# TOMORROW starts here.

CISCO

Cisco live!

# Unified Communications Directory Integrations (SSO)

BRKUCC-2664

Chris Gascoigne
Consulting Systems Engineer

# Agenda

- Identity and Directory challenges
- Directory Integration
- Single Sign-On Technologies
- Enabling SAML SSO On-Prem
- Enabling SAML SSO Cloud
- Key Takeaways and Q&A

# Identity and Directory Challenges

# Why Identity Matters?

## Improve Adoption

- 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."

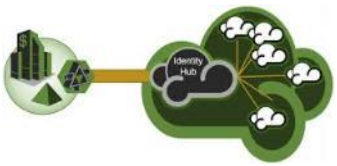
## Reduce Cost

- 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

- 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

# Cisco Identity Management Challenge



Bridge Services Cloud & OnPrem

Many client's, many OS’s, in different devices

Microsoft® Office 365

Google Apps

GoToMeeting

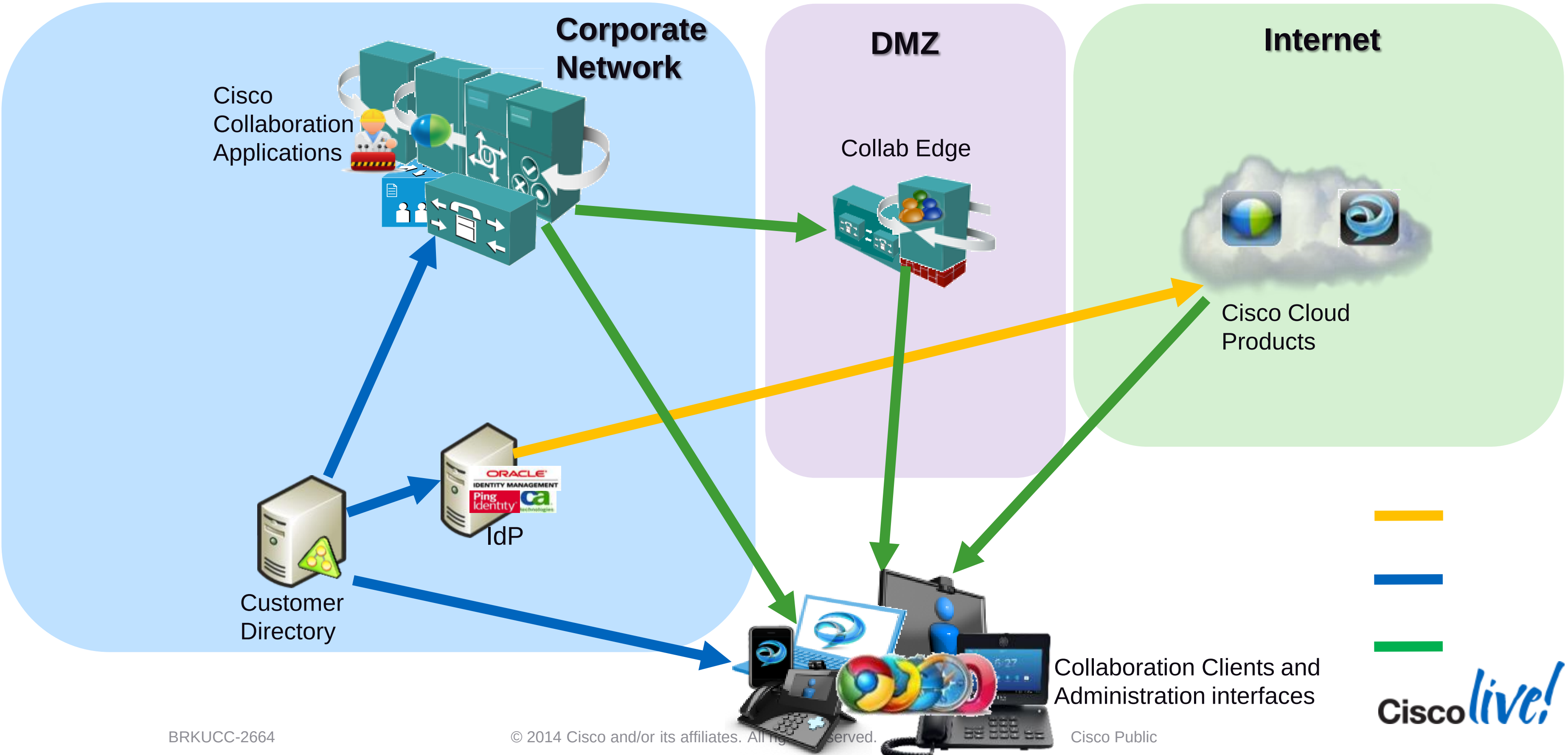
skype

Windows Azure

Many players with different solutions

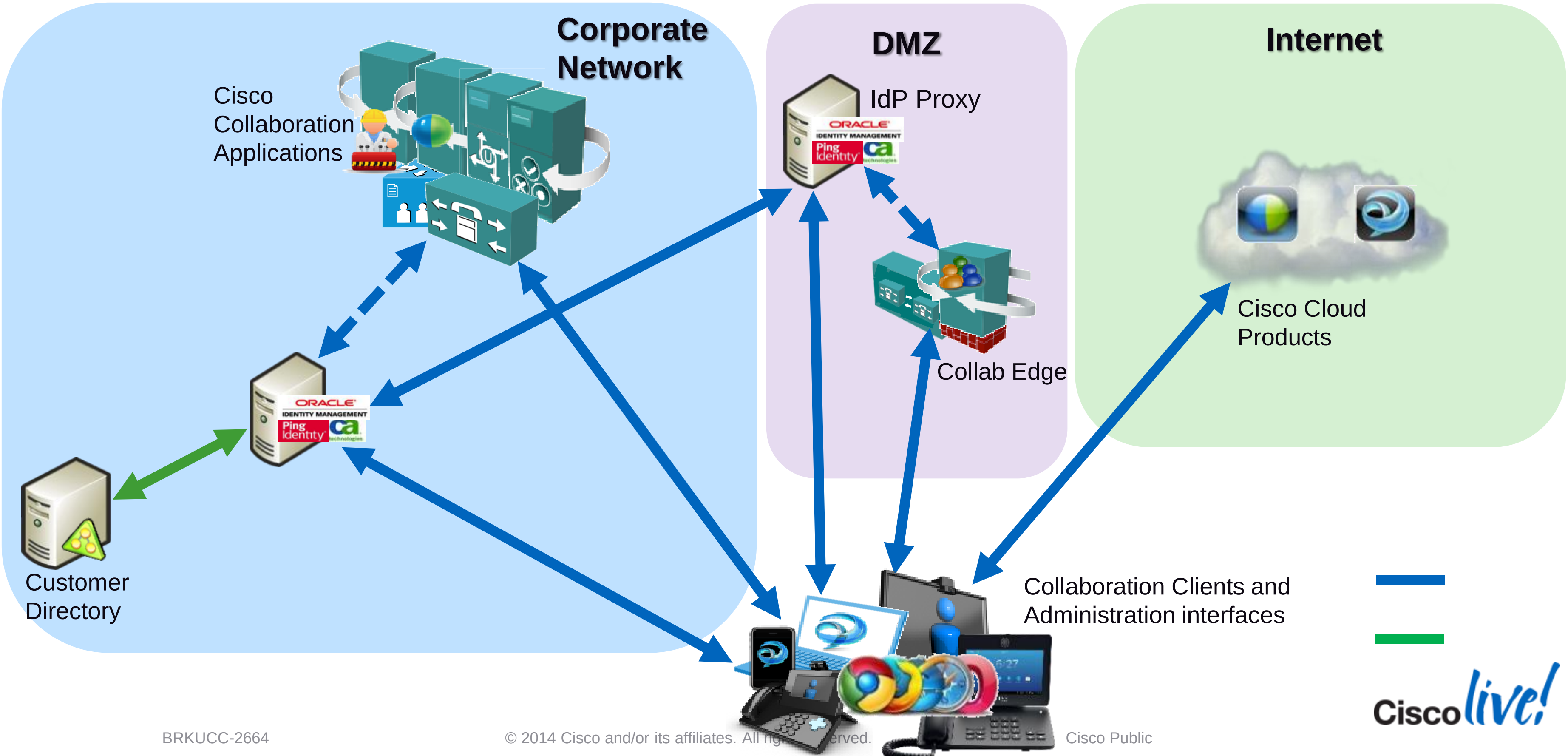
# Identity Architecture

## Collaboration System Release 10

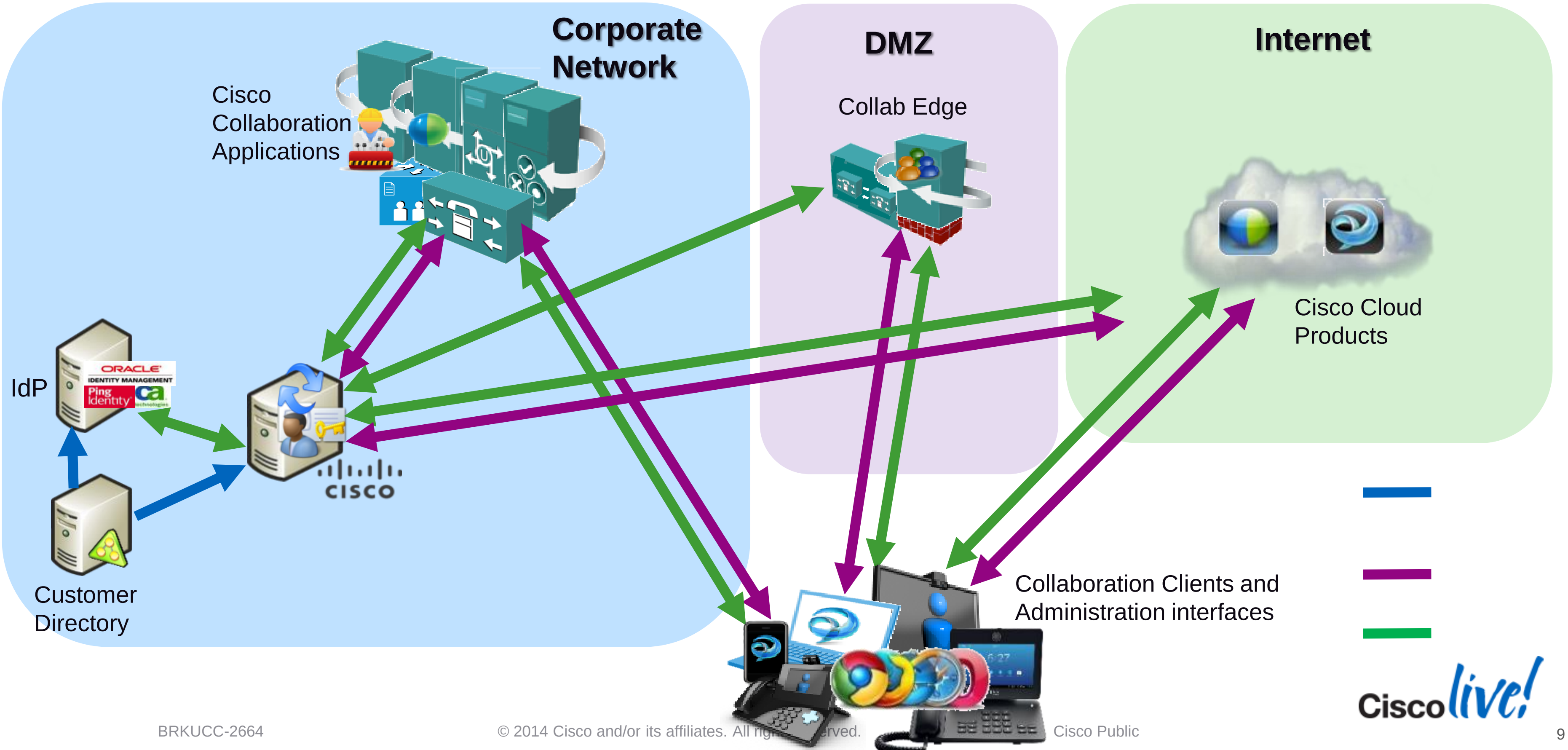

Corporate Network
DMZ
Internet
Cisco Collaboration Applications
Collab Edge
Cisco Cloud Products
ORACLE IDENTITY MANAGEMENT
Ping Identity
ca technologies
IdP
Customer Directory
Collaboration Clients and Administration interfaces

# Identity Architecture

## Collaboration System Release 10.x



# Identity Architecture – End Goal



Corporate Network

Cisco Collaboration Applications

DMZ

Collab Edge

Internet

Cisco Cloud Products

IdP

Customer Directory

Collaboration Clients and Administration interfaces

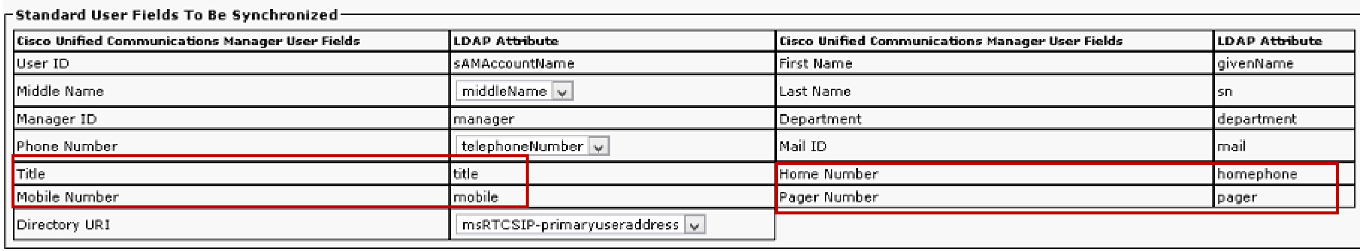
# Directory Integration

# Directory Synchronisation Changes

## Attributes visibility in 9.x and 10.x

| | Upto 9.X | 10.x |
|---|---|---|
| User ID | Yes | Yes |
| Last Name | Yes | Yes |
| Middle Name | Yes | Yes |
| First Name | Yes | Yes |
| **Tittle** | No | Yes |
| Department | Yes | Yes |
| Manager ID | Yes | Yes |

| | Upto 9.X | 10.x |
|---|---|---|
| Phone Number | Yes | Yes |
| **Mobile Number** | No | Yes |
| **Home Number** | No | Yes |
| **Pager Number** | No | Yes |
| Directory URI | Yes | Yes |
| Mail ID | Yes | Yes |



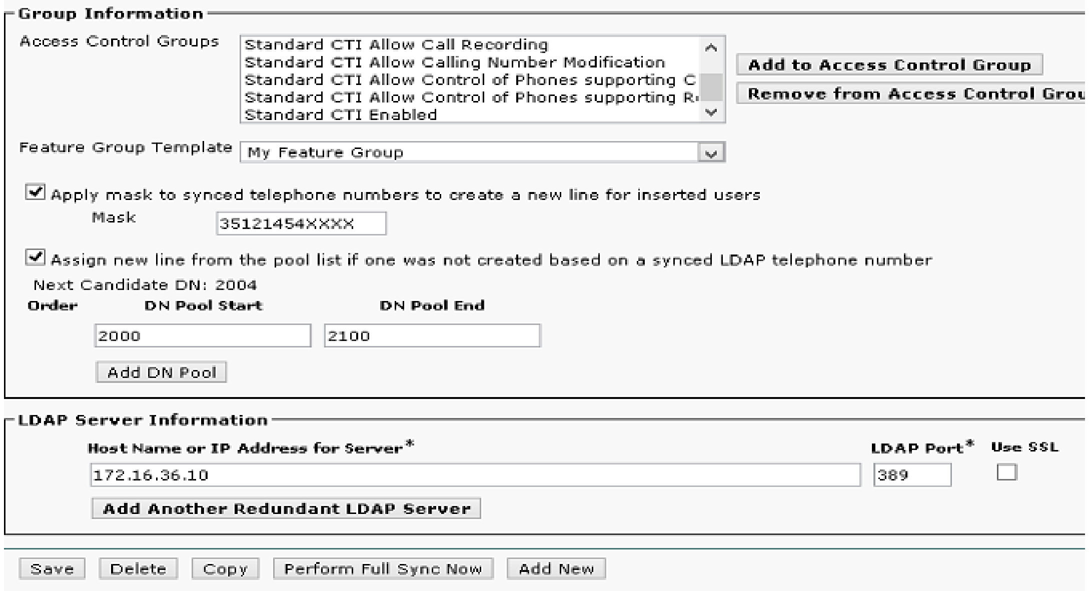
Standard User Fields To Be Synchronized

| 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 |
| Title | title | Home Number | homephone |
| Mobile Number | mobile | Pager Number | pager |
| Directory URI | msRTCSIP-primaryuseraddress | | |

# Directory Synchronisation Changes

## Extra information required

With the introduction of Self-Provision devices and it's need for creating groups based on LDAP queries/details, a lot changed when we synchronise user information from an LDAP sources



**Group Information**

Access Control Groups:
- Standard CTI Allow Call Recording
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of Phones supporting C
- Standard CTI Allow Control of Phones supporting R
- Standard CTI Enabled

Feature Group Template: My Feature Group

☑ Apply mask to synced telephone numbers to create a new line for inserted users

Mask: 35121454XXXX

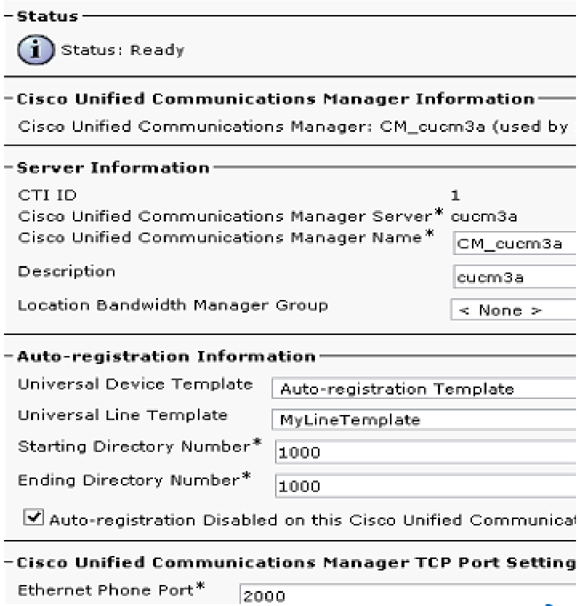
☑ Assign new line from the pool list if one was not created based on a synced LDAP telephone number

Next Candidate DN: 2004

| Order | DN Pool Start | DN Pool End |
|---|---|---|
| | 2000 | 2100 |

**LDAP Server Information**

| Host Name or IP Address for Server* | LDAP Port* | Use SSL |
|---|---|---|
| 172.16.36.10 | 389 | □ |



**Status**

Status: Ready

**Cisco Unified Communications Manager Information**

Cisco Unified Communications Manager: CM_cucm3a (used by

**Server Information**

| | |
|---|---|
| CTI ID | 1 |
| Cisco Unified Communications Manager Server* | cucm3a |
| Cisco Unified Communications Manager Name* | CM_cucm3a |
| Description | cucm3a |
| Location Bandwidth Manager Group | < None > |

**Auto-registration Information**

| | |
|---|---|
| Universal Device Template | Auto-registration Template |
| Universal Line Template | MyLineTemplate |
| Starting Directory Number* | 1000 |
| Ending Directory Number* | 1000 |

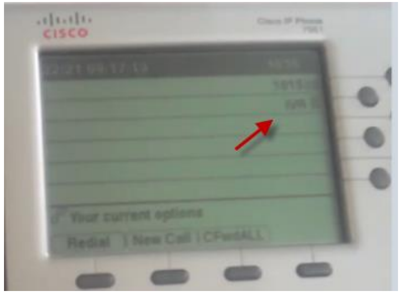
☑ Auto-registration Disabled on this Cisco Unified Communicat

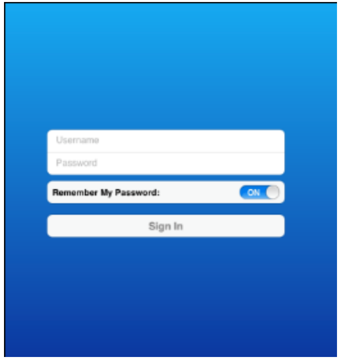
**Cisco Unified Communications Manager TCP Port Setting**

Ethernet Phone Port*: 2000

# Self-Provisioning

- IVR Self-Provision – For non-GUI capable devices
- GUI Self-Provision – For advance IP endpoints
- GUI Self-Provision – For software endpoints

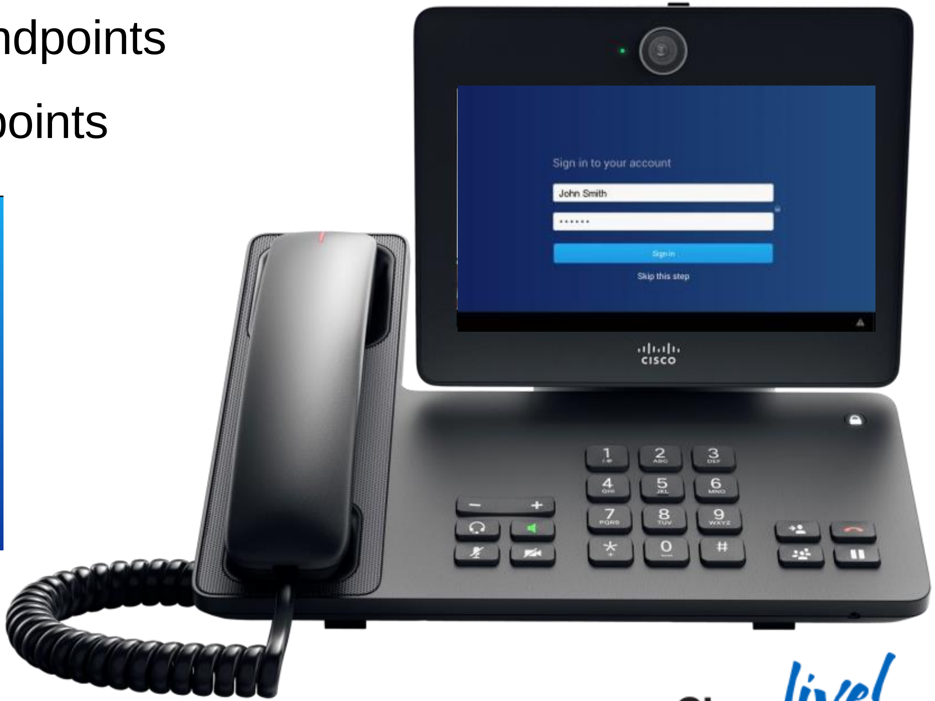



Username

Password

Remember My Password: ON

Sign In


Sign in to your account

John Smith

••••••

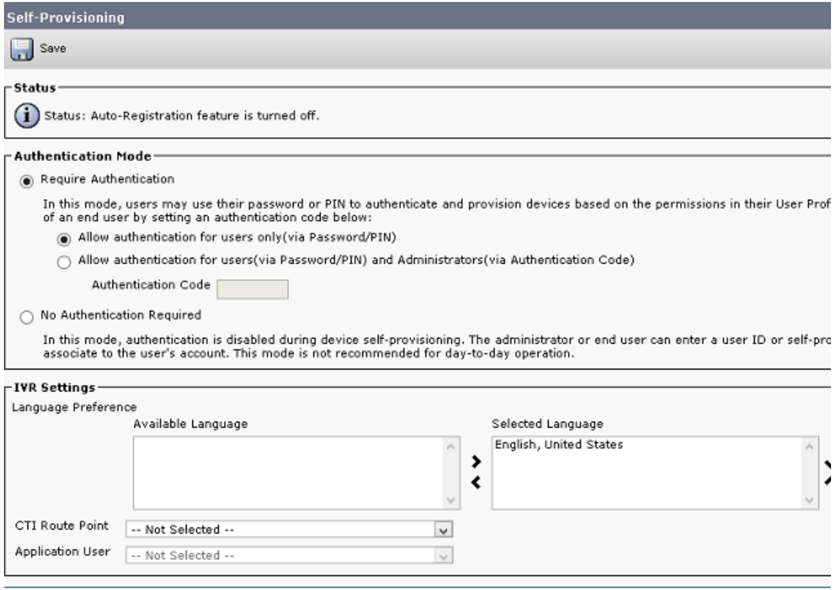
Sign in

Skip this step

**Note :** for the TUI phones will need to register in CUCM before the user can Self-Enroll

# Self-Provisioning

- Admin needs to decide on the level of authentication required for the Self-Provisioning process.
    - No Authentication
    - Authentication with user Pin/Password
    - Authentication with user Pin/Password and extra administrator Authentication Code



**Self-Provisioning**

**Status**

Status: Auto-Registration feature is turned off.

**Authentication Mode**

● Require Authentication

In this mode, users may use their password or PIN to authenticate and provision devices based on the permissions in their User Prof
of an end user by setting an authentication code below:

● Allow authentication for users only(via Password/PIN)

○ Allow authentication for users(via Password/PIN) and Administrators(via Authentication Code)

Authentication Code

○ No Authentication Required

In this mode, authentication is disabled during device self-provisioning. The administrator or end user can enter a user ID or self-pro
associate to the user's account. This mode is not recommended for day-to-day operation.

**IVR Settings**

Language Preference

Available Language

Selected Language: English, United States

CTI Route Point: -- Not Selected --

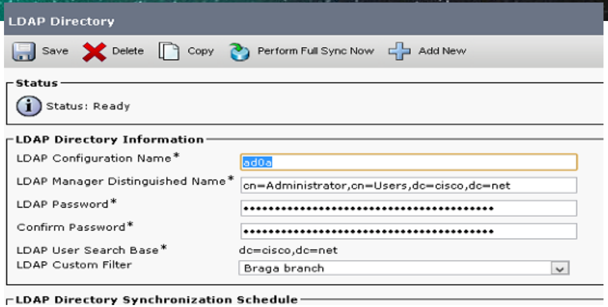
Application User: -- Not Selected --

# How Do We Create Different “Locations” For Self-Provisioning?

We need to create one LDAP Synchronisation Agreement per group of devices with the same characteristics ( normally region/location in CUCM terms )

In the case of an Active Directory LDAP source the best practices will be to synchronise against a Global Catalogue and create an LDAP filter that will identify users in a given location.

This synchronisation agreement will be associated with a Feature Group Template and that will define the characteristics of the Self-Provisioned Device



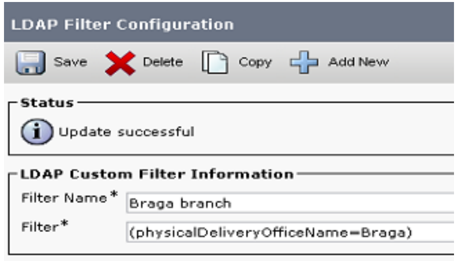
**Status**

Status: Ready

**LDAP Directory Information**

| | |
|---|---|
| LDAP Configuration Name* | ad0a |
| LDAP Manager Distinguished Name* | cn=Administrator,cn=Users,dc=cisco,dc=net |
| LDAP Password* | •••••••••••••••••••••••••••••••••••••••• |
| Confirm Password* | •••••••••••••••••••••••••••••••••••••••• |
| LDAP User Search Base* | dc=cisco,dc=net |
| LDAP Custom Filter | Braga branch |

**LDAP Directory Synchronization Schedule**

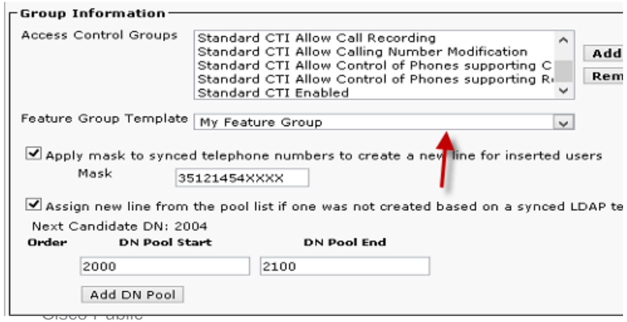


**Status**

Update successful

**LDAP Custom Filter Information**

| | |
|---|---|
| Filter Name* | Braga branch |
| Filter* | (physicalDeliveryOfficeName=Braga) |



**Group Information**

Access Control Groups:
Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification
Standard CTI Allow Control of Phones supporting C
Standard CTI Allow Control of Phones supporting R
Standard CTI Enabled

Feature Group Template: My Feature Group

☑ Apply mask to synced telephone numbers to create a new line for inserted users

Mask: 35121454XXXX

☑ Assign new line from the pool list if one was not created based on a synced LDAP te

Next Candidate DN: 2004

| Order | DN Pool Start | DN Pool End |
|---|---|---|
| | 2000 | 2100 |

# LDAP Filters

There is a rich syntax to create ldap filters :

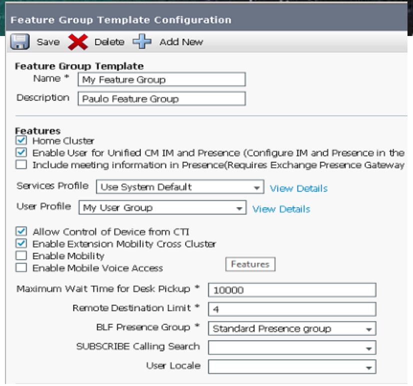
| | | |
|---|---|---|
| Equality | (attribute=abc) | (&(objectclass=user)(cn=Paulo Jorge Correia) |
| Negation | (!(attribute=abc)) | (!objectClass=computer) |
| Presence | (attribute=*) | (Department=*) |
| Absence | (!(attribute=*)) | (!manager=*) |
| Greater than | (attribute>=abc) | (telephoneNumber>=5000) |
| Less than | (attribute<=abc) | (telephoneNumber<=6000) |
| Wildcards | | (mail=*@cisco.com) |

You can get more information in :

http://www.ldapexplorer.com/en/manual/109010000-ldap-filter-syntax.htm

# What is a Feature Group Template

Various FGT ( Feature Group Template ) parameters include Home Cluster ,Enable Mobility, Enable EMCC, Calling Search Space, Enable User for Unified CM IM and Presence, User Locale, Enable Mobile Voice Access etc.



**Feature Group Template**

Name * My Feature Group
Description Paulo Feature Group

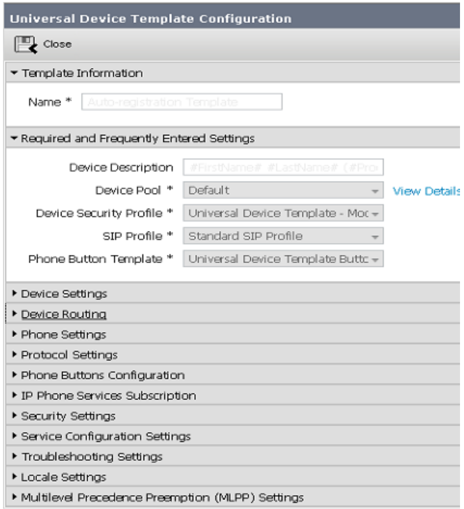
**Features**

☑ Home Cluster
☑ Enable User for Unified CM IM and Presence (Configure IM and Presence in the
☐ Include meeting information in Presence(Requires Exchange Presence Gateway

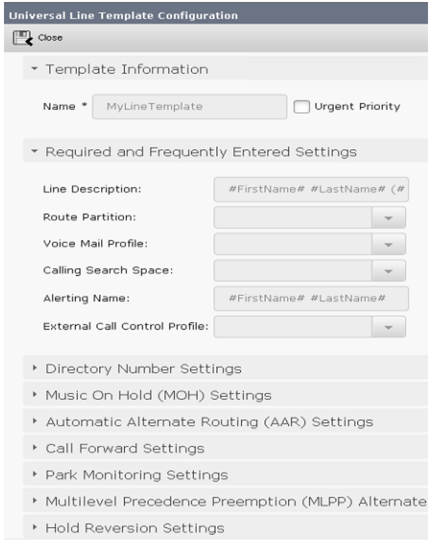
Services Profile Use System Default View Details
User Profile My User Group View Details

☑ Allow Control of Device from CTI
☑ Enable Extension Mobility Cross Cluster
☐ Enable Mobility
☐ Enable Mobile Voice Access

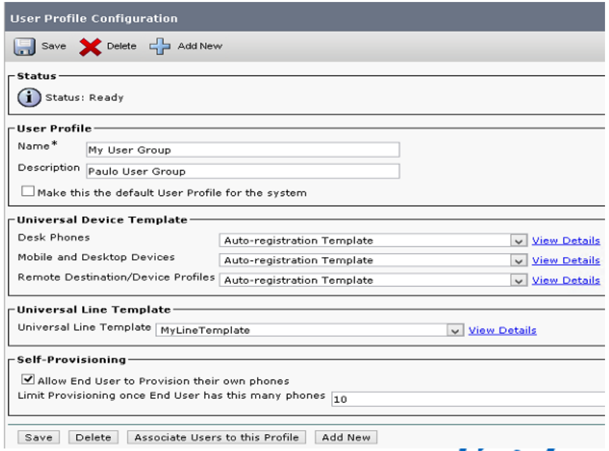
Maximum Wait Time for Desk Pickup * 10000
Remote Destination Limit * 4
BLF Presence Group * Standard Presence group
SUBSCRIBE Calling Search
User Locale


Universal Device Template Configuration
Close
Template Information
Required and Frequently Entered Settings
Device Settings
Device Routing
Phone Settings
Protocol Settings
Phone Buttons Configuration
IP Phone Services Subscription
Security Settings
Service Configuration Settings
Troubleshooting Settings
Locale Settings
Multilevel Precedence Preemption (MLPP) Settings

Name * Auto-registration Template
Device Description #FirstName# #LastName# (#Pro
Device Pool * Default View Details
Device Security Profile * Universal Device Template - Moc
SIP Profile * Standard SIP Profile
Phone Button Template * Universal Device Template Buttc


Universal Line Template Configuration
Close
Template Information
Required and Frequently Entered Settings
Directory Number Settings
Music On Hold (MOH) Settings
Automatic Alternate Routing (AAR) Settings
Call Forward Settings
Park Monitoring Settings
Multilevel Precedence Preemption (MLPP) Alternate
Hold Reversion Settings

Name * MyLineTemplate ☐ Urgent Priority
Line Description: #FirstName# #LastName# (#
Route Partition:
Voice Mail Profile:
Calling Search Space:
Alerting Name: #FirstName# #LastName#
External Call Control Profile:



**Status**

Status: Ready

**User Profile**

Name* My User Group
Description Paulo User Group
☐ Make this the default User Profile for the system

**Universal Device Template**

Desk Phones Auto-registration Template View Details
Mobile and Desktop Devices Auto-registration Template View Details
Remote Destination/Device Profiles Auto-registration Template View Details

**Universal Line Template**

Universal Line Template MyLineTemplate View Details

**Self-Provisioning**

☑ Allow End User to Provision their own phones
Limit Provisioning once End User has this many phones 10

# Performance

- The maximum number of users that may be synced into a cluster is 160,000. This user account limit is enforced in release 10.0(1).
  - Up to 80,000 accounts are supported in release 8.6(2)-9.x
  - Up to 60,000 accounts are supported in release 6.x-8.6(1)
- The maximum number of LDAP sync agreements is 20 in release 10.0.
  - Earlier releases support up to 5 agreements
- Using 20 LDAP sync agreements with 160,000 user accounts simultaneously is not supported.
- Initial synchronisation times increase substantially (multiple hours) as the number of users and the number of sync agreements increase.

**Cisco recommends:**

- Configure < 10 agreements when 160,000 User Accounts are synced
- Configure up to 20 sync agreements when the total number of user accounts is < 80,000

# Performance

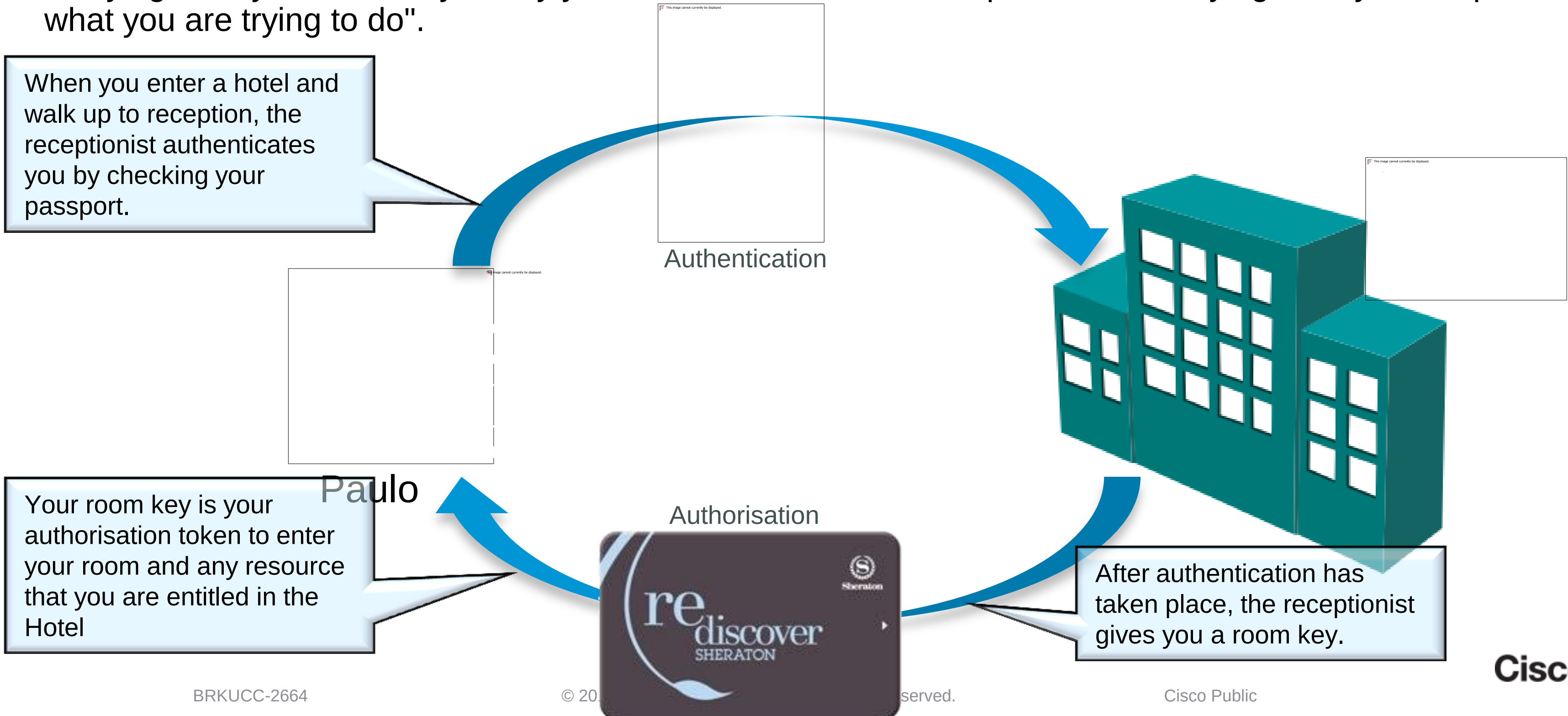
- Initial synchronisation for 60,000 User Accounts:
  - Unified CM 7.1(x) with 5 agreements ~30 minutes
  - Unified CM 8.0(1) with 5 agreements ~22 minutes
- Initial synchronisation for 80,000 User Accounts:
  - Unified CM 8.6(2) with 5 agreements ~24 minutes
  - Unified CM 9.x with 5 agreements ~38 minutes
  - Unified CM 10.0(1) with 10 agreements ~44 minutes
  - Unified CM 10.0(1) with 20 agreements ~2 hours
- Initial synchronisation for 160,000 User Accounts:
  - Unified CM 10.0(1) with 10 agreements ~3 hours
- Subsequent synchronisation operations may take more/less time depending on the number of changes between synchronisation intervals.
- If custom LDAP attributes are configured, synchronisation times could be increased, potentially double.

# Single Sign-On Technologies

# 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.

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

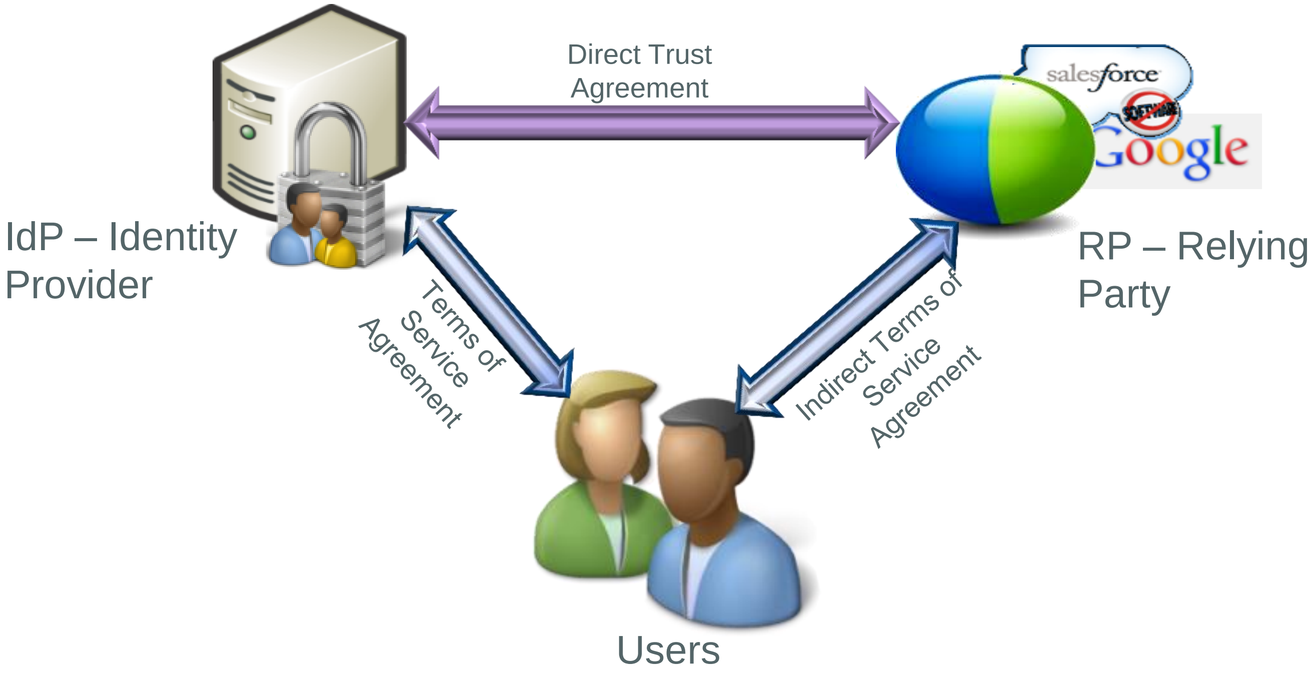
Your room key is your authorisation token to enter your room and any resource that you are entitled in the Hotel

This image cannot currently be displayed.
Authentication
This image cannot currently be displayed.
This image cannot currently be displayed.
Paulo
Authorisation
Sheraton
re discover
SHERATON

# 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.

# Identity Framework



# Role of Identity Providers (IdP)

Validate who you are?

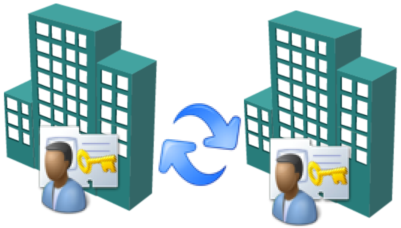
- Review personally identifying information to **prove you are who you say you are** (identity proofing), such as drivers license, passport, or biometric data
- Assign **attributes** (name, role, email address) in the identity management system.

**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.

# What is Federated Identity ?

- No long term employee credentials necessary on partner sites
- Automated user provisioning and removal
- Managed access to employee information
- Minimise sharing of attributes about a user
- Single sign-on
- Scalable establishment of relations

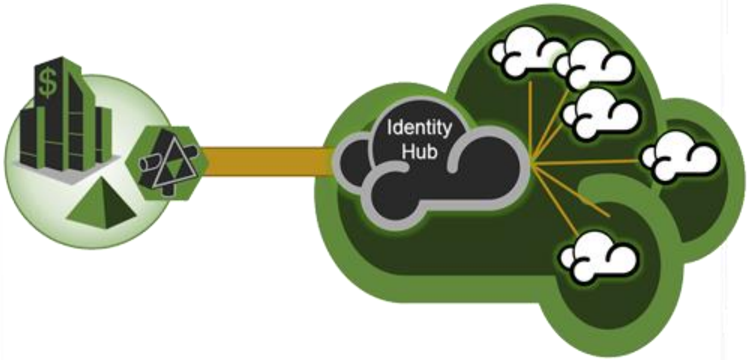


**"The only real problem is scaling. All others inherit from that one."**

**Mike O'Dell, Chief Scientist UUNET, 2000**

# What Does Federated Identity Buy Us?

- Describes the technologies, standards and use-cases which serve to enable the **portability of identity information** across otherwise autonomous security domains.



- **Provides the trust** needed for sharing these attributes between two or more parties in electronic transactions.

- **Facilitates user access** to online applications or resources through one user account.

# SSO Protocols

**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.

# SAML 2.0

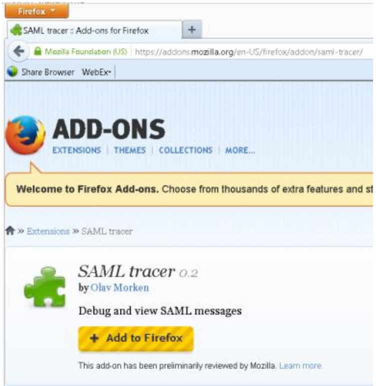
- The SAML standard is managed by the OASIS Security Services Technical Committee
  – http://www.oasis-open.org/committees/security

SAML is a protocol specification to use when two servers need to share users identity information. Nothing in the SAML specification provides the actual authentication service, with it we can :

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

# Firefox is your Friend

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


Firefox
SAML tracer :: Add-ons for Firefox
Mozilla Foundation (US) https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/
Share Browser WebEx
ADD-ONS
EXTENSIONS
THEMES
COLLECTIONS
MORE...
» Extensions » SAML tracer
Add to Firefox

**Welcome to Firefox Add-ons.** Choose from thousands of extra features and st

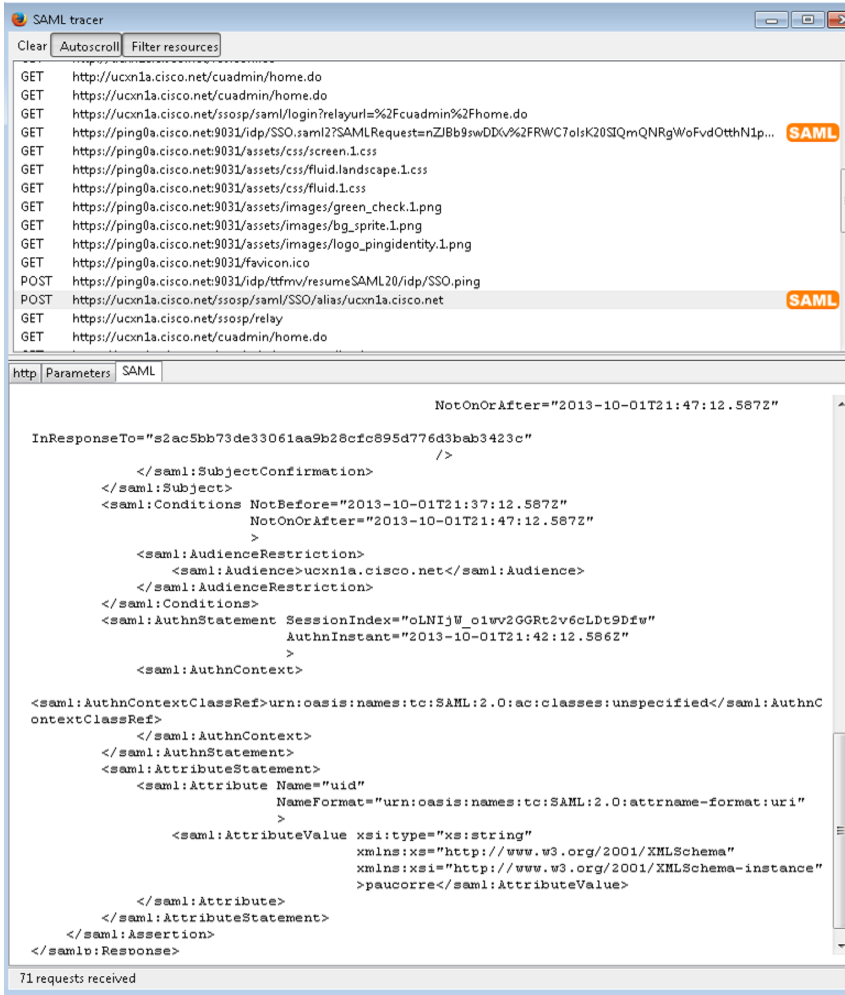
*SAML tracer* 0.2

by Olav Morken

Debug and view SAML messages

This add-on has been preliminarily reviewed by Mozilla. Learn more

It allow you to get the call flow of you SAML interaction and also decodes it



```
GET     http://ucxn1a.cisco.net/cuadmin/home.do
GET     https://ucxn1a.cisco.net/cuadmin/home.do
GET     https://ucxn1a.cisco.net/ssosp/saml/login?relayurl=%2Fcuadmin%2Fhome.do
GET     https://ping0a.cisco.net:9031/idp/SSO.saml2?SAMLRequest=nZJBb9swDDXv%2FRWC7olsK20SIQmQNRgWoFvdOtthN1p...
GET     https://ping0a.cisco.net:9031/assets/css/screen.1.css
GET     https://ping0a.cisco.net:9031/assets/css/fluid.landscape.1.css
GET     https://ping0a.cisco.net:9031/assets/css/fluid.1.css
GET     https://ping0a.cisco.net:9031/assets/images/green_check.1.png
GET     https://ping0a.cisco.net:9031/assets/images/bg_sprite.1.png
GET     https://ping0a.cisco.net:9031/assets/images/logo_pingidentity.1.png
GET     https://ping0a.cisco.net:9031/favicon.ico
POST    https://ping0a.cisco.net:9031/idp/ttfmv/resumeSAML20/idp/SSO.ping
POST    https://ucxn1a.cisco.net/ssosp/saml/SSO/alias/ucxn1a.cisco.net
GET     https://ucxn1a.cisco.net/ssosp/relay
GET     https://ucxn1a.cisco.net/cuadmin/home.do
```

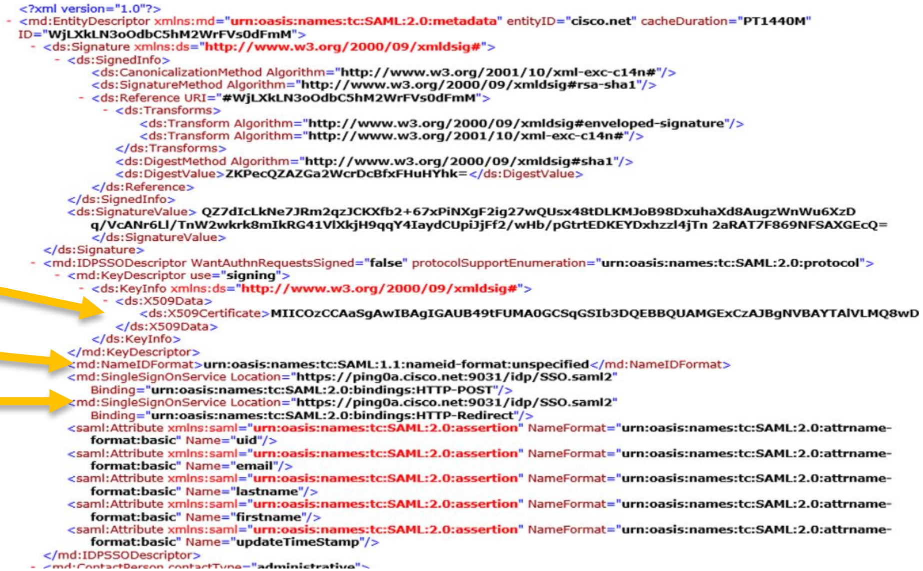
```
                                               NotOnOrAfter="2013-10-01T21:47:12.587Z"

InResponseTo="s2ac5bb73de33061aa9b28cfc895d776d3bab3423c"
                                               />
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2013-10-01T21:37:12.587Z"
                         NotOnOrAfter="2013-10-01T21:47:12.587Z"
                         >
            <saml:AudienceRestriction>
                <saml:Audience>ucxn1a.cisco.net</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement SessionIndex="oLNIjW_o1wv2GGRt2v6cLDt9Dfw"
                             AuthnInstant="2013-10-01T21:42:12.586Z"
                             >
            <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnC
ontextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="uid"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >paucorre</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

71 requests received

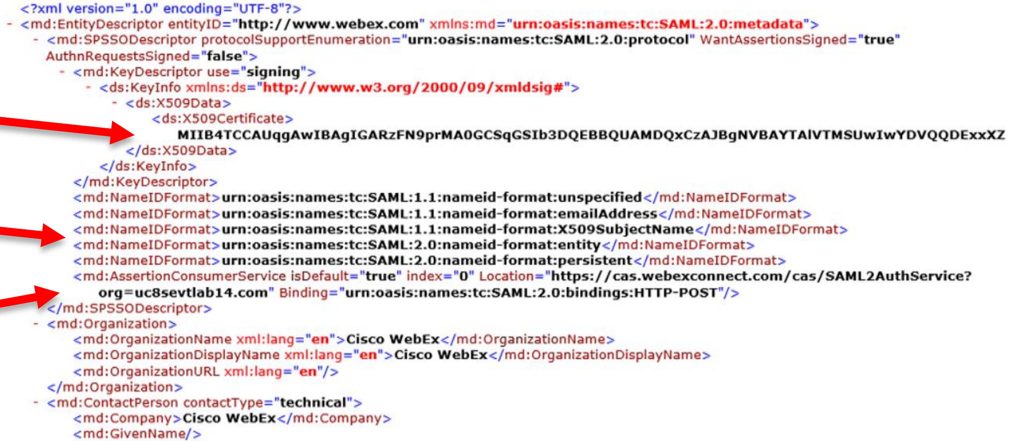
# SAML 2.0 Flow

## Trust Agreement

Metadata Exchange



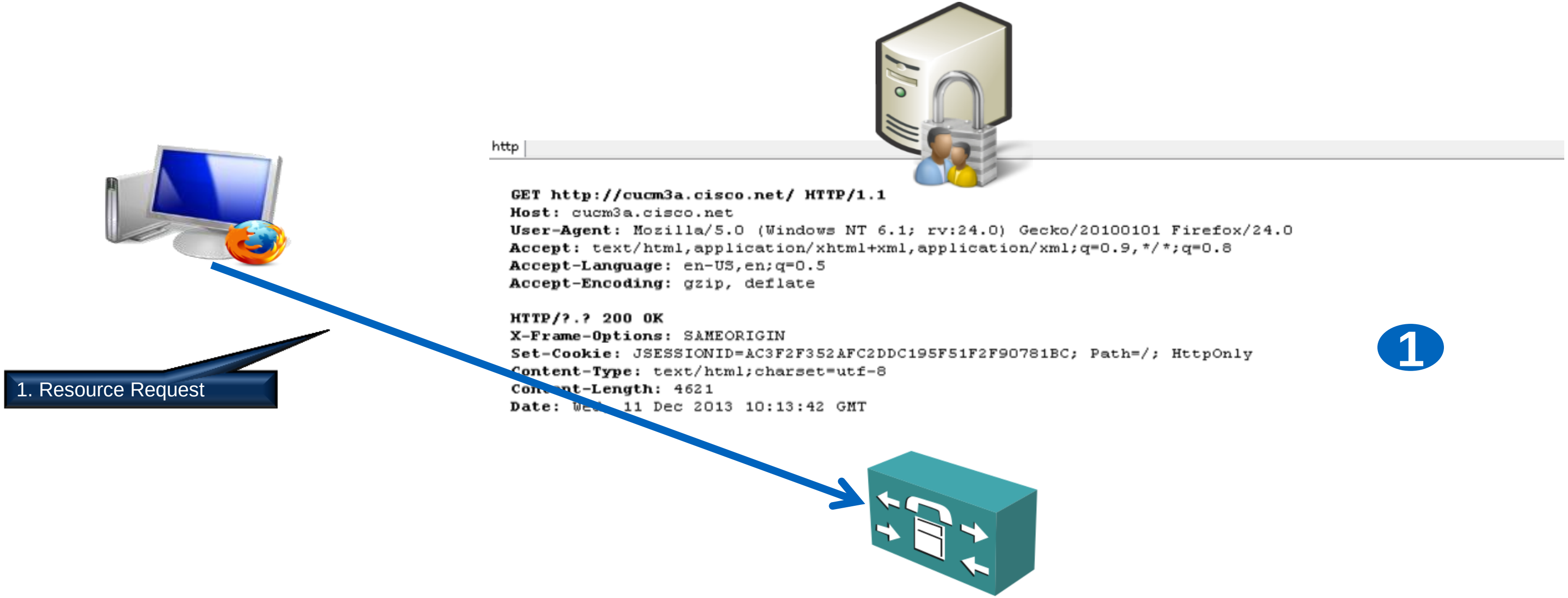
```
  <?xml version="1.0"?>
- <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cisco.net" cacheDuration="PT1440M"
  ID="WjLXkLN3oOdbC5hM2WrFVs0dFmM">
  - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:SignedInfo>
        <ds:CanonicalizationMethod 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>ZKPecQZAZGa2WcrDcBfxFHuHYhk=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue> QZ7dIcLkNe7JRm2qzJCKXfb2+67xPiNXgF2ig27wQUsx48tDLKMJoB98DxuhaXd8AugzWnWu6XzD
        q/VcANr6Ll/TnW2wkrk8mIkRG41VlXkjH9qqY4IaydCUpiJjFf2/wHb/pGtrtEDKEYDxhzzl4jTn 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>MIICOzCCAaSgAwIBAgIGAUB49tFUMA0GCSqGSIb3DQEBBQUAMGExCzAJBgNVBAYTAlVLMQ8wD
          </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"/>
      <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>
              MIIB4TCCAUqgAwIBAgIGARzFN9prMA0GCSqGSIb3DQEBBQUAMDQxCzAJBgNVBAYTAlVTMSUwIwYDVQQDExxXZ
          </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://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

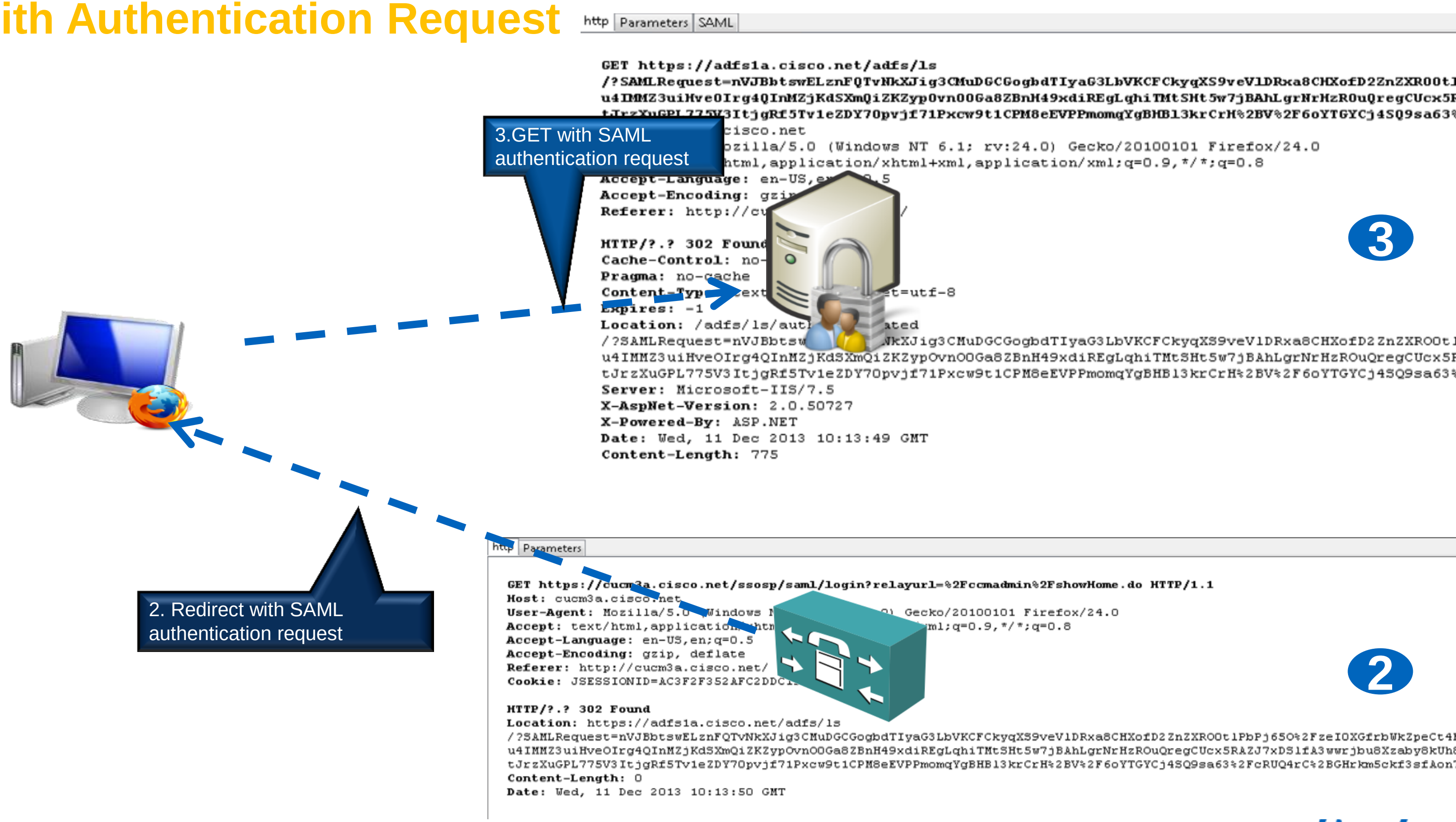
## Resource Request



```
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/?.? 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
```

# SAML 2.0 Flow

## Redirect with Authentication Request

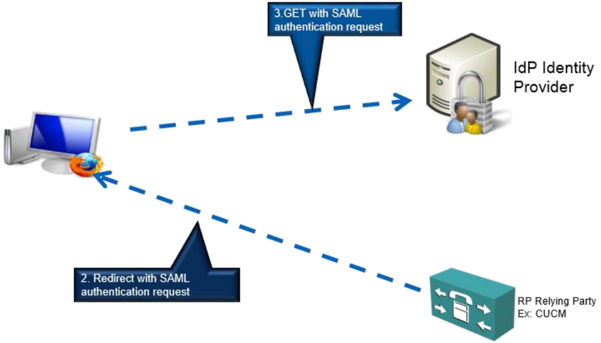


```
GET https://adfs1a.cisco.net/adfs/ls
/?SAMLRequest=nVJBbtswELznFQTvNkXJig3CMuDGCGogbdTIyaG3LbVKCFCkyqXS9veV1DRxa8CHXofD2ZnZXR00tI
u4IMMZ3uiHveOIrg4QInMZjKdSXmQiZKZypOvnO0Ga8ZBnH49xdiREgLqhiTMtSHt5w7jBAhLgrNrHzROuQregCUcx5R
tJrzXuGPL775V3ItjgRf5Tv1eZDY7Opvjf71Pxcw9t1CPM8eEVPPmomqYgBHB13krCrH%2BV%2F6oYTGYCj4SQ9sa63%
                  cisco.net
                  ozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
                  html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,e     .5
Accept-Encoding: gzi
Referer: http://cu           /

HTTP/?.? 302 Found
Cache-Control: no-
Pragma: no-cache
Content-Typ   ext            t=utf-8
Expires: -1
Location: /adfs/ls/aut       ated
/?SAMLRequest=nVJBbtsw       NkXJig3CMuDGCGogbdTIyaG3LbVKCFCkyqXS9veV1DRxa8CHXofD2ZnZXROOtI
u4IMMZ3uiHveOIrg4QInMZjKdSXmQiZKZypOvnO0Ga8ZBnH49xdiREgLqhiTMtSHt5w7jBAhLgrNrHzROuQregCUcx5R
tJrzXuGPL775V3ItjgRf5Tv1eZDY7Opvjf71Pxcw9t1CPM8eEVPPmomqYgBHB13krCrH%2BV%2F6oYTGYCj4SQ9sa63%
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Wed, 11 Dec 2013 10:13:49 GMT
Content-Length: 775
```

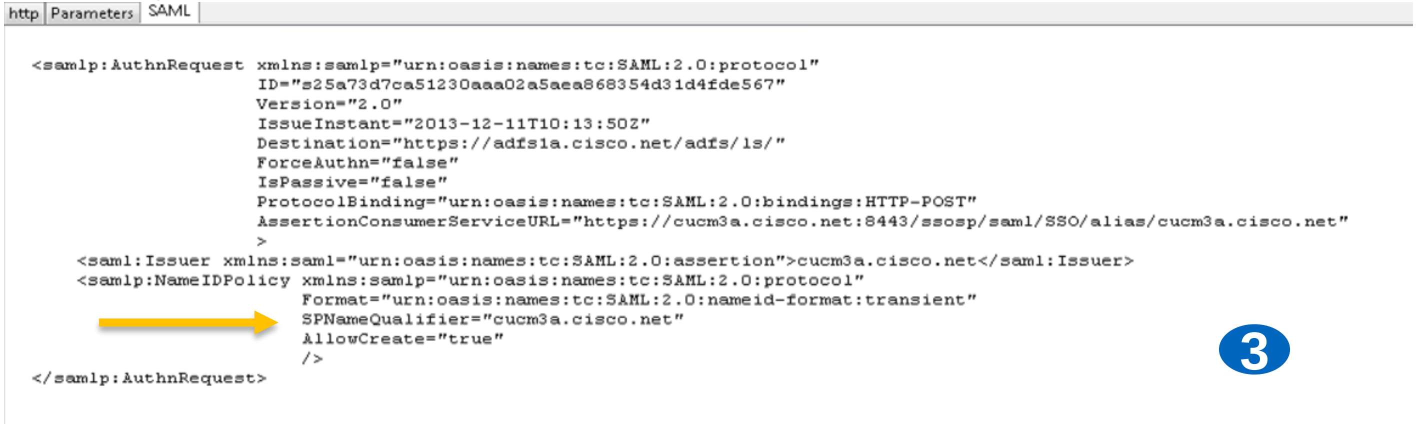
```
GET https://cucm3a.cisco.net/ssosp/saml/login?relayurl=%2Fccmadmin%2FshowHome.do HTTP/1.1
Host: cucm3a.cisco.net
User-Agent: Mozilla/5.0 (Windows N              ) Gecko/20100101 Firefox/24.0
Accept: text/html,application/xhtm              ml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://cucm3a.cisco.net/
Cookie: JSESSIONID=AC3F2F352AFC2DDC1

HTTP/?.? 302 Found
Location: https://adfs1a.cisco.net/adfs/ls
/?SAMLRequest=nVJBbtswELznFQTvNkXJig3CMuDGCGogbdTIyaG3LbVKCFCkyqXS9veV1DRxa8CHXofD2ZnZXROOt1PbPj65O%2FzeIOXGfrbWkZpeCt4I
u4IMMZ3uiHveOIrg4QInMZjKdSXmQiZKZypOvnO0Ga8ZBnH49xdiREgLqhiTMtSHt5w7jBAhLgrNrHzROuQregCUcx5RAZJ7xDS1fA3wwrjbu8Xzaby8kUh8
tJrzXuGPL775V3ItjgRf5Tv1eZDY7Opvjf71Pxcw9t1CPM8eEVPPmomqYgBHB13krCrH%2BV%2F6oYTGYCj4SQ9sa63%2FcRUQ4rC%2BGHrkm5ckf3sfAon7
Content-Length: 0
Date: Wed, 11 Dec 2013 10:13:50 GMT
```

# SAML 2.0 Flow

## Redirect with Authentication Request



3.GET with SAML authentication request
IdP Identity Provider
2. Redirect with SAML authentication request
RP Relying Party
Ex: CUCM

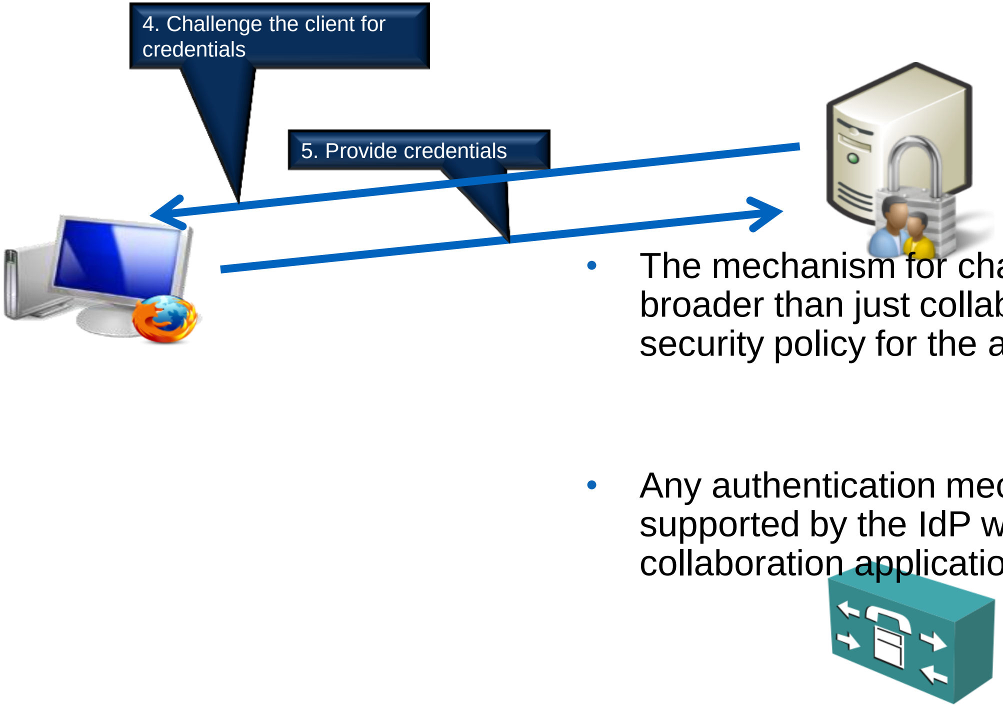


```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    ID="s25a73d7ca51230aaa02a5aea868354d31d4fde567"
                    Version="2.0"
                    IssueInstant="2013-12-11T10:13:50Z"
                    Destination="https://adfs1a.cisco.net/adfs/ls/"
                    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



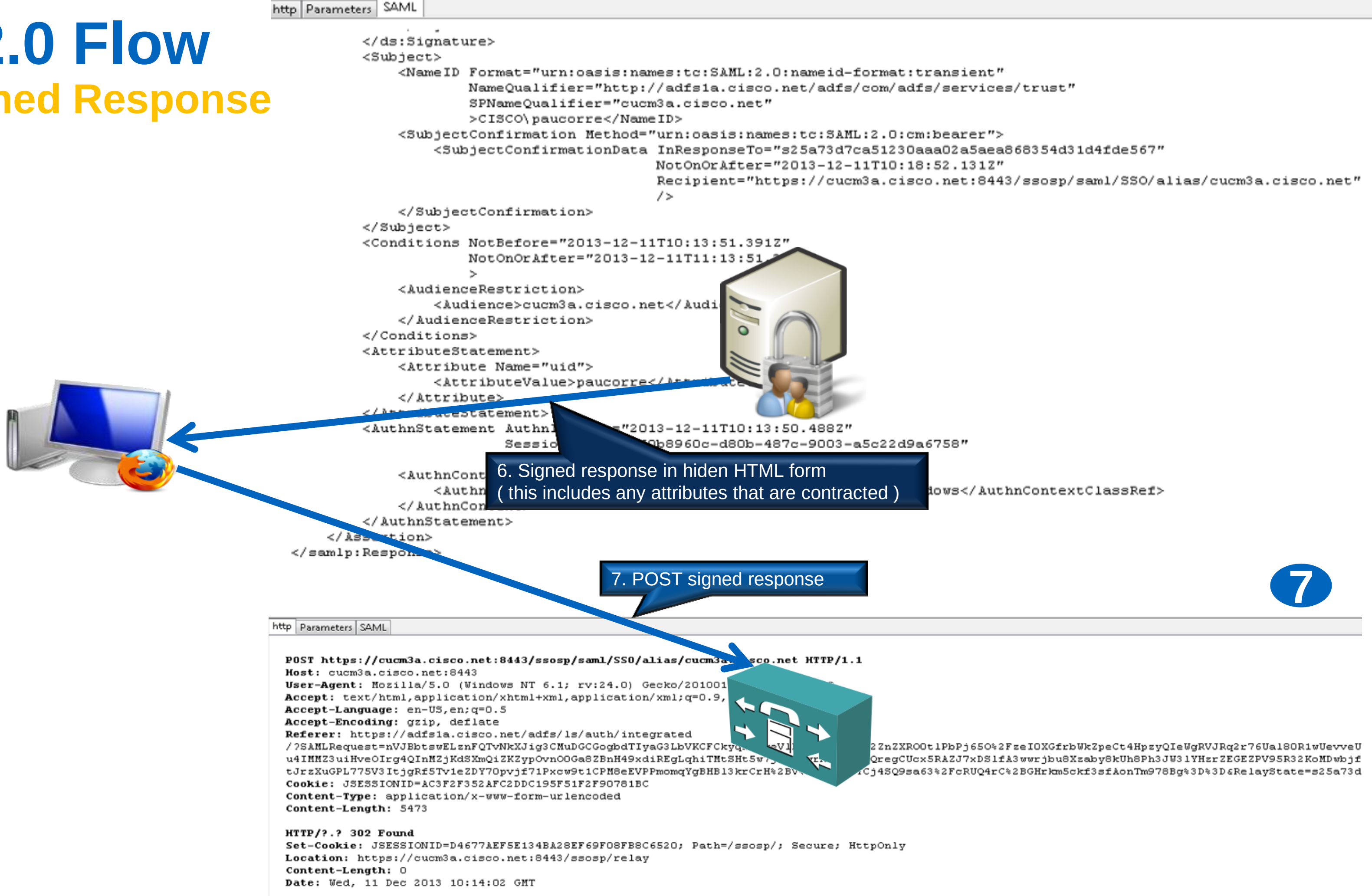
- The mechanism for challenge the users is something broader than just collaboration, it should comply to the security policy for the application in the organisation

4 5

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

# SAML 2.0 Flow

## Post a Signed Response



```
            </ds:Signature>
            <Subject>
                <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                        NameQualifier="http://adfs1a.cisco.net/adfs/com/adfs/services/trust"
                        SPNameQualifier="cucm3a.cisco.net"
                        >CISCO\paucorre</NameID>
                <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <SubjectConfirmationData InResponseTo="s25a73d7ca51230aaa02a5aea868354d31d4fde567"
                                             NotOnOrAfter="2013-12-11T10:18:52.131Z"
                                             Recipient="https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a.cisco.net"
                                             />
                </SubjectConfirmation>
            </Subject>
            <Conditions NotBefore="2013-12-11T10:13:51.391Z"
                        NotOnOrAfter="2013-12-11T11:13:51.
                        >
                <AudienceRestriction>
                    <Audience>cucm3a.cisco.net</Audi
                </AudienceRestriction>
            </Conditions>
            <AttributeStatement>
                <Attribute Name="uid">
                    <AttributeValue>paucorre</
                </Attribute>
            </       Statement>
            <AuthnStatement Authn        ="2013-12-11T10:13:50.488Z"
                            Sessio        0b8960c-d80b-487c-9003-a5c22d9a6758"

                <AuthnCont
                    <Authn                                          dows</AuthnContextClassRef>
                </AuthnCon
            </AuthnStatement>
        </As     tion>
    </samlp:Respo
```

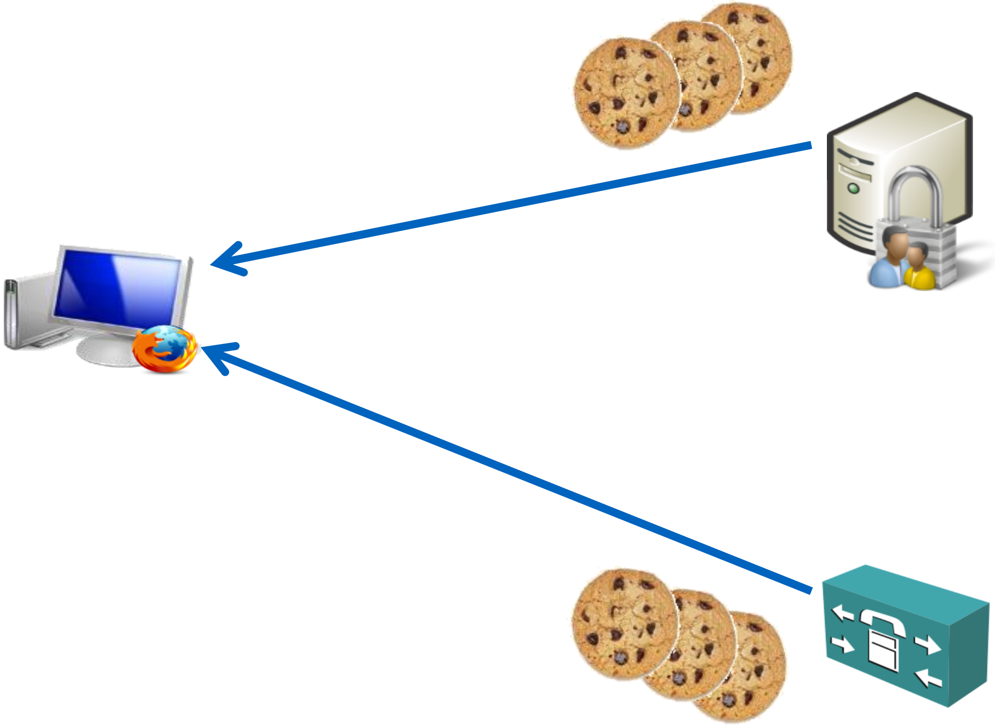
6. Signed response in hiden HTML form
( this includes any attributes that are contracted )

7. POST signed response

```
POST https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a  sco.net HTTP/1.1
Host: cucm3a.cisco.net:8443
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://adfs1a.cisco.net/adfs/ls/auth/integrated
/?SAMLRequest=nVJBbtswELznFQTvNkXJig3CMuDGCGogbdTIyaG3LbVKCFCkyq            2ZnZXROOt1PbPj65O%2FzeIOXGfrbWkZpeCt4HpzyQIeWgRVJRq2r76Ual8OR1wUevveU
u4IMMZ3uiHveOIrg4QInMZjKdSXmQiZKZypOvnO0Ga8ZBnH49xdiREgLqhiTMtSHt5w            QregCUcx5RAZJ7xDS1fA3wwrjbu8Xzaby8kUh8Ph3JW31YHzrZEGEZPV95R32KoMDwbjf
tJrzXuGPL775V3ItjgRf5Tv1eZDY7Opvjf71Pxcw9t1CPM8eEVPPmomqYgBHB13krCrH%2BV       Cj4SQ9sa63%2FcRUQ4rC%2BGHrkm5ckf3sfAonTm978Bg%3D%3D&RelayState=s25a73d
Cookie: JSESSIONID=AC3F2F352AFC2DDC195F51F2F90781BC
Content-Type: application/x-www-form-urlencoded
Content-Length: 5473

HTTP/?.? 302 Found
Set-Cookie: JSESSIONID=D4677AEF5E134BA28EF69F08FB8C6520; Path=/ssosp/; Secure; HttpOnly
Location: https://cucm3a.cisco.net:8443/ssosp/relay
Content-Length: 0
Date: Wed, 11 Dec 2013 10:14:02 GMT
```

# SAML 2.0 Flow

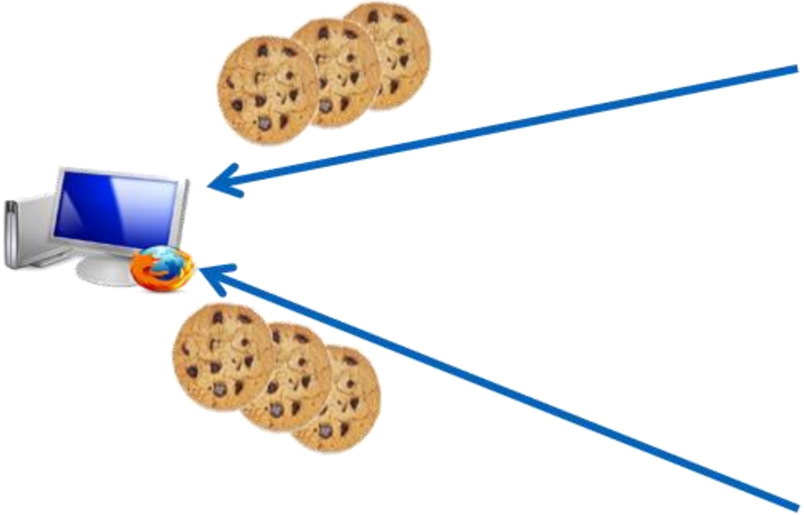
## Cookies to prevent re-authentication

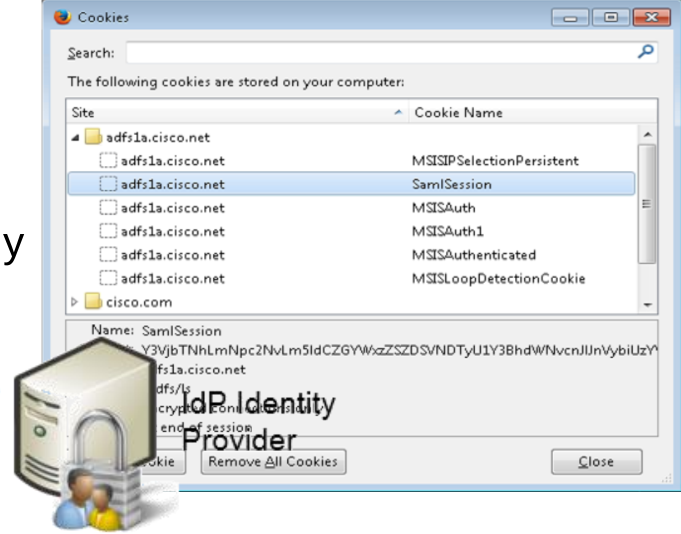


# SAML 2.0 Flow

## Cookies to prevent re-authentication

**IdP Cookie** that normally is valid for 48 hours



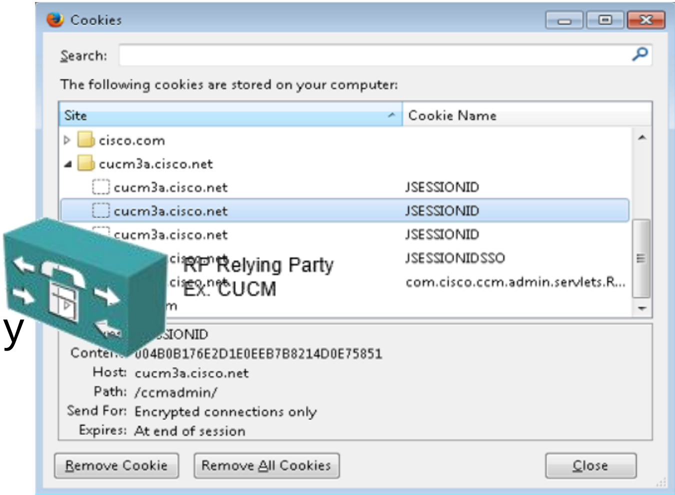


The following cookies are stored on your computer:

| Site | Cookie Name |
|---|---|
| adfs1a.cisco.net | |
| adfs1a.cisco.net | MSISIPSelectionPersistent |
| adfs1a.cisco.net | SamlSession |
| adfs1a.cisco.net | MSISAuth |
| adfs1a.cisco.net | MSISAuth1 |
| adfs1a.cisco.net | MSISAuthenticated |
| adfs1a.cisco.net | MSISLoopDetectionCookie |
| cisco.com | |

Name: SamlSession
Y3VjbTNhLmNpc2NvLm5ldCZGYWxzZSZDSVNDTyU1Y3BhdWNvcnJlJnVybiUzY
fs1a.cisco.net
dfs/ls
crypted connections only
end of session

**Service Cookie** that normally is valid for 30 minutes



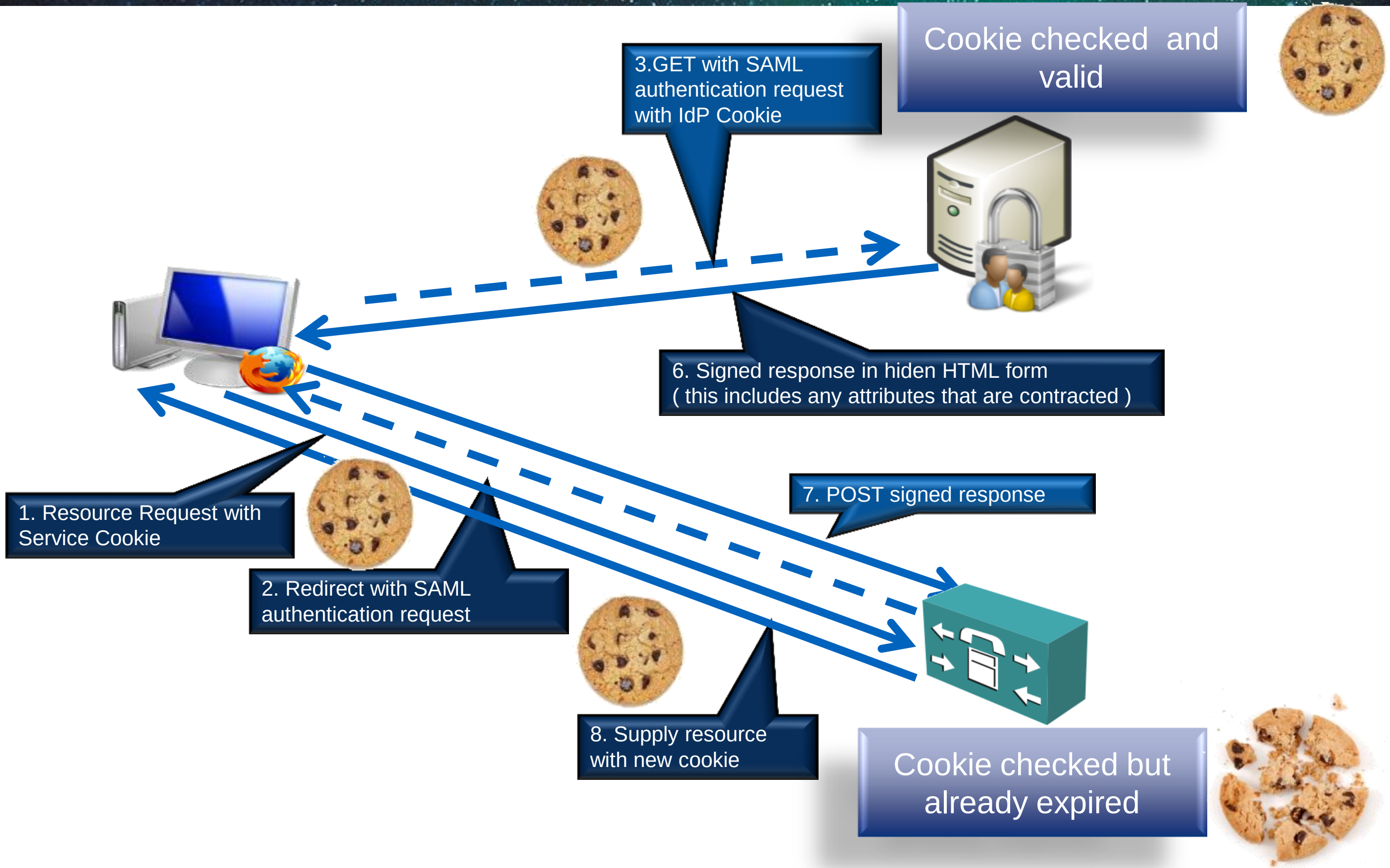
The following cookies are stored on your computer:

| Site | Cookie Name |
|---|---|
| cisco.com | |
| cucm3a.cisco.net | |
| cucm3a.cisco.net | JSESSIONID |
| cucm3a.cisco.net | JSESSIONID |
| cucm3a.cisco.net | JSESSIONID |
| cisco.net | JSESSIONIDSSO |
| cisco.net | com.cisco.ccm.admin.servlets.R... |
| m | |

SSIONID
Conte 004B0B176E2D1E0EEB7B8214D0E75851
Host: cucm3a.cisco.net
Path: /ccmadmin/
Send For: Encrypted connections only
Expires: At end of session

# SAML 2.0 Flow

## Cookies to prevent re-authentication



Cookie checked and valid

3.GET with SAML authentication request with IdP Cookie

6. Signed response in hiden HTML form ( this includes any attributes that are contracted )

7. POST signed response

1. Resource Request with Service Cookie

2. Redirect with SAML authentication request

8. Supply resource with new cookie

Cookie checked but already expired

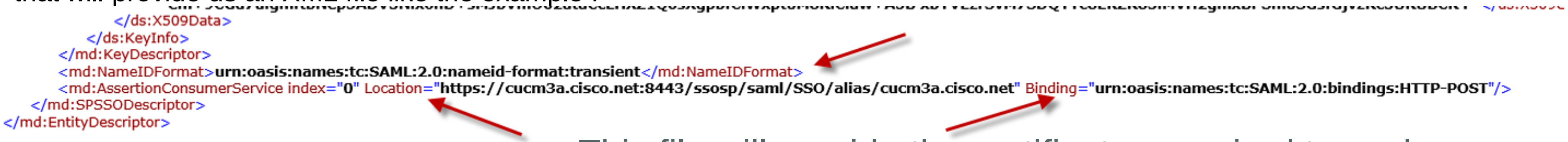
# Enabling SAML SSO On-Prem

# Configuring SAML Integration

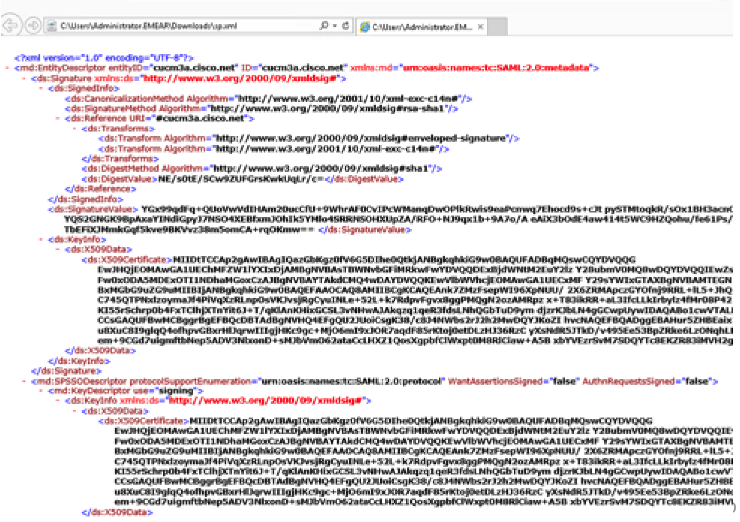
## 1. Get the metadata from the SP

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

- In the example of CUCM we get it from the URL https://<CUCM IP Address or FQDN>:8443/ssosp/ws/config/metadata/sp that will provide us an XML file like the example :



```
            </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>
```



C:\Users\Administrator.EMEAR\Downloads\sp.xml
C:\Users\Administrator.EM...

```
  <?xml version="1.0" encoding="UTF-8"?>
- <md:EntityDescriptor entityID="cucm3a.cisco.net" ID="cucm3a.cisco.net" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <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="#cucm3a.cisco.net">
        - <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>NE/s0tE/SCw9ZUFGrsKwkUqLr/c=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue> YGx99qdFq+QUoVwVdIHAm20ucCfU+9WhrAF0CvIPcWManqDwOPlkRwis9eaPcmwq7Ehocd9s+cJt pySTMtoqkR/sOx1BH3acn
        YQS2GNGK9BpAxaYINdiGpyJ7NSO4XEBfxmJOh1k5YMlo4SRRNSOHXUpZA/RFO+NJ9qx1b+9A7o/A eAlX3bOdE4aw414t5WC9HZQohu/fe61Ps/
        TbEFiXJMmkGqf5kve9BKVvz38m5omCA+rqOKmw== </ds:SignatureValue>
    - <ds:KeyInfo>
      - <ds:X509Data>
          <ds:X509Certificate>MIIDtTCCAp2gAwIBAgIQazGbKgz0fV6G5DIhe0QtkjANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQG
            EwJHQjEOMAwGA1UEChMFZW1lYXIxDjAMBgNVBAsTBWNvbGFiMRkwFwYDVQQDExBjdWNtM2EuY2lz Y28ubmV0MQ8wDQYDVQQIEwZs
            Fw0xODA5MDExOTI1NDhaMGoxCzAJBgNVBAYTAkdCMQ4wDAYDVQQKEwVlbWVhcjEOMAwGA1UECxMF Y29sYWIxGTAXBgNVBAMTEGN
            BxMGbG9uZG9uMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnk7ZMzFsepWI96XpNUU/ 2X6ZRMApczGYOfnj9RRL+lL5+JhQ
            C745QTPNxlzoymaJf4PiVqXzRLnpOsVKJvsjRgCyuINLe+52L+k7RdpvFgvx8ggPMQgN2ozAMRpz x+T83ikRR+aL3IfcLLkIrbylz4fMr08P42
            KI55rSchrp0b4FxTClhjXTnYit6J+T/qKlAnKHixGCSL3vNHwAJAkqzq1qeR3fdsLNhQGbTuD9ym djzrKJbLN4gGCwpUywIDAQABo1cwVTAL
            CCsGAQUFBwMCBggrBgEFBQcDBTAdBgNVHQ4EFgQU2JUoiCsgK38/c8J4NWbs2rJ2h2MwDQYJKoZI hvcNAQEFBQADggEBAHur5ZHBEaix
            u8XuC8I9glqQ4ofhpvGBxrHUqrwIIgjHKc9gc+MjO6mI9xJOR7aqdF85rKtoj0etDLzHJ36RzC yXsNdR5JTkD/v495Ee53BpZRke6LzONqhLl
            em+9CGd7uigmftbNep5ADV3NbxonD+sMJbVm062ataCcLHXZ1QosXgpbfClWxpt0M8RlClaw+A5B xbYVEzrSvM7SDQYTc8EKZR83lMVH2g
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
  - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="false" AuthnRequestsSigned="false">
    - <md:KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
            <ds:X509Certificate>MIIDtTCCAp2gAwIBAgIQazGbKgz0fV6G5DIhe0QtkjANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQG
              EwJHQjEOMAwGA1UEChMFZW1lYXIxDjAMBgNVBAsTBWNvbGFiMRkwFwYDVQQDExBjdWNtM2EuY2lz Y28ubmV0MQ8wDQYDVQQIE
              Fw0xODA5MDExOTI1NDhaMGoxCzAJBgNVBAYTAkdCMQ4wDAYDVQQKEwVlbWVhcjEOMAwGA1UECxMF Y29sYWIxGTAXBgNVBAMTE
              BxMGbG9uZG9uMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnk7ZMzFsepWI96XpNUU/ 2X6ZRMApczGYOfnj9RRL+lL5+
              C745QTPNxlzoymaJf4PiVqXzRLnpOsVKJvsjRgCyuINLe+52L+k7RdpvFgvx8ggPMQgN2ozAMRpz x+T83ikRR+aL3IfcLLkIrbylz4fMr08
              KI55rSchrp0b4FxTClhjXTnYit6J+T/qKlAnKHixGCSL3vNHwAJAkqzq1qeR3fdsLNhQGbTuD9ym djzrKJbLN4gGCwpUywIDAQABo1cwV
              CCsGAQUFBwMCBggrBgEFBQcDBTAdBgNVHQ4EFgQU2JUoiCsgK38/c8J4NWbs2rJ2h2MwDQYJKoZI hvcNAQEFBQADggEBAHur5ZHB
              u8XuC8I9glqQ4ofhpvGBxrHUqrwIIgjHKc9gc+MjO6mI9xJOR7aqdF85rKtoj0etDLzHJ36RzC yXsNdR5JTkD/v495Ee53BpZRke6LzON
              em+9CGd7uigmftbNep5ADV3NbxonD+sMJbVm062ataCcLHXZ1QosXgpbfClWxpt0M8RlClaw+A5B xbYVEzrSvM7SDQYTc8EKZR83lMV
          </ds:X509Data>
```

This file will provide the certificates required to exchange HTTP information

This file also provides information on what is the :

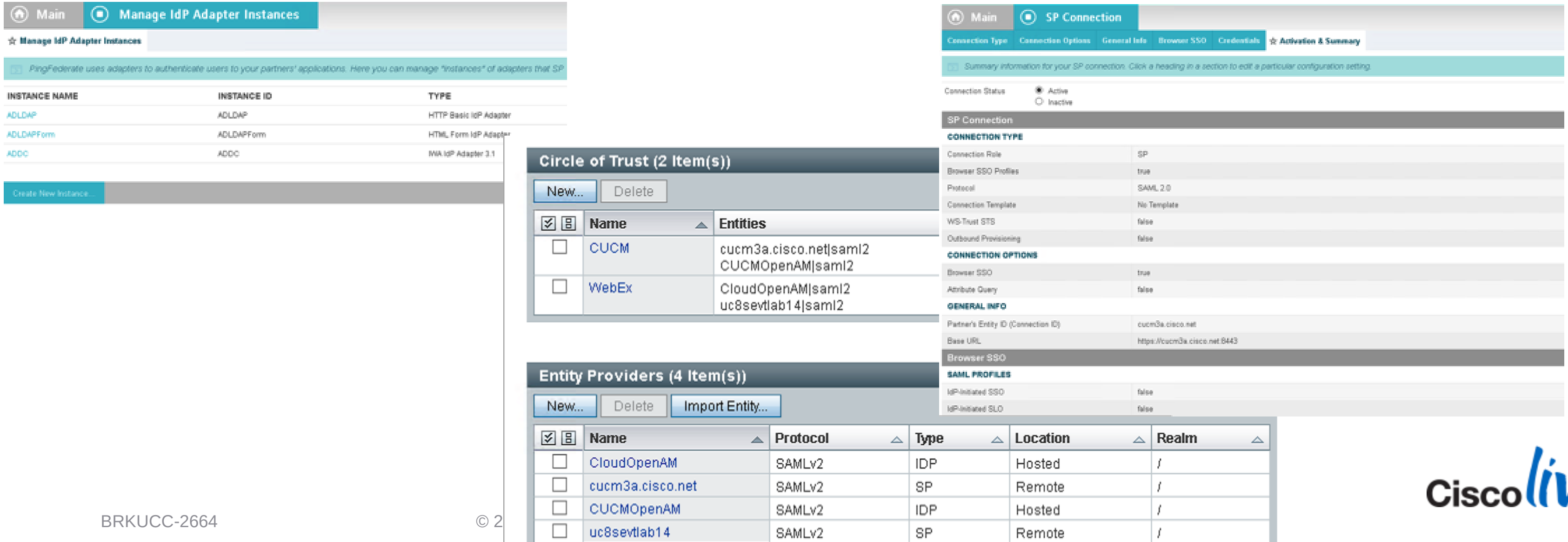
- NameID format
- Location of the Service
- What kind of SAML binding we are going to use

# Configuring SAML Integration

## 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. 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



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 | IWA IdP Adapter 3.1 |

Circle of Trust (2 Item(s))

| ☑ ⌸ | Name | Entities |
|---|---|---|
| □ | CUCM | cucm3a.cisco.net\|saml2<br>CUCMOpenAM\|saml2 |
| □ | WebEx | CloudOpenAM\|saml2<br>uc8sevtlab14\|saml2 |

Entity Providers (4 Item(s))

| ☑ ⌸ | Name | Protocol | Type | Location | Realm |
|---|---|---|---|---|---|
| □ | CloudOpenAM | SAMLv2 | IDP | Hosted | / |
| □ | cucm3a.cisco.net | SAMLv2 | SP | Remote | / |
| □ | CUCMOpenAM | SAMLv2 | IDP | Hosted | / |
| □ | uc8sevtlab14 | SAMLv2 | SP | Remote | / |

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:8443 |

Browser SSO

SAML PROFILES

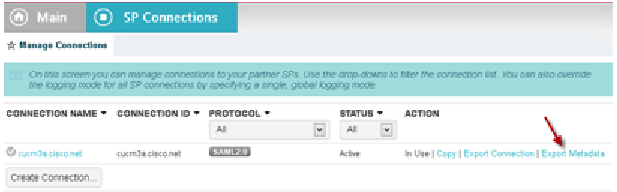
| | |
|---|---|
| IdP-Initiated SSO | false |
| IdP-Initiated SLO | false |

# Configuring SAML Integration

## 3. Export the metadata from the IdP

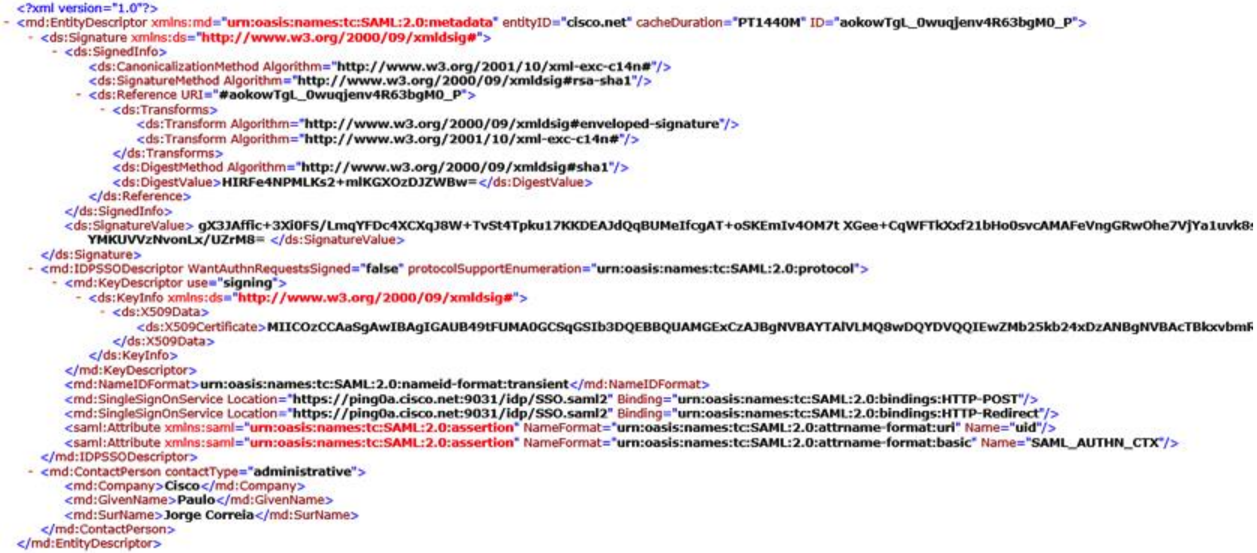
Similar to what we did in the beginning with the Collaboration Application we are going to export the metadata of the IdP to enable SSO on the SP

In our example we export the metadata from PingFederate SP and we include the X509 certificate that we require for the information exchange between the IdP <-> SP



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 |
|---|---|---|---|---|
| | | All | All | |
| cucm3a.cisco.net | cucm3a.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="aokowTgL_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="#aokowTgL_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>HIRFe4NPMLKs2+mlKGXOzDJZWBw=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue> gX3JAffic+3Xi0FS/LmqYFDc4XCXqJ8W+TvSt4Tpku17KKDEAJdQqBUMeIfcgAT+oSKEmIv4OM7t XGee+CqWFTkXxf21bHo0svcAMAFeVngGRwOhe7VjYa1uvk8
        YMKUVVzNvonLx/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>MIICOzCCAaSgAwIBAgIGAUB49tFUMA0GCSqGSIb3DQEBBQUAMGExCzAJBgNVBAYTAlVLMQ8wDQYDVQQIEwZMb25kb24xDzANBgNVBAcTBkxvbmR
          </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/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"/>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" 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="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>
```

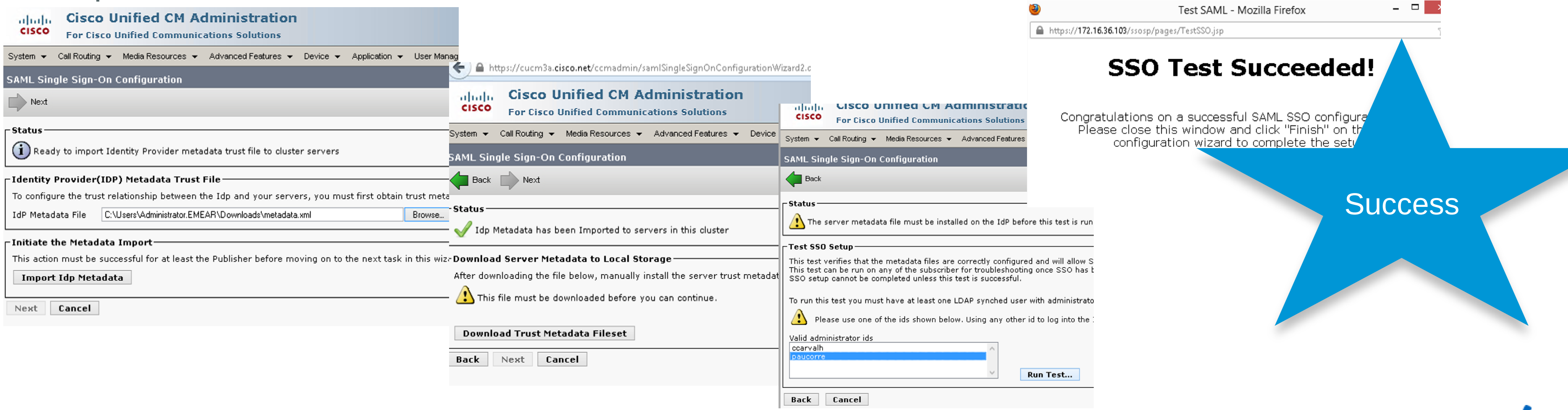
# Configuring SAML Integration

## 4. Import the metadata from the IdP and test the connection

1. Make sure that the Cisco Collaboration products like CUCM, uCNX, IM&P, Prime, CWMS, WebEx is using the same User Directory sources as the IdP.

2. Make sure that you have at least one user with Administration privileges

3. Import the IdP metadata, Download the Metadata Fileset and Run the Connection test



SAML Single Sign-On Configuration

Next

**Status**

Ready to import Identity Provider metadata trust file to cluster servers

**Identity Provider(IDP) Metadata Trust File**

To configure the trust relationship between the Idp and your servers, you must first obtain trust meta

IdP Metadata File C:\Users\Administrator.EMEAR\Downloads\metadata.xml Browse...

**Initiate the Metadata Import**

This action must be successful for at least the Publisher before moving on to the next task in this wiz

Import Idp Metadata

Next Cancel

https://cucm3a.cisco.net/ccmadmin/samlSingleSignOnConfigurationWizard2.c

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Device

SAML Single Sign-On Configuration

Back Next

**Status**

✓ Idp Metadata has been Imported to servers in this cluster

**Download Server Metadata to Local Storage**

After downloading the file below, manually install the server trust metadat

This file must be downloaded before you can continue.

Download Trust Metadata Fileset

Back Next Cancel

Cisco Unified CM Administratic
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features

SAML Single Sign-On Configuration

Back

**Status**

The server metadata file must be installed on the IdP before this test is run

**Test SSO Setup**

This test verifies that the metadata files are correctly configured and will allow S
This test can be run on any of the subscriber for troubleshooting once SSO has b
SSO setup cannot be completed unless this test is successful.

To run this test you must have at least one LDAP synched user with administrato

Please use one of the ids shown below. Using any other id to log into the

Valid administrator ids

ccarvalh
paucorre

Run Test...

Back Cancel

Test SAML - Mozilla Firefox

https://172.16.36.103/ssosp/pages/TestSSO.jsp

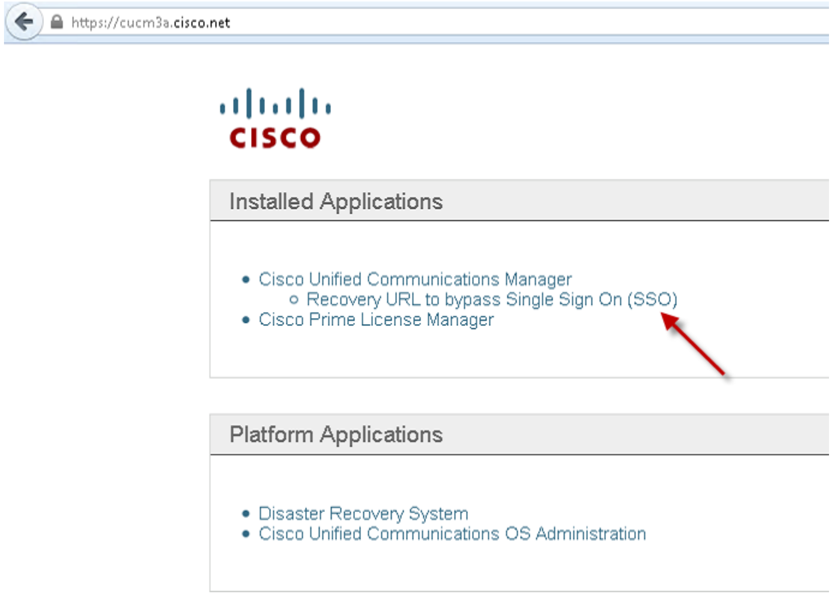
**SSO Test Succeeded!**

Congratulations on a successful SAML SSO configura
Please close this window and click "Finish" on th
configuration wizard to complete the setu

Success

# Administration Login with SSO Enabled

- Even after enabling SSO in the Cisco Collaboration Application, you will have have a way to do a local login with the default application user



https://cucm3a.cisco.net

Installed Applications

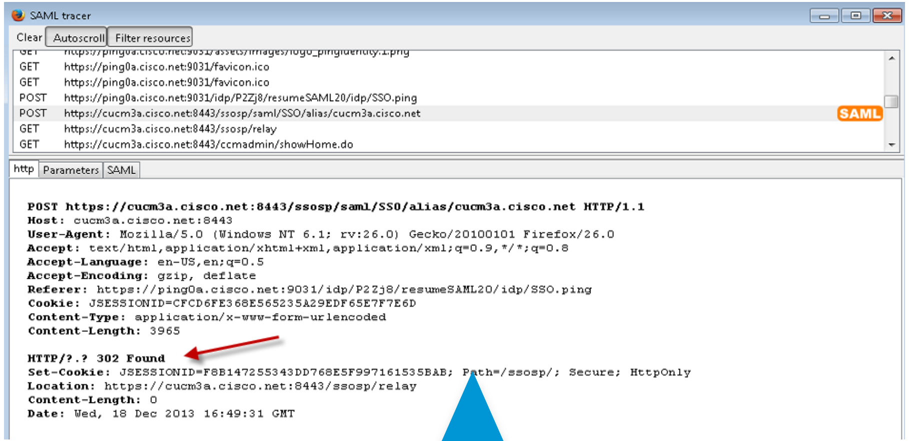
- Cisco Unified Communications Manager
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Prime License Manager

Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

# Administration Login with SSO Enabled

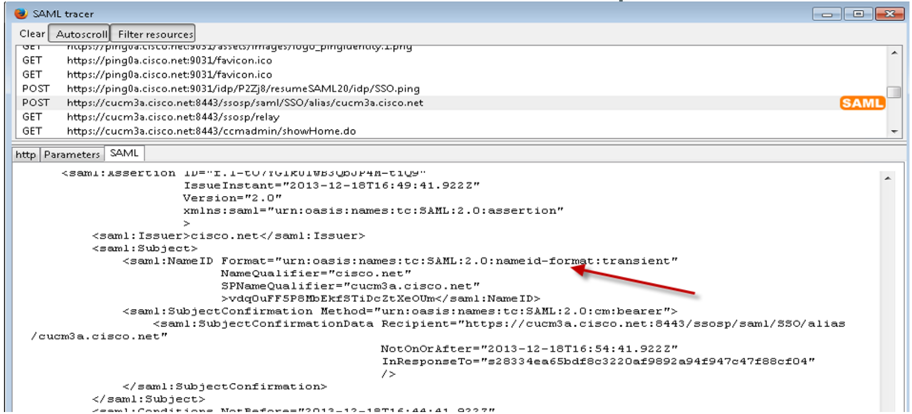
When the user logins to the for example to CUCM he will see and HTTP 302 Found as expected and the Name ID format and the attribute contracted.



```
GET    https://ping0a.cisco.net:9031/assets/images/logo_pingidentity.1.png
GET    https://ping0a.cisco.net:9031/favicon.ico
GET    https://ping0a.cisco.net:9031/favicon.ico
POST   https://ping0a.cisco.net:9031/idp/P2Zj8/resumeSAML20/idp/SSO.ping
POST   https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a.cisco.net
GET    https://cucm3a.cisco.net:8443/ssosp/relay
GET    https://cucm3a.cisco.net:8443/ccmadmin/showHome.do
```

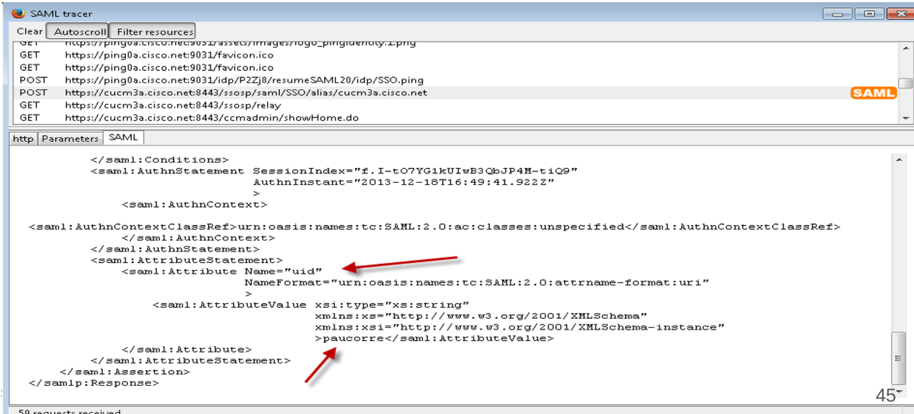
```
POST https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a.cisco.net HTTP/1.1
Host: cucm3a.cisco.net:8443
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:26.0) Gecko/20100101 Firefox/26.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ping0a.cisco.net:9031/idp/P2Zj8/resumeSAML20/idp/SSO.ping
Cookie: JSESSIONID=CFCD6FE368E565235A29EDF65E7F7E6D
Content-Type: application/x-www-form-urlencoded
Content-Length: 3965

HTTP/?.? 302 Found
Set-Cookie: JSESSIONID=F8B147255343DD768E5F997161535BAB; Path=/ssosp/; Secure; HttpOnly
Location: https://cucm3a.cisco.net:8443/ssosp/relay
Content-Length: 0
Date: Wed, 18 Dec 2013 16:49:31 GMT
```

Success



```
GET    https://ping0a.cisco.net:9031/assets/images/logo_pingidentity.1.png
GET    https://ping0a.cisco.net:9031/favicon.ico
GET    https://ping0a.cisco.net:9031/favicon.ico
POST   https://ping0a.cisco.net:9031/idp/P2Zj8/resumeSAML20/idp/SSO.ping
POST   https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a.cisco.net
GET    https://cucm3a.cisco.net:8443/ssosp/relay
GET    https://cucm3a.cisco.net:8443/ccmadmin/showHome.do
```

```
    <saml:Assertion ID="f.I-tO7YG1kUIwB3QbJP4M-tiQ9"
                    IssueInstant="2013-12-18T16:49:41.922Z"
                    Version="2.0"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    >
        <saml:Issuer>cisco.net</saml:Issuer>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                         NameQualifier="cisco.net"
                         SPNameQualifier="cucm3a.cisco.net"
                         >vdqOuFF5P8MbEkfSTiDcZtXeOUm</saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData Recipient="https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias
/cucm3a.cisco.net"
                                              NotOnOrAfter="2013-12-18T16:54:41.922Z"
                                              InResponseTo="s28334ea65bdf8c3220af9892a94f947c47f88cf04"
                                              />
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2013-12-18T16:44:41.922Z"
```



```
GET    https://ping0a.cisco.net:9031/assets/images/logo_pingidentity.1.png
GET    https://ping0a.cisco.net:9031/favicon.ico
GET    https://ping0a.cisco.net:9031/favicon.ico
POST   https://ping0a.cisco.net:9031/idp/P2Zj8/resumeSAML20/idp/SSO.ping
POST   https://cucm3a.cisco.net:8443/ssosp/saml/SSO/alias/cucm3a.cisco.net
GET    https://cucm3a.cisco.net:8443/ssosp/relay
GET    https://cucm3a.cisco.net:8443/ccmadmin/showHome.do
```

```
        </saml:Conditions>
        <saml:AuthnStatement SessionIndex="f.I-tO7YG1kUIwB3QbJP4M-tiQ9"
                             AuthnInstant="2013-12-18T16:49:41.922Z"
                             >
            <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="uid"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >paucorre</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

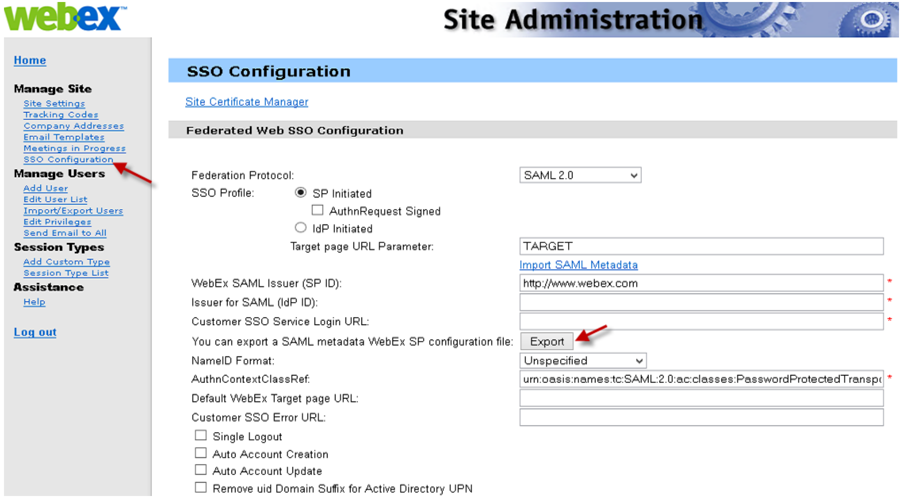
59 requests received

# Enabling SAML SSO 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



SSO Configuration

Site Certificate Manager

Federated Web SSO Configuration

Federation Protocol: SAML 2.0

SSO Profile: ● SP Initiated

□ AuthnRequest Signed

○ IdP Initiated

Target page URL Parameter: TARGET

Import SAML Metadata

WebEx SAML Issuer (SP ID): http://www.webex.com *

Issuer for SAML (IdP ID): *

Customer SSO Service Login URL: *

You can export a SAML metadata WebEx SP configuration file: Export

NameID Format: Unspecified

AuthnContextClassRef: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp *

Default WebEx Target page URL:

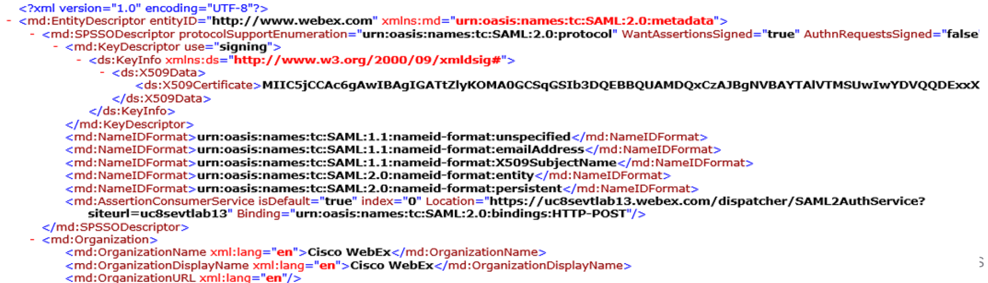
Customer SSO Error URL:

□ Single Logout

□ Auto Account Creation

□ Auto Account Update

□ Remove uid Domain Suffix for Active Directory UPN



```
  <?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>MIIC5jCCAc6gAwIBAgIGATtZlyKOMA0GCSqGSIb3DQEBBQUAMDQxCzAJBgNVBAYTAlVTMSUwIwYDVQQDExxX
          </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"/>
```

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

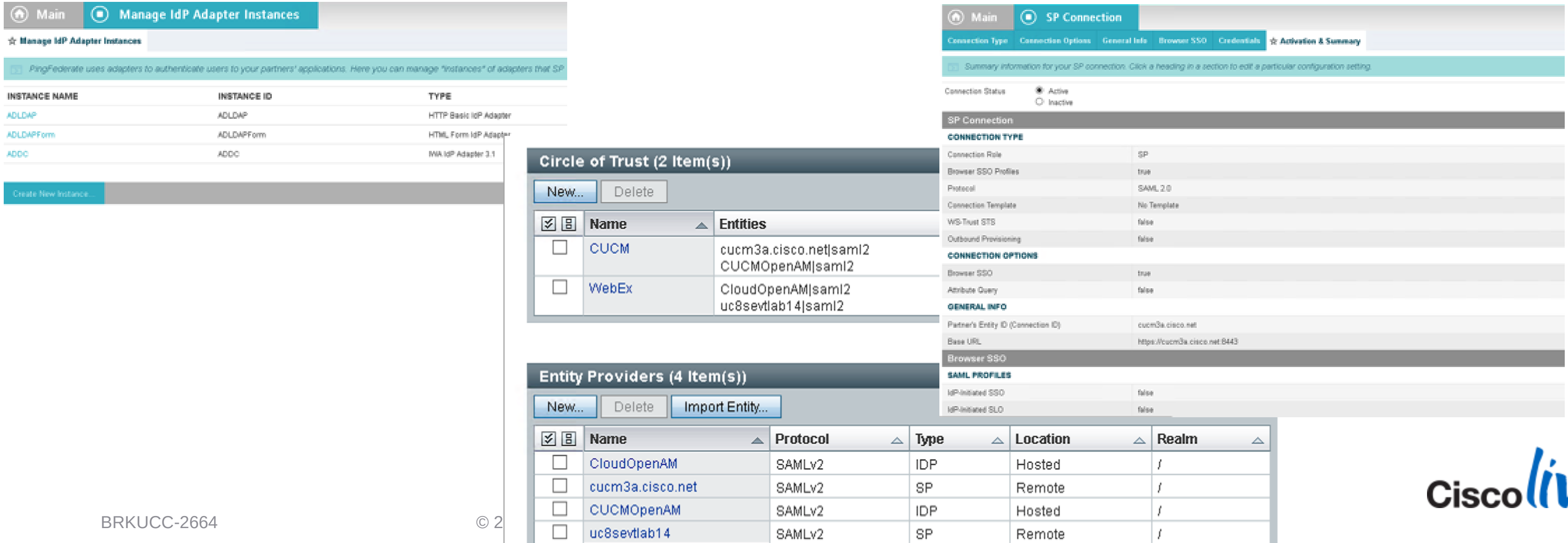
  *SAML 2.0 using HTTP-POST*

# 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



*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 | IWA IdP Adapter 3.1 |

**Circle of Trust (2 Item(s))**

| ☑ ⌸ | Name | Entities |
|---|---|---|
| □ | CUCM | cucm3a.cisco.net\|saml2<br>CUCMOpenAM\|saml2 |
| □ | WebEx | CloudOpenAM\|saml2<br>uc8sevtlab14\|saml2 |

**Entity Providers (4 Item(s))**

| ☑ ⌸ | Name | Protocol | Type | Location | Realm |
|---|---|---|---|---|---|
| □ | CloudOpenAM | SAMLv2 | IDP | Hosted | / |
| □ | cucm3a.cisco.net | SAMLv2 | SP | Remote | / |
| □ | CUCMOpenAM | SAMLv2 | IDP | Hosted | / |
| □ | uc8sevtlab14 | SAMLv2 | SP | Remote | / |

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

Connection Status ● Active ○ Inactive

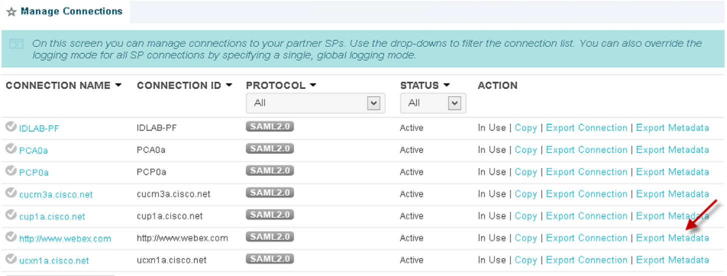
| SP Connection | |
|---|---|
| **CONNECTION TYPE** | |
| Connection Role | SP |
| Browser SSO Profiles | true |
| Protocol | SAML 2.0 |
| Connection Template | No Template |
| WS-Trust STS | false |
| Outbound Provisioning | false |
| **CONNECTION OPTIONS** | |
| Browser SSO | true |
| Attribute Query | false |
| **GENERAL INFO** | |
| Partner's Entity ID (Connection ID) | cucm3a.cisco.net |
| Base URL | https://cucm3a.cisco.net:8443 |
| 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 )

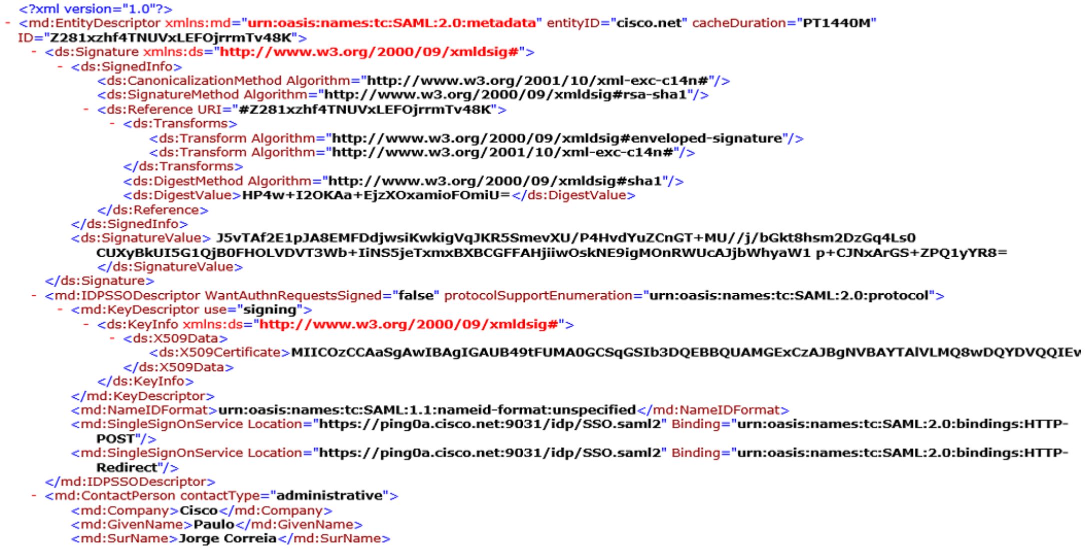
In our example we export the metadata from PingFederate SP and we include the X509 certificate, binding services and locations



☆ 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 ▾<br>All | STATUS ▾<br>All | ACTION |
|---|---|---|---|---|
| ✓ IDLAB-PF | IDLAB-PF | SAML2.0 | Active | In Use \| Copy \| Export Connection \| Export Metadata |
| ✓ PCA0a | PCA0a | SAML2.0 | Active | In Use \| Copy \| Export Connection \| Export Metadata |
| ✓ PCP0a | PCP0a | SAML2.0 | Active | In Use \| Copy \| Export Connection \| Export Metadata |
| ✓ cucm3a.cisco.net | cucm3a.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 |
| ✓ ucxn1a.cisco.net | ucxn1a.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="Z281xzhf4TNUVxLEFOjrrmTv48K">
  - <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="#Z281xzhf4TNUVxLEFOjrrmTv48K">
        - <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+EjzXOxamioFOmiU=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue> J5vTAf2E1pJA8EMFDdjwsiKwkigVqJKR5SmevXU/P4HvdYuZCnGT+MU//j/bGkt8hsm2DzGq4Ls0
        CUXyBkUI5G1QjB0FHOLVDVT3Wb+IiNS5jeTxmxBXBCGFFAHjiiwOskNE9igMOnRWUcAJjbWhyaW1 p+CJNxArGS+ZPQ1yYR8=
        </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>MIICOzCCAaSgAwIBAgIGAUB49tFUMA0GCSqGSIb3DQEBBQUAMGExCzAJBgNVBAYTAlVLMQ8wDQYDVQQIEv
          </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>
```

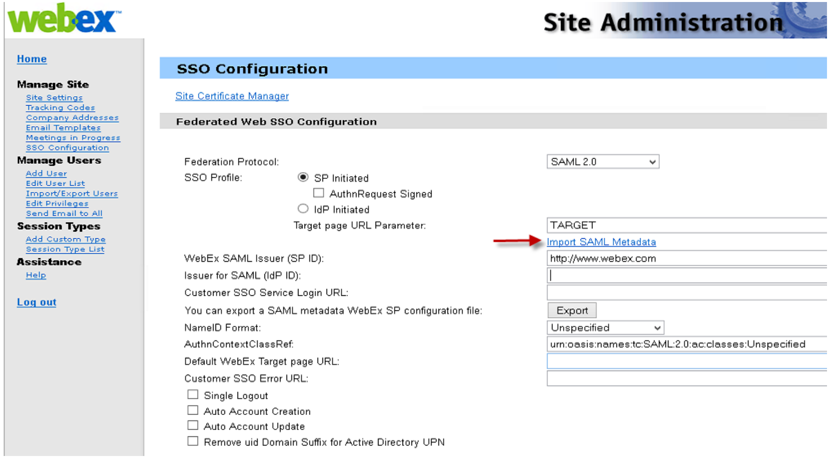
# WebEx Integration for SSO

## 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

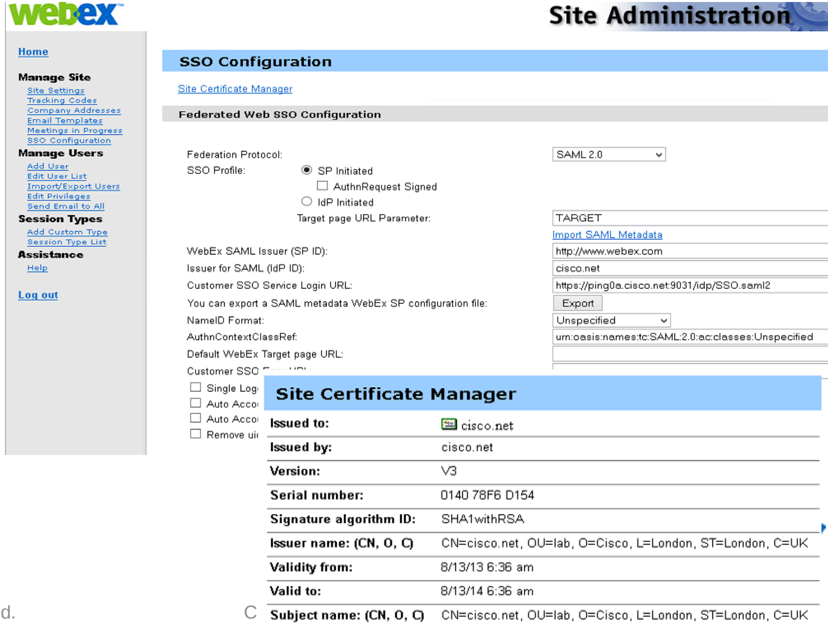


**SSO Configuration**

Site Certificate Manager

**Federated Web SSO Configuration**

Federation Protocol: SAML 2.0
SSO Profile: ● SP Initiated
□ AuthnRequest Signed
○ IdP Initiated
Target page URL Parameter: TARGET
Import SAML Metadata
WebEx SAML Issuer (SP ID): http://www.webex.com
Issuer for SAML (IdP ID):
Customer SSO Service Login URL:
You can export a SAML metadata WebEx SP configuration file: Export
NameID Format: Unspecified
AuthnContextClassRef: urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified
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



**SSO Configuration**

Site Certificate Manager

**Federated Web SSO Configuration**

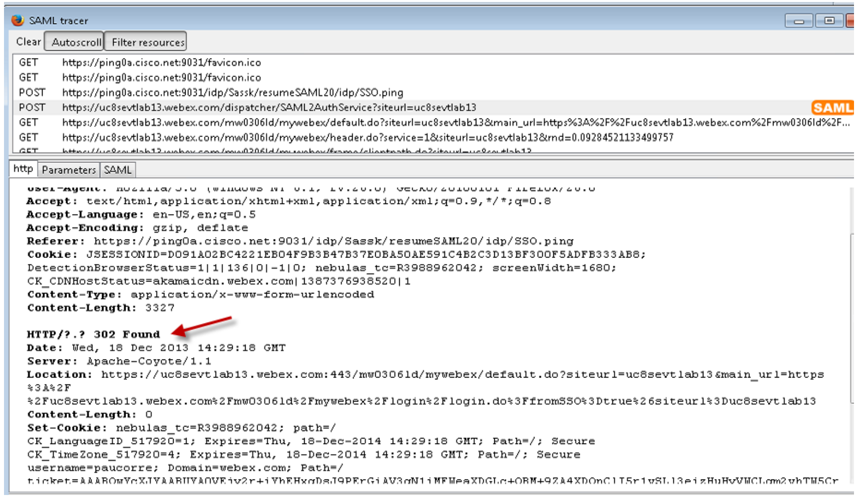
Federation Protocol: SAML 2.0
SSO Profile: ● SP Initiated
□ AuthnRequest Signed
○ IdP Initiated
Target page URL Parameter: TARGET
Import SAML Metadata
WebEx SAML Issuer (SP ID): http://www.webex.com
Issuer for SAML (IdP ID): cisco.net
Customer SSO Service Login URL: https://ping0a.cisco.net:9031/idp/SSO.saml2
You can export a SAML metadata WebEx SP configuration file: Export
NameID Format: Unspecified
AuthnContextClassRef: urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified
Default WebEx Target page URL:
Customer SSO
□ Single Log
□ Auto Acco
□ Auto Acco
□ Remove ui

**Site Certificate Manager**

| | |
|---|---|
| **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 |
| **Subject name: (CN, O, C)** | CN=cisco.net, OU=lab, O=Cisco, L=London, ST=London, C=UK |

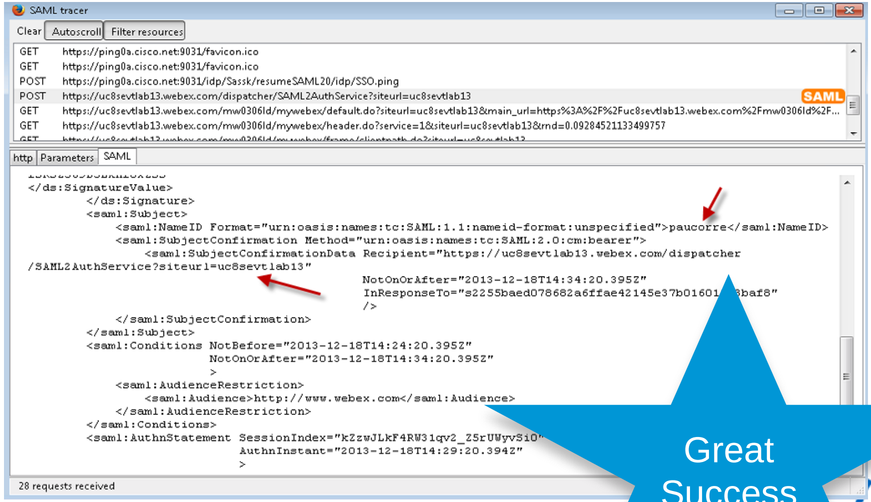
# Using SSO

When the user logins to the WebEx MC you will see and HTTP 302 Found as expected and the Name ID of the user login.



```
GET     https://ping0a.cisco.net:9031/favicon.ico
GET     https://ping0a.cisco.net:9031/favicon.ico
POST    https://ping0a.cisco.net:9031/idp/Sassk/resumeSAML20/idp/SSO.ping
POST    https://uc8sevtlab13.webex.com/dispatcher/SAML2AuthService?siteurl=uc8sevtlab13
GET     https://uc8sevtlab13.webex.com/mw0306ld/mywebex/default.do?siteurl=uc8sevtlab13&main_url=https%3A%2F%2Fuc8sevtlab13.webex.com%2Fmw0306ld%2F...
GET     https://uc8sevtlab13.webex.com/mw0306ld/mywebex/header.do?service=1&siteurl=uc8sevtlab13&rnd=0.09284521133499757
GET     https://uc8sevtlab13.webex.com/mw0306ld/mywebex/frame/clientpath.do?siteurl=uc8sevtlab13
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:26.0) Gecko/20100101 Firefox/26.0
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
Referer: https://ping0a.cisco.net:9031/idp/Sassk/resumeSAML20/idp/SSO.ping
Cookie: JSESSIONID=D091A02BC4221EB04F9B3B47B37E0BA50AE591C4B2C3D13BF300F5ADFB333AB8;
DetectionBrowserStatus=1|1|136|0|-1|0; nebulas_tc=R3988962042; screenWidth=1680;
CK_CDNHostStatus=akamaicdn.webex.com|1387376938520|1
Content-Type: application/x-www-form-urlencoded
Content-Length: 3327

HTTP/?.? 302 Found
Date: Wed, 18 Dec 2013 14:29:18 GMT
Server: Apache-Coyote/1.1
Location: https://uc8sevtlab13.webex.com:443/mw0306ld/mywebex/default.do?siteurl=uc8sevtlab13&main_url=https
%3A%2F
%2Fuc8sevtlab13.webex.com%2Fmw0306ld%2Fmywebex%2Flogin%2Flogin.do%3FfromSSO%3Dtrue%26siteurl%3Duc8sevtlab13
Content-Length: 0
Set-Cookie: nebulas_tc=R3988962042; path=/
CK_LanguageID_517920=1; Expires=Thu, 18-Dec-2014 14:29:18 GMT; Path=/; Secure
CK_TimeZone_517920=4; Expires=Thu, 18-Dec-2014 14:29:18 GMT; Path=/; Secure
username=paucorre; Domain=webex.com; Path=/
ticket=AAABQwYcXJYAABUYAOVEjv2r+jYbEHxgDsJ9PErGiAV3gN1iMFWeaXDGLc+QBM+9ZA4XDOnClI5r1vSL13eizHuHyVWCLgm2vbTW5Cr
```



```
GET     https://ping0a.cisco.net:9031/favicon.ico
GET     https://ping0a.cisco.net:9031/favicon.ico
POST    https://ping0a.cisco.net:9031/idp/Sassk/resumeSAML20/idp/SSO.ping
POST    https://uc8sevtlab13.webex.com/dispatcher/SAML2AuthService?siteurl=uc8sevtlab13
GET     https://uc8sevtlab13.webex.com/mw0306ld/mywebex/default.do?siteurl=uc8sevtlab13&main_url=https%3A%2F%2Fuc8sevtlab13.webex.com%2Fmw0306ld%2F...
GET     https://uc8sevtlab13.webex.com/mw0306ld/mywebex/header.do?service=1&siteurl=uc8sevtlab13&rnd=0.09284521133499757
GET     https://uc8sevtlab13.webex.com/mw0306ld/mywebex/frame/clientpath.do?siteurl=uc8sevtlab13
```

```
</ds:SignatureValue>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">paucorre</saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData Recipient="https://uc8sevtlab13.webex.com/dispatcher
/SAML2AuthService?siteurl=uc8sevtlab13"
                                              NotOnOrAfter="2013-12-18T14:34:20.395Z"
                                              InResponseTo="s2255baed078682a6ffae42145e37b01601[illegible]baf8"
                                              />
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2013-12-18T14:24:20.395Z"
                         NotOnOrAfter="2013-12-18T14:34:20.395Z"
                         >
            <saml:AudienceRestriction>
                <saml:Audience>http://www.webex.com</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement SessionIndex="kZzwJLkF4RW31qv2_Z5rUWyvSiO"
                             AuthnInstant="2013-12-18T14:29:20.394Z"
                             >
```

28 requests received

Great Success

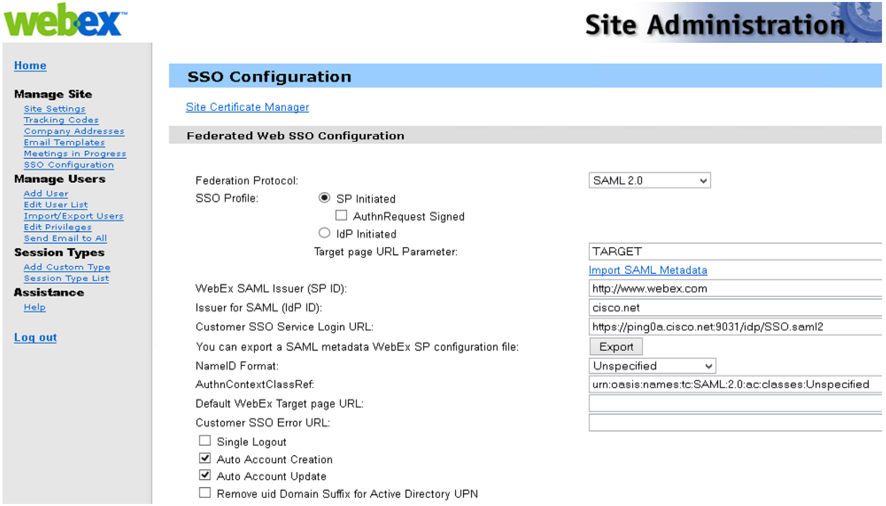
# WebEx User Account Management Options

| Option | Description |
|---|---|
| Manual updates through Org Admin | • Admin can use Org Admin to manually update user accounts |
| File import to Org Admin | • Admin can create and update accounts by importing a change file into Org Admin |
| Directory Integration<br>(FTP approach and will be depreciated soon) | • Semi-automatic method for creating, updating and deactivating user accounts and groups.<br>• 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<br>• **Advanced Services engagement** |
| Single Sign-On | • SSO can be configured to automatically create accounts when user logs-in to Connect for the first time<br>• SAML assertion provides user information<br>• Accounts can be created and updated but not deactivated |

# 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 )



webex — Site Administration

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

**SSO Configuration**

Site Certificate Manager

**Federated Web SSO Configuration**

Federation Protocol: SAML 2.0

SSO Profile: ● SP Initiated
□ AuthnRequest Signed
○ IdP Initiated

Target page URL Parameter: TARGET

Import SAML Metadata

WebEx SAML Issuer (SP ID): http://www.webex.com

Issuer for SAML (IdP ID): cisco.net

Customer SSO Service Login URL: https://ping0a.cisco.net:9031/idp/SSO.saml2

You can export a SAML metadata WebEx SP configuration file: Export

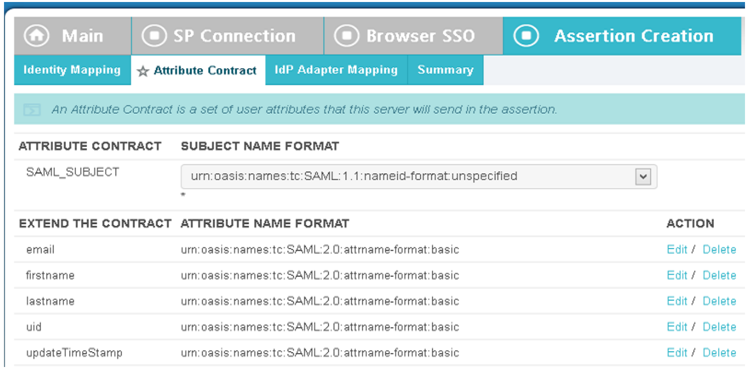
NameID Format: Unspecified

AuthnContextClassRef: urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified

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



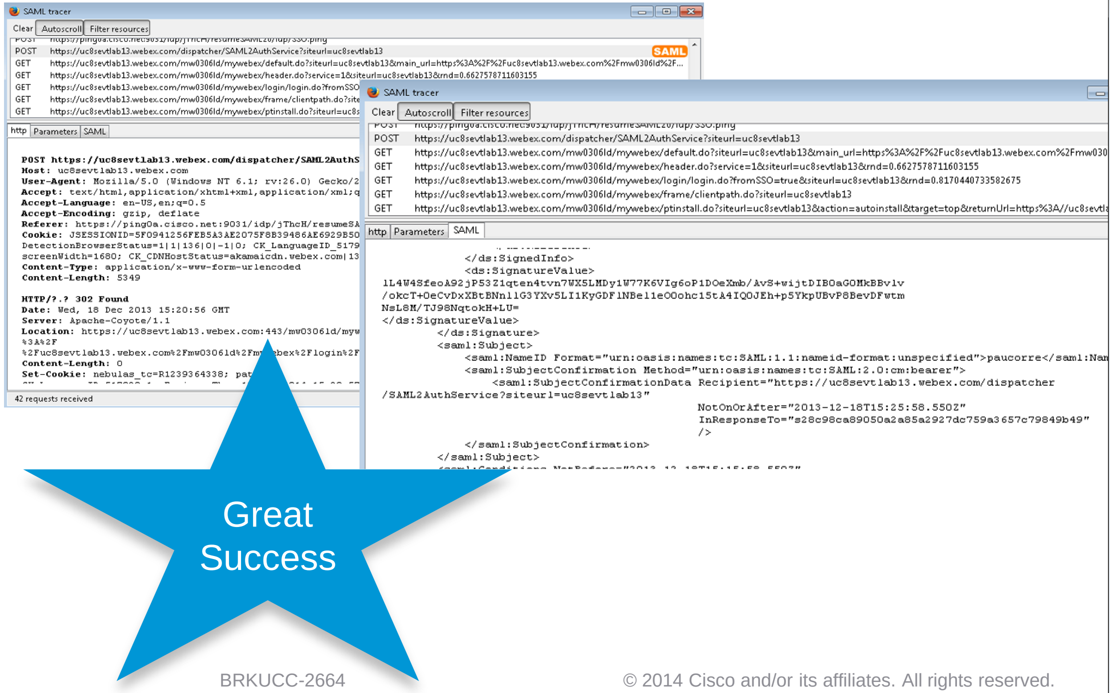
*An Attribute Contract is a set of user attributes that this server will send in the assertion.*

| ATTRIBUTE CONTRACT | SUBJECT NAME FORMAT |
|---|---|
| SAML_SUBJECT | 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 | Edit / Delete |
| firstname | urn:oasis:names:tc:SAML:2.0:attrname-format:basic | Edit / Delete |
| lastname | urn:oasis:names:tc:SAML:2.0:attrname-format:basic | Edit / Delete |
| uid | urn:oasis:names:tc:SAML:2.0:attrname-format:basic | Edit / Delete |
| updateTimeStamp | urn:oasis:names:tc:SAML:2.0:attrname-format:basic | Edit / Delete |

# What is the Result when the Users Login with Auto Account Creation and Update Enabled

When the user logins to 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.



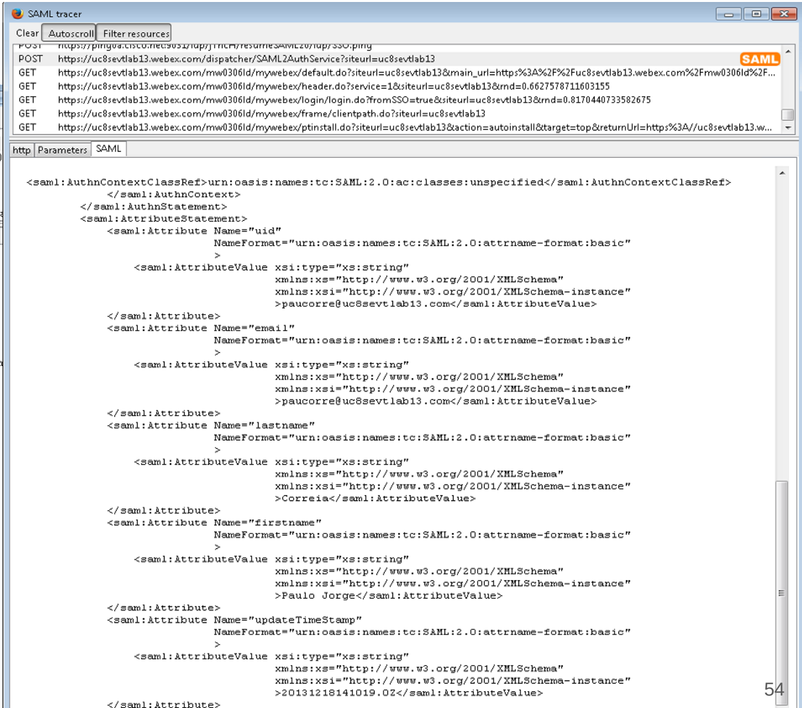
```
POST   https://ping0a.cisco.net:9031/idp/jThcH/resumeSAML20/idp/SSO.ping
POST   https://uc8sevtlab13.webex.com/dispatcher/SAML2AuthService?siteurl=uc8sevtlab13
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/default.do?siteurl=uc8sevtlab13&main_url=https%3A%2F%2Fuc8sevtlab13.webex.com%2Fmw0306ld%2F...
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/header.do?service=1&siteurl=uc8sevtlab13&rnd=0.6627578711603155
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/login/login.do?fromSSO
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/frame/clientpath.do?site
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/ptinstall.do?siteurl=uc8s
```

```
POST https://uc8sevtlab13.webex.com/dispatcher/SAML2AuthS
Host: uc8sevtlab13.webex.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:26.0) Gecko/2
Accept: text/html,application/xhtml+xml,application/xml;q
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ping0a.cisco.net:9031/idp/jThcH/resumeSA
Cookie: JSESSIONID=5F0941256FEB5A3AE2075F8B39486AE6929B50
DetectionBrowserStatus=1|1|136|0|-1|0; CK_LanguageID_5179
screenWidth=1680; CK_CDNHostStatus=akamaicdn.webex.com|13
Content-Type: application/x-www-form-urlencoded
Content-Length: 5349

HTTP/?.? 302 Found
Date: Wed, 18 Dec 2013 15:20:56 GMT
Server: Apache-Coyote/1.1
Location: https://uc8sevtlab13.webex.com:443/mw0306ld/myw
%3A%2F
%2Fuc8sevtlab13.webex.com%2Fmw0306ld%2Fmy    ebex%2Flogin%2F
Content-Length: 0
Set-Cookie: nebulas_tc=R1239364338; pat
```

42 requests received

```
POST   https://ping0a.cisco.net:9031/idp/jThcH/resumeSAML20/idp/SSO.ping
POST   https://uc8sevtlab13.webex.com/dispatcher/SAML2AuthService?siteurl=uc8sevtlab13
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/default.do?siteurl=uc8sevtlab13&main_url=https%3A%2F%2Fuc8sevtlab13.webex.com%2Fmw030
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/header.do?service=1&siteurl=uc8sevtlab13&rnd=0.6627578711603155
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/login/login.do?fromSSO=true&siteurl=uc8sevtlab13&rnd=0.8170440733582675
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/frame/clientpath.do?siteurl=uc8sevtlab13
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/ptinstall.do?siteurl=uc8sevtlab13&action=autoinstall&target=top&returnUrl=https%3A//uc8sevtla
```

```
            </ds:SignedInfo>
            <ds:SignatureValue>
1L4W4SfeoA92jP53Z1qten4tvn7WX5LMDy1W77K6VIg6oP1DOeXmb/AvS+wijtDIBOaGOMkBBvlv
/okcT+0eCvDxXBtBNnllG3YXv5LI1KyGDF1NBel1eO0ohc15tA4IQOJEh+p5YkpUBvP8BevDFwtm
NsL8M/TJ98NqtokH+LU=
</ds:SignatureValue>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">paucorre</saml:Nam
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData Recipient="https://uc8sevtlab13.webex.com/dispatcher
/SAML2AuthService?siteurl=uc8sevtlab13"
                                              NotOnOrAfter="2013-12-18T15:25:58.550Z"
                                              InResponseTo="s28c98ca89050a2a85a2927dc759a3657c79849b49"
                                              />
            </saml:SubjectConfirmation>
        </saml:Subject>
```



```
POST   https://ping0a.cisco.net:9031/idp/jThcH/resumeSAML20/idp/SSO.ping
POST   https://uc8sevtlab13.webex.com/dispatcher/SAML2AuthService?siteurl=uc8sevtlab13
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/default.do?siteurl=uc8sevtlab13&main_url=https%3A%2F%2Fuc8sevtlab13.webex.com%2Fmw0306ld%2F...
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/header.do?service=1&siteurl=uc8sevtlab13&rnd=0.6627578711603155
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/login/login.do?fromSSO=true&siteurl=uc8sevtlab13&rnd=0.8170440733582675
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/frame/clientpath.do?siteurl=uc8sevtlab13
GET    https://uc8sevtlab13.webex.com/mw0306ld/mywebex/ptinstall.do?siteurl=uc8sevtlab13&action=autoinstall&target=top&returnUrl=https%3A//uc8sevtlab13.w...
```

```
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="uid"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >paucorre@uc8sevtlab13.com</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="email"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >paucorre@uc8sevtlab13.com</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="lastname"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >Correia</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="firstname"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >Paulo Jorge</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="updateTimeStamp"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >20131218141019.0Z</saml:AttributeValue>
            </saml:Attribute>
```

# 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

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2014 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
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 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 cisco TM