

NETOP REMOTE CONTROL AZURE AD AND ADFS INTEGRATION



NETOP[®]

RemoteControl

Secure Remote Management and Support

April 28th, 2021

Contents

Configure the authentication provider.....	3
Azure AD.....	3
Create the enterprise application in Azure AD.....	3
A. Creating the Netop Portal application Azure AD from the Application gallery.....	3
Add users and groups to the application.....	7
Configure single sign-on.....	9
Configure the application permissions.....	17
Configure Certificates & secrets.....	21
B. Creating the Netop Portal application Azure AD as a Non-gallery application.....	24
Add users and groups to the application.....	27
Configure single sign-on.....	29
Configure the application permissions.....	35
Configure certificates & secrets.....	39
Configure Azure AD in the Netop Portal.....	42
ADFS integration with the Netop Portal.....	47
Add Netop Portal as a Trusted Relying Party.....	47
Add Claim Rules for the Netop Portal Relying Party.....	55
Configure the Netop Portal.....	67
Remote session using ADFS.....	68
Managing the ADFS users.....	69

Configure the authentication provider

Azure AD

Create the enterprise application in Azure AD

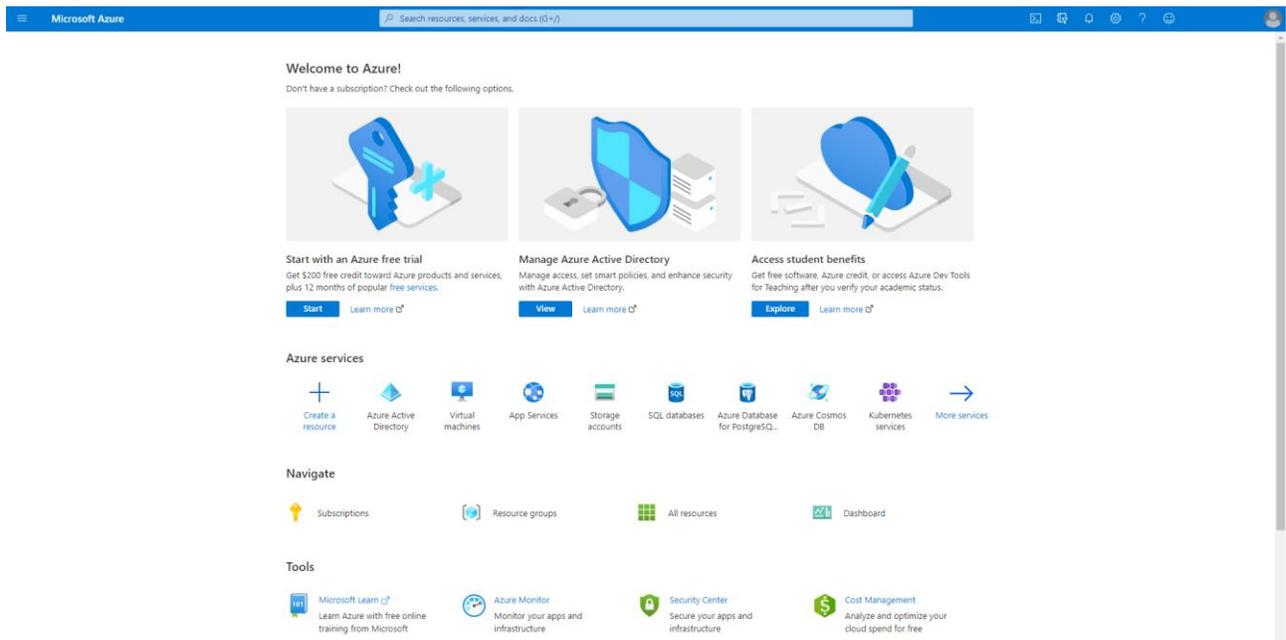
There are two methods of creating the enterprise application in Azure AD:

- A. You can add the **Netop Portal** application from the Application gallery in the Enterprise applications section. Refer to the following [link](#) for additional information on how you can add and configure the application from the application gallery.
- B. You can create the **Netop Portal** application from the Non-gallery application section

A. Creating the Netop Portal application Azure AD from the Application gallery

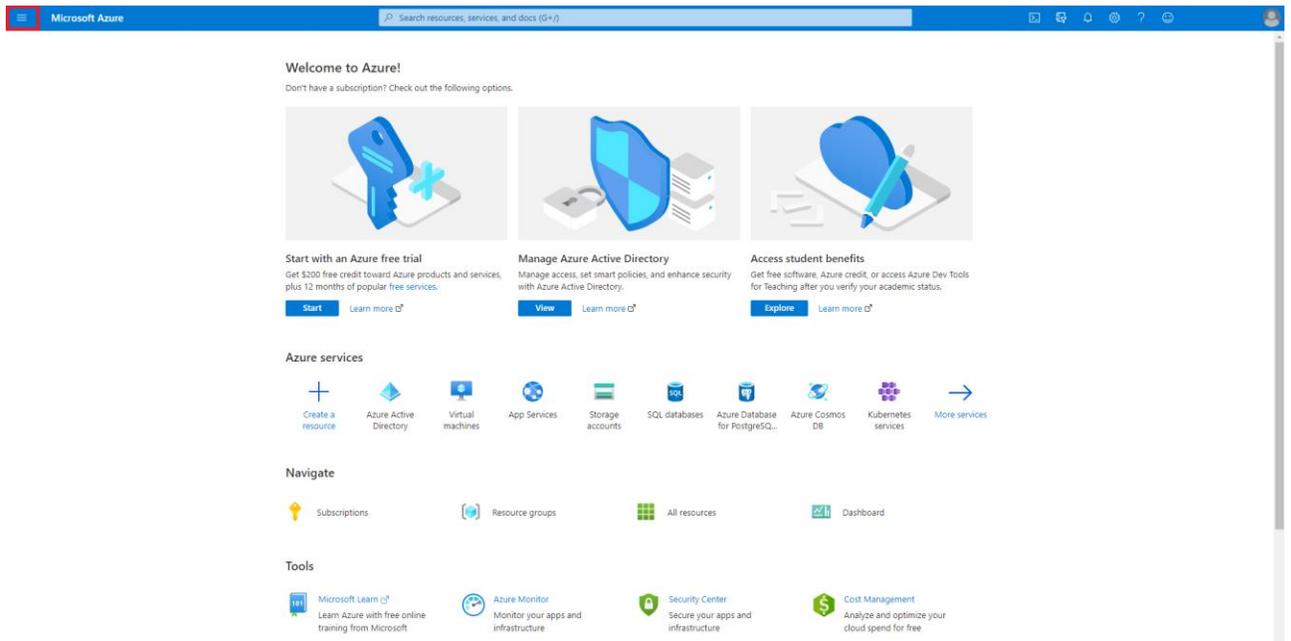
To create the **Netop Portal** application in **Azure AD**, proceed as follows:

1. Log in the [Azure Portal](#).

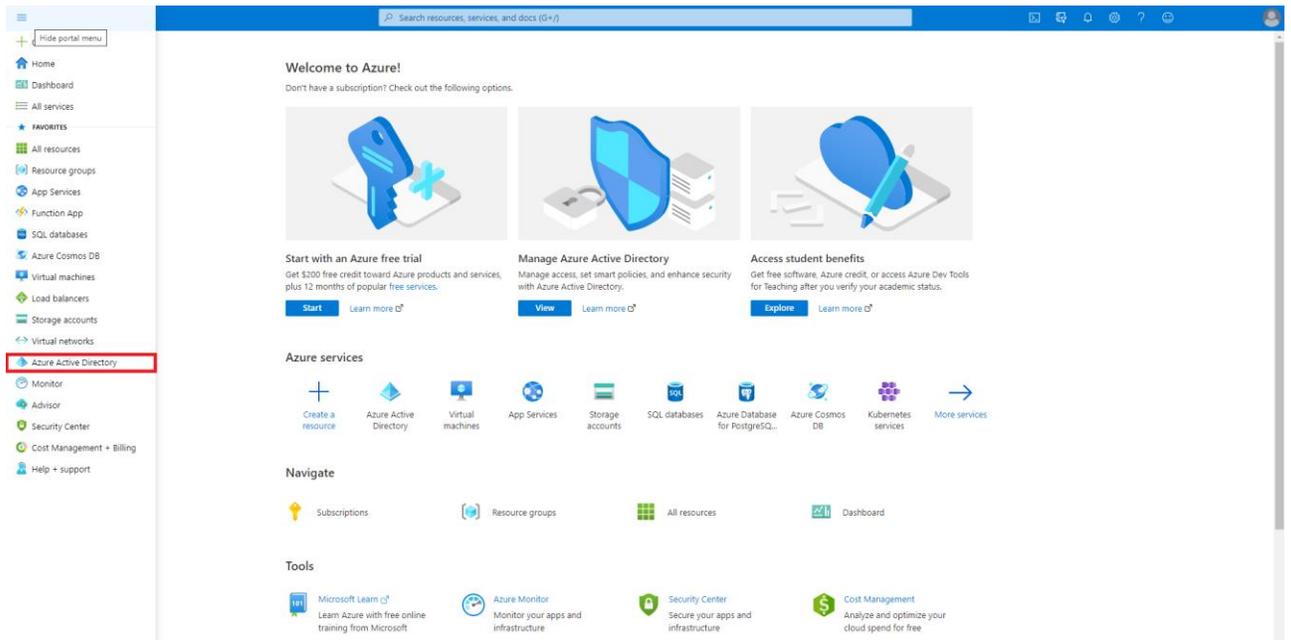


2. Go to **Azure Active Directory**.

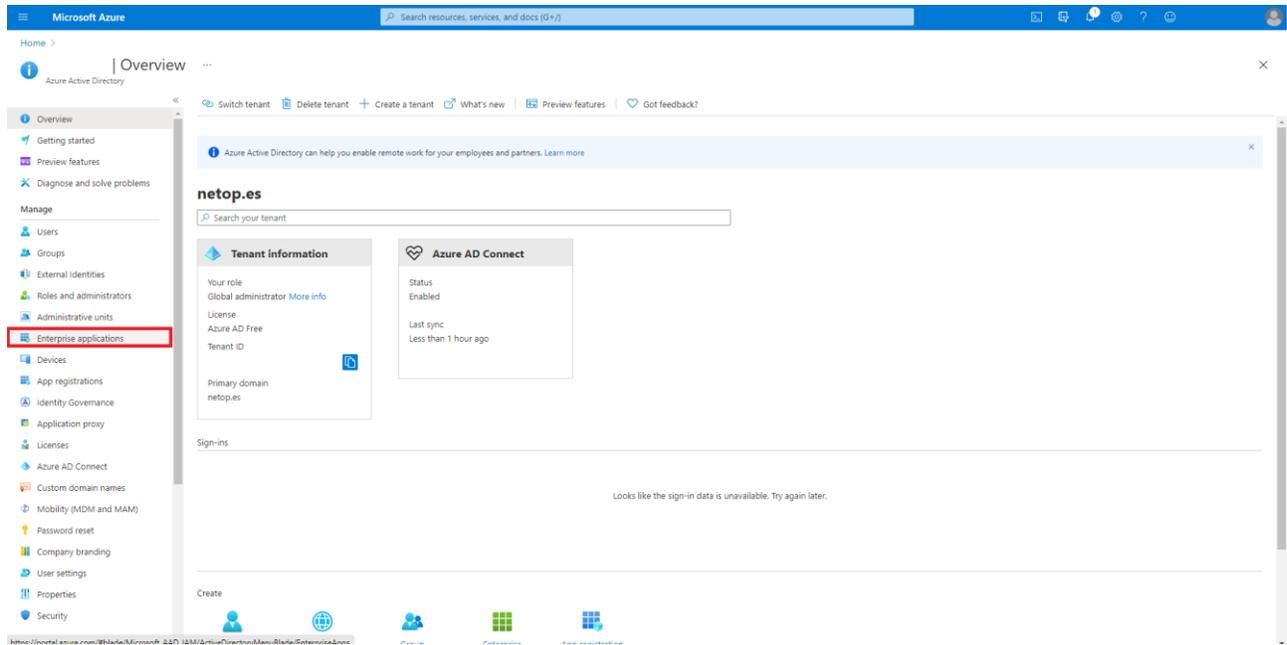
2.1. Click on the **More** button.



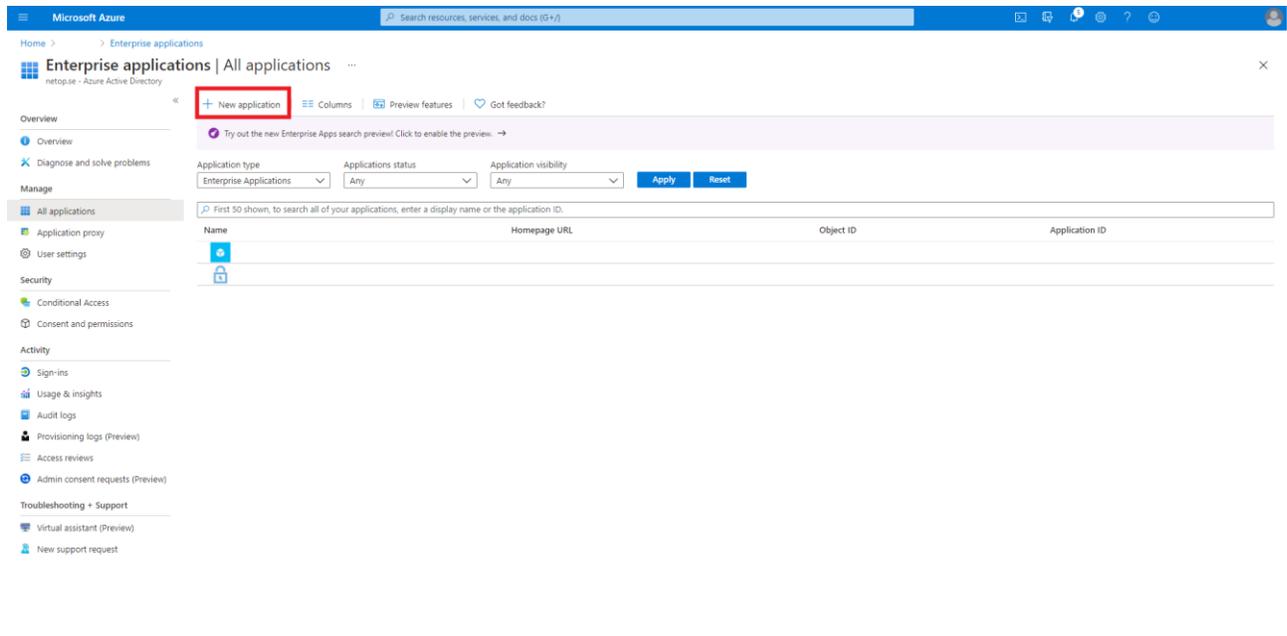
2.2. Click on **Azure Active Directory**.



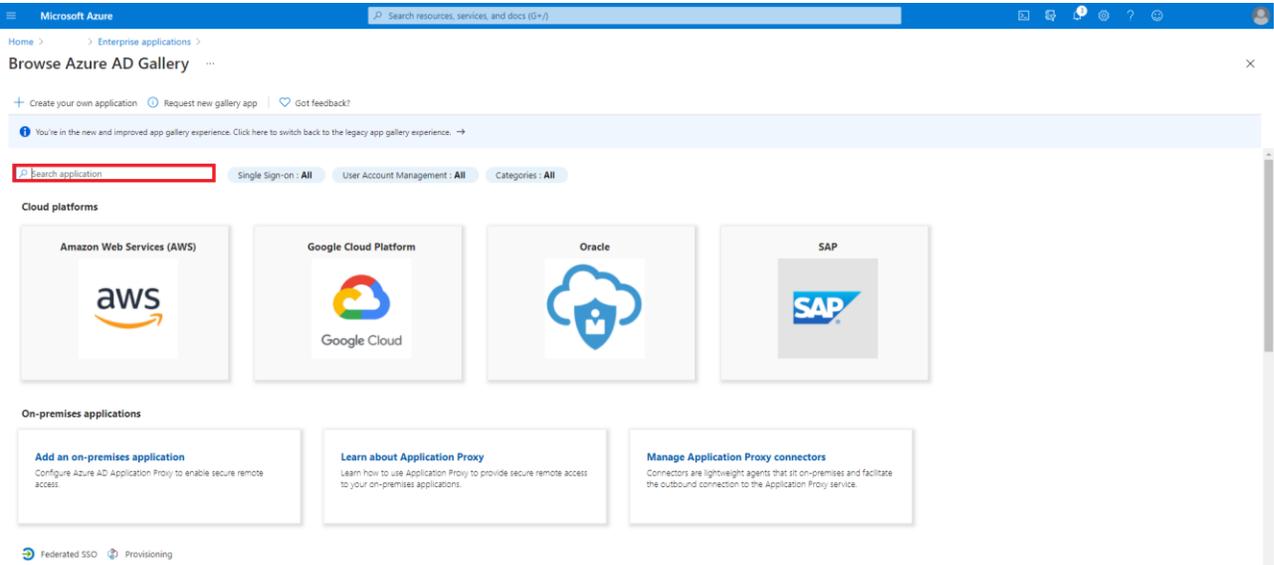
3. Go to Enterprise applications.



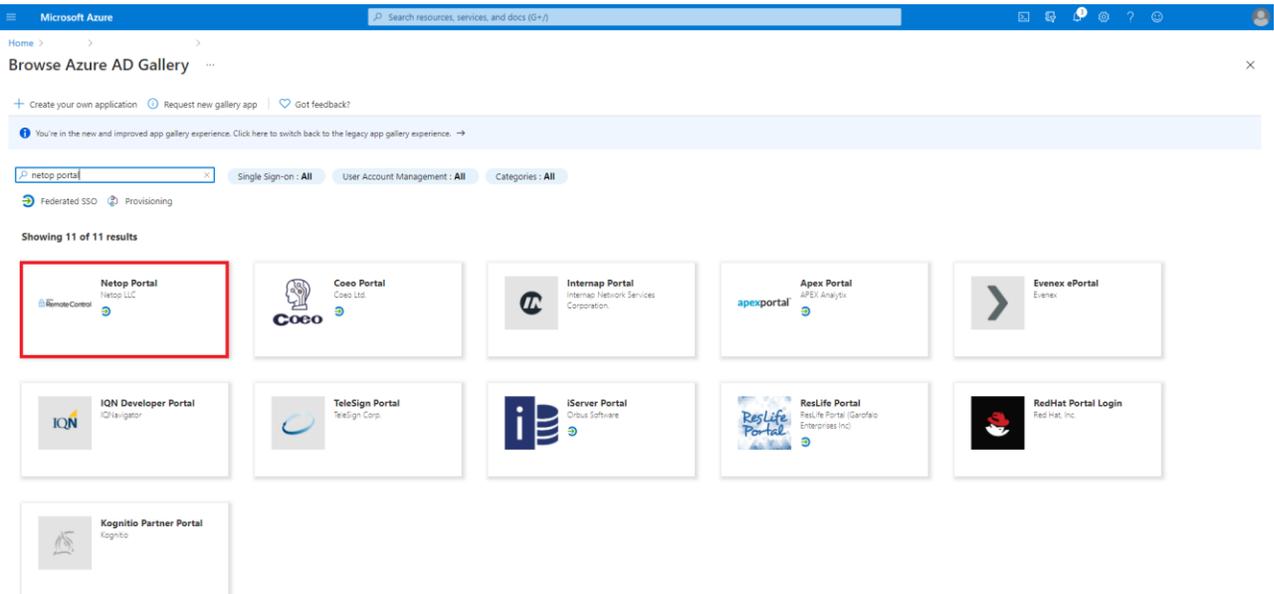
4. Click on the New application button.



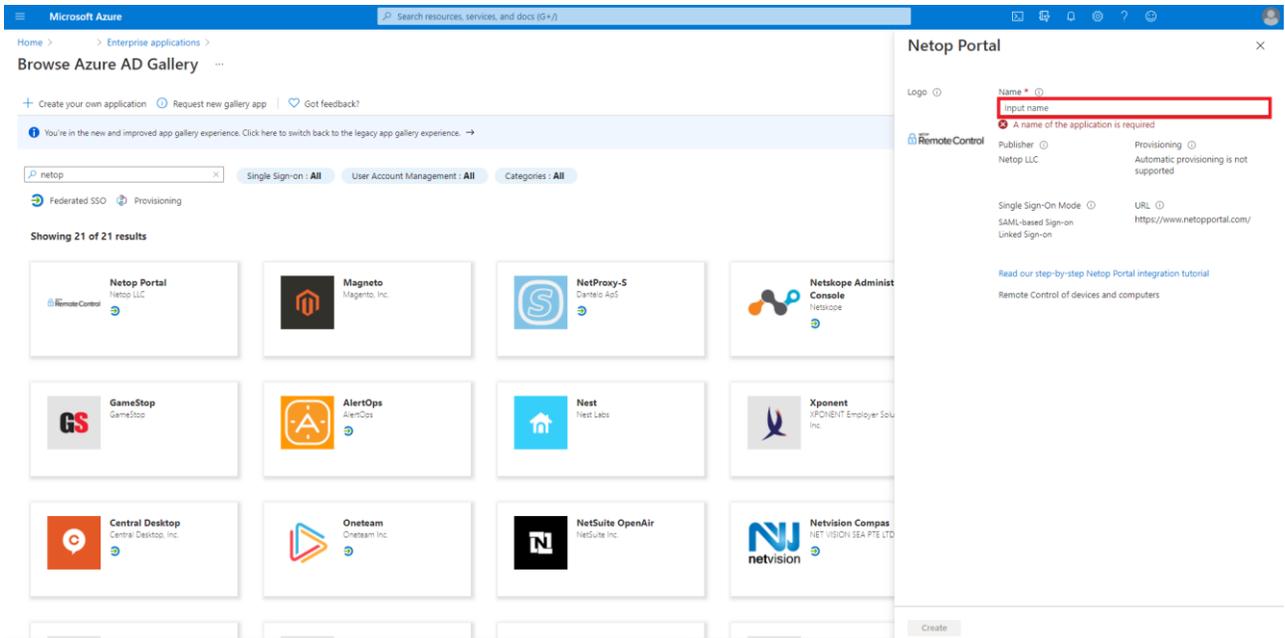
5. In the **Search application** entry field, specify **Netop Portal**.



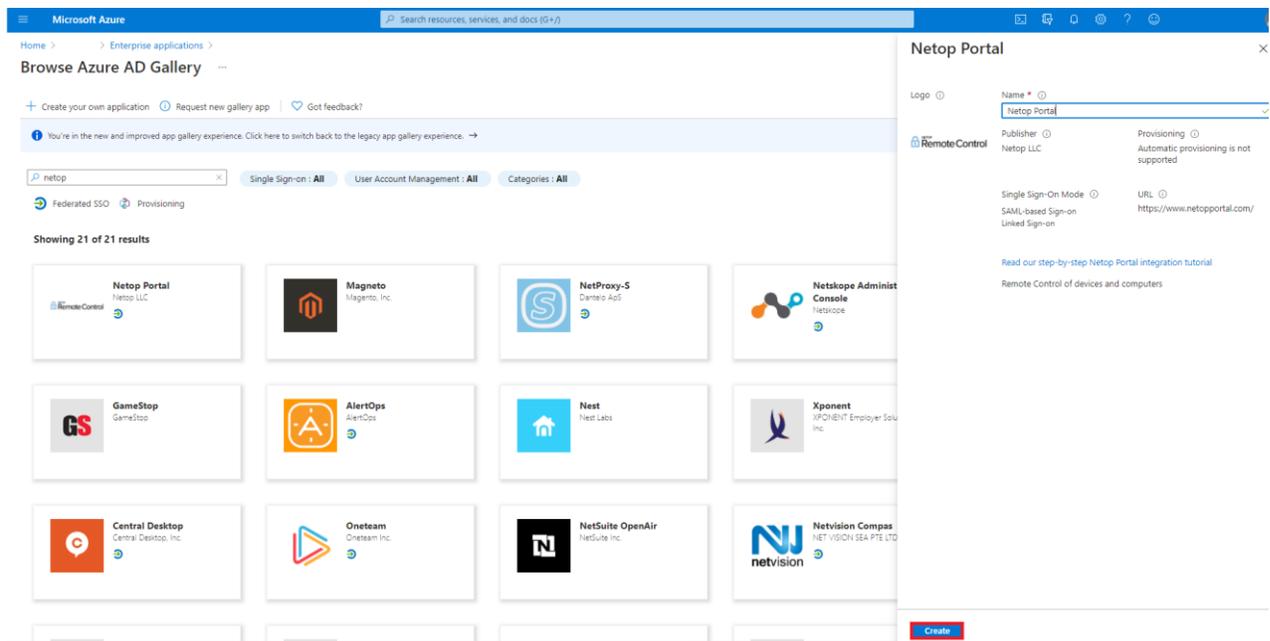
6. Click on the **Netop Portal** icon.



7. If necessary, you can specify a different application name than **Netop Portal** in the **Name entry** field.



8. Click on the **Create** button to finish adding the **Netop Portal** application to the **Azure Portal**.



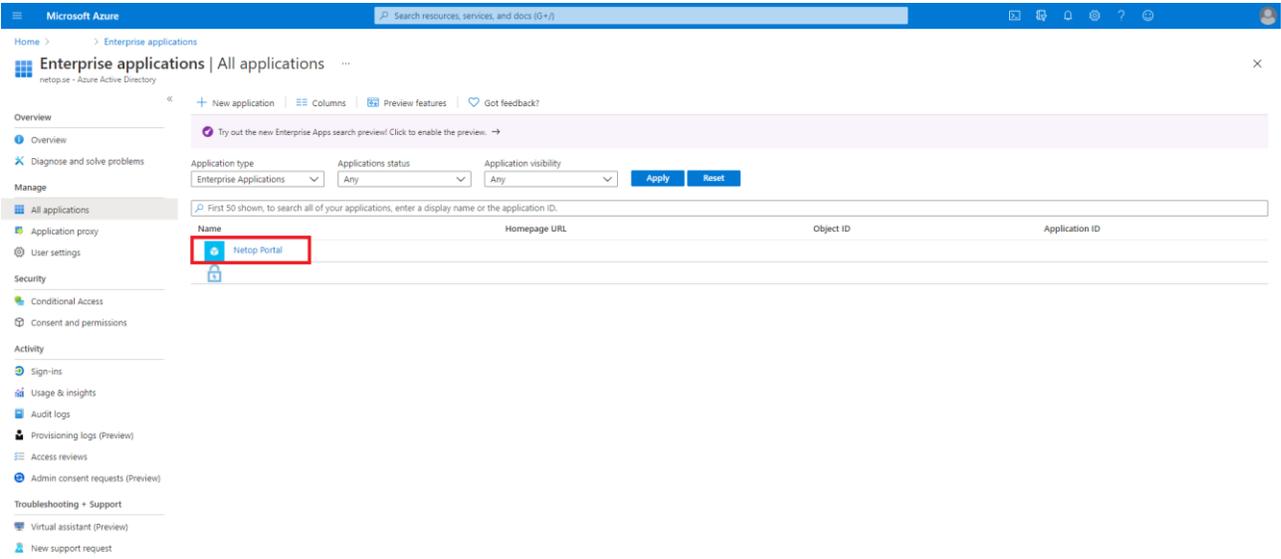
The application is created successfully and added to the **Enterprise applications** section.

Add users and groups to the application

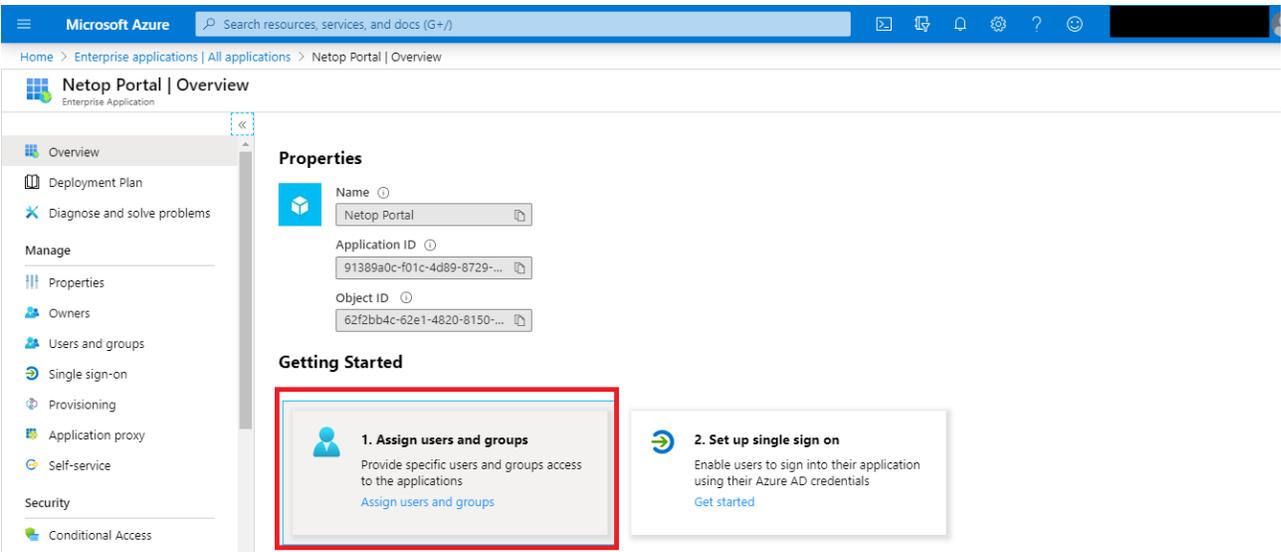
To add users and groups to the application, proceed as follows:

1. Go to **Azure Active Directory**.
2. Go to **Enterprise applications**.

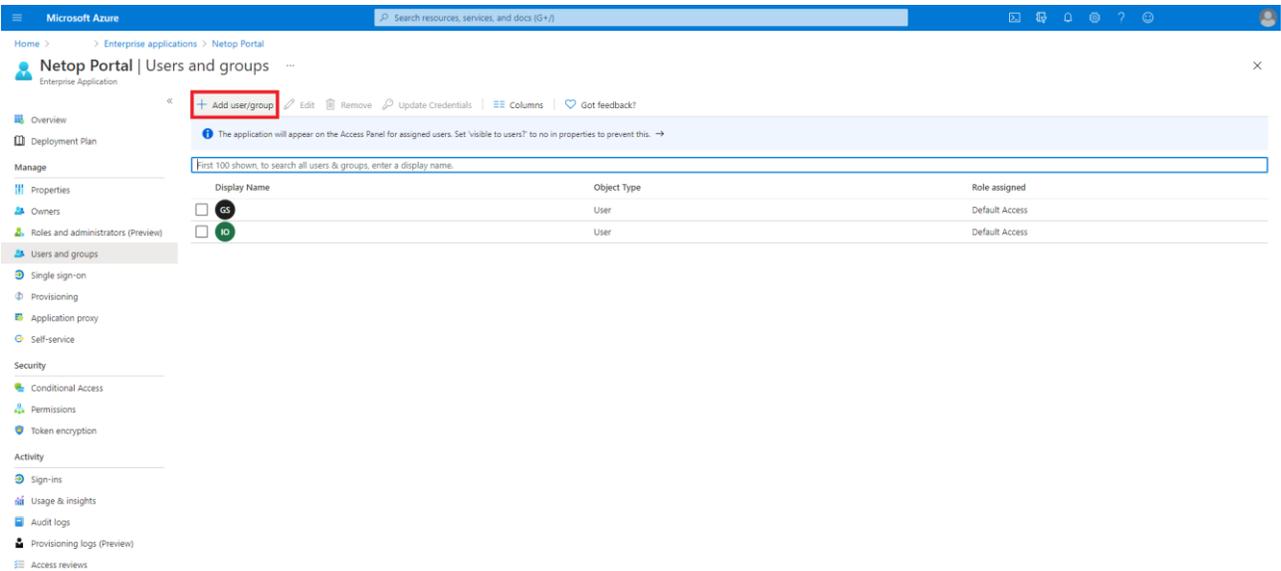
3. Click on the newly created **Netop Portal** application.



4. Click on **Assign users and groups**.

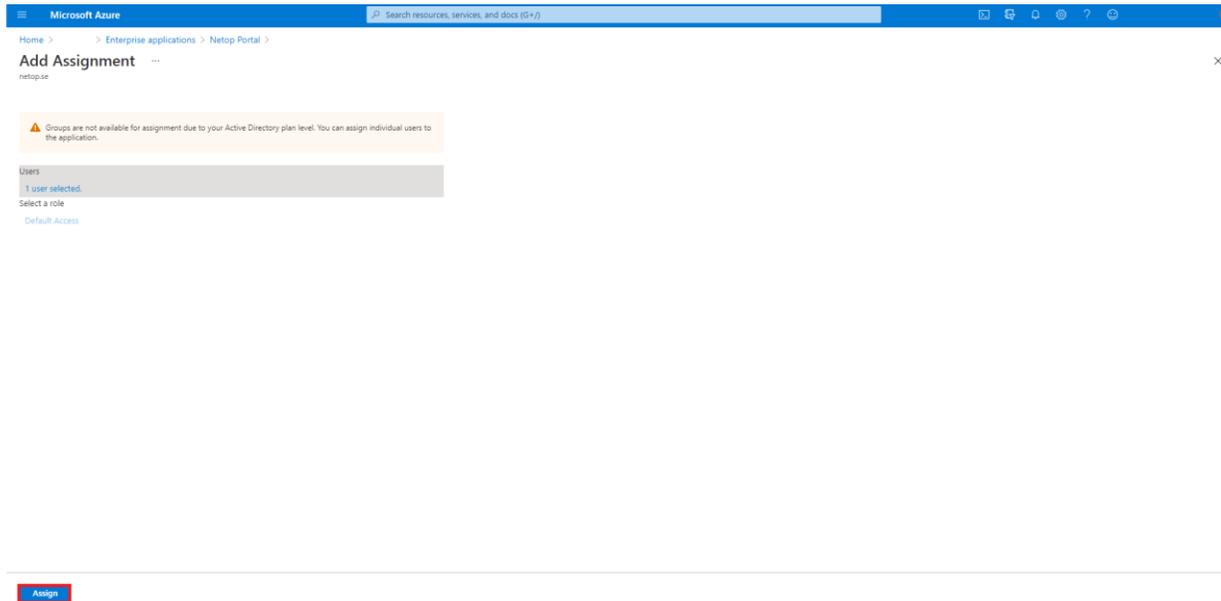


5. Click on the **Add User/group** button to add the allowed users or groups.



NOTE: Make sure that the users that you add are from the **Windows Server AD**.

6. After you finish adding the users and groups, click on the **Assign** button.

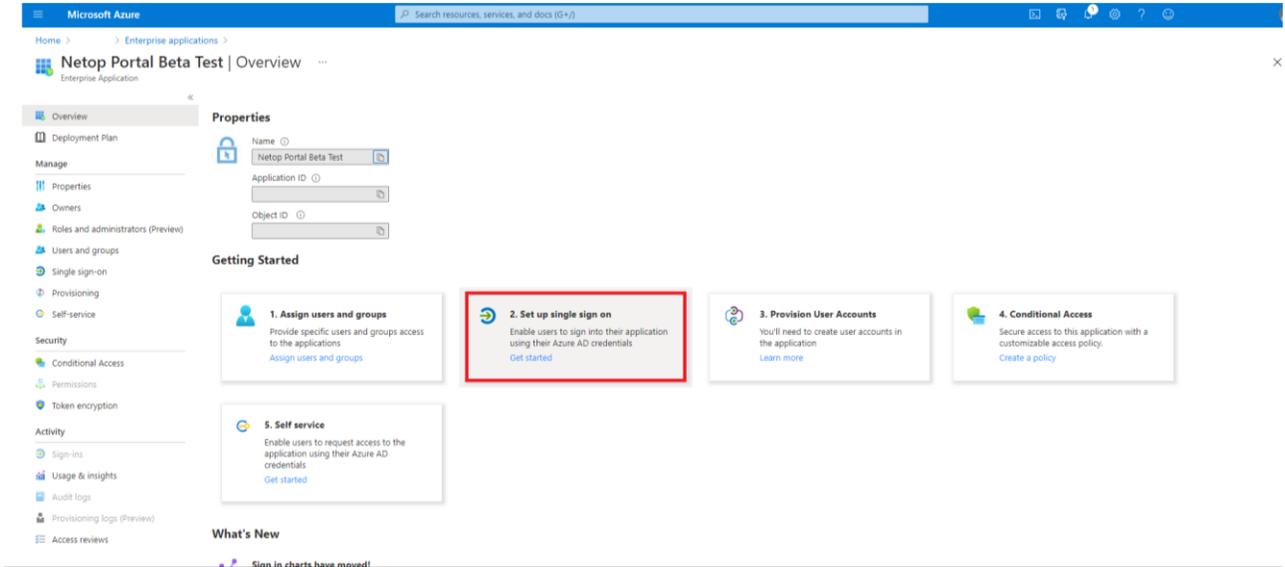


Configure single sign-on

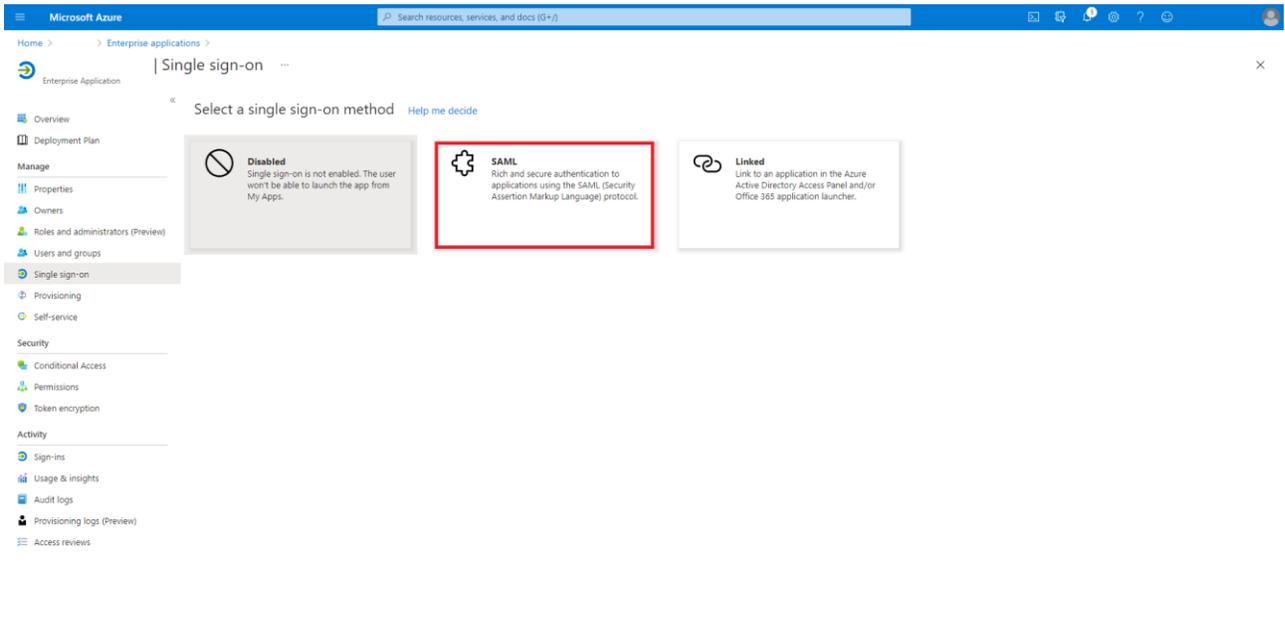
To configure the single sign-on, proceed as follows:

1. Go to **Azure Active Directory**.
2. Go to **Enterprise applications**.
3. Click on the newly created **Netop Portal** application.

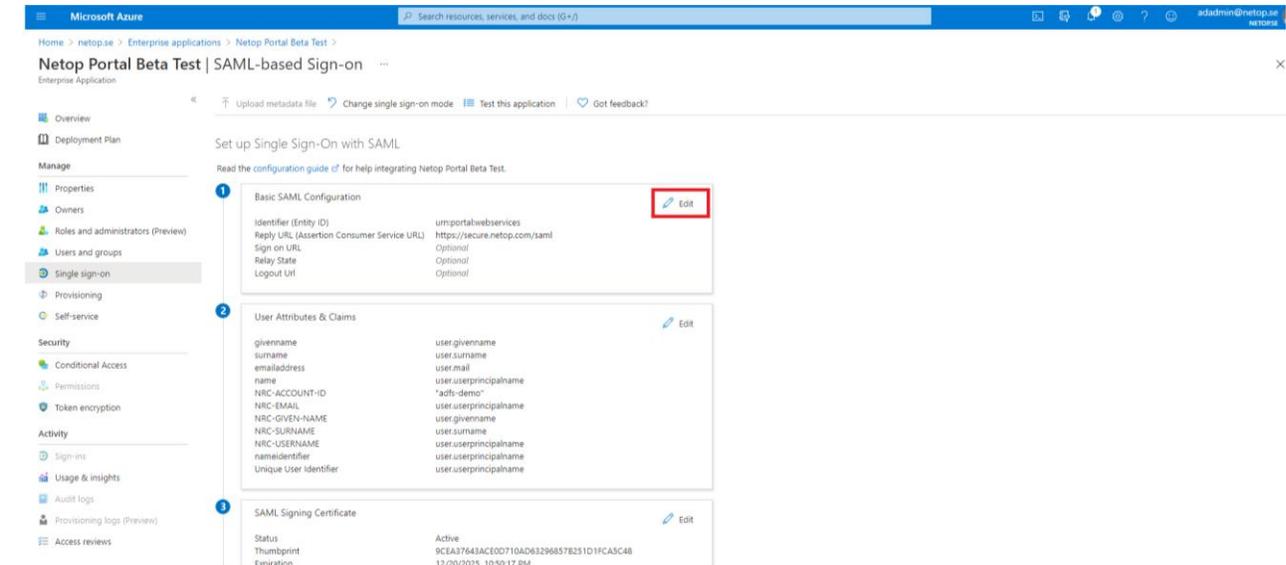
4. Click on **Set up single sign-on.**



5. Click on **SAML.**



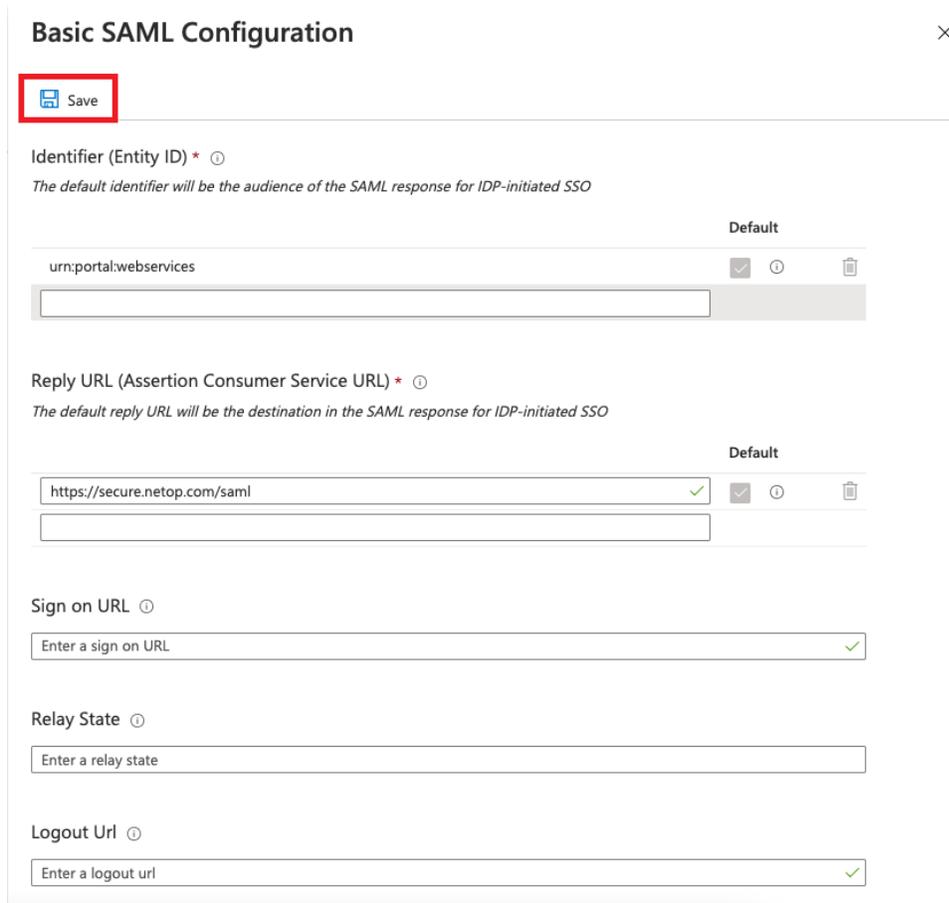
6. In the **Basic SAML Configuration** group, click on the **Edit** button.



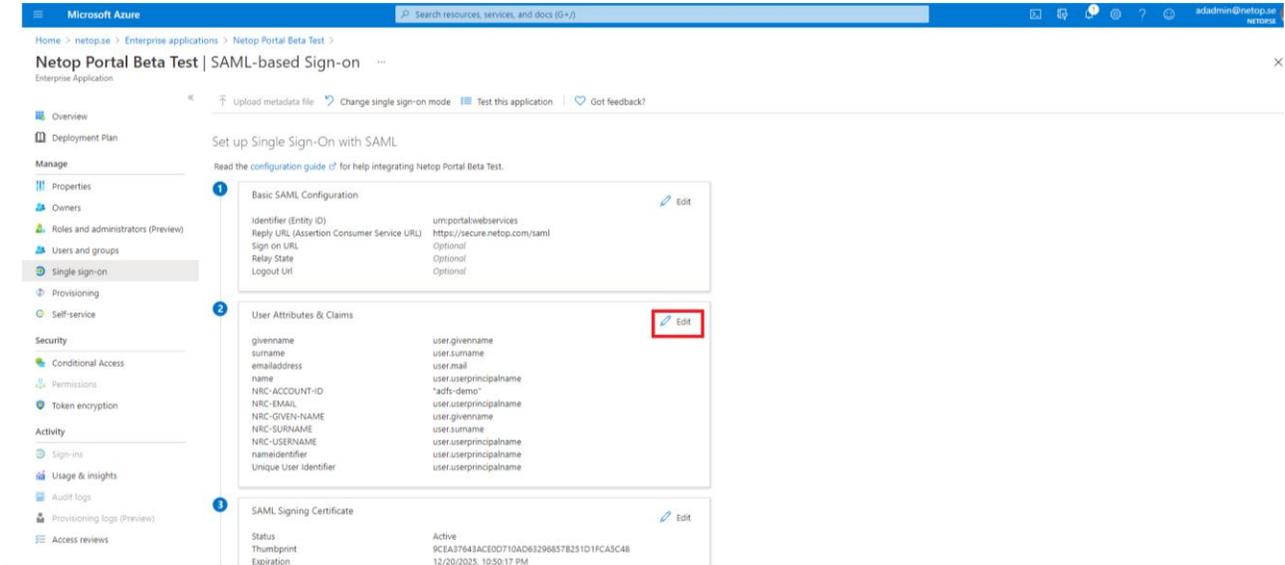
7. Verify the following settings:

Field name	Value
Identifier (Entity ID)	urn:portal:webservicess
Reply URL	https://secure.netop.com/saml

8. Click on the **Save** button to save your changes.



9. In the **User Attributes & Claims** group, click on the **Edit** button.



10. Verify the following claims:

Name	Namespace	Source	Source attribute
NRC-ACCOUNT-ID	https://secure.netop.com	Attribute	This is the domain identifier that you both specify here and in the Netop Portal ADFS/Azure AD configuration.
NRC-USERNAME	https://secure.netop.com	Attribute	user.userprincipalname
NRC-GIVEN-NAME	https://secure.netop.com	Attribute	user.givenname
NRC-SURNAME	https://secure.netop.com	Attribute	user.surname
NRC-EMAIL	https://secure.netop.com	Attribute	user.mail

NOTE: When adding the **Netop Portal** application from the Azure AD Browse Application gallery section, the above claims are created automatically. The default attributed value to the NRC-ACCOUNT-ID user is set to “ads-demo”. Modify this value as per your requirements.

The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**:

11. Click on the **Add a group claim** button to add the following Group claim:

Microsoft Azure

Home > Enterprise applications > SAML-based Sign-on > User Attributes & Claims

+ Add new claim + **Add a group claim** Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname (nameid-for... ***
https://secure.netop.com/NRC-EMAIL	user.userprincipalname ***
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname ***
https://secure.netop.com/NRC-SURNAME	user.surname ***
https://secure.netop.com/NRC-USERNAME	user.userprincipalname ***
nameidentifier	user.userprincipalname ***
https://secure.netop.com/NRC-ACCOUNT-ID	"netportal" ***

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 ***

11.1. Select the **All groups** option from the Which groups associated with the user should be returned in the claim section.

Microsoft Azure

Home > SAML-based Sign-on > User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname (nameid-for... ***
https://secure.netop.com/NRC-EMAIL	user.userprincipalname ***
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname ***
https://secure.netop.com/NRC-SURNAME	user.surname ***
https://secure.netop.com/NRC-USERNAME	user.userprincipalname ***
nameidentifier	user.userprincipalname ***
https://secure.netop.com/NRC-ACCOUNT-ID	"netop" ***

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 ***

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

None

All groups

Security groups

Directory roles

Groups assigned to the application

Source attribute *

Group ID

Advanced options

Customize the name of the group claim

Name (required)

Namespace (optional)

Emit groups as role claims

Save

- 11.2. Click on the **Customize the name of the group claim.**
- 11.3. Specify the required name and namespace of the claim:
- Name: **NRC-GROUPS**
 - Namespace: **https://secure.netop.com**

Microsoft Azure

Home > > SAML-based Sign-on >

User Attributes & Claims ...

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname (nameid-for-... ***
https://secure.netop.com/NRC-EMAIL	user.userprincipalname ***
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname ***
https://secure.netop.com/NRC-SURNAME	user.surname ***
https://secure.netop.com/NRC-USERNAME	user.userprincipalname ***
nameidentifier	user.userprincipalname ***
https://secure.netop.com/NRC-ACCOUNT-ID	*netop* ***

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 ***

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

None

All groups

Security groups

Directory roles

Groups assigned to the application

Source attribute *

Group ID

Advanced options

Customize the name of the group claim

Name (required)

Namespace (optional)

Emit groups as role claims

Save

12. Click on the **Save** button to save your changes.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'User Attributes & Claims' section is visible, displaying a table of required and additional claims. On the right, the 'Group Claims' configuration panel is open, showing options for which groups to return in the claim and advanced options for customizing the claim name and namespace. A 'Save' button is visible at the bottom right of the configuration panel.

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...]
https://secure.netop.com/NRC-EMAIL	user.userprincipalname
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname
https://secure.netop.com/NRC-SURNAME	user.surname
https://secure.netop.com/NRC-USERNAME	user.userprincipalname
nameidentifier	user.userprincipalname
https://secure.netop.com/NRC-ACCOUNT-ID	"netop"

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

NOTE: Make sure that you save the following information:

- The **Federation Metadata XML** file

The screenshot shows the 'SAML Signing Certificate' configuration page. It displays the status as 'Active' and provides details for the thumbprint, expiration date, and notification email. The 'App Federation Metadata Url' is highlighted with a red box. Below the URL, there are three 'Download' links: 'Certificate (Base64)', 'Certificate (Raw)', and 'Federation Metadata XML', with the last one also highlighted with a red box.

- The **Login URL**

The screenshot shows the 'Set up Netop Portal' configuration page. It instructs the user to configure the application to link with Azure AD. The 'Login URL' field is highlighted with a red box, and its value is also highlighted with a red box. Other fields include 'Azure AD Identifier' and 'Logout URL', each with a copy icon to its right. A link for 'View step-by-step instructions' is also visible.

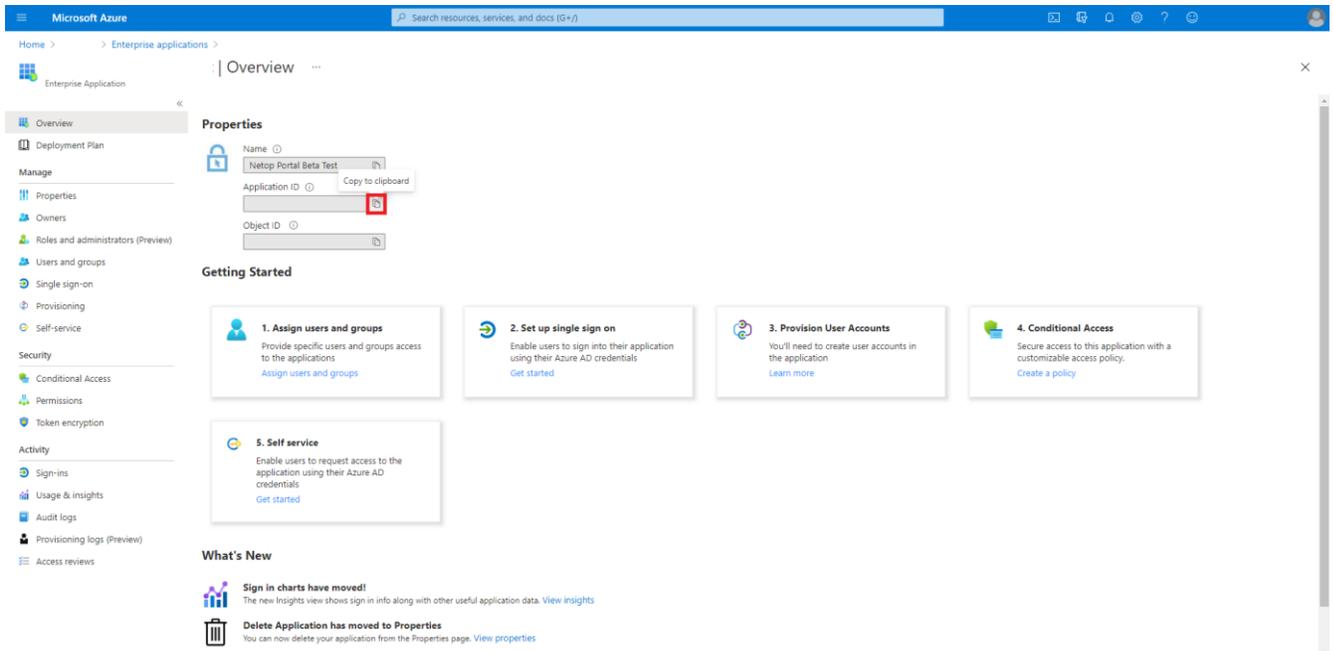
If you plan on using the Azure AD groups then it is necessary that you also save the **Application ID**

- **Application ID**

To retrieve the Application ID value from the Azure Portal, proceed as follows:

- 1.1. Go to the **Azure Portal**.
- 1.2. Go to **Windows Active Directory**.

- 1.3. Go to **Enterprise Applications**.
- 1.4. Select the Netop Portal application.
- 1.5. Go to **Overview**.
- 1.6. Click on the **Copy to clipboard** button.

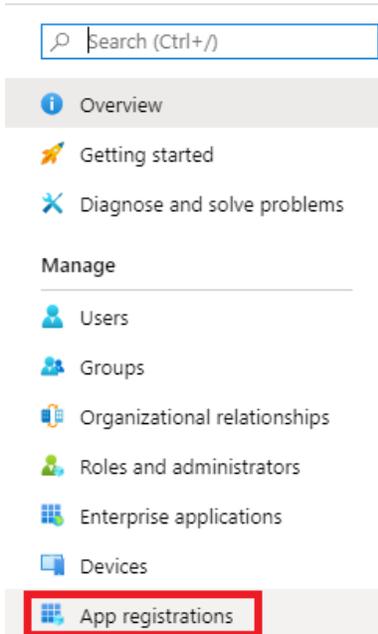


Configure the application permissions

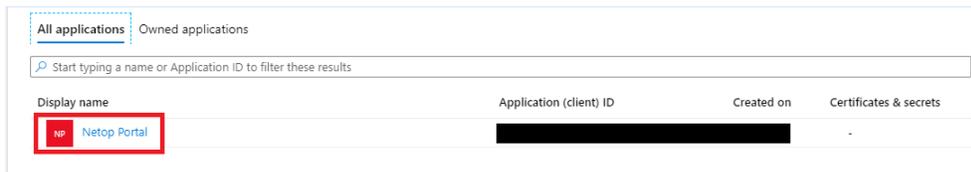
The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**.

To configure the application permissions, proceed as follows:

1. Go to **Azure Active Directory**.
2. Go to **App registrations**.



3. Click on the **Netop Portal** application.



4. Click on the **View API permissions** button.

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API permissions

Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps

View all quickstart guides

5. Click on the **Add a permission** button to add the necessary permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for home

Add a permission

API / Permissions name	Type	Description	Admin consent req...	Status
No permissions added				

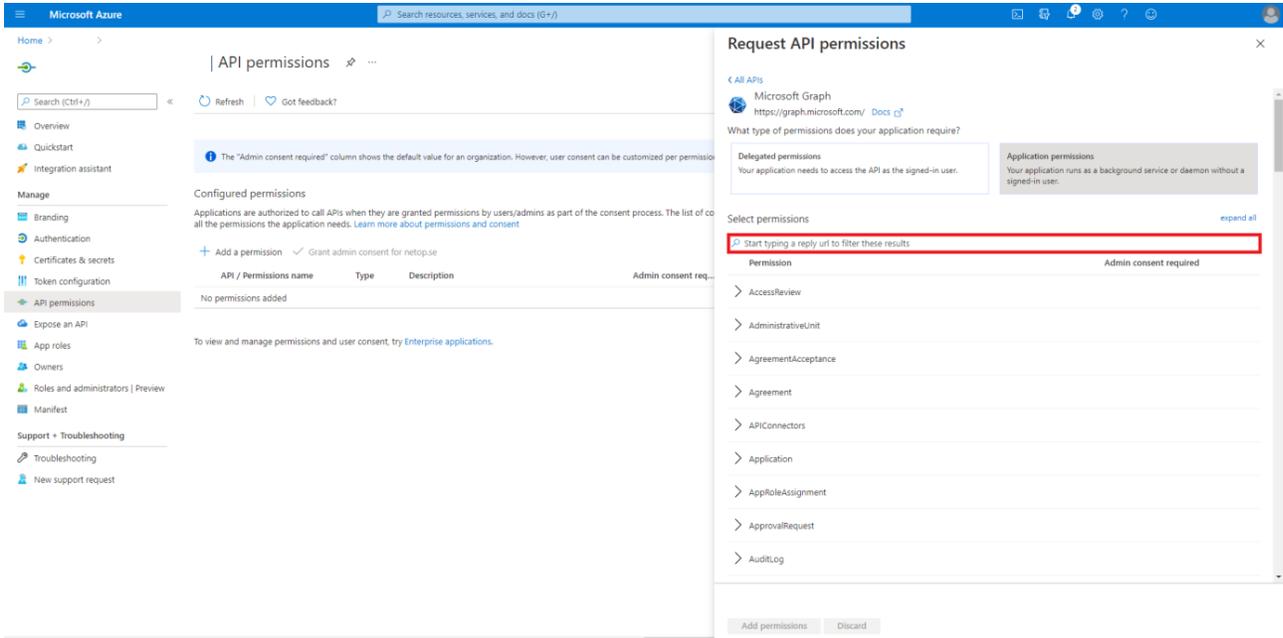
6. Click on Microsoft Graph.

The screenshot shows the Microsoft Azure portal interface. On the left is a navigation pane with categories like Overview, Manage, and Support. The main area displays 'API permissions' with a table of configured permissions (currently empty). A 'Request API permissions' dialog box is open on the right. It has tabs for 'Microsoft APIs', 'APIs my organization uses', and 'My APIs'. Under 'Commonly used Microsoft APIs', the 'Microsoft Graph' API is highlighted with an orange border. Below it are other APIs like Azure Service Management and Office 365 Management APIs. Further down are 'More Microsoft APIs' including Azure Batch, Azure Data Catalog, Azure Data Explorer, Azure Data Explorer (with Multifactor Authentication), Azure Data Lake, Azure DevOps, Azure Import/Export, Azure Key Vault, and Azure Maps.

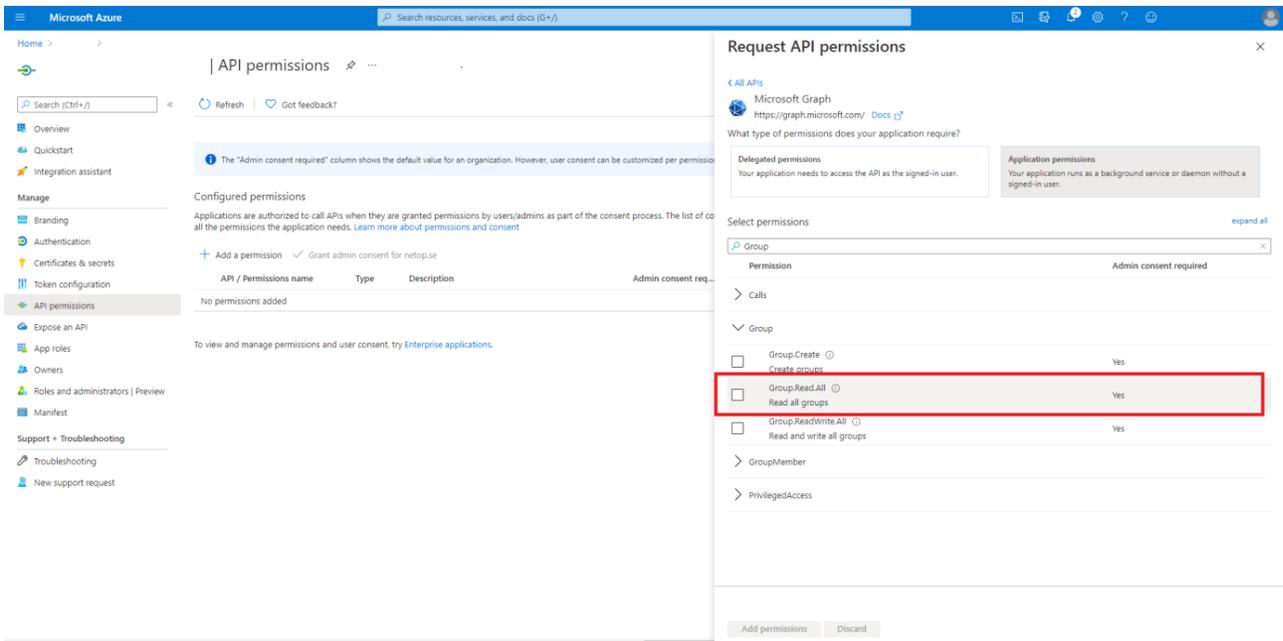
7. Click on Application permissions.

This screenshot shows the same Microsoft Azure portal interface as the previous one, but the 'Request API permissions' dialog box is now showing the 'All APIs' tab. It lists 'Microsoft Graph' with its URL and a 'Docs' link. Below this, it asks 'What type of permissions does your application require?' and offers two options: 'Delegated permissions' (highlighted with a light blue background) and 'Application permissions' (highlighted with a red border). The 'Application permissions' option includes the text: 'Your application runs as a background service or daemon without a signed-in user.' At the bottom of the dialog, there are 'Add permissions' and 'Discard' buttons.

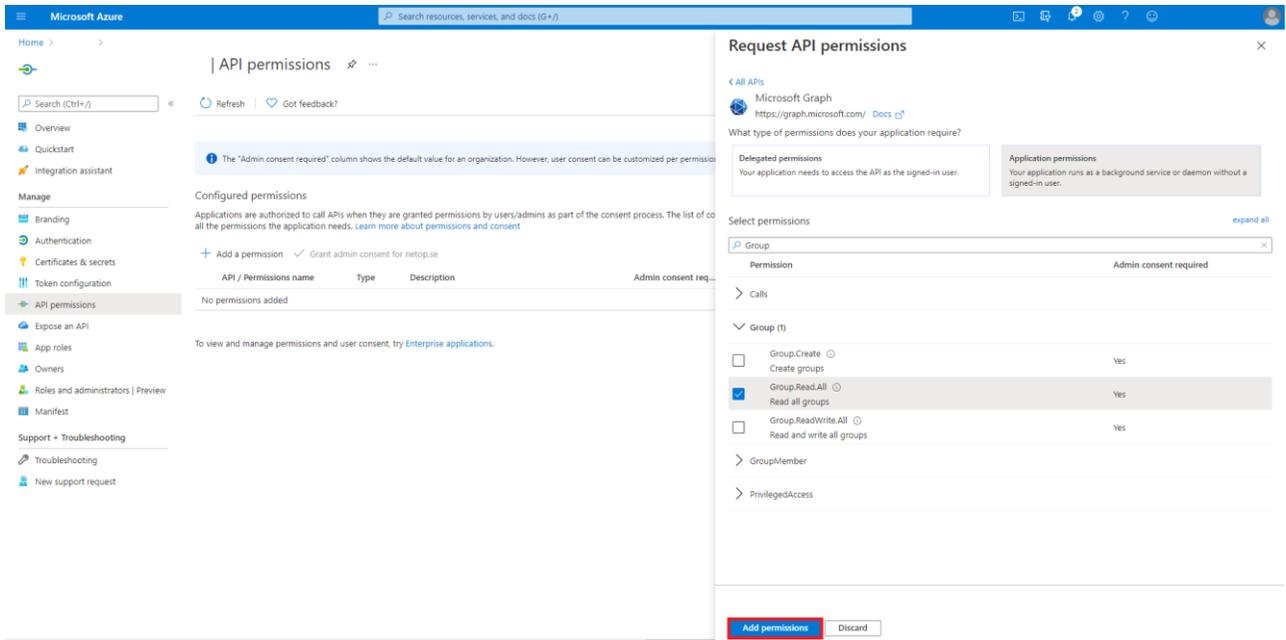
8. Search for Group in the **Start typing a reply url to filter these results** search field.



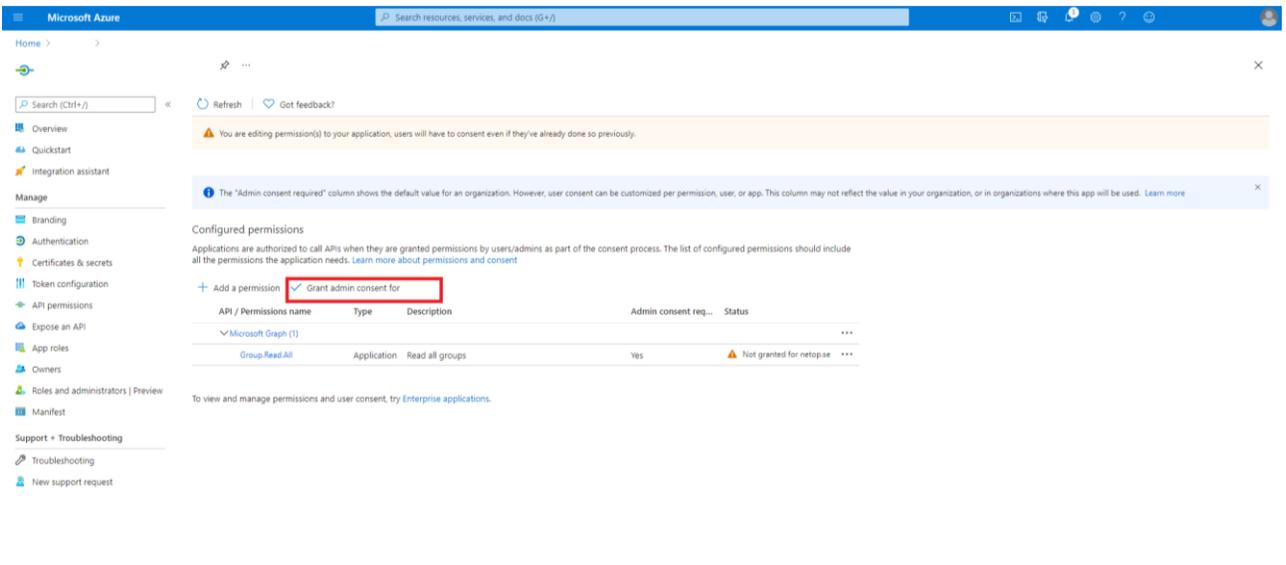
9. Click on the **Group.Read.All** option.



10. Click on the **Add permissions** button to add your permission.



11. Click on the **Grant admin consent for ...** button to grant admin consent for the API permission.



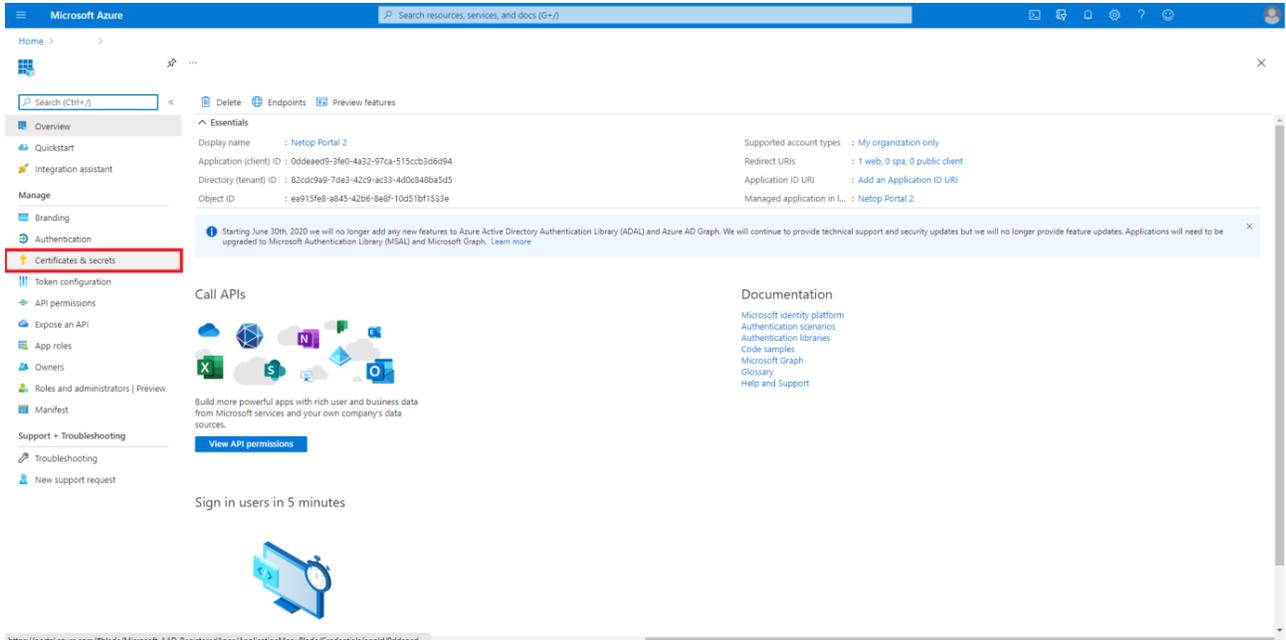
Configure Certificates & secrets

The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**.

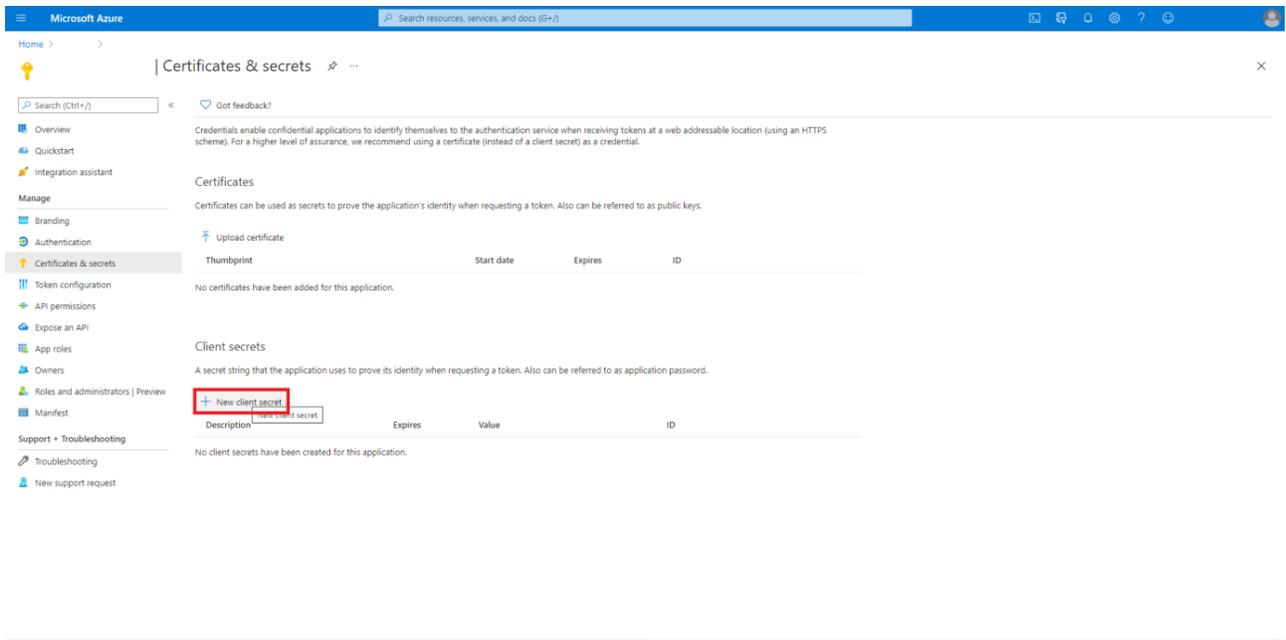
To configure the **Certificates & secrets** for the **Netop Portal** application in the **Azure Portal**, proceed as follows:

1. Go to **Azure Active Directory**.
2. Go to **App registrations**.
3. Click on the **Netop Portal** application.

4. Go to **Certificates & secrets**.



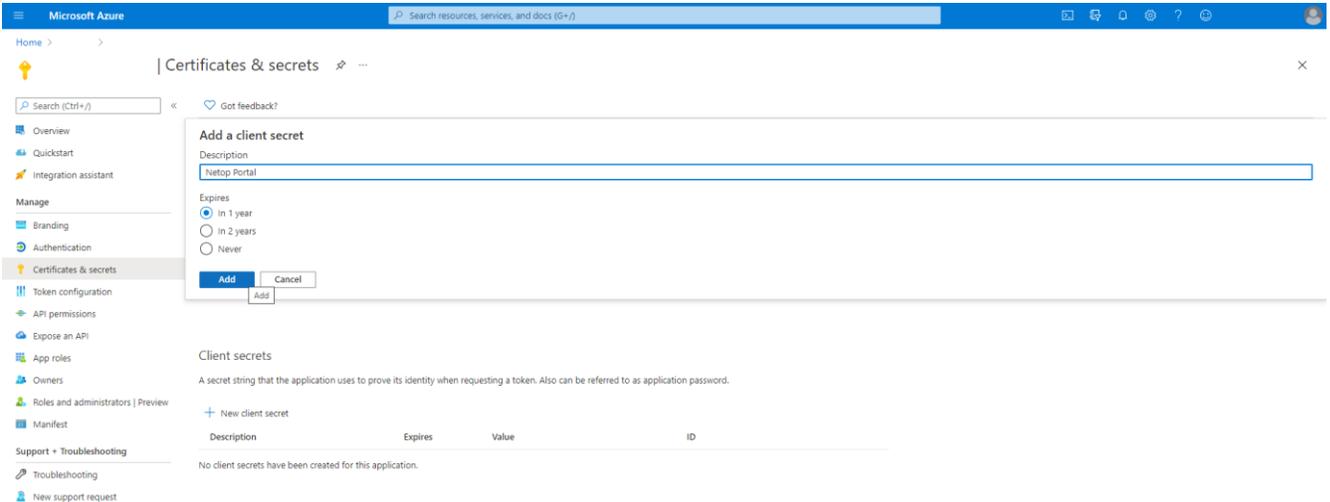
5. Click on the **New client secret** button.



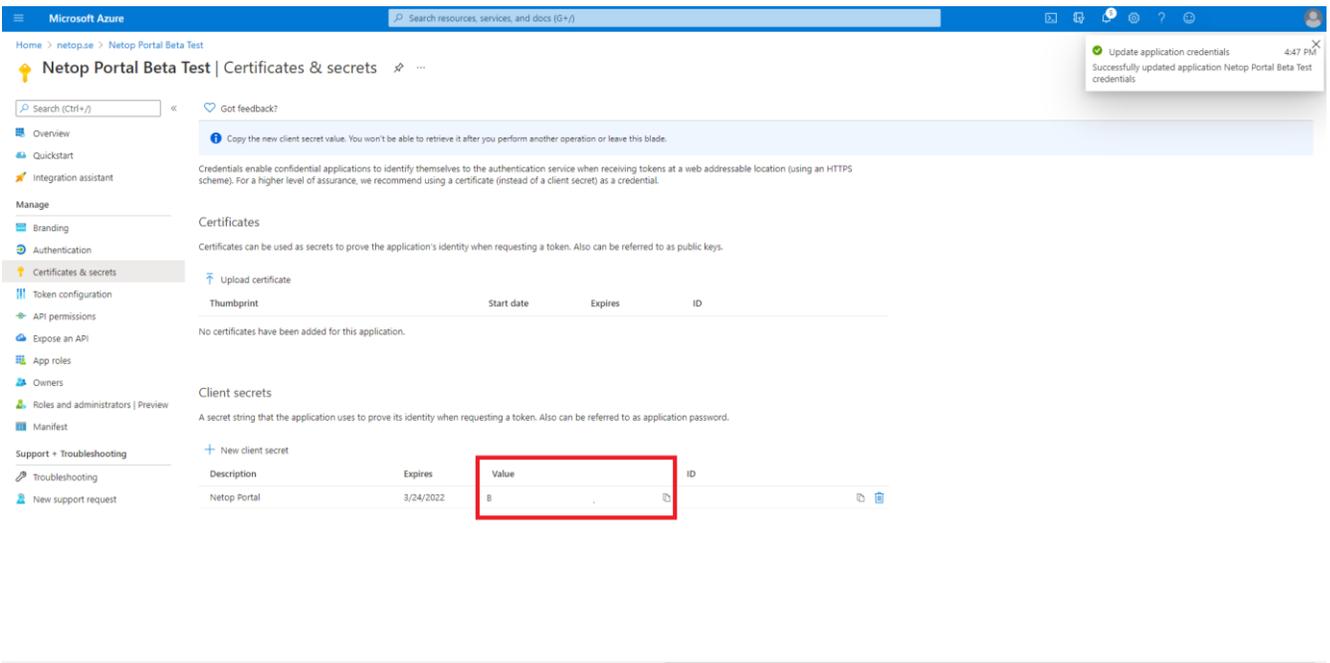
6. Specify a name for the client secret in the **Description** entry field.

7. Specify an expiry date for the client secret accordingly to your needs.

8. Click on the **Add** button.



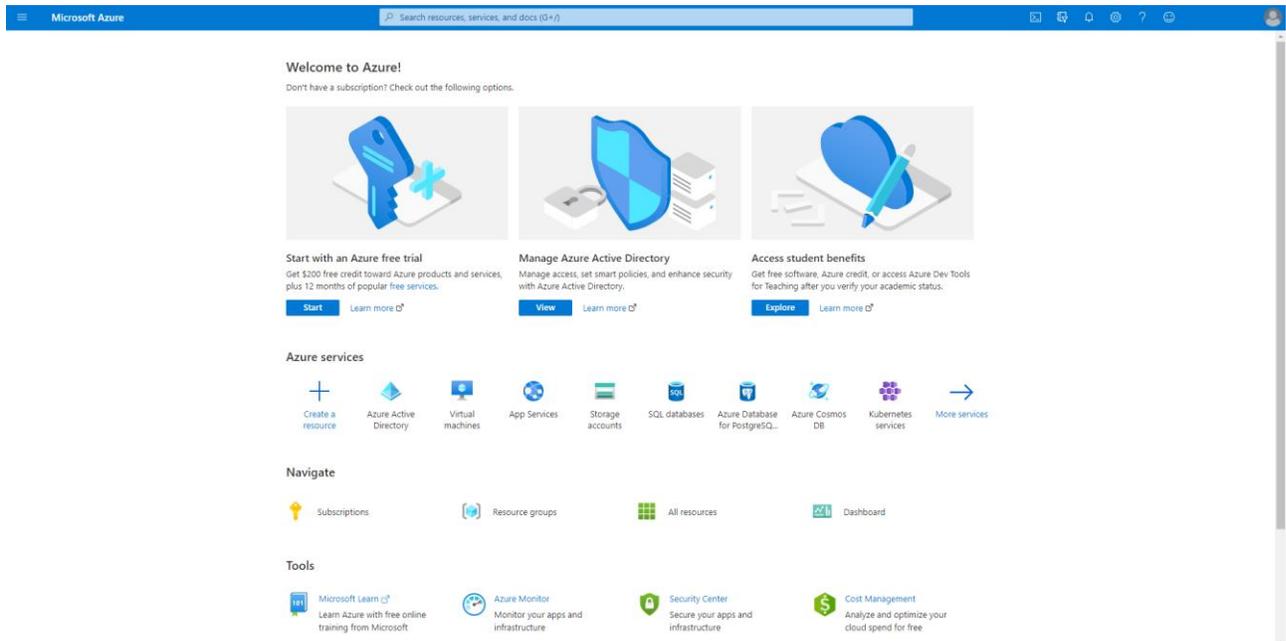
9. Save the client secret value in a text editor or copy it to the clipboard. It is necessary for you to do so, because once you leave this particular page the value will no longer be available for display in plain text.



B. Creating the Netop Portal application Azure AD as a Non-gallery application

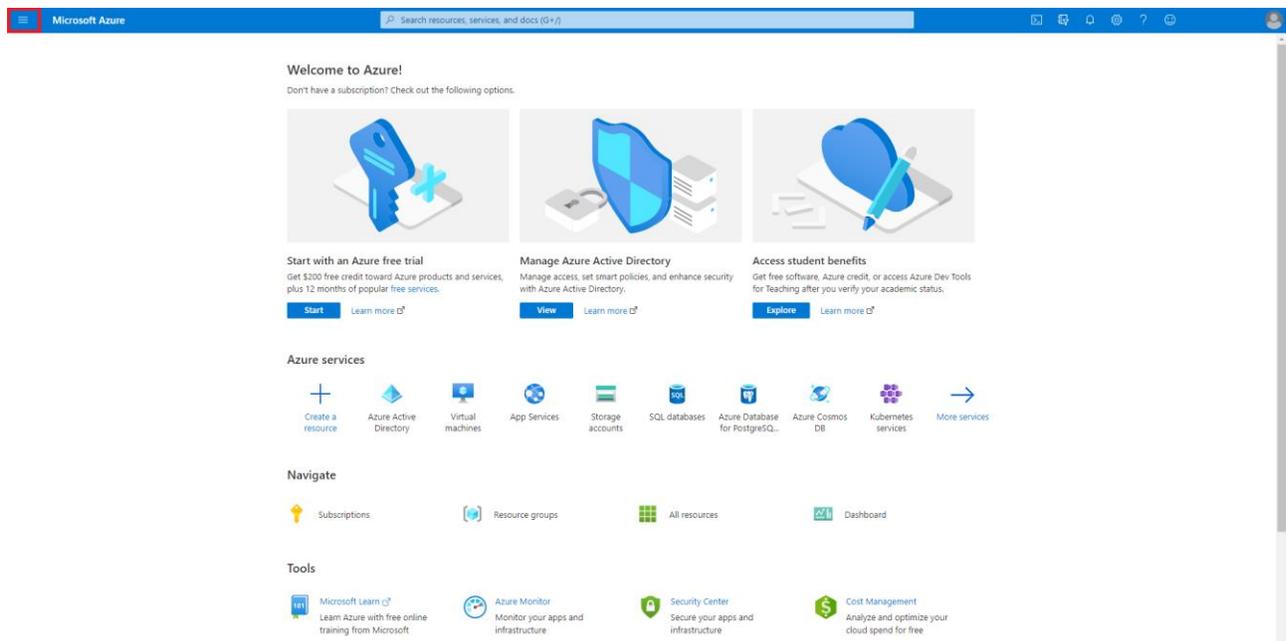
To create the **Netop Portal** application in **Azure AD**, proceed as follows:

1. Log in the [Azure Portal](#).

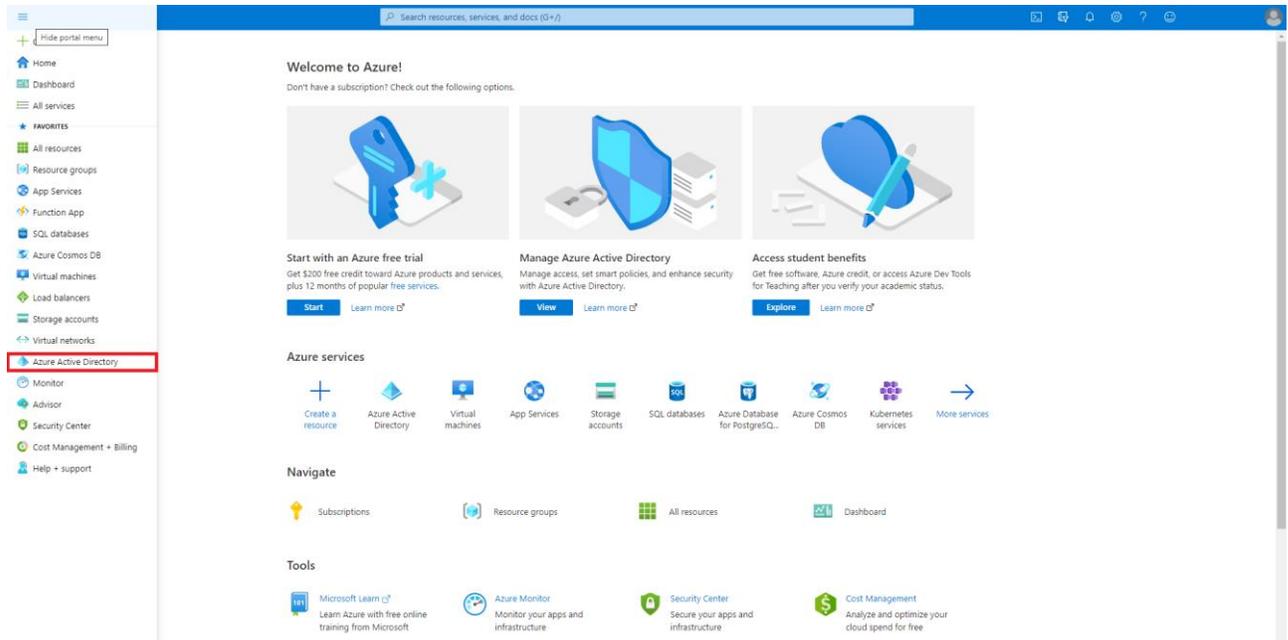


2. Go to **Azure Active Directory**.

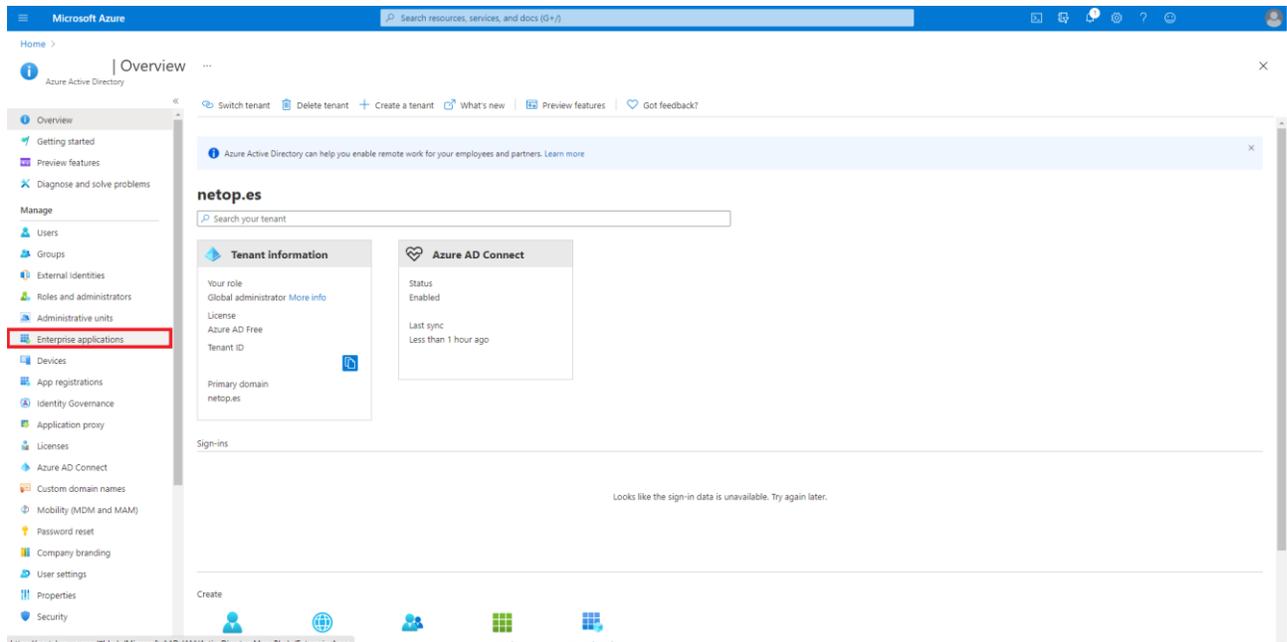
- 2.1. Click on the **More** button.



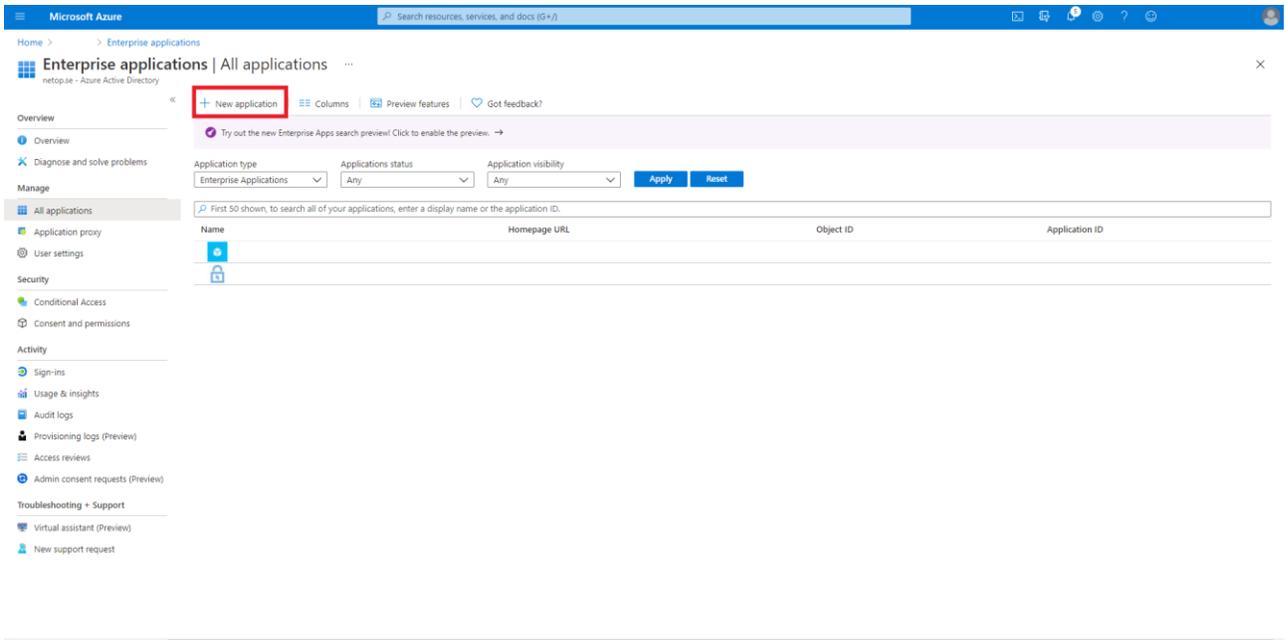
2.2. Click on **Azure Active Directory**.



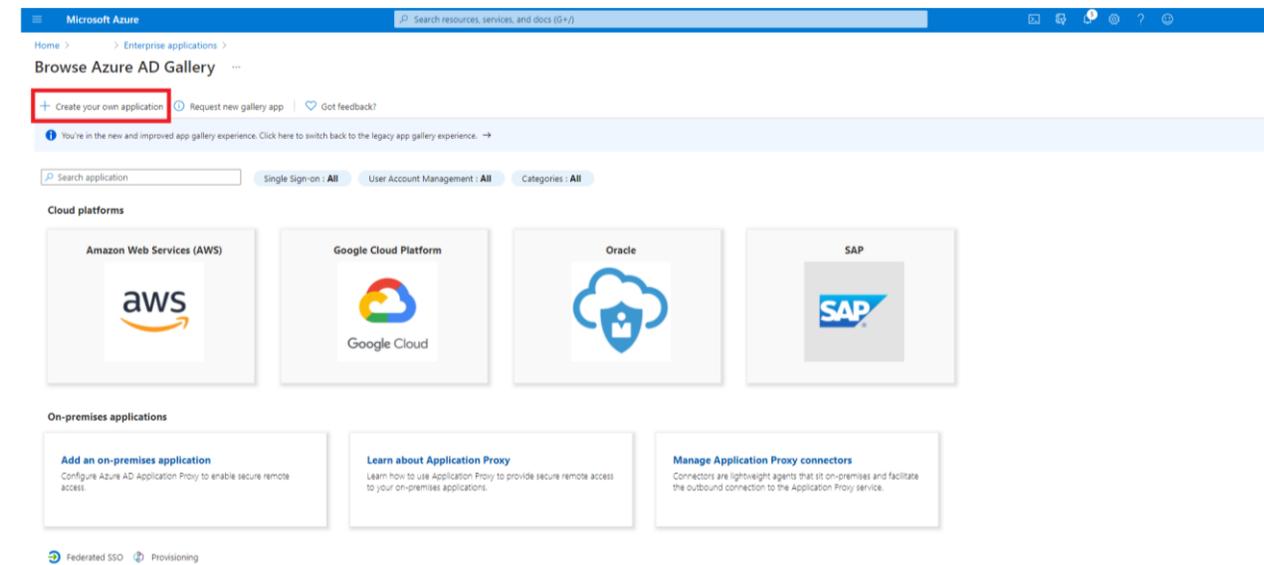
3. Go to **Enterprise applications**.



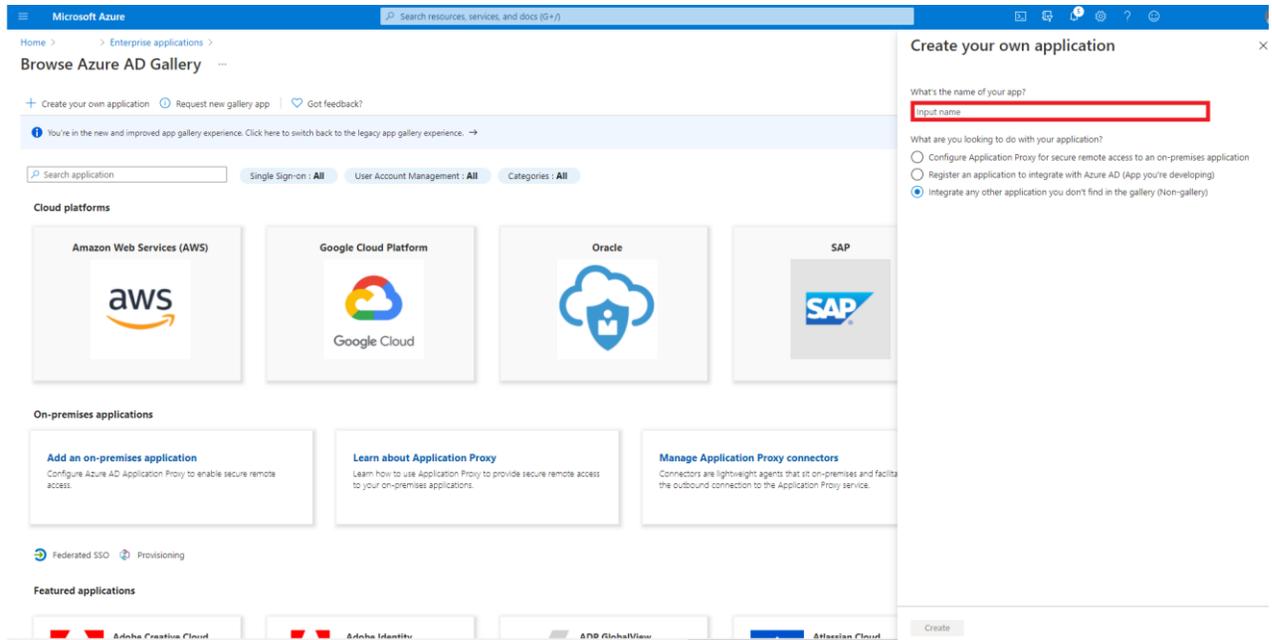
4. Click on the **New application** button.



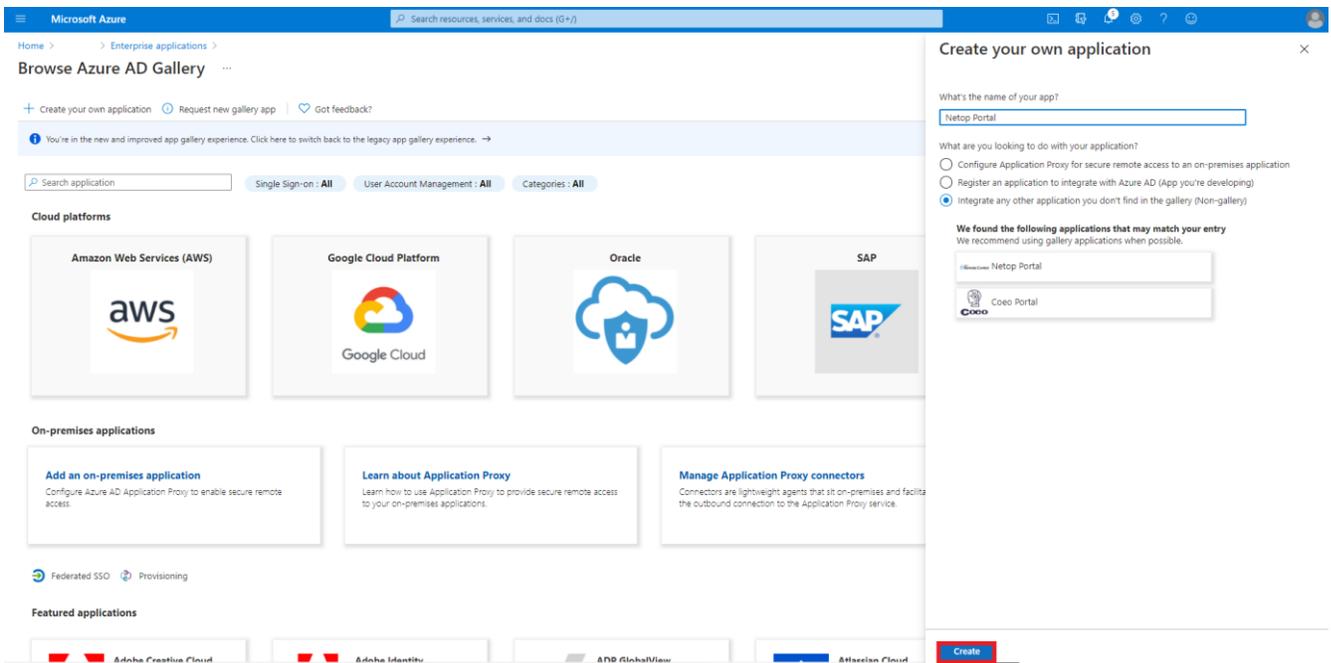
5. Click on the **Create your own application** button.



6. Specify a name for the application in the Input name entry field.



7. Click on the **Create** button to finish adding the Netop Portal application the **Azure Portal**.



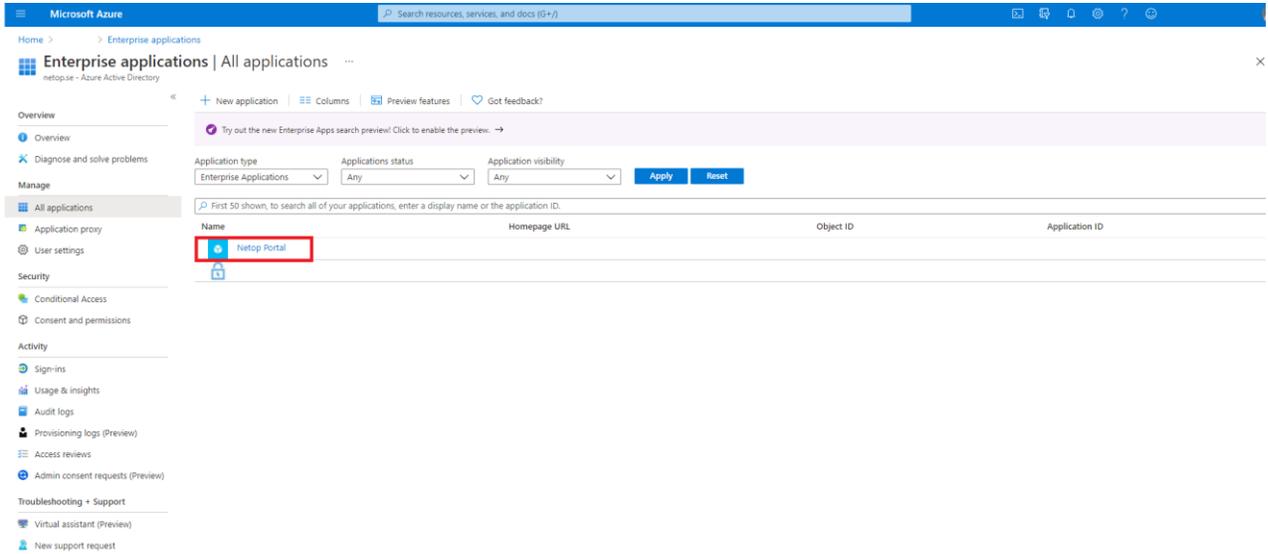
The application is created successfully and added to the **Enterprise applications** section.

Add users and groups to the application

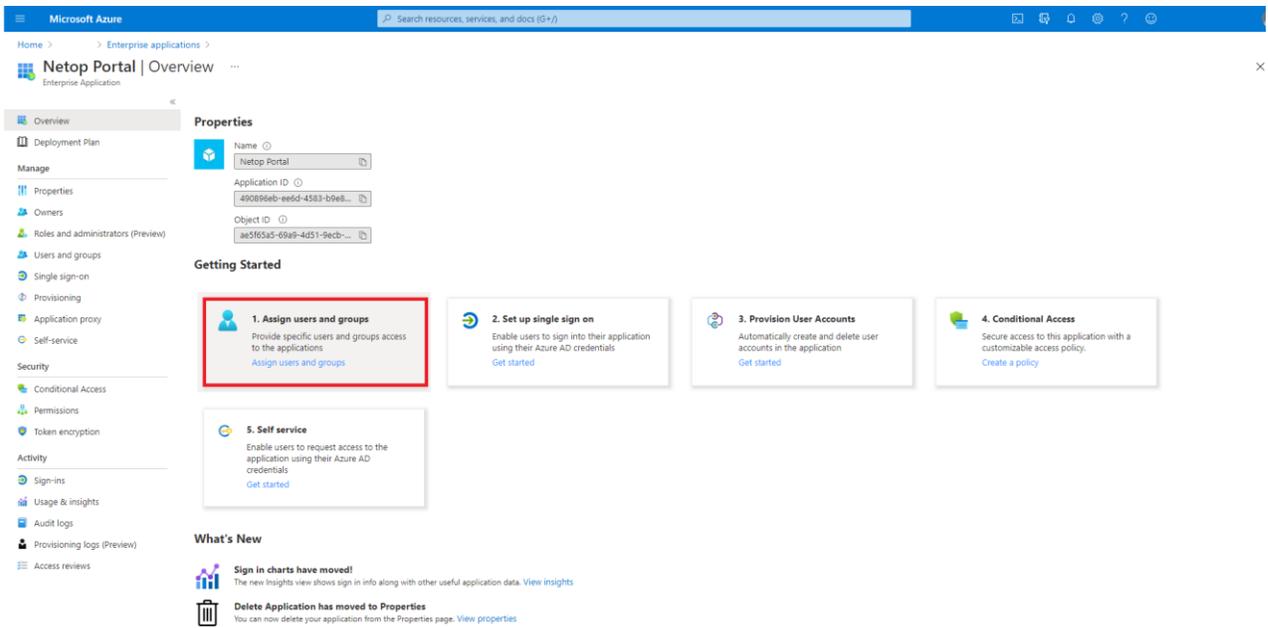
To add users and groups to the application, proceed as follows:

1. Go to **Azure Active Directory**.
2. Go to **Enterprise applications**.

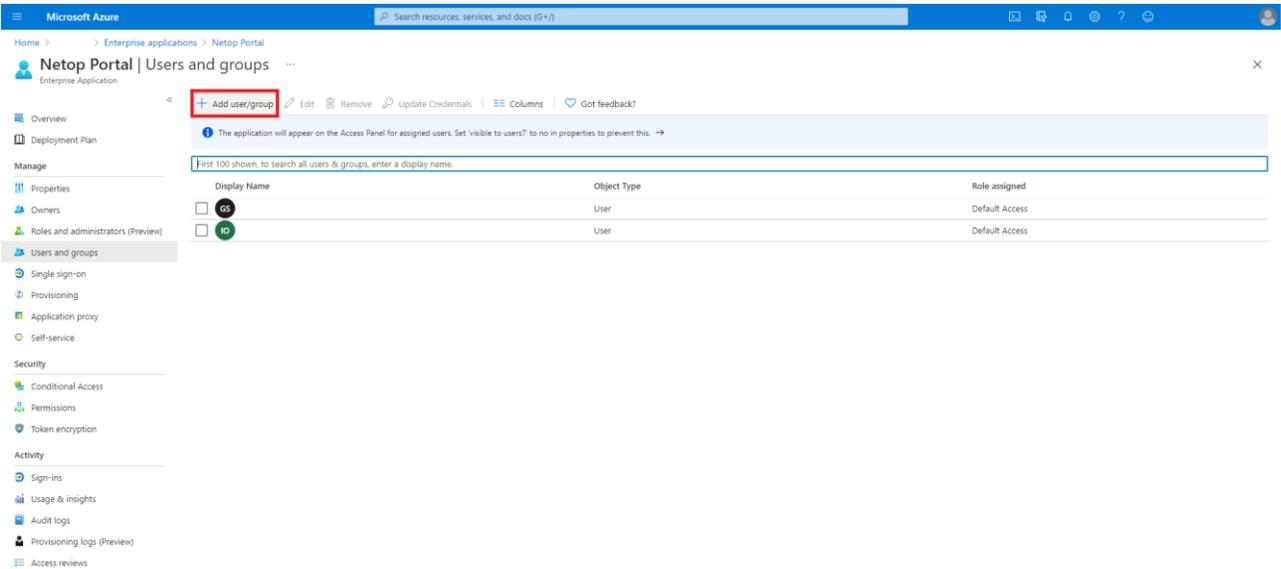
3. Click on the newly created **Netop Portal** application.



4. Click on **Assign users and groups**.

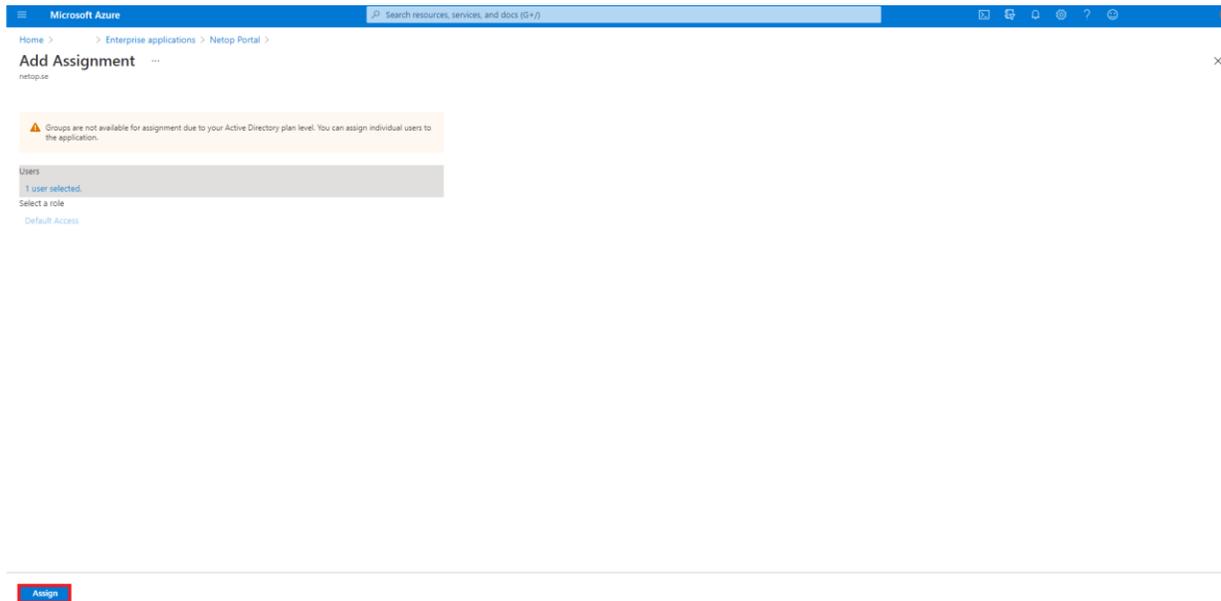


5. Click on the **Add User** button to add the allowed users or groups.



NOTE: Make sure that the users that you add are from the **Windows Server AD**.

6. After you finish adding the users and groups, click on the **Assign** button.

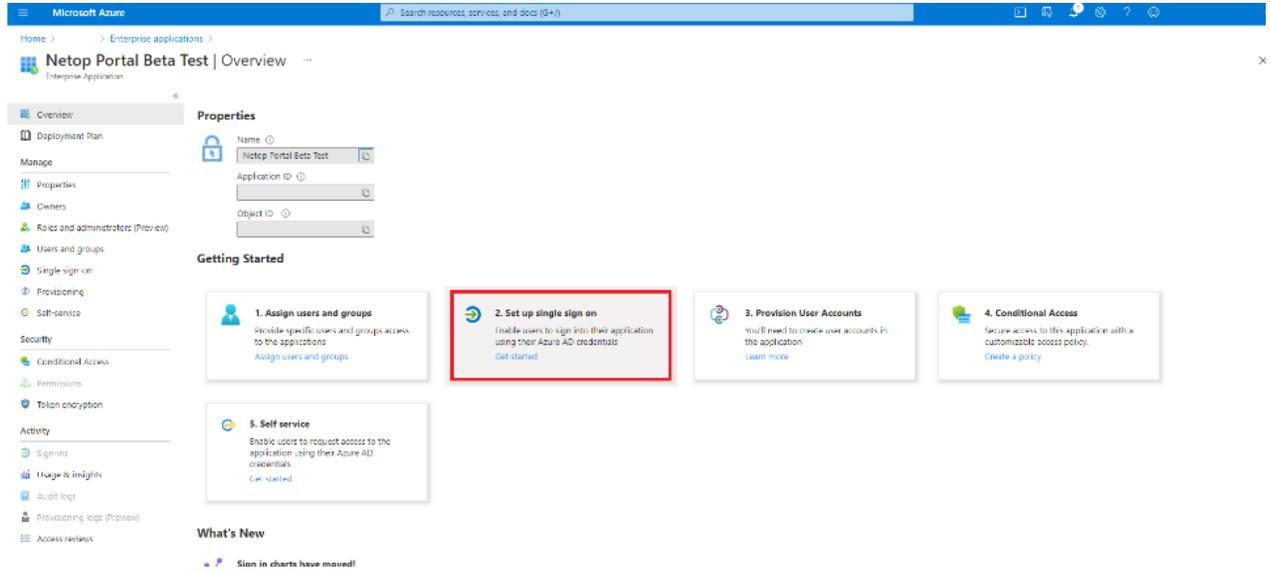


Configure single sign-on

To configure the single sign-on, proceed as follows:

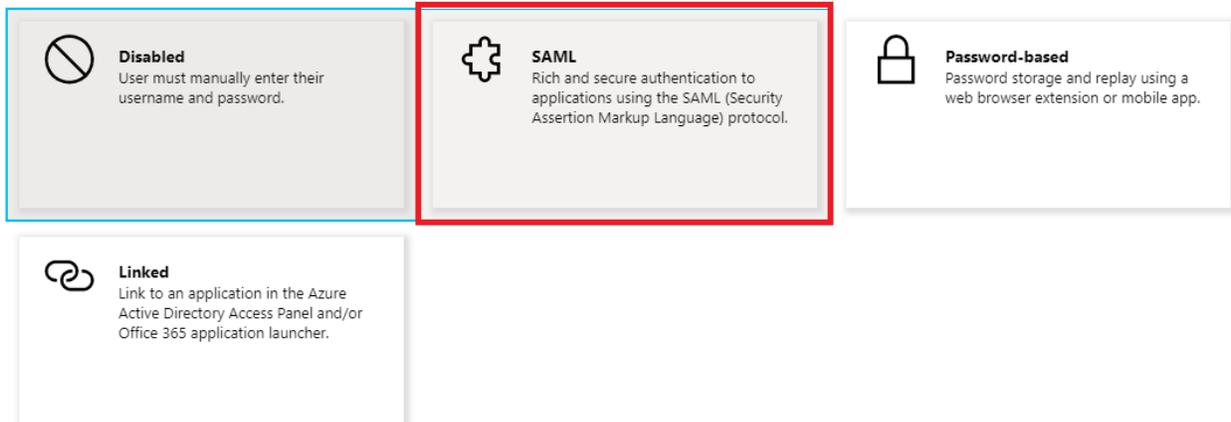
1. Go to **Azure Active Directory**.
2. Go to **Enterprise applications**.
3. Click on the newly created **Netop Portal** application.

4. Click on **Set up single sign-on.**

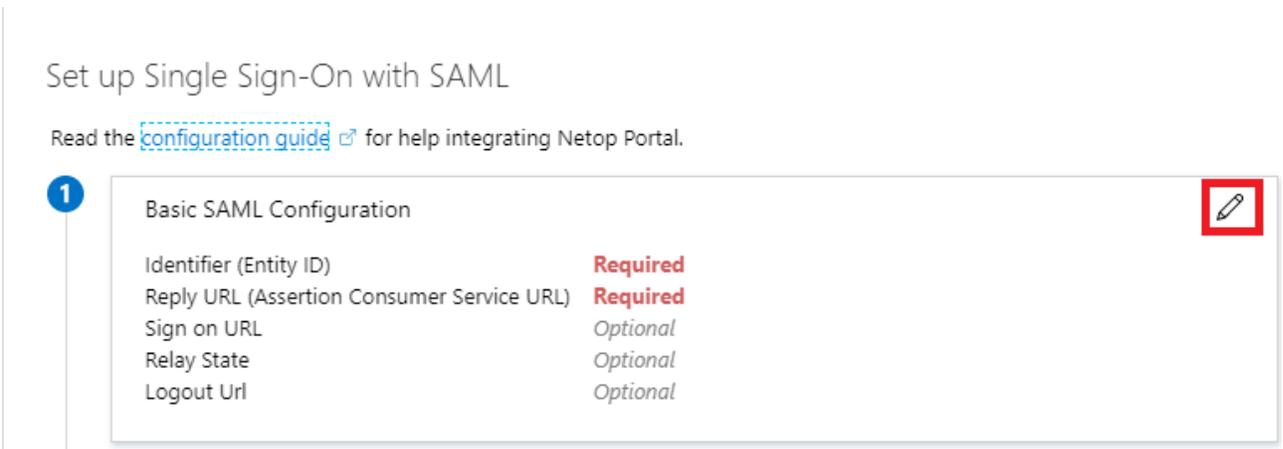


5. Click on **SAML.**

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



6. In the **Basic SAML Configuration** group, click on the **Edit** button.



7. Specify the following settings.

Field name	Value
Identifier (Entity ID)	urn:portal:webservices
Reply URL	https://secure.netop.com/saml

8. Click on the **Save** button to save your changes.

Basic SAML Configuration ×

 Save

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

Default

urn:portal:webservices ⓘ 

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

Default

<https://secure.netop.com/saml> ✓ ⓘ 

Sign on URL ⓘ
Enter a sign on URL ✓

Relay State ⓘ
Enter a relay state

Logout Url ⓘ
Enter a logout url ✓

9. In the **User Attributes & Claims** group, click on the **Edit** button.

2 User Attributes & Claims 

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

10. Click on the **Add new claim** button to create the necessary claims.

Name	Namespace	Source	Source attribute
NRC-ACCOUNT-ID	https://secure.netop.com	Attribute	This is the domain identifier that you both specify here and in the Netop Portal ADFS/Azure AD configuration.
NRC-USERNAME	https://secure.netop.com	Attribute	user.userprincipalname
NRC-GIVEN-NAME	https://secure.netop.com	Attribute	user.givenname
NRC-SURNAME	https://secure.netop.com	Attribute	user.surname
NRC-EMAIL	https://secure.netop.com	Attribute	user.mail

The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**:

11. Click on the **Add a group claim** button to add the following Group claim:

The screenshot shows the 'User Attributes & Claims' configuration page in the Microsoft Azure portal. The 'Add a group claim' button is highlighted with a red box. Below the button, there are two tables: 'Required claim' and 'Additional claims', each listing claim names and their corresponding values.

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname (nameid-for-...
https://secure.netop.com/NRC-EMAIL	user.userprincipalname
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname
https://secure.netop.com/NRC-SURNAME	user.surname
https://secure.netop.com/NRC-USERNAME	user.userprincipalname
nameIdentifier	user.userprincipalname
https://secure.netop.com/NRC-ACCOUNT-ID	"netop"

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

11.1. Select the **All groups** option from the Which groups associated with the user should be returned in the claim section.

The screenshot shows the 'Group Claims' configuration page in the Microsoft Azure portal. The 'All groups' radio button is highlighted with a red box. The page shows options for selecting which groups are associated with the user and returned in the claim.

Group Claims
Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- None
- All groups
- Security groups
- Directory roles
- Groups assigned to the application

Source attribute *

Group ID

Advanced options

- Customize the name of the group claim
- Name (required)
- Namespace (optional)
- Emit groups as role claims

Save

- 11.2. Click on the **Customize the name of the group claim.**
- 11.3. Specify the required name and namespace of the claim:
 - Name: **NRC-GROUPS**
 - Namespace: **https://secure.netop.com**

The screenshot shows the Microsoft Azure portal interface for configuring group claims. The main area displays a table of required and additional claims. The right-hand pane is titled 'Group Claims' and contains several sections: 'Which groups associated with the user should be returned in the claim?' with radio buttons for 'None', 'All groups', 'Security groups', 'Directory roles', and 'Groups assigned to the application'; 'Source attribute *' with a dropdown menu set to 'Group ID'; and 'Advanced options' where the checkbox 'Customize the name of the group claim' is checked and highlighted with a red box. Below this checkbox are input fields for 'Name (required)' and 'Namespace (optional)'. A 'Save' button is visible at the bottom of the right-hand pane.

12. Click on the **Save** button to save your changes.

This screenshot shows the same 'Group Claims' configuration page as the previous one, but with the 'Name (required)' field filled with 'NRC-GROUPS' and the 'Namespace (optional)' field filled with 'https://secure.netop.com'. The 'Save' button at the bottom of the right-hand pane is now highlighted with a red box, indicating it is the next step in the process.

Make sure that you save the following information:

- The **Federation Metadata XML** file

3

SAML Signing Certificate 	
Status	Active
Thumbprint	70F19DDC96EB823EECD2E9BF8A750A961F0E0F6
Expiration	4/2/2023, 12:32:08 PM
Notification Email	andrei@nrcazuretest.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/cd5f608a-30... 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- The **Login URL**

4

Set up Netop Portal

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

Login URL	https://login.microsoftonline.com/cd5f608a-30... 
Azure AD Identifier	https://sts.windows.net/cd5f608a-30a6-4ec3-b... 
Logout URL	https://login.microsoftonline.com/common/wsf... 

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

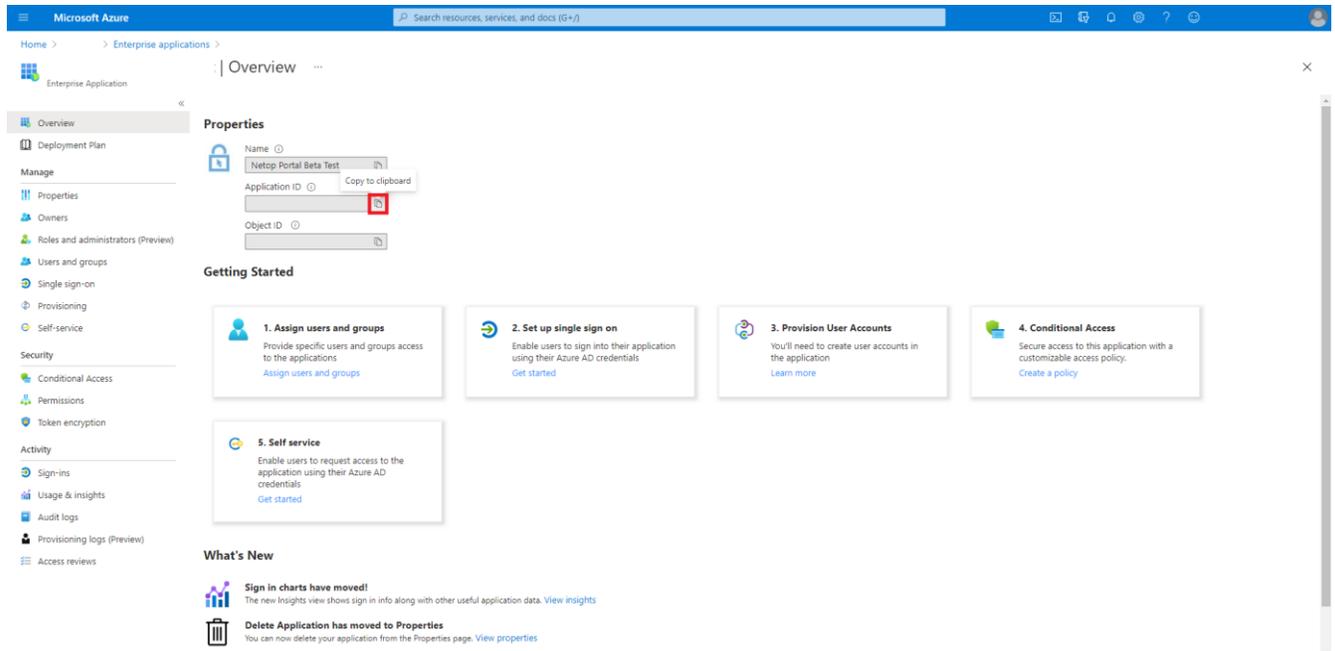
If you plan on using the Azure AD groups then it is necessary that you also save the **Application ID**

- **Application ID**

To retrieve the Application ID value from the Azure Portal, proceed as follows:

- 1.1. Go to the **Azure Portal**.
- 1.2. Go to **Windows Active Directory**.
- 1.3. Go to **Enterprise Applications**.
- 1.4. Select the Netop Portal application.
- 1.5. Go to **Overview**.

1.6. Click on the **Copy to clipboard** button.

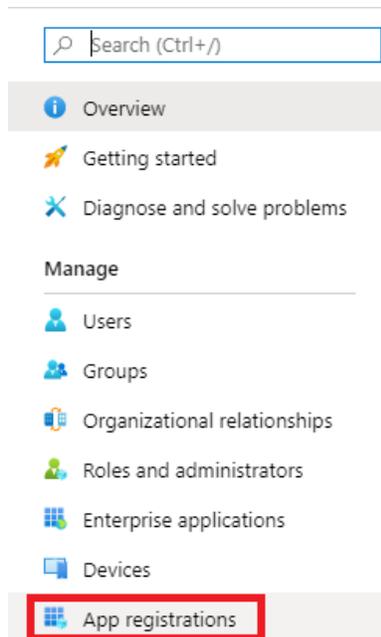


Configure the application permissions

The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**.

To configure the application permissions, proceed as follows:

1. Go to **Azure Active Directory**.
2. Go to **App registrations**.



3. Click on the **Netop Portal** application.

All applications Owned applications

Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates & secrets
NP Netop Portal			

4. Click on the **View API permissions** button.

Call APIs



Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API permissions

Sign in users in 5 minutes



Use our SDKs to sign in users and call APIs in a few steps

View all quickstart guides

5. Click on the **Add a permission** button to add the necessary permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for home

API / Permissions name	Type	Description	Admin consent req...	Status
No permissions added				

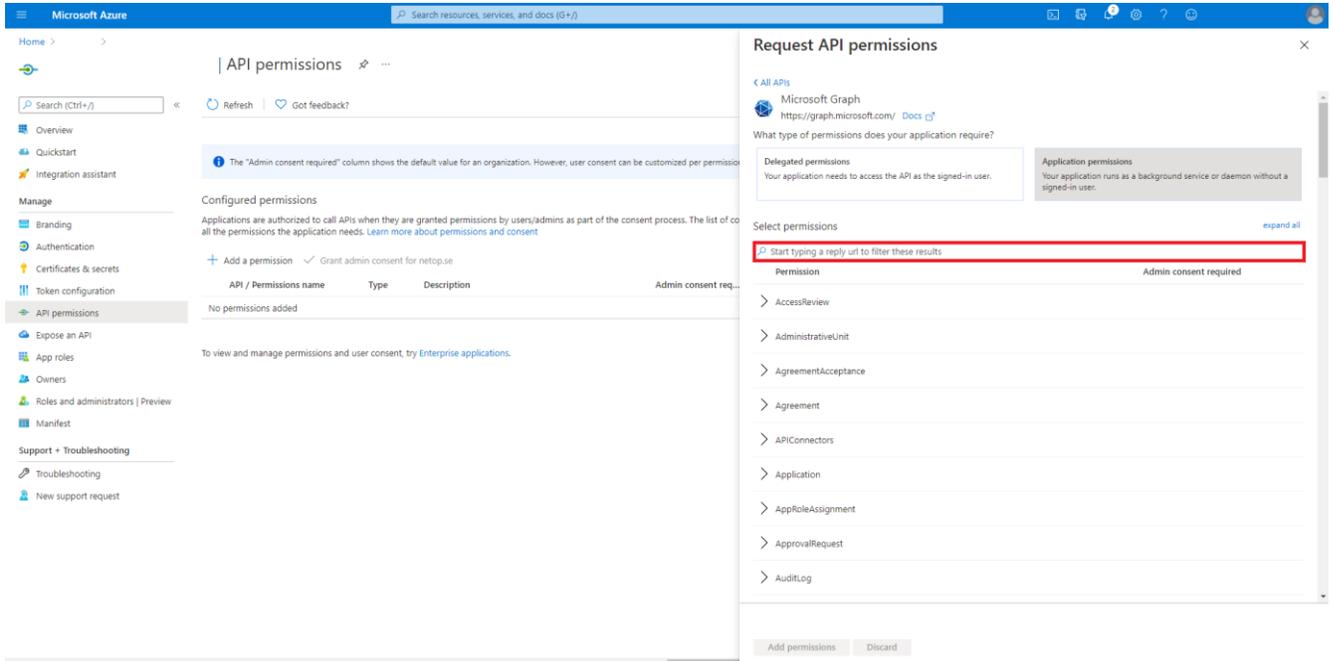
6. Click on Microsoft Graph.

The screenshot shows the Microsoft Azure portal interface. On the left is a navigation pane with 'API permissions' selected. The main area displays 'Configured permissions' with a table that is currently empty. A right-hand pane titled 'Request API permissions' is open, showing a list of 'Commonly used Microsoft APIs'. The 'Microsoft Graph' API is highlighted with an orange border. Below it are other APIs like 'Azure Service Management' and 'Office 365 Management APIs'. Further down, there are 'More Microsoft APIs' including 'Azure Batch', 'Azure Data Catalog', 'Azure Data Explorer', 'Azure Data Explorer (with Multifactor Authentication)', 'Azure Data Lake', 'Azure DevOps', 'Azure Import/Export', 'Azure Key Vault', and 'Azure Maps'.

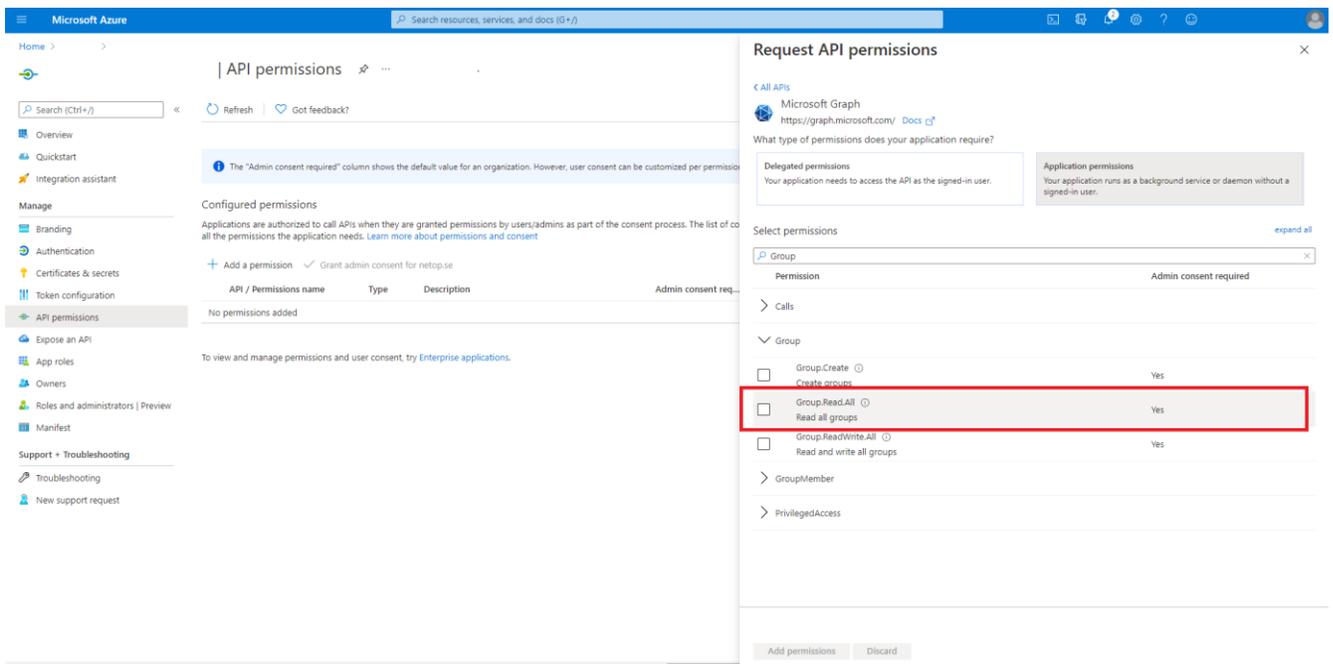
7. Click on Application permissions.

This screenshot shows the same Microsoft Azure portal interface as the previous one, but the 'Request API permissions' dialog box is now showing the 'Application permissions' section. The 'Microsoft Graph' API is selected, and the 'What type of permissions does your application require?' section is visible. The 'Application permissions' option is highlighted with a red border. Below this section, there are two options: 'Delegated permissions' and 'Application permissions'. The 'Application permissions' option is selected, and its description is: 'Your application runs as a background service or daemon without a signed-in user.' At the bottom of the dialog, there are 'Add permissions' and 'Discard' buttons.

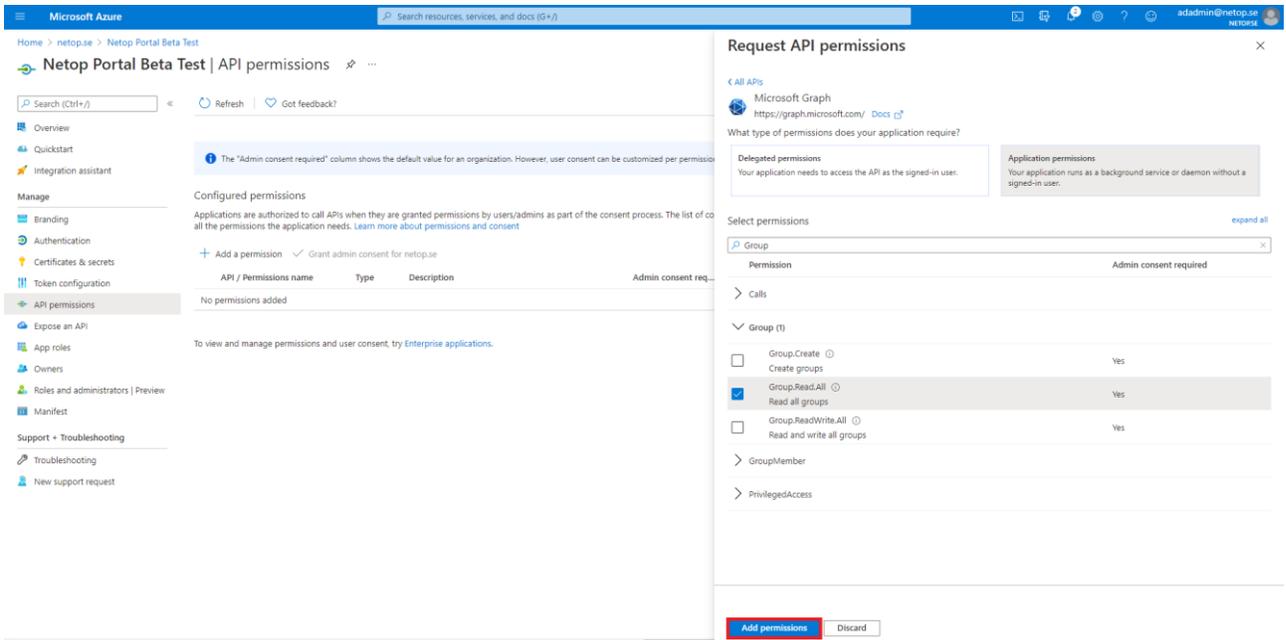
8. Search for Group in the **Start typing a reply url to filter these results** search field.



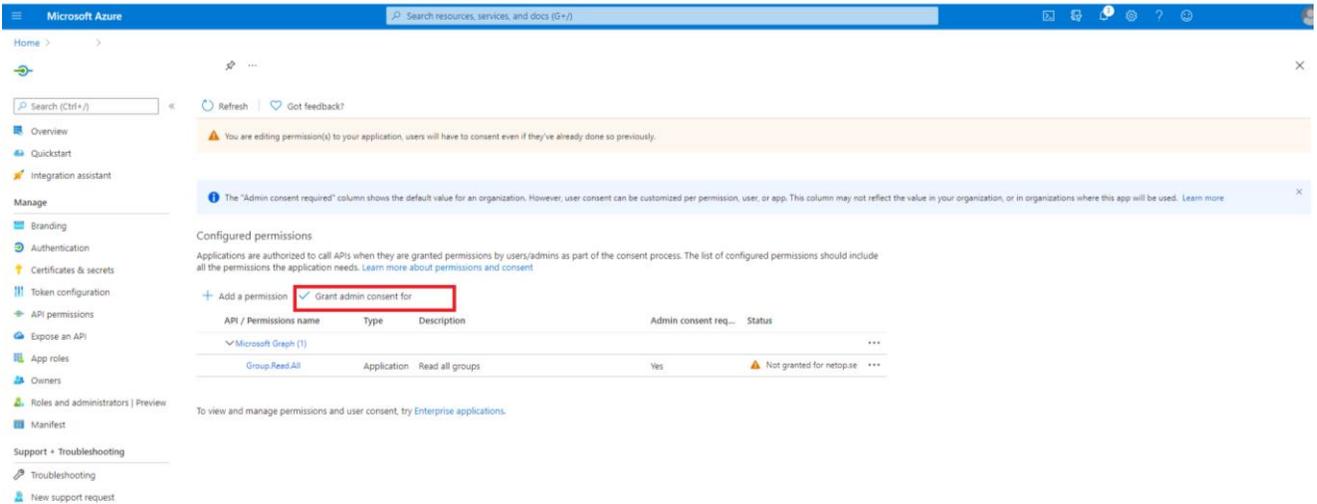
9. Click on the **Group.Read.All** option.



10. Click on the **Add permissions** button to add your permission.



11. Click on the **Grant admin consent for ...** button to grant admin consent for the API permission.

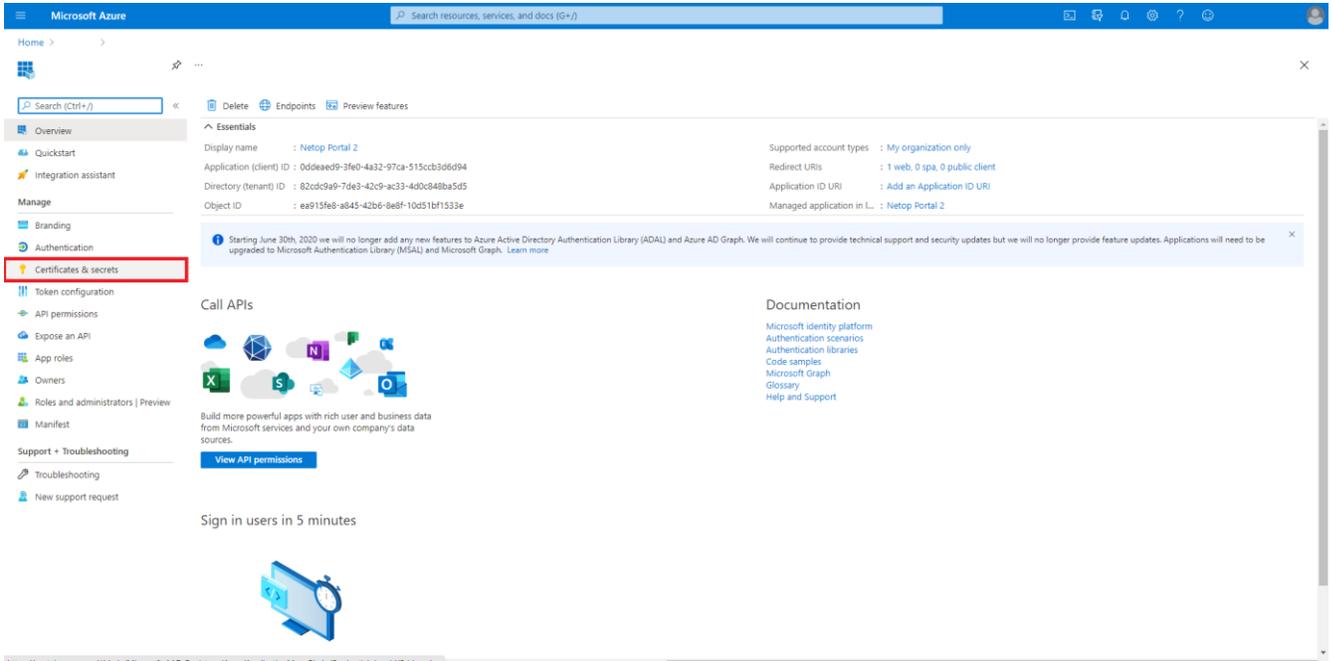


Configure certificates & secrets

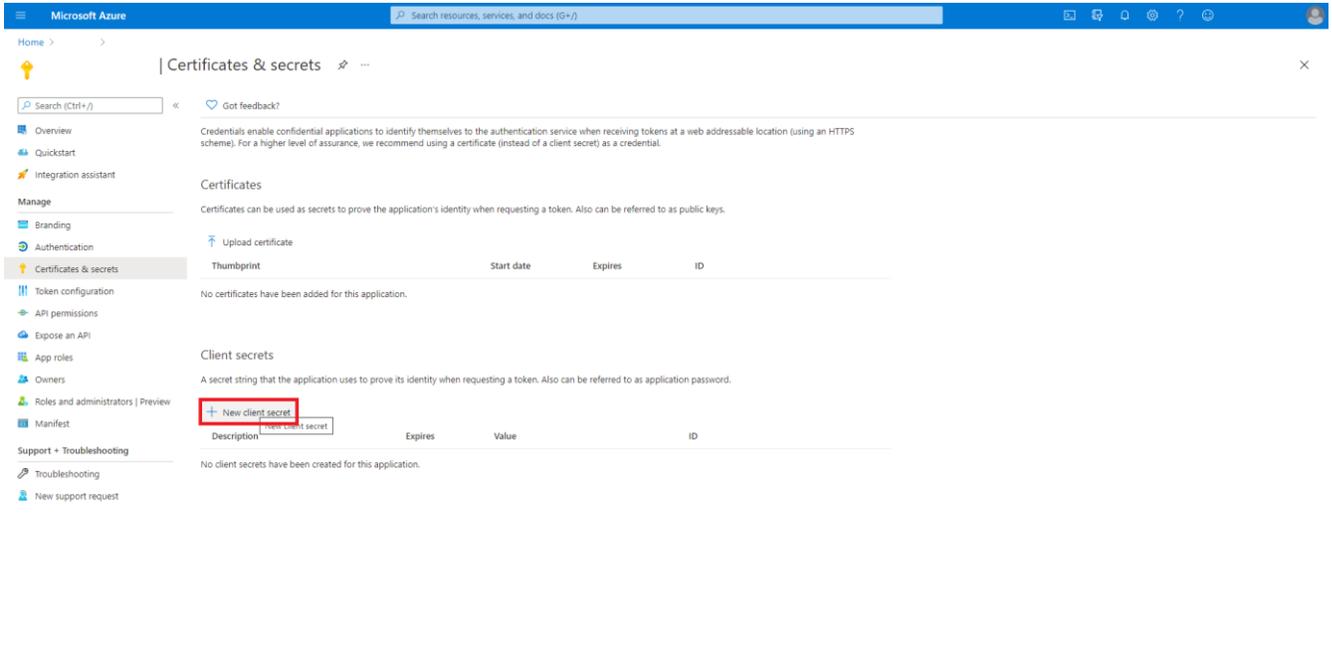
To configure the certificates & secrets for the Netop Portal application in the Azure Portal, proceed as follows:

1. Go to **Azure Active Directory**.
2. Go to **App registrations**.
3. Click on the **Netop Portal** application.

4. Go to **Certificates & secrets**.



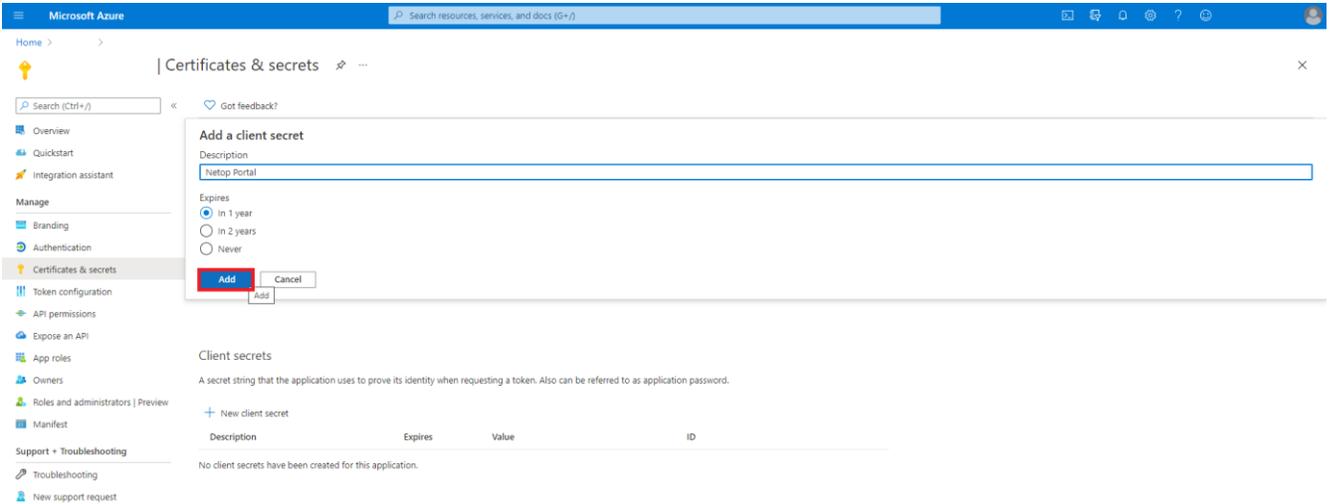
5. Click on the **New client secret** button.



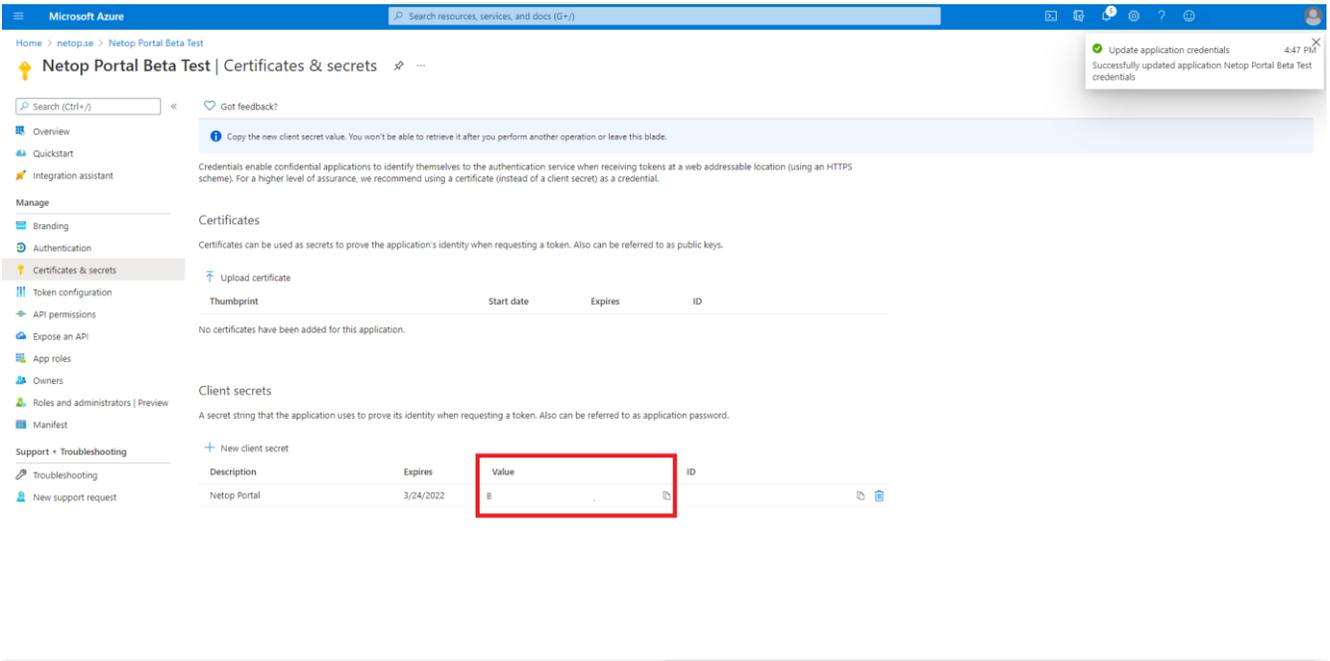
6. Specify a name for the client secret in the **Description** entry field.

7. Specify an expiry date for the client secret accordingly to your needs.

8. Click on the **Add** button.



9. Save the client secret value in a text editor or copy it to the clipboard. It is necessary for you to do so, because once you leave this particular page the value will no longer be available for display in plain text.



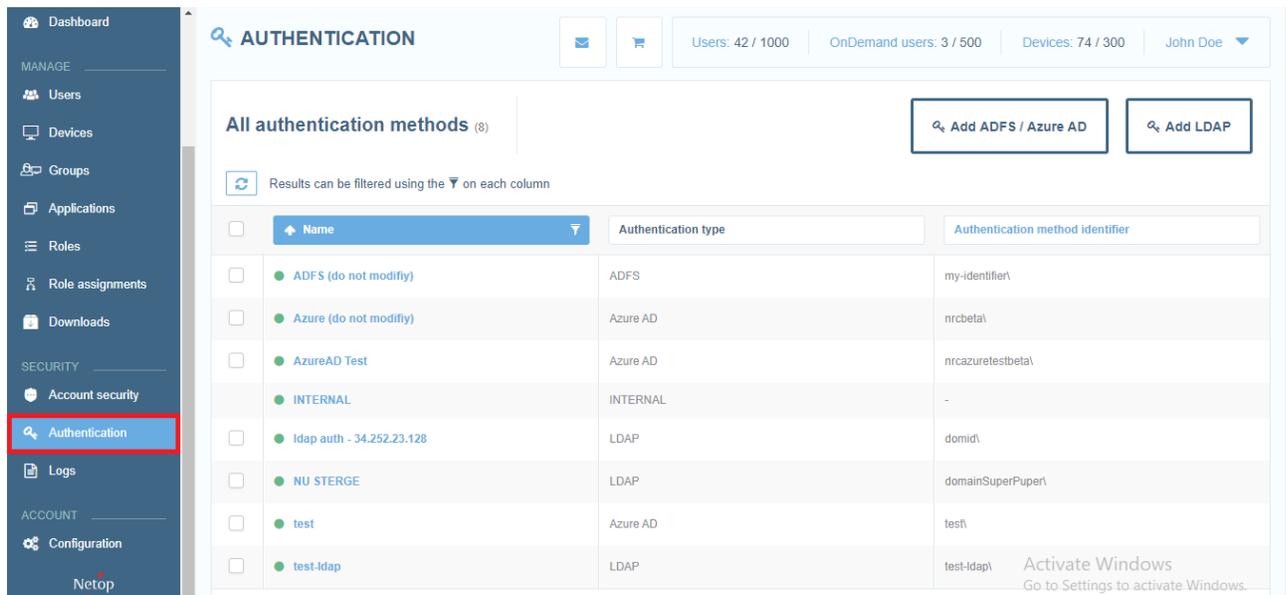
Configure Azure AD in the Netop Portal

To configure the **ADFS/Azure AD** authentication method in the **Netop Portal**, proceed as follows:

1. Log in to the [Netop Portal](#).

NOTE: Make sure that you use an administrator account.

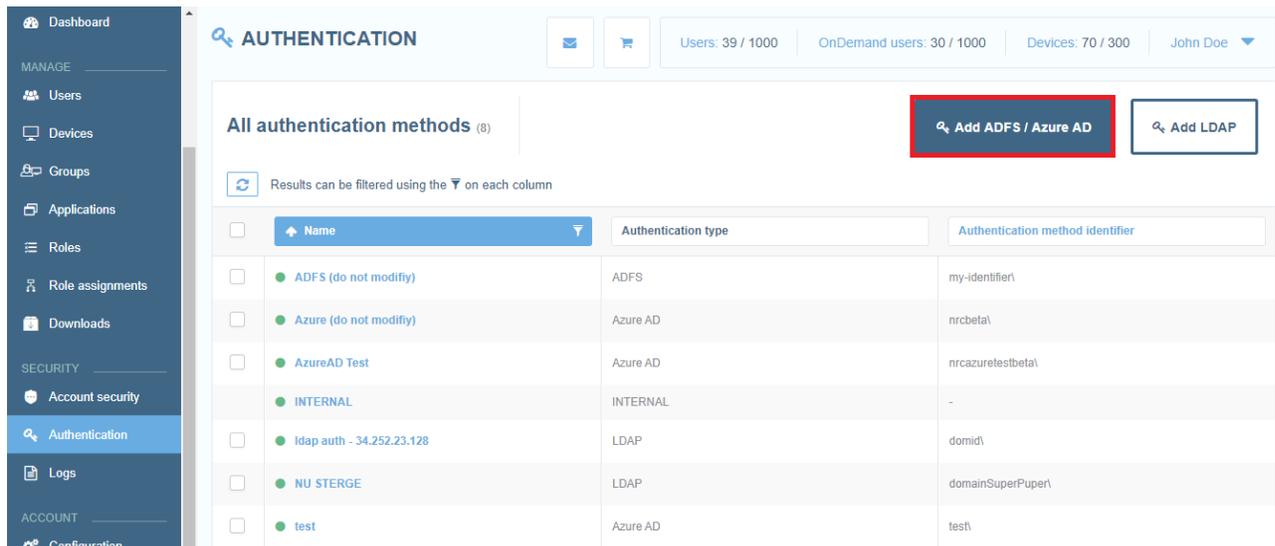
2. Go to **Authentication**.



The screenshot shows the Netop Portal Authentication page. The left sidebar is visible with the 'Authentication' menu item highlighted in red. The main content area displays 'All authentication methods (8)' and a table of existing methods. The 'Add ADFS / Azure AD' button is highlighted with a red box.

Name	Authentication type	Authentication method identifier
ADFS (do not modify)	ADFS	my-identifier\
Azure (do not modify)	Azure AD	nrcbeta\
AzureAD Test	Azure AD	nrcazuretestbeta\
INTERNAL	INTERNAL	-
ldap auth - 34.252.23.128	LDAP	domid\
NU STERGE	LDAP	domainSuperPuper\
test	Azure AD	test\
test-ldap	LDAP	test-ldap\

3. Click on the **Add ADFS / Azure AD** button.



The screenshot shows the Netop Portal Authentication page after clicking the 'Add ADFS / Azure AD' button. The button is now highlighted with a red box. The table of authentication methods remains the same as in the previous screenshot.

Name	Authentication type	Authentication method identifier
ADFS (do not modify)	ADFS	my-identifier\
Azure (do not modify)	Azure AD	nrcbeta\
AzureAD Test	Azure AD	nrcazuretestbeta\
INTERNAL	INTERNAL	-
ldap auth - 34.252.23.128	LDAP	domid\
NU STERGE	LDAP	domainSuperPuper\
test	Azure AD	test\

4. Specify a name for the authentication method in the **Name** entry field.

ADD ADFS / AZURE AD Close ✕

More information on how to integrate with ADFS and Azure AD is available [here](#).

Name ✓

Enabled (This authentication method is enabled)

Authentication type ?

The authentication type will be automatically filled in once you upload the FederationMetadata.xml file.

Domain identifier ?

This will be used when logging in (domain identifier/username)

IdP ?

Identity Provider's (IdP) URL

Group (Optional) ?

The user will become a member of this group on first login.

ADFS / Azure AD FederationMetadata.xml file ?

5. Click on the toggle button to enable or disable the authentication method.

6. In the **Domain identifier** entry field, specify the same value as the one specified in the NRC-ACCOUNT-ID user claim.

ADD ADFS / AZURE AD Close ✕

More information on how to integrate with ADFS and Azure AD is available [here](#).

Name ✓

Enabled (This authentication method is enabled)

Authentication type ?

The authentication type will be automatically filled in once you upload the FederationMetadata.xml file.

Domain identifier ✓

This will be used when logging in (domain identifier/username)

IdP ?

Identity Provider's (IdP) URL

Group (Optional) ?

The user will become a member of this group on first login.

ADFS / Azure AD FederationMetadata.xml file ?

7. In the **IdP** field, copy the **Login URL** from the **Set up Single sign on with SAML** page in the Azure AD portal.

ADD ADFS / AZURE AD Close x

More information on how to integrate with ADFS and Azure AD is available [here](#).

Name
Azure AD ✓

Enabled (This authentication method is enabled)

Authentication type ▼ ⓘ
The authentication type will be automatically filled in once you upload the FederationMetadata.xml file.

Domain identifier
netopazure ✓
This will be used when logging in (domain identifier/username)

IdP
https:// ✓
Identity Provider's (IdP) URL

Group (Optional) ▼
The user will become a member of this group on first login.

ADFS / Azure AD FederationMetadata.xml file Browse ⓘ

Save

8. In the **ADFS/Azure AD FederationMetadata.xml** field, click on the **Browse** button.

ADD ADFS / AZURE AD Close x

More information on how to integrate with ADFS and Azure AD is available [here](#).

Name
Azure AD ✓

Enabled (This authentication method is enabled)

Authentication type ▼ ⓘ
The authentication type will be automatically filled in once you upload the FederationMetadata.xml file.

Domain identifier
netopazure ✓
This will be used when logging in (domain identifier/username)

IdP
https:// ✓
Identity Provider's (IdP) URL

Group (Optional) ▼
The user will become a member of this group on first login.

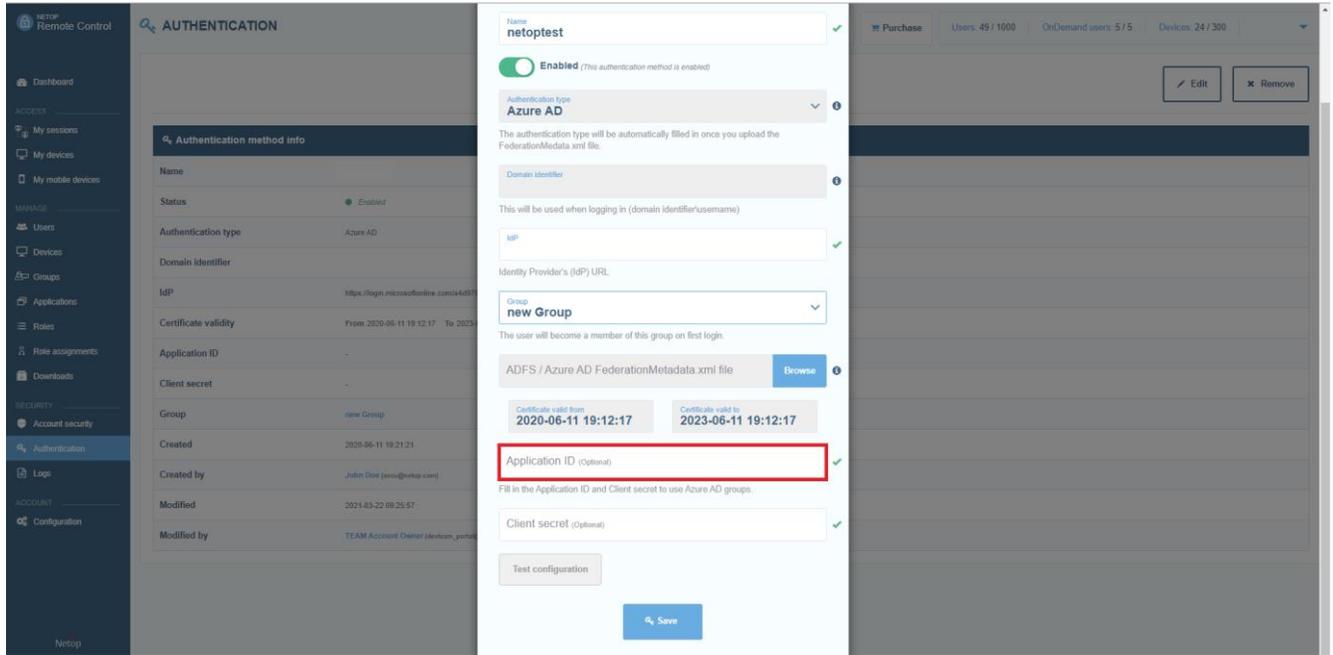
ADFS / Azure AD FederationMetadata.xml file **Browse** ⓘ

Save

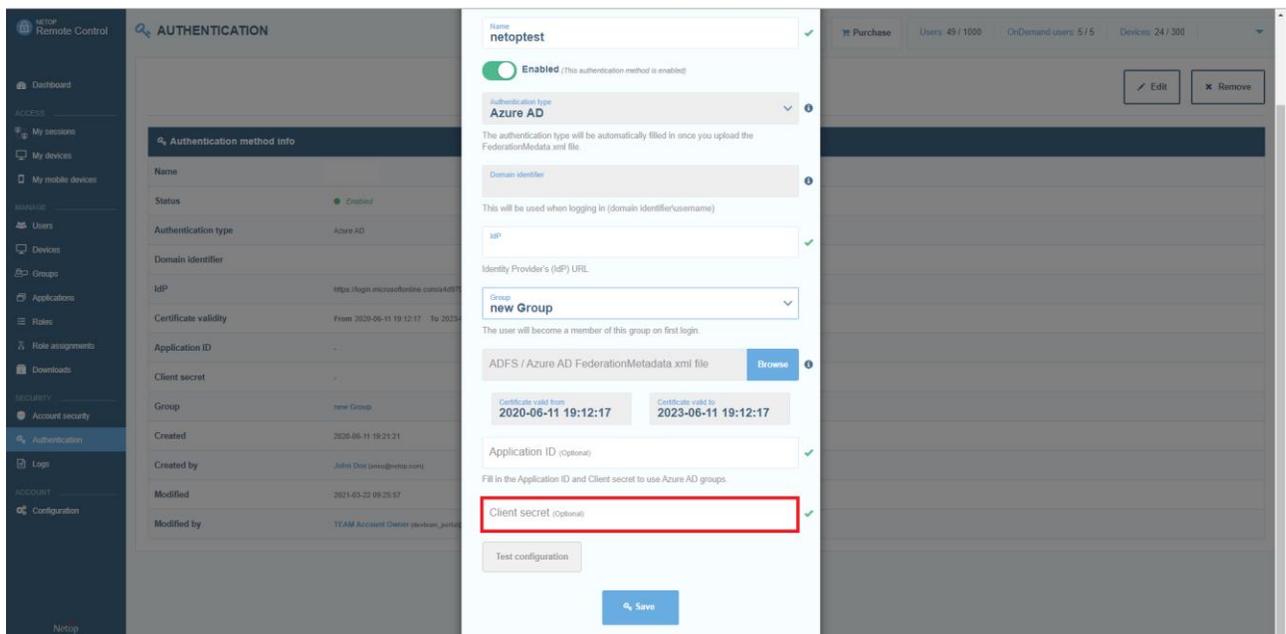
9. Go to the file path where you saved the **FederationMetadata.xml** file, select it, and click on **Open**.

The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**.

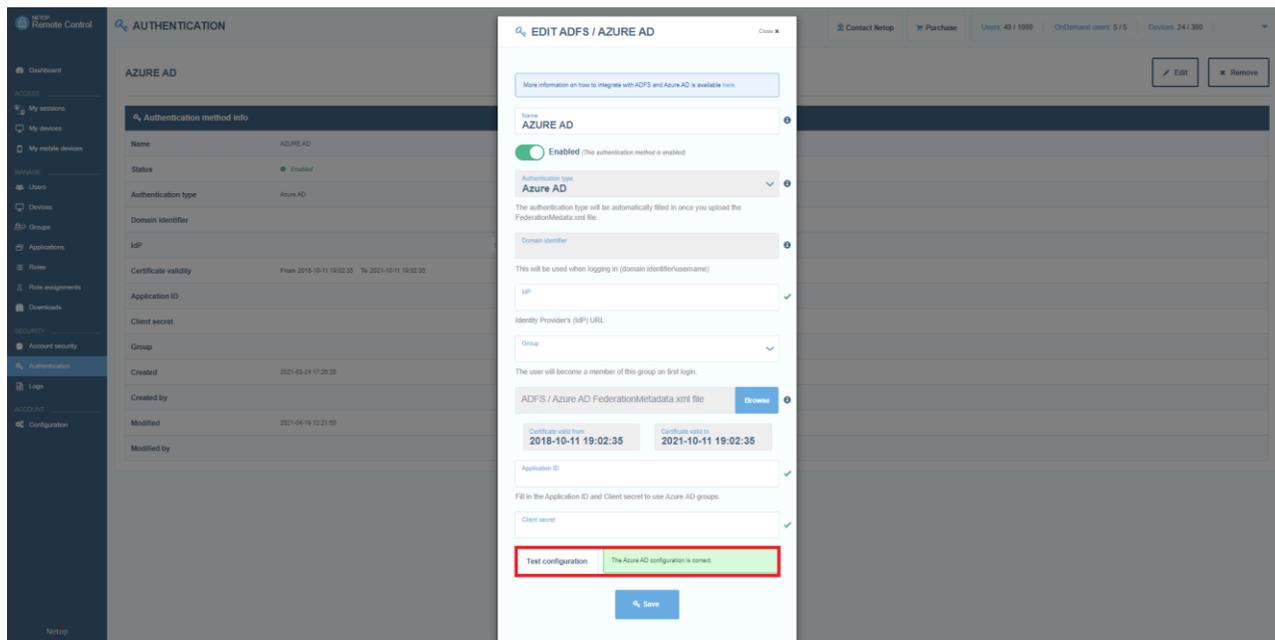
10. In the **Application ID** entry field, specify the Netop Portal **Application ID** from the **Azure Portal**.



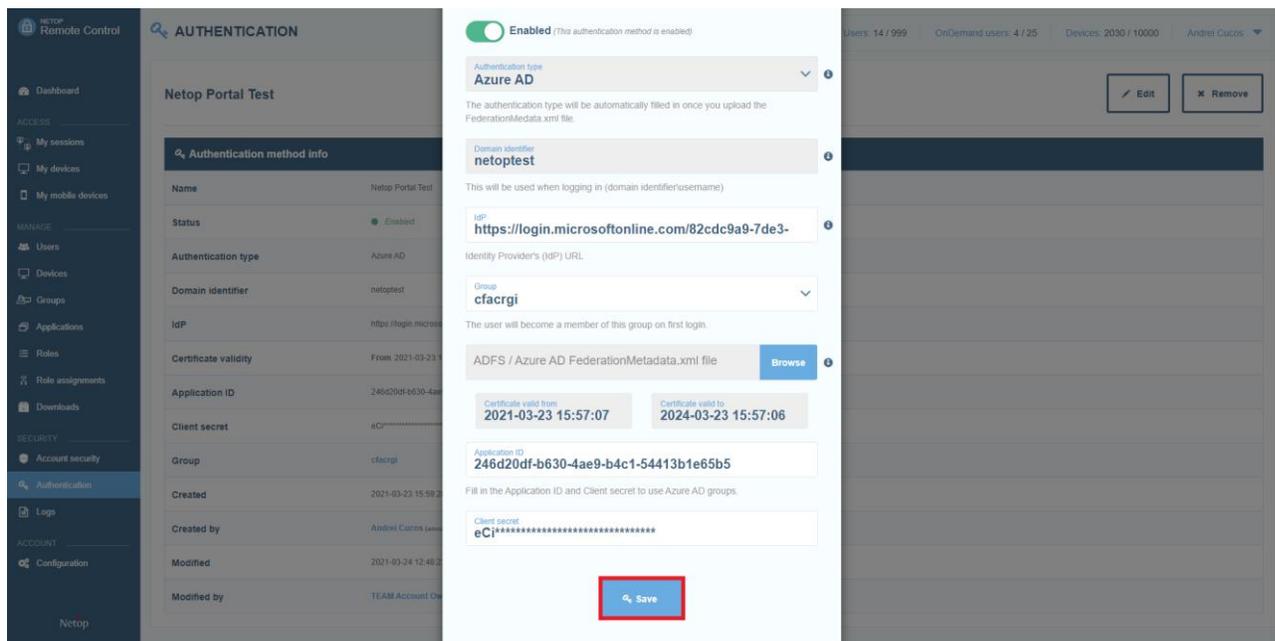
11. In the **Client secret** entry field, specify the client secret value from the **Certificates & secrets** page in the Azure Portal.



12. To test your configuration, click on the **Test configuration** button. “*The Azure AD configuration is correct.*” text message is displayed if the configuration is successful, or an error message is displayed if the configuration was unsuccessful.



13. Click on **Save** to save your configuration.



ADFS integration with the Netop Portal

The ADFS integration with the **Netop Portal** requires setting up a two-way trust. ADFS requires to be configured to trust the **Netop Portal** as a relying party.

Pre-requisites

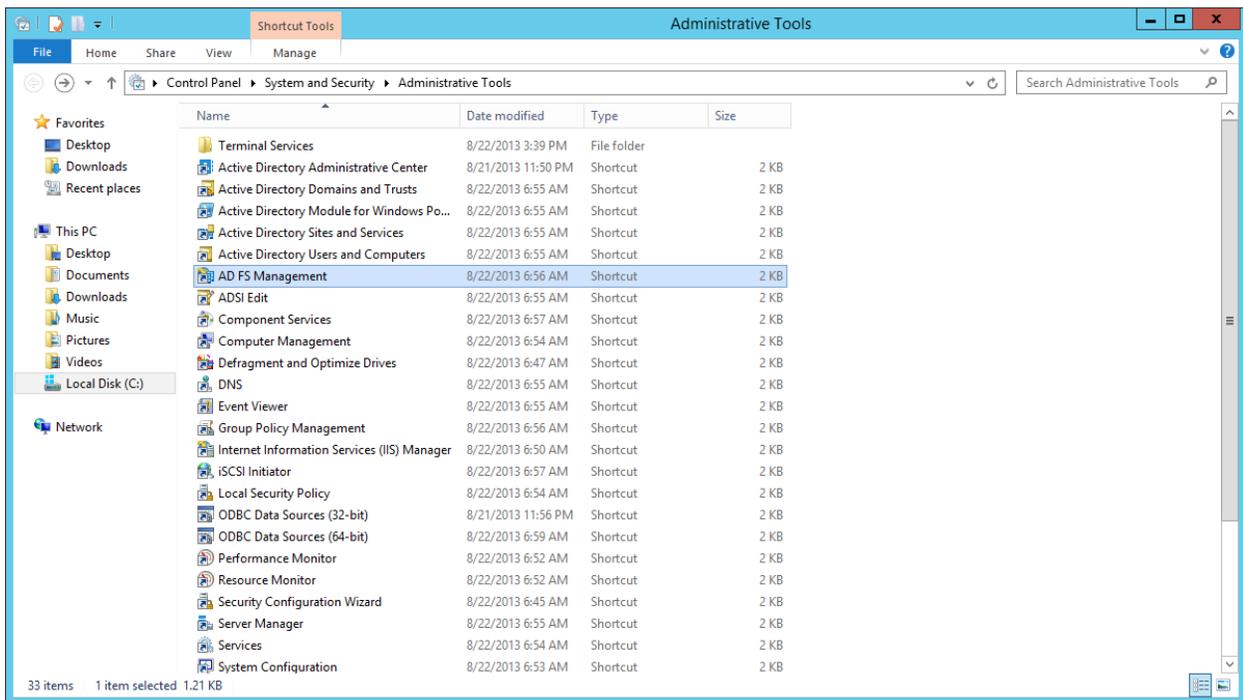
- ADFS 2.0 or later is installed (for more information on how to install ADFS 2.0, refer to the following [link](#))
- The users that authenticate by using ADFS are required to have the following LDAP fields non empty:
 - E-Mail-Addresses
 - Given-Name
 - User-Principal-Name

NOTE: The following procedure uses the Windows Server 2012 R2 Operating System.

Add Netop Portal as a Trusted Relying Party

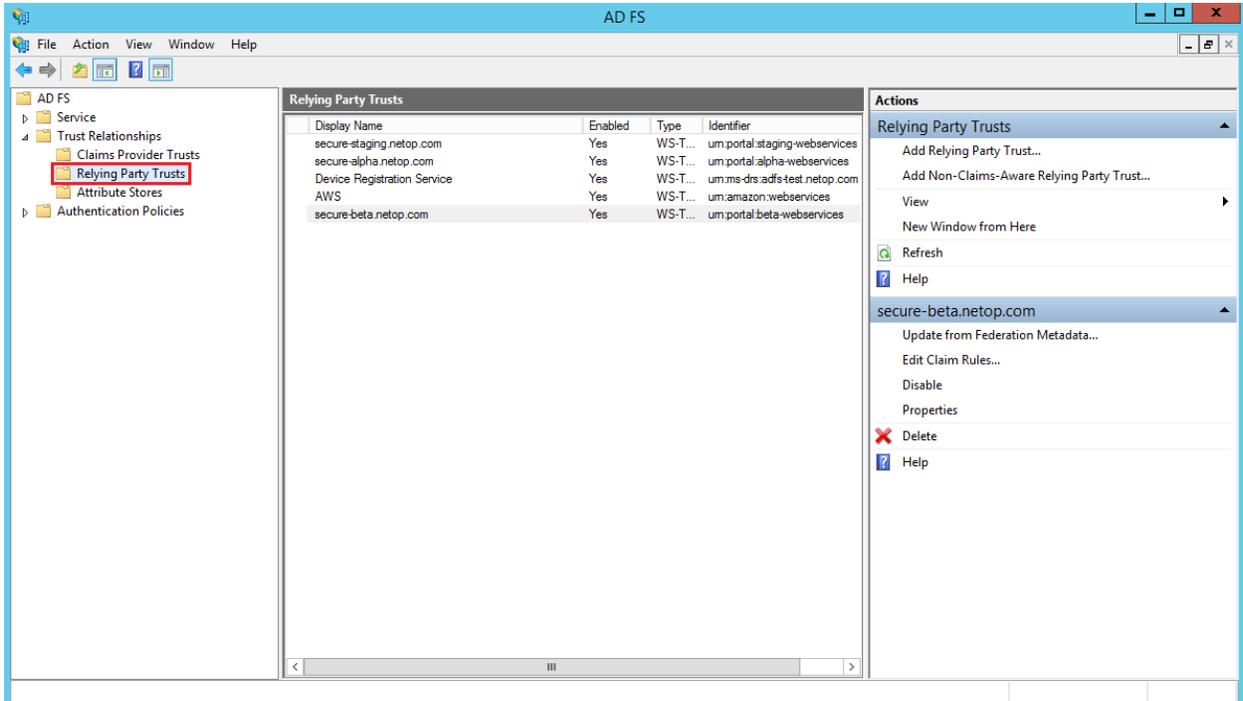
To add the **Netop Portal** as a Trusted Relying Party, proceed as follows:

1. Connect to your ADFS server.
2. Open the ADFS Management Console.

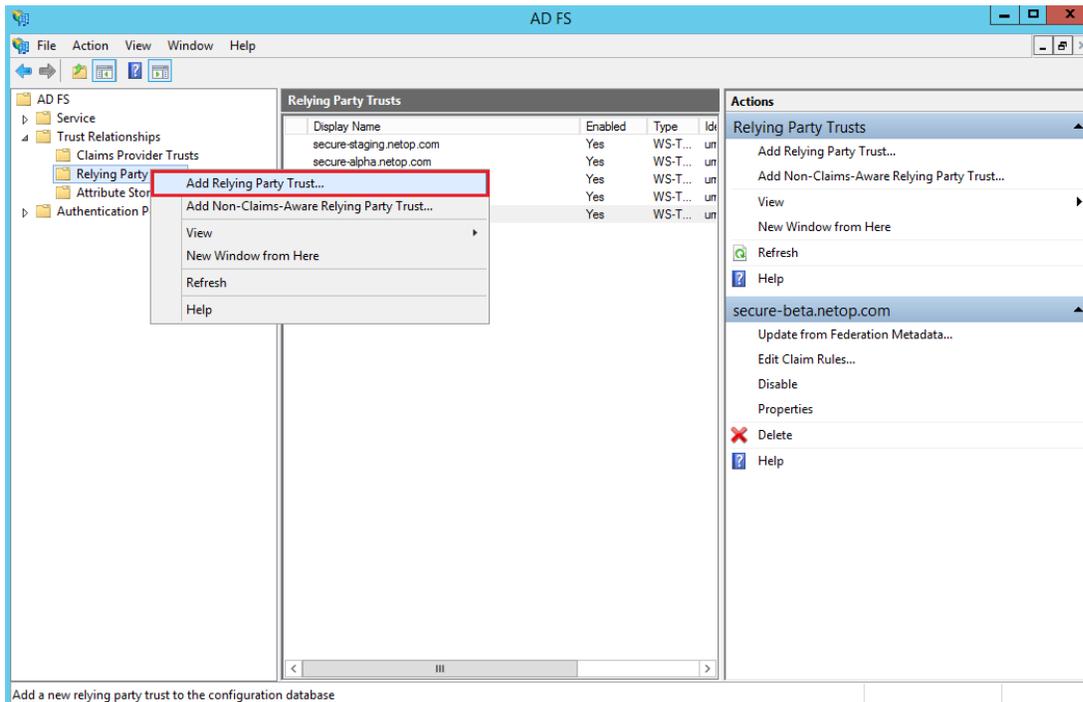


3. Go to **Trust Relationships**.

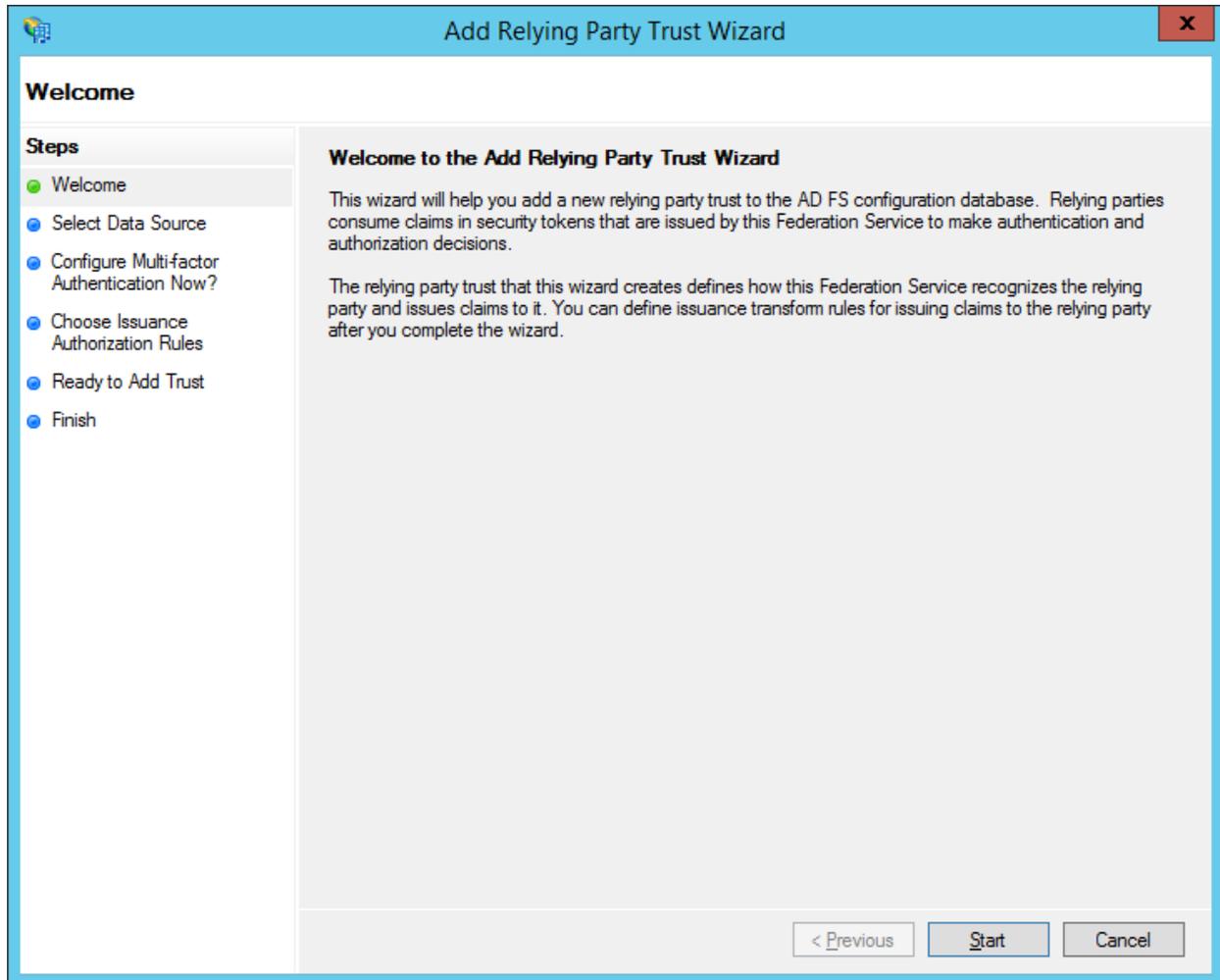
4. Right-click on **Relying Party Trust**.



5. Select the **Add Relying Party Trust** option. The Add Relying Party Trust Wizard is displayed.



6. Click on **Start**.

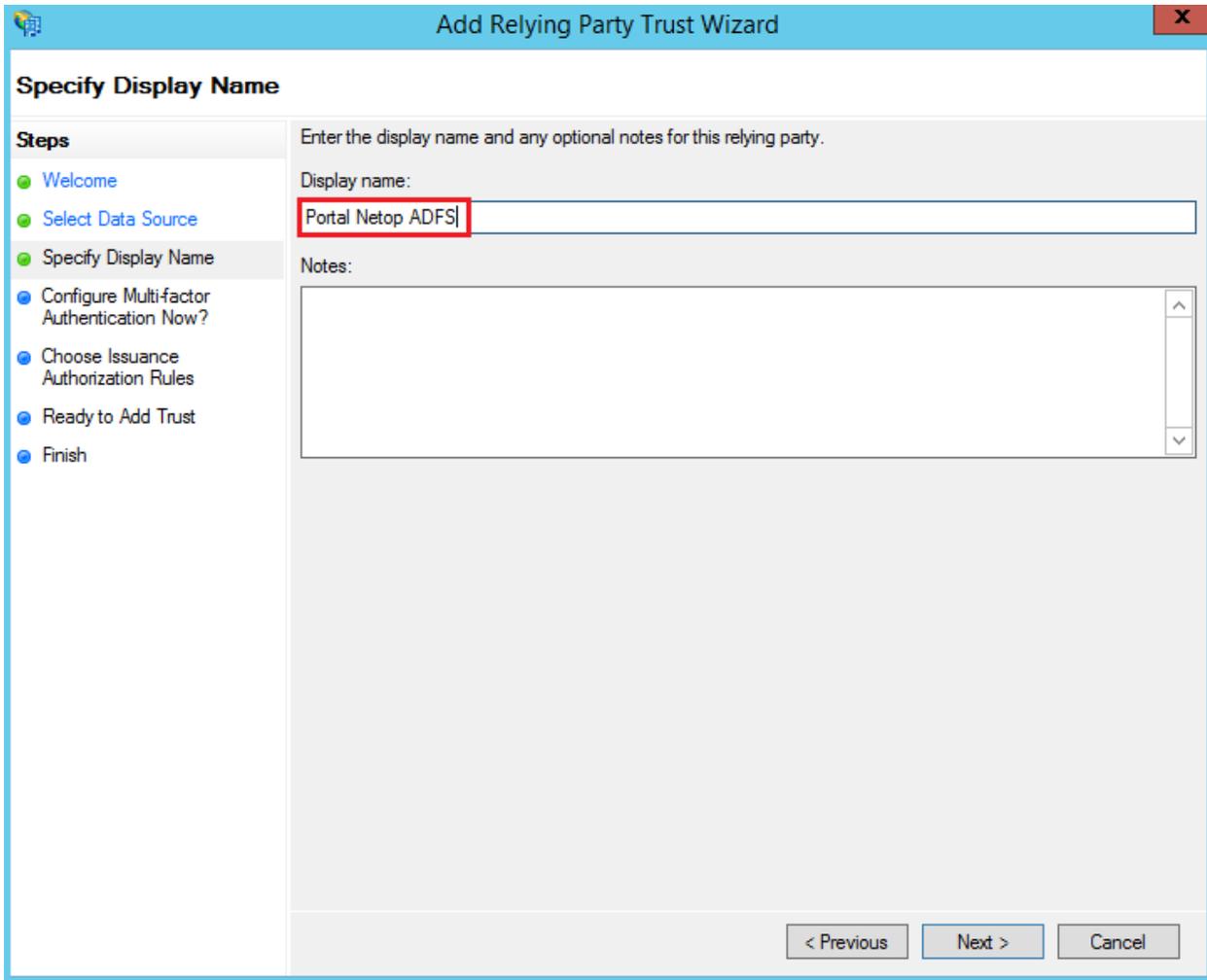


7. Select the **Import data about the relying party published online or on a local network** option.
8. In the Federation metadata address (host name or URL specify the following: <https://secure.netop.com/saml/metadata.xml>). The XML metadata file is a standard SAML metadata document that describes the **Netop Portal** as a relying party.

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The main area is titled "Select Data Source". On the left, a "Steps" pane lists the wizard's progress: "Welcome" (completed), "Select Data Source" (current step), "Configure Multi-factor Authentication Now?", "Choose Issuance Authorization Rules", "Ready to Add Trust", and "Finish". The main content area contains the instruction "Select an option that this wizard will use to obtain data about this relying party:" followed by three radio button options. The first option, "Import data about the relying party published online or on a local network", is selected. Below it, a text box contains the URL "https://secure.netop.com/saml/metadata.xml" and an example "Example: fs.contoso.com or https://www.contoso.com/app". The second option is "Import data about the relying party from a file", with a text box for the file location and a "Browse..." button. The third option is "Enter data about the relying party manually". At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

9. Click on **Next**.

10. In the display name field, specify the **Display name** for the relying Party.



11. Click on **Next**.

12. Select the **I do not want to configure...** option.

Add Relying Party Trust Wizard

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

I do not want to configure multi-factor authentication settings for this relying party trust at this time.

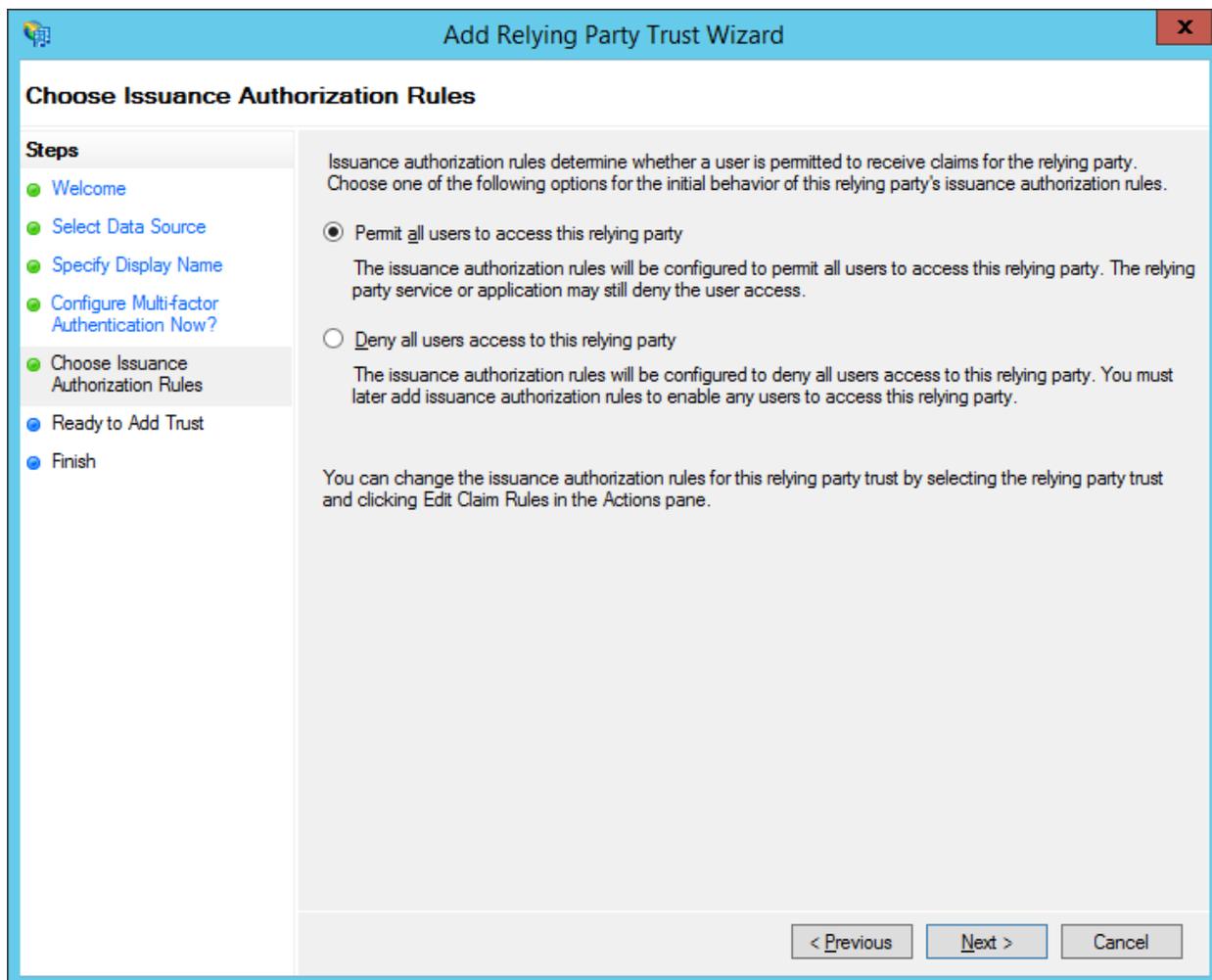
Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the [Authentication Policies](#) node. For more information, see [Configuring Authentication Policies](#).

< Previous Next > Cancel

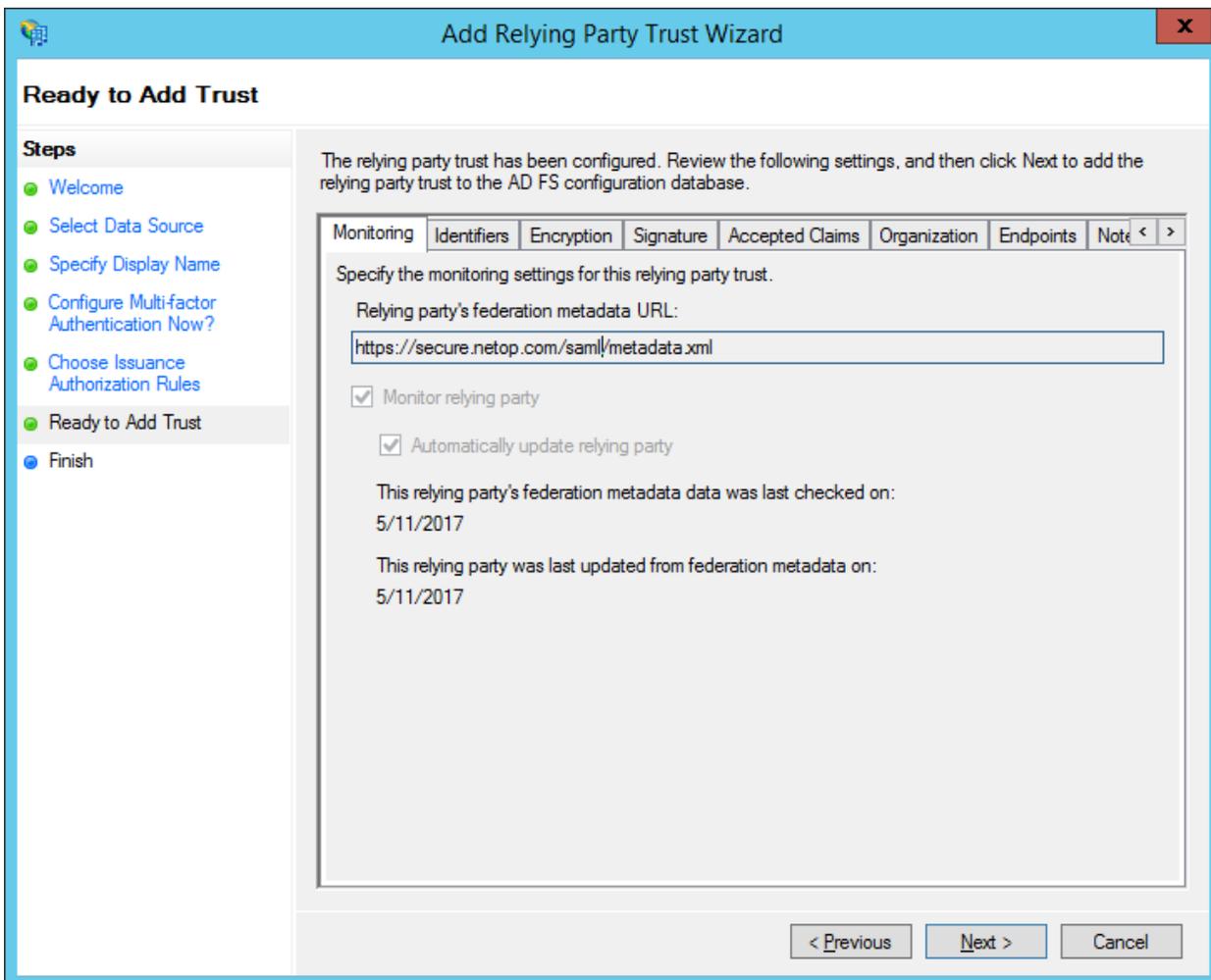
13. Click on **Next**.

14. Select the **Permit all users to access this relying party** option.

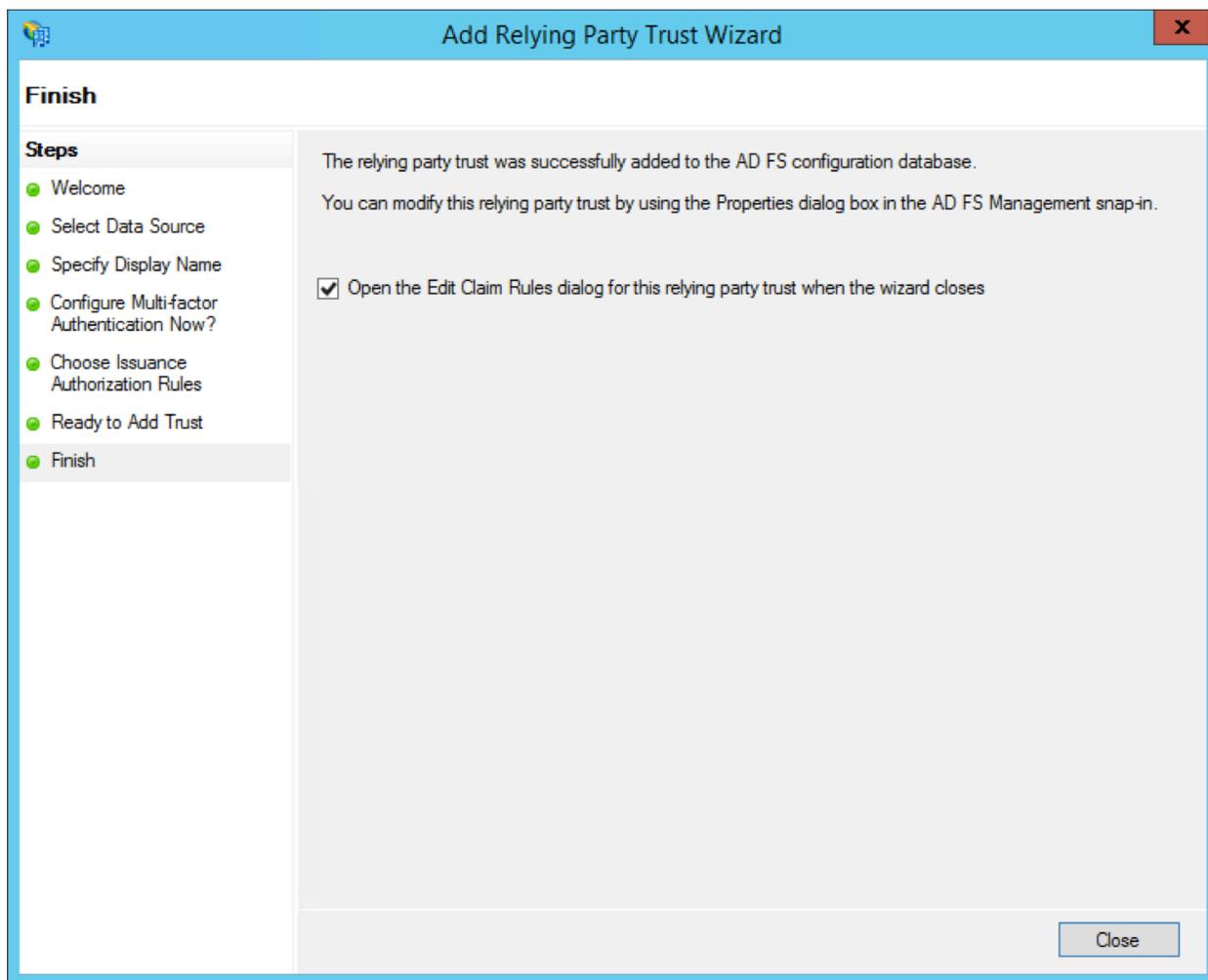


15. Click on **Next**.

16. Review your settings and click on **Next**.



17. Select the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** checkbox.



18. Click on **Close** to finalize the setup. The Netop Portal is added as a relying party.

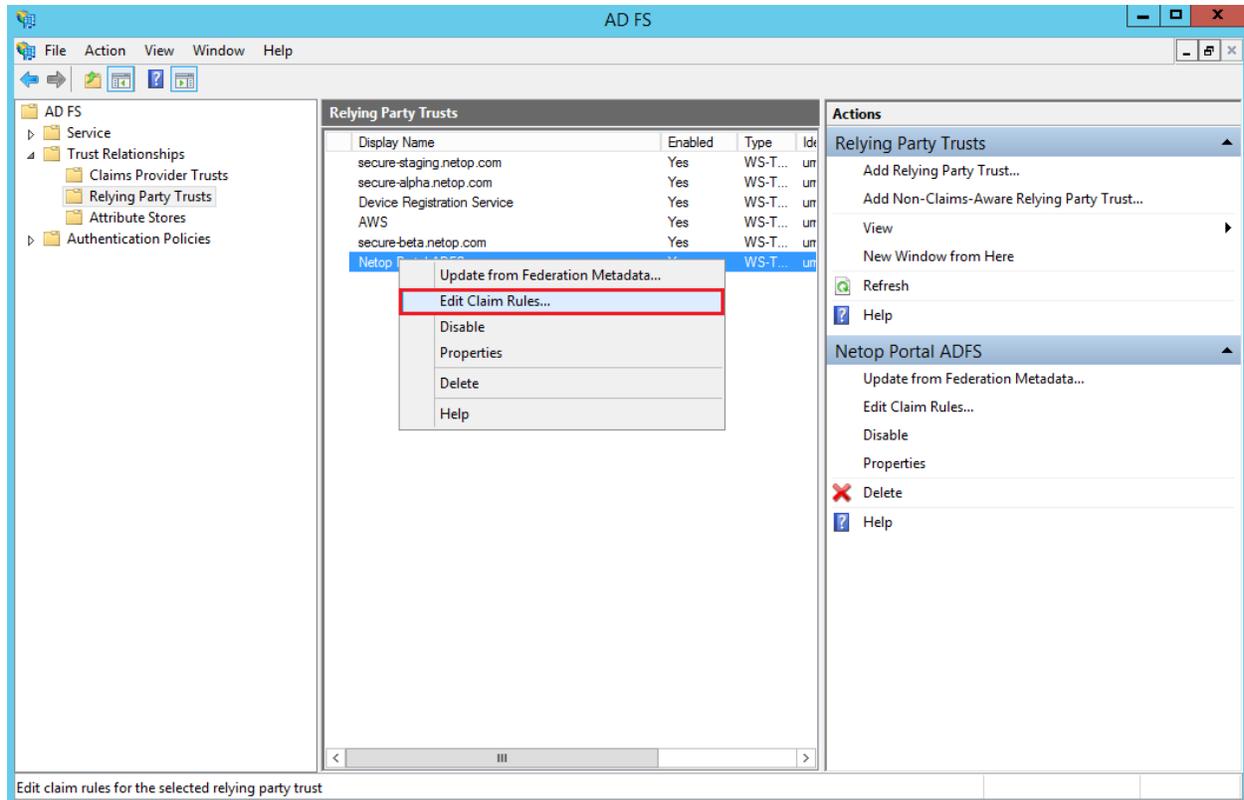
Add Claim Rules for the Netop Portal Relying Party

It is necessary that you add the Claim Rules so that the elements that the **Netop Portal** requires, which the ADFS does not provide them by default (NameId, AccountId, Email, First name and Principal name), are added to the SAML authentication response.

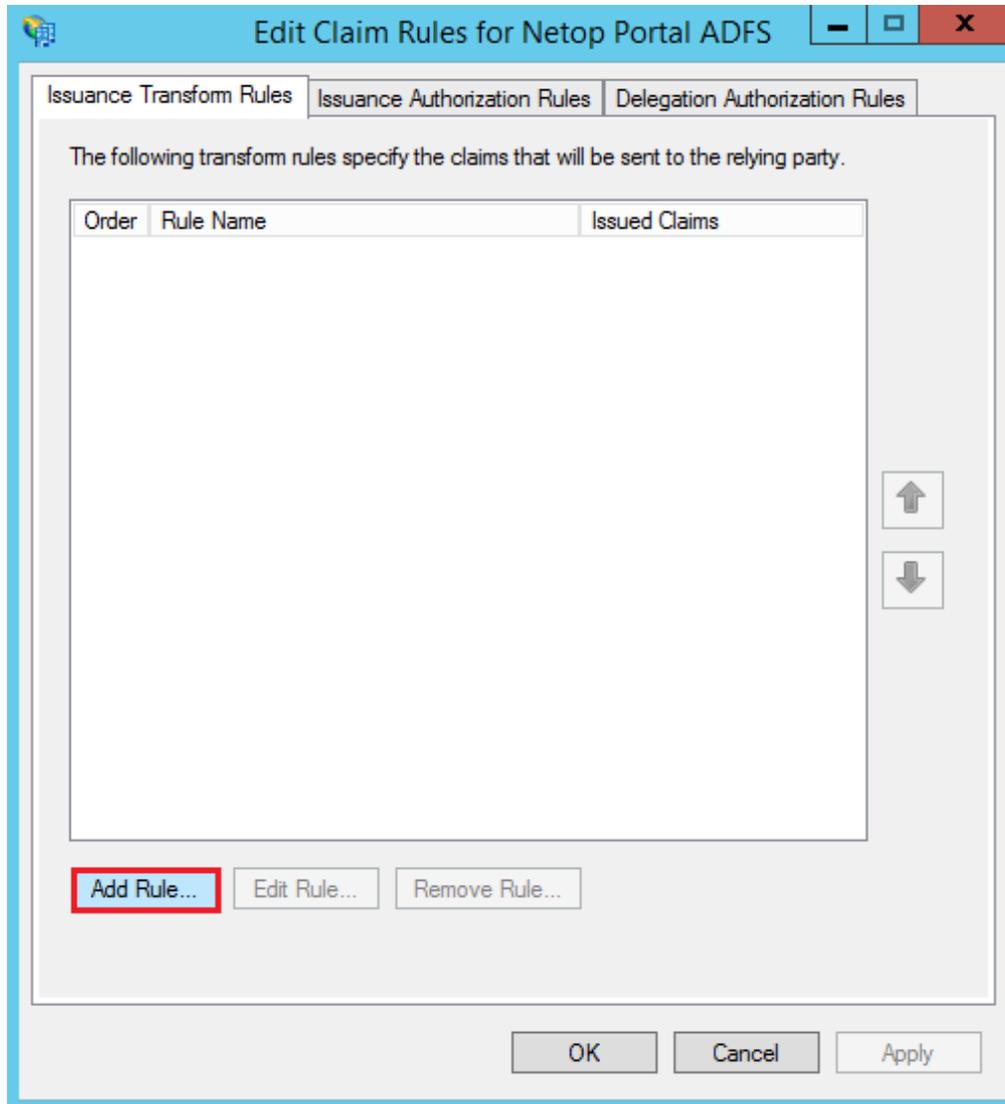
To add the Claim Rules, proceed as follows:

1. Right-click on the relying party (in this case Netop Portal ADFS).

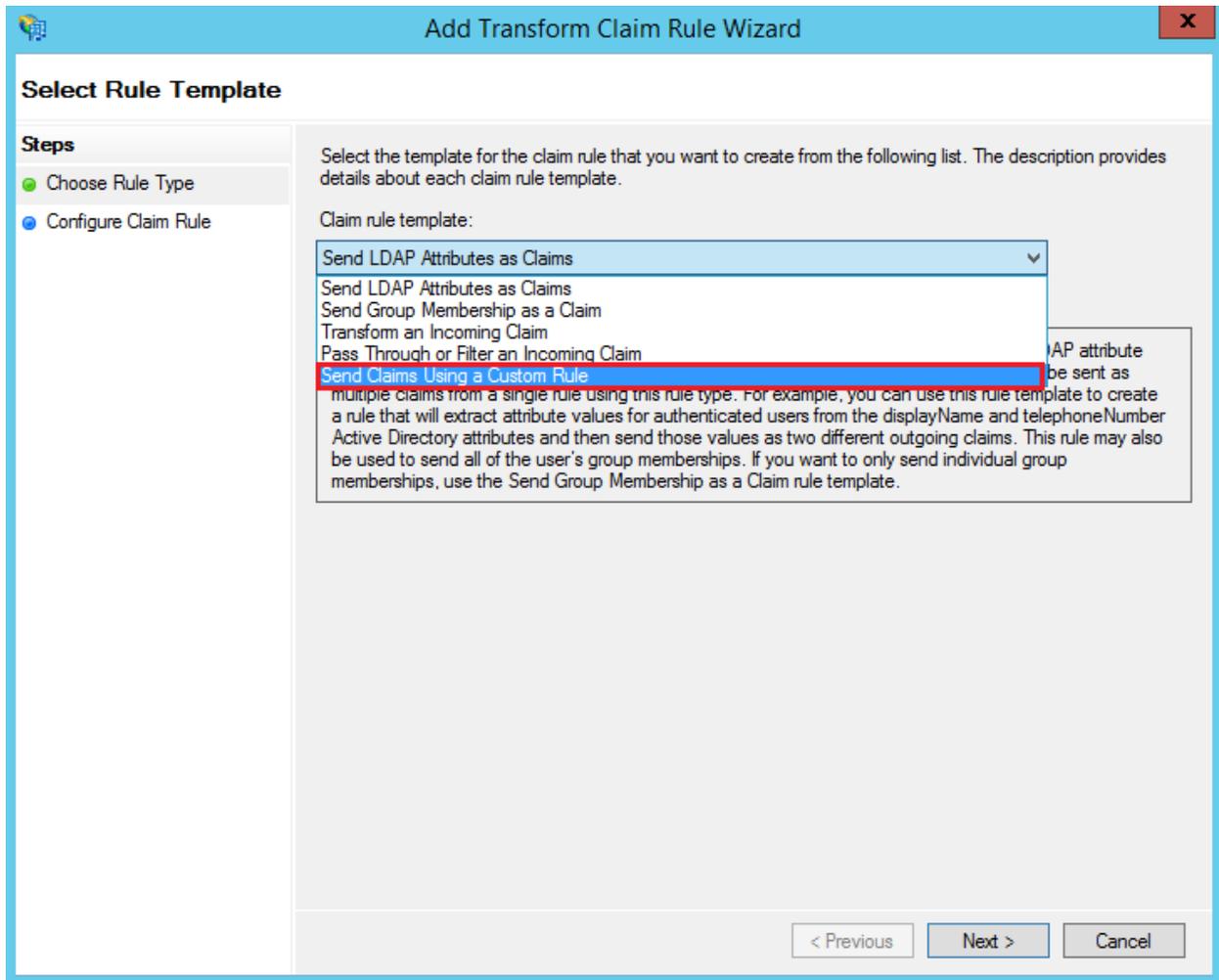
2. Select the **Edit Claim Rules** option.



3. In the **Edit Claim Rules for <relying party>** dialog box, click on the **Add Rule** button.



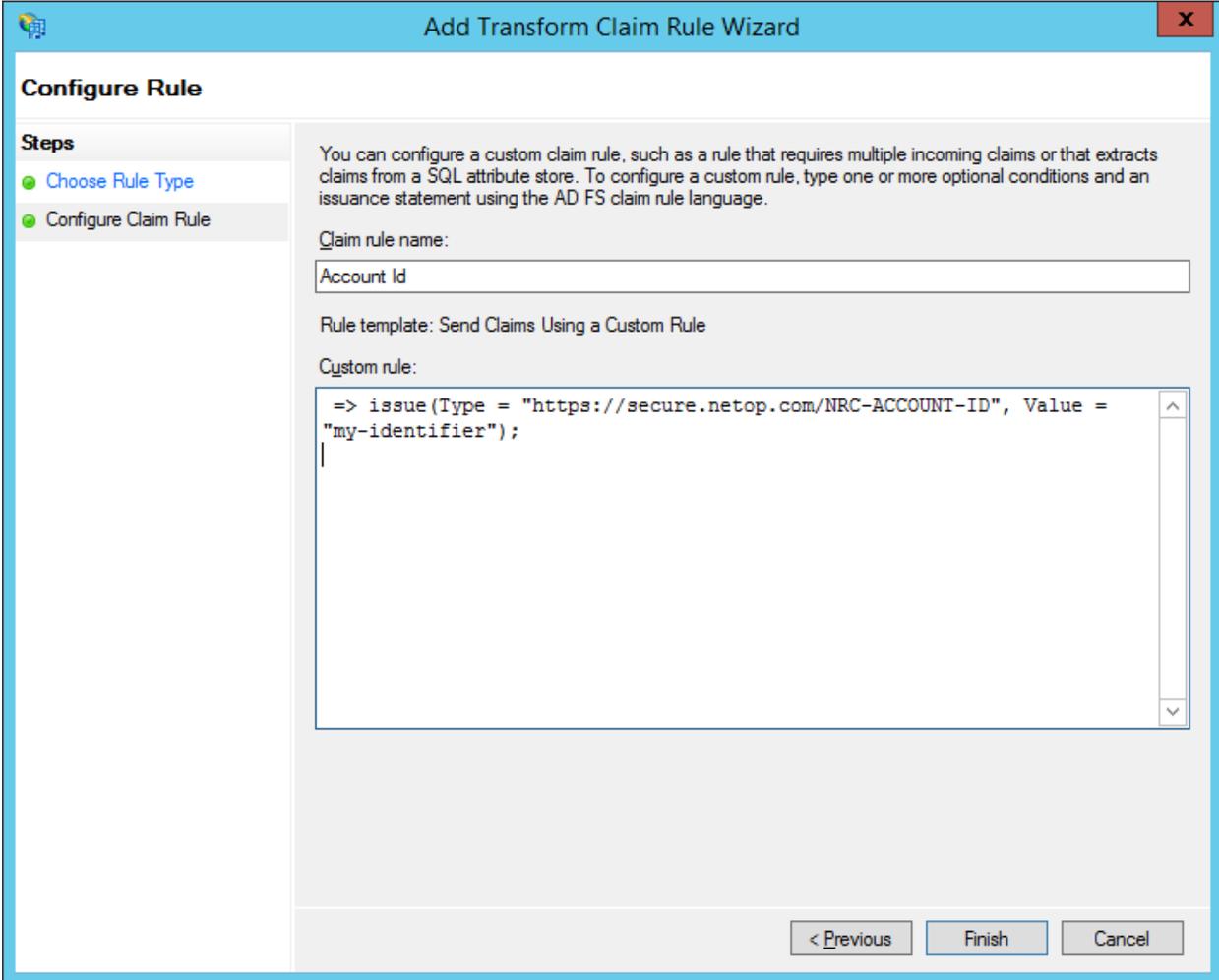
4. Select **Send Claims Using a Custom Rule** option from the **Claim rule template** drop-down menu.



5. Specify the following values:

- **Claim rule name:** Account Id
- **Custom rule:** => issue(Type = "https://secure.netop.com/NRC-ACCOUNT-ID", Value = "<Account identifier>");

Make sure that you replace the <Account identifier> with the account identifier that you use in the **Netop Portal** (in this example, the “my-identifier”) is used as the account identifier.



The screenshot shows a Windows-style dialog box titled "Add Transform Claim Rule Wizard" with a close button (X) in the top right corner. The main area is titled "Configure Rule". On the left, there is a "Steps" pane with two items: "Choose Rule Type" (indicated by a green dot) and "Configure Claim Rule" (indicated by a green dot and highlighted). The main content area contains the following text and fields:

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

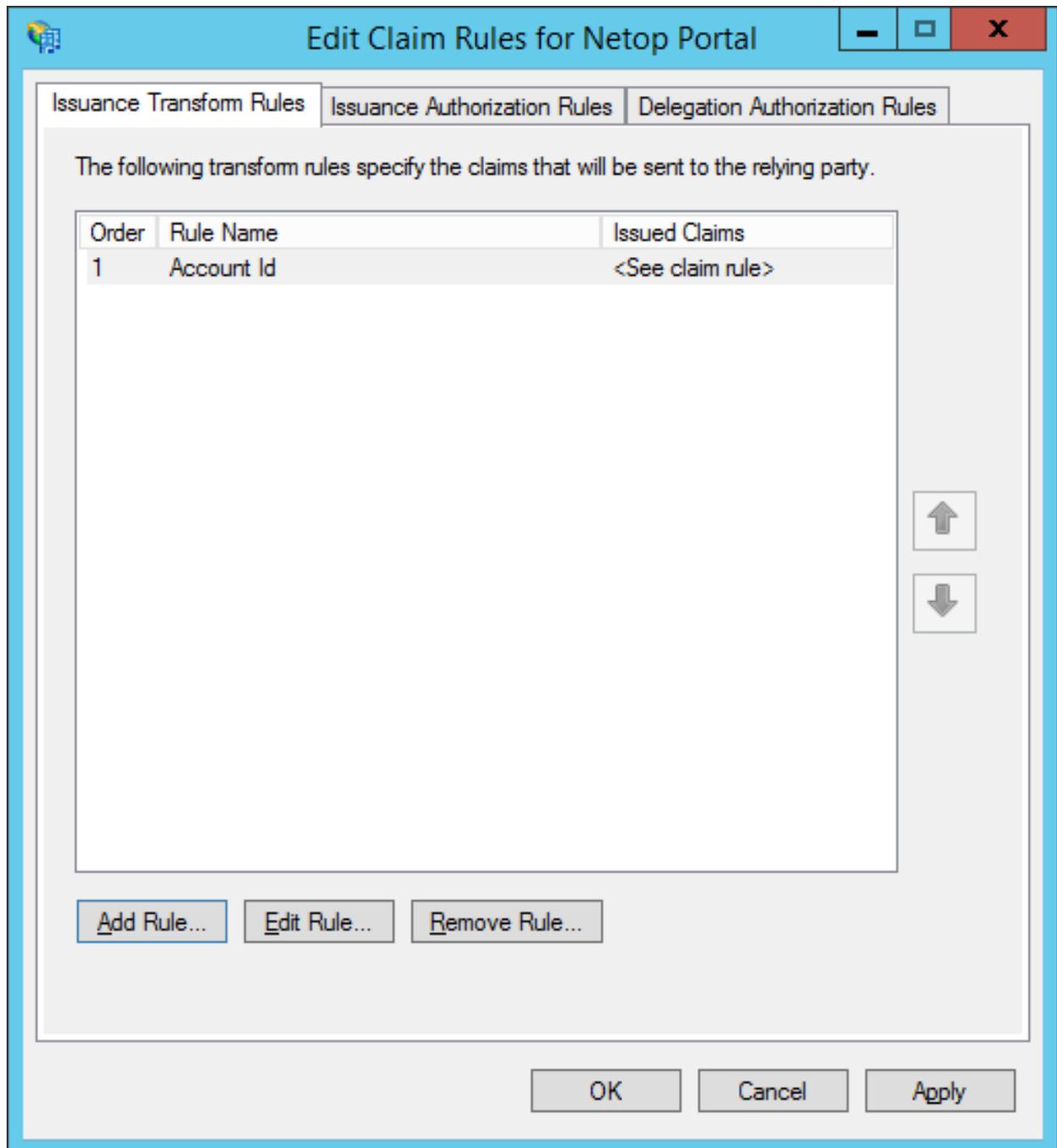
Rule template: Send Claims Using a Custom Rule

Custom rule:

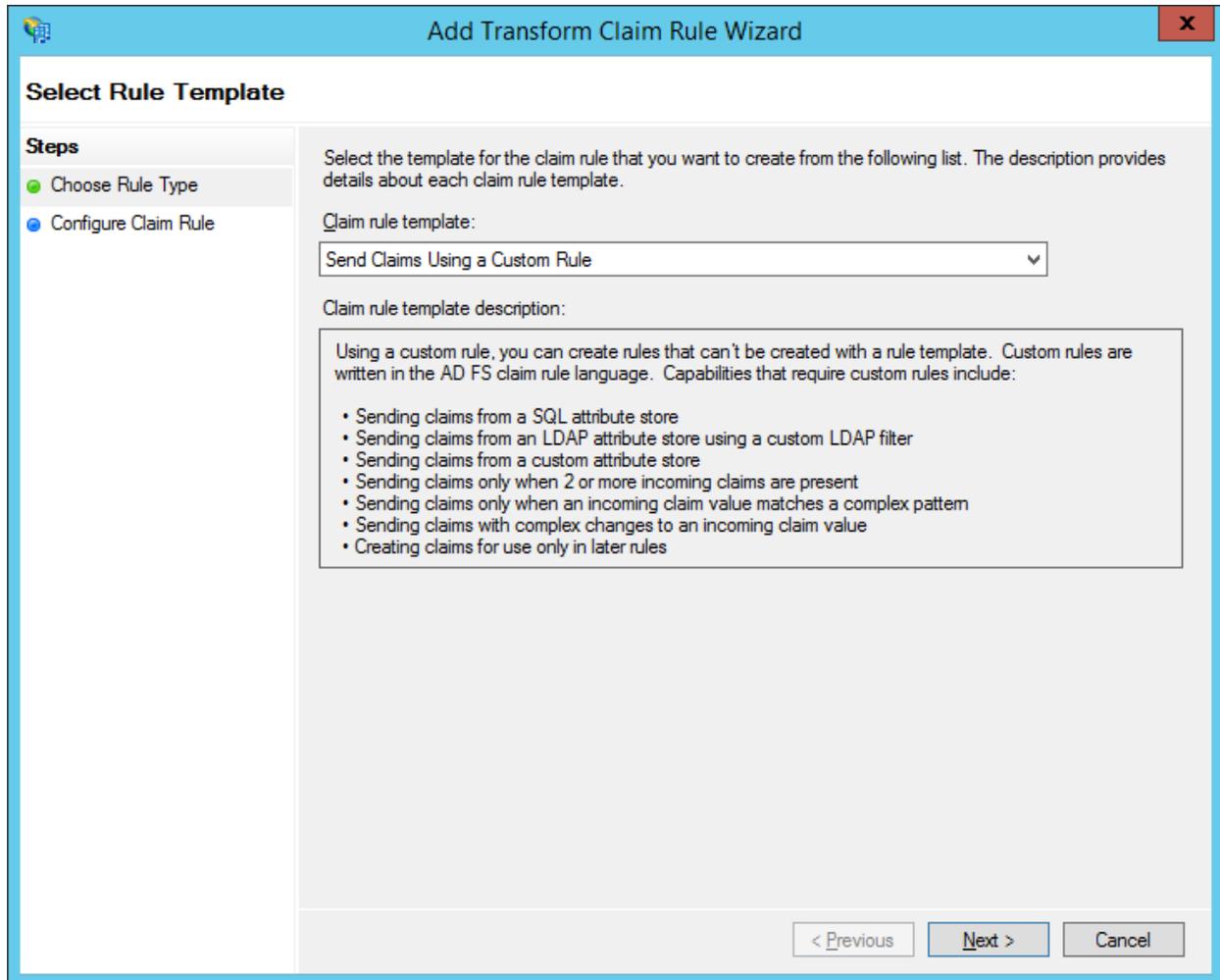
At the bottom right, there are three buttons: "< Previous", "Finish", and "Cancel".

6. Click on **Finish**.

7. In the **Edit Claim Rules for <relying party>** dialog box, click on the **Add Rule** button.



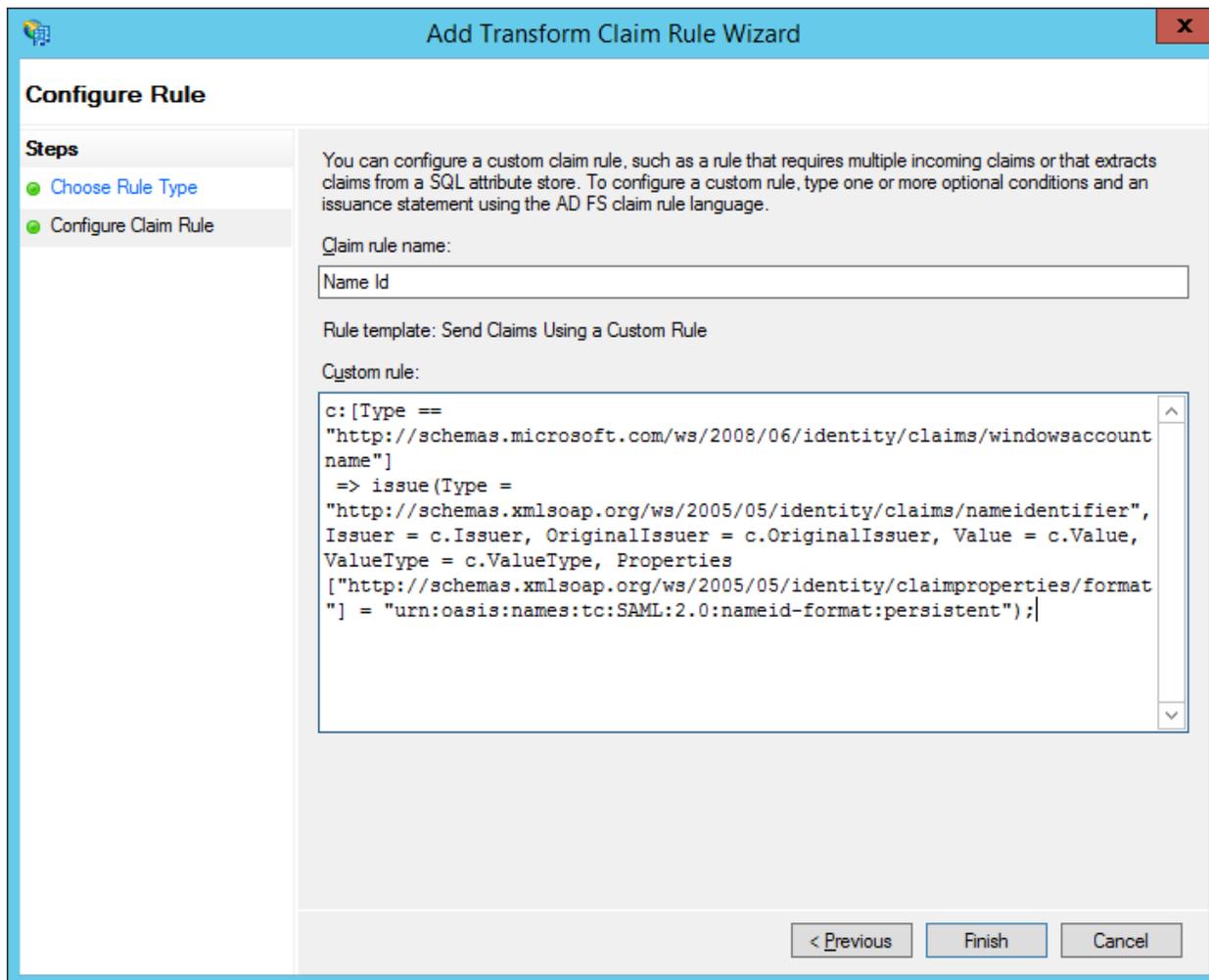
8. Select **Send Claims Using a Custom Rule** option from the Claim rule template drop-down menu.



9. Specify the following values:
- **Claim rule name:** Name Id
 - **Custom rule:**

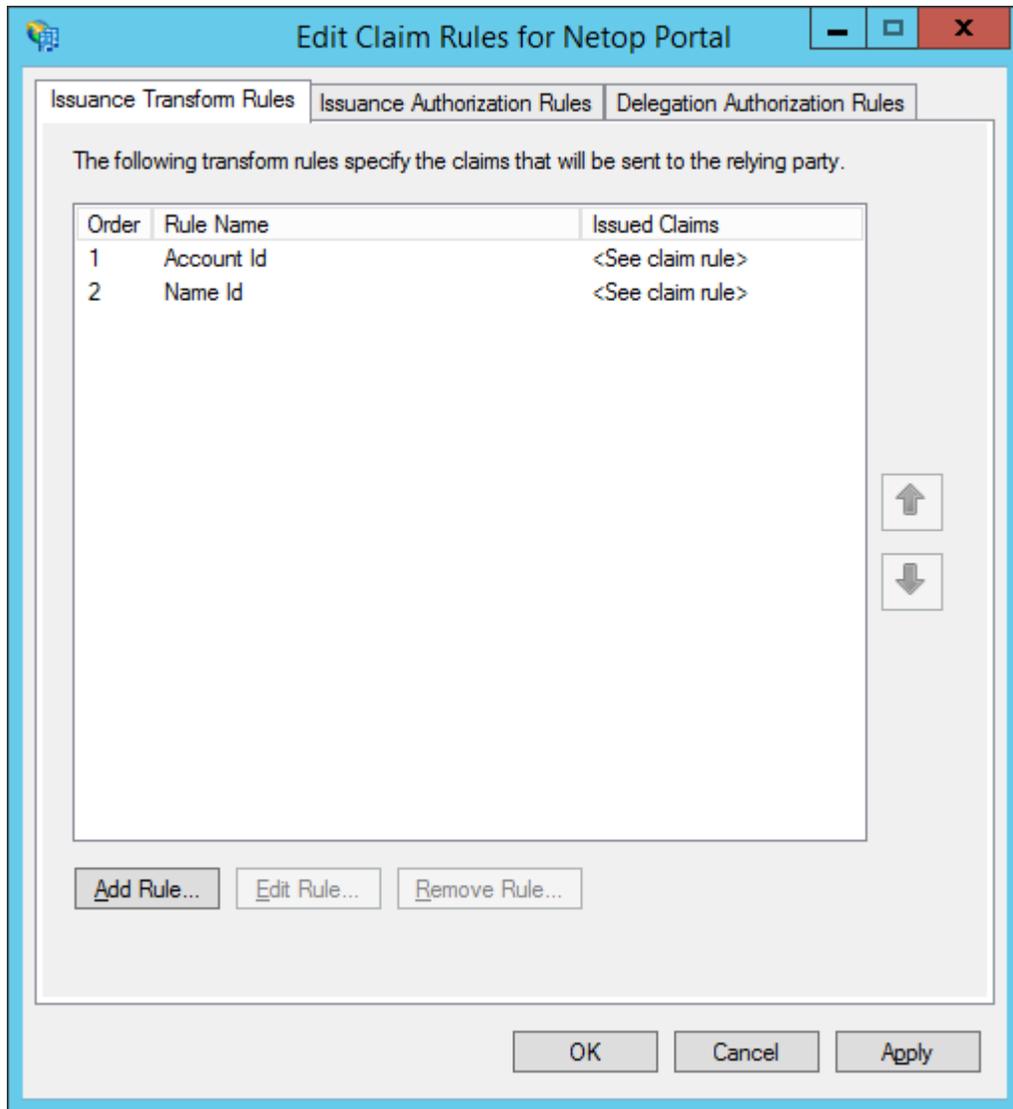
```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname  
"]  
  
=> issue(Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",  
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,  
ValueType = c.ValueType,
```

```
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent");
```

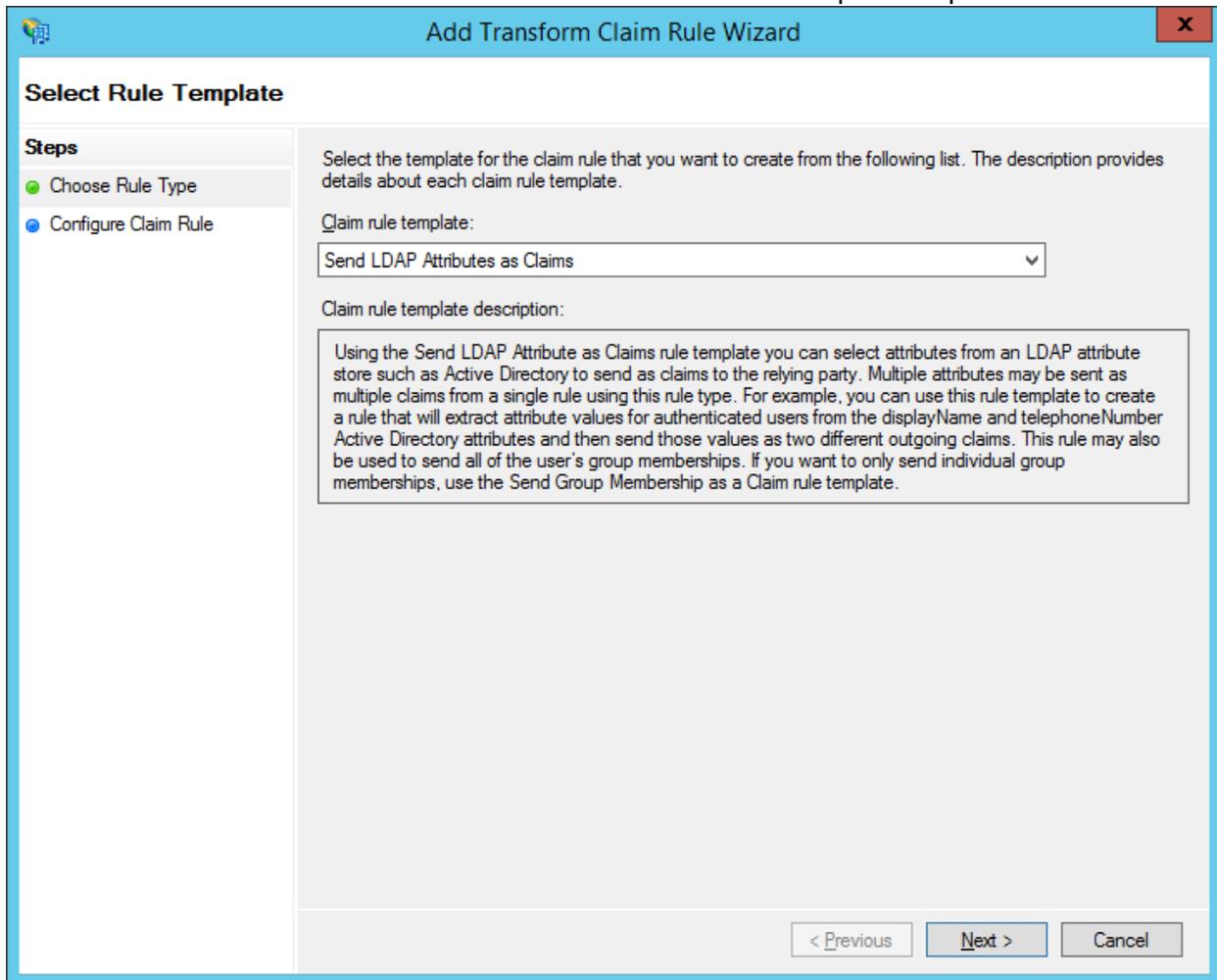


10. Click on Finish.

11. In the **Edit Claim Rules for <relying party>** dialog box, click on **Add Rule**.



12. Select **Send LDAP Attributes as Claims** from the Claim rule template drop-down menu.



13. Specify the following values.

- **Claim rule name:** User details
- **Attribute store:** Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP attribute	Outgoing Claim Type
E-Mail-Addresses	https://secure.netop.com/NRC-EMAIL
Given-Name	https://secure.netop.com/NRC-GIVEN-NAME
Surname	https://secure.netop.com/NRC-SURNAME
User-Principal-Name	https://secure.netop.com/NRC-USERNAME

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- **Configure Claim Rule**

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: User details

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

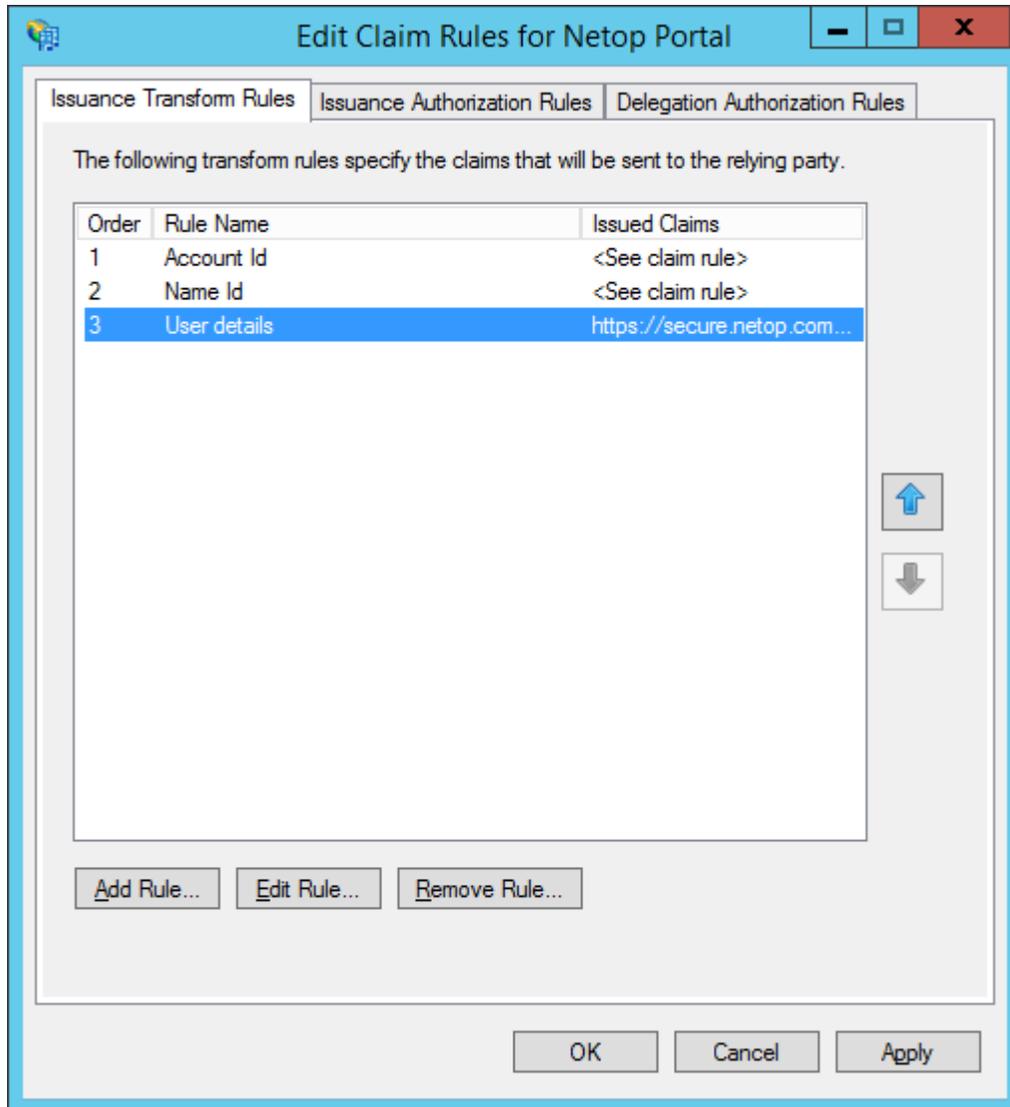
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	https://secure.netop.com/NRC-EMAIL
	Given-Name	https://secure.netop.com/NRC-GIVEN-NAME
	Surname	https://secure.netop.com/NRC-SURNAME
▶	User-Principal-Name	https://secure.netop.com/NRC-USERNAME
*		

< Previous Finish Cancel

14. Click on **Finish**.

15. Click on **OK**.



16. You finished with the necessary configuration on the ADFS server.

Configure the Netop Portal

To configure the ADFS integration with the Netop Portal, proceed as follows:

1. Sign in the **Netop Portal** with an Account administrator type of user.
2. Go to **Dashboard**.
3. Go to **Authentication**.
4. Click on the **Add ADFS / Azure AD** button.
5. Specify a name for the Authentication type.
6. Toggle the **Enable** button, to enable or disable the authentication type. By default, it is set to **Enable**.
7. In the Domain Identifier field, specify the same value that you used in creating the Account Claim rule.
8. In the **IdP** entry field, specify the Identity Provider's (IdP) URL. This is the ADFS URL used for authenticating the user.

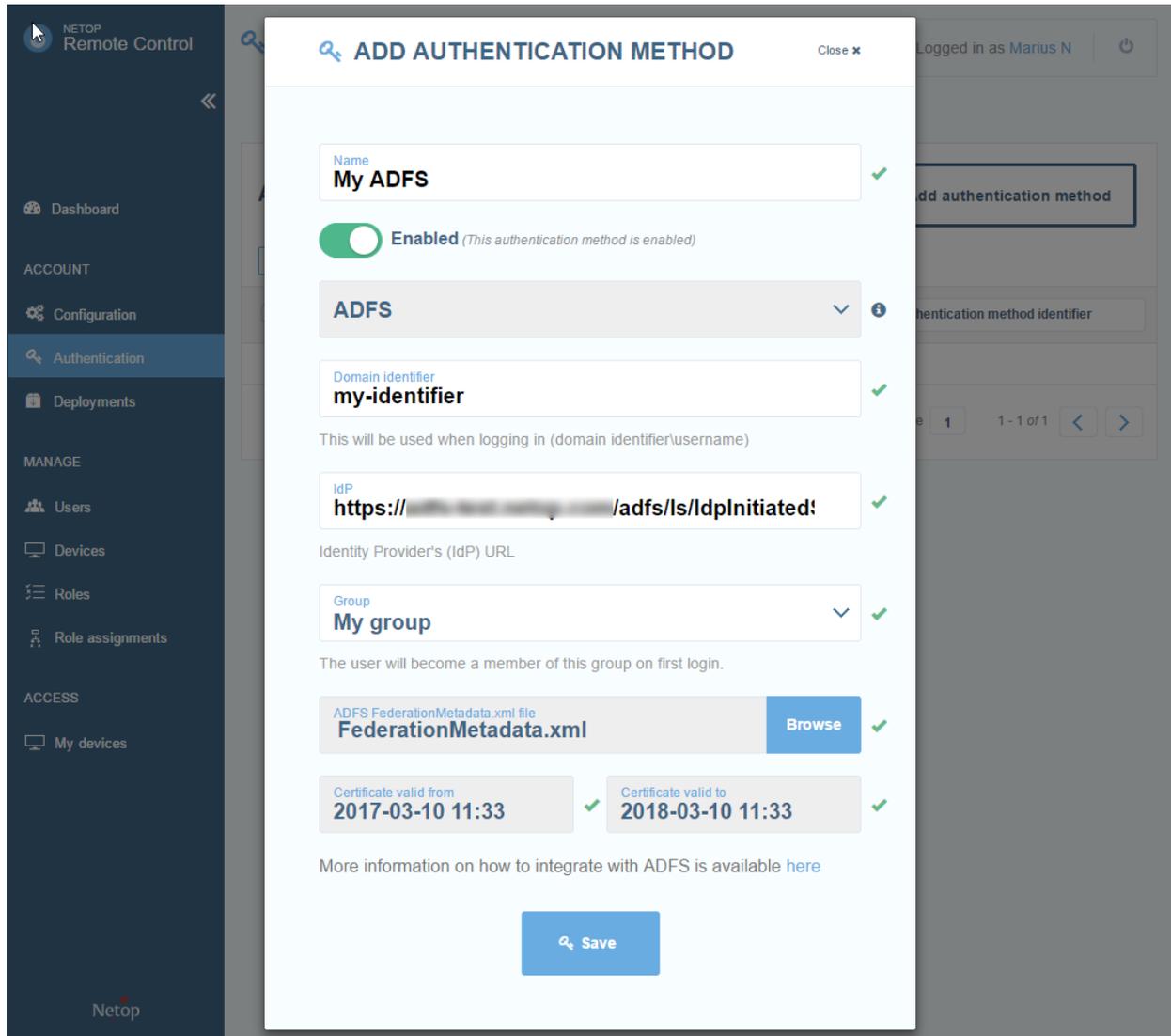
NOTE: The default value is

`https://somedomain.com/adfs/ls/IdpInitiatedSignOn.aspx.`

9. Specify a group for the authentication. This is an optional step.

10. Browse for the ADFS FederationMetadata.xml file. The ADFS FederationMetadata.xml file is specific to ADFS based on the various settings. It can generally be retrieved from <https://somedomain.com/FederationMetadata/2007-06/FederationMetadata.xml>.

NOTE: When uploading the FederationMetada.xml, the embedded certificate is parsed and its validity interval is displayed (Certificate valid from – Certificate valid to).



11. To save your modifications, click on **Save**.

Remote session using ADFS

Prerequisites:

- **Guest** and **Host** are version 12.60 or later
- Role assignments that are defined in the **Netop Portal** that allow ADFS based users to connect to the Host
- Make sure the **Host** is configured to **Use Netop Portal** access rights

Managing the ADFS users

On the first login using ADFS, a user gets created into the **Netop Portal**. The user type is **User**.

The screenshot displays the Netop Portal's 'USERS' management interface. The left sidebar contains navigation options: Dashboard, ACCOUNT (Configuration, Authentication, Deployments), MANAGE (Users, Devices, Roles, Role assignments), and ACCESS (My devices). The main content area shows a table of users. The table has columns for Name, Type, Group, Authentication method, and Modified. A single user is listed, highlighted with a red border:

Name	Type	Group	Authentication method	Modified
Some User (someuser@netop.com)	User	xxx	my adfs	2017-05-12 04:22:58

The new user works like a regular user, except:

- The user cannot change his password, first name, and email from the **Netop Portal**, which are synced with the ADFS server
- The user cannot be set as an Account owner
- The user cannot be used for the phonebook as predefined credentials