Single Sign-On Setup with OpenSSO and Cisco WebEx

10/8/2009

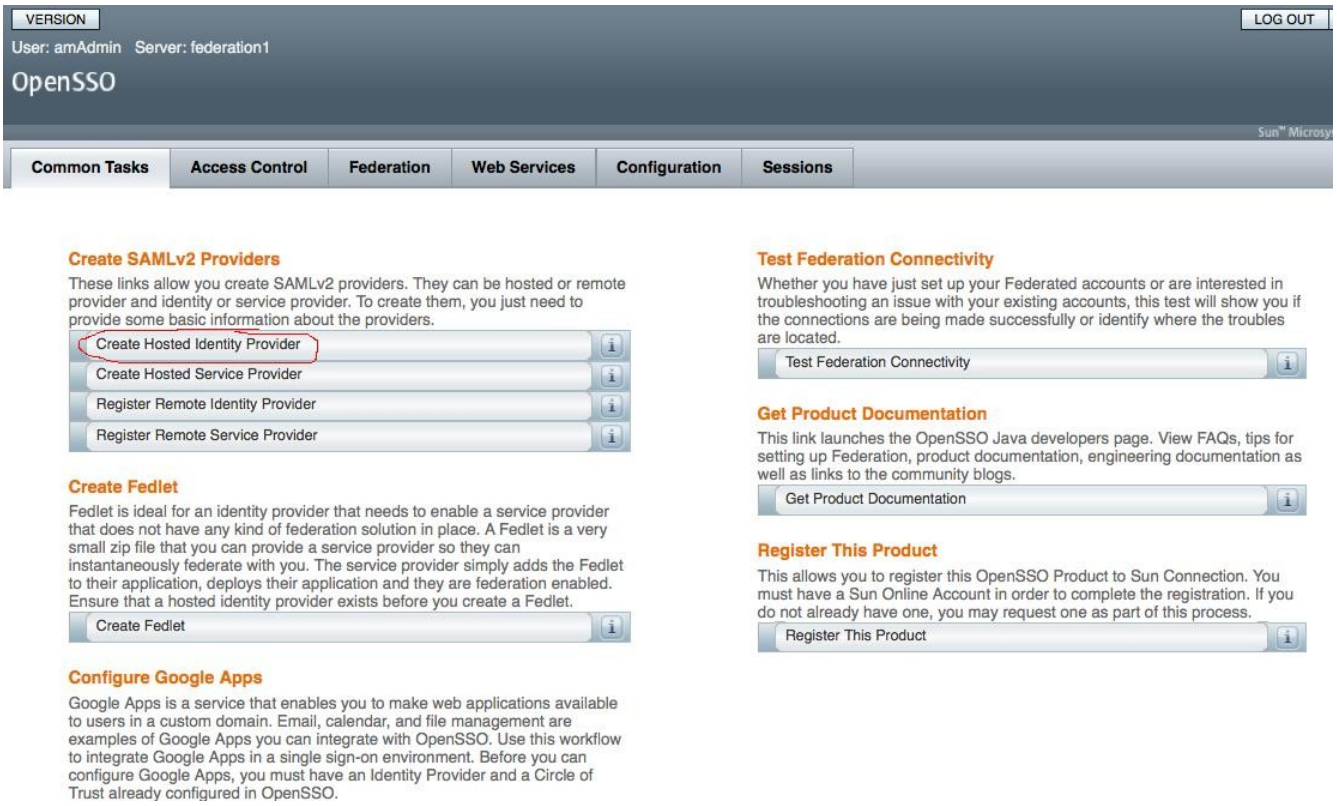
OpenSSO and WebEx both support SAML2 and SAML1 protocols for enabling enterprise federation single sign-on. This document describes the configuration steps that are required to enable SAML2 Single Sign-On on both sides.

SAML2 setup between OpenSSO and WebEx

1. Configure OpenSSO

1.1 Login to the OpenSSO Administration Console.

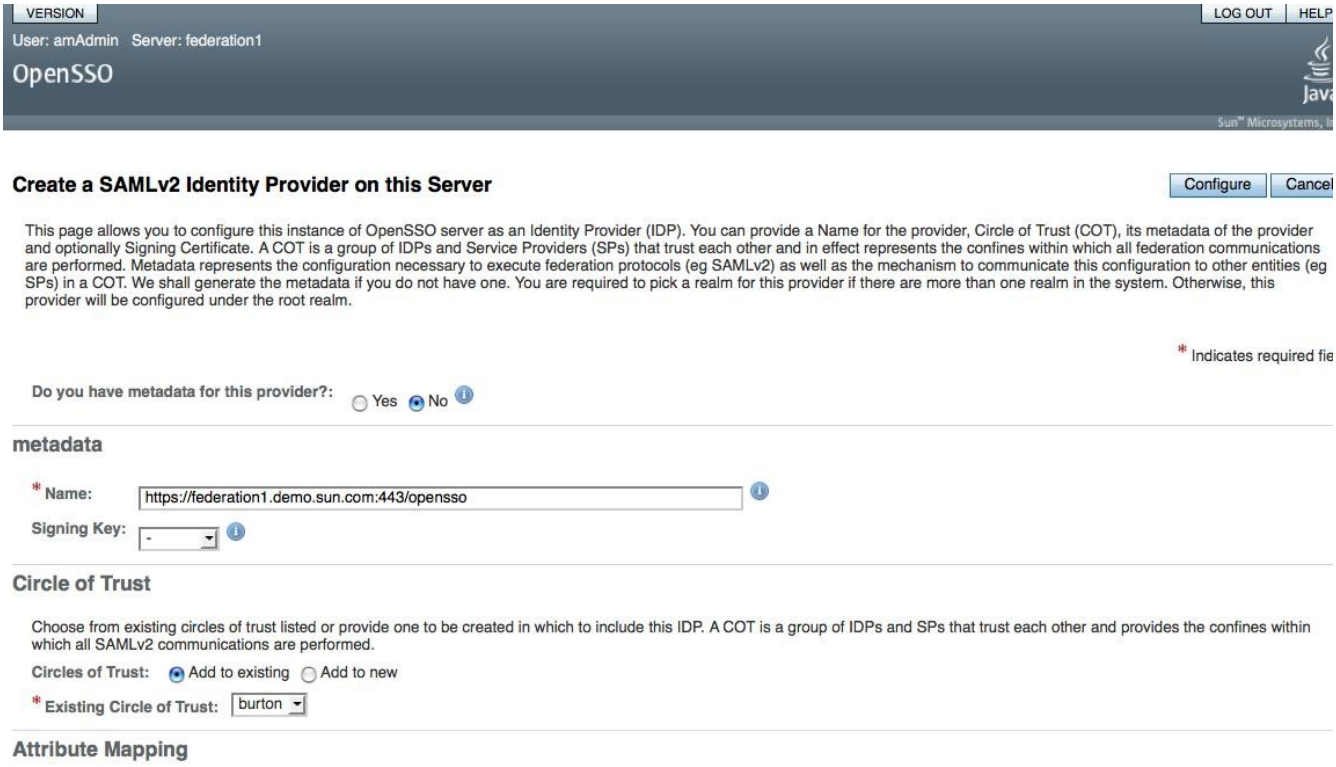
1.2 Navigate to Common Tasks -> Create SAML v2 Providers ->Click on Create Hosted Identity Provider.



1.3 Click on Hosted Identity Provider. This opens a new page to create Hosted Identity Provider Configuration.

As you can see from the picture below, you could choose the default entity id based on the host name where OpenSSO is deployed, but you can choose your own. The signing key is read from OpenSSO keystore (check OpenSSO documentation how to provision your own

private key). Similarly the circle of trust (cot), you can choose any existing cot if there's one, otherwise, you can choose to create new one. The attribute mapping defined here applies to all the service providers that the IDP interacts with, but you could also choose per service provider and the corresponding attribute mapping would be defined in the respective remote service provider configuration described later.
Click "Configure".



This will create the Hosted Identity Provider Configuration.

1.4 Prepare the remote metadata for WebEx that can be imported into OpenSSO and store it as webexsp.xml in your favorite folder.

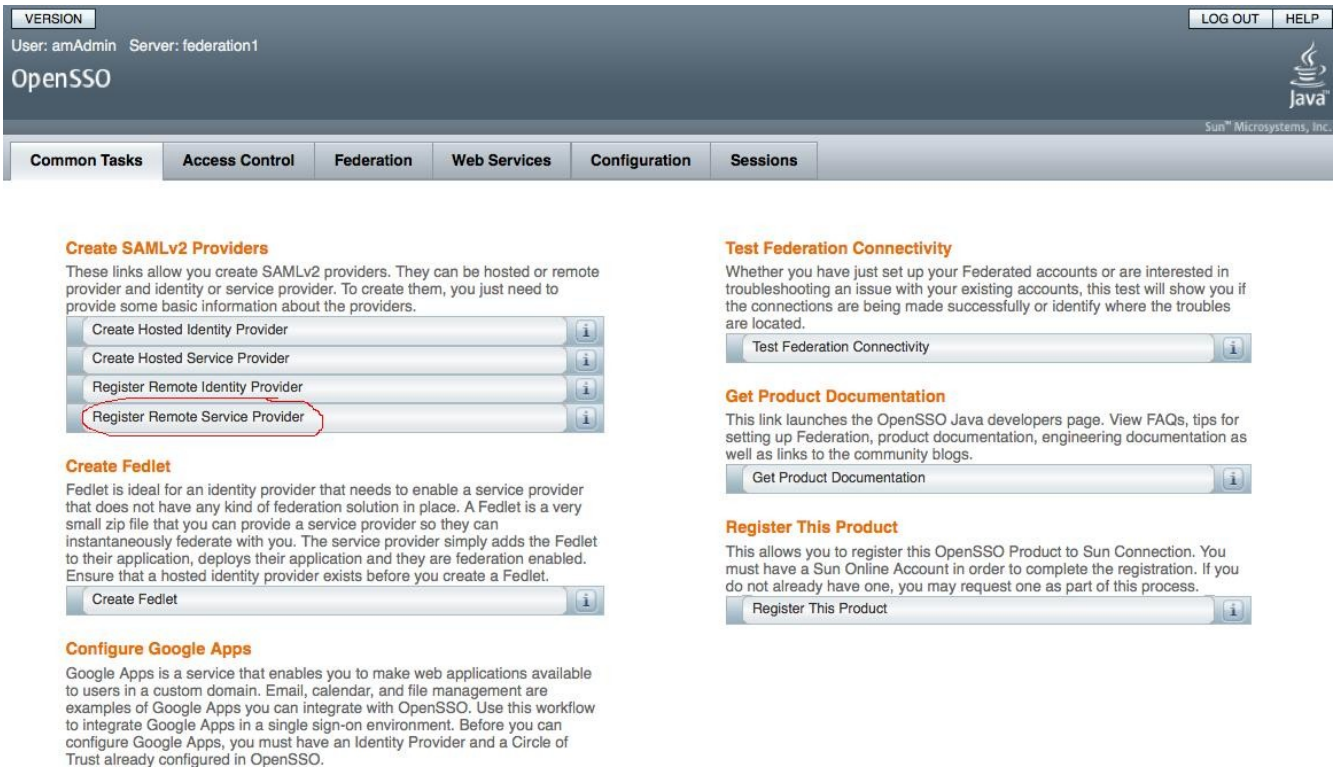
```
<EntityDescriptor  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
        entityID="https://sunmicrosystems-test.webex.com">
    <SPSSODescriptor
          AuthnRequestsSigned="false"
         WantAssertionsSigned="true"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <NameIDFormat>
            urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
        </NameIDFormat>
        <AssertionConsumerService
                    index="0"
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Location="https://sunmicrosystems-
test.webex.com/dispatcher/SAML2AuthService.do?siteurl=sunmicrosystem-test"/>
```

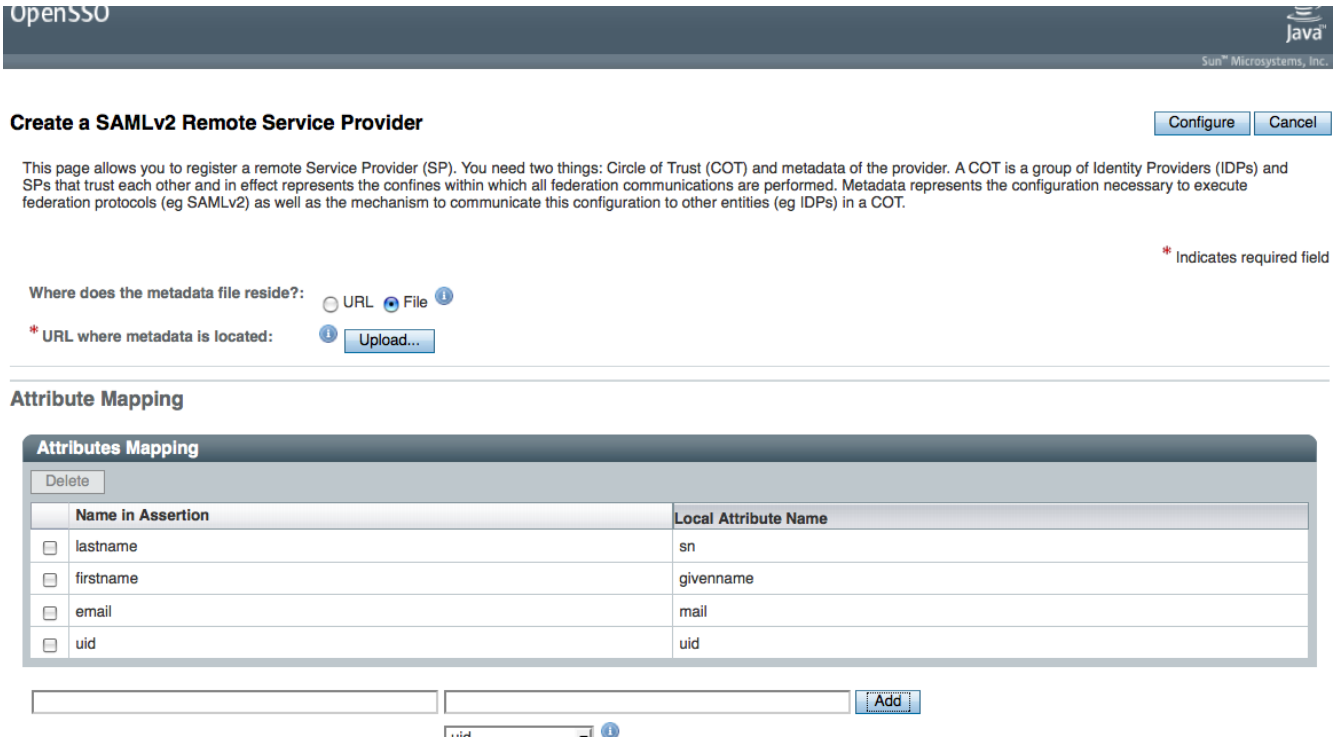
```
  </SPSSODescriptor>
</EntityDescriptor>
```

The entityID is your site id created by the WebEx. Modify Assertion Consumer Service URL and entityID as per your WebEx configuration in this xml file.

1.5 Import your metadata into OpenSSO

Go to Admin Console -> Common Tasks -> Register Remote Service Provider. The following two pictures drive the configuration as required.





As you can see above, choose the "File" option and Upload the webexsp.xml. WebEx requires the attribute mapping as defined above for auto account creation. The required attribute mapping are:

lastname=sn
firstname=givenname
email=mail
uid=uid

The format here is:

<SAMLAttributeName>=<Real attribute name>

Note: The users must be provisioned with these attributes. By default, it has lastname, first name and uid, but you have to provision the email id attribute value. You can do this from OpenSSO console. This is outside of SAML2 federation configuration.

1.6 OpenSSO setup is now ready. You can manage edit/view these configurations by going into Admin Console ->Federation

Make sure that the created entities are part of the same circle of trust.

2. Configure WebEx site:

2.1 Login into administration url for your WebEx site.

2.2 Click on SSO Configuration. In Federation SSO Configuration, enter the following values:

Federation Protocol : SAML 2.0

WeEx SAML Issuer (SP): <Your WebEx site id>

Issuer for SAML (IDP): <Your IDP entity id> i.e. https://federatio1.demo.sun.com:443/opensso

Customer SSO Service Login URL : <Federated single sign-on url>

i.e. https://federation1.demo.sun.com:443/opensso/SSORedirect/metaAlias/idp
You can check this in OpenSSO Admin Console -> Federation-> IDP entity id -> Service URLs -> Single Sign On Service URL

NameID Format: Choose your preferred name id format and as configured in OpenSSO

Authn Context Ref:

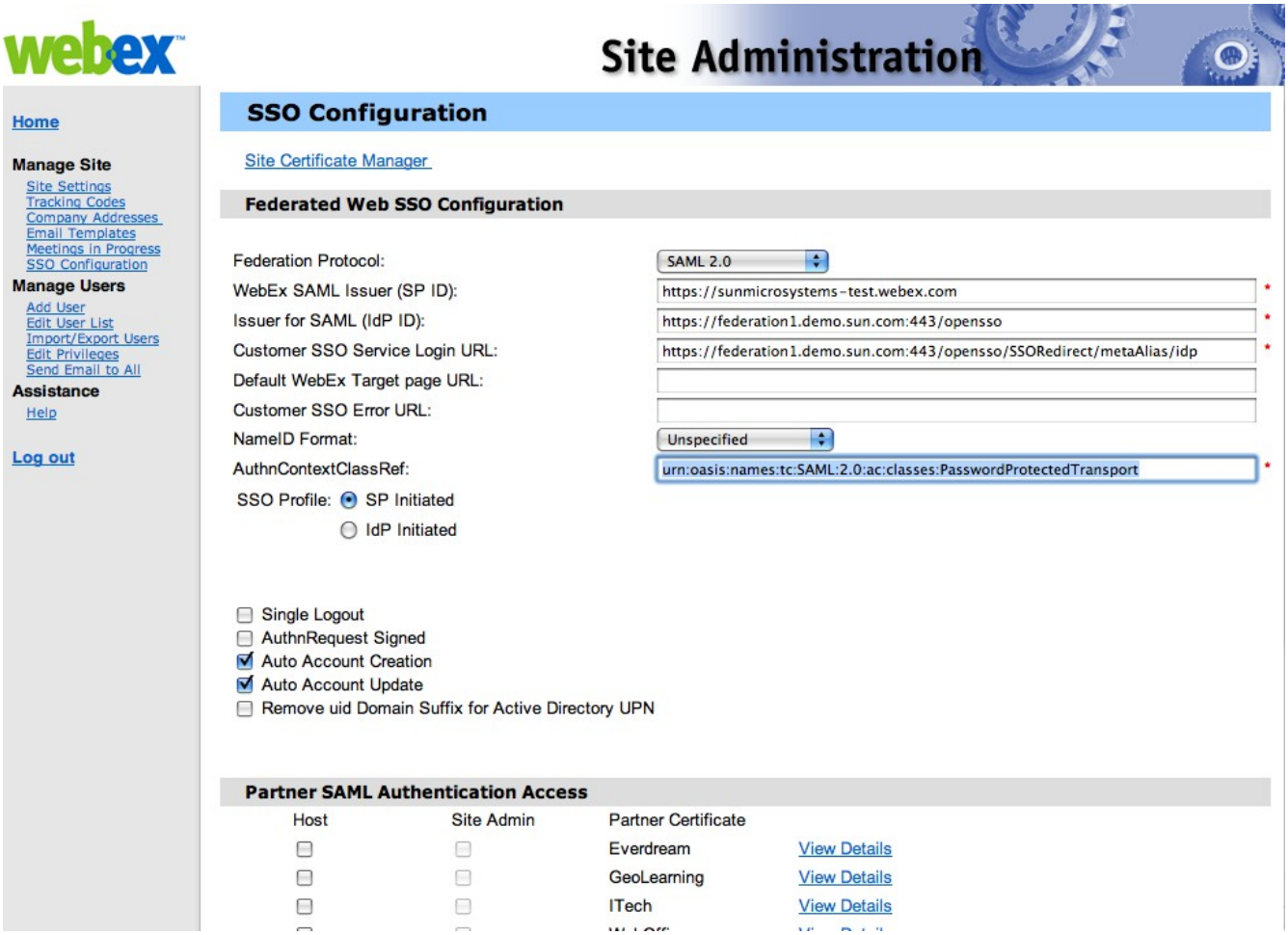
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

SSO Configuration: Choose SP initiated or IDP initiated (OpenSSO supports both)

Enable "Auto Account Creation" and "Auto Account Update".

Update/Save the configuration.

The following picture represents the configuration at WebEx:



3. Testing the setup:

3.1 You can test the Host Login from your WebEx site for SP initiated SSO. Login at IDP with your user name and password. After successful login, you should be able to see your WebEx site.

3.2 You could also test the IDP initiated SSO from OpenSSO by invoking the following URL:

https://federation1.demo.sun.com/opensso/saml2/jsp/idpSSOInit.jsp?metaAlias=/idp&spEntityID=https://sunmicrosystems-test.webex.com&RelayState=https://sunmicrosystems-test.webex.com/

Note: The URL changes based on the host name, site url etc.