



*TOMORROW  
starts here.*

Cisco *live!*



# Providing Single Signon (SSO) with Enterprise Identity Services and Directory Integration

BRKUCC-2664

Paulo Jorge Correia

Technical Solutions Architect

#clmel

Cisco *live!*

# Agenda

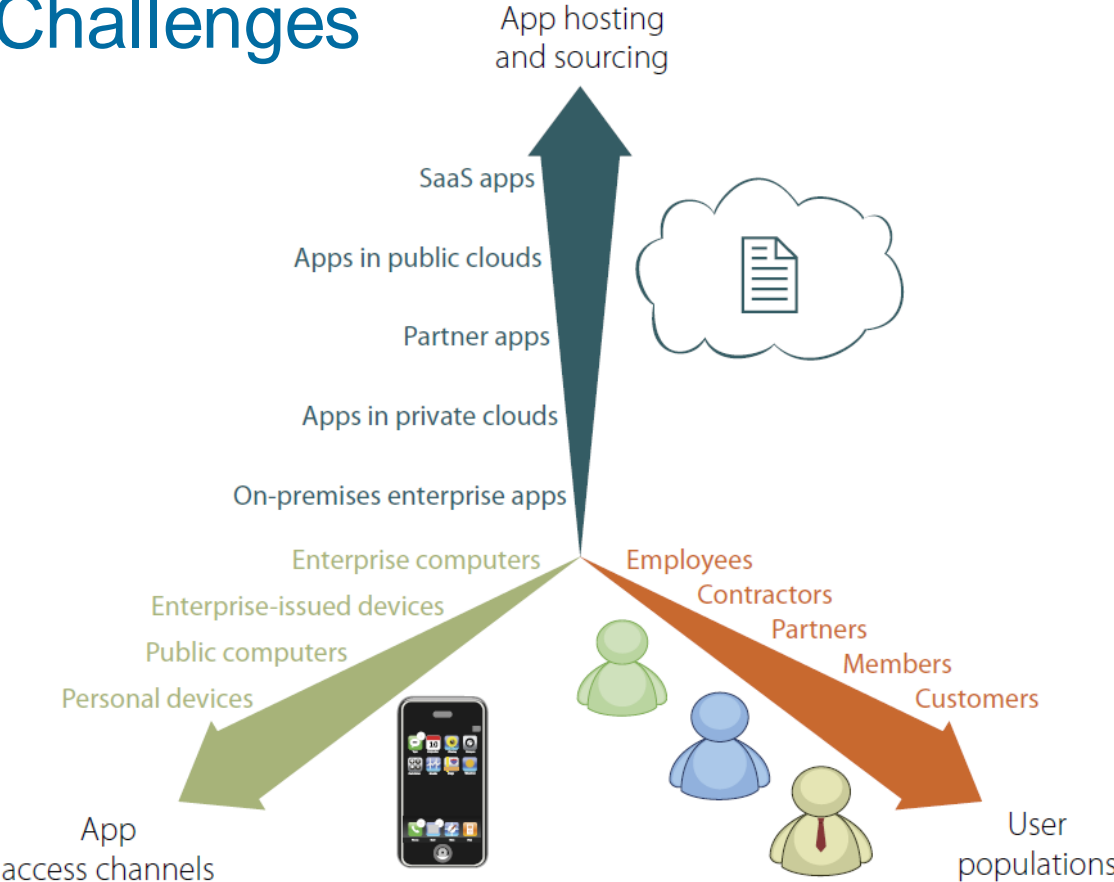
- Identity Challenges and Market analysis
- Identity Technologies and Components
- SAMLv2 Protocol Deep Dive
- OAuth Protocol
- How cookie/tokens work?
- Cisco Collaboration Common Identity Architecture
- User perception for authentication
- Identity in Customer Private Cloud
- Single Sign-On for Jabber
- Identity in Cisco Public Cloud
- Key Takeaways



A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern urban landscape is visible, featuring a prominent pedestrian bridge with blue lighting and several tall buildings with illuminated windows. The overall scene is a blend of dynamic light and static architectural elements.

# Identity Challenges and Market Analysis

# Identity Challenges



Source : Forrester Research, Inc.



# Summer of Fun 2012

Company	Attack	Number of Identities	Mitigation
Apple	Matt Honan – Wired – hacked using forgotten password and Amazon services resulting full press expose on Wired, Industry press	1+	Two factor authentication and security questions now deployed
Dropbox	Employee account compromised and file containing customer emails was stolen. User's with same password were compromised using posted lists.	200+	Two factor authentication now offered, password aging rules, risk based authentication
LinkedIn	6.5 Million password hashes stolen from DB and 100K+ released on web. LinkedIn sued for \$5M by users but trial thrown out based on privacy policy and inability to prove user was harmed materially	6.5 million password hashes	Email sent to all users to reset passwords, HTTPS used across entire site,
Twitter	Hacker announces White House bombed. The stock market dropped 150 points & \$136B market value. AP, Guardian and 60Minutes Twitter account compromised via a phishing attack in which a user was tricked into handing over a password.	Three– AP, The Guardian & 60 Minutes	Two factor authentication now offered -

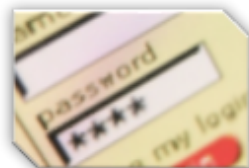
# Need For Strong Authentication

Additional identification steps significantly increases security

- Username and passwords are no match for today's sophisticated hackers
- Solution is easy to deploy and easy to use... ensuring user adoption
- Strong Authentication strengthens identity and access security by combining two or more identifiable elements



**Something you  
HAVE**



**Something you  
KNOW**



**Something you  
ARE**

A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a modern pedestrian bridge with a glass railing and blue lighting spans across the street. In the background, several tall buildings are lit up with various colors, including blue and purple. The overall scene is vibrant and dynamic.

# Identity Technologies and Components



# Which protocols do we see in SSO today?

**SAML** is a set of standards that have been defined to **share information about who a user is**, what **his set of attributes are**, and give you a way to grant/deny access to something or even request authentication. Two different organisation want to establish trust relations without exchanging passwords

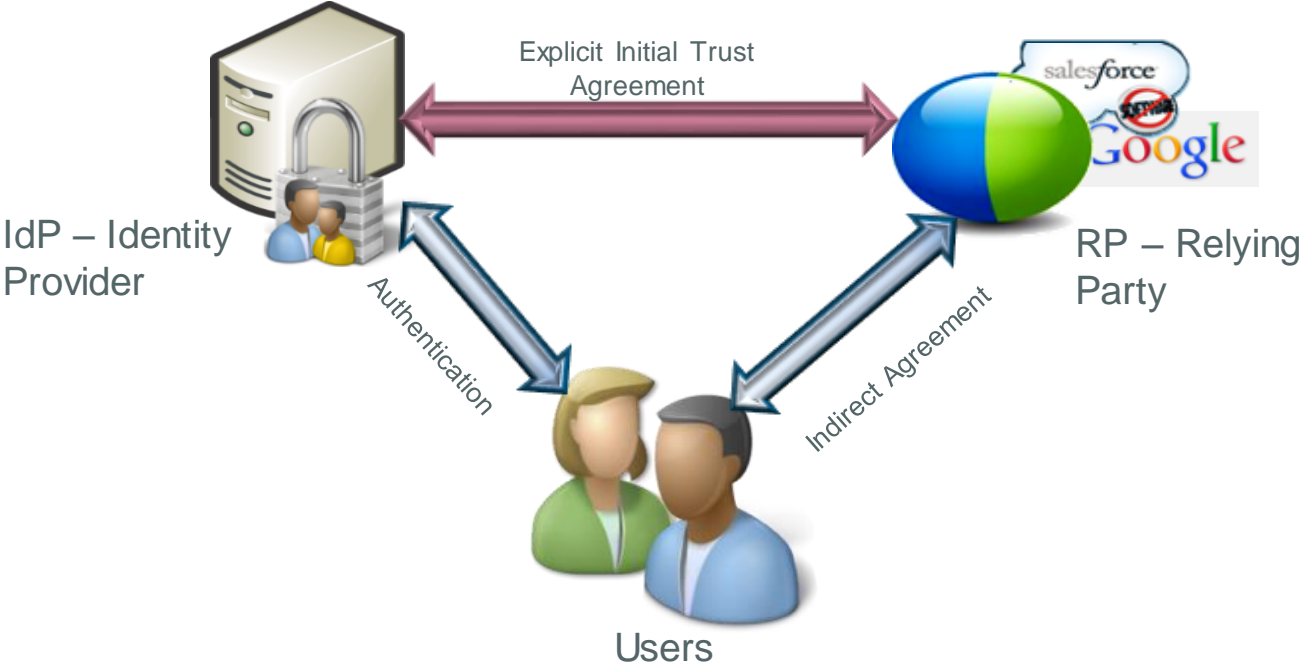


**OAuth** is more about **delegating access to something**. You are basically allowing an **application to impersonate you**. It is used to grant access to API's that can do something on your behalf. For example you want to write an application that will use other applications like twitter, Gmail and Google Talk.



Cisco *live!*

# Identity Framework



# Authentication and Authorisation (AuthN and AuthZ)

The process of **authorisation** is distinct from that of **authentication**. Whereas authentication is the process of verifying that "you are who you say you are", authorisation is the process of verifying that "you are permitted to do what you are trying to do".

When you enter a hotel and walk up to reception, the receptionist authenticates you by checking your passport.



Authentication



Paulo

You do not need your passport to enter your room. Your room key authorises you to enter your room only, and not any other rooms. The room key / authorisation token does not identify the holder of the key / token.

Your room key is your authorisation token to enter your room and any resource that you are entitled in the Hotel



Authorisation

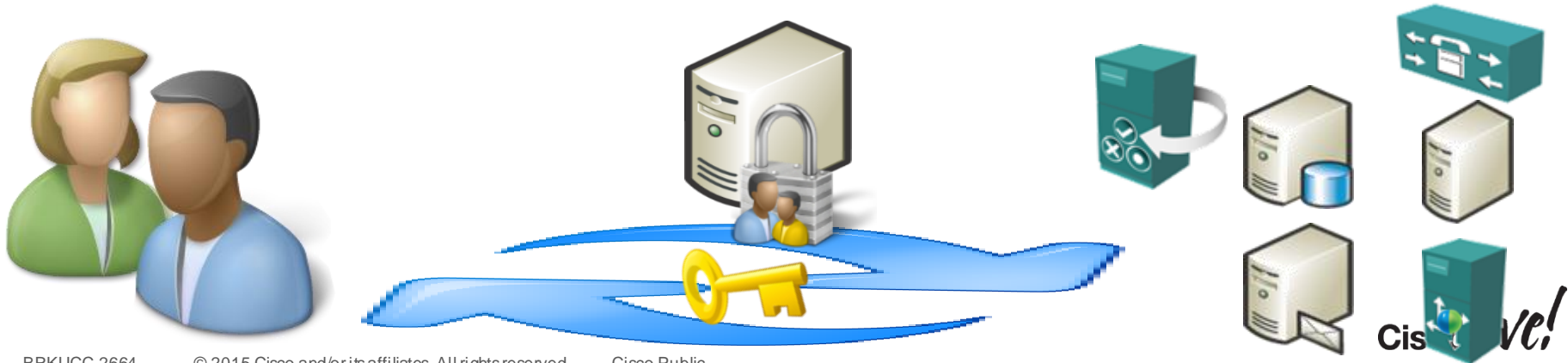


After authentication has taken place, the receptionist gives you a room key.

# Single Sign-On Definition

Single Sign-On (SSO) is a session/user authentication process that permits a user to provide credentials **only once** in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

With SSO the barriers for deploying stronger authentication is much lower.



# Role of Identity Providers (IdP)

## Validate who you are?

- Review personally identifying information to **prove you are who you say you are** (identity proofing), such as drivers license, passport, or biometric data
- Assign **attributes** [(name, role, email address)] in the identity management system.



## **Validate** and **transact** authentication requests?

- Verifying that the person seeking access to a resource is the one previously identified and approved by utilising some form of authentication system, often a username and password.

# Which IdP Does Cisco Supports ?

Cisco supports any IdP vendor that is compliant with the **SAMLv2** Oasis Standard.

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

- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 11.0
- PingFederate 6.10.0.4



FORGEROCK



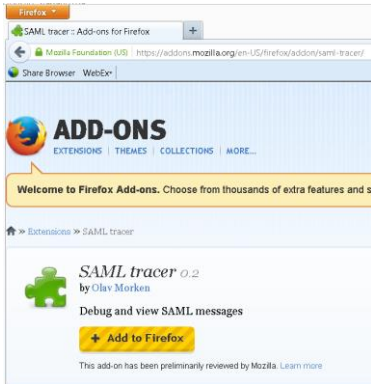
Cisco *live!*

A nighttime photograph of a city street. In the background, there are modern buildings with lit windows and a pedestrian bridge with blue lighting. The middle ground shows a road with traffic lights and some vehicles. The foreground is dominated by long, colorful light trails from moving vehicles, creating a sense of motion and energy. The overall scene is illuminated by city lights, creating a vibrant and dynamic atmosphere.

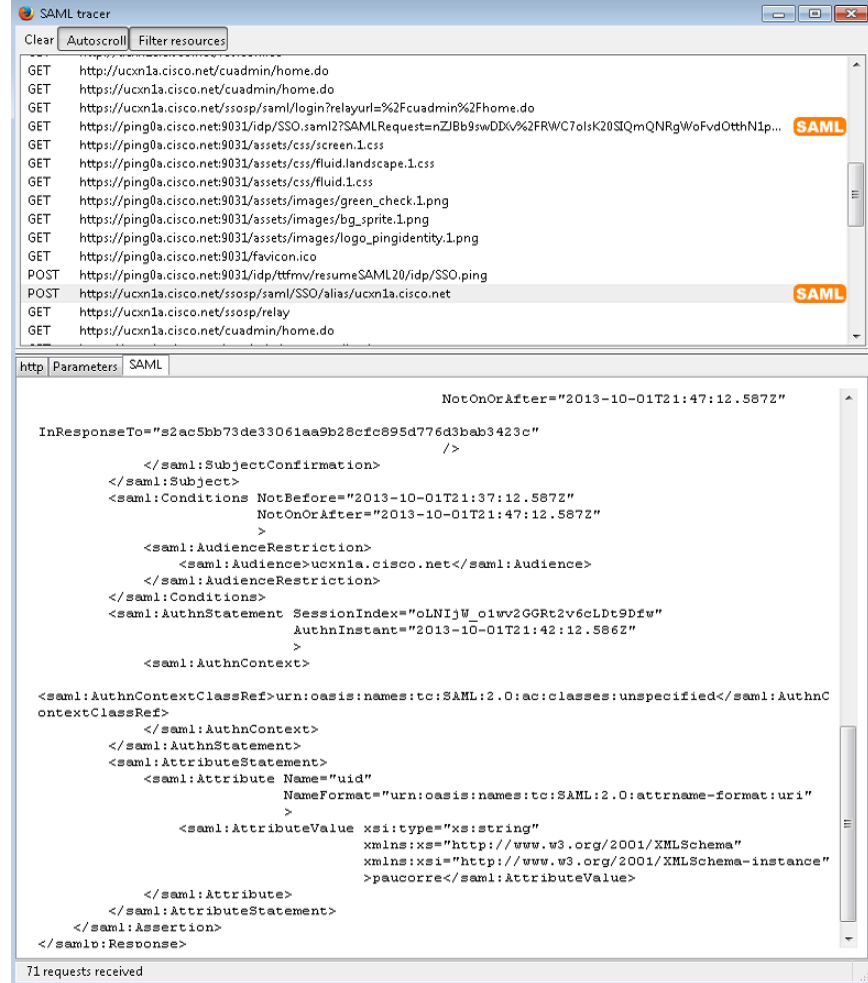
# SAMLv2 Protocol Deep Dive

# Firefox is your friend!

Firefox allow you to have an add-on that can decode SAML called SAML tracer



It allow you to get the flow of your SSO interaction and also decodes SAML



Cisco live!



# SAML 2.0 Flow

## Trust Agreement



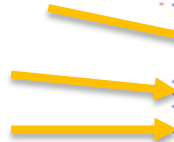
IdP Identity Provider

Metadata Exchange



RP Relying Party  
Ex: WebEx

```
<?xml version="1.0"?>
- <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cisco.net" cacheDuration="PT1440M"
ID="WjLXkLN3oOdbC5hM2wRFvs0dFmM">
- <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:SignedInfo>
- <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
- <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
- <ds:Reference URI="#WjLXkLN3oOdbC5hM2wRFvs0dFmM">
- <ds:Transforms>
- <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
- <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
- </ds:Transforms>
- <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
- <ds:DigestValue>ZKPECQZAZGa2WcrDCBfxFHUhtk=</ds:DigestValue>
- </ds:Reference>
- </ds:SignedInfo>
- <ds:SignatureValue> QZ7d1cLkNe7Jm2qzJCKXfb2+67xPINXgF2ig27wQUsx48TDLMk0B98DxuaXd8AugzWnWu6XzD
q/VcANr6L1nW2wkrk8m1krG41VlXkjH9qqY41aydCUpiJfF2/wHb/pGrtrEDKEYDzhz4Jtn 2aRAT7F869NFSAXGecQ=
- </ds:SignatureValue>
- </ds:Signature>
- <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
- <md:KeyDescriptor use="signing">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:X509Data>
- <ds:X509Certificate>MIICoCCAaSAgAwIBAgIGAUB49FUUMA0GCSqSIB3DQEBBQUAMGExCzAJBgNVBAYTAIVLMQ8wDQYJKoZIhvcNAQELBQADggEBAQ
- </ds:X509Certificate>
- </ds:KeyInfo>
- </md:KeyDescriptor>
- <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
- <md:SingleSignOnService Location="https://pingba.cisco.net:9031/ldp/SSO.saml2"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
- <md:SingleSignOnService Location="https://pingba.cisco.net:9031/ldp/SSO.saml2"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
- <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="uid"/>
- <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="email"/>
- <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="lastname"/>
- <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="firstname"/>
- <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="updateTimeStamp"/>
- </md:IDPSSODescriptor>
- <md:ContactPerson contactType="administrative">
```



```
<?xml version="1.0" encoding="UTF-8"?>
- <md:EntityDescriptor entityID="http://www.webex.com" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
- <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true"
AuthnRequestsSigned="false">
- <md:KeyDescriptor use="signing">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:X509Data>
- <ds:X509Certificate>
MIIB4TCCAUqgAwIBAgIGARzFN9prMA0GCSqSIB3DQEBBQUAMQcXzAJBgNVBAYTAIVTMSUwIwYDVQQDEExxZXZ
- </ds:X509Certificate>
- </ds:KeyInfo>
- </md:KeyDescriptor>
- <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
- <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
- <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
- <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:entity</md:NameIDFormat>
- <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
- <md:AssertionConsumerService isDefault="true" index="0" Location="https://cas.webexconnect.com/cas/SAML2AuthService?
org=uc8sevtlab14.com" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
- </md:SPSSODescriptor>
- <md:Organization>
- <md:OrganizationName xml:lang="en">Cisco WebEx</md:OrganizationName>
- <md:OrganizationDisplayName xml:lang="en">Cisco WebEx</md:OrganizationDisplayName>
- <md:OrganizationURL xml:lang="en">
- </md:Organization>
- <md:ContactPerson contactType="technical">
- <md:Company>Cisco WebEx</md:Company>
- <md:GivenName/>
```

# SAML 2.0 Flow

## Resource Request



1. Resource Request



IdP Identity  
Provider

http

```
GET http://cucm3a.cisco.net/ HTTP/1.1
Host: cucm3a.cisco.net
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

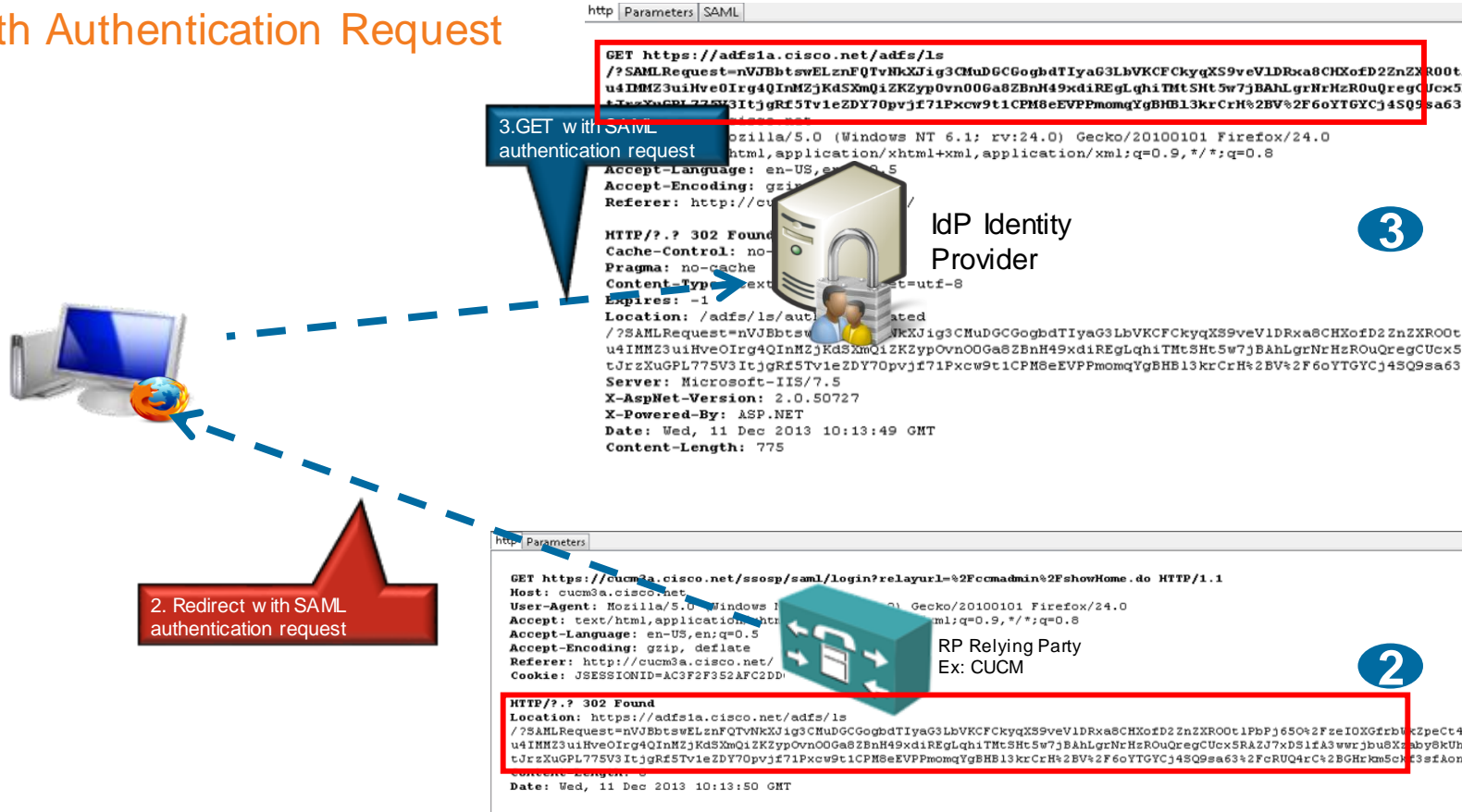
HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=AC3F2F352AFC2DDC195F51F2F90781BC; Path=/; HttpOnly
Content-Type: text/html;charset=utf-8
Content-Length: 4621
Date: Wed, 11 Dec 2013 10:13:42 GMT
```



Ex: CUCM

# SAML 2.0 Flow

## Redirect with Authentication Request



# SAML 2.0 Flow

## Redirect with Authentication Request

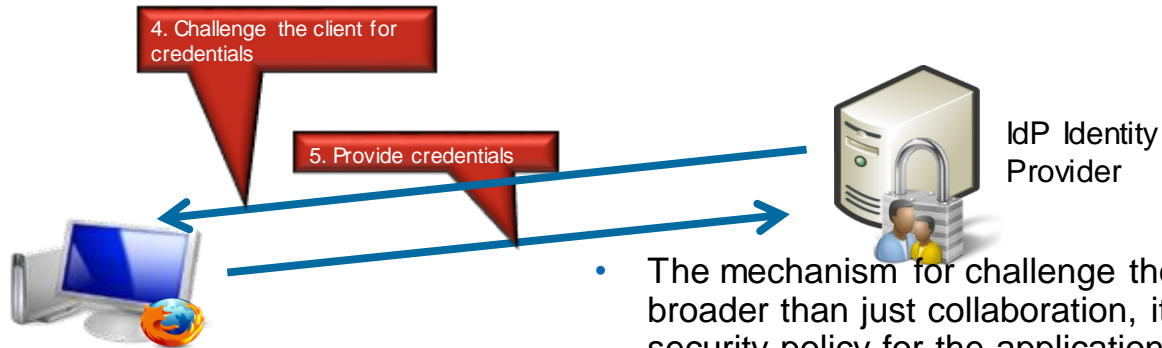


```
http Parameters SAML
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s25a73d7ca51230aaa02a5aea868354d31d4fde567"
  Version="2.0"
  IssueInstant="2013-12-11T10:13:50Z"
  Destination="https://adfs1a.cisco.net/adfs/ls/"
  ForceAuthn="false"
  IsPassive="false"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  AssertionConsumerServiceURL="https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a.cisco.net"
  >
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">cucm3a.cisco.net</saml:Issuer>
  <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
    SPNameQualifier="cucm3a.cisco.net"
    AllowCreate="true"
    />
</samlp:AuthnRequest>
```

3

# SAML 2.0 Flow

## Identify the User



- The mechanism for challenge the users is something broader than just collaboration, it should comply to the security policy for the application in the organisation

4 5

- Any authentication mechanism, single or multi factor, supported by the IdP will be supported by the collaboration applications





A long-exposure photograph of a city street at night. The image shows a wide road with a pedestrian bridge in the background. The street is filled with light trails from cars, creating a sense of motion. The buildings in the background are lit up, and there are several flags on poles on the left side. The overall scene is vibrant and dynamic.

# OAuth Protocol

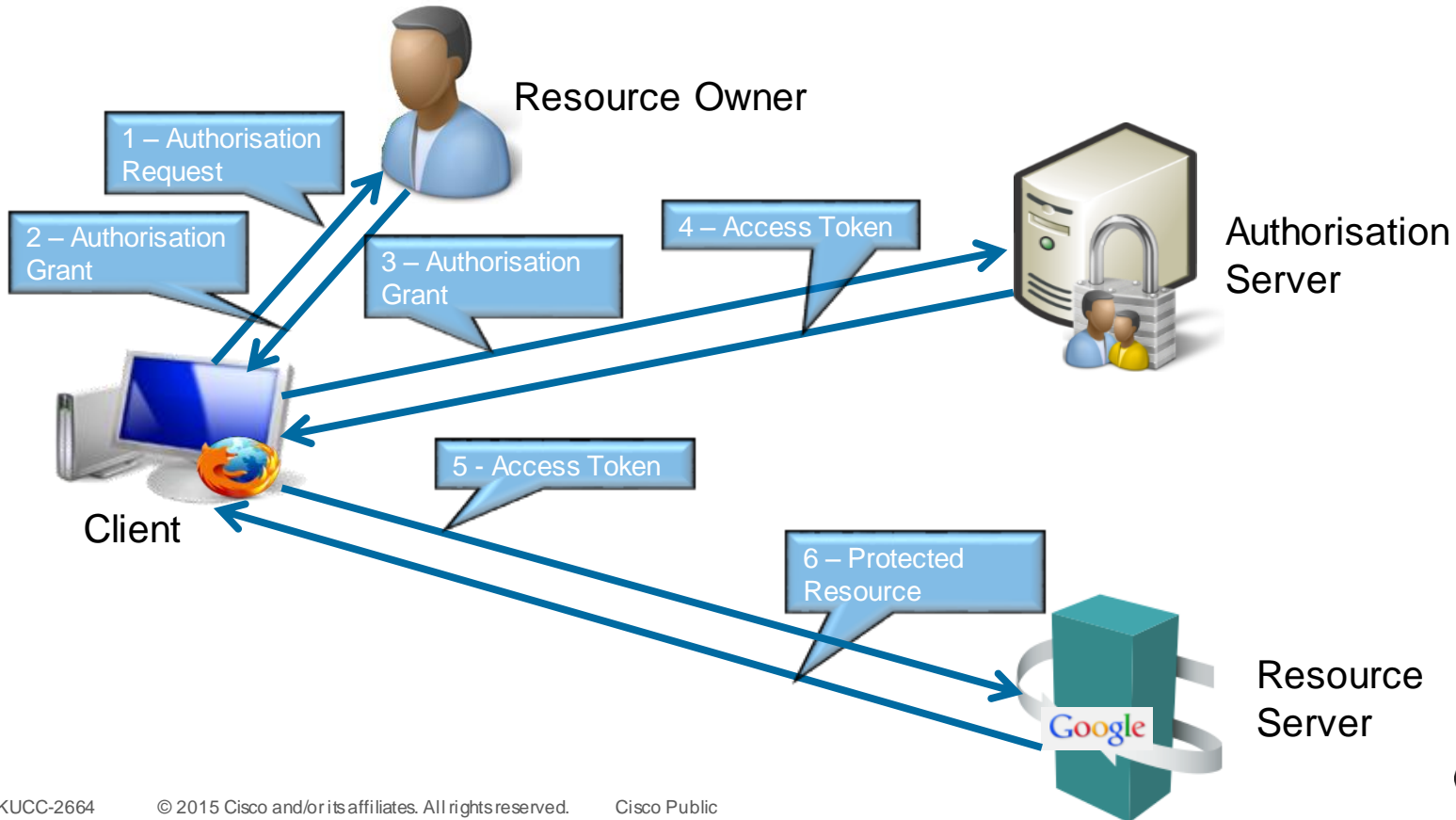


# OAuth 2.0

- The OAuth 2.0 **authorisation protocol** enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.
- It is an Authorisation protocol
  - **Valet key concept**
  - Eliminate the need for web sites to ask for passwords when you are accessing to your information.
  - The resource owner authorise a client to access to resources in a server
  - Client can be web app, desktop/phone app, JS in browser



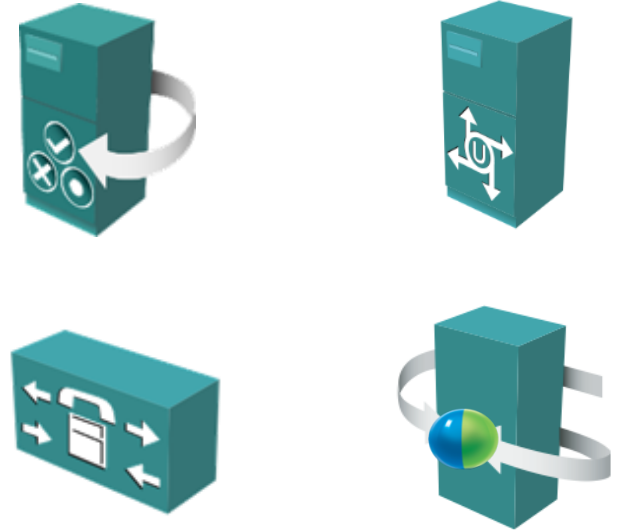
# OAuth 2 Flow



# Why we need OAuth in Cisco collaboration products?

Jabber clients need to access to non-HTML services and  
Avoid overloading the IdP with SAML requests

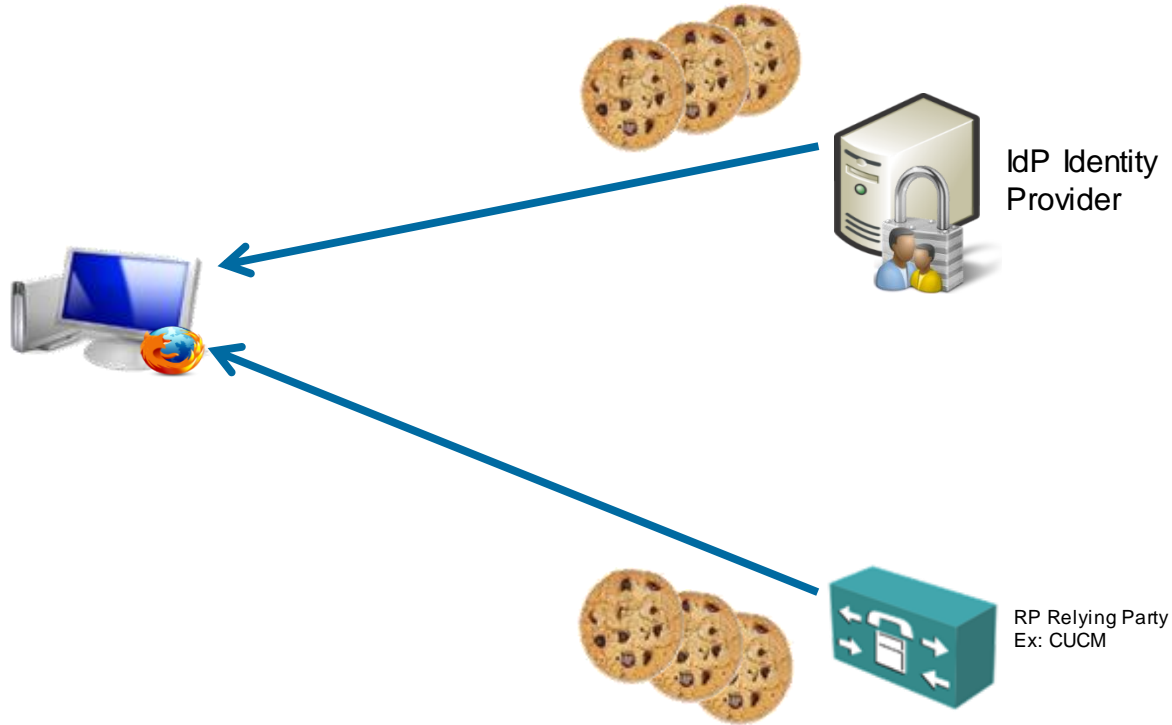
- CUCM UDS
- CUCM CTI
- CUCM SIP
- IM&P SOAP
- IM&P XMPP
- UCxN VMRest



A nighttime photograph of a city street with light trails from cars. In the background, there are modern buildings with lit windows and a pedestrian bridge. The foreground is dominated by long, curved light trails in yellow, orange, and red, suggesting a long exposure of traffic. A semi-transparent black banner is overlaid across the middle of the image, containing white text.

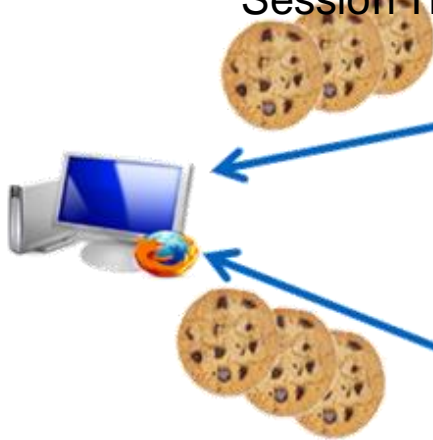
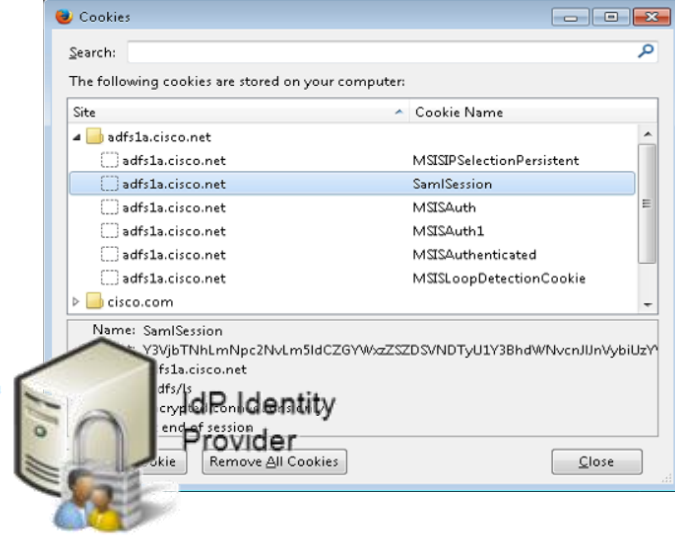
How cookie/tokens work and why they prevent re-authentication?

# SAML Cookies to Prevent Re-authentication

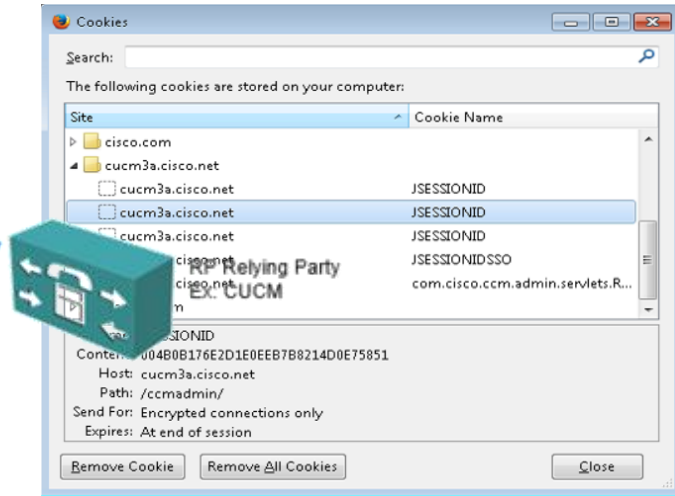


# SAML Cookies to Prevent Re-authentication

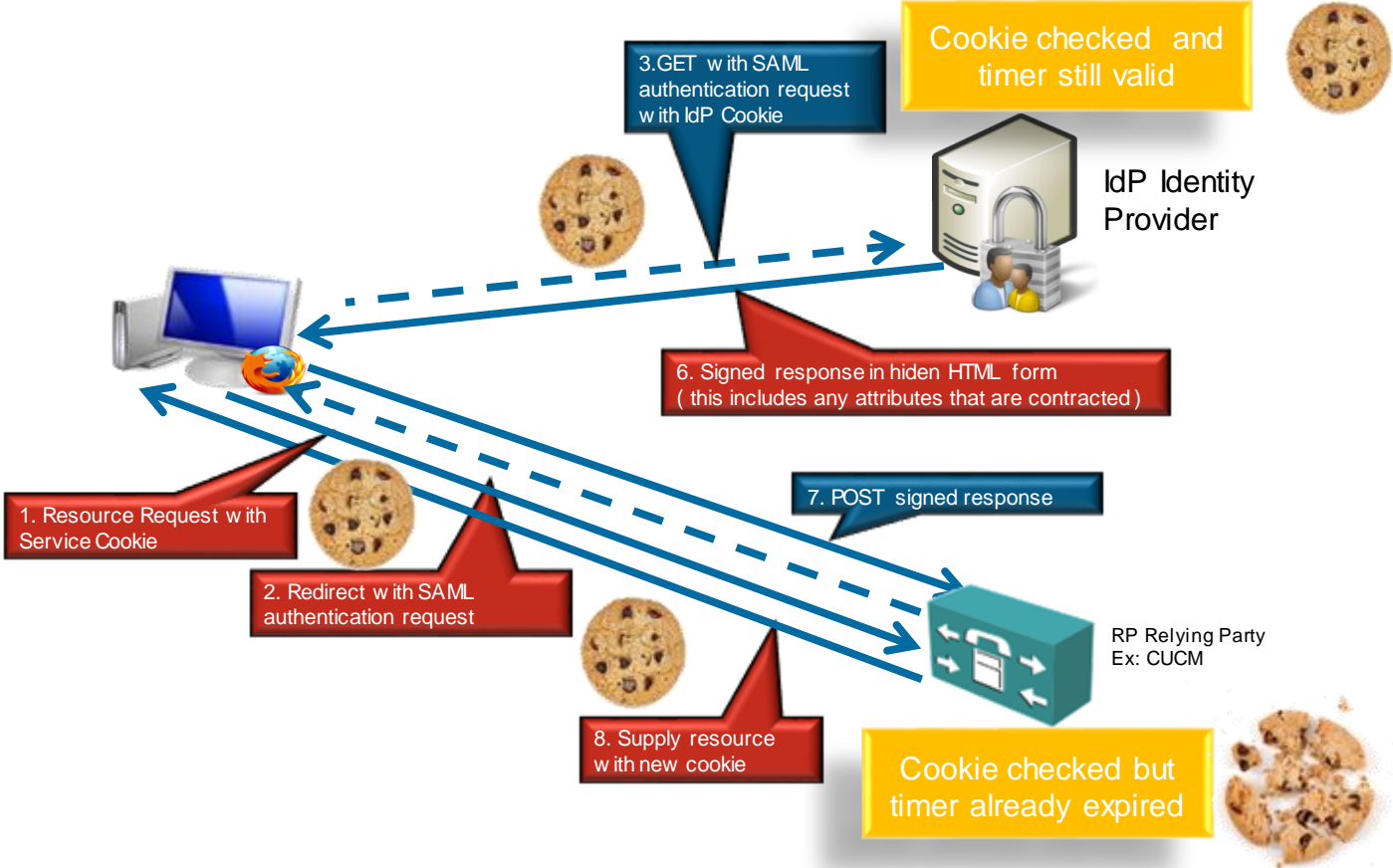
**IdP Cookie** -> our recommendation for the Session Timer is 48 hours



**Service Cookie** -> Our recommendation for the Session Timer is 30 minutes



# SAML 2.0 Cookies to Prevent Re-authentication



# Type of Cookies

## Session Cookies

- Are limited to a single browser instance (i.e. jabber)
- Cookie does not survive exiting jabber and cannot be used by any other browser session while jabber is running
- Typically this type of session requires IDP login at every jabber launch

## Persistent Cookies

- Persistent cookies are available to all instances of a given browser (i.e. jabber and platform browser, Internet Explorer, Safari or Chrome)
- Logging into other apps prior to jabber may mean jabber does not require an IDP login

## Cookie Realm (OpenAM)

- OpenAM IDP support realms. These are essentially persistent cookies, but only shared between certain applications



Cisco *live!*

# OAuth Tokens

**OAuth Access Token:** A token that authorises a bearer to access a protected resource. An Access Token is issued by the Authorisation service to an OAuth Client.

Access Tokens are typically issued to a **particular user** with a **particular scope** and with a **specific expiry time**.

**OAuth Refresh Token:** A token that an OAuth Client can use to request a new Access Token on expiry of an existing Access Token.





# Durations for Tokens and Cookies

If the Application SAML session timer is bigger than the 75% of the duration of the OAuth token, then there will never be a re-authentication request to the IdP.

SSO Configuration	
<a href="#">OAuth Token Expiry Timer</a> *	<input type="text" value="60"/> 60
<a href="#">Redirect URIs for Third Party SSO Client</a>	<input type="text"/>

```
172.16.36.109 - PuTTY
login as: admin
admin@172.16.36.109's password:
Command Line Interface is starting up, please wait ...


Welcome to the Platform Command Line Interface

VMware Installation:
 1 vCPU: Intel(R) Xeon(R) CPU E7- 2860 @ 2.27GHz
Disk 1: 80GB, Partitions aligned
4096 Mbytes RAM


admin:set webapp session timeout ?
Syntax:
set webapp session timeout minutes

minutes mandatory The number of minutes after which sessions are declared to be
invalid; range is 5 to 35000.


admin:set webapp session timeout 50
```



**IdP Cookie**  
Timers recommended are :  
8 hours for Idle timeout  
48 hours for Absolute timeout



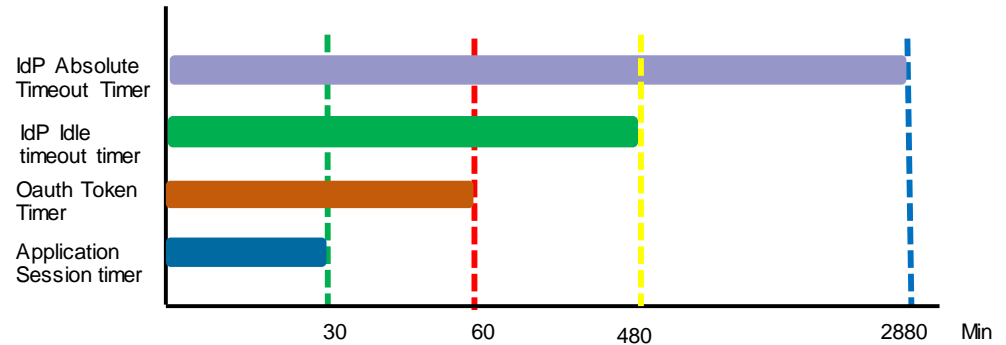
**Application Cookie**  
Timer default 30 minutes



**OAuth Token**  
Timer default 60 minutes

# Durations for Tokens and Cookies

- The IdP Idle timeout timer, if exists, needs to be larger than 75% of the OAuth timer, or re-authentication happen every time a request arrives to the IdP



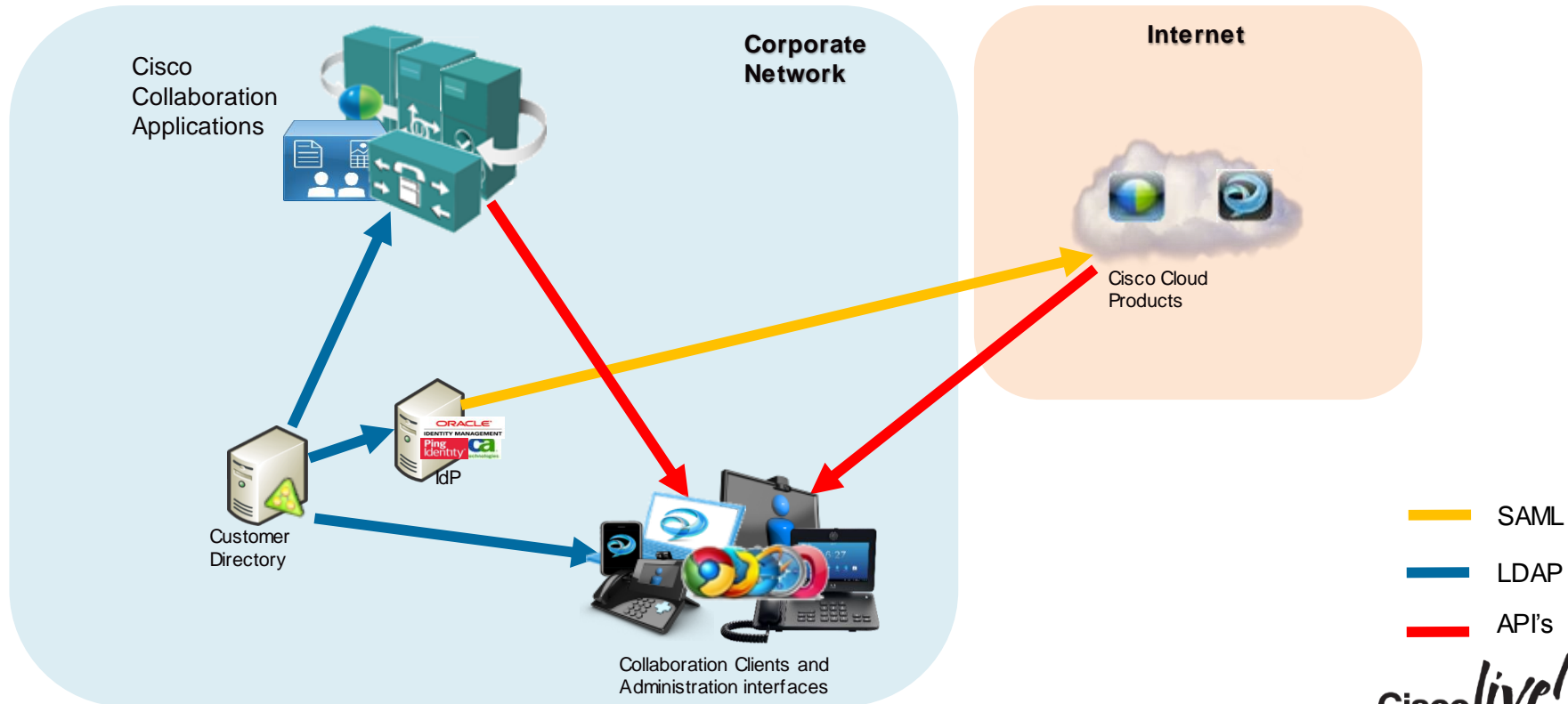
- When Jabber is active and IdP idle timeout is larger than 75% of the OAuth timer than re-authentication will only happen at the IdP Absolute timeout timer

A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with a glass railing spans across the street. The background features several modern buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

# Cisco Collaboration Common Identity Architecture

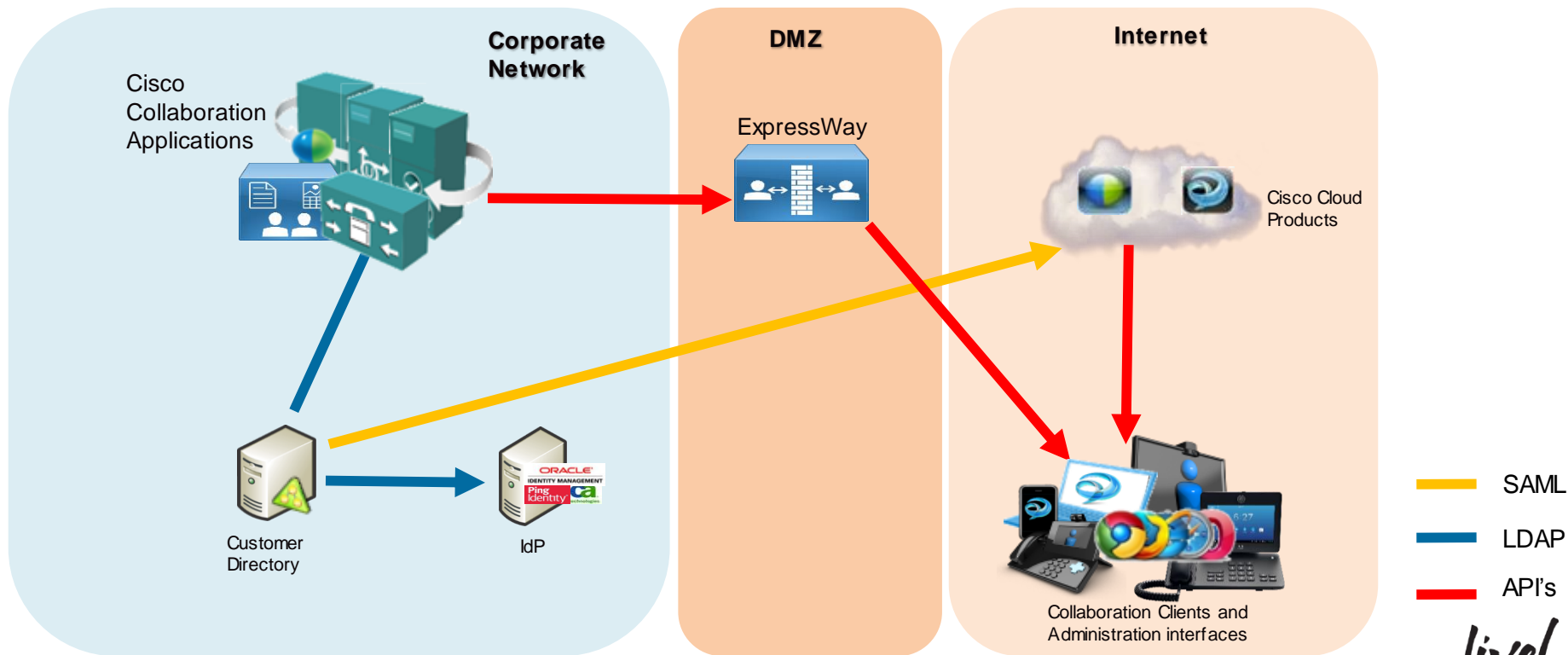
# Cisco Collaboration Identity System Release 10.X

User Attributes access when clients are inside the customer network



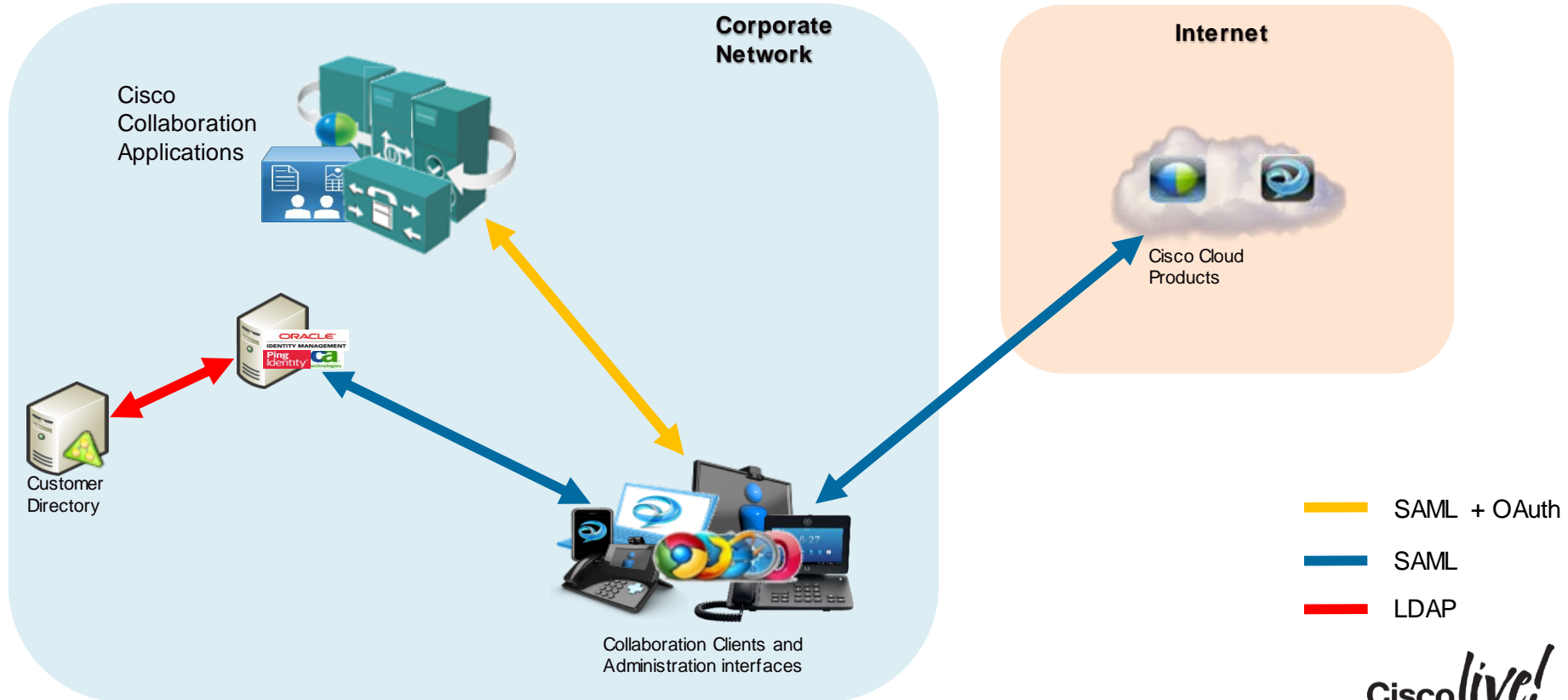
# Cisco Collaboration Identity System Release 10.X

User Attributes access when clients are outside the customer network



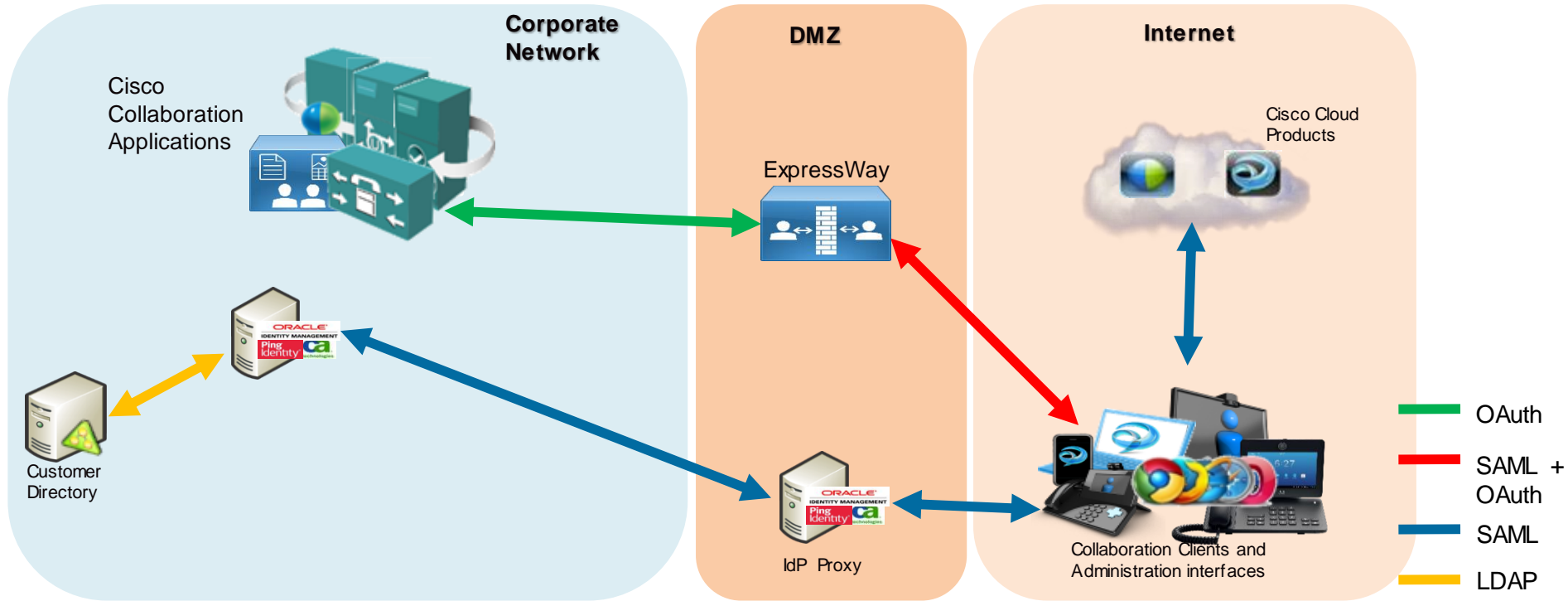
# Cisco Collaboration Identity System Release 10

Single Sign-On when clients are inside the customer network



# Cisco Collaboration Identity System Release 10

Single Sign-On when clients are inside the customer network



# What end goal for the Common Identity Architecture?

**Common Identity  
Services**

**Single Contact  
Store**

**Single Identity  
Store and Sync**

**Aligned Contact /  
Directory API**

**Single SAML  
SSO Mechanism**

**Single OAuth  
Authorisation  
Token Mechanism**



A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with blue lighting spans across the street. In the background, there are several tall buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights.

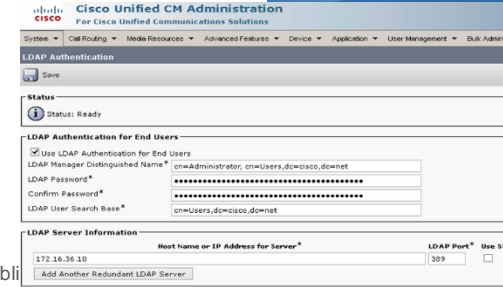
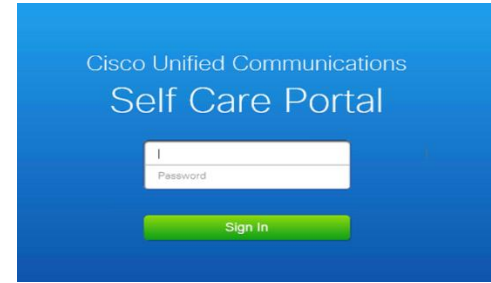
# User perception for authentication with different mechanisms

# Minimum Expected in any Deployment

- There is a single source for user information in the organisation, that is the corporate LDAP
- All Cisco application get the authentication from same source, Customer corporate LDAP.
  - Any authentication request is done though an LDAP bind to the corporate directory.
  - CUCM and Unity Connections need to have LDAP Authentication configured.

## User Experience

- User provides the same corporate password as the rest of the non-UC applications.
- Most of the Cisco UC apps have the option to save the password, the user will only prompt for it again when corporate password is changed.
- Authentication process isn't shared between applications.



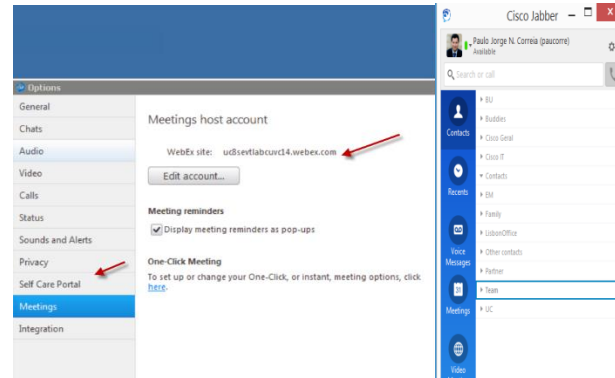
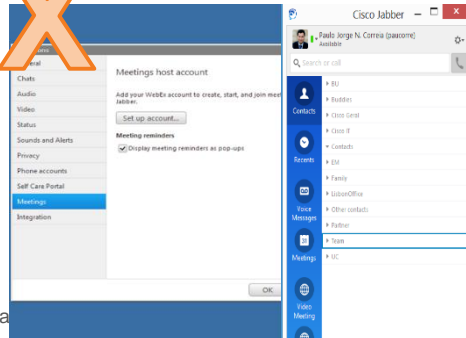
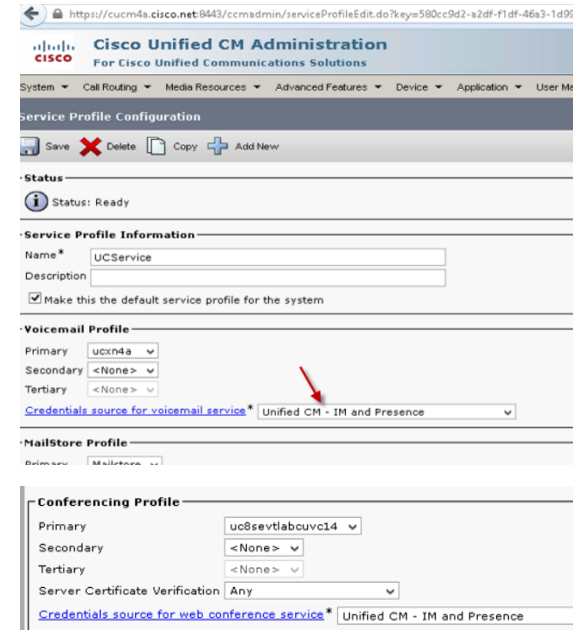
CiscoLive!

# On Premise Jabber Optimisations

- Jabber consumes services from different Cisco Applications ( CUCM, connections, Webex ) .
- We can configure the service profile to use the same login credentials for connecting to all the Cisco Applications.
- For WebEx meeting Centre or CWMS you need to make sure use the same user credentials as CUCM

## User Experience

- After the change of corporate password or at first login only Jabber login credentials will be needed, no need to provide password in the Jabber Options



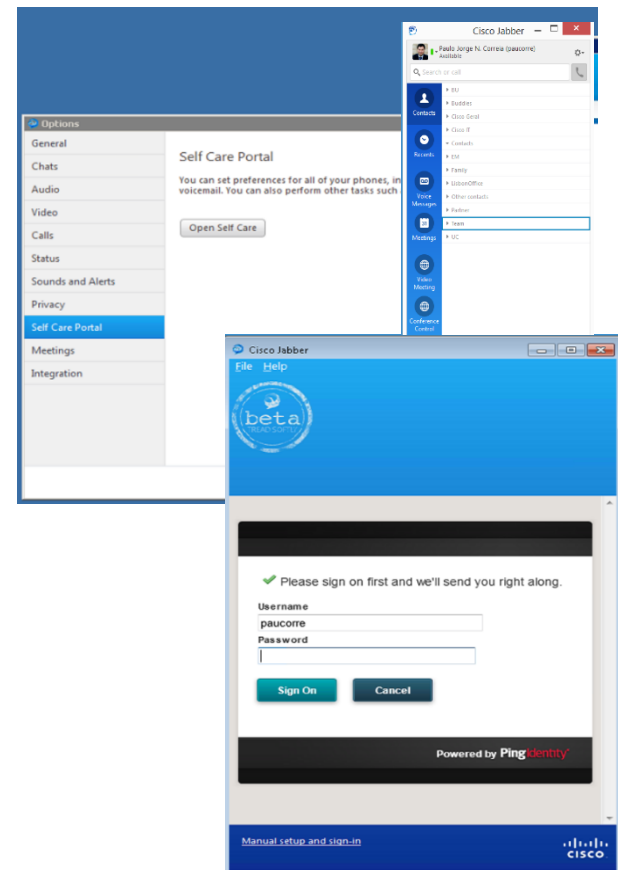
Cisco live!

# What SSO with username/password authentication will bring us?

- It will require the deployment of an IdP, it will check username and password from corporate directory, most of them uses LDAP bind.
- As side effect delivers auto provision and update of WebEx products
- The User experience of the Form can be customised in most of the IdP's

## User Experience

- Cross launch in the same browser session of other apps without the need for re-authenticate.
- Very agnostic experience supporting any kind of device and operating system

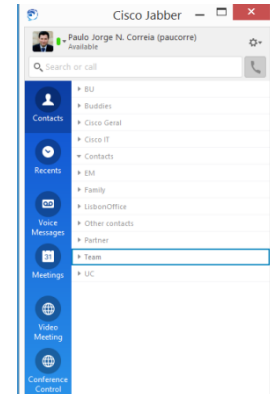
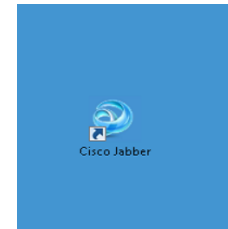
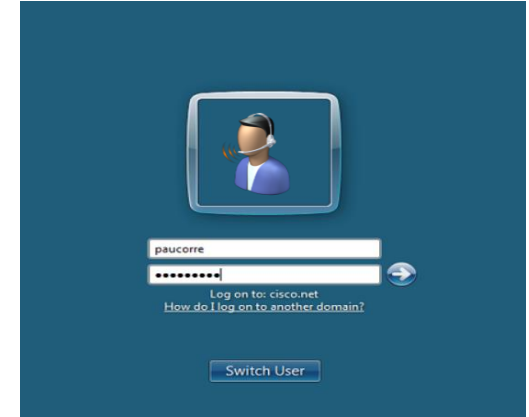


# What SSO with Kerberos authentication will bring us ?

- Customer is only looking for Jabber for Windows, Mac or iOS
- Customer is not going to use outside the corporate firewall.
- The users login to their PC, Mac or iOS device that is part of a AD Domain.

## User Experience

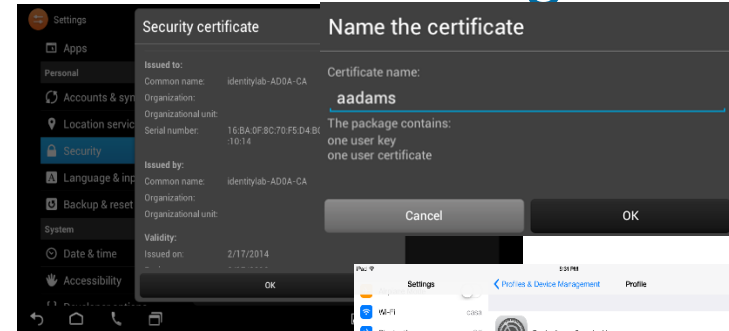
- It's just magic credentials aren't asked at all, since it relies on initial windows login.
- If credentials are changed in AD there isn't any need to provide new credentials to the Collaboration clients



**CiscoLive!**

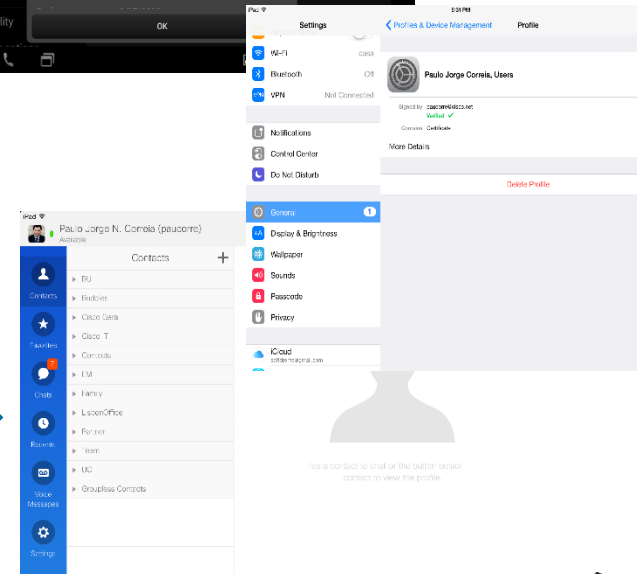
# What SSO with certificate authentication will bring us?

- Will require that the customer uses its own Enterprise CA or buy certificates from a public CA.
- Specially useful for deployment in mobile devices that run Cisco Collaboration applications, assuming the customer already owns and has MDM that will help in the certificates deployment.
- Since we use WebView on mobile devices there is a limitation where the certificate store isn't accessible before Android LE
- Apple still doesn't allow for WebView to access to the certificate store



## User Experience

- It's just magic credentials aren't asked at all.
- If credentials are changed in AD there isn't any need to provide new credentials to the Collaboration clients



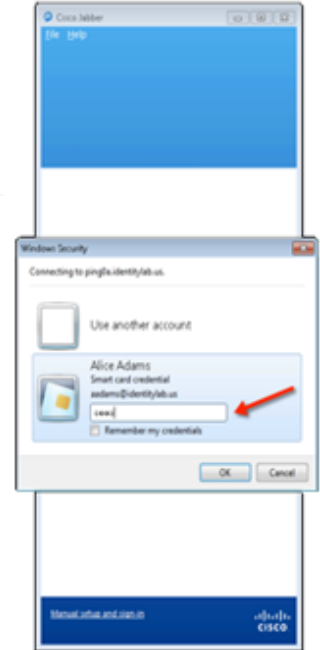
Cisco live!

# What SSO with SmartCards authentication will bring us?

- Most secure way of providing authentication, but requires the OS capabilities of “read” the smartcards.
- Smartcard isn't much different from certificate authentication, major difference is that the certificate isn't local to the device but it is store in the smartcard itself.
- Another difference is that a smartcard solution always use two factor authentication, and needs a PIN, password or pass phase for the second factor authentication.

## User Experience

- A Pin/Password/Pass Phrase needs to be provided for the second factor authentication.
- If credentials are changed in AD nothing changes in the normal login process of the user.
- Most use mechanism for two factor authentication



# Recommendation for Jabber for Windows

## Simple Authentication

- Most of the customer that what to deliver SSO in Windows platform always want to use Kerberos
- When outside the corporate network and can't reach the Kerberos KDC then a fallback to username/password is the most common use authentication mechanism.



## Strong Authentication

- A lot of customers uses smartcards
- Other customers will use One Time Passwords as the main method or as a second factor authentication





# Recommendation for Jabber for Mac

## Simple Authentication

- Most of the customer will use simple username/password to connect their Mac's
- We might see in some more structured organisation when they have a mix of Mac's and PC's that the Mac is also integrate into a Windows Domain, which means that the Mac's also use Kerberos.



## Strong Authentication

- Most customers will use One Time Passwords as the main method or as a second factor authentication



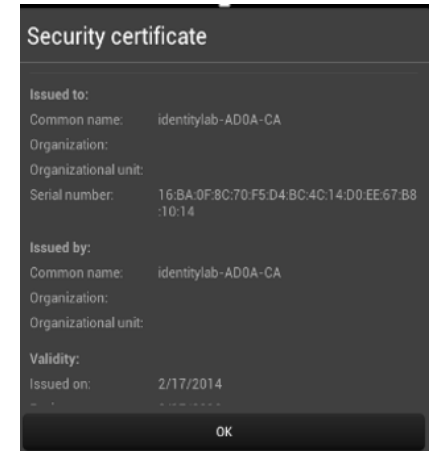
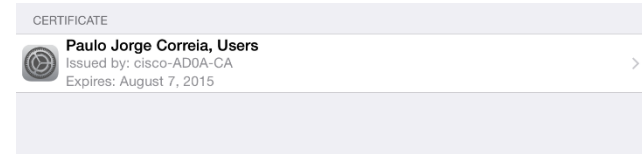
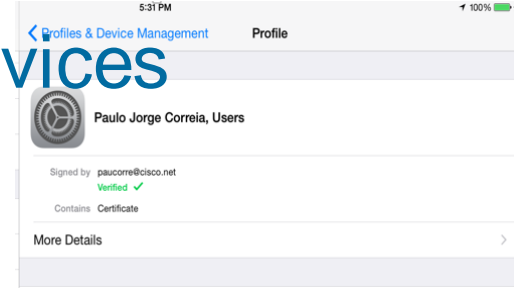
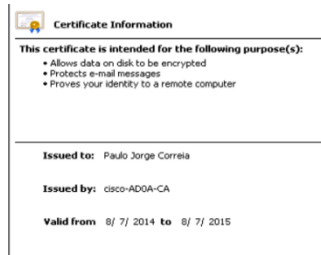
# Recommendation Jabber for Mobile Devices

## Simple Authentication

- Certificate should be the best option if OS allow and can protect rogue application to have access to them.
- More advance customer might use more advance mechanism like the IMEI of a mobile phone
- The most common use will be username/password

## Strong Authentication

- Most customers will use One Time Passwords as the main method or as a second factor authentication



Cisco live!

# What SSO with selecting different authentication mechanisms based on Device/OS/Client will bring us?

- SAML is a HTTP based which means that all the authentication request to the IdP comes with an User-Agent, based on that user agent we can select different kind of authentication.
- Will remove restrictions that we had on specific some authentication protocols on specific Devices/Operating Systems.
- Best compromise from user experience considering, security and variety of devices that our collaboration clients run on

## User Experience

- Depends what which authentication mechanism is chosen for each device/application

Manage Adapter Selector Instances

Enable Adapter Selector Instances to be applied across connections as authentication policy during SSO processing. Multiple Selector Instances can be applied in the specified order. Map each selector result value to an IdP Adapter Instance or to another Adapter Selector for evaluation of criteria.

Enable Adapter Selection

Fail if No Selection

SELECTOR INSTANCE NAME	SELECTOR RESULT VALUES	INSTANCE
MSIE	No	--None--
	Yes	Kerberos - (Adapter)
DX650	No	--None--
	Yes	Certificates - (Adapter)
AppleDevices	No	--None--
	Yes	HTMLform - (Adapter)
--None--		

DEFAULT ADAPTERS

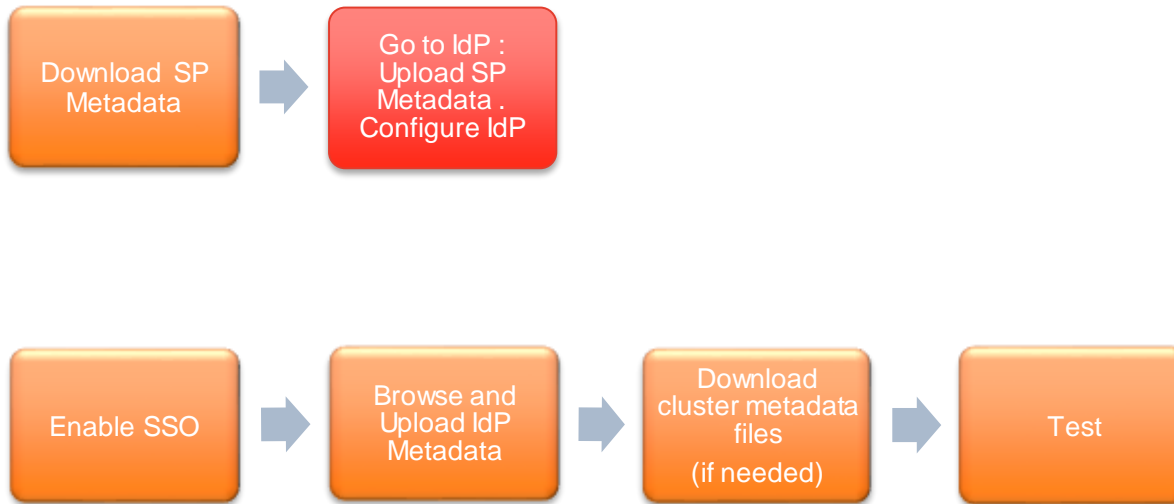
HTTPBasic

--None--



# Identity in Customer Private Cloud

# What Needs to be Configured to Enable SSO in CUCM



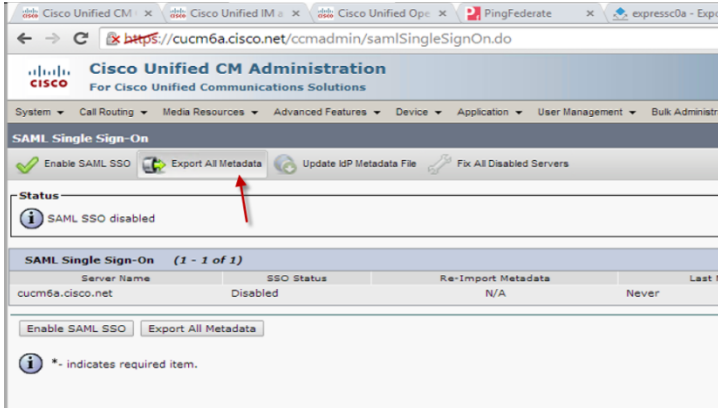
# Enabling SSO in CUCM

## Get the metadata from the SP (CUCM)

Download  
SP  
Metadata

Need to get the metadata from the collaboration products like CUCM, uCXN, IM&P, Prime.

```
</ds:X509Data>  
</ds:KeyInfo>  
</md:KeyDescriptor>  
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>  
<md:AssertionConsumerService index="0" Location="https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a.cisco.net" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>  
</md:SPSSODescriptor>  
</md:EntityDescriptor>
```



This file will provide the **certificates** required to the HTTPS connection to the IdP

This file also provides extra information for SAML to work :

- **NameID** format  
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
- **Location** of the Service  
https://<CUCM FQDN>:8443/ssosp/saml/SSO/alias/<CUCMFQDN>
- What kind of SAML **binding** we are going to use  
SAML 2.0 using HTTP-POST and HTTP-REDIRECT

Cisco live!

# Enabling SSO in CUCM

## Configuring the IdP

Go to IdP :  
Upload SP  
Metadata .  
Configure IdP

Most of the vendors always have two major tasks that together define the agreement between the IdP<->SP:

1. Configuring the IdP part, where we define what authentication mechanism we are going to use.
2. With the metadata xml file that we got from the Cisco Collaboration Product we configure the SP component

INSTANCE NAME	INSTANCE ID	TYPE
ADLDAP	ADLDAP	HTTP Basic IdP Adapter
ADLDAPForm	ADLDAPForm	HTML Form IdP Adapter
ADDC	ADDC	WSA IdP Adapter 3.1

Create New Instance

Name	Entities
<input type="checkbox"/> CUCM	cucm3a.cisco.net saml2 CUCMOpenAM saml2
<input type="checkbox"/> WebEx	CloudOpenAM saml2 uc8sevtlab14 saml2

Name	Protocol	Type
<input type="checkbox"/> CloudOpenAM	SAMLv2	IDP
<input type="checkbox"/> cucm3a.cisco.net	SAMLv2	SP
<input type="checkbox"/> CUCMOpenAM	SAMLv2	IDP
<input type="checkbox"/> uc8sevtlab14	SAMLv2	SP

Connection Type	Connection Role
SP Connection	SP

Browser SSO Profiles	Protocol
true	SAML 2.0

Connection Template	WS-Trust STS
No Template	false

Outbound Provisioning	Browser SSO
false	true

Attribute Query	Patrol's Entity ID (Connection ID)
false	cucm3a.cisco.net

Base URL	Browser SSO
https://cucm3a.cisco.net/843	

SAML Profiles	SP-Initiated SSO
	false

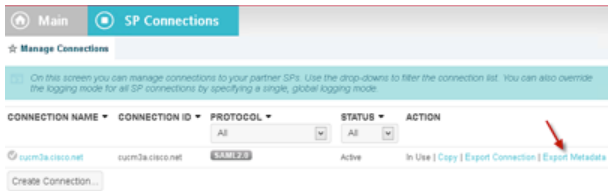
SP-Initiated SLO	SP-Initiated SLO
	false

# Enabling SSO in CUCM

## Export the metadata from the IdP

Go to IdP :  
Upload SP  
Metadata .  
Configure IdP

Similar to what we did in the beginning with the Collaboration Application we are going to export the metadata of the IdP to enable SSO on the SP

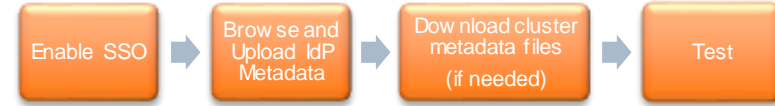


```
<?xml version="1.0"?>
- <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cisco.net" cacheDuration="PT1440M" ID="aokowTgI_0wuqjenv4R63bgM0_P">
  - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      - <ds:Reference URI="#aokowTgI_0wuqjenv4R63bgM0_P">
        - <ds:Transforms>
          - <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          - <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>HIRFe4NPMLK52+mKGOzDJZWBw</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>gX3JAffic+3Xi0FS/LmqYFDc4XCXqJ8W+TvSt4TpkU17KKDEAJdQqBUMeIfcgAT+oSKEmIv40M7t XGee+CqWFTk0xf21bHo0svcAMAFeVngGRw0he7VjYa1uvk8:
      YMKlUVzNvonLx/UzrM8</ds:SignatureValue>
    </ds:Signature>
  - <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    - <md:KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
          <ds:X509Certificate>MIIC0zCCAa5gAwIBAgI GAUB49IFUMA0GCSqGSIB3DQEBBQUAMGEExCzAJBgNVBAYTAIVLMQ8wDQYDVQQIEWZMb25kb24xZDzANBgNVBACTBkxvbmFm
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
      <md:SingleSignOnService Location="https://ping0a.cisco.net:9031/ldp/SSO.saml2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:SingleSignOnService Location="https://ping0a.cisco.net:9031/ldp/SSO.saml2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-format:uri" Name="uid"/>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-format:basic" Name="SAML_AUTHN_CTX"/>
    </md:IDPSSODescriptor>
    - <md:ContactPerson contactType="administrative">
      <md:Company>Cisco</md:Company>
      <md:GivenName>Paulo</md:GivenName>
      <md:SurName>Jorge Correia</md:SurName>
    </md:ContactPerson>
  </md:EntityDescriptor>
```



# Enabling SSO in CUCM

## Going through the wizard



1. Import the IdP metadata
2. Download the Metadata from all node is the cluster if needed
3. Run the Connection test

The image shows three sequential screenshots of the Cisco Unified CM Administration web interface during the SSO configuration wizard:

- Step 1: Identity Provider (IDP) Metadata Trust File** - The user has selected a metadata file at `C:\Users\Administrator\EMEAR\Downloads\metadata.xml` and clicked "Browse". The status indicates "IdP Metadata has been Imported to servers in this cluster".
- Step 2: Download Trust Metadata File Set** - The user has clicked "Download Trust Metadata File Set". A warning icon indicates that the file must be downloaded before continuing.
- Step 3: Test SSO Setup** - The user is prompted to run a test. A warning icon states that the metadata files are copied to the local storage. Below, there is a list of valid administrator IDs with "oconvalh" and "oconcorre" selected. A "Run Test..." button is visible.



## SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

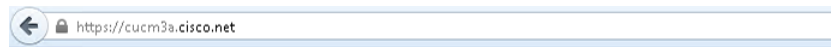


Great Success

Cisco live!

# What happen to the Administration login page after SSO enable?

Even after enabling SSO in the Cisco Collaboration Application, you still have a way to use the Administration pages with the initial application user



<https://<CUCM IP address or FQDN>/ccmadmin/showRecovery.do>



## Installed Applications

- Cisco Unified Communications Manager
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Prime License Manager

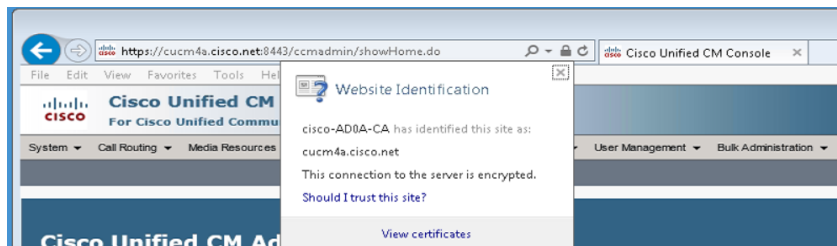


## Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

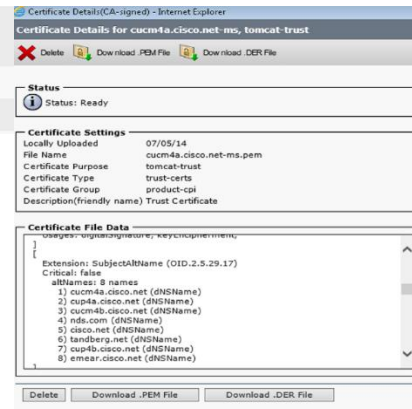
# Tomcat certificate what is used for?

Provide trusted identification for the Administration and User web browsing into our products



Provide trusted identification for Jabber when it connects to the different Cisco Services ( CUCM, IM&P, Unity Connection )

tomcat	<a href="https://cucm4a.cisco.net-ms">cucm4a.cisco.net-ms</a>	CA-signed	Multi-server(SAN)	cisco-AD0A-CA
tomcat-trust	<a href="https://cisco-AD0A-CA">cisco-AD0A-CA</a>	Self-signed	cisco-AD0A-CA	cisco-AD0A-CA
tomcat-trust	<a href="https://cucm4a.cisco.net-ms">cucm4a.cisco.net-ms</a>	CA-signed	Multi-server(SAN)	cisco-AD0A-CA

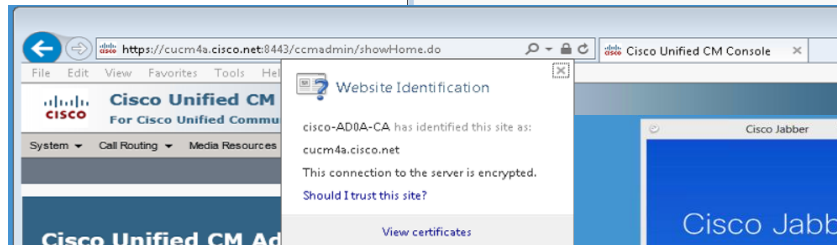
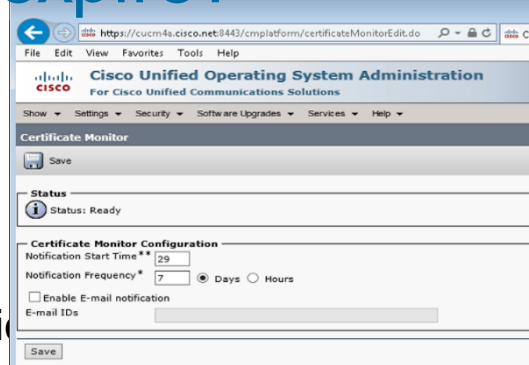


With version CUCM 10.5 we introduce the concept of Multi SAN certificates to avoid the need of providing and certificate per node of the cluster

# What happens when Tomcat certificate expire?

When signed by an enterprise CA or even a public CA, normally the certs have a validity of 2 years. Our products can notify when a certificate is going to expire.

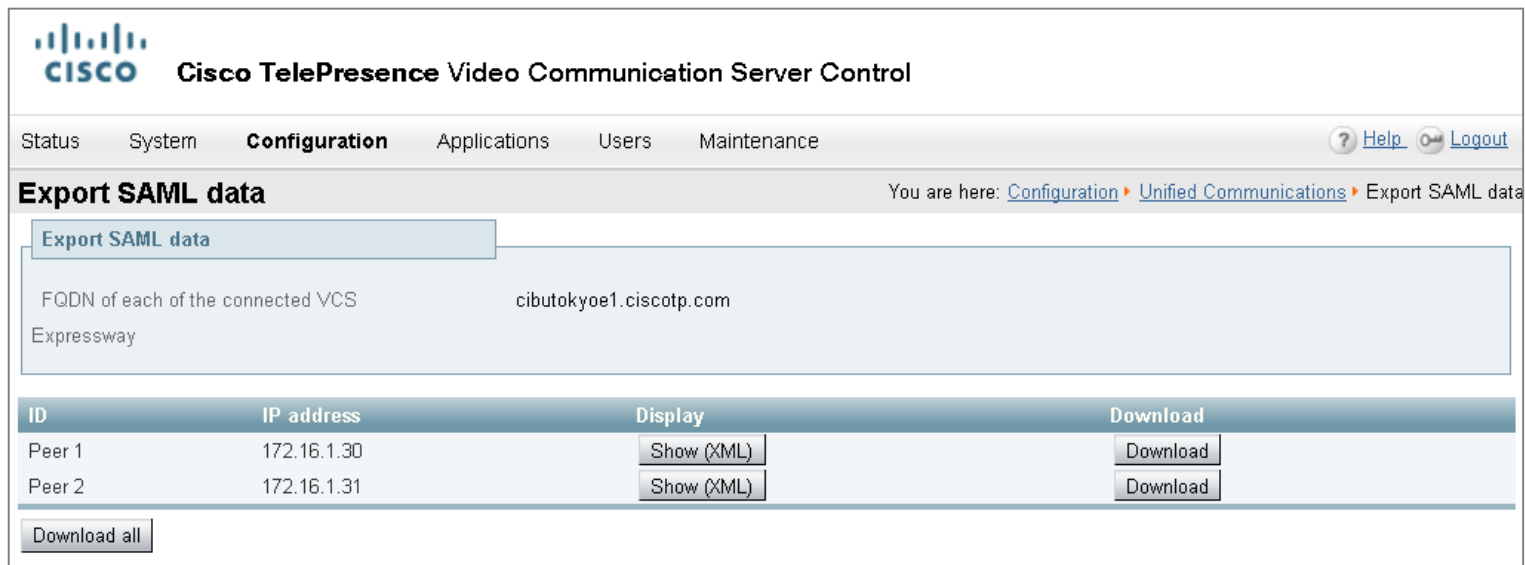
Tomcat certification expiration was never a show stopper for communication before SSO.



But **with SSO** everything changes, because if the Tomcat certificate is no longer valid then the SAML exchange will **fail**.

# Single-Sign-On configuration in Expressway

- Export the SAML metadata file from the (master) Expressway Core  
**Configuration > Unified Communications > Export SAML data**
- Import the metadata from Expressway Core into your IdP when configuring the SAML agreement

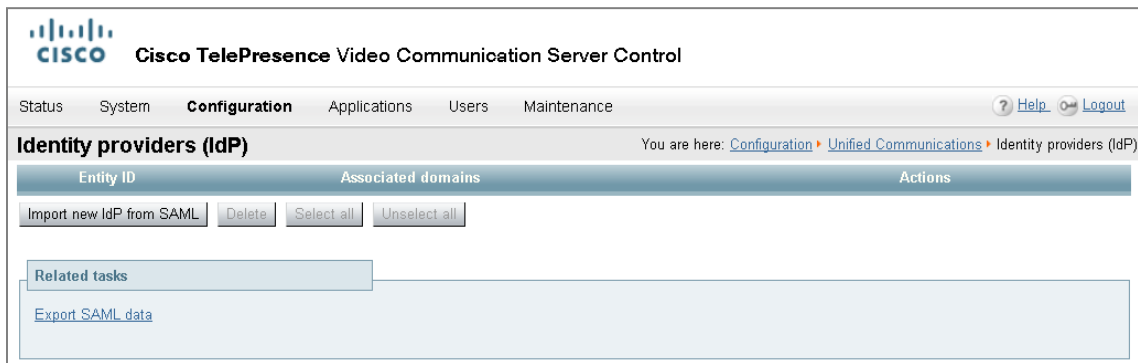


The screenshot displays the Cisco TelePresence Video Communication Server Control interface. The top navigation bar includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The 'Configuration' tab is active. The breadcrumb trail shows 'Configuration > Unified Communications > Export SAML data'. The main content area is titled 'Export SAML data' and shows the FQDN of each of the connected VCS Expressway as 'cibutokyo1.ciscottp.com'. Below this, there is a table with two columns: 'ID' and 'IP address'. The table lists two peers: Peer 1 with IP address 172.16.1.30 and Peer 2 with IP address 172.16.1.31. Each row has a 'Display' column with a 'Show (XML)' button and a 'Download' column with a 'Download' button. A 'Download all' button is located at the bottom left of the table area.

ID	IP address	Display	Download
Peer 1	172.16.1.30	Show (XML)	Download
Peer 2	172.16.1.31	Show (XML)	Download

# Single-Sign-On configuration in Expressway

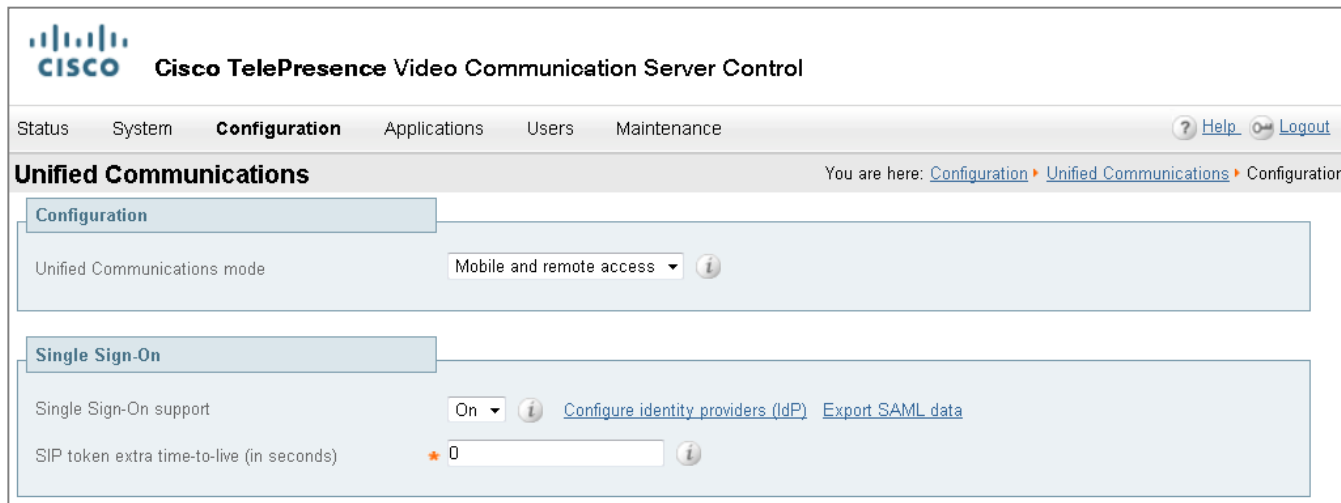
- Create the Identity Provider on the Expressway Core, by importing the SAML metadata file from the IdP
  - Configuration > Unified Communications > Identity providers (IdP)*
- Associate the IdP with the SIP domain on the Expressway Core
  - Configuration > Domains*



The screenshot displays the Cisco TelePresence Video Communication Server Control interface. At the top, the Cisco logo and the text "Cisco TelePresence Video Communication Server Control" are visible. Below this, a navigation bar includes "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". A "Help" icon and a "Logout" button are also present. The main content area is titled "Identity providers (IdP)" and includes a breadcrumb trail: "You are here: Configuration > Unified Communications > Identity providers (IdP)". Below the title, there is a table with columns for "Entity ID", "Associated domains", and "Actions". The "Actions" column contains buttons for "Import new IdP from SAML", "Delete", "Select all", and "Unselect all". A "Related tasks" section is located below the table, featuring a link for "Export SAML data".

# Single-Sign-On configuration in Expressway

- Enable SSO in Expressway Core  
**Configuration > Unified Communications > Configuration**



The screenshot displays the Cisco TelePresence Video Communication Server Control web interface. At the top, the Cisco logo and the title "Cisco TelePresence Video Communication Server Control" are visible. Below the title, a navigation bar includes "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "Configuration" tab is selected. In the top right corner, there are links for "Help" and "Logout".

The main content area is titled "Unified Communications" and includes a breadcrumb trail: "You are here: Configuration > Unified Communications > Configuration". Under the "Unified Communications" heading, there are two configuration sections:

- Configuration**: This section contains the "Unified Communications mode" setting, which is currently set to "Mobile and remote access".
- Single Sign-On**: This section contains two settings:
  - "Single Sign-On support" is set to "On". It includes links for "Configure identity providers (IdP)" and "Export SAML data".
  - "SIP token extra time-to-live (in seconds)" is set to "0".

# Single-Sign-On configuration in Expressway

- Enable SSO in Expressway Edge

**Configuration > Unified Communications > Configuration**

The screenshot shows the Cisco TelePresence Video Communication Server Expressway configuration interface. The breadcrumb path is Configuration > Unified Communications > Configuration. The 'Unified Communications mode' is set to 'Mobile and remote access'. Under the 'Single Sign-On' section, 'Single Sign-On support' is set to 'On' and 'Declare SSO support' is set to 'No'.

Configuration	Description/Behavior
Yes	Declare to clients that SSO is supported by the users' home Unified CM clusters. The clients will be told to attempt SSO, without further checking
No	Defer the client requests inwards. The clients will only attempt SSO if they find it is enabled on the requested node(s)

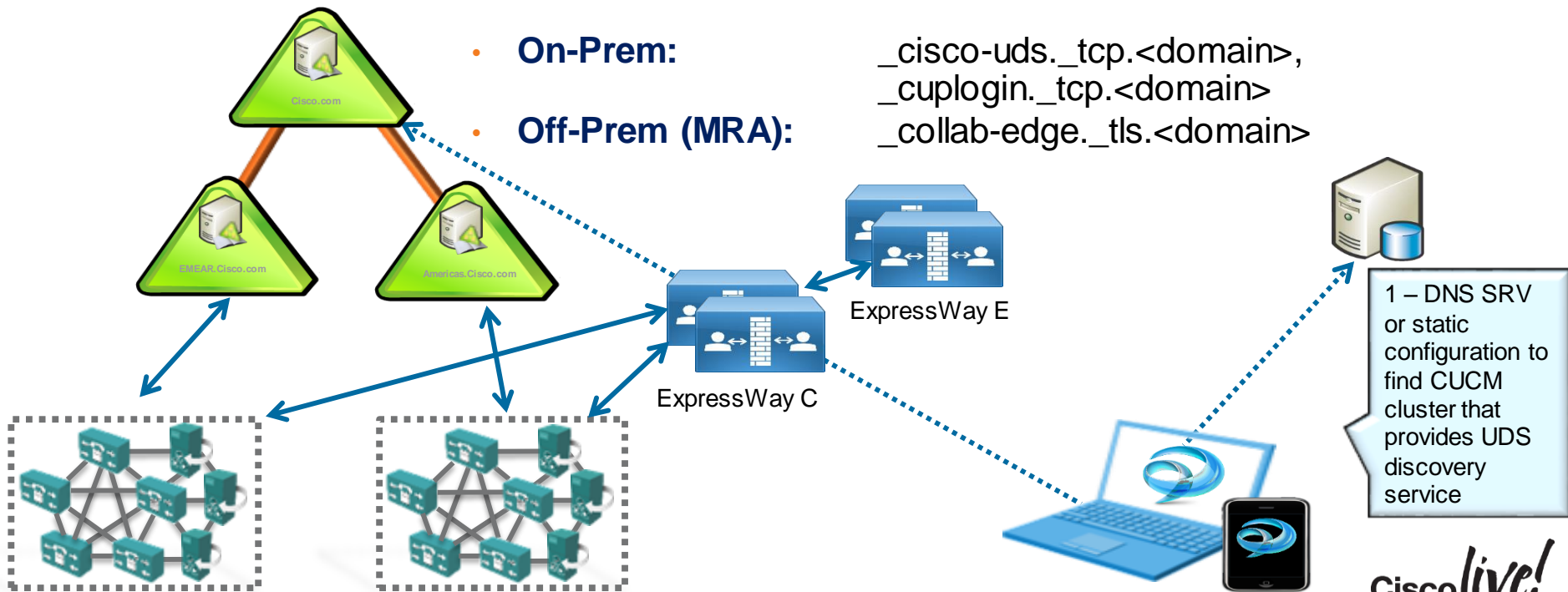


A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern pedestrian bridge with blue lighting spans across the street. Tall buildings with illuminated windows and signs are visible, along with several flags on poles to the left. The overall scene is a dynamic urban environment.

# Single Sign-On for Jabber

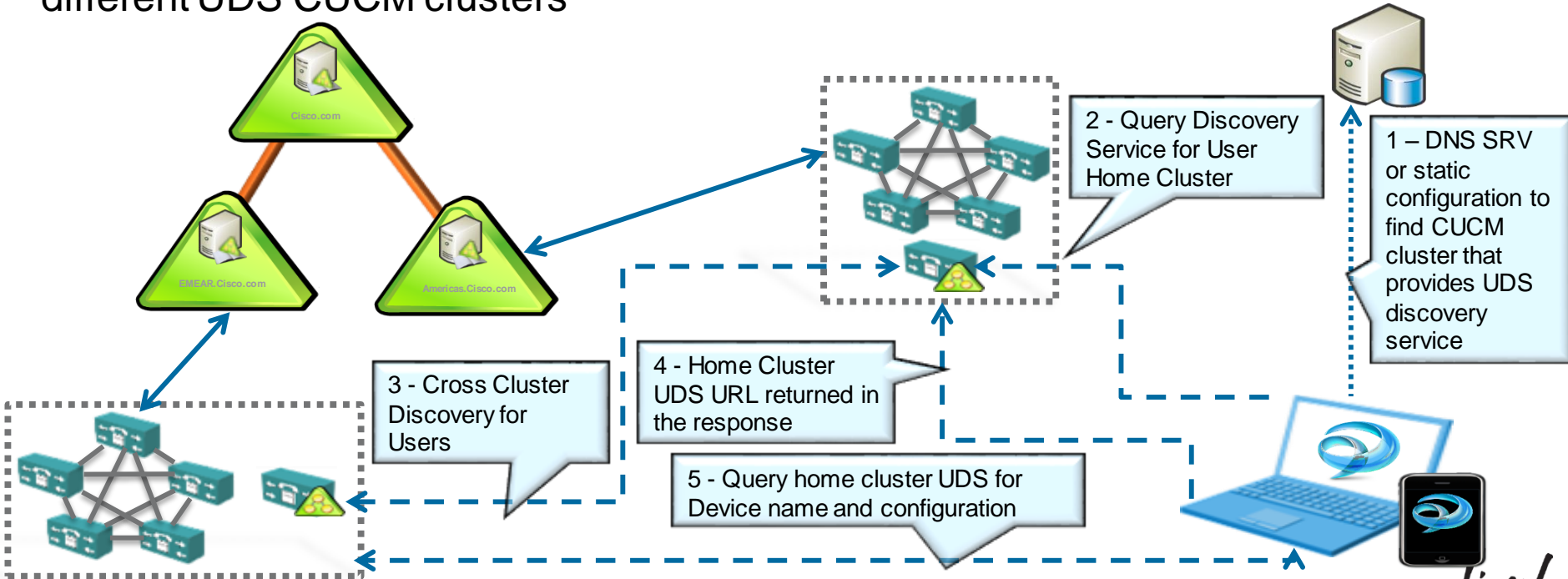
# Jabber Service Discovery

Jabber client uses DNS to determine if it is on or off premise connection and to discover the address of the node that it needs to connect to

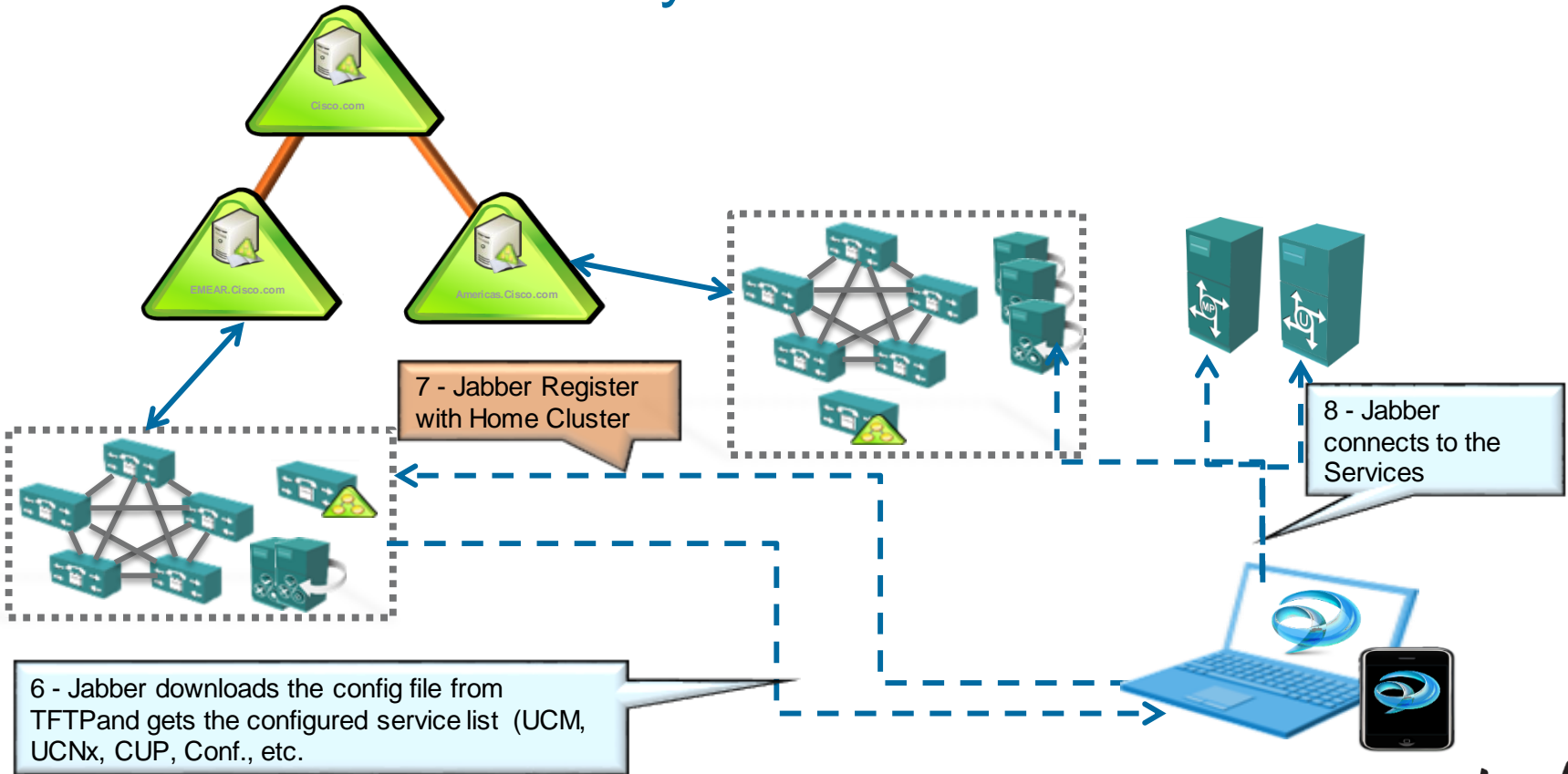


# Jabber Service Discovery

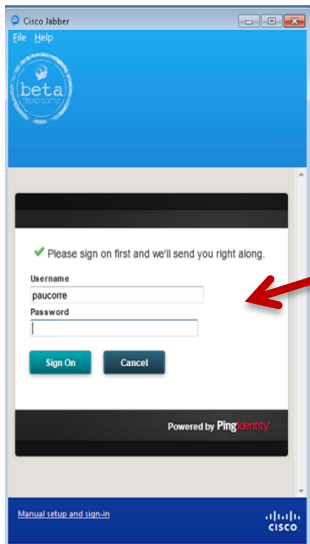
The direction for UDS is to allow dynamic discover of the home cluster for a specific user, and to get information from users directory information across different UDS CUCM clusters



# Jabber Service Discovery



# Embedded Browser



Embedded Browser

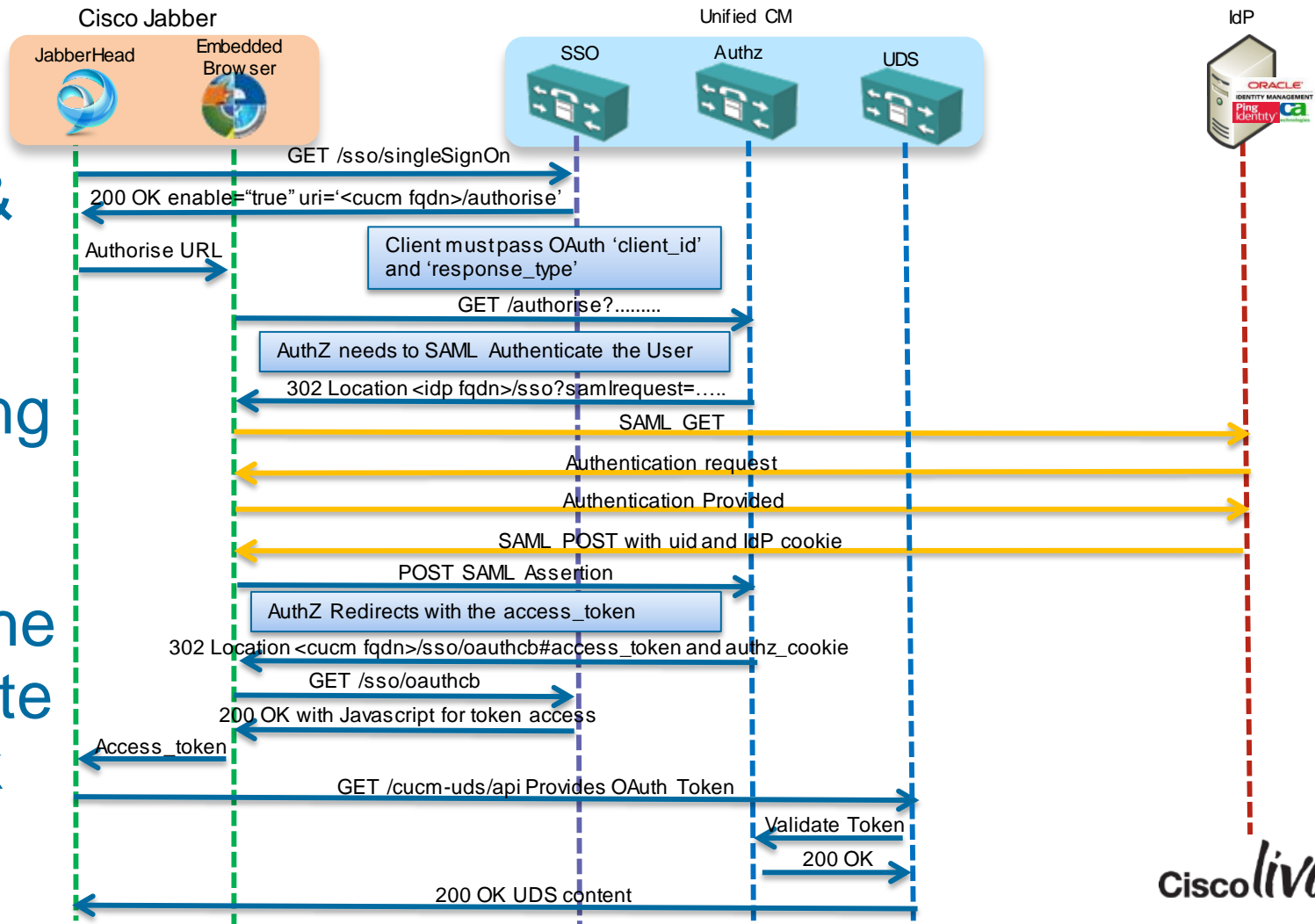
OS	Windows	MAC	iOS	Android
Browser Control API	Iweb Browser2	WebView	UIWebView	WebView
Underlying browser technology	IE	Safari	WebKit	WebKit
Control shares cookies with native OS browser	Yes	Yes	NO	NO

If we use **session cookies** then we **can't share** them with the native OS browser, that sharing can only be achieved with **persistent cookies**.

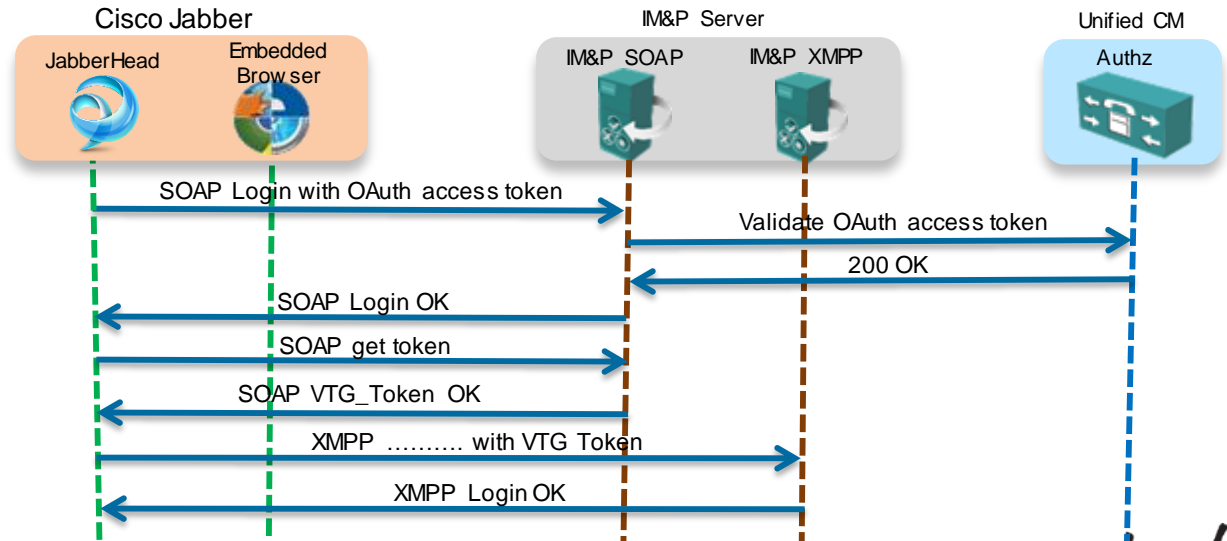
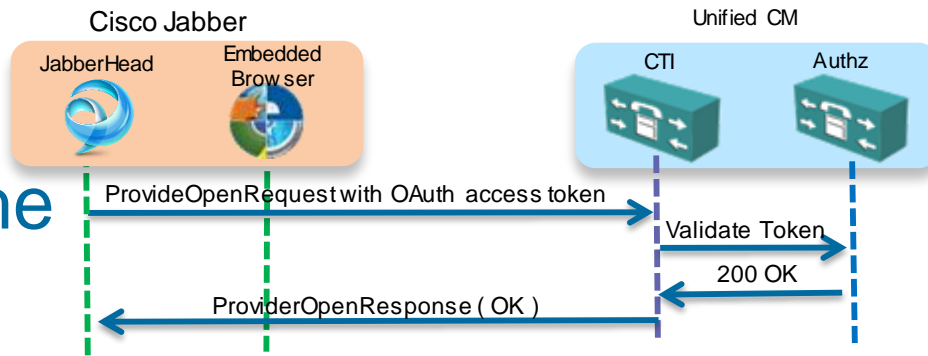
- Native OS Browser or WebView are the mechanisms for **Jabber to talk to IdP**
- Browser **delegates** the authentication process from the Jabber to the **OS Browser**

Cisco *live!*

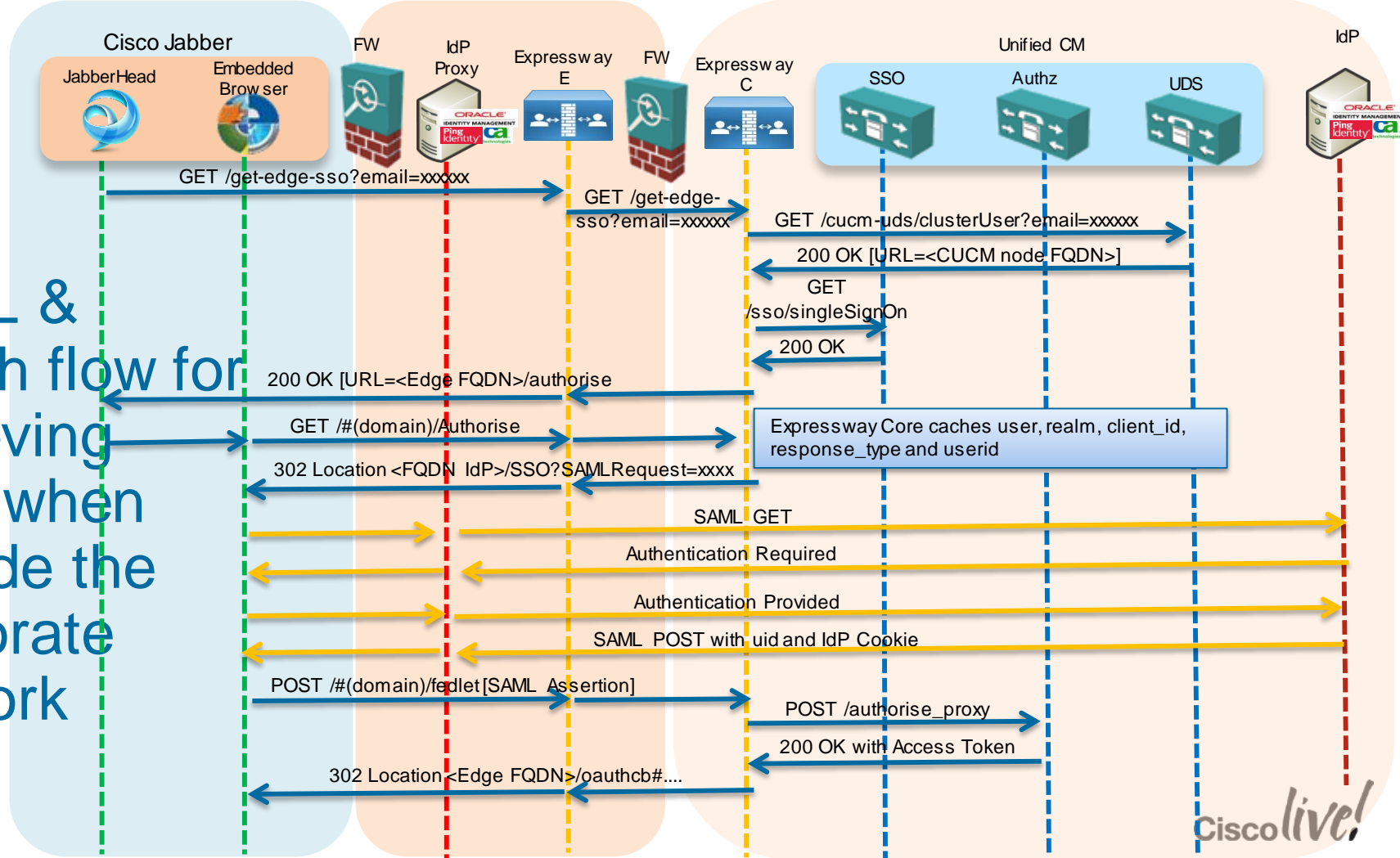
# SAML & OAuth flow for achieving SSO when inside the corporate network



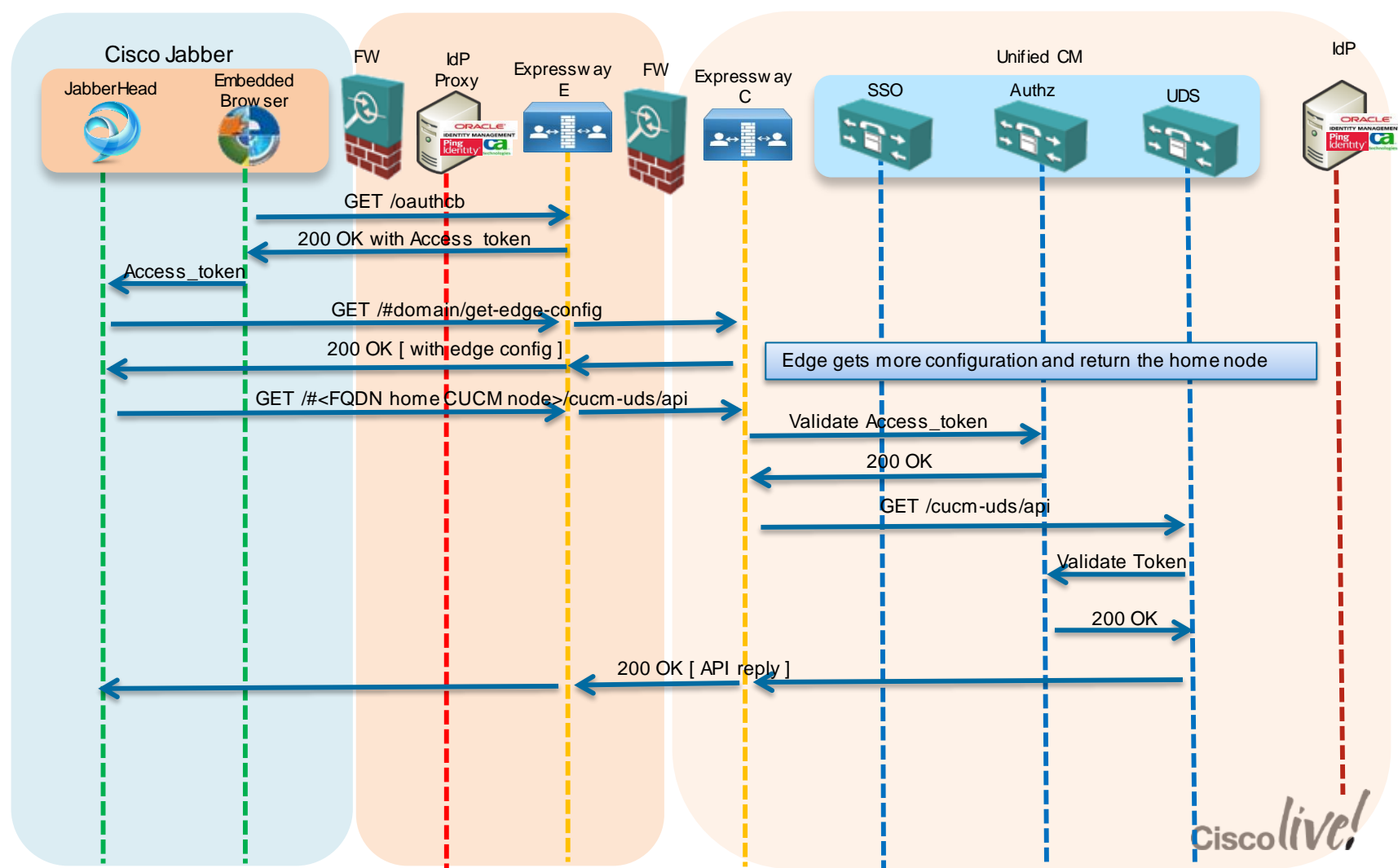
Using the OAuth token to access CTI and IM&P when inside the corporate network



# SAML & OAuth flow for achieving SSO when outside the corporate network







# SSO Inside and Outside Customer Network

## Required version

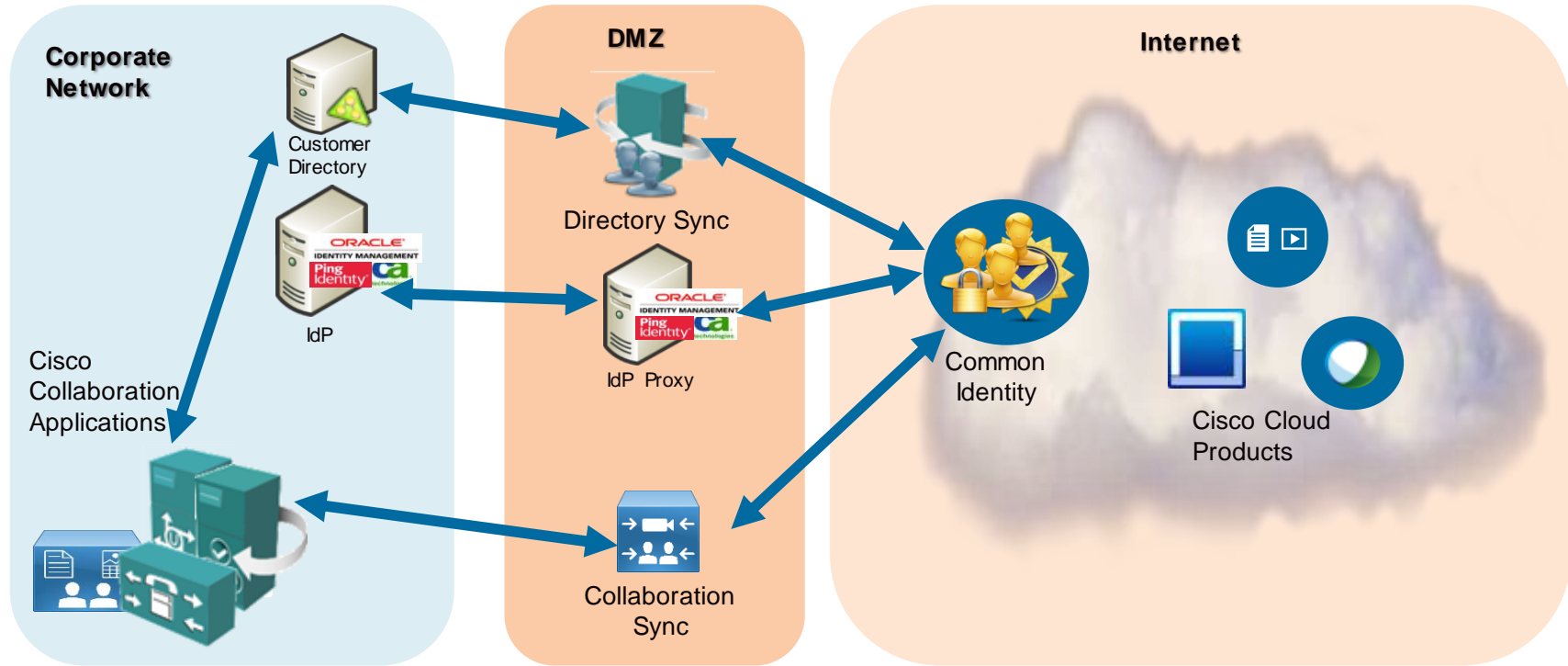
Component	Software Version
Expressway/VCS	X8.5.1 or later version
Unified CM	10.5.2 or later version
Unified IM&P	10.5.2 or later version
Unity Connection	10.5.2 or later version
Jabber for Windows	10.6 or later version
Jabber for iPad/iPhone	10.6 or later version
Jabber for Android	10.6 or later version
Jabber for MAC	10.6 or later version

A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern cityscape is visible with illuminated buildings and a prominent pedestrian bridge structure. The overall atmosphere is dynamic and urban.

# Identity in Cisco Public Cloud

# Cisco Collaboration Cloud Solution

## Identity Perspective





# Key Takeaways

# What will this identity architecture bring us?

- Align with **market standards**
- **Integration** of Cisco Collaboration Architecture in the broader Identity architecture of our customers.
- The same user identity for **on premise** and **cloud services**
- **Eliminate mismatch** in user attributes between the different collaboration products
- Bring more **synergies** between collaboration products.

# Key Takeaways

- Your customer identity strategy should not be focus only in the collaboration application, but should **cover all their IT applications**.
- With some many ways of deploying and consuming applications, your customer should understand that **following standards** is the only way to deliver identity services, **inside and outside** the organisation and for **any kind of device**.
- The need for **security and compliance rules** is a must today, and a **consolidated identity solution** for all the apps in their IT deployment, is the base to achieve that goal



Q&A

Cisco *live!*



# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2015 T-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  
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm



### Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. [www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)

**Cisco** *live!*



Thank you.

Cisco *live!*



**CISCO**

# Appendix

A nighttime photograph of a city street. The foreground is dominated by long, curved light trails from moving vehicles, primarily in shades of yellow and orange. In the background, there are modern buildings with lit windows and a pedestrian bridge structure. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

## Identity in Cisco Public Cloud

# WebEx integration for SSO

## 1. Get the metadata from the SP ( WebEx )

Need to get the metadata from the WebEx site in the SSO configuration

The screenshot shows the 'Site Administration' page for WebEx. The 'SSO Configuration' section is active, displaying 'Federated Web SSO Configuration'. The 'Federation Protocol' is set to 'SAML 2.0'. The 'SSO Profile' has 'SP Initiated' selected. The 'Target page URL Parameter' is 'TARGET'. The 'WebEx SAML Issuer (SP ID)' is 'http://www.webex.com'. The 'NameID Format' is 'Unspecified'. The 'Export' button is highlighted with a red arrow.

This file will provide the **certificates** required to exchange HTTP information

This file also provides information on what is the :

- **NameID** formats accepted by the Webex Site, we recommend the use of  
*urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*
- **Location of the Service**  
*https://<SiteName>.webex.com/dispatcher/SAML2AuthService?siteurl=<SiteName>*
- What kind of **SAML binding** we are going to use

*SAML 2.0 using HTTP-POST*

Cisco *live!*

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://www.webex.com" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="false"
  <md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIIC5jCCAc6wAIBAgIcATZlyKOMA0GCSqGSIb3DQEBBQUAMQxwCzAJBgNVBAYTAiVMSUw1wYDVQQDEoxx
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified </md:NameIDFormat>
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress </md:NameIDFormat>
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName </md:NameIDFormat>
    <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:entity </md:NameIDFormat>
    <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:persistent </md:NameIDFormat>
    <md:AssertionConsumerService isDefault="true" Index="0" Location="https://uc8sevtlab13.webex.com/dispatcher/SAML2AuthService?
    siteurl=uc8sevtlab13" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  </md:SPSSODescriptor>
  </md:Organization>
  <md:OrganizationName xml:lang="en">Cisco WebEx</md:OrganizationName>
  <md:OrganizationDisplayName xml:lang="en">Cisco WebEx</md:OrganizationDisplayName>
  <md:OrganizationURL xml:lang="en"/>
</md:EntityDescriptor>
```

# WebEx integration for SSO

## 2. Configuring the IdP ( IdP and SP Components )

Most of the vendors always have two major tasks that together define the agreement between the IdP<->SP:

1. When configuring the IdP part, we need to define what authentication mechanism we are going to use.

2. With the metadata xml file that we got from WebEx we configure the SP component

Main Manage IdP Adapter Instances

★ Manage IdP Adapter Instances

PingFederate uses adapters to authenticate users to your partners' applications. Here you can manage "instances" of adapters that SP

INSTANCE NAME	INSTANCE ID	TYPE
ADLDAP	ADLDAP	HTTP Basic IdP Adapter
ADLDAPForm	ADLDAPForm	HTML Form IdP Adapter
ADDC	ADDC	IPA IdP Adapter 3.1

Create New Instance

Circle of Trust (2 Item(s))

New... Delete

<input checked="" type="checkbox"/>	Name	Entities
<input type="checkbox"/>	CUCM	cucm3a.cisco.net saml2 CUCMOpenAM saml2
<input type="checkbox"/>	WebEx	CloudOpenAM saml2 uc8sevtlab14 saml2

Entity Providers (4 Item(s))

New... Delete Import Entity...

<input checked="" type="checkbox"/>	Name	Protocol	Type	Location	Realm
<input type="checkbox"/>	CloudOpenAM	SAMLv2	IDP	Hosted	/
<input type="checkbox"/>	cucm3a.cisco.net	SAMLv2	SP	Remote	/
<input type="checkbox"/>	CUCMOpenAM	SAMLv2	IDP	Hosted	/
<input type="checkbox"/>	uc8sevtlab14	SAMLv2	SP	Remote	/

Main SP Connection

Connection Type Connection Options General Info Browser SSO Credentials Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status  Active  Inactive

SP Connection

CONNECTION TYPE

Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

CONNECTION OPTIONS

Browser SSO	true
Attribute Query	false

GENERAL INFO

Partner's Entity ID (Connection ID)	cucm3a.cisco.net
Base URL	https://cucm3a.cisco.net/6443

BROWSER SSO

SAML PROFILES

IdP-Initiated SSO	false
IdP-Initiated SLO	false

# WebEx integration for SSO

## 3. Export the metadata from the IdP

Similar to what we did in the beginning with the WebEx Site we are going to export the metadata of the IdP to enable SSO on the SP (SP)

In our example we export the metadata from PingFederate SP and we include the X509 certificate, binding services and locations

★ Manage Connections

On this screen you can manage connections to your partner SPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all SP connections by specifying a single, global logging mode.

CONNECTION NAME	CONNECTION ID	PROTOCOL	STATUS	ACTION
IDLAB-PF	IDLAB-PF	SAML2.0	Active	In Use   Copy   Export Connection   Export Metadata
PCADa	PCADa	SAML2.0	Active	In Use   Copy   Export Connection   Export Metadata
PCP0a	PCP0a	SAML2.0	Active	In Use   Copy   Export Connection   Export Metadata
ucum3a.cisco.net	ucum3a.cisco.net	SAML2.0	Active	In Use   Copy   Export Connection   Export Metadata
cup1a.cisco.net	cup1a.cisco.net	SAML2.0	Active	In Use   Copy   Export Connection   Export Metadata
http://www.webex.com	http://www.webex.com	SAML2.0	Active	In Use   Copy   Export Connection   Export Metadata
ucm1a.cisco.net	ucm1a.cisco.net	SAML2.0	Active	In Use   Copy   Export Connection   Export Metadata

```
<?xml version="1.0"?>
- <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cisco.net" cacheDuration="PT1440M"
  ID="Z281xzhf4TNUVxLEF0jrrmTv48K">
  - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      - <ds:Reference URI="#Z281xzhf4TNUVxLEF0jrrmTv48K">
        - <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>HP4w+I2OKAa+EjzXOXamioF0mIU=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue> J5vTAf2E1pJAEMFDdJwsikWkigVqJKR5SmevXU/P4HvdYUzCnGT+MU//j/bGkt8hsm2DzGq4Ls0
      CUXyBkUI5G1QjB0FHOLVDVT3Wb+IINS5jeTmxmBXBCGFFAHjiwOskNE9iGMOnRWUcAJjBWhyaW1 p+CJNxArGS+ZPQ1yYR8=
    </ds:SignatureValue>
  </md:EntityDescriptor>
- <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  - <md:KeyDescriptor use="signing">
    - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      - <ds:X509Data>
        <ds:X509Certificate>MIICoZCCAaSgAwIBAgIGAUB49tFUMA0GCSqSgSIb3DQEBBQUAMGExCzAJBgNVBAYTAIVLMQ8wDQYDQQIEV
          POST/
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:SingleSignOnService Location="https://ping0a.cisco.net:9031/idp/SSO.saml2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
      POST"/>
    <md:SingleSignOnService Location="https://ping0a.cisco.net:9031/idp/SSO.saml2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
      Redirect"/>
  </md:IDPSSODescriptor>
- <md:ContactPerson contactType="administrative">
  <md:Company>Cisco</md:Company>
  <md:GivenName>Paulo</md:GivenName>
  <md:SurName>Jorge Correia</md:SurName>
```

# WebEx integration for SSO

## 4. Import the metadata from the IdP

Change the AuthContextClassDef to `urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified`

Now back to the WebEx configuration we will import the metadata from the IdP.

After the Importing you will notice that information on IdP ID, Login URL and Certificated fulfill

The screenshot shows the WebEx Site Administration interface. On the left is a navigation menu with options like Home, Manage Site, Manage Users, Session Types, and Assistance. The main content area is titled 'Site Administration' and 'SSO Configuration'. Under 'Federated Web SSO Configuration', the Federation Protocol is set to 'SAML 2.0'. The SSO Profile is 'SP Initiated'. The Target page URL Parameter is 'TARGET'. The WebEx SAML Issuer (SP ID) is 'http://www.webex.com'. The Issuer for SAML (IdP ID) is empty. The Customer SSO Service Login URL is 'http://www.webex.com'. The NameID Format is 'Unspecified'. The AuthContextClassRef is 'urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified'. The Default WebEx Target page URL is empty. The Customer SSO Error URL is empty. There are checkboxes for Single Logout, Auto Account Creation, Auto Account Update, and Remove uid Domain Suffix for Active Directory UPN. An 'Export' button is visible. A red arrow points to the 'Import SAML Metadata' link in the 'TARGET' field. A blue arrow points from this link to the right-hand screenshot.

The right-hand screenshot shows the 'Site Administration' page with the 'SSO Configuration' tab selected. The 'Federated Web SSO Configuration' section is visible. The Federation Protocol is 'SAML 2.0'. The SSO Profile is 'SP Initiated'. The Target page URL Parameter is 'TARGET'. The WebEx SAML Issuer (SP ID) is 'http://www.webex.com'. The Issuer for SAML (IdP ID) is 'cisco.net'. The Customer SSO Service Login URL is 'https://ping0a.cisco.net/9031/idp/SSO.saml2'. The NameID Format is 'Unspecified'. The AuthContextClassRef is 'urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified'. The Default WebEx Target page URL is empty. The Customer SSO Error URL is empty. There are checkboxes for Single Log, Auto Acco, Auto Acco, and Remove ui. The 'Site Certificate Manager' section is also visible, showing 'Issued to: cisco.net', 'Issued by: cisco.net', 'Version: V3', 'Serial number: 0140 78F6 D154', 'Signature algorithm ID: SHA1withRSA', 'Issuer name: (CN, O, C) CN=cisco.net, OU=lab, O=Cisco, L=London, ST=London, C=UK', 'Validity from: 8/13/13 6:36 am', 'Valid to: 8/13/14 6:36 am', and 'Subject name: (CN, O, C) CN=cisco.net, OU=lab, O=Cisco, L=London, ST=London, C=UK'.



# WebEx 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>• <b>Advanced Services engagement</b></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>

# WebEx User Account Creation and Update

To enable the provision using SAML we need :

- Change the WebEx site configuration to enable the creation and update
- Add extra attributes in the IdP to the Synchronisation agreement ( email, firstname, lastname, uid and updateTimeStamp )



[Home](#)

**Manage Site**

- [Site Settings](#)
- [Tracking Codes](#)
- [Company Addresses](#)
- [Email Templates](#)
- [Meetings in Progress](#)
- [SSO Configuration](#)

**Manage Users**

- [Add User](#)
- [Edit User List](#)
- [Import/Export Users](#)
- [Edit Privileges](#)
- [Send Email to All](#)

**Session Types**

- [Add Custom Type](#)
- [Session Type List](#)

**Assistance**

- [Help](#)

[Log out](#)

## Site Administration

### SSO Configuration

[Site Certificate Manager](#)

---

#### Federated Web SSO Configuration

Federation Protocol:

SSO Profile:  SP Initiated  
 AuthnRequest Signed  
 IdP Initiated

Target page URL Parameter:

WebEx SAML Issuer (SP ID):

Issuer for SAML (IdP ID):

Customer SSO Service Login URL:

You can export a SAML metadata WebEx SP configuration file:

NameID Format:

AuthnContextClassRef:

Default WebEx Target page URL:

Customer SSO Error URL:

Single Logout  
 Auto Account Creation  
 Auto Account Update  
 Remove uid Domain Suffix for Active Directory UPN

Main | SP Connection | Browser SSO | **Assertion Creation**

Identity Mapping | **Attribute Contract** | IdP Adapter Mapping | Summary

An Attribute Contract is a set of user attributes that this server will send in the assertion.

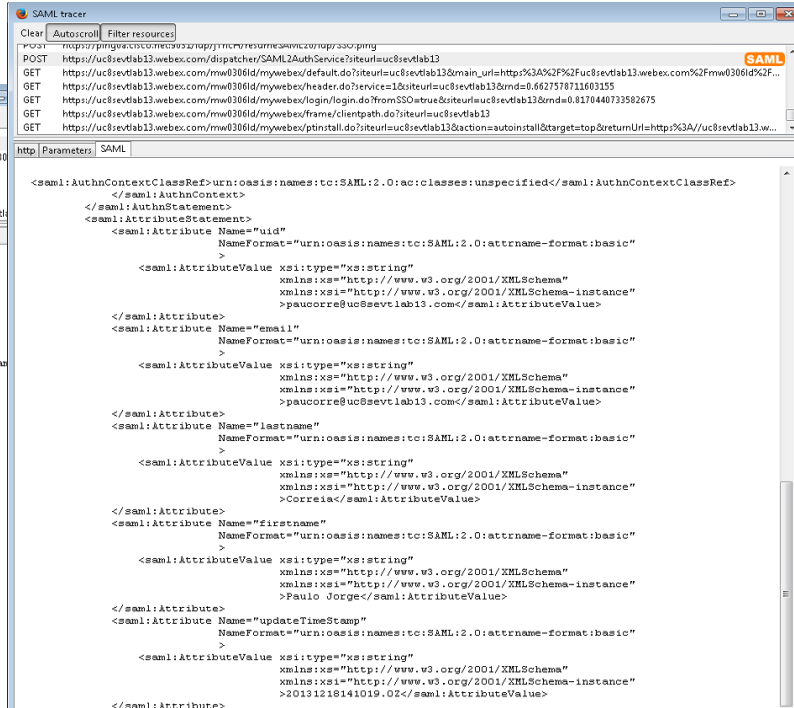
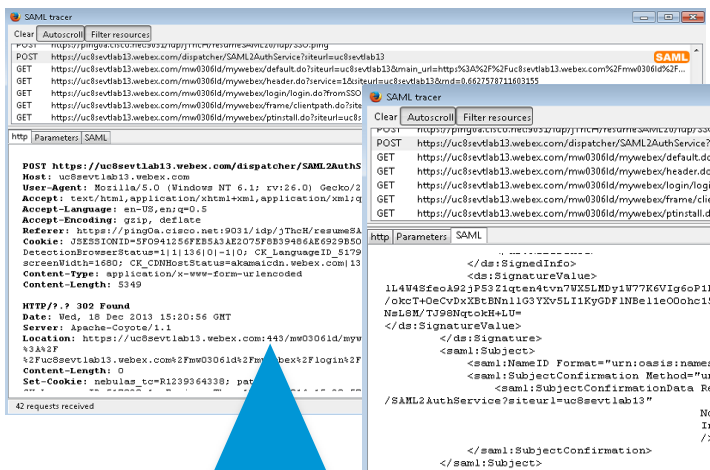
ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT	
SAML_SUBJECT	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>	

EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
email	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit / Delete</a>
firstname	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit / Delete</a>
lastname	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit / Delete</a>
uid	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit / Delete</a>
updateTimeStamp	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit / Delete</a>

# What is the result when the Users login with Auto Account Creation and Update enabled

When the user logs into the WebEx MC, in the SAML tracer you will see and HTTP 302 Found as expected, the Name ID of the user login and we have information on the attributes contracted.



Great Success



**CISCO**