

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

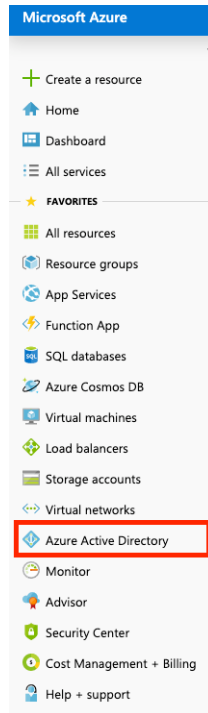
Procedure Overview

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)

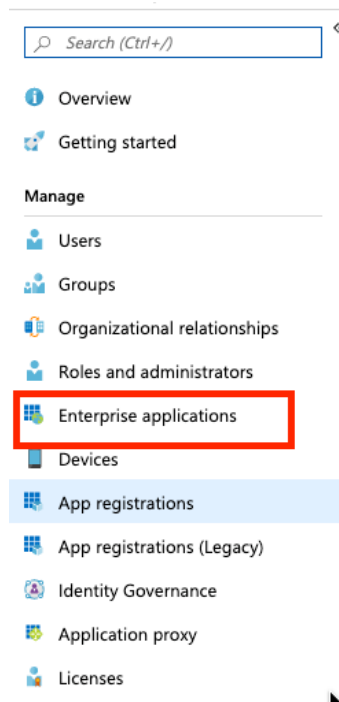
Configuring SSO in Azure Active Directory and Netskope

1. Login to the Microsoft Azure Portal.

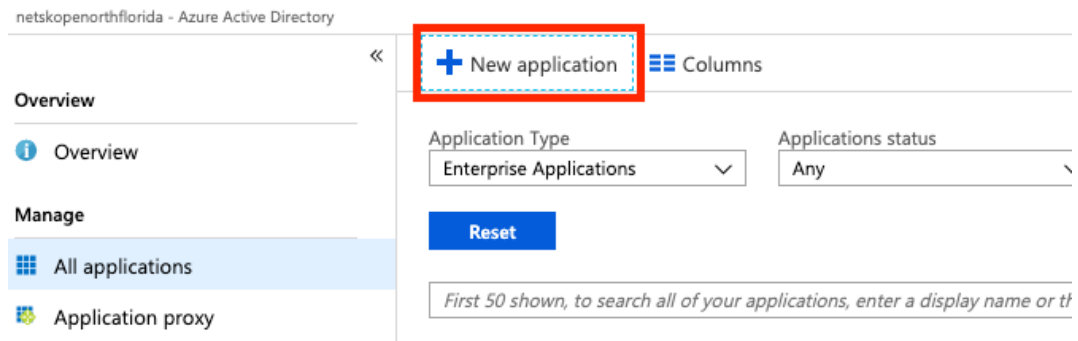
2. Select Azure Active Directory:



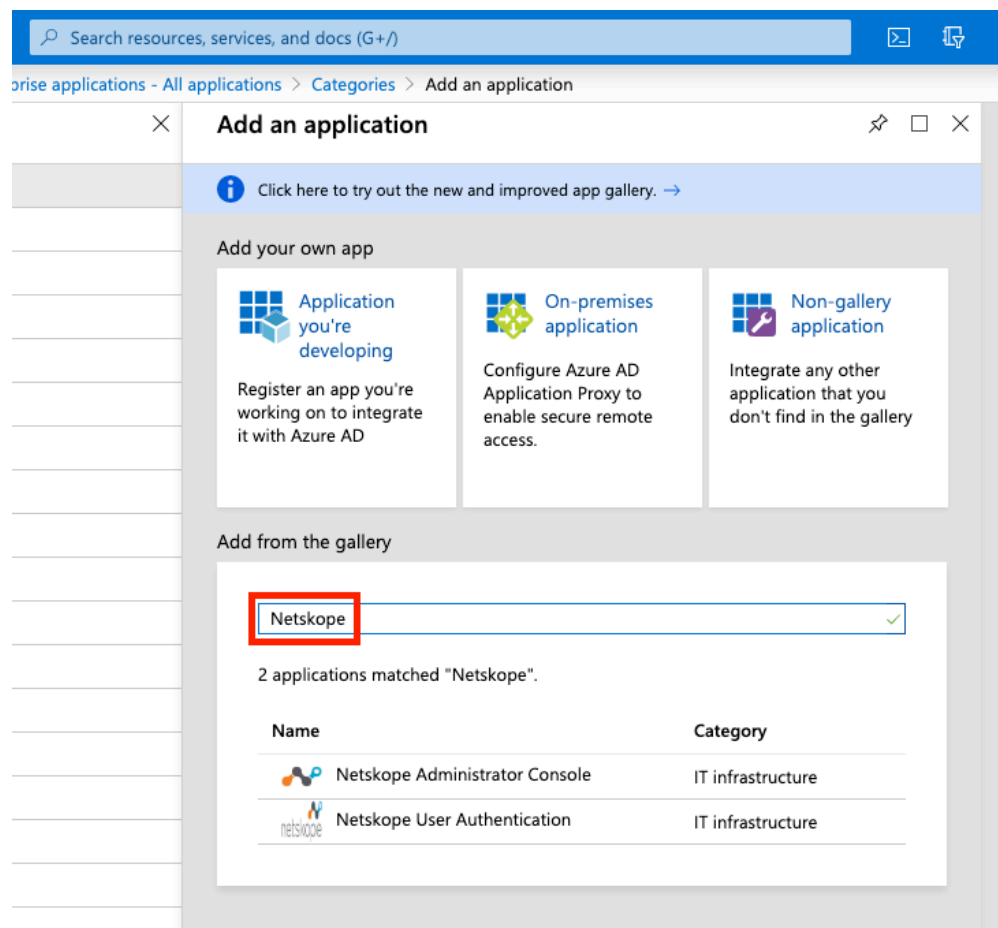
3. Select Enterprise applications:



4. Select New application:





5. Search for Netskope in the gallery.



6. Select "Netskope Administrator Console."

✓

2 applications matched "Netskope".

Name	Category
 Netskope Administrator Console	IT infrastructure
 Netskope User Authentication	IT infrastructure

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.

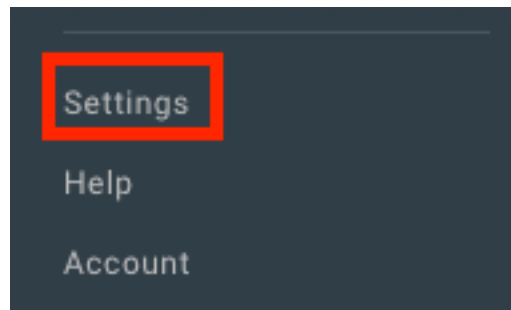
**Linked**
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

11. Click the pencil icon under Basic SAML Configuration.

1

Basic SAML Configuration		
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State	Optional	
Logout Url	Optional	

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

Netskope Settings

When configuring the Netskope app in the IdP, use the following settings:

- Assertion Consumer Service URL: [Redacted]
- Service Provider Entity Id: [Redacted]**
- Netskope Single Logout Service Response URL: [Redacted]
- Netskope Single Logout Service Request URL: [Redacted]
- Netskope SAML Certificate: [DOWNLOAD](#) [PREVIEW](#)

[DOWNLOAD NETSKOPE METADATA](#)

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

Identifier (Entity ID) * ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

[Redacted] ✓

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

Netskope Settings

When configuring the Netskope app in the IdP, use the following settings:

- Assertion Consumer Service URL: [Redacted]**
- Service Provider Entity Id: [Redacted]
- Netskope Single Logout Service Response URL: [Redacted]
- Netskope Single Logout Service Request URL: [Redacted]
- Netskope SAML Certificate: [DOWNLOAD](#) [PREVIEW](#)

[DOWNLOAD NETSKOPE METADATA](#)

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

* Reply URL (Assertion Consumer Service URL) ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

☒ ⓘ ...

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

Netskope Settings

When configuring the Netskope app in the IdP, use the following settings:

ⓘ Assertion Consumer Service URL:

ⓘ Service Provider Entity Id:

ⓘ Netskope Single Logout Service Response URL:

ⓘ Netskope Single Logout Service Request URL:

ⓘ Netskope SAML Certificate: [DOWNLOAD](#) [PREVIEW](#)

[DOWNLOAD NETSKOPE METADATA](#)

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

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

20. Click “Save.”

Basic SAML Configuration

 Save

Identifier (Entity ID) * ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

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

User Attributes & Claims 

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Admin-role	user.assignedroles
Unique User Identifier	user.userprincipalname

22. 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	***

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.

Save
 Discard changes

Name

Namespace

Source *
 ☒ Attribute
 ☐ Transformation

Source attribute *

- 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

Namespace

Source *
 ☒ Attribute
 ☐ Transformation

Source attribute *

Claim conditions

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

^ Claim conditions

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

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 the list
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 ×

Search

- 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
- 1 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	<i>Select a User type and Source to enable the list</i>

- 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

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

25. Download the SAML Signing Certificate in Base64 format:

SAML Signing Certificate

Status

Active

Thumbprint

6C388CE18239D4D484671B21E2DCD1C28B904112

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](#)

26. 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.

i

SSO Enabled: Yes

i

Sign SSO Authentication Request: Yes

i

IdP URL

i

IdP Entity ID

i

IdP Certificate: A certificate has been uploaded

PREVIEW

i

SLO Enabled: No

i

Sign SLO Request/Response: No

i

IdP SLO URL: Not yet configured

EDIT SETTINGS

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

Settings




SSO

- ☒ Enable SSO
- ☒ Sign SSO Authentication Request
- ☐ Disable Force Authentication

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`

Set up Netskope Administrator Console

You'll need to configure the application to link with Azure AD.

Login URL	<code>https://login.microsoftonline.com/da7e068e-9a...</code>	
Azure AD Identifier	<code>https://sts.windows.net/da7e068e-9af2-4314-8...</code>	
Logout URL	<code>https://login.microsoftonline.com/common/wsf...</code>	

[View step-by-step instructions](#)

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

Settings

SSO

- ☒ Enable SSO
- ☒ Sign SSO Authentication Request

IDP URL

IDP ENTITY ID

IDP CERTIFICATE

SLO

- ☐ Enable SLO
- ☐ Sign SLO Request/Response




IDP SLO URL

CANCEL SUBMIT

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`.

Set up Netskope Administrator Console

You'll need to configure the application to link with Azure AD.

Login URL	<code>https://login.microsoftonline.com/da7e068e-9a...</code>	
Azure AD Identifier	<code>https://sts.windows.net/da7e068e-9af2-4314-8...</code>	
Logout URL	<code>https://login.microsoftonline.com/common/wsf...</code>	

[View step-by-step instructions](#)

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:

Settings

SSO

☒ Enable SSO

☒ Sign SSO Authentication Request

IDP URL

IDP ENTITY ID

IDP CERTIFICATE

SLO

☐ Enable SLO

☐ Sign SLO Request/Response

IDP SLO URL

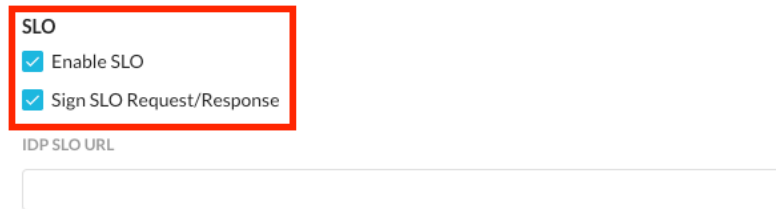
32. Open the certificate file you downloaded in Step 18 from the Azure Portal in a text editor. Copy the entire certificate string including the Begin Certificate and End Certificate lines:

```
1 -----BEGIN CERTIFICATE-----
2
3
4
5
6
7
8
9
10 -----
11
12
13
14
15 w6AopP3DRuKNmaDMszxw
16 -----END CERTIFICATE-----
```

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

The screenshot shows the 'Settings' window for SSO configuration. The 'SSO' section is active, with 'Enable SSO' and 'Sign SSO Authentication Request' checked. The 'IDP URL' and 'IDP ENTITY ID' fields are present but empty. The 'IDP CERTIFICATE' field is highlighted with a red box and contains a large black redacted area. The 'SLO' section below has 'Enable SLO' and 'Sign SLO Request/Response' unchecked, and an empty 'IDP SLO URL' field. At the bottom are 'CANCEL' and 'SUBMIT' buttons.

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

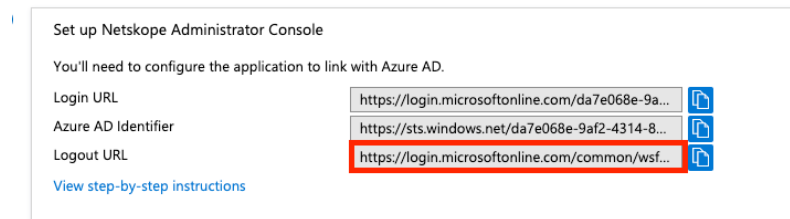


SLO

- ☒ Enable SLO
- ☒ Sign SLO Request/Response

IDP SLO URL

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>



Set up Netskope Administrator Console

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/da7e068e-9a...
Azure AD Identifier	https://sts.windows.net/da7e068e-9af2-4314-8...
Logout URL	https://login.microsoftonline.com/common/wsf...

[View step-by-step instructions](#)

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



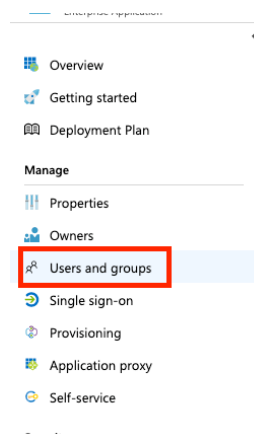
SLO

- ☒ Enable SLO
- ☒ Sign SLO Request/Response

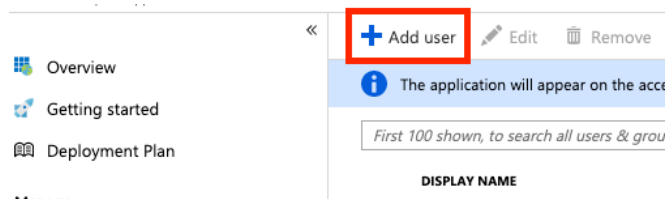
IDP SLO URL

37. Click Submit.

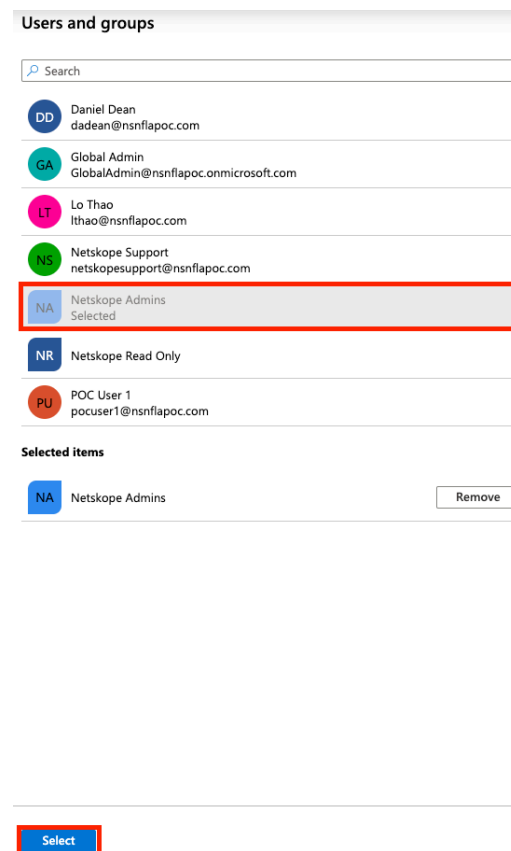
38. Navigate back to the Netskope Administrator Console Overview and select Users and groups:



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.”

Select Role

Enter role name to filter items...

Tenant Admin

User

Selected Role

User

Select

43. 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.