

# What You Make Possible



# Unified Communications and Directory Integrations

BRKUCC-2664

# Agenda

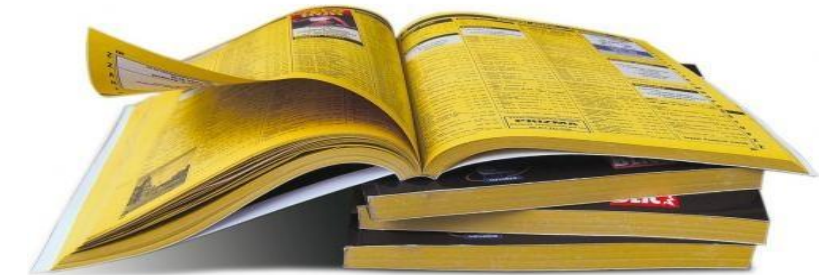
- Today's challenges for directories and Authentication & Authorisation Services
- What is UDS?
- How Cisco Applications use directory services
- OpenAM and how to support SSO across different domains
  - Rely on Microsoft Kerberos implementation and use SPN
  - Create multiple Kerberos sync agreements from OpenAM with the KDC in each domain
- A broader view on Authorisation and Authentication services
- Key Takeaways and Q&A

# Today's Challenges for Directories and Authentication and Authorisation Services

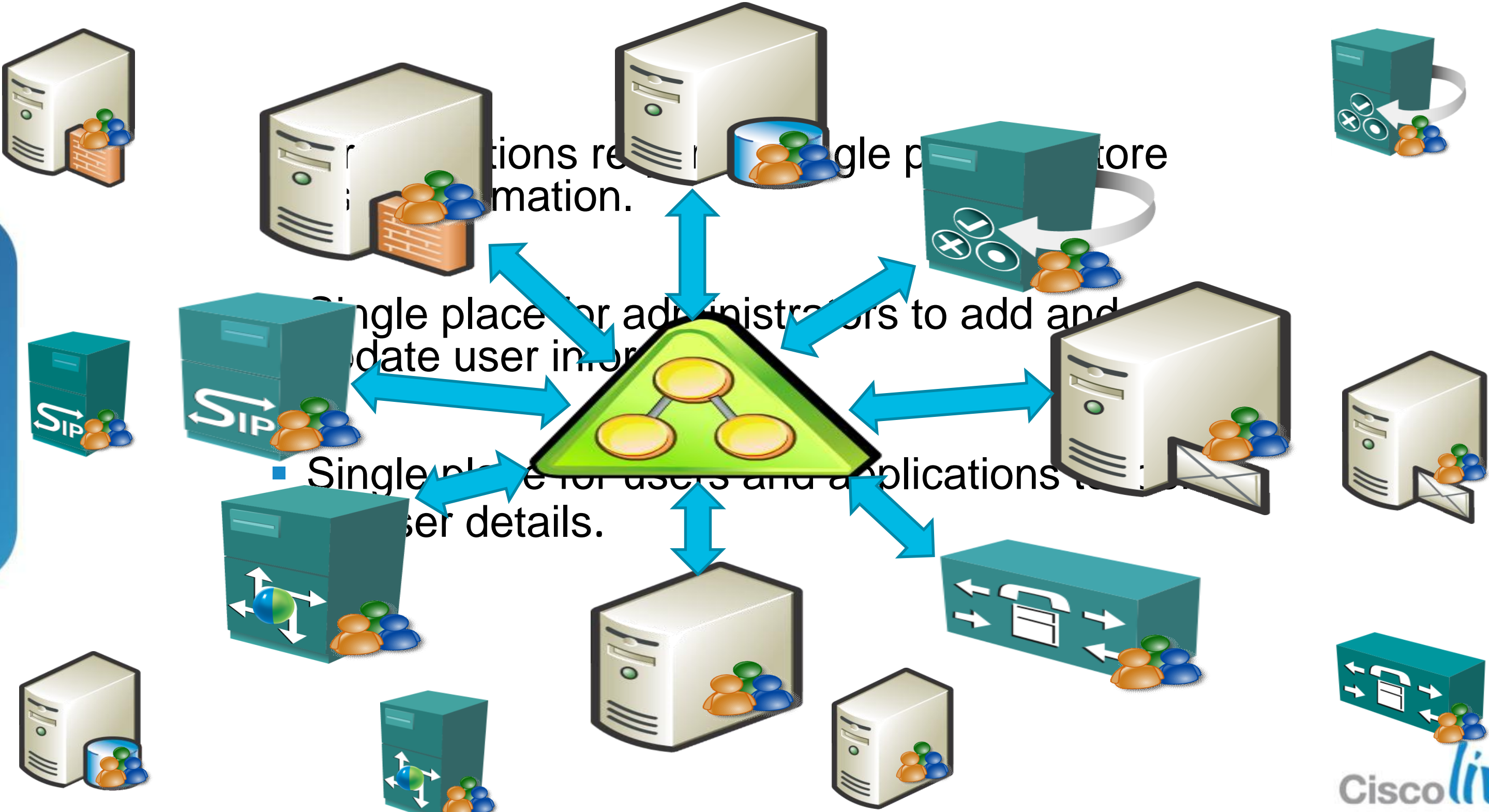


# What is a User Directory?

- A directory service is a publicly available database of structured information.
- The most common example of a directory service is your local White Pages - it contains names, addresses, etc.
- All information indexed for easy browsing and searching.
- The service can be categorised as 'write-once-read-many-times'.



# Where to Store the User Information?

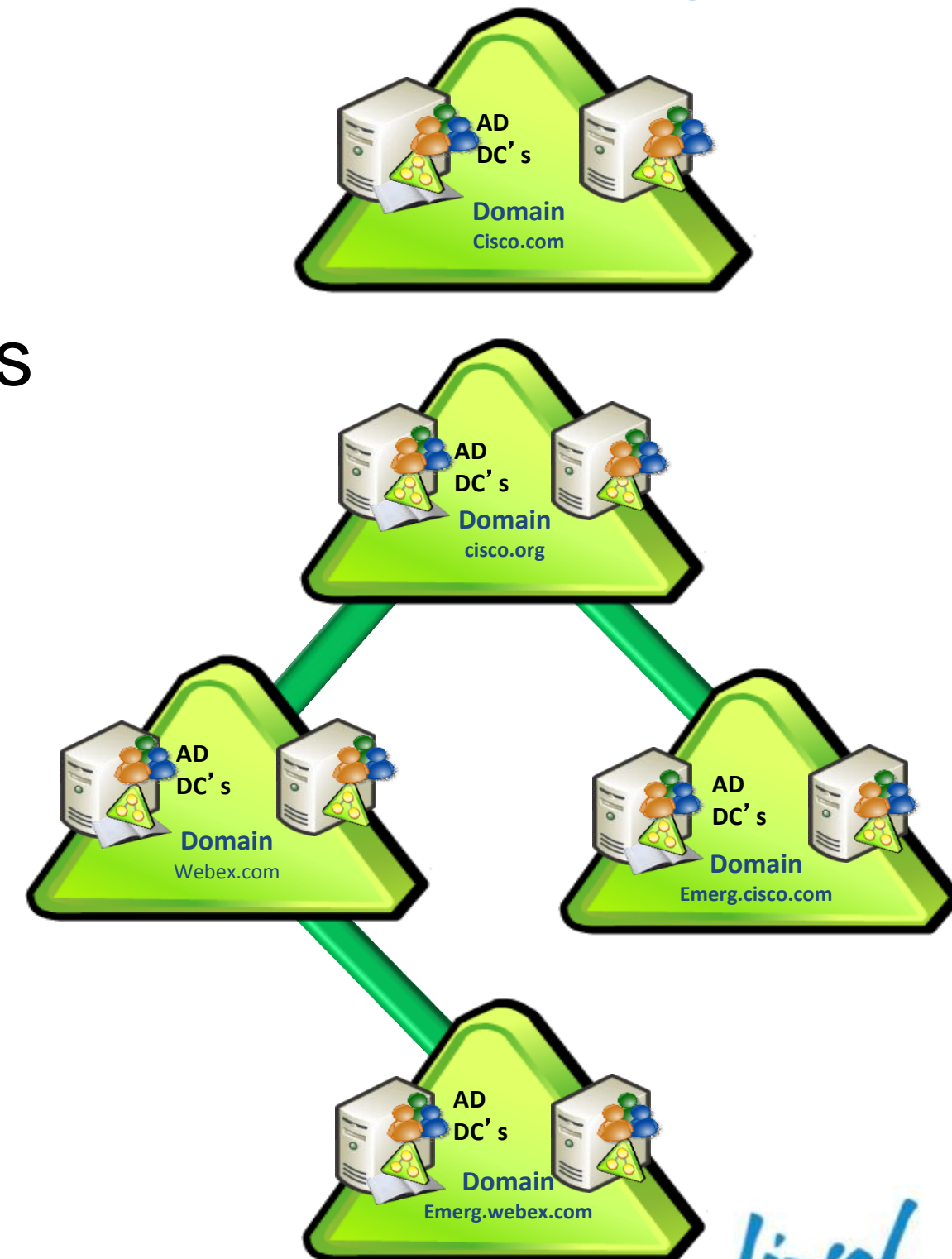


# What do we See in Organisations Today?

- Almost all the organisations already have an Active directory infrastructure.
- Organisations consolidate user passwords in AD, but they don't fully use it as a user directory source for other applications.

**In the rest of the presentation we are going to cover different architectures to simplify the complexity of AD deployments**

**Check Appendix A for the Basic Concepts of Active Directory**

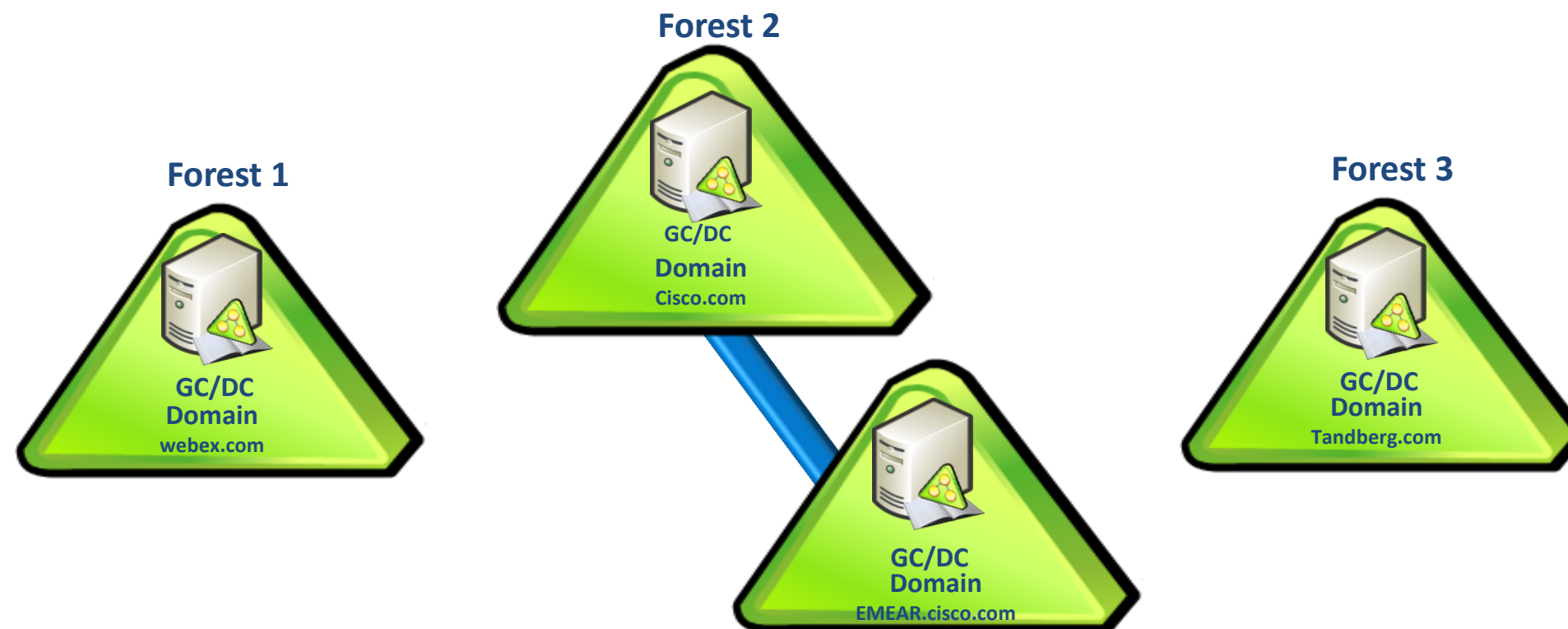


Cisco live!

# But Sometimes it Gets Very Complicated

...

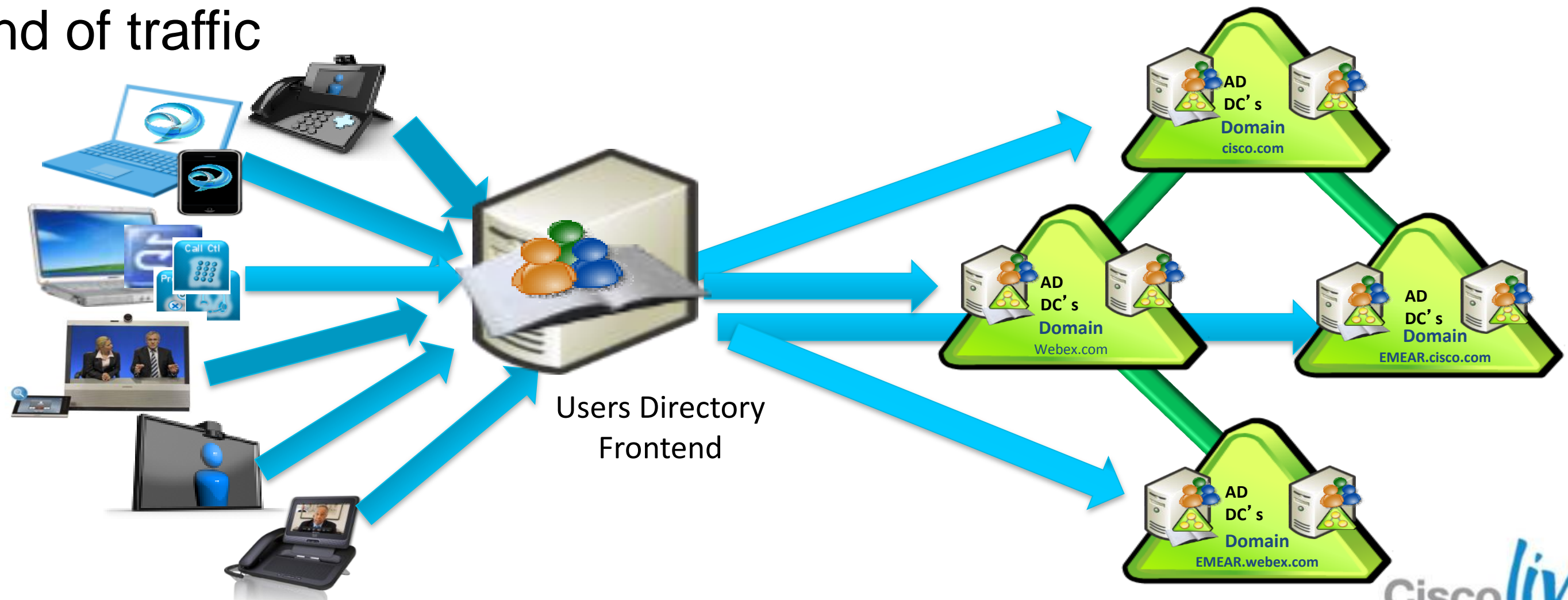
Complex AD deployments that aren't prepared to consolidate user information in a single point of contact





# Applications are Becoming More Dependent on User Directories

We start to have more and more applications that need to consult the LDAP database in every task that they execute... That is **too** heavy for the AD DC's that aren't designed for that kind of traffic



# Why Identity Matters

## Improve Adoption

- Enable Eagle Vision
- Make it easy to integrate with enterprise identity customers with industry standards and tools
- Common Identity facilitates integration between products reduces onboarding and training time for new products

## Reduce Cost

- Gartner estimates 20-50% of support costs related to password management
- Cisco IT estimates \$250/user/year cost of password management
- Build features not security

## Meet Security & Compliance Requirements

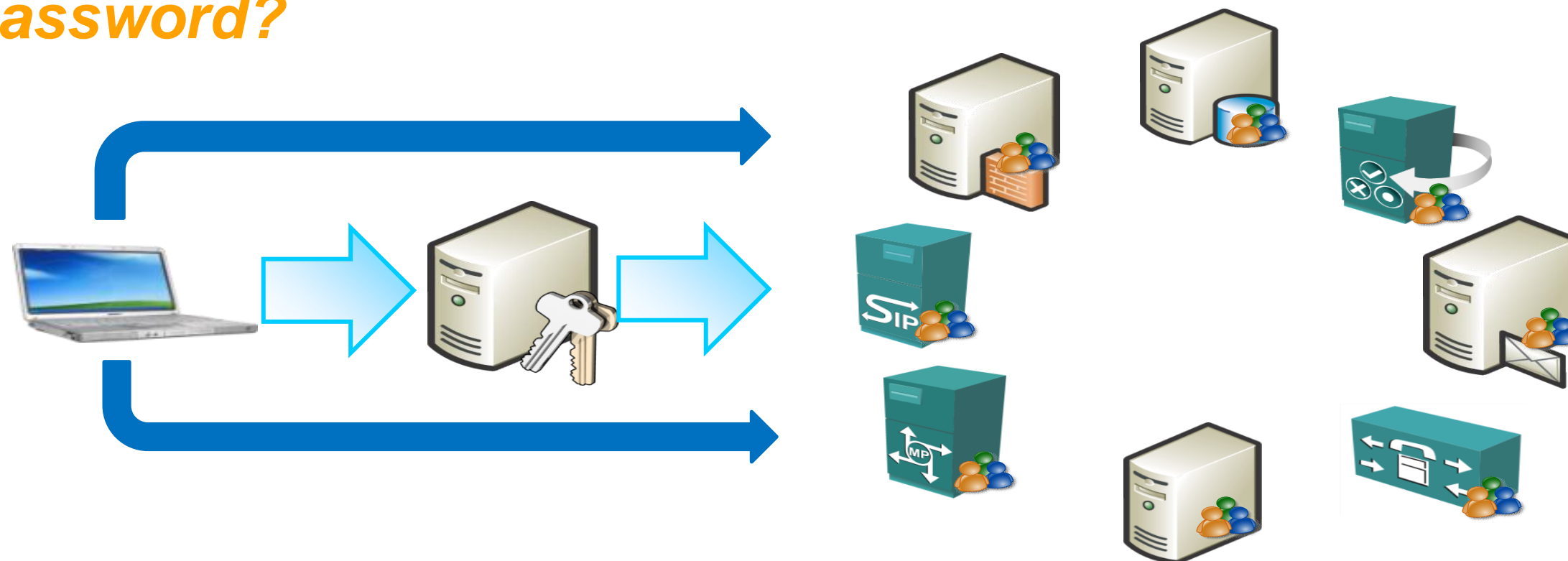
- Increasing threat vectors for enterprise identities
- Gartner Predicts: “By 2016, 40% of enterprises will make proof of independent security testing a precondition for using any type of cloud service.”

# Users Want to Provide Authentication Only Once

With so many systems and applications that need user directory information and authentication..... Users are complaining more and more every day...

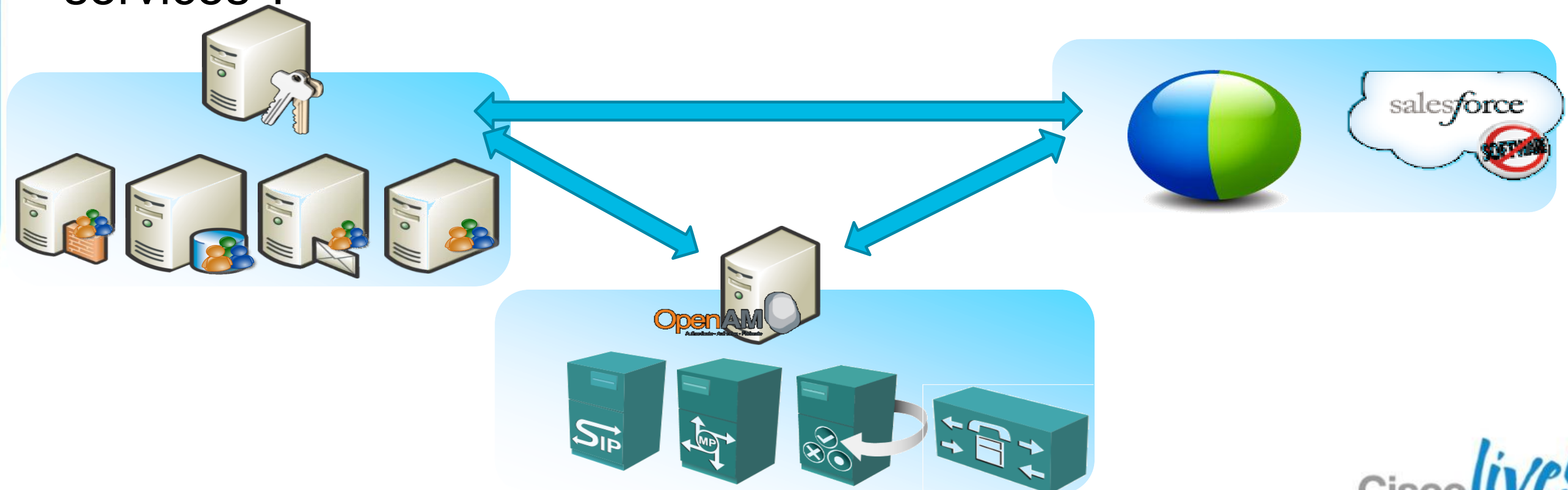
*Why should I have to provide credentials in every system that I use?*

*Why do I need to update all the applications when I change my password?*



# Additional Authentication Challenges

- What to do when the organisation already has an Identity and Access Management System ?
- How to bring Single Sign-On and user information to the cloud services ?

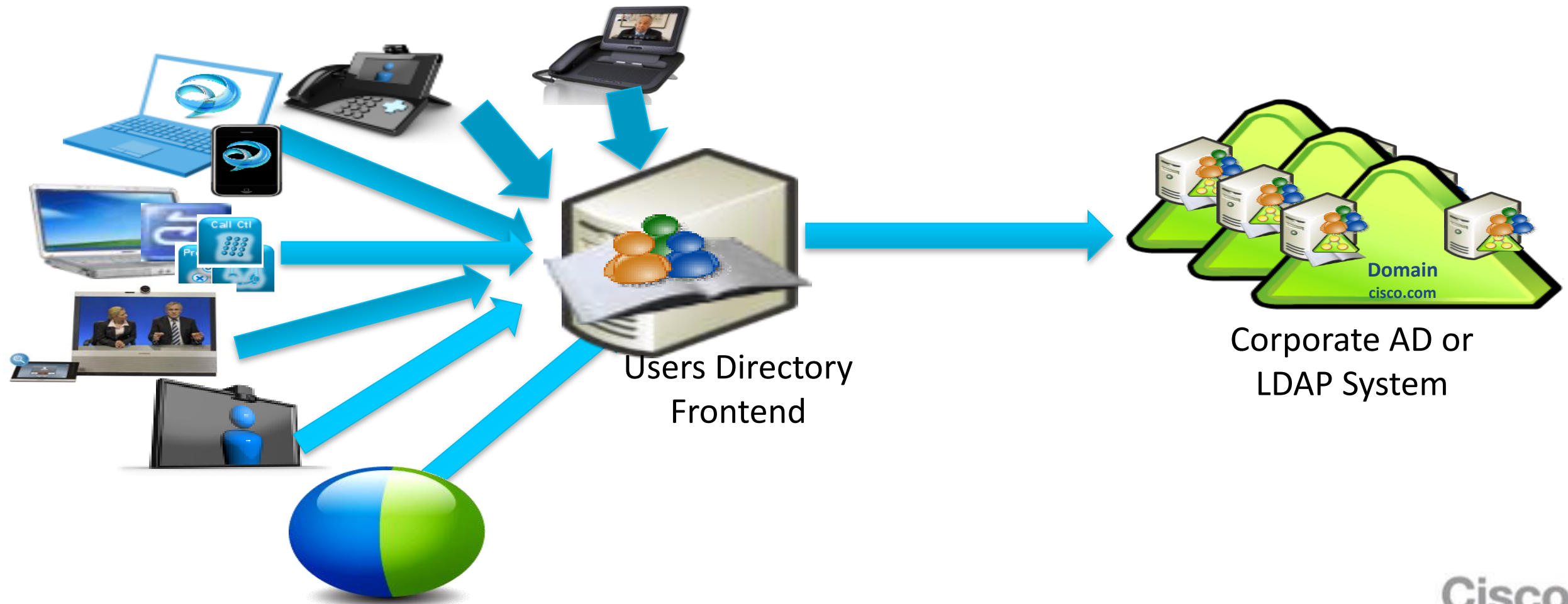


# What is UDS?



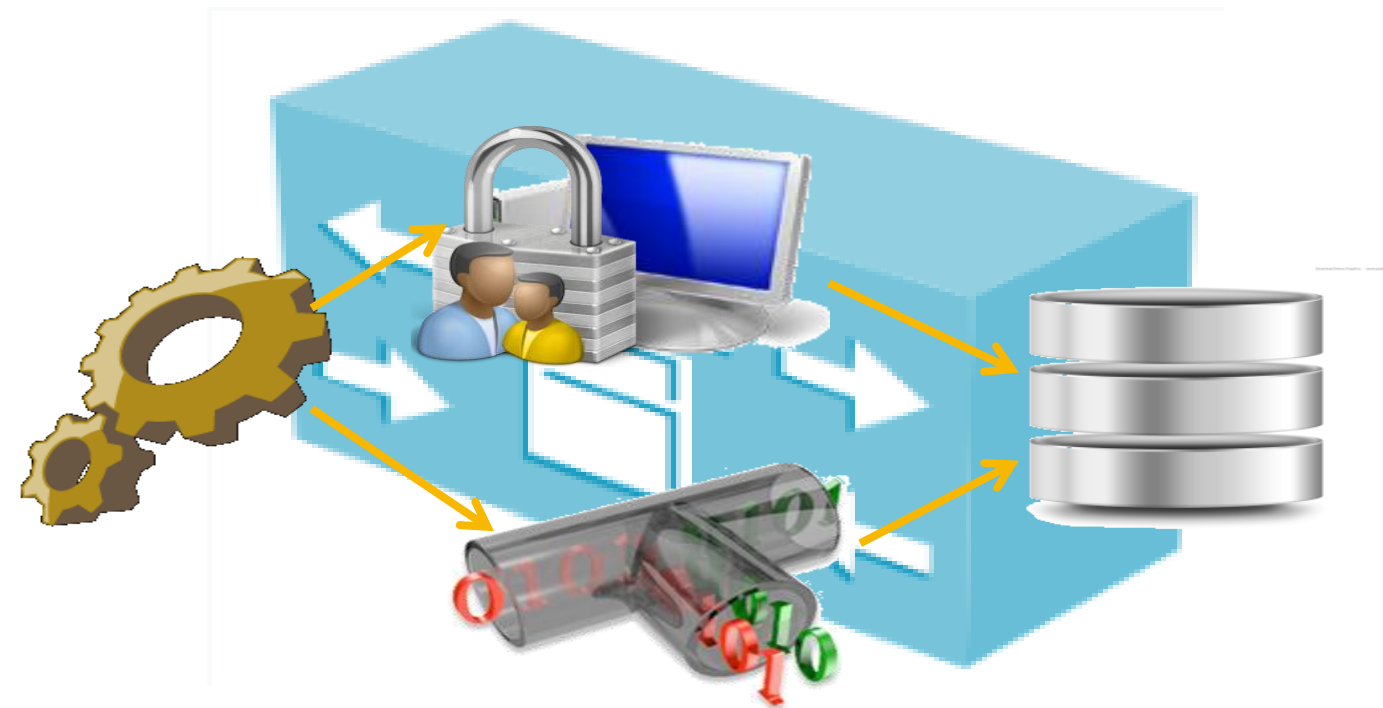
# User Directory Requests

We start to have more and more applications that need to consult the LDAP database in every task that they execute... That is too heavy for the AD DC's that aren't designed for that kind of traffic .....and too even heavy even for an LDAP System.



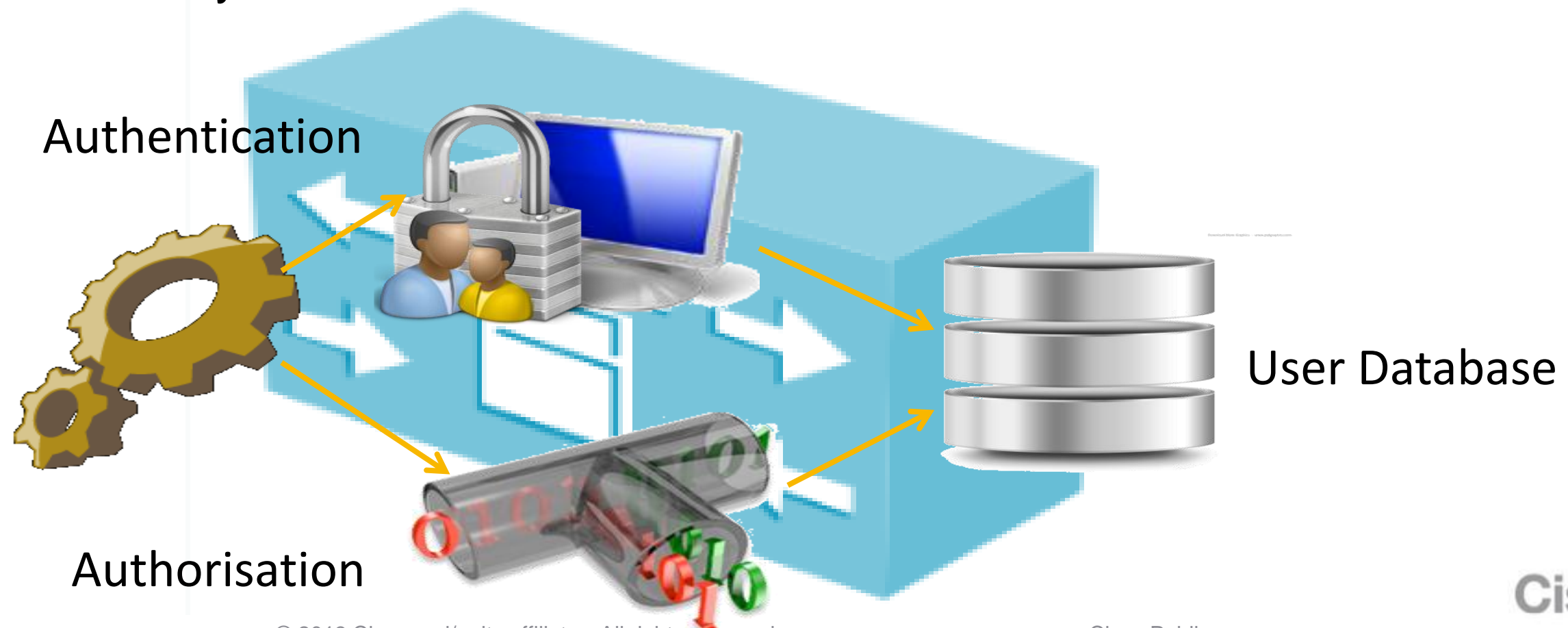
# What is User Data Service?

- User Data Service is a new Cisco web service running on each Unified CM Subscriber (enabled by default) which facilitates the exchange of User-based information (e.g. Search and Single Sign On) for our clients.



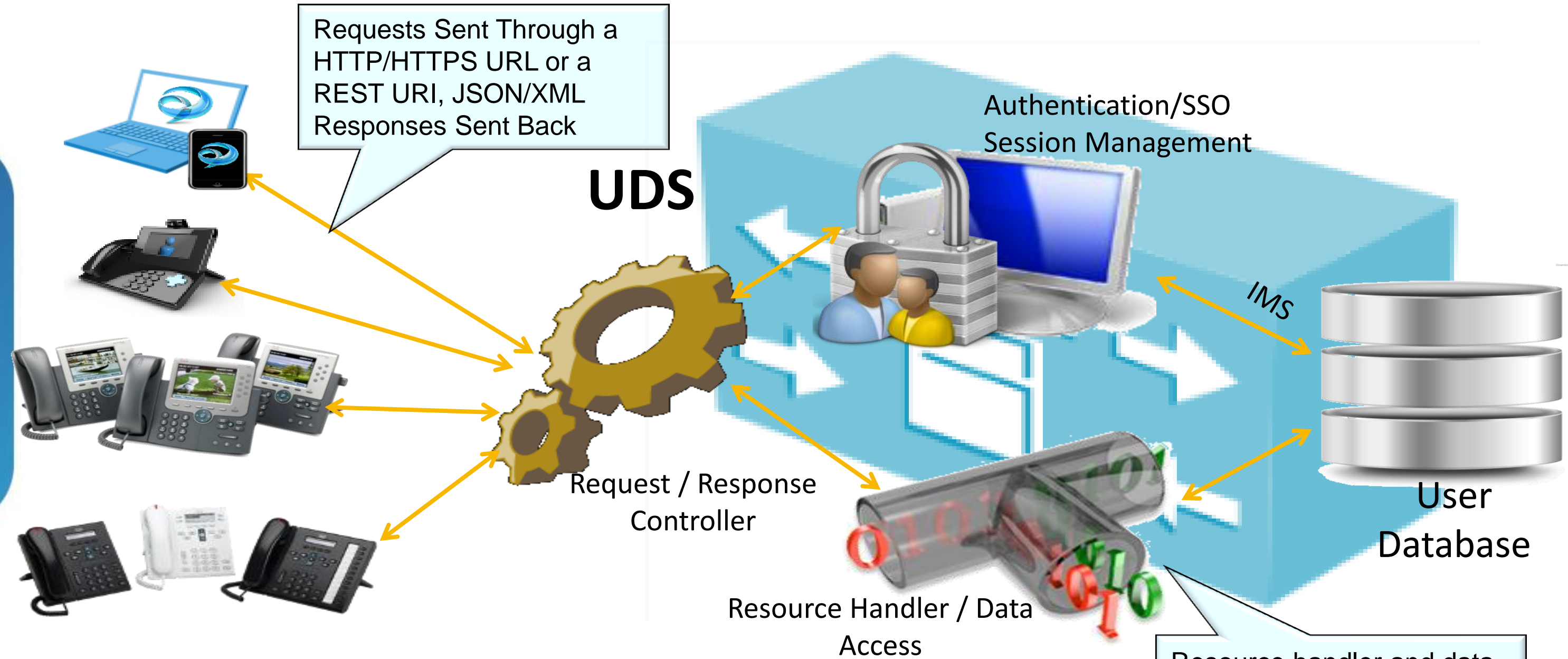
# UDS Components

- Authentication
  - SSO (Bypass Authentication with Assumption Policy Agent Intercepts HTTPS Request)
  - Basic Authentication vs. IMS
- Authorisation
  - User Can Only Access His/Her Own Data with Userid Included in URL.





# UDS Architecture



Requests Sent Through a HTTP/HTTPS URL or a REST URI, JSON/XML Responses Sent Back

**UDS**

Authentication/SSO Session Management

Request / Response Controller

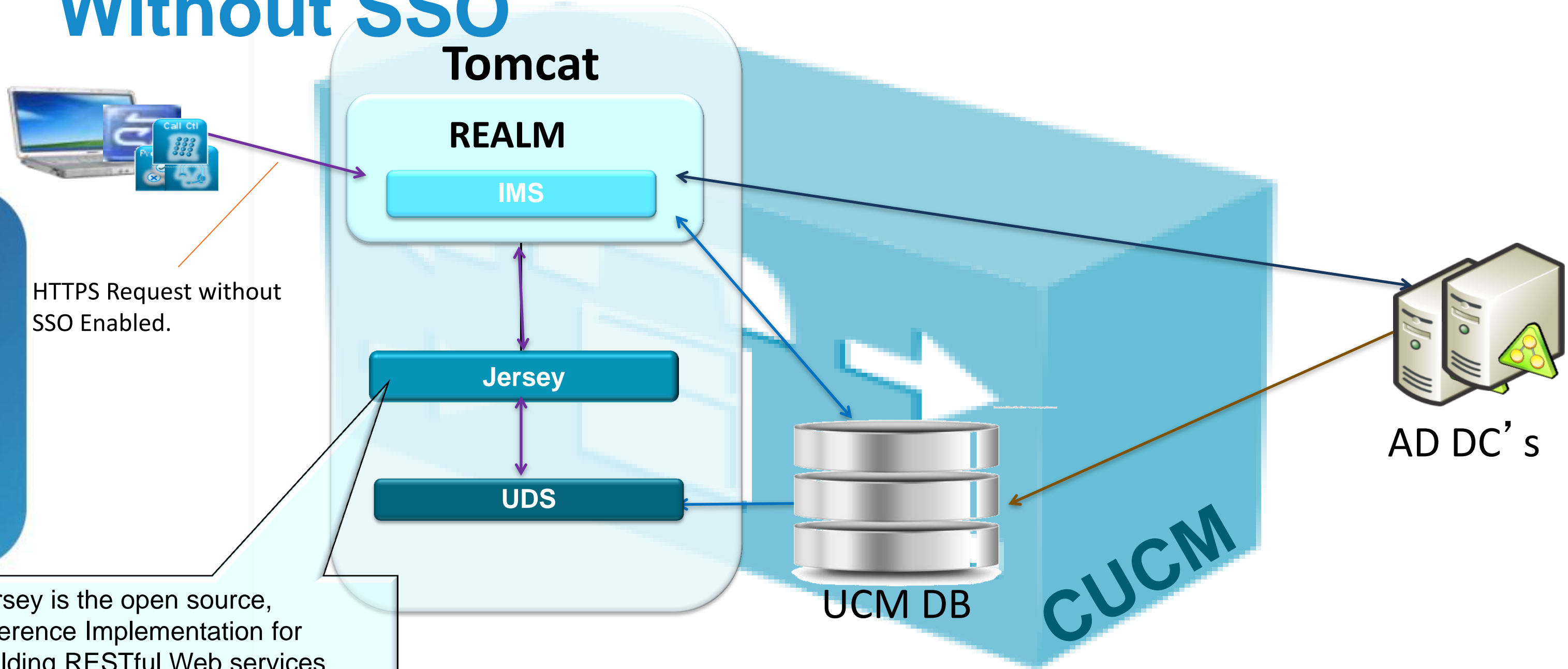
Resource Handler / Data Access

IMS

User Database

Resource handler and data access will be generated during build time based on the resource definition.

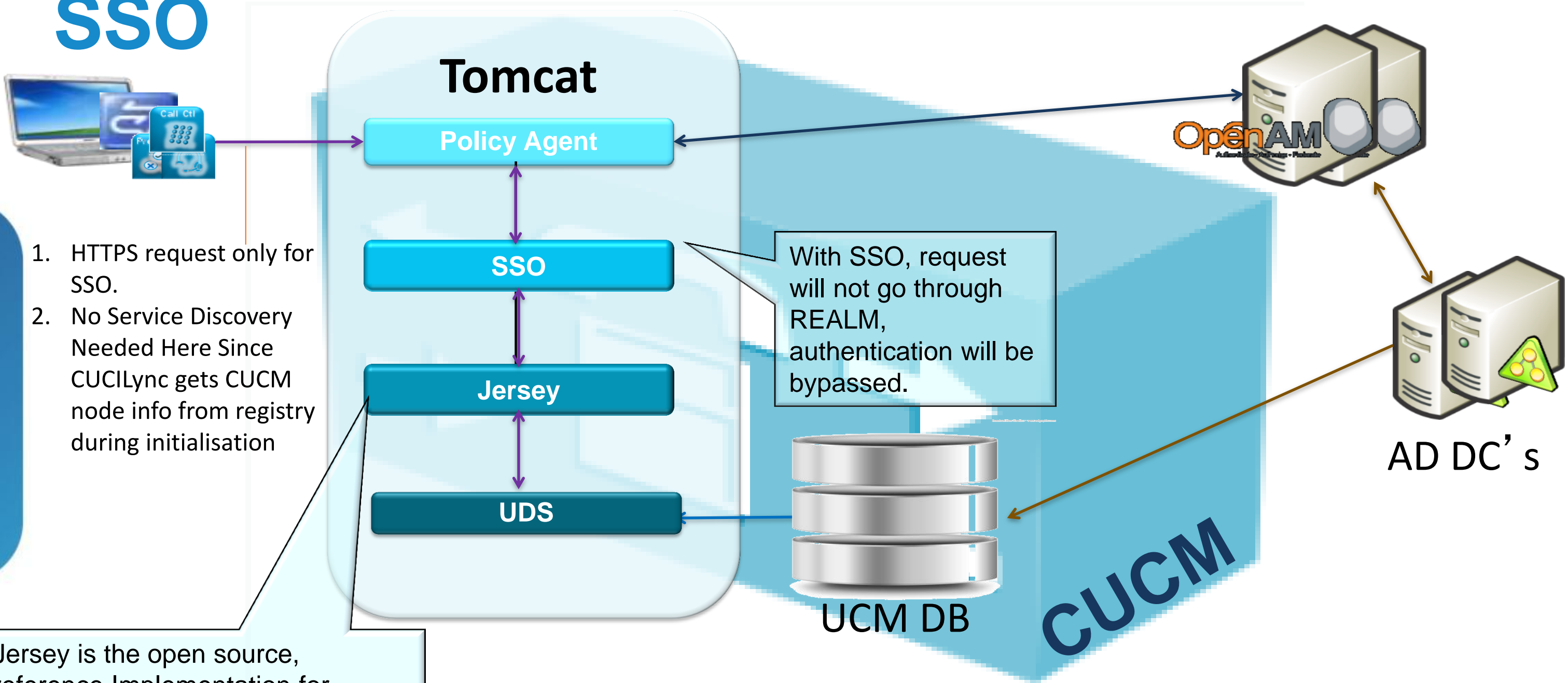
# Authentication Components for UDS Without SSO



HTTPS Request without SSO Enabled.

Jersey is the open source, reference Implementation for building RESTful Web services <http://jersey.java.net/>

# Authentication Components for UDS with SSO



1. HTTPS request only for SSO.
2. No Service Discovery Needed Here Since CUCILync gets CUCM node info from registry during initialisation

With SSO, request will not go through REALM, authentication will be bypassed.

Jersey is the open source, reference Implementation for building RESTful Web services <http://jersey.java.net/>

# Directory Structure for large Organisations

- Organisations with multiple clusters need to have one addressable LDAP entity/structure per cluster (OU, Domain, AD Forest), that means that each cluster has its own user information.
- User information from cluster to cluster is different, this is a requirement for features like Cross Cluster Extension Mobility.



# Cluster and Service Discovery

- Home cluster discovery is implemented using UDS (User Discovery Service) which allows the Jabber clients to locate their home cluster and configuration storage.
- A global instance of UDS finds the home cluster and the home cluster UDS finds the TFTP-served config file.
- Service discovery is the process whereby the 9.0 client retrieves the config file from the home cluster TFTP server, registers with the home cluster, and connects to all UC services configured for this user

Digest Credentials

Confirm Digest Credentials

---

**Service Settings**

Home Cluster

License User for Unified CM IM and Presence (Configure IM and Presence)

UC Service Profile

---

**Device Information**

https://sw016b-102/ccadmin/serviceProfileDetail.do?setToken=05k...

### Service Profile

Status: Ready

Name\*

Description

Make this the default service profile for the system

---

**Voicemail Profile**

Primary

Secondary

Tertiary

Credentials source for voicemail service\*

---

**MailStore Profile**

Primary

Secondary

Tertiary

Inbox Folder\*

Trash Folder\*

Polling Interval (in seconds)\*

Allow dual folder mode

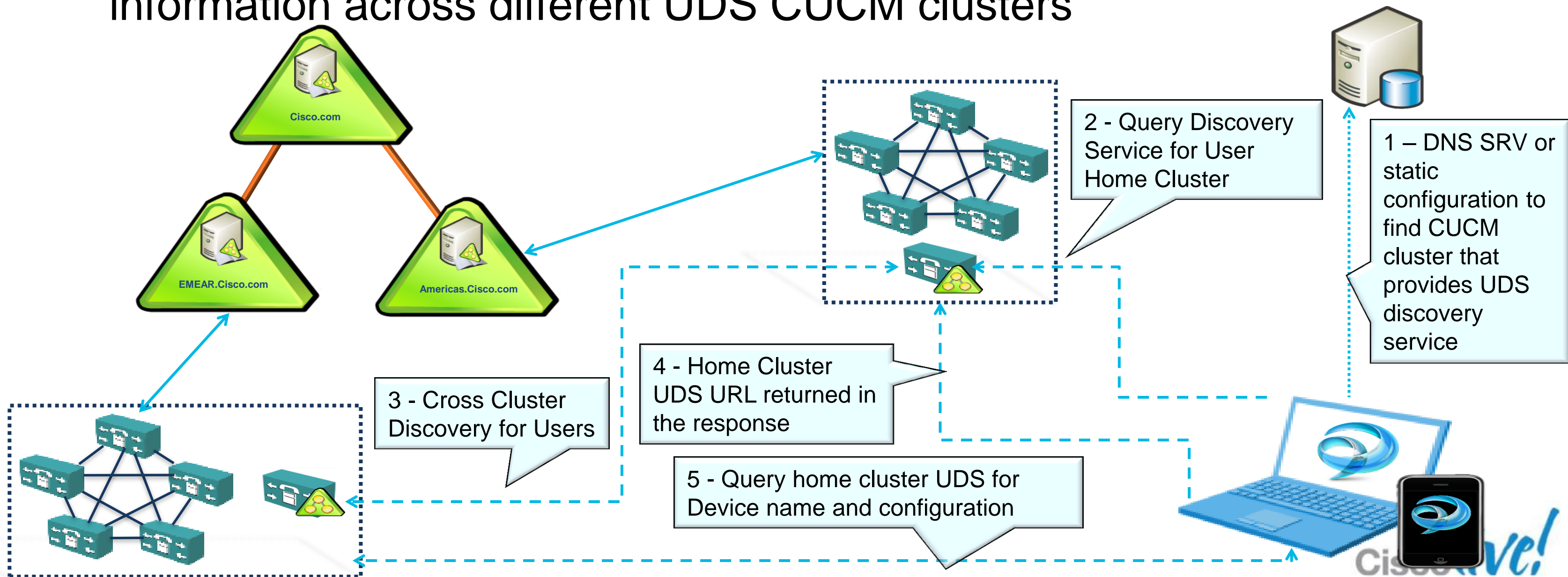
---

**Conferencing Profile**

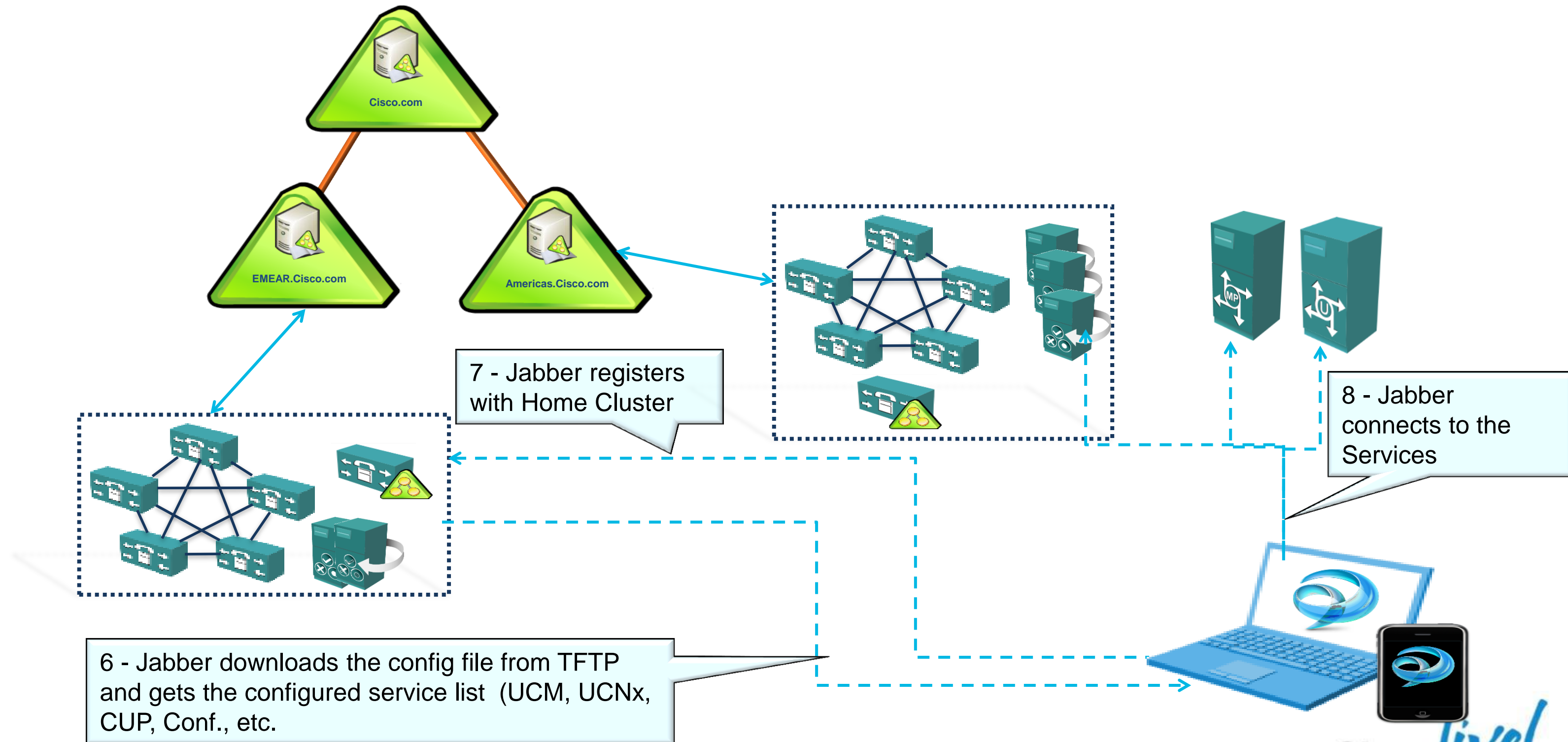
Primary

# User Base Cluster Discovery

- The direction for UDS is to allow dynamic discover of the home cluster for a specific user, and to get information from users directory information across different UDS CUCM clusters



# Service Discovery



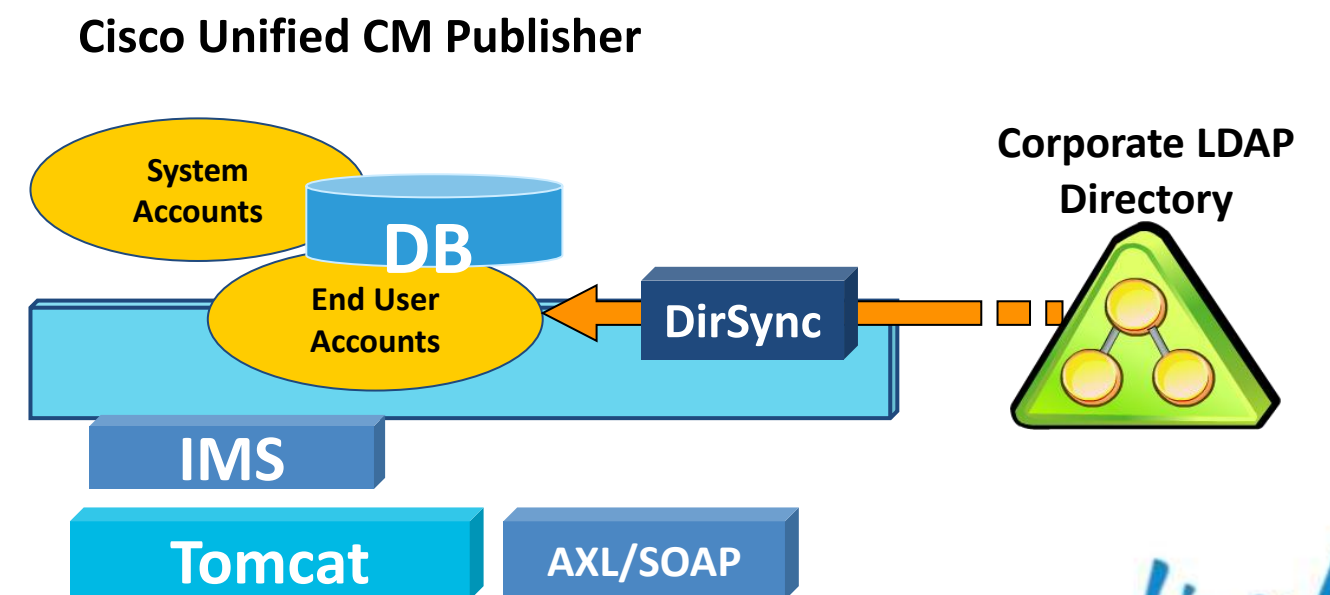
# How Cisco Applications Use Directory Services





# Performance and Scalability of User Directory Synchronisation in CUCM

- Initial synchronisation for 60,000 User Accounts in Unified CM 7.1(x) takes roughly 30 minutes.
- Initial synchronisation for 60,000 User Accounts in Unified CM 8.0(1) takes roughly 22 minutes.
- Initial synchronisation for 80,000 User Accounts in Unified 8.6(1) or later takes roughly 19 minutes
- Subsequent synchronisation operations may take more/less time depending on the number of changes between synchronisation intervals.



# Custom User Fields

- In the current scenario there are 13 default attributes (hardcoded) which are synchronised along with the users.
- Custom User Fields are additional LDAP attributes which would be synchronised.
- Custom User Fields Names must be the same across all synchronisation agreements.
- Up to five Custom User Fields can be added.

**Standard User Fields To Be Synchronized**

Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	telephoneNumber	Mail ID	mail
Directory URI	msRTCSIP-primaryuseraddress		

**Custom User Fields To Be Synchronized**

Custom User Field Name	LDAP Attribute
address	address

**Custom User Fields To Be Synchronized**

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

Custom User Field Name	LDAP Attribute
code	countrycode
license	carlicense

# Local Users and LDAP Synchronisation

- CUCM 9.0 and later allows the simultaneous support for both LDAP synchronised and manually added end users.
- There is an option to convert LDAP users to local users.

**End User Configuration**

Status: Ready

**User Information**

User Status: Active LDAP Synchronized User

User ID: harry

PIN: [Redacted]

Confirm PIN: [Redacted]

Last name\*: potter

Middle name:

First name: harry

Directory URI:

Telephone Number:

Mail ID:

Manager User ID:

Department:

User Locale: < None >

Associated PC:

Digest Credentials: [Redacted]

Confirm Digest Credentials: [Redacted]

**Convert User Account**

Convert LDAP Synchronized User to Local User

**Service Settings**

Home Cluster

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

UC Service Profile: < None > [View Details](#)

**Device Information**

Find and List Users

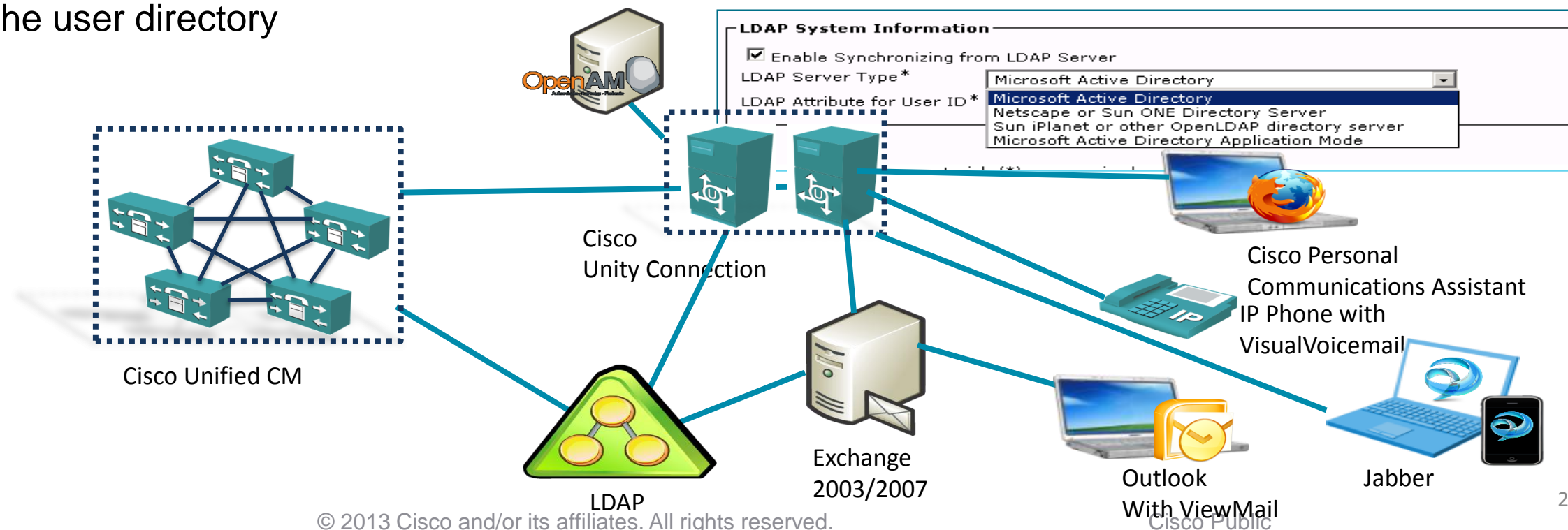
6 records found

User ID	First Name	Last Name	Department	User Status
harry	harry	potter		Active Local User
herm	herm	granger		Active LDAP Synchronized User
neville	neville	longbottom		Active LDAP Synchronized User
ron	ron	weasley		Active LDAP Synchronized User

# Unity Connection User Directory Integration

- Three approaches to integrate user directory in Unity Connection
  - Importing users from a CSV file to the Connections database
  - Getting the user from CUCM database using AXL/SOAP
  - Connection to an LDAP engine the same mechanisms and limitations discussed before in CUCM

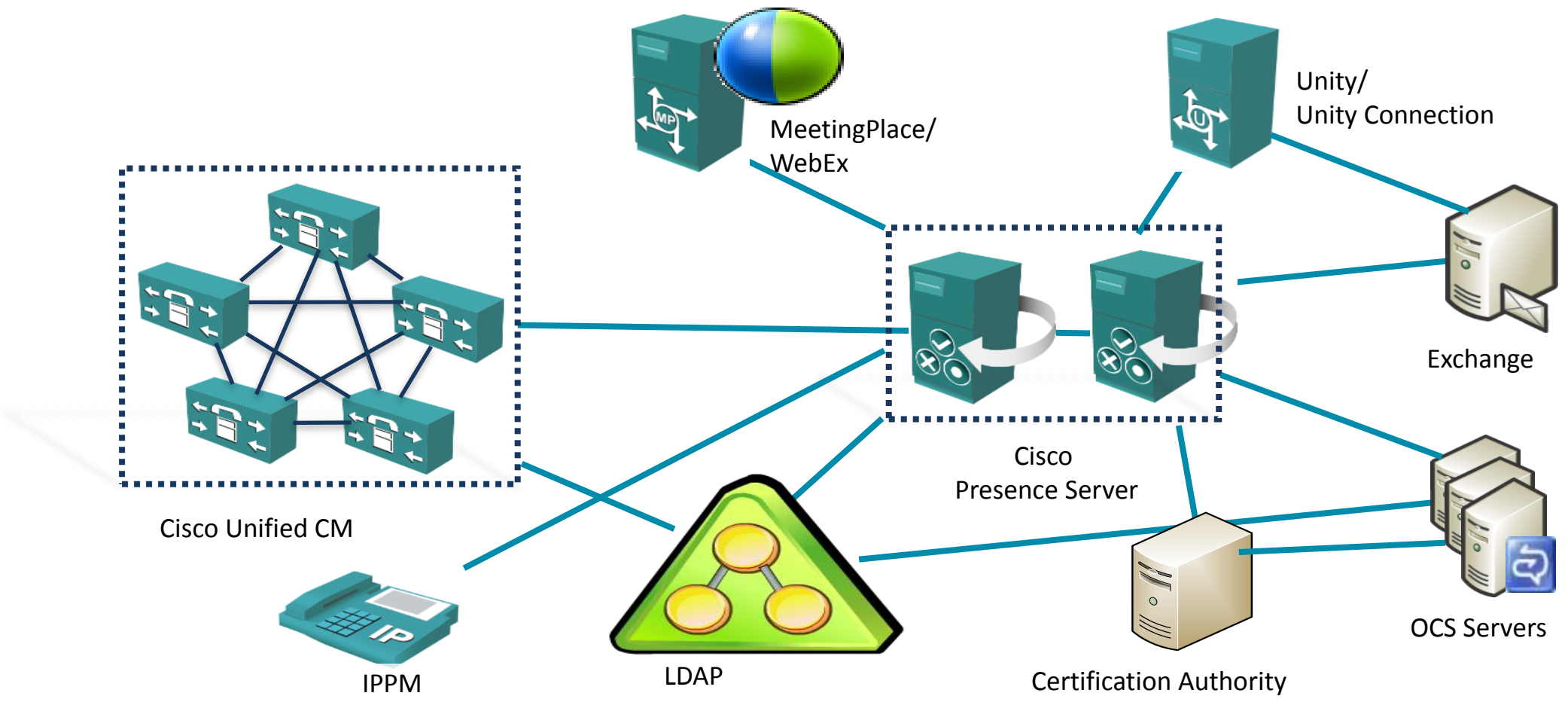
**Note:** if you use SSO you need to choose LDAP for the user directory



# Presence Server User Directories

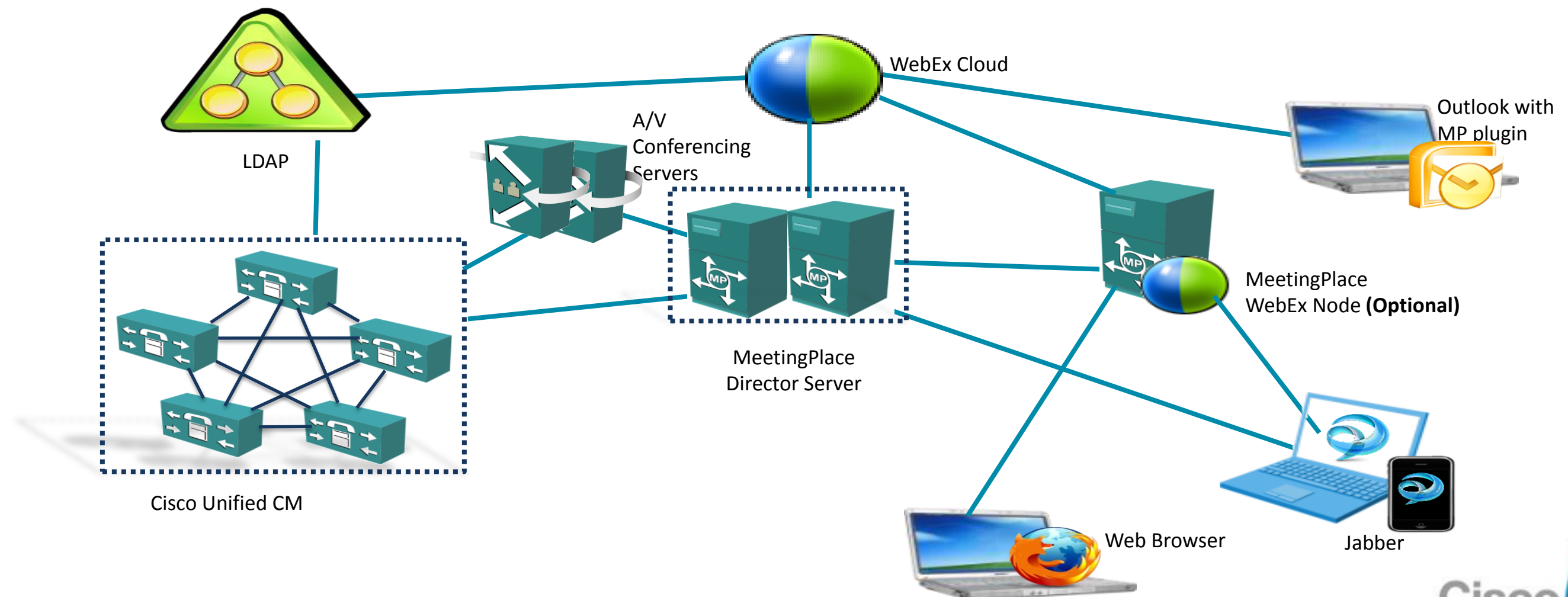
## Integration

CUP gets the user and password information from CUCM through the sync agent.



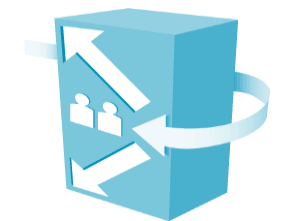
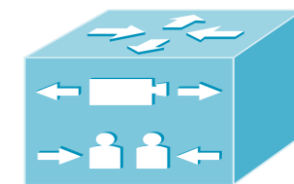
# MeetingPlace User Directories Integration

- In version 8.5 everything changes 😊
- MeetingPlace recommended way is to synchronise on-premise LDAP source with WebEx and it will populate user information into MeetingPlace



# Video Applications Directory Integration

- Two main products that consume user directory information and require authentication :
  - VCS (Video Communication Server)
  - TMS (TelePresence Management Suite)
- All the other products (Endpoints, MCU, Gateways, TP Server, etc.), can get it from VCS / TMS.



# VCS (Video Communication Server)

## Administrators

- Users can be provisioned locally or imported from an LDAP/S Engine
- User can be authenticated using local password or if LDAP integration is used, Basic or SASL authentication is available.

## Endpoints Registration

- User database can be populated from:
  - Locally added
  - Populated from the TMS database
  - Populated from LDAP/S including AD DC
- Users can be authenticated using the following methods:
  - Local Password
  - Through LDAP/S binding using SASL or basic passwords
  - NTLMv2



# TMS (TelePresence Management Suite)

- TMS is part of a Microsoft domain, and uses IIS to provide interface to the users. So by default, without any additional administration configuration, user authentication is integrated with Windows logon.
- When users access to the Web Interface TMS will get the User details from AD GC using ADSI Libraries, and populate its internal database.
- User database population can also be achieved from generic LDAP/S synchronisation.
- Accepts different mechanisms for Authentication:
  - NTLMv2
  - AD Kerberos
  - LDAP/S simple authentication
- From the user information gathered from the different sources TMS is going to create the phone books for the endpoints.

# WebEx Social LDAP Integration

- There are two ways of integration with LDAP sources (AD, OpenLDAP):
  - LDAP Authentication - The WebEx Social user database will be populated with the details imported from the LDAP source when the user first logins to the system. Can be performed from "Quad" Nodes only.
  - LDAP Synchronisation – The WebEx Social user database will be populated at specific time and all the user that match the LDAP filter will be imported.
- LDAP and LDAPS methods are supported
- Users can be created locally as well as imported from LDAP source.

The screenshot shows the 'LDAP Authentication' configuration page. It has tabs for 'General', 'LDAP Authentication', 'LDAP Directory Sync', 'CAS', 'NTLM', 'OpenID', 'Open SSO', and 'SiteMinder'. The 'LDAP Authentication' tab is active. Under 'Enabled', there is a checked checkbox. A blue callout bubble points to the 'Enabled' checkbox with the text: 'Be careful if enable it will disable local user, including the administrators'. Below this, there is a 'Required' checkbox which is unchecked. Under 'Default Values', there are three radio buttons: 'Microsoft Active Directory Server' (selected), 'OpenLDAP', and 'Other Directory Server'. There is a 'Reset Values' button. At the bottom, there is a 'Connection' section.

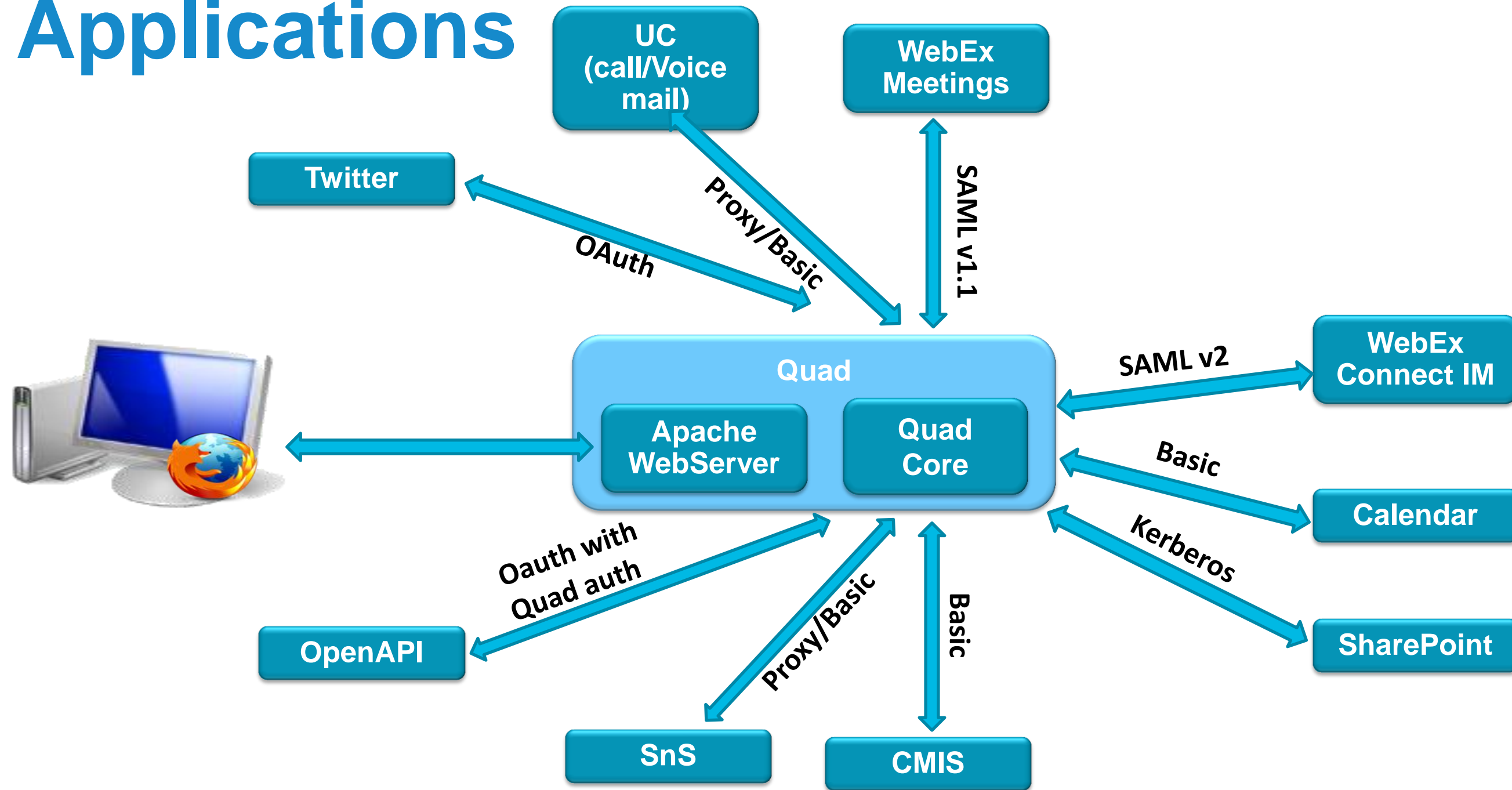
The screenshot shows the 'Configuration' section of the WebEx Social configuration page. It has a sidebar with links for 'General', 'Authentication', 'Users', 'Mail Host Names', and 'Email Notifications'. The 'Authentication' link is selected. Under 'Authentication', there are sections for 'Identification' (with links for 'Addresses', 'Phone Numbers', and 'Additional Email Addresses') and 'Miscellaneous' (with links for 'Display Settings' and 'Google Apps'). There are 'Save' and 'Cancel' buttons at the bottom.

The screenshot shows the 'Authentication Search Filter' and 'Import Search Filter' fields. The 'Authentication Search Filter' field contains the text '(sAMAccountName=@screen\_name@)'. The 'Import Search Filter' field contains the text '(objectClass=person)'. There are help icons next to both fields.

# WebEx Social Single Sign-On

- WebEx Social supports NTLM version 1.
  - NTLM is a Microsoft protocol that can be used for authentication through IE & Firefox
- WebEx Social supports non-standard based SSO solutions – these are created as one offs and need to be customised:
  - CA Site Minder
  - Oracle access manager - OAM
  - Shibboleth
  - OAuth
  - Kerberos

# WebEx Social Authentication in External Applications



# WebEx Cloud User Account Management Options

Option	Description
Manual updates through Org Admin	<ul style="list-style-type: none"> <li>• Admin can use Org Admin to manually update user accounts</li> </ul>
File import to Org Admin	<ul style="list-style-type: none"> <li>• Admin can create and update accounts by importing a change file into Org Admin</li> </ul>
Directory Integration (FTP approach and will be depreciated soon)	<ul style="list-style-type: none"> <li>• Semi-automatic method for creating, updating and deactivating user accounts and groups.</li> <li>• Customer creates scripts to capture account changes in their Active Directory. The change files are uploaded to a WebEx FTP server and automatically imported into Connect user DB</li> <li>• Advanced Services engagement</li> </ul>
Single Sign-On	<ul style="list-style-type: none"> <li>• SSO can be configured to automatically create accounts when user logs-in to Connect for the first time</li> <li>• SAML assertion provides user information</li> <li>• Accounts can be created and updated but not deactivated</li> </ul>
Cisco Cloud Connect	<ul style="list-style-type: none"> <li>• Connect to AD for Windows Server 2003 &amp; 2008 and quickly onboard new identities</li> <li>• Syncs all the changes that happens in AD</li> </ul>

# Cisco Cloud Connector 1.0

The screenshot shows the Cisco Cloud Connector dashboard. At the top, it displays the Cisco logo and the text "cloud connector". Below this, there are navigation tabs for "Dashboard" and "Configuration". The main content area is divided into several sections:

- Current Synchronization:** Shows a status of "idle" with a green checkmark.
- Last Synchronization:** Displays two synchronization events. The first is an incremental sync on 3/2/2012 at 12:58 PM, which finished at the same time. The second is a requested full sync on 3/2/2012 at 2:41 PM, which finished at the same time. Both show "No errors".
- Connectors:** A table with columns "Connector" and "Last Connection". It lists one connector, "WNTVMQ4VE", with a last connection time of "3/2/2012 2:41 PM".
- Cloud Statistics:** Shows "Users: 46" and "Groups: 8".
- Synchronization Schedule:** Shows a full sync "Every Sun at 3:30 AM" and an incremental sync "Every 10 minutes".
- Next Synchronization:** Shows a full sync on "3/4/2012 3:30 AM" and an incremental sync on "3/2/2012 2:51 PM".
- Configuration Summary:** A text box stating "All objects will be synchronized. Delete threshold has been set to 21 objects. Log level is info."

The screenshot shows the configuration page for attribute mapping in Cisco Cloud Connector. It features a "Linking Attribute" dropdown menu set to "sAMAccountName". Below this is a table for mapping "Active Directory Attribute Names" to "Cisco Cloud Attribute Names".

Active Directory Attribute Names	Cisco Cloud Attribute Names
C	C
D	D
I	I
departmentNumber	departmentNumber
cn	cn
telephoneNumber	telephoneNumber
postalAddress	postalAddress
objectGUID	onPremObjectGUID
employeeNumber	employeeNumber
displayName	displayName
mobile	mobile
	jobberID
	locale
	timezone

At the bottom of the configuration page, there are "Apply" and "Cancel" buttons.

## Easy Enterprise

Connect to AD for Windows Server 2003 & 2008 and quickly onboard new identities

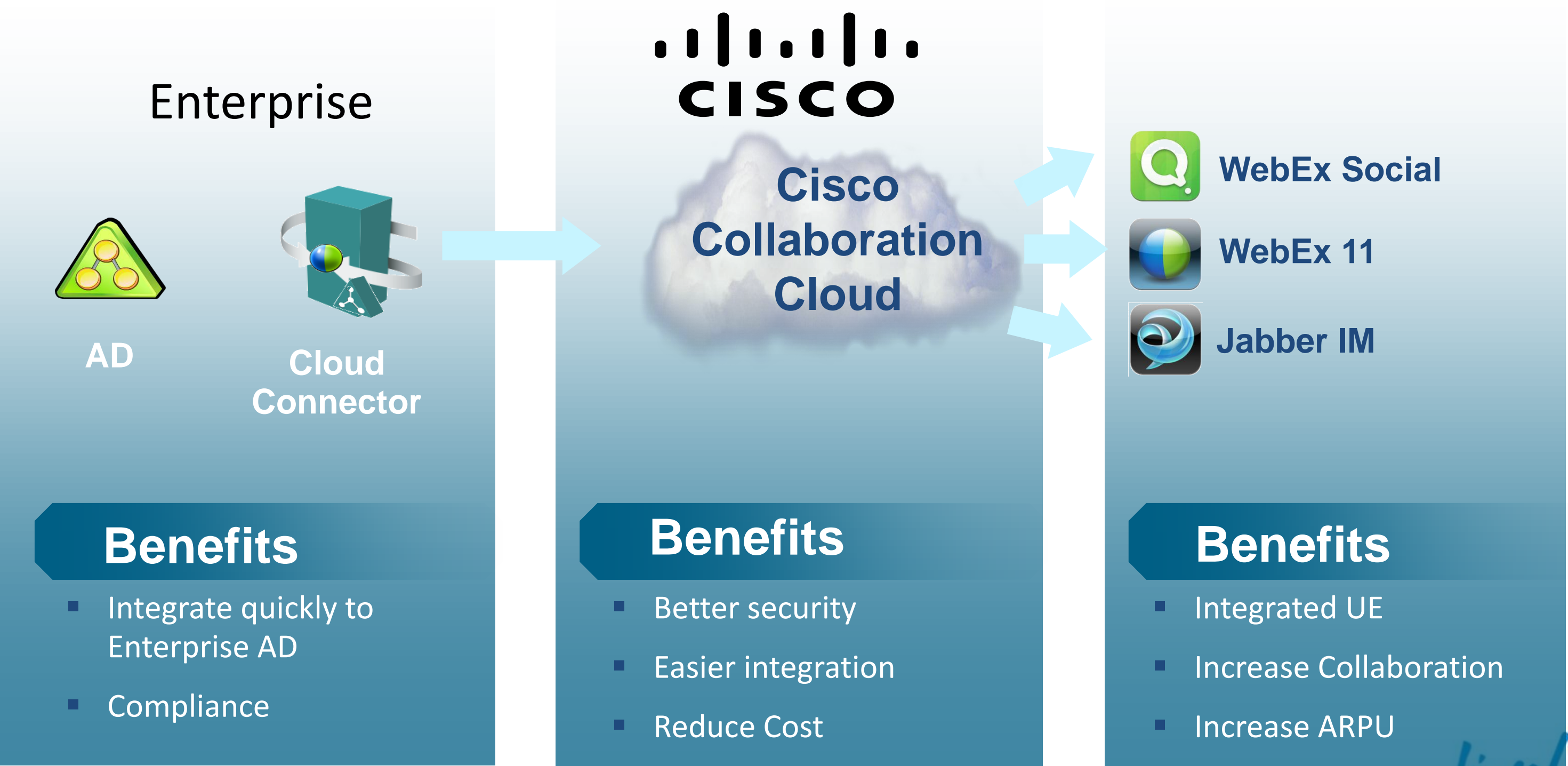
## Easy to Manage

Sync changes to ensure customers can get access

## Easy Compliance

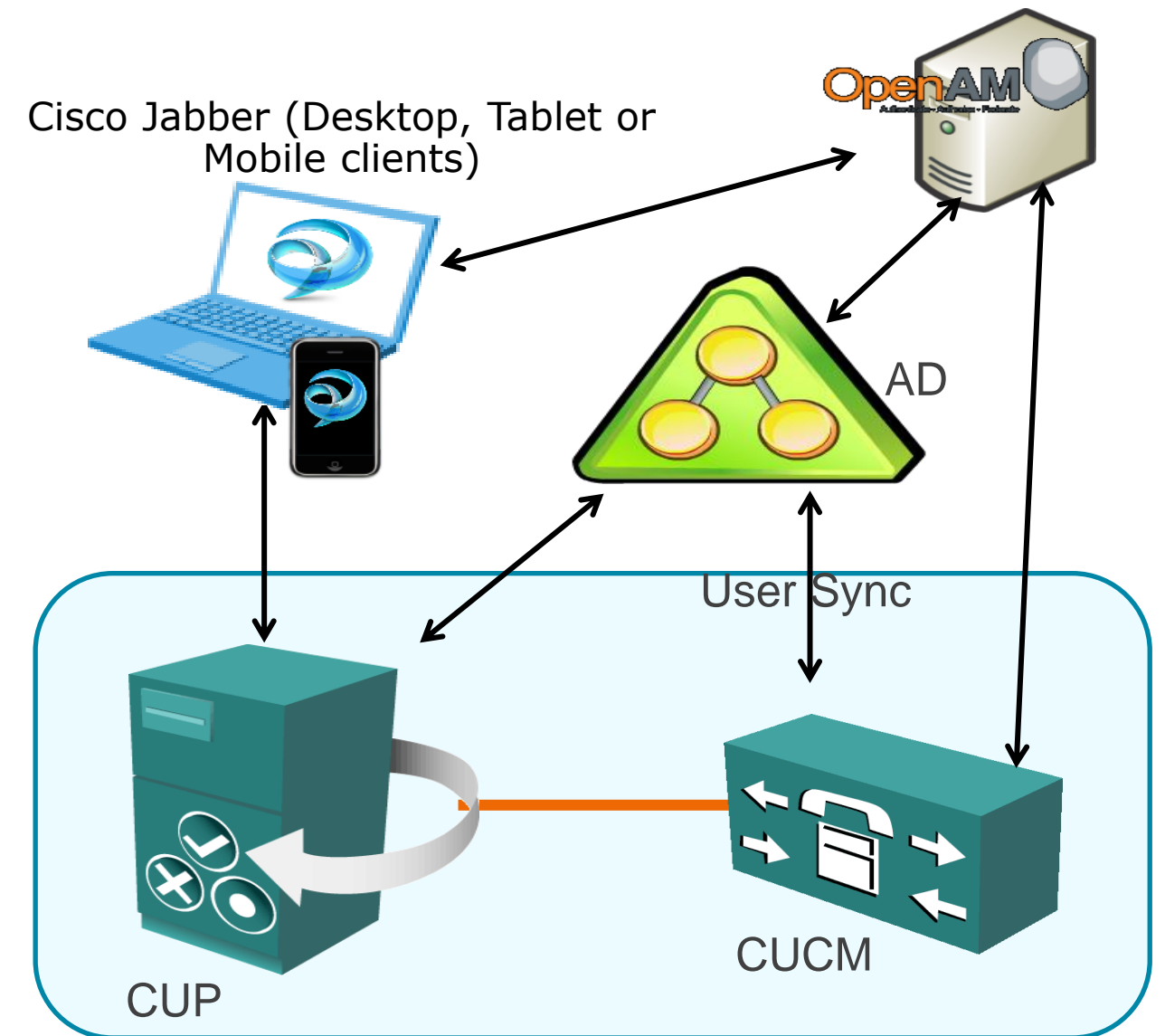
Stay in sync with changes to better manage password resets and de-provisioning

# Cisco Cloud Connector Benefits



# Jabber Login

- DNS SRV lookup to locate CUP
- A SOAP login will be initiated with CUP
  - If AD authentication is enable in CUCM, CUP will contact the AD.
  - If CUCM local Authentication is used CUCM will be used
  - If SSO is enabled in CUCM the CUCM Policy agent will be used for Authentication
- Upon success, CUP returns various details such as primary/backup XMPP nodes, LDAP, WebEx profiles etc.

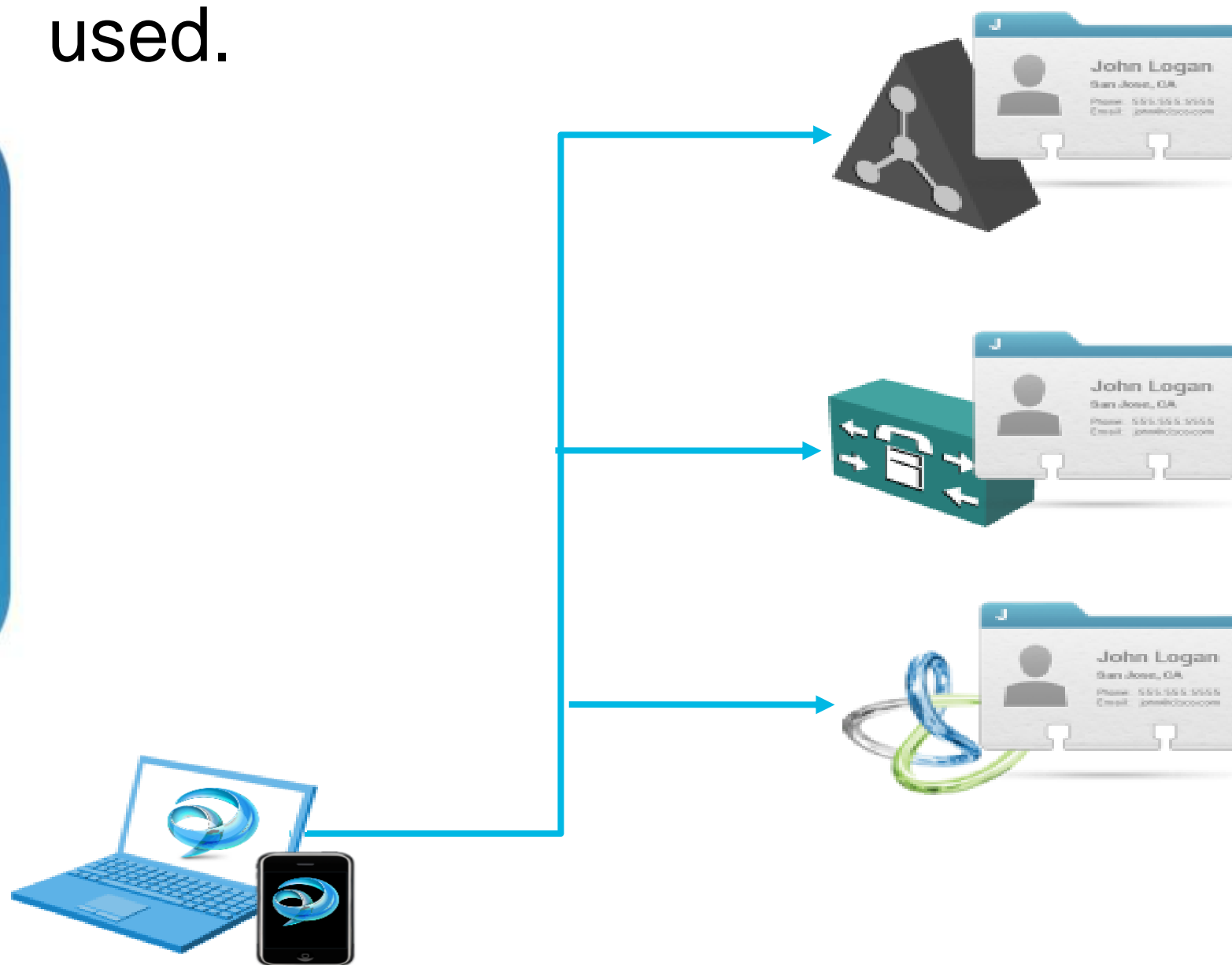




# Cisco Jabber for Windows

## Understanding Contact Record Sources

Based on client operating mode appropriate record sources will be used.



**Auto detect Active Directory/LDAP  
(on prem)**

Recommended pre 8.6(2)

**UC Manager UDS Service  
(on prem)**

Recommended for 8.6(2) +

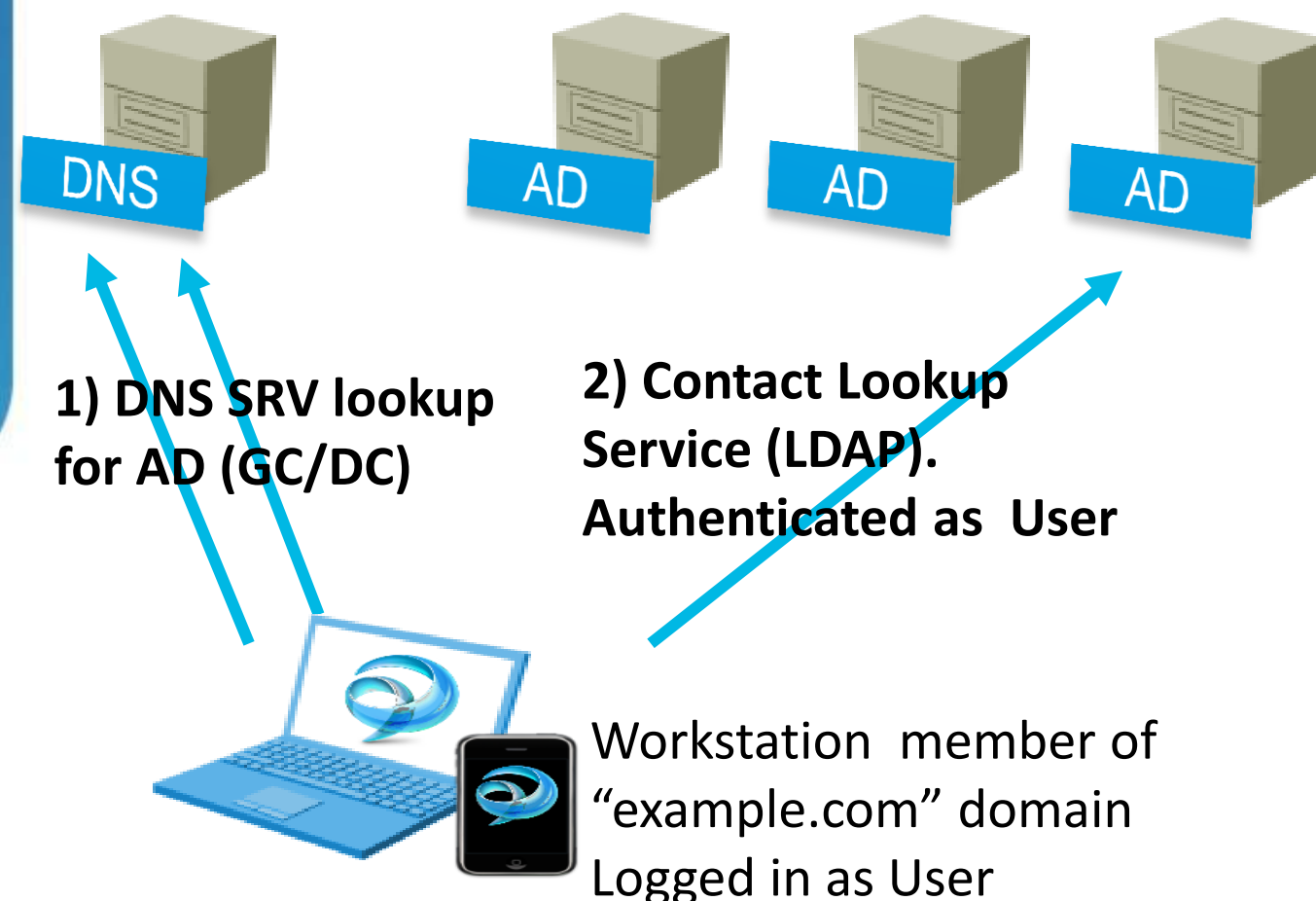
**Webex Corporate Directory (Cloud)**

# Cisco Jabber for Windows (on premise)

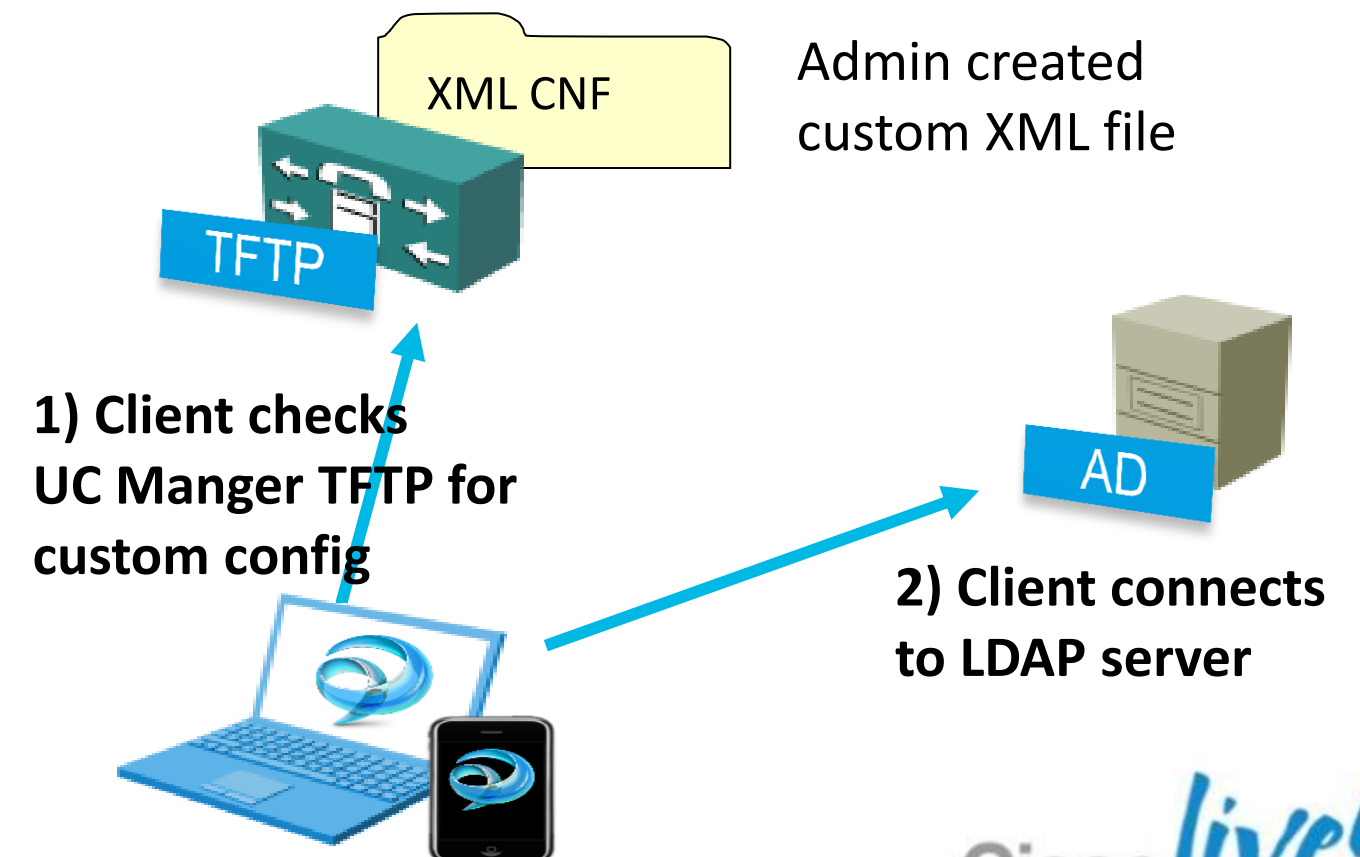
## Active Directory Contact Record Source

- Active directory record source connects to AD/LDAP
- Used updated version of EDI integration from CUPC/CUCILYNC
- Ambiguous name resolution (ANR) is used for search which is more efficient and uses less server resources than previous searching methods.

### Auto-discovery configuration



### Custom Configuration



# EDI – Enhanced Directory Integration

## Custom Directory Access Parameters

### Connection Settings

Connection Type  
UseSecureConnection  
UseSSL  
PrimaryServerName  
Port1  
SecondaryServerName  
Port2

### Search

SearchBase1  
SearchBase2  
SearchBase3  
BaseFilter

### Attribute Map

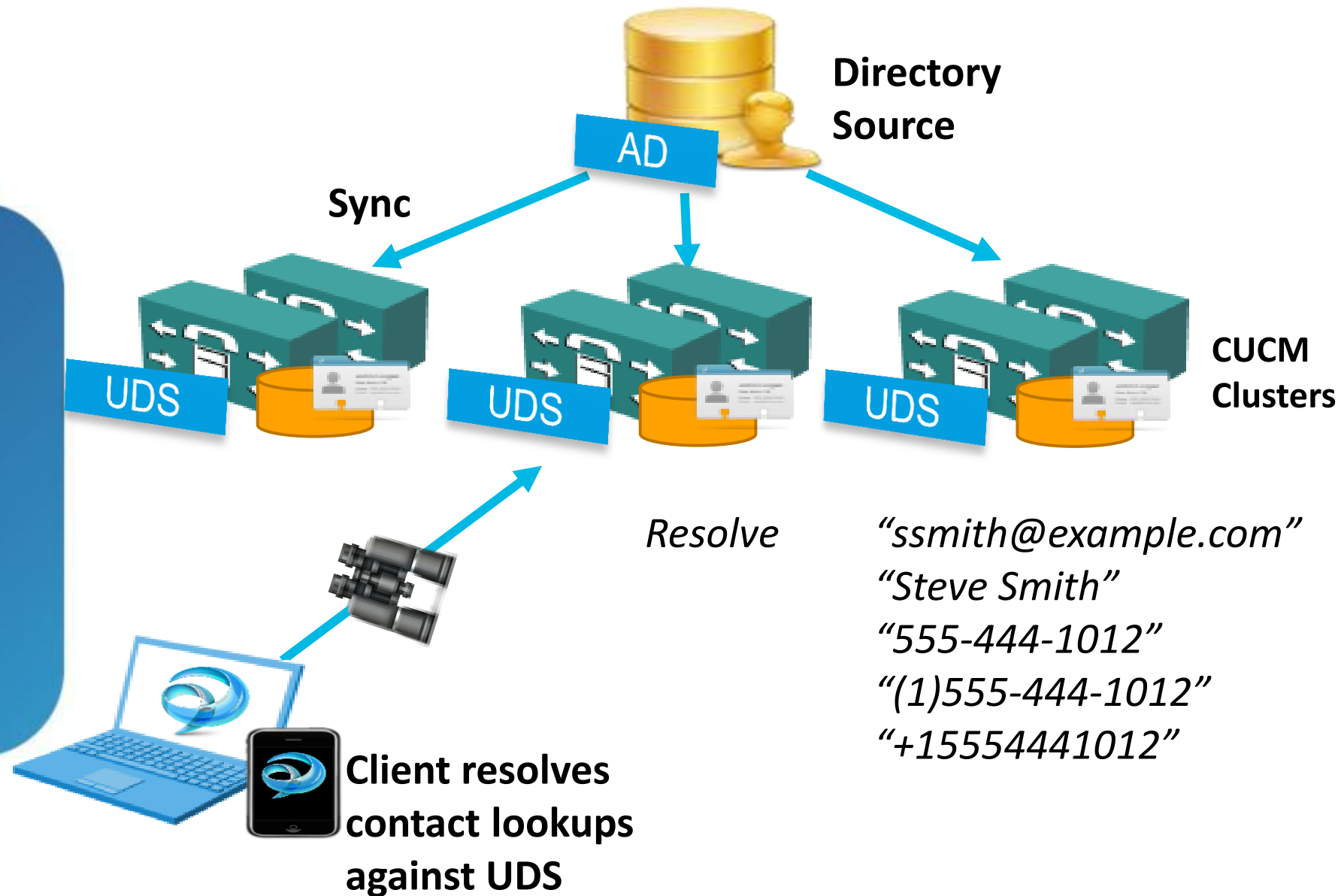
CommonName	Nickname
FirstName	PostalCode
LastName	State
EmailAddress	StreetAddress
SipUri	PhotoURI
BusinessPhone	CompanyName
HomePhone	UserAccount
OtherPhone	Domain
PreferredNumber	Location
Title	

### Authentication

UseWindowsCredentials  
ConnectionUsername  
ConnectionPassword

# Cisco Jabber for Windows (on premise)

## UDS Contact Record Source



- When using the UDS Contact Record Source the client performs contact resolution against communication manager.
- The communications manager User Data Service provides an optimised contact lookup service from CUCM 8.6(2)
- UDS provides a cross cluster contact service supporting up to 80,000 contacts.

# Single Sign-On with OpenAM

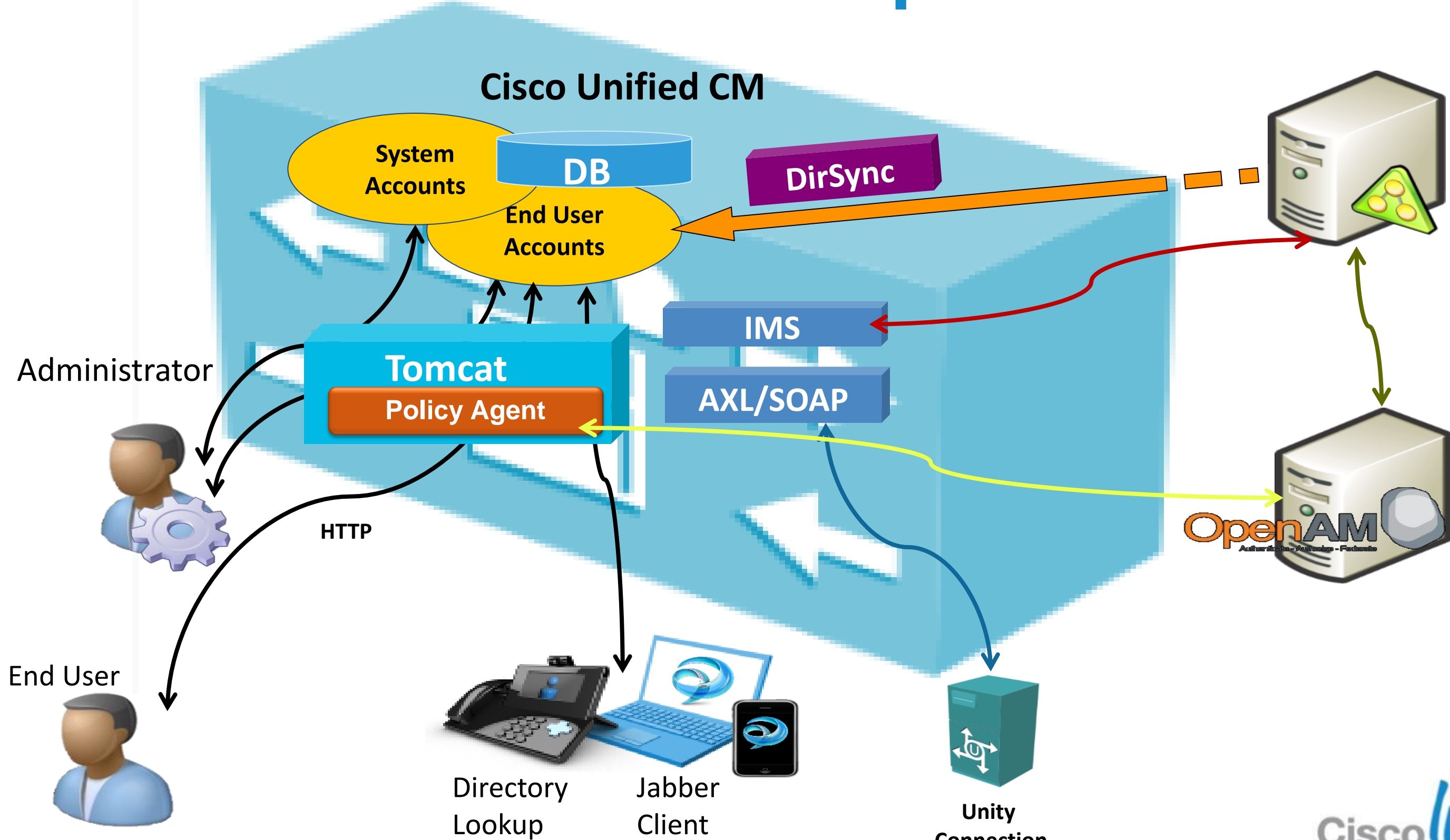


# Authorisation & Authentication Services

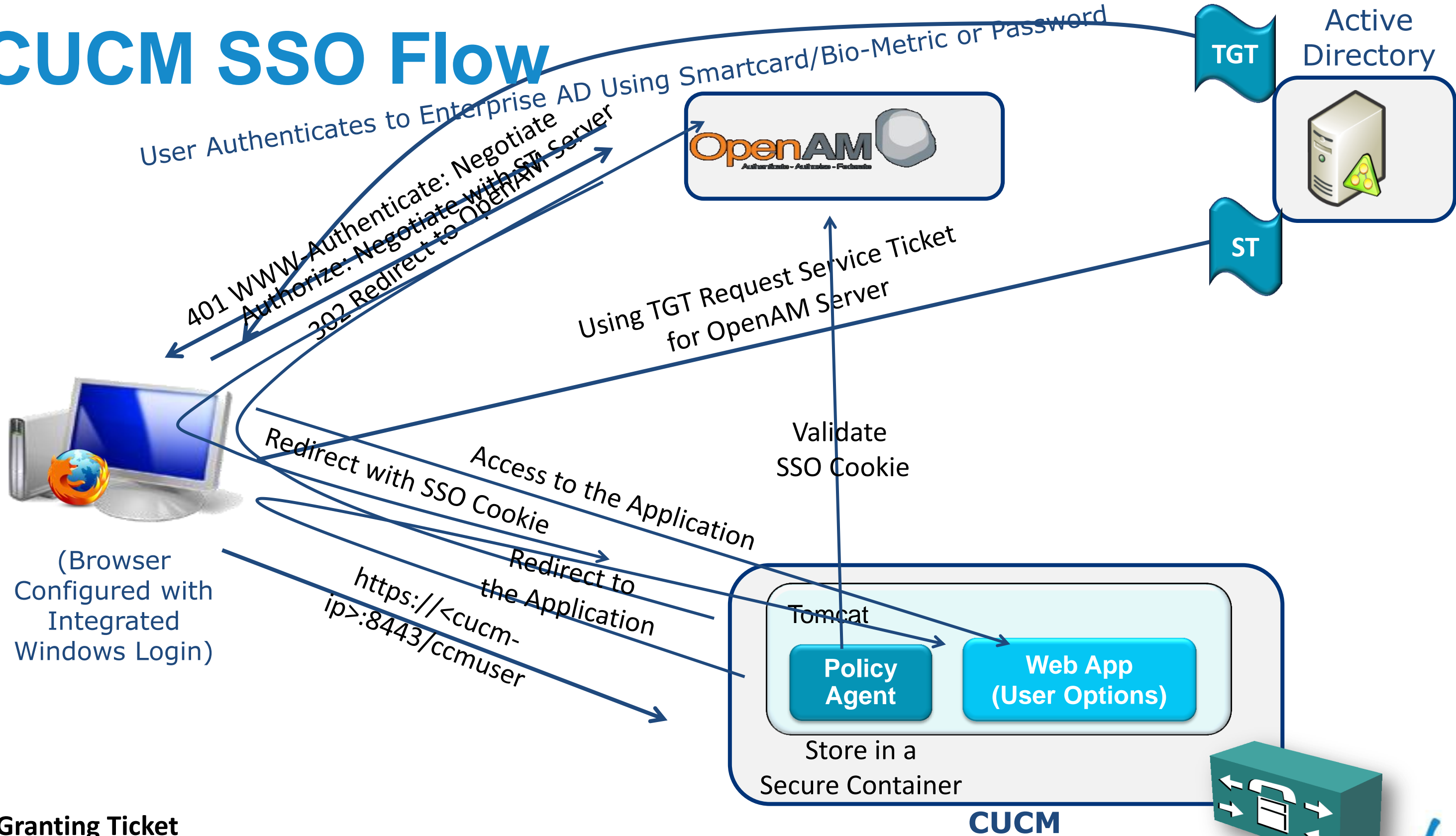
## Solution Support by Cisco Collaboration Portfolio

- Integration of the [Cisco Identity Management System \(IMS\)](#) with the [Open Web Single Sign-On architecture](#), which is an open source initiative started by Sun Microsystems
- After the acquisition of Sun Microsystems by Oracle, Oracle announced that OpenSSO would no longer be their strategic product. OpenSSO continues to be developed and supported by ForgeRock under the name of [OpenAM](#).
- OpenAM provides open source Authentication, Authorisation, Entitlement and Federation software.
- OpenAM provides core identity services to simplify the implementation of transparent single sign-on (SSO) as a security component in a network infrastructure

# CUCM Interaction with OpenAM



# CUCM SSO Flow



TGT: Ticket Granting Ticket  
 ST: Service Ticket



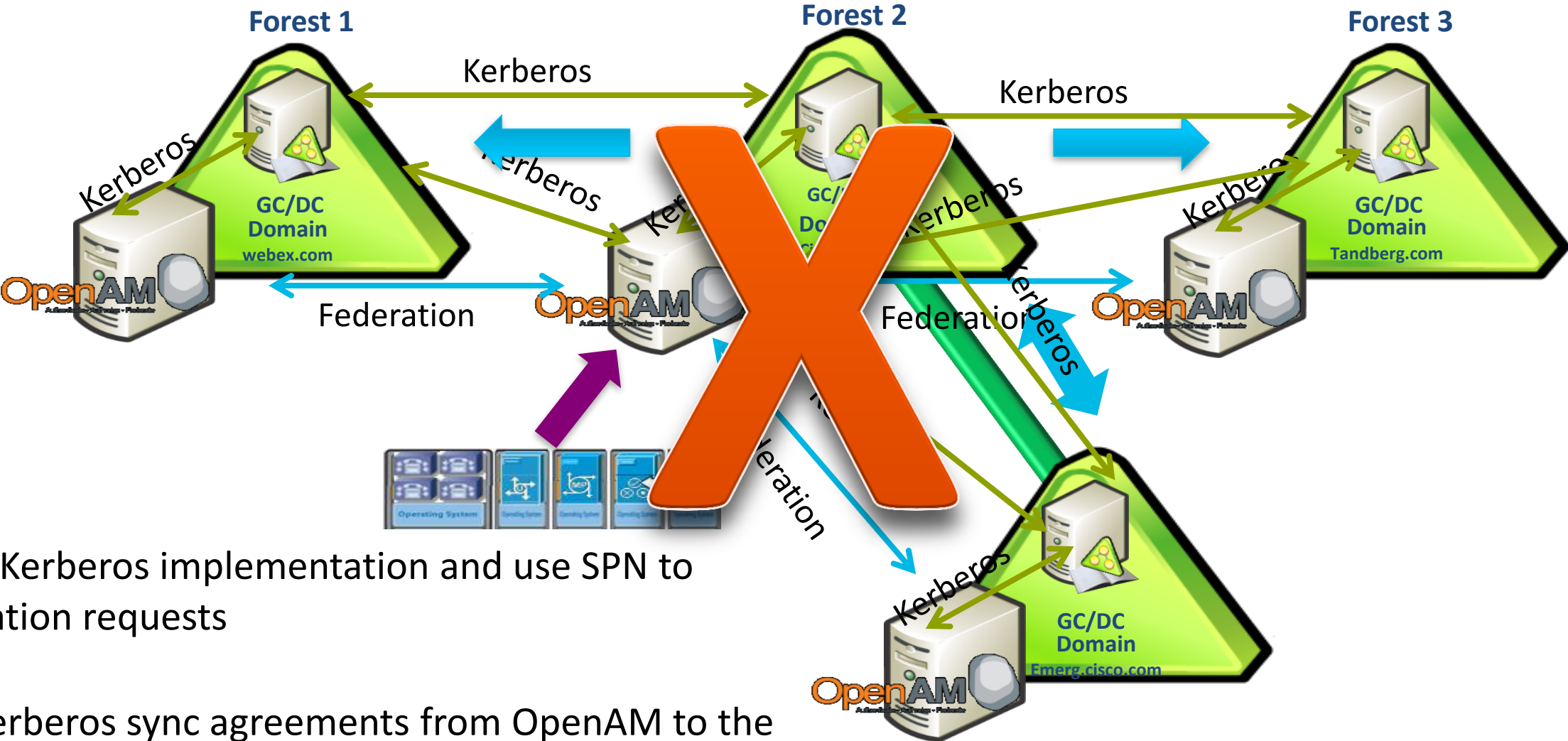


# SSO with Multiple Domains



# SSO with Multiple Domains

One possible solution could be hard to maintain



Rely on Microsoft Kerberos implementation and use SPN to “relay” authentication requests

Create multiple Kerberos sync agreements from OpenAM to the KDC of each domain

# SSO with Multiple Domains

Rely on Microsoft Kerberos implementation and use SPN



# Kerberos Service Principal Names (SPN)

- Unique identifier for a service running on a server
- Before Kerberos can use a SPN to authenticate a service, the SPN must be registered on an account object
- It uses the AD attribute ServicePrincipalName
- Registered with SETSPN.exe or ADSIEdit, and stored as AD property
- Pattern: **<service class>/<host>:<port> <service name>**

**Examples on how to add an SPN:**

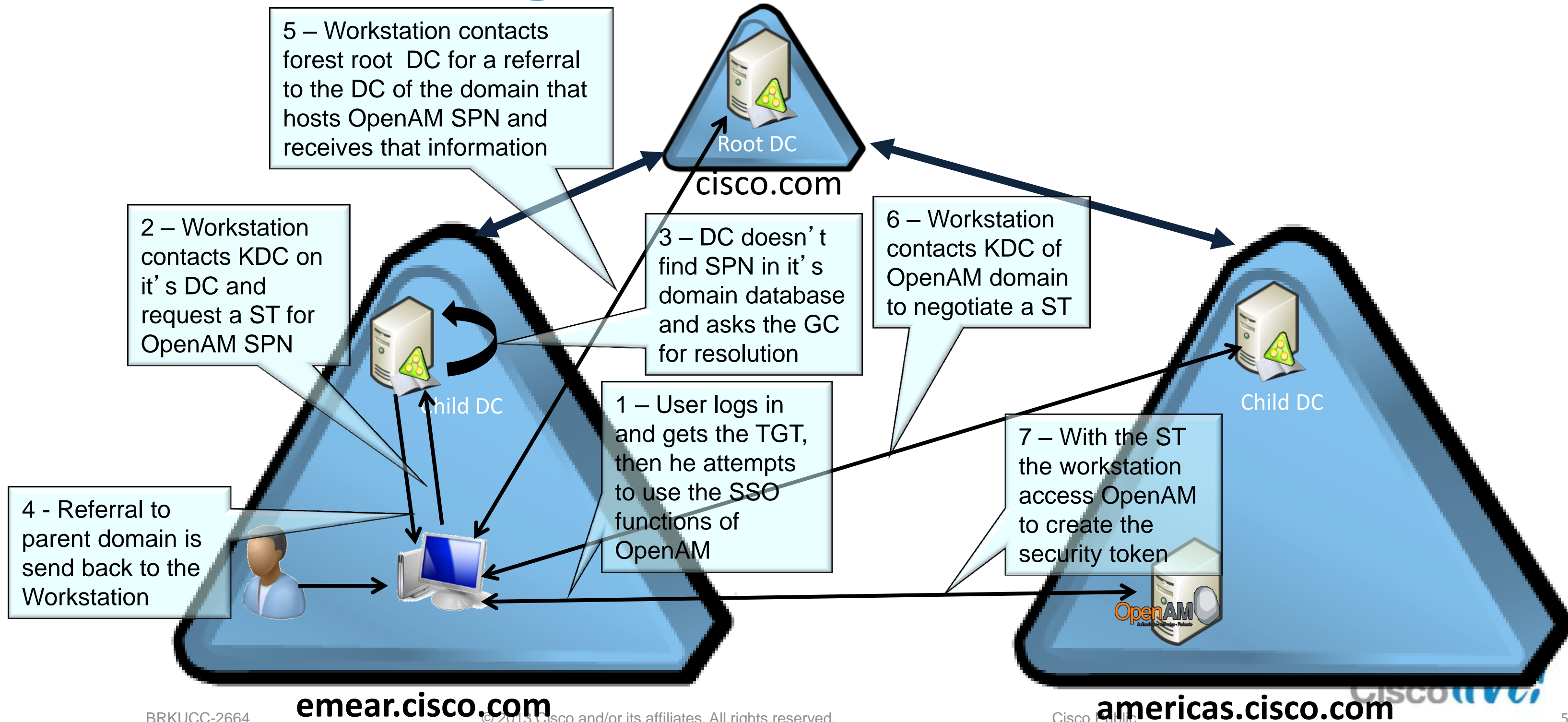
**Setspn -A HTTP/sso.cisco.com:8443 CISCO\CiscoSSO**

**\*\* The SPN format is not a URL! \*\***

# KTPass and its Role

- Configures the server principal name for the host or service in Active Directory Domain Services (AD DS) and generates a .keytab file that contains the shared secret key of the service.
- The .keytab file is based on the Massachusetts Institute of Technology (MIT) implementation of the Kerberos authentication protocol.
- The Ktpass command-line tool allows non-Windows services that support Kerberos authentication to use the interoperability features provided by the Kerberos Key Distribution Center (KDC) service in Windows Server.

# Kerberos Authentication Over Domain Trusts in a Single Forest



# Prerequisites for SSO in a Single Forest

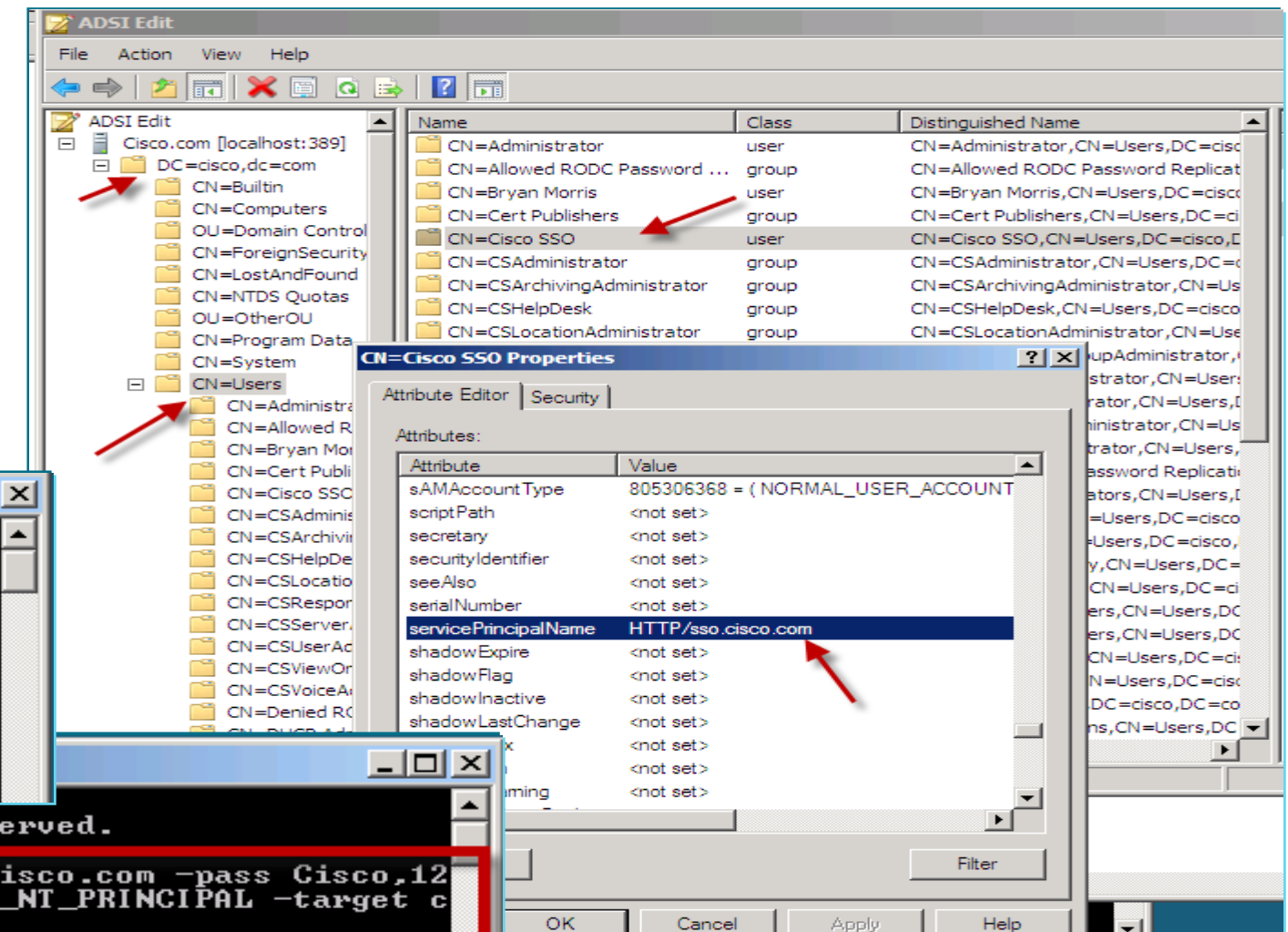
- Create a user domain account that will be used by OpenAM
- Create the SPN in AD
- Create the keytab file with KTPass
- Copy the keytab file to known location configured in OpenAM

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

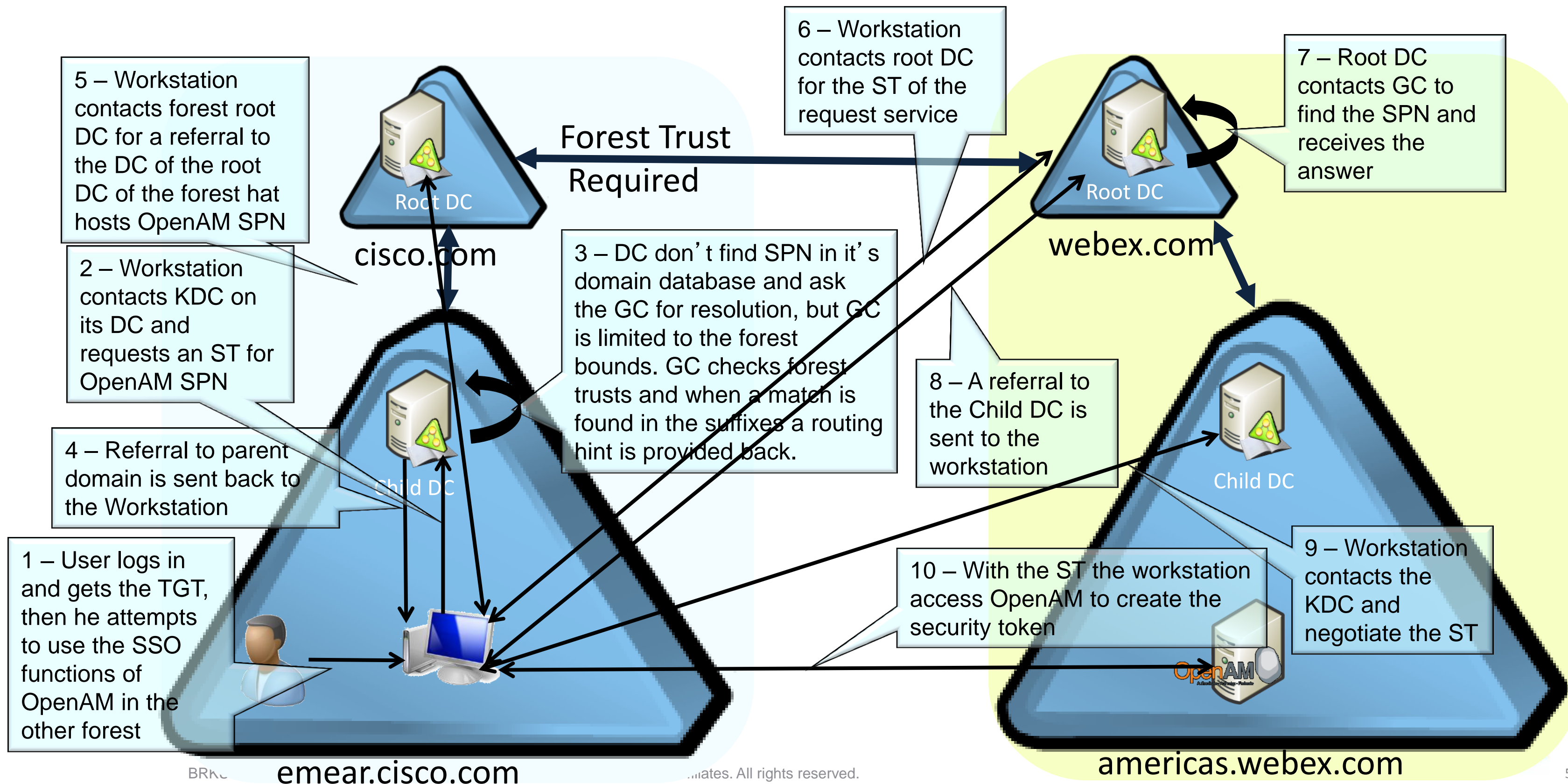
C:\Users\Administrator>setspn -A HTTP/sso.cisco.com:8443 CISCO\CiscoSSO
Registering ServicePrincipalNames for CN=Cisco SSO,CN=Users,DC=cisco,DC=com
HTTP/sso.cisco.com:8443
Updated object
C:\Users\Administrator>
```

```
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ktpass -princ host/sso.cisco.com@cisco.com -pass Cisco,123 -mapuser ciscosso -out CiscoSSO.host.keytab -ptype KRB5_NT_PRINCIPAL -target cisco.com
Using legacy password setting method
Successfully mapped host/sso.cisco.com to ciscosso.
Key created.
Output keytab to CiscoSSO.host.keytab:
Keytab version: 0x502
keysize 63 host/sso.cisco.com@cisco.com ptype 1 <KRB5_NT_PRINCIPAL> vno 6 etype
0x17 <RC4-HMAC> keylength 16 <0xbe043946e72148e800dc9cac66eddd30>
C:\Users\Administrator>
```



# Kerberos Authentication Process Over Different Forests





# Prerequisites for SSO with Multiple Forests

- Same process as described in the slides for single AD forest
- Outbound trust for the forest that we want to extend SSO to

The image displays a sequence of screenshots from the Active Directory management console, illustrating the steps to configure a trust relationship. The main window, 'Active Directory Domains and Trusts', shows a tree view with 'em.cisco.com' selected. Overlaid on this are three 'New Trust Wizard' dialog boxes. The first dialog shows the 'Trust Type' selection screen, where 'Forest trust' is selected. The second dialog shows the 'Direction of Trust' selection screen, where 'One-way: outgoing' is selected. The third dialog shows the 'Sides of Trust' selection screen, where 'Both this domain and the specified domain' is selected. A fourth 'Cisco.com Properties' dialog box is also visible, showing the 'Trusts' tab with a table of outgoing trusts.

Domain Name	Trust Type	Transitive
em.cisco.com	Child	Yes
tandberg.com	Forest	Yes
webex.com	Forest	Yes

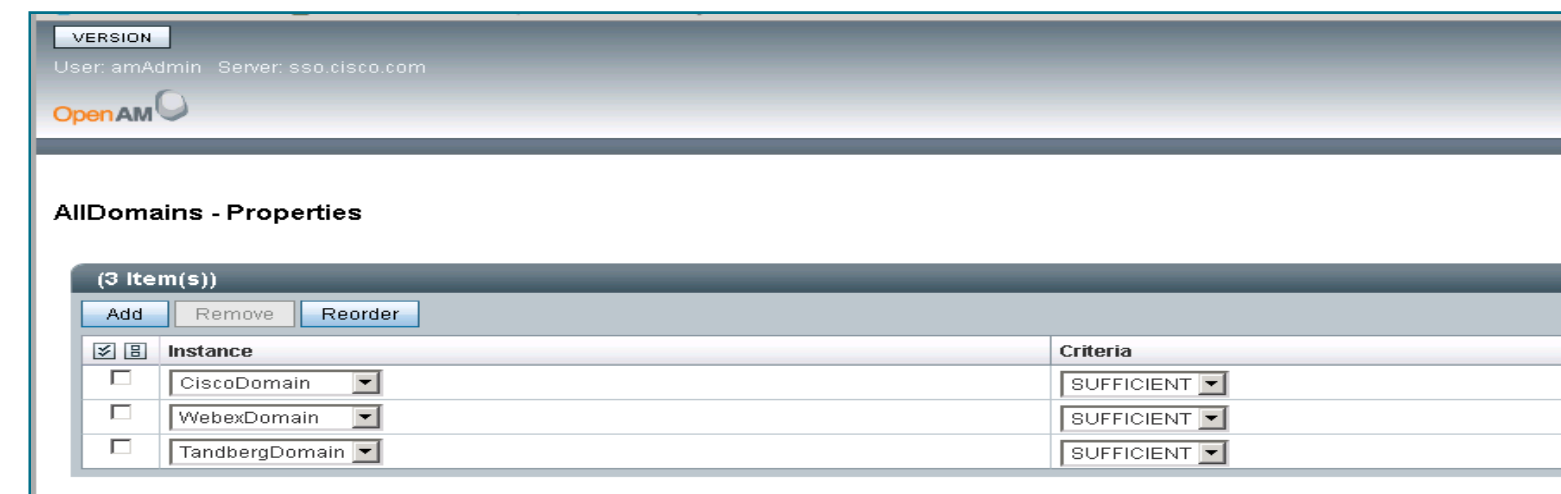
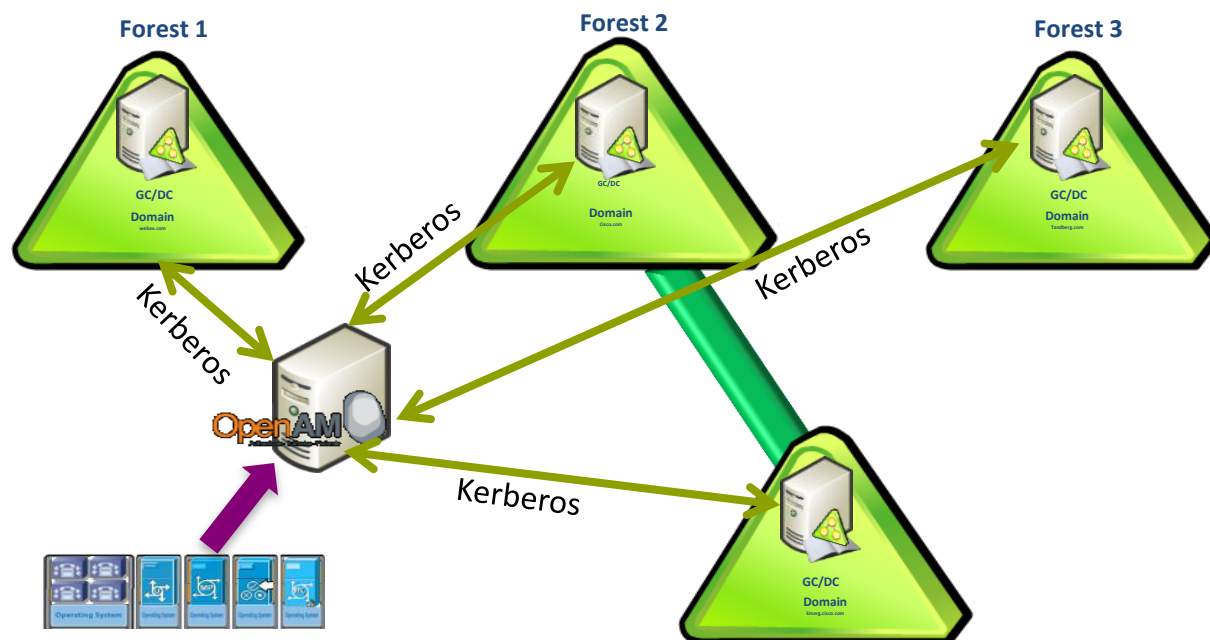
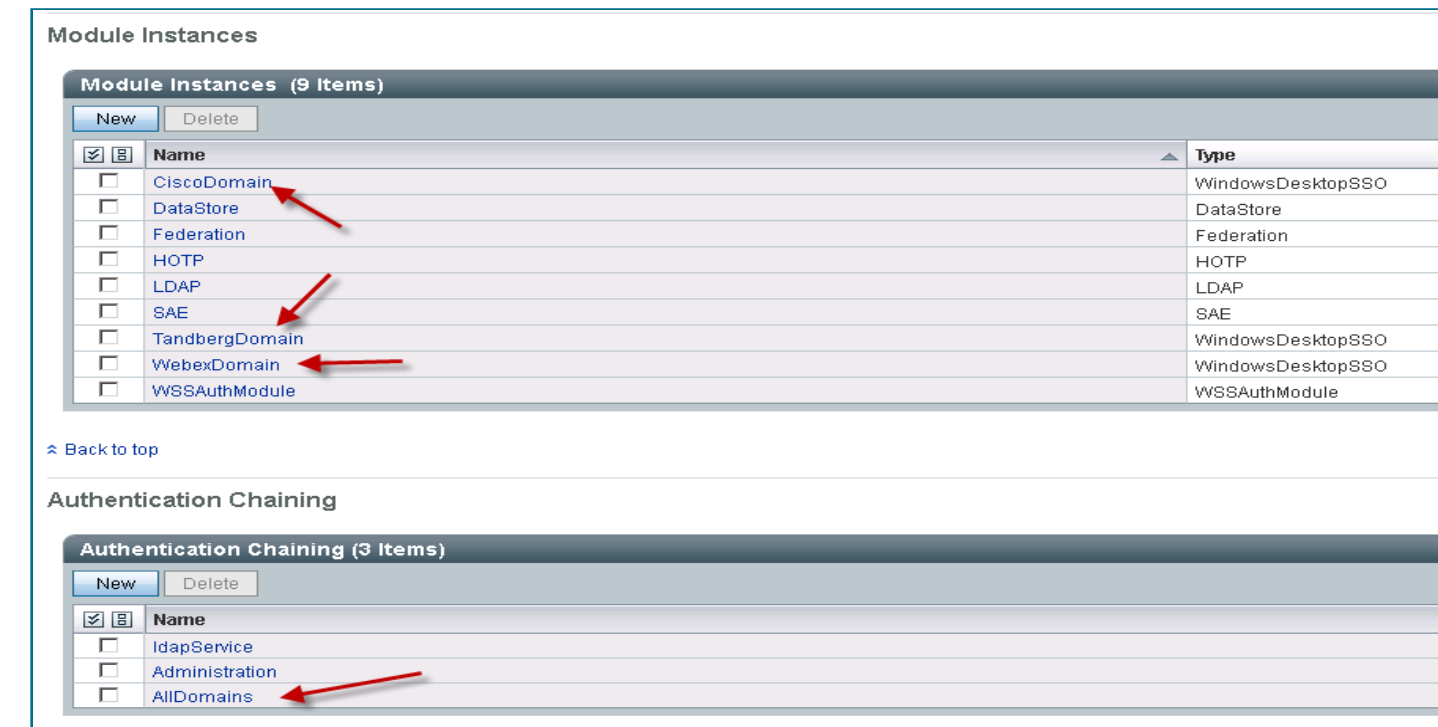
# SSO with Multiple Domains

Multiple Kerberos Sync Agreements



# Individual Kerberos Agreements with Each Domain

- Create a User domain account in each domain that will be used by OpenAM
- Create the keytab file with KTPass for each domain
- Copy the keytab files to a known location to be referenced by OpenAM

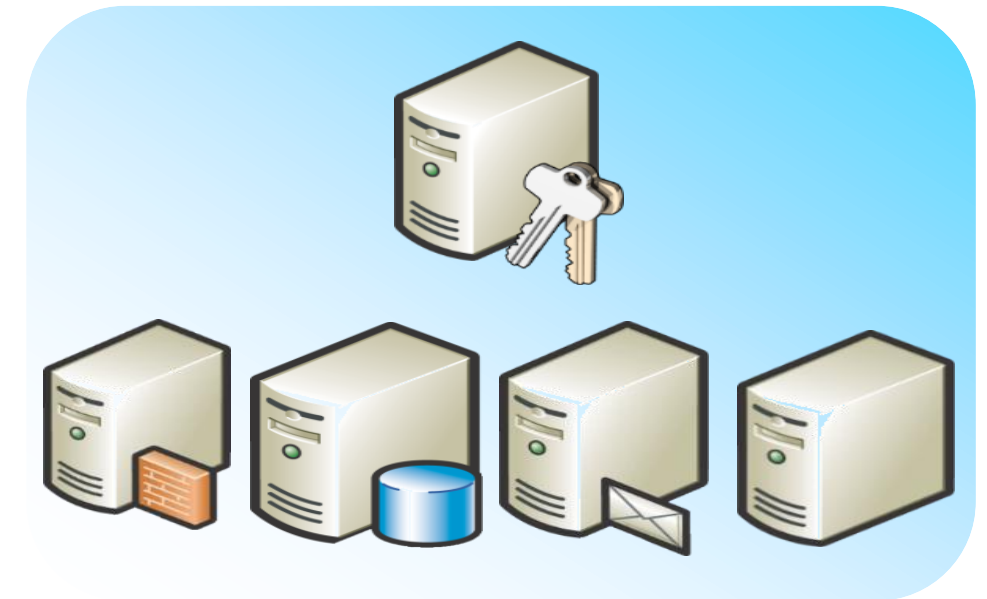


# A Broader View on Authorisation and Authentication Services



# What Other Scenarios Are There in A&A for Our Collaboration Portfolio

- There is already an identity management solution in the customer network, that delivers SSO and user directories.
- We have an organisation that also has cloud services in addition to the on-premise.



# Identity and Access Management?

“In the information systems security space, **identity management** recently emerged as a new term that covers the following areas of computing:

- **Provisioning.** Adds new users to network operating system directories and application server directories, both inside an enterprise and outside at partner information systems.
- **Password management.** Enables users to have a single set of credentials to sign on to the company information systems. Additionally, it enables users to self-administer their passwords, user account data, and privileges.
- **Access control.** Enables the system to recognise security policies for groups of users. For example, a security policy would prevent people from changing their own job title and instead route a request for a job title change to the appropriate authority.



From IBM [Developerworks](#)

**Note :** Sometime we can see it also as IDMS ( Identity Management System )

# Example of IAM's

- **Identity and Access Management** (IAM) systems available in the market:
  - CA SiteMinder and Identity Manager
  - FragleRock OpenIDM
  - IBM Tivoli Identity Manager
  - Novell Identity Manager
  - Oracle Identity manager
  - Microsoft Forefront Identity Manager

The logo for Tivoli software, featuring the word "Tivoli." in white on a red rectangular background, followed by the word "software" in a black sans-serif font.The logo for OpenIDM, with "OpenIDM" in orange and grey text, a grey cube icon to the right, and the tagline "Initiate - Validate - Perpetuate" in small black text below.The logo for Microsoft Forefront Identity Manager, featuring a green and white globe icon, the text "Microsoft®" in small font, and "Forefront Identity Manager" in a larger black font.The logo for CA technologies, with the tagline "agility made possible™" in blue above the stylized "ca" logo in blue and green, with "technologies" in green below.The logo for Oracle Identity Management, featuring the word "ORACLE®" in red above a horizontal line, and "IDENTITY MANAGEMENT" in black below.The Cisco live! logo, with "Cisco" in grey and "live!" in a blue, stylized font.

# Why Do We Need SAML 2.0?

- Single Sign-On across domains
- Cookies prevent the need for reauthorisation
- SSO interoperability (before SAML little)
- Web Service Security (SAML allows for the exchange of assertions within a SOAP document)
- Federated Identity (consolidate identities across organisational boundaries)





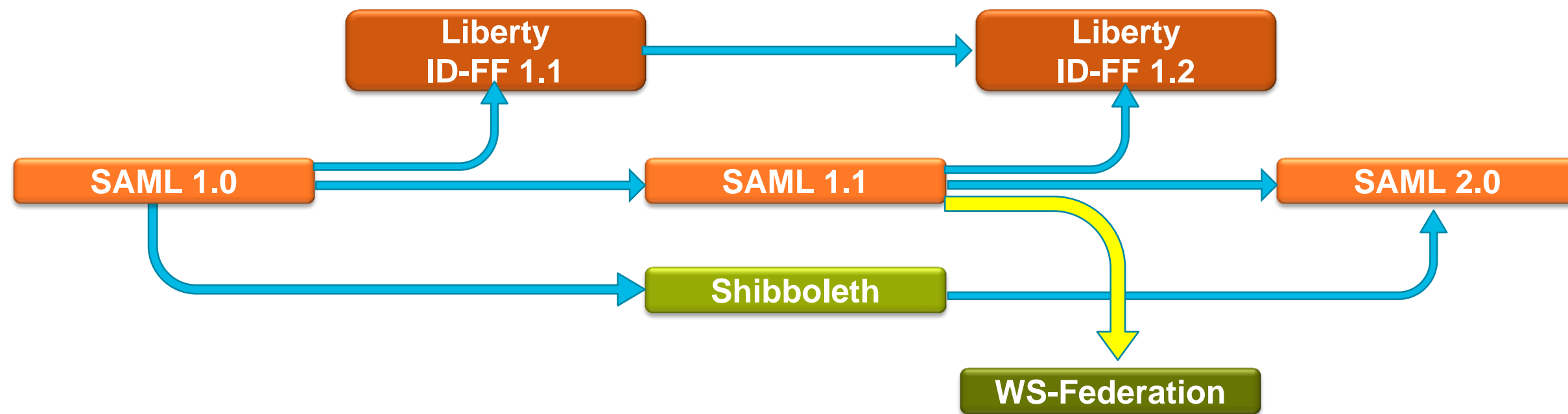
# SAML (Security Access Markup Language) 2.0

The SAML standard is managed by the OASIS Security Services Technical Committee



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

SAML is a protocol specification to use when two servers need to share authentication information. Nothing in the SAML specification provides the actual authentication service...

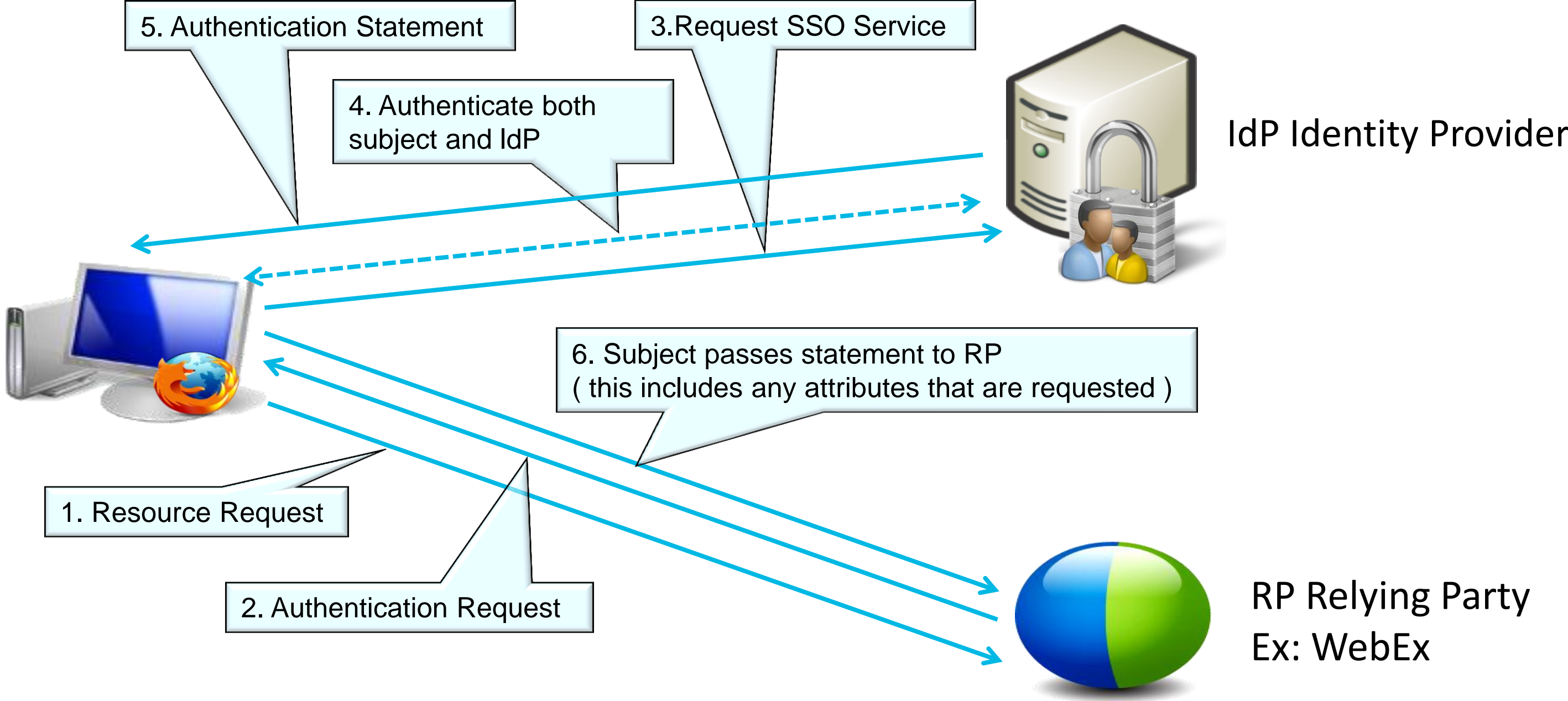


2002

2005



# SAML 2.0 Flow

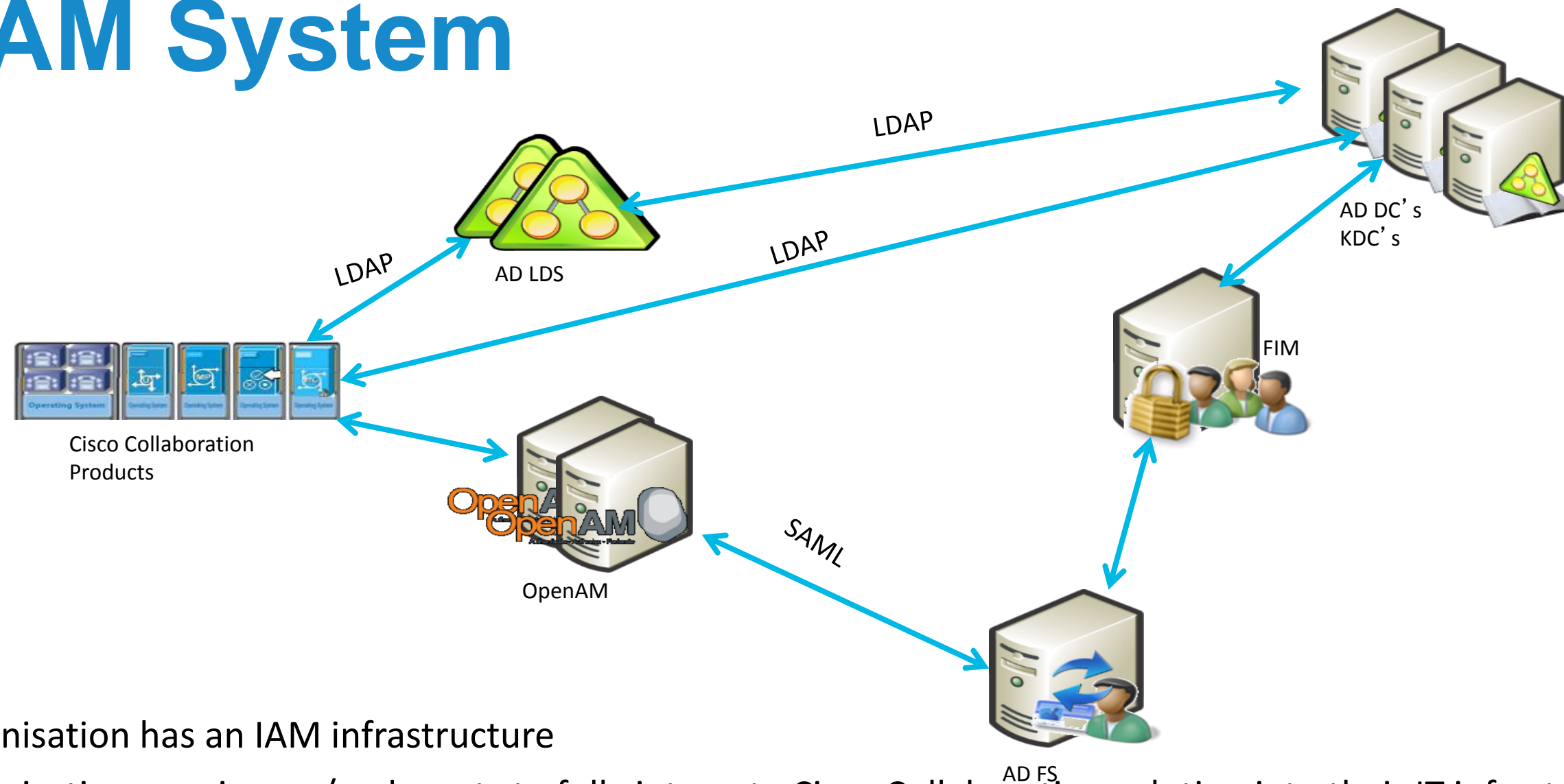


# Federations Mechanisms Supported by OpenAM

- OpenAM supports several open federation technologies including the Security Access Markup Language (**SAML**) versions 1 and 2, **WS-Federation**, and the Liberty Alliance Project Identity Federation Framework (**Liberty ID-FF**).
- **SAML** Standard for passing credentials between different Internet domains that have their own authentication systems.



# When the Organisation Already has an IAM System



Organisation has an IAM infrastructure

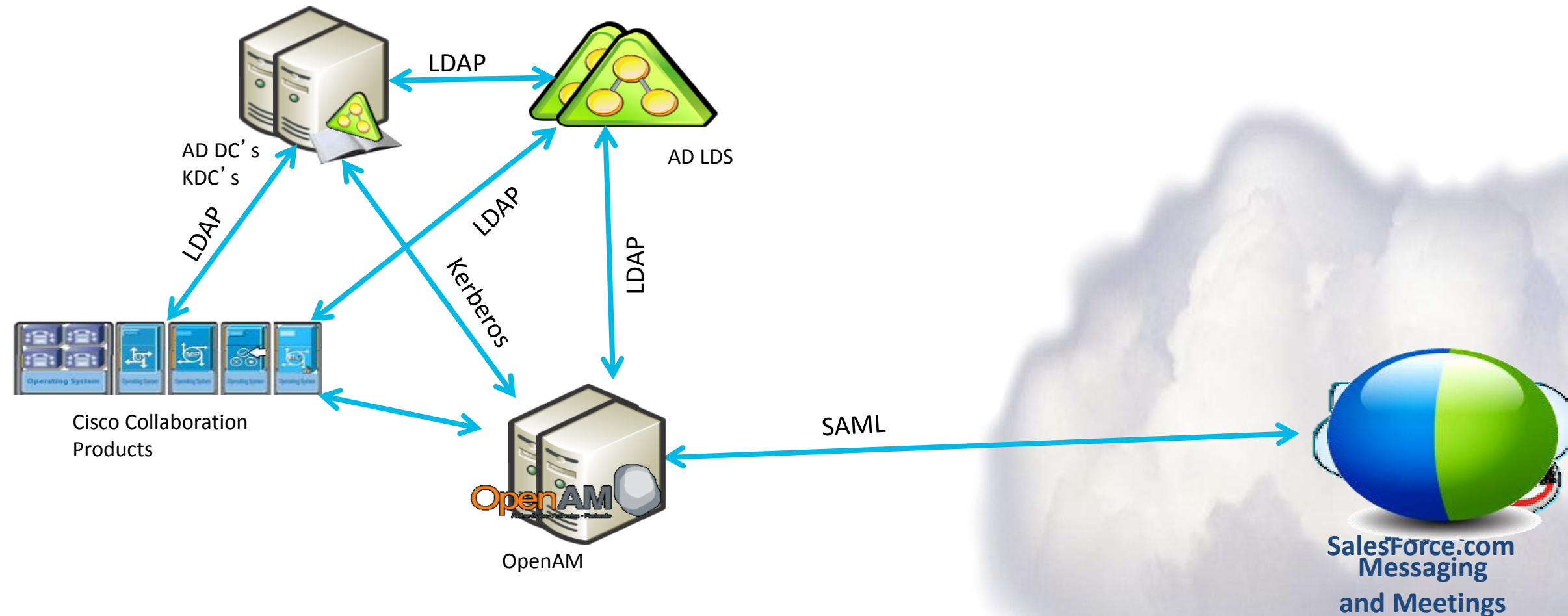
Organisation acquires or/and wants to fully integrate Cisco Collaboration solution into their IT infrastructure

First step is to have a common user database

In some organisations it isn't possible to get the information directly from AD DC so we need to use an LDAP frontend

For Single Sign-On, OpenAM can federate with the IAM system

# When the Customer Needs to Extend SSO to a Cloud Service



Organisation enables SSO for Cisco on-Premise Collaboration Products

In some organisations it isn't possible to get the information directly from AD DC so we need to use an LDAP frontend

OpenAM needs to have its own user database gathered from the LDAP frontend

OpenAM federates with cloud services like Salesforce.com using SAML

Apart from the authentication, SAML can also populate cloud services like Webex with user information, so there isn't a need to add users twice ( on-premise and cloud )

# Populating WebEx with User Information

- Auto Account Create (only needed if automatic user creation is required)
  - Requires “firstname”, “lastname”, “uid”, and “email”
  - Users are assigned the default session type / policy action
- Auto Account Update (only needed if automatic user information update)
  - Requires “updateTimeStamp”
  - Users accounts will be updated when the “updateTimeStamp”
  - value is incremented
  - Only values passed in the assertion will be updated

The screenshot displays the 'Site Administration' page for WebEx, specifically the 'SSO Configuration' section. The left sidebar contains navigation links for Home, Manage Site, Manage Users, Session Types, Assistance, and Log out. The main content area is titled 'SSO Configuration' and includes a 'Federated Web SSO Configuration' section. Key settings visible include: Federation Protocol set to SAML 2.0; SSO Profile with 'SP Initiated' selected; Target page URL Parameter set to TARGET; WebEx SAML Issuer (SP ID) as https://uc8sev7lab13.webex.com; Issuer for SAML (IdP ID) as https://sso.cisco.com:8443/opensso; Customer SSO Service Login URL as https://sso.cisco.com:8443/opensso/SSO; NameID Format set to Unspecified; and AuthnContextClassRef set to urn:oasis:names:tc:SAML:2.0:ac:classes... At the bottom, there are checkboxes for 'Single Logout', 'Auto Account Creation', 'Auto Account Update', and 'Remove uid Domain Suffix for Active Directory UPN'. Red arrows point to the 'Auto Account Creation' and 'Auto Account Update' checkboxes, which are both checked.

# Limitations of SAML Integration with WebEx

VERSION  
User: amAdmin Server: sso.cisco.com  
OpenAM

General Services Group

Edit User - Carla Carvalho Save Re

First Name: Paulo Jorge  
\* Last Name: Correia  
\* Full Name: Paulo Jorge Correia  
Password: Edit  
Email Address: paucorre@cisco.com  
Employee Number:  
Telephone Number: 1111  
Home Address:  
\* User Status:  Active  Inactive  
Account Expiration Date:  
Format: mm/dd/yyyy hh:mm  
User Authentication Configuration:  Administration  AllDomains  [empty]  IdapService

- Users cannot sign in if they have been deactivated by the Identity Provider (IdP) or “Federation Server”, therefore accounts cannot be deactivated with SSO
- When accounts have been deactivated by the IdP, then the accounts will no longer be granted access, but these accounts will be still be “active” in “Centres” and WebEx Connect until they have been deactivated by a Site Admin

# Key Takeaways and Q&A



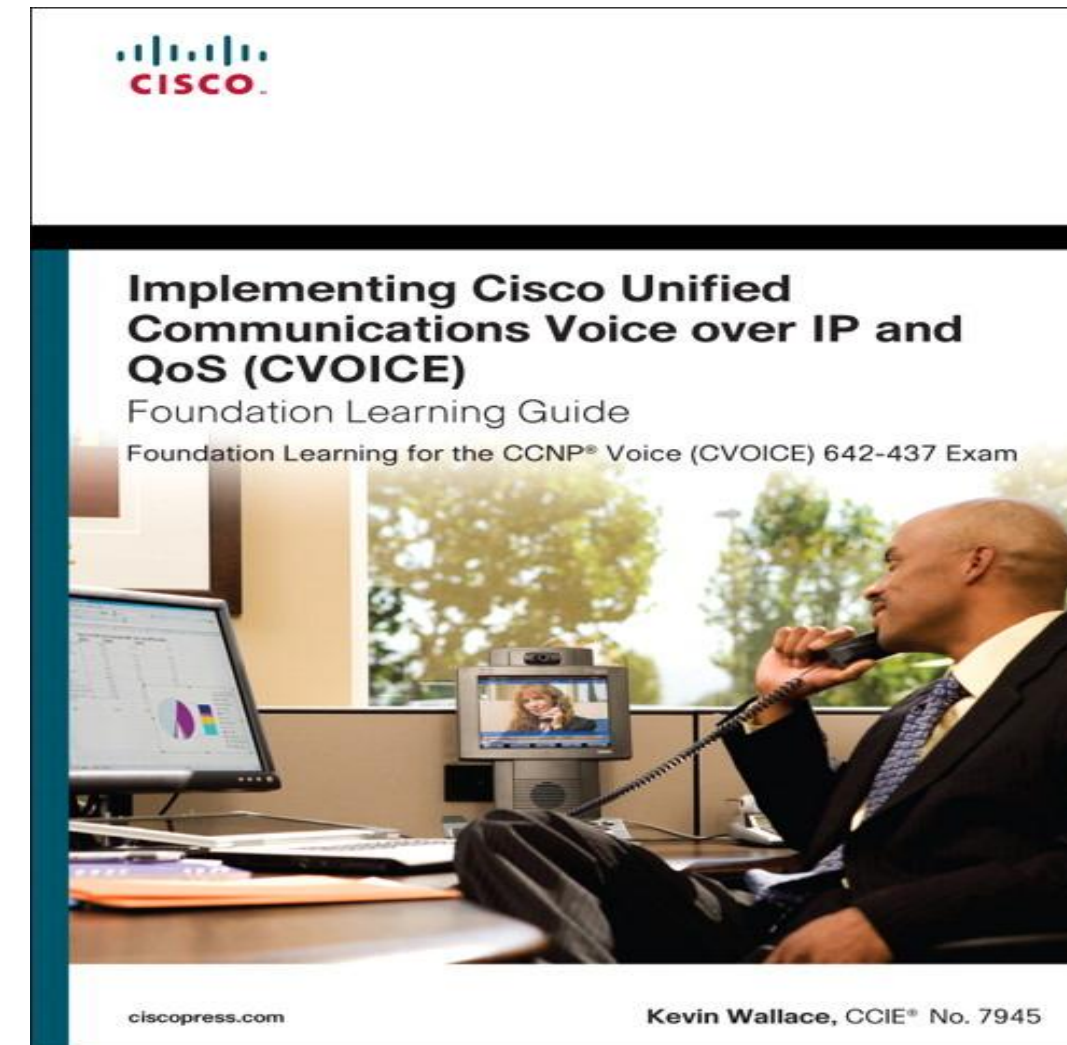
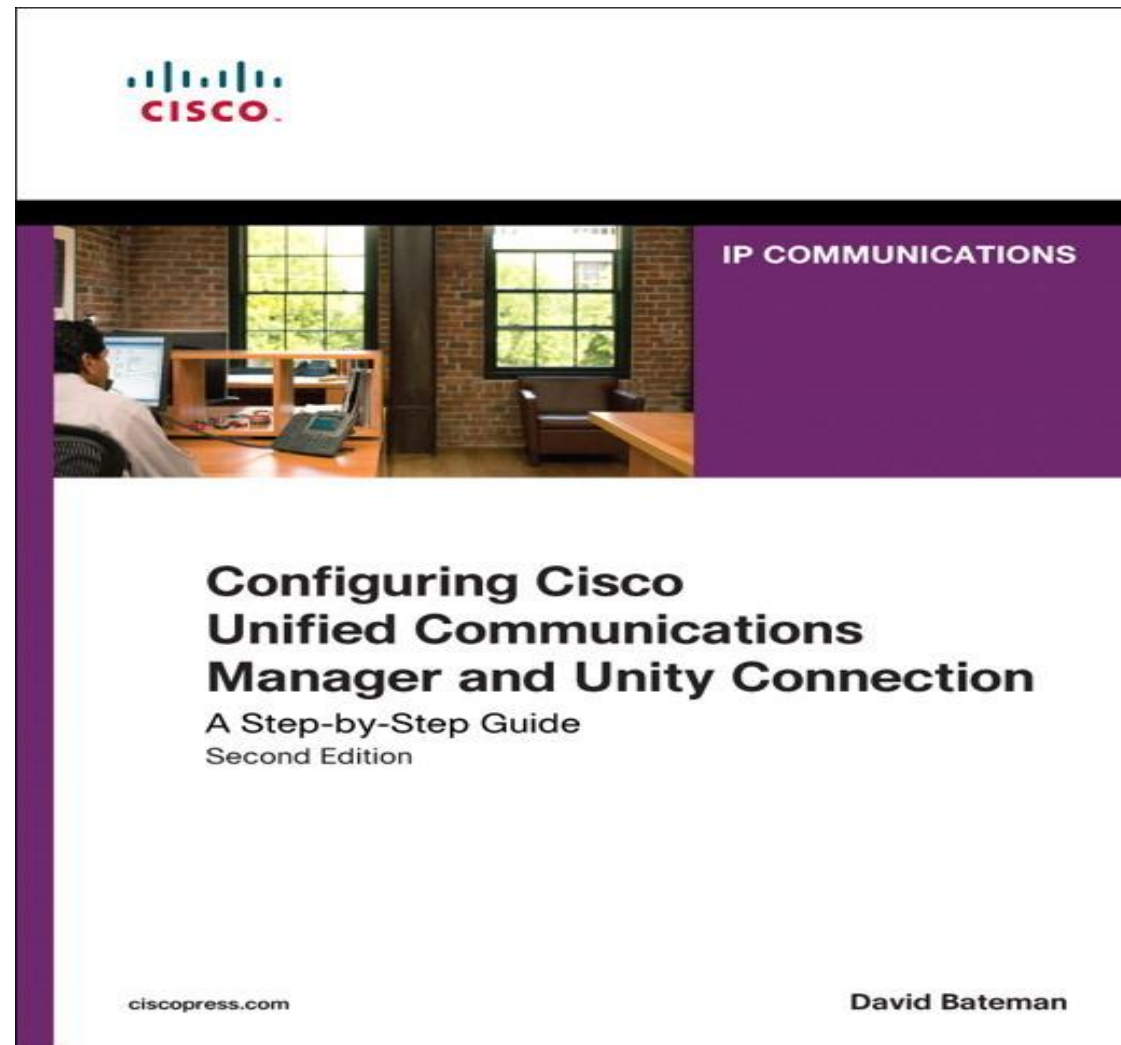


# Key Takeaways

- Directory and A&A services should be carefully considered when planning a collaboration project
- Cisco is building an open, Web 2.0 based interface that will allow consolidation of user directory information into a single location.
- There are multiple options to support SSO when the organisations have multiple AD domains, tree, forest. A decision must be taken based on the needs and security policy of the organisation.
- If there is already an Identity and Access Management system inside the organisation the collaboration solution should integrate with it.
- Every organisation is considering cloud to complement or replace the on-premise services and that should not be a show stopper for an integrated directory and Single Sign-On Strategy

# Recommended Reading

BRKUCC-2664



# Q & A



# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

[www.ciscoliveaustralia.com/portal/login.wv](http://www.ciscoliveaustralia.com/portal/login.wv)

Cisco *live!*

