Cisco webex

Enabling Single Sign-On for Common Identity using Ping Federate

cisco

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http:// www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Table of Contents

1

Introduction

Introduction

This document covers the configuration of the required software components essential for achieving a Single Sign-on (SSO) solution with WebEx Messenger using Ping Federate.

2

Enabling SSO for WebEx Messenger

Configure Federated Web SSO

1. Log into http://www.webex.com/go/connectadmin with your administration credentials.
2. Select the **Configuration tab** > **System Settings** > **Security Settings**.
3. Select **Federated Web SSO Configuration**.
4. In the **WebEx SAML Issuer (SP ID)** field, enter the name for the SAML agreement.

Note: You can use the fully qualified domain name (FQDN) of your organization.

5. Complete all the required fields.
6. Select **Export** to export the metadata to a location on your computer. You will import this file next.

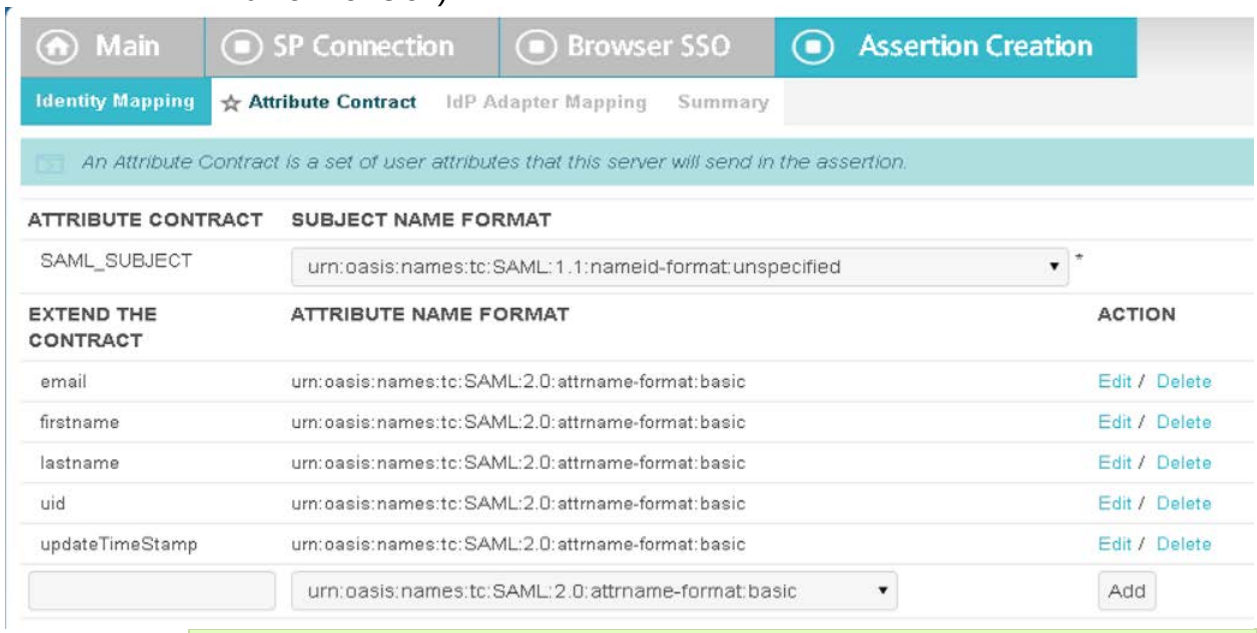
Create a New SP Connection

1. Go to PingFederate https://ping0a.uc8sevtlab13.com:9999/pingfederate/app.
2. In **SP Connections**, select **Create New**.

3. Select **Do not use a template for this connection**.
4. Select **Next**.
5. Select the **Browser SSO Profiles** check box.
6. Select **Next**.
7. Select **Choose File** to navigate to and select the metadata file.
8. Select **Next**.
9. Ensure all information is correct in the **General Info** tab.
10. Select **Done**.

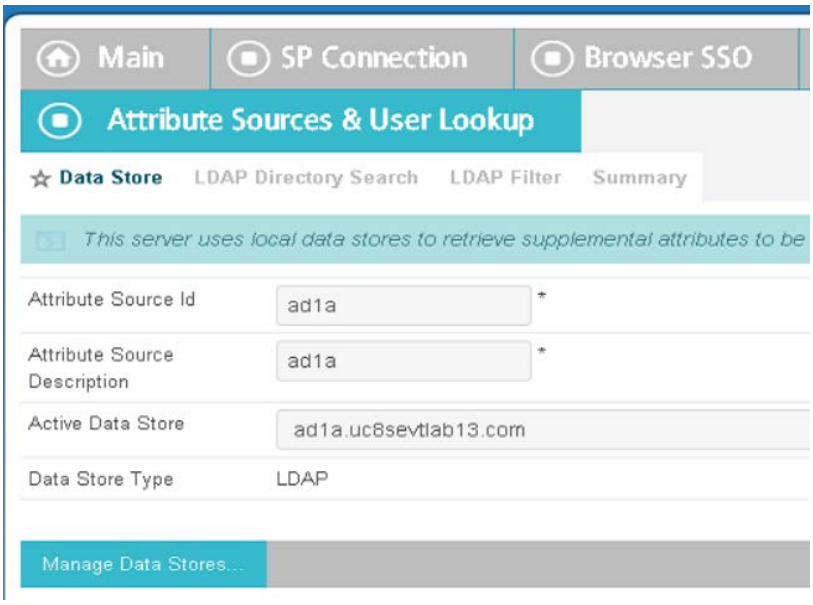
Configure the Browser SSO

1. Select **Configure Browser SSO**.
2. Select the **SP-Initiated SSO** check box.
3. Select **Next**.
4. Select **Configure Assertion Creation**.
5. Select the **Standard** radio button.
6. Select **Next to** add all the attributes that Messenger needs for JIT (Just in time Provision).

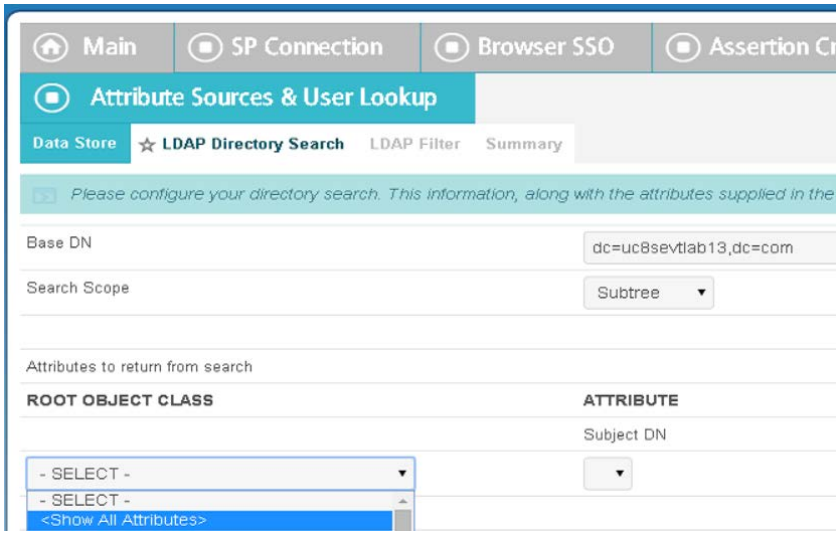


Note: If JIT is not required you can skip this step.

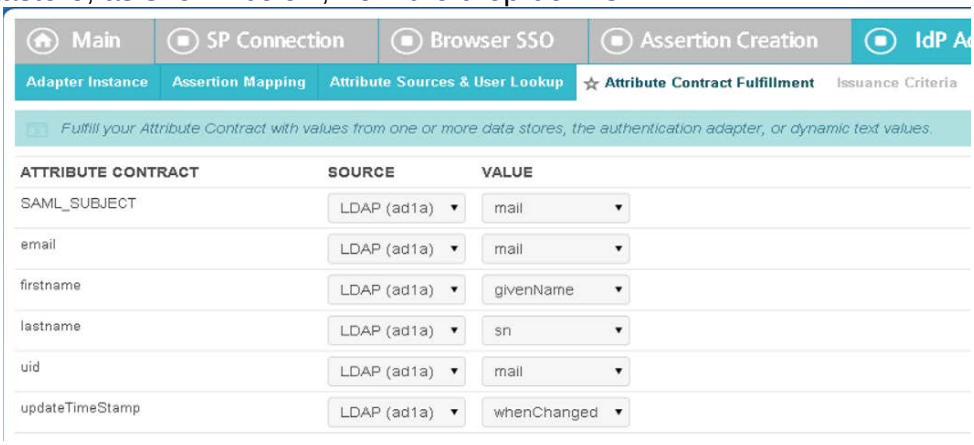
7. Select **Next**.
8. Select **Map New Adapter Instance....** to map to an authentication mechanism you have previously configured in PingFederate.
9. From the **ADAPTER INSTANCE** drop-down, select the adapter instance.
10. Select **Next**.
11. Select **Retrieve additional attributes from multiple data stores using one mapping**.
12. Select **Next**.
13. Select **Add Attribute Source** which in this case is is the active directory domain controller for our domain.



14. Select **Next**.
15. Specify the **Base DN** and select the root object class **<Show All Attributes>**.

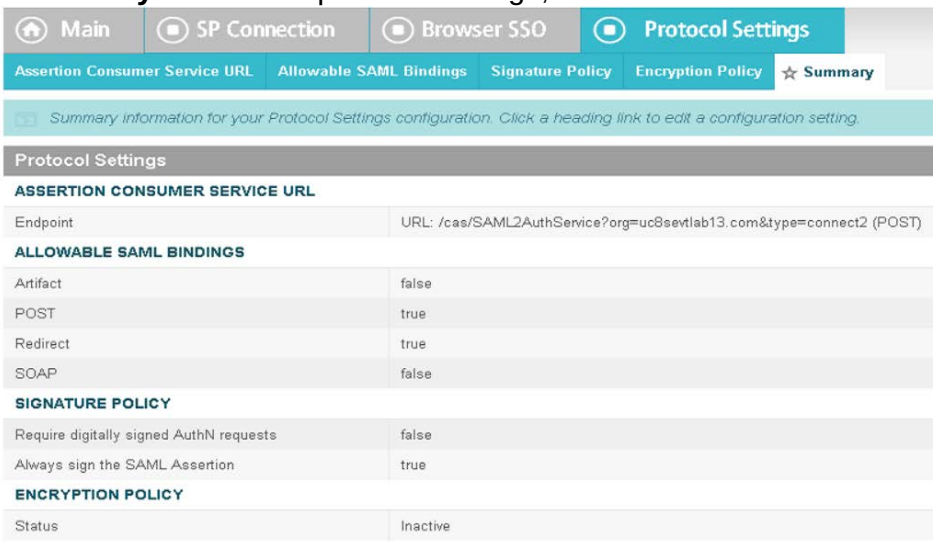


16. Select **Add Attribute** to add all the AD attributes to comply to the JIT attributes requested in the assertion.
17. Select **Next**.
18. In the Filter text box, enter the ldap filter containing the username provided by the user.
19. Select **Next**.
20. Select the source and value for the assertion attributes provided by the AD datastore, as shown below, from the drop-downs.



The asseration configuration is shown below.

21. Select **Done**.
22. Select **Next**.
23. Select **Configure Protocol Settings**.
24. Select the **Post** and **Redirect** check boxes.
25. Select **Summary** to view the protocol settings, as shown below.



26. Select **Done**.

Configure Certificate for the Assertion and Activate

1. In the **SP Connection** tab, select **Configure Credentials**.

2. Select the certificate you created for the SAML assertions.
3. Select **Next**.
4. Select **Done**.
5. Select the **Next**.
6. In the **Activation & Summary** tab, ensure the **Active** radio button is selected.
7. Select **Save.**

Export the Metadata

1. In the **SP Connection** tab, select the **Export Metadata** link.
2. Select the signing certificate from the drop-down.
3. Select **Export**.

Import SAML Metadata in WebEx Messenger

1. Log into http://www.webex.com/go/connectadmin with your administration credentials.
2. Select the **Configuration tab** > **System Settings** > **Security Settings**.
3. Select **Federated Web SSO Configuration**.
4. Select **Import SAML Metadata** to import the metadata file you downloaded.
5. In the **AuthContextClassRef** field, enter urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified.

This string ensures that Ping Federate can deliver Kerberos and Form based authentication.

Important: For Cisco Jabber to work with Cisco WebEx Messenger Instant Messenger and Presence and deliver on-premise Cisco Unified Call Manager (CUCM) and Unity connection, you must provide the UC details for CUCM and connections in the Webex Messenger administrator portal.

To use SSO in Cisco WebEx Messenger and Cisco WebEx Meeting Center, ensure loose integration is enabled for both.

See ***Cisco Unified Communications Integration with Cisco WebEx*** and ***Provision Loosely Coupled Integration*** in the Cisco WebEx Messenger Administration Guide.

Migration from WebEx Messenger to Common Identity SSO Authentication

Request to Add Domain to Common Identity

Contact your Customer Success Manager (CSM) or Universal Agent (UA) to submit an ops request to add the domain to CI or email: ci-messenger-sync@cisco.com.

Create a Password in CI

As none of the users migrated from Cisco WebEx Messenger have a password, you must create a password for an existing administrator now.

1. Connect to Https://web.ciscospark.com and enter the email address of the administrator.
2. Select **Next**.
3. Select **Can't access your account?**.

   An email is automatically sent to that user asking them to reset their password.

Configure SSO in Cloud Collaboration Management

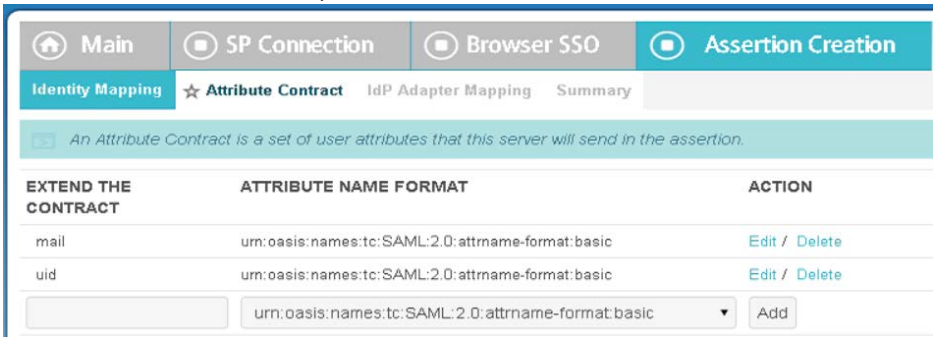
1. Connect to https://admin.ciscospark.com using the email address and password that you previously reset.
2. From the top navigation bar, select **Service Setup** > **Enterprise Settings** to download the CI metadata to configure Ping Federate.
3. In the **Enterprise Settings** window, select **Integrate a 3rd-party identity provider (Advanced)**.
4. Select **Next**.
5. Select **Download Metadata File** to browse to and save the metadata file.

Create a New SP Connection for CI

1. Go to your PingFederate Administration portal https://ping0a.uc8sevtlab13.com:9999/pingfederate/app.
2. Select **Create New**.
3. Select the **Do not use a template for this connection** radio button.
4. Select **Next**.
5. Select **Browser SSO Profiles**.
6. Select the **Import Metadata** tab.
7. Select **Choose File** to browse to and import the metadata file dwnloaded from Cisco WebEx Messenger.
8. Select **Next**.
9. Review the information in the **General** tab.
10. Select **Done**.

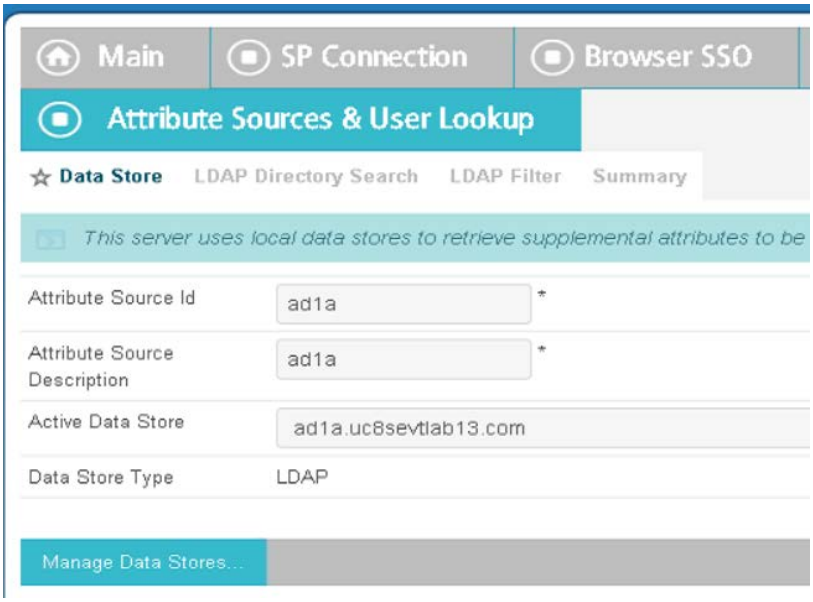
Configure the Browser SSO for CI

1. Select **Configure Browser SSO**.
2. Select the **SP-Initiated SSO** check box.
3. Select **Next**.
4. Select **Configure Assertion Creation**.
5. Select the **Transient** radio button and the check box below it.
6. Extend the contract attributes, as shown below.

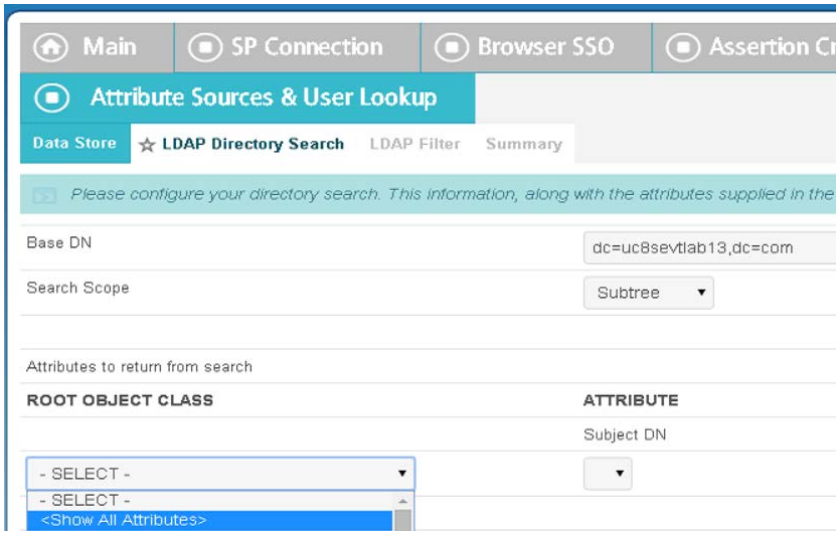


7. Select **Next**.

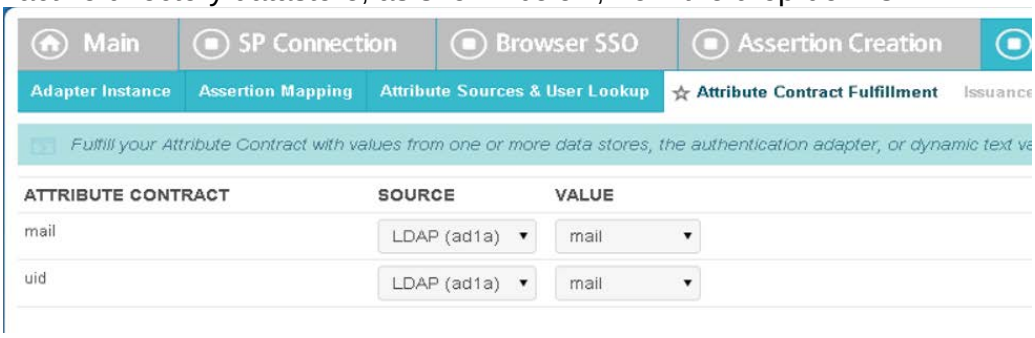
8. Select **Map New Adapter Instance**.
9. From the **ADAPTER INSTANCE** drop-down, select the the authentication mechanism you configured previously.
10. Select **Next**.
11. Select the **Retrieve additional attributes from multiple data stores using one mapping** radio button.
12. Select **Next**.
13. Select **Add Attribute Source** which in this case is is the active directory domain controller for our domain.



14. Select **Next**.
15. Specify the **Base DN** and select the root object class **<Show All Attributes>**.

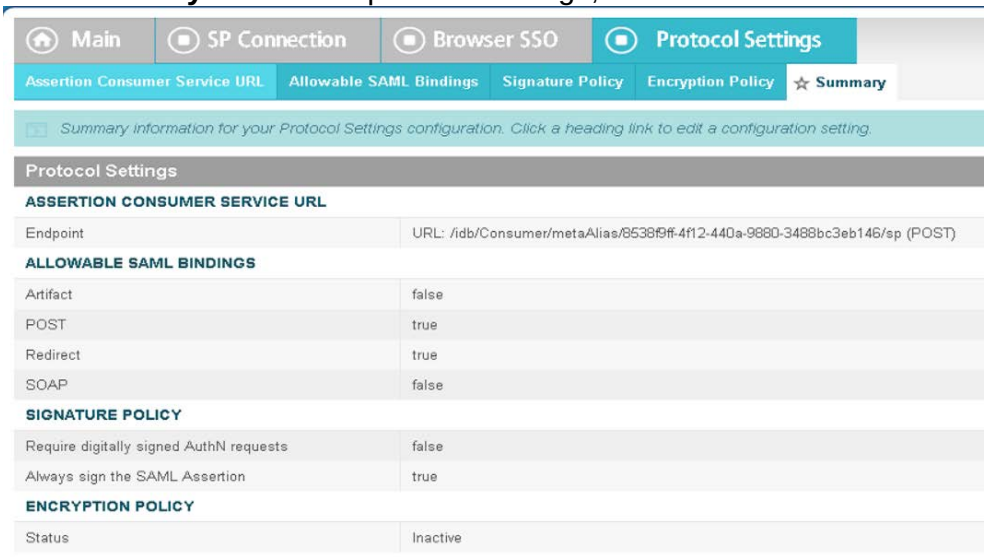


16. Select **Add Attribute** to add the mail attribute from the active directory.
17. Select **Next**.
18. In the Filter text box, enter the ldap filter containing the username provided by the user.
19. Select **Next**.
20. Select the source and value for the assertion attributes provided by the active directory datastore, as shown below, from the drop-downs.



The asseration configuration is shown below.

21. Select **Done**.
22. Select **Next**.
23. Select **Configure Protocol Settings**.
24. Select the **Post** and **Redirect** check boxes.
25. Select **Next**.
26. Select the **Always sign the SAML Assertion** check box.
27. Select **Summary** to view the protocol settings, as shown below.



28. Select **Done**.

Configure Certificate for the Assertion and Activate

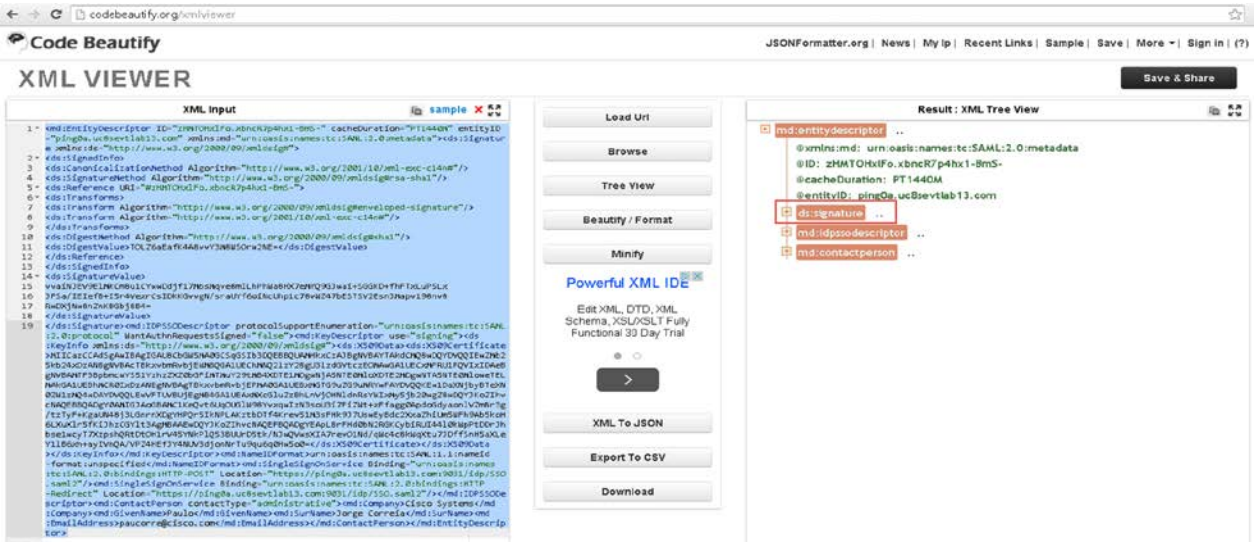
1. In the **SP Connection** tab, select **Configure Credentials**.
2. Select the certificate you created for the SAML assertions.
3. Select **Next**.
4. Select **Done**.
5. Select the **Next**.
6. In the **Activation & Summary** tab, ensure the **Active** radio button is selected.
7. Select **Save.**

Export and Edit the Metadata for CI

1. In the **SP Connection** tab, select the **Export Metadata** link.
2. Select the signing certificate from the drop-down.
3. Select **Export**.
4. Use an XML editor to remove the elements not required in CI.

Note: There are several XML editors available online but we recommend Code Beautify http://codebeautify.org/xmlviewer.

5. In the XML editor, browse to the metatdata file you exported.
6. Remove all the XML Tags except entitydescriptor, idpssodescriptor and contact person..



7. Select **Download** to download the edited file.
8. The metadata file should look like this:

```
<?xml version="1.0"?>
- <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="ping0a.uc8sevtlab13.com" cacheDuration="PT1440M" ID="Jg1_f0P2GAmNX4H54euo
  - <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>MIICazCCAdSgAwIBAgIGAU8CbGW5MA0GCSqGSIb3DQEBBQUAMHkxCzAJBgNVBAYTAkdCMQ8wDQYDVQQIEwZMb25kb24xDzAN
          </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.uc8sevtlab13.com:9031/idp/SSO.saml2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:SingleSignOnService Location="https://ping0a.uc8sevtlab13.com:9031/idp/SSO.saml2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    </md:IDPSSODescriptor>
  - <md:ContactPerson contactType="administrative">
      <md:Company>Cisco Systems</md:Company>
      <md:GivenName>Paulo</md:GivenName>
      <md:SurName>Jorge Correia</md:SurName>
      <md:EmailAddress>paucorre@cisco.com</md:EmailAddress>
    </md:ContactPerson>
  </md:EntityDescriptor>
```

Complete SSO Configuration in Cloud Collaboration Management

1. Connect to https://admin.ciscospark.com using the email address and password that you previously reset.
2. From the top navigation bar, select **Service Setup** > **Enterprise Settings** to download the CI metadata to configure Ping Federate.
3. In the **Enterprise Settings** window, select **Integrate a 3rd-party identity provider (Advanced)**.
4. Select **Next**.
5. Select **Import** to browse to and import the edited metatadata file.

A success message is displayed when the import of the metadata file is complete.

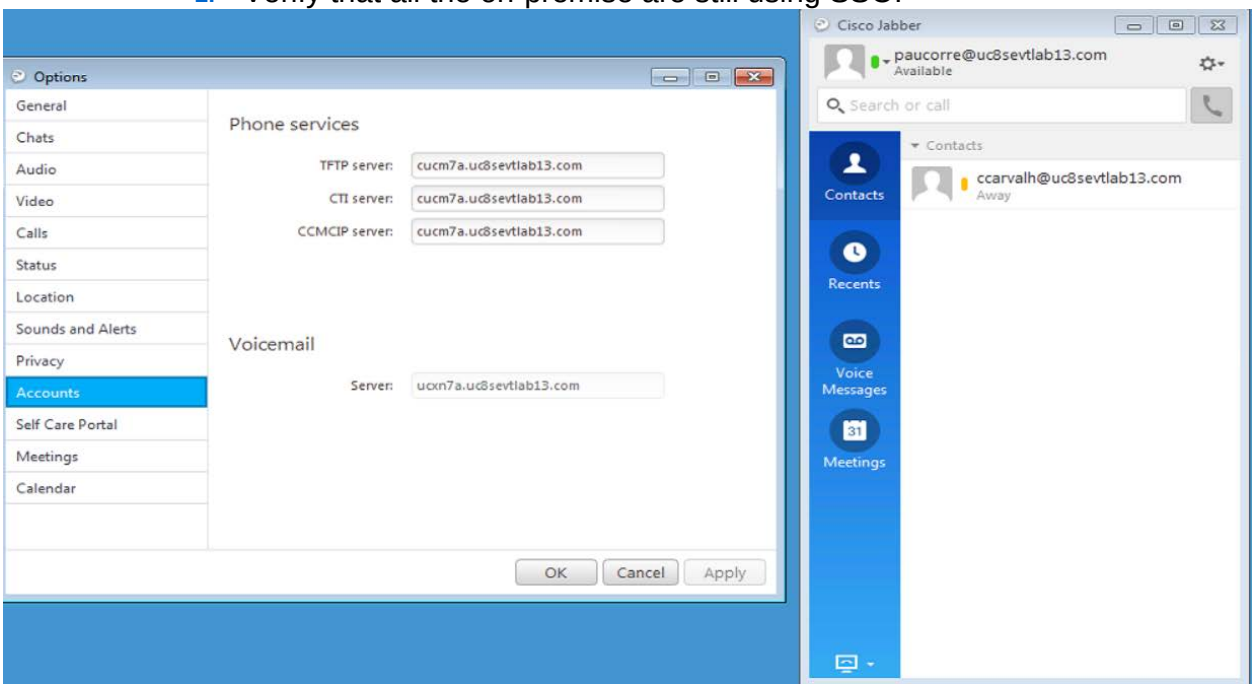
6. Select **Next**.
7. Select **Test SSO Configuration** .
8. Sign in with the administrator details.

Redirect Authentication

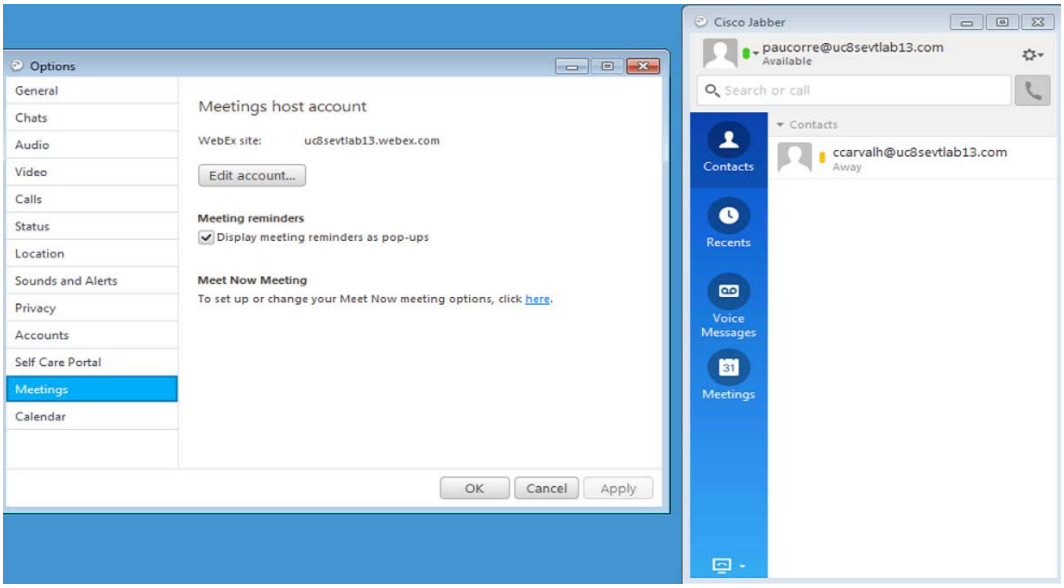
- Before you can verify the Jabber authentication in CI, authentication must be redirected from the WebEx Messenger platform to the CI platform, To do this contact the CSM to update the existing ops request or submit a new ops request or email: ci-messenger-sync@cisco.com.

Verification of Cisco Jabber Authentication in CI

1. Start Cisco Jabber.
2. Verify that all the on-premise are still using SSO.



3. Verify that WebEx Meeting Center is enabled for loose Integration.



4. Finally, verify that Cisco Jabber logs contain the string idbroker.webex.com, indicating that it is connecting to CI.

2015-06-05 09:34:31,893 DEBUG [0x000016e4] [ervices\impl\TransportHttpClient.cpp(87)] [csfunified.telemetry.TransportHttpClient] [CSFUnified::telemetry::TransportHttpClient::getAccessTokenForMetricsService] - About to execute access token request: [url] https://idbroker.webex.com/idb/oauth2/v1/access_token [method] 1
[followRedirects] 1
[transferTimeout] 0
[connectionTimeout] 0
[numRetries] 0
[authType] 1
[acceptable cryptographic protocols] TLS_1_0 TLS_1_1 TLS_1_2
[useSystemProxy] 1
[header] User-Agent:
[size of body] 64
2015-06-05 09:34:31,893 DEBUG [0x000016e4] [sf-netutils\src\common\PolicySet.cpp(84)] [csf.common.PolicySet] [csf::common::PolicySet::getPolicy] - Successfully found Policy with nature EDGE_USAGE [NEVER_USE]
2015-06-05 09:34:31,893 DEBUG [0x000016e4] [ls\src\http\BasicHttpClientImpl.cpp(253)] [csf.httpclient] [csf::http::BasicHttpClientImpl::execute] - Edge policy enforced successfully with transformed Url: https://idbroker.webex.com/idb/oauth2/v1/access_token for request #1
2015-06-05 09:34:31,893 DEBUG [0x000016e4] [etutils\src\http\HttpRequestData.cpp(71)] [csf.httpclient] [csf::http::HttpRequestData::consumeEasyCURLConnection] - Acquired lock (_easyCurlConnectionMutex)
2015-06-05 09:34:31,893 DEBUG [0x000016e4] [etutils\src\http\HttpRequestData.cpp(80)] [csf.httpclient] [csf::http::HttpRequestData::consumeEasyCURLConnection] - Releasing lock (_easyCurlConnectionMutex)

2015-06-05 09:34:31,894 INFO [0x000016e4] [etutils\src\http\CurlHttpUtils.cpp(1015)] [csf.httpclient] [csf::http::CurlHttpUtils::configureEasyRequest] - *-----* Configuring request #1 POST https://idbroker.webex.com/idb/oauth2/v1/access_token