

# 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

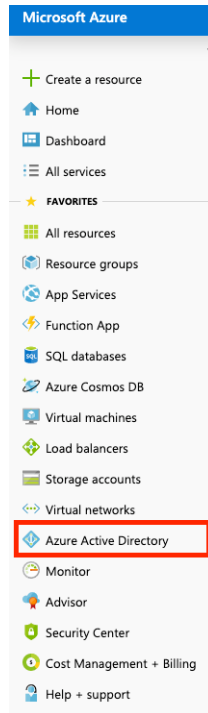
## Procedure Overview

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 – 26)
3. Assign Users and/or Groups to the Netskope application in Azure AD (Steps 27 – 32)

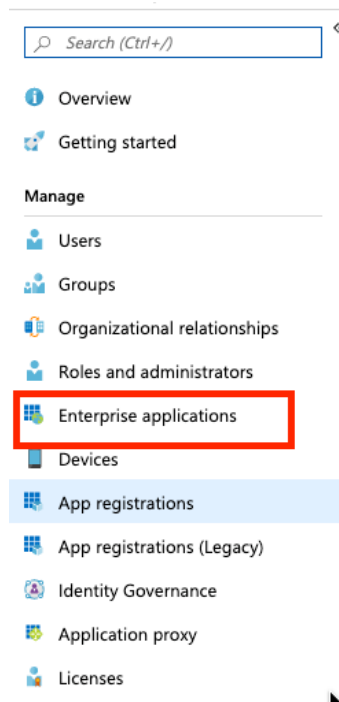
## Configuring SSO in Azure Active Directory and Netskope

1. Login to the Microsoft Azure Portal.

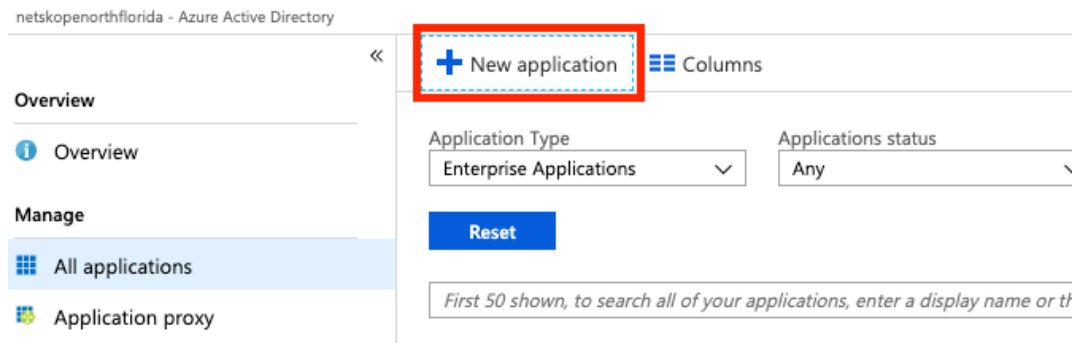
2. Select Azure Active Directory:



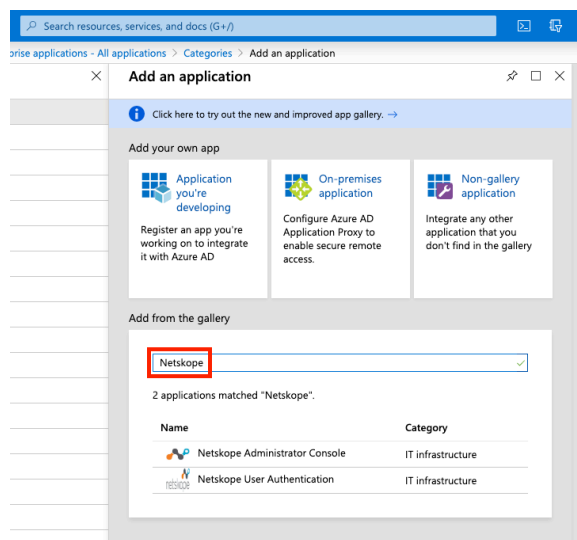
3. Select Enterprise applications:



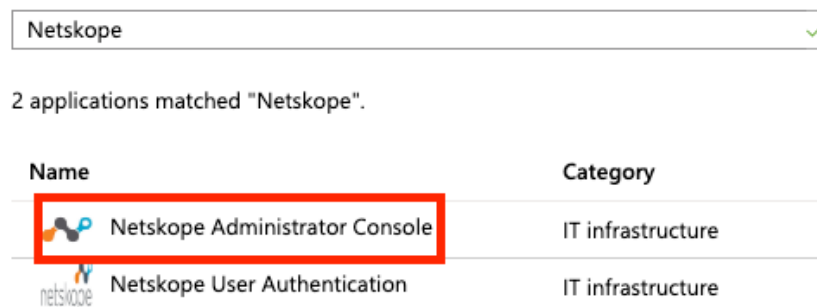
4. Select New application:



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.

Netskope

Use Azure AD to manage administrator access and enable single sign-on with Netskope Cloud Security Administrator Console. Requires an existing Netskope Cloud Security subscription.

Use Microsoft Azure AD to enable user access to Netskope Administrator Console.


Requires an existing Netskope Administrator Console subscription.

Name ⓘ  
Netskope Administrator Console

Publisher ⓘ  
Netskope

Single Sign-On Mode ⓘ  
SAML-based Sign-on

URL ⓘ  
<https://www.netskope.com/>


Logo ⓘ  


Add

8. Click Add.

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


**Properties**


 Name ⓘ Netskope Administrator... ⓘ


Application ID ⓘ aced4e91-3e99-40e8-9... ⓘ


Object ID ⓘ a0a39fc8-a5bd-4565-a... ⓘ


**Getting Started**

 **1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)

 **2. Set up single sign on**  
Enable users to sign into their application using their Azure AD credentials  
[Get started](#)

 **3. Provision User Accounts**  
Automatically create and delete user accounts in the application  
[Get started](#)

 **4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)

 **5. Self service**  
Enable users to request access to the application using their Azure AD credentials  
[Get started](#)


**What's New**


-


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

#### Console - Single sign-on


Select a single sign-on method [Help me decide](#)

**Disabled**  
User must manually enter their username and password.

**SAML**  
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

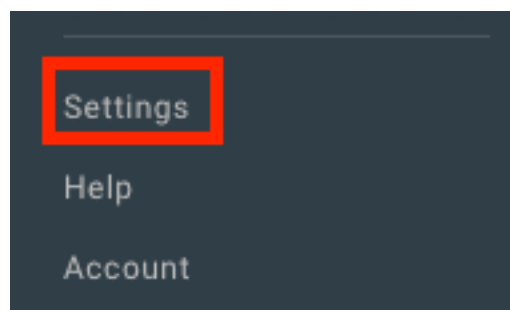
**Linked**  
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

11. Click the pencil icon under Basic SAML Configuration.

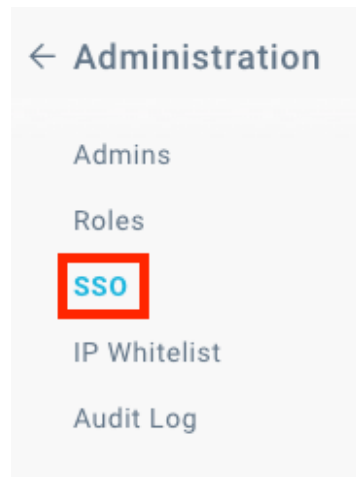
1 Basic SAML Configuration 

Identifier (Entity ID)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

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. Paste this into the Identifier (Entity ID) field in the Azure portal. See Figure 1.

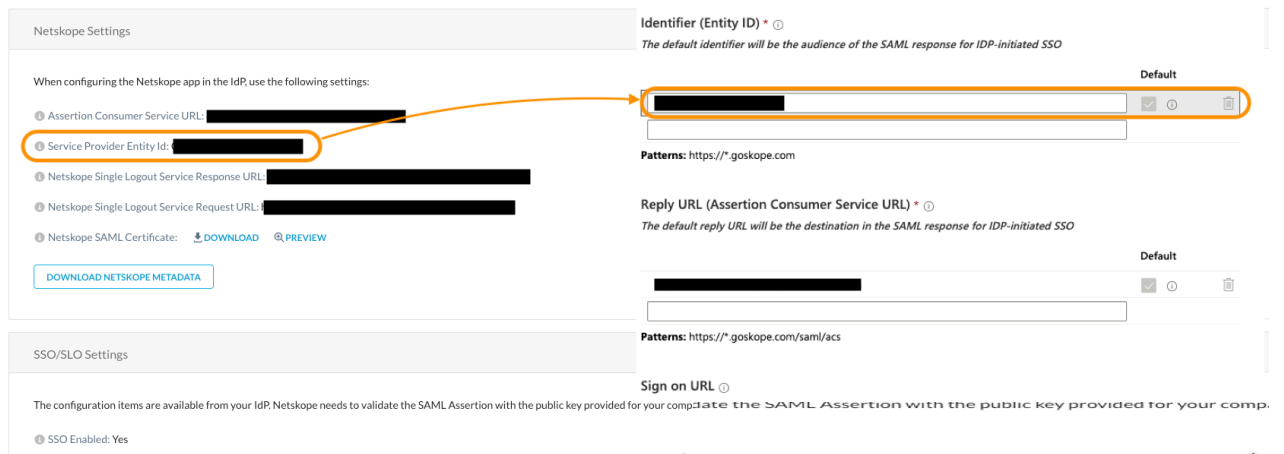


Figure 1

15. Copy the URLs from Netskope according to Figure 2:

1. Assertion Consumer Service URL to Reply URL (Assertion Consumer Service URL)
2. Netskope Single Logout Service Request URL to Logout Url

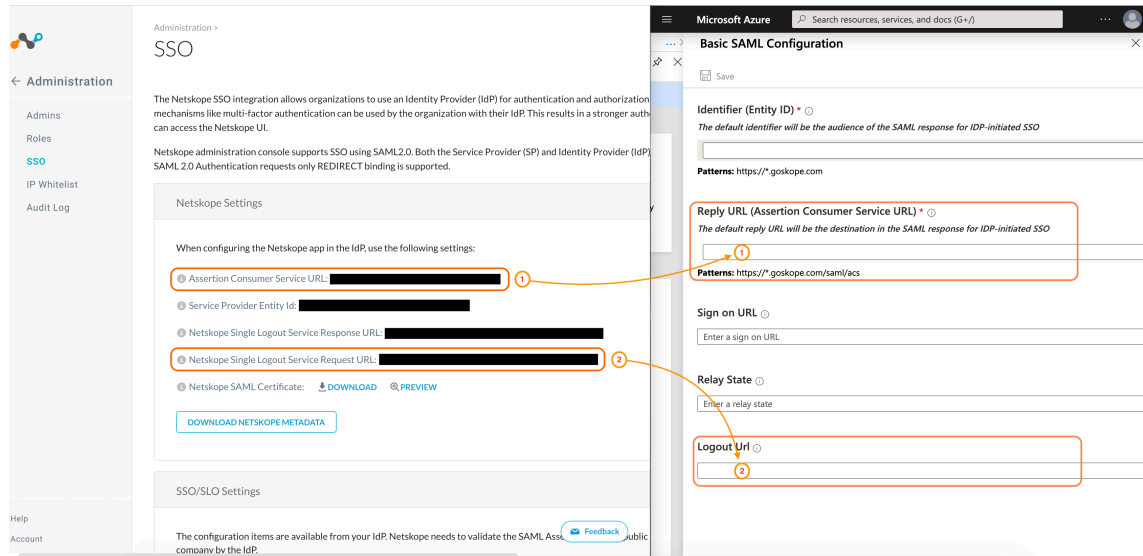


Figure 2

16. Click “Save.”



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





18. Click on the admin-role claim.

Required claim		
Claim name	Value	
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress]	***
admin-role	Multiple conditions	***
Additional claims		
Claim name	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail	***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	***

19. 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.

 Save  Discard changes

Name

admin-role

Namespace

Enter a namespace URI

Source \*

☒ Attribute ☐ Transformation



Source attribute \*

Tenant Admin

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

- Click Claim conditions.

#### Manage claim

 Save  Discard changes

Name

admin-role

Namespace

Enter a namespace URI

Source \*

☒ Attribute ☐ Transformation

Source attribute \*

user.assignedroles

Claim conditions



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

Claim conditions

Returns the claim only if all the conditions below are met.

**i** Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. [Read the documentation](#) for more information.

User type	Scoped Groups	Source	Value
Members	Select groups	<input type="radio"/> Attribute <input type="radio"/> Transformation	Select a User type and Source to enable ...
Select from drop down	Select groups	<input type="radio"/> Attribute <input type="radio"/> Transformation	Select a User type and Source to enable the list

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

Select groups

AS Audit Site  
AuditSite@nsnflapoc.com

EC Event Coordinators  
EventCoordinators@nsnflapoc.com

F Forensics  
Forensics@nsnflapoc.com

NA Netskope Admins  
Selected

NR Netskope Read Only

SS Sensitive Site  
SensitiveSite@nsnflapoc.com

t testsite  
testsite@nsnflapoc.com

Selected groups

NA Netskope Admins

Remove

Select

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



Source	Value
<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation	<input type="text" value="Tenant Admin"/>
<input type="radio"/> Attribute <input type="radio"/> Transformation	Select a User type and Source to enable the list

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

User type	Scoped Groups	Source	Value
Members	1 groups	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation	"Tenant Admin"
Members	Select groups	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation	"ReadOnlyCCI"

- Click "Save"

#### Manage claim

 Save  Discard changes

Name

admin-role

Namespace

Enter a namespace URI

Source

☒ Attribute ☐ Transformation

Source attribute

Select from drop down or type a constant

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

21. Download the SAML Signing Certificate in Base64 format:

SAML Signing Certificate

Status

Active

Thumbprint

6C388CE18239D4D484671B21E2DCD1C2BB904112


Expiration

5/30/2022, 11:35:45 AM

Notification Email

sshiflett@netskopenorthflorida.com

App Federation Metadata Url

https://login.microsoftonline.com/de4d866c-d74... 

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)


Federation Metadata XML


[Download](#)


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


SSO/SLO Settings


The configuration items are available from your IdP. Netskope needs to validate the SAML Assertion IdP.


 SSO Enabled: Yes


 Sign SSO Authentication Request: Yes


 IdP URL

 IdP Entity ID

 IdP Certificate: A certificate has been uploaded [PREVIEW](#)

 SLO Enabled: No

 Sign SLO Request/Response: No

 IdP SLO URL: Not yet configured

[EDIT SETTINGS](#)

23. Check the boxes to “Enable SSO” and “Sign SSO Authentication Request.” See Figure 3.

24. From the Azure Portal, copy the following info to Netskope.

1. Login URL to IDP URL
2. Azure AD Identifier to IDP Entity ID
3. The certificate you downloaded in step 20 to IDP Certificate.
4. Logout URL to IDP SLO URL

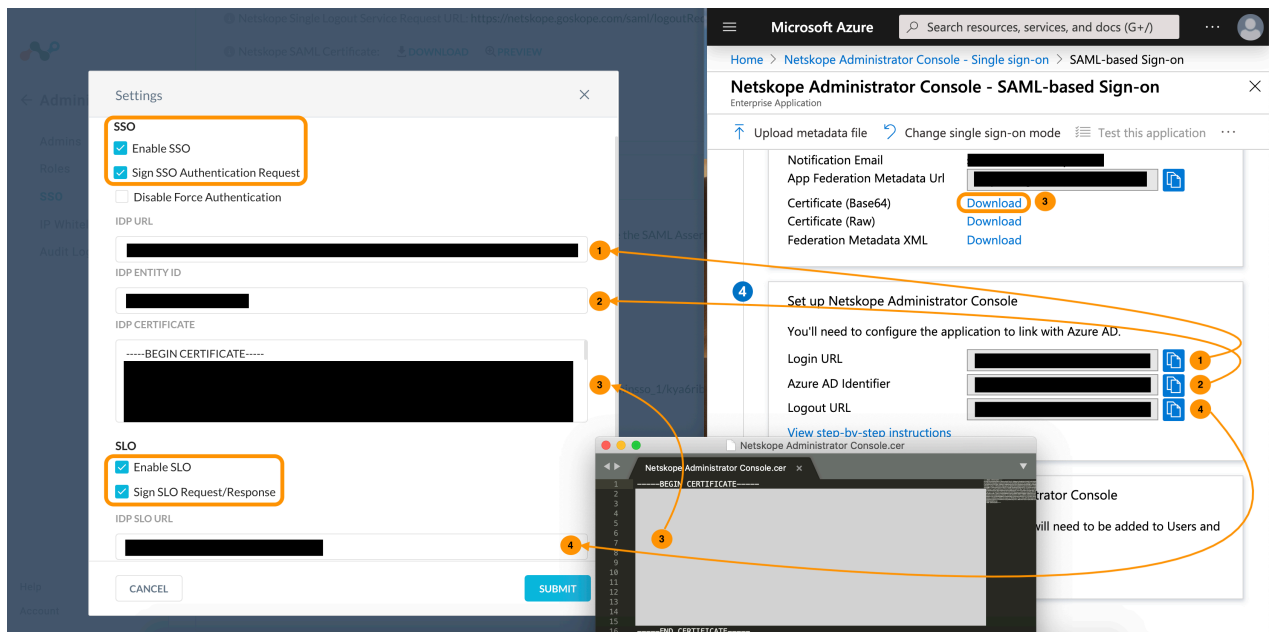
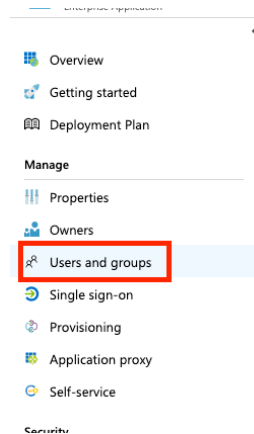


Figure 3

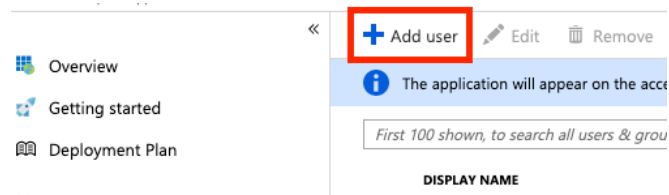
25. Check the boxes to Enable SLO and Sign SLO Request/Response. See Figure 3.

26. Click Submit.

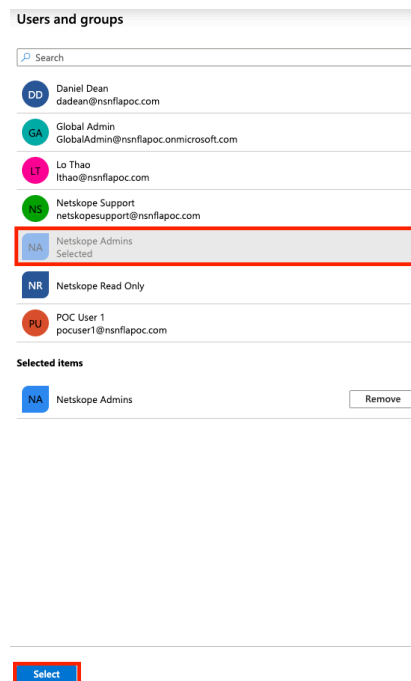
27. Navigate back to the Netskope Administrator Console Overview and select Users and groups:



28. Click Add user:



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



30. Click "Select Role"

Users and groups  
2 groups selected.

\*Select Role  
None Selected

31. Select the User role and click "Select."

Select Role

Enter role name to filter items...

Tenant Admin

User

Selected Role  
User

Select

32. Click Assign.

Add Assignment

Users and groups  
2 groups selected.

\*Select Role  
User

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 initiated login as both should work.