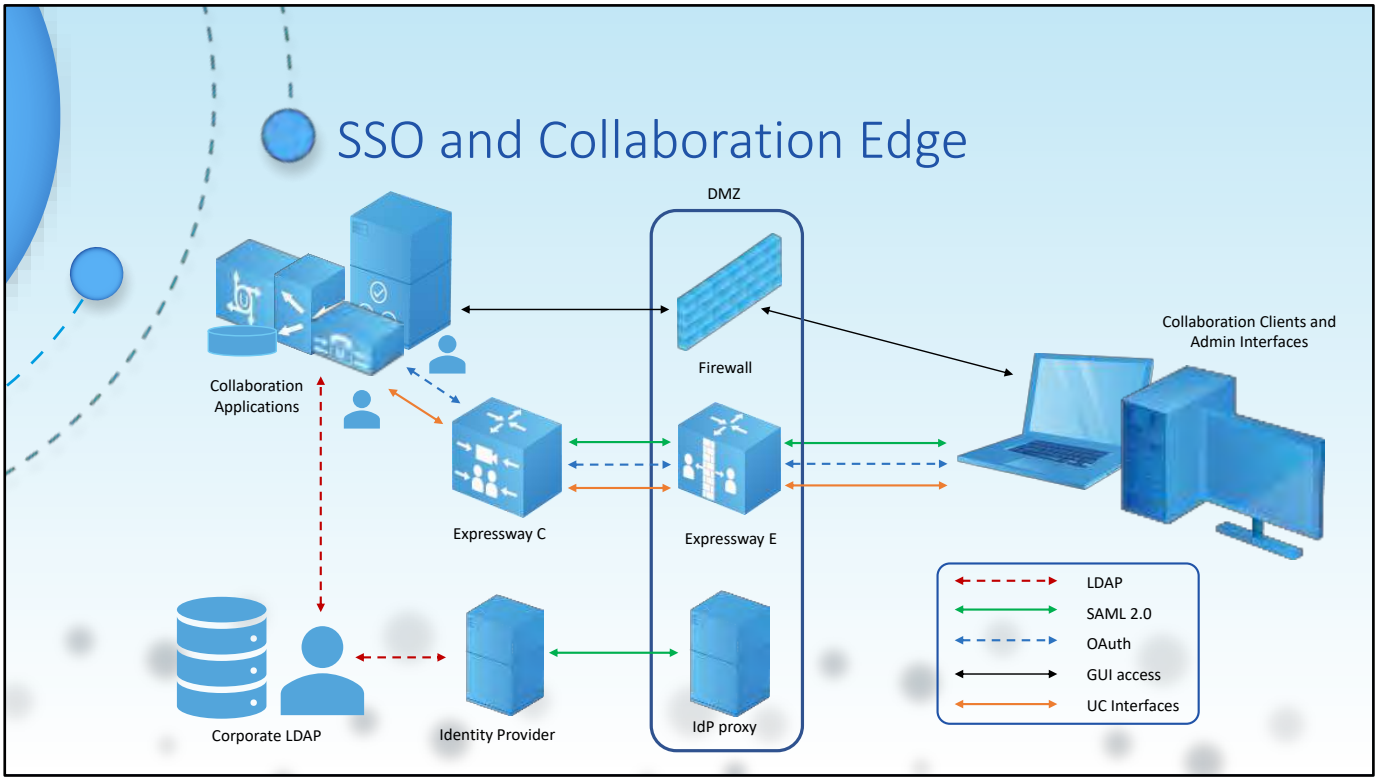


Using an OAuth Token to Authenticate to a Web Service



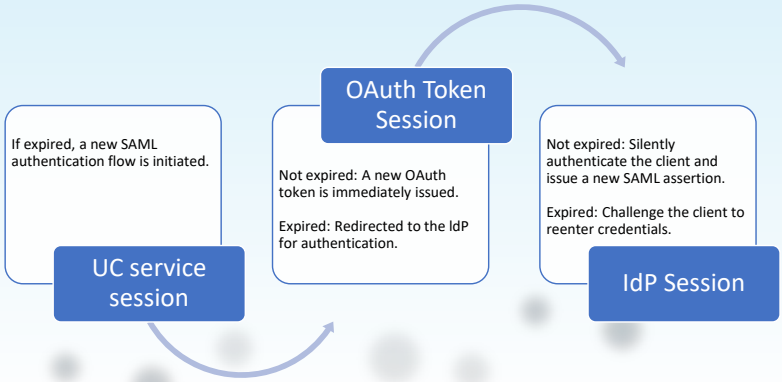
Using an OAuth Token to Authenticate to a Web Service





Session and Token Expiration Timers Overview

When receiving a request from a client, the service, the IdP, and the authorization service check if the requesting client already has an active session



Session and OAuth token expiration times interact as follows:

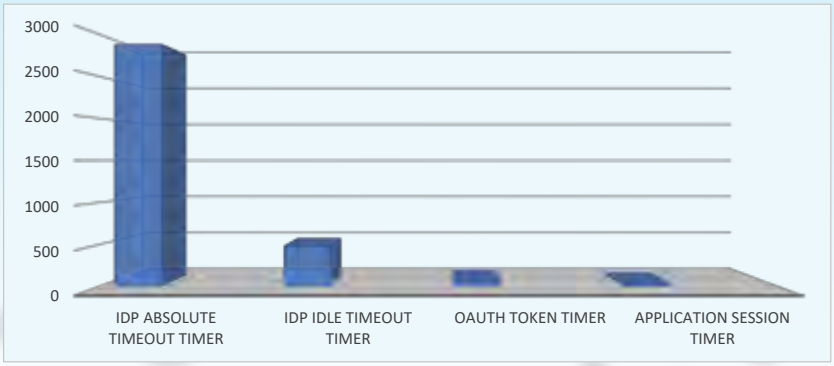
When the OAuth token is about to expire (25% remaining lifetime), the client will request a new token from the authorization service.

If the authorization session has expired, the client will request a new assertion from the IdP.

If the IdP session has expired, the IdP will challenge the client to reenter credentials.

All three timer values impact network load and throughput. Whenever a timer expires, the client must signal over the network to get a new token or establish a new session.

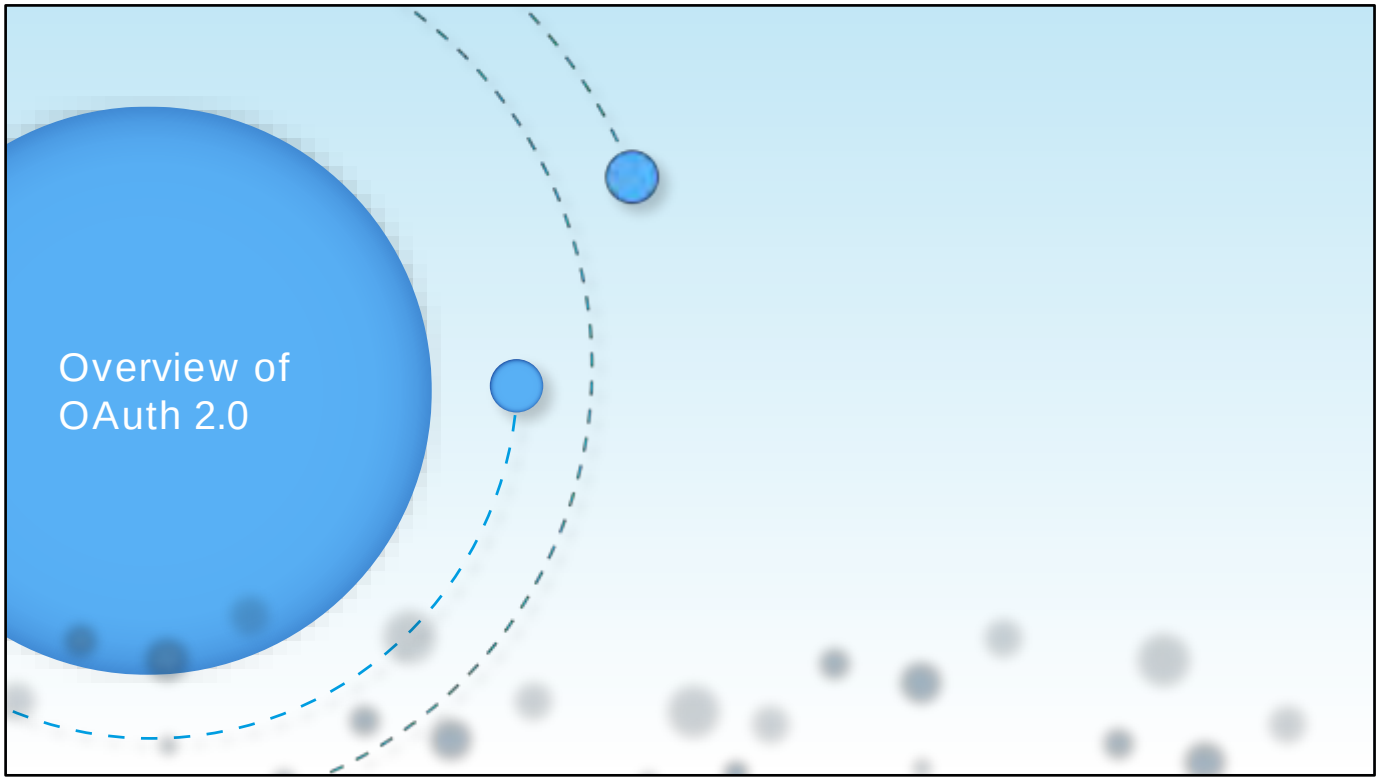
Recommended Timer Values



Recommended Timer Values

The recommended timeout values are as follows:

- OAuth access token timeout: 1 hour
- Unified Communications service session timeout: 30 minutes
- IdP idle timeout: 8 hours
- IdP session timeout: 48 hours



Overview OAuth 2.0

OAuth is an authorization protocol

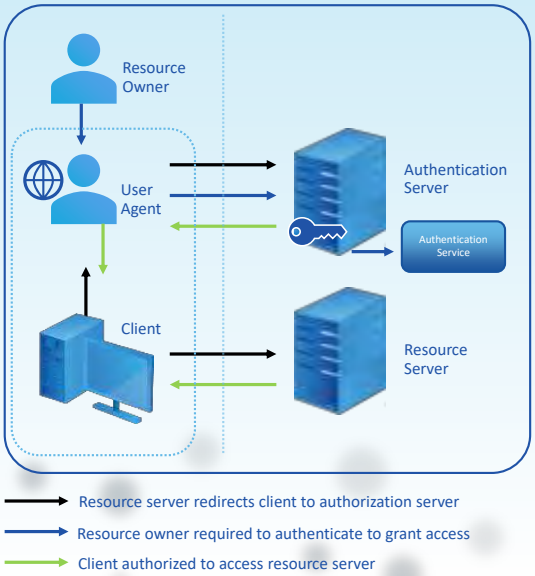
Open standard defined by the IETF OAuth Working group

OAuth 2.0 was released as RFC6749 in 2010

OAuth is heavily used on the Internet today

Framework Specification

- Resources Owner (user)
- Resource Server (Unified CM)
- Client (Cisco jabber or User Agent)
- Authorization Server (Unified CM OAuth)



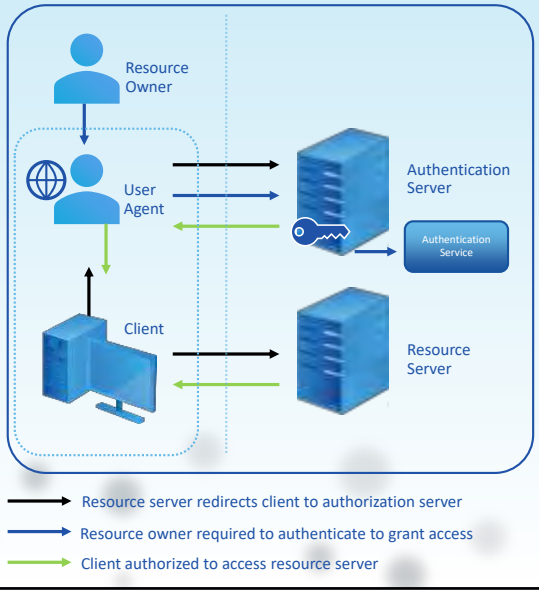
Overview OAuth 2.0

When Access to Multiple services required

Jabber needs to athecate only once

Jabber pass token to access all these services

If Token expires, re-login required



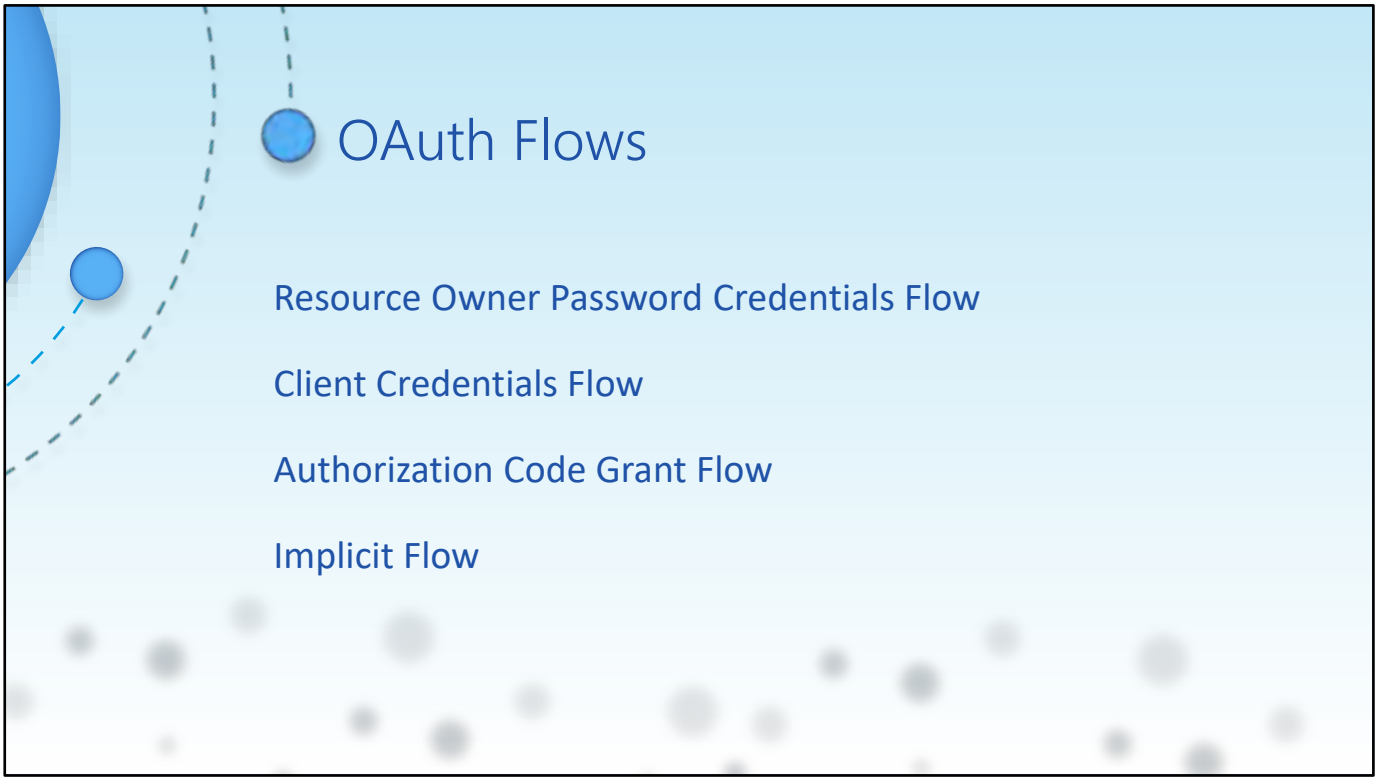
Authentication & Authorization

Authentication

- Confirming a person (or thing's) identity
- Could use Certificate or Other Proof of identity such as social media login
- Authentication define who the user is not what they can do

Authorization

- Authorization is the process of defining access rights or privileges to an entity



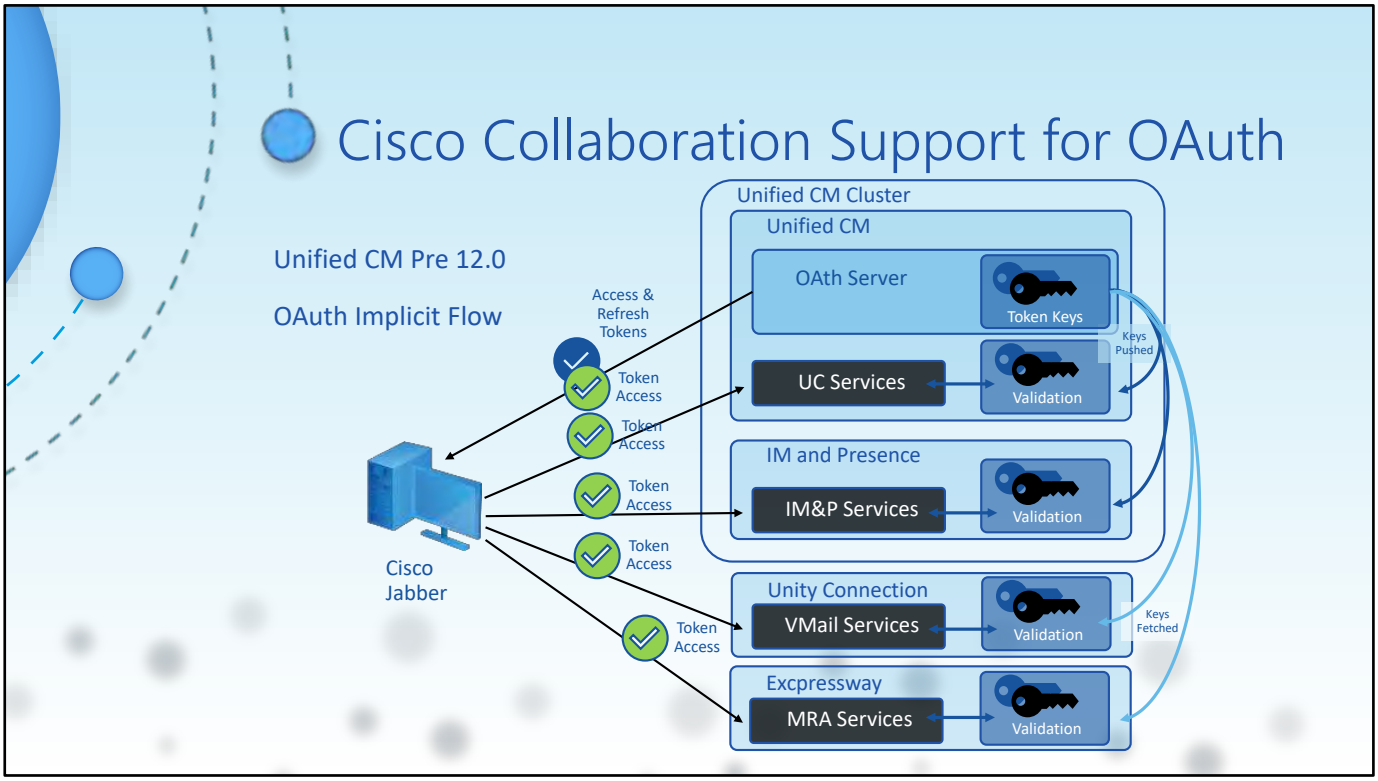
Why use OAuth for Authorization

A user is not required to share credentials with a 3rd party application

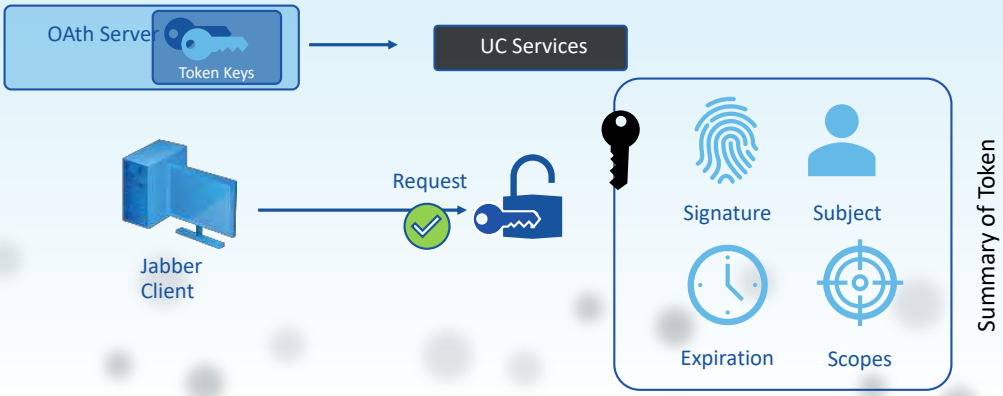
Reduction in security attack surface.

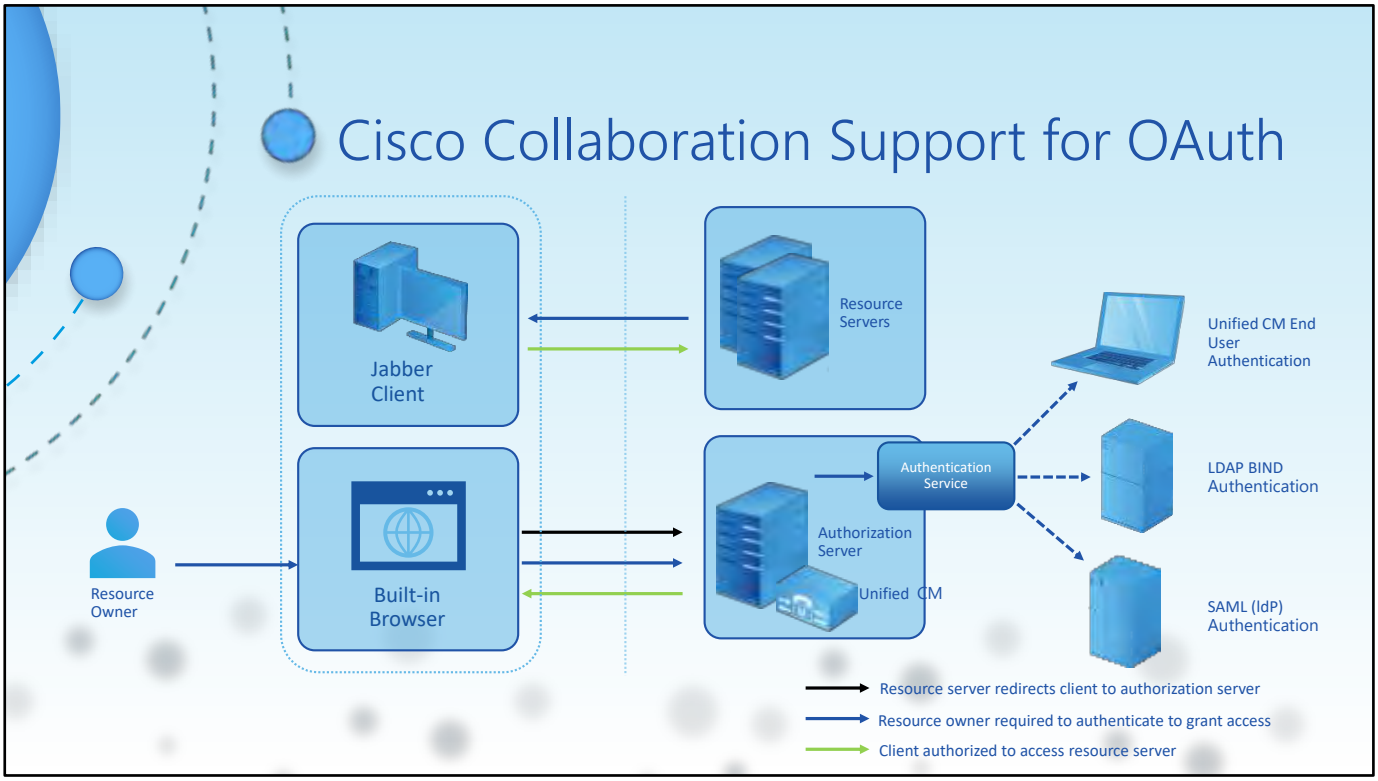
Allows for stronger authentication methods (multi-factor, biometric) when combining OAuth with SAML 2.0 based single sign-on

Cisco Collaboration Support for OAuth



Cisco Collaboration Support for OAuth





OAuth Authorization Code Grant Flow

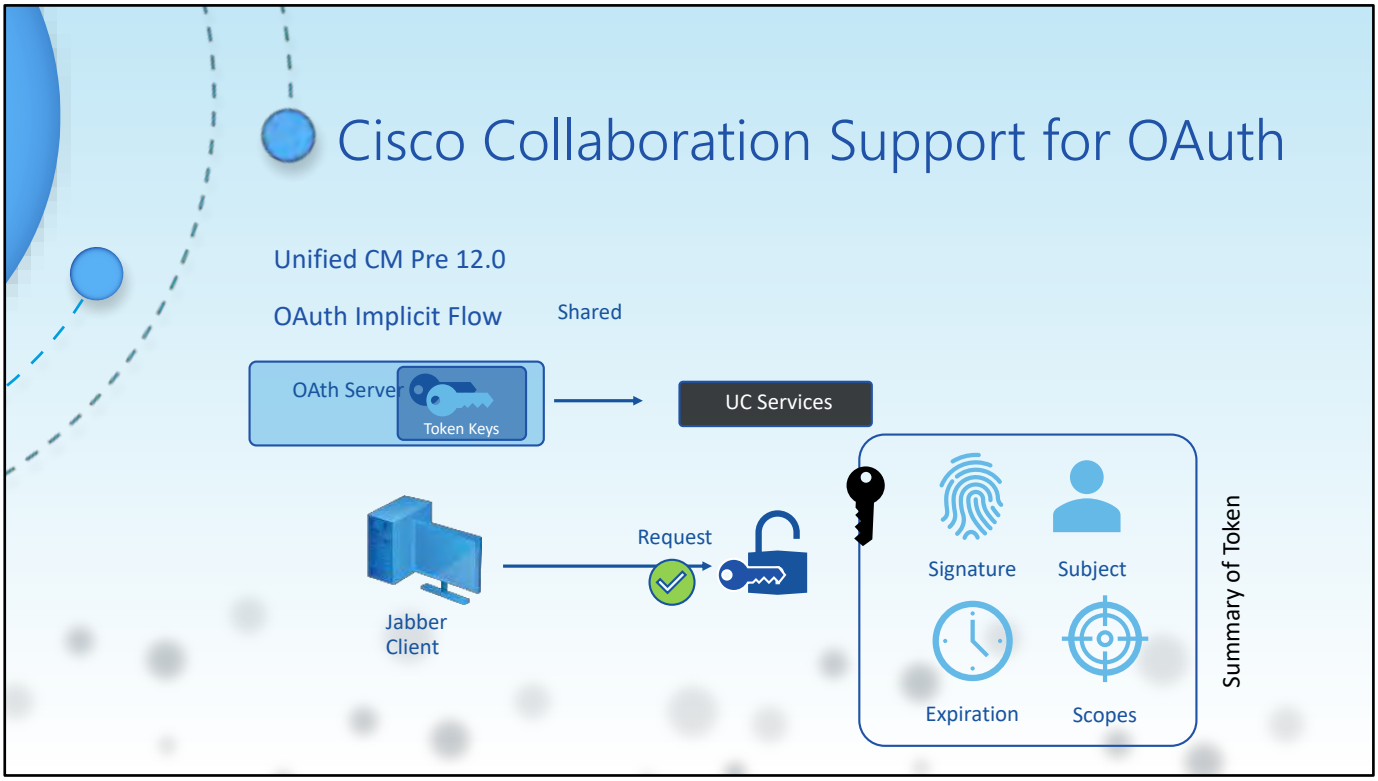
12.0 OAuth architecture has been built on the OAuth Authorization Code grant

The authorization code grant flow provides a method for a client to obtain access

This flow is also based on redirection

Requires the client to be able to interact with an HTTP user-agent (web browser) controlled by the user

The client will make an initial request to the authorization server using HTTPS



Why OAuth Authorization Code Grant Flow is better

In the implicit grant flow the access token is passed to the Jabber client via a HTTP user agent (browser)

The OAuth authorization code grant flow supports the use of refresh tokens

As the user is authenticating less frequently users are more accepting of stronger/multi-factor authentication schemes.

The OAuth authorization code grant also reduces the load on the authentication/Identity provider, as the refresh token is used to gain new access tokens

End User Experience with OAuth

Authentication Experience

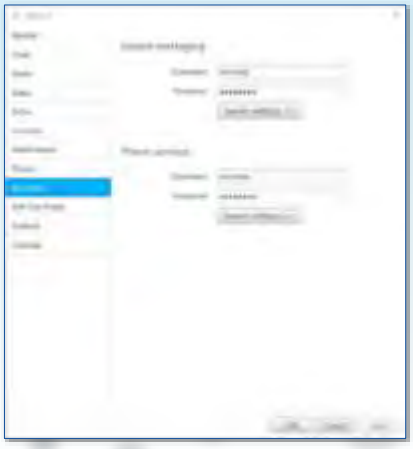
Token Based Authorization Experience

Token Refresh Experience

- Access Token
- Refresh Token

Account Credentials

Default Accounts Tab



OAth Accounts Tab

How to Enable OAuth

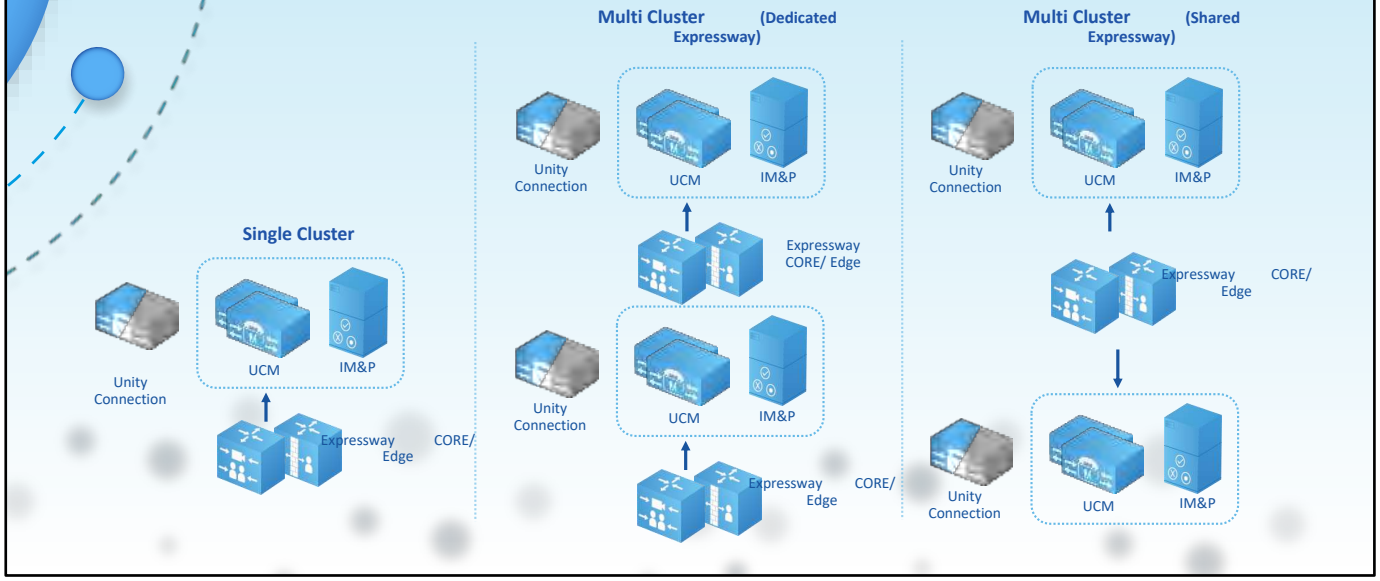
Cisco Unified Communications Manager 11.5.1(SU3) and later

Cisco Unified Communications Manager IM and Presence Service 11.5.1(SU3) and later

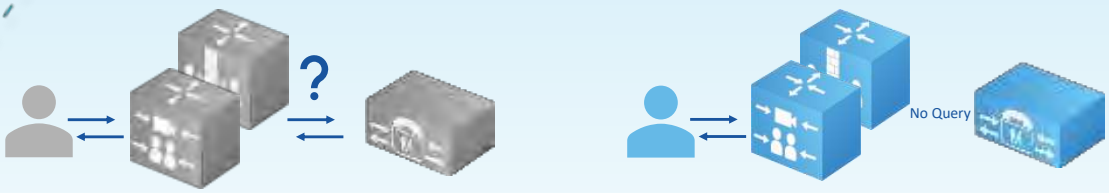
Cisco Expressway X8.10.1 and later

Cisco Unity Connection Server 11.5.1(SU3)

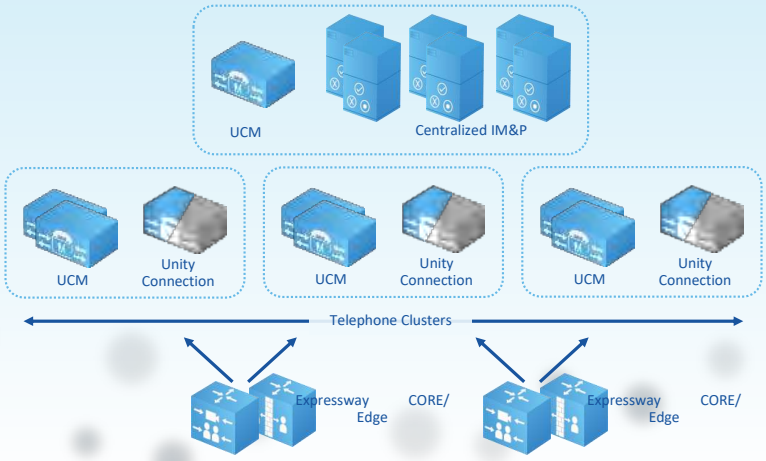
How to Enable OAuth



Two Method of Operation



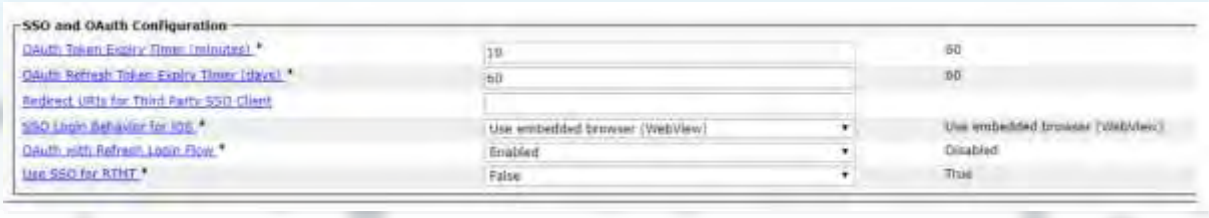
Distributed Telephony clusters with centralized IM&P cluster



Enabling Unified CM & IM&P

To enable OAuth perform the following procedure

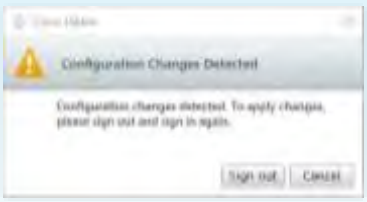
1. Go to Cisco Unified Communications Manager Admin > System > Enterprise Parameters > SSO and OAuth Configuration
2. "Select OAuth with Refresh Login Flow" set Enable/Disable support OAuth feature
3. Set "OAuth Access Token Expiry Timer (minutes)"
4. Set "OAuth Refresh Token Expiry Timer (days)"
5. Click "Save" button, OAuth will be effective immediately

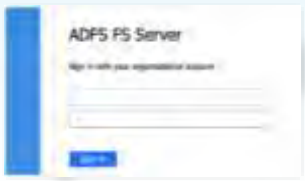


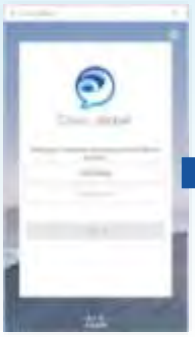
Enabling Unity Connection

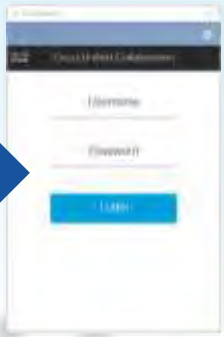
Enabling Cisco Jabber Client

1. Cluster is NOT enabled for OAuth nor SSO
2. Cluster is enabled for SSO and OAuth WITHOUT refresh token (Pre 12.0 model)
3. 12.0 Cluster is enabled for OAuth with refresh using Local or LDAP based authentication
4. 12.0 Cluster is enabled for SSO and OAuth WITH refresh tokens (12.0 model)









Enabling Expressway

Connect to the Expressway-C server and navigate to

Configuration > Unified Communications > Configuration

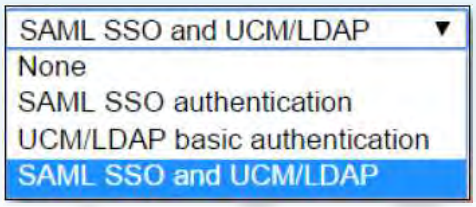
Toggle "Authorize by OAuth token with refresh" to On to enable OAuth operation and click save at the bottom of the page.

Navigate to the Configuration > Unified Communications > Unified CM servers

Additional MRA Access Control Details

MRA Access control menu that allows an administrator to enable the new OAuth with Refresh token login flow

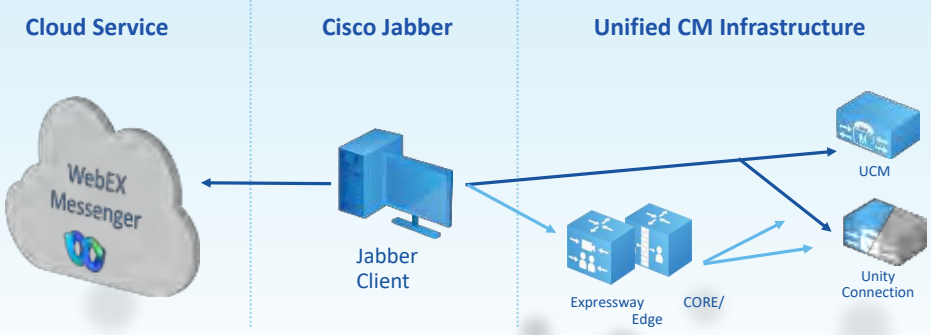
The default values for these controls represent the most secure configuration option when paired with the Unified CM 12.0 architecture



Additional MRA Access Control Details

1. Cluster is NOT enabled for OAuth nor SSO
2. Cluster is enabled for SSO and OAuth WITHOUT refresh token (Pre 12.0 model)
3. 12.0 Cluster is enabled for OAuth with refresh using Local or LDAP based authentication
4. 12.0 Cluster is enabled for SSO and OAuth WITH refresh tokens (12.0 model)

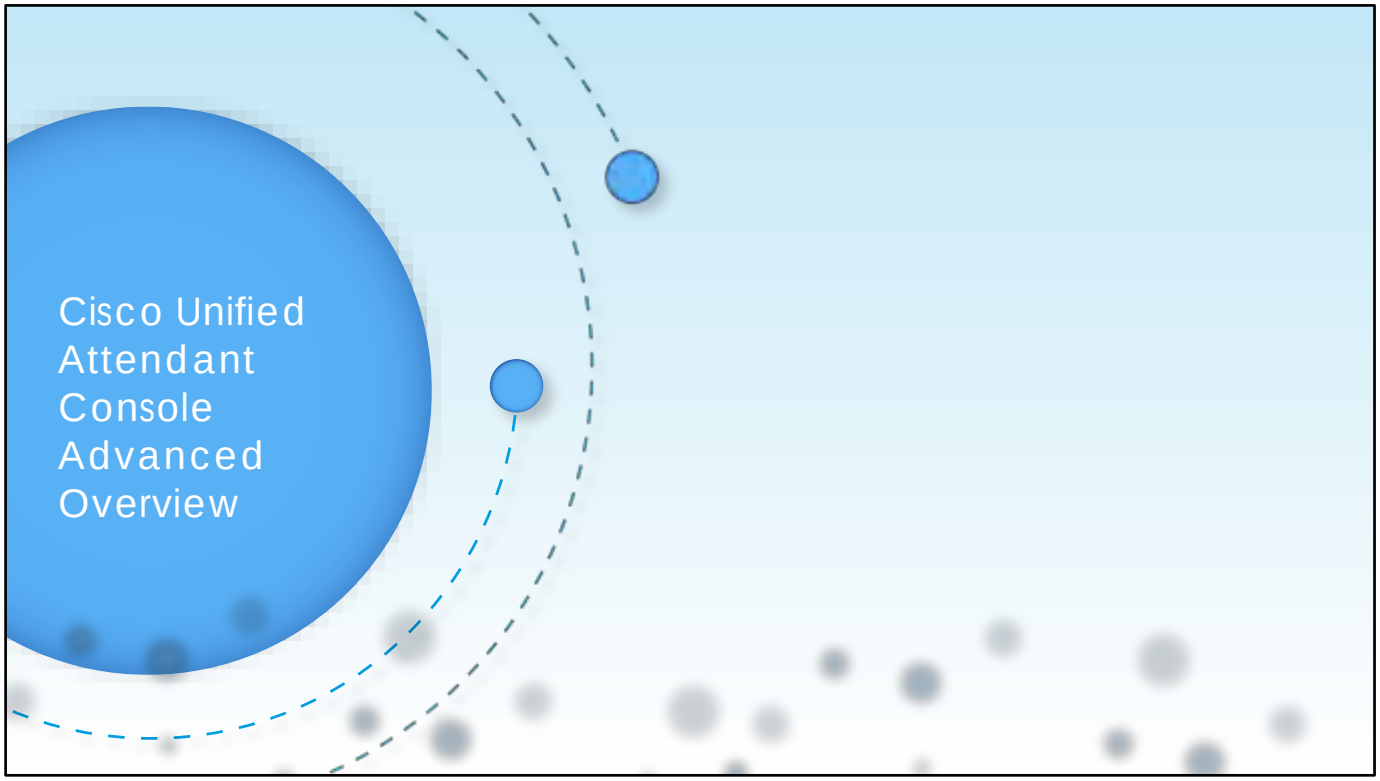
Hybrid deployment with WebEx Messenger



Key and Token Management

Conclusions

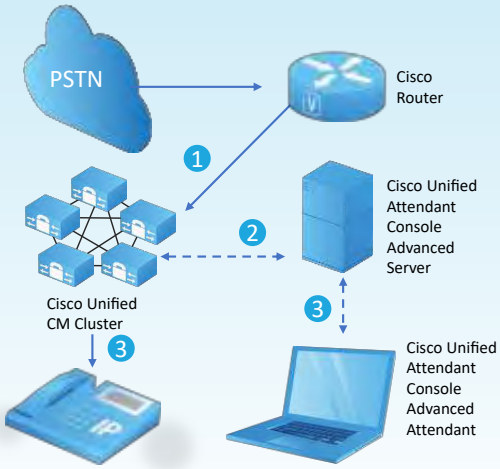
- OAuth 2.0
  - Overview
  - Enabling OAuth
  - Access Control
  - Key and Token Management



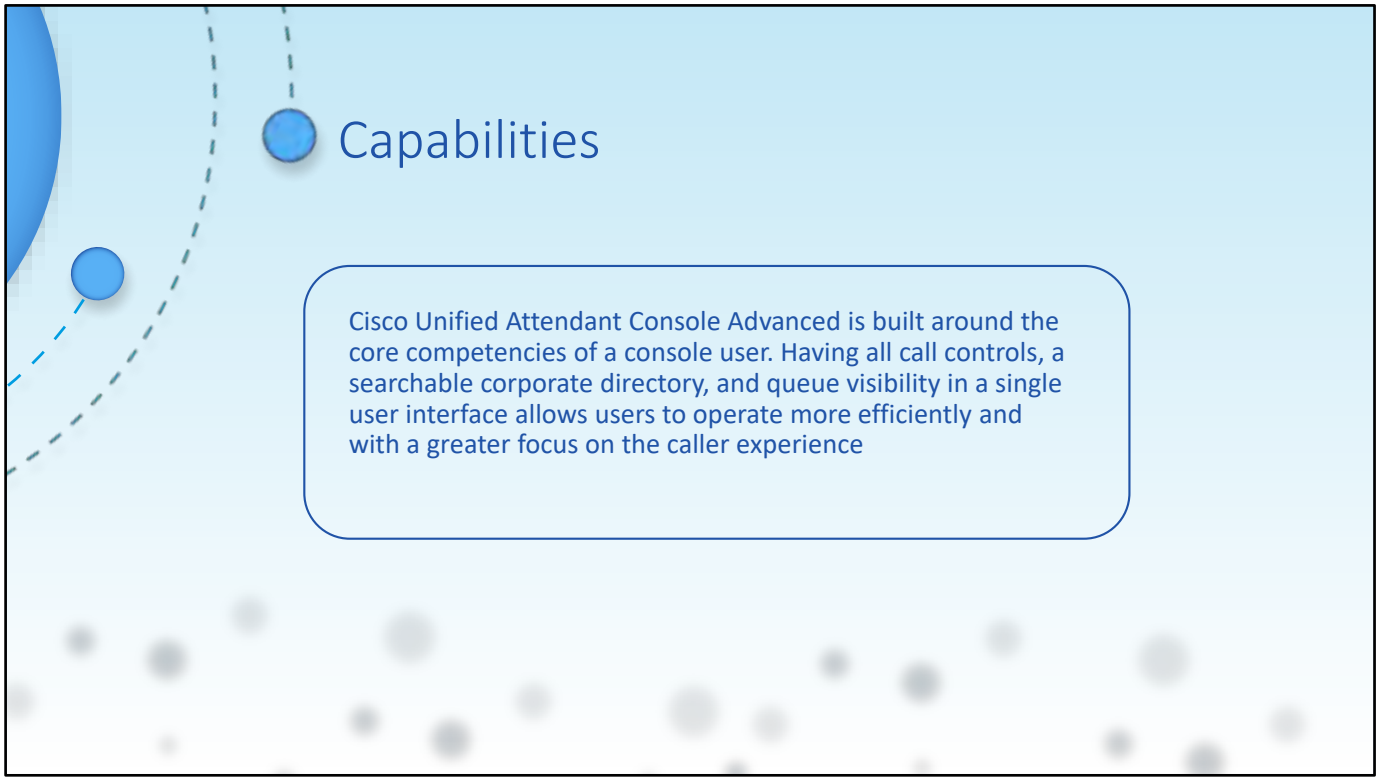
Overview

Cisco Unified Attendant Console Advanced provides receptionists with a software interface to answer and forward large volumes of calls as they come into an organization. Calls can be answered, placed on hold, or forwarded (either with or without being answered first).

Flow



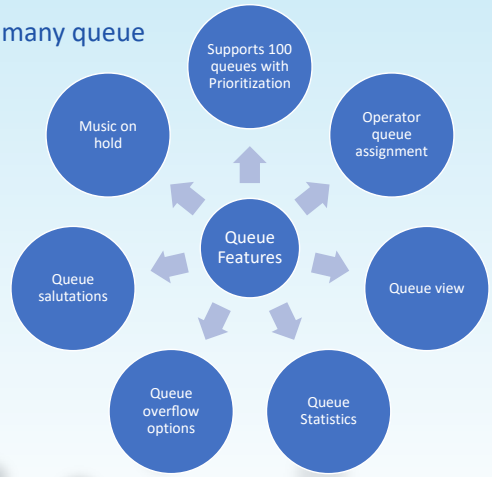
1. Calls are delivered from the PSTN to Cisco Unified Communications Manager via the voice gateway.
2. The call is routed to a CTI route point
3. The call is delivered by the Cisco Unified Communications Manager to the attendant console via the IP phone.



Queue Features

Cisco Unified Attendant Console Advanced has many queue features.

- Support for 100 queues with prioritization
- Operator queue assignment
- Queue view
- Queue statistics
  - Number of calls abandoned
  - Number of operators logged in
  - Number of operators available to answer calls
- Queue overflow options
- Queue salutations
- Music on hold



Directory Features

Cisco Unified Attendant Console Advanced supports the following directory features:

- Active Directory, Cisco Unified Communications Manager, iPlanet directory integration
- Manually add contacts
- Bulk add, update, and delete contacts
- Personal directory groups
- Search options
- Presence integration

Telephony Features

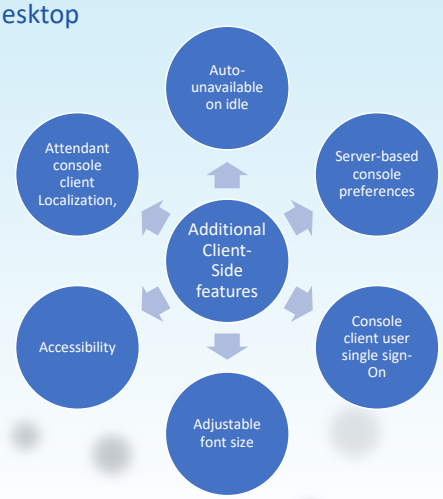
When integrated with Cisco Unified Communications Manager, Cisco Unified Attendant Console Advanced has many telephony features.

- Operator handset ringing
- Transfer reversion (call recall)
- Call Park
- Call Park recall
- Call toggle
- Conference
- Emergency Mode switch

Additional Client-Side Features

You must install the Cisco Unified Attendant Console Advanced client application on the supported desktop

- Auto-unavailable on idle
- Server-based console preferences
- Console client user single sign-on
- Adjustable font size
- Accessibility
- Attendant console client localization

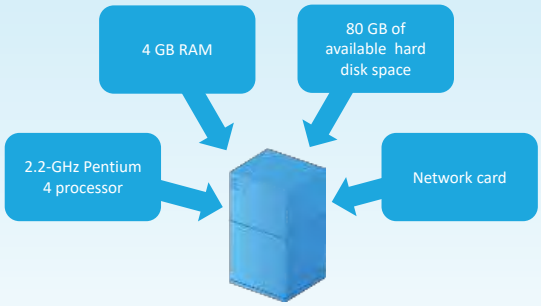


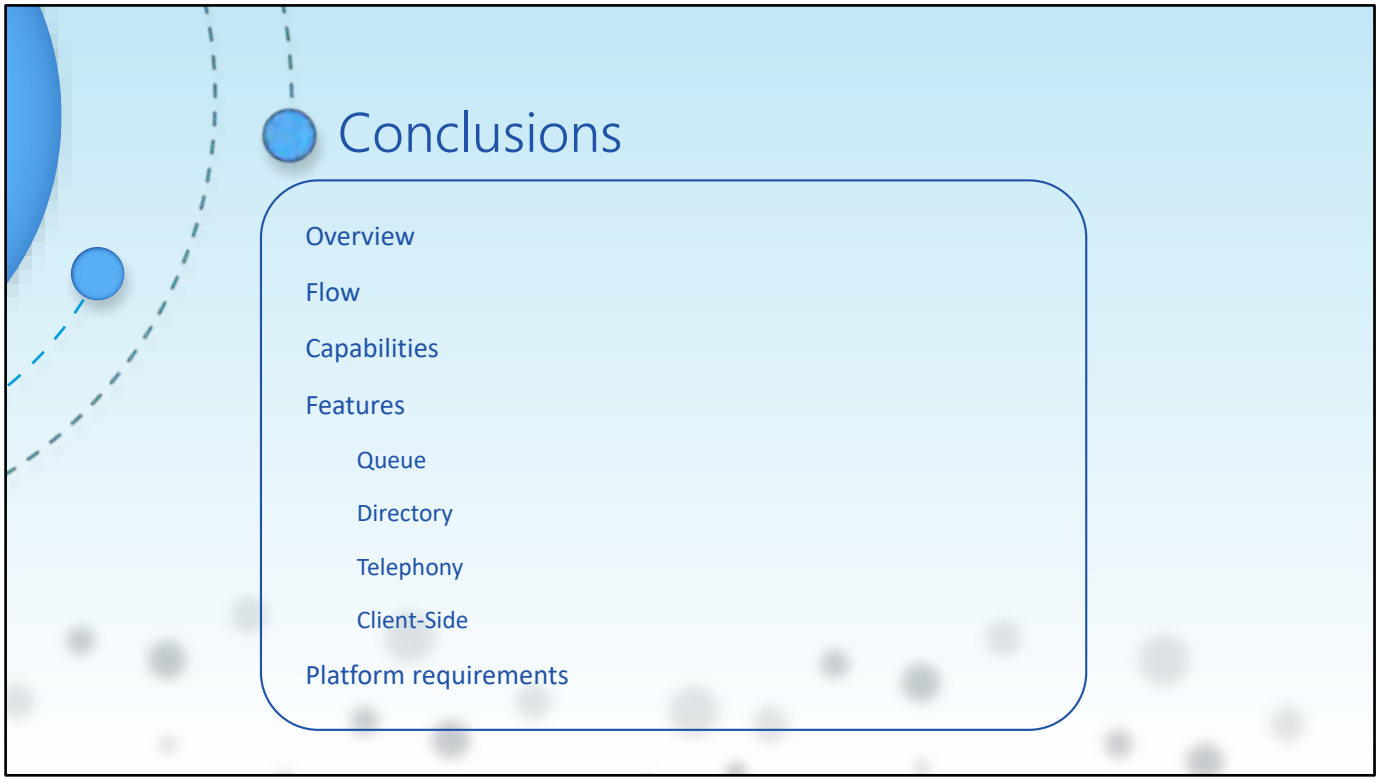
Platform Requirements

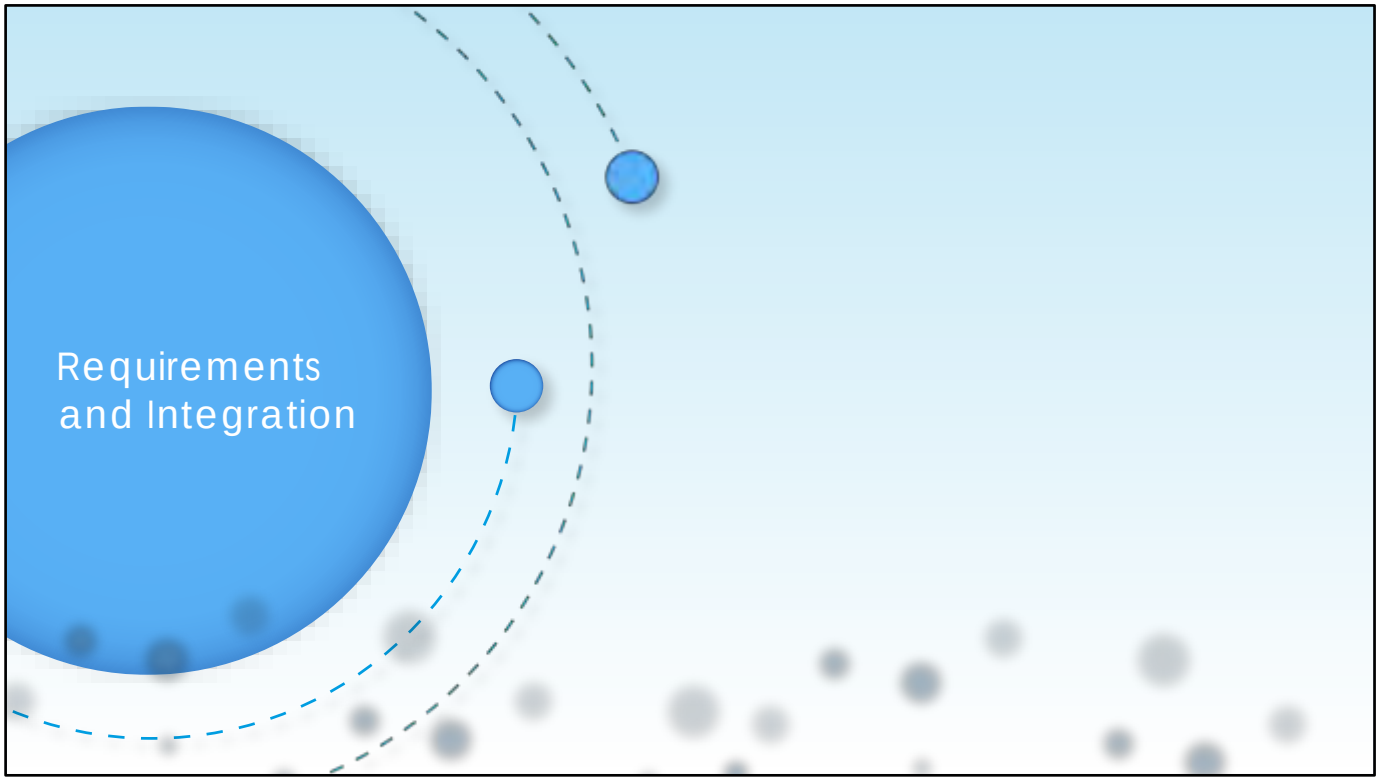
The Cisco Unified Attendant Console Advanced server is not supported in a production environment if it is running on a desktop PC

Requirement

- 2.2-GHz Pentium 4 processor
- 4 GB RAM
- 80 GB of available hard disk space
- Network card, which is connected to the network using TCP/IP
- NIC teaming is not supported





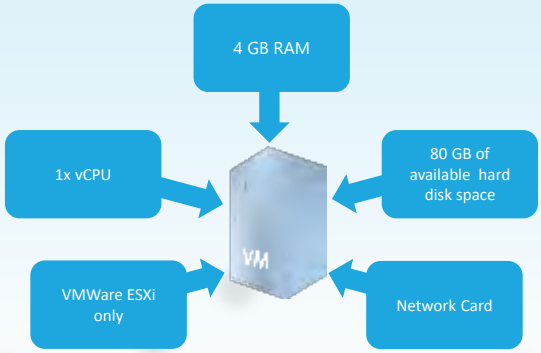


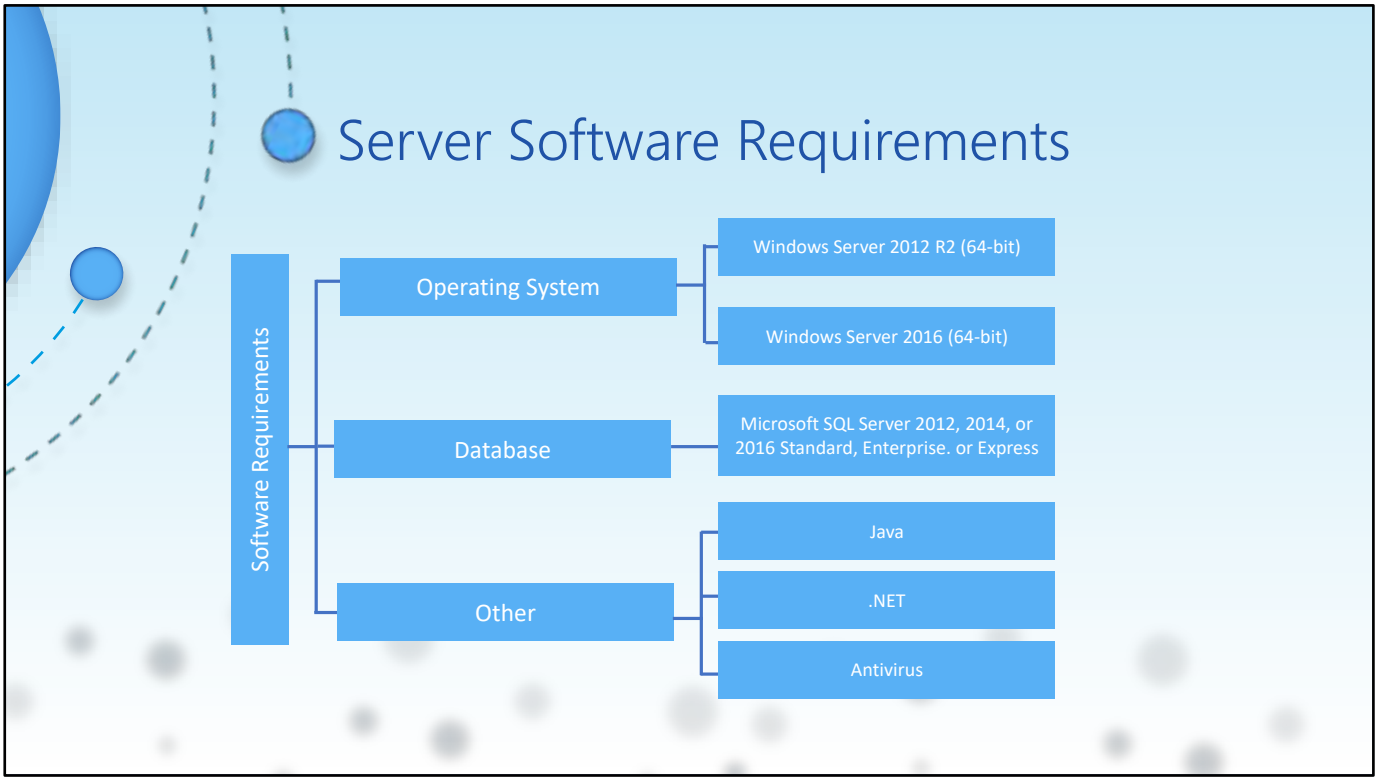
VMware Guest Machine Requirements

In a production environment, Cisco Unified Attendant Console Advanced server is supported on the VMware ESXi (vMotion included) hypervisor, running on a host machine that is Cisco Unified Communications Virtualization supported hardware

Requirement

- 1x vCPU unrestricted
- 4 GB RAM
- 80 GB of available hard disk space





SQL Server Requirements

The Cisco Unified Attendant Console Advanced server does not support multiple SQL database instances or named instances, and requires exclusive use of and access to a local installation of SQL Server

If you are installing Microsoft SQL Server yourself, you must install it locally on the Cisco Unified Attendant Console Advanced server. Cisco Unified Attendant Console Advanced does not support the use of external SQL Servers

Due to security restrictions and the resource demands of a domain controller, Microsoft advises against installing SQL Server on a domain controller. (For more information, see http://support.microsoft.com/kb/2032911.) Consequently, Cisco Unified Attendant Console Advanced is not supported if installed on a domain controller

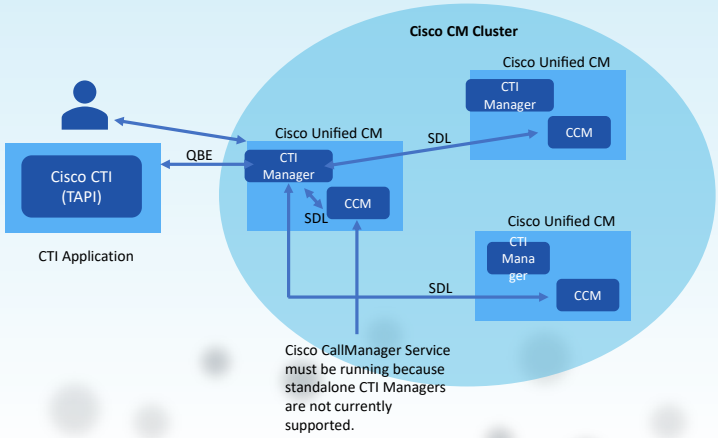
To ensure system security, your SQL installation must be configured according to your company's SQL system hardening guidelines. Take care to ensure that all Cisco Unified Attendant Console Advanced-specific configuration requirements are still met after hardening

Overview

Cisco Unified Attendant Console Advanced provides call control and device monitoring via CTI connections between the Cisco Unified Attendant Console Advanced server and the Cisco Unified Communications Manager cluster

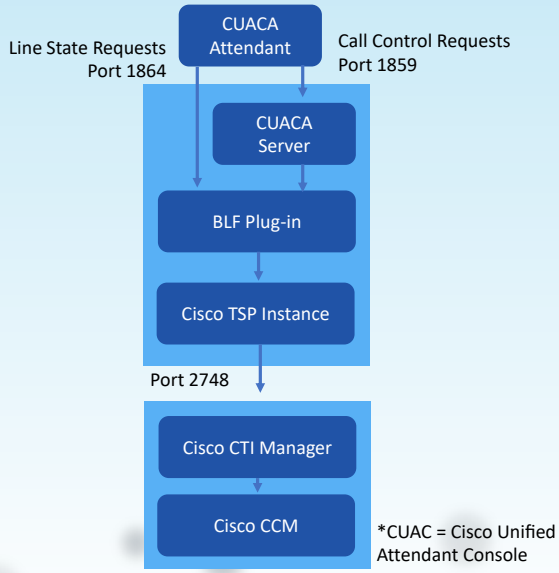
CTI Architecture and Components

- CTI Application
- Cisco CallManager Services
- CTI Manager
- SDL



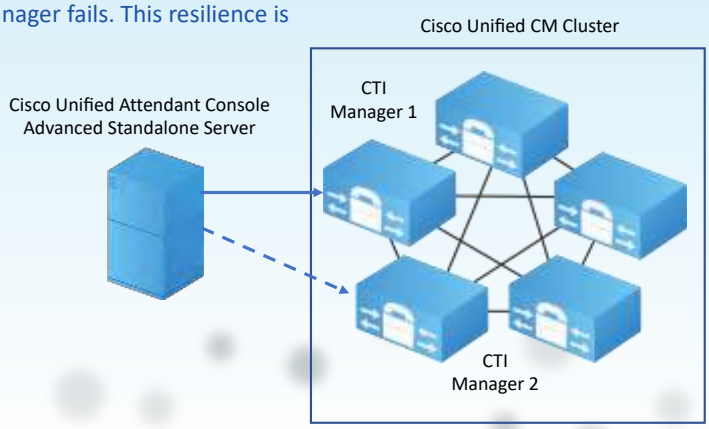
Overview

The Cisco Unified Attendant Console Advanced server sends call control requests via CTI interface, and Cisco Unified Communications Manager acts upon those requests, returning confirmation messages when the action is complete



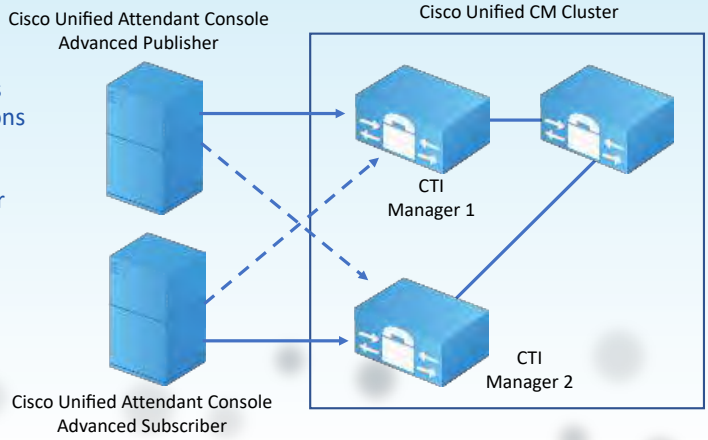
Standalone Cisco Unified Attendant Console Advanced Server

The Cisco Unified Attendant Console Advanced servers can be configured to use multiple Cisco TSP instances, providing a backup CTI Manager if the primary CTI Manager fails. This resilience is configured in Cisco TSP itself.

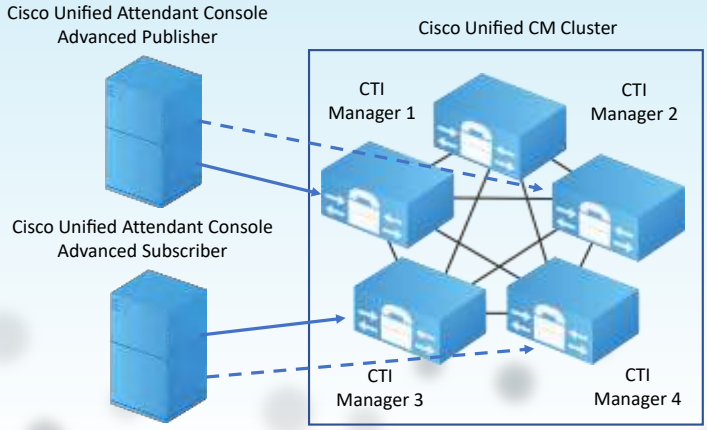


Resilient Cisco Unified Attendant Console Advanced Servers on a Small Cisco Unified Communications Manager Cluster

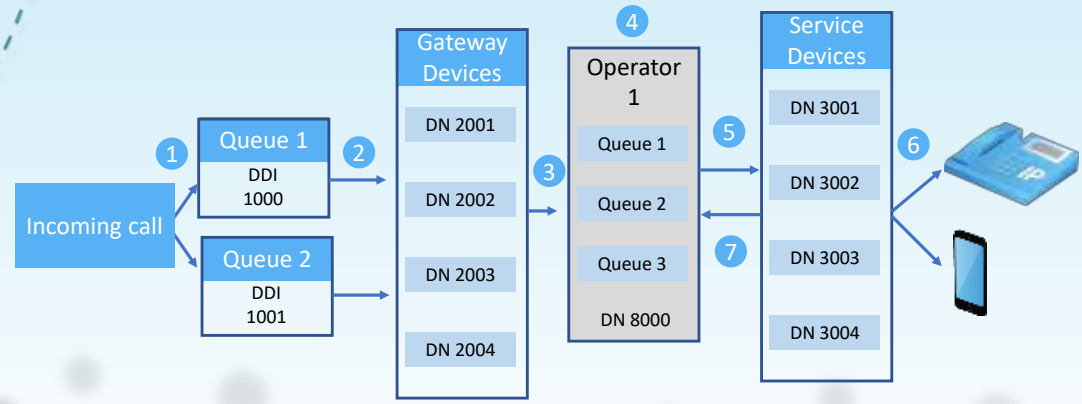
This example has only three nodes in the Cisco Unified Communications Manager cluster. The top node is the publisher (primary) server and the lower two are subscriber (secondary) servers.



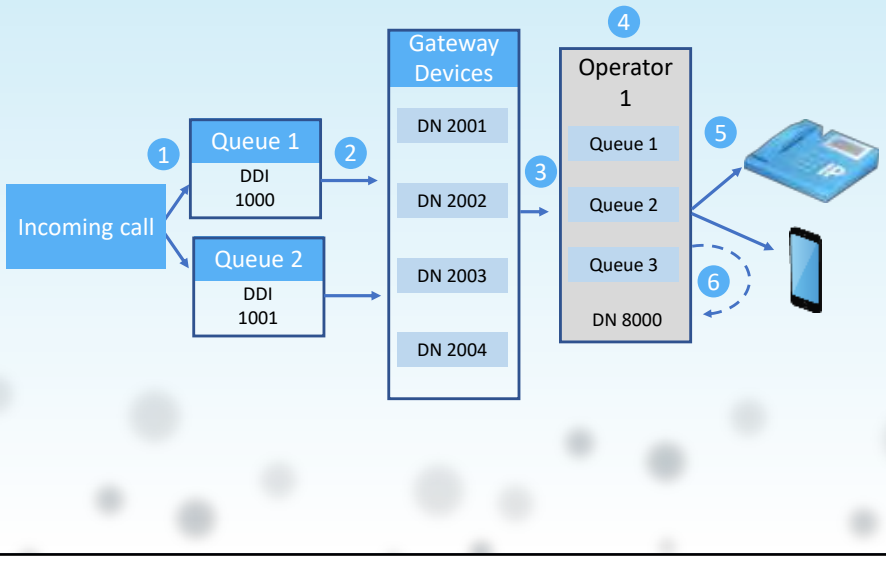
Resilient Cisco Unified Attendant Console Advanced Servers on a Large Cisco Unified Communications Manager Cluster



Call Flow During Blind Transfer

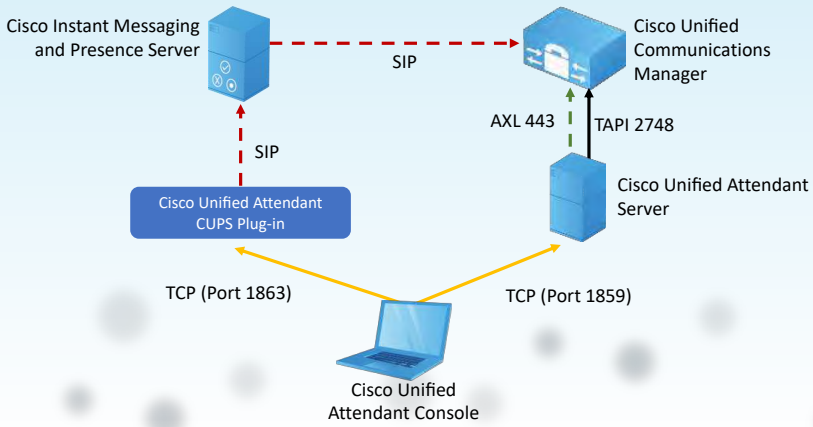


Call Flow During Consultation Transfer



Cisco Unified Communications Manager IM and Presence Service Integration overview

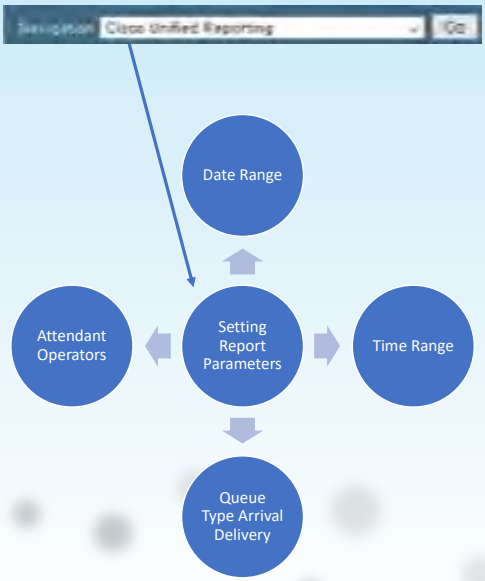
The Cisco Unified Presence configuration is stored in an XML file with the same name as the Cisco Unified Presence executable and the .config extension. For example, Cisco Presence server plug-in.exe.config.



Reporting

Cisco Unified Reporting enables you to create reports using the information coming through Cisco Unified Attendant Console Advanced. You must enable Cisco Unified Reporting during installation

In order to access Cisco Unified Reporting you need to login to Cisco Unified Attendant Console Administration. Please note that only administrators can access Cisco Unified Attendant Console Advanced Administration



Incoming Calls by Date and Time System Report

The Incoming Calls by Date and Time report is a summary of the incoming calls in the queues during a specific period. A single line of information is provided for a particular date, time, and queue

Specify the following parameters before running this report:

- From and To Date
- Start and End Time
- Queues
- Abandoned Call Timer
- Arrival or Delivery Queue

Incoming Calls by Date and Time	A summary of the incoming calls in the queues during a specific period. A single line of information is provided for a particular date. time, and queue.
Operator Calls by Time	A summary or incoming and outbound calls involving specific attendant operators by time, on a single date. A line of information is displayed per hour per operator.
Operator Calls by Queue	A summary of the queued calls that attendant operators take during a specific date range. The summary data is grouped by date, with a line of information per operator on that date.
Operator Availability	The daily availability of one or more operators between the start and end date. Statistics are displayed for each logged-in period with totals for each day.
Overflowed Calls by Date	Summarizes the calls that overflow from arrival queues—the first, direct destinations of calls. Queues that only receive rerouted calls are not included in this report.

Incoming Calls by Date and Time System Report

The Incoming Calls by Date and Time report is a summary of the incoming calls in the queues during a specific period. A single line of information is provided for a particular date, time, and queue.

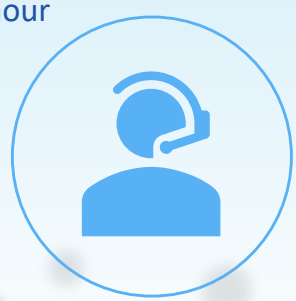
Specify the following parameters before running this report:

- From and To Date
- Start and End Time
- Queues
- Abandoned Call Timer
- Arrival or Delivery Queue

Field	Description
Total Calls	This field shows the number of calls that reached Cisco Unified Attendant Console Advanced.
Answered Calls	This field shows the number of answered calls.
Abandoned Calls	This field shows the number of abandoned calls.
Overflowed Calls	This field shows the number of calls that overflowed to a queue, device. or external number.
% Answered	This field shows the percentage of answered calls.
% Abandoned	This field shows the percentage of abandoned calls.
% Overflowed	This field shows the percentage of overflow calls.
Average Answered Wait	This field shows the average time that calls wait before being answered.
Average Answered Talk Time	This field shows the average talk time for answered calls.
Average Abandoned Wait	This field shows the average time that a caller waits before the call is abandoned.
Answer Time Profile	For 10, 20, 30, 40 (seconds). this field shows the cumulative percentage of calls that are answered in less than the specified number of seconds. 40+ is the percentage of calls that are answered after 40 or more seconds.
Longest Wait	This field shows the longest time that a call had to wait to be answered.
Break Hour	This field shows the break hours.

Operator Calls by Time System Report

The Operator Calls by Time report is a summary of incoming and outbound calls involving specific attendant operators by time, on a single date. A line of information is displayed per hour per operator.

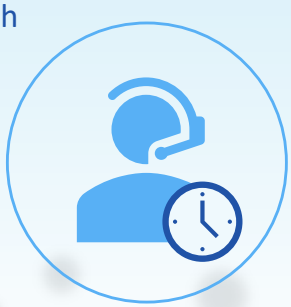


Operator Calls by Queue System Report

The Operator Calls by Queue report is a summary of the queued calls that attendant operators during a specific date range. The summary data is grouped by date, with a line of information per operator on that date.

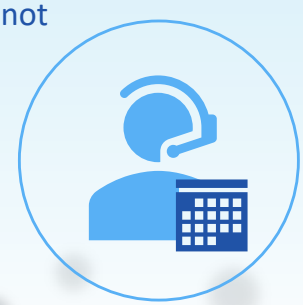
Operator Availability Report

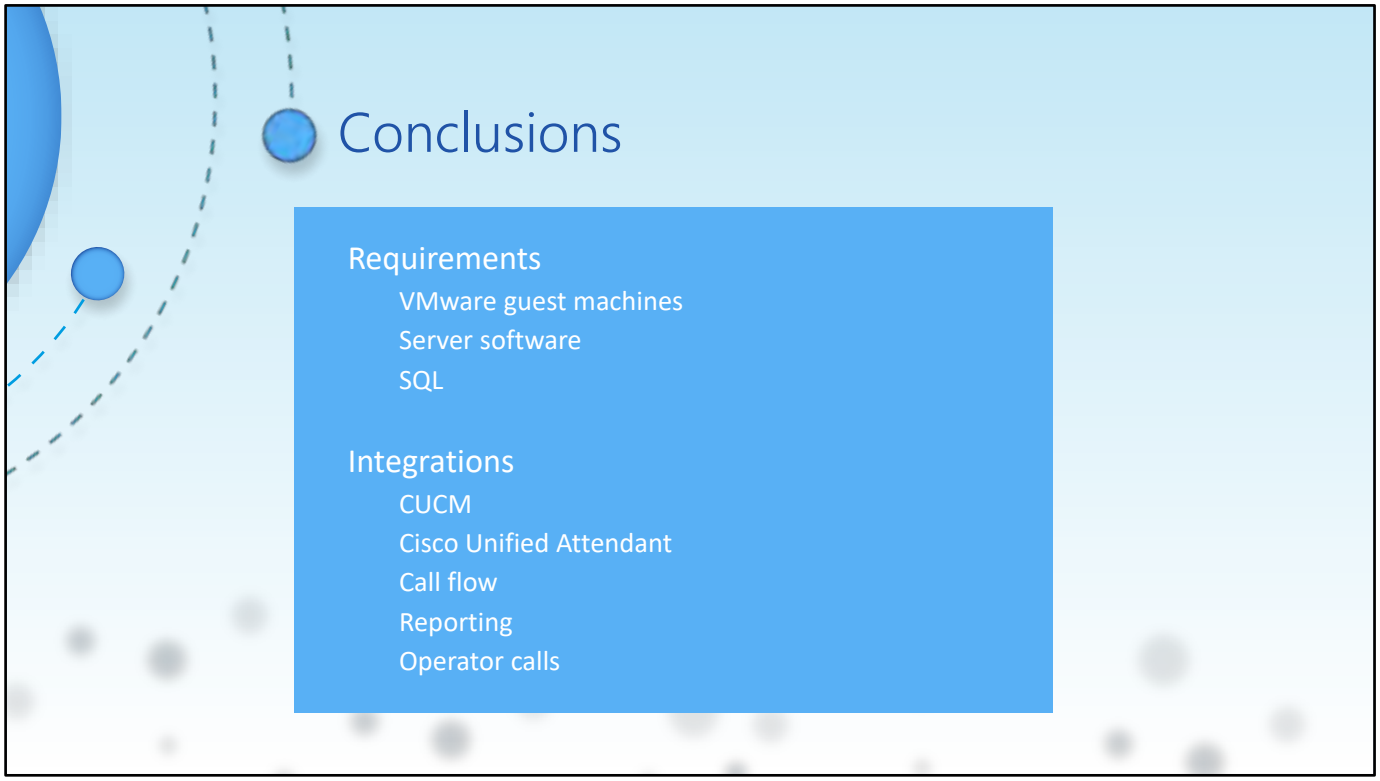
The Operator Availability report shows the daily availability of one or more operators between the start and end date. Statistics are displayed for each logged-in period, with totals for each day.

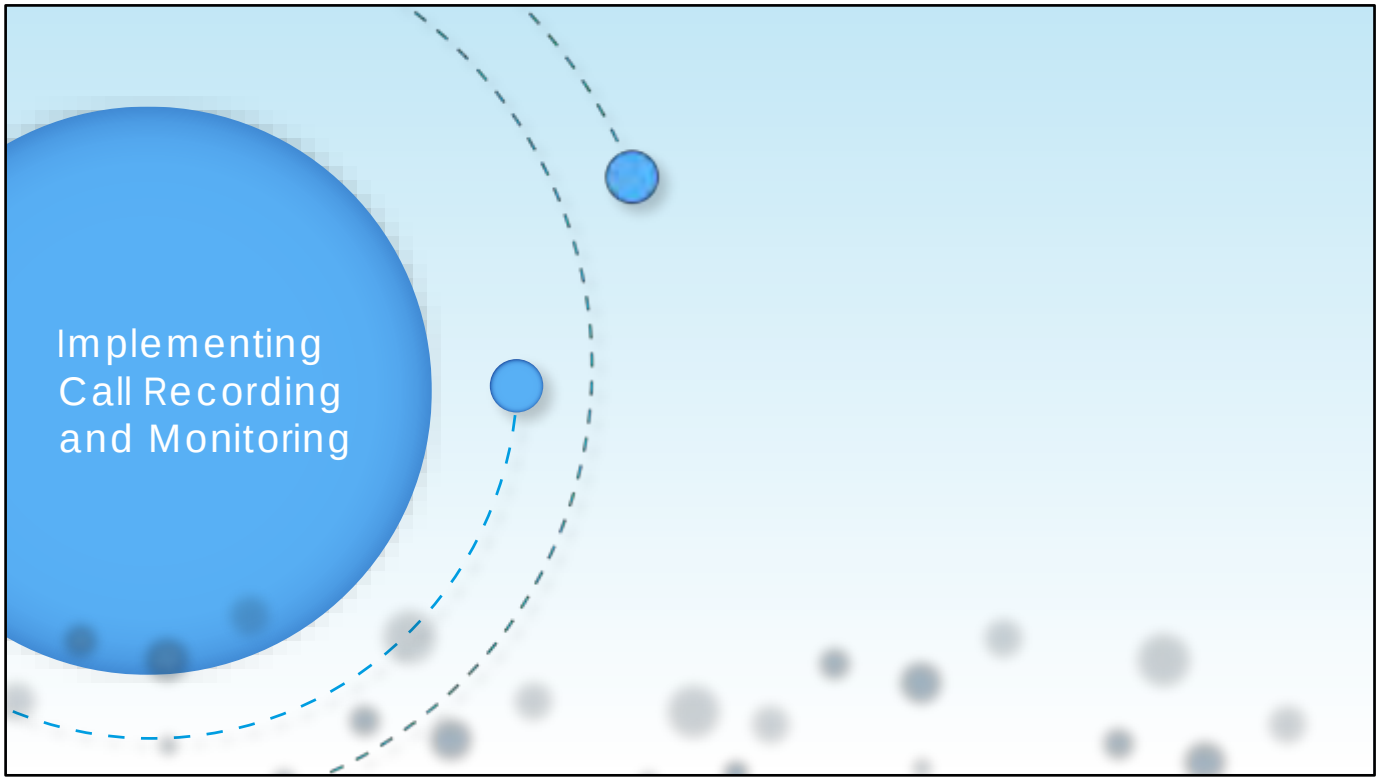


Overflowed Calls by Date System Report

The Overflowed Calls by Date report summarizes the calls that overflow from arrival queues, the first, direct destinations of calls. Queues that only receive rerouted calls are not included in this report.







Overview

Call monitoring and recording solutions provide a way to monitor and record audio and video calls that traverse various components in a Cisco Unified Communications and Collaboration solution, such as Cisco Unified IP phones, Cisco Unified Border Element devices, or Cisco switches. Customers can then use these recordings for various purposes including compliance, transcription, speech analysis, podcasting, and blogging.

Overview

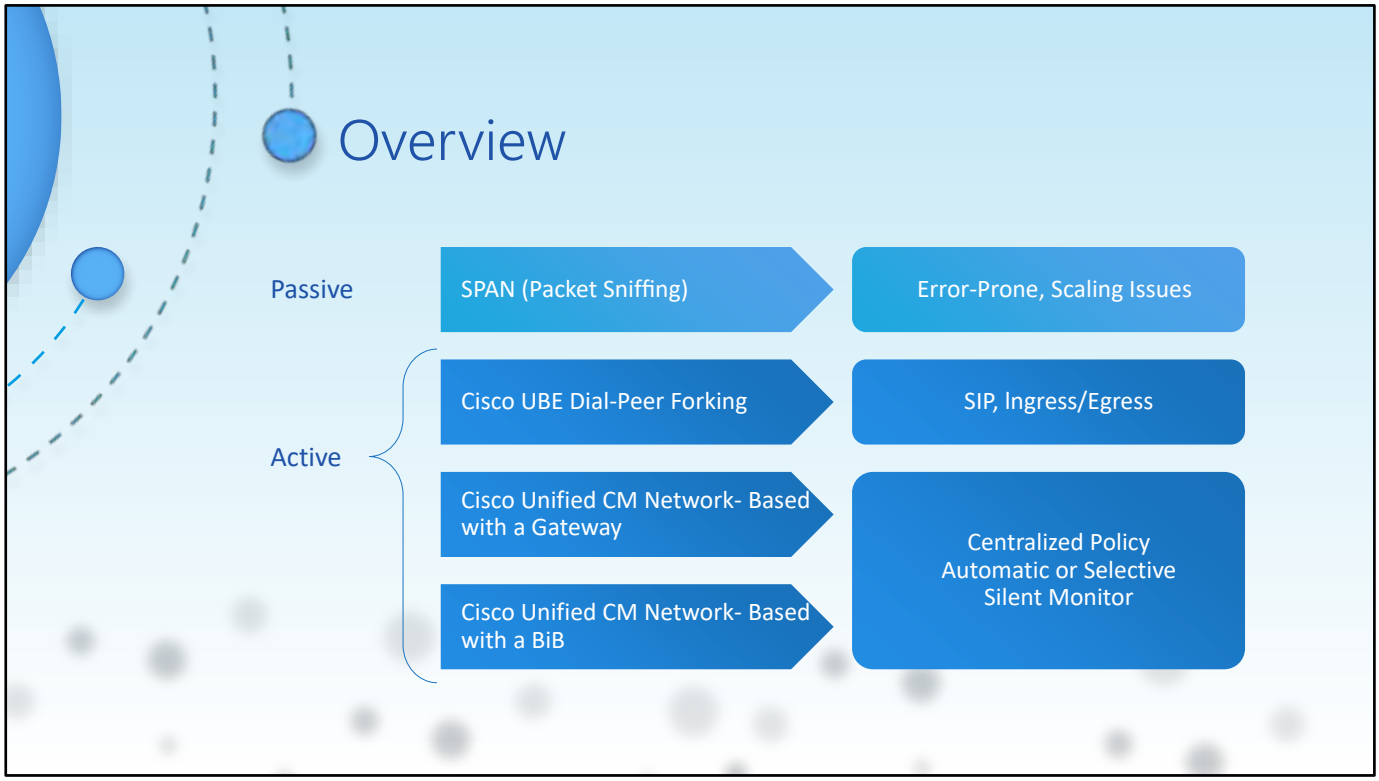
Call recording means to record a telephone call or other audio source for review later.

You can record audio calls, video calls or even record only audio portion of a video call

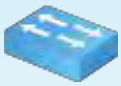
Call monitoring allows someone to eavesdrop on a phone conversation while the call is taking place

The most common scenario for call monitoring is in a call center where a call agent is speaking with a customer and supervisor can hear both call participants, but neither of the call participants can hear the supervisor

Calls can be monitored and recorded if required.



Call Recording and Monitoring Components



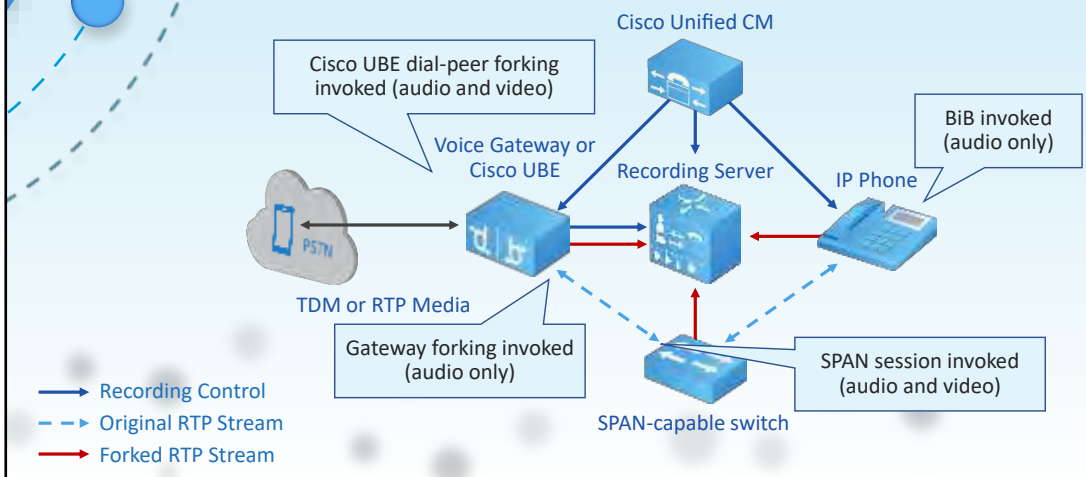
SPAN-Capable device
The switch that sends a copy of all network packets traversing a port or VLAN to another port where a recording or monitoring server analyzes those packets.

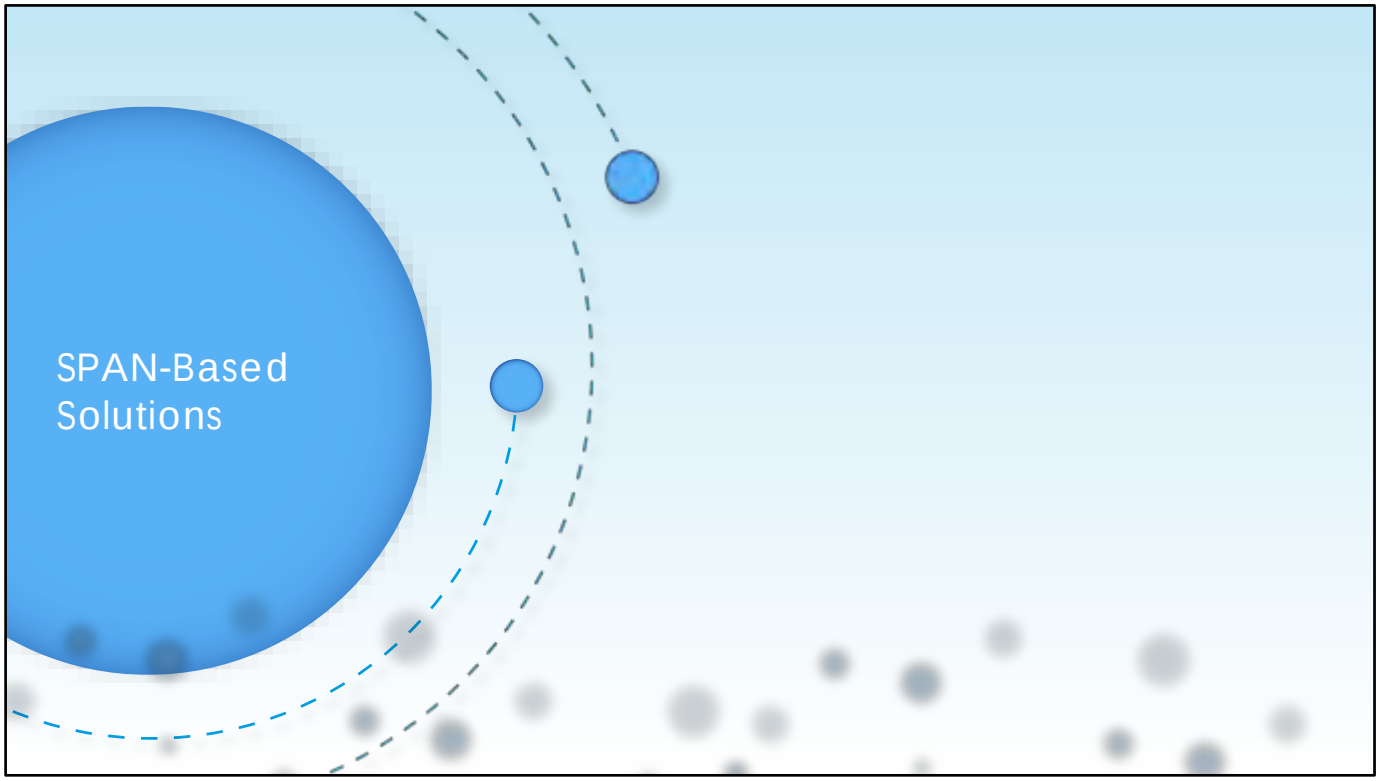

Forking Device
The device, endpoint, or gateway that is responsible for duplicating the incoming and outgoing RTP streams.


Call Control
The application that is responsible for controlling the forking device, starting the forking session, and coordinating with the recording engine.

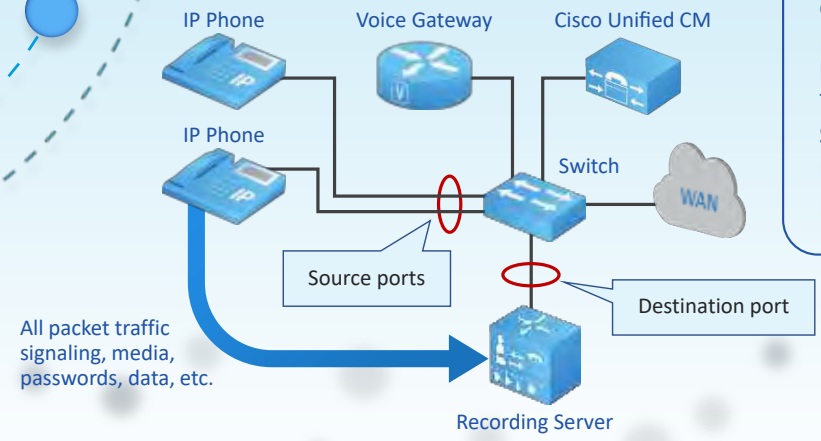
Recording/Monitoring Engine
The application responsible for receiving and recording the forked RTP streams from the forking device.

Call Recording and Monitoring Components



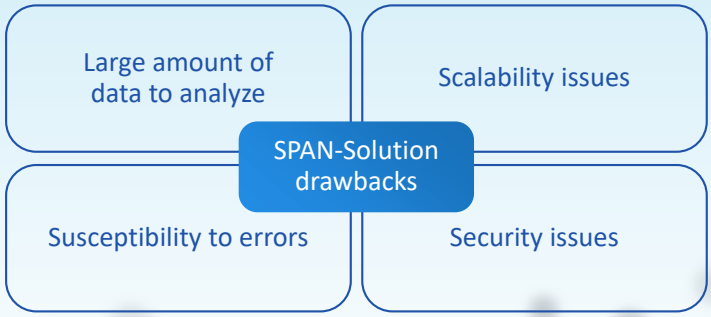


SPAN-Based Solutions



- All packets on the network must be captured by the recording system.
- Isolates relevant media and metadata by from sifting through all packet traffic
- Susceptible to errors
- Does not scale well
- Insecure

SPAN-Based Solution Drawbacks



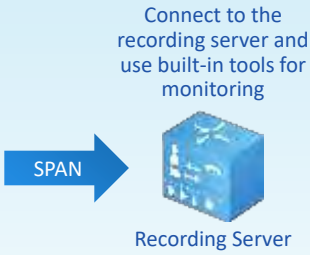
Call Monitoring Using a SPAN-Based Solution

A SPAN-based solution does not differentiate between call recording and call monitoring, because port mirroring simply forks media streams to the recording server

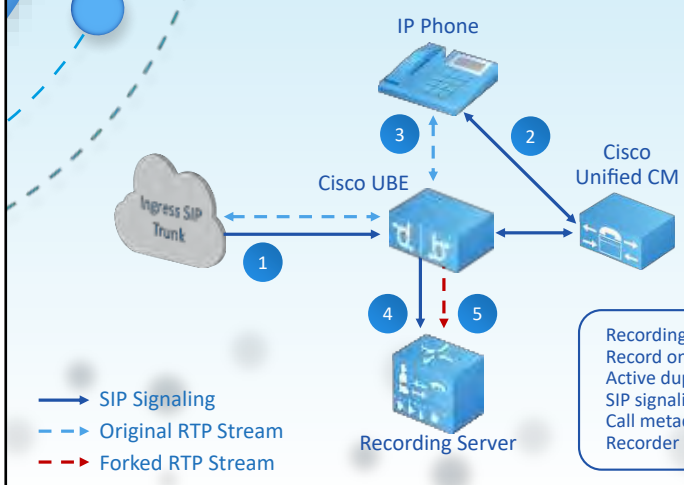
The recording server must provide monitoring capabilities in addition to recording capabilities

For example, while a recording is in progress, Cisco MediaSense allows a third-party streaming-media player or the built-in media player in MediaSense to monitor the session

To monitor a call from a third-party streaming-media player, a client must specify an RTSP URI that can supply HTTP-BASIC credentials and can handle a 302 redirect



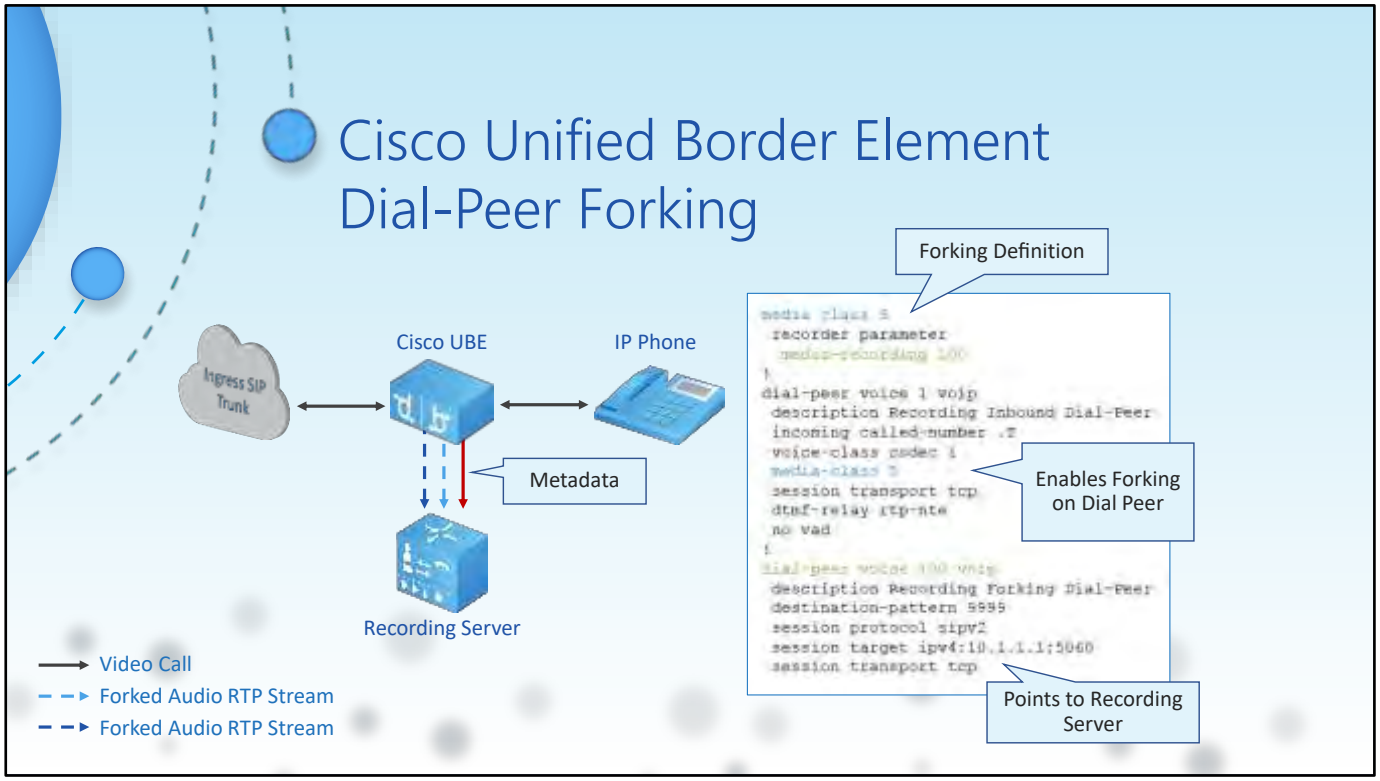
Cisco Unified Border Element Dial-Peer Forking

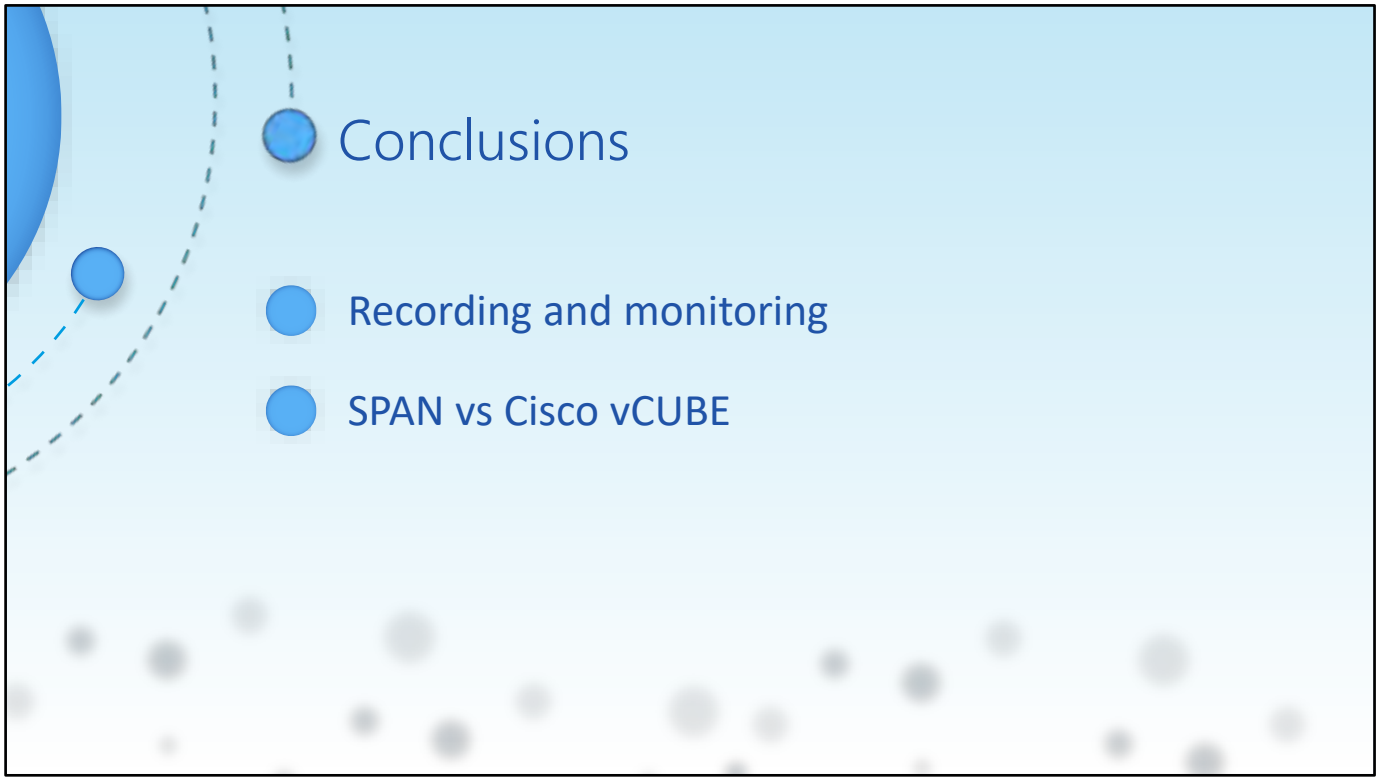


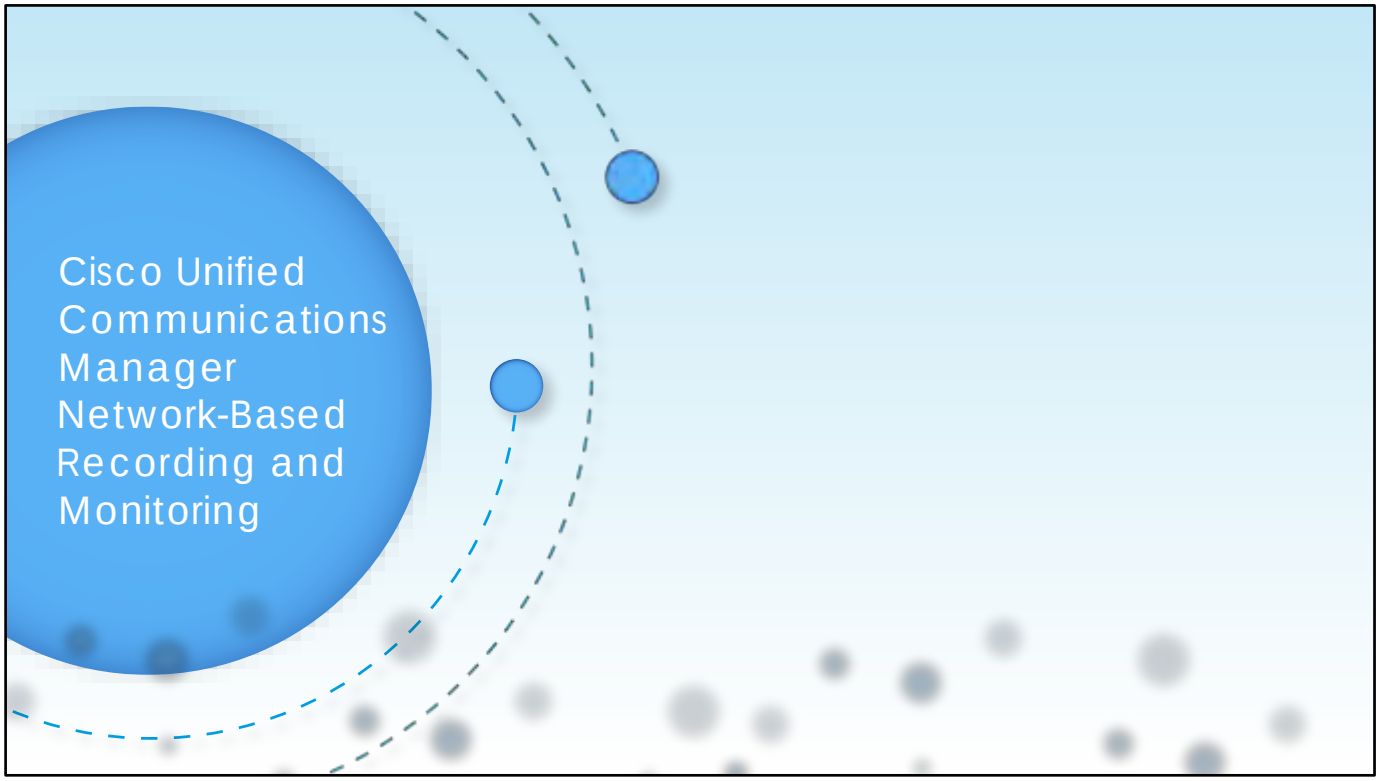
Cisco UBE can be configured to fork the media of a connected call to a recording server and can thus capture the end-to-end conversation from the caller perspective, no matter how the call traverses through the enterprise.

- Recording session invoked by IOS dial peer
- Record on inbound or outbound peer
- Active duplication of all media streams at Cisco UBE
- SIP signaling controls recording sessions
- Call metadata sent via SIP header
- Recorder captures media and metadata

Cisco Unified Border Element Dial-Peer Forking

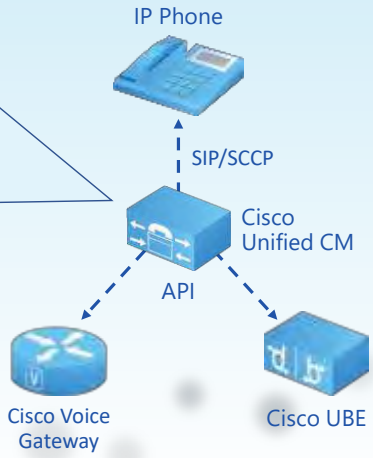






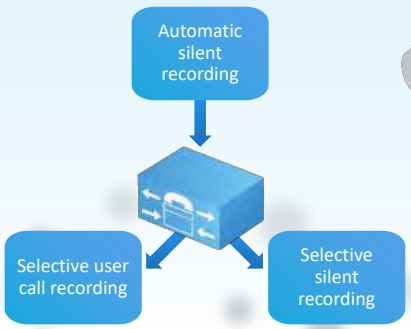
Network-Based Recording and Monitoring

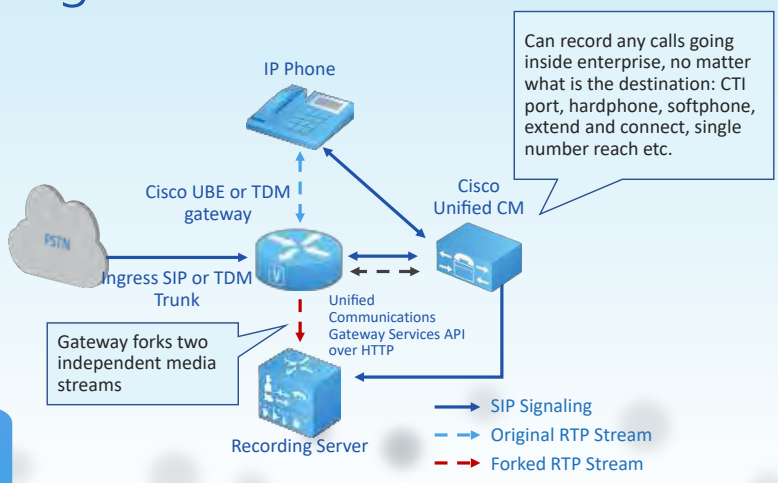
- Allows Cisco Unified CM routed calls to be recorded
  - Regardless of device, location, or geography
- Centralized recording policy control
  - Encompasses BiB and gateway recording
  - Cisco Unified CM selects the best available forking source.
- Cisco Unified CM always provides metadata
  - It resides in the FROM header of the SIP INVITE and other SIP messages.
- Failover is automatic.
  - Forking device Is undetectable to the user.



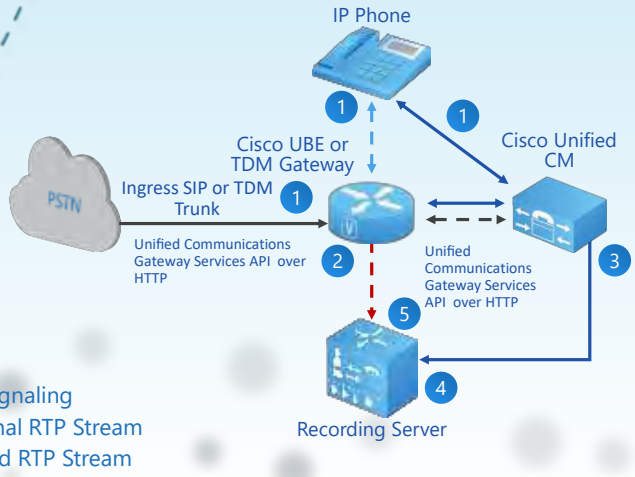
Network-Based Recording and Monitoring

Selection of the recording mode is accomplished by assigning a recording profile to each instance of a line where recording is required.





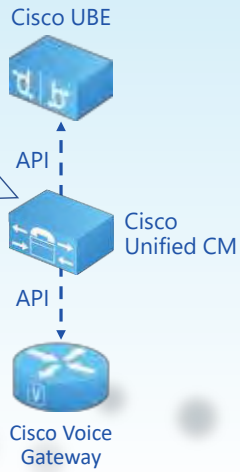
Cisco Unified Communications Manager Network-Based Recording with a Gateway



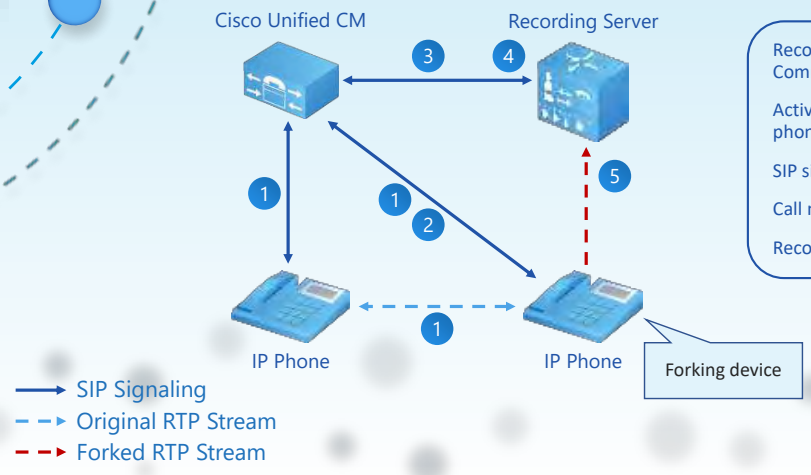
- Recording session invoked by Cisco Unified Communications Manager
- Active duplication of all media streams at Cisco UBE or TDM gateway
- SIP signaling controls recording sessions.
- Call metadata is sent via the SIP header.
- Recorder captures media and metadata.

Cisco Unified Communications Manager Network-Based Recording with a Gateway

- Supported with Cisco Unified CM Release 10.0 and higher.
  - Requires SIP between Cisco Unified Communications Manager and the gateway.
    - Any protocol or interface on the other side
- Router platform must support the Unified Communications Services API
  - Cisco ISR G2, ISR G3 (4000 Series), ASR 1000 Series (including virtual Cisco UBE)
    - Cisco IOS Software Release 15.3(3)M or later
    - Cisco IOS XE Release 3.10S or later
- Cisco AS5400 Series Universal Gateways are not supported.

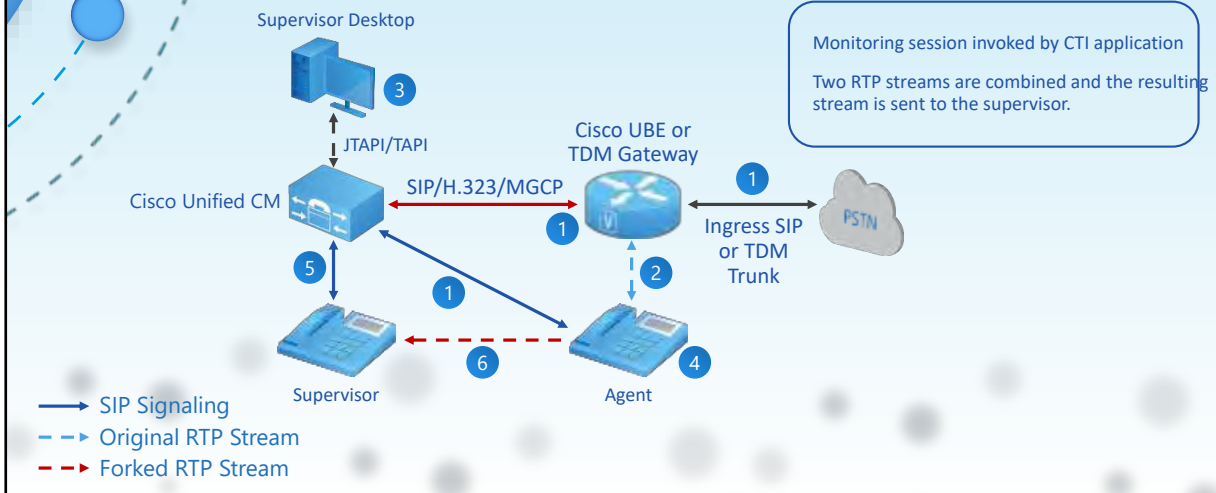


Cisco Unified Communications Manager Network-Based Recording with a BiB



- Recording session invoked by Cisco Unified Communications Manager
- Active duplication of all media streams at the phone BiB
- SIP signaling controls recording sessions.
- Call metadata is sent via the SIP header.
- Recorder captures media and metadata.

Call Monitoring Using Cisco Unified Communications Manager



Monitoring session invoked by CTI application

Two RTP streams are combined and the resulting stream is sent to the supervisor.

Network-Based Recording vs. Cisco Unified Border Element Dial-Peer Forking

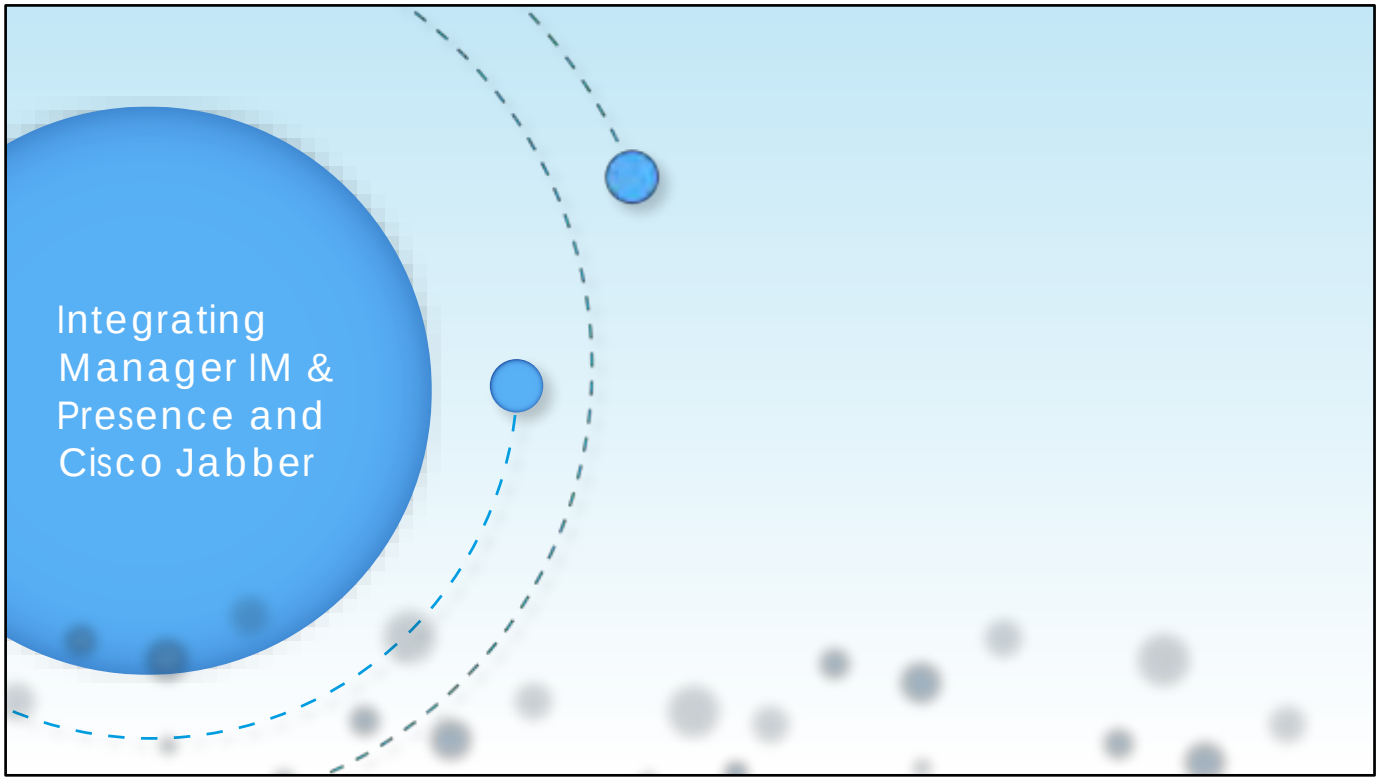
Network-Based Recording	Cisco UBE Dial-Peer Forking
Added to Cisco Unified Communications Manager configuration.	Added to Cisco UBE dial-peer configuration.
Phone or Cisco UBE gateway is the forking device.	Cisco UBE is the forking device.
Controlled by a recording profile assigned to the line.	Controlled by dial-peer selection.
Full-time and selective recording	Full-time recording only
Audio-only call recording	Audio and video call recording
Forking device can change during a call.	Anchored at Cisco UBE until released.

Implement Cisco Unified Communications Manager Call Recording and Monitoring

Demo Time

Conclusions

- Network-based recording and monitoring
  - Gateway
  - BiB
  - Network-Based Recording vs. Cisco Unified Border Element Dial-Peer Forking
  - Demo



Overview

Cisco Jabber is a suite of Cisco Unified Communications applications that allows seamless interaction with your contacts from anywhere.

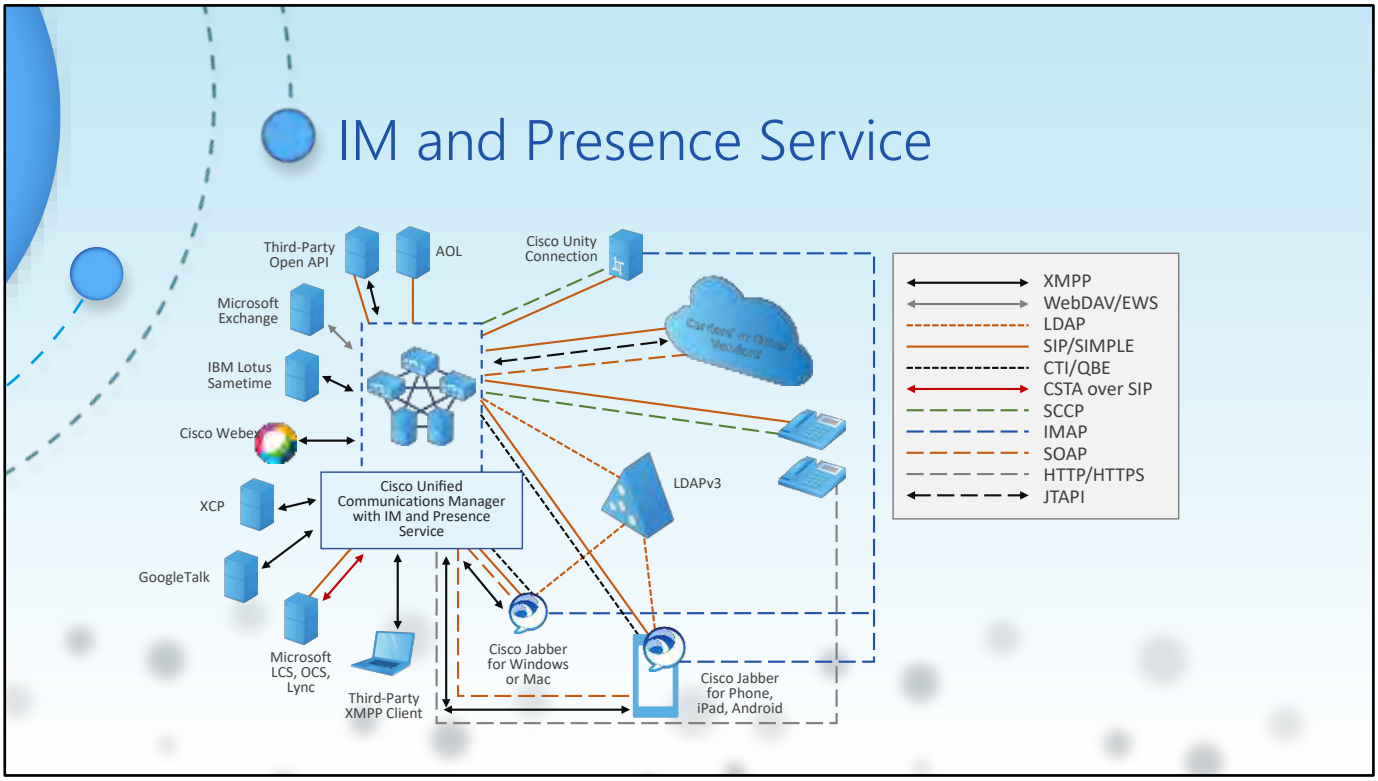
- Offers IM, presence, audio and video calling, voicemail, and conferencing.
- To offer such functionality, Cisco Jabber has to be integrated with many additional Cisco or third-party components
  - Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service)
  - Cisco Unity Connection
  - LDAP servers
  - Microsoft Exchange, and more.

Cisco Unified Communications Manager IM and Presence and Cisco Jabber Integration Overview

Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) comprises many components that enhance the value of a Cisco Unified Communications solution. The following figure shows the IM and Presence Service architecture and the protocols and interfaces that are used to connect to other applications. It encompasses the following:

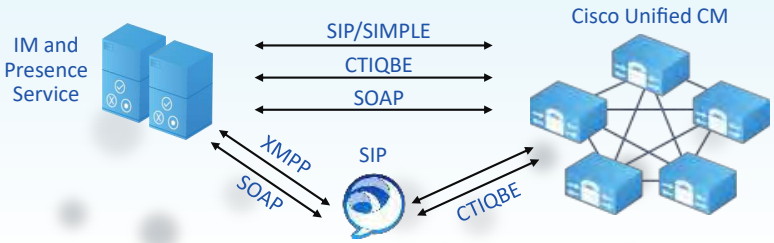
- Cisco IM and Presence Service
- Cisco Unified Communications Manager
- Cisco Jabber
- Cisco Unity Connection
- Lightweight Directory Access Protocol (LDAP) Server v3.0
- Cisco Collaboration voice and video endpoints
- Third-party presence server
- Third-party XMPP clients
- Third-party applications

IM and Presence Service



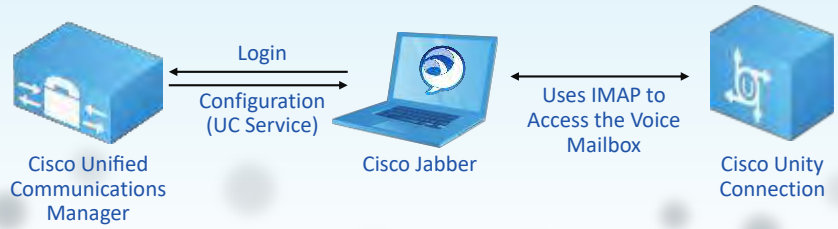
Integration with Cisco Unified Communications Manager and IM and Presence Service

Even the basic functionality of Cisco Jabber requires integration with Cisco Unified Communications Manager and IM and Presence servers. The following figure shows the communications protocols that are involved in this integration.



Integration with Cisco Unity Connection

Cisco Jabber clients use Cisco Unity Connection to retrieve voicemails



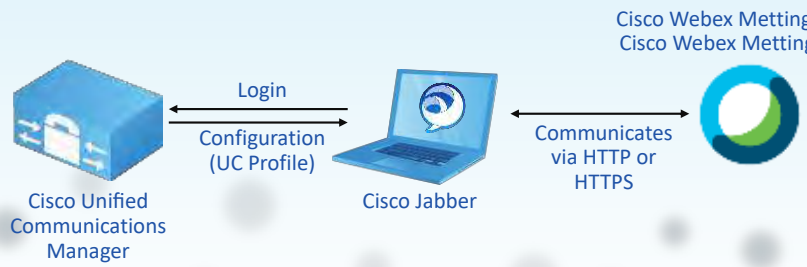
Integration for voice mailbox access in Jabber

Cisco Jabber voicemail integration uses IMAP to access the voice mailbox, which provides the following features

- Users can access voice messages directly from the conversation history pane in the Cisco Jabber client.
- Users can play and delete messages with the integrated media player directly from the Cisco Jabber client.
- Users can easily access presence and availability information about the voicemail caller in the Cisco Jabber client. The user can click to, call the person, to start a web chat, video, or other multimedia session.

Integration with Conferencing Servers

Cisco Jabber uses Cisco Webex for its web conferencing capability.



Webex: HTTP and HTTPS

The web conferencing features of Cisco Webex use HTTP or HTTPS as the transport protocol. You can also add the Cisco TelePresence Management Suite as a video conference scheduling portal.

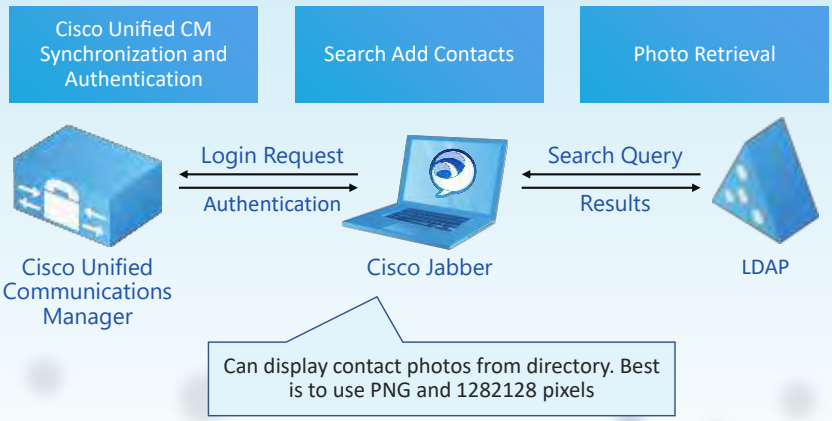
Making a web conference with Cisco Webex

VS

Making audio/video conference with Cisco Meeting Server or Cisco TelePresence Server/MCU*

*Cisco TelePresence Server and TelePresence MCU are EoS/EoL

Integration with LDAP



Integration with Microsoft Exchange

The IM and Presence Service can retrieve a calendar state and aggregate it into the presence status via the calendar module interface with Microsoft Exchange 2010 or 2013 server-side integration. The following table shows the reachability mappings, and how the IM and Presence Service correlates the status of meetings (as shown in Microsoft Outlook calendar) in the availability status of users on the IM and Presence Service:

Microsoft Outlook state	IM and Presence Service State
Free/Tentative	Available
Busy	In a meeting
Out-of-Office	Away
Away	Away

Integration with Microsoft Exchange

Microsoft Exchange

Uses Microsoft Exchange for calendar integration and presence status.

Cisco Unified IM and Presence

Cisco Unified Communications Manager

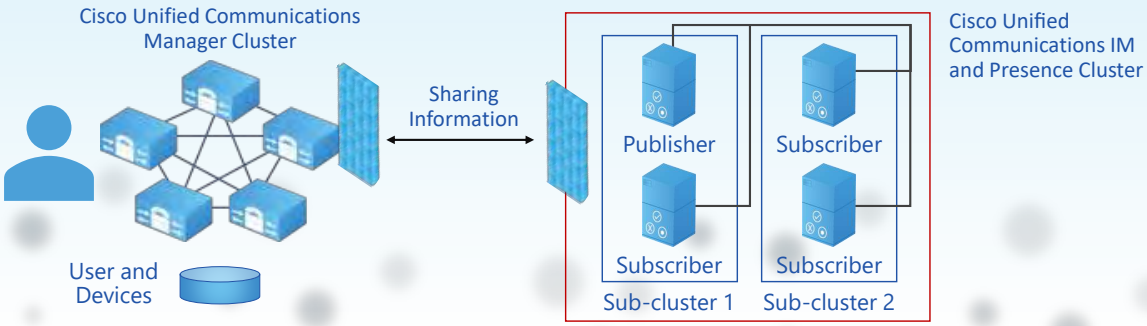
Conclusions

Integrations

- Overview
- IM and Presence Service
- Cisco Unity Connection
- Voice mailbox access
- Webex
- LDAP
- Microsoft exchange

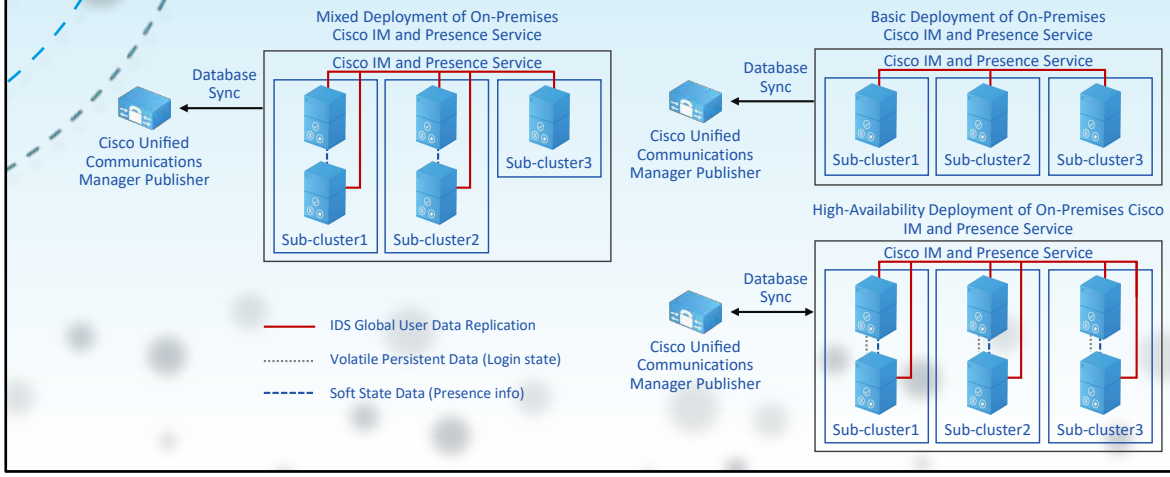
Cisco Unified Communications Manager and IM and Presence Service Clusters

Intracluster traffic participates at a very low level between IM and Presence Service and Cisco Unified Communications Manager and between the IM and Presence Service publisher and subscriber nodes.



IM and Presence Service High Availability

IM and Presence Service relies on the sub-cluster to provide high availability for Cisco Jabber clients.



Capacity

Active/Standby

There are 15,000 users in total; 5,000 users are assigned to the first node of each subcluster

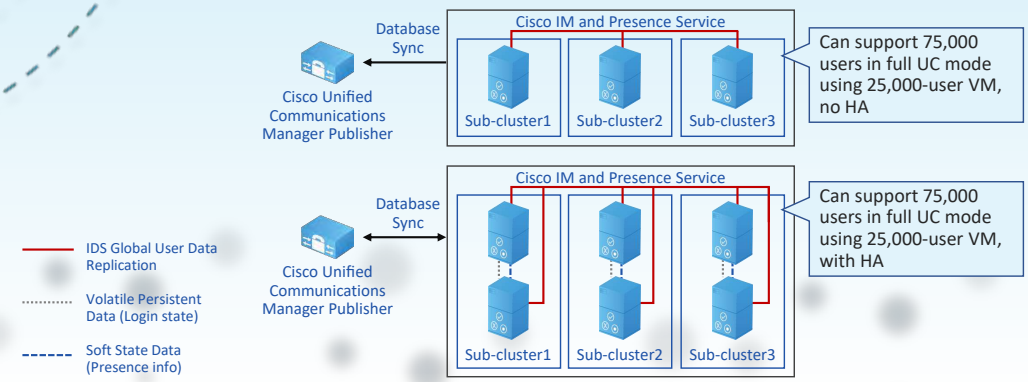
Active/Active

There are 15,000 users in total; 2,500 users are evenly balanced across the six nodes

Cluster Size

The IM and Presence Service cluster supports a maximum of 75,000 users in full unified communications mode, across three single IM and Presence Service nodes deployed with the 25,000-user virtual machine (VM) configuration template but with no high availability

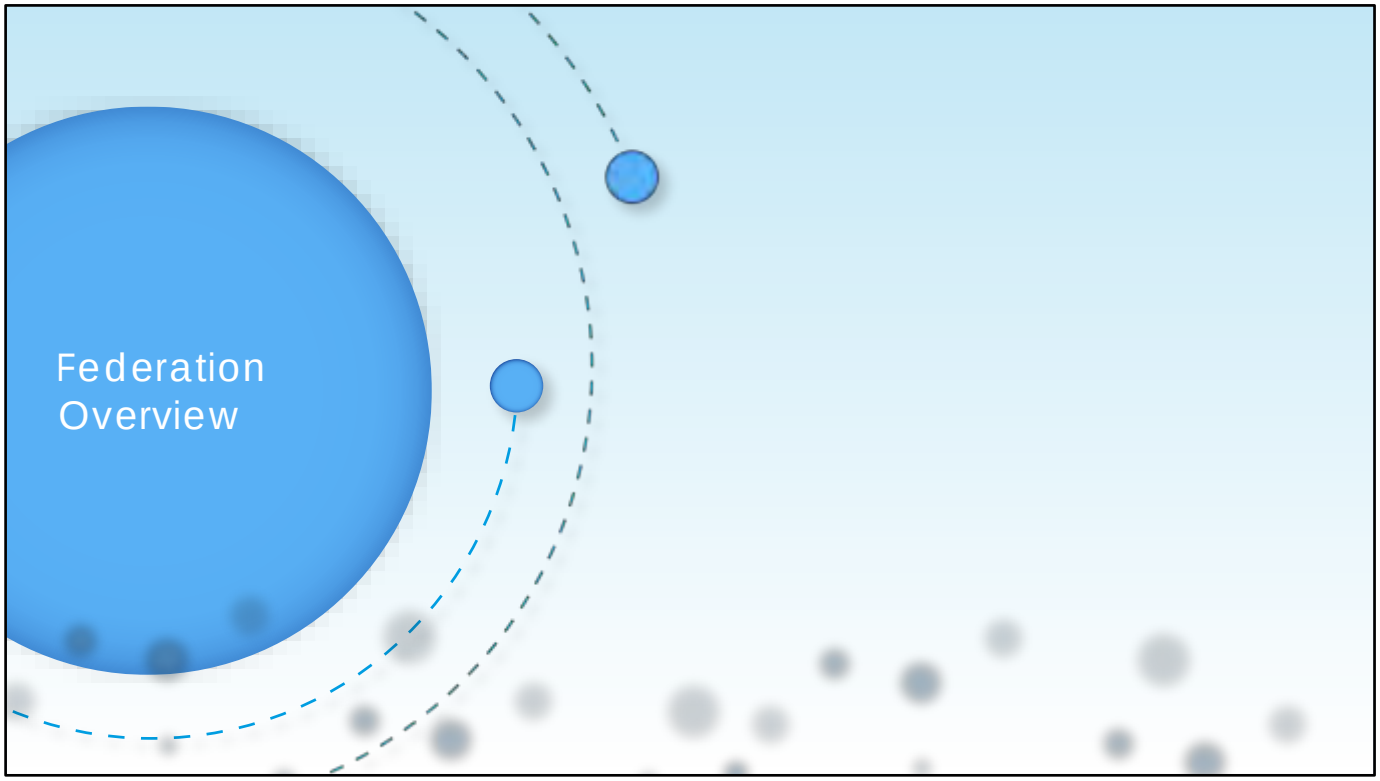
A high-availability deployment for 75,000 users would require three IM and Presence Service sub-cluster pairs that are deployed with the 25,000-user VM configuration template option.



Conclusions

Cisco Unified Communications Manager and IM and Presence Service Clusters

- High availability
- Capacity
- Cluster size

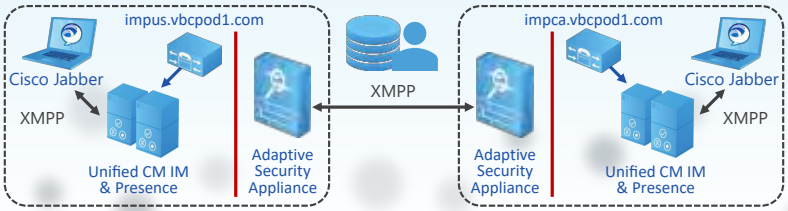


Cisco Unified Communications Manager IM and Presence Service Federation Overview

IM and Presence Service federation, allows you to connect multiple domains, or to connect two systems within a single domain. These processes are referred to as multidomain (interdomain) or intradomain federation, respectively.

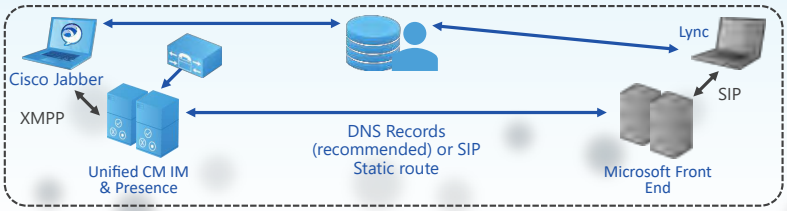
Cisco Unified Communications Manager IM and Presence Service Interdomain Federation Overview

IM and Presence Service allows for business-to-business communications by enabling interdomain federation, which allows the sharing of IM and Presence Service communications between domains



Cisco Unified Communications Manager IM and Presence Service Interdomain Federation Overview

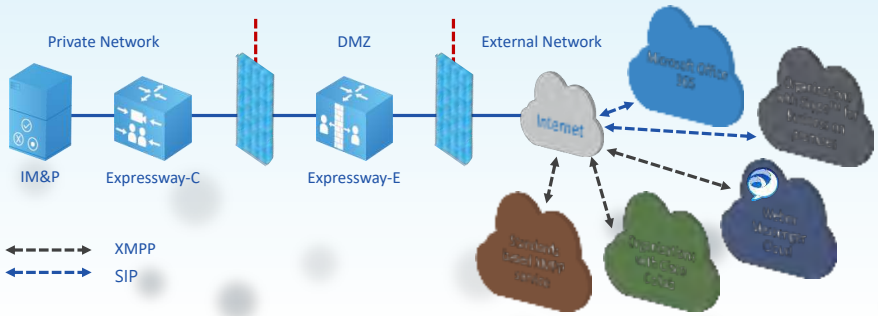
The previous figure shows a basic intradomain federation deployment within the same domain, example.com. The typical use case is to configure partitioned intradomain federation, which enables IM and Presence Service client users and Microsoft Skype for Business or Microsoft Lync users within the same enterprise to exchange presence availability and IMs. This integration allows both IM and Presence Service and the Microsoft server to host a common domain or set of domains. Each user within those domains is enabled on either IM and Presence Service or the Microsoft server



Cisco Unified Communications Manager IM and Presence Multidomain Deployment

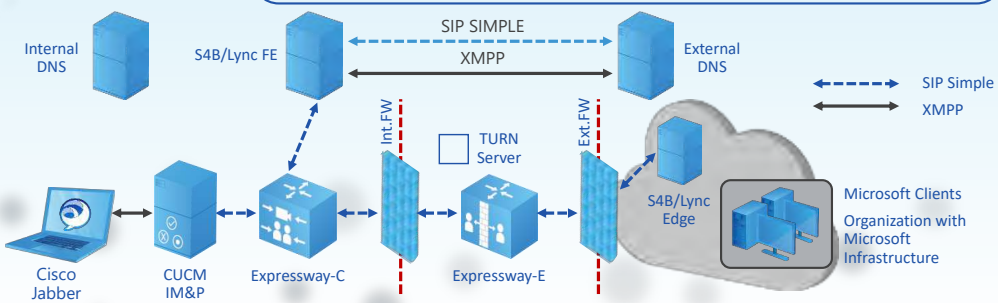
SIP Federation Deployments

IM and Presence Service supports SIP federation with Microsoft systems, such as Skype for Business on-premises or Microsoft Office 365.



Cisco Unified Communications Manager IM and Presence Multidomain Deployment

The following diagram demonstrates both a business-to-business federation and a single-enterprise network federation for a Skype for Business server.



Cisco Unified Communications Manager IM and Presence Multidomain Deployment

The IM and Presence Service uses the standard SIP (RFC 3261) to federate with the following applications:

- Microsoft Office 365 (business-to-business)
- Microsoft Skype for Business 2015, Standard Edition and Enterprise Edition (business-to-business)
- Microsoft Lync 2010 and 2013, Standard Edition and Enterprise Edition
- Microsoft Office Communications Server Release 2 (OCS R2), OCS 2007

SIP Federation Configuration Flow

The figure shows a list of tasks to configure interdomain federation with an on-premises or remote Skype for Business server. These steps work to enable both: a business-to-business integration with another business that is deploying an on-premises Skype for Business server; and within a single enterprise, to configure interdomain federation between the IM and Presence Service and an on-premises Skype for Business server

Follow these steps on the IM and Presence Service server:

Step 1. Turn on Federation Services on the IM and Presence Service (Cisco XCP SIP Federation Connection Manager service).

Step 2. Add a Federated domain entry for each Skype for Business domain with which you want to federate.

Step 3. Configure a static route for Skype for Business users. The static route must use TLS and point to Cisco Expressway-C.

Step 4. Add inbound ACL entries for each Cisco Expressway-C server so that Expressway-C can access the IM and Presence Service without authentication.

Step 5. Restart the Cisco XCP Router.

Steps for Cisco Espressways

Follow these steps on the Cisco Expressways:

Step 1a. For business-to-business interdomain federation, you must deploy both Cisco Expressway-C and Expressway-E.

Step 1b. For intracompany interdomain federation, you can deploy only a Cisco Expressway-C cluster, because the communication does not need to extend across the WAN.

Step 2. Configure a DNS SRV record (_sipfederationtls._tcp.domain) to make your Cisco Expressway-E known to business partners.

Follow these steps on the Cisco Expressways:

Steps for Skype for Business

Follow these steps on the Skype for Business server:

Skype for Business Server

Step 1. Configure user trust settings for federated IM and Presence Service users.

Step 2. Configure global access edge settings for SIP federation.

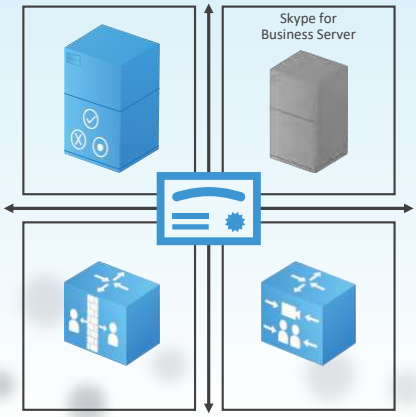
Step 3. If the **Global Access Edge** settings on the Skype for Business server do not allow all domains, add a specific entry for the IM and Presence Service domain.

Step 4. You must add Cisco Expressway manually as a SIP Federation Provider for IM and Presence Service if you are not using a DNS SRV record to route traffic from Skype for Business.

Follow these steps on the Skype for Business server:

Exchanging Certificates

Finally, you need to exchange certificates among the servers in your deployment.



XMPP Federation Deployments

Overview

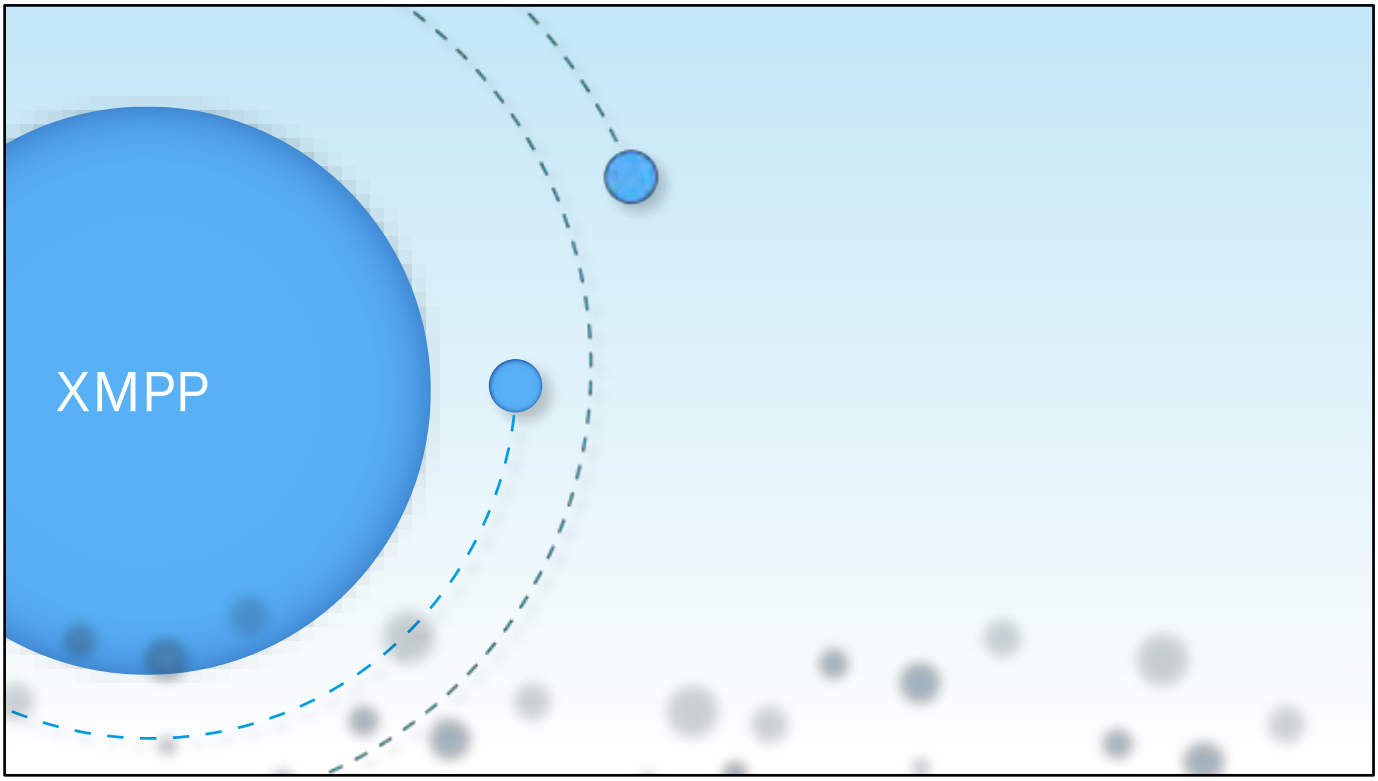
Interdomain Federation Overview

Multidomain Deployment

SIP Federation Configuration Flow

Steps

Certificates



XMPP Federation Deployments

You can use XMPP federation to integrate with another IM and Presence Service cluster in another domain over the Internet.

- It is possible to configure external XMPP federation from an on-premises IM and Presence Service server through Cisco Expressway or through the IM and Presence Service.

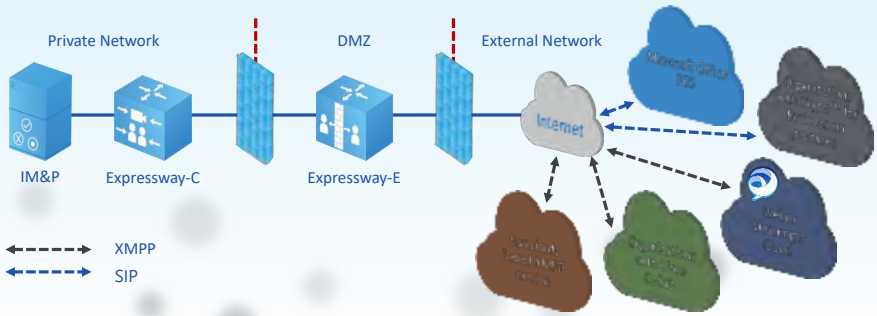
The preferred method for deploying external XMPP federation is through Cisco Expressway.

- enables users who are registered with the IM and Presence Service to communicate via Cisco Expressway-E with users from a different XMPP deployment.

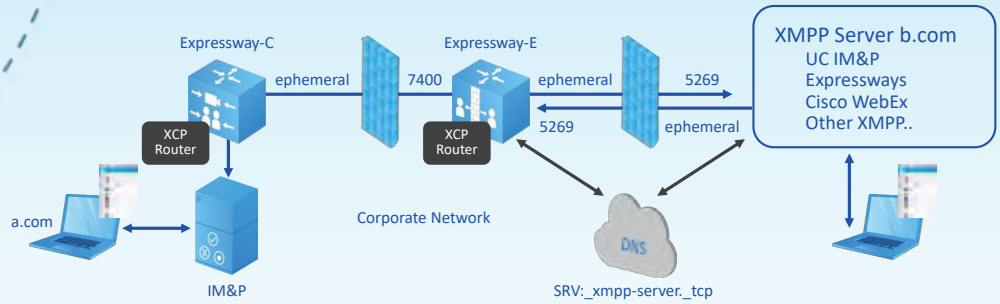
XMPP Federation

Cisco Expressway-E supports XMPP federation with the following entities:

- Cisco Unified Communications Manager IM and Presence Service Release 9.1 or later
- Cisco WebEx Connect Release 6.x
- XMPP standards-compliant servers



XMPP Federation Deployments



XMPP Federation Configuration Flow

Step 1. Configure a DNS SRV record (_xmpp-server-_tcp.externaldomain) to make your IM and Presence Service aware of the external domain.

Step 2. Validate the email address for federation.

Step 3. Ensure that the IM and Presence Service is operational and has XMPP federation is turned off.

Follow these steps on Cisco Expressways:

Step 1. Configure a DNS SRV record (_xmpp-server._tcp.domain) to make your Expressway-E known to business partners.

Step 2. Expressway-E: Enable XMPP federation.

Step 3. Expressway-E: Optionally, configure static routes (if not using DNS lookup).

Step 4. Expressway-E: Configure XMPP parameters (Dialback secret, TLS settings, and Allow/Deny List).

Step 5. Expressway-C: Configure the domains that are enabled for XMPP federation.

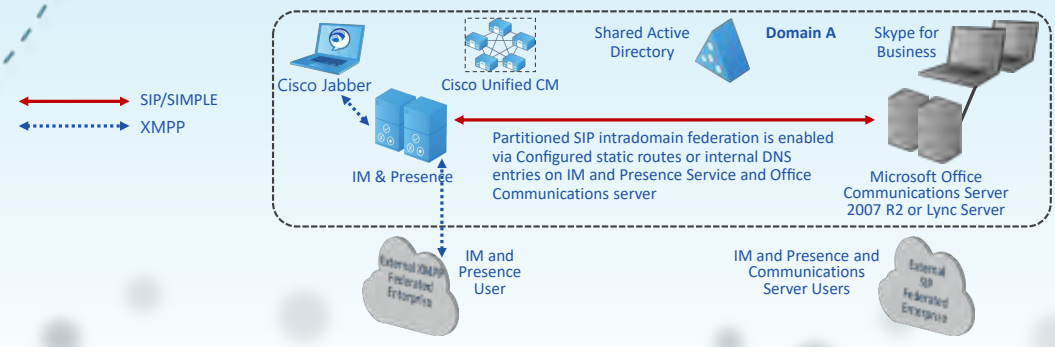
You also need to complete the following steps:

Step 1. Check that the correct firewall ports are open (5269 and 7400).

Step 2. Complete the server certificate requirements:

- IM and Presence Service certificates (cup-xmpp and tomcat).
- Cisco Expressway certificates (need to incorporate relevant Subject Alternate Name entries).

Cisco Unified Communications Manager IM and Presence Intradomain Federation

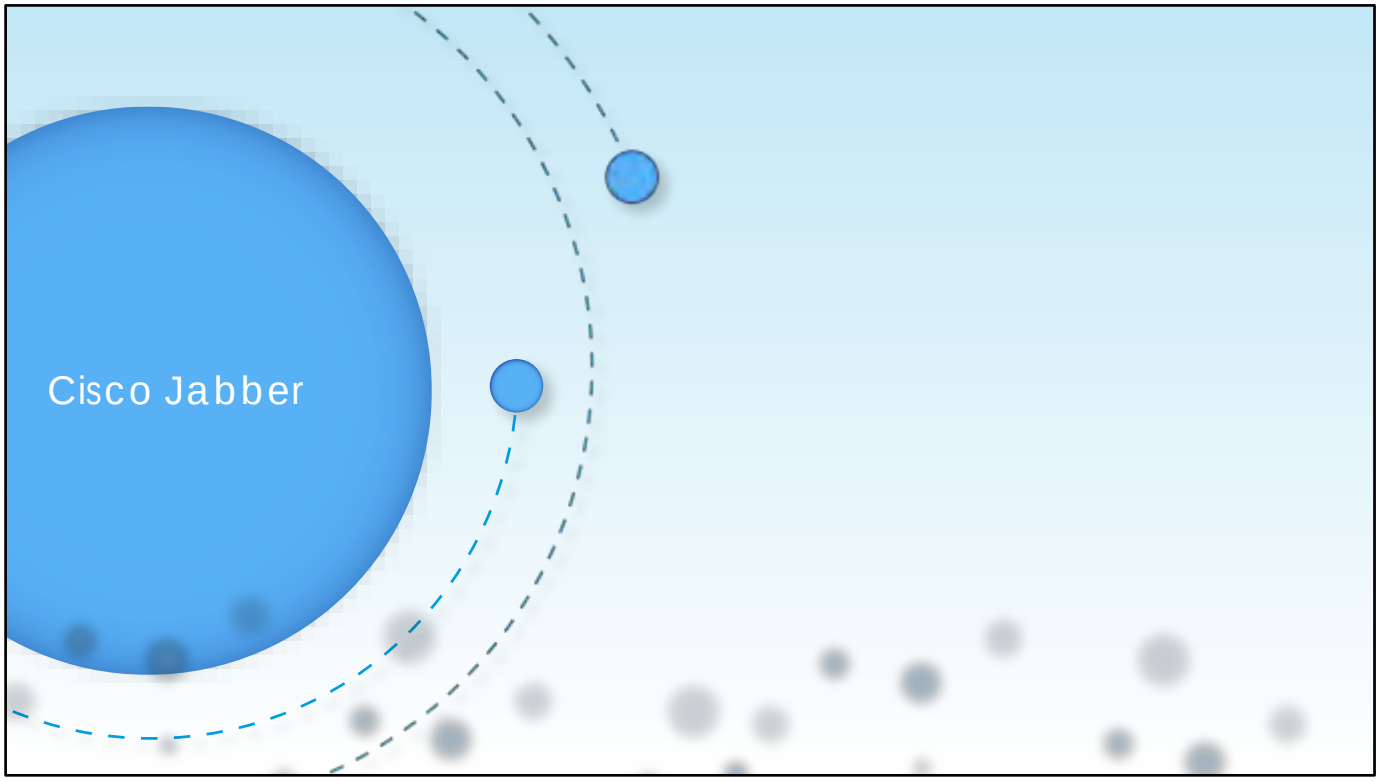


Conclusions

XMPP

Federation

Steps on Cisco Expressways



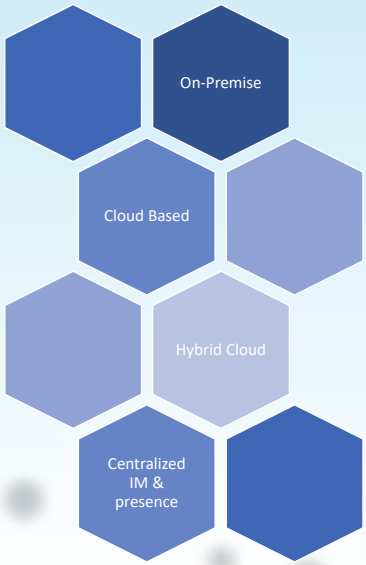
Cisco Jabber Deployment Options

Jabber Client Deployment Overview

Your choice of deployment depends primarily on your product choice for IM and presence and the requirement for additional services such as voice and video, voicemail, and desk phone control

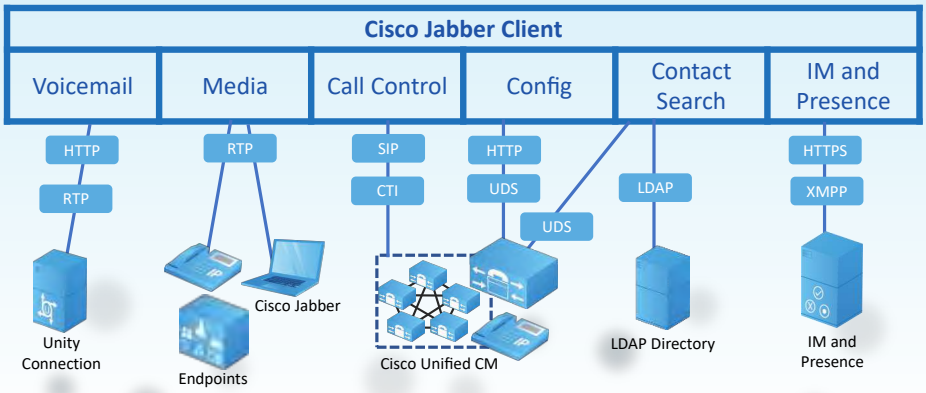
Cisco Jabber desktop clients support the following deployment models:

- On-premises deployment models
- Cloud-based deployment models
- Hybrid cloud-based and on-premises deployment models
- Centralized IM and presence deployments



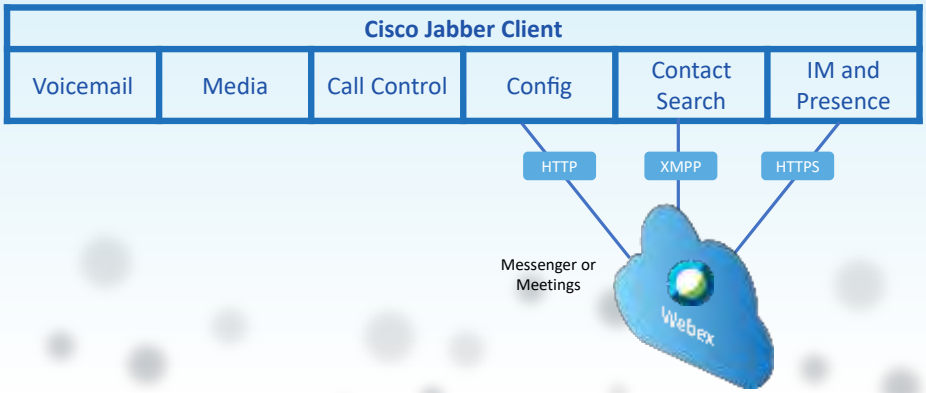
On-Premises Deployment

In the on-premises deployment model, all services are set up and configured on an enterprise network that you manage and maintain.



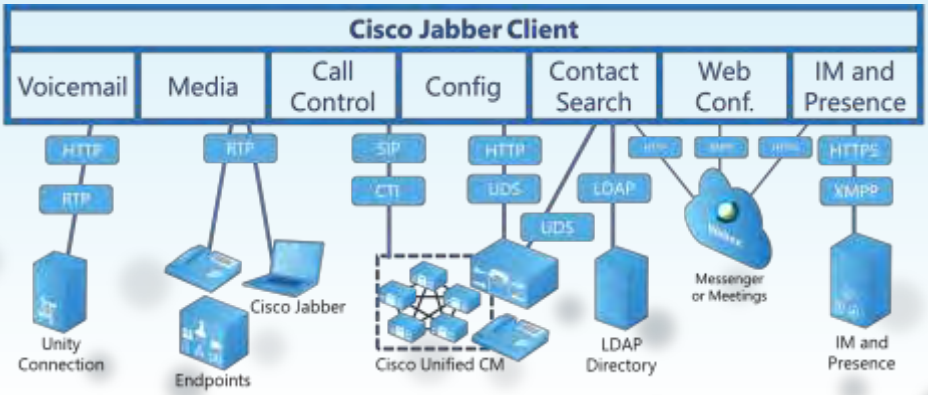
Cloud-Based Deployment

In the cloud-based deployment model, all (or most) services are hosted in the cloud using Cisco Webex. When implementing a cloud-based deployment model using Cisco Webex, you manage and monitor your cloud-based deployment with the Cisco Webex Administration Tool



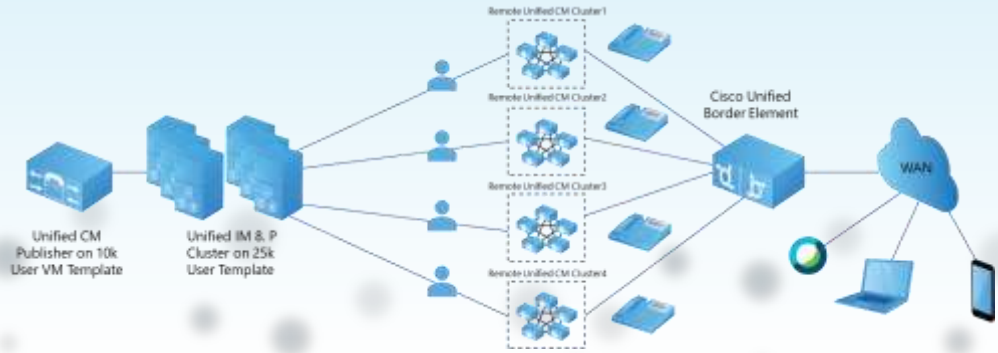
Hybrid Cloud-Based and On-Premises Deployment

In a hybrid deployment, the cloud-based services that are hosted on Cisco Webex Messenger service are combined with Cisco Unified Communications Manager and Cisco Unity Connection.



Centralized IM and Presence Deployment

Centralized IM and Presence Service deployment can provide presence services to multiple remote Cisco Unified Communications Manager voice and video clusters. In a centralized deployment, IM and Presence Service manages all presence-related services for all the users across the remote Cisco Unified Communications Manager clusters, and each remote Cisco Unified CM cluster manages the voice and video needs of its own users.



Cisco Jabber in Deskphone Control Mode

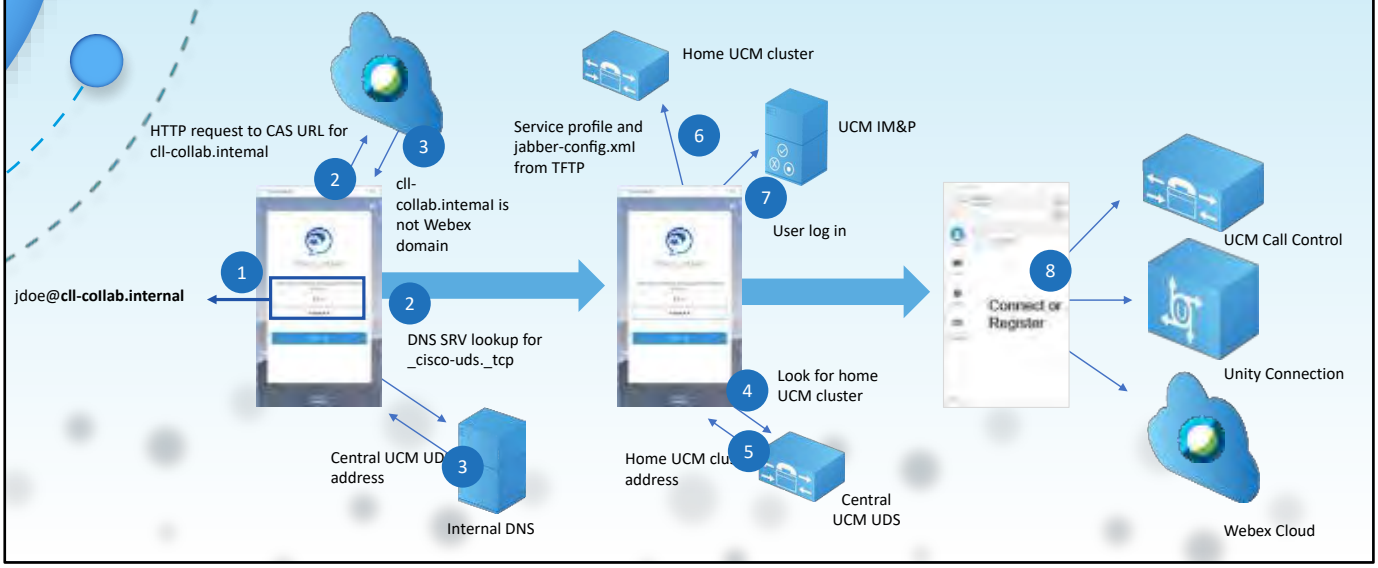
You can use Cisco Jabber in deskphone control mode to control the desk phone to initiate and answer calls.

Cisco Jabber in Softphone Mode

You can use Cisco Jabber in softphone mode to call when access to a desk phone device is not available.

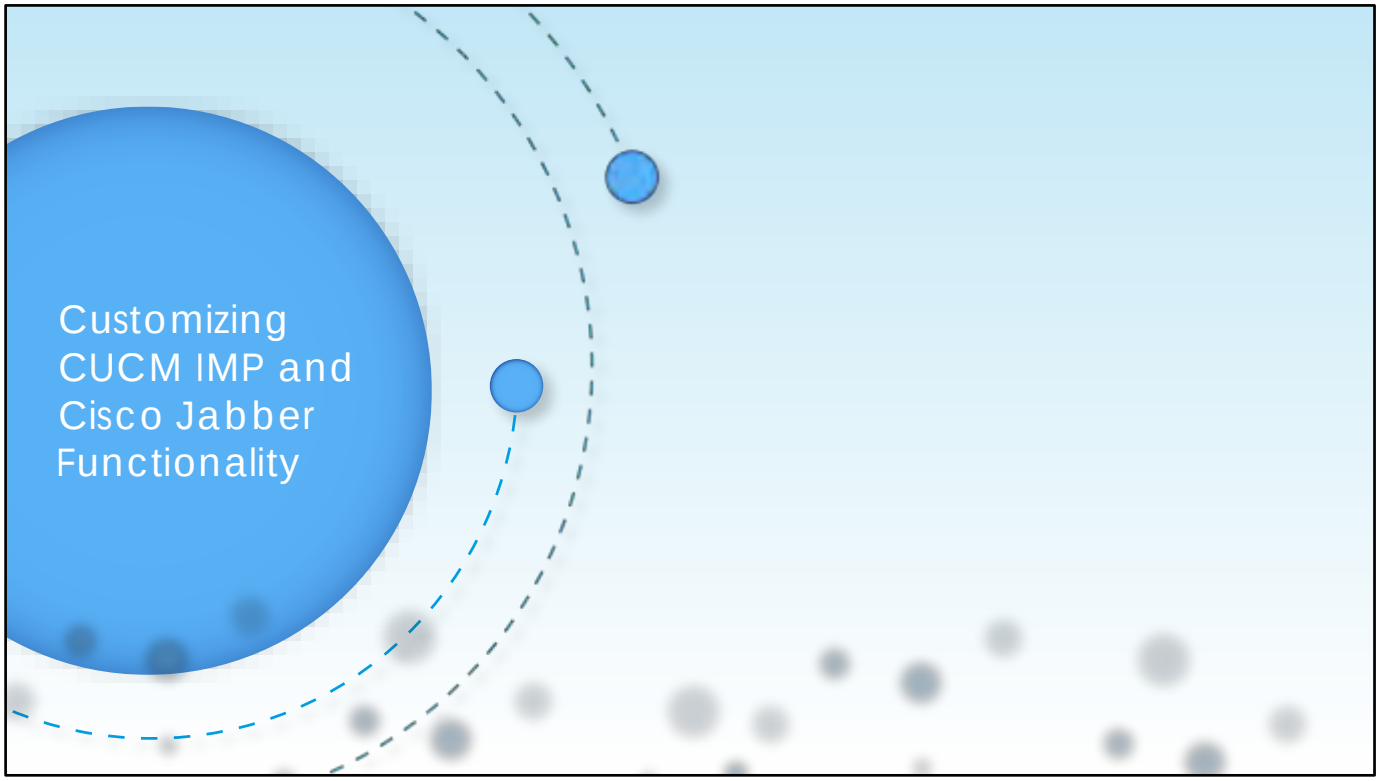
Cisco Jabber Service Discovery Process

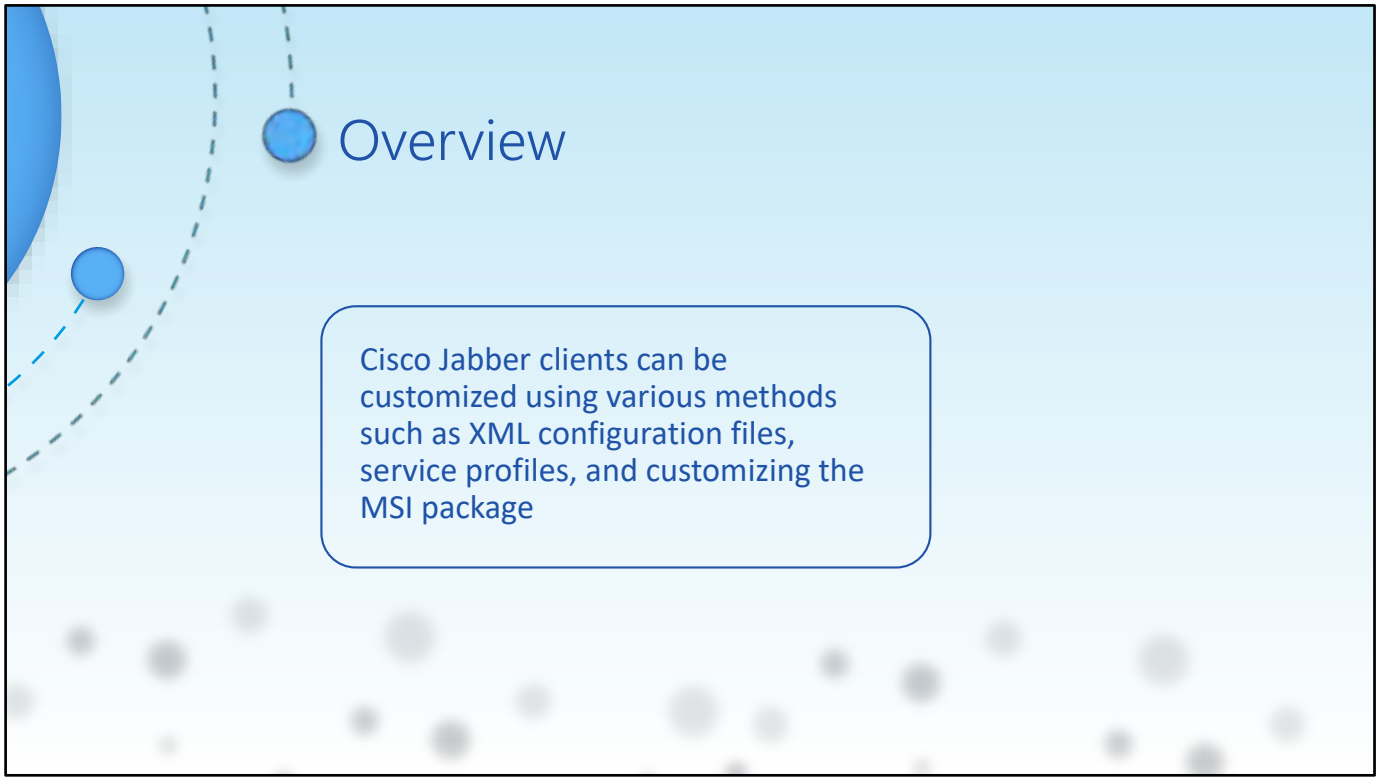
To discover available services, the Cisco Jabber client does the following:



Cisco Jabber Deployment Options

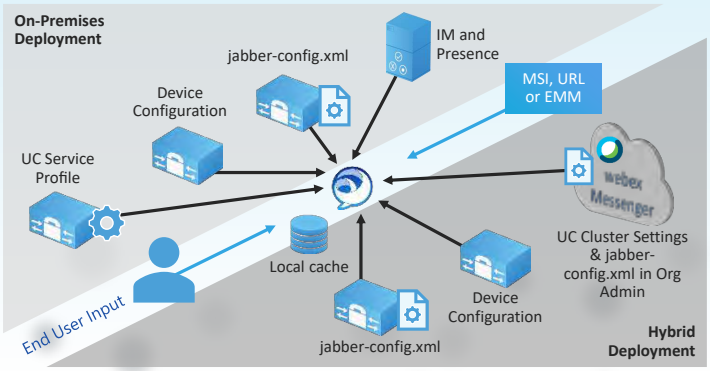
- Cisco Jabber
  - Deployment Options
    - On-Prem
    - Cloud-based
    - Hybrid
    - Centralized IM and Presence deployment
  - Desk phone control mode
  - Softphone mode
  - Service discovery process





Cisco Jabber Customization Overview

Multiple options are available to configure Cisco Jabber clients, but using the client XML configuration file gives you full control of most Cisco Jabber options



Cisco Jabber Customization Overview

Jabber Settings for on premise IM&P

Service Profiles from Cisco Unified CM

Phone Configuration in Cisco Unified CM

Cisco Unified Communications Manager IM and Presence settings

Client configuration files: Jabber-config.xml file from TFTP Server

Highest Priority

Cisco Jabber Customization Overview

Jabber Settings for Webex Cloud IM&P

Webex Administration settings

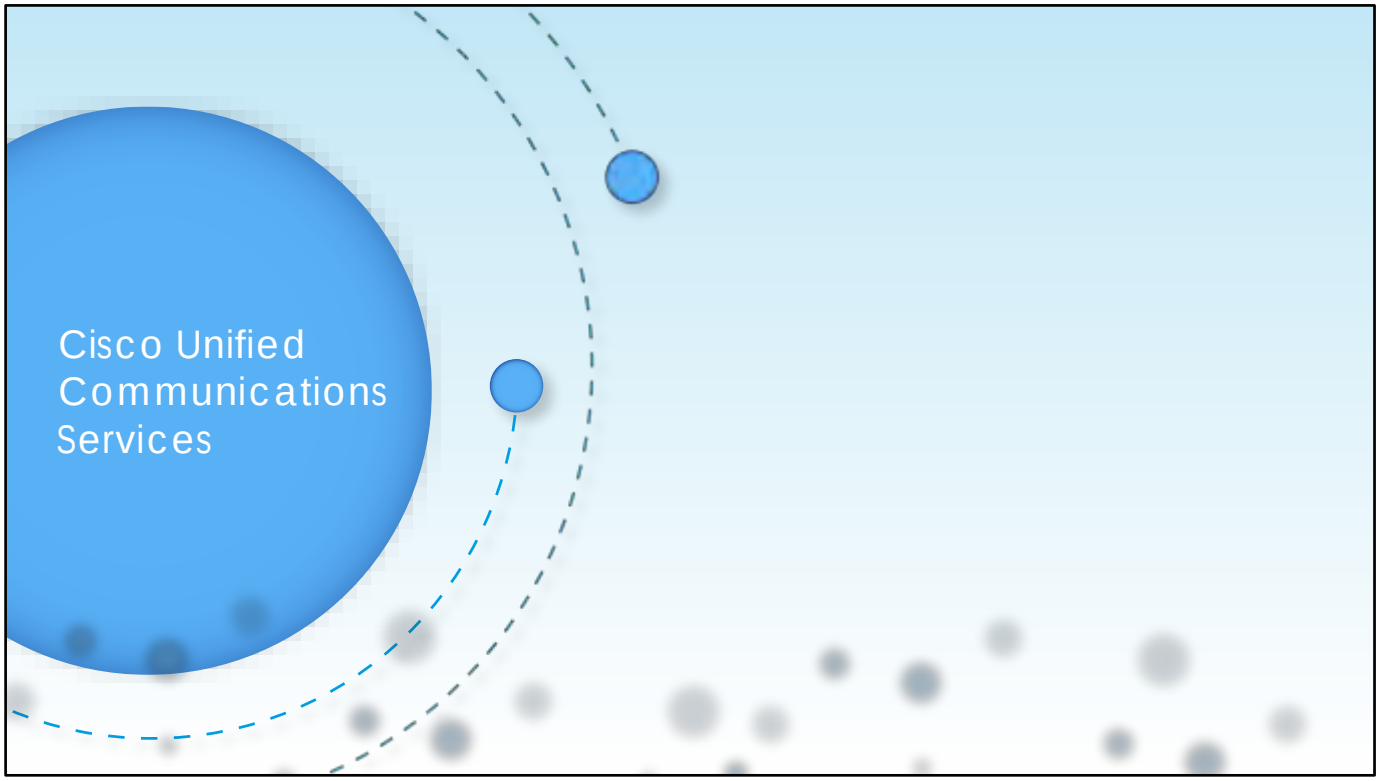
Service Profiles from Cisco Unified CM

Phone Configuration in Cisco Unified CM

Client configuration files: Jabber-config.xml file from Webex Administration

Client configuration files: Jabber-config.xml file from Cisco Unified CM

Highest Priority



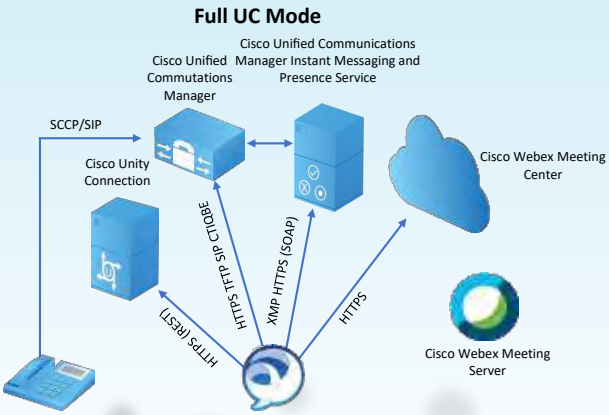
On-Premises Deployment

In an on-premises deployment, you set up, manage, and maintain all services on your corporate network

You can deploy Cisco Jabber in the following modes:

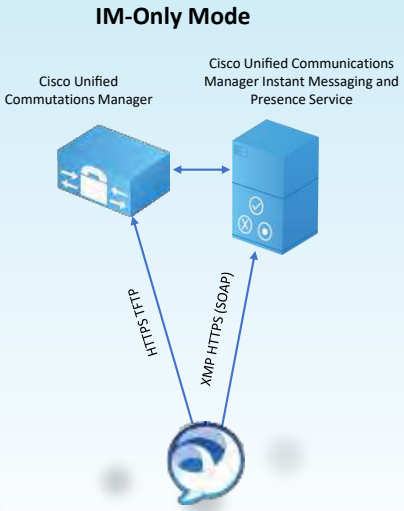
IM Mode

Full UC mode: To deploy full UC mode, enable instant messaging and presence capabilities, provision voicemail and conferencing capabilities, and provision users with devices for audio and video



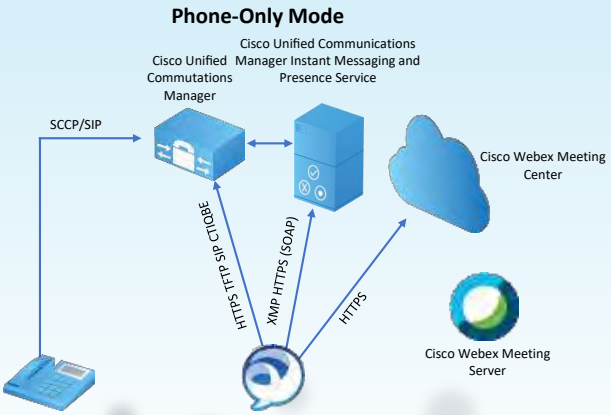
IM-only mode

IM-only: To deploy IM-only mode, enable instant messaging and presence capabilities. Do not provision users with devices.



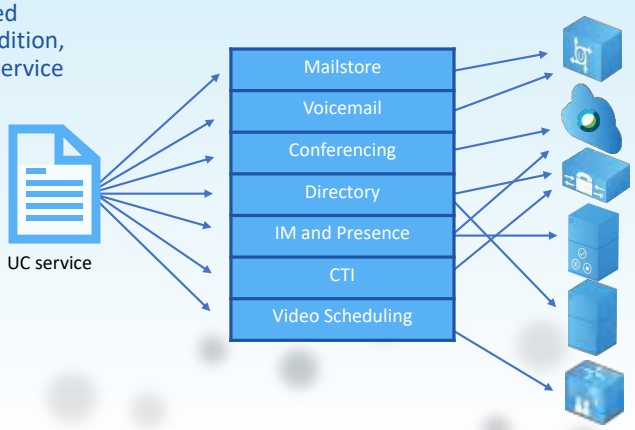
Phone-only mode

Phone-only mode: In phone-only mode, primary authentication for the user is to Cisco Unified Communications Manager. To deploy phone-only mode, provision users with devices for audio and video capabilities. You can also provision users with additional services such as voicemail.



Cisco Unified Communications Manager Services Overview

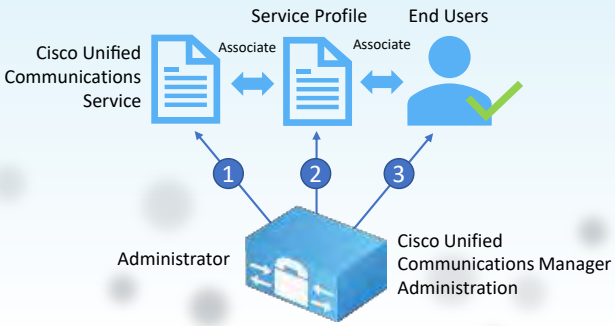
Presence is enabled per user in the user configuration in Cisco Unified Communications Manager. In addition, you must assign services to the service profile.



Service Profiles

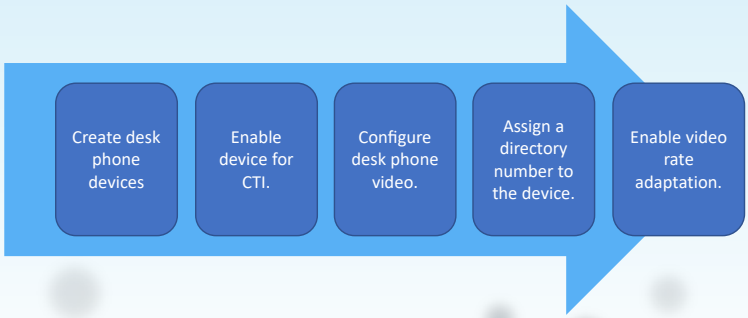
With the service profile and the Cisco Unified Communications services that you chose in the profile, you can add feature access to Cisco Jabber.

When service discovery or manual configuration is complete, Jabber must authenticate and download a service profile and, if available, the jabber-config.xml file.



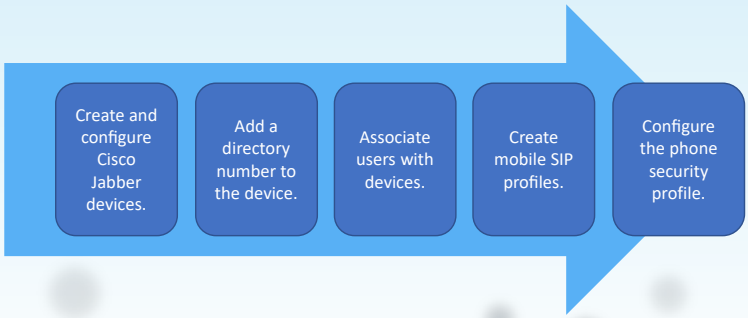
Configure Desk Phone Control Mode

In deskphone control mode, Cisco Jabber allows control of the desk phone to initiate and answer calls.



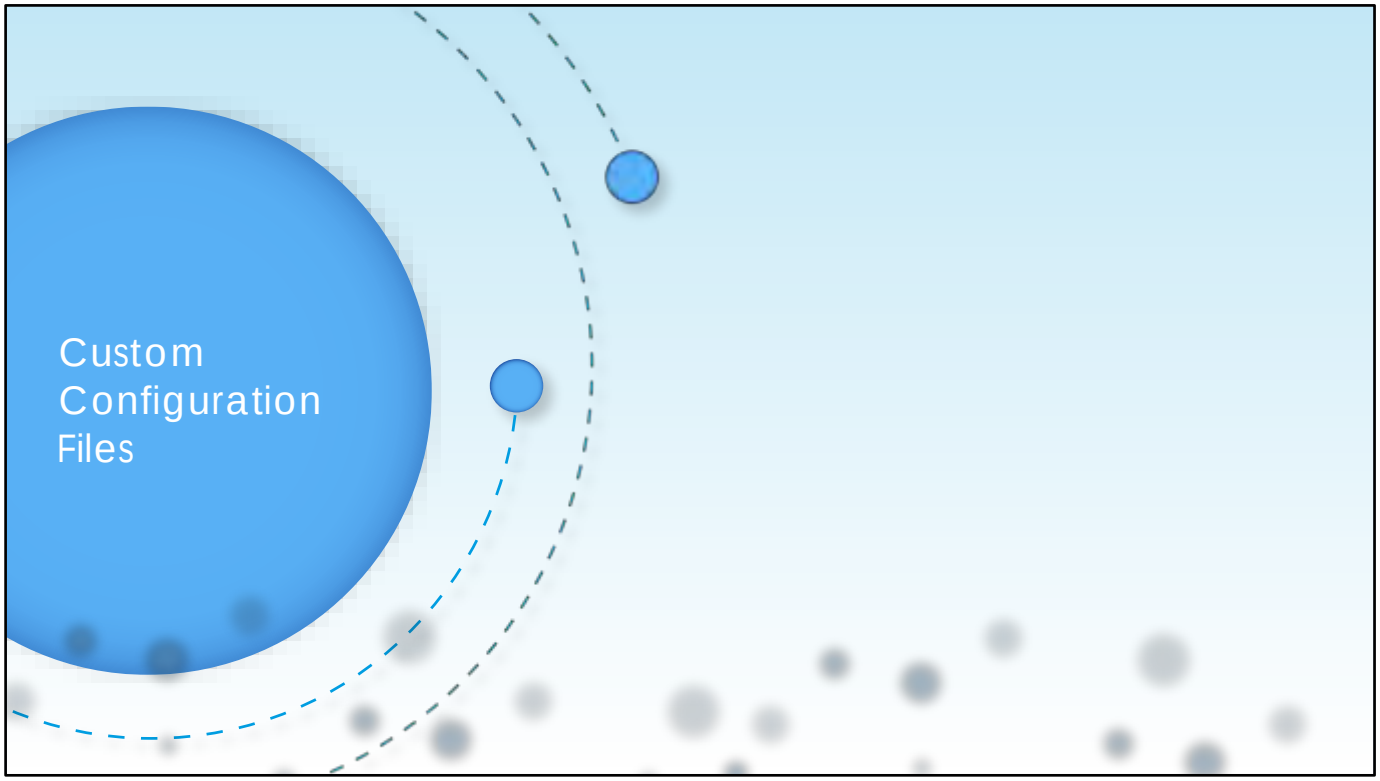
Configure Softphone Mode

Cisco Jabber can place calls in softphone mode, when access to a desk phone device is not available.



Conclusions

- On Premises
- IM Mode only
- Phone-only
- CUCM services overview
- Service profiles
- Desk phone mode
- Softphone mode



Custom Configuration Files

You can use Cisco Jabber configuration files to control client settings.

Cisco Jabber User Configuration XML File

You can create a Cisco Jabber XML configuration file in a few steps.

Configuration Overview

If the service profile does not provide access to the settings, the client can download the jabber-config.xml file. You can view the current jabber-config.xml file at http://<Unified-CM-IPaddress>:6970/jabber-config.xml.

http://<Unified-CM-IPaddress>:6970/jabber-config.xml

- Enable Persistent Chat
- Enable URI dialing
- Load on operating system start
- Docked window
- Enable screen capture
- File transfer controls
- Enable video
- Enable chat history

Global and Group Configuration Files

Cisco Jabber configuration files can be applied globally or to individual users.

Global Configuration Files	Group Configuration Files
All Cisco Jabber for Windows users	Subsets of Cisco Jabber for Windows users
Default name: jabber-config.xml	Takes priority over global configuration files

Global Configuration Files

Global configuration files apply to all Cisco Jabber for Windows users. Cisco Jabber for Windows downloads the global configuration file from your TFTP server during the login sequence.

The default name for the global configuration file is jabber-config.xml.

Users are signed in and use software phones for calls:

Cisco Jabber for Windows notifies users about the change to their configuration settings.

Users sign out.

Users sign in.

Cisco Jabber for Windows loads the group configuration settings.

Users are signed in and use desk phones for calls:

Users sign out.

Users sign in.

Cisco Jabber for Windows notifies the users about the change to their configuration settings.

Users sign out.

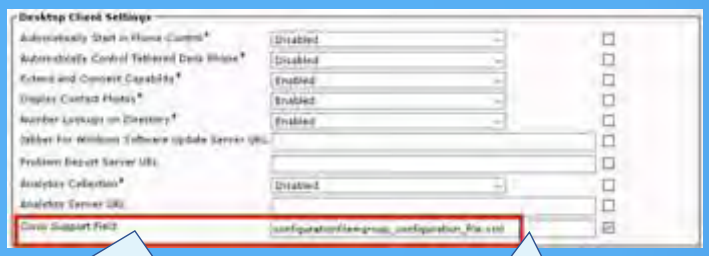
Users sign in.

Cisco Jabber for Windows loads the group configuration settings.

If users choose the option to use software phones for calls before they sign out, Cisco Jabber for Windows notifies users to sign out and sign in again to load the group configuration settings.

Group Configuration File Names

Specify the name of the group configuration files in the Cisco Support field in the Cisco Unified CSF device configuration in Cisco Unified Communications Manager.



Instead use TFTP_FILE_NAME installation argument if users have desk phone devices only

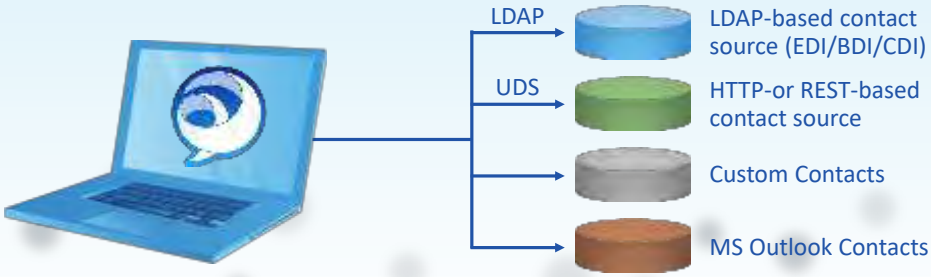
Specify name of group config file here

Configuration File Structure

Cisco Jabber configuration relies on XML structure.

Contact Sources

A contact source is a collection of data for users. When users search for contacts or add contacts in the Cisco Jabber client, the contact information is read from a contact source.



What Is a Contact Source?

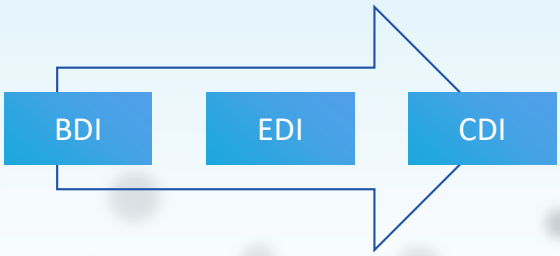
Cisco Jabber retrieves information from the contact source to populate contact lists and update contact cards in the client and other areas that display contact information. When the client receives incoming communications, for example, an instant message or a voice or video call, the contact source is used to resolve the contact information

In on-premises deployments, the client requires one of the following contact sources to resolve directory lookups for user information:

- LDAP: If you have a corporate directory, LDAP is used for directory lookups.
- Cisco Unified Communications Manager UDS: If you do not have a corporate directory or if your deployment includes users who are connecting with Cisco Expressway mobile and remote access, you can use this option.

Cisco Jabber LDAP Contact Source

Cisco Jabber relies on EDI, BDI, or CDI integrate with LDAP contact sources.

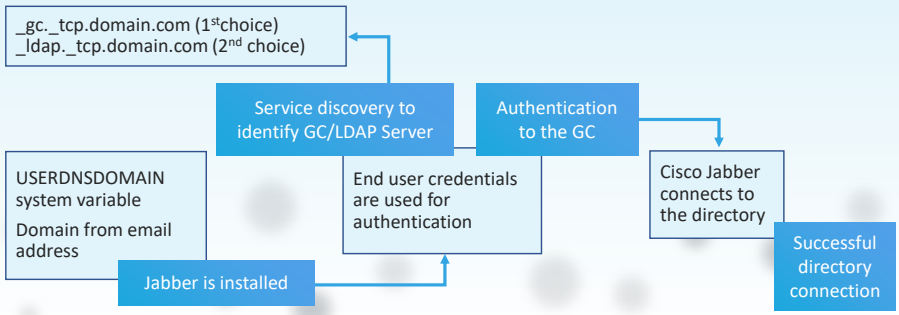


Cisco Directory Interface

CDI is the default method of directory integration for on-premises Jabber clients and is recommended from Jabber 11.8. CDI uses service discovery to determine the LDAP server.

The following are the default settings for on-premises deployments with CDI:

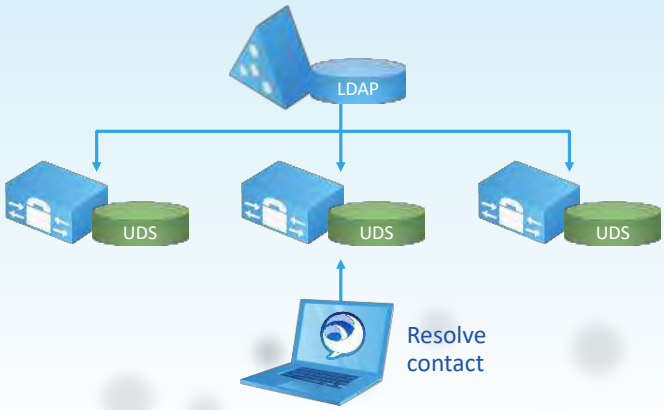
- Cisco Jabber integrates with Active Directory as the contact source.
- Cisco Jabber automatically discovers and connects to a Global Catalog (GC).



Cisco User Data Service Directory Access

User Data Service (UDS) is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

- Cisco Jabber is connected via mobile and remote access
- Does not support photo objects. A Web source must be used instead.
- Cisco UCM supports connections for 50 percent of the total OVA size (e.g. 2500-user OVA template supports up to 1250 UDS users per server and 5000 in a cluster)



Contact Photos

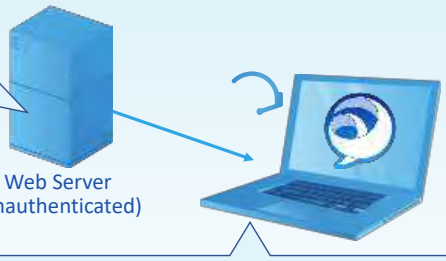
The Cisco Jabber experience is greatly enhanced with contact photos.

Cisco Jabber retrieves and displays contact photos with the following methods:

URI substitution: Cisco Jabber dynamically builds a URL to connect photos with a directory attribute and a URL template.

UDS doesn't support photo objects, therefore photos must be loaded from web server.

Photos can be JPG, PNG or BMP with a recommended size of 128x128 pixels; Jabber will resize/crop photos to fit client interface



Web Server (unauthenticated)

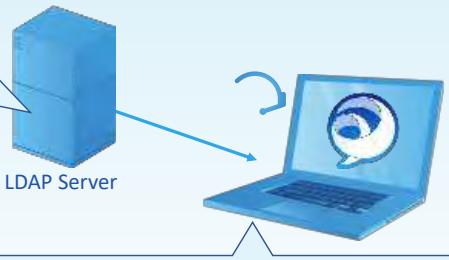
You must add following lines to jabber-config.xml for UDS photo operation

```
<UdsPhotoUriWithToken>http://www.photo/url/path/%%uid%%.jpg</UdsPhotoUriWithToken>
```

Contact Photos

Binary objects: Cisco Jabber retrieves the binary data for the photo from your database. If you are using binary objects from Microsoft Active Directory, PhotoUriWithToken attribute should not be set in the jabber-config.xml file. However if your LDAP server doesn't store photos they can be loaded from a web server. If this case you will need to set PhotoUriWithToken attribute

Jabber CDI can retrieve photos directly from LDAP Server Photos can be JPG, PNG or BMP with a recommended size of 128x128 pixels; Jabber will resize/crop photos to fit client interface



If your LDAP server doesn't hold photos they can be loaded from a web server. You must add following lines to iabber-config.xml for photo operation

```
<PhotoUriSubstitutionEnabled>True</PhotoUriSubstitutionEnabled>
<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>
<PhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg</PhotoUriWithToken>
```

Policies

On-Premise Policies: File Transfers

Managed file transfer (MFT) allows Cisco Jabber to transfer files to other users, ad hoc group chat rooms, and persistent chat rooms. The files are stored in a repository on an external file server and the transaction is logged to an external database.

```
<DisableMFTForConversationTypes>P2P;PersistentChat</DisableMFTForConversationTypes>
```

Restricts users from transferring certain file types

Can disable Managed File transfer option for P2P, Group Chat and Persistent Chat

Use a semicolon to delimit multiple file extensions

```
<Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
```

Restricts users from transferring certain file types.

You must set the file extensions as the value, for example, .exe.

Use a semicolon to delimit multiple file extensions.

Policies

The following example shows the semicolon-delimited conversation types:

```
<DisableMFTForConversationTypes>P2P;PersistentChat</DisableMFTForConversationTypes>
```

Disallowed_File_Transfer_Types policy applies to all Cisco Jabber clients. It restricts users from transferring certain file types. You must set the file extensions as the value, for example, .exe. Use a semicolon to delimit multiple file extensions, for example, .exe;.msi;.rar;.zip.

The following example shows the semicolon-delimited file extensions:

The following example shows the semicolon-delimited file extensions:

```
<Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
```

```
<File_Transfer_Enabled>false</File_Transfer_Enabled>
```

Specifies if users can transfer files to each other using the Cisco Jabber client

- true (default): Users can transfer files to each other.
- false: Users cannot transfer files to each other.

```
<PreferredFT>P2P</PreferredFT>
```

Specifies the preferred method of transferring files in the Cisco Jabber client if Managed File Transfer and Peer-to-Peer File Transfer are enabled.

- MFT: Files are transferred using the managed file transfer option.
- P2P: Files are transferred using peer-to-peer file transfer.

The following example shows the semicolon-delimited file extensions:

File_Transfer_Enabled policy applies to all Cisco Jabber clients. It specifies if users can transfer files to each other using the Cisco Jabber client.

- true (default): Users can transfer files to each other.
- false: Users cannot transfer files to each other.

The following example shows that users cannot transfer files to each other:

```
<File_Transfer_Enabled>fa1se</File_Transfer_Enabled>
```

The following example shows that users are using peer-to-peer file transfer:

```
<PreferredFT>P2P</PreferredFT>
```

On-Premise Policies: Screen Capture

Screen_Capture_Enabled policy applies to Cisco Jabber for Windows. It specifies if users can perform screen capture.

- true (default): Users can perform screen capture.
- false: Users cannot perform screen capture

The following example shows that users cannot perform screen capture:

```
<Screen_Capture_Enabled>false</screen_Capture_Enabled>
```

```
<Screen_Capture_Enabled>false</screen_Capture_Enabled>
```

On-Premise Policies: Screen Capture

ShowScreenCaptureButton policy applies to Cisco Jabber for Desktop Clients. It specifies if the Screen capture button is enabled.

true (default): Screen capture button is enabled.

false: Screen capture button is disabled.

```
<ShowScreenCaptureButton>false</ShowScreenCaptureButton>
```

Disabling this parameter will hide the Screen capture button in Windows and disable it for Mac

Embedded Tabs

Embedded tabs apply to Cisco Jabber for desktop and mobile clients.

- Enabled and configured in jabber-config.xml
- HTML and JavaScript capabilities
- Custom applications and pop-ups

Embedded Tabs

Custom embedded tabs display HTML content in the client interface. The custom embedded tab can only be configured using the jabber-config.xml file. The following XML snippet shows the structure for custom tab definitions:

```
<jabber-plugin-config>
  <browser-plugin>
    <page refresh="" preload="" internal="">
      <tooltip></tooltip>
      <icon></icon>
      <url></url>
    </page>
  </browser-plugin>
</jabber-plugin-config>
```

Embedded Tabs

An example below shows jabber-config.xml file that enabled custom tab inn Cisco Jabber and added Hello World page there. You can see sample HTML code that allows you to IM or call end user with one click.

jabber-config.xml

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <client>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="false" preload="false">
          <tooltip>Hello</tooltip>
          <url>http://server/hello.html</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </client>
</config>
```

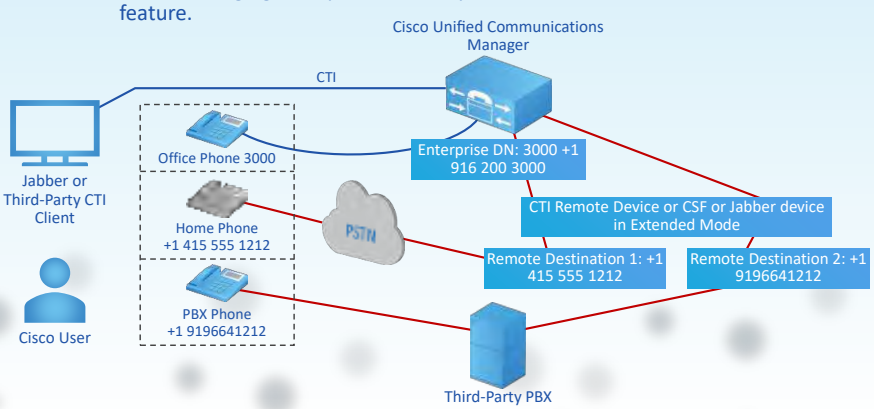
HTML sample

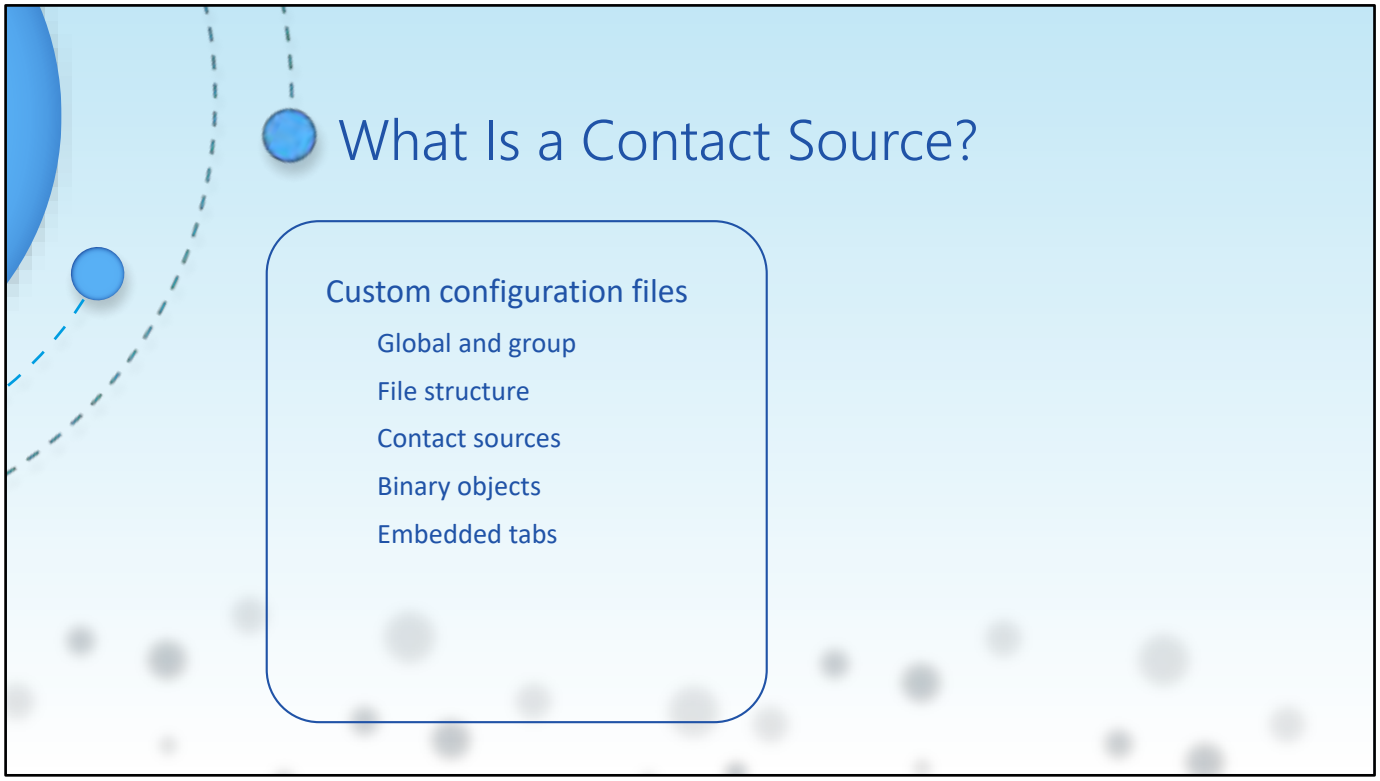
```
<html>
<h1>Hello World</h1>
<a href="im:jdoe@cll-collab.internal">IM John</a><br>
<a href="xmpp:jdoe@cll-collab.internal">IM John</a><br>
<a href="tel:11001">Call John</a><br>
</html>
```

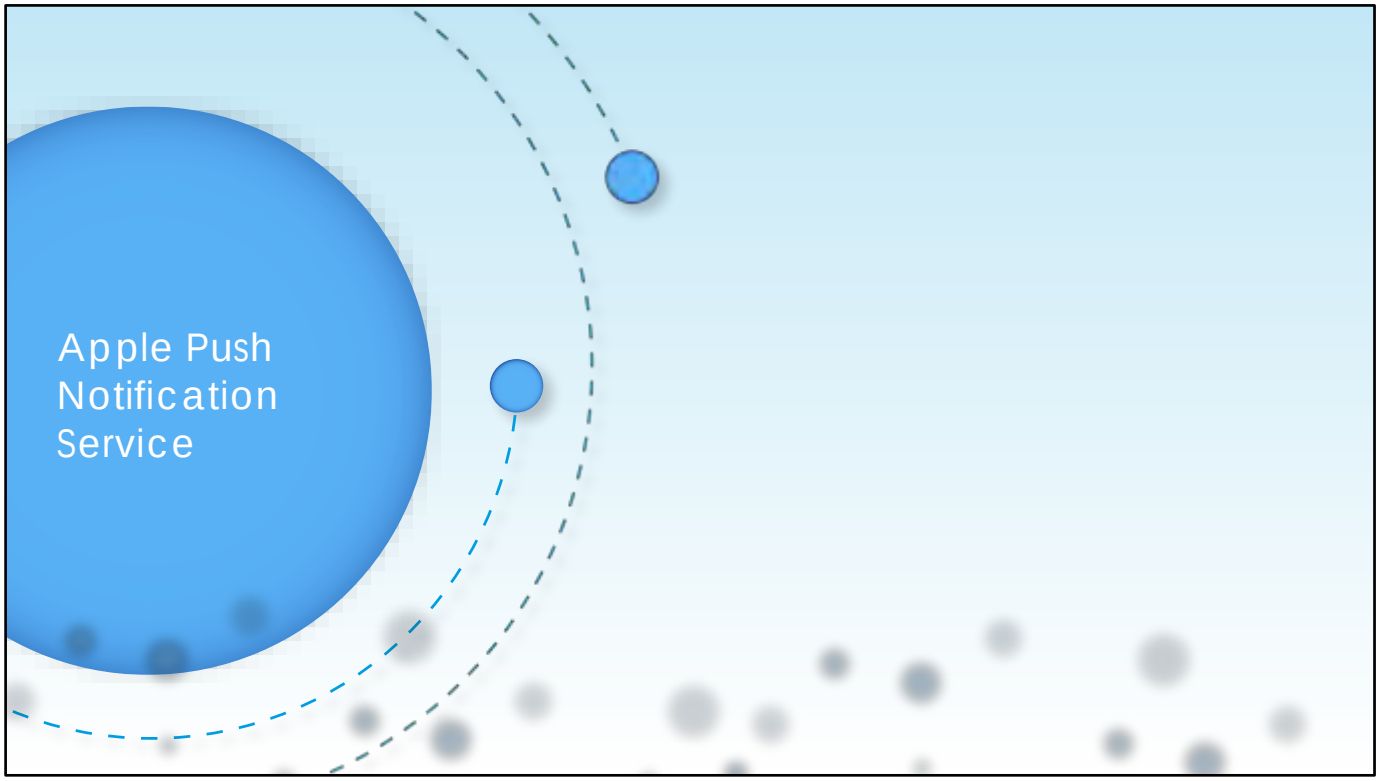
Cisco Jabber Extend and Connect

With Cisco Jabber Extend and Connect, telecommuters and business travelers can input the phone number of their preferred voice device into a Jabber client running on their Windows PC, and Cisco Unified Communications Manager routes all voice traffic directly to that phone number.

The following figure represents the system architecture for the Extend and Connect feature.







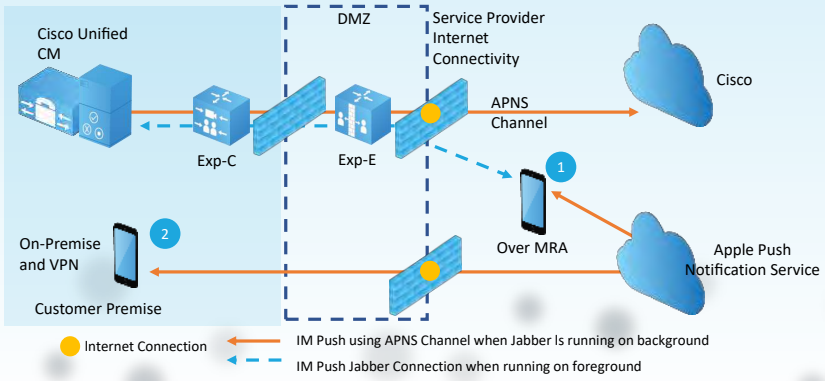
Apple Push Notification Service

With Apple Push Notifications (APN), your deployment uses Apple's cloud-based Push Notification service to push notifications for voice and video calls, instant messages, and Cisco Webex invitations to Cisco Jabber for iPhone and iPad clients that are running in suspended mode. Push Notifications allows your system to maintain a persistent communication with Cisco Jabber. Push Notifications is required both for Cisco Jabber for iPhone and iPad clients that connect from within the enterprise network, and for clients that register to an on-premise deployment via Expressway's Mobile and Remote Access (MRA) feature.

Push Notifications is required only for Cisco Jabber for iPhone and iPad clients. The feature is not supported for Android and is not applicable for Windows and Mac users.

Apple Push Notification Service

The following figure illustrates: (1) an MRA deployment where the Cisco Jabber client that connects with an on-premises Cisco Unified Communications Manager and IM and Presence Service deployment via Expressway, and (2) a Cisco Jabber for iPhone or iPad client that connects directly to the on-premises deployment from within the enterprise network.



Cloud Onboarding

There are some prerequisites to be met to onboard Push Notifications for on-premises deployments. Cisco Unified Communications Manager and Cisco Unified IM and Presence must be configured for external DNS for connectivity using Port 443 to:

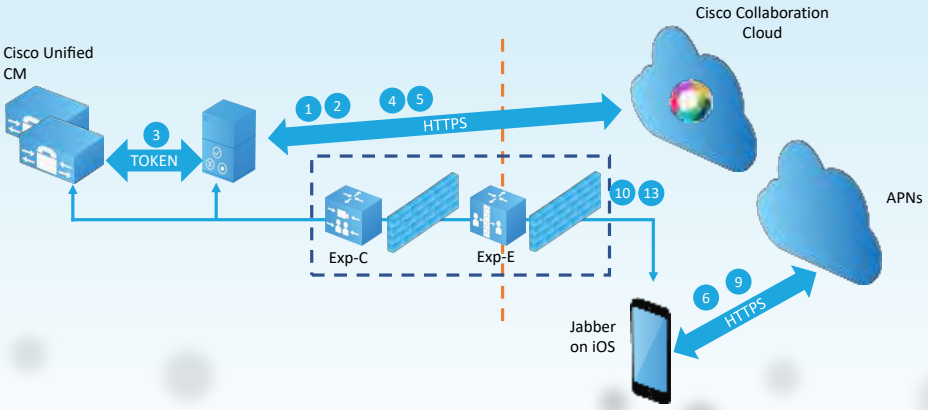
Fusion Onboarding Service at fos-a.wbx2.com Cisco Unified Communications Manager connects to this service for Push Notification subscription requests. Cisco Unified CM communicates with the Fusion Onboarding Service (FOS) in order to provision a Common Identity (CI) machine account.

Push REST service at push.webexconnect.com. Cisco Unified Communications Manager and Cisco Unified IM and Presence connect to this service to send Push Notifications.

Common Identity service at idbroker.webex.com. Cisco Unified Communications Manager and Cisco Unified IM and Presence authenticates to this service prior to sending a Push Notification.

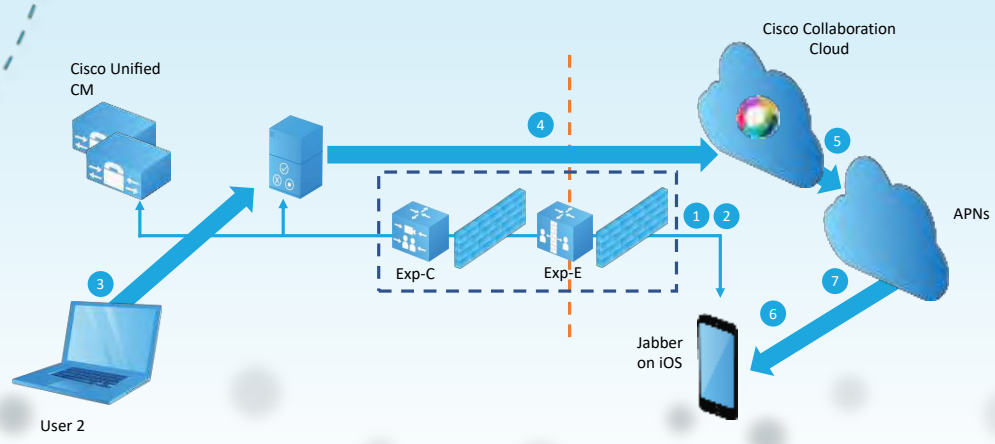
Cloud Onboarding

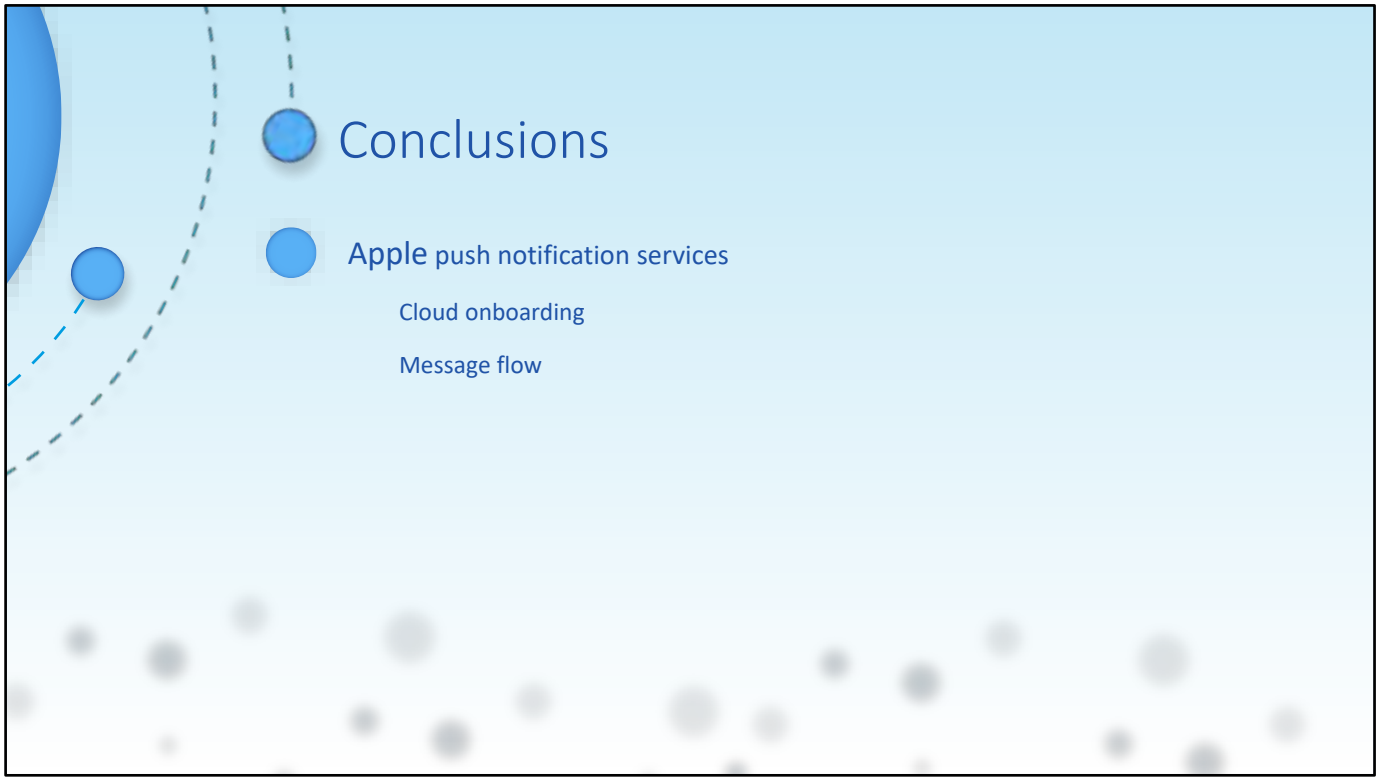
The following diagram explains how Cisco Cloud Onboarding is performed:

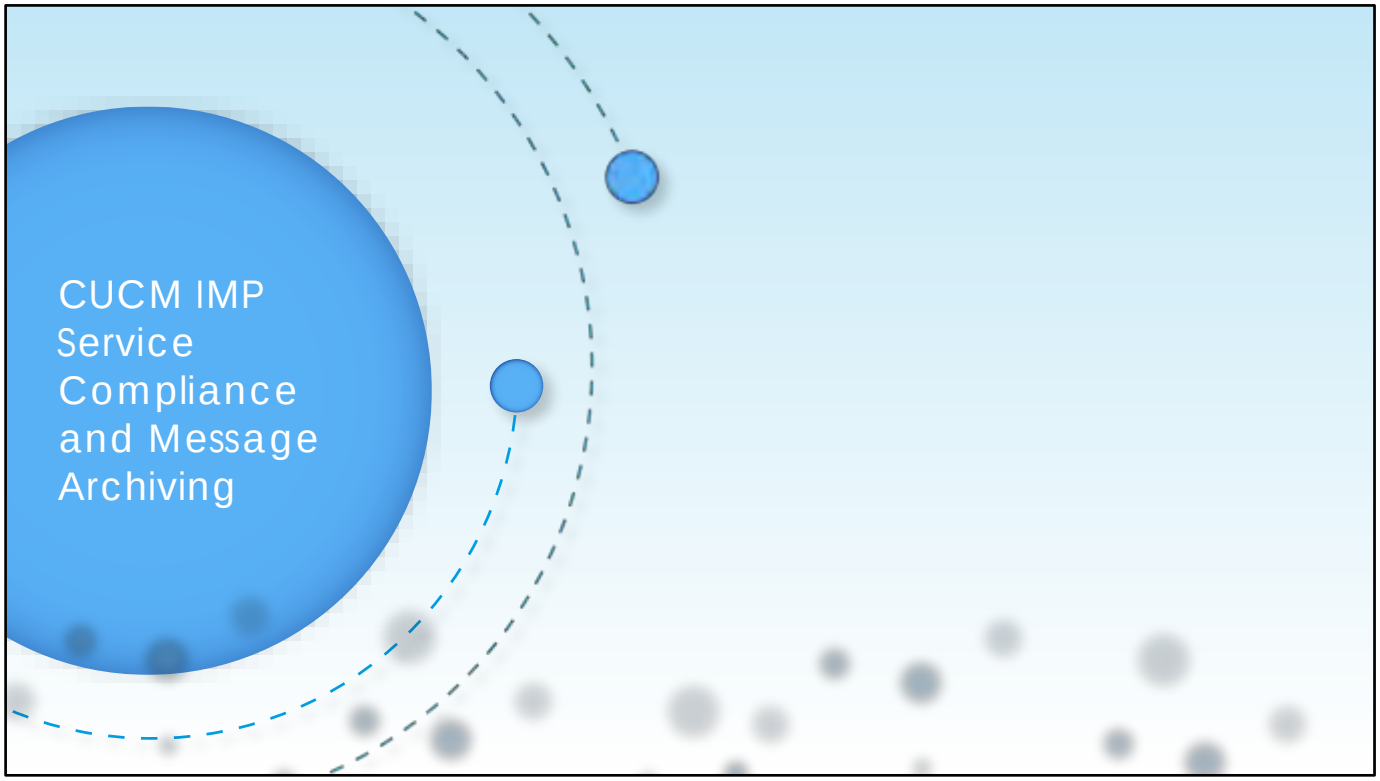


Message Flow

The following diagram explains Apple Push Notification Message Flow:







Overview

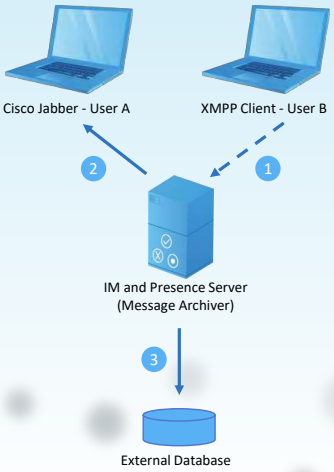
Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) includes a message archiver component that allows for logging of point-to-point, text conferencing, federated, and intercluster messages in an external database as part of nonblocking compliance (the one which doesn't block non-compliant messages exchanged between users). A blocking third-party compliance solution that allows logging of messages and applies policy to message delivery and message content, would need to be provided through a third-party compliance server solution.

Enterprise Instant Messaging Compliance and Archiving Overview

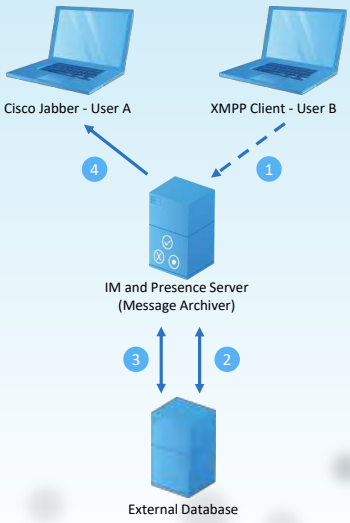
Many industries require that instant messages adhere to the same regulatory compliance guidelines that apply to all other business records. To comply with these regulations, your system must log and archive all business records, and the archived records must be retrievable.

Enterprise Instant Messaging Compliance and Archiving Overview

Native IM compliance (sometimes called IM Archiving) provides logging of all compliance-related data to an external database. All IM traffic passes through the IM and Presence Service node (via the message archiver component) and is simultaneously logged to the external database. Each IM log contains the sender and recipient information, the time stamp, and the message body. This includes chat messages and group chat messages.



Third-Party IM Compliance

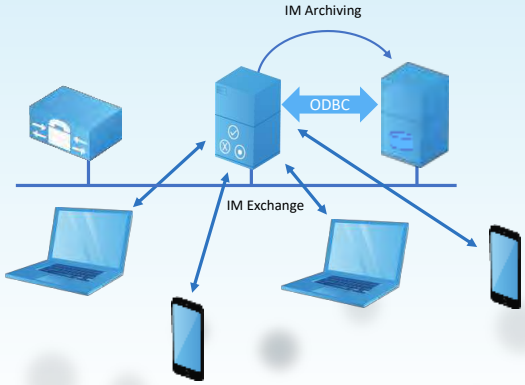


External Database Overview

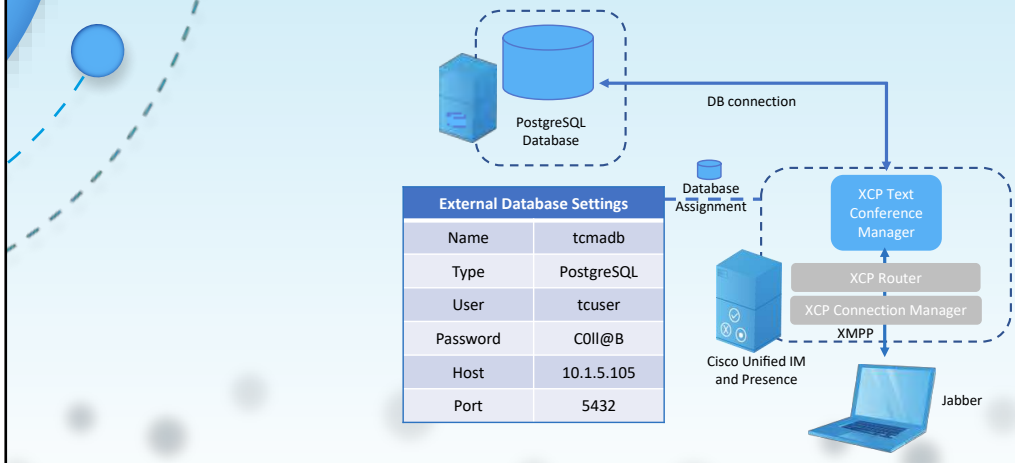
PostgreSQL 8.3.x through 9.4.1

Oracle 9g, 10g, 11g, and 12c

Microsoft SQL 2012, 2014, and 2016



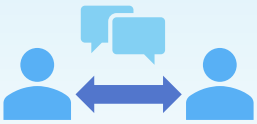
PostgreSQL External Database Integration



External Database Settings	
Name	tcmadb
Type	PostgreSQL
User	tcuser
Password	C0ll@B
Host	10.1.5.105
Port	5432

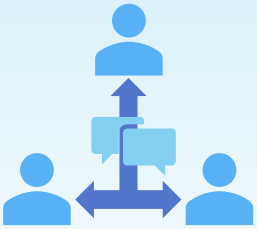
Persistent Chat

The IM and Presence Service supports IM exchange in both ad hoc chat rooms and persistent chat rooms. By default, the Text Conference component in the IM and Presence Service is set up and configured to manage IM exchange in ad hoc chat rooms.



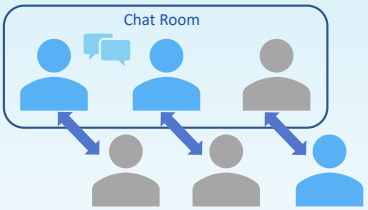
Point to Point Chat

- Ad-hoc
- Person to person
- Non-Persistent



Ad-Hoc Group Chat

- Ad-hoc group chat
- initiator defined subject
- Non-Persistent (Room)



Chat Room

- Admin enabled Feature
- Pre-defined Chat Room
- Users enter, leave and re-enter room.
- Conversation Persistent

Chat

My Rooms: Rooms of which I am a member

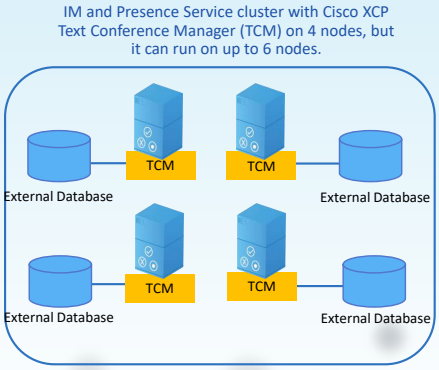
Filters: User-defined filtered chat and room views

All Rooms: Catalog of all rooms that are defined in a deployment

- Must have a 1:1 mapping of the external database instance for each of the nodes in the cluster
- An external DB must be associated with the Text Conference Manager service (service will not start if DB is not active of not reachable)
- You may archive all the messages in a chat room (optional)
- Consider DB size Consider the number of IMs in your environment and the overall volume of traffic that results

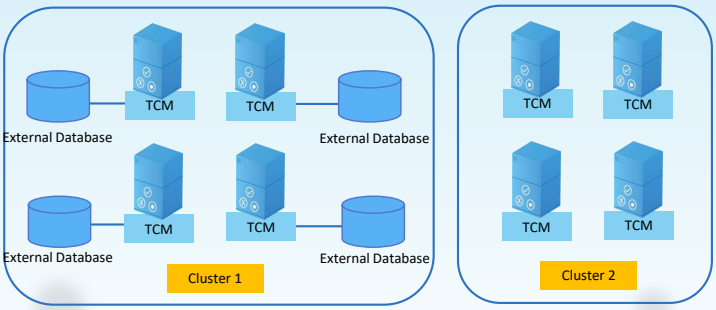
Deployment Considerations for Persistent Chat

You should consider the following when deploying persistent chat:



Deployment Considerations for Persistent Chat

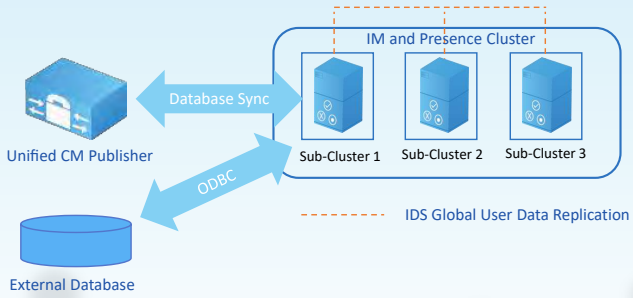
IM and Presence Service cluster with Cisco XCP Text Conference Manager (TCM) on one cluster only.



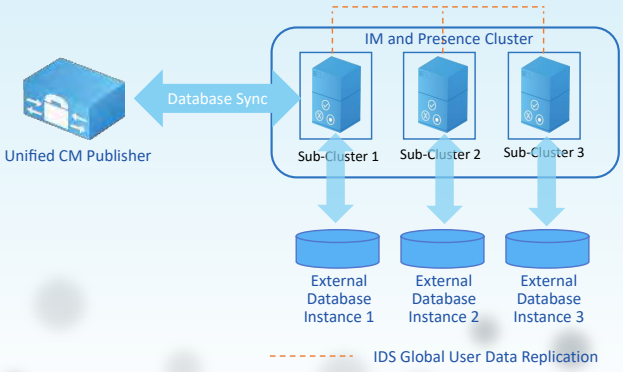
User in Cluster 2 can create or use chat rooms on any node in Cluster 1

Message Archiving

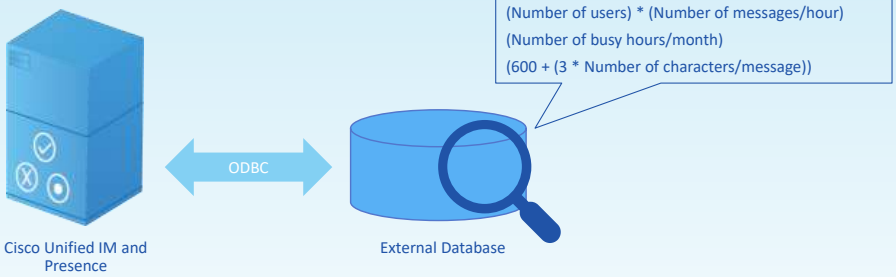
The IM and Presence Service contains a message archiver component that allows for logging of point-to-point, text conferencing, federated, and intercluster messages into an external database as part of nonblocking compliance.

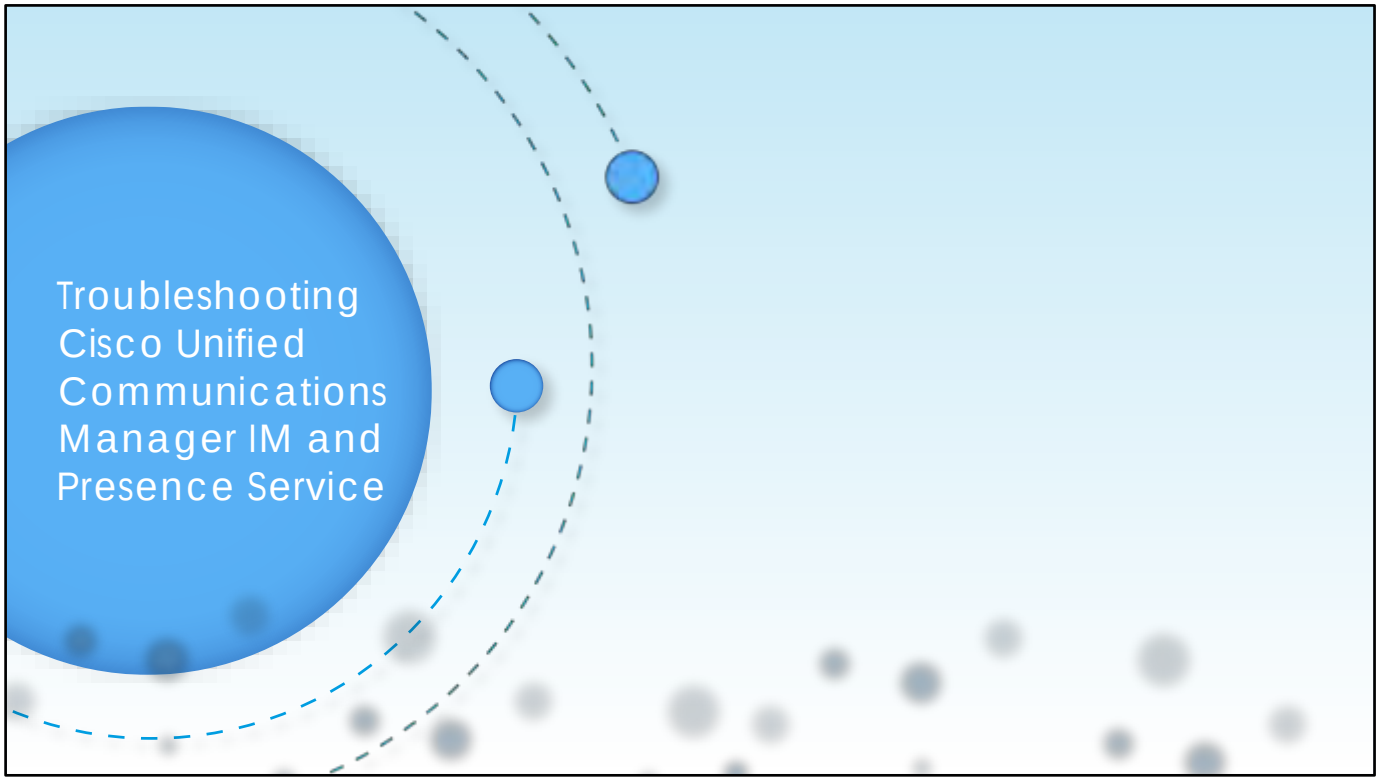


Message Archiving



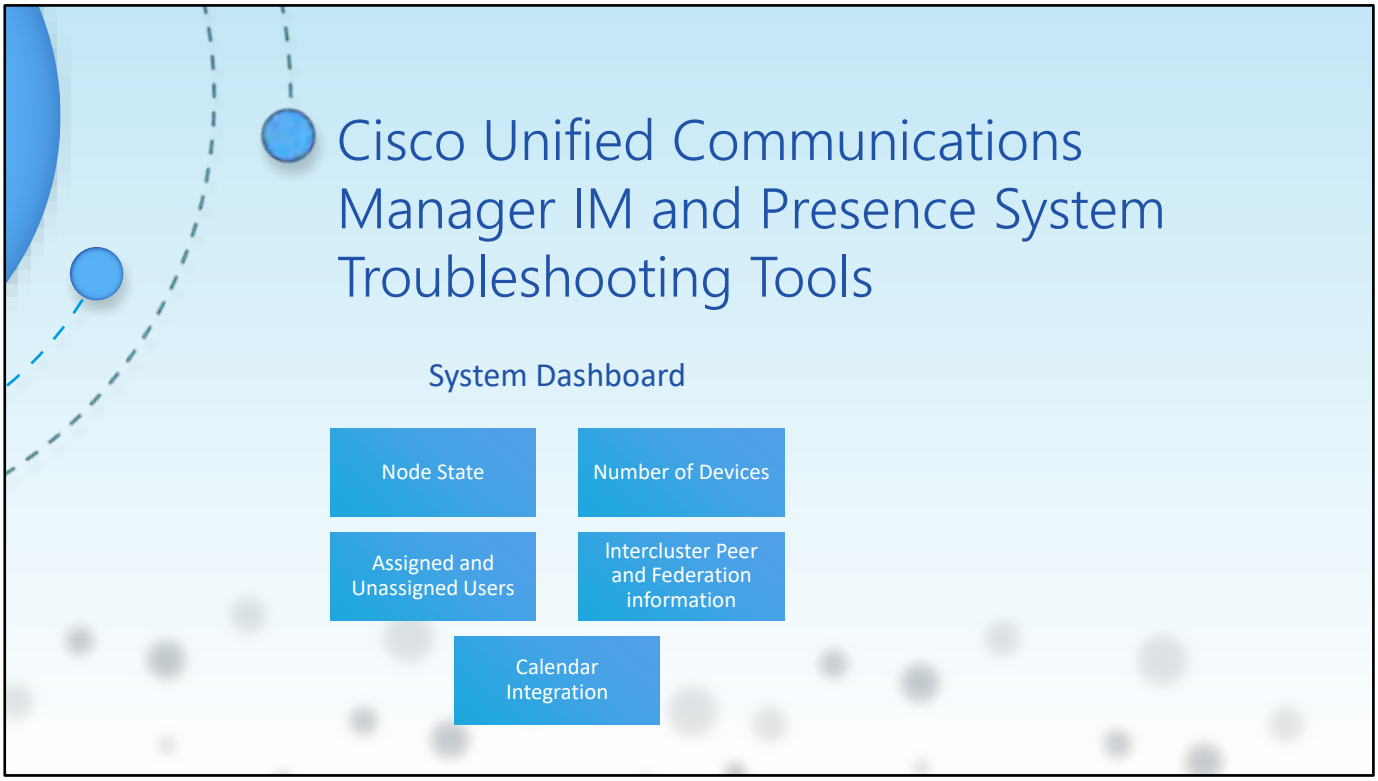
Message Archiving





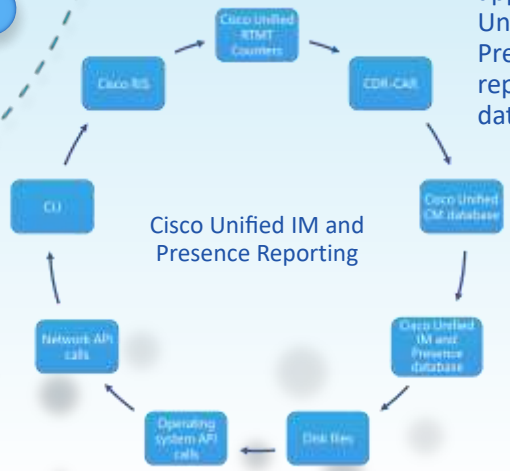
Overview

The Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) system troubleshooter and the Cisco Jabber Connection Status tool can help you resolve presence issues quickly. This section presents and resolves some common Cisco Jabber issues and introduces tracing.

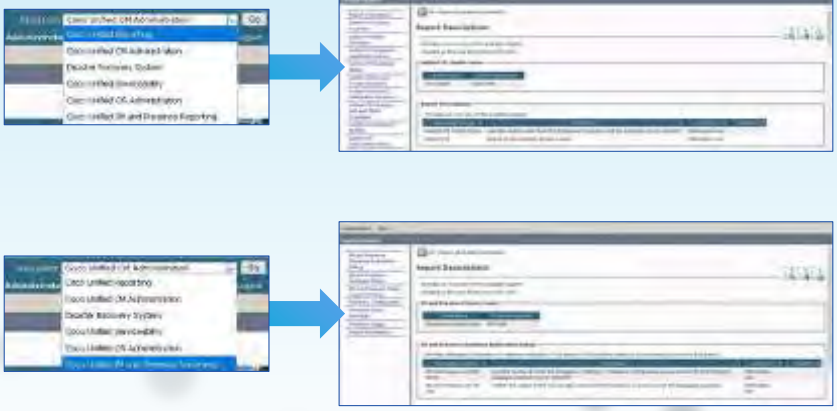


IM and Presence Service Reporting

The IM and Presence Service Reporting web application, which is accessed from the Cisco Unified Communications Manager and IM and Presence Service consoles, generates consolidated reports for troubleshooting or inspecting cluster data.

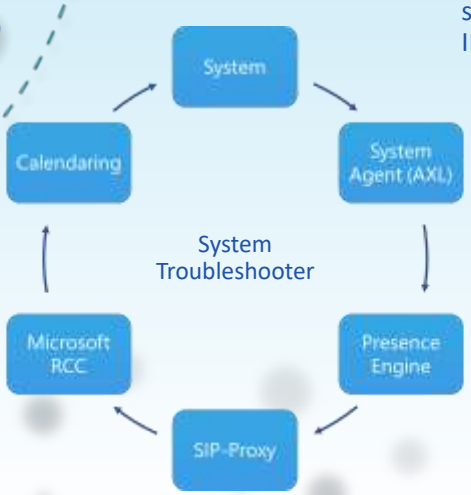


IM and Presence Service Reporting

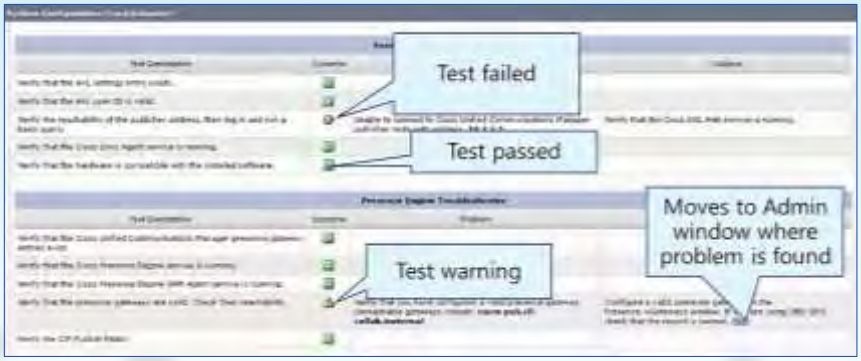


System Troubleshooter

The system troubleshooter is a helpful tool that supports you in troubleshooting the integration of IM and Presence Service with other applications.



System Troubleshooter



Cisco Unified Real-Time Monitoring Tool

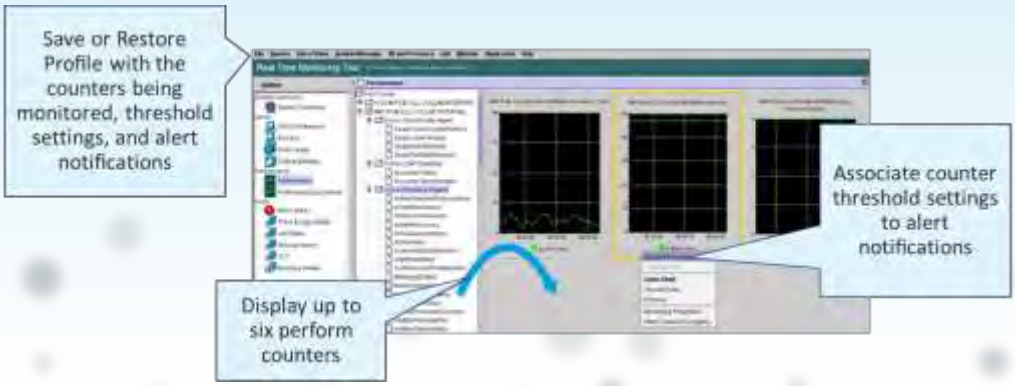
Performance Monitoring in Cisco Unified RTMT

Performance monitoring, system summary status, and server status are indicated in Cisco Unified RTMT.

- Performance Monitoring in Cisco Unified RTMT.
- Receive notifications in the form of an email message.
- Associate counter threshold settings to alert notifications.
- Display up to six perfmon counters in one chart.

Performance Monitoring

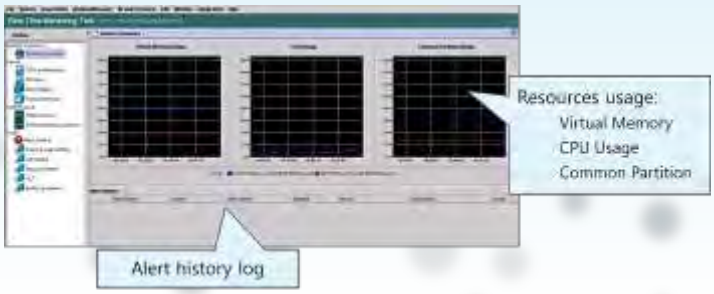
Cisco Unified RTMT integrates with IM and Presence Service and Cisco Unified Serviceability software. Cisco Unified RTMT displays performance information for all IM and Presence Service components. Cisco Unified RTMT provides alert notifications to troubleshoot performance issues. The tool also periodically polls performance counters to display data for that counter. You can view performance monitoring counters in a chart or table format.



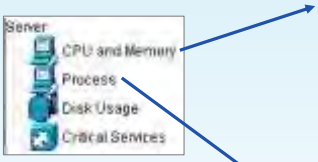
System Summary Status

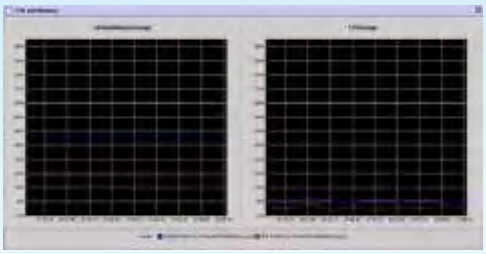
Cisco Unified RTMT provides a set of default monitoring objects that help you monitor the health of the system. Default objects include performance counters or critical event status for the system and other supported services. The system summary in Cisco Unified RTMT allows you to monitor important common information in one monitoring pane. In the system summary, you can view information about the following predefined objects:

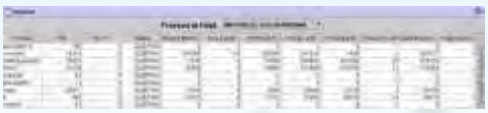
- Virtual memory usage
- CPU usage
- Common partition usage
- Alert history log



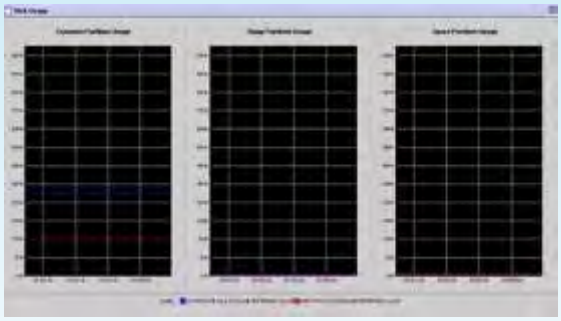
Server Status

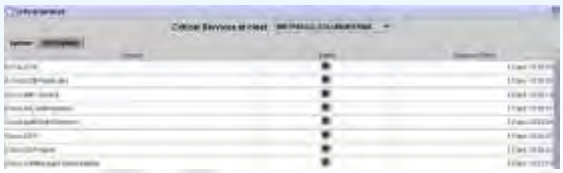






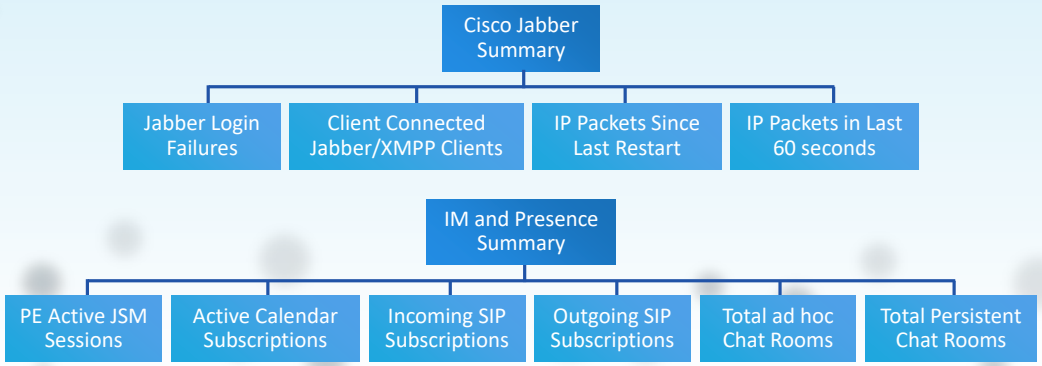
Server Status





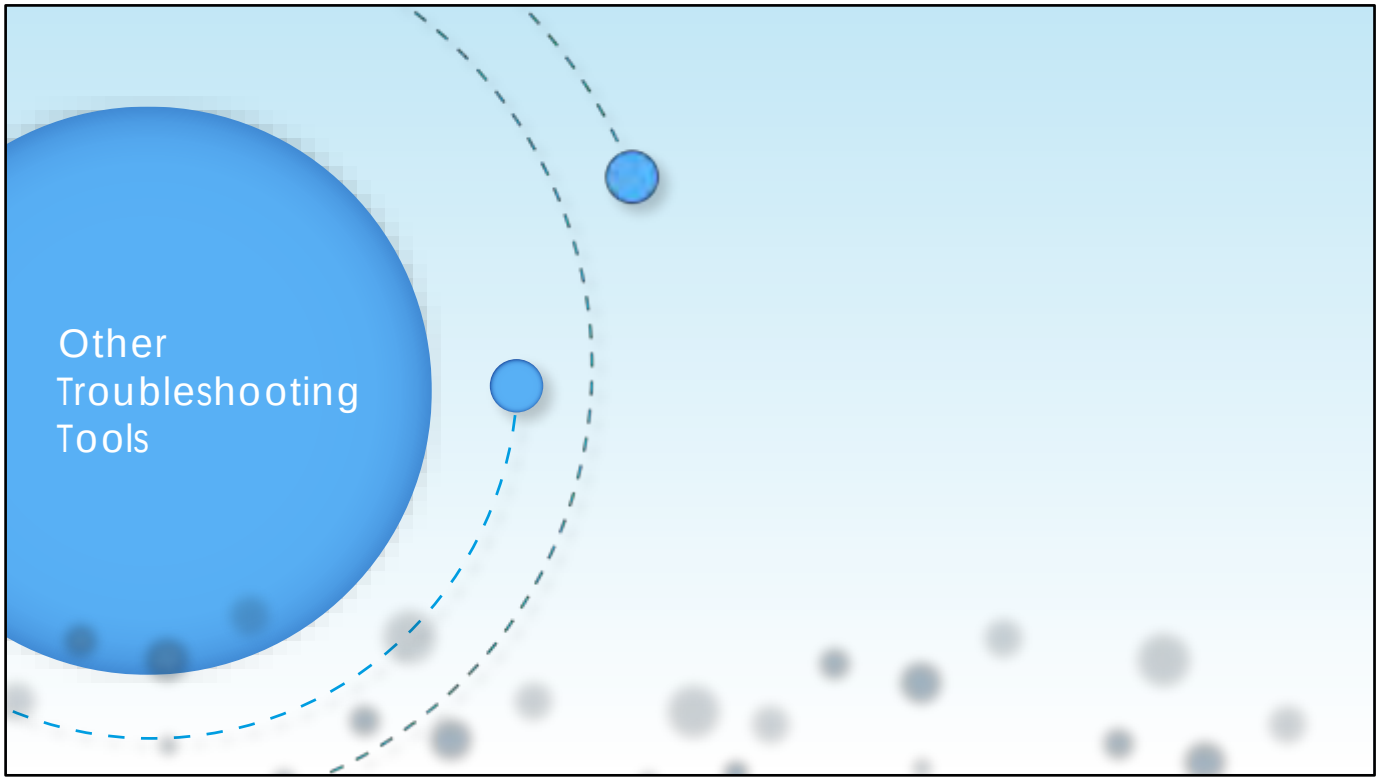
IM and Presence Service and Cisco Jabber Summary Monitoring

Cisco Unified RTMT provides a set of important performance counters that assist you in monitoring the overall performance of the IM and Presence Service and Cisco Jabber.



Conclusions

- Overview
  - Tools
  - Service reporting
  - System troubleshooter
  - Real time monitoring tool
  - Performance monitoring
  - System summary status
  - Server status



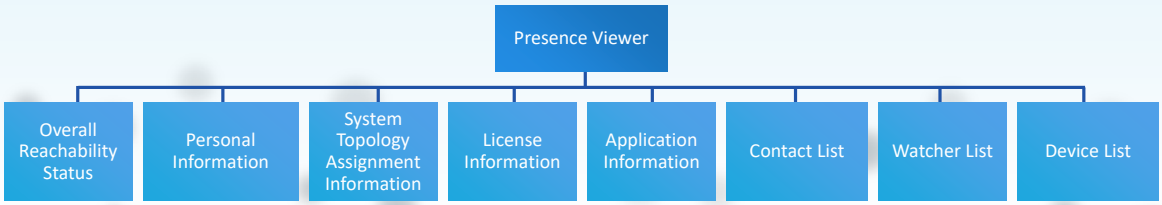
Presence Viewer

You can use the Presence Viewer to troubleshoot single-user-related issues

The Presence Viewer is a diagnostic tool that enables you to view the presence status of a user in IM and Presence Service, and to identify presence-related issues. For example, you can enter the user ID of an end user, and monitor the login status of that user in various applications, for example, Cisco Jabber, and Microsoft Lync Client

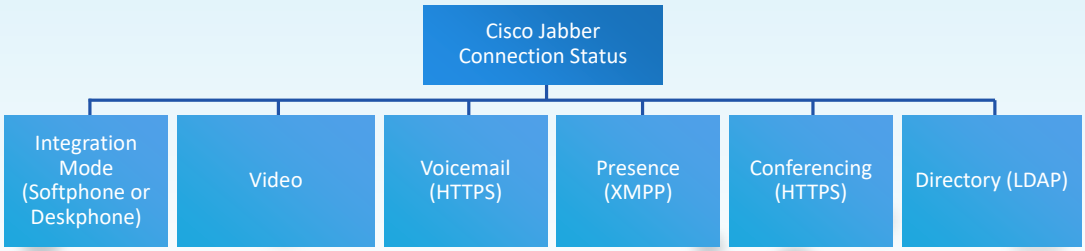
You can also determine how the presence status of a particular user appears to another user, who is known as a watcher

The Presence Viewer tool can only be accessed by Cisco Unified Communications Manager administrators



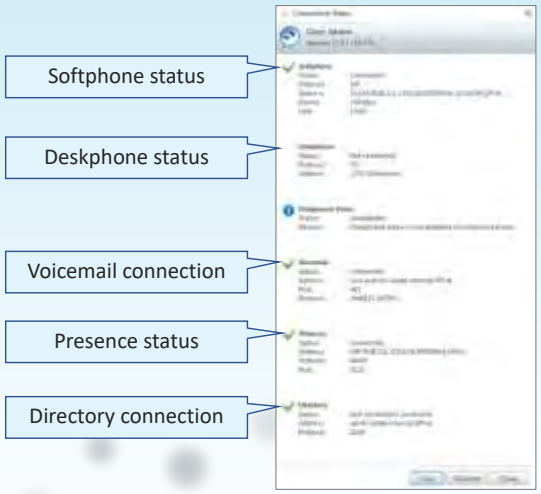
Cisco Jabber Connection Status

Cisco Jabber includes a connection status tool to view and check the Cisco Unified Communications service parameters. The connection status tool was called the server health tool in previous Cisco Jabber releases.



Cisco Jabber Connection Status

The information for a particular application is only shown when a logged-in user has a UC Service that is configured for that application—for example, the voicemail service. If the user does not have a voicemail service that is applied via the configured service profile, you do not see voicemail-related information. The error notification tool shows errors with a description, error code, date, and time.



Apple Push Notifications Troubleshooting

Apple Push Notifications impacts many components, some of which are hosted locally and some of which are in the cloud. Because multiple components are involved (and some of them are out of your control), it is best to involve Cisco Technical Assistance Center (TAC) if there are any issues

Cisco Management Agent Service: /var/log/active/cm/trace/cmas/log4j/

Cisco Push Notification Service: /var/log/active/cm/trace/ccmpns/log4j/

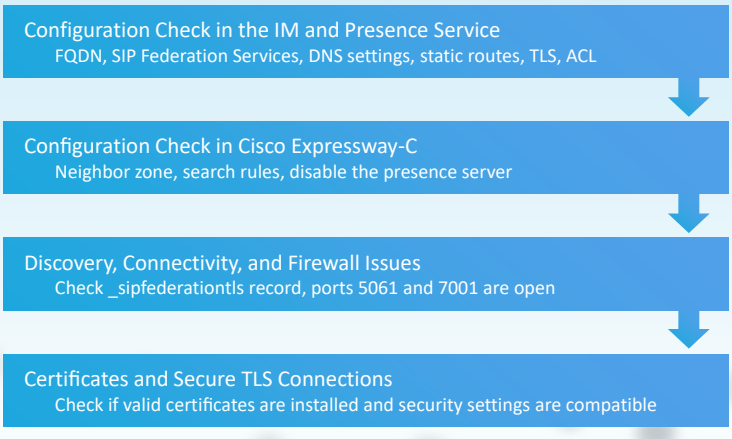
Cisco TAC	Multiple components out of our control involved Send troubleshooting information to Cisco Cloud
Cisco Unified RTMT Performance Counters	System > Performance > CUCM > Cisco Callmanager: NumberOfPushReqSent System > Performance > IM/P > Cisco XCP Push Counters: PushEnabledSessionsApns, PushErrorsApns.
Cisco Unified RTMT Traces	Cisco Management Agent Service: /var/log/active/cm/trace/cmas/log4j/ Cisco Push Notification Service: /var/log/active/cm/trace/ccmpns/log4j/

IM and Presence Service Multidomain Deployment Troubleshooting

Troubleshooting SIP Federation

Troubleshooting XMPP Federation

Troubleshooting SIP Federation



Troubleshooting SIP Federation

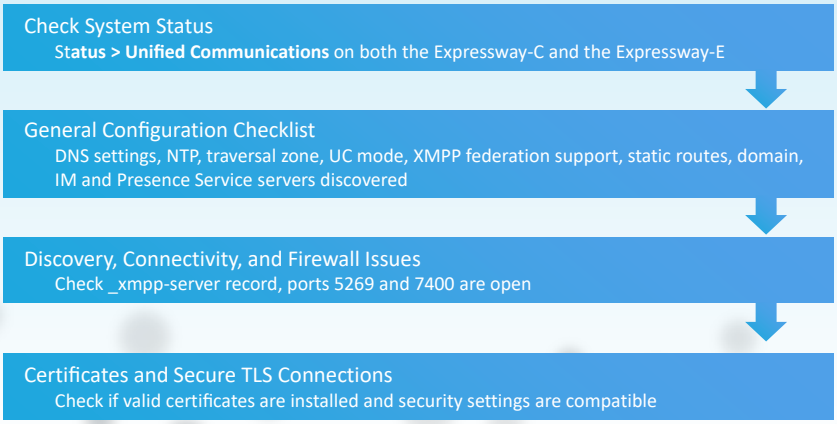
You may need to look at logs and traces if the configuration check does not help fix the issue.

Cisco Unified IM and Presence Tracing
- Logs for XCP SIP Federation Connection Manager
- Logs for SIP Proxy
- Logs for XCP Router

Microsoft Server SIP Tracing
- The Skype for Business, Lync, OCS SIP Proxy component is responsible for all SIP request routing

Troubleshooting XMPP Federation

The figure shows a list of items to be checked when troubleshooting an external XMPP federation



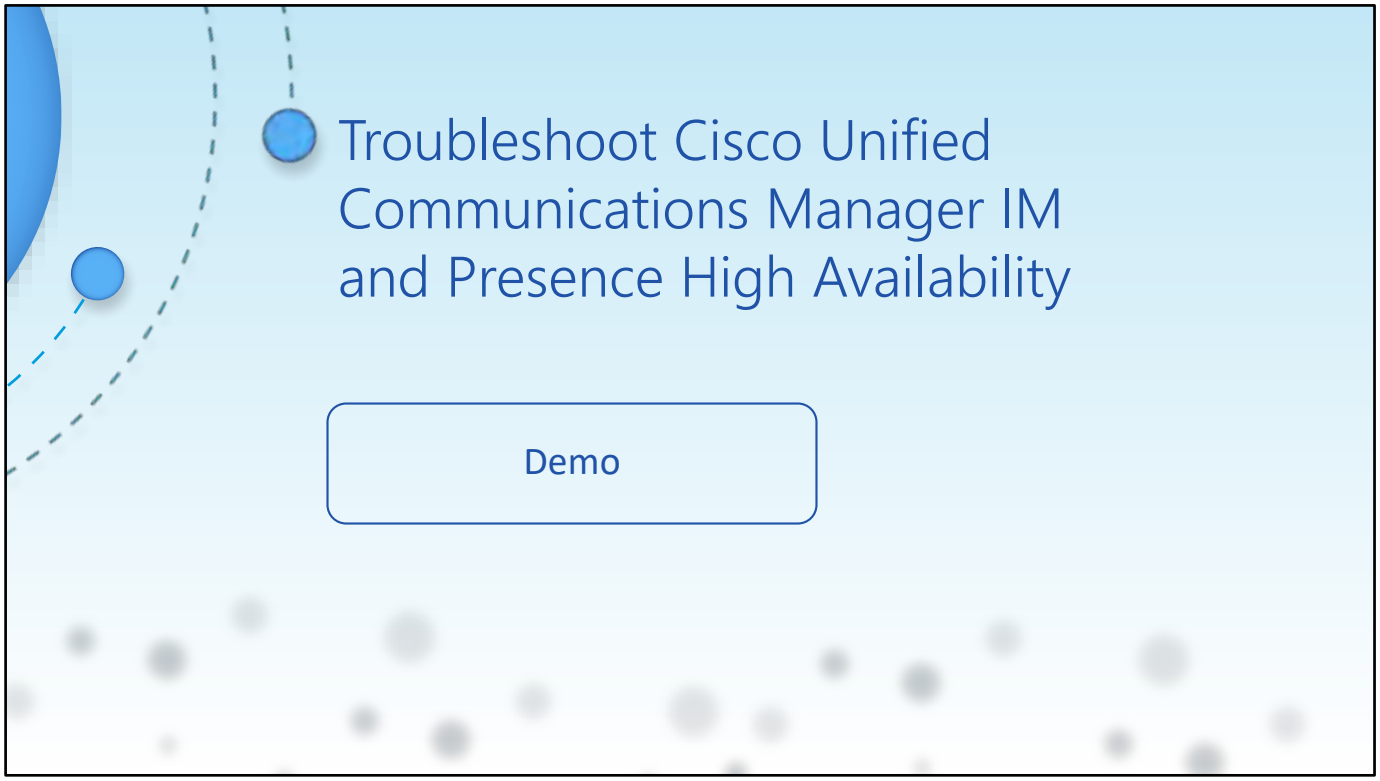
Troubleshooting XMPP Federation

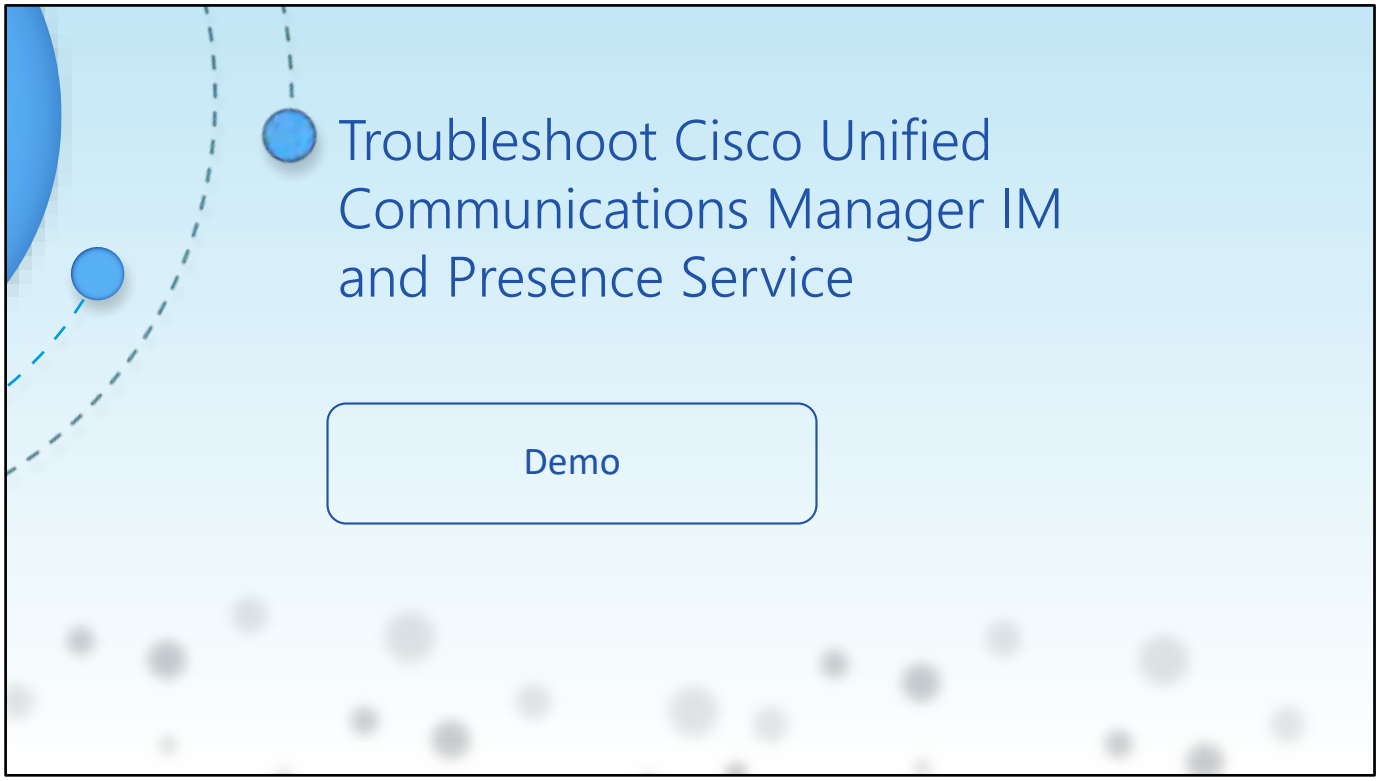
Check the Event Log

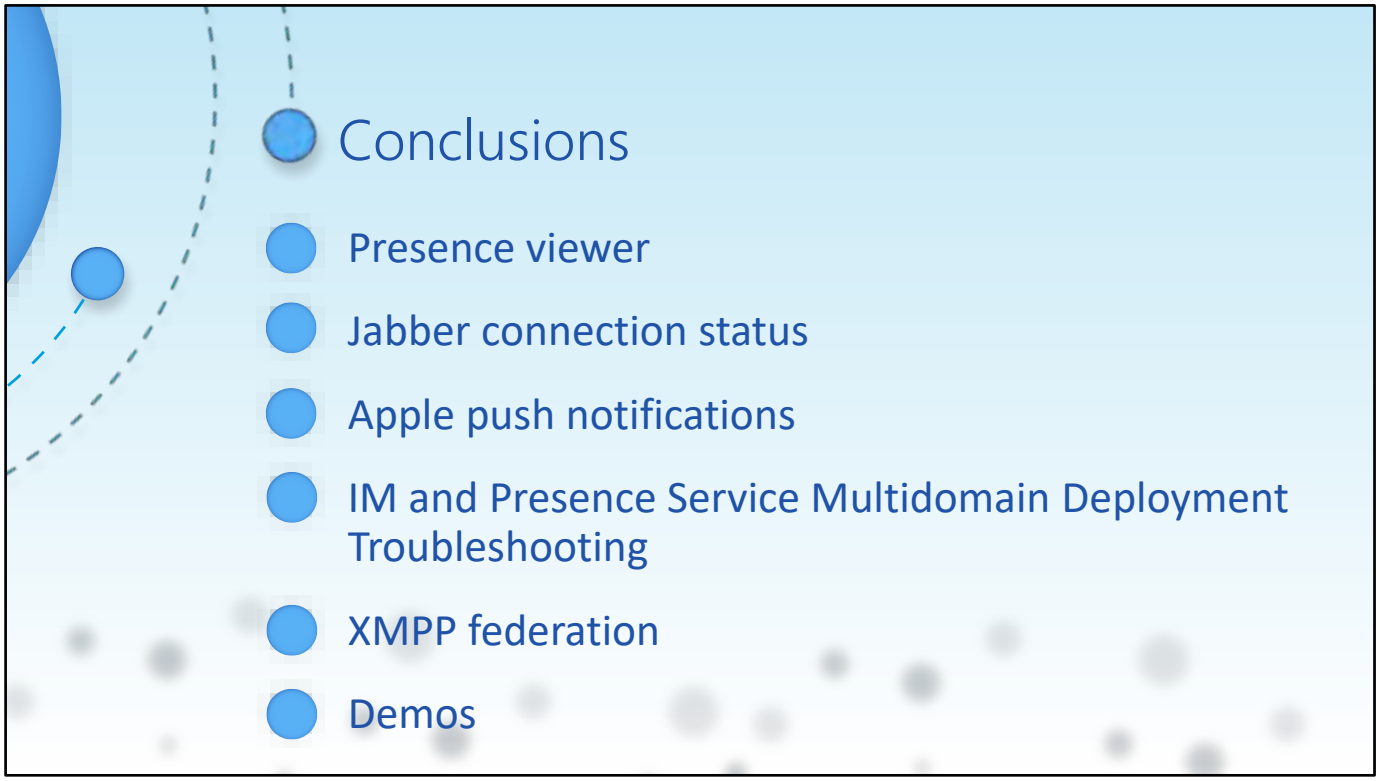
Events related to XMPP federation are tagged with Module="XMPPFederation" (on the Expressway-E).

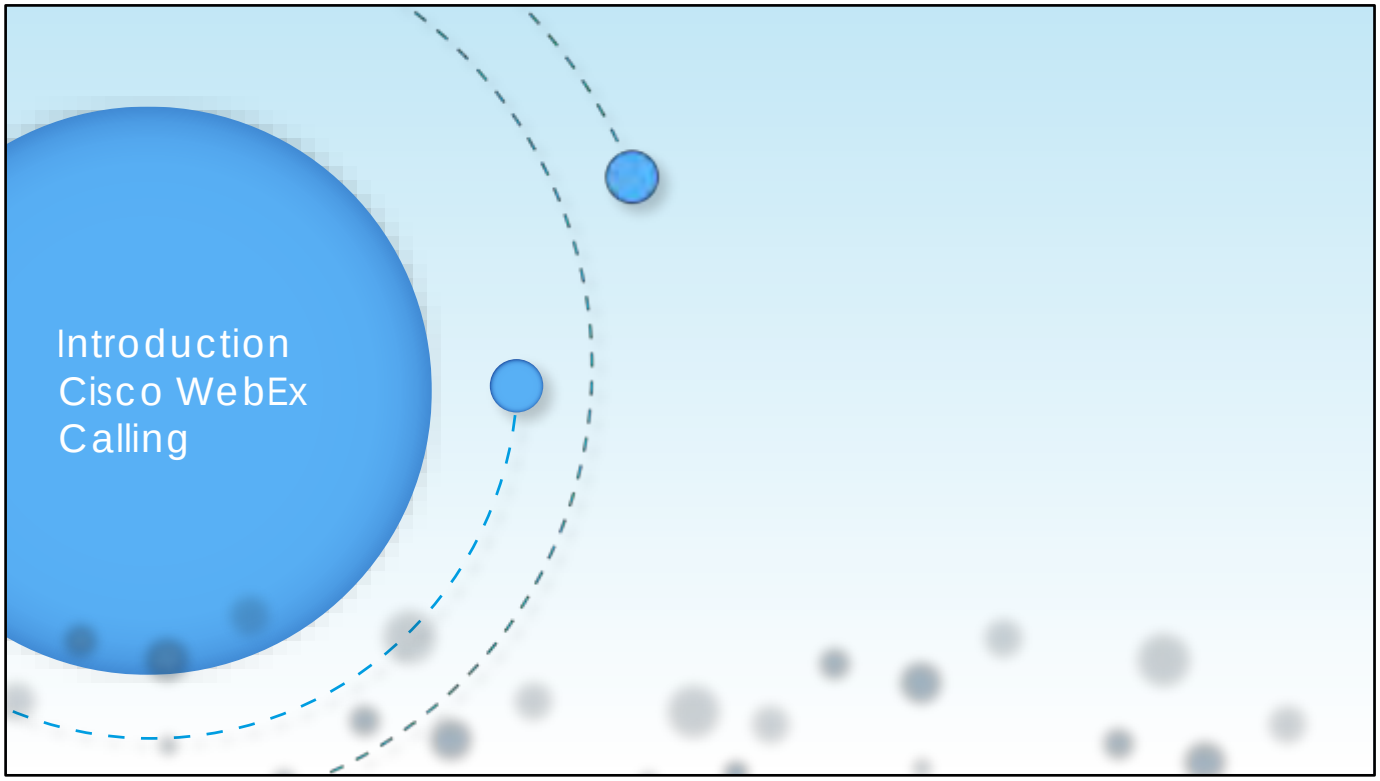
Check the Event Log

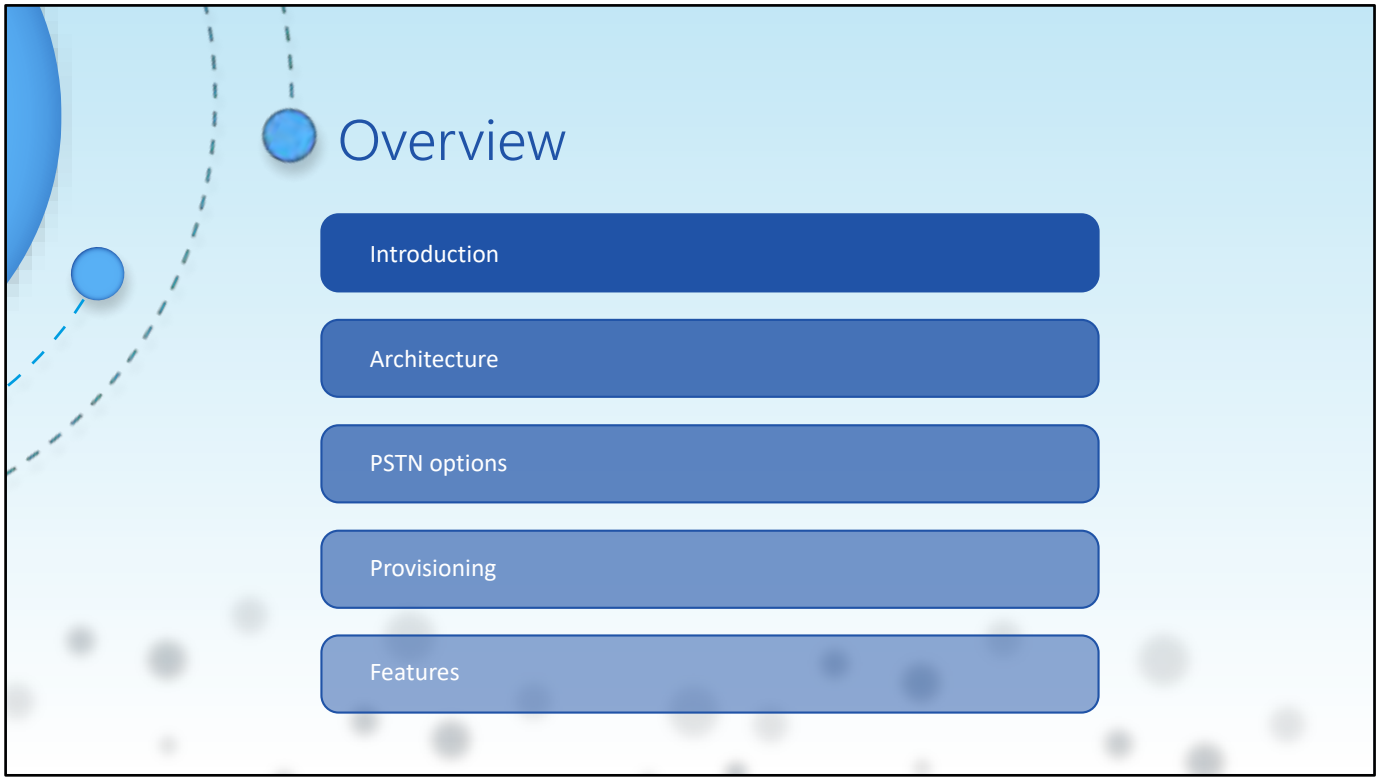
When performing diagnostic logging (**Maintenance > Diagnostics > Diagnostic logging**), set the develop.xcp.federation support log (**Maintenance > Diagnostics > Advanced > Support Log configuration**) to debug level.











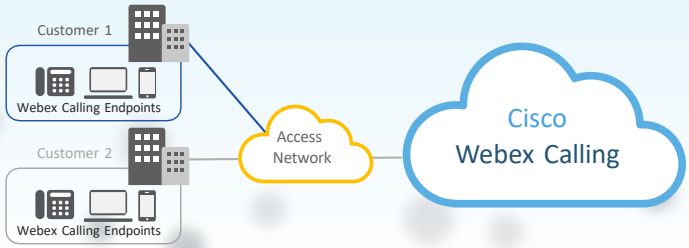
The Cisco Webex Calling Platform

Fully-featured cloud PBX powered by proven technology

Deployed in Geo-redundant Cisco Data Centers

Partner sells the service, owns customer relationship

Cisco owns and supports platform and service, can bring opportunities



Cisco MPP portfolio

Basic

Cisco® IP Phone 6800 Series

Cisco IP Phone 7800 Series

Telephony adapters

Cisco ATA 190 series

Basic product line

Conference

Cisco IP Conference Phone 7832 and 8832

Conference room

Advanced

Cisco IP Phone 8800 Series

MPP 6800 DECT

Advanced product line

Video

Cisco 88x5 Series Video Phone

Video

Accessories

Key Expansion Modules
Headsets

Accessories

Soft Clients

Webex Teams with Integrated Calling

OR

Standalone **Cisco Webex Calling app**

Webex Calling Architecture

Regions and Datacenters

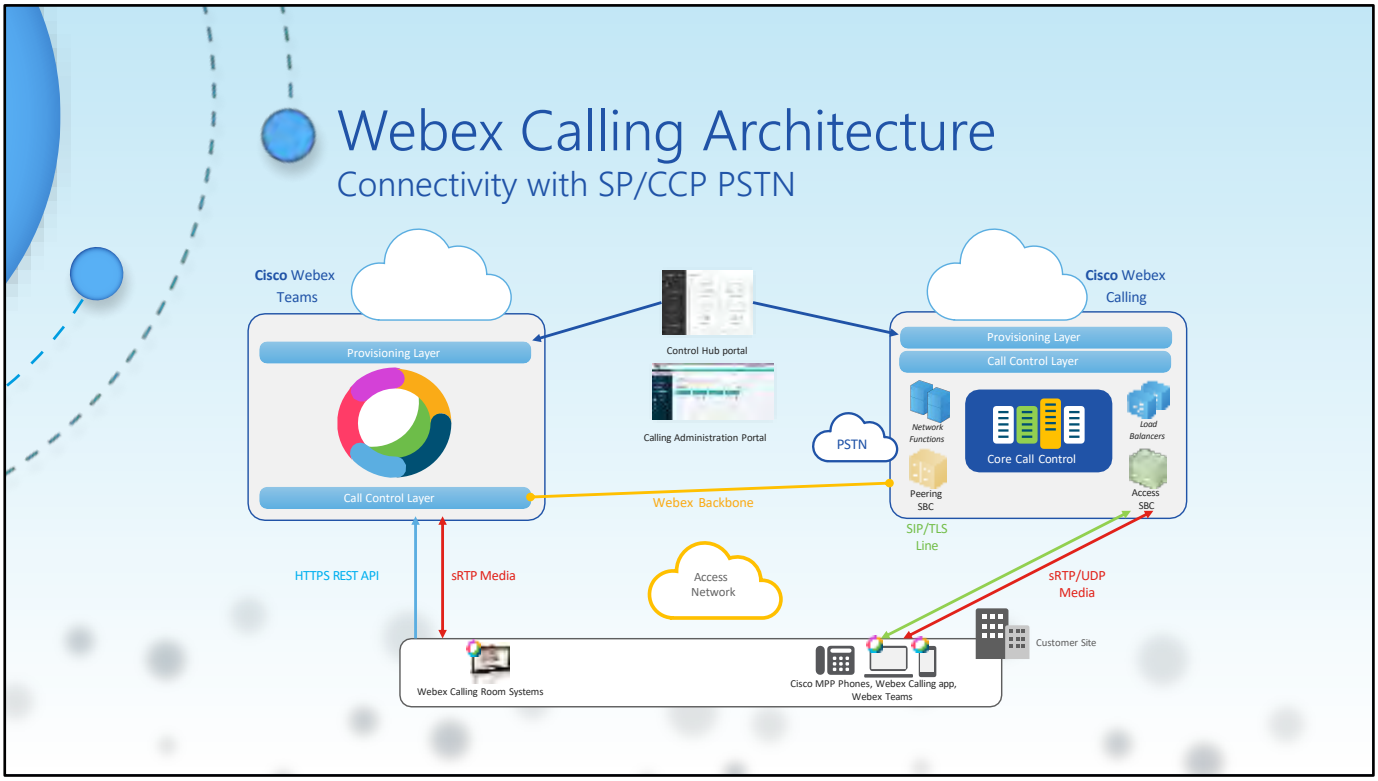
Webex Calling operates four regional platforms:

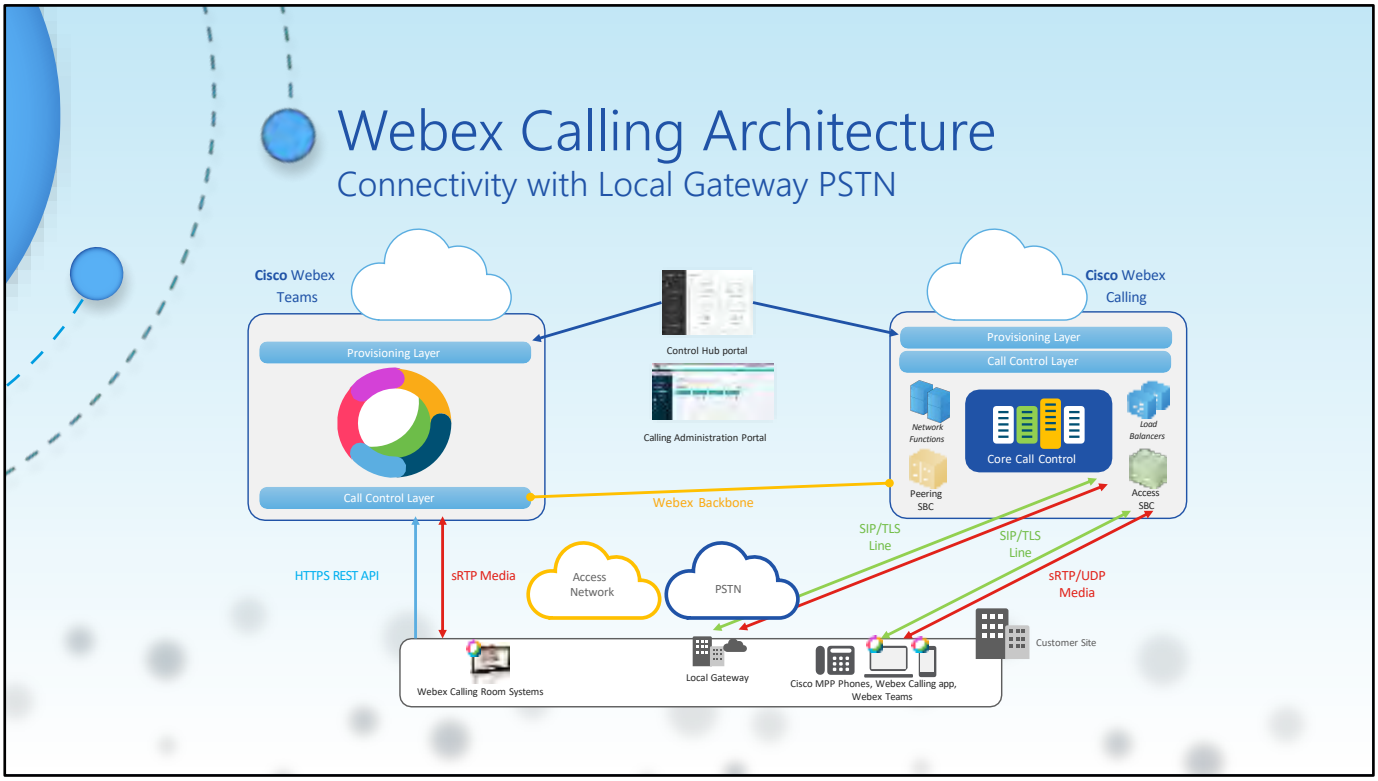
North America, EMEAR, APJC(Japan and APJC(Australia).

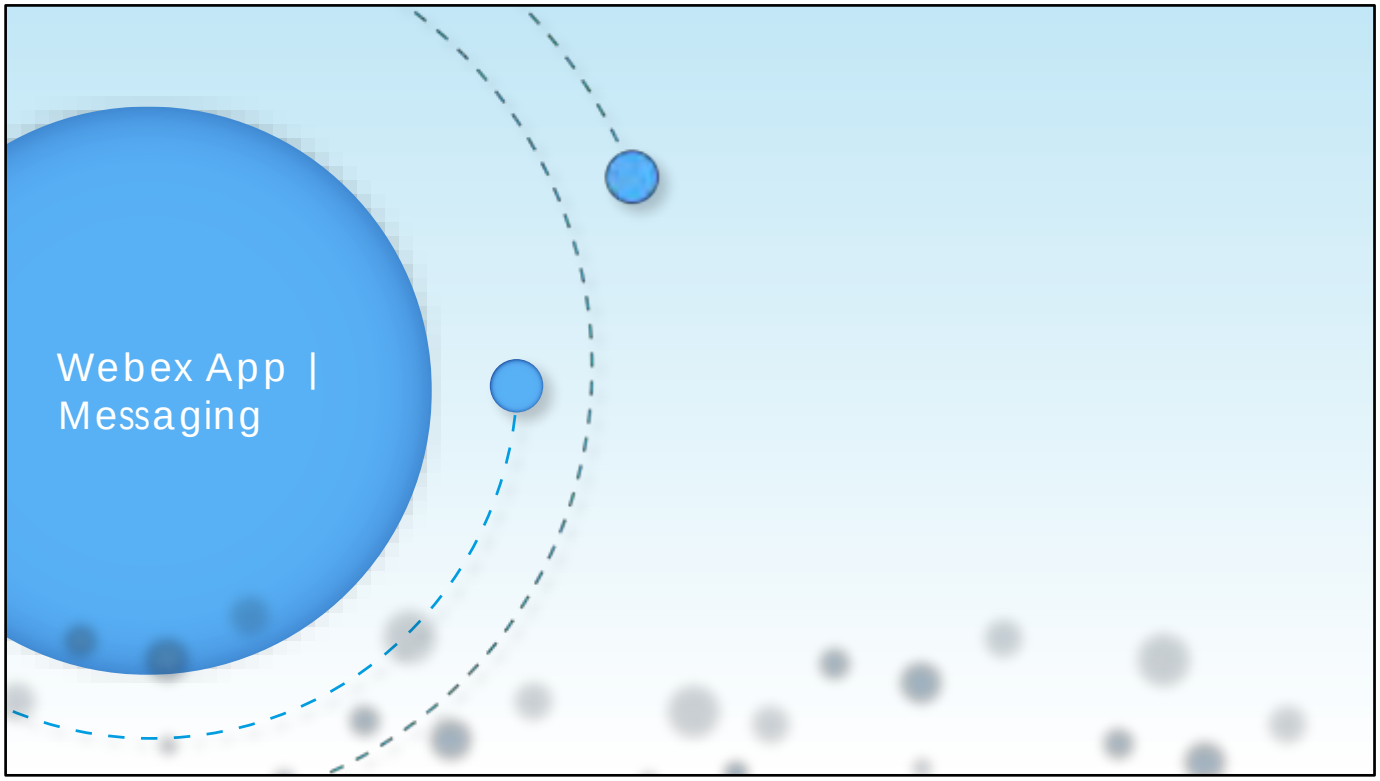
Each region contains localizations for all supported countries. This ensures that from a single location, the Partner can provide services globally to their Enterprise Customers.

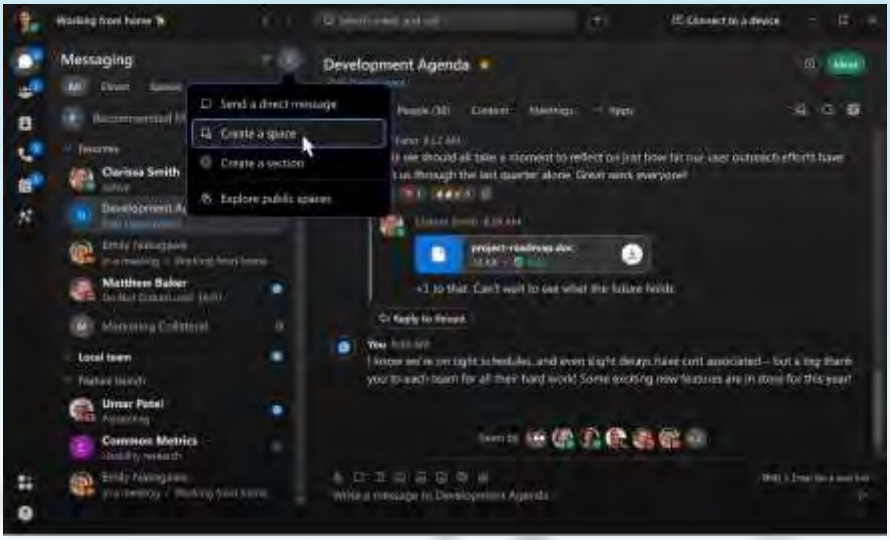
Data and traffic are stored and processed within the regional platform.

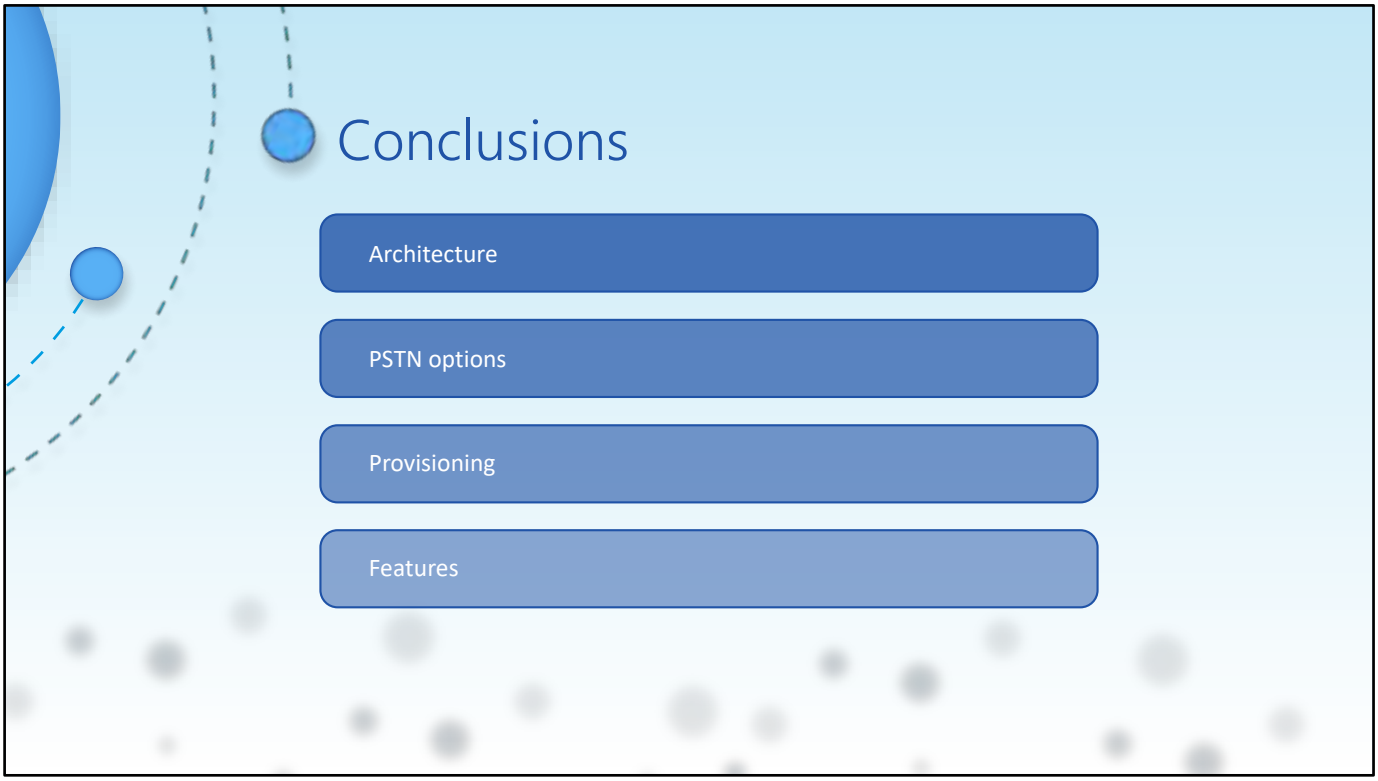
Regional Data Center Locations

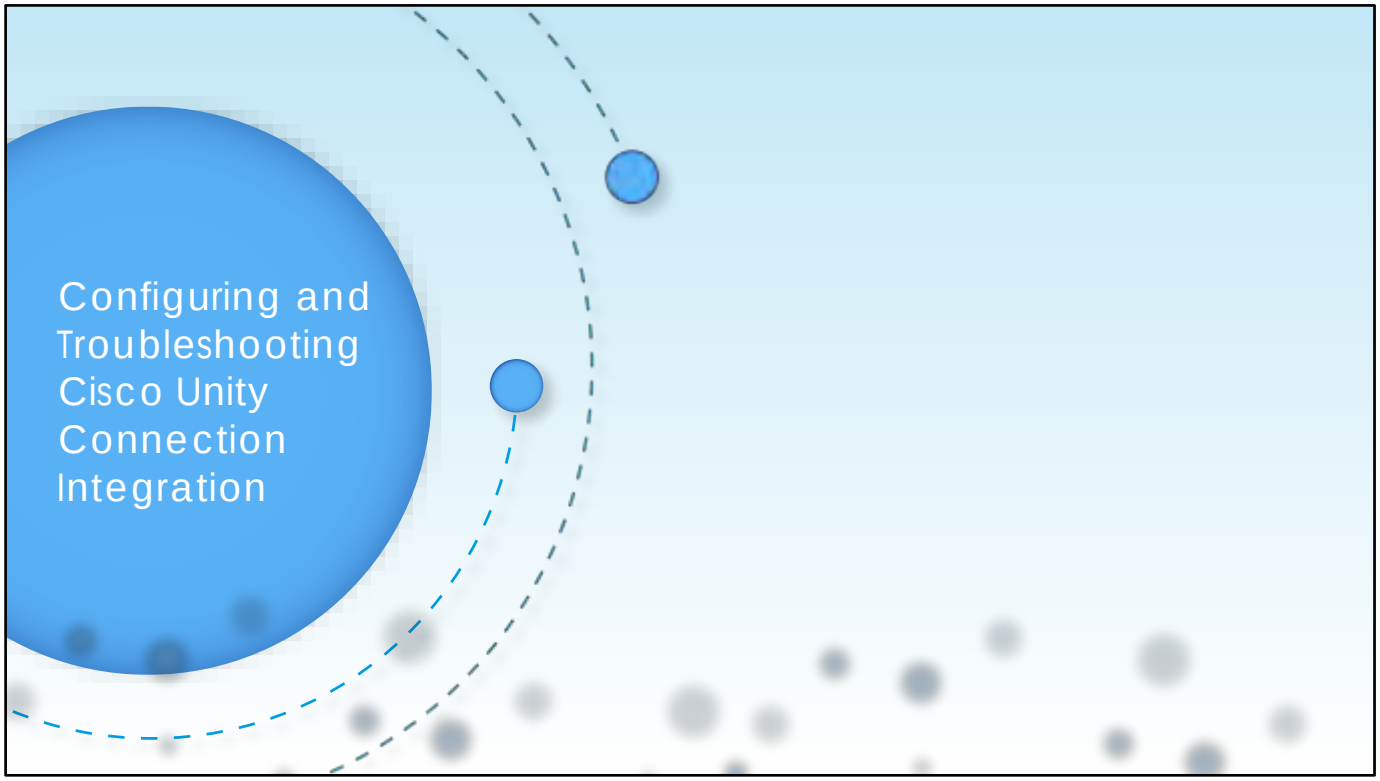












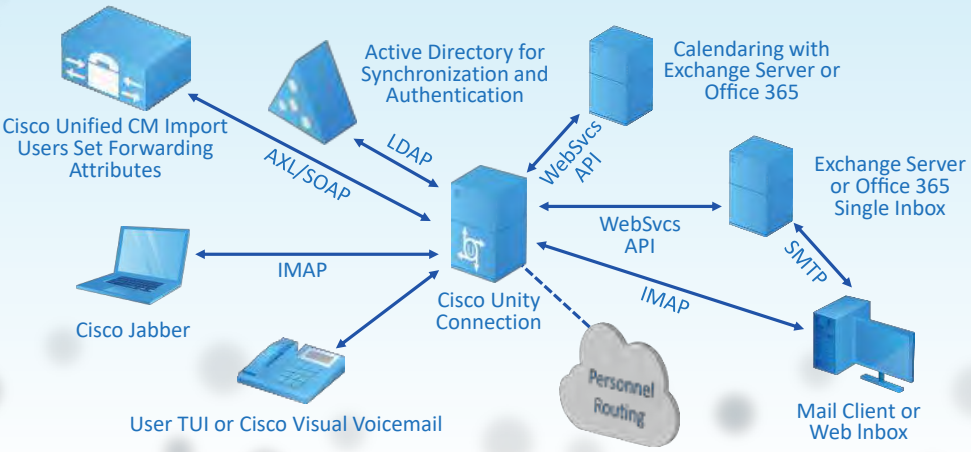
Overview

Phone system integration is essential because it enables communication between Cisco Unity Connection and the phone system, and provides users with the following features:

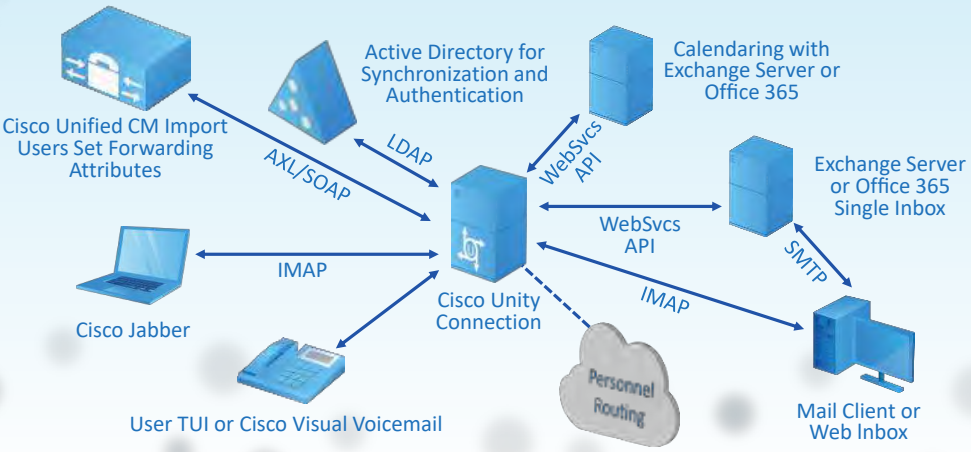
- Calls to a user extension that does not answer are forwarded to the personal greeting of the user.
- Calls to a user extension that is busy are forwarded to the busy greeting of the user.
- Cisco Unity Connection receives caller ID information from the phone system (if available).
- A user has easy access to messages by pressing a button on the phone and entering a password.
- Cisco Unity Connection identifies the user who leaves a message during a forwarded internal call, based on the extension from which the call originated.
- Messages that are left for a user activate the Message Waiting Indicator (MWI) on the extension

Cisco Unity Connection natively integrates with Cisco Unified Communications Manager (Cisco Unified CM) and with Cisco Unified Communications Manager Express through Skinny Client Control Protocol (SCCP) or through a Session Initiation Protocol (SIP) trunk. You can also integrate Cisco Unity Connection with a circuit-switched phone system

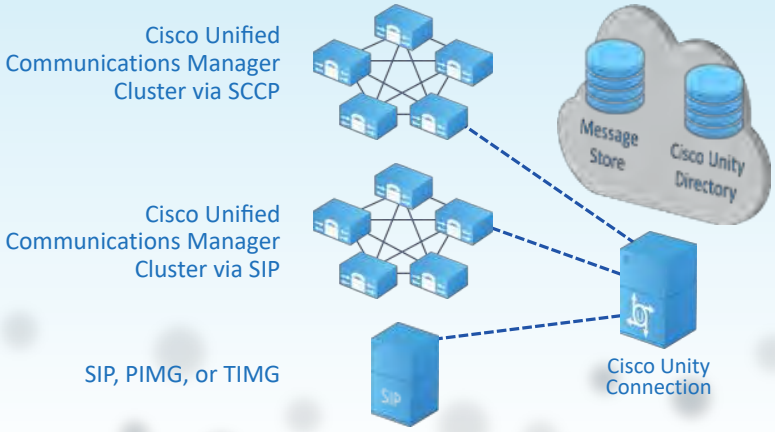
Overview of Cisco Unity Connection Integration



Overview of Cisco Unity Connection Integration (cont'd)



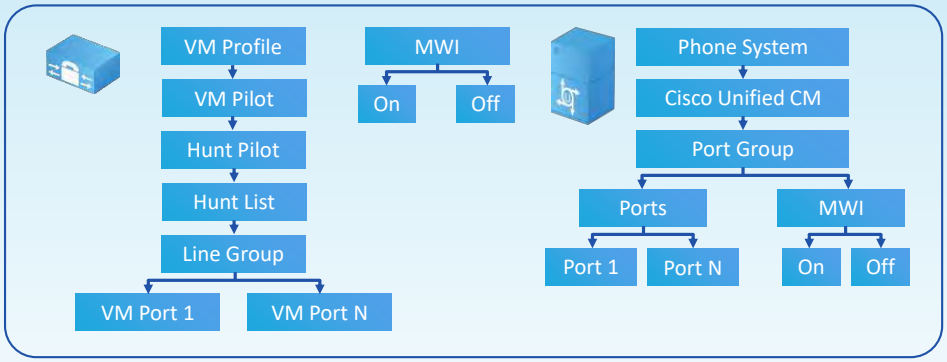
Microsoft Active Directory Integration



Unity Connection Integration

- Can integrate with phone systems like Cisco Unified CM and with qualified circuit-switched phone systems
- Supports simultaneous integrations with multiple
- Third-party phone-system integrations can be accomplished through a SIP trunk using one the following

SCCP Integration



Voice Mail Port Wizard in Cisco Unified CM automatically generates the voicemail ports, and puts the ports into the line group.

The hunt list and hunt pilot need to be configured manually.

SCCP integration uses TCP port 2000 for regular communication and TCP port 2443 for secure communication.

SIP Integration

The voicemail pilot and a route pattern are used to call the voice-messaging system

No explicit MWI numbers are required

SIP integration is required for video greetings

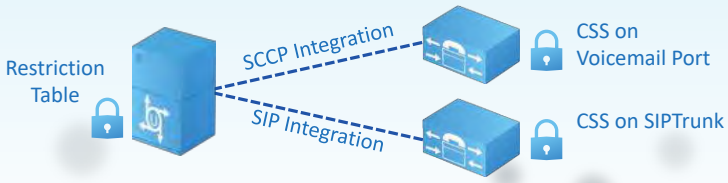
SIP integration uses TCP/UDP port 5060 for regular communication and port 5061 for secure communication

Common Mistake of Integration

Calls to Cisco Unity Connection are failing	Parts are failing to register	MWI problems
Phone system settings do not match.	Device name prefix issues.	MWI is not enabled for voicemail ports.
		Voicemail ports for MWI are too busy.
		Incorrect MWI extensions.
Routing rules are working incorrectly.		MWI is disabled for the user.
		Incorrect phone system.
		CSS issues
		Dial plan overlap

Integration Consideration

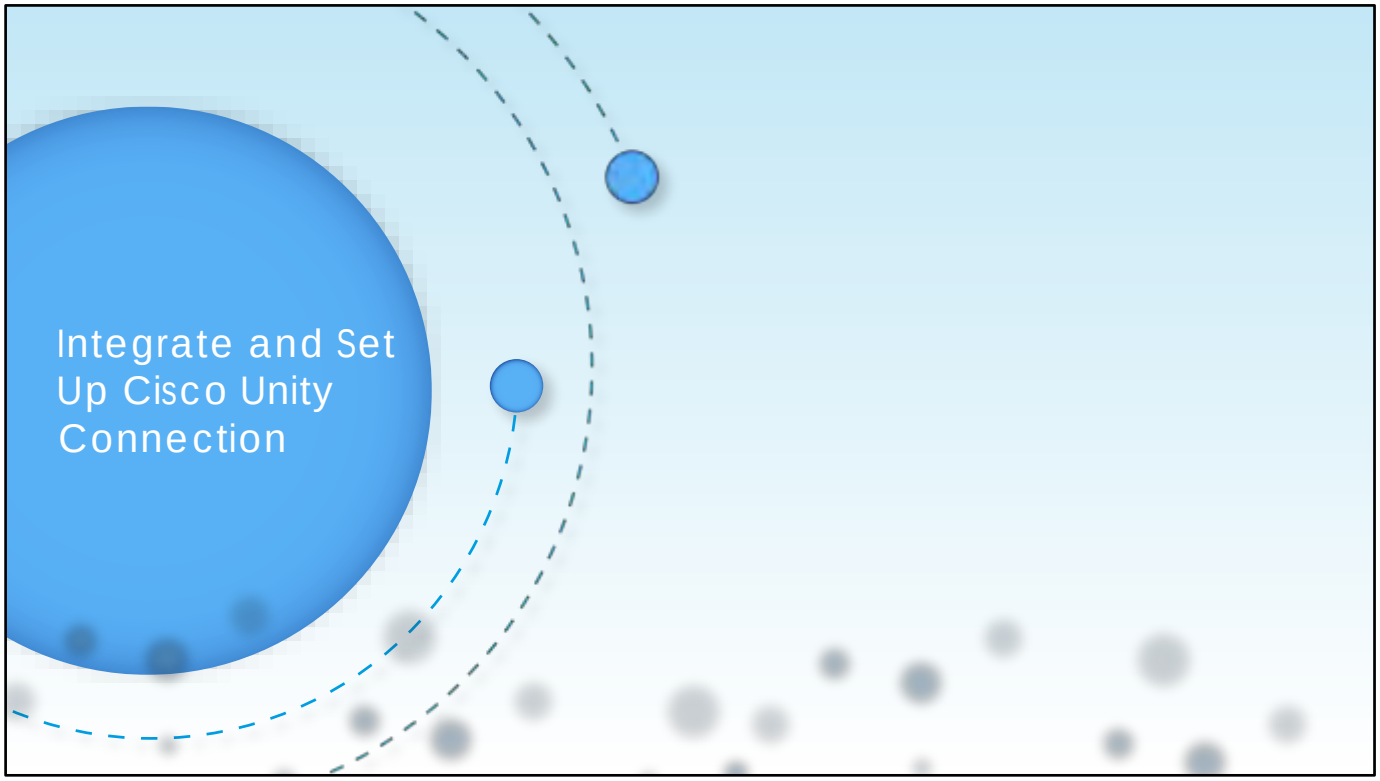
There are some things that you need to consider when integrating Cisco Unity Connection with Cisco Unified Communications Manager to secure Cisco Unity Connection, implement proper MWI handling, and prevent toll fraud



Authentication Rule

Conclusions

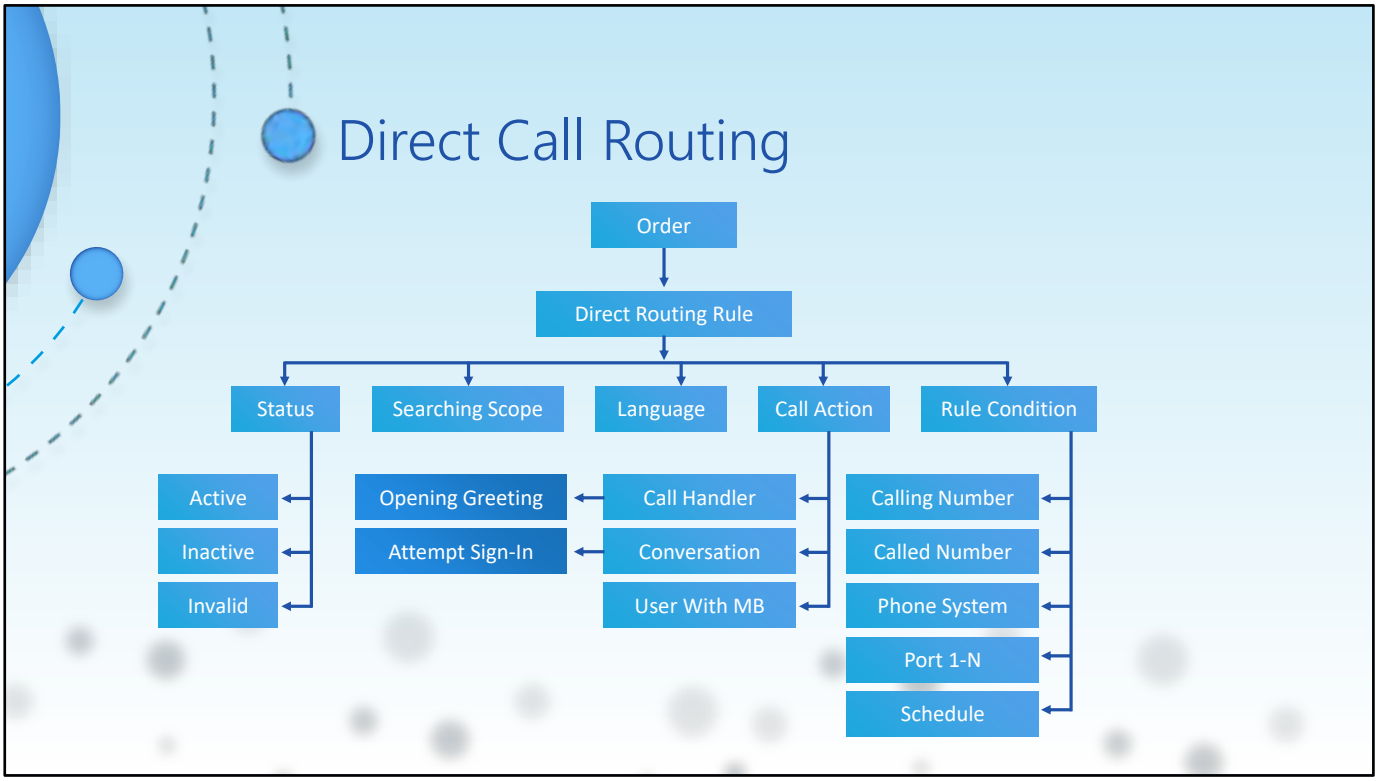
- Overview
  - Cisco Unity Connection Integration
  - Microsoft Active Directory Integration
  - Unity Connection Integration
  - SCCP Integration
  - SIP Integrations
  - Common mistakes
  - Consideration
  - Authentication rules



Default Call-Routing Behavior

By default, two direct and two forwarded call-routing rules exist in Cisco Unity Connection.

- For direct calls, the user can log into the mailbox by entering the PIN.
- For forwarded calls in which a caller dials an extension that is not answering, the call is forwarded to Cisco Unity Connection.



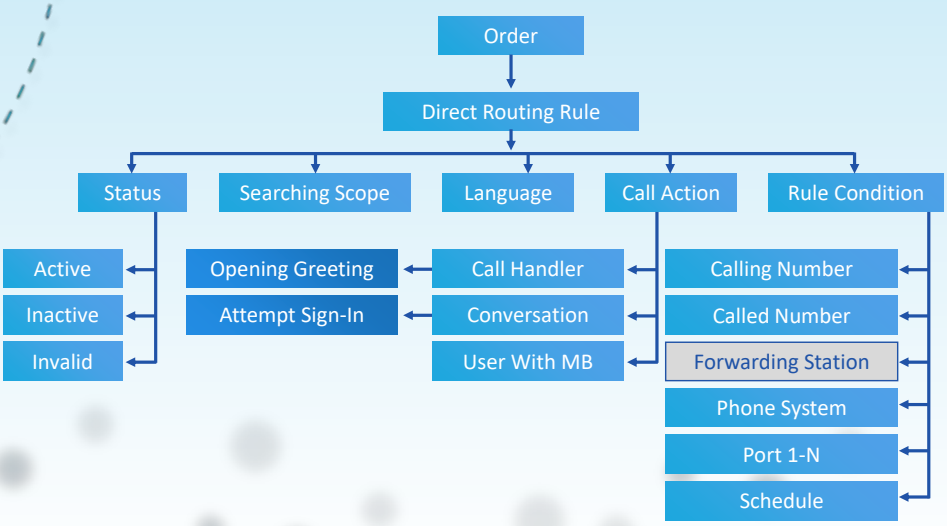
Direct Call Routing

When a direct call-routing rule is used, calls can be filtered and an action can be applied. Callers can be sent to the following options:

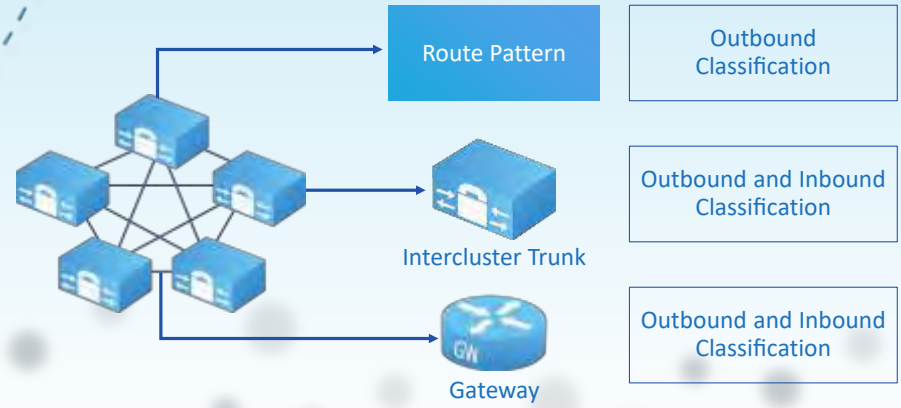
- Calling Number: The rule is applied for a specified calling number, such as 11001 or 123*, for all calls starting with 123.
- Dialed Number: The rule is applied for a specified dialed number such as t number of a call handler.
- Port: The rule is applied for a specified incoming port (1 to n).
- Phone System: The rule is applied for a specified phone system that delivers the call. This condition can be chosen if more than one phone system exists.
- Schedule: The rule is applied for the chosen schedule, such as all weekdays, or any customized schedule

Call actions can be used in combination with rule conditions.

Forwarded Call Routing



Configure Call Forward Based on Call Classification



Call Classification

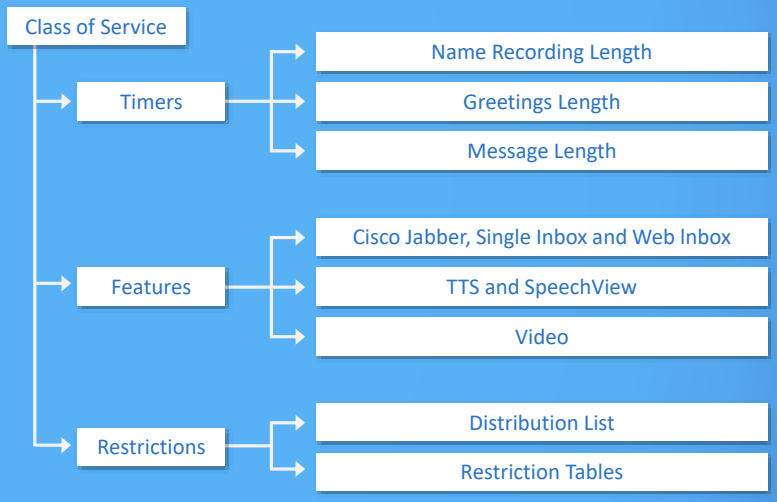
The default call classification is as follows:

- Route patterns are set to off-net.
- Trunks are set to the system default.
- Gateways are set to the system default.
- IP phones are always on-net and cannot be changed

The call classification service parameter (system default) is set to off-net by default

When configuring route patterns, you can configure the Allow Device Override parameter.

Configure Cisco Unity Connection Users

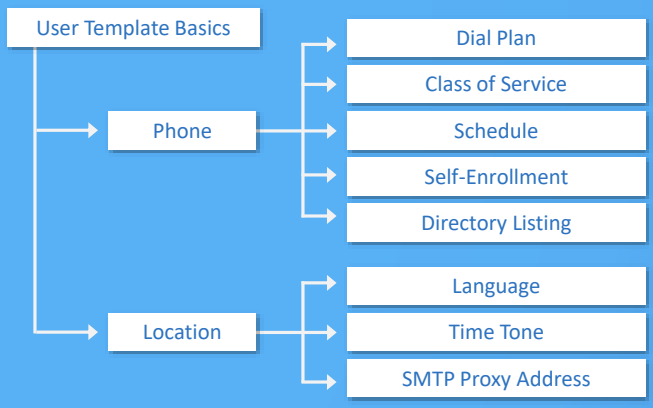


Most Commonly Used Features

1. Record the name of the user.
2. Choose to be listed in the directory.
3. Enable video greetings.
4. View or manage alternate extensions.
5. Change call-screening or holding options.
6. Set advanced features:

Cisco Unity Connection User Templates

- Templates must be created before any user is created because templates are applied only once when a user is added or imported to Cisco Unity Connection. Changes in the CoS are also applied to existing users

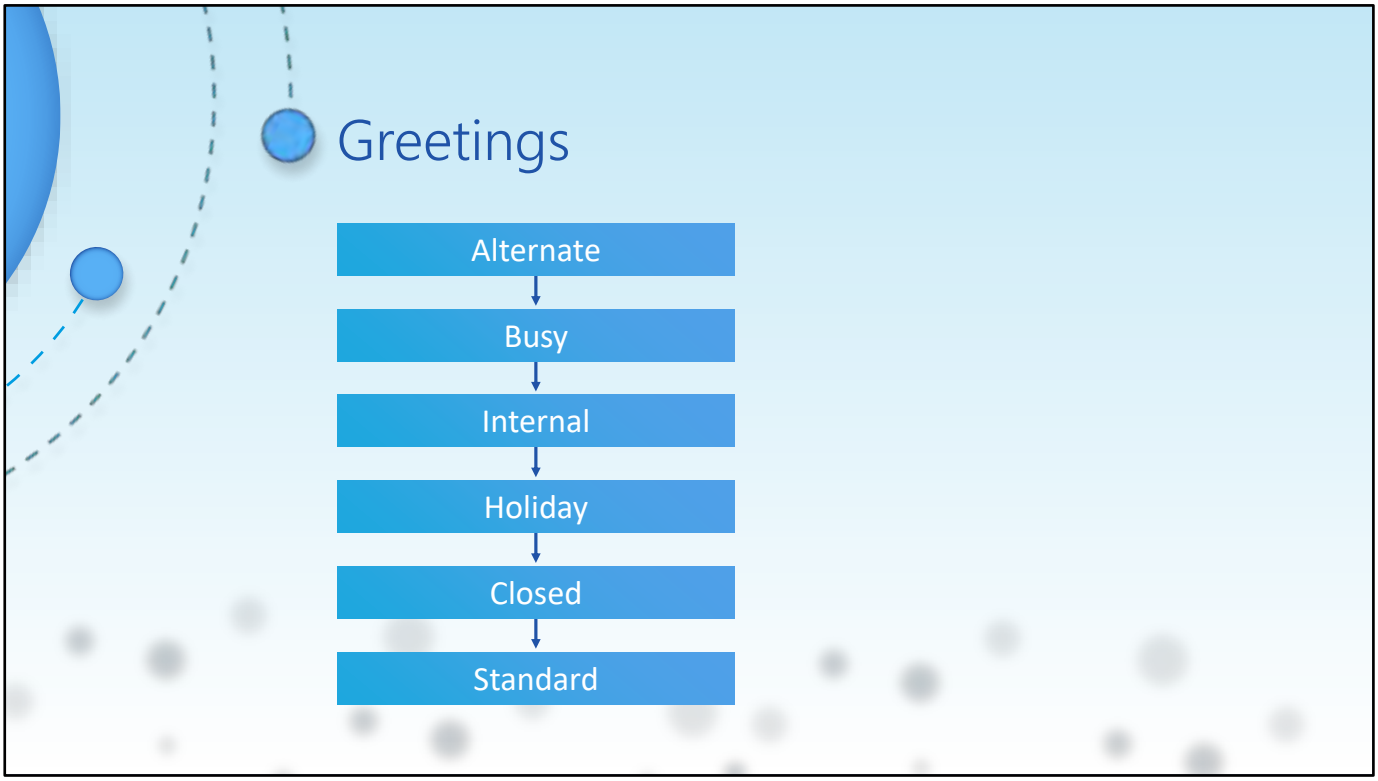


Cisco Unity Connection User Templates

- The most important settings in the user template are as follows:
  - Add a name for the template that describes, for example, the user function, such as employee or manager.
  - The dial plan is set in the phone section and defines the partition to which the user belongs and in which search space the user can search when sending messages.
  - After the Cisco Unity Connection installation, there is one default partition and one search space, which are named after the Cisco Unity Connection system hostname.
  - These partition and search space elements form the dial plan and are associated with the default voicemail user template.
  - The default voicemail user CoS is assigned with the default user template.
  - The schedule is set by default to Weekdays.

Cisco Unity Connection User Templates

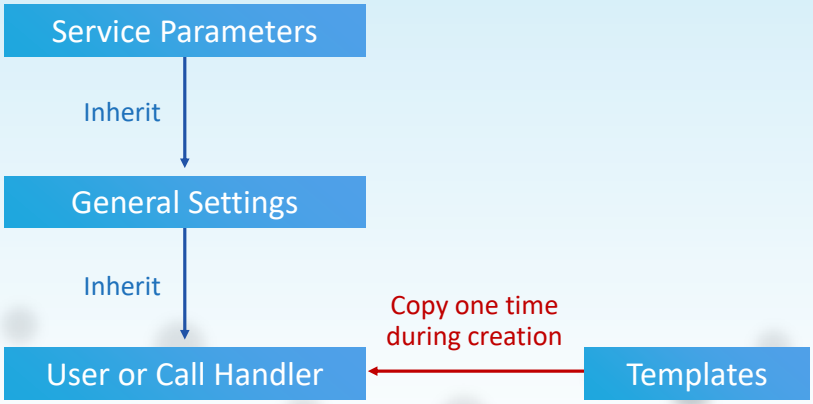
- The most important settings in the user template are as follows:
  - The schedule should be changed to All Hours so that the individual greeting of the end user is always played.
  - You can disable the listing of users in the directory depending on the company policies.
  - The language is set in the location section. This setting is important in a multinational deployment and in a single-site deployment in which different groups might expect callers from only certain countries.
  - The time zone is used for generating time stamps for voice messages.
  - The setting of a proper time stamp helps users get correct information about when a message was received because the time zone of the user location is used.



Message Aging Policy and Mailbox Quotas

- Aging Policy and Mailbox Quotas are defined
  - At system level
  - In user template
  - On User Account
- Text alert can be defined to send warning
- Aging Rule can be define to ensure hard disk does not get filled up
- Read Message can moved to deleted folder
- 15 Day Default setting – Messages in deleted folder will be permanently deleted.

Modify Service, Enterprise, and Advanced Settings

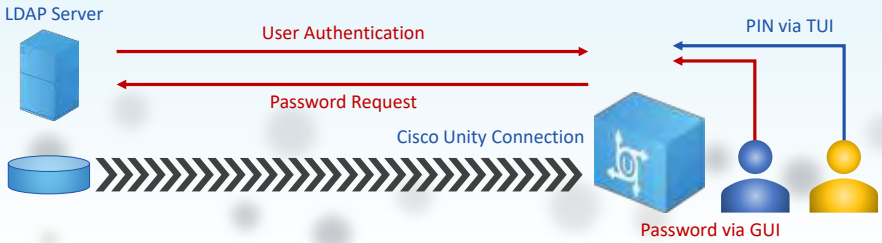


Integrate Cisco Unity Connection with the LDAP Server

LDAP integration has two parts. In LDAP synchronization, users are imported from the LDAP server to Cisco Unity Connection.

Cisco Unity Connection cannot copy any information to the LDAP server.

LDAP integration comprises LDAP synchronization and LDAP authentication:



Implement Schedules

Cisco Unity Connection also uses schedules to manage calls

Call handler transfer rules can be varied based on a schedule

Schedules also affect when user and call handler greetings play

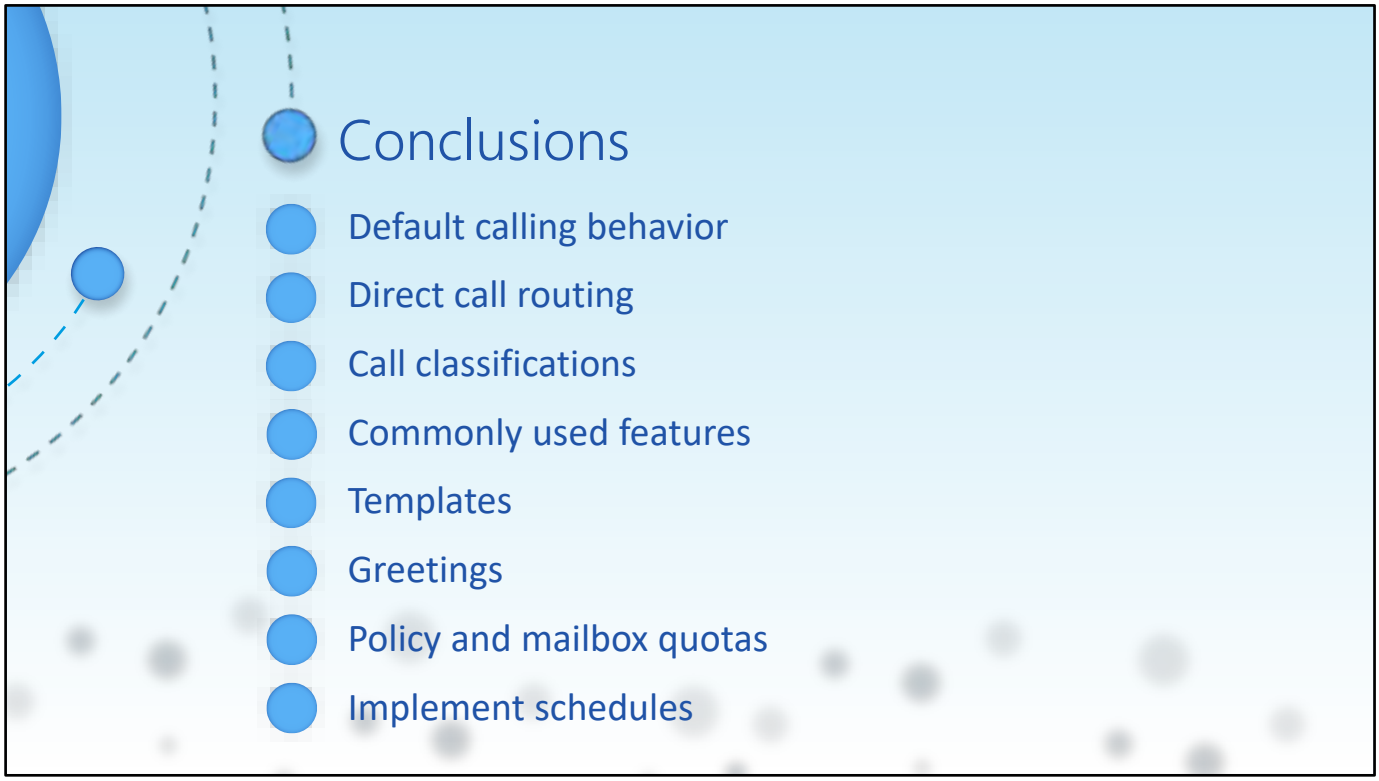
Cisco Unity Connection offers three predefined schedules

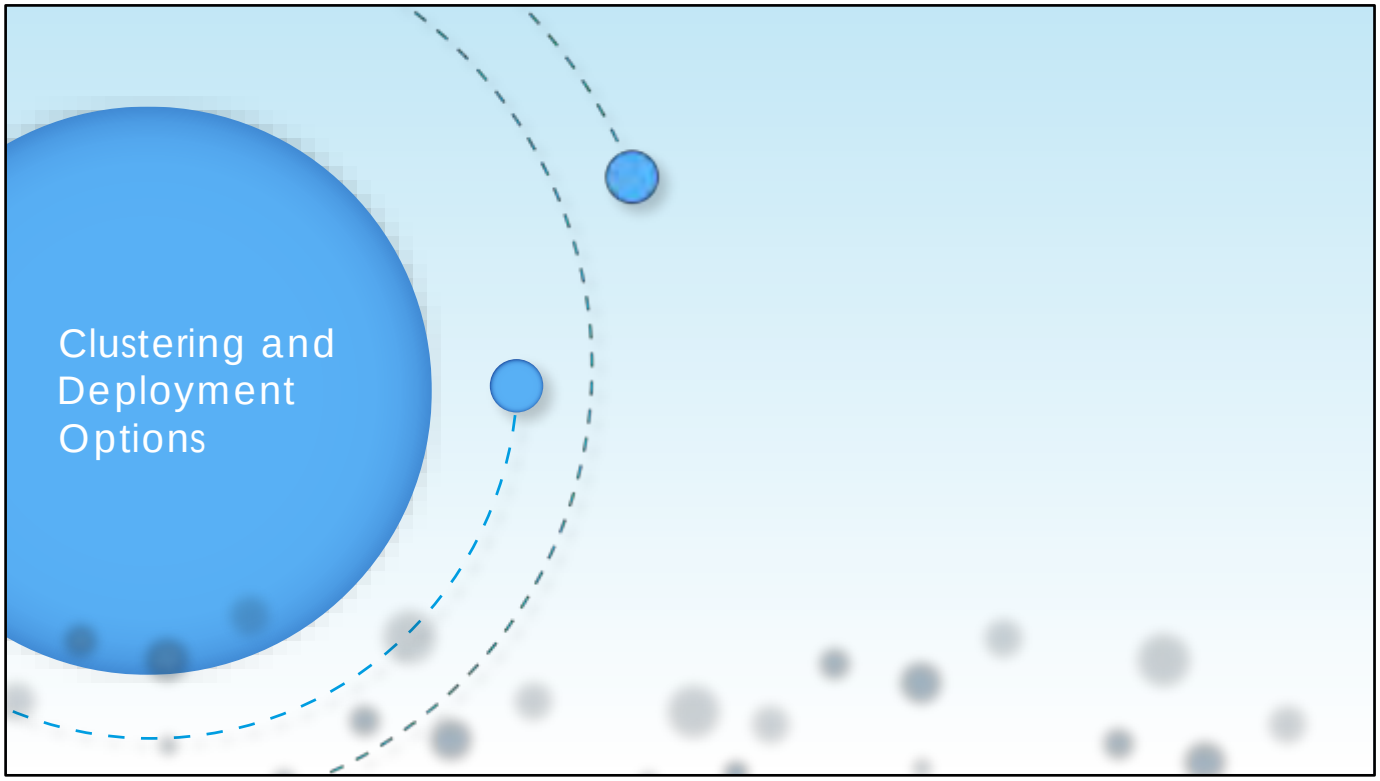
- All Hours
- Weekdays
- Voice Recognition

All can be modified, but not deleted

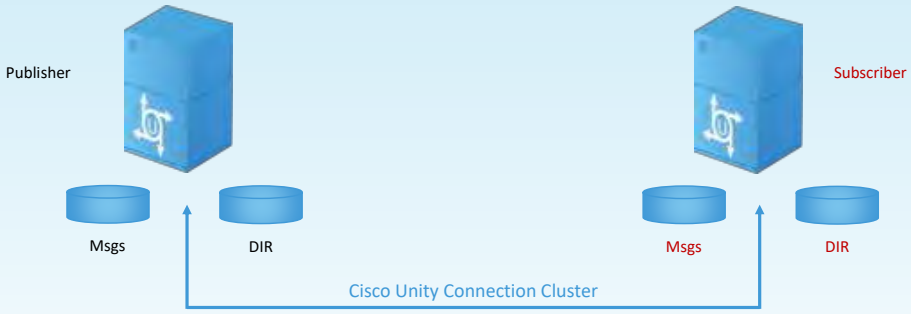
By default, the Weekdays schedule is configured to observe standard hours from 8:00 a.m. through 5:00 p.m. (0800 through 1700), Monday through Friday

- **Standard hours**
- **Closed Hours**





Clustering Options



Cisco Unity Connection supports high availability and redundancy:

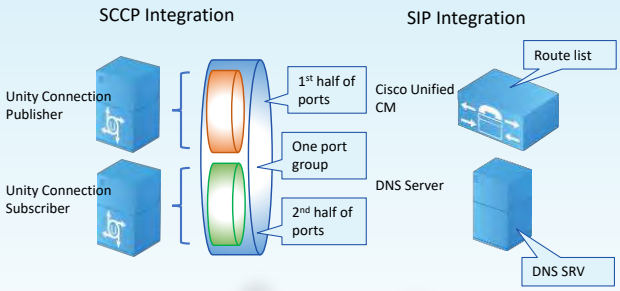
- A maximum of two servers are supported in a cluster pair.
- One server is designated as a publisher.
- The second server is designated as a subscriber or secondary server.
- You can load balance calls and clients in a Cisco Unity Connection cluster.

Balancing the Cisco Unity Connection Call Load

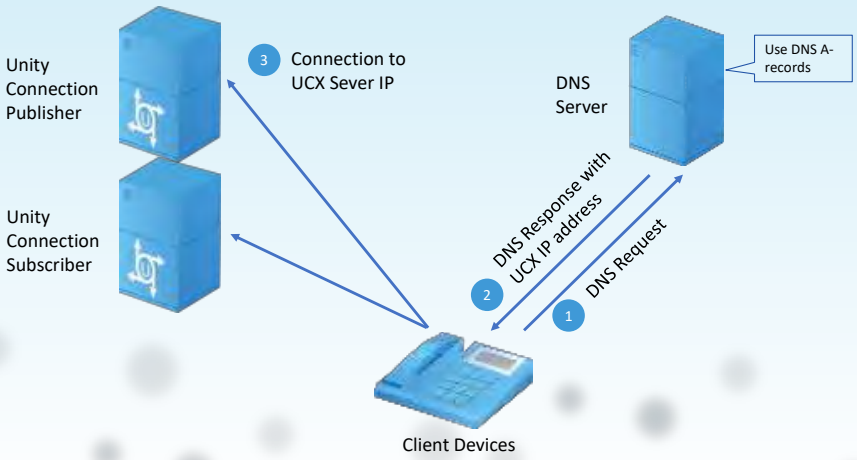
When integrating Cisco Unity Connection with Cisco Unified Communications Manager by SCCP, it is possible to balance the voice traffic that the Cisco Unity Connection server pair manages. In Cisco Unity Connection Administration, all the ports are in a single port group. The first half of the answering ports and dial-out ports are assigned to the publisher server and the remaining ports are assigned to the subscriber server in the Cisco Unity Connection cluster.

When integrating with Cisco Unified Communications Manager through a SIP trunk, it is possible to balance voice traffic that the Cisco Unity Connection cluster server pair manages using one of the following methods:

- Use a route list in Cisco Unified Communications Manager
- Use DNS-SRV (RFC 2782)
- Use a SIP gateway DNS-SRV



Load-Balancing Clients in a Cisco Unity Connection Cluster

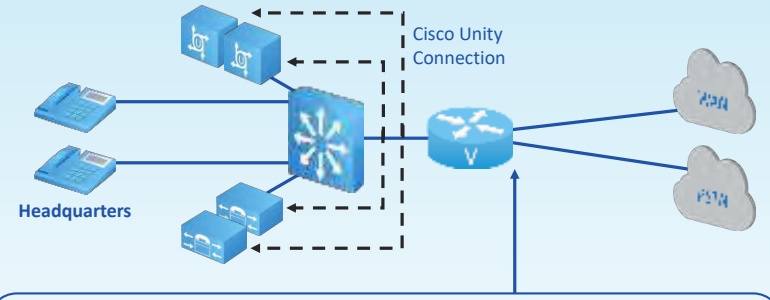


Deployment Options

Cisco Unity Connection and Cisco Unified Communications Manager deployment models, including single-site messaging, centralized messaging, and distributed messaging, can be combined to suit customer requirements. When choosing a deployment model, you must consider a range of issues such as the following:

- Centralized messaging allows you to consolidate servers and administration. However, you must plan for access to voice messages during WAN outages and you must perform the appropriate QoS and capacity planning for voice-messaging traffic and call traffic.
- Distributed messaging may require more servers and administrative overhead, but combined with distributed call processing, it requires less capacity on intersite WAN links.

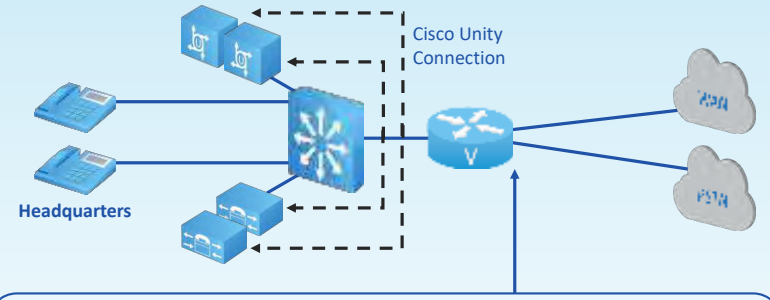
Single-Site Deployment



A standalone server supports as many as 20,000 voicemail users and 250 voicemail ports. A cluster with two Cisco Unity Connection servers offers high availability for 20,000 users and 500 voicemail ports.

Deployment is easy and uses only one codec (Opus as the line codec and G.711 as the recording codec); transcoders and traffic-pattern evaluation are not necessary

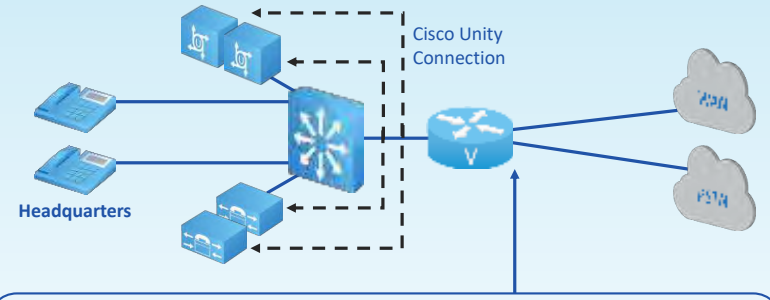
Single-Site Deployment



A standalone server supports as many as 20,000 voicemail users and 250 voicemail ports. A cluster with two Cisco Unity Connection servers offers high availability for 20,000 users and 500 voicemail ports.

Deployment is easy and uses only one codec (Opus as the line codec and G.711 as the recording codec); transcoders and traffic-pattern evaluation are not necessary

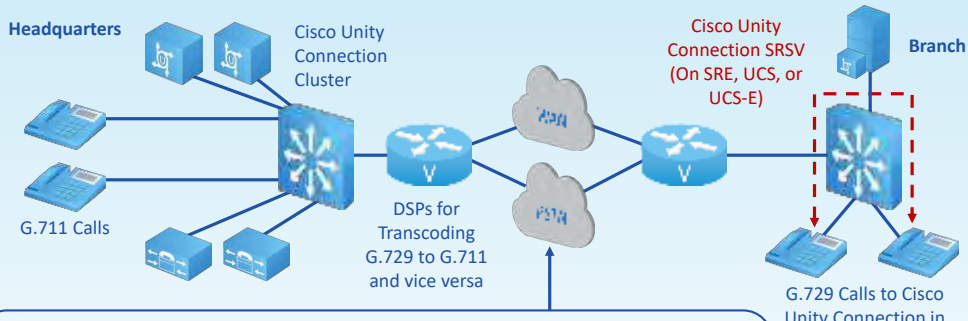
Single-Site Deployment



A standalone server supports as many as 20,000 voicemail users and 250 voicemail ports. A cluster with two Cisco Unity Connection servers offers high availability for 20,000 users and 500 voicemail ports.

Deployment is easy and uses only one codec (Opus as the line codec and G.711 as the recording codec); transcoders and traffic-pattern evaluation are not necessary

Centralized Multisite Deployment

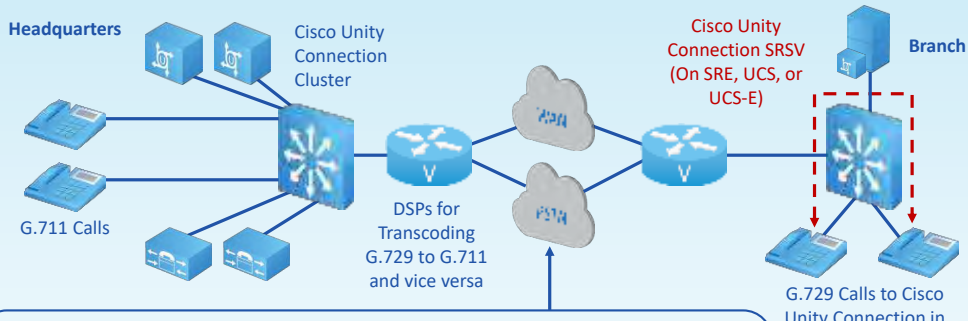


Cisco Unity Connection and the WAN must be highly reliable.

Cisco Unity Connection SRSV (virtualized and installed on a Cisco SRE module or Cisco UCS/UCS-E) offers voice messaging to branch IP phones during a WAN failure.

G.729 calls over the WAN require traffic-pattern evaluation, CAC, and transcoders to be configured.

Centralized Multisite Deployment

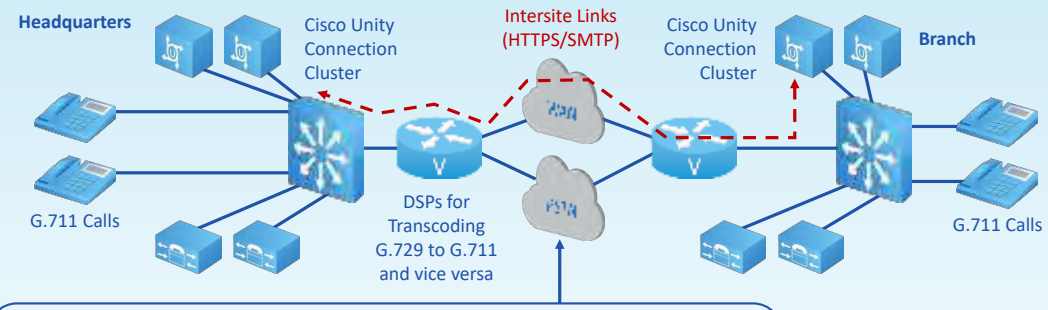


Cisco Unity Connection and the WAN must be highly reliable.

Cisco Unity Connection SRSV (virtualized and installed on a Cisco SRE module or Cisco UCS/UCS-E) offers voice messaging to branch IP phones during a WAN failure.

G.729 calls over the WAN require traffic-pattern evaluation, CAC, and transcoders to be configured.

Decentralized Multisite Deployment

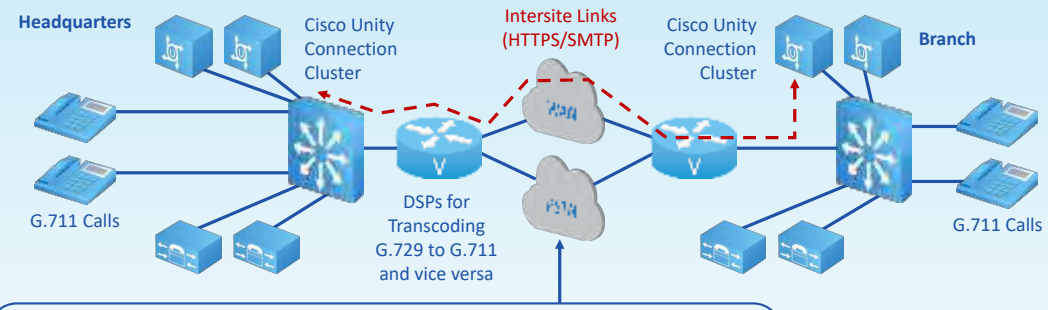


Each site has its own call-processing and voice-messaging system and is self-sufficient.

Intersite links may connect the Cisco Unity Connection clusters in both locations.

Messages are sent to remote users via G.729 over the WAN when the phone is used.

Decentralized Multisite Deployment

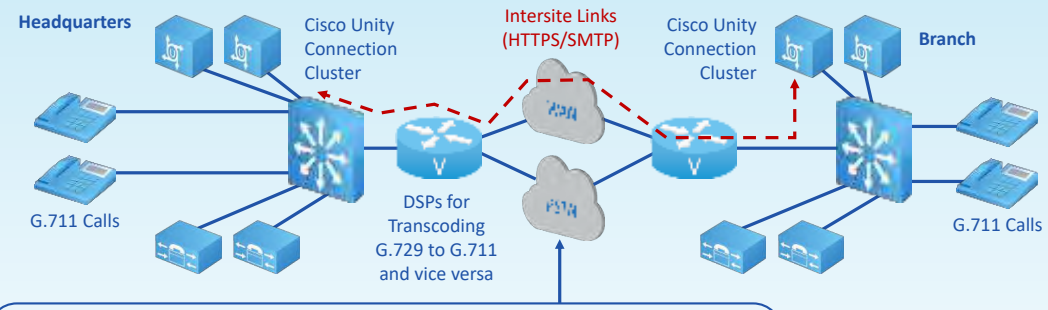


Each site has its own call-processing and voice-messaging system and is self-sufficient.

Intersite links may connect the Cisco Unity Connection clusters in both locations.

Messages are sent to remote users via G.729 over the WAN when the phone is used.

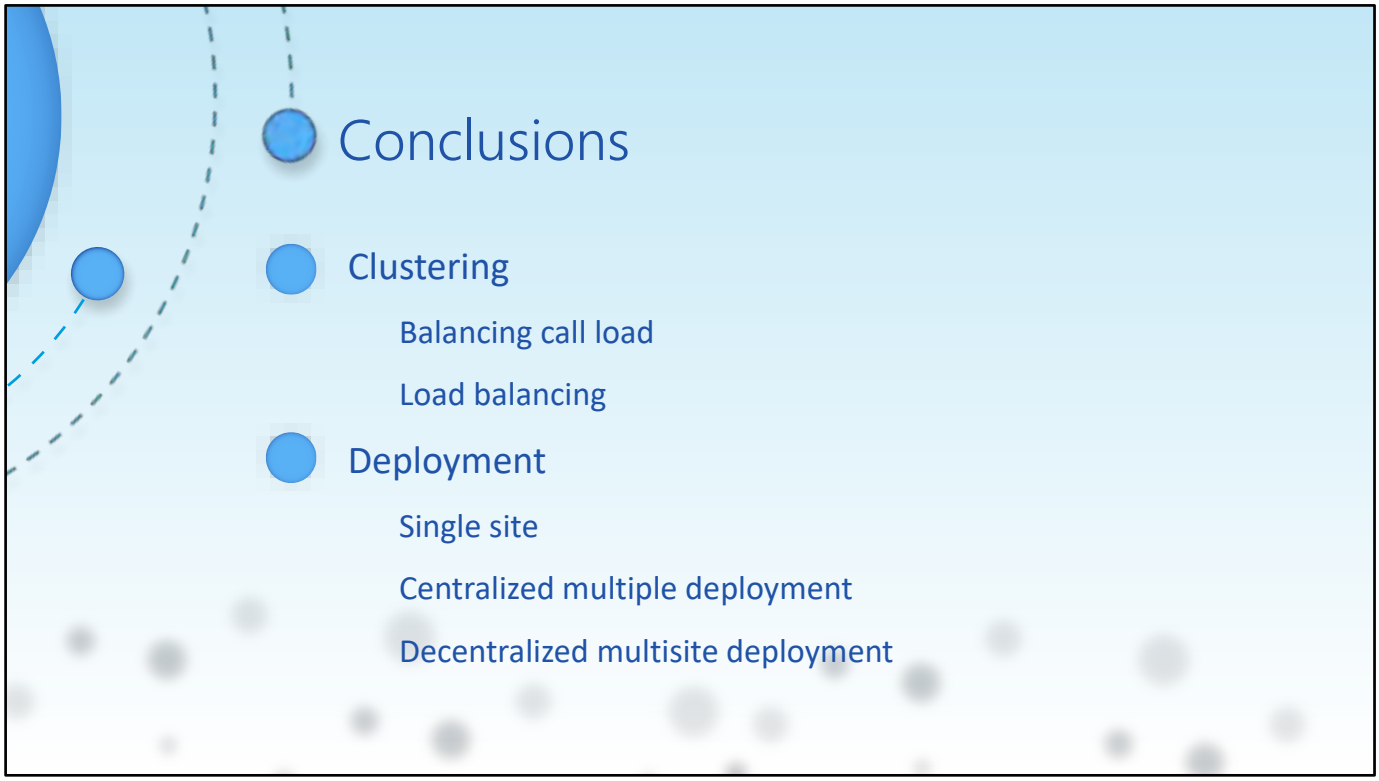
Decentralized Multisite Deployment

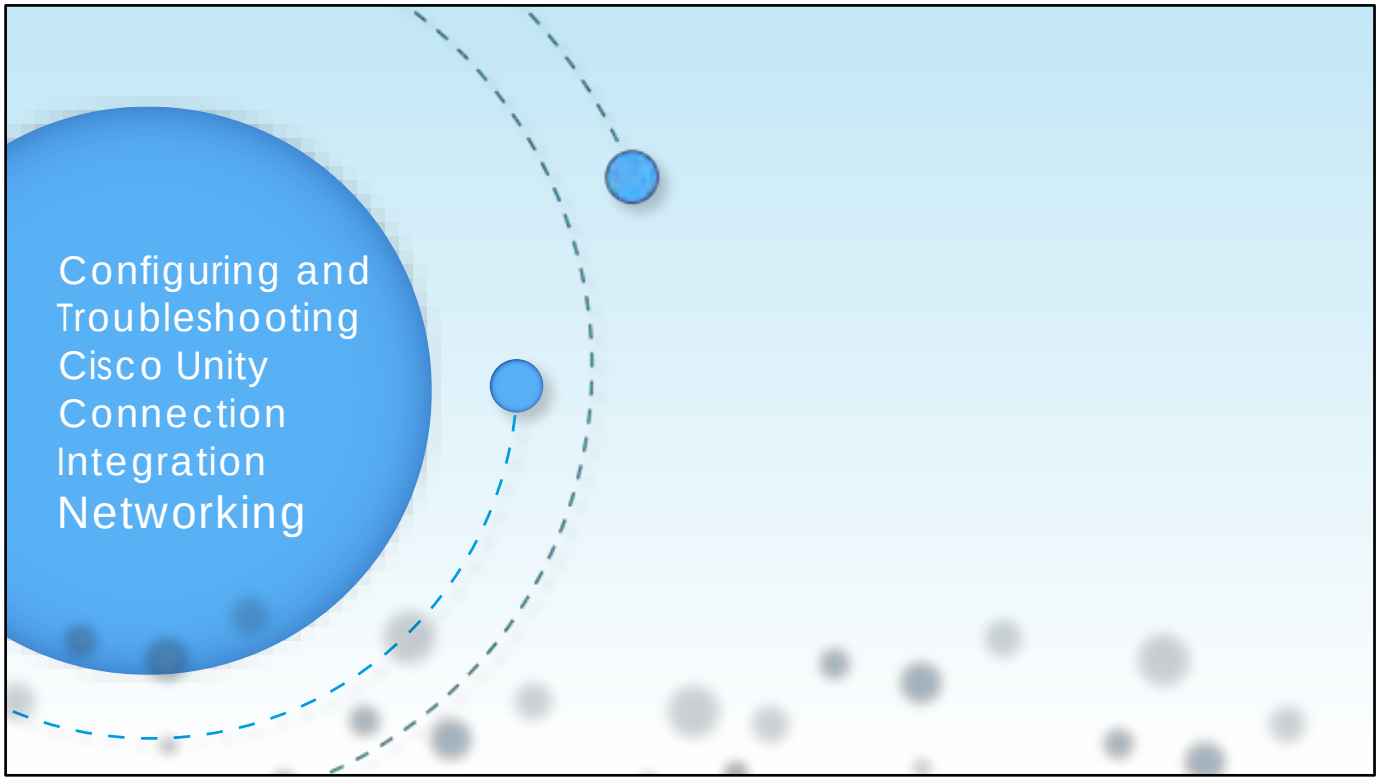


Each site has its own call-processing and voice-messaging system and is self-sufficient.

Intersite links may connect the Cisco Unity Connection clusters in both locations.

Messages are sent to remote users via G.729 over the WAN when the phone is used.

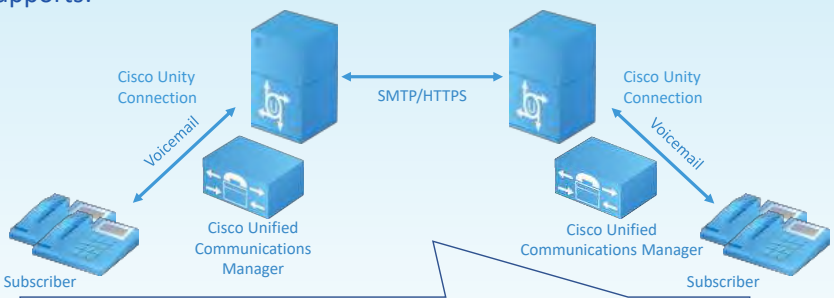




Overview of Networking

Cisco Unity Connection supports:

- Legacy networking
  - **Intrasite**
  - **Intersite**
- **HTTPS Networking**
- **VPIM Networking**



Messaging is among multiple Cisco Unity Connection servers.

Users can send messages to subscribers on other networked servers (by name or extension).

Example: Use the IP phone to forward fax and email messages to any subscriber in the organization

Cisco Unity Connection Digital Voicemail Network

Objects such as the following are replicated in a Cisco Unity Connection digital voicemail network:

- Users
- System distribution lists (including membership)
- Partitions
- Search spaces
- Recorded voice names

Legacy Networking – Intrasite

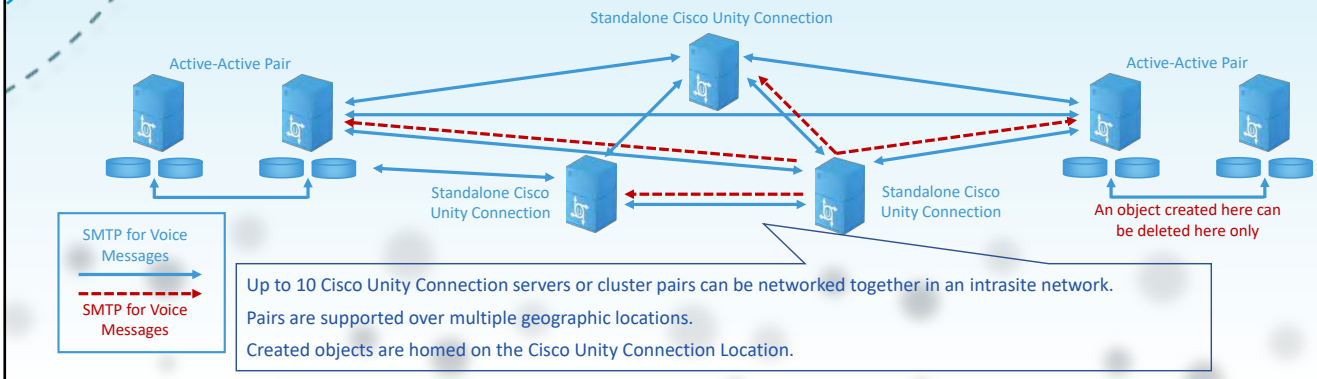
Two or more Cisco Unity Connection servers or clusters (up to a maximum of 10 clusters) to form a well-connected network, referred to as a Cisco Unity Connection site

The servers that are joined to the site are referred to as locations

Cluster counts as one location in the site

Linked to every other location in the site via an intrasite link

Intrasite networking is supported only with Cisco Business Edition 6000/7000



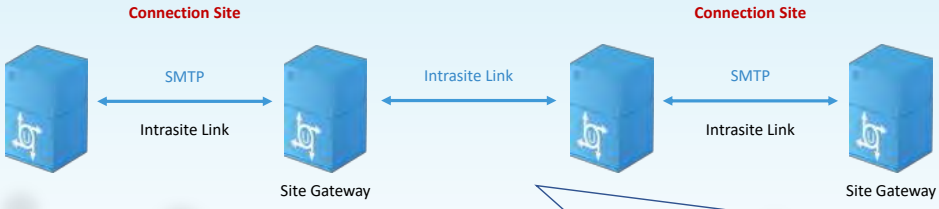
Legacy Networking – Intersite

Two Cisco Unity Connection sites also can be joined to support a maximum of 20 locations for businesses that need more than 10 locations

Only one intersite link is supported per site, so you can link a single Cisco Unity Connection site to another Cisco Unity Connection site

To create an intersite link, choose a single location from each site to act as a gateway to the other site

All directory synchronization communications pass between the two site gateways



Cisco Unity Connection sites can be linked to other Cisco Unity Connection sites using an intersite link.

A single location from each site acts as a gateway to the other site. Only one intersite link is supported per site.

The intersite link increases network capacity to a maximum of 20 Cisco Unity Connection servers.

Legacy Networking – Intersite

Cisco Unity Connection supports HTTPS Networking, that allows you to connect different Cisco Unity Connection servers and clusters in a single site network

HTTP networking provides more scalable Cisco Unity Connection deployments as compared to legacy networking

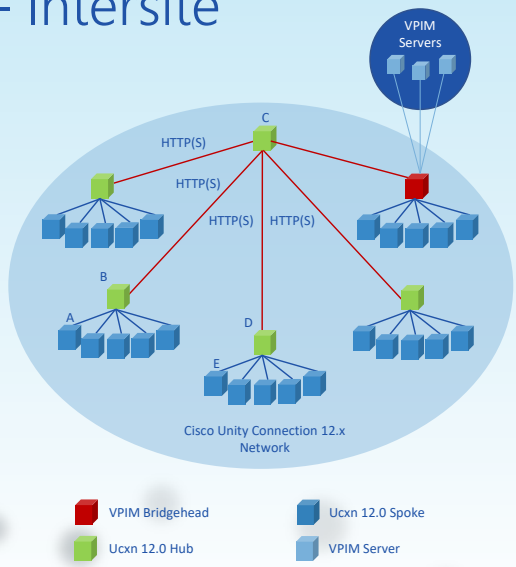
The architecture of HTTPS networking is scalable both in terms of number of Cisco Unity Connection locations and the total directory size

Legacy and HTTPS networking are not simultaneously supported in the same network

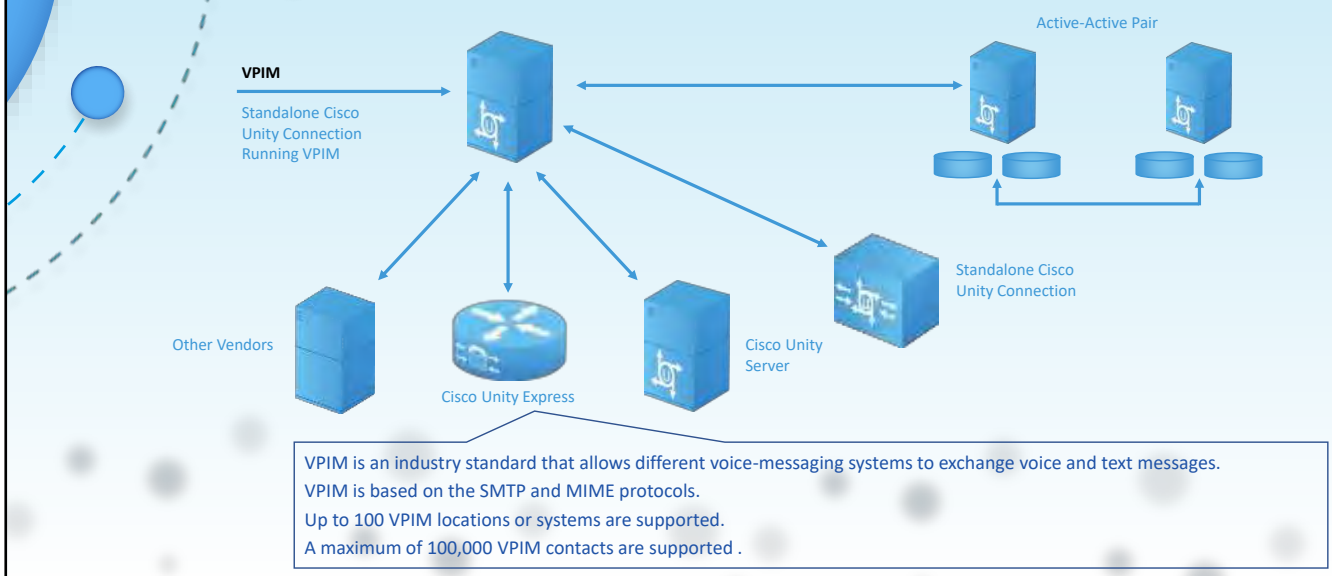
VPIM networking is supported only with Cisco Business Edition 6000/7000

Cisco Unity Connection Version 12.x has separate limits for user, contacts, distribution list

- 100,000 users
- 150,000 contacts
- 100,000 system distribution lists
- 25,000 users per system distribution list



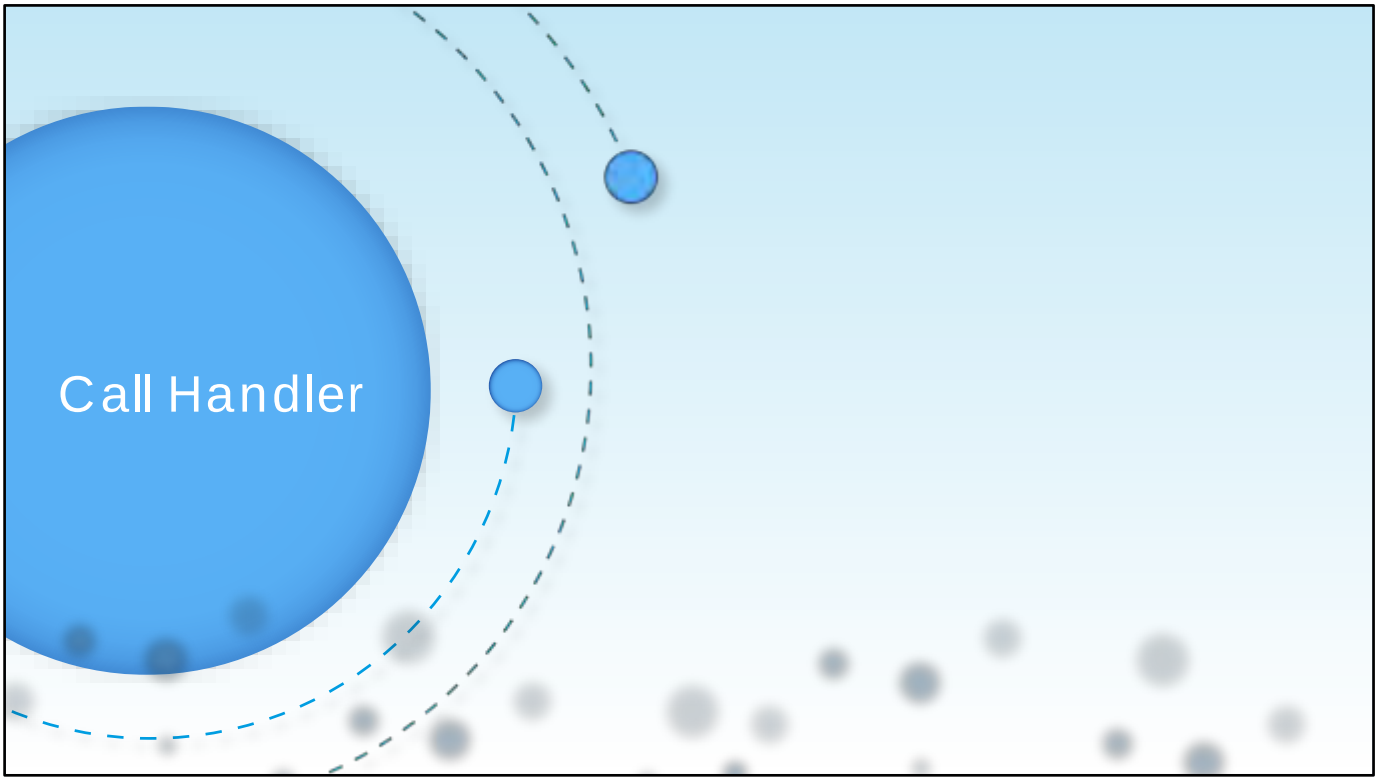
VPIM Networking



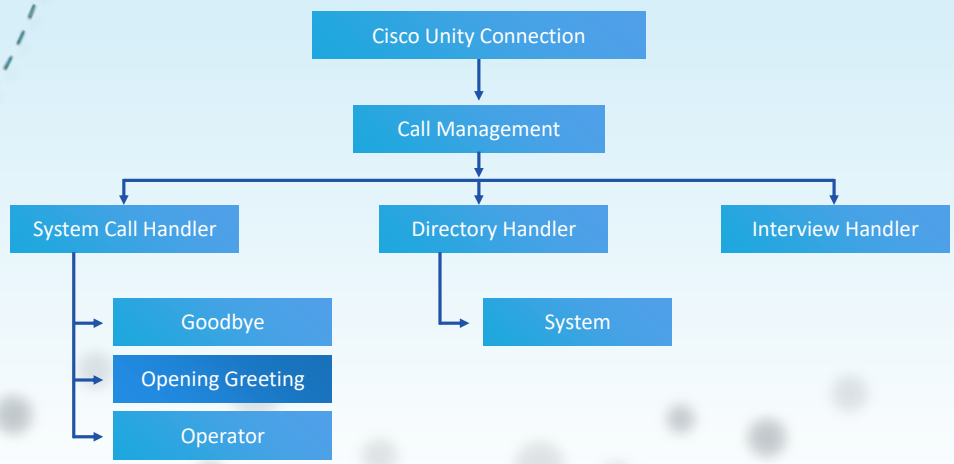
VPIM is an industry standard that allows different voice-messaging systems to exchange voice and text messages.
VPIM is based on the SMTP and MIME protocols.
Up to 100 VPIM locations or systems are supported.
A maximum of 100,000 VPIM contacts are supported .

Conclusions

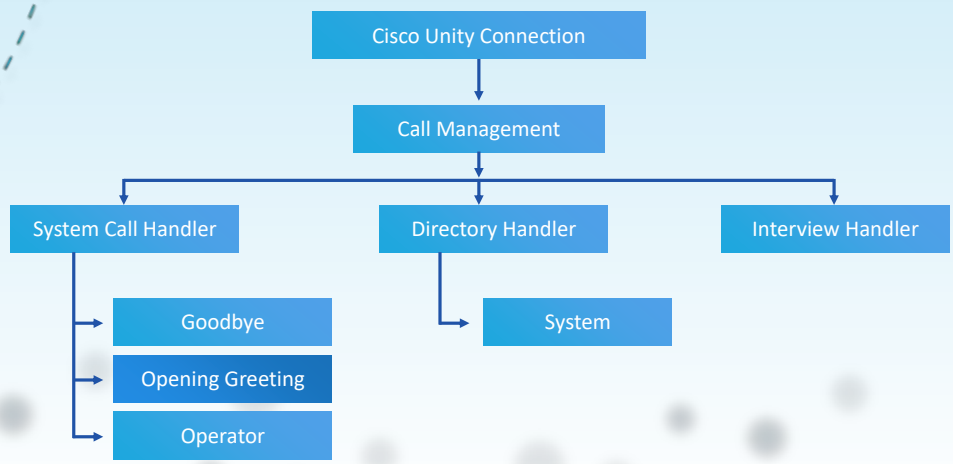
- Overview
  - Digital voicemail
  - Intrasite
  - Intersite
  - HTTPS Networking
  - VPIM

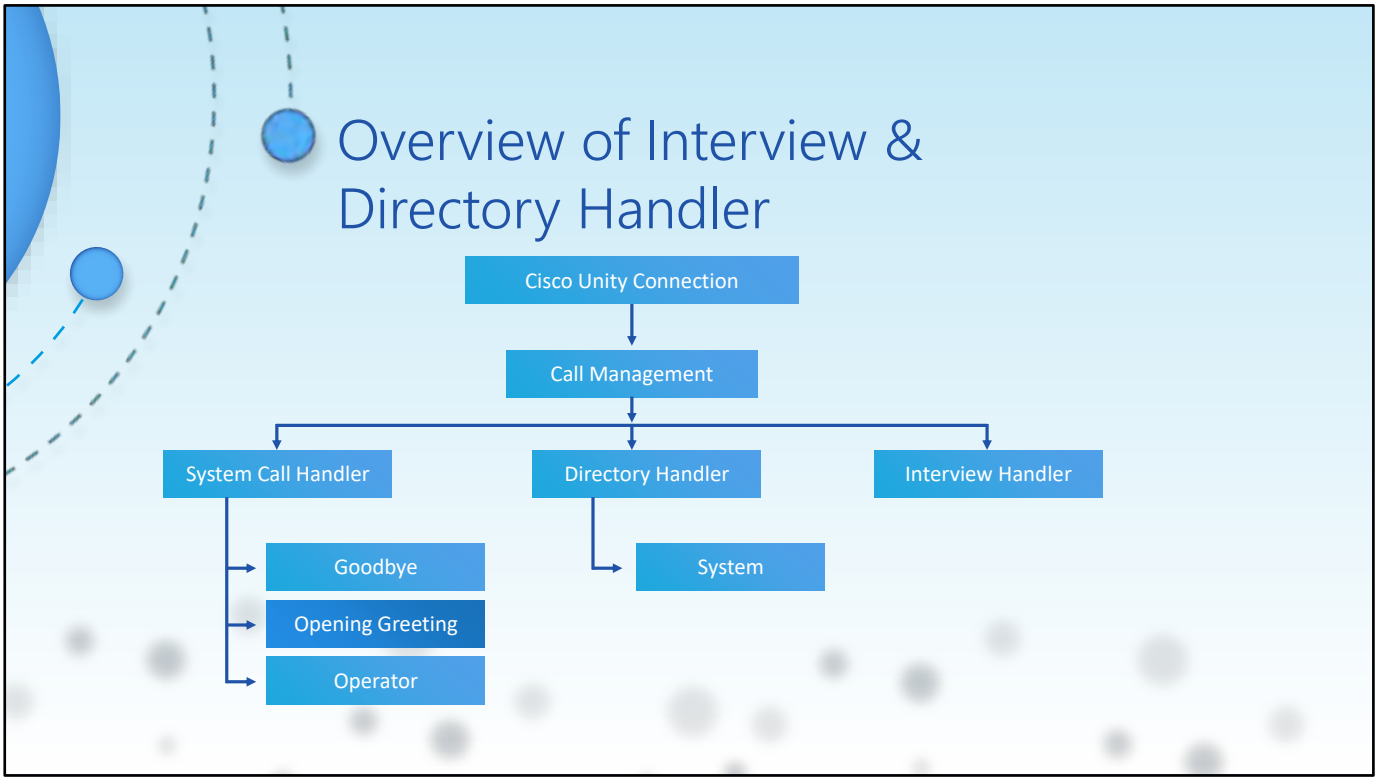


Overview of CallHandler



Overview of System CallHandler



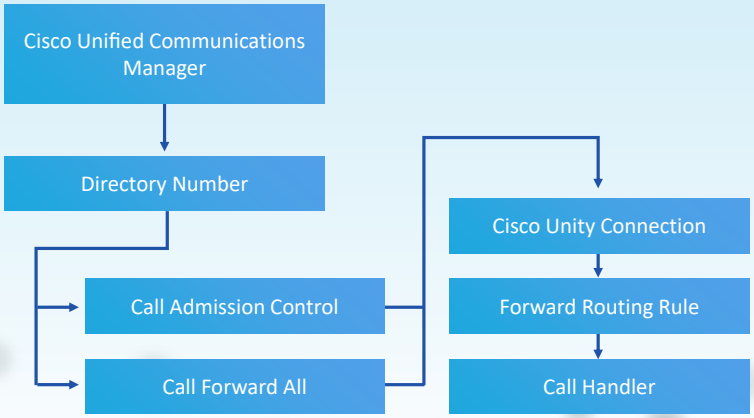


Call Handler Comparison

Each call handler is dedicated to a specific purpose and is therefore limited in its options, but is optimized for its required tasks. The following table gives you a quick overview of the call handlers and what each handler does

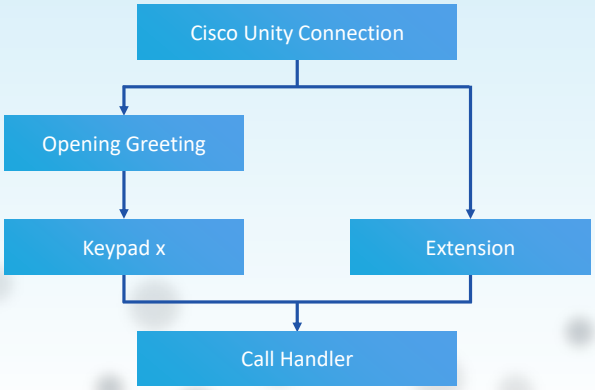
Options	System Call Handler	Directory Handler	Interview Handler
Call handler templates	Yes		
Transfer rules	Yes		
Caller input	Yes	Limited	
Greeting management	Yes	Limited	
Postgreeting recording	Yes		
After message or interview action	Yes		Yes
Interview questions			Yes
Call handler owners	Yes		

Call Handler Reachability

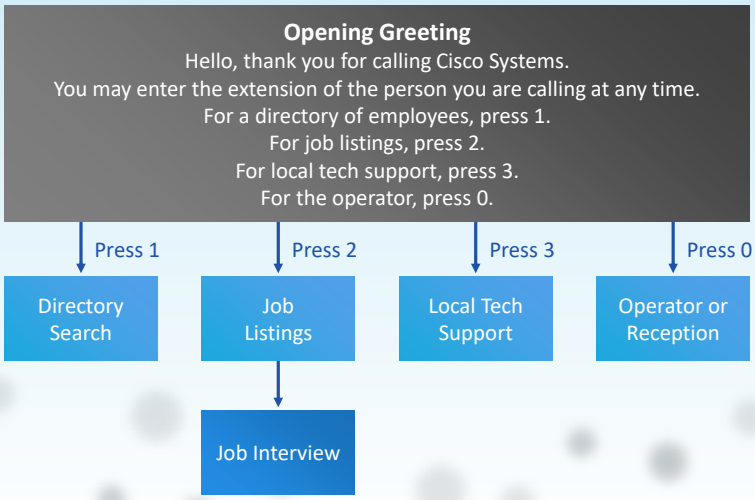


Call Handler Reachability

A caller who already reached Cisco Unity Connection (for example, the opening greeting) can choose a call handler from a menu, by entering a predefined and configured digit), or dial the extension of the call handler.



Auto-Attendant Example



System Call Handler

As an Automated Attendant | As a Message Recipient | To Transfer Calls | To Offer Prerecorded Audiotext

System call handlers provide caller direction through a customized set of configurable features. These features consist of greetings, caller input, transfer, and message settings. The various options that are included in these features provide you with the tools that are required to design and build an audiotext application to support your unique business needs and requirements.

As an automated attendant: A call handler can act as a human operator to answer and direct calls by playing greetings and responding to keys pressed by the user. The automated attendant can provide a menu of options (for example, “For Sales, press 1; for Service, press 2; for our business hours, press 3.”)

To offer prerecorded audiotext: A call handler can provide information that customers request frequently (for example, “Our normal business hours are Monday through Friday, 8 a.m. to 5 p.m.”), or to play a prerecorded message that all callers hear before they can interact with the system

As a message recipient: A call handler can take messages for the organization (for example, “All of our customer service representatives are busy. Please state your name, phone number, and account number. We will return your call as soon as possible.”).

To transfer calls: A call handler can route callers to a user (for example, after hours, you could transfer calls that come to a technical support call handler directly to the mobile phone of the person who is on call), or to another call handler.

Cisco Unity Connection 12.x supports 40,000 system call handlers.

Default System Call Handlers

Opening Greeting | Operator | Goodbye

Cisco Unity Connection includes the following predefined call handlers. You can edit these call handlers, but you cannot delete them

Opening greeting: This call handler acts as an automated attendant, plays the greeting that callers first hear when they call your organization, and performs the actions that you specify. The opening greeting call-routing rule transfers all incoming calls to the Opening Greeting call handler.

By default, the opening greeting call handler allows callers to press star (*) to reach the Sign-In conversation, or press pound (#) to reach the operator call handler. Messages that are left in the opening greeting call handler are sent to the Undeliverable Messages distribution list.

Operator: Calls are routed to this call handler when callers press “0” or do not press any key (the default setting). You can configure the operator call handler so that callers can leave a message or can be transferred to a live operator

By default, the operator call handler allows callers to press * to reach the Sign-In conversation, or press # to reach the opening greeting call handler. Messages that are left in the operator call handler are sent to the mailbox for the operator user

Goodbye: This call handler plays a short goodbye message and then hangs up if there is no caller input.

By default, the goodbye call handler allows callers to press * to reach the Sign-In conversation, or press # to reach the opening greeting call handler. If you change the After Greeting action from Hang Up to Take Message, messages that are left in the goodbye call handler are sent to the Undeliverable Messages distribution list.

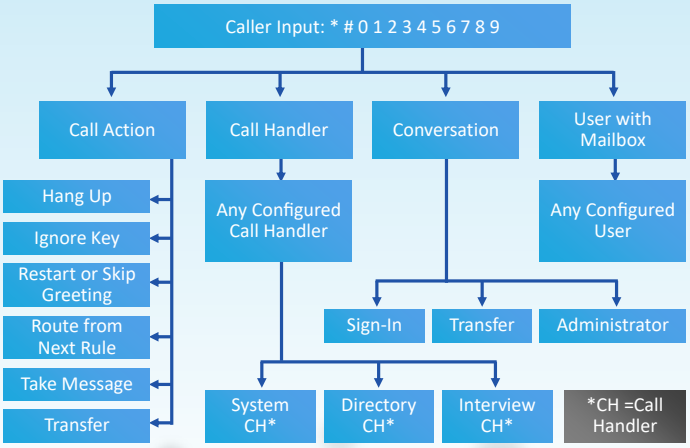
Each call handler provides a unique experience for the caller. All default call handlers can be modified, or new call handlers can be created to define the user experience. To better understand these call handlers, you need to explore the default call handlers and how they can be modified to meet the needs of each organization. Usually, these default call handlers are used and modified to provide access to users and resources.

Caller Input

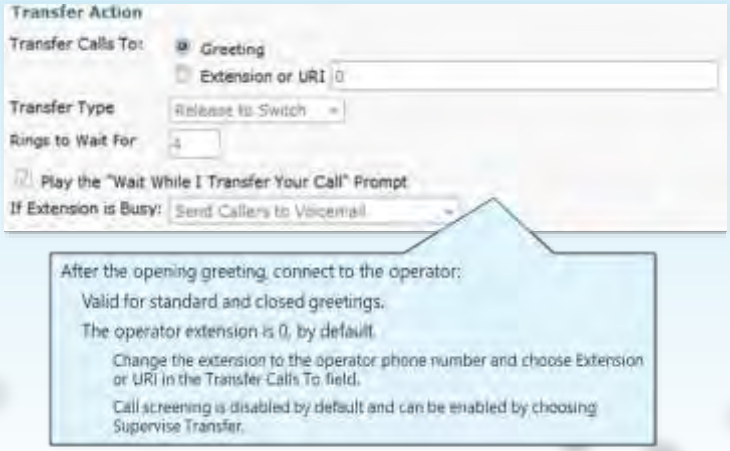
To define the action that Cisco Unity Connection takes in response to phone keys that callers press, choose from the options that are presented in the following figure. The caller needs to be informed of the selection options within the greeting.

In addition to choosing any configured call handler or choosing users with a mailbox, you can choose the following call actions:

- Hang Up
- Ignore Key
- Restart Greeting
- Route from Next Call Routing Rule
- Skip Greeting
- Take Message
- Transfer to Alternate Contact Number



Operator Call Handler



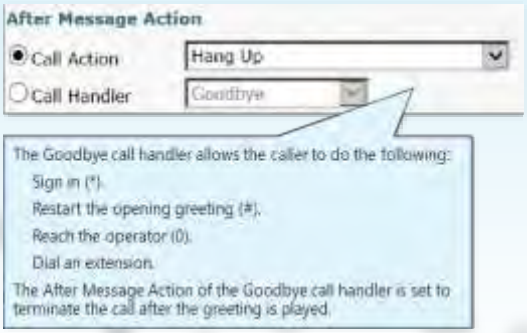
Operator Call Handler

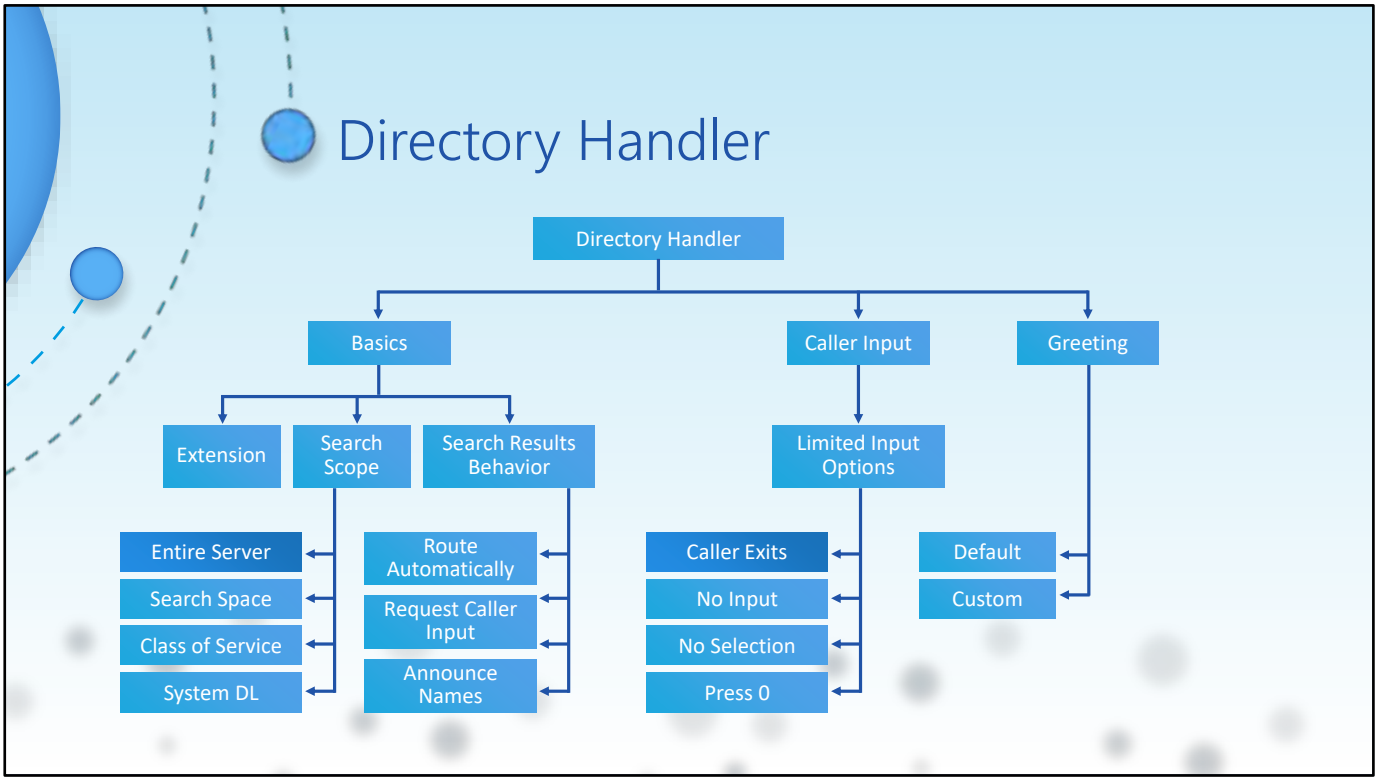
Operator Not Available

If the operator is unavailable, the caller can leave a message. The message recipient is the operator, which is a preconfigured user with a mailbox and the assigned extension 99990. To listen to the operator messages, call Cisco Unity Connection from any phone and press the Messages button or dial the voicemail pilot number. Press the asterisk or star key (*) to reach the sign-in menu, then enter the ID 99990 and the PIN. After the message is taken, the goodbye call handler is chosen

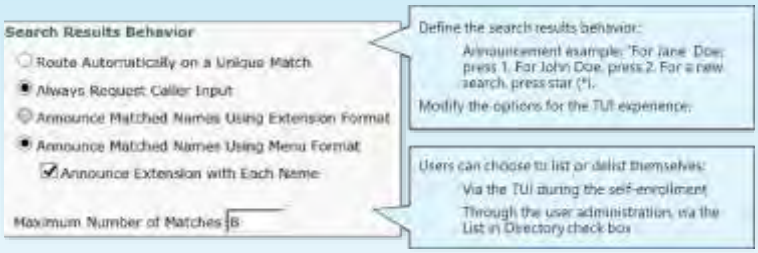
Goodbye Call Handler

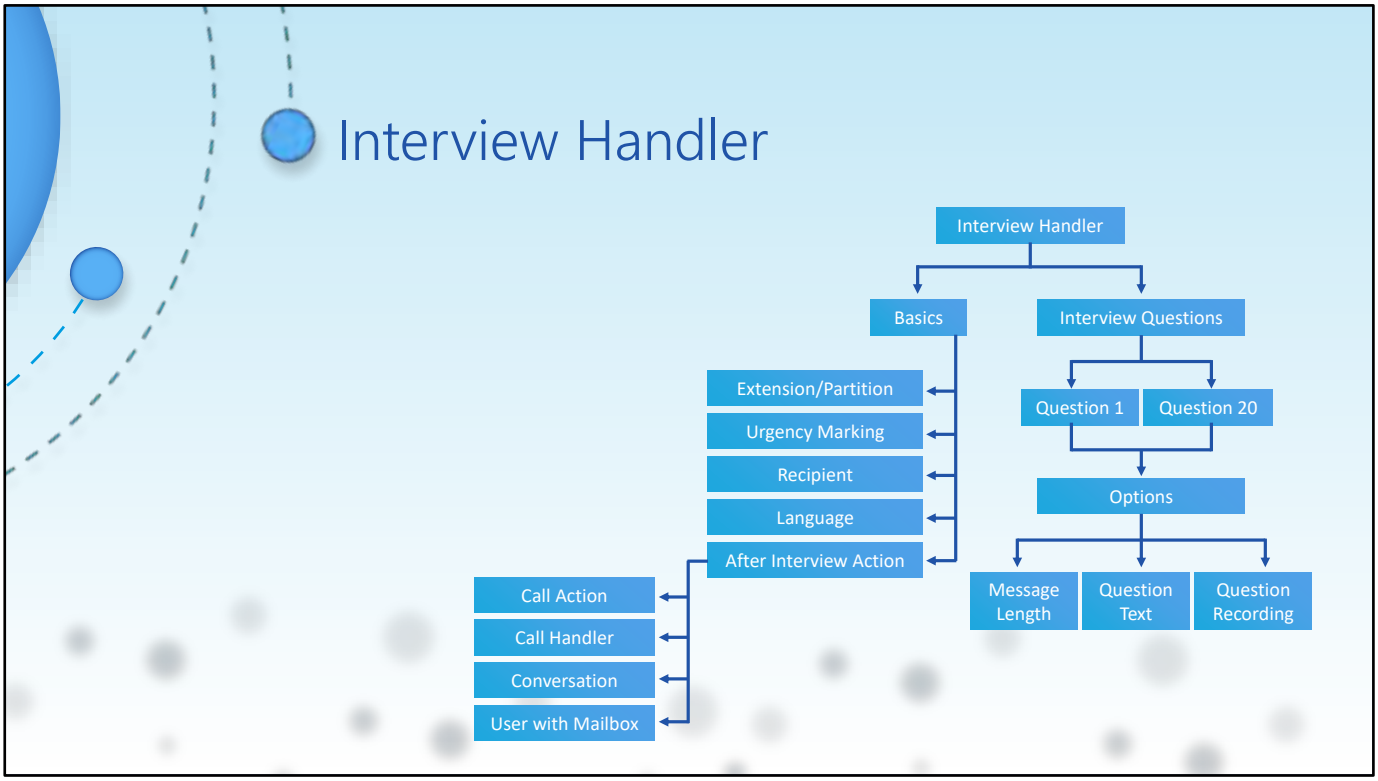
The goodbye call handler allows the caller to sign in, restart the opening greeting, reach the operator, or dial an extension. However, the goodbye call handler greeting only announces the option to dial an extension. By default, the other three options are not announced during the greeting. If the caller does not choose any option during that greeting (which is 5 seconds long), the call is terminated





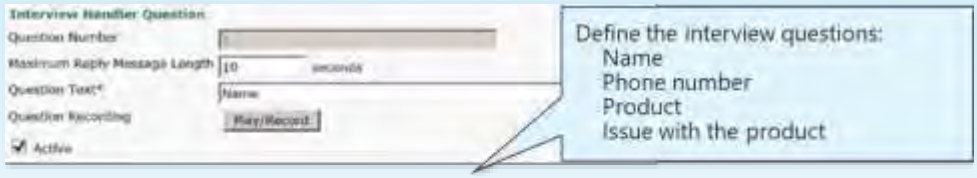
Search Results Behavior



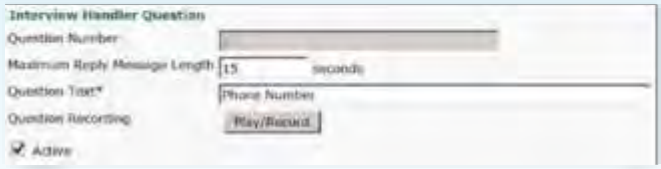


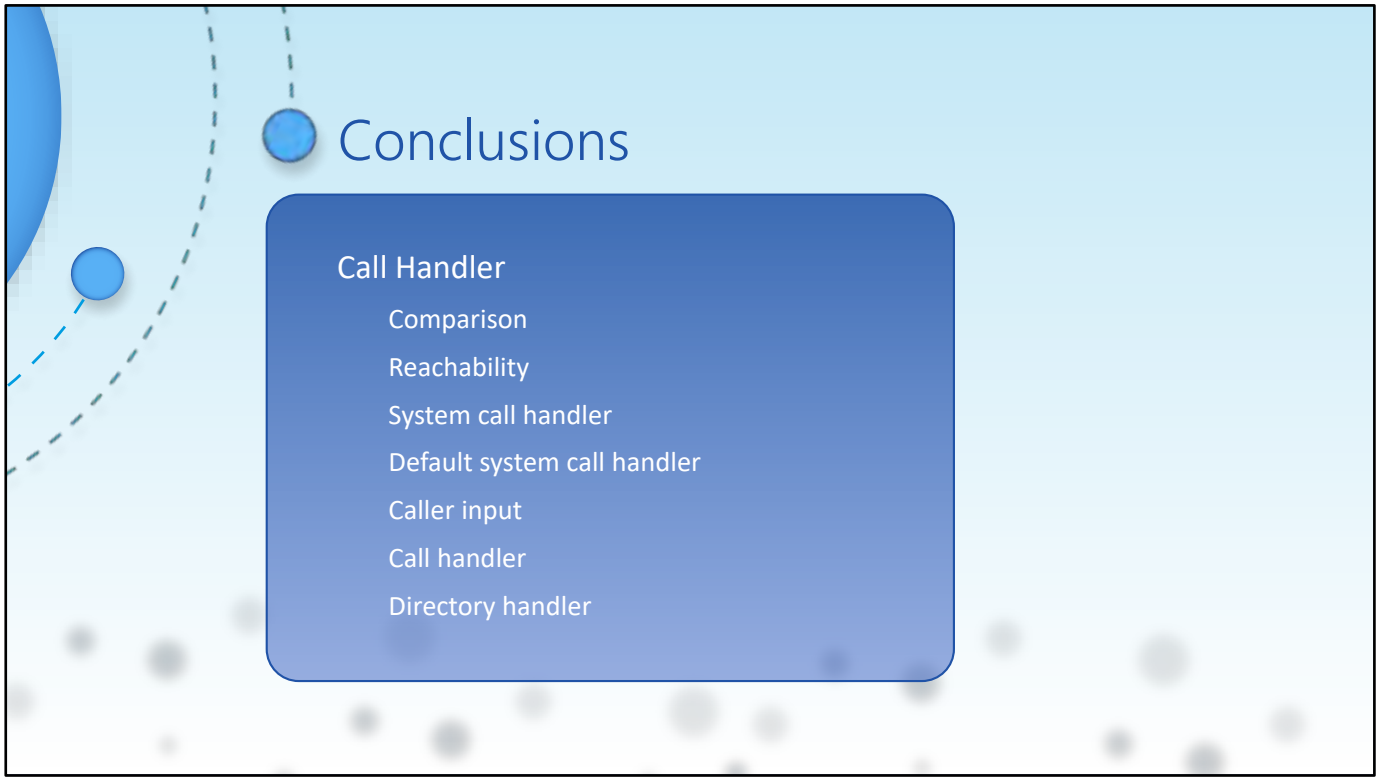
Product Line Use Case Example

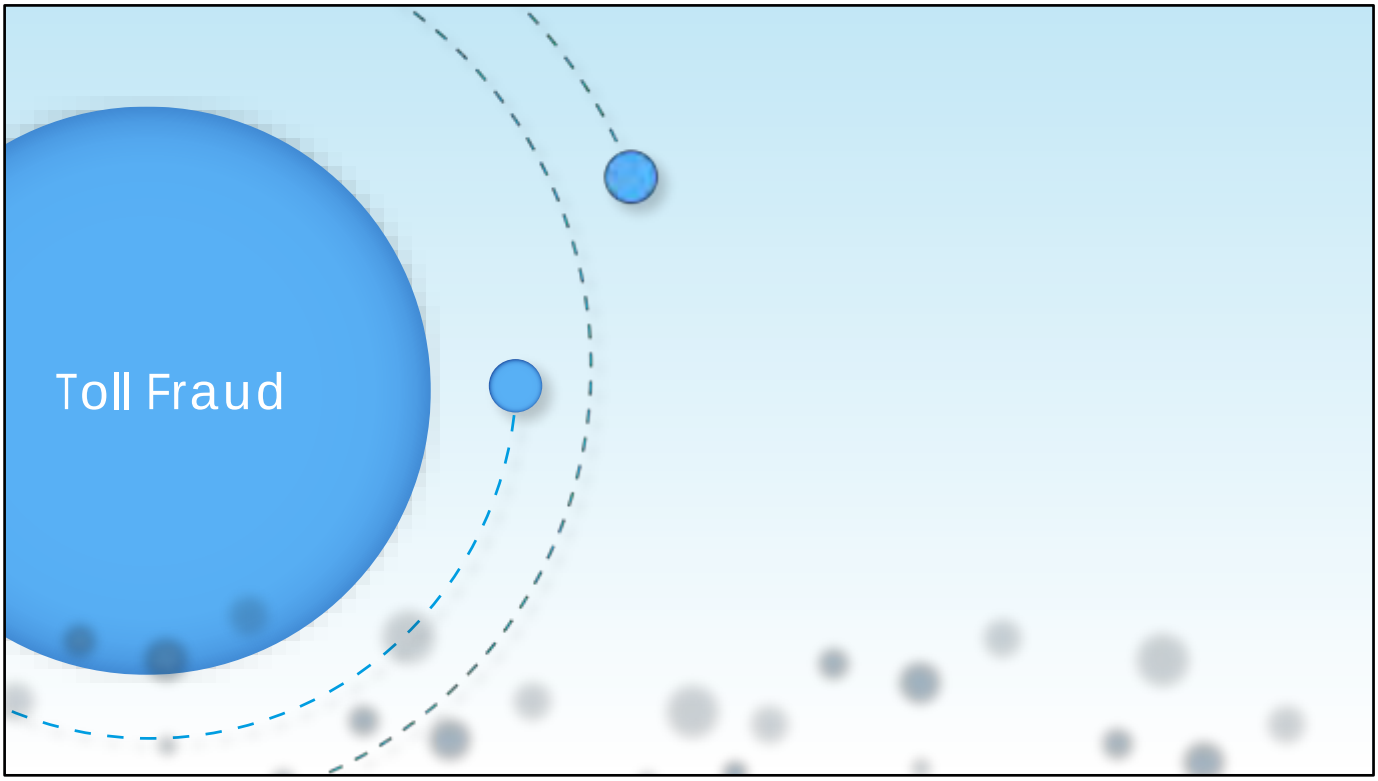
Question 1



Questions 2-20



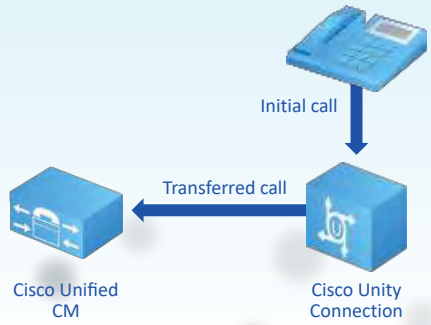




Toll Fraud

Call can be transferred by:

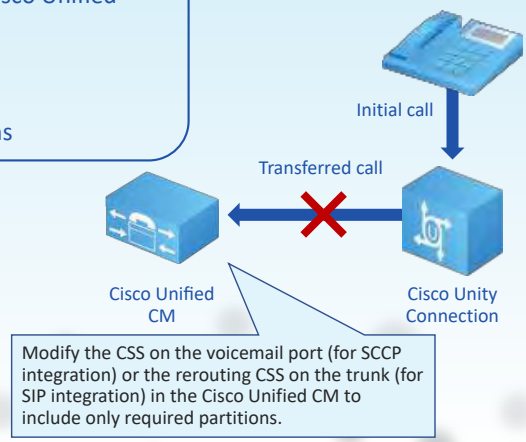
- Call action **Transfer to Alternate Contact Number** under **Caller Input**
- Dial the number if the **Allow Transfers to Numbers Not Associated with Users or Call Handlers** check box is checked on the Greeting page
- Conversation option after greeting:
  - **Caller System Transfer**
  - **User System Transfer**
- Dial extension while greeting is played
- Use the After Greeting action



Toll Fraud Prevention in Cisco Unity Connection

Set up restriction tables to control the following:

- Call transfer
- Recording and playback by phone from Cisco Unified Communications applications
- Delivering faxes
- Sending message notifications
- Creating user-defined alternate extensions



Toll Fraud Prevention in Cisco Unified Communications Manager

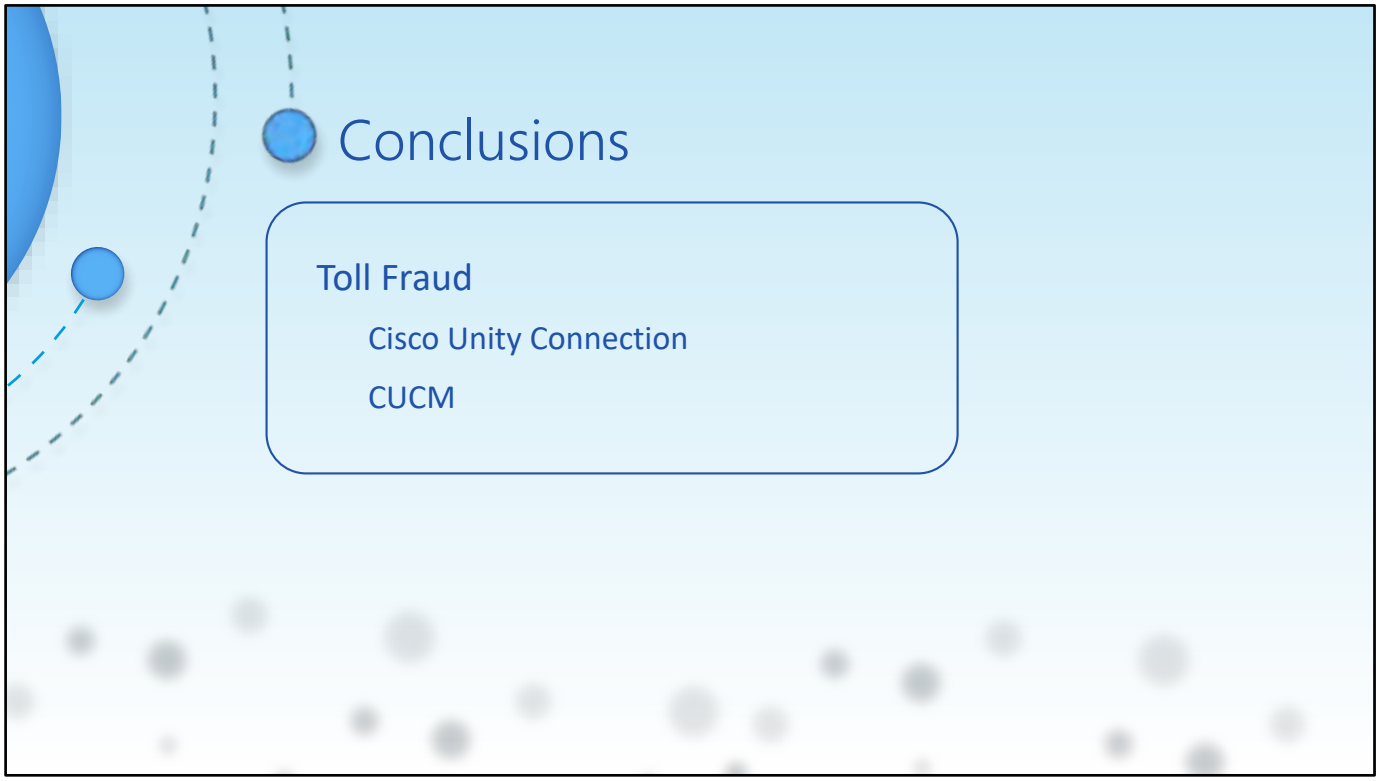
There are some integration requirements for transfers from Cisco Unity Connection to work:

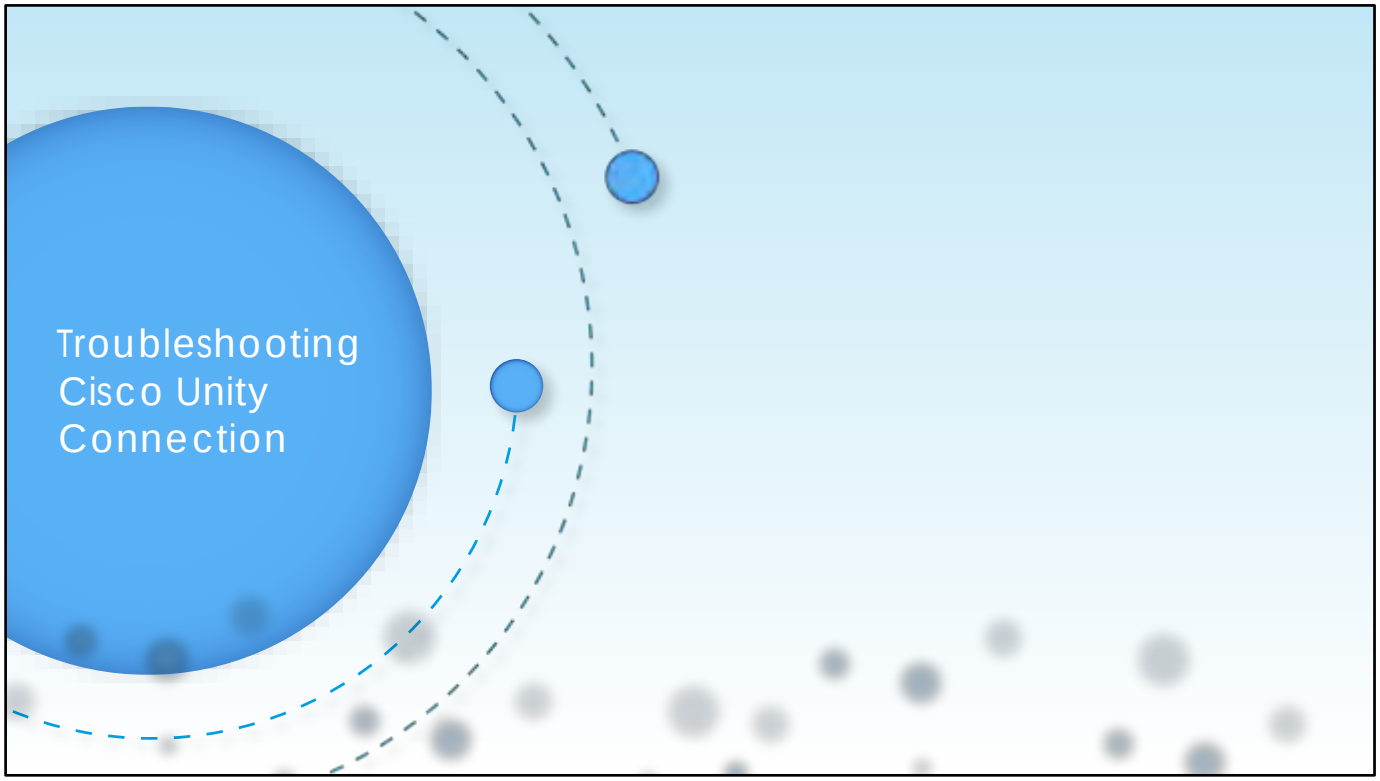
If the integration between Cisco Unified Communications Manager and Cisco Unity Connection is SCCP, the voicemail port CSS must have the partition of the route pattern to the PSTN number.

If the integration between Cisco Unified Communications Manager and Cisco Unity Connection is SIP, the SIP trunk rerouting CSS must have the partition of the route pattern to the PSTN number.

If the call is transferred via a CTI route pattern or translation pattern, the voicemail port or SIP trunk must have access to it and the CSS of CTI route pattern or translation pattern must have the partition of the route pattern to the PSTN number.

Therefore, to prevent toll fraud calls, you need to modify the CSS on the voicemail port or the rerouting CSS on the trunk in Cisco Unified Communications Manager to include only required partitions



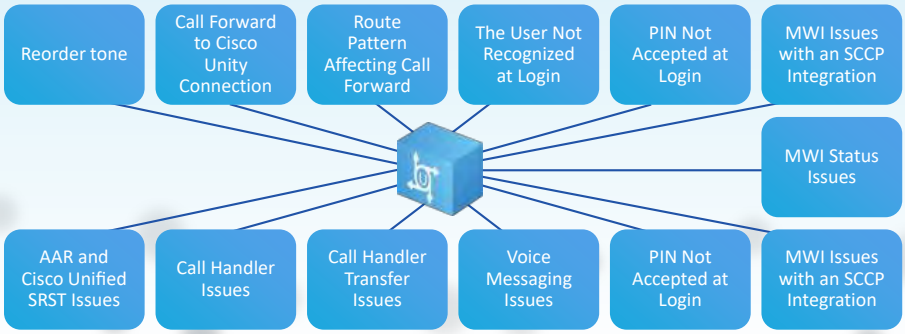


Overview

Sometimes you might encounter problems with Cisco Unity Connection, just like with any other system. To resolve the problem, you first have to identify the symptoms using proper troubleshooting tools. Then you can follow recommended troubleshooting procedures to quickly resolve all issues.

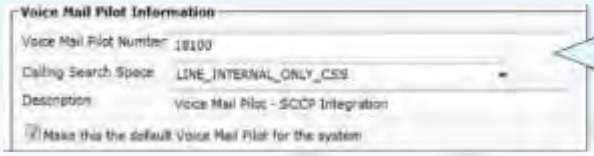
Overview

The following is a list of the most common Cisco Unity Connection errors. Some of these errors appear during configuration, some appear after weeks, and some appear from one day to the next.



Reorder Tone

IP phones need a CSS that is set to reach Cisco Unity Connection when the user manually dials the voicemail pilot number.



The Messages softkey also requires the CSS to be set on the IP phone to reach Cisco Unity Connection.

Call Forward to Cisco Unity Connection

Differentiate CFB, CFNA, CFNC, and CFUR*.

Enable Call Forward.

CFB = Call Forward Busy
CFNA = Call Forward No Answer
CFNC = Call Forward No Coverage
CFUR = Call Forward Unregistered

Call Forward to Cisco Unity Connection

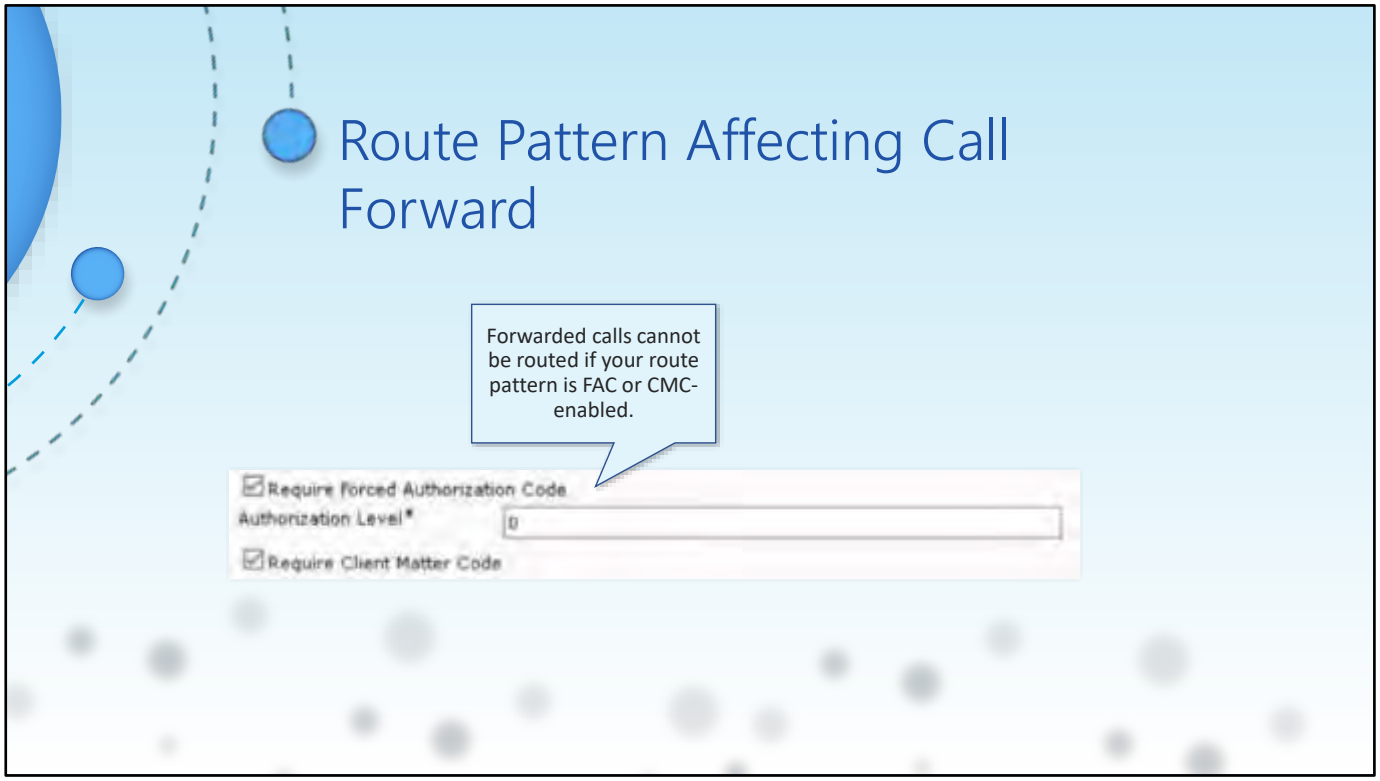
Route Pattern Affecting Call Forward

Route pattern collects only the 0 and one other digit

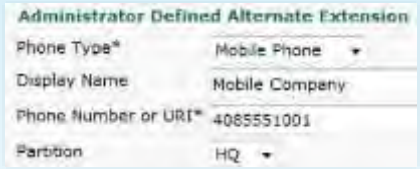
Longer number causes issues

To fix the issue, you need to create an extra route pattern just for Call Forward and without overlap ending enabled.

Route Pattern Affecting Call Forward



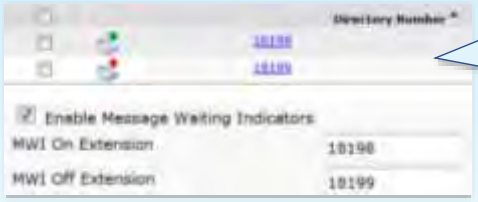
Login Not Working: The User Is Not Recognized



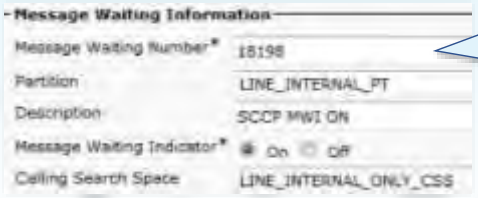
Alternate number is misconfigured or incorrect. Note that number normalization and globalization can modify the calling number. This issue can be detected by using the Cisco Unity Connection Port Monitor in the RTMT.

The voicemail mask can modify the calling number that is sent to Cisco Unity Connection.

MWI Issues with an SCCP Integration



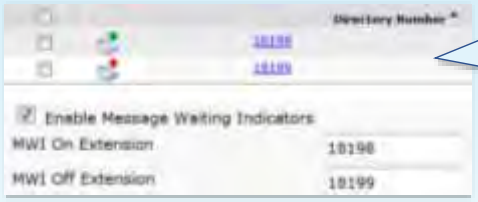
Verify that these numbers are also configured for MWI on and off in Cisco Unity Connection.



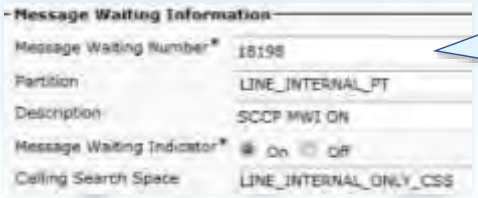
MWI numbers need a CSS.

CSS must be able to call the IP phone to turn the MWI on or off.

MWI Issues with an SCCP Integration



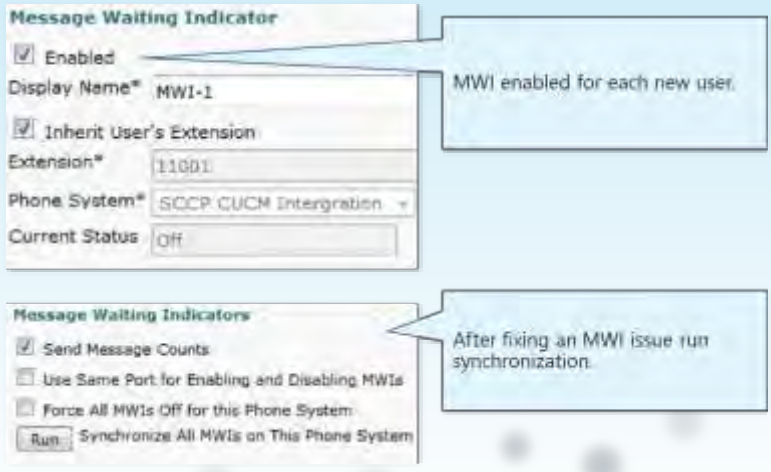
Verify that these numbers are also configured for MWI on and off in Cisco Unity Connection.



MWI numbers need a CSS.

CSS must be able to call the IP phone to turn the MWI on or off.

MWI Status

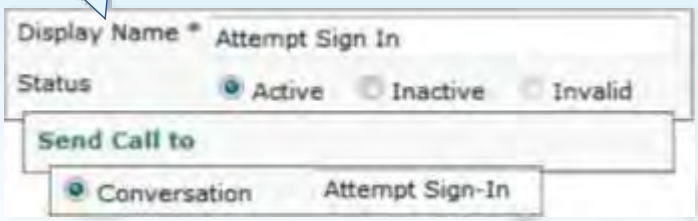


Wrong Greeting

Default rules:

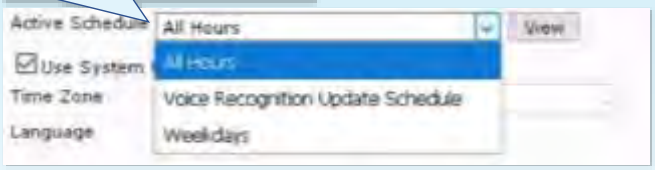
Attempt Sign In

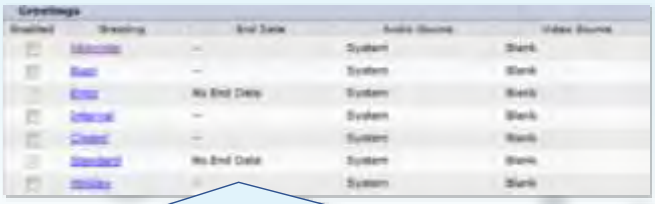
Switch Status to Inactive.



Time Schedule

By default, call handlers use All Hours and users use Weekdays.

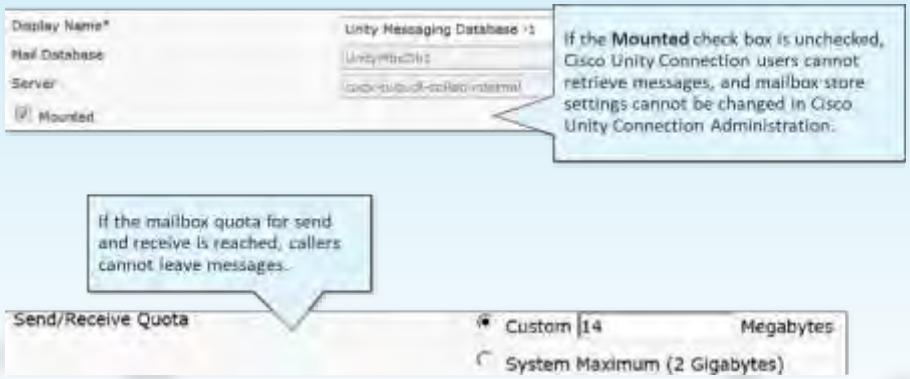




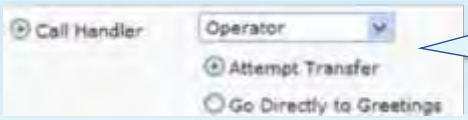
The closed greeting is not enabled by default; users have an All Hours schedule.

If no closed greeting is enabled, then the standard greeting is used.

Voice Messaging Issues



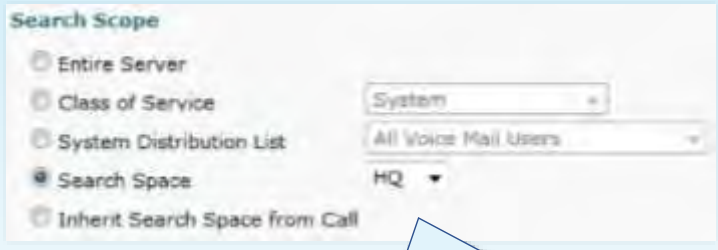
Call Handler Transfer Issues



When a call is transferred via the Call Handler you need to specify transfer destination.

When you use the Transfer to Alternate Contact Number option for Call Action, specify Transfer Type.

Call Handler Transfer Issues

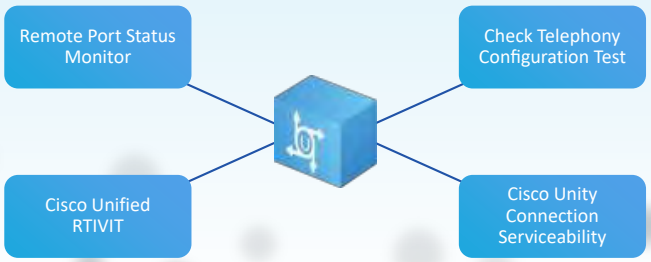


For directory handlers, most issues occur in the Search Scope settings.

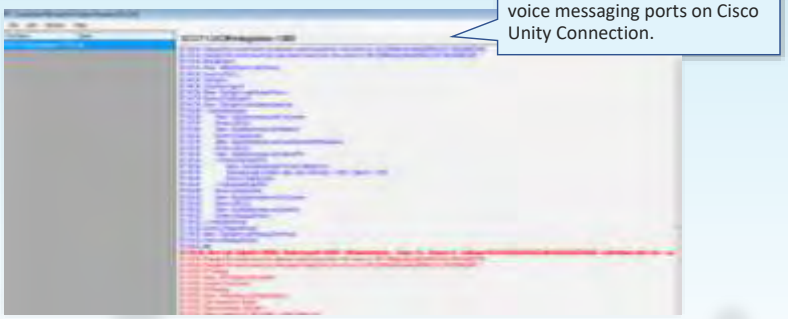
Interview handlers need defined questions. Without a recorded question, the call handler will not play anything.

Integration Troubleshooting Tools

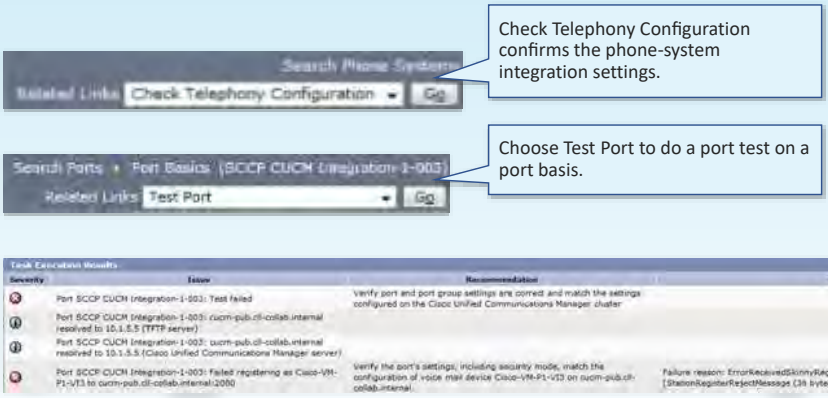
Cisco Unity Connection has plenty of troubleshooting tools that may help you fix any problems related to integration with the phone system. The following is a list of these tools



Remote Port Status Monitor



Check Telephony Configuration Test



Check Telephony Configuration Test

In Cisco Unified CM, go to the Cisco Voice Mail Port overview and verify that the ports show as registered.

To verify that the ports and the integration are working on both systems, press the Messages button on any phone using the default voicemail profile. If no users are configured, then the standard opening greeting is played.

Cisco Unity Connection Serviceability

Cisco Unified Serviceability, a web-based troubleshooting tool for Cisco Unity Connection, provides the following functionality:

- Alarms and events are saved for troubleshooting and providing alarm message definitions.
- Trace information is saved to various log files for troubleshooting.
- You can turn on, turn off, and view Feature Services under the Service Activation window.
- An interface is provided for starting and stopping features and network services.
- Daily reports are generated and archived; for example, the alert summary or server statistics reports
- The number of threads and processes in the system are monitored; cache is used to enhance performance

Depending on the service and component involved, you may complete serviceability-related tasks in both Cisco Unified Serviceability and Cisco Unity Connection Serviceability. For example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem

Cisco Unified RTMT

Cisco Unified RTMT, which runs as a client-side application, uses HTTPS and TCP to monitor system performance, device status, device discovery, and CTI applications for Cisco Unity Connection. Cisco Unified RTMT can connect directly to devices via HTTPS to troubleshoot system problems. Cisco Unified RTMT can also monitor the voice messaging ports on Cisco Unity Connection.

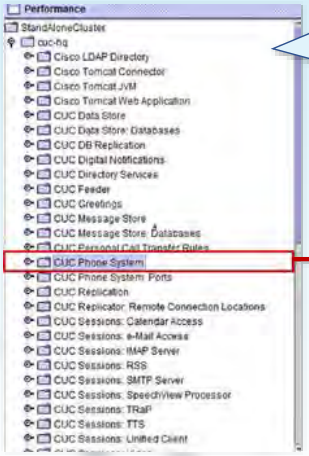
Runs as a client-side application and uses HTTPS, TCP, and CTI.

Cisco Unified Real-Time Monitoring Tool

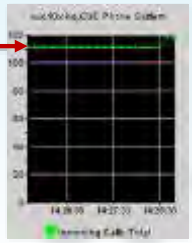
Cisco Unity Connection allows monitoring in real time:

- Via Cisco Unified RTMT: Download the plug-in for installation.
- System tab allows monitoring of the CPU, memory, and so on; also use performance counters and alerts.
- Launch the Port Monitor via the Unity Connection tab

Cisco Unity Connection Performance Counters

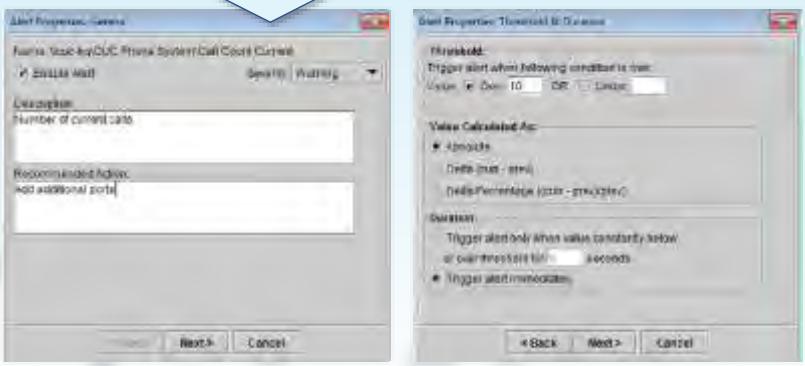


To monitor Cisco Unity Connection in detail, use performance counters. Each menu has many performance counters that can be added to the performance pane.



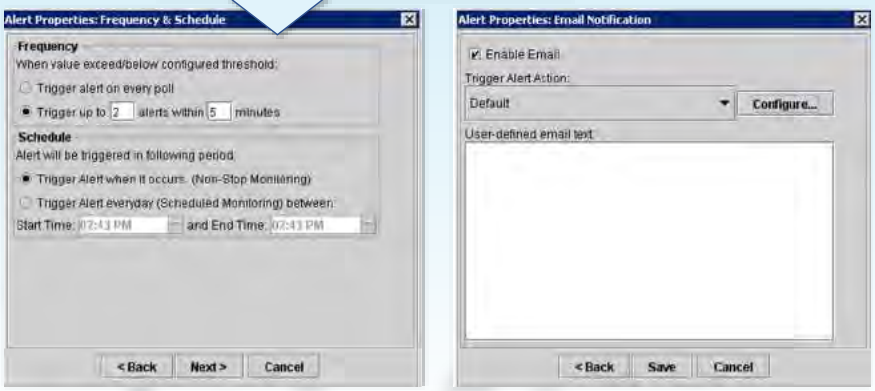
Alert Properties

To be notified if thresholds are reached, specify an alert.
Right-click the performance counter and choose Alert Properties.



Alert Properties

Specify the frequency and schedule.
Enable email and set the alert action.



Conclusions

Troubleshooting overview

- Common errors
- Reorder tone
- Call forwarding
- Route patterns
- MWI
- Greetings, Scheduling, and Messaging
- Call handler
- Troubleshooting tools
- Cisco unity
- Alerts