

IDP ADFS - OpenID Connect

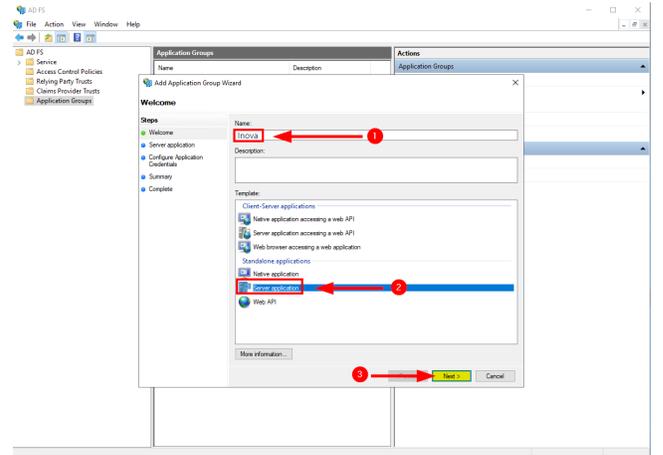
Instructions

Connect to your ADFS server and open the **AD FS console**:

1. Click on **Application Groups**
2. Click on **Add Application Group...** in the actions pane.



1. **Name the application** as you wish (e.g. "Inova")
2. Select **Server application**
3. Click on **Next**



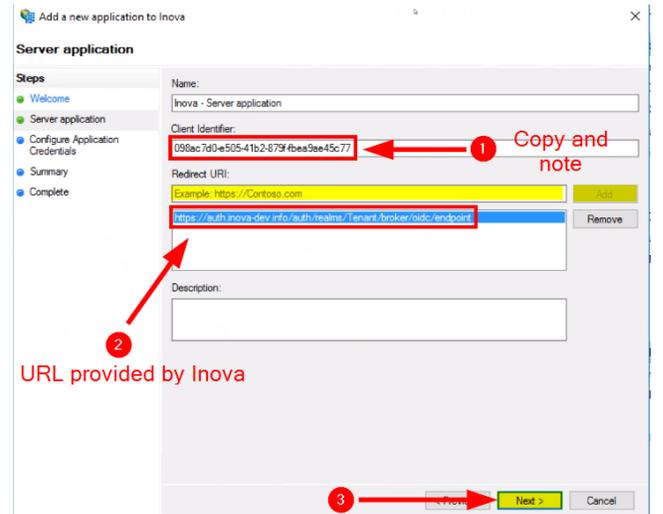
1. **Client Identifier:**
Copy and note the Client Identifier
It will be needed to continue setting up the SSO on Inova's end
2. **Redirect URI:**
https://auth.inova-application.com/auth/realms/<realm_name>/broker/oidc-adfs/endpoint

Then Click on **Add**

3. Click on **Next**

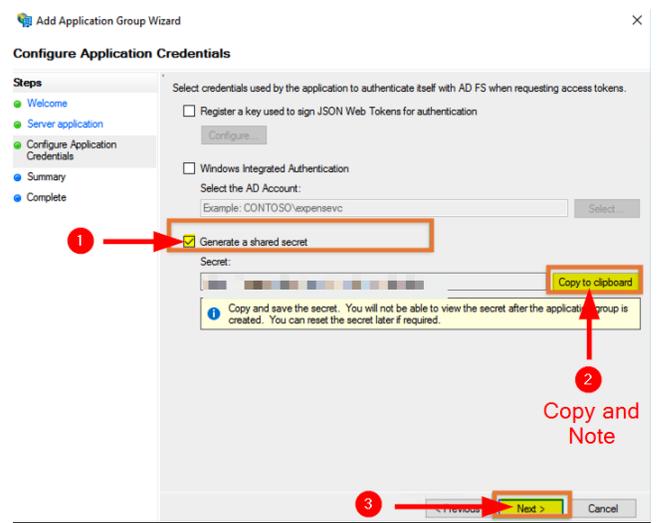
IMPORTANT: Please ensure that the domain **auth.inova-application.com** is whitelisted on your end

Replace **<realm_name>** by the one provided by Inova.



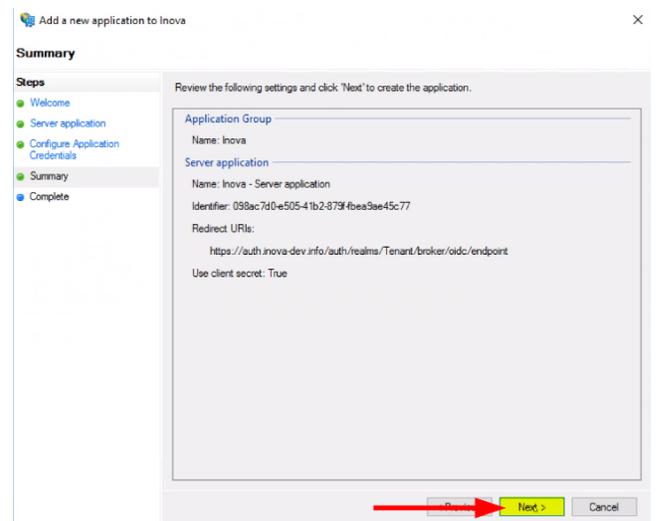
1. Check the **Generate a shared secret** checkbox. **Copy and note it**
2. Copy the password by clicking on **Copy to clipboard** and **note it**
3. Click on **Next**

It will be needed to continue setting up the SSO on Inova's end

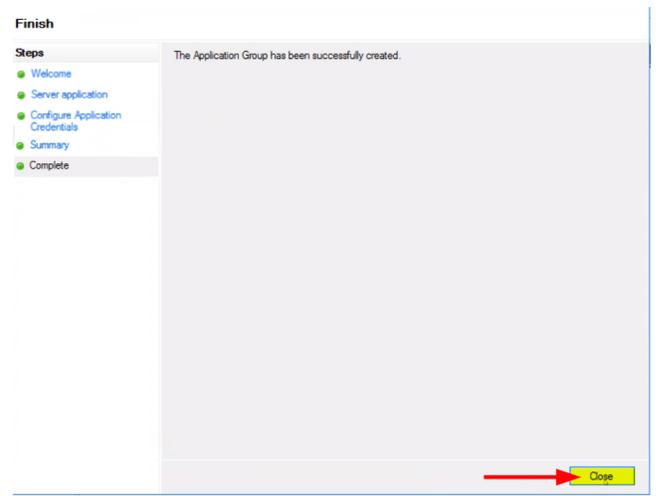


Copy and Note

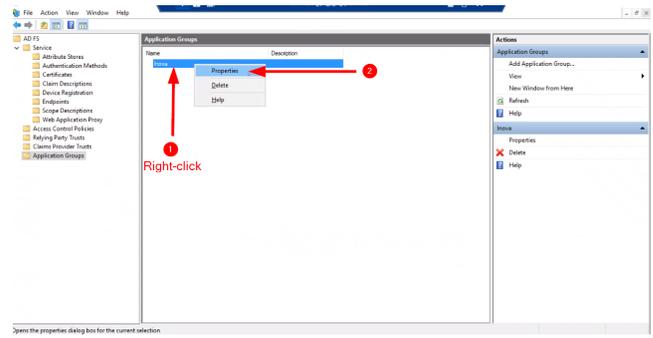
Validate the configuration and click on **Next**



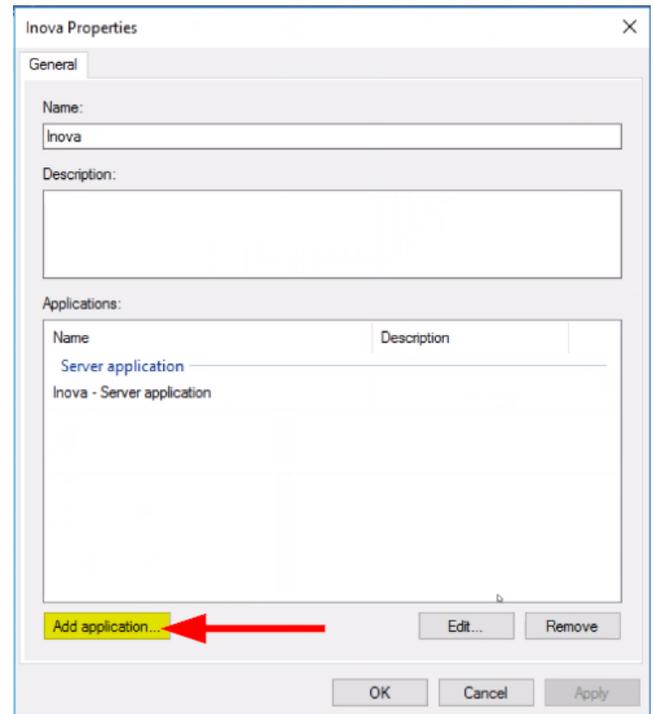
Click on **Close**



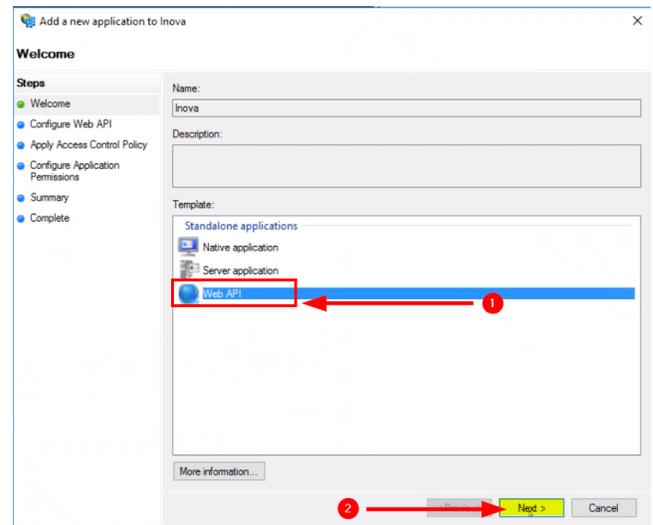
1. **Right-click** on the application your created
2. Click on **Properties**



Click on **Add application...**



1. Select **Web API**
2. Click on **Next**



1. Enter the **Client Identifier** noted previously
2. Click on **Add**
3. Click on **Next**

Configure Web API

Name: Inova - Web API

Identifier: 098ac7d0e50541b2879f4bea9be45c77

Description:

Client Identifier noted previously

Next >

1. Choose an **access control policy**
2. Click on **Next**

⚠ Make sure that the Inova users are allowed, otherwise they won't be able to sign in to the application.

Choose Access Control Policy

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone
Permit everyone and require MFA	Grant access to everyone and require MFA...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA...
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require...
Permit everyone and require MFA from unauthenticated	Grant access to everyone and require MFA...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFA...
Permit everyone for intranet access	Grant access to the intranet users
Permit specific group	Grant access to users of one or more speci...

Policy: Permit everyone

I do not want to configure the access control policy at this time. No users will be permitted access for this application.

Next >

1. Ensure **allatclaims** and **openid** scopes are checked
2. Click on **Next**

⚠ It is very important to have those 2 scopes checked for the setup to be working

Configure Application Permissions

Configure permissions to enable client applications to access this Web API.

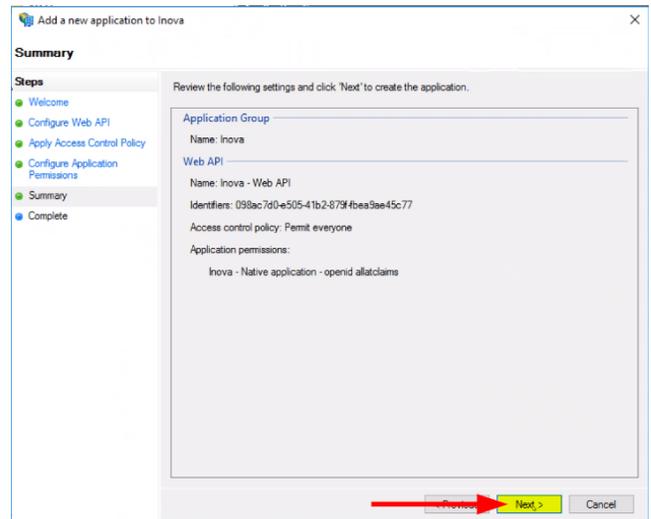
Client application (caller): Inova - Server application

Permitted scopes:

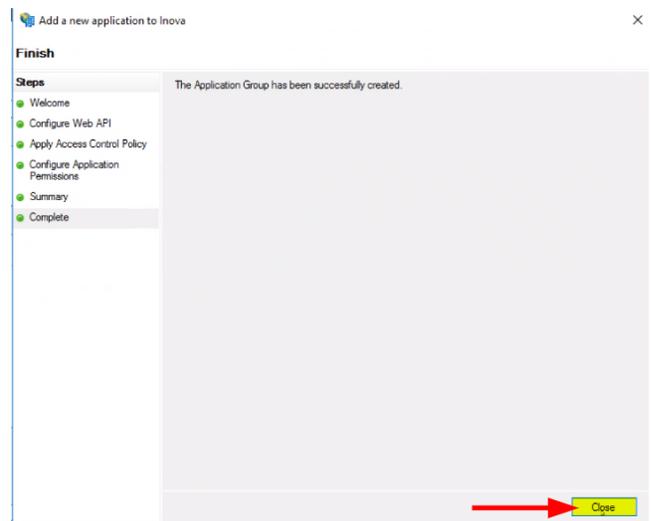
Scope Name	Description
<input checked="" type="checkbox"/> allatclaims	Requests the access token claims in the identity token.
<input type="checkbox"/> aza	Scope allows broker client to request primary refresh token.
<input type="checkbox"/> email	Request the email claim for the signed in user.
<input type="checkbox"/> logon_cert	The logon_cert scope allows an application to request logo...
<input checked="" type="checkbox"/> openid	Request use of the OpenID Connect authorization protocol.
<input type="checkbox"/> profile	Request profile related claims for the signed in user.
<input type="checkbox"/> user_impersonation	Request permission for the application to access the resour...
<input type="checkbox"/> von_cert	The von_cert scope allows an application to request VPN...

Next >

Validate the configuration and click on **Next**

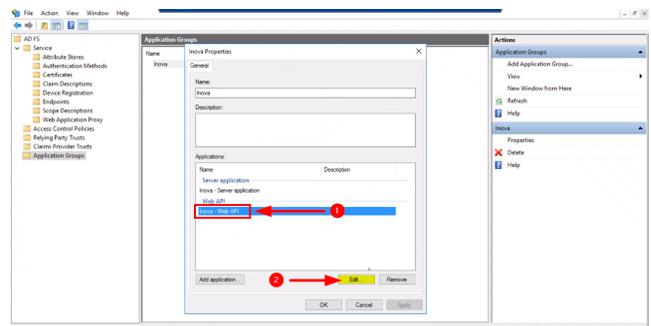


Click on **Close**

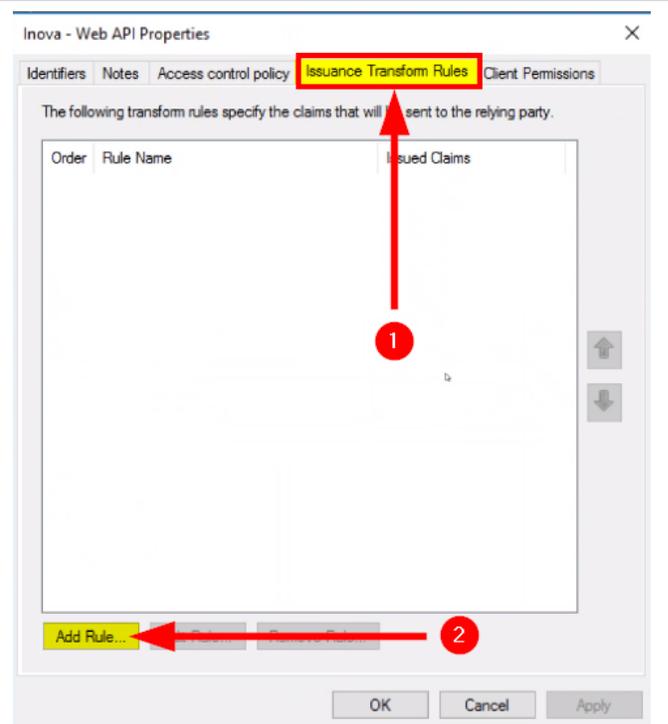


Back on the Inova Properties window:

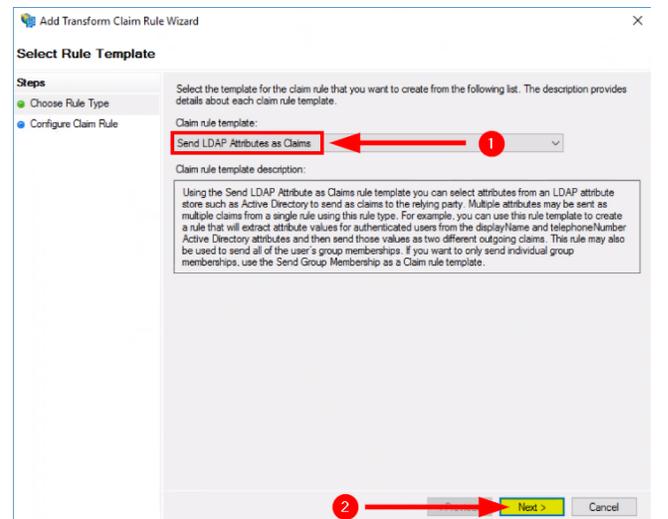
1. Select your **Web API** application
2. Click on **Edit**



1. Click on the **Issuance Transform Rules** tab
2. Click on **Add Rule...**

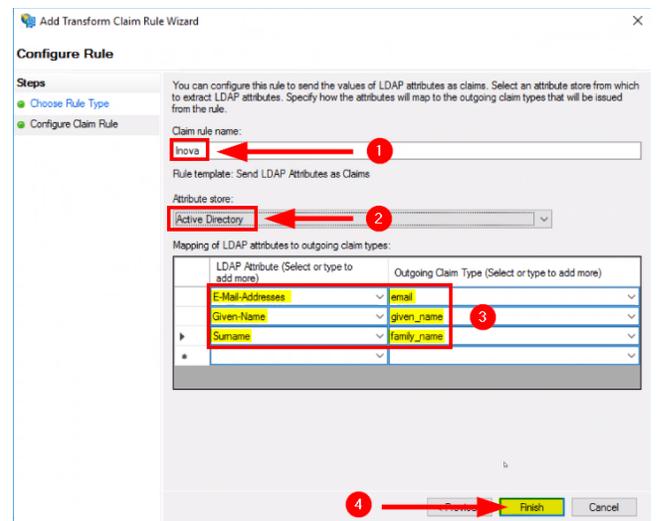


1. **Claim rule template:**
Select **Send LDAP Attributes as Claims**
2. Click on **Next**



1. **Claim rule name:**
Enter a name (e.g. "Inova")
2. **Attribute store:**
Select **Active Directory**
3. **Mapping of LDAP attributes outgoing claim types:**
Add 3 entries exactly as follow:
E-mail-Addresses email
Given-Name given_name
Surname family_name
4. Click on **Finish**

 Please respect this naming to avoid any attribute mapping issue.



Click on **OK**

Inova - Web API Properties

Identifiers Notes Access control policy Issuance Transform Rules Client Permissions

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Inova	email.given_name.family_...

Add Rule... Edit Rule... Remove Rule...

OK Cancel Apply

Click on **OK**

AD FS

Application Groups

Name: Inova

Description:

Applications:

Add application OK Cancel Apply

Send the elements you noted previously to Inova:

1. **Client Identifier**
2. **Client secret**
3. **ADFS OpenID Connect Metadata file URL** (e.g. <https://<your-domain>/adfs/.well-known/openid-configuration>)

