NETOP REMOTE CONTROL AZURE AD AND ADFS INTEGRATION

NETOP®

RemoteControl

Secure Remote Management and Support

April 28th, 2021

NETOP RemoteControl

Contents

Configure the authentication provider

Azure AD

Create the enterprise application in Azure AD

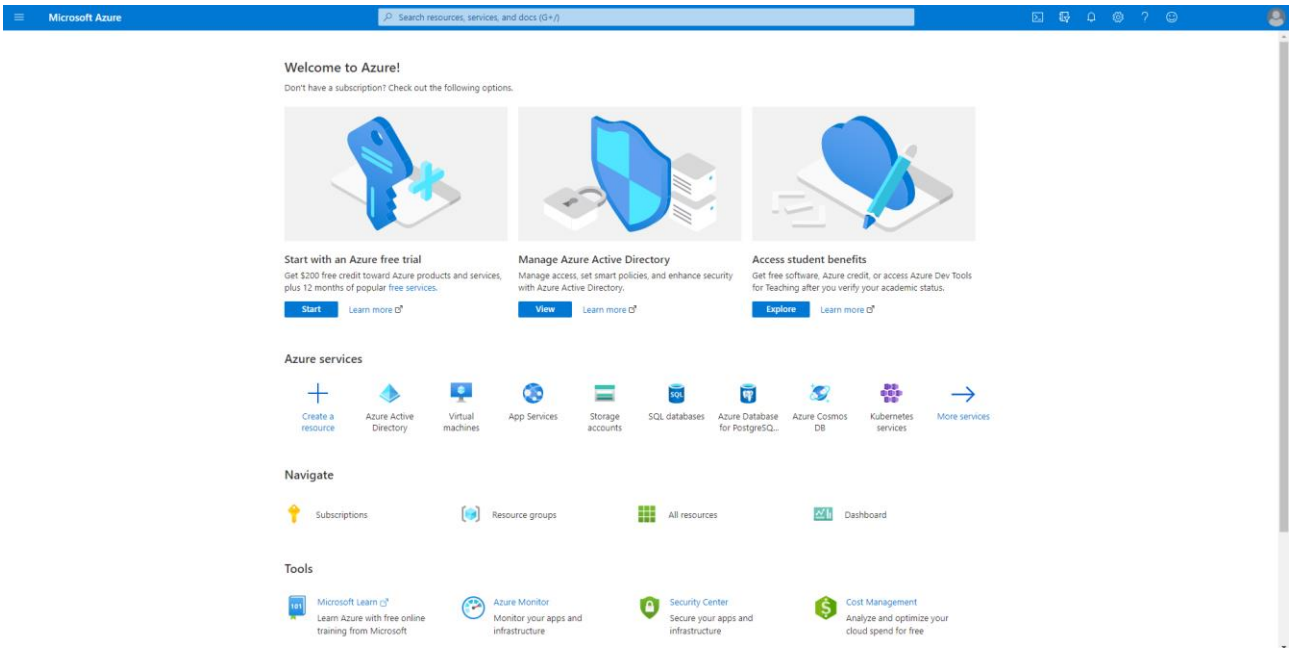
There are two methods of creating the enterprise application in Azure AD:

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

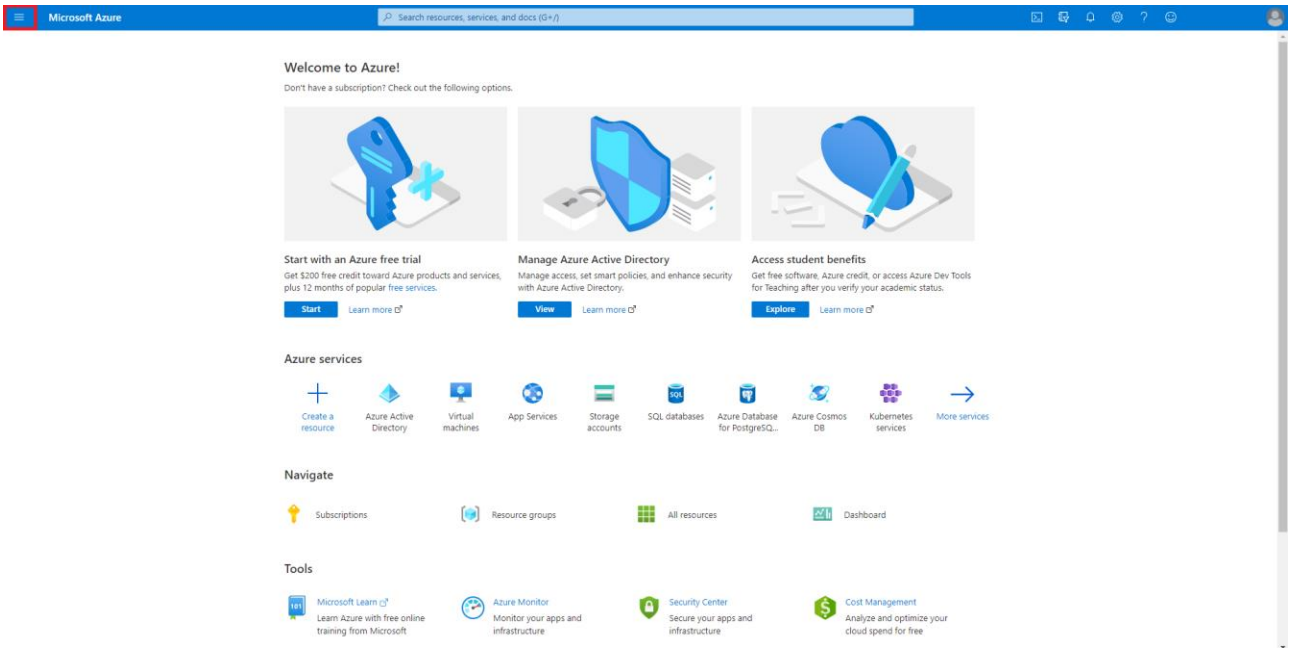
To create the **Netop Portal** application in **Azure AD**, proceed as follows:

1. Log in the Azure Portal.

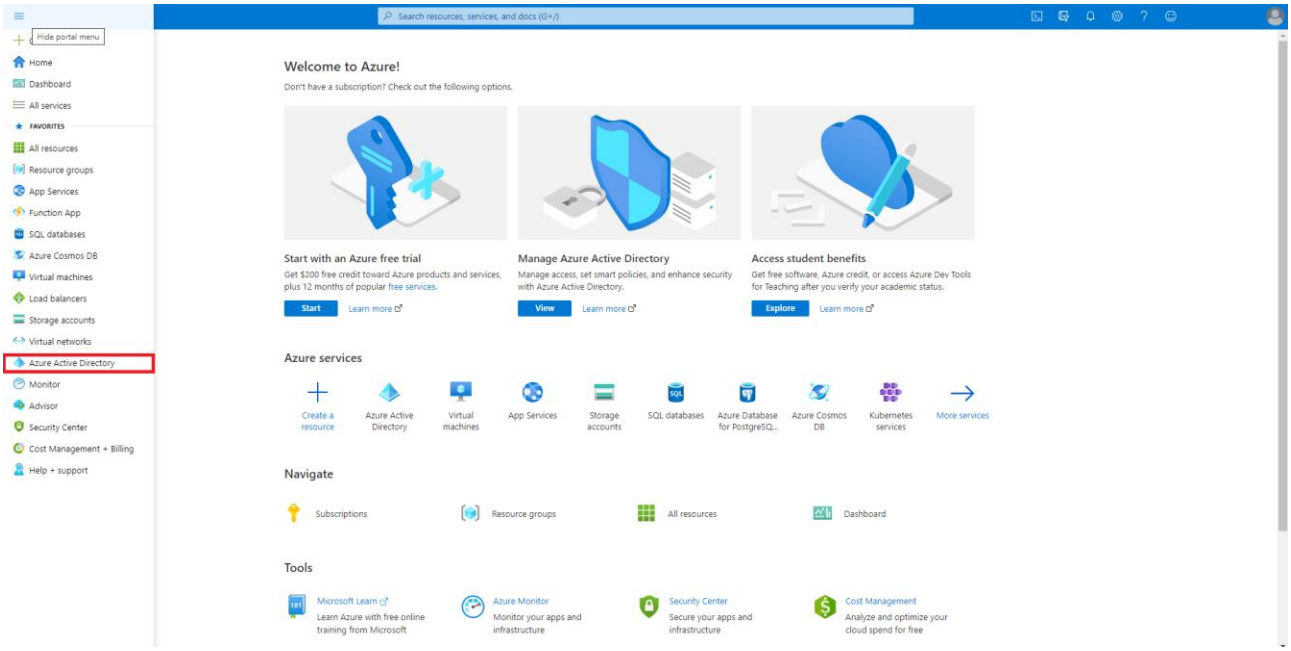


2. Go to **Azure Active Directory.**

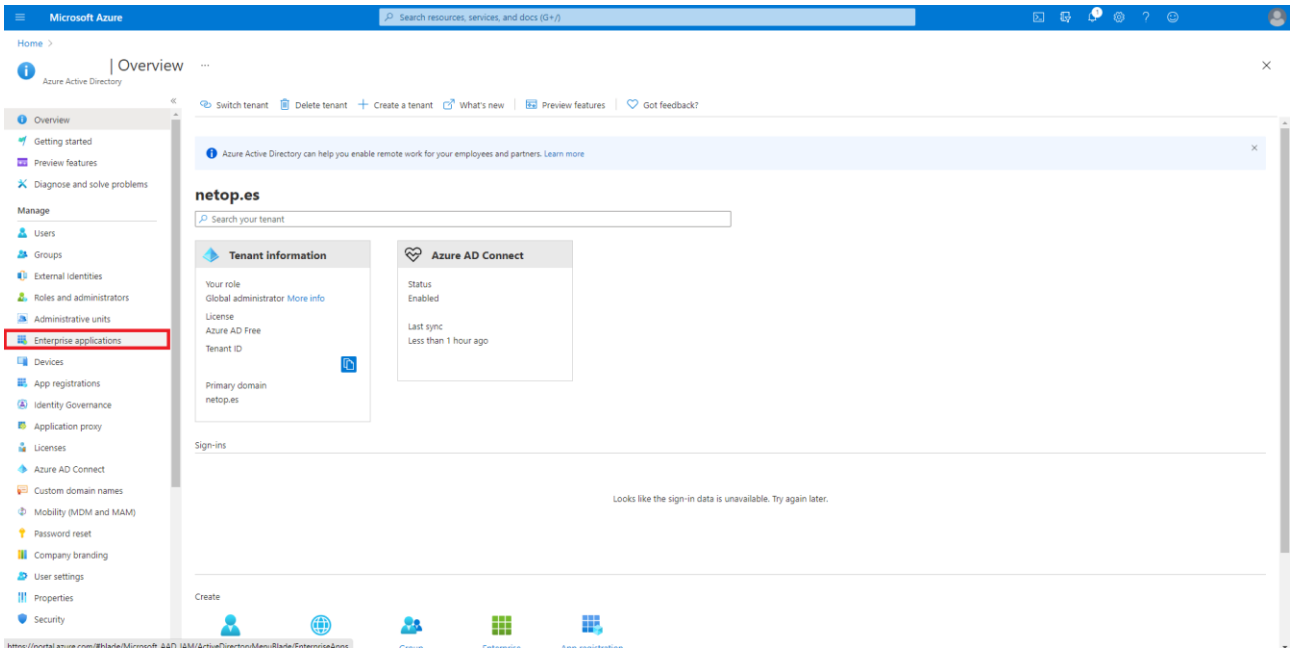
2.1. Click on the **More** button.



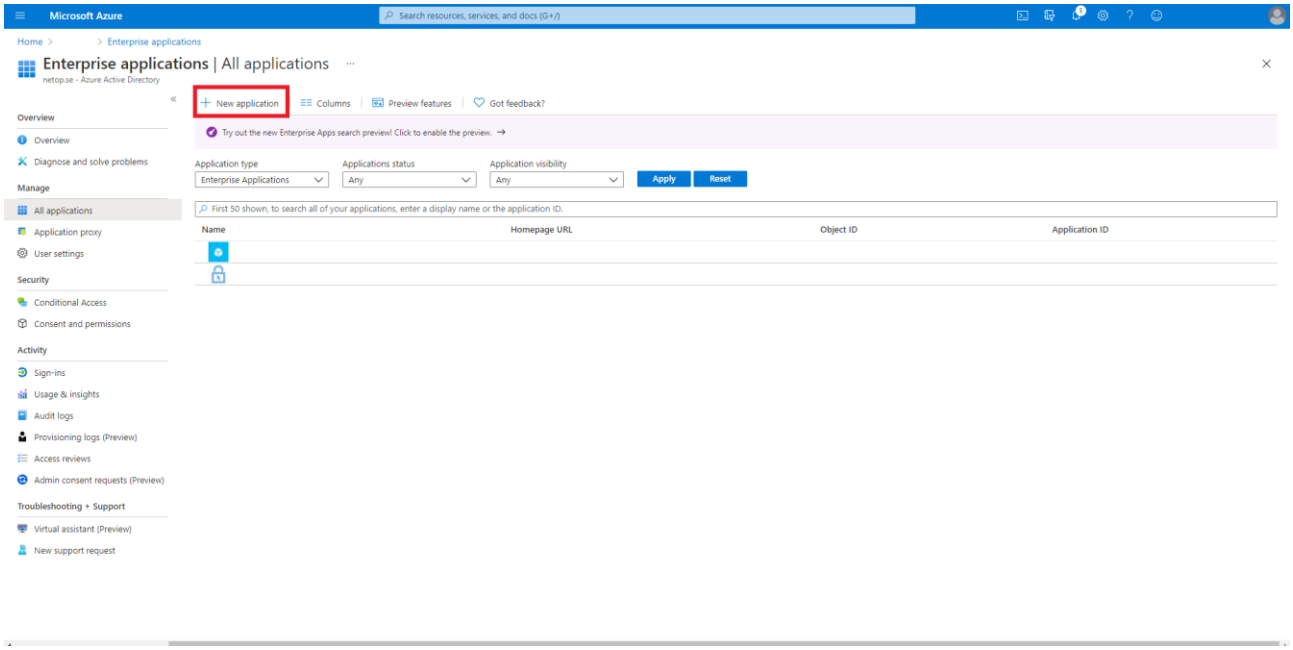
2.2. Click on **Azure Active Directory**.



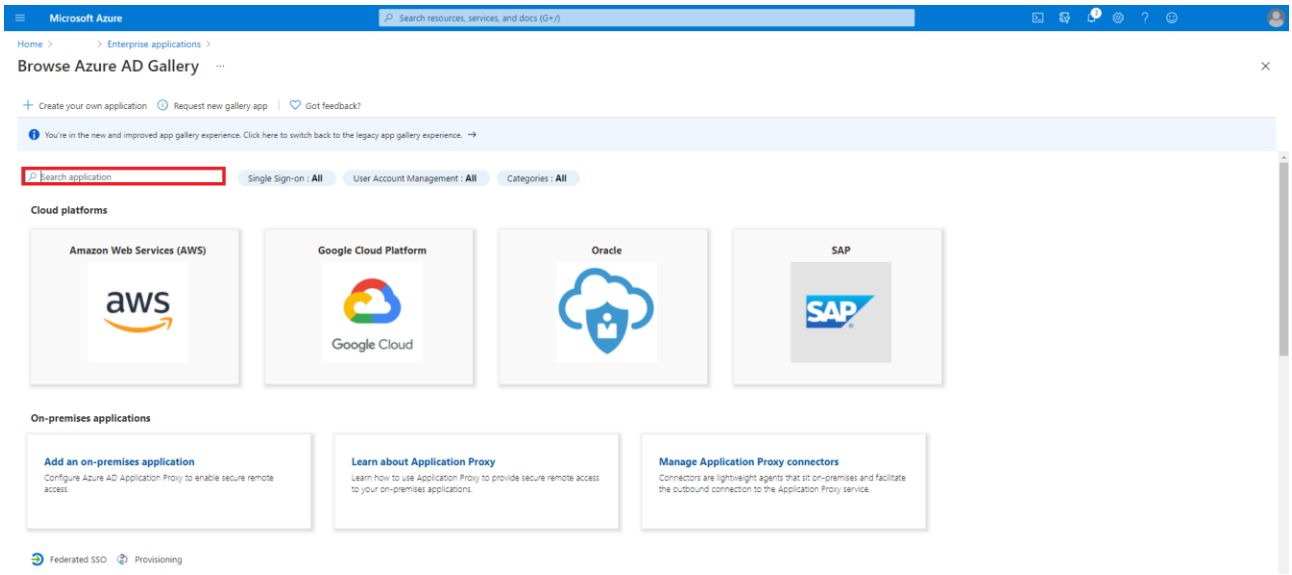
3. Go to **Enterprise applications.**



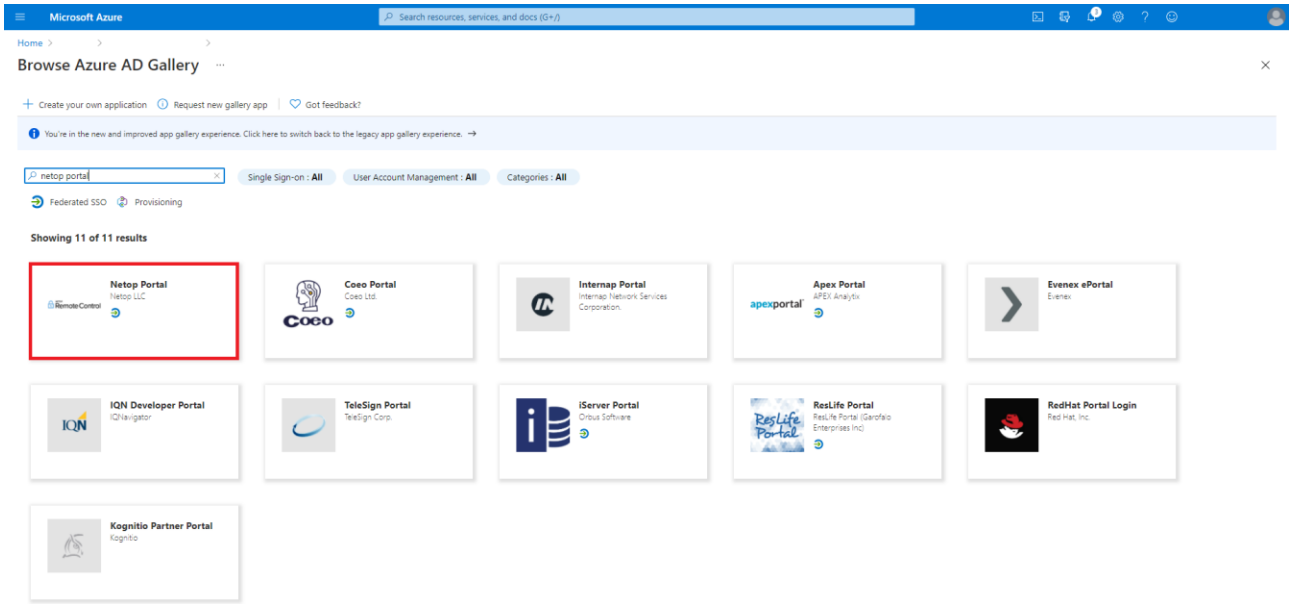
4. Click on the **New application** button.



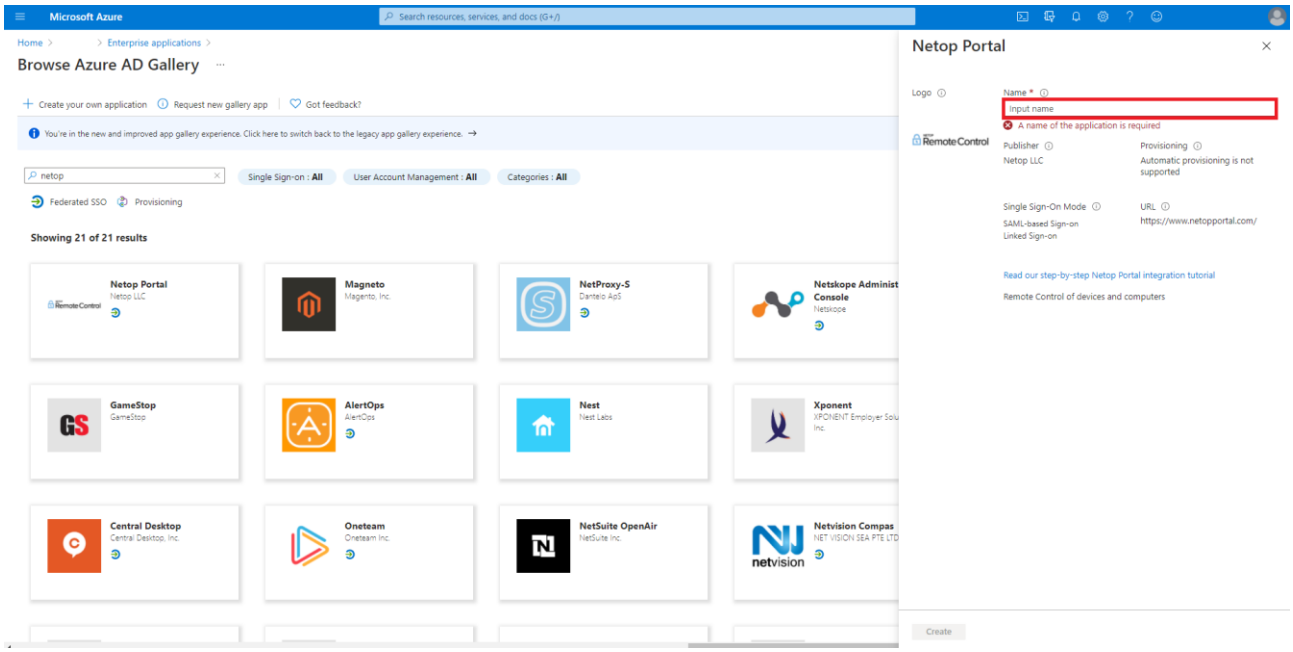
5. In the **Search application** entry field, specify **Netop Portal**.



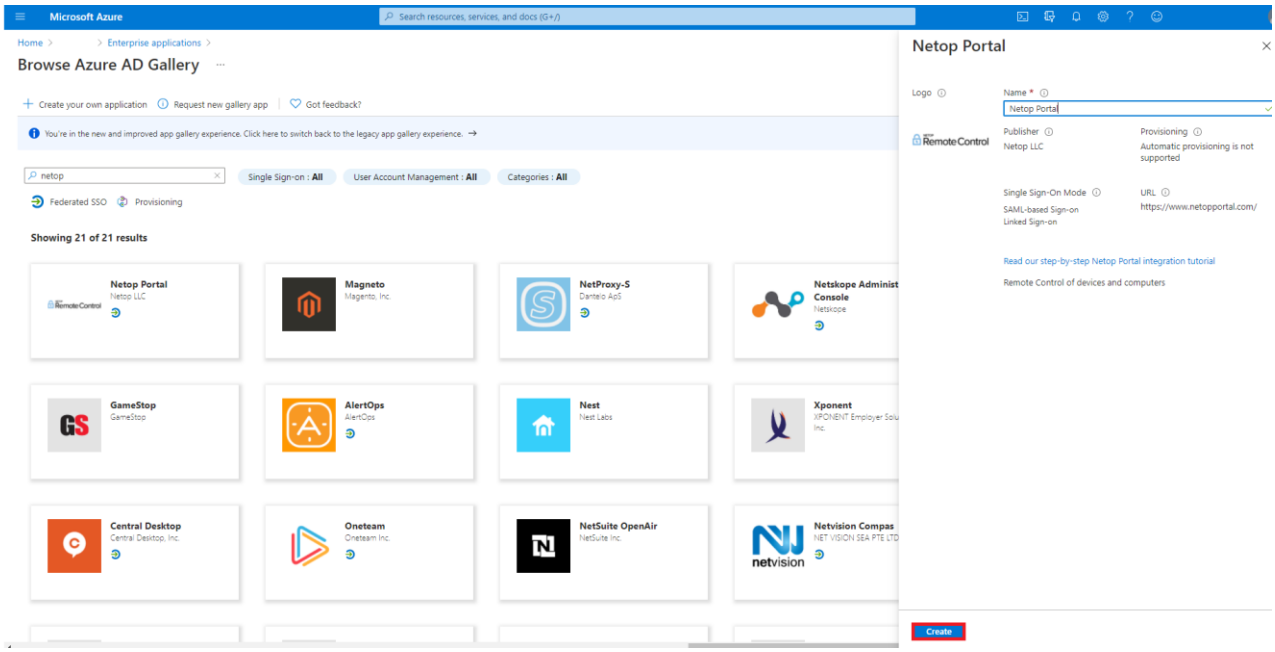
6. Click on the **Netop Portal** icon.



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**.



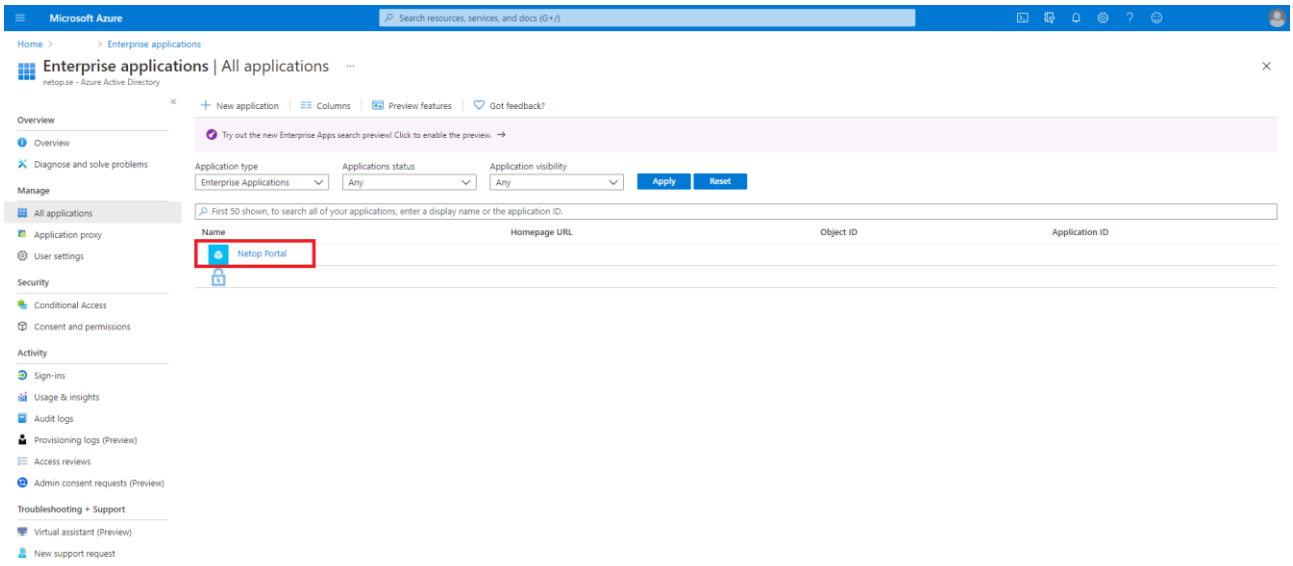
The application is created successfully and added to the **Enterprise applications** section.

Add users and groups to the application

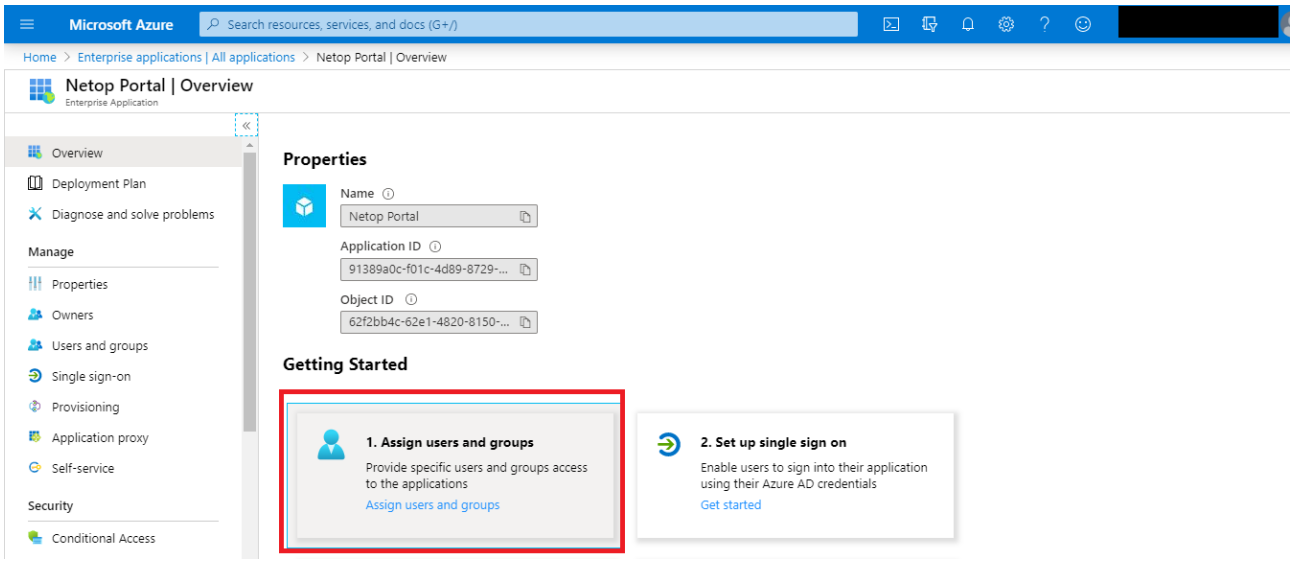
To add users and groups to the application, proceed as follows:

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

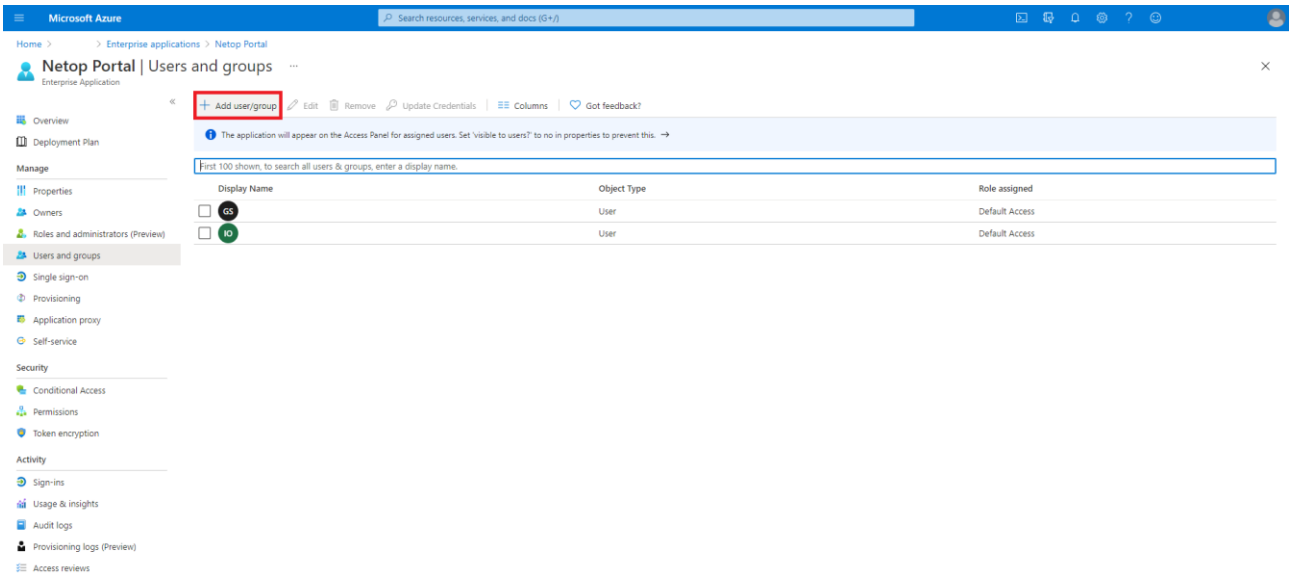
3. Click on the newly created **Netop Portal** application.



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

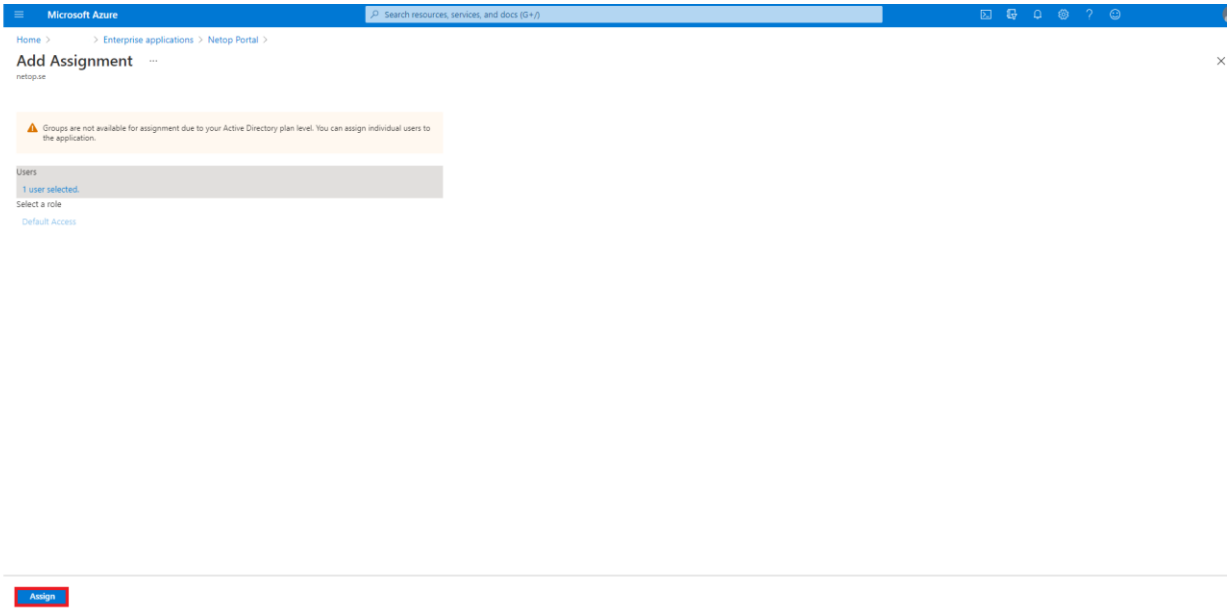


5. Click on the **Add User/group** button to add the allowed users or groups.



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.

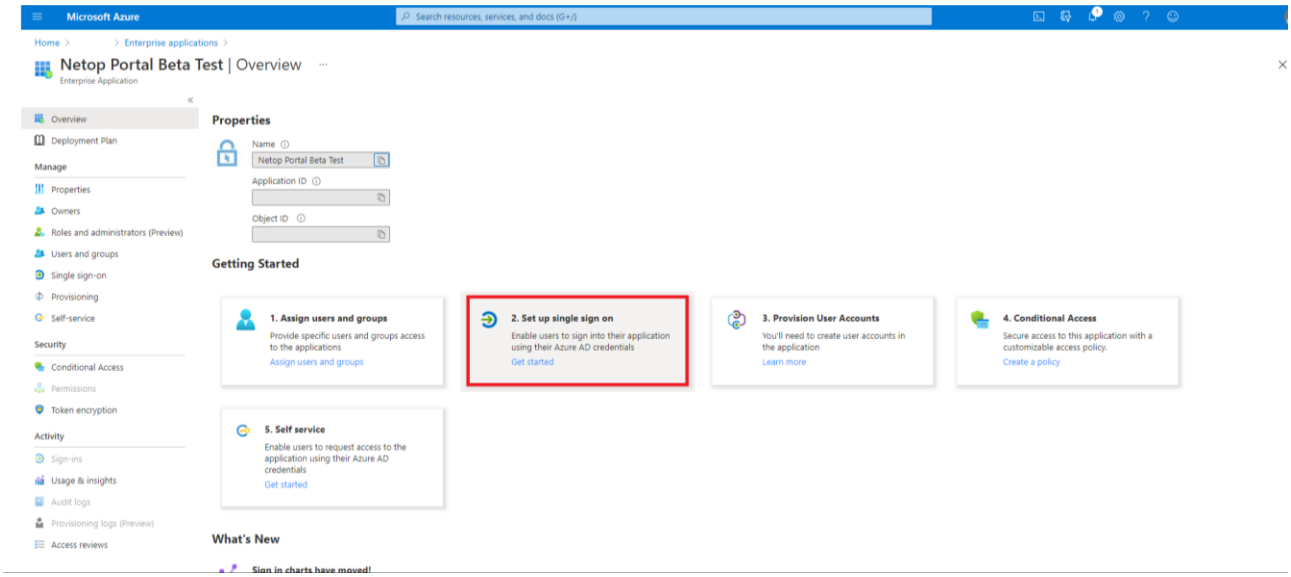


Configure single sign-on

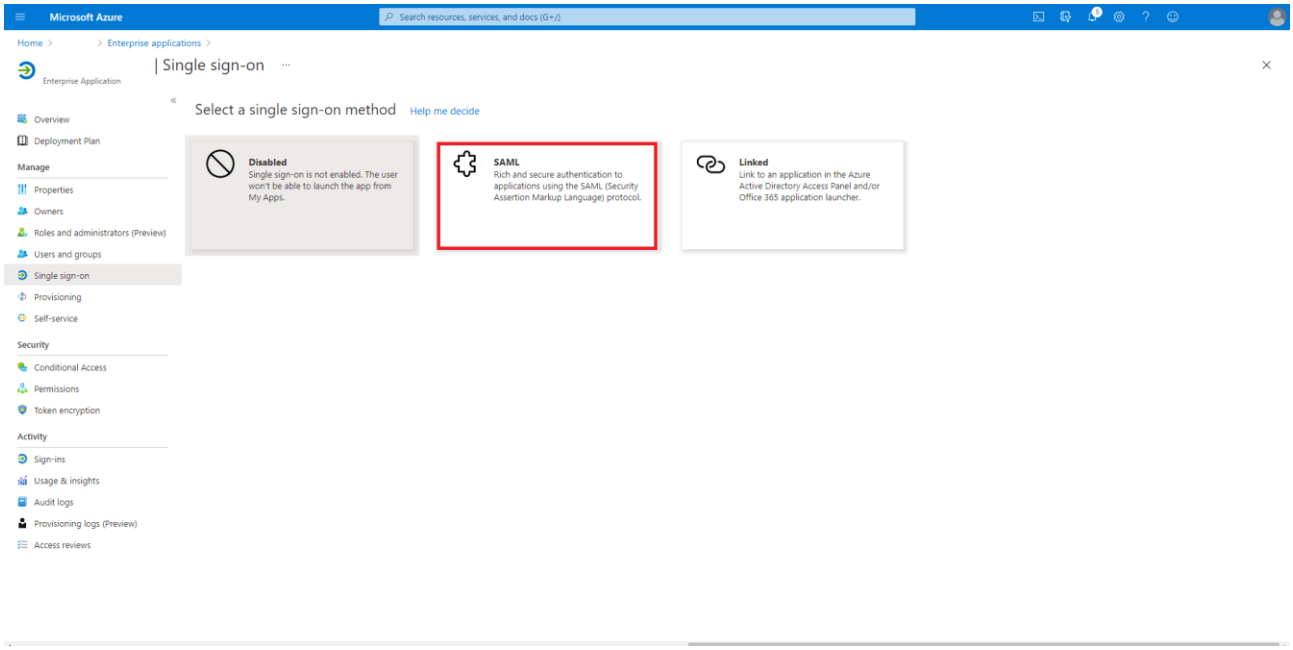
To configure the single sign-on, proceed as follows:

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

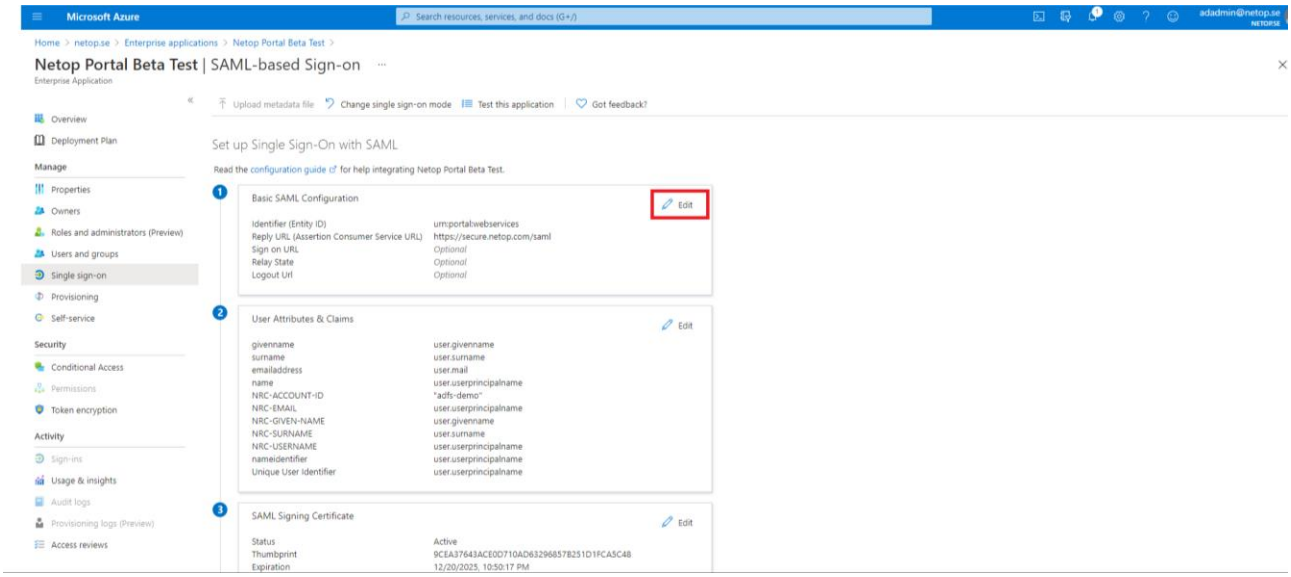
4. Click on **Set up single sign-on.**



5. Click on **SAML**.



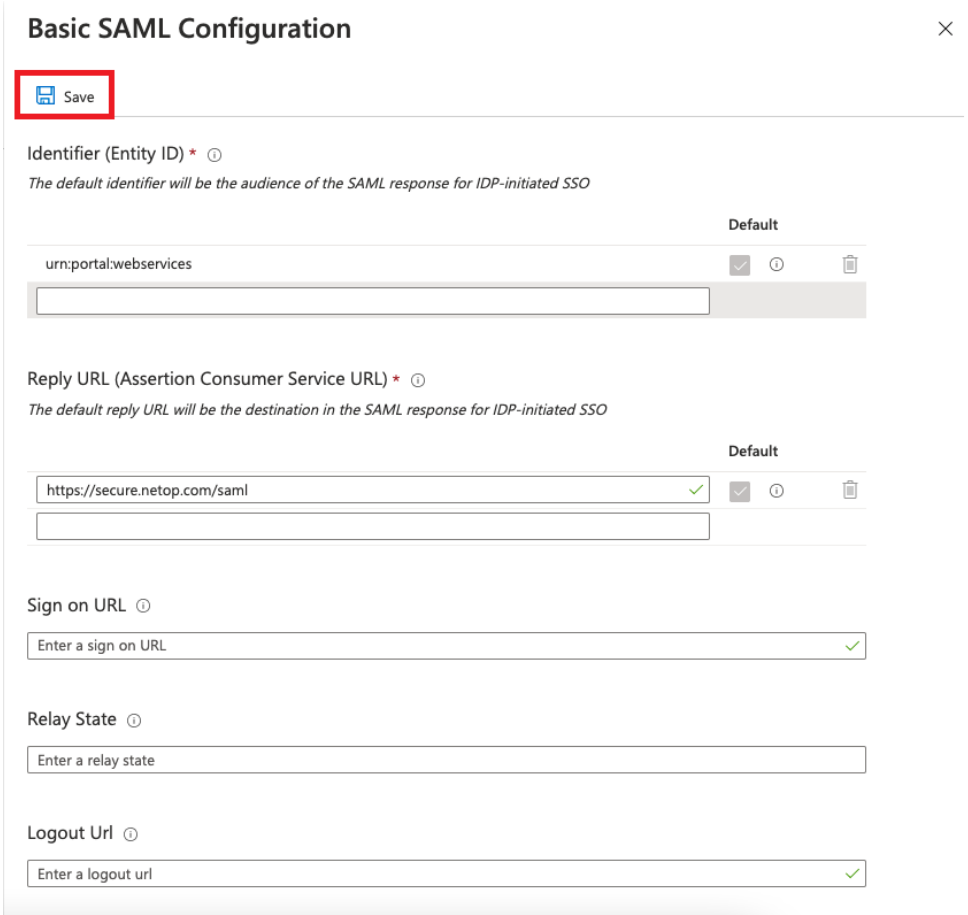
6. In the **Basic SAML Configuration** group, click on the **Edit** button.



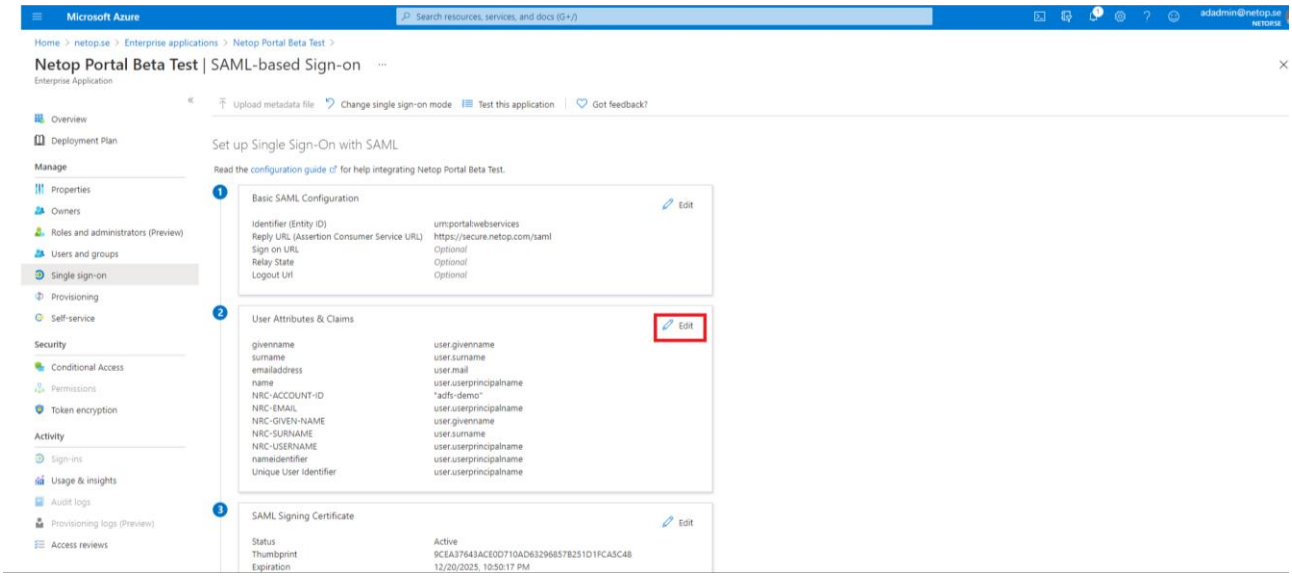
7. Verify the following settings:

Field name	Value
Identifier (Entity ID)	urn:portal:webservices
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.



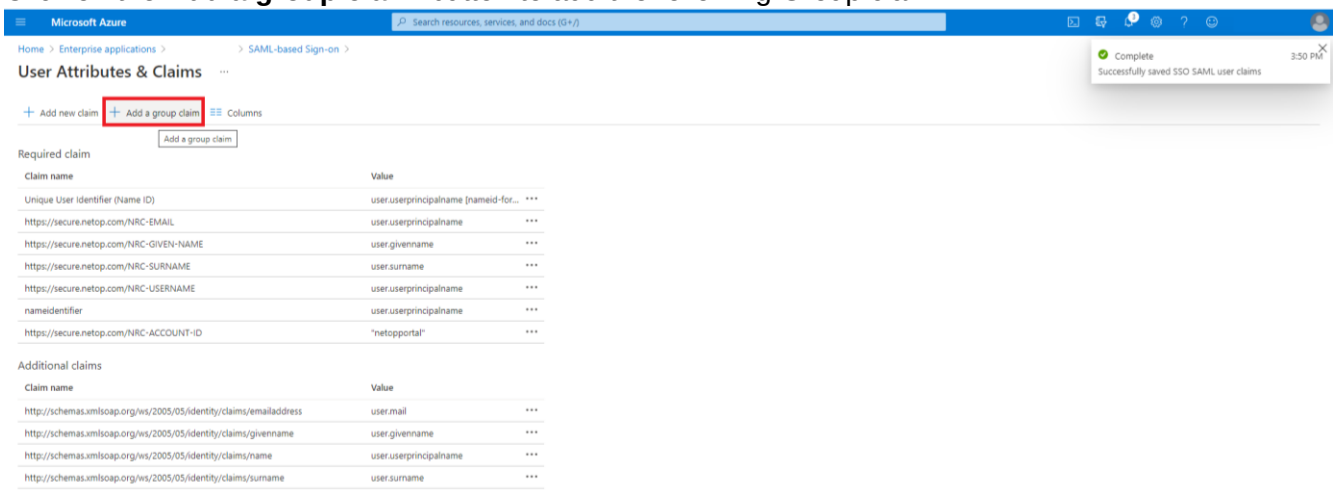
10. Verify the following claims:

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

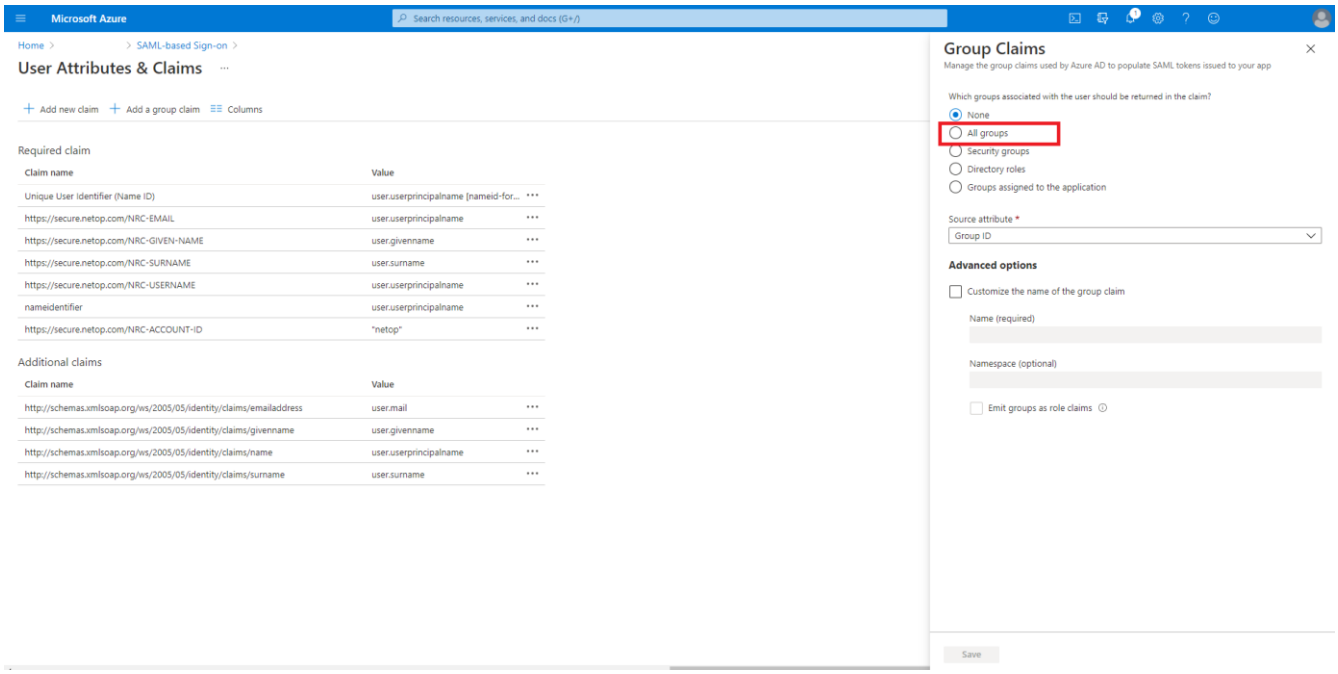
NOTE: When adding the **Netop Portal** application from the Azure AD Browse Application gallery section, the above claims are created automatically. The default attributed value to the NRC-ACCOUNT-ID user is set to “adfs-demo”. Modify this value as per your requirements.

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:



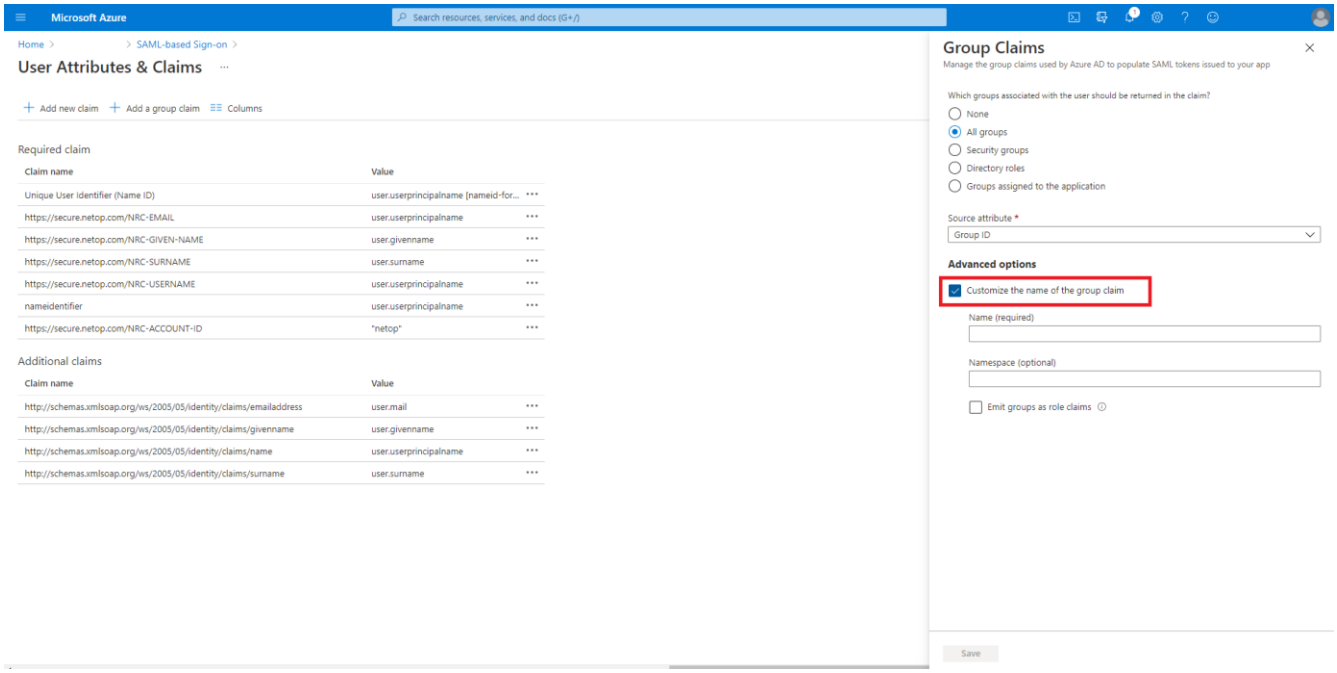
11.1. Select the **All groups** option from the Which groups associated with the user should be returned in the claim section.



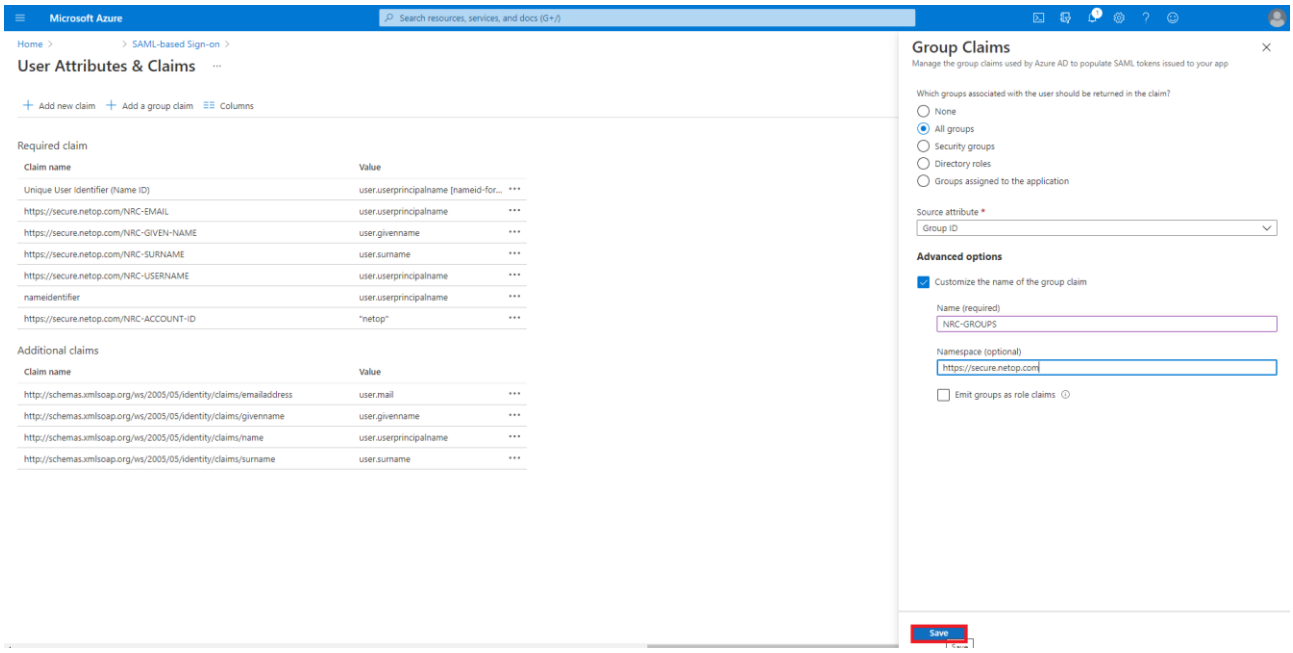
11.2. Click on the **Customize the name of the group claim.**

11.3. Specify the required name and namespace of the claim:

- Name: **NRC-GROUPS**
- Namespace: **https://secure.netop.com**

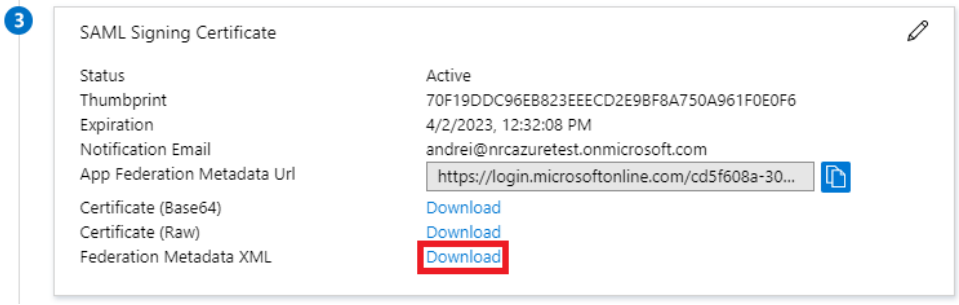


12. Click on the **Save** button to save your changes.

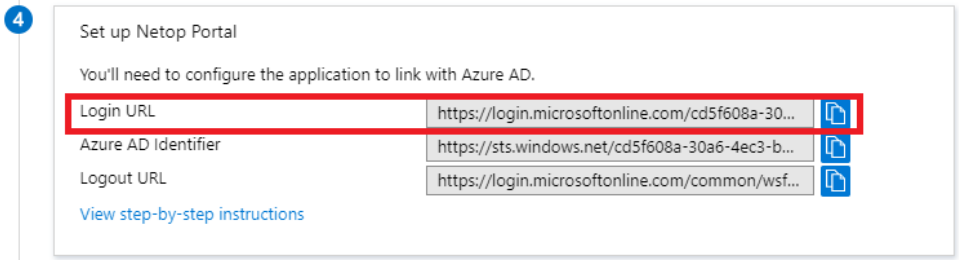


NOTE: Make sure that you save the following information:

- The **Federation Metadata XML** file



- The **Login URL**



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**.

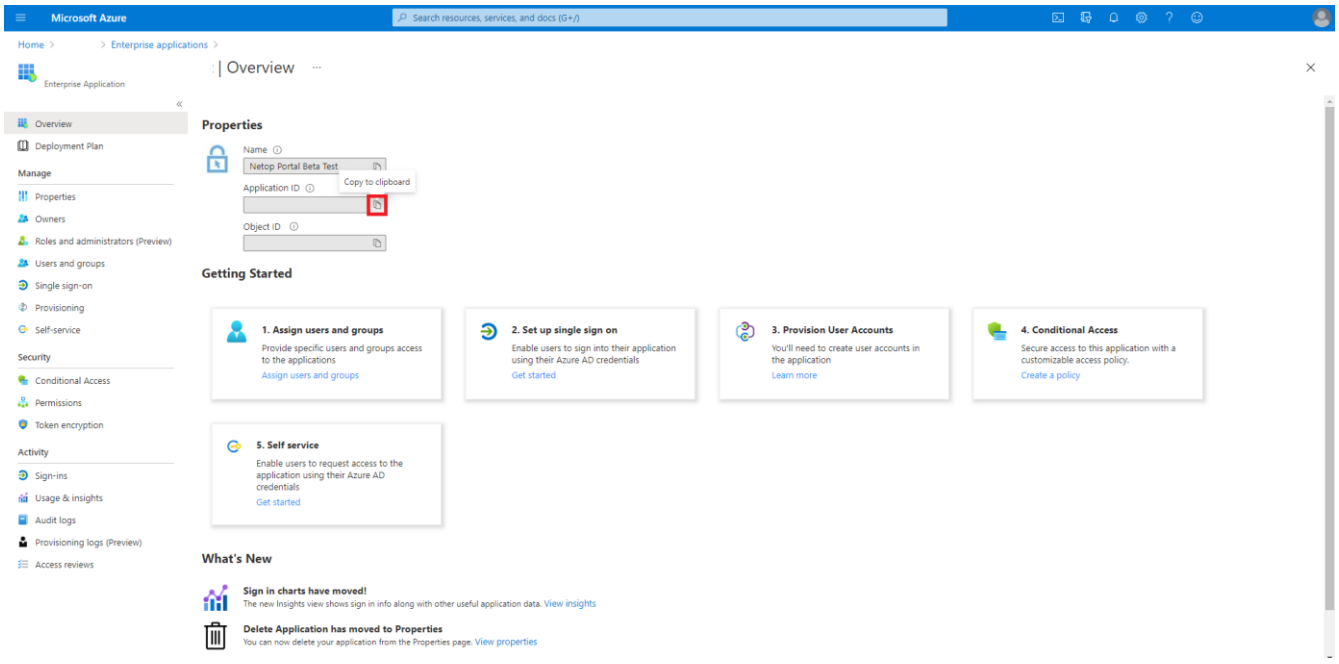
1.2. Go to **Windows Active Directory**.

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.

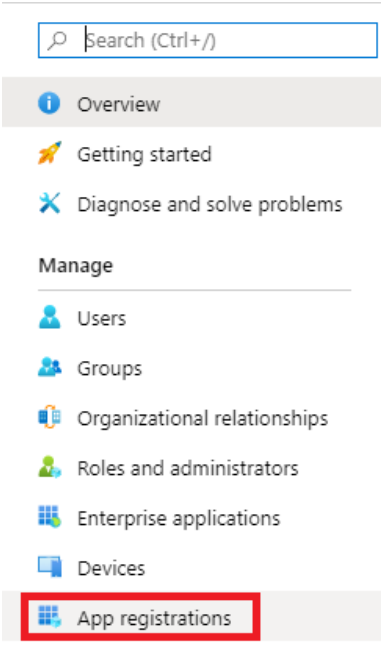


Configure the application permissions

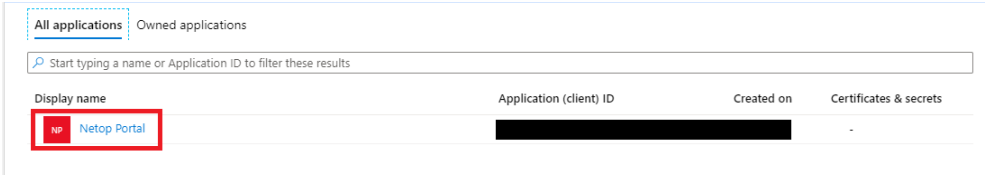
The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**.

To configure the application permissions, proceed as follows:

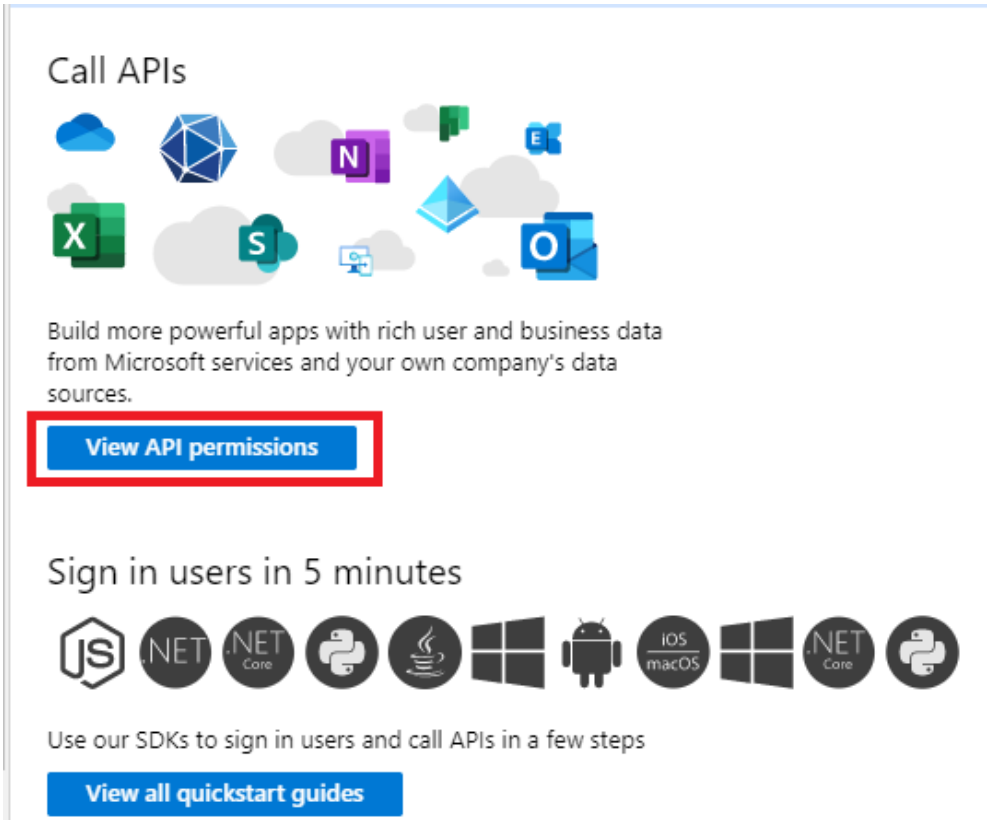
1. Go to **Azure Active Directory**.
2. Go to **App registrations**.



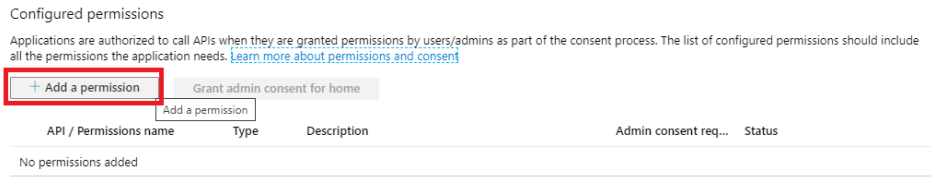
3. Click on the **Netop Portal** application.



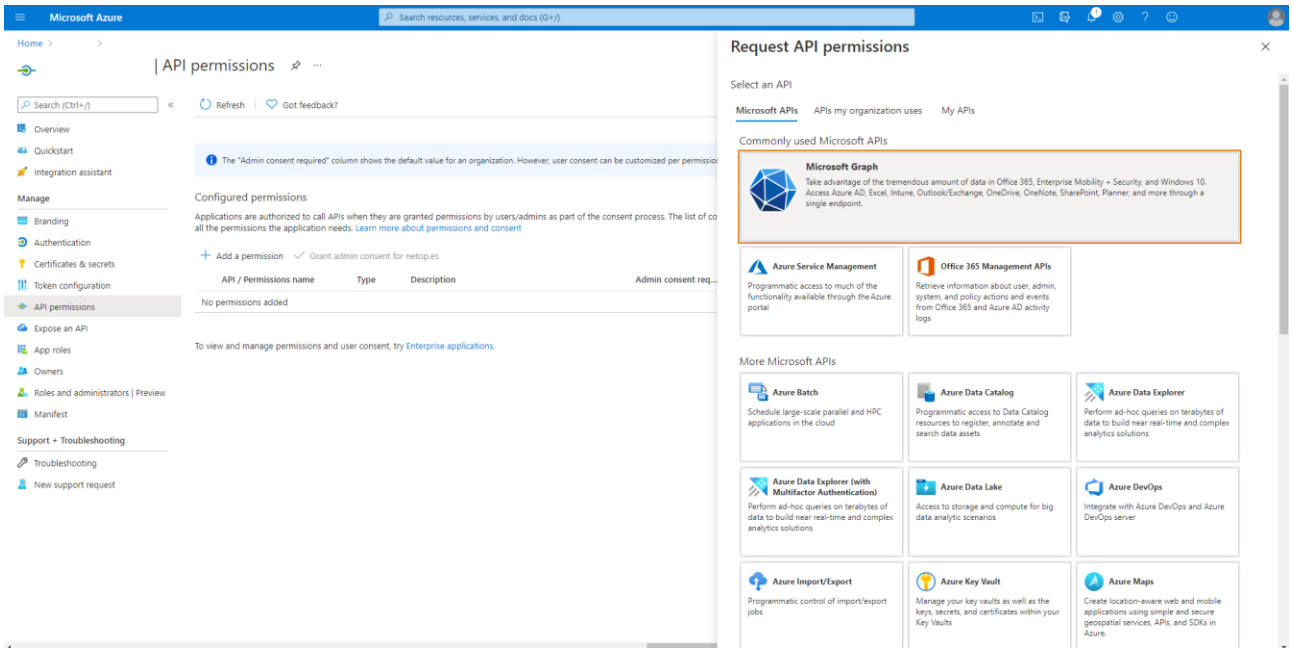
4. Click on the **View API permissions** button.



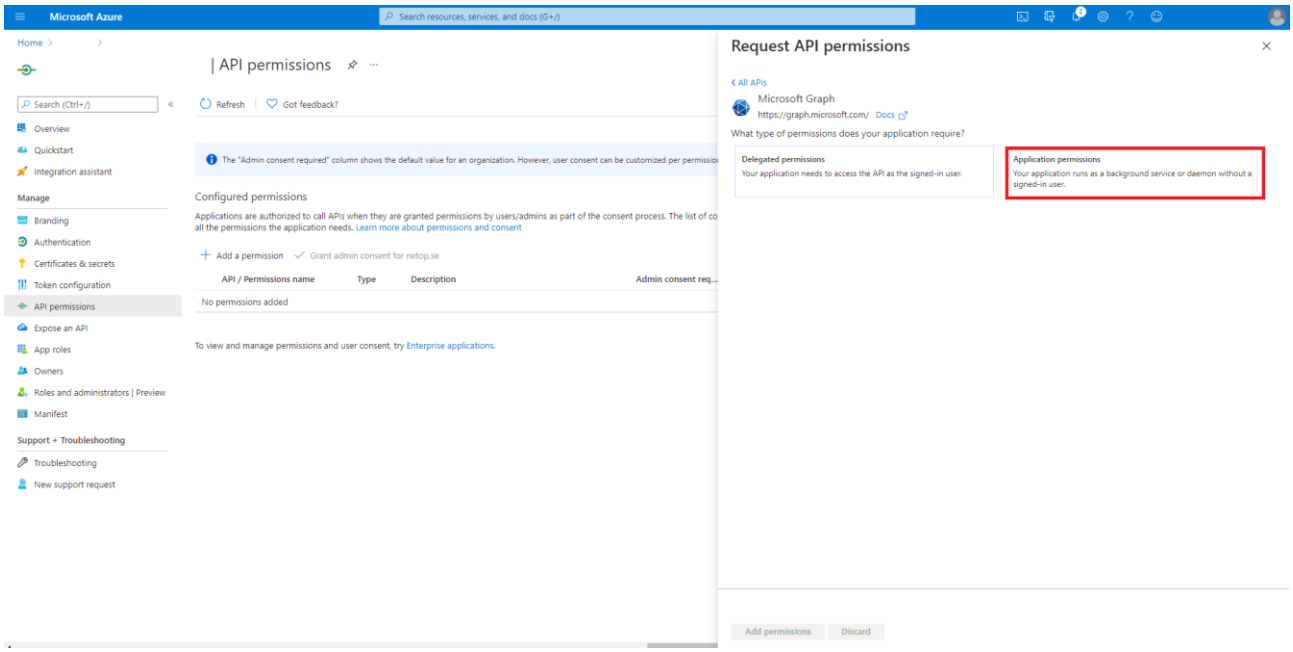
5. Click on the **Add a permission** button to add the necessary permissions.



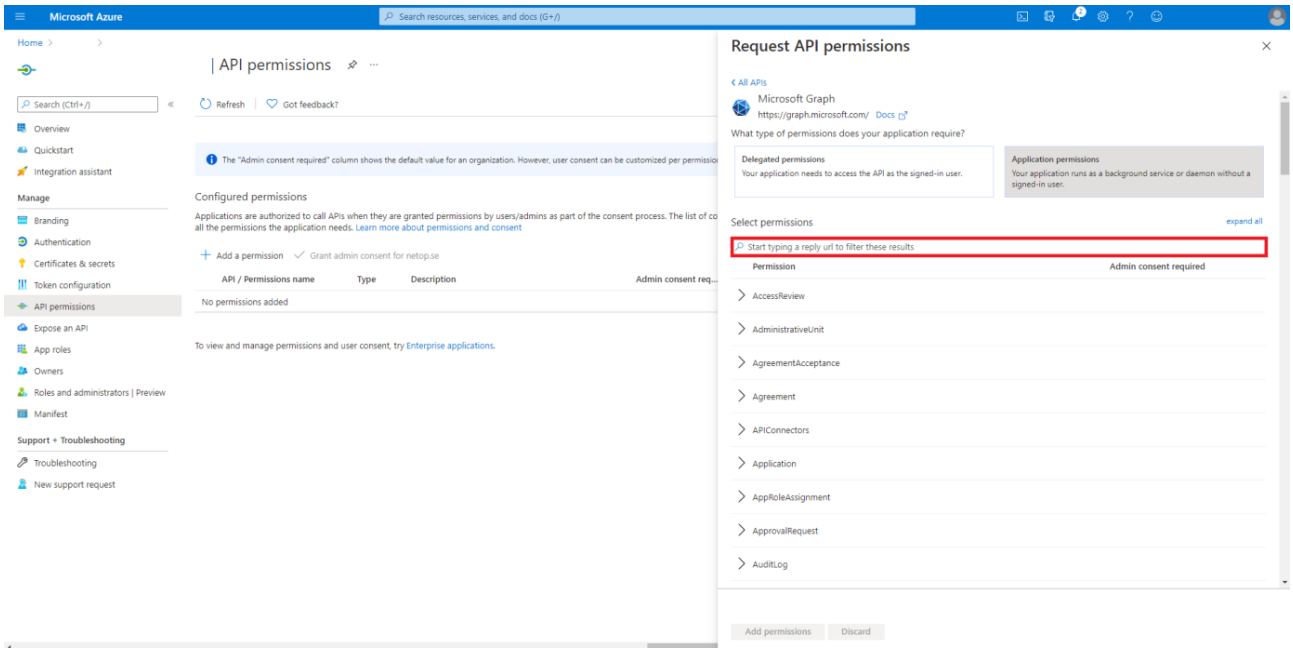
6. Click on Microsoft Graph.



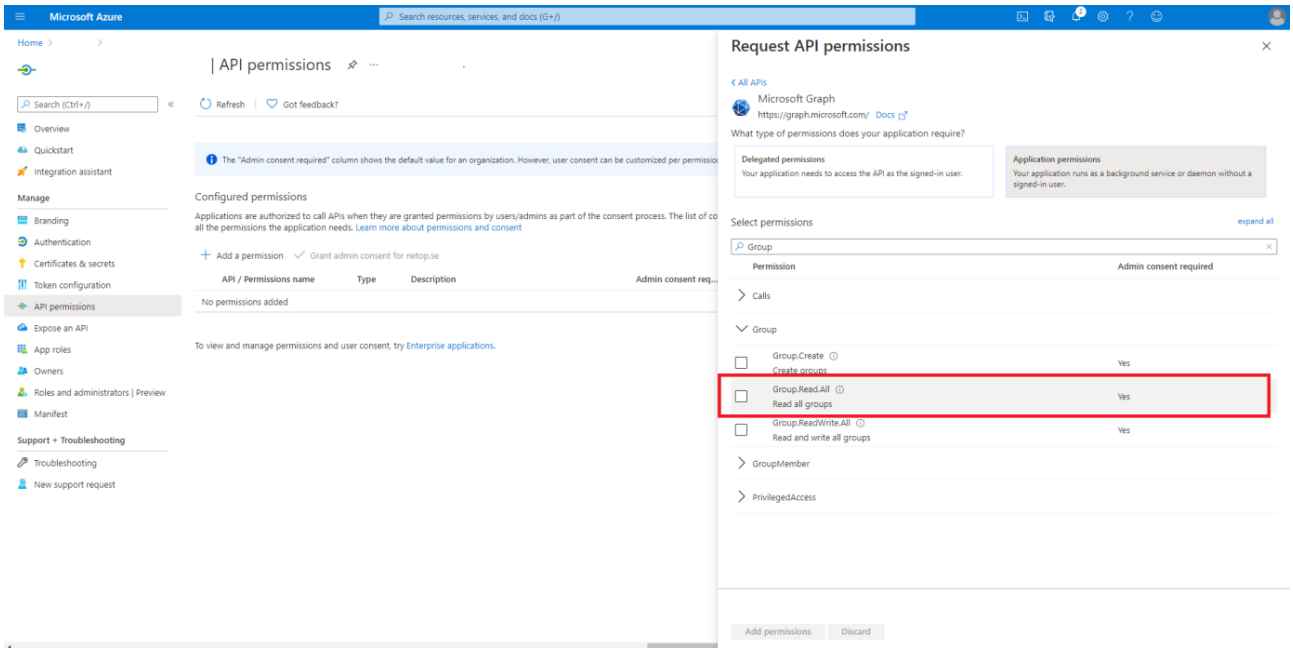
7. Click on **Application permissions**.



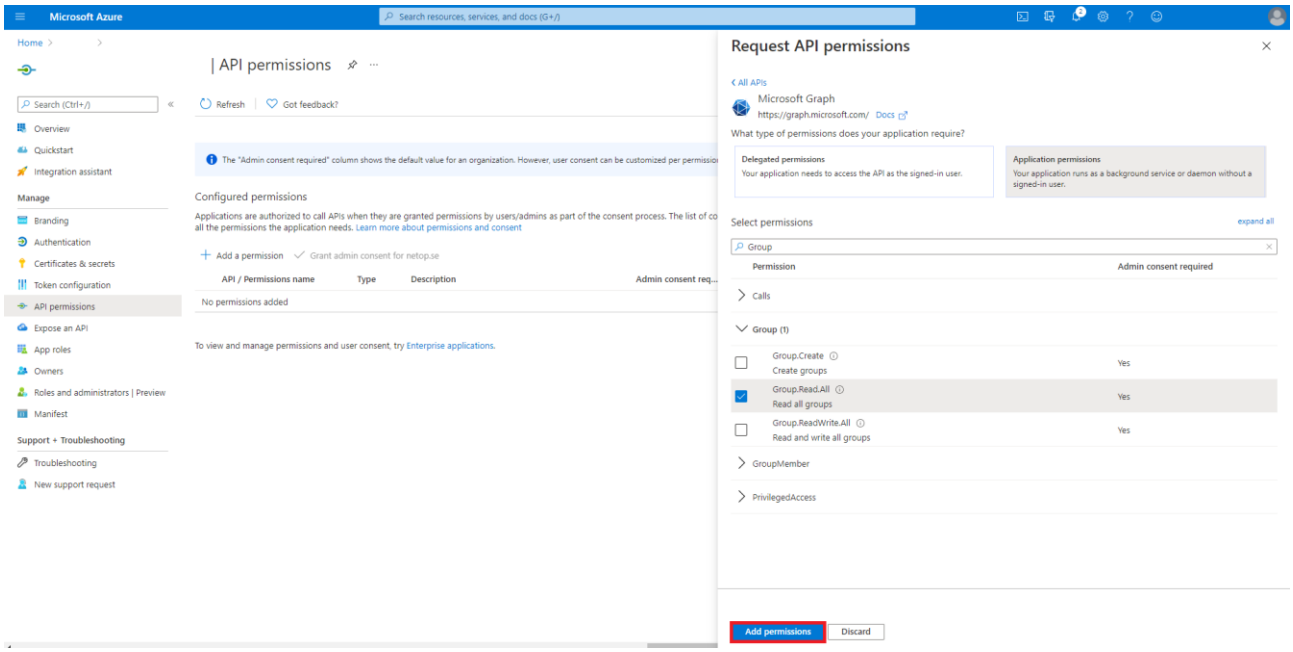
8. Search for Group in the **Start typing a reply url to filter these results** search field.



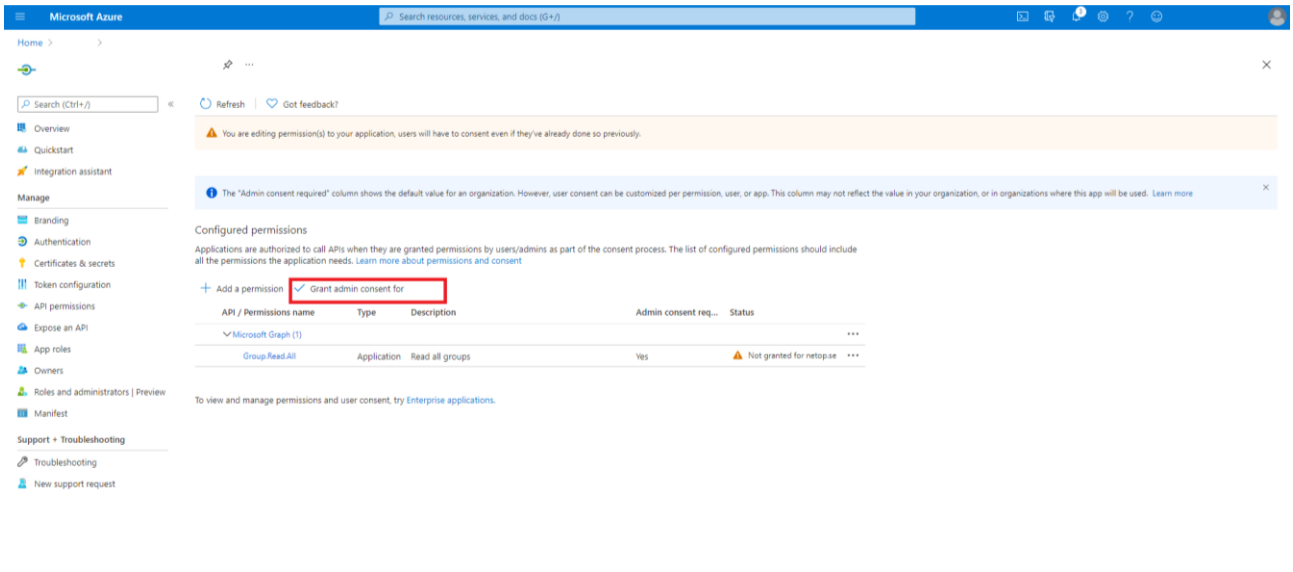
9. Click on the **Group.Read.All** option.



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.



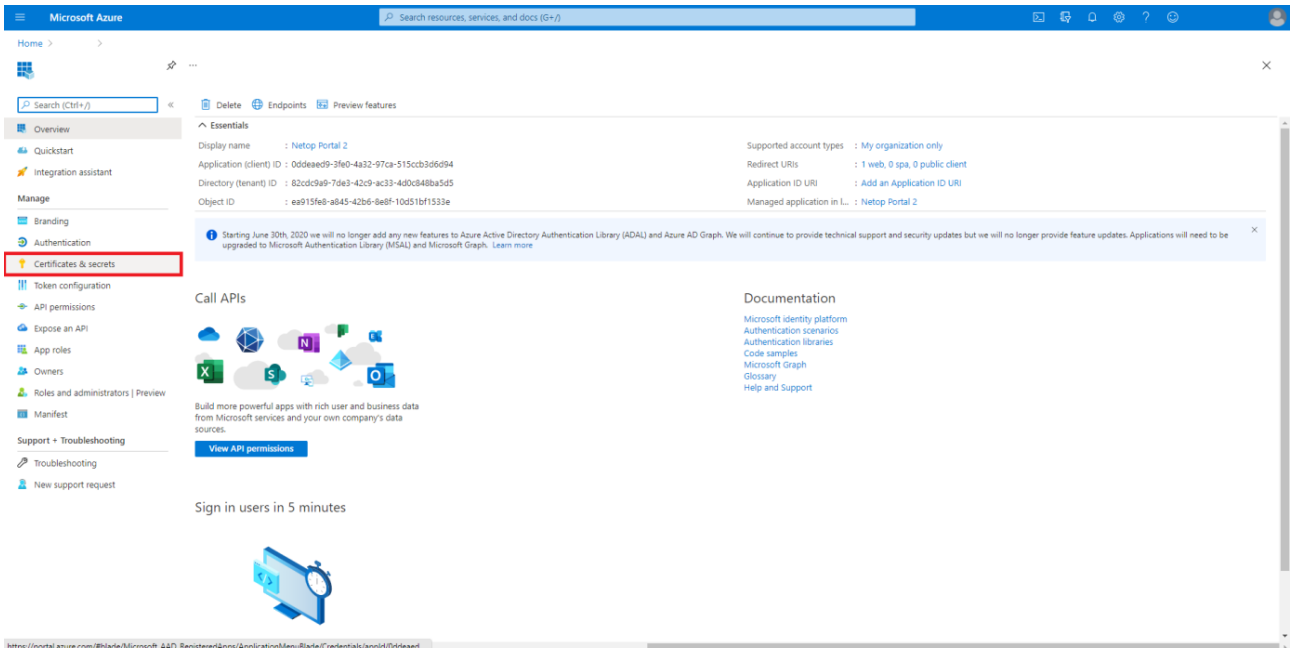
Configure Certificates & secrets

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

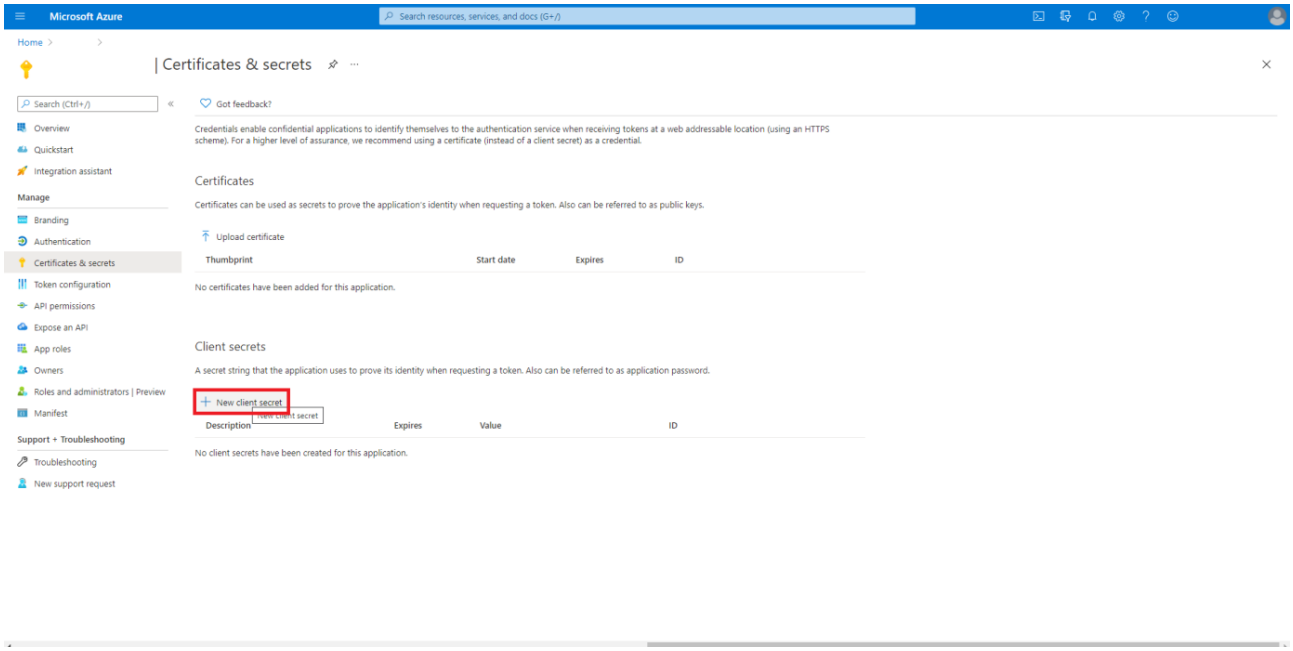
To configure the **Certificates & secrets**for the **Netop Portal** application in the **Azure Portal**, proceed as follows:

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

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

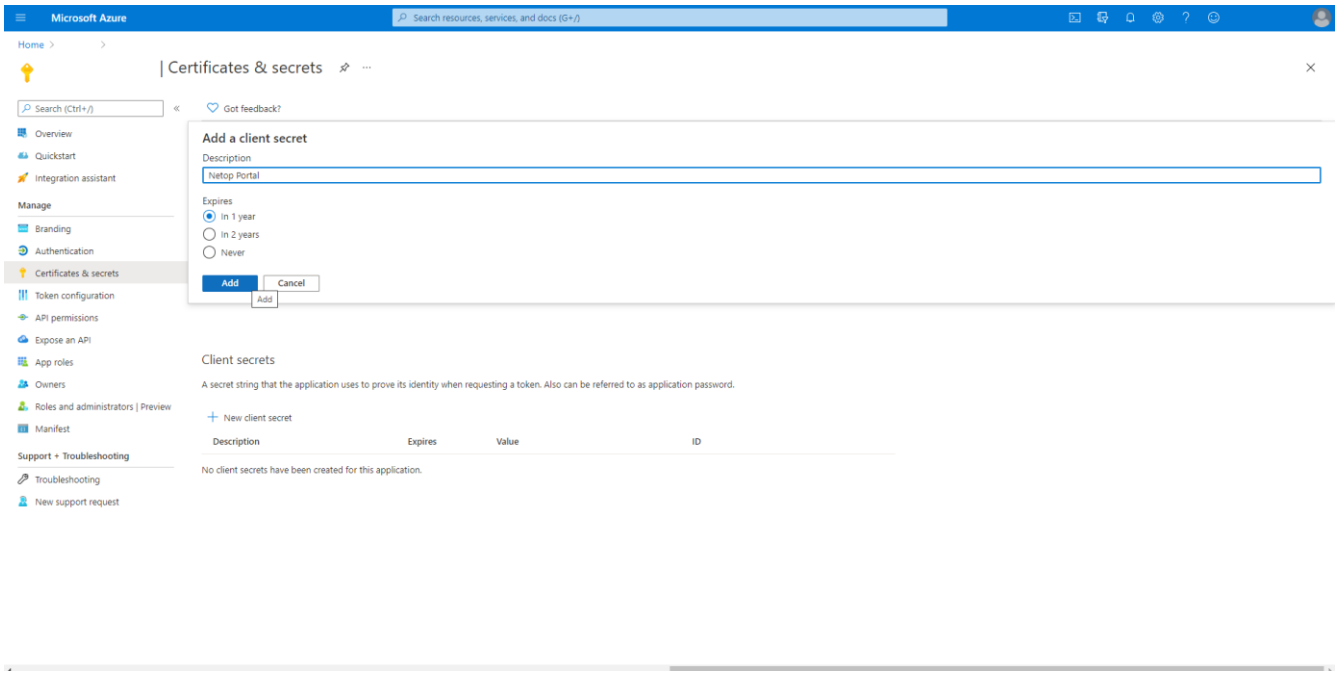


5. Click on the **New client secret** button.

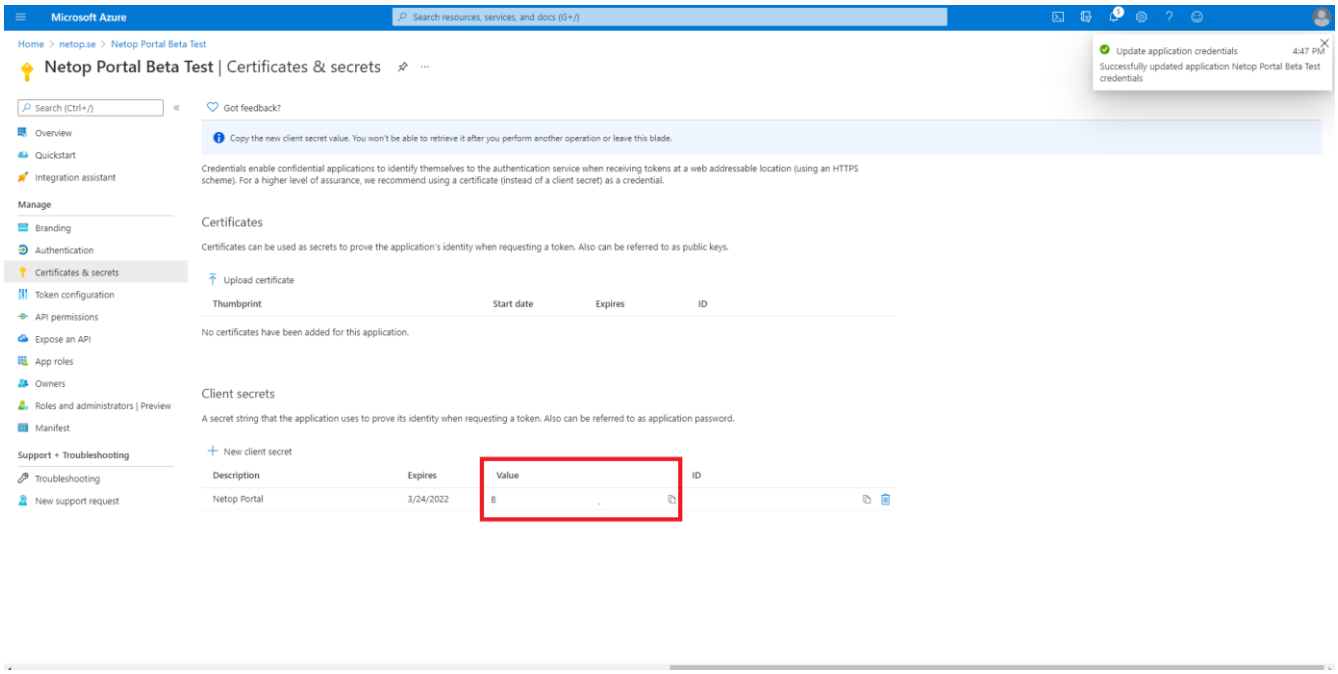


6. Specify a name for the client secret in the **Description** entry field.
7. Specify an expiry date for the client secret accordingly to your needs.

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



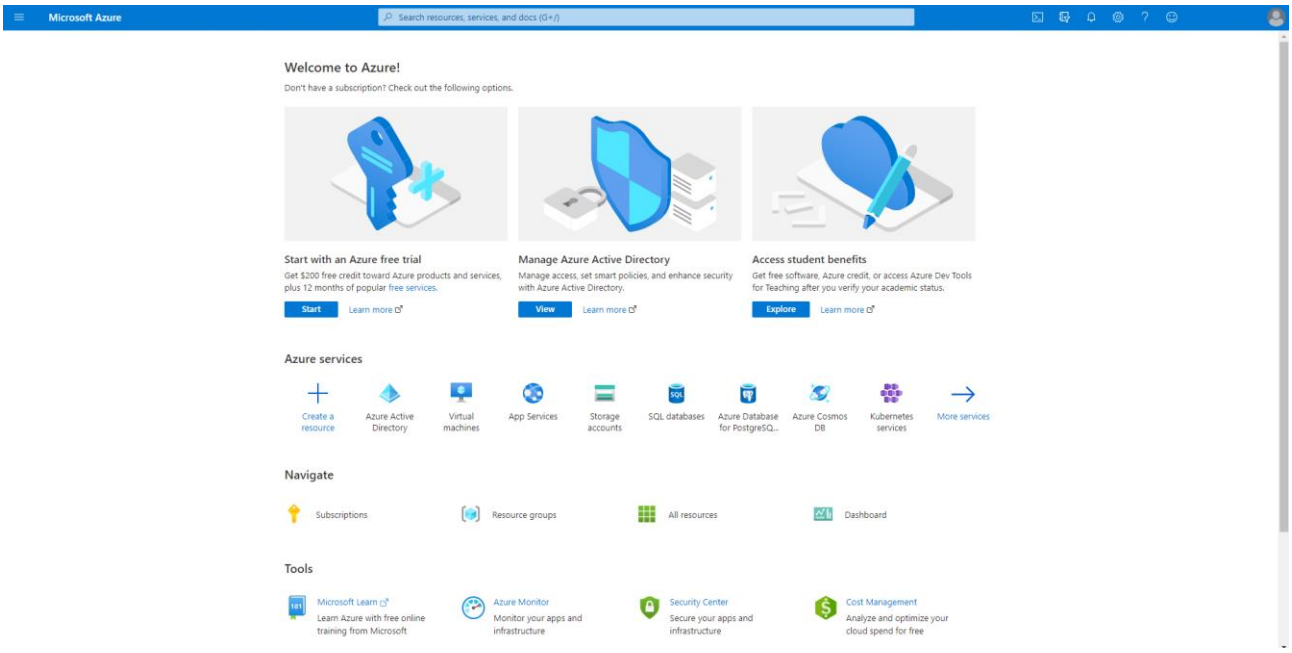
9. Save the client secret value in a text editor or copy it to the clipboard. It is necessary for you to do so, because once you leave this particular page the value will no longer be available for display in plain text.



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

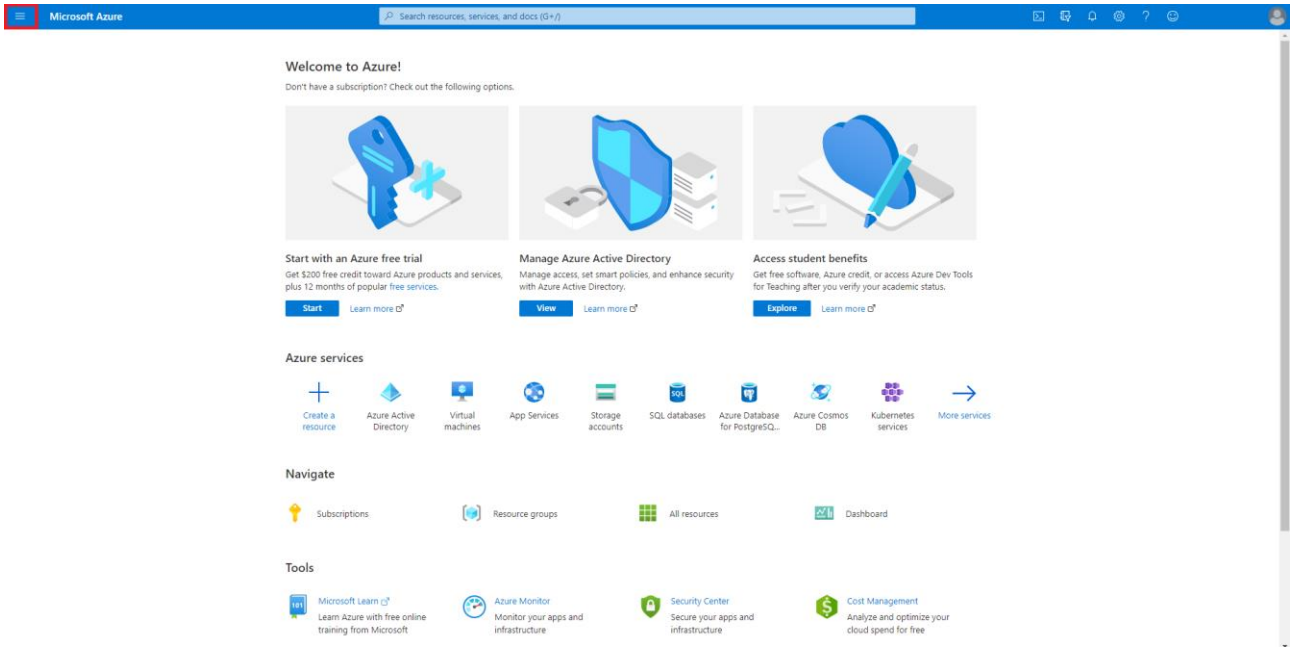
To create the **Netop Portal** application in **Azure AD**, proceed as follows:

1. Log in the Azure Portal.

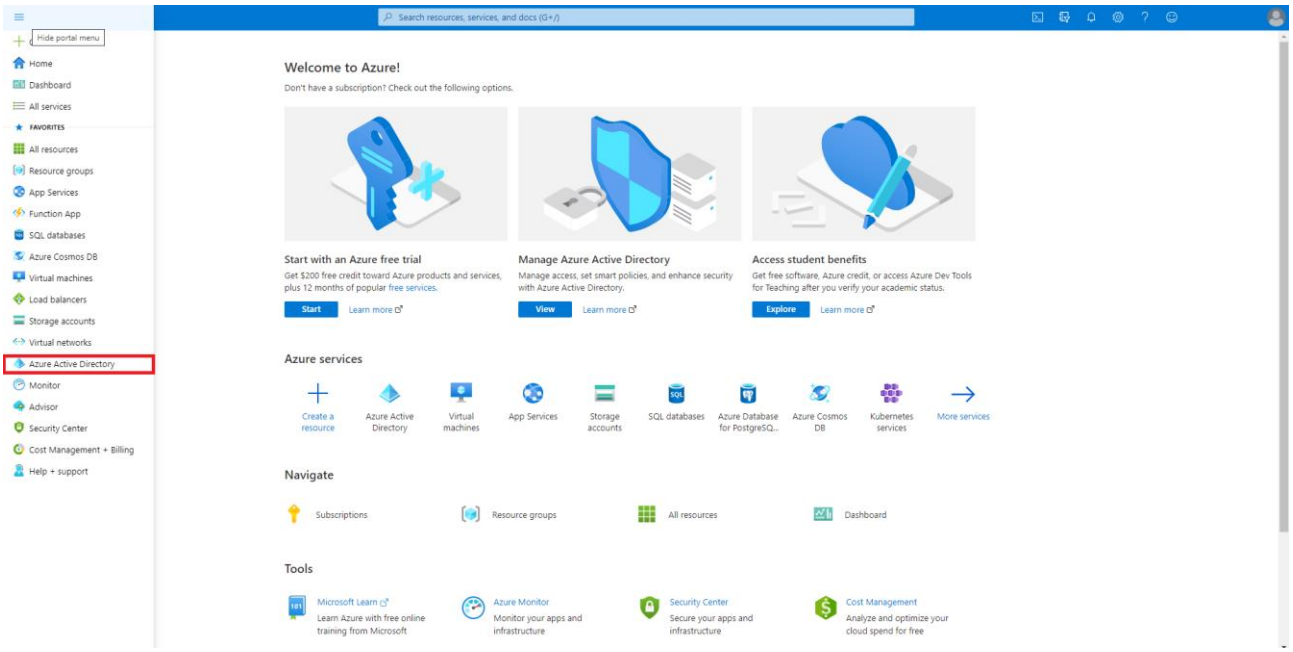


2. Go to **Azure Active Directory.**

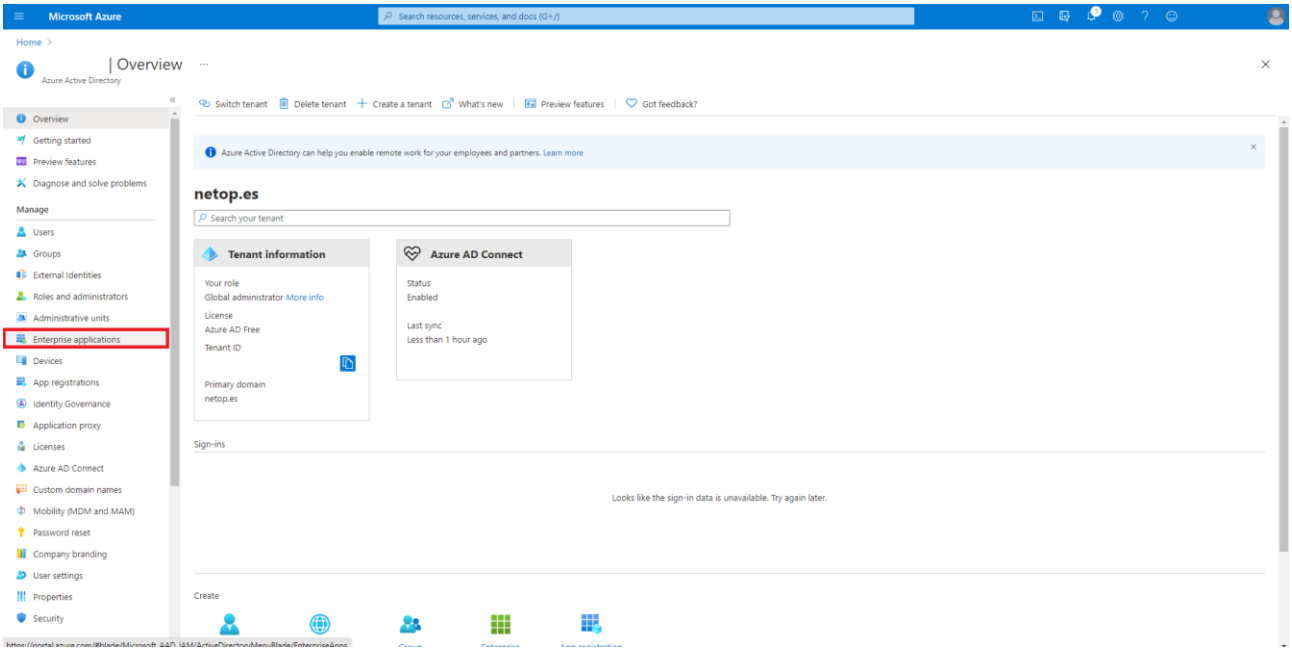
   2.1. Click on the **More** button.



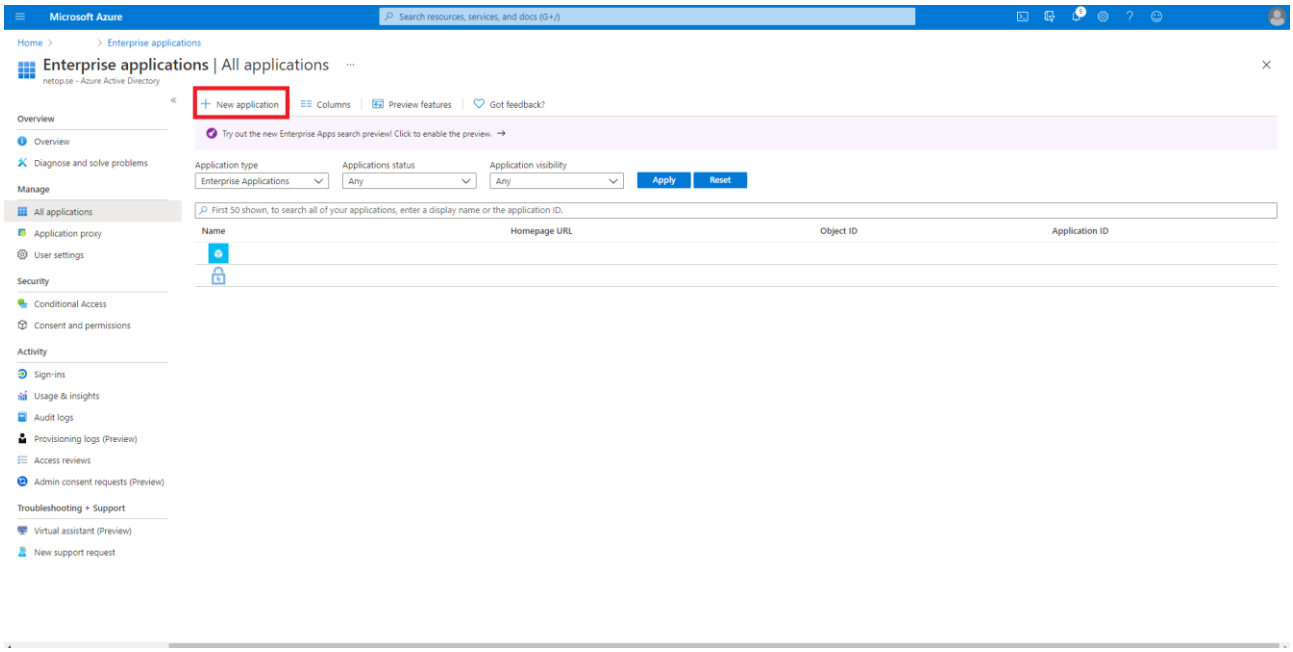
2.2. Click on **Azure Active Directory**.



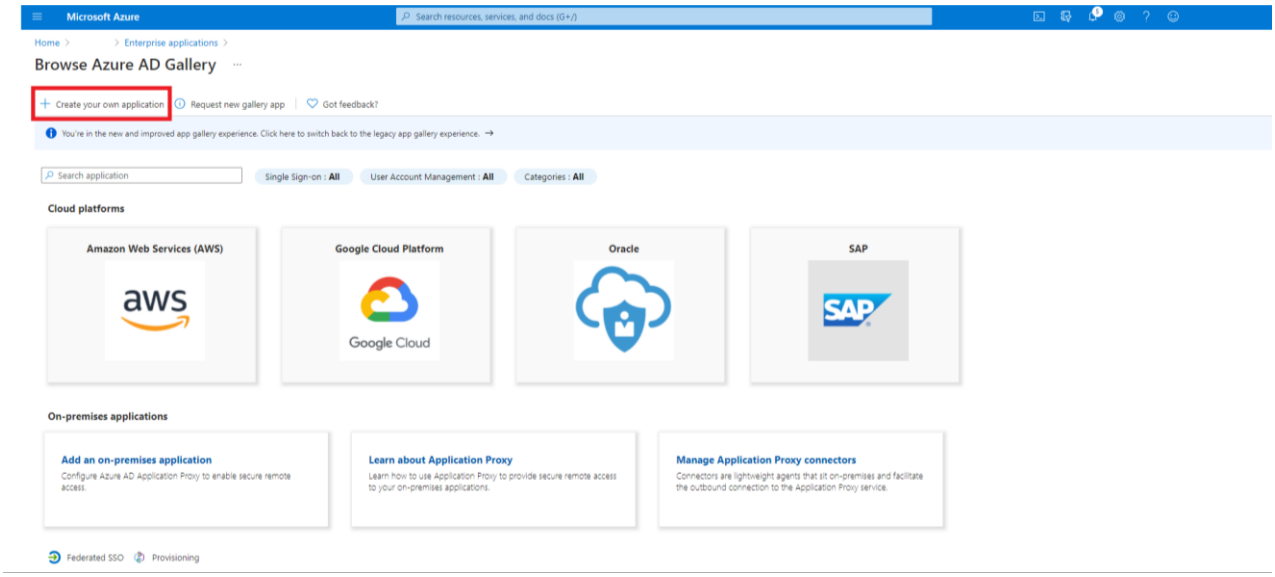
3. Go to **Enterprise applications.**



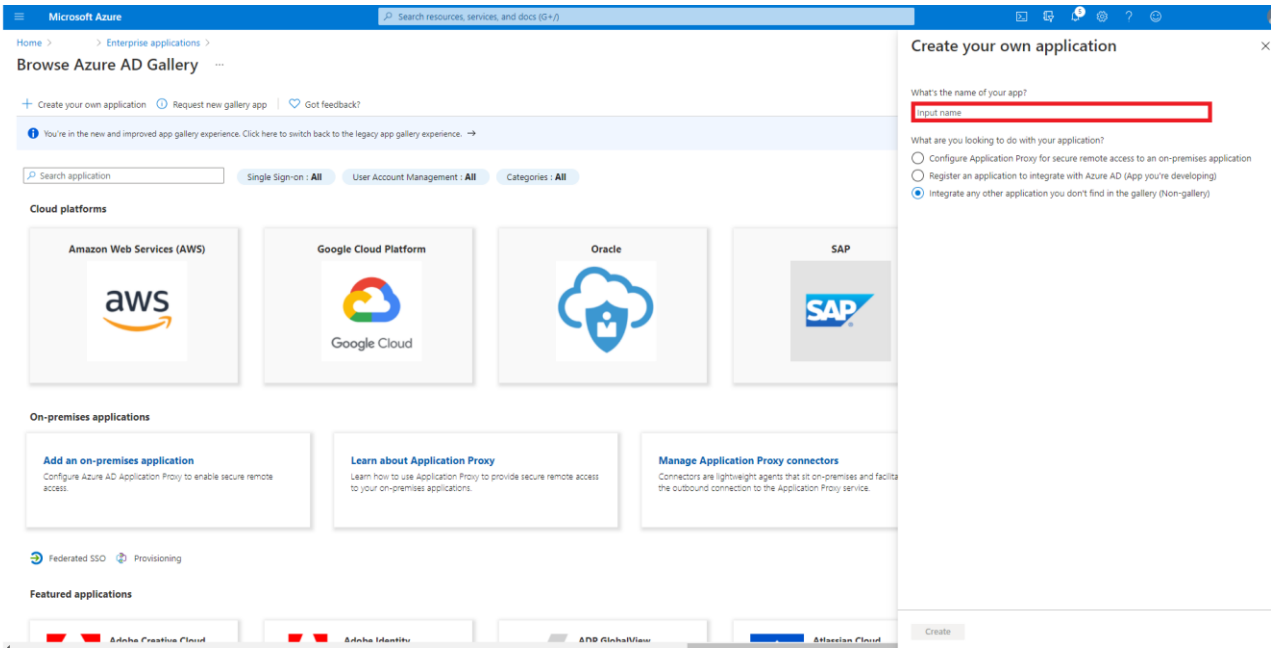
4. Click on the **New application** button.



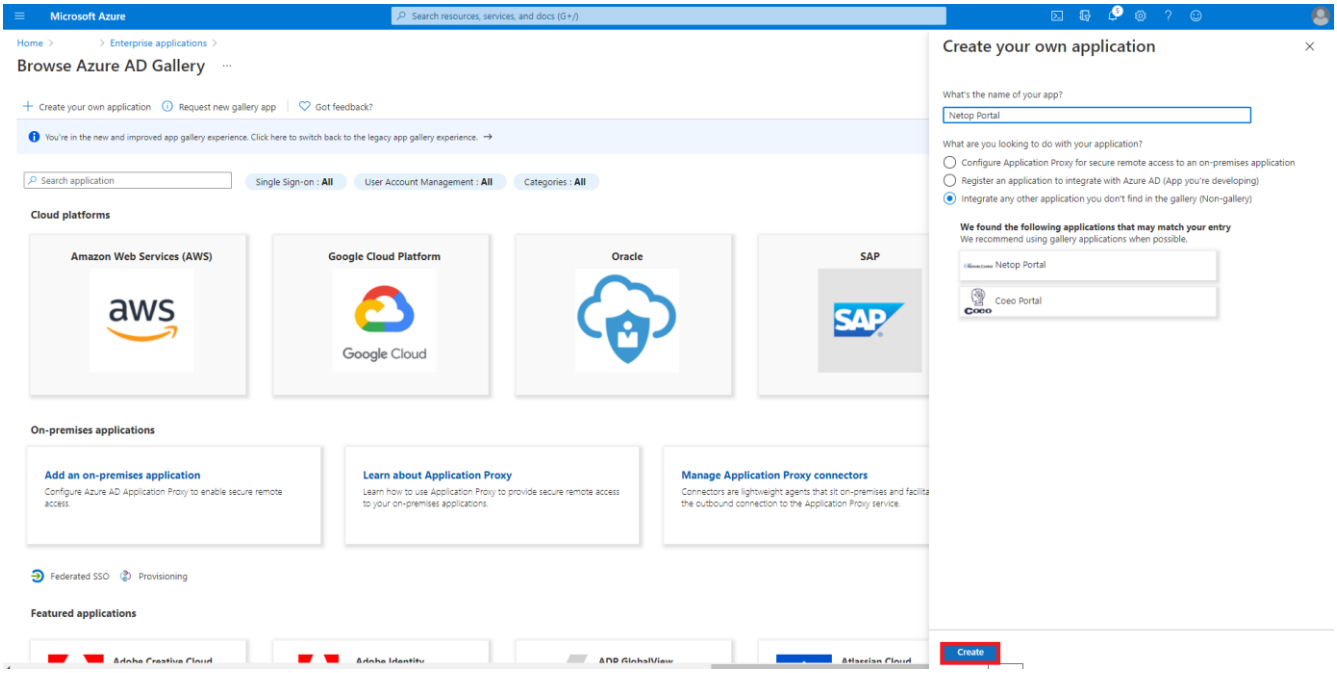
5. Click on the **Create your own application** button.



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**.



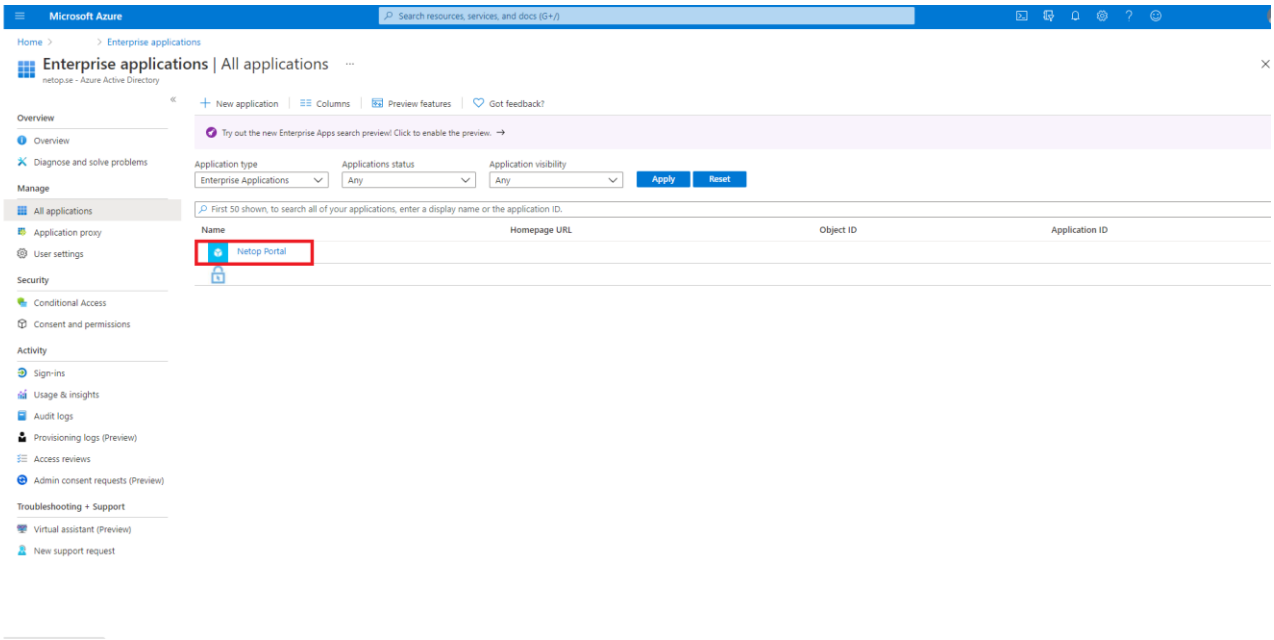
The application is created successfully and added to the **Enterprise applications** section.

Add users and groups to the application

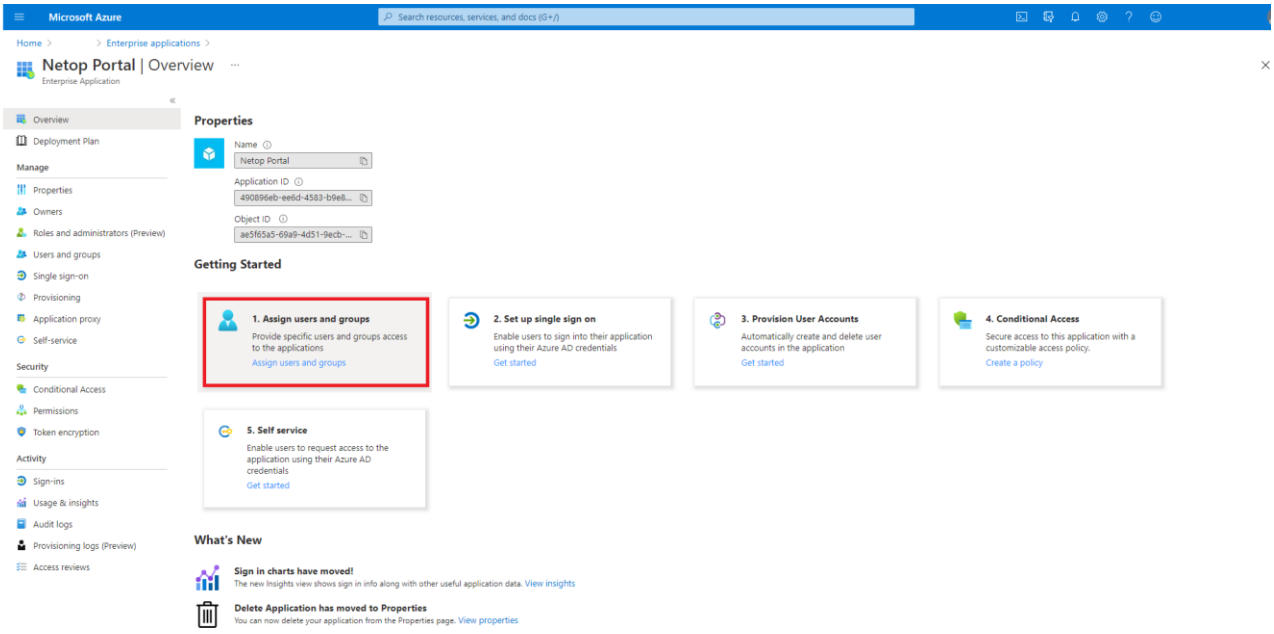
To add users and groups to the application, proceed as follows:

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

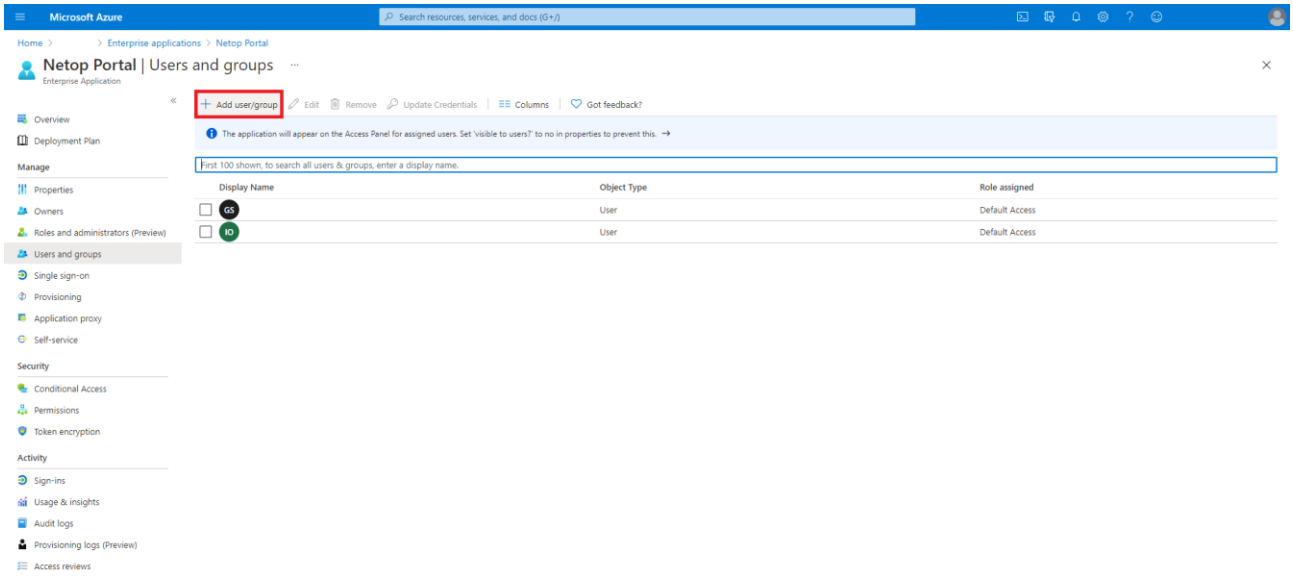
3. Click on the newly created **Netop Portal** application.



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

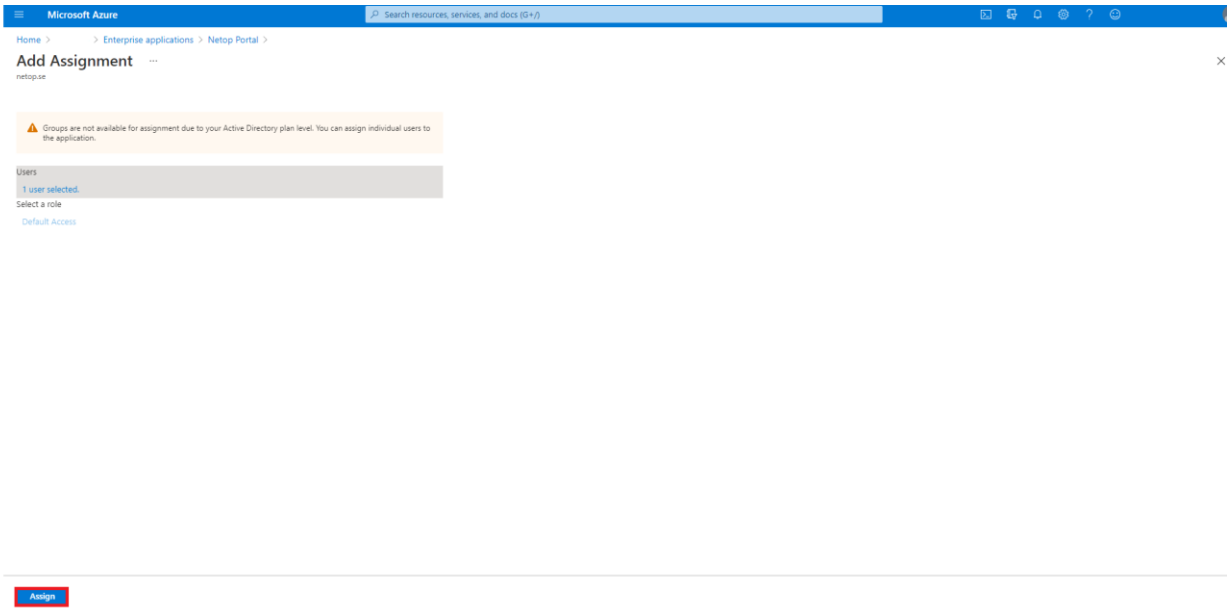


5. Click on the **Add User** button to add the allowed users or groups.



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.

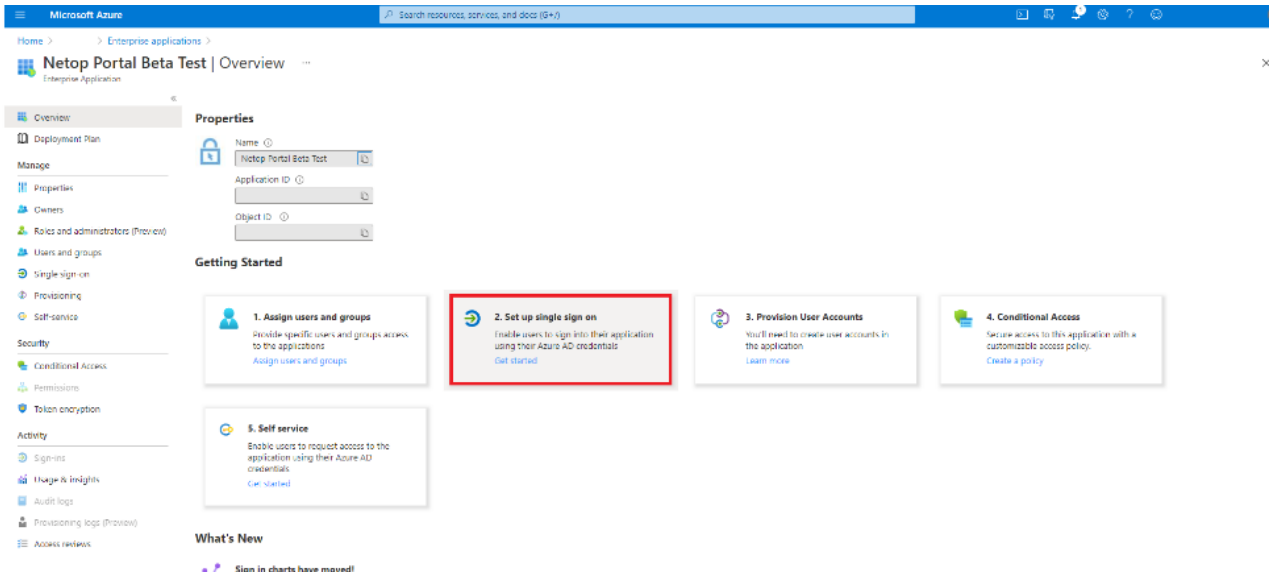


Configure single sign-on

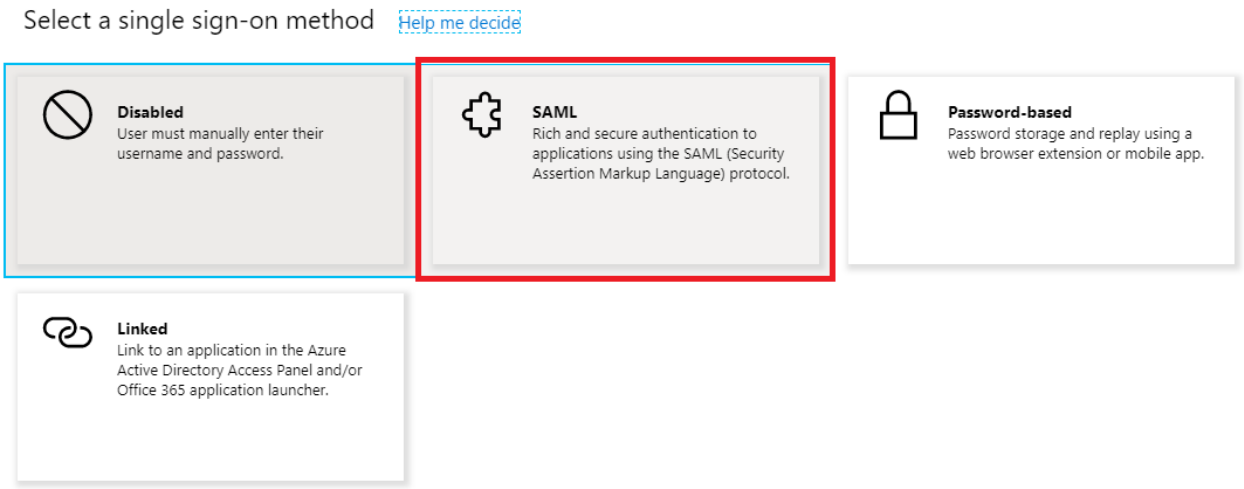
To configure the single sign-on, proceed as follows:

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

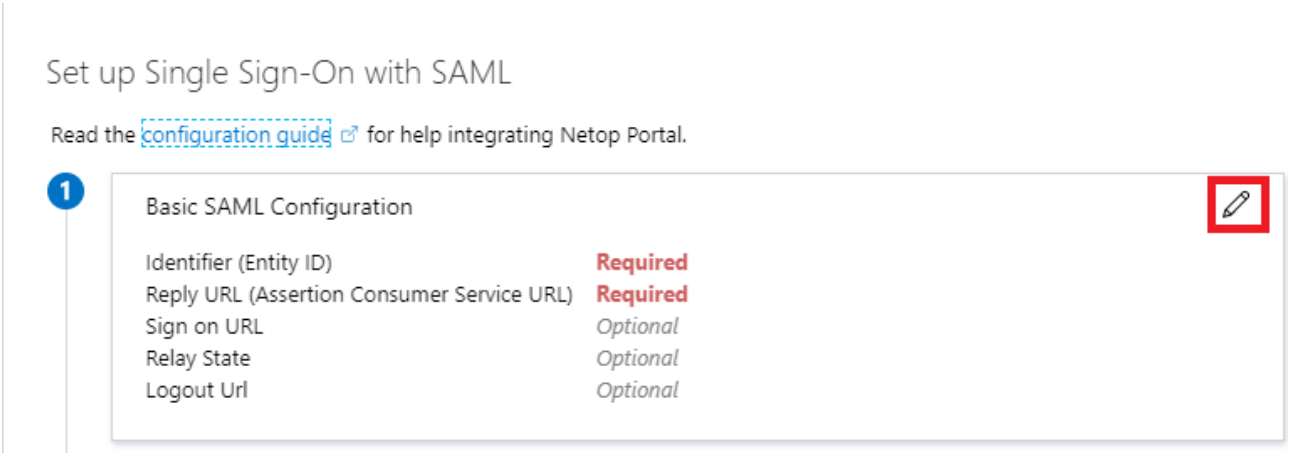
4. Click on **Set up single sign-on.**



5. Click on **SAML**.



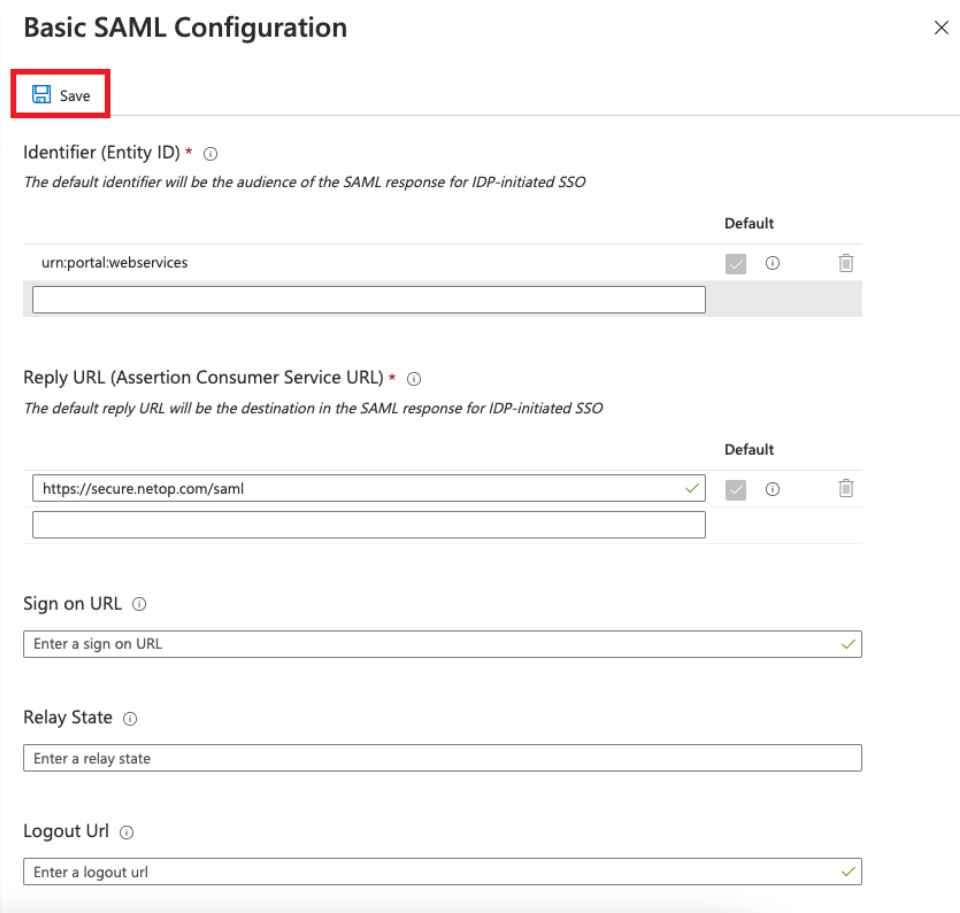
6. In the **Basic SAML Configuration** group, click on the **Edit** button.



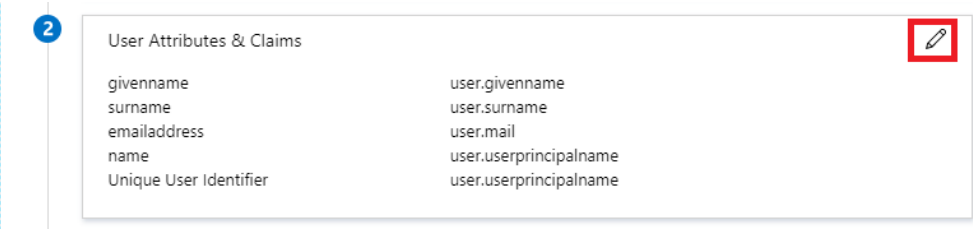
7. Specify the following settings.

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.



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

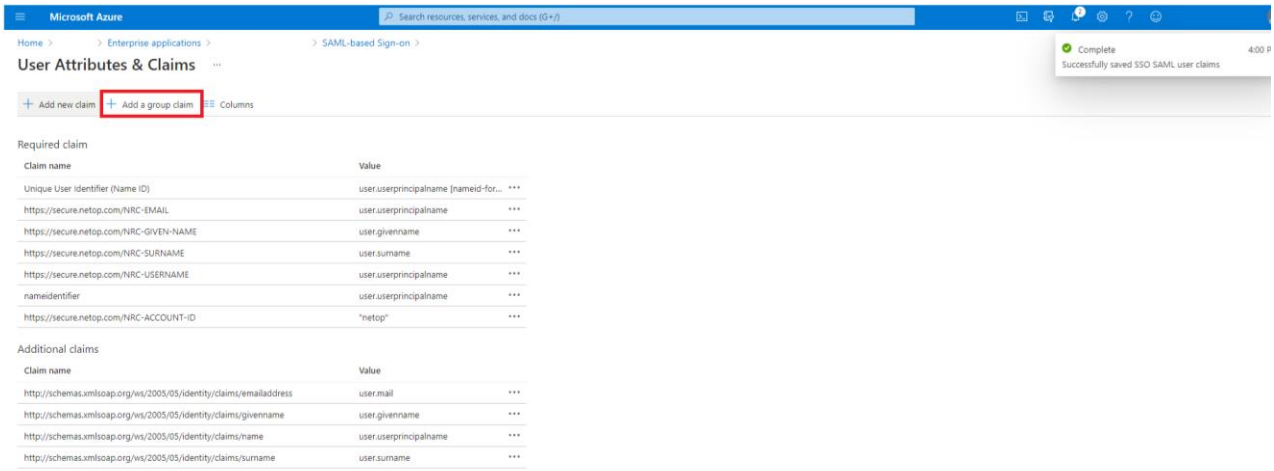


10. Click on the **Add new claim** button to create the necessary claims.

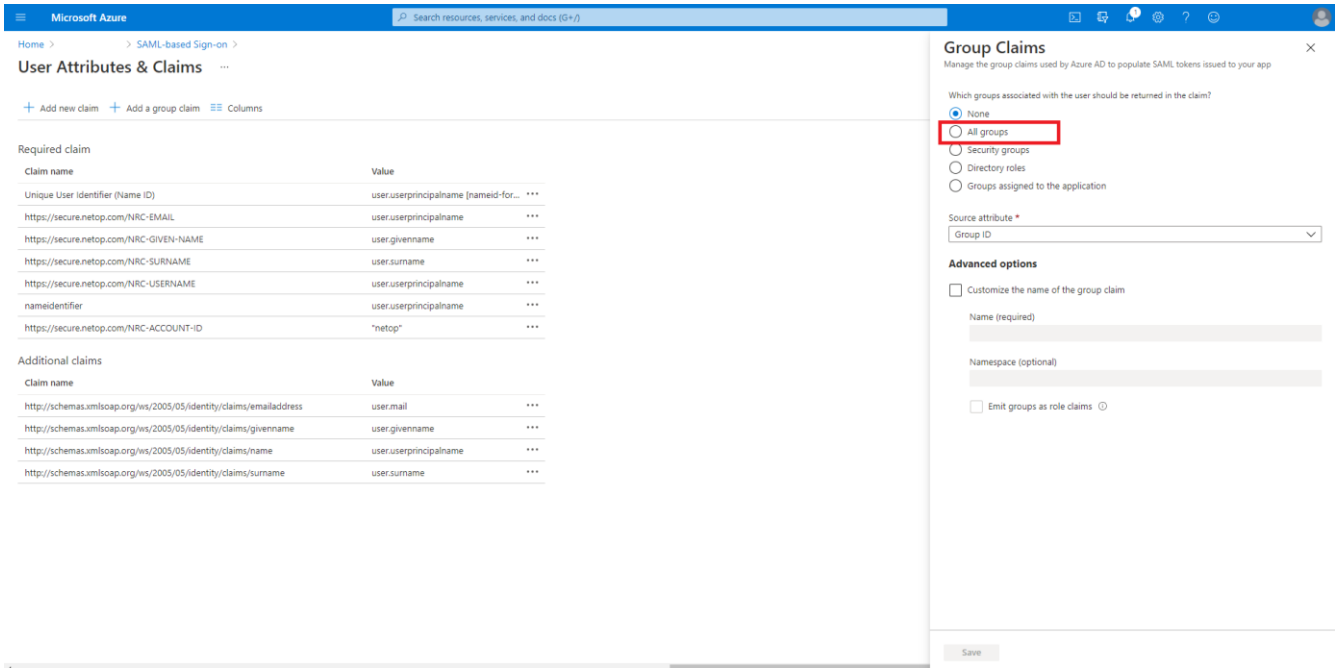
Name	Namespace	Source	Source attribute
NRC-ACCOUNT-ID	https://secure.netop.com	Attribute	This is the domain identifier that you both specify here and in the **Netop Portal** ADFS/Azure AD configuration.
NRC-USERNAME	https://secure.netop.com	Attribute	user.userprincipalname
NRC-GIVEN-NAME	https://secure.netop.com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



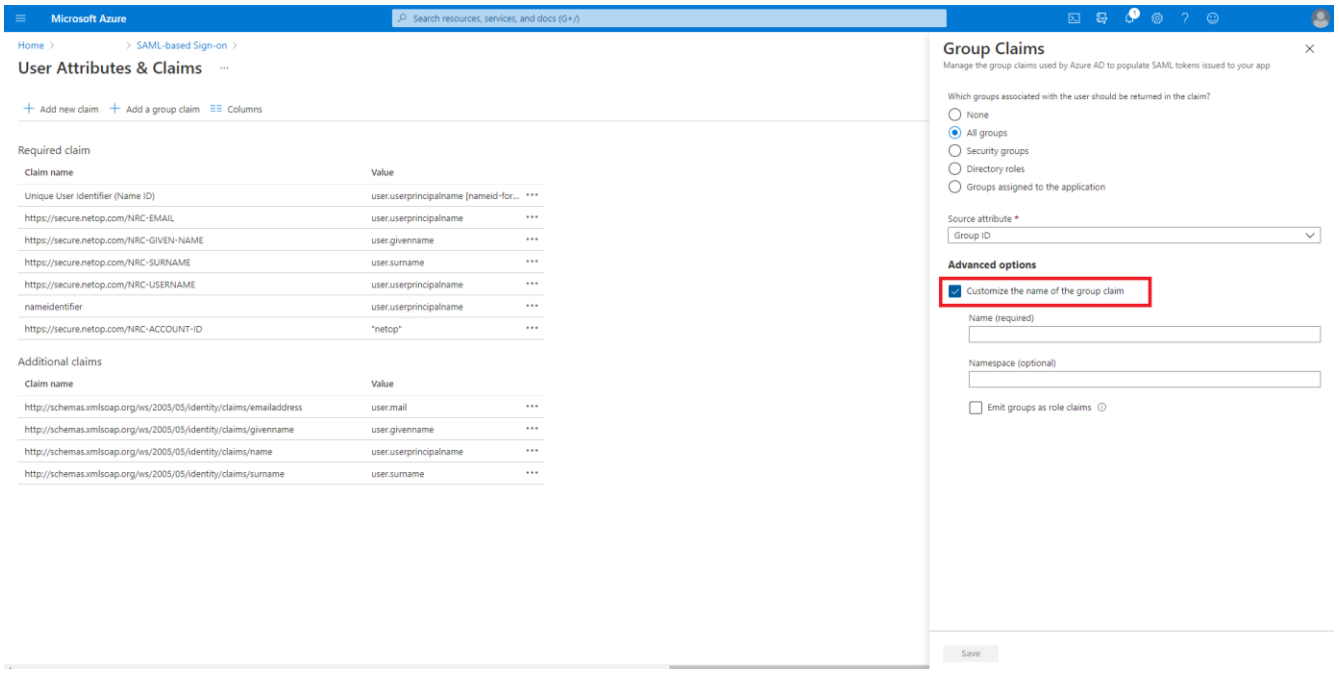
11.1. Select the **All groups** option from the Which groups associated with the user should be returned in the claim section.



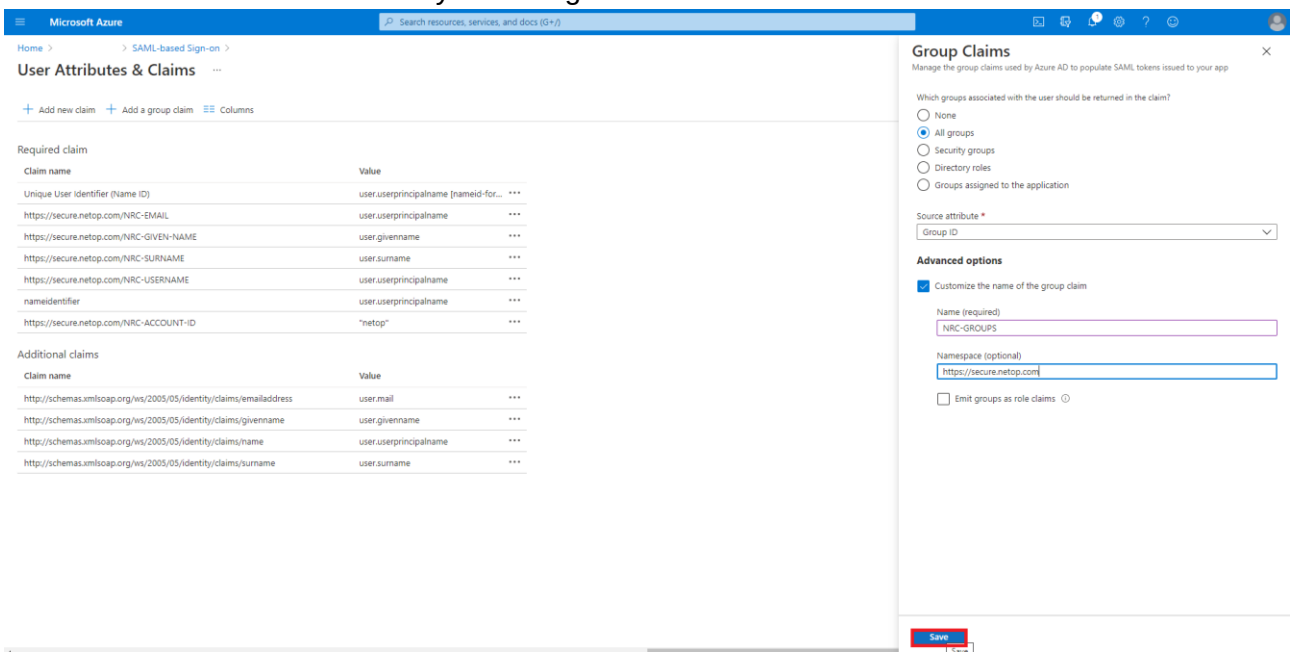
11.2. Click on the **Customize the name of the group claim.**

11.3. Specify the required name and namespace of the claim:

- Name: **NRC-GROUPS**
- Namespace: **https://secure.netop.com**

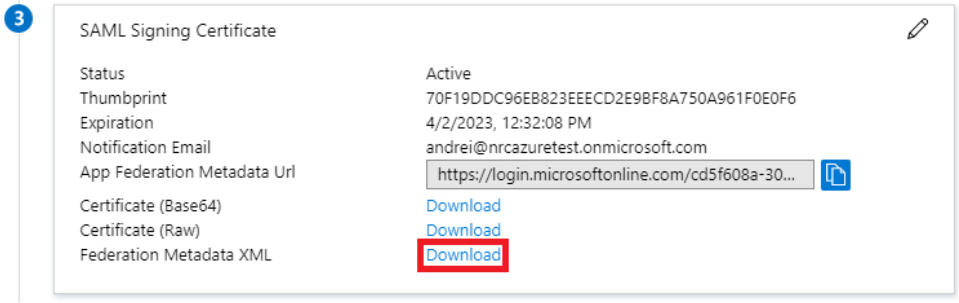


12. Click on the **Save** button to save your changes.

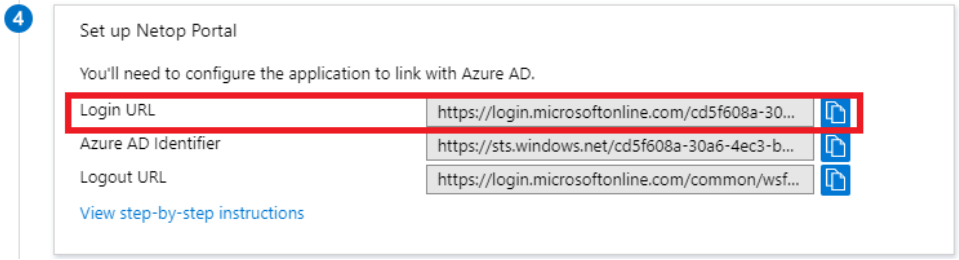


Make sure that you save the following information:

- The **Federation Metadata XML** file



- The **Login URL**



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**.

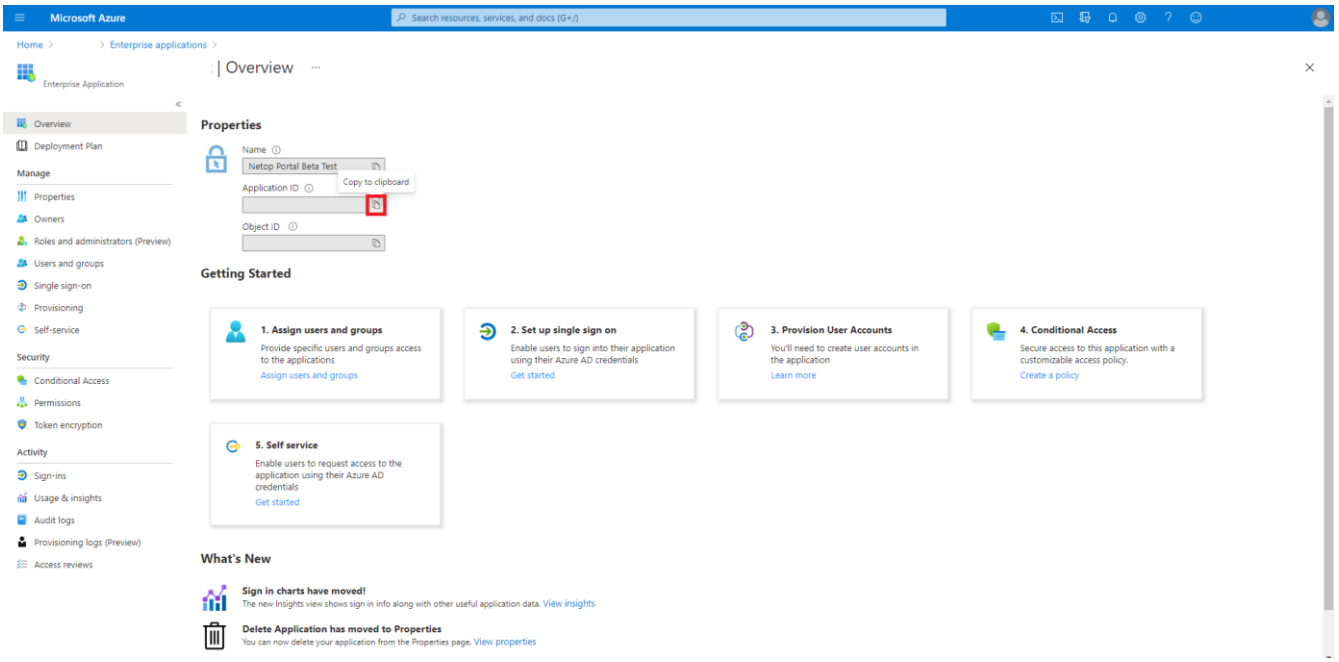
1.2. Go to **Windows Active Directory**.

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.

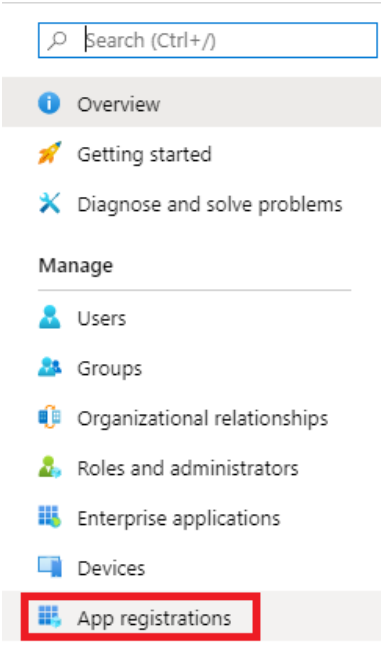


Configure the application permissions

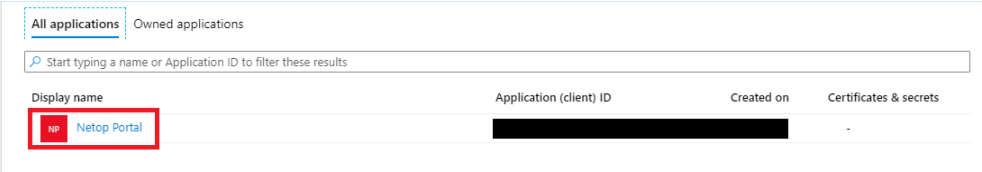
The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**.

To configure the application permissions, proceed as follows:

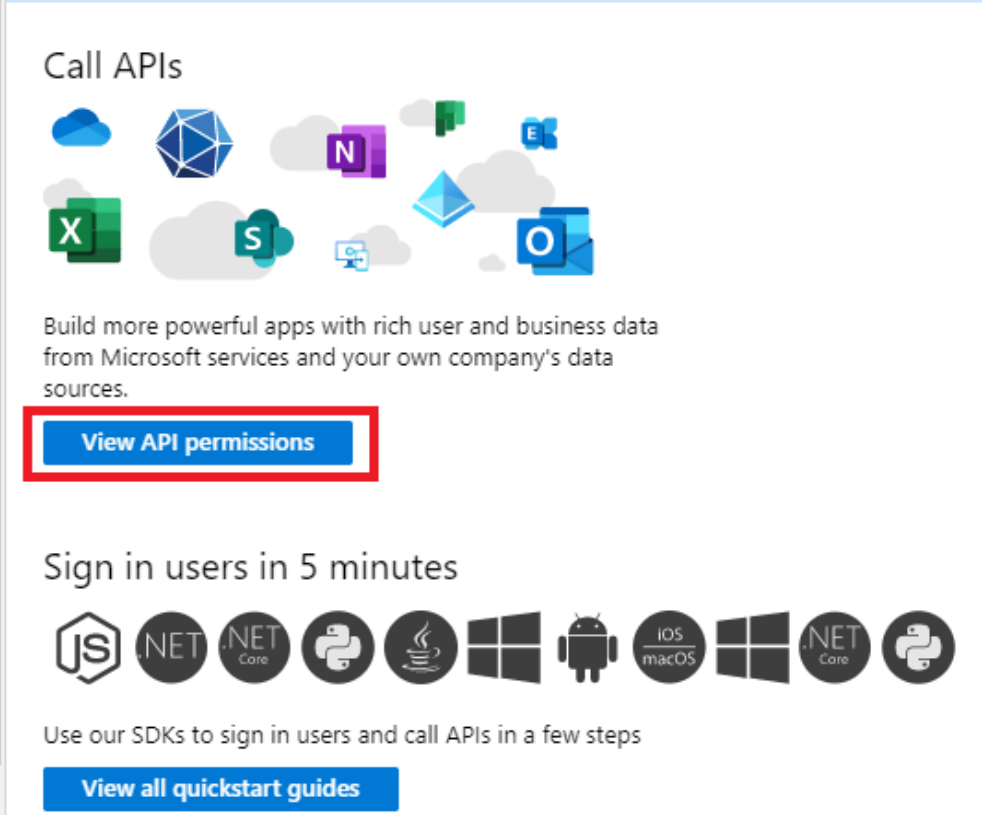
1. Go to **Azure Active Directory**.
2. Go to **App registrations**.



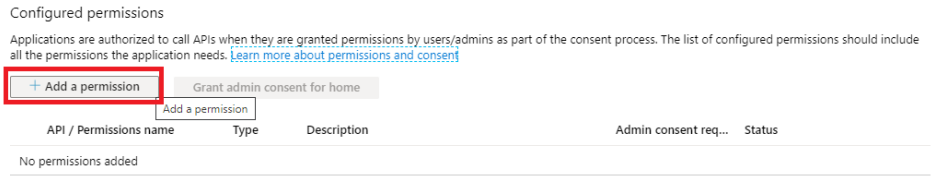
3. Click on the **Netop Portal** application.



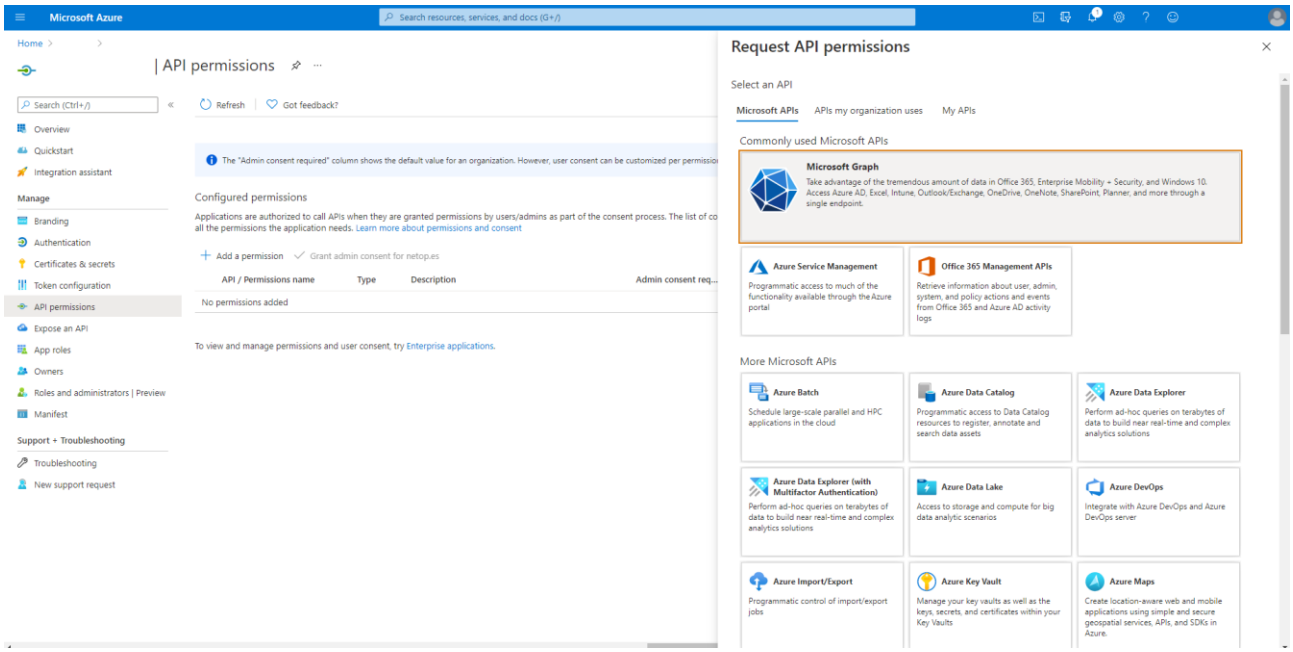
4. Click on the **View API permissions** button.



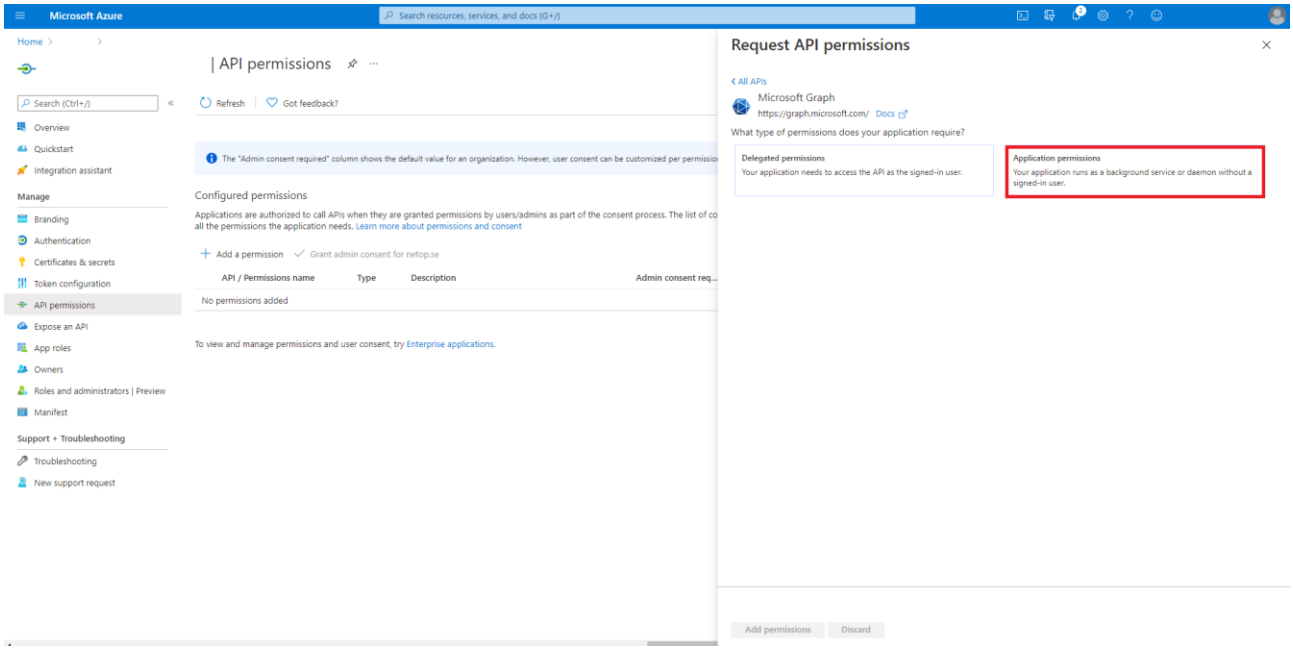
5. Click on the **Add a permission** button to add the necessary permissions.



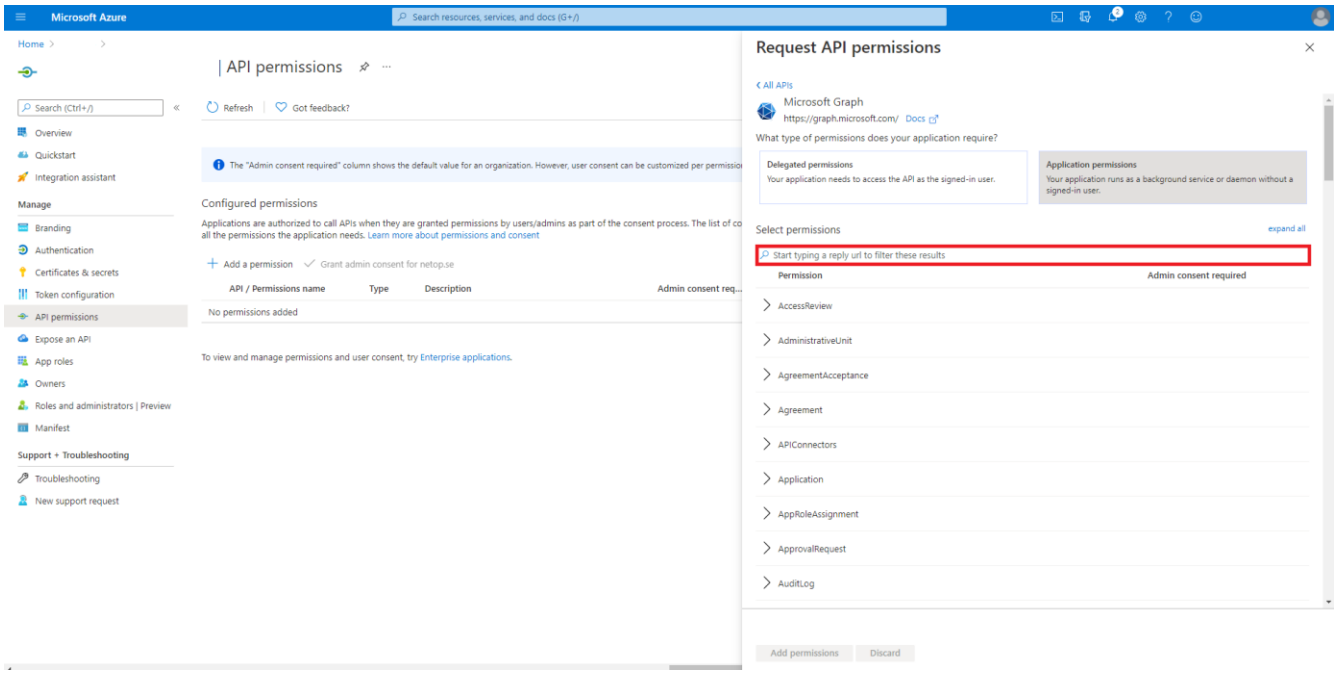
6. Click on Microsoft Graph.



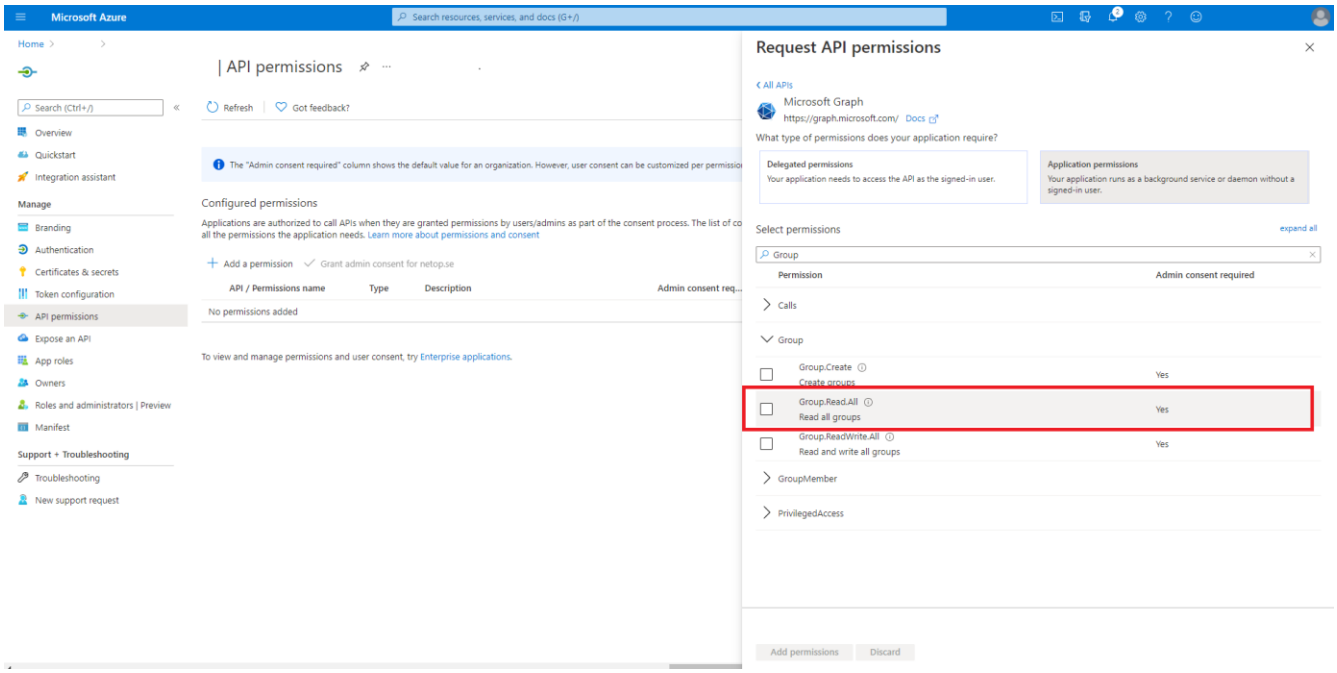
7. Click on **Application permissions**.



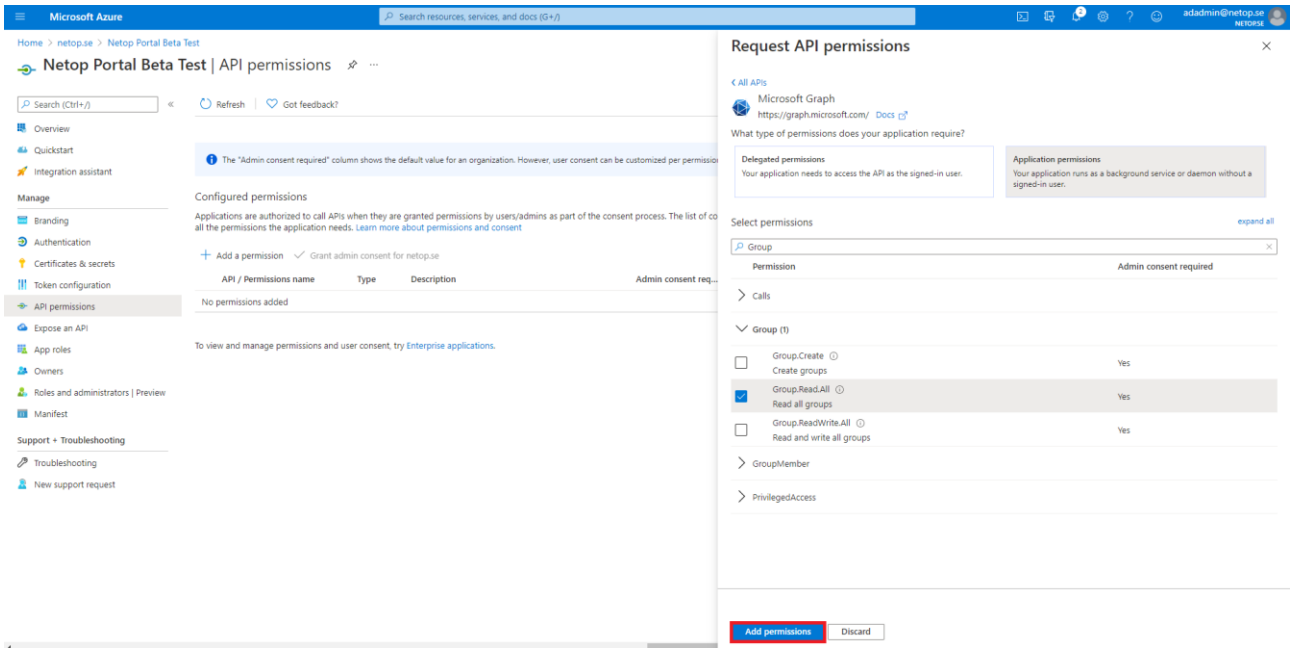
8. Search for Group in the **Start typing a reply url to filter these results** search field.



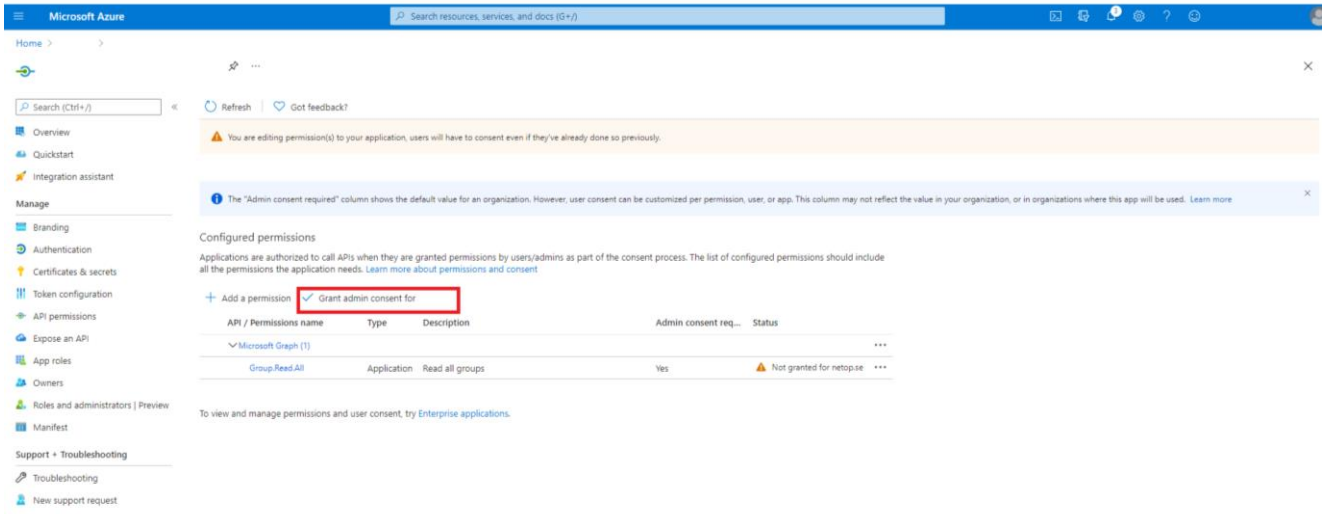
9. Click on the **Group.Read.All** option.



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.

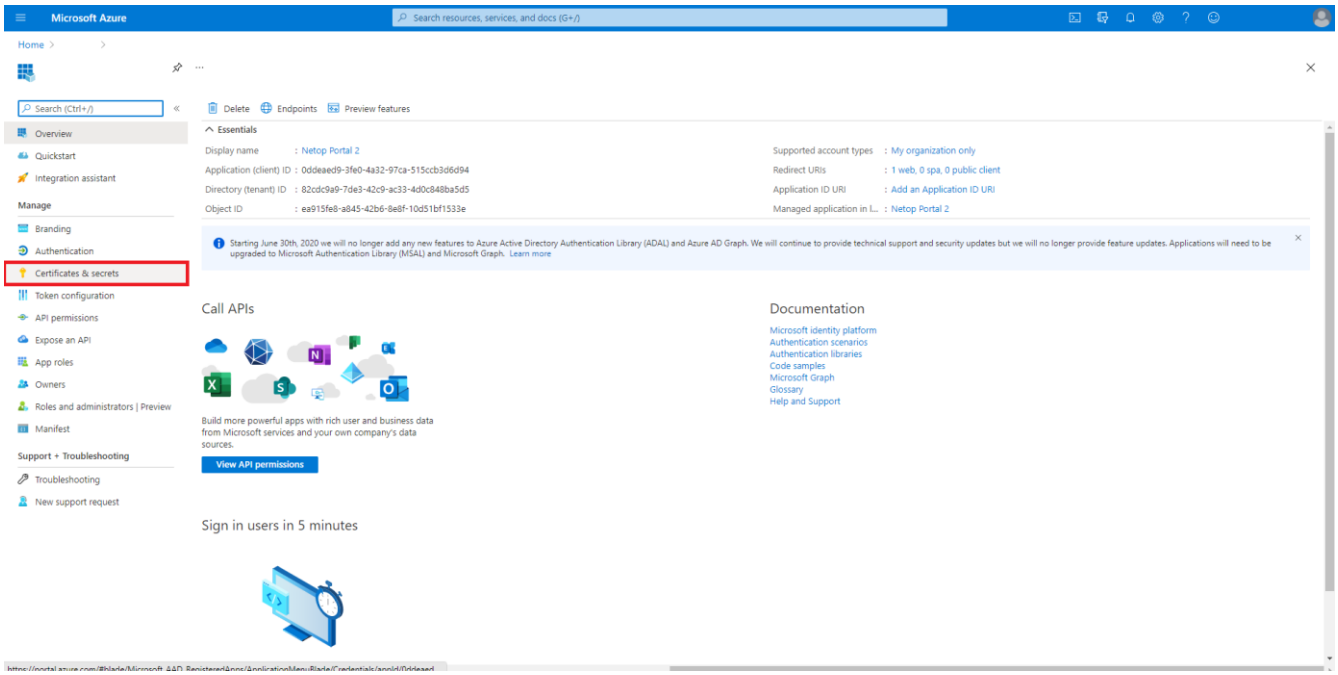


Configure certificates & secrets

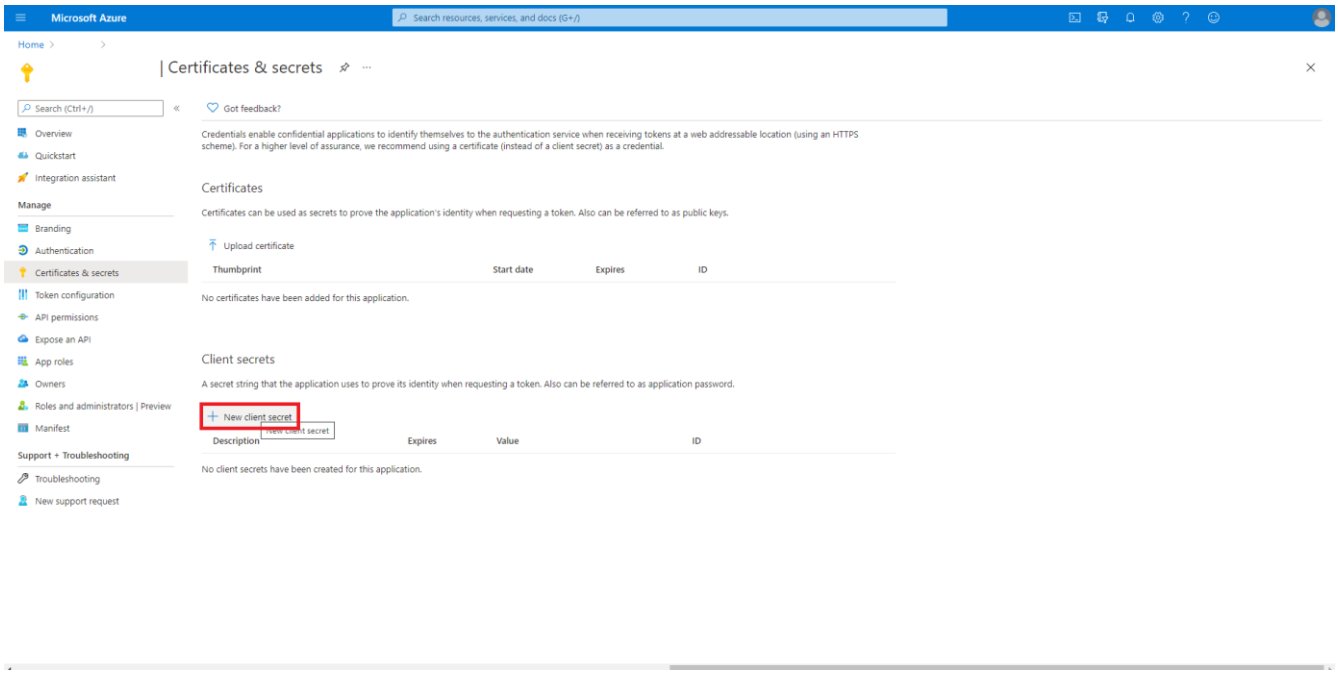
To configure the certificates & secrets for the Netop Portal application in the Azure Portal, proceed as follows:

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

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

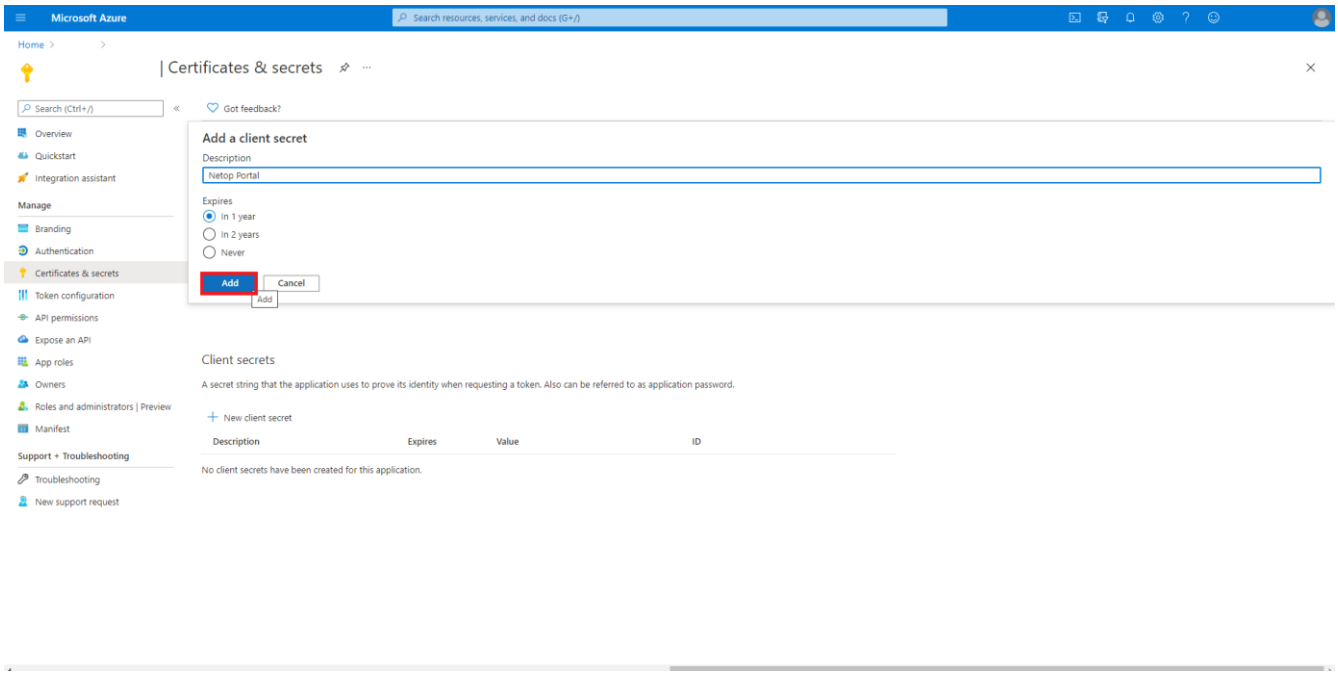


5. Click on the **New client secret** button.

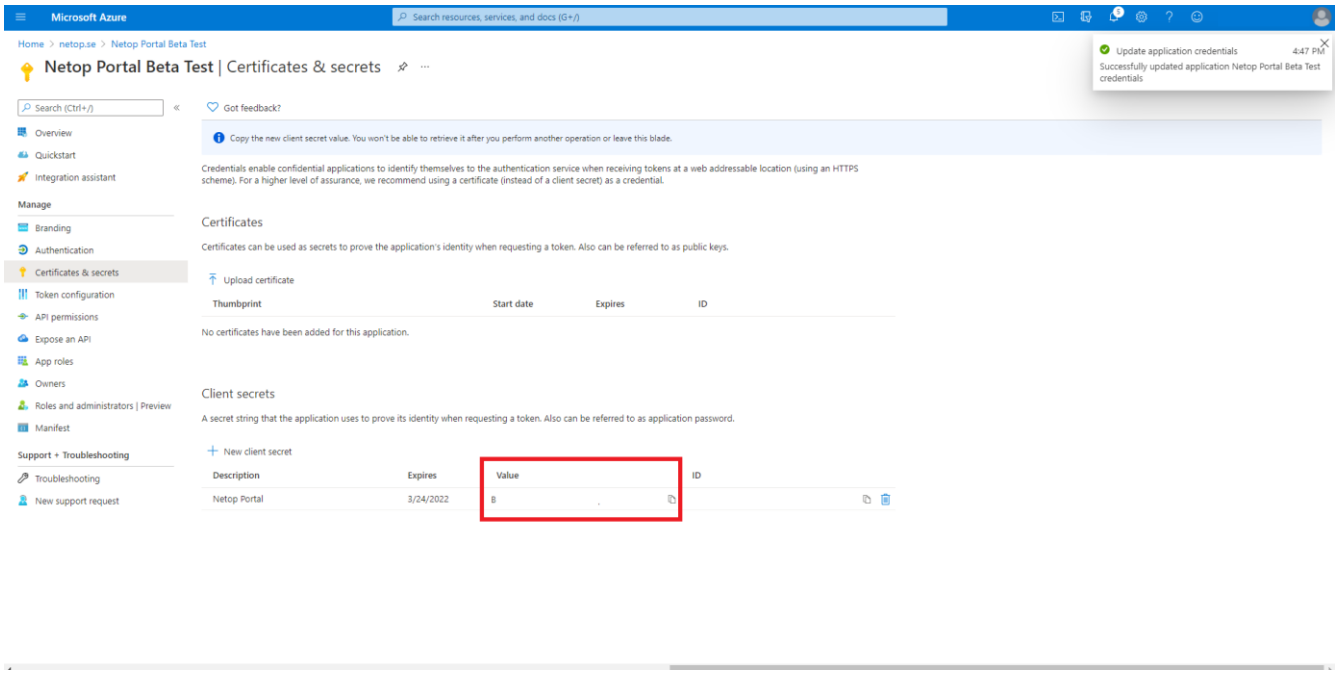


6. Specify a name for the client secret in the **Description** entry field.
7. Specify an expiry date for the client secret accordingly to your needs.

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.



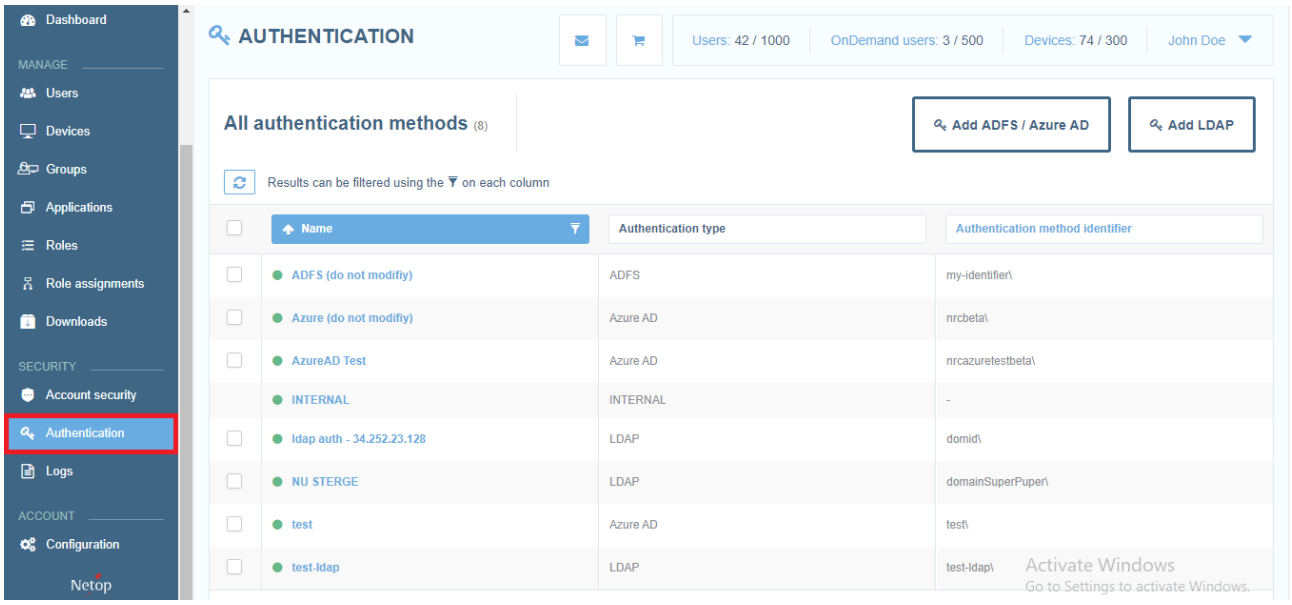
Configure Azure AD in the Netop Portal

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

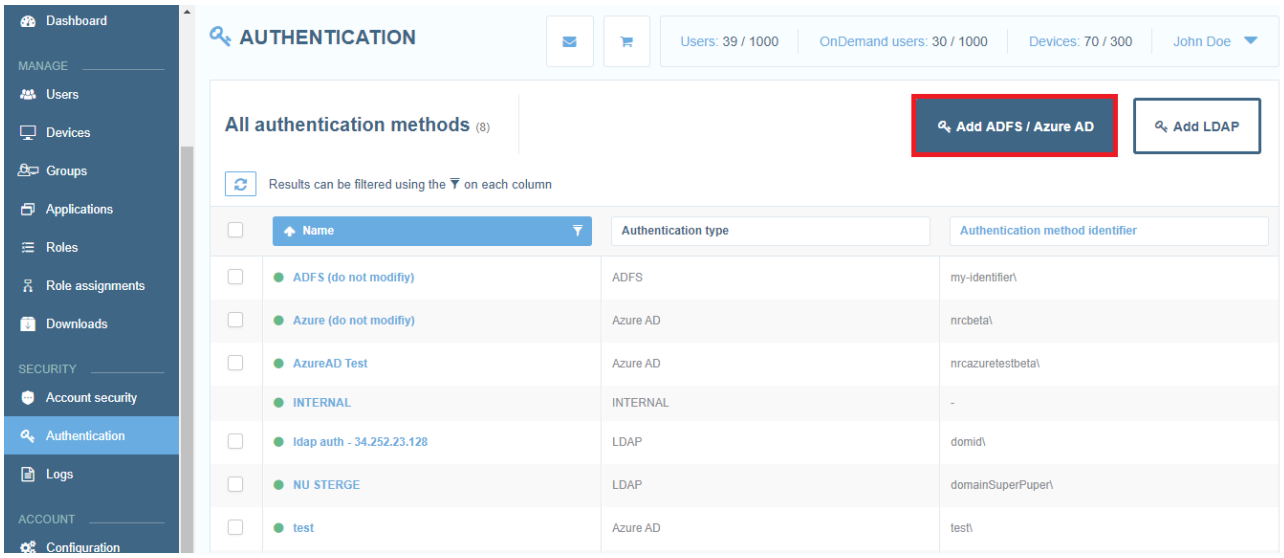
1. Log in to the Netop Portal.

   NOTE: Make sure that you use an administrator account.

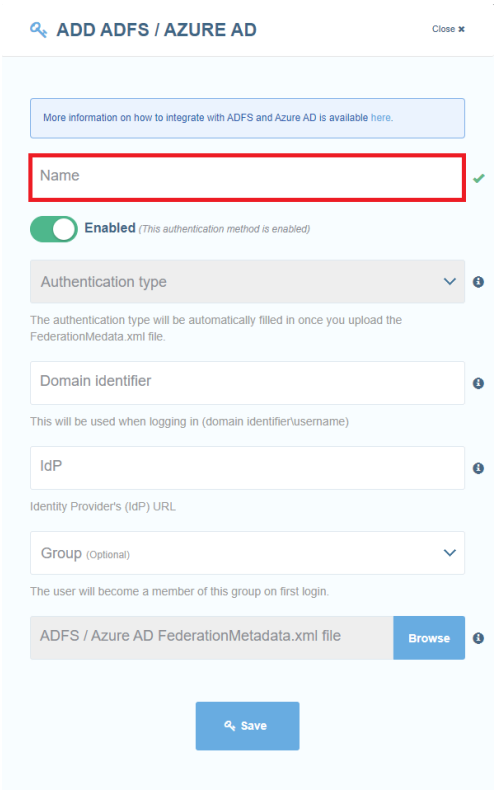
2. Go to **Authentication**.



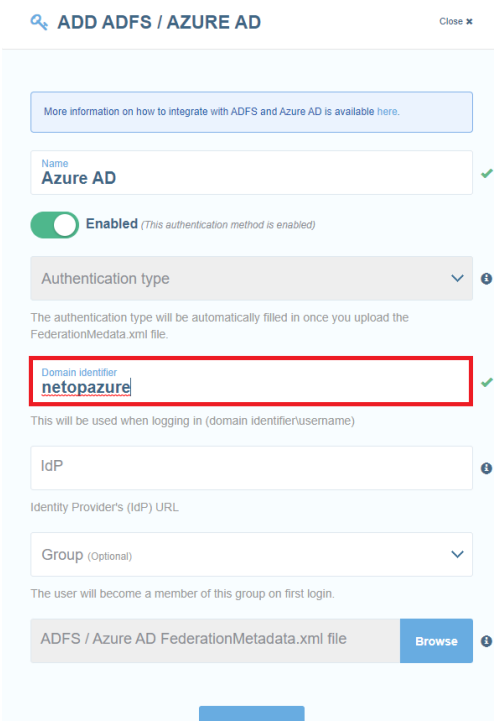
3. Click on the **Add ADFS / Azure AD** button.



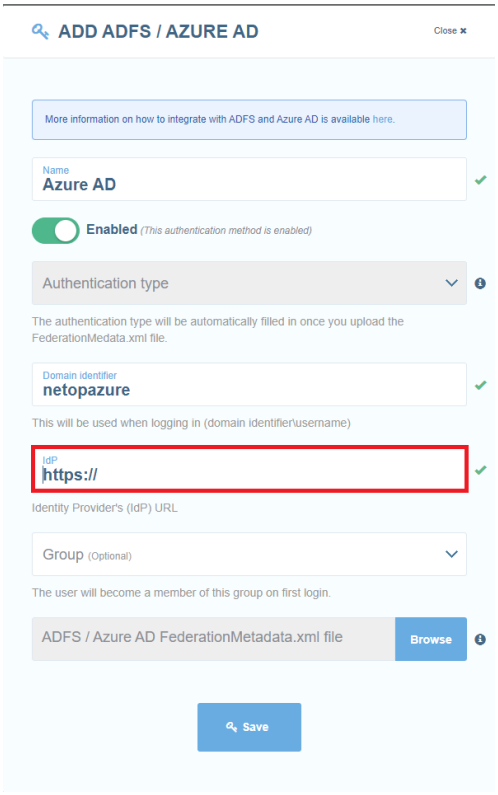
4. Specify a name for the authentication method in the **Name** entry field.



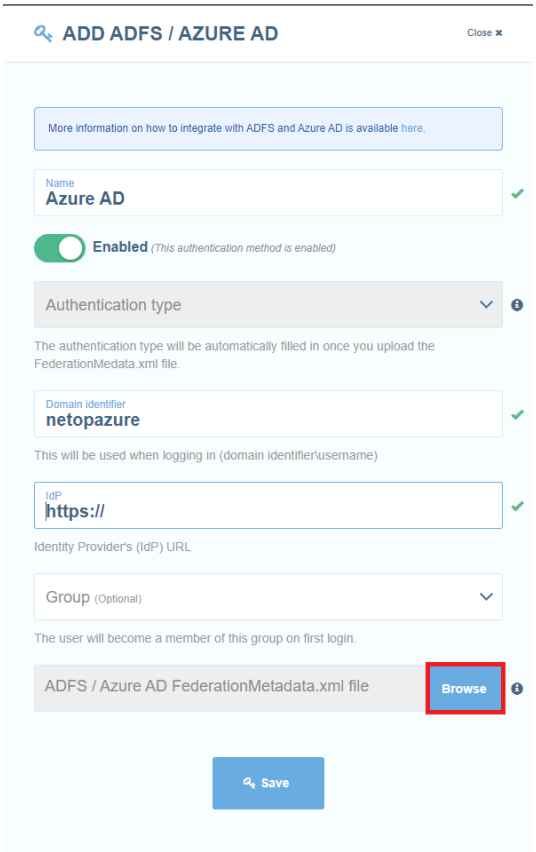
5. Click on the toggle button to enable or disable the authentication method.
6. In the **Domain identifier** entry field, specify the same value as the one specified in the NRC-ACCOUNT-ID user claim.



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



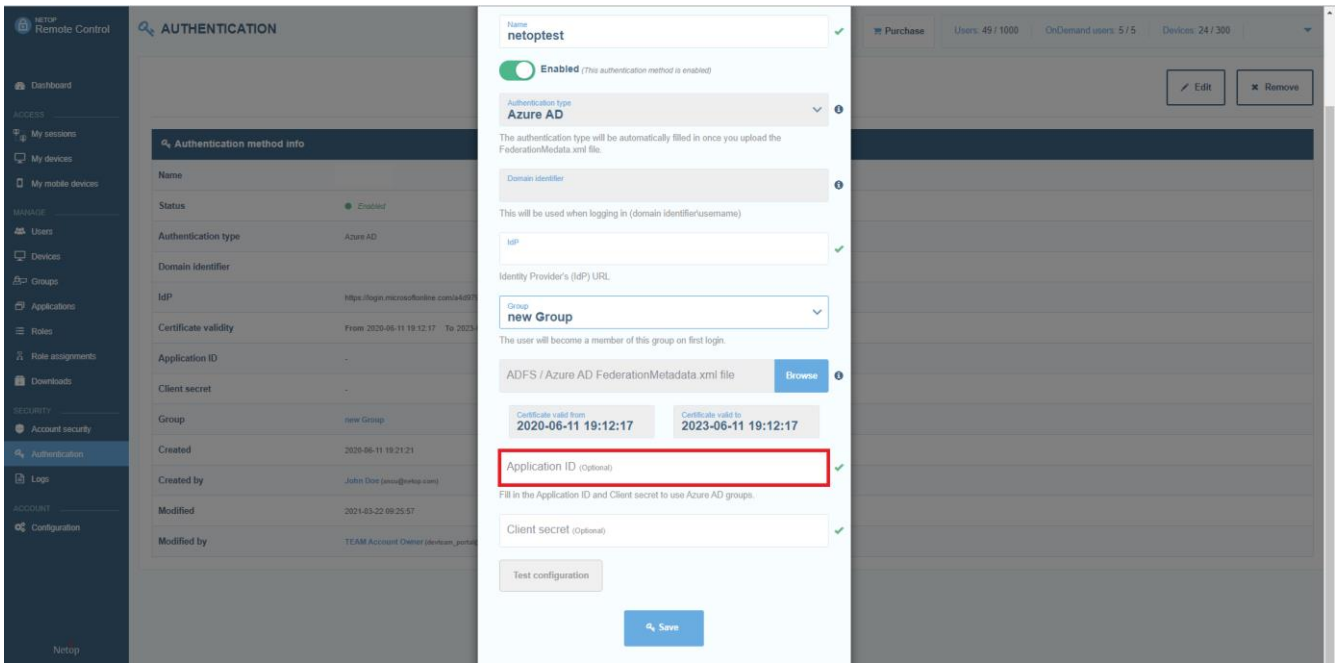
8. In the **ADFS/Azure AD FederationMetadata.xml** field, click on the **Browse** button.



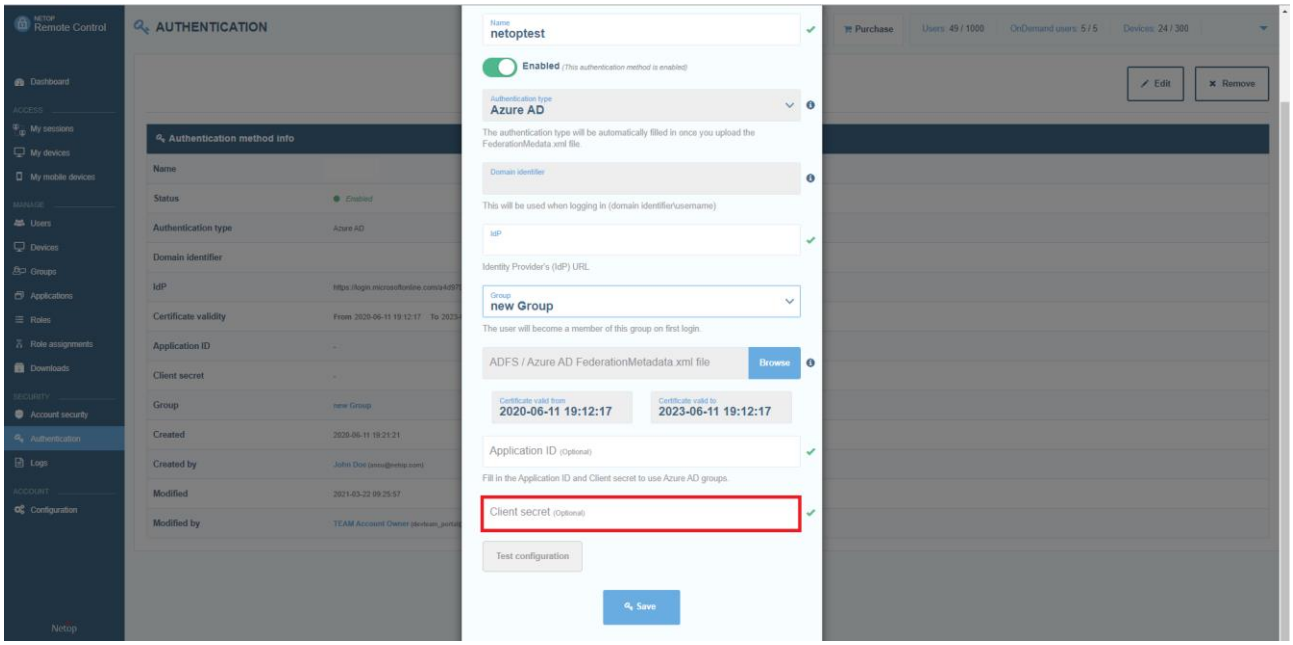
9. Go to the file path where you saved the **FederationMetadata.xml** file, select it, and click on **Open**.

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

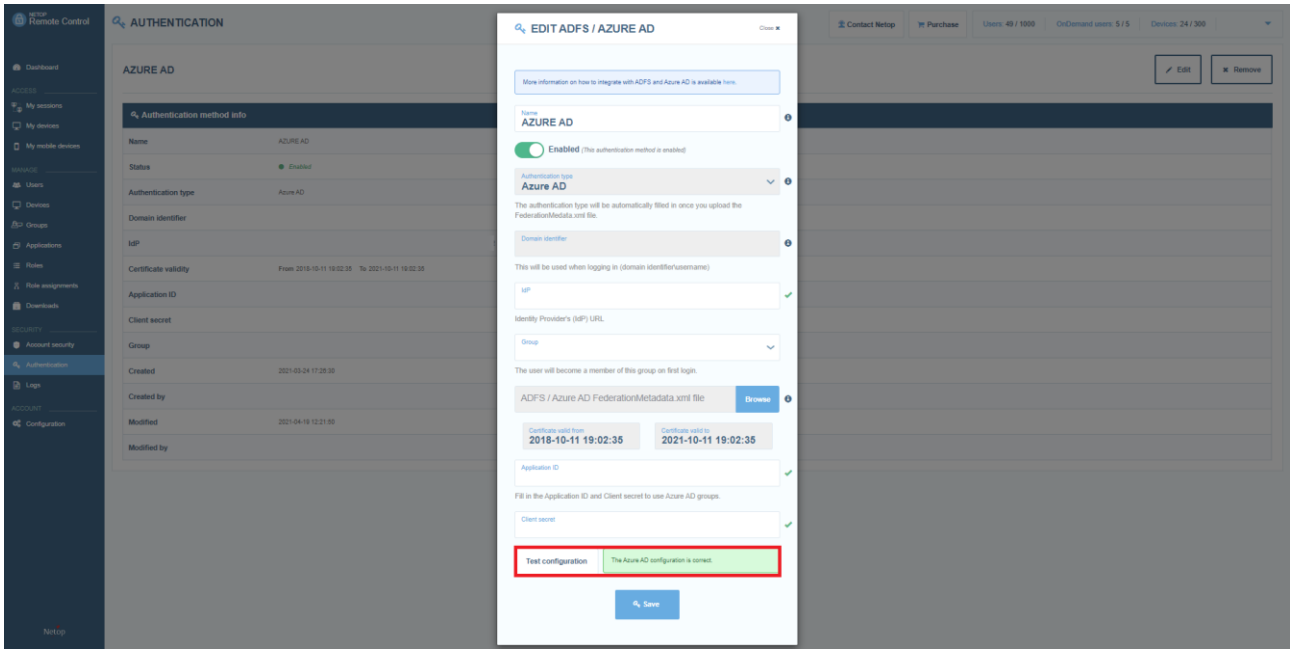
10. In the **Application ID** entry field, specify the Netop Portal **Application ID** from the **Azure Portal**.



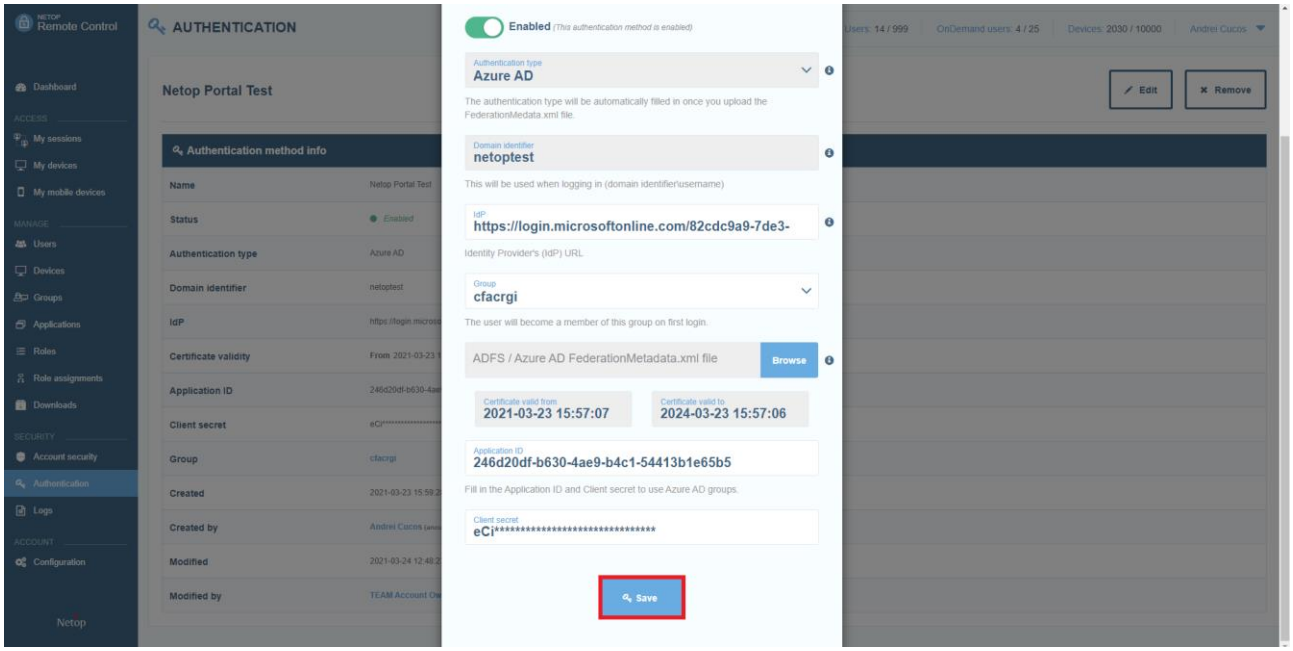
11. In the **Client secret** entry field, specify the client secret value from the **Certificates & secrets** page in the Azure Portal.



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

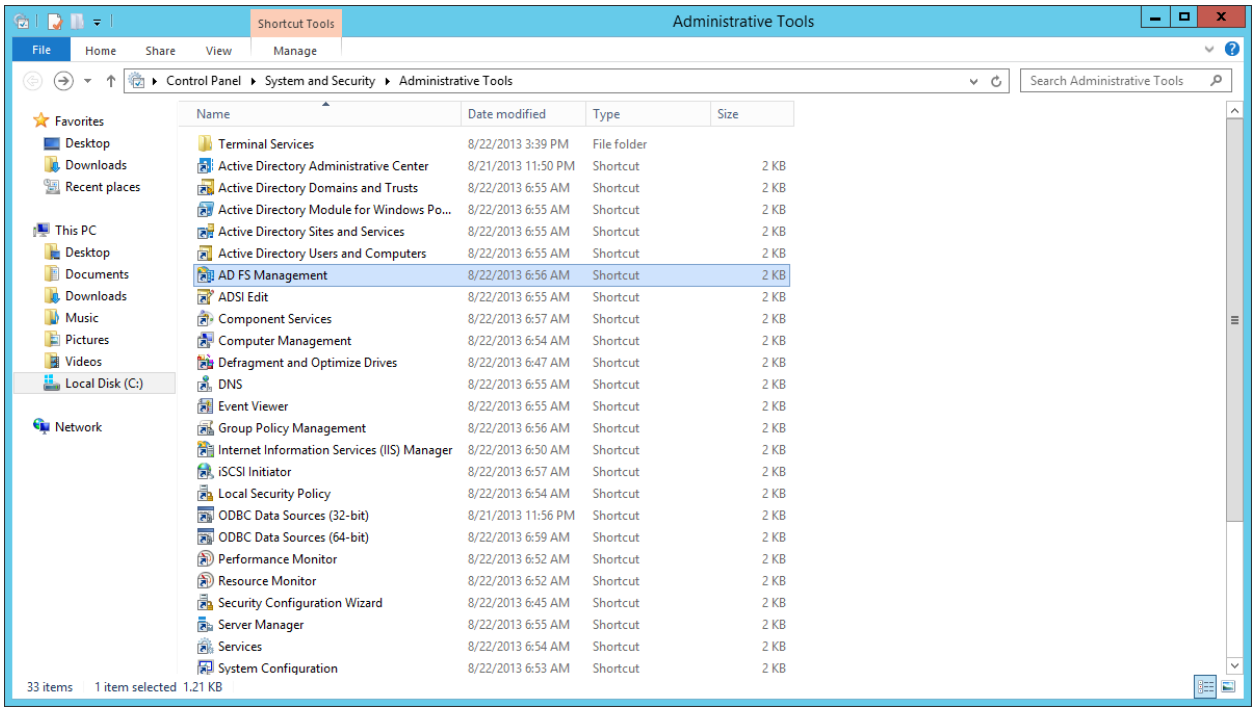
- ADFS 2.0 or later is installed (for more information on how to install ADFS 2.0, refer to the following link)
- The users that authenticate by using ADFS are required to have the following LDAP fields non empty:
  - E-Mail-Addresses
  - Given-Name
  - User-Principal-Name

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

Add Netop Portal as a Trusted Relying Party

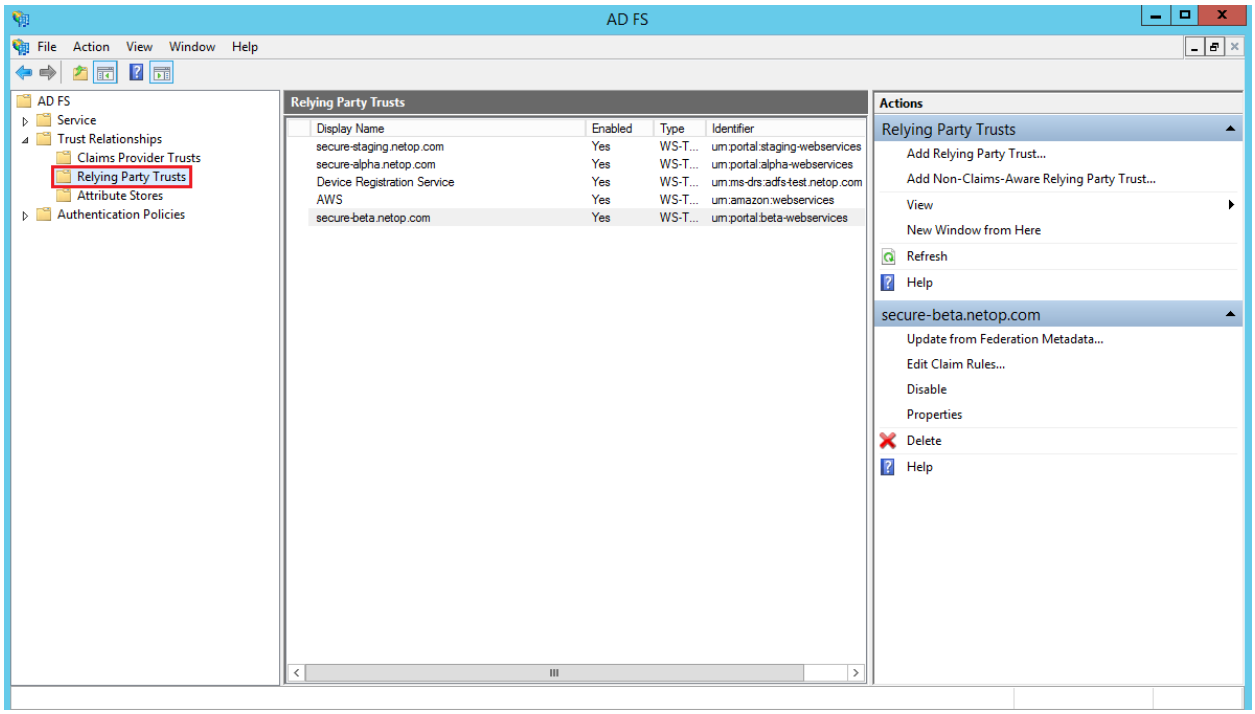
To add the **Netop Portal** as a Trusted Relying Party, proceed as follows:

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

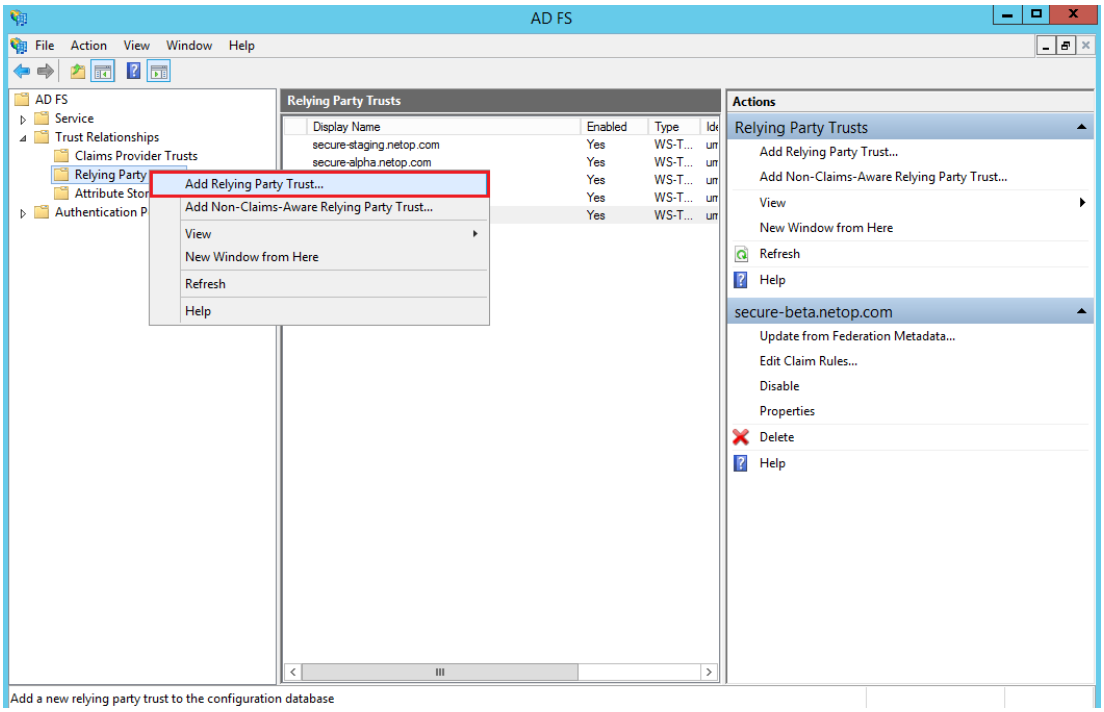


3. Go to **Trust Relationships**.

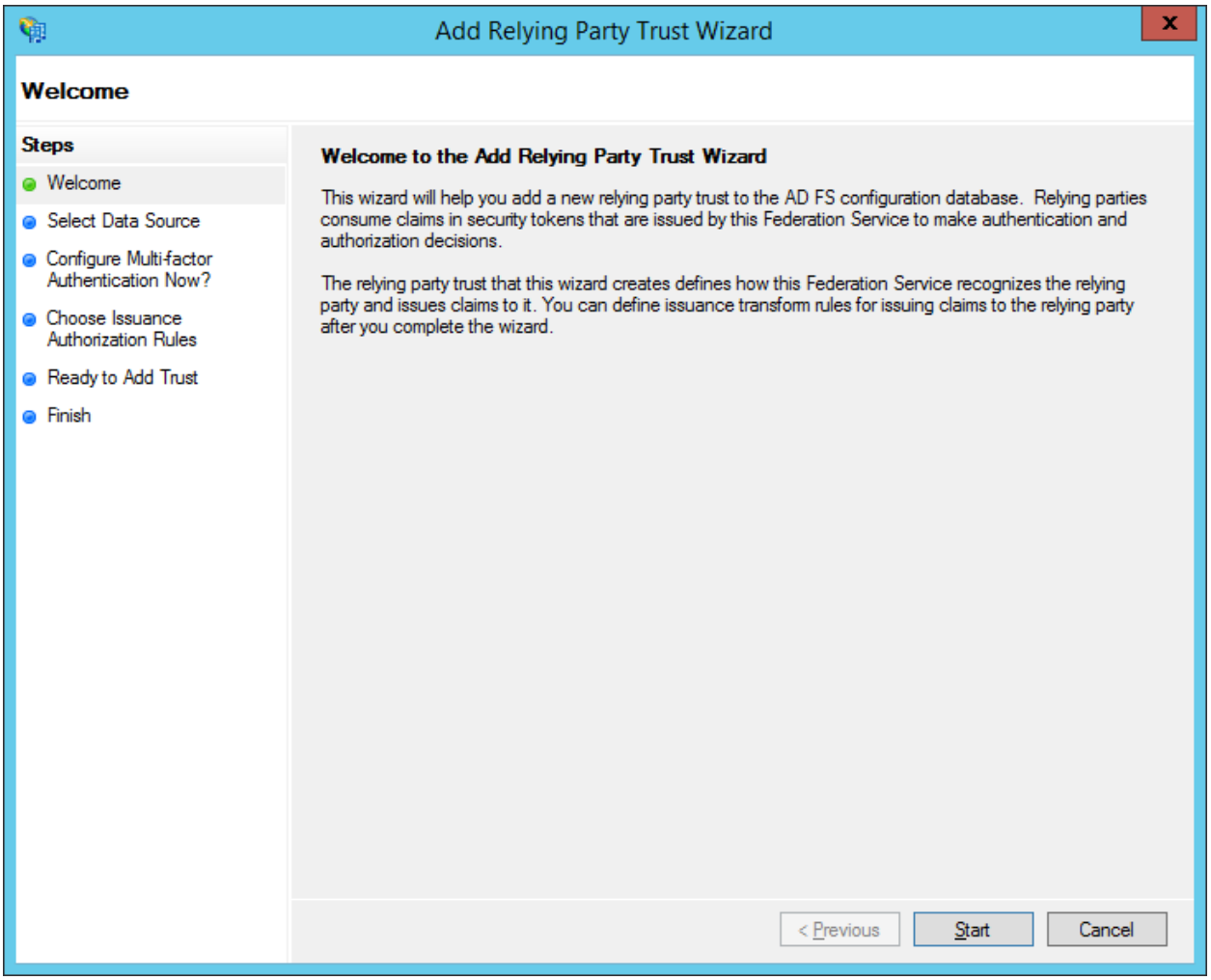
4. Right-click on **Relying Party Trust.**



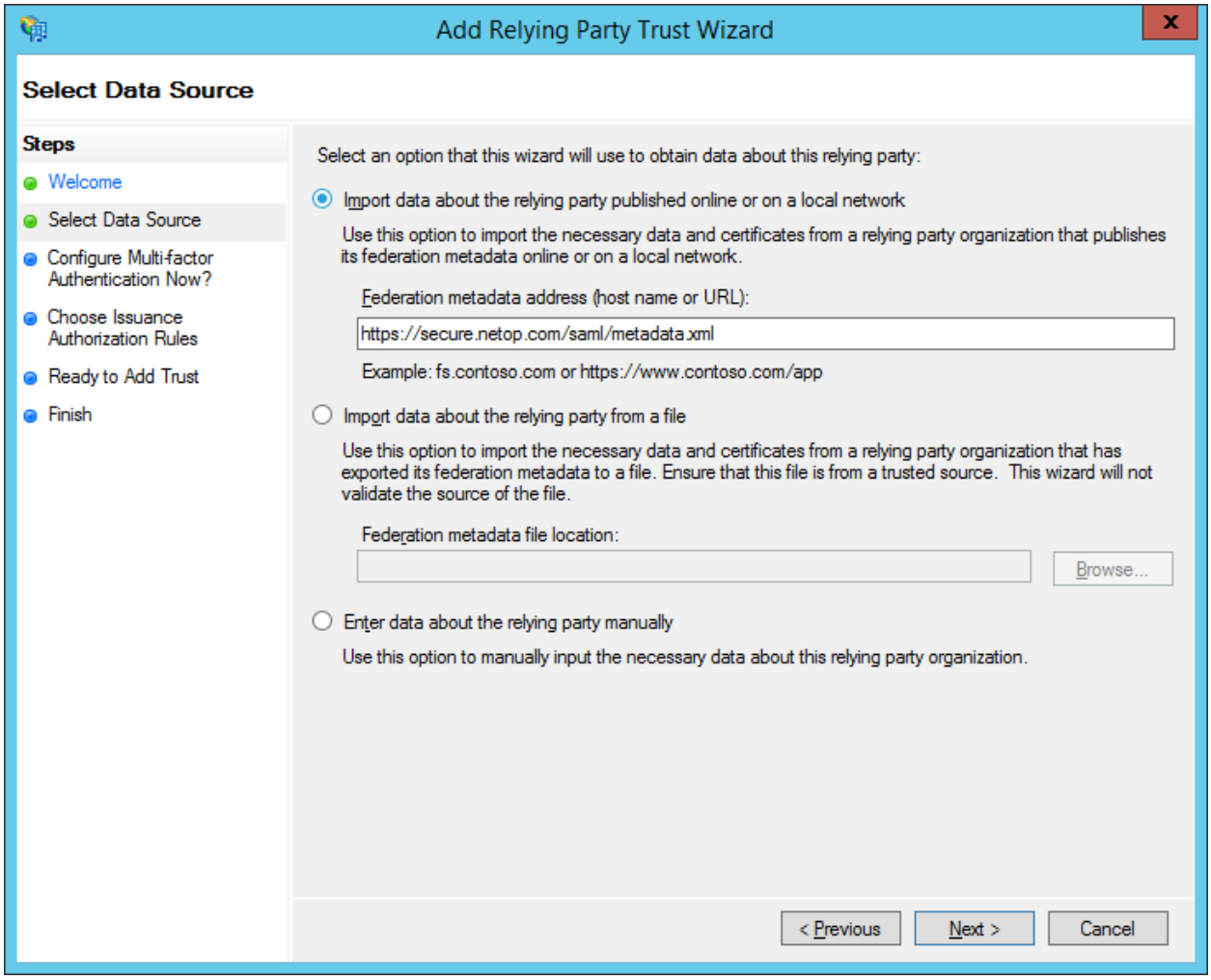
5. Select the **Add Relying Party Trust** option**.** The Add Relying Party Trust Wizard is displayed.



6. Click on **Start.**

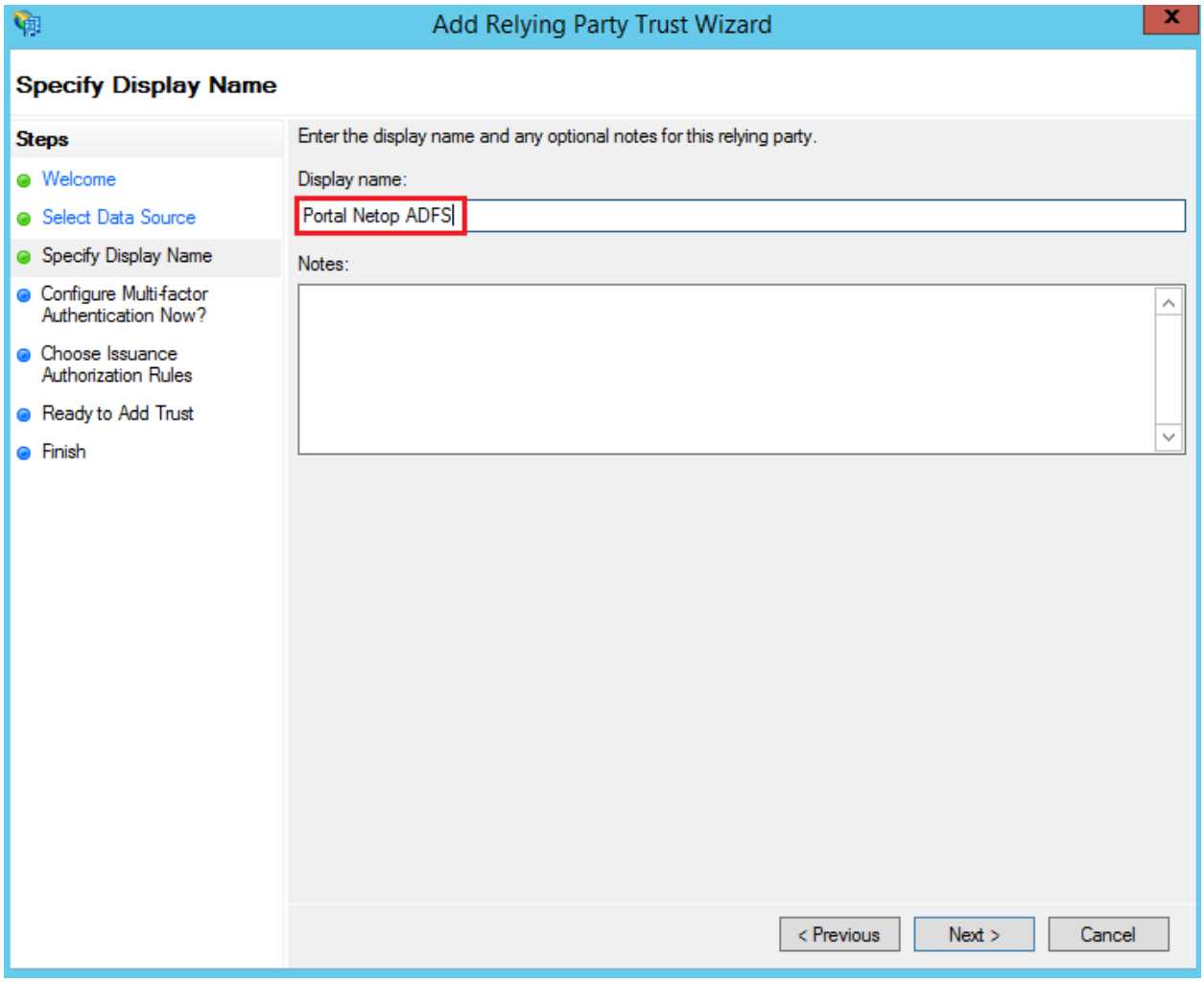


7. Select the **Import data about the relying party published online or on a local network** option.
8. In the Federation metadata address (host name or URL specify the following: [https://secure.netop.com/saml/metadata.xml)](https://secure.netop.com/saml/metadata.xml). The XML metadata file is a standard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



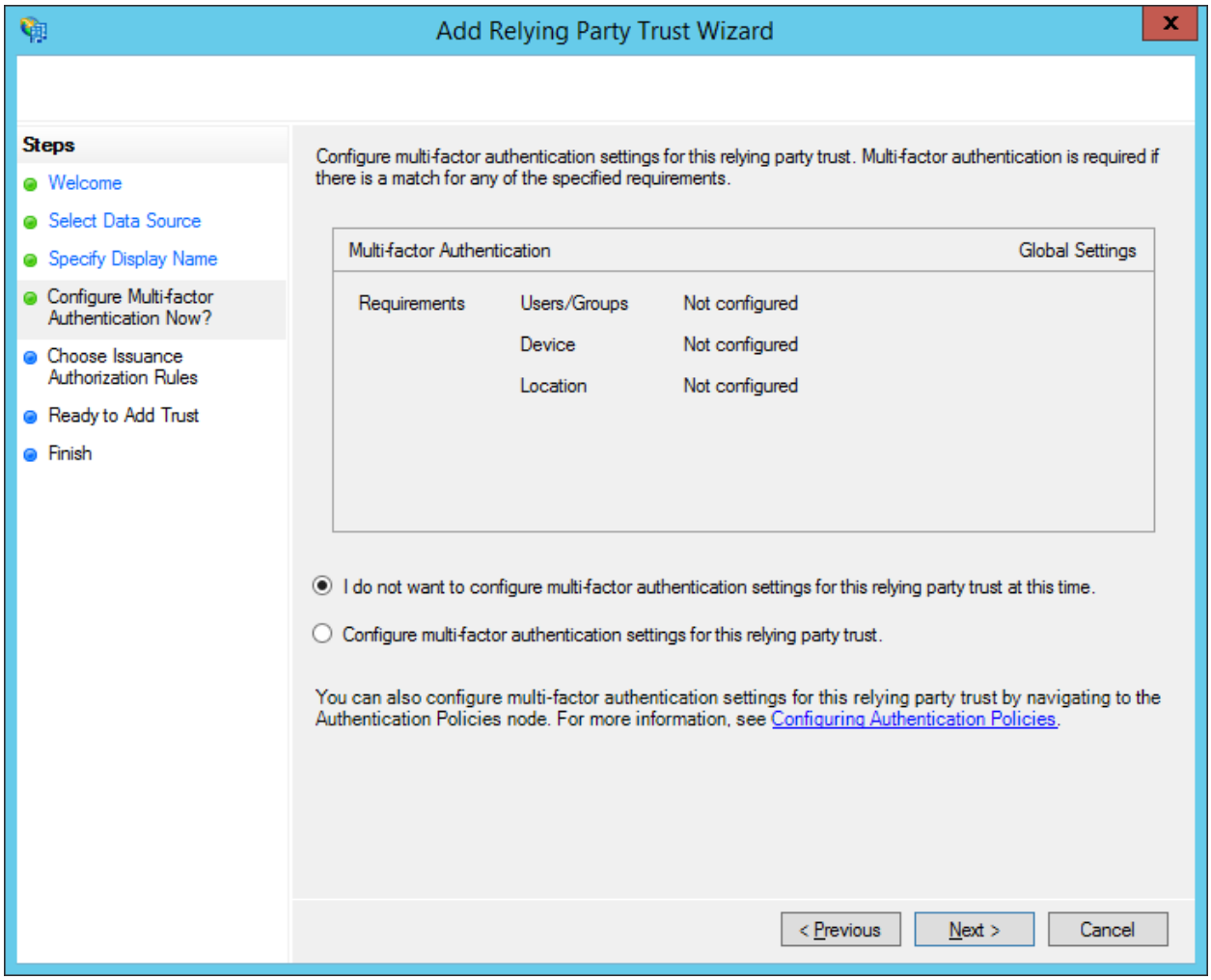
9. Click on **Next**.

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



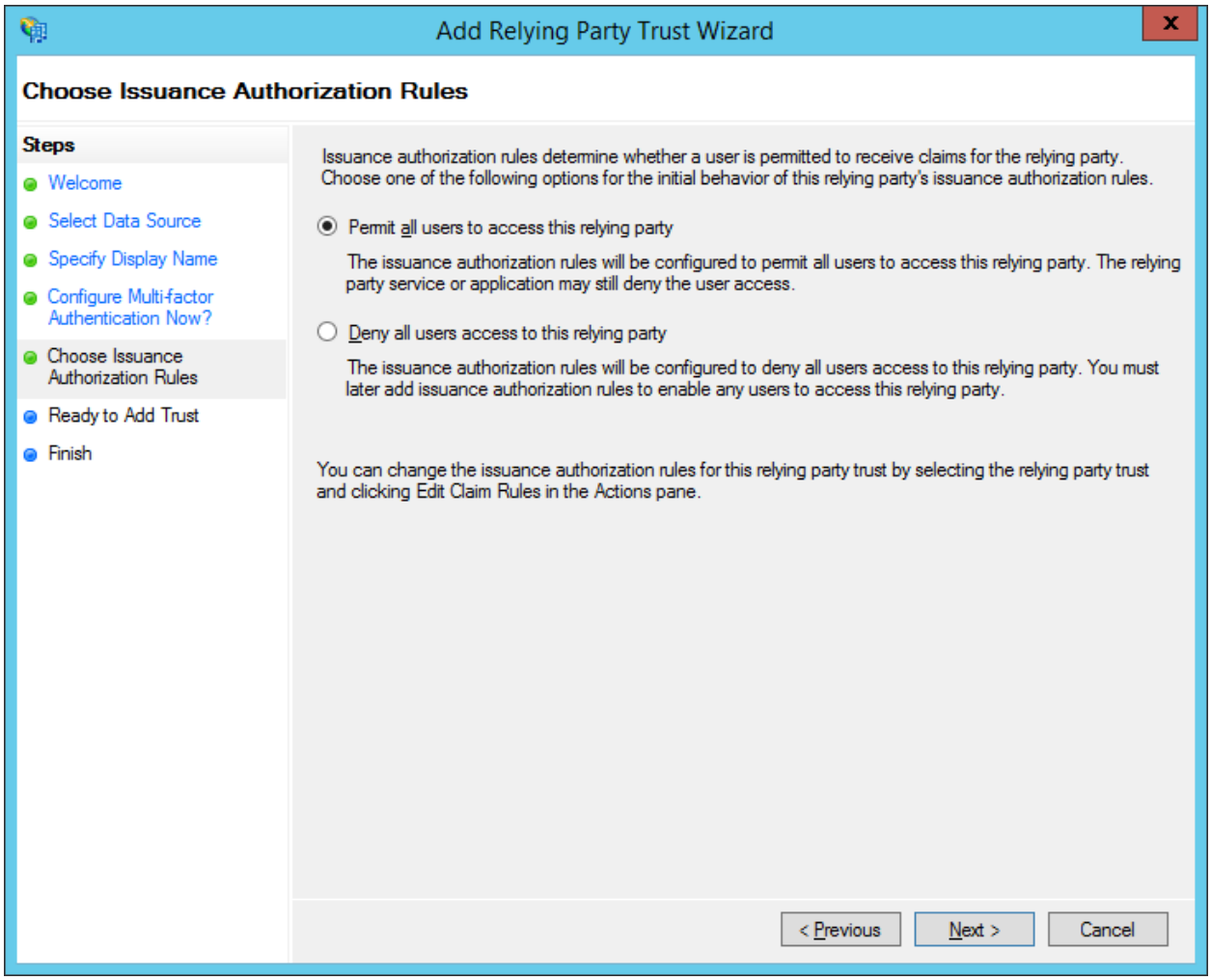
11. Click on **Next.**

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



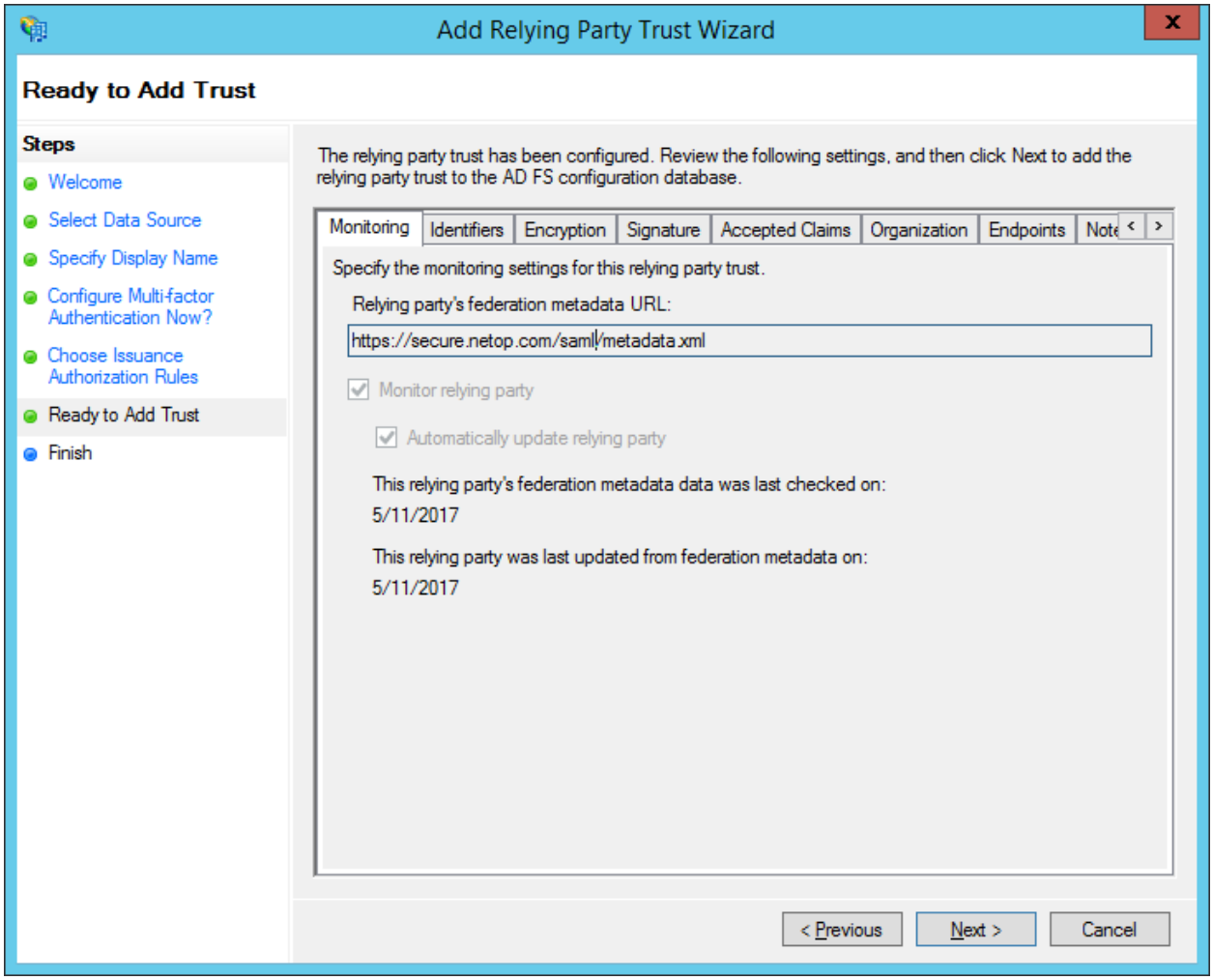
13. Click **on Next.**

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

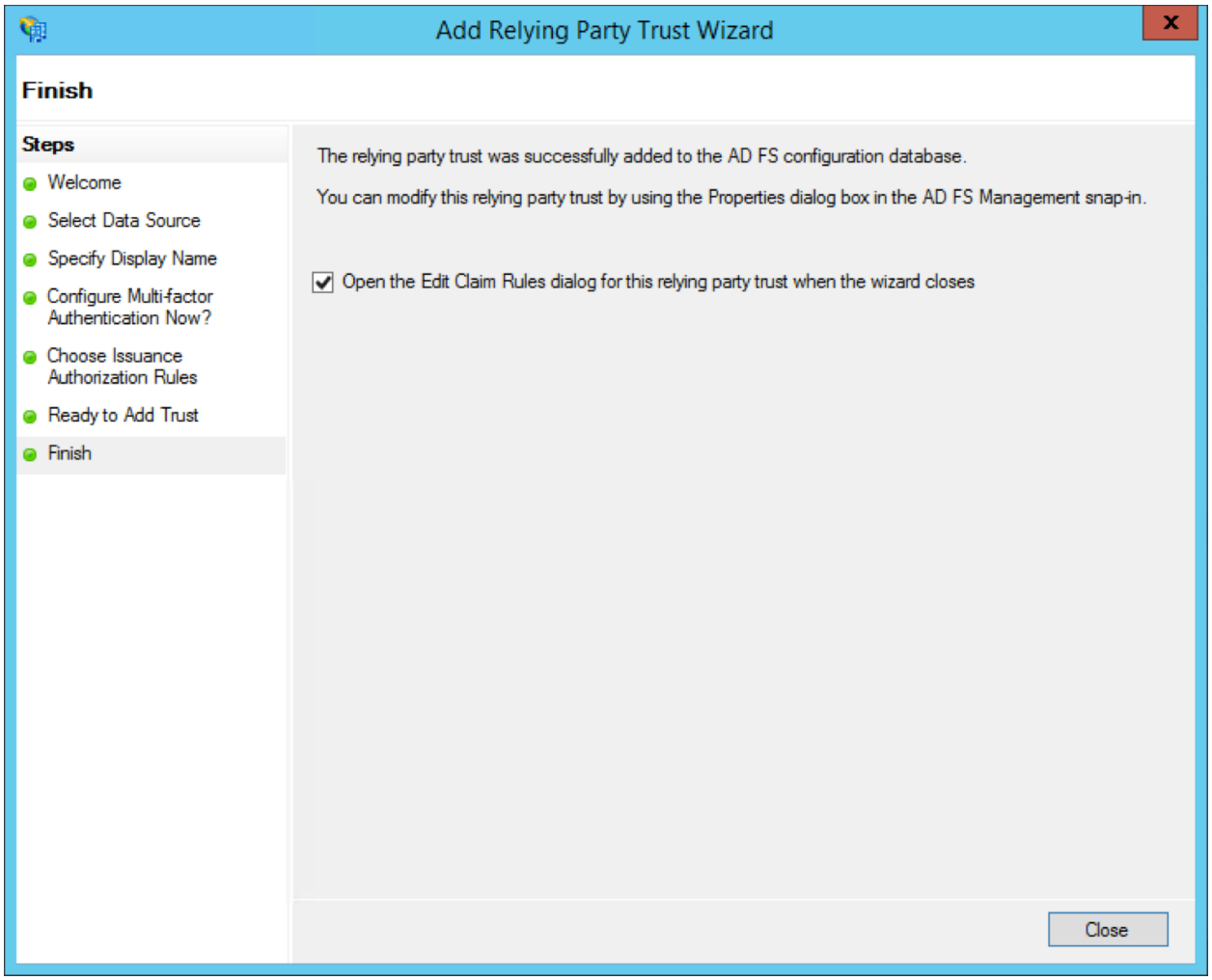


15. Click on **Next.**

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



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



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

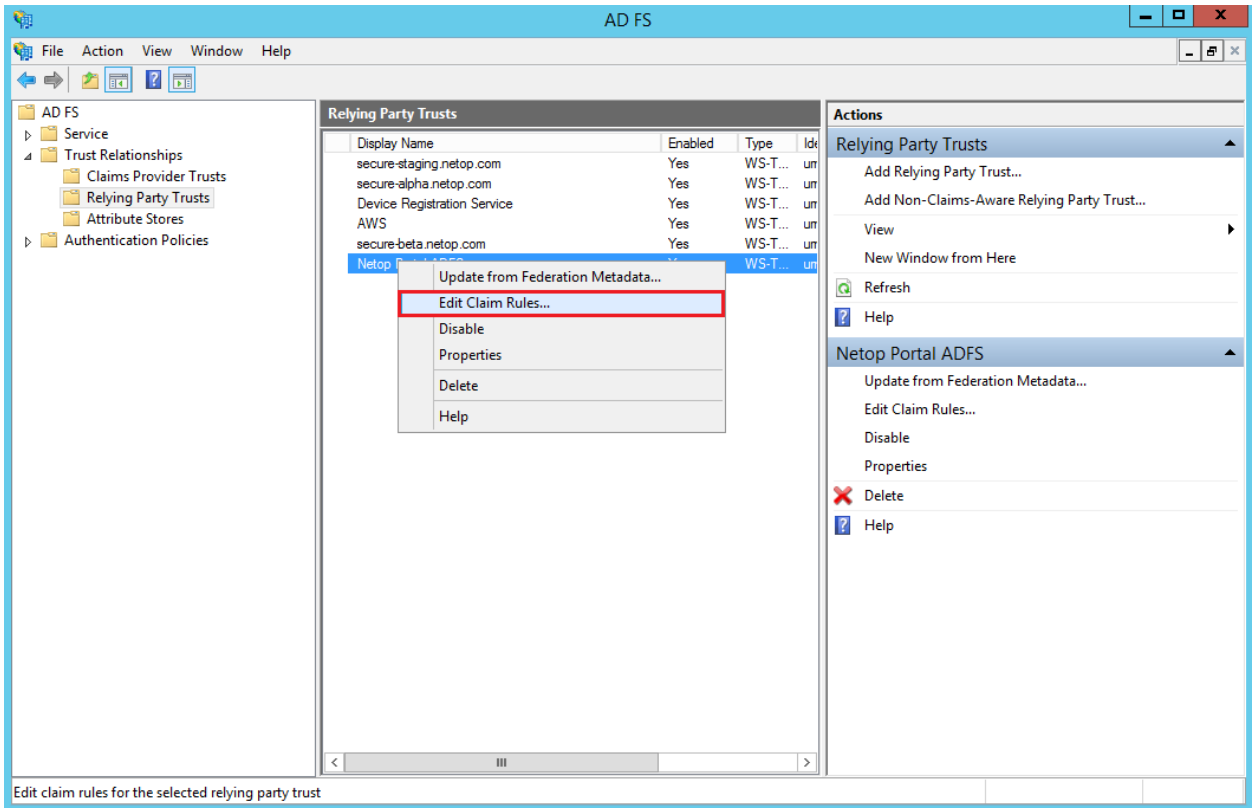
Add Claim Rules for the Netop Portal Relying Party

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.

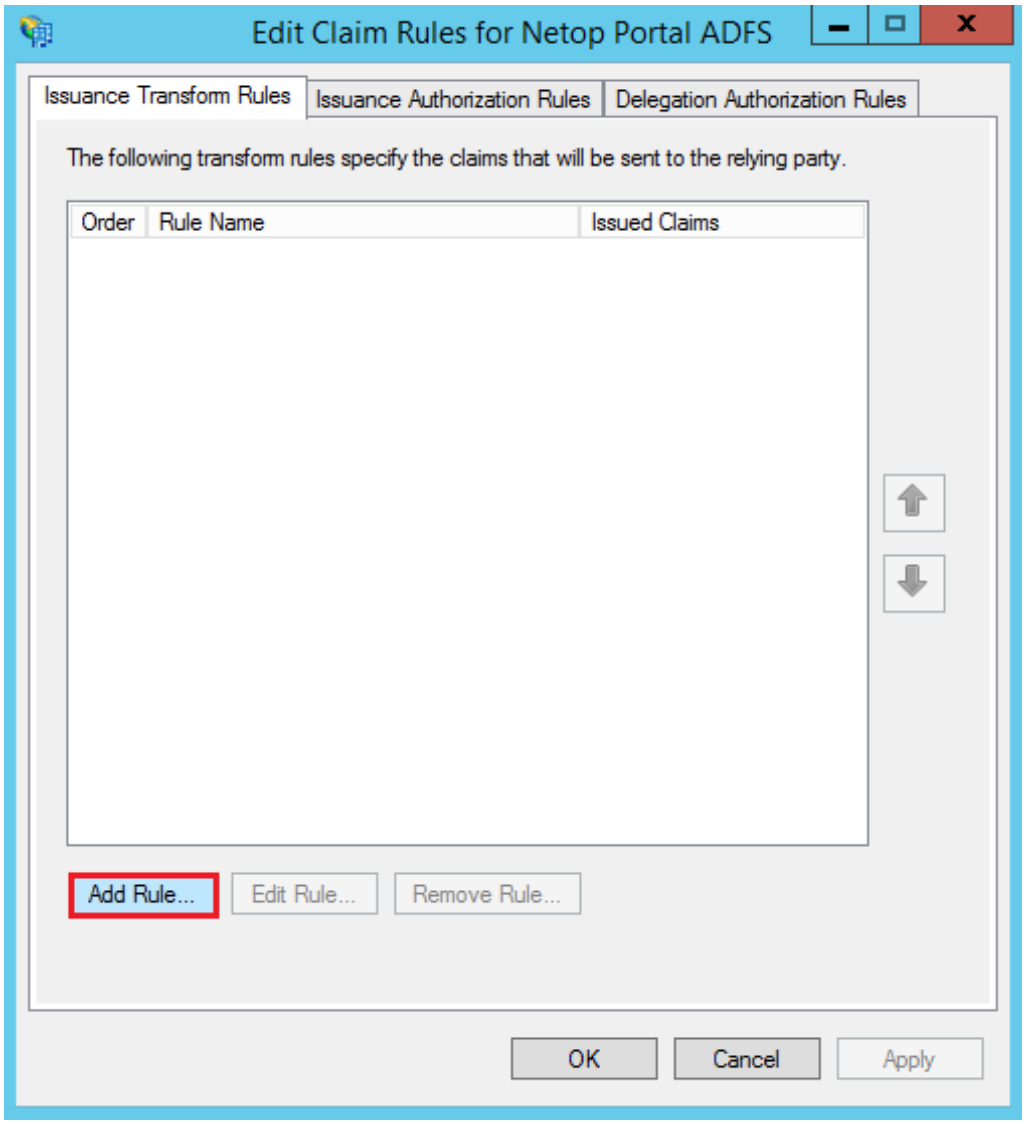
To add the Claim Rules, proceed as follows:

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

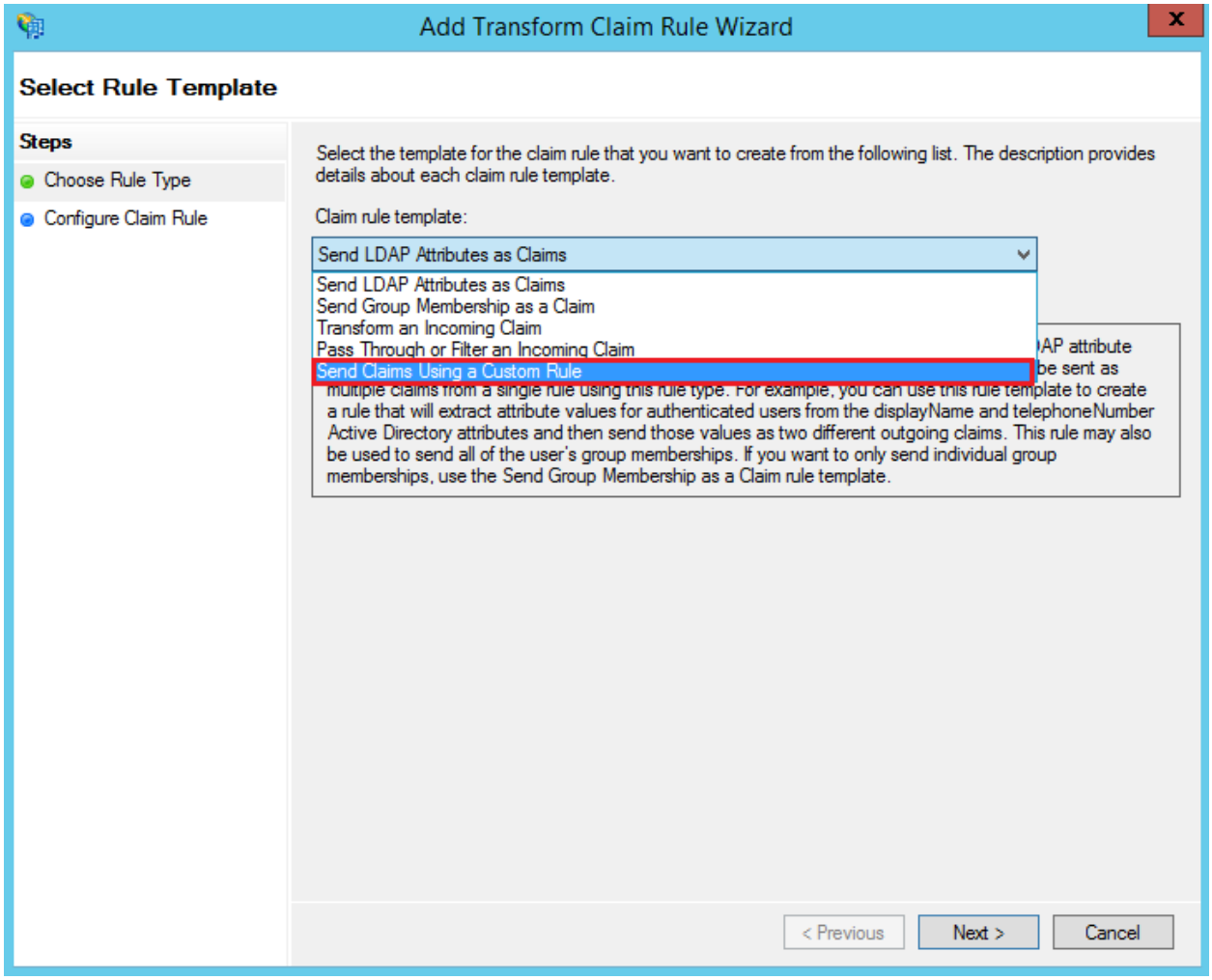
2. Select the **Edit Claim Rules** option.



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

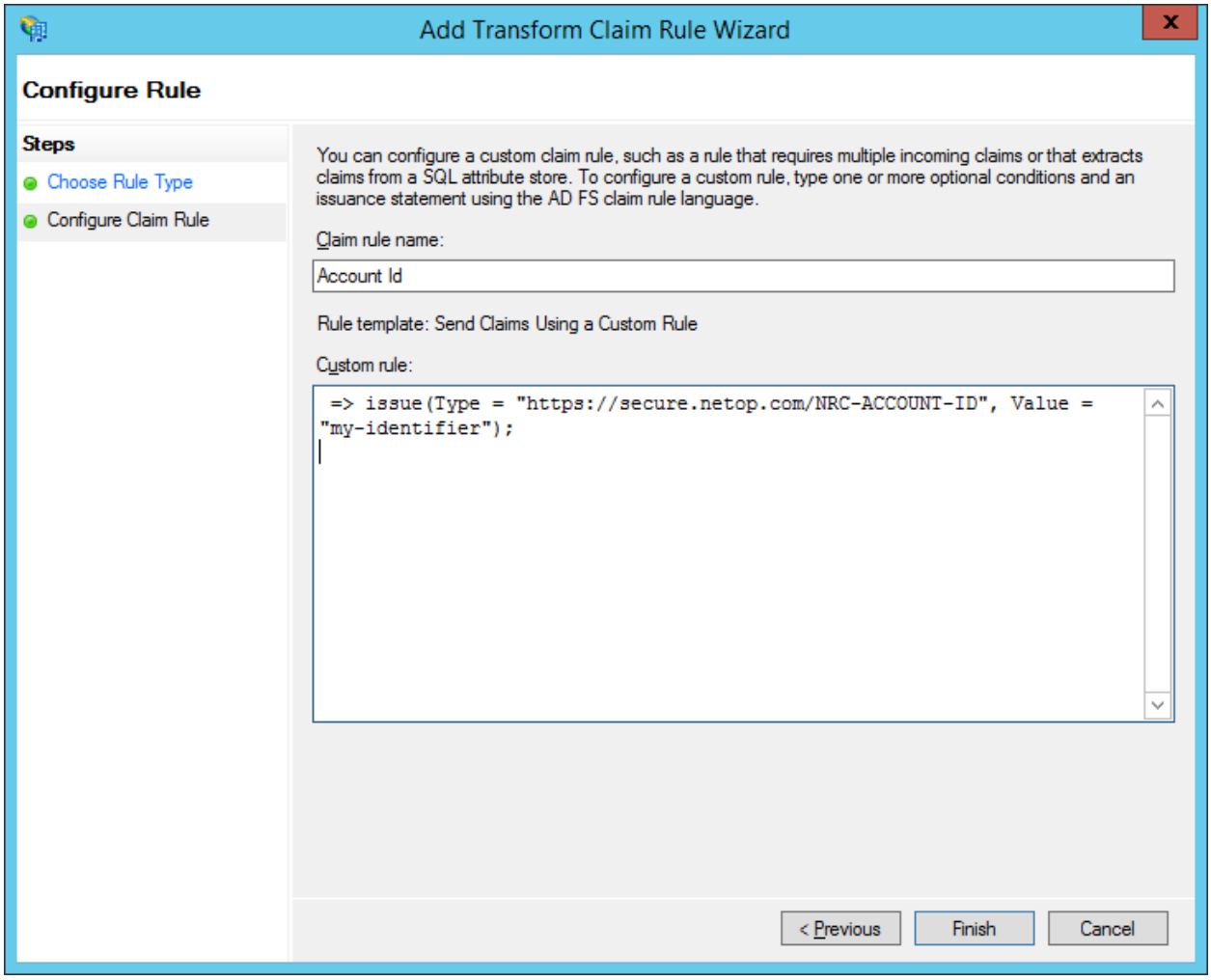


4. Select **Send Claims Using a Custom Rule** option from the **Claim rule template** drop-down menu**.**



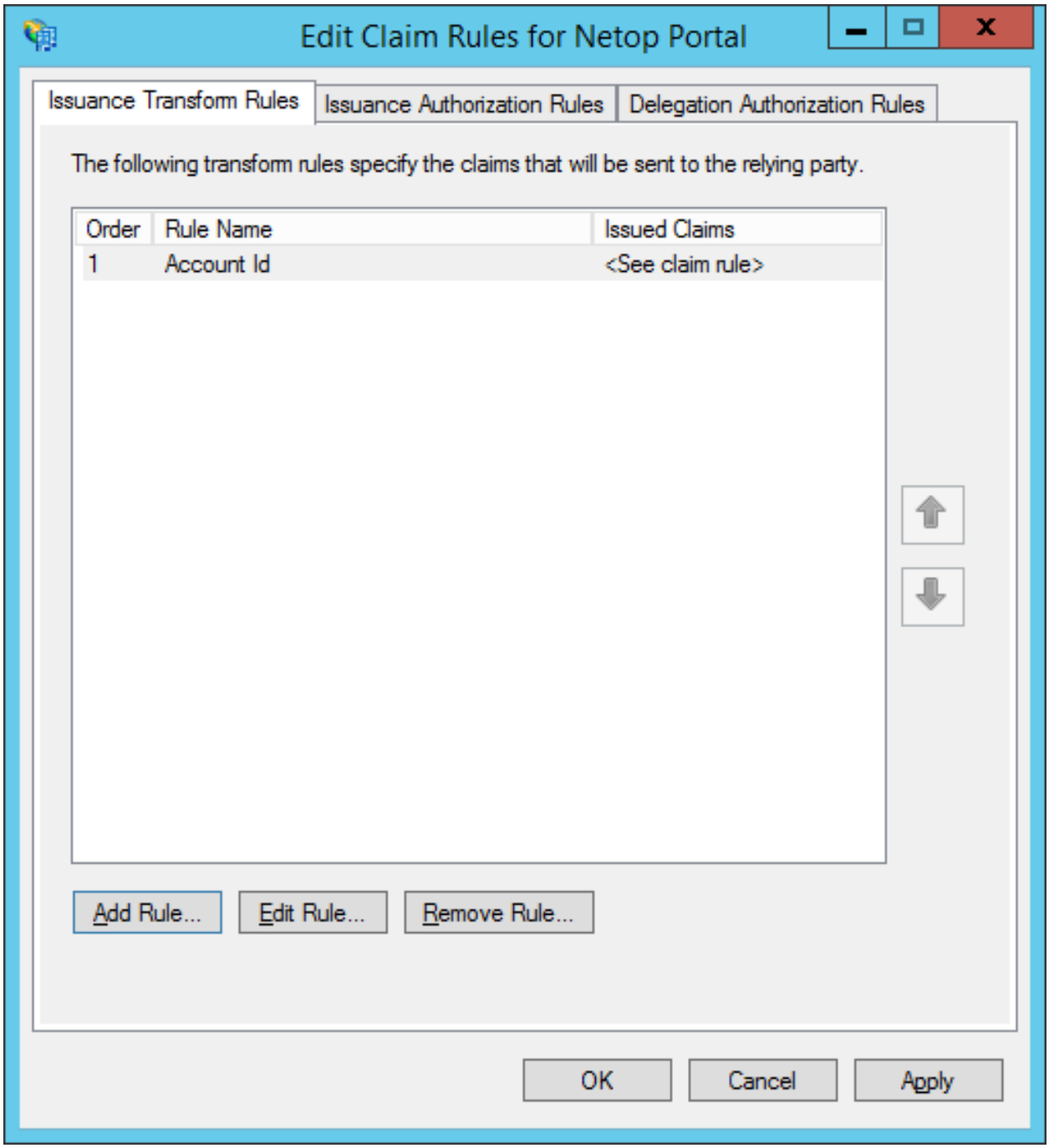
5. Specify the following values:
   - **Claim rule name:** Account Id
   - **Custom rule:** => issue(Type = "https://secure.netop.com/NRC-ACCOUNT-ID", Value = **"<Account identifier>**");

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.

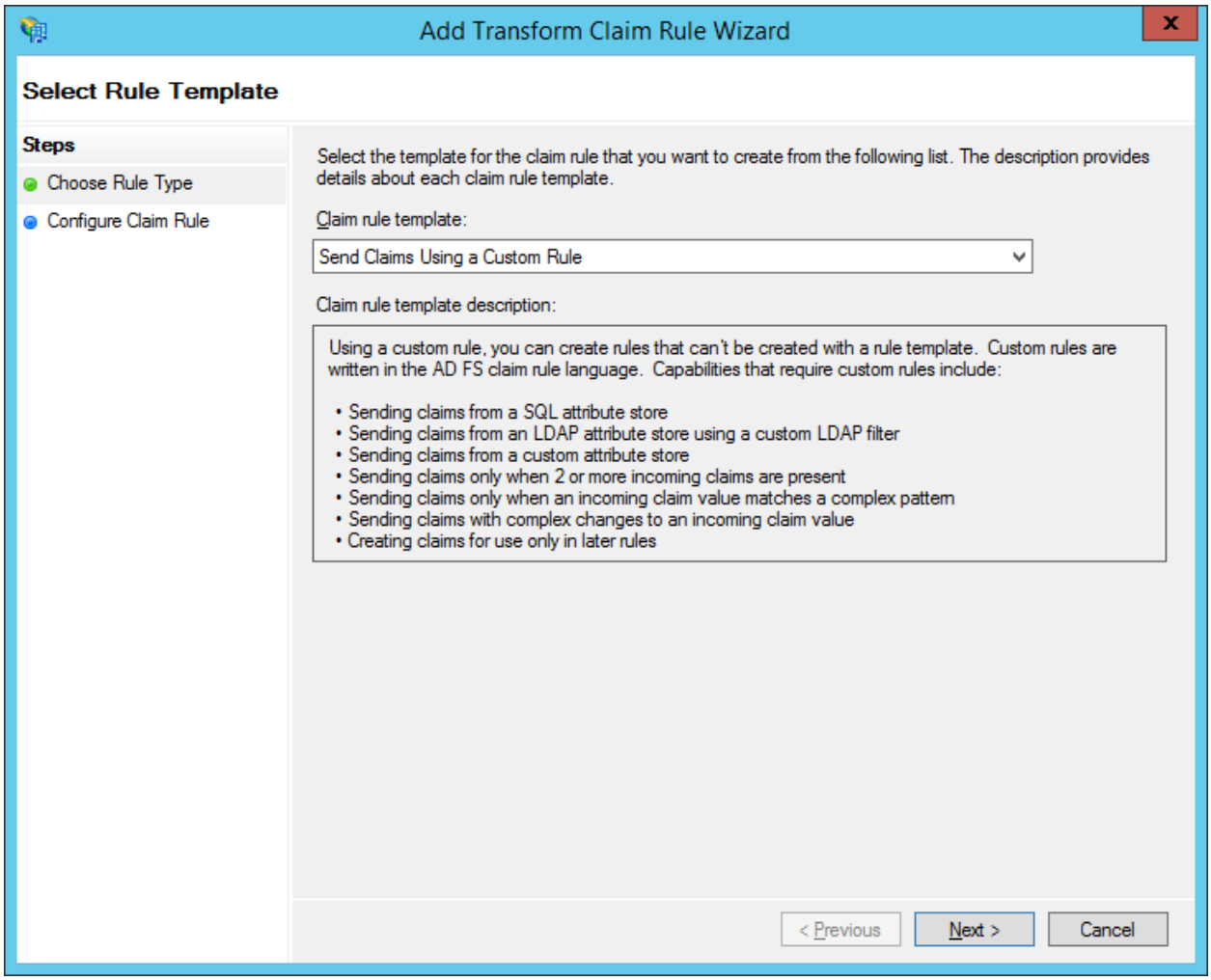


6. Click on **Finish**.

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



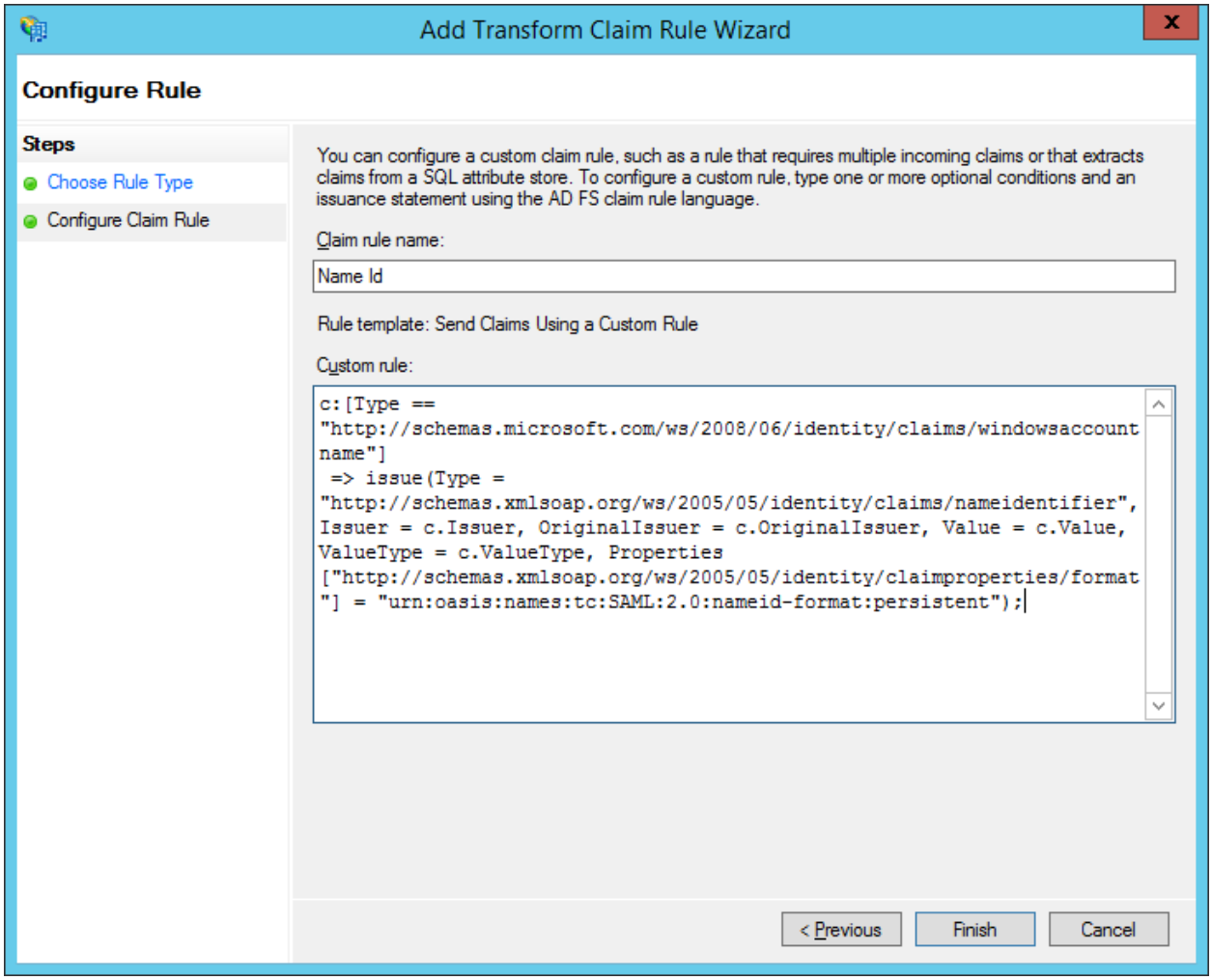
8. Select **Send Claims Using a Custom Rule** option from the Claim rule template drop-down menu**.**



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

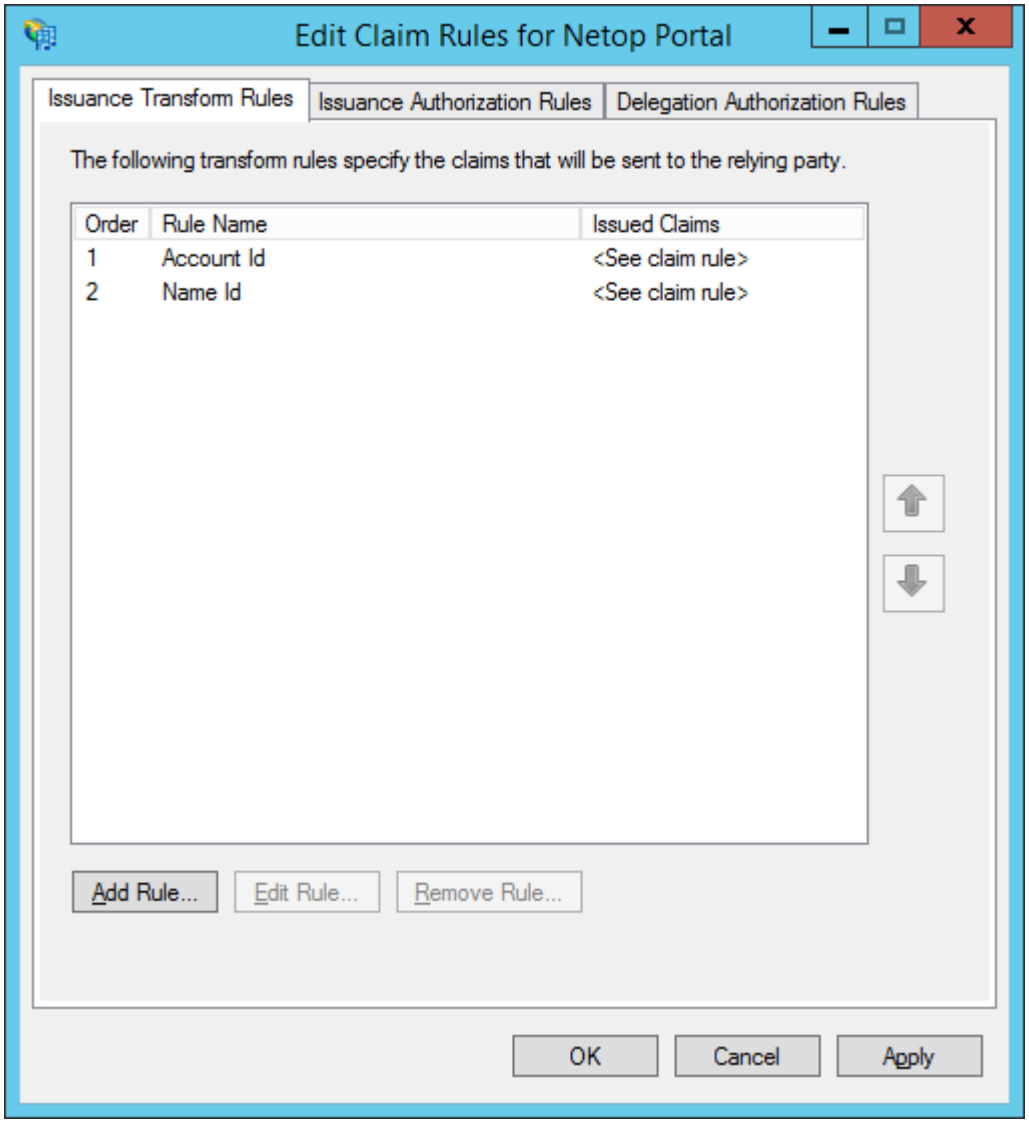
```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname
"]

 => 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");
```

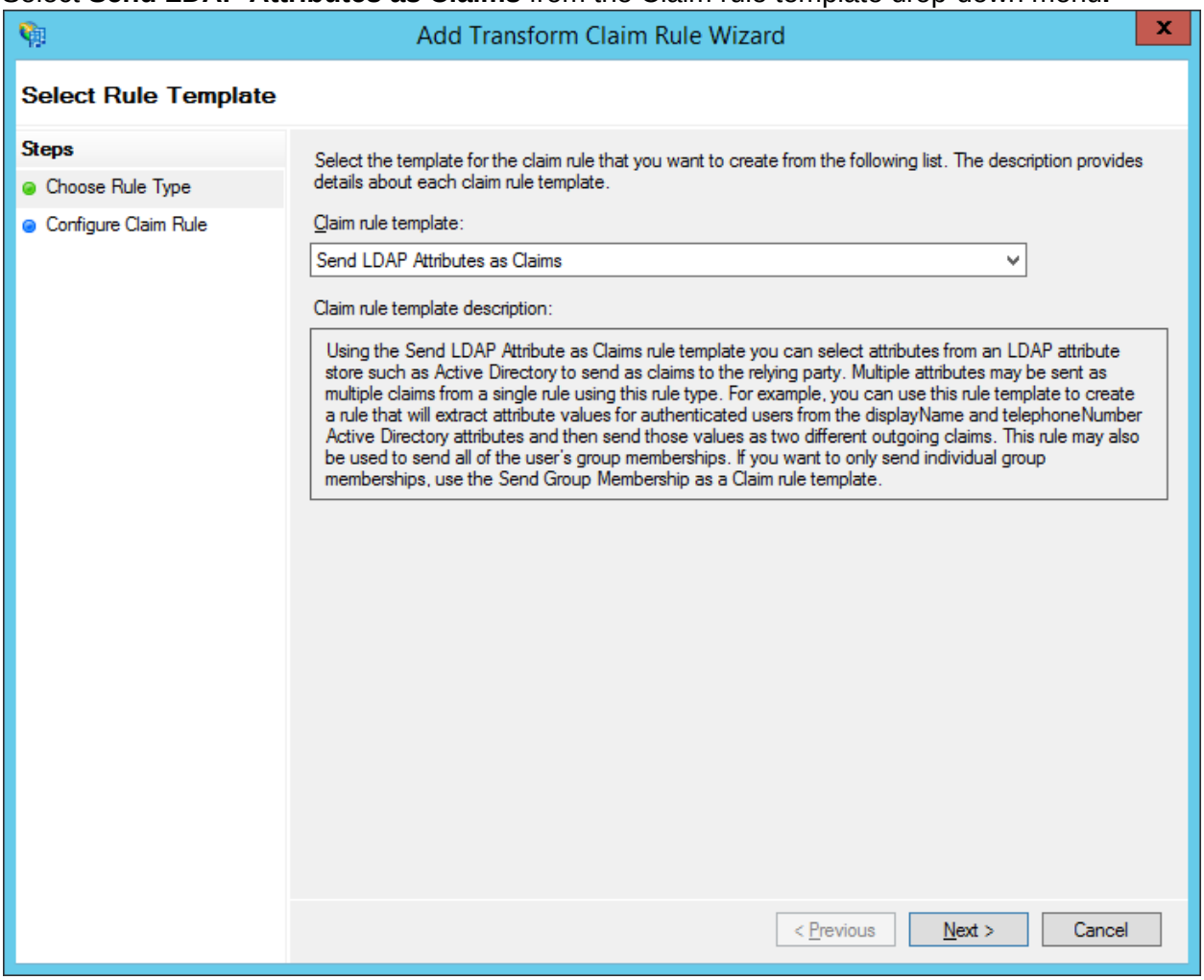


10. Click on Finish.

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**.**

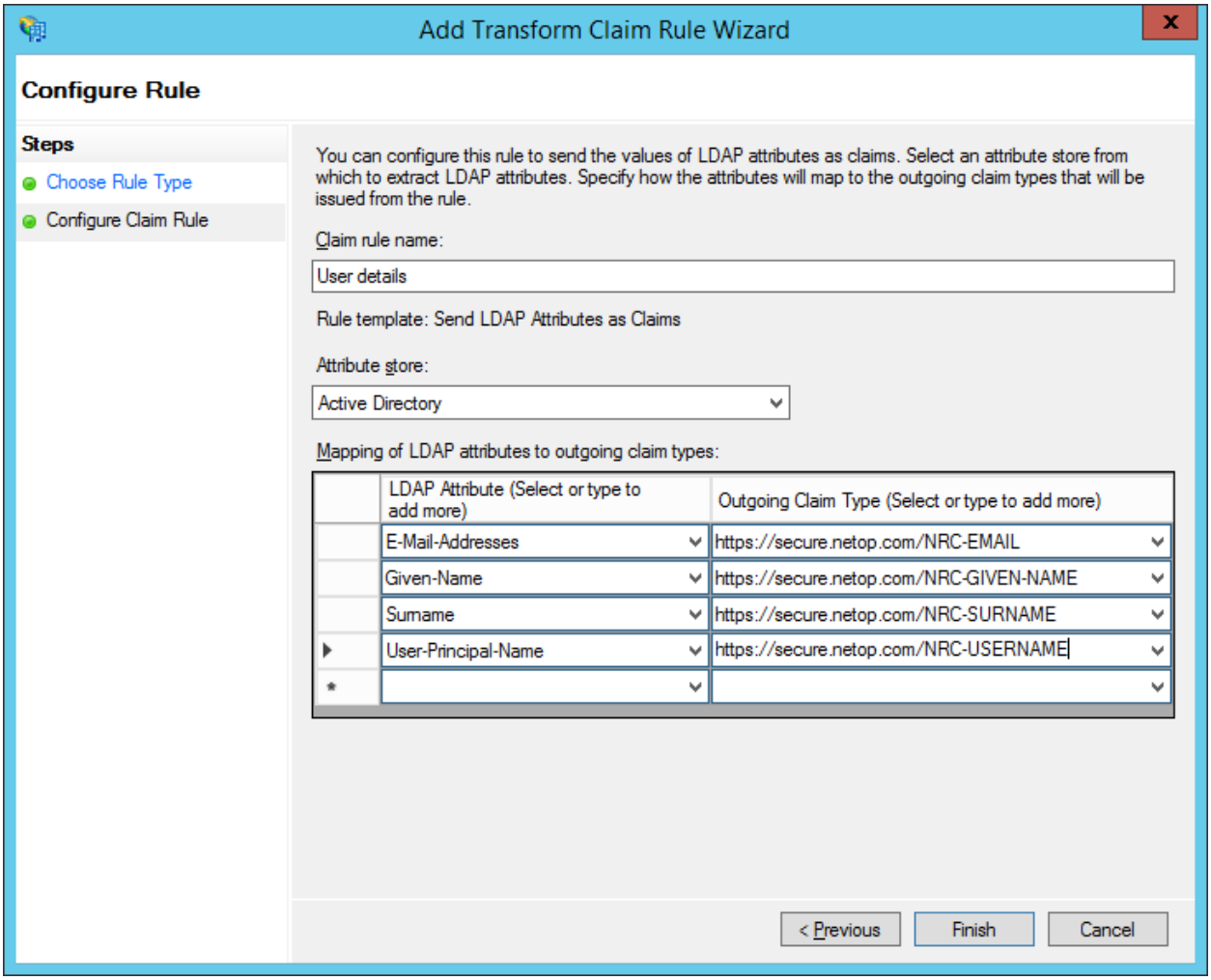


13. Specify the following values.

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

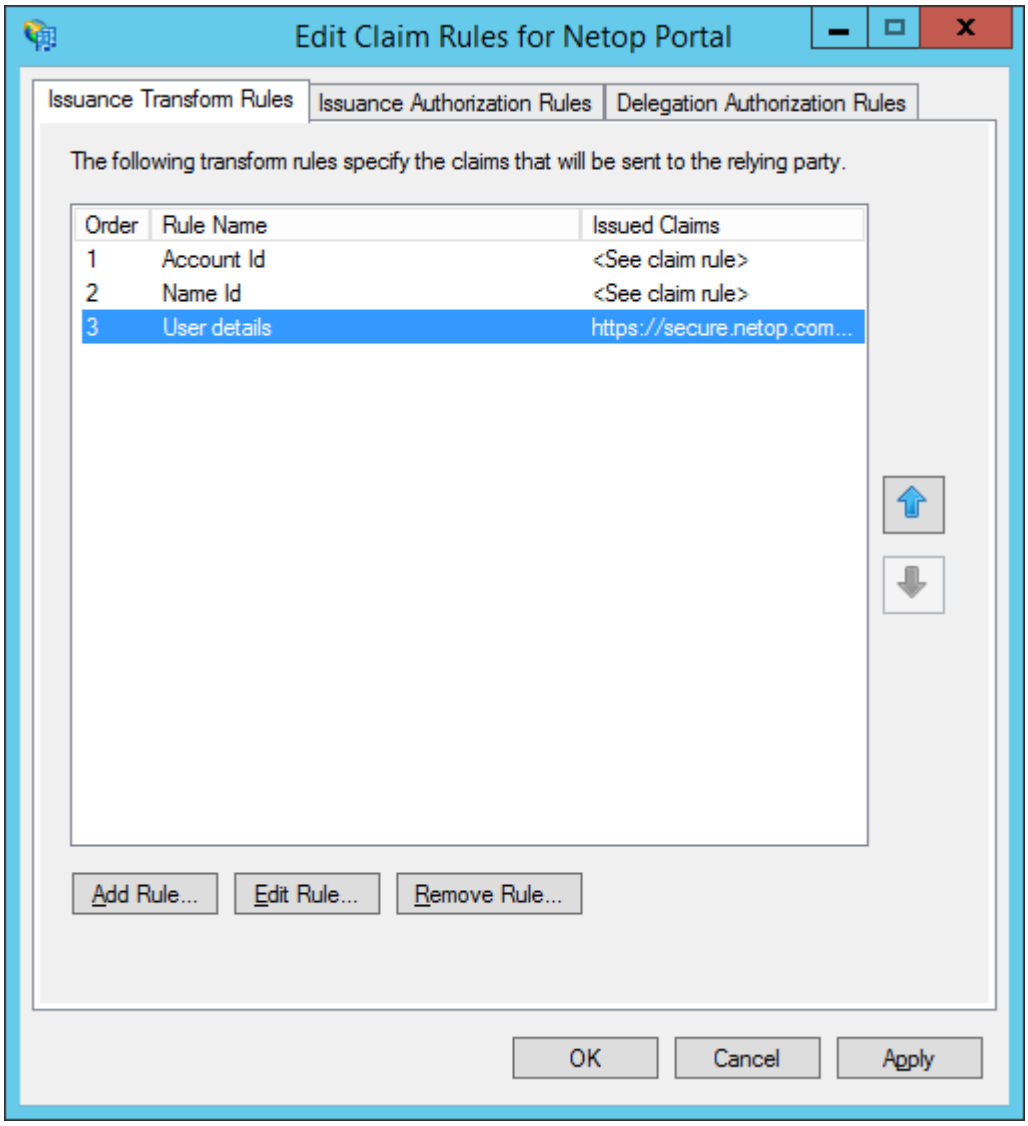
Mapping of LDAP attributes to outgoing claim types:

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



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:

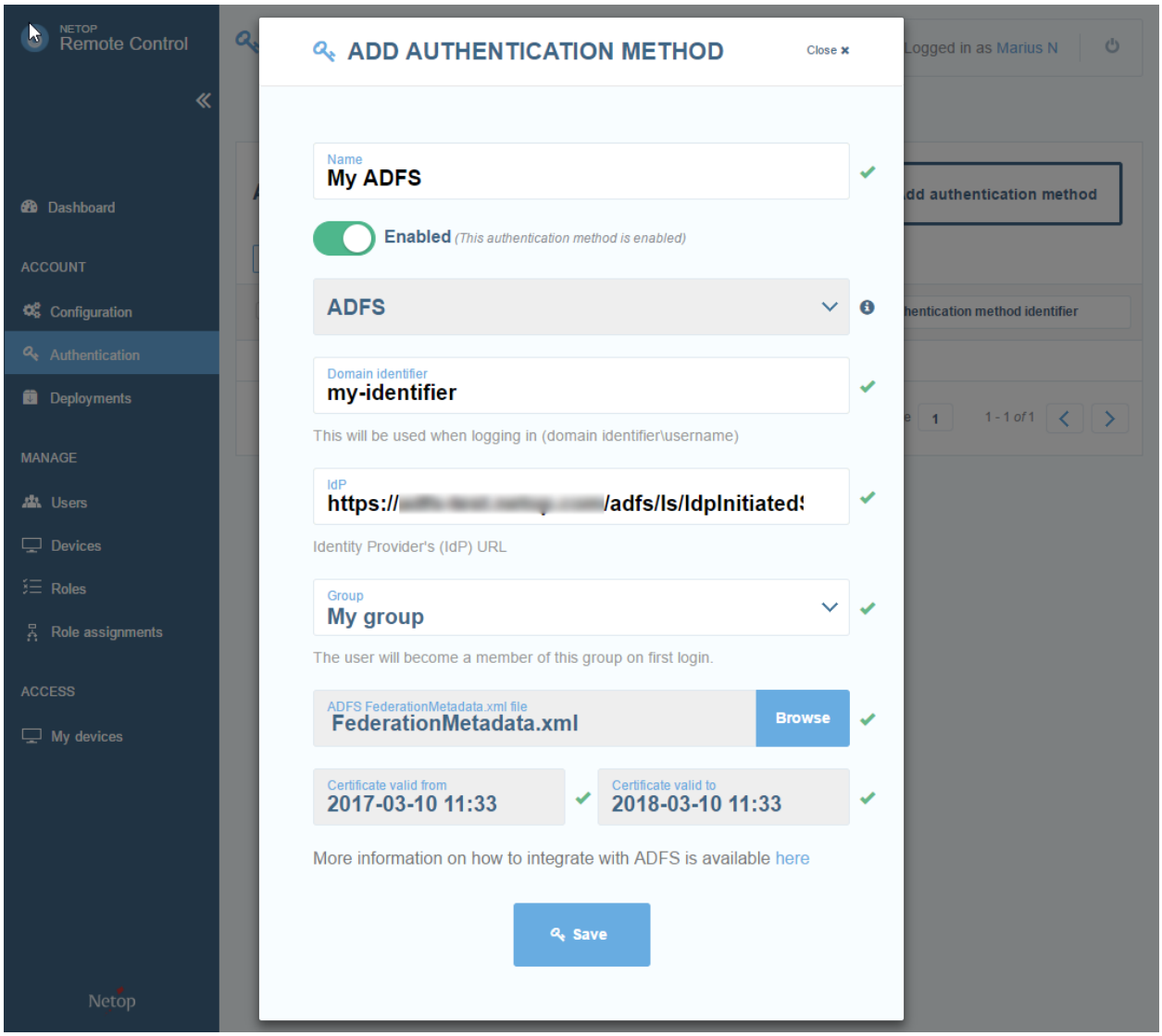
1. Sign in the **Netop Portal** with an Account administrator type of user.
2. Go to **Dashboard**.
3. Go to **Authentication**.
4. Click on the **Add ADFS / Azure AD** button.
5. Specify a name for the Authentication type.
6. Toggle the **Enable** button, to enable or disable the authentication type.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

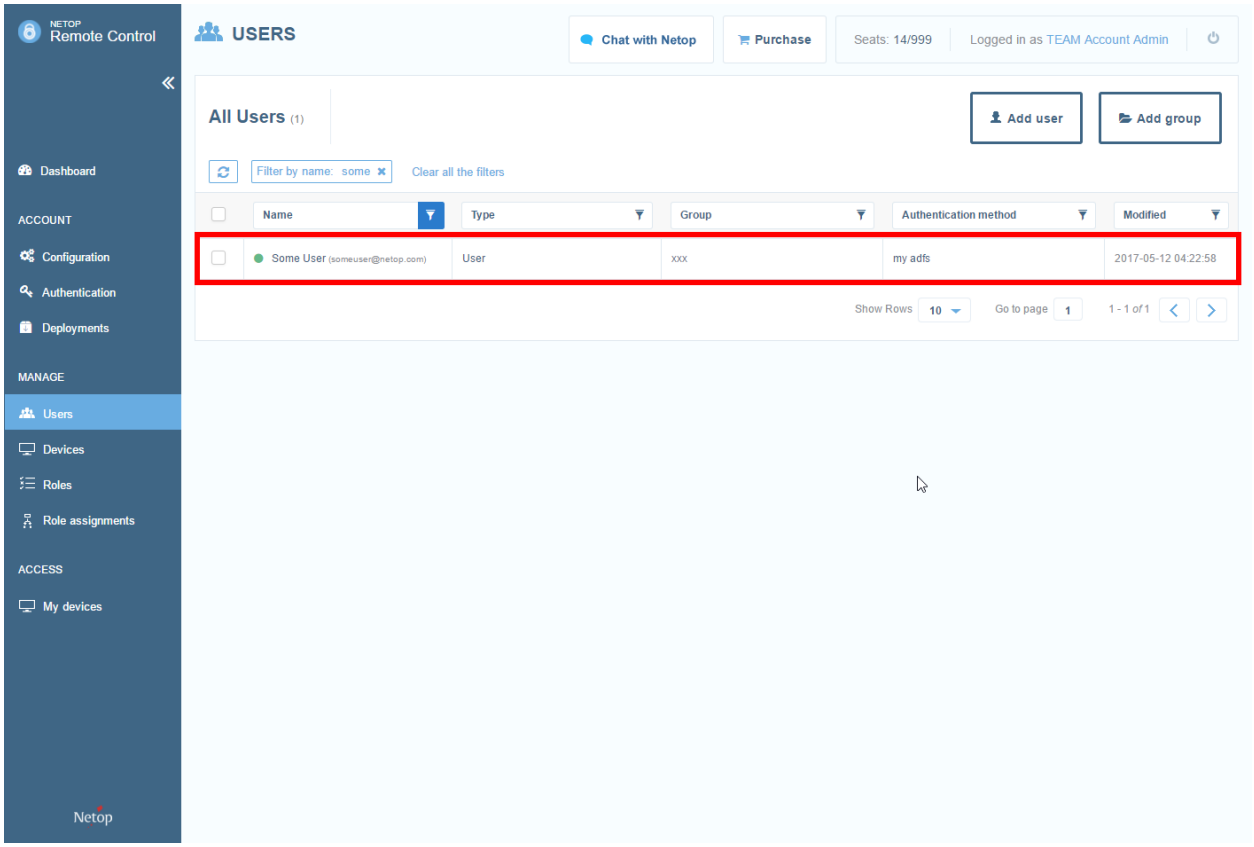
Remote session using ADFS

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 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