

# Lasernet 10 Configuring Azure AD Authentication.

Input and Output Management

Thomas Barnekov, Adam McStravick  
Revision 3  
2023-08-09

Formpipe.

# Contents.

<b>1 Introduction.....</b>	<b>3</b>
<b>2 Configure Azure Active Directory.....</b>	<b>4</b>
2.1 Create an Azure AD App registration.....	4
2.2 Configure authentication settings.....	6
2.3 Configure App Roles.....	7
2.4 Configure the Enterprise application registration.....	8
2.5 Assign users and groups to the Admin.Global App Role.....	9
2.6 Collect information required to configure Lasernet ..	10
<b>3 Configure Lasetnet Configuration Server.....</b>	<b>12</b>
3.1 Locate or create the ServerSettings.json file.....	12
3.2 Configure TLS bindings.....	12
3.3 Add authentication settings for Azure AD authentication.....	13
3.4 Start or Restart the Lasetnet Config service.....	13
<b>4 Configuring additional user permissions in Azure AD and Lasetnet.....</b>	<b>15</b>
4.1 Add a new App Role to the Azure App registration..	15
4.2 Assign users and groups to the new App Role.....	16
4.3 Add a new External Role in Lasetnet.....	16
4.4 Add a new Security Role in Lasetnet.....	17
4.5 Configure new Security Role.....	18
<b>5 Configuring alternative authentication providers.....</b>	<b>21</b>
5.1 Adding an alternative provider to ServerSettings.json .....	21
<b>6 Using alternative authentication providers.....</b>	<b>22</b>
6.1 Using alternative authentication providers in native applications.....	22
6.2 Using alternative authentication providers in web applications.....	22

# 1 Introduction.

Lasernet has support for authenticating users against external authentication providers such as Azure Active Directory. Lasernet relies on OpenID Connect as the authentication protocol.

Lasernet is tested against Azure Active Directory but it should be possible to use other authentication providers instead.

In order for Lasetnet to work with an external authentication provider, the provider must support the OpenID Connect Implicit Flow and be able to issue ID Tokens with a customizable 'roles' claim.

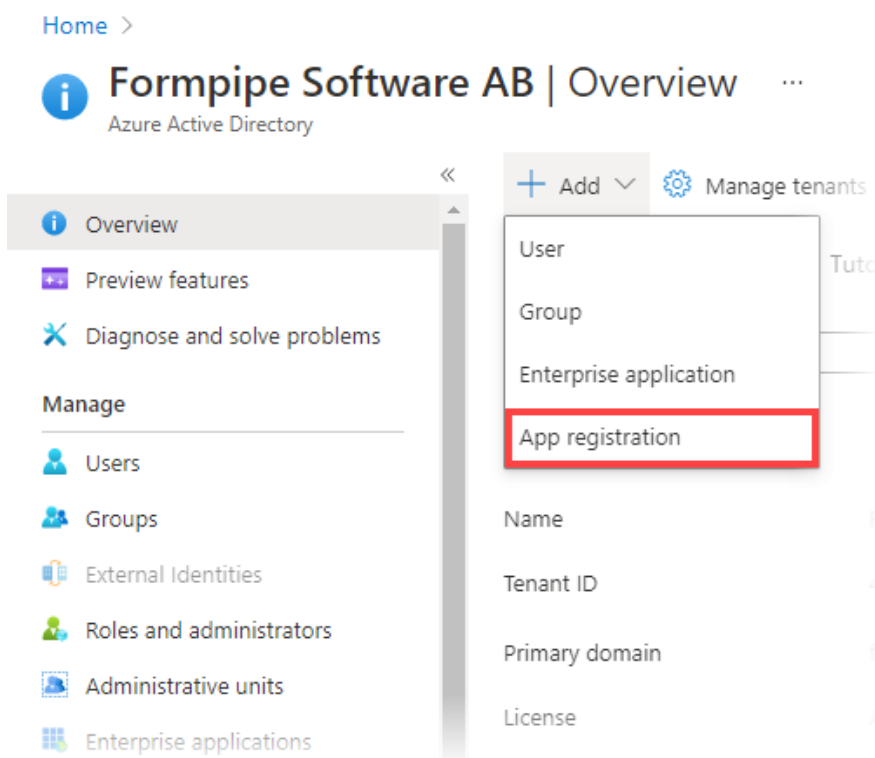
In order to manage user permissions in Lasetnet, it must be possible to assign users to specific 'roles' claims.

## 2 Configure Azure Active Directory.

In order to allow Lasernet to authenticate users against Microsoft Azure Active Directory, you must configure an App registration.

### 2.1 Create an Azure AD App registration

1. Log in to the Azure Portal.
2. Navigate to **Azure Active Directory**.
3. Click **Add** and select **App registration** in the drop-down menu.



#### 4. Fill in the Name and Redirect URI fields.

### Register an application ...

#### \* Name

The user-facing display name for this application (this can be changed later).

Lasernet ✓

#### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Formpipe Lasernet only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

#### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼  ✓

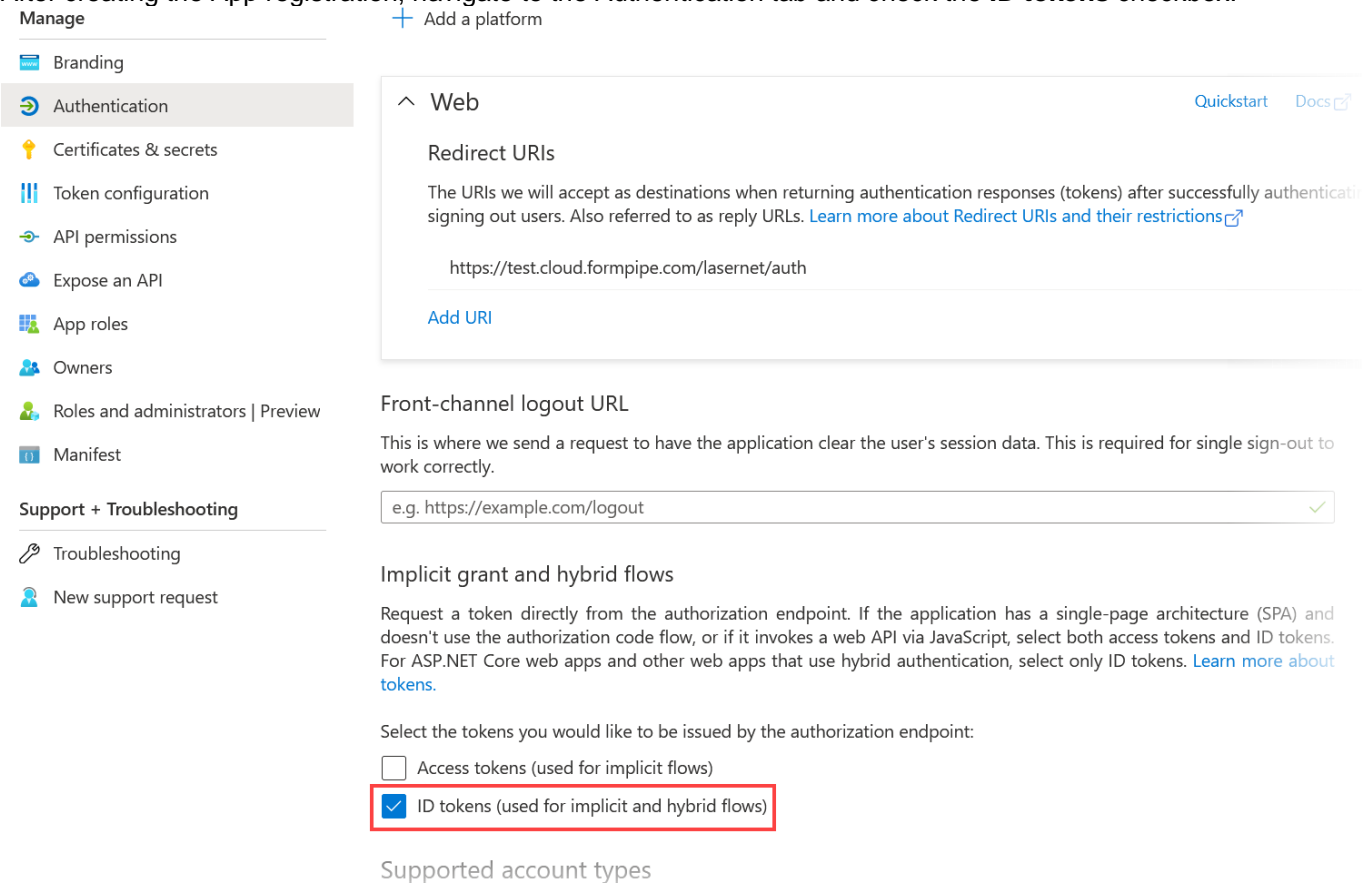
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

#### Notes:

- Name is shown to the users when they log in.
- Make sure 'Accounts in this organization only' is selected (default).
- Redirect URI must be set to <https://<FQDN-of-Lasernet-Server>:33443/lasernet/auth>  
If Lasernet is run on a different port than 33443, this must be reflected in the Redirect URI (ex. <https://lasernet.mydomain.com:9443/lasernet/auth>).
- Click the Register button to complete the App registration.

## 2.2 Configure authentication settings

1. After creating the App registration, navigate to the Authentication tab and check the **ID tokens** checkbox.



Manage + Add a platform

- Branding
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

**Support + Troubleshooting**

- Troubleshooting
- New support request

Web Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://test.cloud.formpipe.com/lasernet/auth

[Add URI](#)

---

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout ✓

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

Access tokens (used for implicit flows)

ID tokens (used for implicit and hybrid flows)

Supported account types

2. (Optional) Add additional Redirect URIs to the list if required.

3. Click **Save**.

**Notes:**

- You need a Redirect URI for each FQDN you use to access Lasernet (including localhost).
- For access to Lasename Web Client you need to add a Redirect URI for https://<FQDN>/lasernet/client as well.

## 2.3 Configure App Roles

Azure AD users are granted access to Lasernet using App Roles. These roles will define a user's permissions in Lasetnet.

Lasetnet comes with a predefined role for administrative access called 'Admin.Global'. We need to configure this App Role in Azure AD to be able to access Lasetnet initially.

1. Select the App Roles tab.
2. Click **Create an App Role**.
3. Fill in the form as shown.

### Create app role

✕

Display name \* ⓘ

 ✓

Allowed member types \* ⓘ

Users/Groups

Applications

Both (Users/Groups + Applications)

Value \* ⓘ

 ✓

Description \* ⓘ

 ✓

Do you want to enable this app role? ⓘ

### Notes:

- Display name and Description can be configured to your liking.
- Value must be set to 'Admin.Global'.
- Allowed member types should be Users/Groups in order to be able to assign Azure AD users to this role.

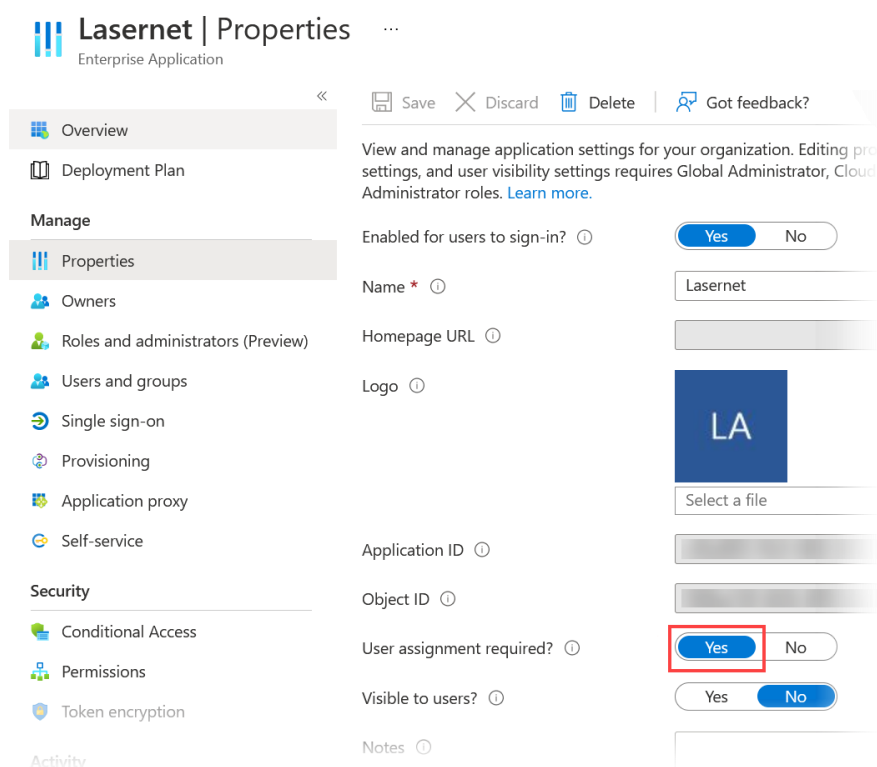
4. Click **Apply**.

Additional App Roles can be added and configured as needed.

## 2.4 Configure the Enterprise application registration

1. Navigate to Azure Active Directory.
2. Select the Enterprise applications tab.
3. Search for the Lasernet app registration using the name you provided when creating the app registration.
4. Select the app registration in the search results.
5. Click the Properties tab.
6. Set 'User assignment required?' to **Yes**.

[Home](#) > [Formpipe Lasernet](#) > [Enterprise applications](#) > [Lasernet](#)



**Lasernet | Properties**  
Enterprise Application

Save Discard Delete Got feedback?

View and manage application settings for your organization. Editing properties, and user visibility settings requires Global Administrator, Cloud Administrator roles. [Learn more.](#)

Enabled for users to sign-in?  Yes  No

Name \*

Homepage URL

Logo

Application ID

Object ID

User assignment required?  Yes  No

Visible to users?  Yes  No

Notes

7. Click **Save**.



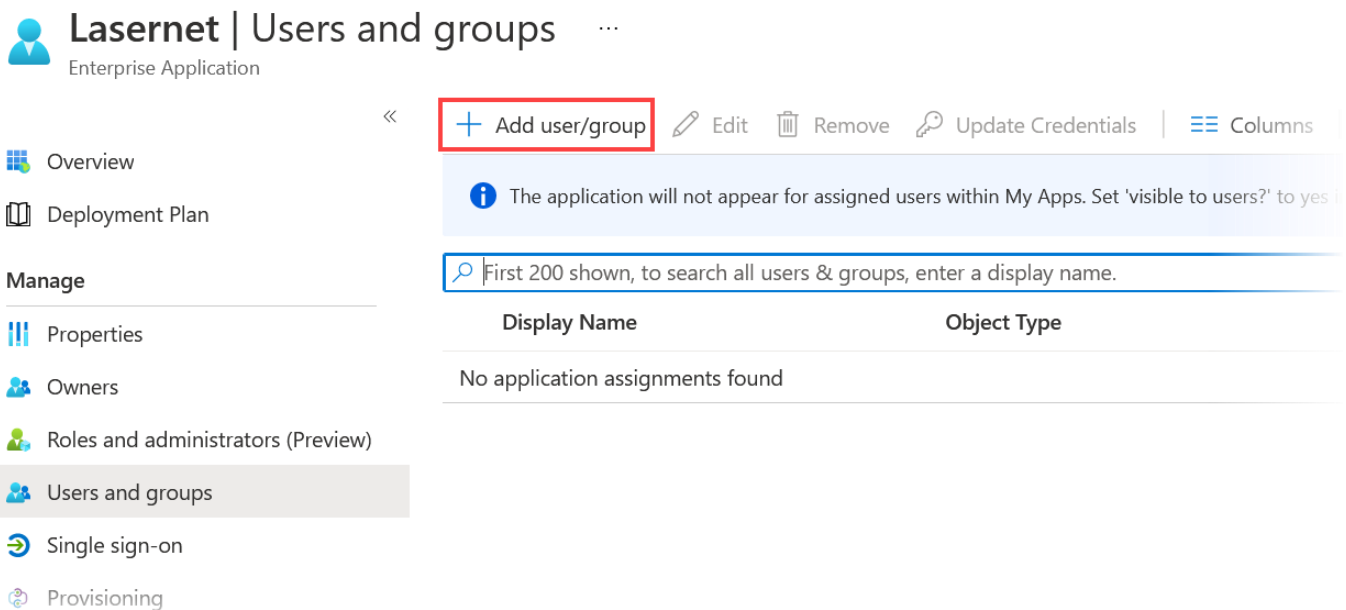
## 2.5 Assign users and groups to the Admin.Global App Role

In order to access Lasernet for the first time we must assign one or more users/groups to the administrative role using Azure AD.

User assignment is done through the Azure Portal ► Azure Active Directory ► Enterprise Applications

1. Select the Users and groups tab.
2. Click **Add user/group**.

[Home](#) > [Formpipe Lasernet](#) > [Enterprise applications](#) > [Lasernet](#)



**Lasernet** | Users and groups ...  
Enterprise Application

« **+ Add user/group** Edit Remove Update Credentials | Columns

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
No application assignments found	

Manage

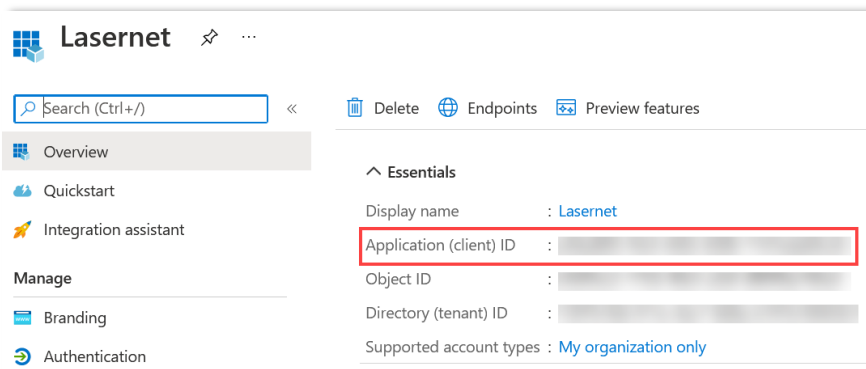
- Overview
- Deployment Plan
- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups**
- Single sign-on
- Provisioning

3. Select a user or group.
  4. If the user isn't assigned the 'Global administrators' role, you must select it manually.
- Note:** If no other App Roles are configured, the role assignment will default to 'Global administrators'.
5. Click **Assign**.

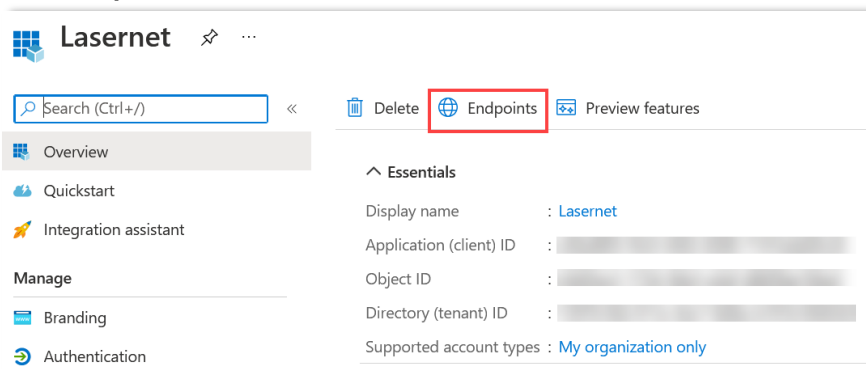
## 2.6 Collect information required to configure Lasernet

In order to configure Lasetnet for Azure Active Directory authentication we need to collect some information about the App Registration we just created.

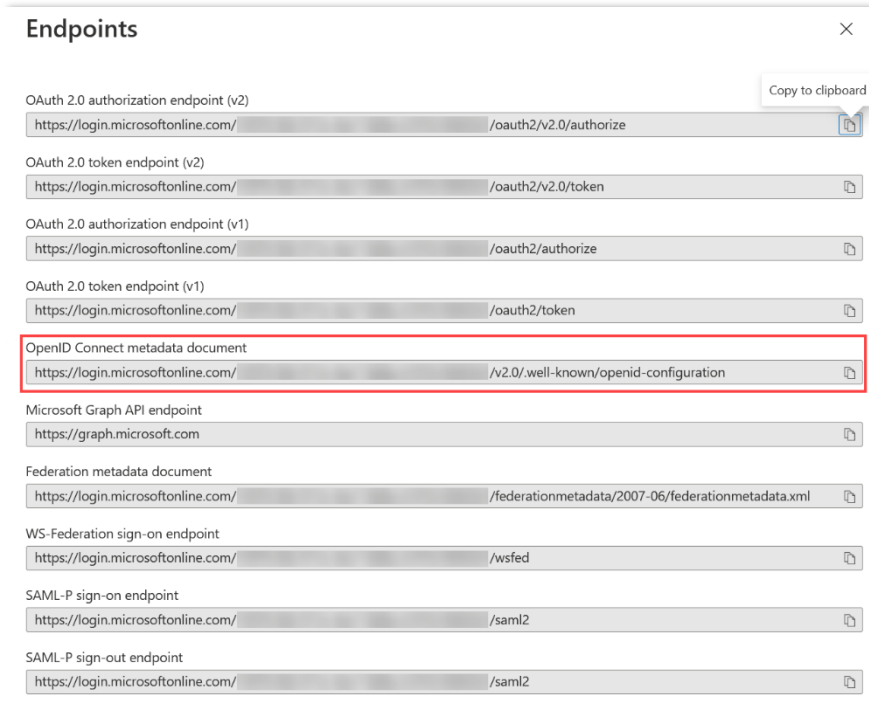
1. Navigate to the Azure Portal ► Azure Active Directory.
2. Go to App registrations and locate the App registration for Lasetnet.
3. From the 'Overview' pane copy the 'Application (client) ID' and store it for later.



### 4. Click Endpoints



5. Copy the value for the 'OpenID Connect Metadata document' endpoint and store it for later.



The screenshot shows a dialog box titled "Endpoints" with a close button (X) in the top right corner. A "Copy to clipboard" button is located in the top right of the dialog. The list of endpoints is as follows:

- OAuth 2.0 authorization endpoint (v2): `https://login.microsoftonline.com/.../oauth2/v2.0/authorize`
- OAuth 2.0 token endpoint (v2): `https://login.microsoftonline.com/.../oauth2/v2.0/token`
- OAuth 2.0 authorization endpoint (v1): `https://login.microsoftonline.com/.../oauth2/authorize`
- OAuth 2.0 token endpoint (v1): `https://login.microsoftonline.com/.../oauth2/token`
- OpenID Connect metadata document: `https://login.microsoftonline.com/.../v2.0/well-known/openid-configuration`**
- Microsoft Graph API endpoint: `https://graph.microsoft.com`
- Federation metadata document: `https://login.microsoftonline.com/.../federationmetadata/2007-06/federationmetadata.xml`
- WS-Federation sign-on endpoint: `https://login.microsoftonline.com/.../wsfed`
- SAML-P sign-on endpoint: `https://login.microsoftonline.com/.../saml2`
- SAML-P sign-out endpoint: `https://login.microsoftonline.com/.../saml2`

## 3 Configure Lasernet Configuration Server.

In order to configure LAsernet for Azure Active Directory authentication we must configure the LAsernet Configuration server with the information collected in 2.6.

### 3.1 Locate or create the ServerSettings.json file

If the LAsernet Config service has been started, it will have generated a ServerSettings.json file in the runtime directory (typically located in C:\ProgramData\Formpipe Software\LAsernet 10\Config\Default).

If the file does not exist, you can create it manually using a text editor (make sure the file extension is '.json' and not '.txt').

### 3.2 Configure TLS bindings

In order to avoid certificate warnings when accessing the LAsernet sites in a browser you must configure certificate bindings in ServerSettings.json.

If no bindings are configured LAsernet will auto-generate self-signed certificates for 'localhost', '<machine name>' and (if applicable) '<machine name>.<active directory domain name>'.

LAsernet can use certificates installed in the Windows certificate store (under Computer certificates) or certificates stored on disk as PFXs.

In order to configure custom bindings you must modify the Bindings object under the "Service" object in ServerSettings.json.

The Bindings object is an array of Bindings with the following format:

Property	Type	Description
Hostname	String	(Required) The hostname for which to bind a certificate
Thumbprint	String	(Optional) This will force LAsernet to use the certificate with the specified thumbprint in the Windows Certificate store.
PFX	String	(Optional) A path and filename to the certificate (including private key) stored in PFX format.
Password	String	(Required when using PFX) Specifies the password for the PFX file.

If only Hostname is specified, LAsernet will attempt to find a suitable certificate for the specified hostname in the Windows Certificate store. If no suitable certificate is found, LAsernet will generate a self-signed certificate for this hostname.

### 3.3 Add authentication settings for Azure AD authentication

In order to configure Lasernet for Azure AD authentication we must add an Authentication object to the "Service" object in ServerSettings.json.

```
{
  "Service": {
    "Bindings": [
      ...
    ],
    "Authentication": {
      "Type": "External",
      "Providers": {
        "Default": {
          "OIDCMetadataEndpoint": "<OpenID Connect metadata document URI>",
          "ClientId": "<Application (client) ID>"
        }
      }
    }
  }
}
```

The Authentication object contains the following properties:

Property	Default value	Description
Type	"Local"	Tells Lasetnet whether to use local or external users (OpenID Connect). Can be set to either 'Local' or 'External'.
Providers	<empty>	Contains a list of named authentication provider objects. When external configuration is used you must add at least one provider. One of the providers must be named "Default" and will be used if the user doesn't specify a provider when logging in.

The format of a Provider object is as follows:

Property	Description
ClientId	Contains the Application (Client) ID identifying the App registration in Azure AD.
OIDCMetadataEndpoint	Contains the URI of the OpenID Connect Metadata document for the Azure AD tenant. The OpenID Connect Metadata document provides Lasetnet with the information required to validate the JWT tokens issued by Azure AD.

It is possible to configure several different providers in the ServerSettings.json file. In order to authenticate using a different provider, the user has to specify the name of the configured provider when attempting to log in.

### 3.4 Start or Restart the Lasetnet Config service

In order apply the changes to ServerSettings.json you must restart the Lasetnet Config Service using the Services control panel in Windows.

Once the Lasernet Config Service has finished restarting you should be able to log in to the Configuration website using Azure AD authentication. Only users assigned the Admin.Global role will initially be allowed access.

## 4 Configuring additional user permissions in Azure AD and Lasernet.

Lasernet uses Security Roles to manage permissions for users. Lاسernet Security Roles are bound to App Roles in Azure Active Directory by means of External Roles in Lاسernet. Azure AD users and groups can be assigned any number of App Roles thereby allowing granular permission management directly in Azure AD.

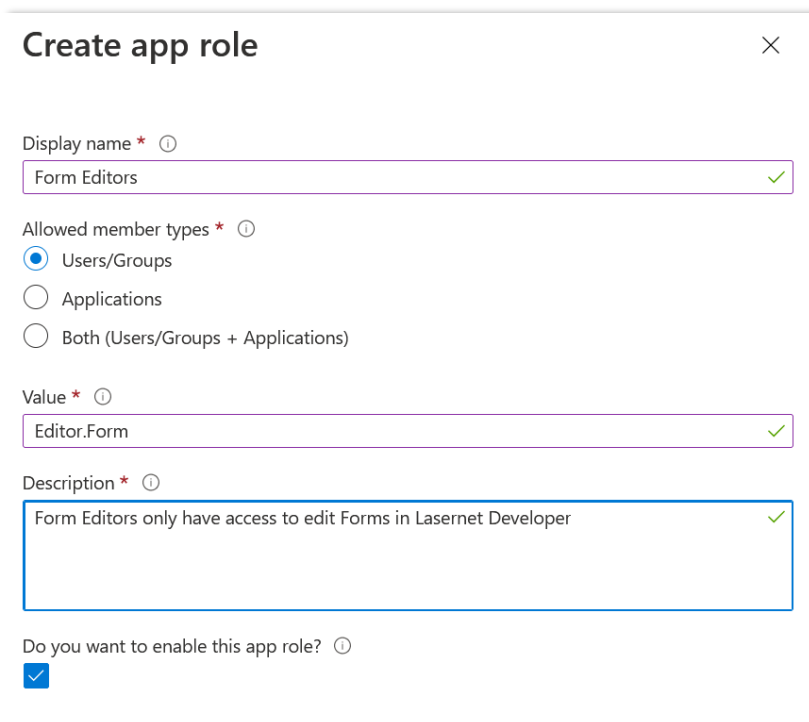
The process of binding users to specific permissions requires the following steps:

1. Add an App Role to the App registration in Azure AD.
2. Assign users and groups to the App Role.
3. Add an External Role in Lاسernet.
4. Add and configure a Security Role in Lاسernet (if necessary).
5. Add the External Role to one or more Security Roles in Lاسernet.

In this example we will show how to configure Lاسernet and Azure Active Directory to allow specific users to only edit Forms in Lاسernet Developer.

### 4.1 Add a new App Role to the Azure App registration

1. Navigate to your App registration for Lاسernet by going to Azure Portal ► Azure Active Directory ► App registrations.
2. Go to the App Roles tab and click **Add Role**.
3. Fill in the information as shown.



### Create app role

Display name \* ⓘ

Form Editors ✓

Allowed member types \* ⓘ

Users/Groups

Applications

Both (Users/Groups + Applications)

Value \* ⓘ

Editor.Form ✓

Description \* ⓘ

Form Editors only have access to edit Forms in Lاسernet Developer ✓

Do you want to enable this app role? ⓘ

**Note:** The name you enter into the Value field must match the name entered when creating the External Role in step 4.3.

4. Click **Apply**.

## 4.2 Assign users and groups to the new App Role

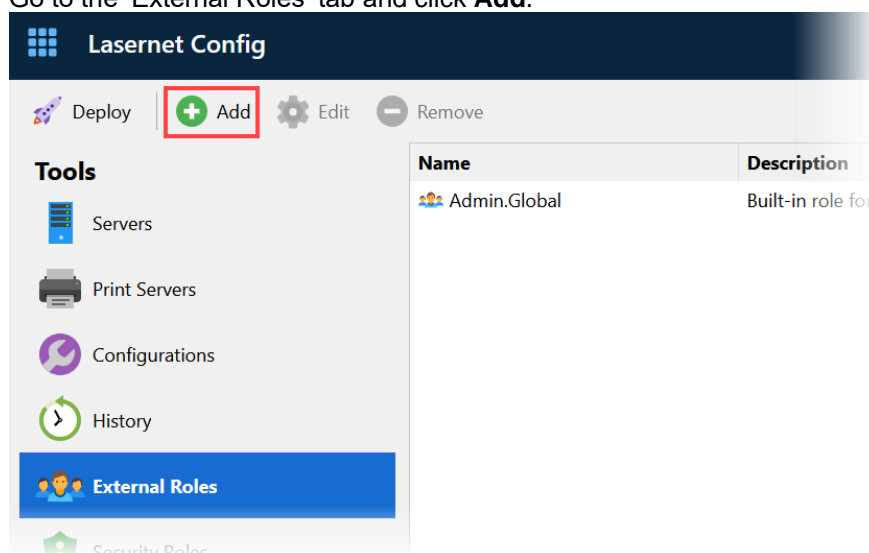
1. Navigate to Azure Portal ► Azure Active Directory ► Enterprise applications.
2. Locate and click your App registration by using the search function.
3. Go to the Users and groups tab and click **Add user/group**.
4. Select one or more users/groups which will be allowed to edit forms in Lasernet.
5. Select the Form Editors role.
6. Click **Assign**.

## 4.3 Add a new External Role in Lasetnet

The External Role in Lasetnet is the glue that binds Azure App Roles together with Lasetnet Security Roles. Every App Role you define in the Azure App registration must have a corresponding External Role in Lasetnet. The binding between an Azure App Role and a Lasetnet External Role is done by name, so it is important that the Name field of the External Role matches the Value field of the corresponding App Role.

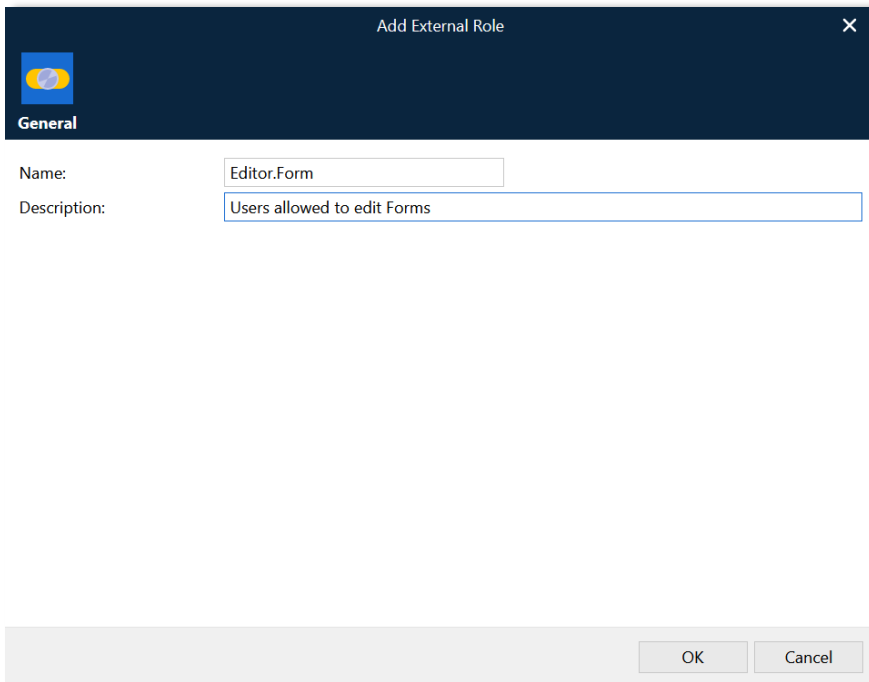
An External Role can be assigned to one or more Security Groups.

1. Navigate and log in to the Lasetnet Configuration Server website (<https://localhost:33443/lasetnet/config>).
2. Go to the 'External Roles' tab and click **Add**.





3. Fill in the form and click **OK**.



**Add External Role**

**General**

Name:

Description:

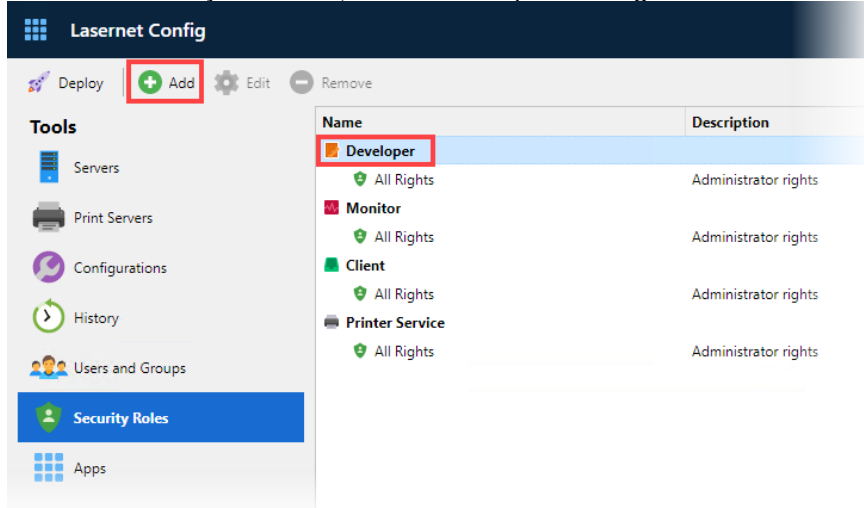
OK Cancel

**Note:** Ensure the name matches the Value entered when creating the App Role in step 4.1.

## 4.4 Add a new Security Role in Lasernet

A Security Role defines which permissions are granted to its members. Security Roles are separated into areas corresponding to the different Lasetnet applications.

1. Go to the Security Roles tab, select Developer in the grid and click **Add**.



**Lasernet Config**

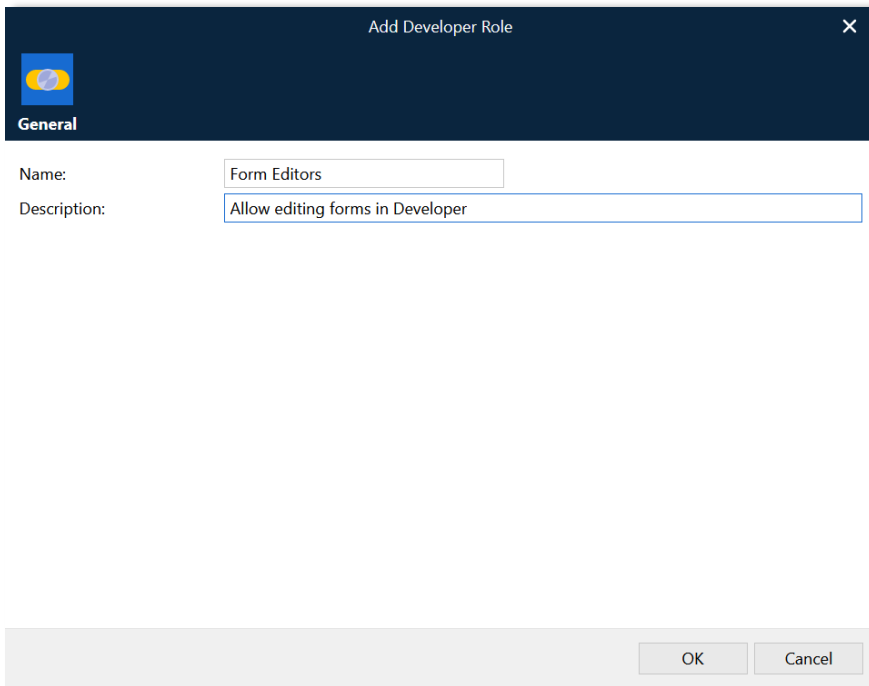
Deploy **Add** Edit Remove

**Tools**

- Servers
- Print Servers
- Configurations
- History
- Users and Groups
- Security Roles**
- Apps

Name	Description
<b>Developer</b>	All Rights Administrator rights
<b>Monitor</b>	All Rights Administrator rights
<b>Client</b>	All Rights Administrator rights
<b>Printer Service</b>	All Rights Administrator rights

2. Fill in the form and click **OK**.



**Add Developer Role**

**General**

Name:

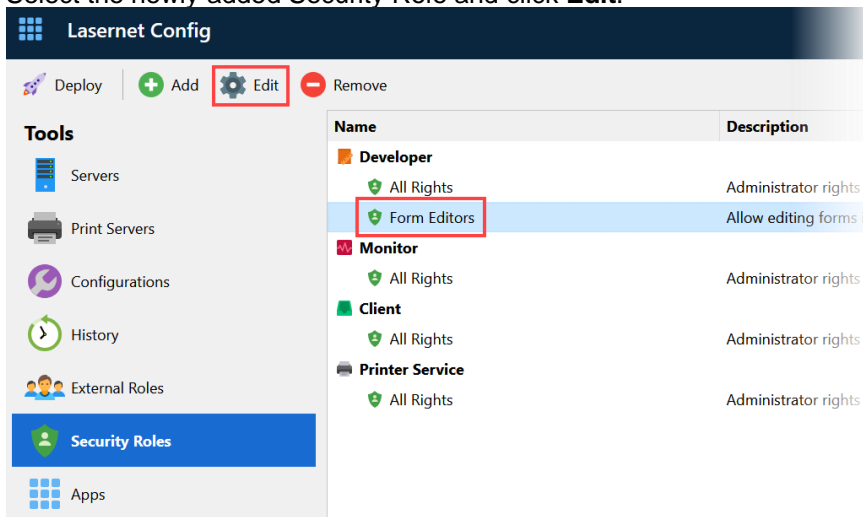
Description:

OK Cancel

## 4.5 Configure new Security Role

We will configure the newly created Security Role to only allow access to edit Forms. The users assigned to this role will be denied access to the Lasernet Configuration website, to deploy configurations or access any other part of the configuration in the Developer.

1. Select the newly added Security Role and click **Edit**.



**Lasernet Config**

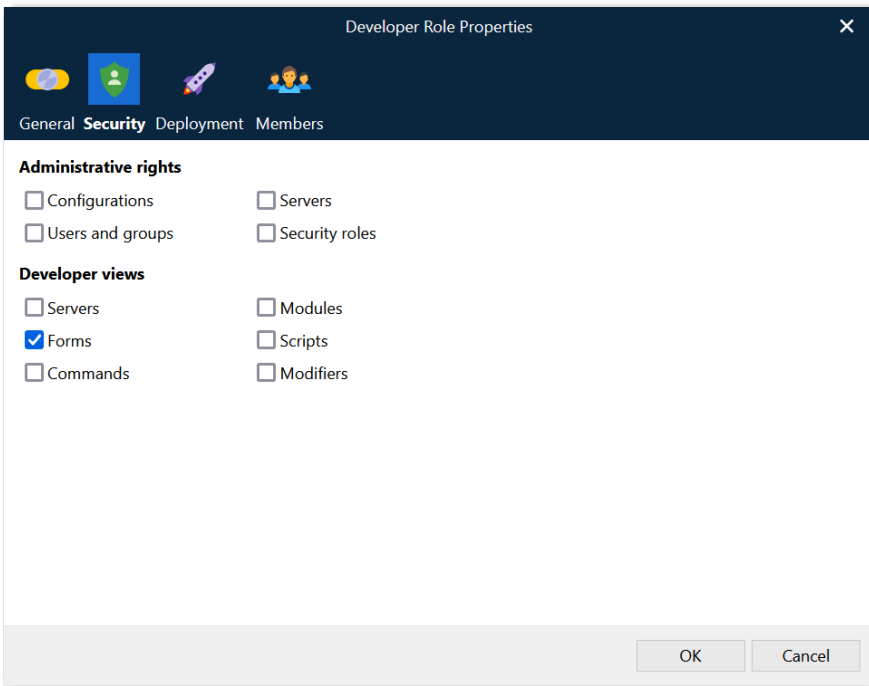
Deploy Add Edit Remove

**Tools**

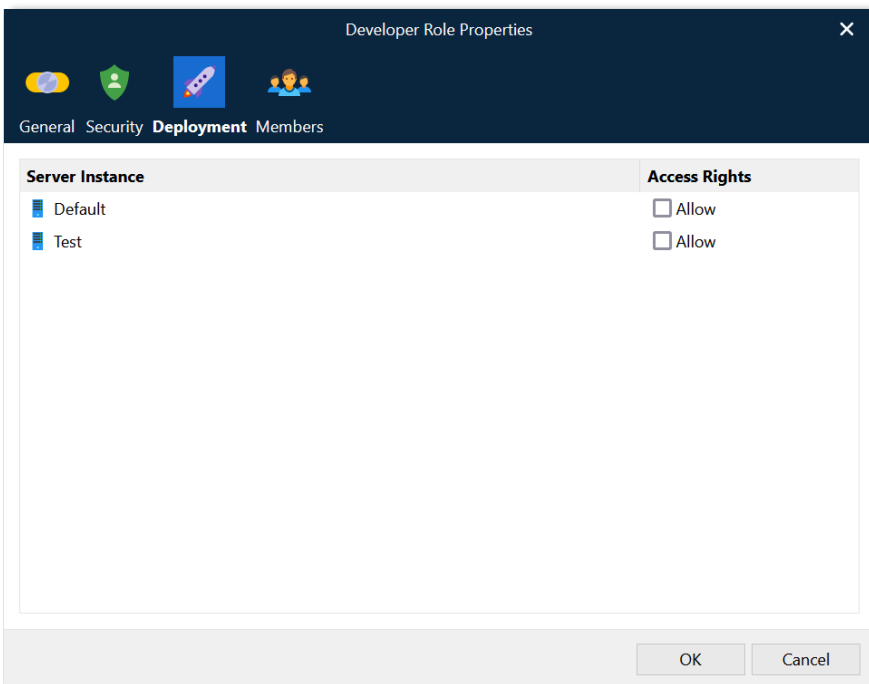
- Servers
- Print Servers
- Configurations
- History
- External Roles
- Security Roles**
- Apps

Name	Description
<b>Developer</b>	
All Rights	Administrator rights
<b>Form Editors</b>	Allow editing forms in
<b>Monitor</b>	
All Rights	Administrator rights
<b>Client</b>	
All Rights	Administrator rights
<b>Printer Service</b>	
All Rights	Administrator rights

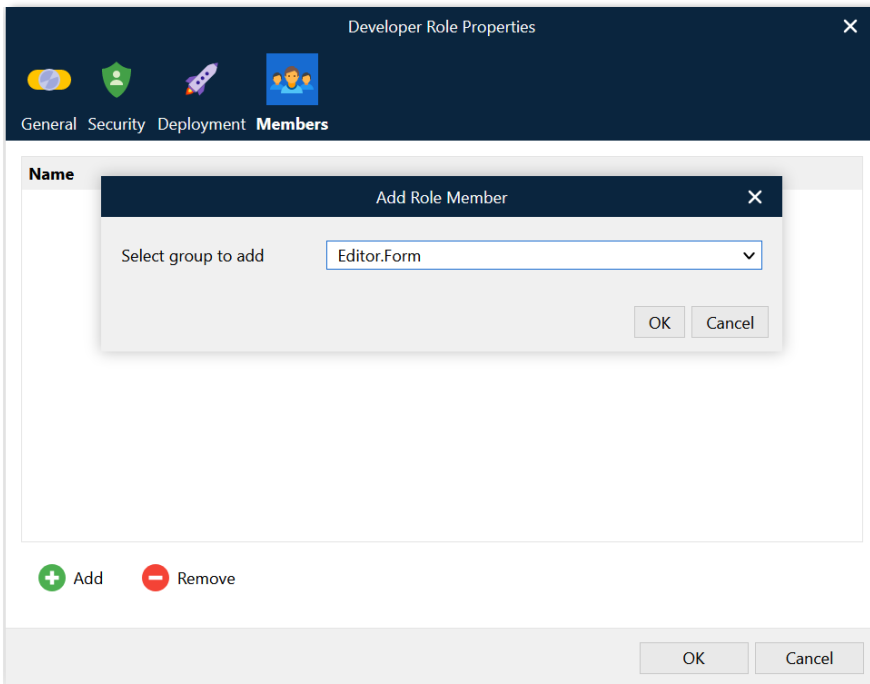
2. Navigate to the Security tab and uncheck all boxes except 'Forms'.



3. Navigate to the Deployment tab and uncheck any boxes.



4. Navigate to the Members tab and add the newly created External Role 'Editor.Form' and click **OK**.



5. Finish editing the Security Role by clicking **OK**.

Now the users selected in step 4.2 will be able to log in to Lasernet Developer using their Azure AD credentials and edit forms.

## 5 Configuring alternative authentication providers.

It is possible to configure multiple authentication providers in Lasernet. The “Default” authentication provider described in section 3.3 will be used if no other provider is specified by the user when logging in. If the user specifies an unknown provider, the “Default” provider will be used.

### 5.1 Adding an alternative provider to ServerSettings.json

Additional authentication providers must be specified in Lasetnet Config Service’s ServerSettings.json file located in C:\ProgramData\Formpipe Software\Lasetnet 10\Config\Default.

To add an alternative provider, you must add a named object to the “Provider” object.

In this example we will add an additional provider called “Backup” by editing the “Authentication” section of ServerSettings.json as shown below.

```
{
  "Service": {
    "Bindings": [
      ...
    ],
    "Authentication": {
      "Type": "External",
      "Providers": {
        "Default": {
          "ClientId": "<Application (client) ID>",
          "OIDCMetadataEndpoint": "<OpenID Connect metadata document URI>"
        },
        "Backup": {
          "ClientId": "<Application (client) ID>",
          "OIDCMetadataEndpoint": "<OpenID Connect metadata document URI>"
        }
      }
    }
  }
}
```

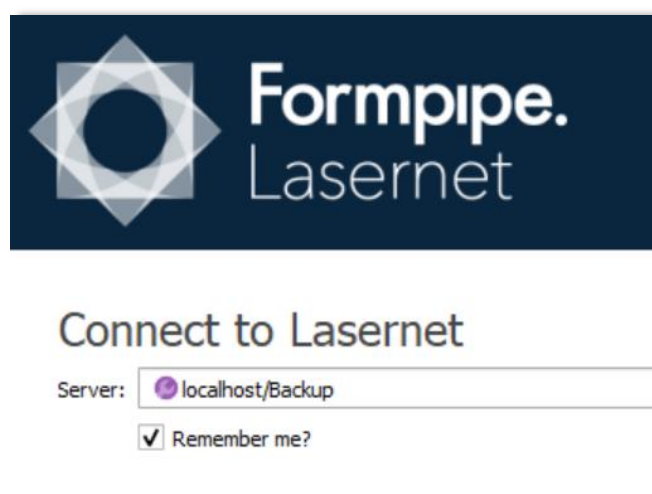
After editing ServerSettings.json the Lasetnet Config service must be restarted using the Service Manager.

## 6 Using alternative authentication providers.

### 6.1 Using alternative authentication providers in native applications

To log in using an alternative authentication provider it is necessary to specify the name of the alternative authentication provider when connecting to the Lasernet Configuration server.

The alternative authentication provider must be specified in the Server field of the Connect dialog:



If the Lasename Configuration service is running on another port than the default (33443), the port must also be specified in the server field in this format: `<servername>:<port>/<provider>`

### 6.2 Using alternative authentication providers in web applications

To log in to a Lasename web site using an alternative authentication provider it is necessary to specify the name of the alternative authentication provider in the URL.

To connect to the Lasename Config web site using the “Backup” provider, use this URL:

<https://localhost:33443/lasernet/config?provider=Backup>

Please note that provider selection must be done in a fresh browser since the provider selection is stored in the browser. It is not possible to switch providers without closing and starting a new browser.