Single Sign On Configuration for Netskope UI Using Azure Active Directory Gallery Application

This guide outlines the process of configuring Azure Active Directory for Single Sign On (SSO) to the Netskope UI. Netskope now offers a gallery application in Azure AD for both admin SSO and user provisioning via SCIM. This guide covers configuring the Azure AD gallery application for admin SSO. You will need the following:

- Azure Active Directory Subscription that supports Enterprise Applications
- A Netskope tenant
- An Azure Active directory user with which to test functionality

Procedure Overview

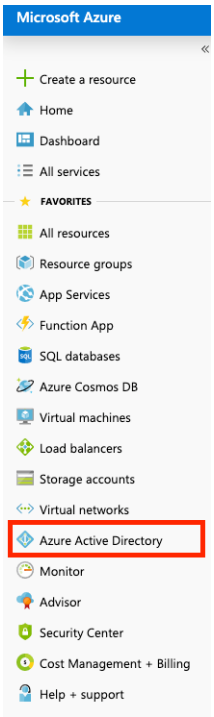
1. Create Enterprise Application and Configure SSO in Azure Active Directory (Steps 1 – 11)
2. Exchange SSO configuration parameters between Netskope and Azure AD(Steps 12 – 37)
3. Assign Users and/or Groups to the Netskope application in Azure AD (Steps 31 – 43)

Version 2.0 – Last Updated January 24th, 2020 – Samuel Shiflett – sshiflett@netskope.com

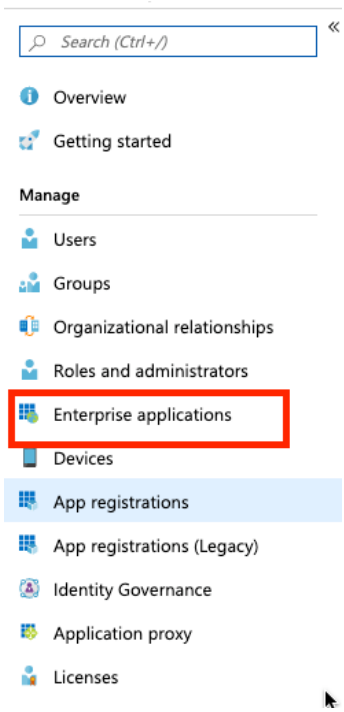
Configuring SSO in Azure Active Directory and Netskope

1. Login to the Microsoft Azure Portal.

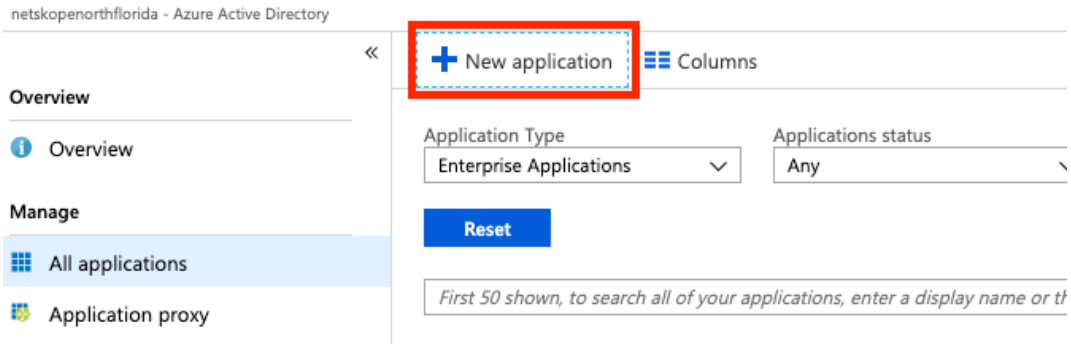
2. Select Azure Active Directory:



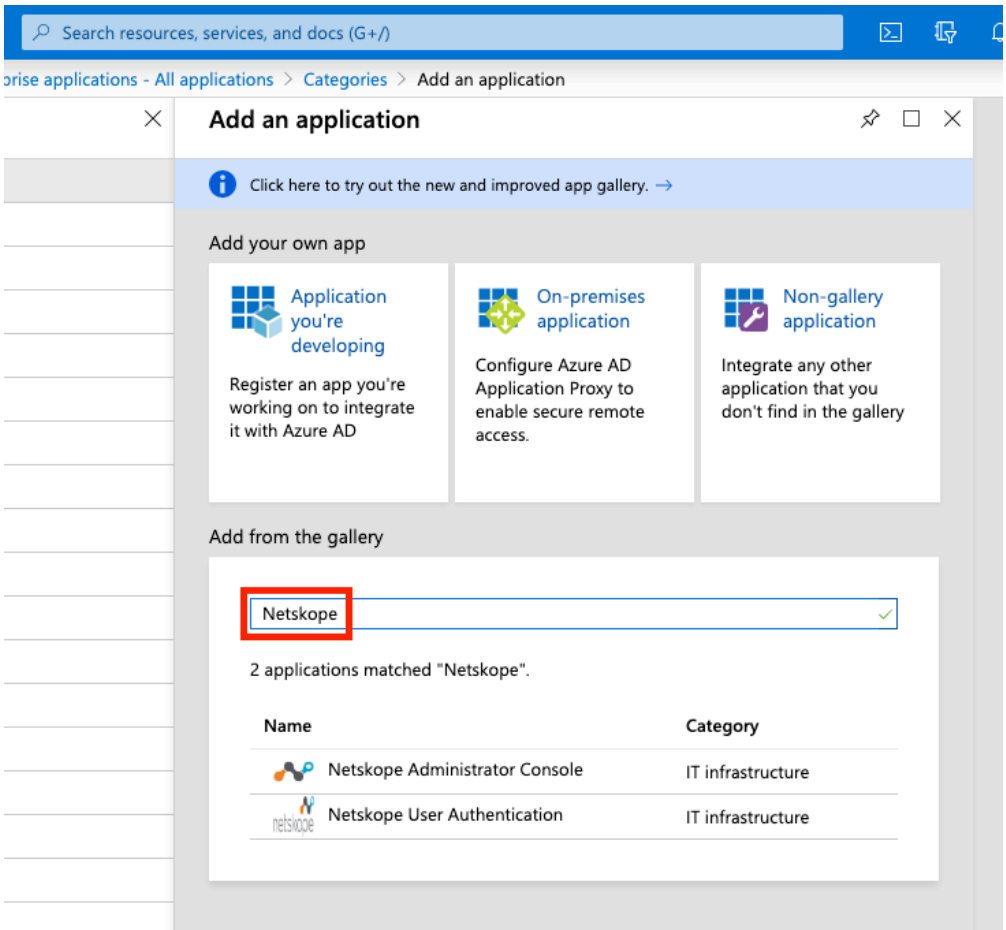
3. Select Enterprise applications:



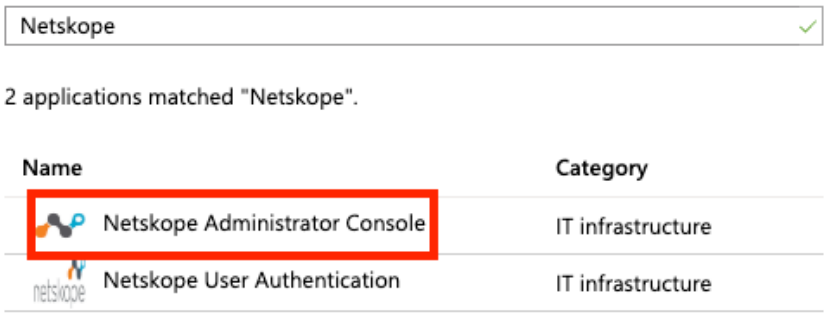
4. Select New application:



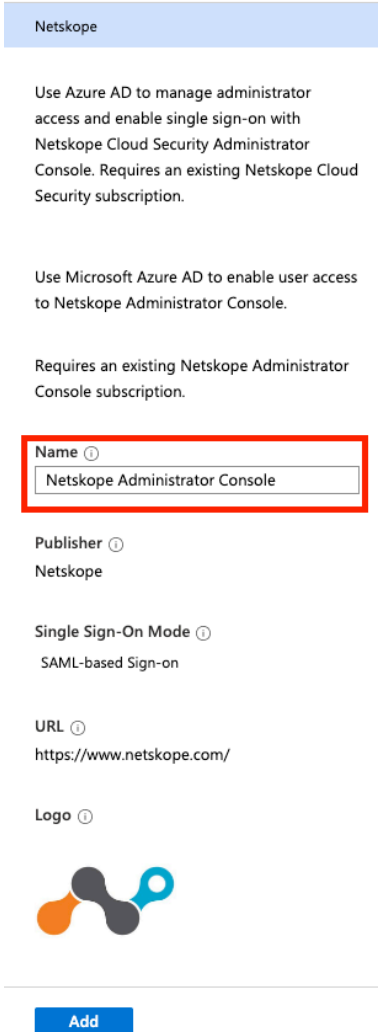
5. Search for Netskope in the gallery.



6. Select “Netskope Administrator Console.”

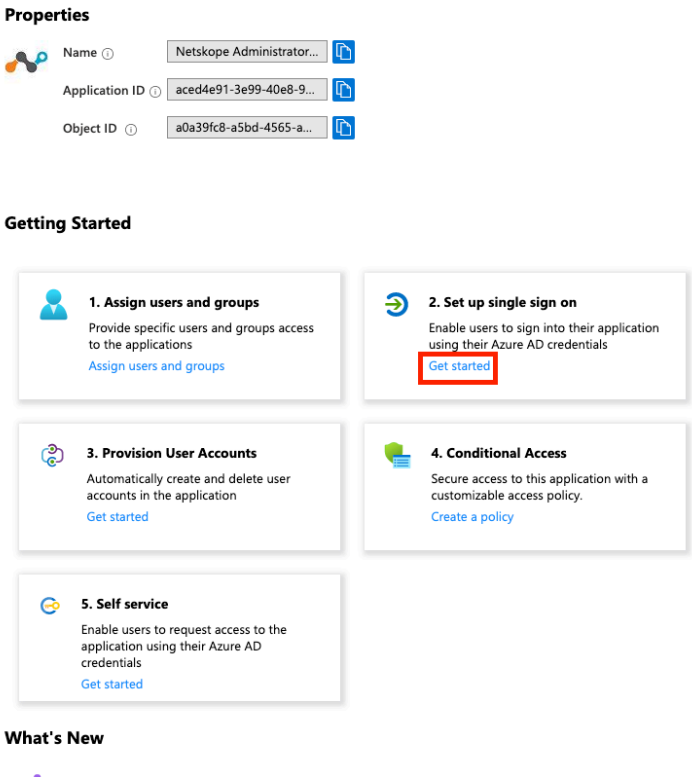


7. Provide a name for the application. Keep in mind that this is the name your users will see on their Access Panel.

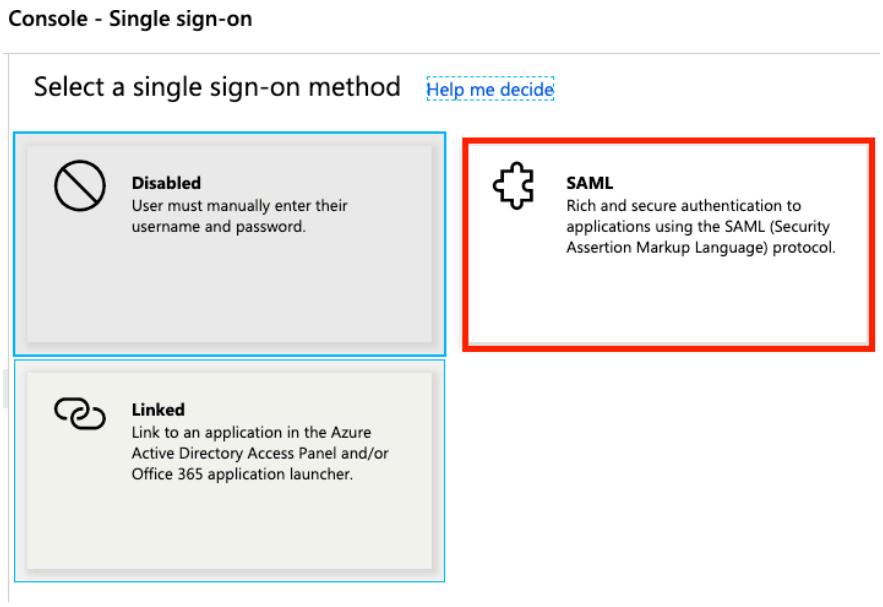


8. Click Add.

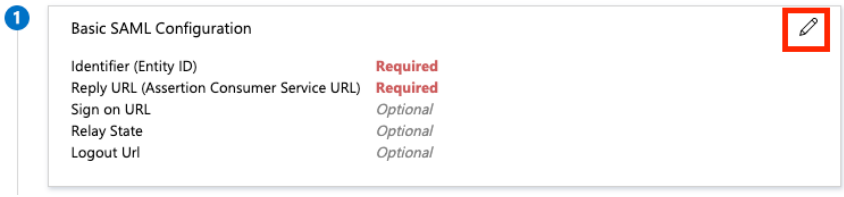
9. Select “Get Started” on the “Set up single sign” on tile.



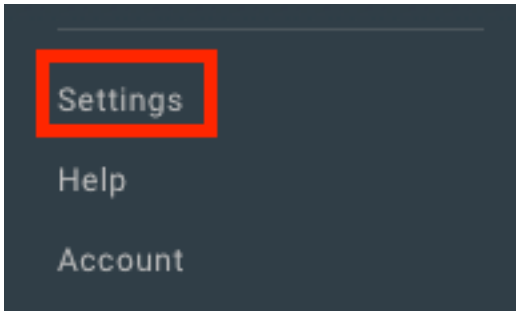
10. Select SAML for the single sign-on method.



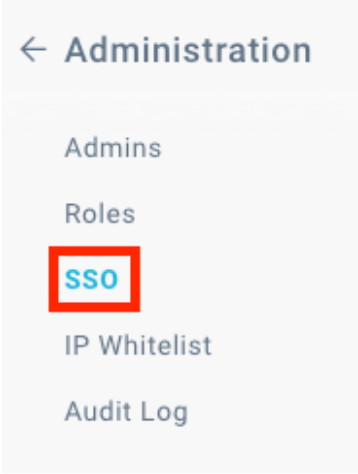
11. Click the pencil icon under Basic SAML Configuration.



12. You will need URLs and information from Netskope at this point. Login to your Netskope tenant and navigate to Settings on the bottom left:

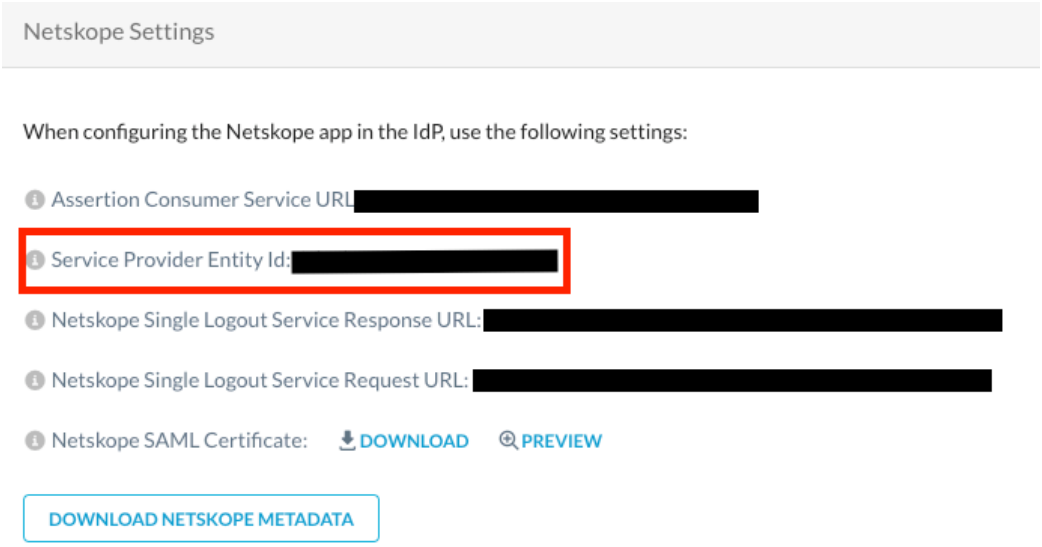


13. Navigate to Administration and then SSO in the right pane:

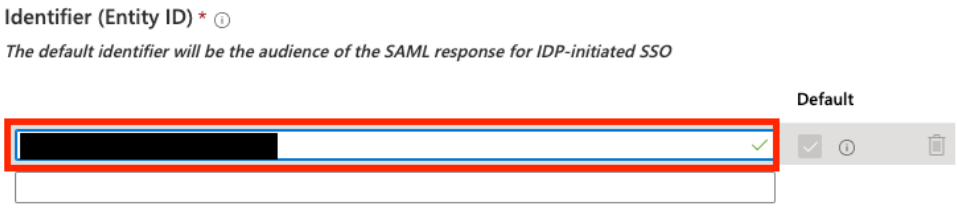


14. Copy the string from Service Provider Entity ID under the Netskope Settings section:

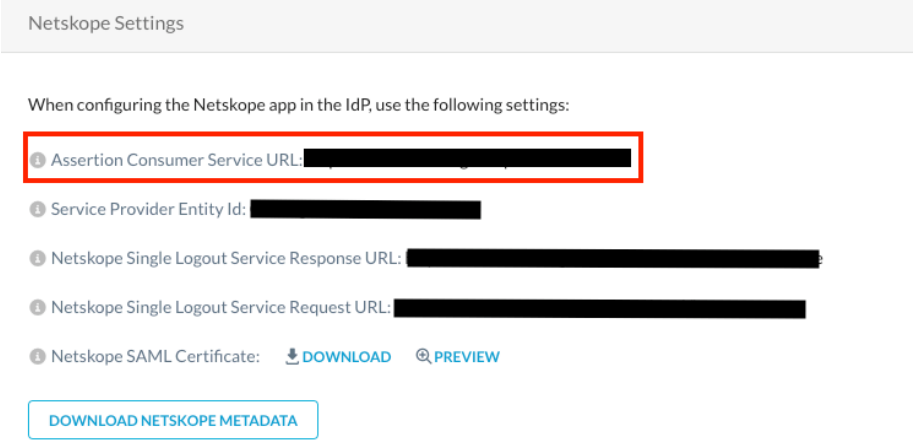
    The string should be similar to Cdc7athjXYFU06mul



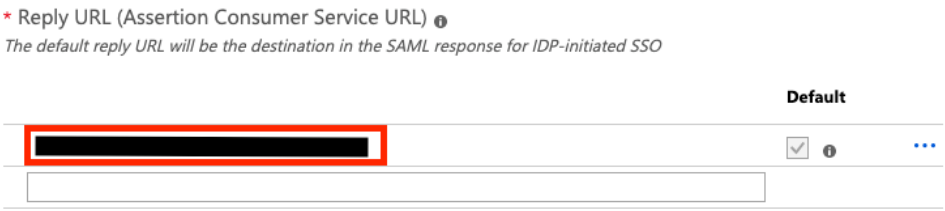
15. In the Azure Portal, paste that string into the Identifier (Entity ID) field:



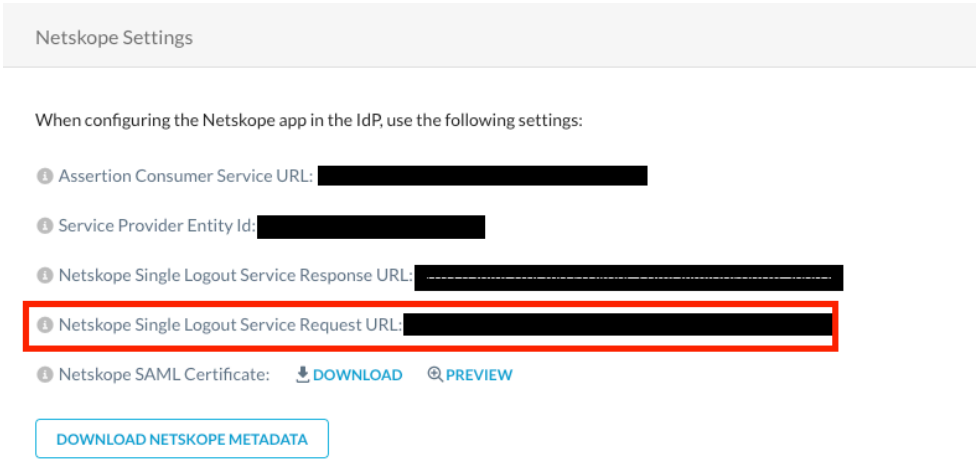
16. Copy the URL from the Assertion Consumer Service URL. The URL should be similar to https://<tenantname>goskope.com/saml/acs



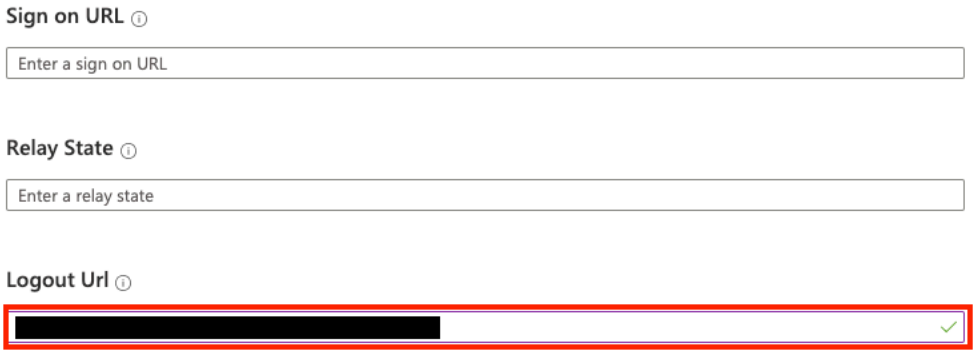
17. Paste the URL into the field for Reply URL (Assertion Consumer Service URL).



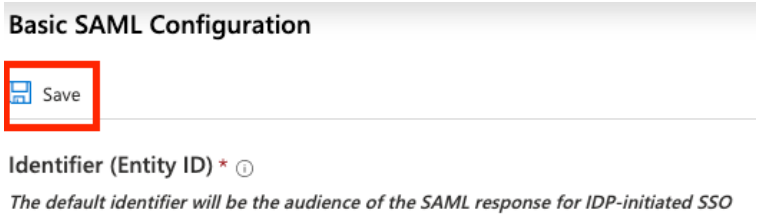
18. Copy the URL from the Netskope Single Logout service Request URL. The URL should be similar to https://<tenantname>goskope.com/saml/logoutRequest



19. Paste the URL into the field for Logout URL.

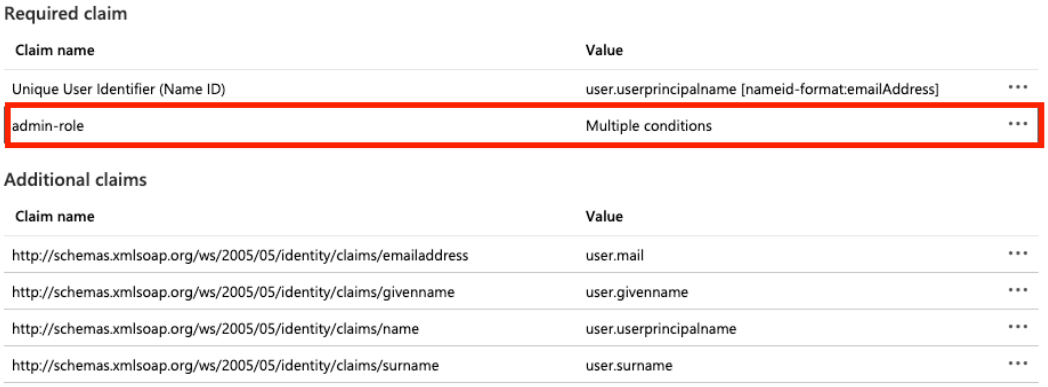


20. Click “Save.”



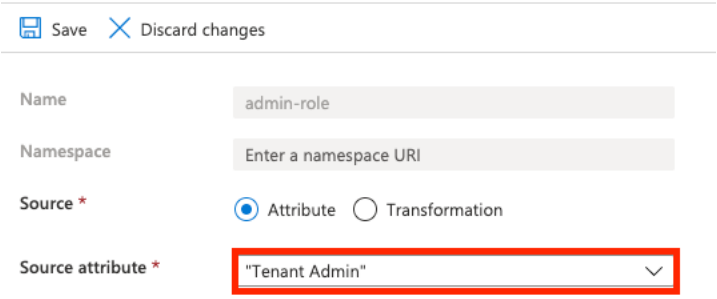
21. Click the pencil icon for User Attributes & Claims:

22. Click on the admin-role claim.

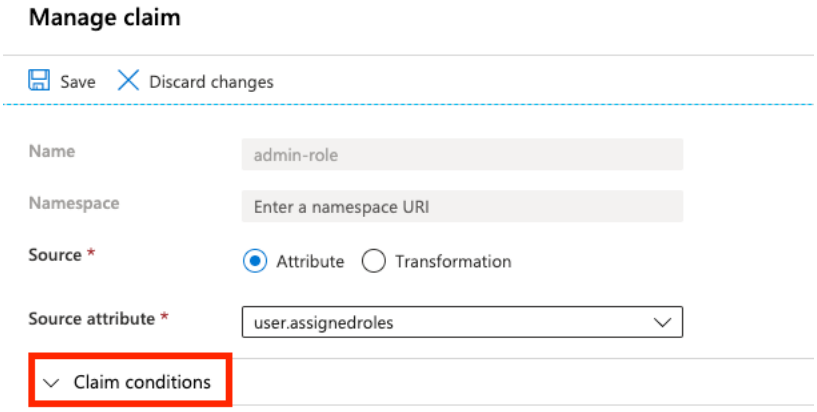


23. This pane is for the user attribute that will be passed to Netskope representing the admin role. By default, AzureAD uses the user.assignedroles as the attribute that is passed to Netskope during the single sign-on process. You can assign the admin role a number of ways but two examples are listed below:

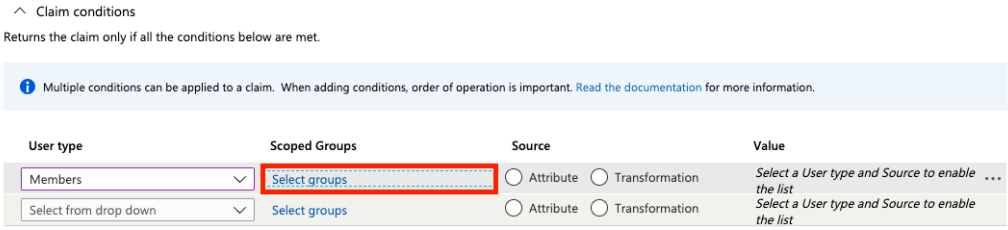
- If all members accessing the Netskope UI require the same role then you can statically assign a role by entering the role name in the “Source attribute” field. This must match the name of the role in the Netskope UI.



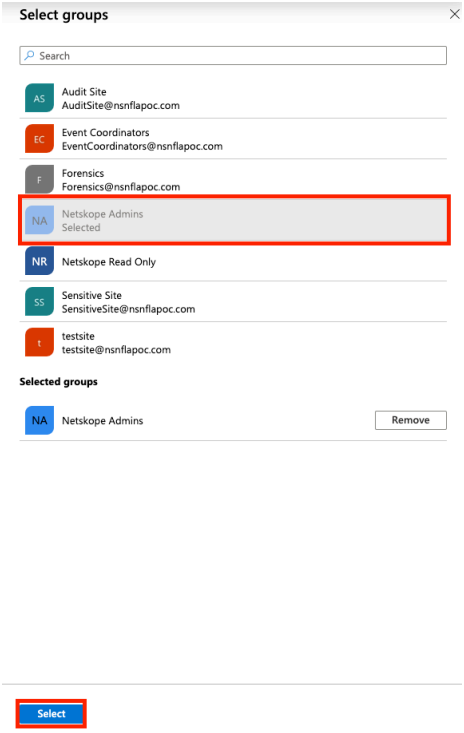
- You can also pass the admin role based on specific users or groups by using Claim conditions.
  - Click Claim conditions.



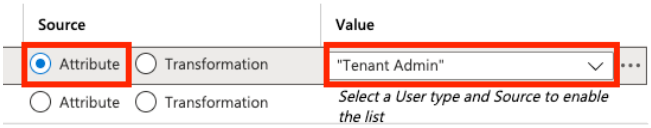
  - Select User type “Members” and click “Select groups”:



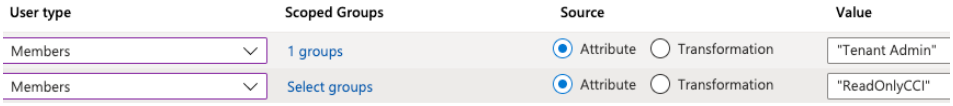
- Select the group(s) you want to scope the role to and click “Select.”



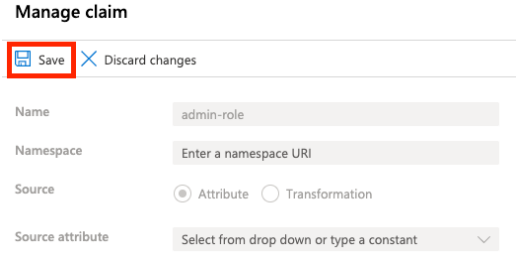
- Select the “Attribute” radio button and enter the admin role you want to assign to the selected group.



- Repeat the above steps for each group and role that needs access.

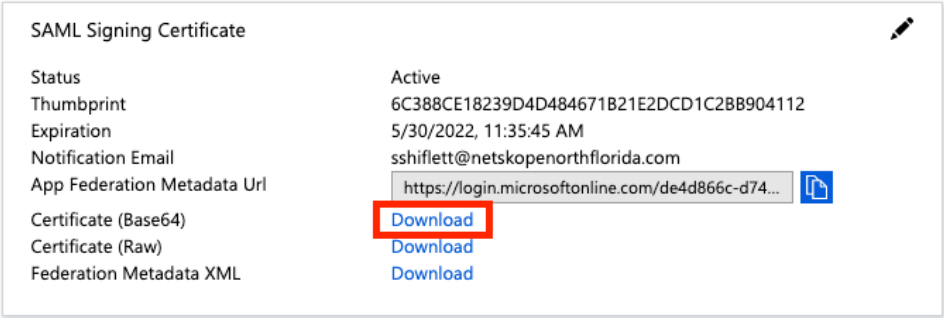


- Click “Save”

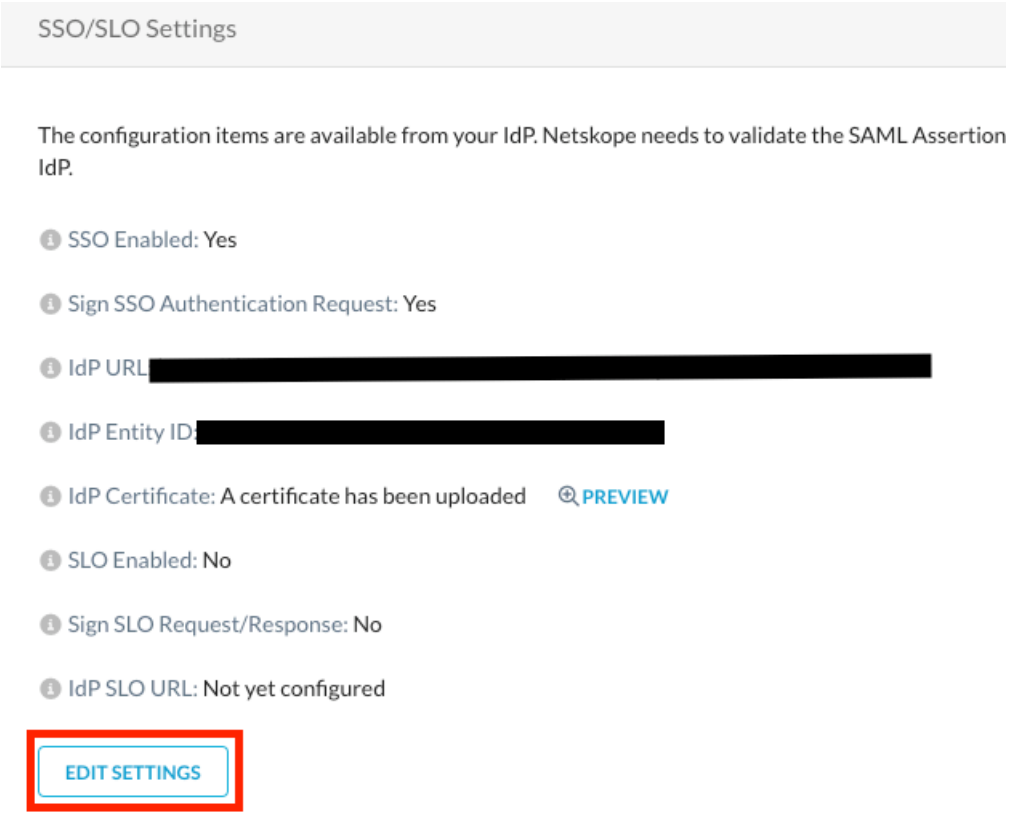


24. Exit out of the User Attributes and Claims pane.

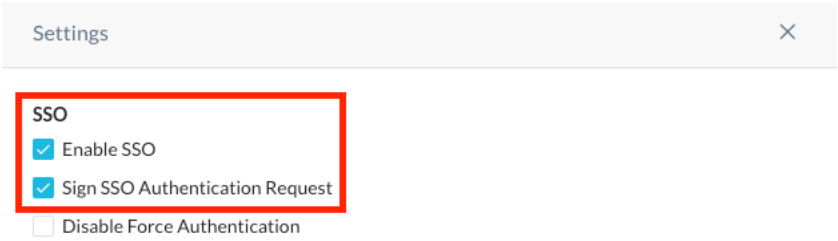
25. Download the SAML Signing Certificate in Base64 format:



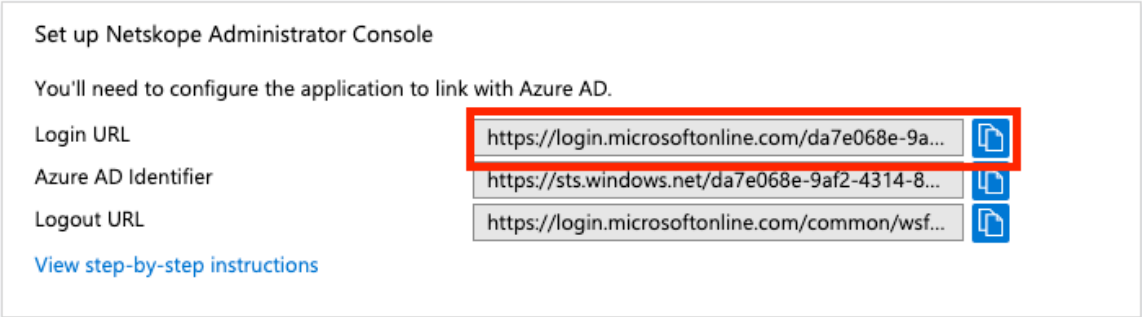
26. Navigate back to the Netskope portal and select Edit Settings under SSO/SLO Settings:



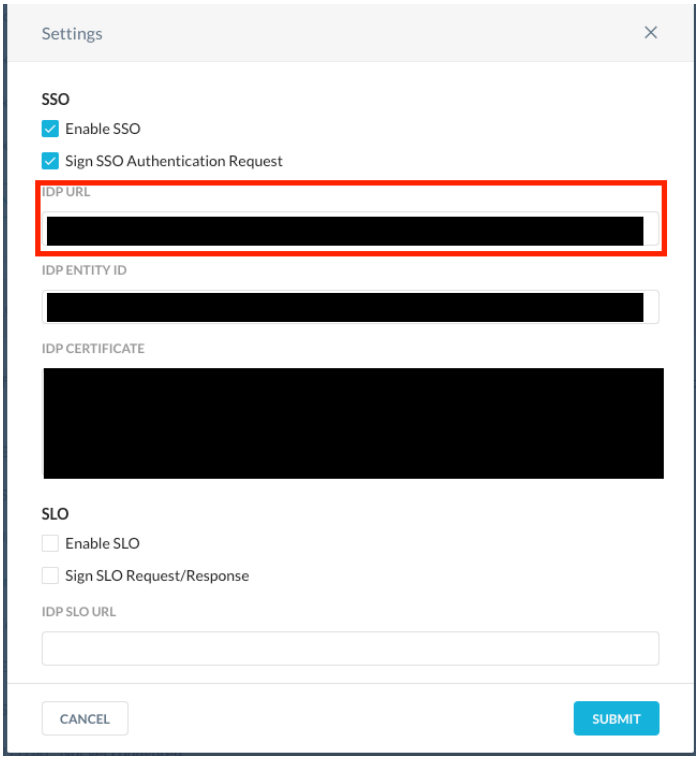
27. Check the boxes for Enable SSO and Sign SSO Authentication Request.



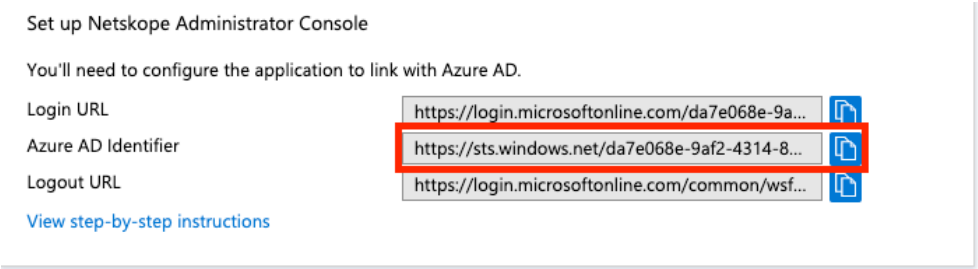
28. Copy the Login URL from the Azure Portal under the Set up <Your Application Name> section. The login URL should be similar to https://login.microsoftonline.com/88ca94db-d34f-44ae-8bc7-de7b7fcd25ed/saml2



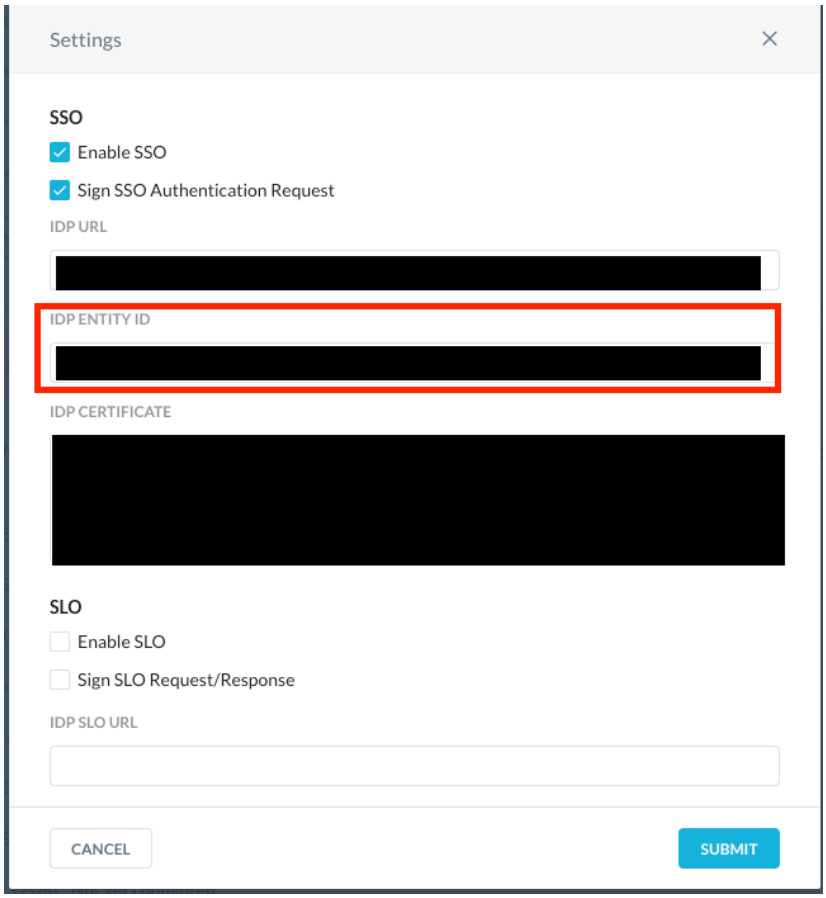
29. Paste the Login URL from the Azure Portal to the IDP URL field in the SSO Settings window in the Netskope portal:



30. Copy the URL from the Azure AD Identifier field under the Set up Netskope SSO section. It should be similar to https://sts.windows.net/88ca94db-d34f-44ae-8bc7-de7b7fcd25ed.

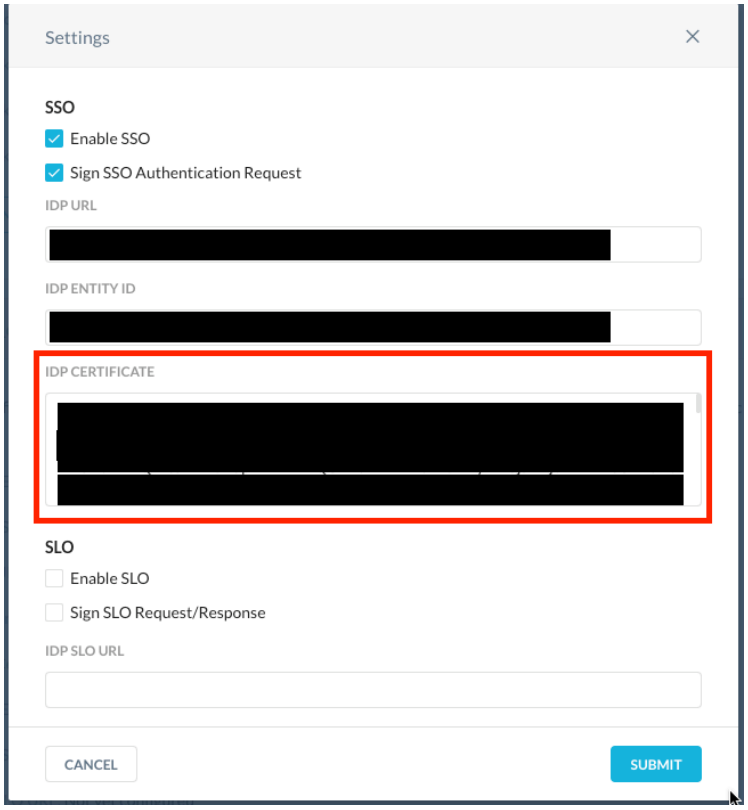


31. Paste the string from the Azure AD Identifier field from the Azure Portal to the IDP Entity ID field in the SSO Settings window in the Netskope portal:

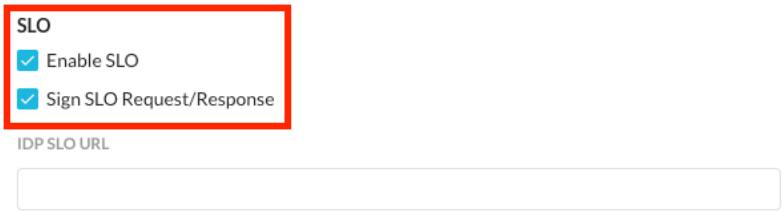


32. Open the certificate file you downloaded in Step 18 from the Azure Portal in a text editor. Copy the entire certificate string including the Begin Certificate and End Certificate lines:

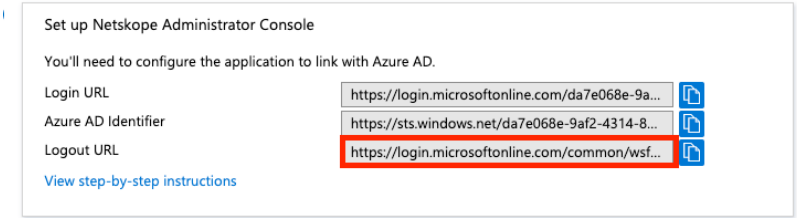
33. Paste the certificate string into the IDP Certificate field of the SSO Settings window of the Netskope portal:



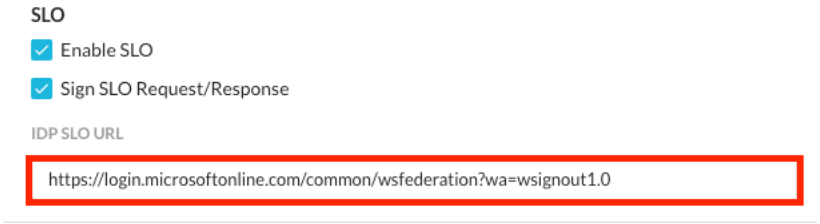
34. Check the “Enable SLO” and “Sign SLO Request/Response” boxes.



35. Copy the URL from the Logout URL field in the Azure portal. It should be similar to https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

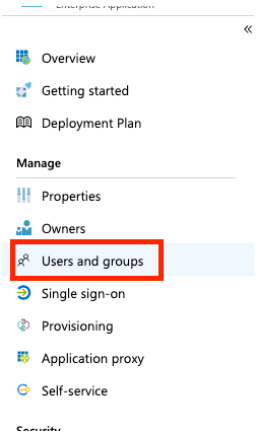


36. Past the URL into the IDP SLO URL in the Netskope portal.

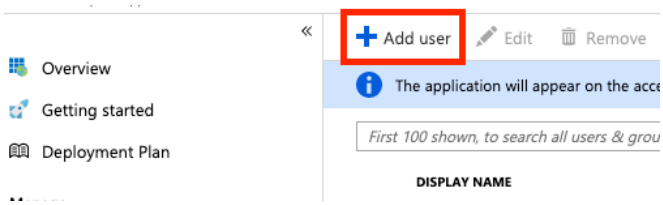


37. Click Submit.

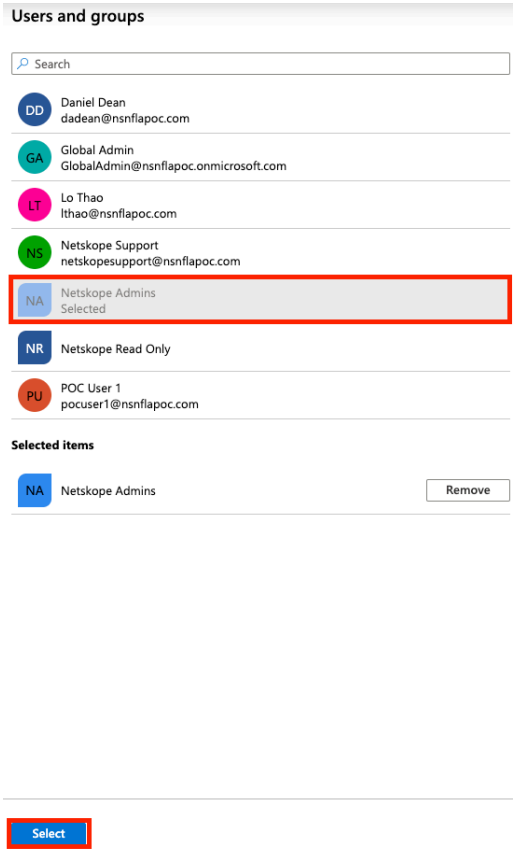
38. Navigate back to the Netskope Administrator Console Overview and select Users and groups:



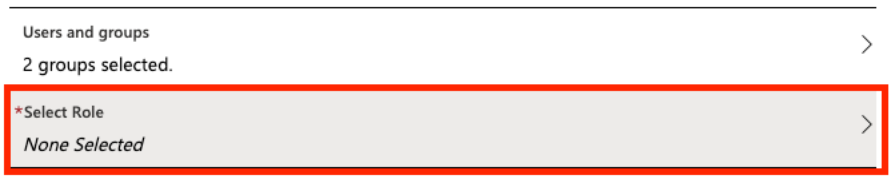
39. Click Add user:



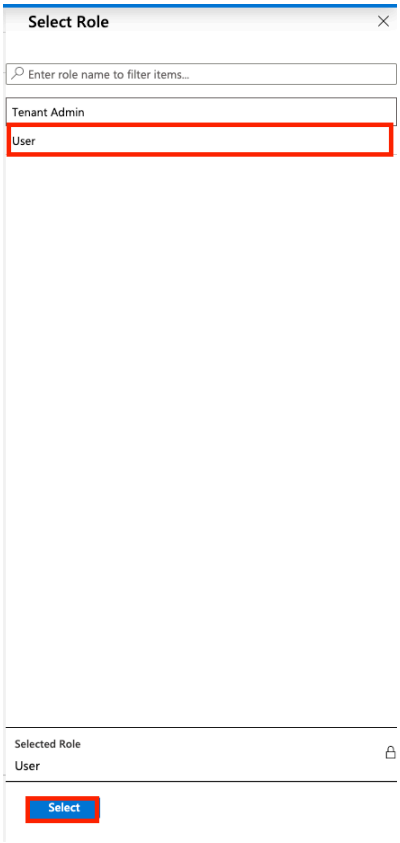
40. Click Users and groups and select the user(s) and group(s) who need access and then click Select.



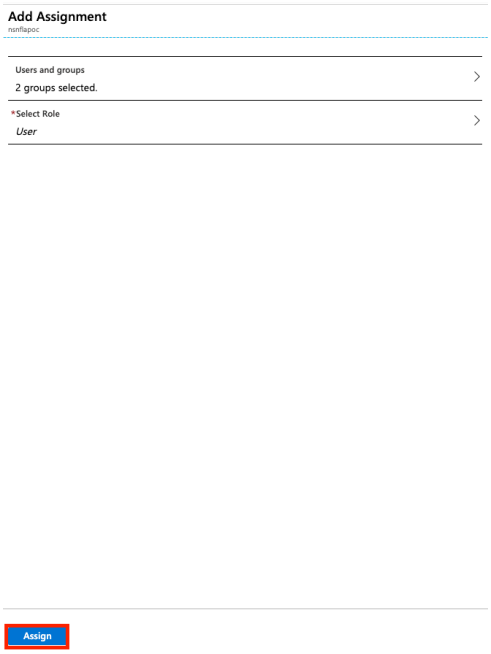
41. Click “Select Role”



42. Select the User role and click “Select.”



43. Click Assign.



This completes the setup. You can test by going directly to your tenant (tenantname.goskope.com) and verifying that SSO works. You can also try an Azure AD initated login as both should work.