Shibboleth-IdP based SSO for AARNET-Plus Zoom Customers

(N.Witheridge 12th March 2015)

Zoom supports Single sign-on (SSO) access based on SAML 2.0. When a user accesses Zoom for the first time by SSO, the user is **auto-provisioned**. If the user already has an account created and has previously accessed via Zoom authentication, the user accessing via SSO will be identified as the existing user based on their email address attribute (primary identifier for Zoom accounts).

Zoom's guidelines are at: https://support.zoom.us/hc/en-us/articles/201363003-Getting-Started-with-SSO

Zoom isn't registered with the AAF as an SP, as each customer has its own Zoom SP based on its vanity URL & customer-specific SP metadata. Hence institutional IdP configuration performed by an institution to enable SSO access to Zoom is independent of any configuration related to its participation in the AAF.

The following steps are required to configure SSO access to Zoom, and are performed by the institution's **Zoom administrator**.

Note, examples below are based on SSO configuration experience with Edith Cowan University (ECU).

1. Obtain a 'vanity' URL for your institution

Access https://zoom.us/account and configure an institution specific **vanity URL**

Typically https://institutionabbrev.zoom.us e.g. https://ecu.zoom.us

2. Enable SSO access to Zoom for your institution

Access https://zoom.us/account/sso, and select "**Enable Single Sign-On**" to display the SAML tab.

3. Enter SSO Information (register your institutional IdP with Zoom)

Access your institutional IdP metadata, typically https://inst_IdP_DomainName/idp/shibboleth
(or request the metadata or below information from your IdP administrator).

Enter the institution's IdP information (from IdP metadata) under the SAML tab.

- **Sign-in page URL**: <SingleSignOnService, either POST or Redirect binding>

  e.g. (text in red) `Location=https://aaf-idp.ecu.edu.au/idp/profile/SAML2/POST/SSO`

- **Sign-out page URL**: <SingleLogoutService> *optional*

- **Certificate**: <X509Certificate>
  Notes: Use the Signing certificate, and remove the Begin Certificate and End Certificate"

  e.g.
  ```
  <ds:X509Certificate>
          MIIDNDCCAhygAwIBAgIVAOgIBqdjU5+O1bsU/tGY+Q68IyuLMA0GCSqGSIb3DQEB
           :
          cCb/ZXNYMBM=
  </ds:X509Certificate>
  ```

- **Issuer**: < IdP EntityID from your IdP metadata> * Note: full EntityID, not just IdP domain name.

  e.g. `entityID=https://aaf-idp.ecu.edu.au/idp/shibboleth`

- Select the appropriate **Binding** (corresponding to Sign-in page) and **Default user type**

4. Configure trust for the Zoom SP in your IdP

The following process and examples are for the Shibboleth SAML2.0 IdP implementation. For other SAML IdP implementations, request assistance from your local IdP administrator.)

After SSO has been configured & saved under the SAML tab, obtain your **Zoom SP metadata** from : https://institutionabbrev.zoom.us/saml/metadata/sp (e.g. save to /var/shibboleth-idp/metadata/zoom_sp_metadata.xml) and configure it as trusted metadata in your IdP configuration (add a metadata element in relying-party.xml).

E.g. adding a metadata in relying-party.xml:

```
    <MetadataProvider id="Zoom_SP_Metadata"
                      xsi:type="ResourceBackedMetadataProvider"
                      xmlns="urn:mace:shibboleth:2.0:metadata">
      <MetadataResource xsi:type="resource:FilesystemResource"
                        file="/var/shibboleth-idp/metadata/zoom_sp_metadata.xml" />
    </MetadataProvider>
```

Also, **disable encrypted assertions** for SAML transactions with the Zoom SP, by adding a RelyingParty element in relying-party.xml.

E.g. of RelyingParty attribute for ECU:

```
<RelyingParty id="ecu.zoom.us" provider=https://aaf-idp.ecu.edu.au/idp/shibboleth
              defaultSigningCredentialRef="IdPCredential" >
    <ProfileConfiguration xsi:type="saml:SAML2SSOProfile" includeAttributeStatement="true"
                          assertionLifetime="PT5M" assertionProxyCount="0"
                          signResponses="never"
                          signAssertions="always"
                          encryptAssertions="never"
                          encryptNameIds="never"/>
</RelyingParty>
```

5. Configure your IdP to send the following attributes to the Zoom SP

The users email address is used as the unique user identifier in Zoom. Configure your idP to release the following attributes.

Attribute	Recommended SAML Attribute Name	Required
Email Address	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Yes
First Name	urn:oid:2.5.4.42	No
Last Name	urn:oid:2.5.4.4	No

E.g.AttributeFilterPolicy element added to attribute-filter.xml:

```
:
    <AttributeFilterPolicy id="releaseToZoom">
        <PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="ecu.zoom.us" />
        <AttributeRule attributeID="email">
            <PermitValueRule xsi:type="basic:ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="givenName">
            <PermitValueRule xsi:type="basic:ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="surname">
             <PermitValueRule xsi:type="basic:ANY"/>
        </AttributeRule>
    </AttributeFilterPolicy>
:
```

6. Test SSO Access

After configuring and restarting the institutional IdP, test SSO access to Zoom.

Using a web browser, access https://institutionabbrev.zoom.us and click on the SSO login button (or access https://institutionabbrev.zoom.us/signin directly).

To login via SSO via the Zoom application (from the desktop or mobile client), select “Sign In with SSO” and enter the institutional vanity URL under “SSO URL”, and click “continue”.