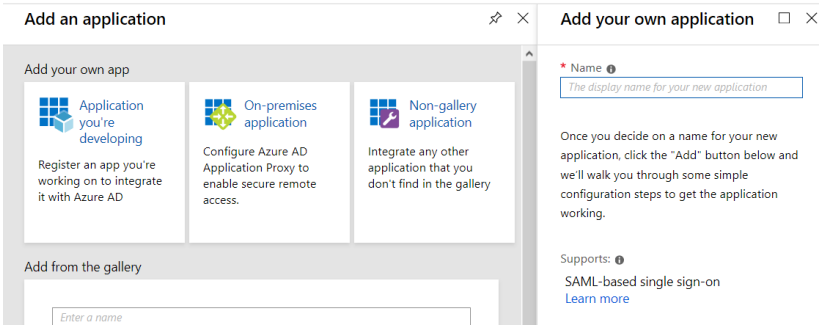
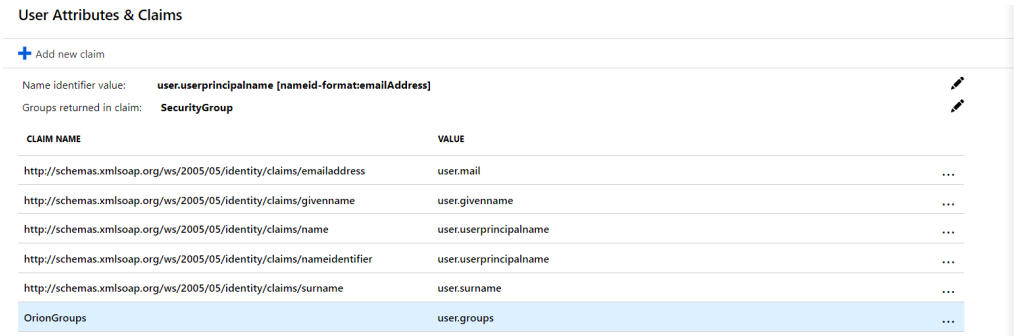
Solarwinds SAML to Azure AD

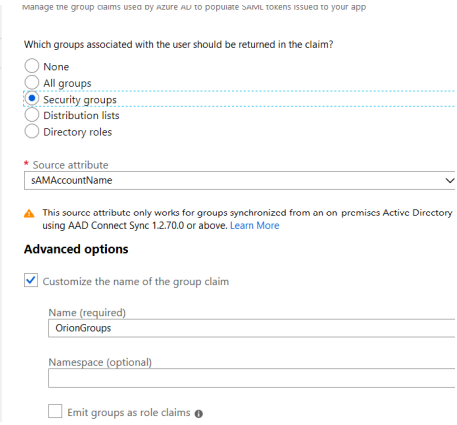
Tuesday, August 6, 2019 2:58 PM

1. Go to portal.azure.com and create a non-gallery enterprise app

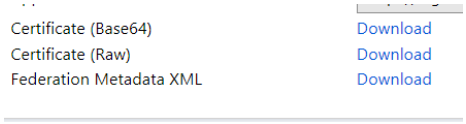


2. After giving your app a name and creating the app on the next page go to the single sign-on link and choose SAML
3. In SAML Settings
   a. Under Basic SAML Configuration set the following values
      i. Identifier (Entity ID) - FQDN of your Solarwinds instance - like - https://solarwinds.my-company.com
      ii. Reply URL (Assertion Consumer Service URL) - link to the SAML login page - like - https://solarwinds.my-company.com/Orion/SamlLogin.aspx
      iii. Leave everything else as is
   b. Under User Attributes & Claims
      i. Leave all user attributes as is
      ii. Add a group claim
         1) Choose Security groups
         2) Change Source Attribute to sAMAccountName - this will limit the groups you can use to on prem only
         3) Customize the name of the group claim to OrionGroups
   c. Save all the settings

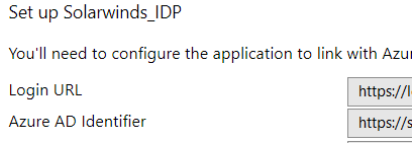




4. Under SAML Signing Certificate
   a. Click the download link next to Certificate (base64) - save this somewhere easy to get to (do not install on your computer if asked) - you will need to open with a text editor like VS Code in order to copy the contents into a text field during the Solarwinds SAML set up



5. Under Set up {Name of your Enterprise App}
   a. Copy the **Login URL** link
   b. Copy **Azure AD Identifier** Link and save for later



6. Go into the Solarwinds Admin setting and choose SAML Configuration
7. Set the **Orion Web Console External URL** to the FQDN of your Solarwinds instance - like - https://solarwinds.my-company.com - click next
8. Under Edit Identity Provider

a. Set **Identity Provider Name** to something like 'Azure AD'
b. Set **SSO Target URL** to the link you copied in **step 5.a** - the **Login URL** from the Azure enterprise application setup
c. Set **Issuer URI** to the link you copied in **step 5.b** - the **Azure AD Identifier** from the Azure enterprise application setup
d. In the **X.509 Signing Certificate** field you will copy the contents of the certificate file you downloaded **step 4.a** - include all text (including the BEGIN CERTIFICATE and END CERTIFICATE lines).

9. Save your configuration
10. The last step is to add users that can login. You will need to assign users/groups or both to the Azure AD Enterprise Application before they can authenticate to against Azure and get routed back to the Solarwinds app
    a. Go to portal.azure.com -> enterprise applications -> users and groups
    b. Click Add user
        i. Add users and groups
11. Go in to your Solarwinds instance
    a. All settings -> Manage Accounts
        i. Add your SAML individual users or groups - the name that you enter here must match the username or group name exactly as in Azure AD
12. That's it