



Installatiehandleiding

CityControl met Azure Active Directory

1. App registration toevoegen in Azure Active Directory

Om te kunnen koppelen met AzureAD (Azure Active Directory) dienen we een app registration toe te voegen.

Home > Azure Active Directory | App registrations

Overview
Preview features
Diagnose and solve problems

Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security attributes
Licenses
Cross-tenant synchronization
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
User settings
Properties

+ New registration | Endpoints | Troubleshooting | Refresh | Download | Preview features | Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications | **Owned applications** | Deleted applications

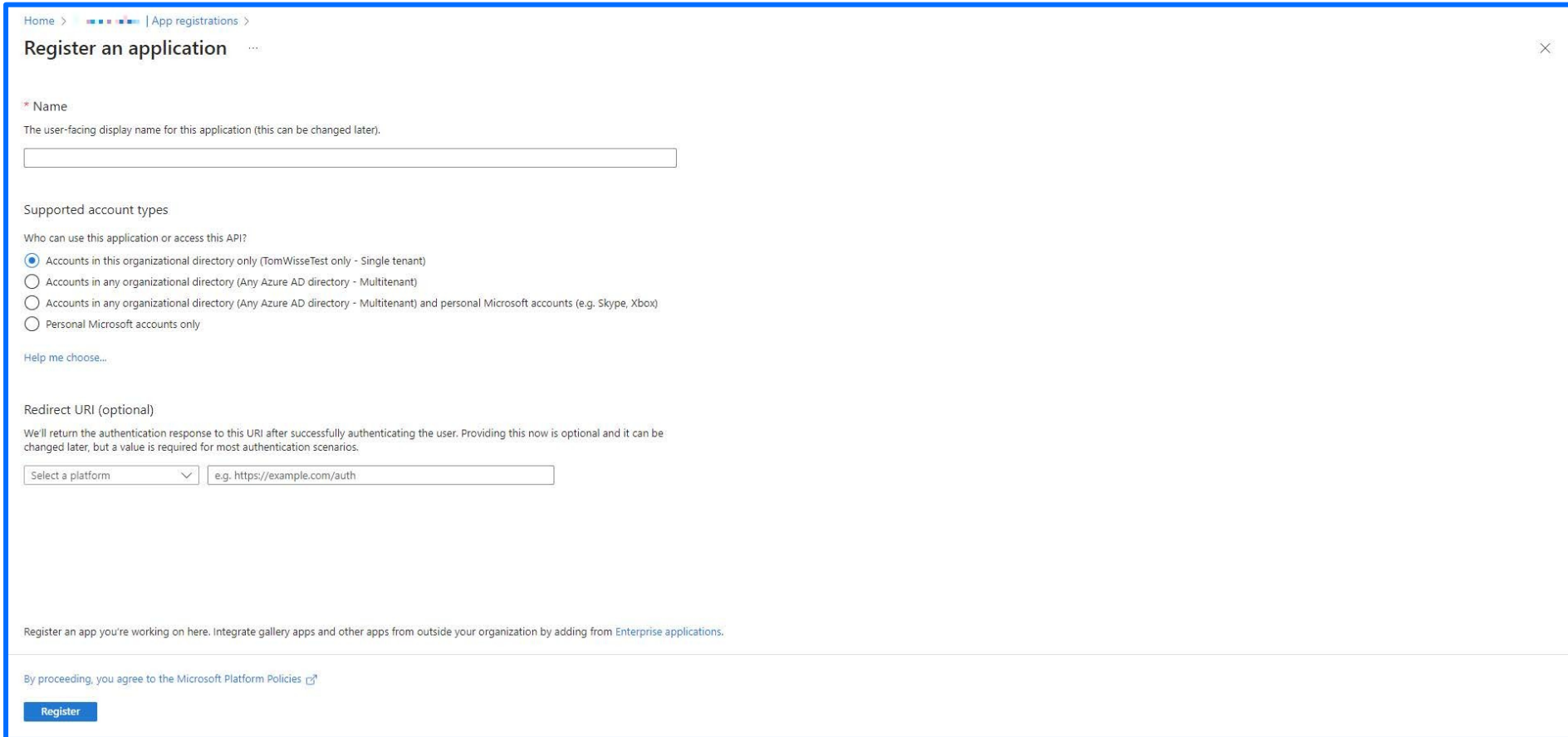
Start typing a display name or application (client) ID to filter these r... Add filters

1 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
CityControl Testomgeving	ff00a3e2-4fab-4f80-957c-12c909cdefc0	6/6/2023	Current

1. Selecteer **Azure Active Directory** in de azure portal
2. Selecteer **App registrations**
3. Selecteer **New registration**

2. Registreer een app registration



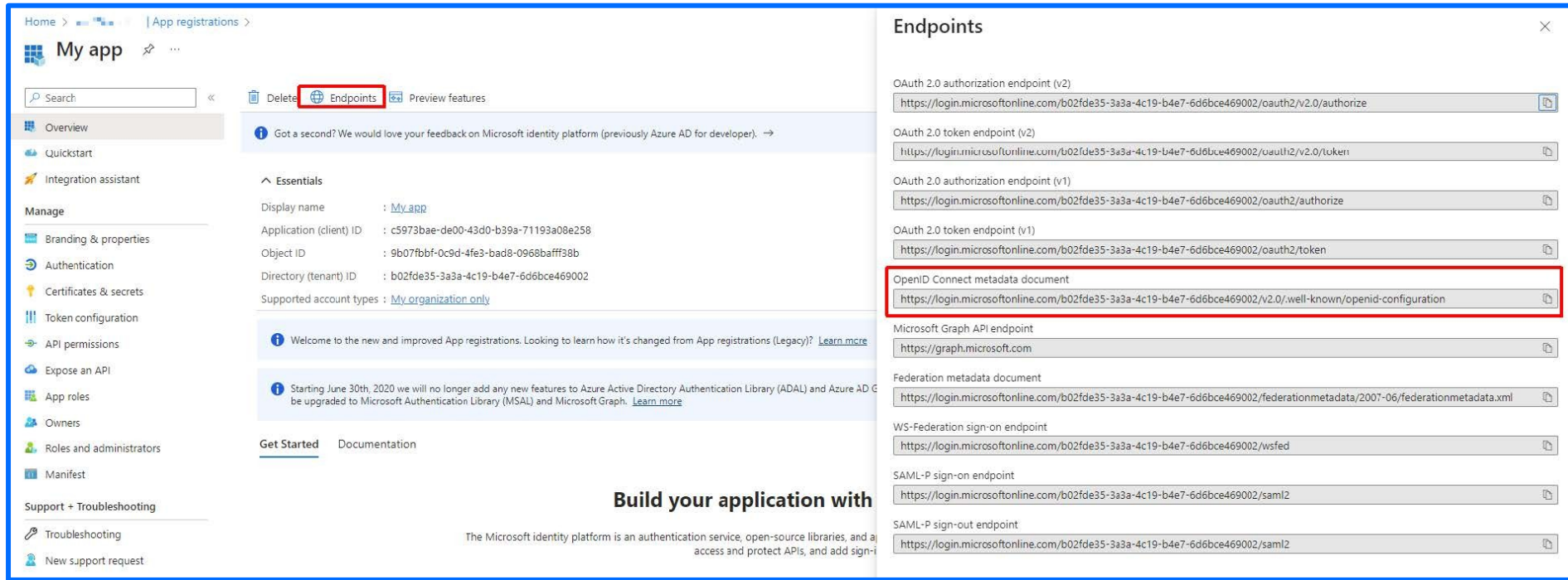
The screenshot shows the 'Register an application' page in the Azure portal. The page is titled 'Register an application' and has a close button in the top right corner. It contains the following sections:

- Name:** A text input field for the user-facing display name. Below it, a note states: 'The user-facing display name for this application (this can be changed later).'
- Supported account types:** A section titled 'Who can use this application or access this API?' with four radio button options:
 - ☒ Accounts in this organizational directory only (TomWisseTest 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 onlyA link 'Help me choose...' is provided below the options.
- Redirect URI (optional):** A section with a note: '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.' It includes a dropdown menu labeled 'Select a platform' and a text input field containing 'e.g. https://example.com/auth'.
- Footer:** A note at the bottom says: 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).' Below this is a link to 'Microsoft Platform Policies' and a blue 'Register' button.

1. Voer bij **Name** een naam in
2. Kies bij **Supported account types** voor de waarde **Accounts in this organizational directory only ([] - Single tenant)**
3. **Redirect URI (optional)** slaan we over. Die weten we nog niet
4. Selecteer **Register**

3. App registration wordt aangemaakt

Je komt uit op de overzichtspagina van de betreffende registration.



The screenshot shows the Azure portal interface for an application registration. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The main content area is titled 'My app' and shows the 'Endpoints' tab selected. The 'Endpoints' tab displays a list of endpoints for the application. The 'OpenID Connect metadata document' endpoint is highlighted with a red box. The 'Endpoints' tab also shows the 'Application (client) ID' and 'Object ID'.

Endpoints

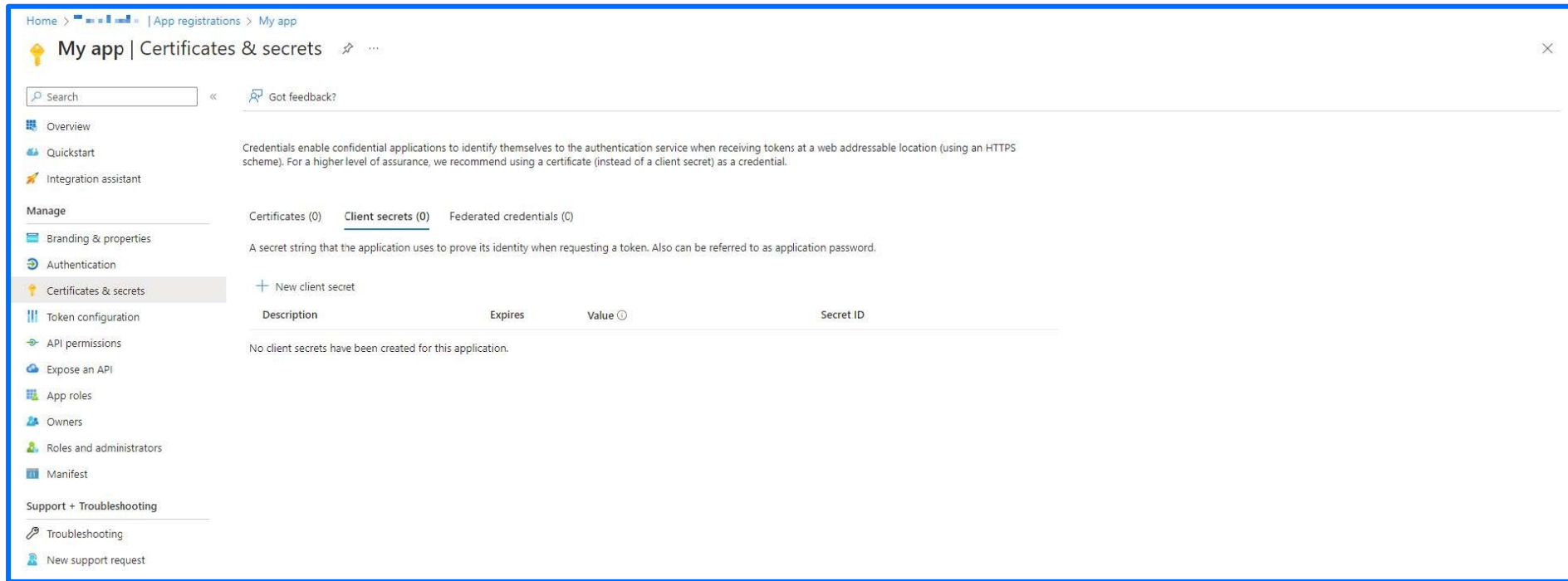
- OAuth 2.0 authorization endpoint (v2)
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/oauth2/v2.0/authorize>
- OAuth 2.0 token endpoint (v2)
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/oauth2/v2.0/token>
- OAuth 2.0 authorization endpoint (v1)
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/oauth2/authorize>
- OAuth 2.0 token endpoint (v1)
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/oauth2/token>
- OpenID Connect metadata document
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/v2.0/.well-known/openid-configuration>
- Microsoft Graph API endpoint
<https://graph.microsoft.com>
- Federation metadata document
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/federationmetadata/2007-06/federationmetadata.xml>
- WS-Federation sign-on endpoint
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/wsfed>
- SAML-P sign-on endpoint
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/saml2>
- SAML-P sign-out endpoint
<https://login.microsoftonline.com/b02fde35-3a3a-4c19-b4e7-6d6bce469002/saml2>

1. Noteer de volgende waarde:
Application (client) ID
2. Selecteer **Endpoints**
3. Noteer de volgende waarde:
OpenID Connect metadata document

! Onthoud de volgende waardes:

- Application (client) ID
- OpenID Connect metadata document

4. Voeg een client secret toe



1. Selecteer **Certificates & secrets**
2. Selecteer **New client secret**
3. Voer bij **Description** een naam of korte omschrijving in
4. Kies bij **Expires** een waarde. Aangeraden is **Recommended: 180 days (6 months)** te kiezen
5. Selecteer **Add**

Er wordt nu een client secret aangemaakt. Deze wordt getoond in het overzicht.

! Noteer en onthoud Value (= client secret)

Deze wordt maar één keer verstrekt en is niet terug te vinden.

Let op: De client secret heeft een houdbaarheidsdatum en dient periodiek geüpdatet te worden. Dit moet afgestemd worden met Sigmax.

5. Overdracht naar Sigmax

De volgende gegevens dienen gecommuniceerd te worden met Sigmax.

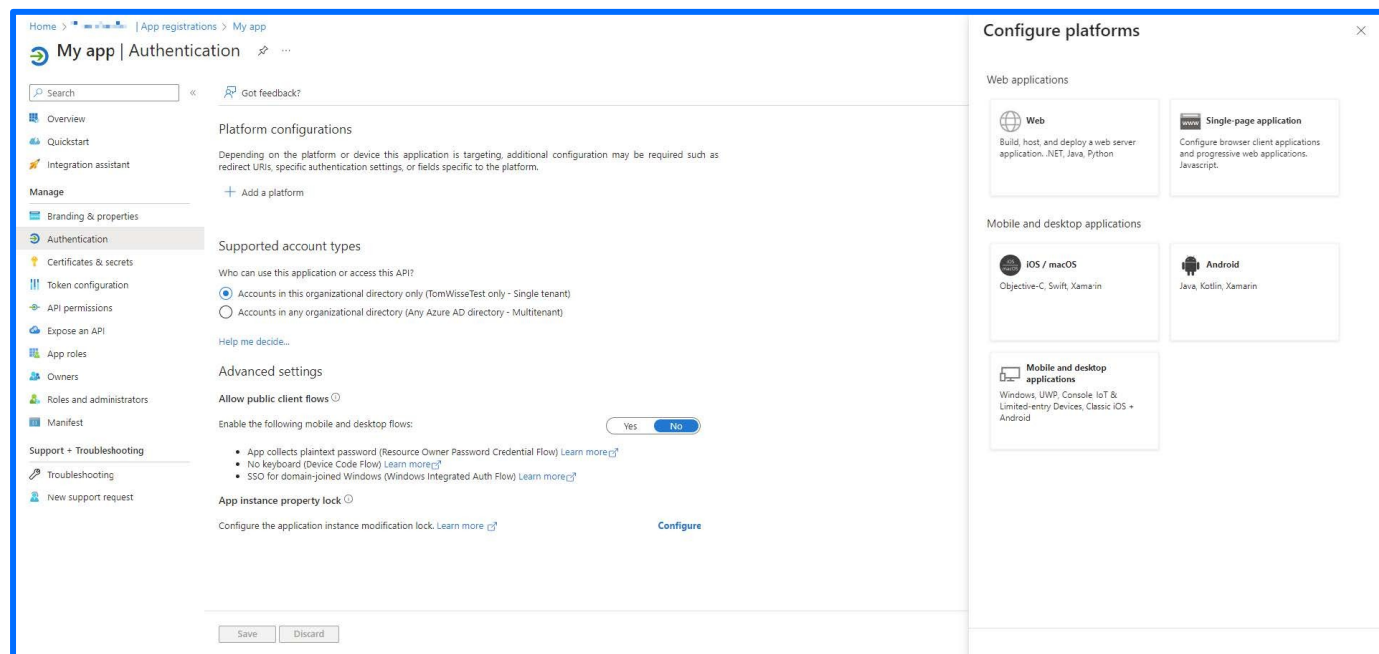
Zij hebben deze waardes nodig om CityControl te configureren zodat ze kunnen inloggen via AzureAD.

Waarde	Omschrijving
Application (client) ID	Client ID
OpenID Connect metadata document	Well known configuration endpoint
Value	Client secret

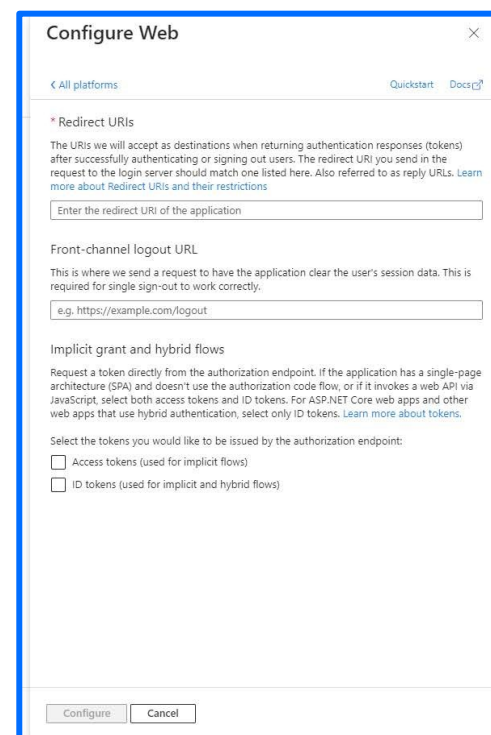


6. Voeg authenticatie toe

Voor deze stap dien je van Sigmax een redirect url te ontvangen. Dit kan Sigmax pas aanleveren nadat de overdracht naar Sigmax heeft plaatsgevonden (zie stap 5).



1. Selecteer **Azure Active Directory** in de azure portal
2. Selecteer **App registrations**
3. Selecteer het item wat in de vorige stappen is aangemaakt
4. Selecteer **Authentication**
5. Selecteer **Add a platform**
6. Selecteer bij **Web applications** de waarde **Web**



Dit dialoog venster verschijnt.

7. Voer bij **Redirect URIs** de aangeleverde url in
8. Selecteer **Configure**

Azure Active Directory is nu correct ingericht zodat Sigmax met CityControl in kan loggen.

Shaping tomorrow's society. Today. Together.

Capitool 13
7521 PL Enschede

P.O. Box 1243
7500 BE Enschede
The Netherlands

T +31 (0)53 480 3100 E
info@sigmax.nl
sigmax.nl

