

Table of Contents

OAuth Sample Client Applications	2
Use case	2
Configuring Access Manager.....	2
Configuring Access Manager Resource Server	2
Configuring Access Manager for Client Applications	4
Creating Users in Admin Console.....	5
Configuring Website and Resource Server	6
Configuring Applications	6
Configuring Insurance Application.....	6
Configuring Fitness Application	6

OAuth Sample Client Applications

These sample client applications aim to provide users with information on how to configure Access Manager for OAuth and how to get an OAuth token from Access Manager. There are four sample items provided:

- Insurance Application: It is an android application that can be deployed to view insurance details. It demonstrates resource owner flow and is developed using ionic framework.
- Fitness Application: It is an android application that can be deployed to view accessible services. It demonstrates authorization code flow and the use of token refresh and token revocation. It is developed using ionic framework.
- Fitness Website: It is a website that can be accessed using a browser to view the accessible services. It demonstrates implicit flow and the use of ID token. It is developed using angular framework.
- Resource Server: It is a springboot application that protects the details of customers and allows access to it through the OAuth protocol.

Use case

Let us consider an insurance company that provides three levels of policies to its customers, Standard, Premium, and Executive. These policies define the privileges of a customer. The insurance company maintains the details of its customers in a resource server. It has an agreement with a fitness company where the fitness company provides different services based on the customer's policy level. The insurance company provides an application to access users' details. Fitness company provides an application and a website. As these are individual entities and different companies, they require a secure way to authenticate and share user details. To enable these applications to access the insurance company's resource server, we can use the OAuth protocol through Access Manager.

Follow the given steps to protect the resource server using Access Manager:

1. [Configure Access Manager](#)
2. [Configure Website and Resource Server](#)
3. [Configure Insurance Application](#)
4. [Configure Fitness Application](#)

Configuring Access Manager

In the following sections, Access Manager configurations are described.

Configuring Access Manager Resource Server

Perform the following steps to configure the Resource Server

1. Navigate to IDP Cluster > OAuth & OpenID Connect > Resource Servers.
2. Create a Resource Server.
3. Navigate to Scopes.
4. Click New.
5. Specify the following:
 - Name: level
 - Description: member level
 - Include claims of type: User Attributes

Dashboard Devices ▾ Policies ▾ Security ▾

Identity Servers ▶ IDPCluster ▶ Identity Provider ▶

Create scope

Step 1 of 2: Specify scope.

Name:

Description:

Include claims of type: ☒ User Attributes ☐ Custom Claims/Permissions

Require user permission: ☒

Allow modification in consent: ☐

6. Click Next.
7. Select <New Attribute Set> in Attribute Set.
8. Specify Set Name.
9. Select Supports WSTrust and OAuth.
10. Click Next.
11. Click New.
12. Specify the following:
 Local attribute: Ldap Attribute:employeeType [LDAP Attribute Profile]
 Remote attribute: MemberType

Add Attribute Mapping

☒ Local attribute:

☐ Constant:

Remote attribute: ☐ Roles ☒ MemberType (optional)

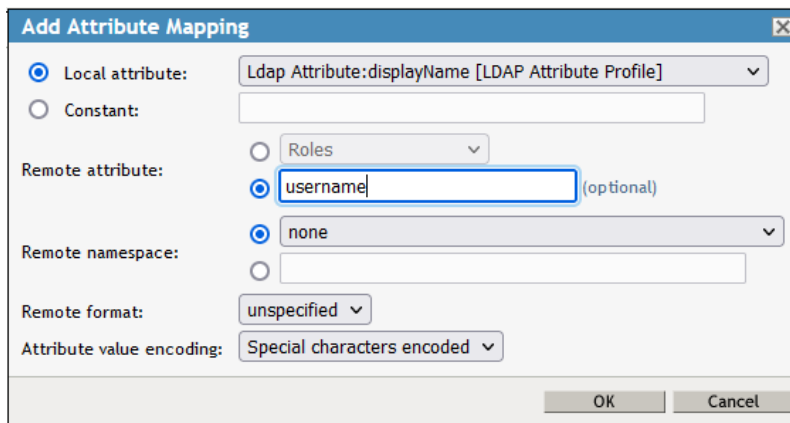
Remote namespace: ☒ none ☐

Remote format:

Attribute value encoding:

OK Cancel

13. Click OK.
14. Click New.
15. Specify the following:
 Local attribute: Ldap Attribute:displayName [LDAP Attribute Profile]
 Remote attribute: username



Add Attribute Mapping

☒ Local attribute: Ldap Attribute:displayName [LDAP Attribute Profile] ▼

☐ Constant:

Remote attribute: ☐ Roles ▼

☒ username (optional)

Remote namespace: ☒ none ▼

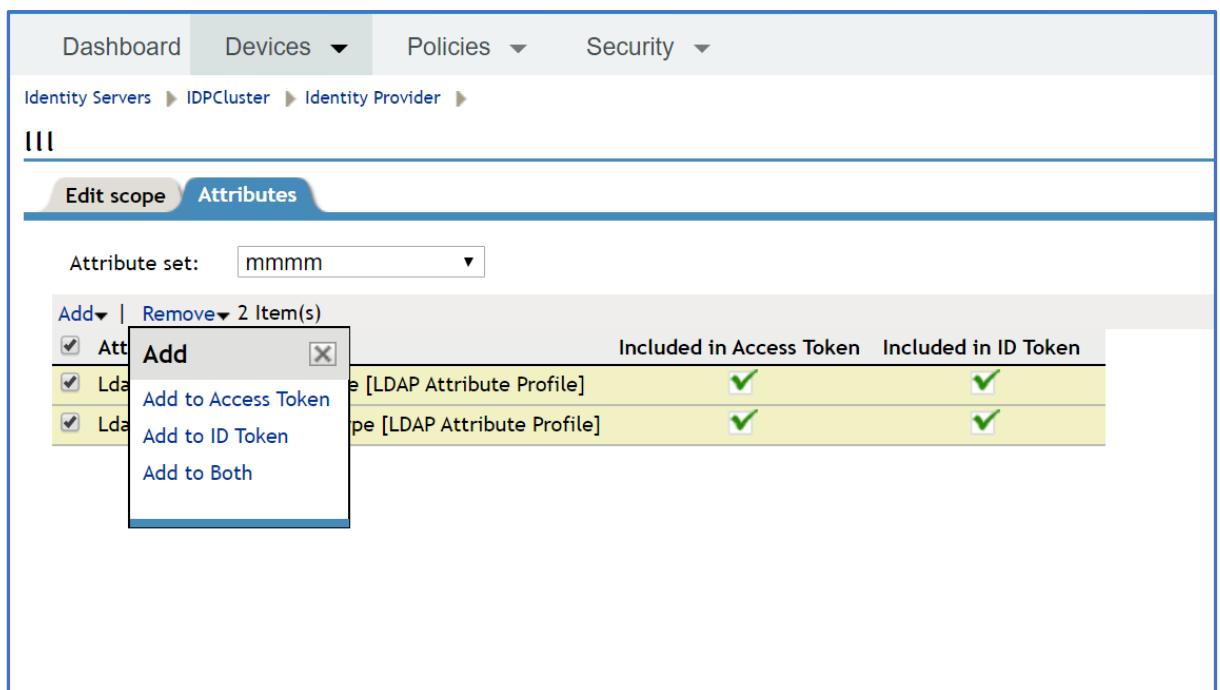
☐

Remote format: unspecified ▼

Attribute value encoding: Special characters encoded ▼

OK Cancel

16. Click OK.
17. Click Finish.
18. Select the Attribute Set created for attribute mapping.
19. Click Add > Add to Both.



Dashboard Devices Policies Security

Identity Servers IDPCluster Identity Provider

Attributes

Attribute set: mmmm ▼

Add Remove 2 Item(s)

		Included in Access Token	Included in ID Token
<input checked="" type="checkbox"/>	Ldap Attribute:displayName [LDAP Attribute Profile]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Ldap Attribute:displayName [LDAP Attribute Profile]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add

Add to Access Token

Add to ID Token

Add to Both

These attributes will be sent with the token when a user requests it.

Refer to [Creating Users in Admin Console](#) for more information.

20. Apply the changes and update IDP.

Configuring Access Manager for Client Applications

Perform the following steps to configure Access Manager for the client applications:

1. Navigate to IDP Cluster > OAuth & OpenID Connect > Global Settings.
2. Specify Authorization Grant LDAP Attribute as nidsOAuthGrant or jpegPhoto.
For more information, see [Configuring OAuth and OpenID Connect](#).
3. Set CORS Domain as Allow All to allow access for requests from any domains.
4. Select all Grant Type(s) and Token Type(s).

5. Navigate to Client Applications and register two clients.
 - a. Register the first client for fitness website and insurance application with the following configuration:
 - i. Login Redirect URIs: `https://{adminconsole}:{port}/fitness/membership`
For more information, see [Configuring Applications](#).
 - ii. Grants Required: Implicit and Resource Owner Credentials
 - iii. Token Types: ID Token and Access Token
 - b. Register the second client for fitness application with the following configuration:
 - i. Login Redirect URIs: `myapp://fitness.com`
 - ii. Grants Required: Authorization Code
 - iii. Token Types: Access Token and Refresh Token

For more information, see [Registering the OAuth Client Application](#) in the [Access Manager 5.0 OAuth Application Developer Guide](#).

Creating Users in Admin Console

Perform the following steps to create users in the Admin Console:

1. Navigate to Admin > Configure Console.
2. Select Roles and Tasks.
3. Select Users > Create User from the left pane.
4. Enter all the required details. Specify novell in Context field.

Create User

Username: *

First name:

Last name: *

Full name:

Context: *

Password:

Retype password:

Note: Failure to enter a password will allow the user to login without a password.

☐ Set simple password
Note: Simple password is required for native file access for Windows and Macintosh users. (Not required when Universal password is enabled)

☐ Copy from template or user object

5. Click OK.
6. Navigate to NMAS > NMAS Users in the left pan and search for the user that you created.
7. Navigate to Other in the General tab.
8. Push employeeType attributes from Unvalued Attributes to Valued Attributes.
In the new window, add the appropriate value (standard, premium, or executive). This will determine the policy level of the member.
Note: This value is case-sensitive.
9. Push displayName attributes from Unvalued Attributes to Valued Attributes.
In the new window, add the appropriate value (For example, John). This will determine the policy level of the selected member.

These attributes are sent along with the access token and the ID token as seen in [Configuring Access Manager Resource Server](#).

Configuring Website and Resource Server

There are two files to be deployed as follows:

- insurance.war – For Resource Server deployment
- fitness.zip – For website deployment

Perform the following steps for deployment:

1. Extract the fitness.zip file and place the fitness folder and insurance.war file in /opt/novell/nam/adminconsole/webapps.
Refresh to verify that a folder named 'insurance' is created.
2. Navigate to /opt/novell/nam/adminconsole/conf/ and open server.xml.
Add the following under <Host>...</Host> section:
<Valve className="org.apache.catalina.valves.rewrite.RewriteValve" />
3. Navigate to /opt/novell/nam/adminconsole/conf/Catalina/localhost and create a file 'rewrite.config' with the following content:
RewriteCond %{REQUEST_PATH} !-f
RewriteRule ^/fitness/(.*) /fitness/index.html
4. For configuration files containing details of NAM setup:
/opt/novell/nam/adminconsole/webapps/fitness/assets/data/config.json for website
/opt/novell/nam/adminconsole/webapps/insurance/WEB-INF/classes/dataclient.properties for resource-server
Enter the details in these files
5. Restart tomcat using the command rcnovell-ac restart.
Access the website, https://{adminconsole-domain}:{port}/fitness

Configuring Applications

In the following sections, the configuration steps for the applications are provided.

Configuring Insurance Application

Perform the following steps to configure the insurance application:

1. Install the Insurance.apk file on your smartphone.
2. Enter the configurations of Access Manager such as IDP URL, Client Secret, Client ID, and API URL when prompted.
3. For the Insurance app, use the “Web-based” Client Application you registered in the Access Manager.
For more information, see [Configuring Access Manager for Client Applications](#).
These details are stored on your local storage and need not be entered again.
4. On the login page, log in with the user id and password of the user that was created.
You should be able to view the details of the user by clicking the View Details button.

Configuring Fitness Application

Perform the following steps to configure the fitness application:

1. Install the Fitness.apk file on your smartphone.

2. Enter the configurations of Access Manager such as IDP URL, Client Secret, Client ID, and API URL when prompted.
3. For this application, use the “Native” Client Application you registered in Access Manager. For more information, see [Configuring Access Manager for Client Applications](#). These details are stored on your local storage and need not be entered again
4. Click the Login button. You will be redirected to the Access Manager login page where you must enter the user id and password for the user you created.

On successful authentication, you will be able to log in and view your features according to the policy level of the user. A refresh token will be saved in the local storage which can be used by the application to log you in on subsequent attempts without redirecting you to the login page.

On clicking the Log Out button, the refresh token gets revoked and then deleted.