

# 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.

VERSION LOG OUT

User: amAdmin Server: federation1

## OpenSSO

Common Tasks Access Control Federation Web Services Configuration Sessions

### Create SAMLv2 Providers

These links allow you create SAMLv2 providers. They can be hosted or remote provider and identity or service provider. To create them, you just need to provide some basic information about the providers.

- Create Hosted Identity Provider
- Create Hosted Service Provider
- Register Remote Identity Provider
- Register Remote Service Provider

### Create Fedlet

Fedlet is ideal for an identity provider that needs to enable a service provider that does not have any kind of federation solution in place. A Fedlet is a very small zip file that you can provide a service provider so they can instantaneously federate with you. The service provider simply adds the Fedlet to their application, deploys their application and they are federation enabled. Ensure that a hosted identity provider exists before you create a Fedlet.

- Create Fedlet

### Configure Google Apps

Google Apps is a service that enables you to make web applications available to users in a custom domain. Email, calendar, and file management are examples of Google Apps you can integrate with OpenSSO. Use this workflow to integrate Google Apps in a single sign-on environment. Before you can configure Google Apps, you must have an Identity Provider and a Circle of Trust already configured in OpenSSO.

### Test Federation Connectivity

Whether you have just set up your Federated accounts or are interested in troubleshooting an issue with your existing accounts, this test will show you if the connections are being made successfully or identify where the troubles are located.

- Test Federation Connectivity

### Get Product Documentation

This link launches the OpenSSO Java developers page. View FAQs, tips for setting up Federation, product documentation, engineering documentation as well as links to the community blogs.

- Get Product Documentation

### Register This Product

This allows you to register this OpenSSO Product to Sun Connection. You must have a Sun Online Account in order to complete the registration. If you do not already have one, you may request one as part of this process.

- Register This Product

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".

VERSION LOG OUT HELP

User: amAdmin Server: federation1

OpenSSO

Sun Microsystems, Inc.

### Create a SAMLv2 Identity Provider on this Server

Configure Cancel

This page allows you to configure this instance of OpenSSO server as an Identity Provider (IDP). You can provide a Name for the provider, Circle of Trust (COT), its metadata of the provider and optionally Signing Certificate. A COT is a group of IDPs and Service Providers (SPs) that trust each other and in effect represents the confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration to other entities (eg SPs) in a COT. We shall generate the metadata if you do not have one. You are required to pick a realm for this provider if there are more than one realm in the system. Otherwise, this provider will be configured under the root realm.

\* Indicates required field

Do you have metadata for this provider?:  Yes  No

#### metadata

\* Name:

Signing Key:

#### Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this IDP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 communications are performed.

Circles of Trust:  Add to existing  Add to new

\* Existing Circle of Trust:

#### Attribute Mapping

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.

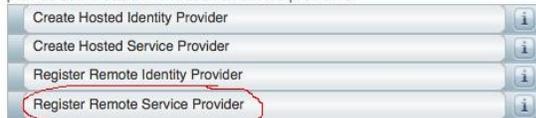
## 1.5 Import your metadata into OpenSSO

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



### Create SAMLv2 Providers

These links allow you create SAMLv2 providers. They can be hosted or remote provider and identity or service provider. To create them, you just need to provide some basic information about the providers.



### Create Fedlet

Fedlet is ideal for an identity provider that needs to enable a service provider that does not have any kind of federation solution in place. A Fedlet is a very small zip file that you can provide a service provider so they can instantaneously federate with you. The service provider simply adds the Fedlet to their application, deploys their application and they are federation enabled. Ensure that a hosted identity provider exists before you create a Fedlet.



### Configure Google Apps

Google Apps is a service that enables you to make web applications available to users in a custom domain. Email, calendar, and file management are examples of Google Apps you can integrate with OpenSSO. Use this workflow to integrate Google Apps in a single sign-on environment. Before you can configure Google Apps, you must have an Identity Provider and a Circle of Trust already configured in OpenSSO.

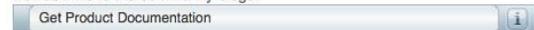
### Test Federation Connectivity

Whether you have just set up your Federated accounts or are interested in troubleshooting an issue with your existing accounts, this test will show you if the connections are being made successfully or identify where the troubles are located.



### Get Product Documentation

This link launches the OpenSSO Java developers page. View FAQs, tips for setting up Federation, product documentation, engineering documentation as well as links to the community blogs.



### Register This Product

This allows you to register this OpenSSO Product to Sun Connection. You must have a Sun Online Account in order to complete the registration. If you do not already have one, you may request one as part of this process.



**Create a SAMLv2 Remote Service Provider**



This page allows you to register a remote Service Provider (SP). You need two things: Circle of Trust (COT) and metadata of the provider. A COT is a group of Identity Providers (IDPs) and SPs that trust each other and in effect represents the confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration to other entities (eg IDPs) in a COT.

\* Indicates required field

Where does the metadata file reside?:  URL  File 

\* URL where metadata is located: 

**Attribute Mapping**

Attributes Mapping	
<input type="button" value="Delete"/>	
Name in Assertion	Local Attribute Name
<input type="checkbox"/> lastname	sn
<input type="checkbox"/> firstname	givenname
<input type="checkbox"/> email	mail
<input type="checkbox"/> uid	uid



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://federation1.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:

[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](#)

**Assistance**

[Help](#)

[Log out](#)

## SSO Configuration

[Site Certificate Manager](#)

### Federated Web SSO Configuration

Federation Protocol: SAML 2.0

WebEx SAML Issuer (SP ID):

Issuer for SAML (IdP ID):

Customer SSO Service Login URL:

Default WebEx Target page URL:

Customer SSO Error URL:

NameID Format: Unspecified

AuthnContextClassRef:

SSO Profile:  SP Initiated  
 IdP Initiated

Single Logout

AuthnRequest Signed

Auto Account Creation

Auto Account Update

Remove uid Domain Suffix for Active Directory UPN

### Partner SAML Authentication Access

Host	Site Admin	Partner Certificate	
<input type="checkbox"/>	<input type="checkbox"/>	Everdream	<a href="#">View Details</a>
<input type="checkbox"/>	<input type="checkbox"/>	GeoLearning	<a href="#">View Details</a>
<input type="checkbox"/>	<input type="checkbox"/>	ITech	<a href="#">View Details</a>
<input type="checkbox"/>	<input type="checkbox"/>	WLOFF	<a href="#">View Details</a>

### 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.