

Veiligheidsbeeld - Externe API client

Het Veiligheidsbeeld biedt een API aan voor externe applicaties. Met deze API kunnen de topics in het Veiligheidsbeeld opgehaald en bewerkt worden. Zo zou bijvoorbeeld het dreigingsniveau van een topic automatisch verhoogd kunnen worden o.b.v. data uit een externe bron.

- [Nieuwe client toevoegen](#)
 - [Client ID](#)
 - [Client secret](#)
 - [API permissions](#)
- [Authenticatie](#)
- [Beschikbare endpoints](#)
 - [Ophalen alle topics](#)
 - [Ophalen van een topic](#)
 - [Bewerken van een topic](#)
- [Nieuwe rollen toevoegen](#)
 - [Code](#)
 - [Azure Portal](#)


Nieuwe client toevoegen


Een nieuwe externe API client toevoegen gaat via het beheren van Azure AD in de Azure Portal. Onder 'App registrations' kan een 'New registration' toegevoegd worden:

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~-/RegisteredApps

Client ID

Noteer na het registreren van de nieuwe applicatie het **Application (client) ID**; deze is nodig voor het authenticeren bij de API:

 **Essentials**

Display name	: TEST	<div>Copy to clipboard</div>
Application (client) ID	: 23fe5ba4-fe55-4bf6-beae-9047dab17d3d 	
Object ID	: bfca70ac-5225-4332-bfe8-87431a21f2f4	
Directory (tenant) ID	: d167ca06-b5ec-450d-a05c-fac0a794b8a3	
Supported account types	: My organization only	

Client secret

Om te kunnen authenticeren als deze client applicatie zijn credentials nodig; dit doen we door een client secret te definiëren. Op de pagina 'Certificates & secrets' kan een nieuw client secret toegevoegd worden. Deze wordt slechts 1x getoond; daarna is deze niet meer in te zien, dus sla deze op een veilige locatie op:

Certificates (0)**Client secrets (1)**Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
Veiligheidsbeeld API	5/3/2025	iZx8Q~kUzUt6fujR-OG9Gwd2GFL.DfAnQ...	3cecf88-72b2-41eb-9714-333e22d6a802

API permissions

Om toegang te krijgen tot specifieke onderdelen van de API moet de client applicatie rechten toegewezen krijgen. Dit kan op de pagina 'API permissions'.
Druk op 'Add a permission', ga naar 'My APIs' in de sidebar die opent, en kies de Veiligheidsbeeld applicatie:

Home > NW4 | App registrations > TEST

TEST | API permissions

Search

Refresh

Got feedback?

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

New support request

The "Admin consent required" column shows your organization, or in organizations where t

Configured permissions

Applications are authorized to call APIs when they all the permissions the application needs. [Learn m](#)

+ Add a permission

Grant admin consen

API / Permissions name	Type
Microsoft Graph (1)	
User.Read	Delegated

To view and manage consented permissions for ir

Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

My APIs

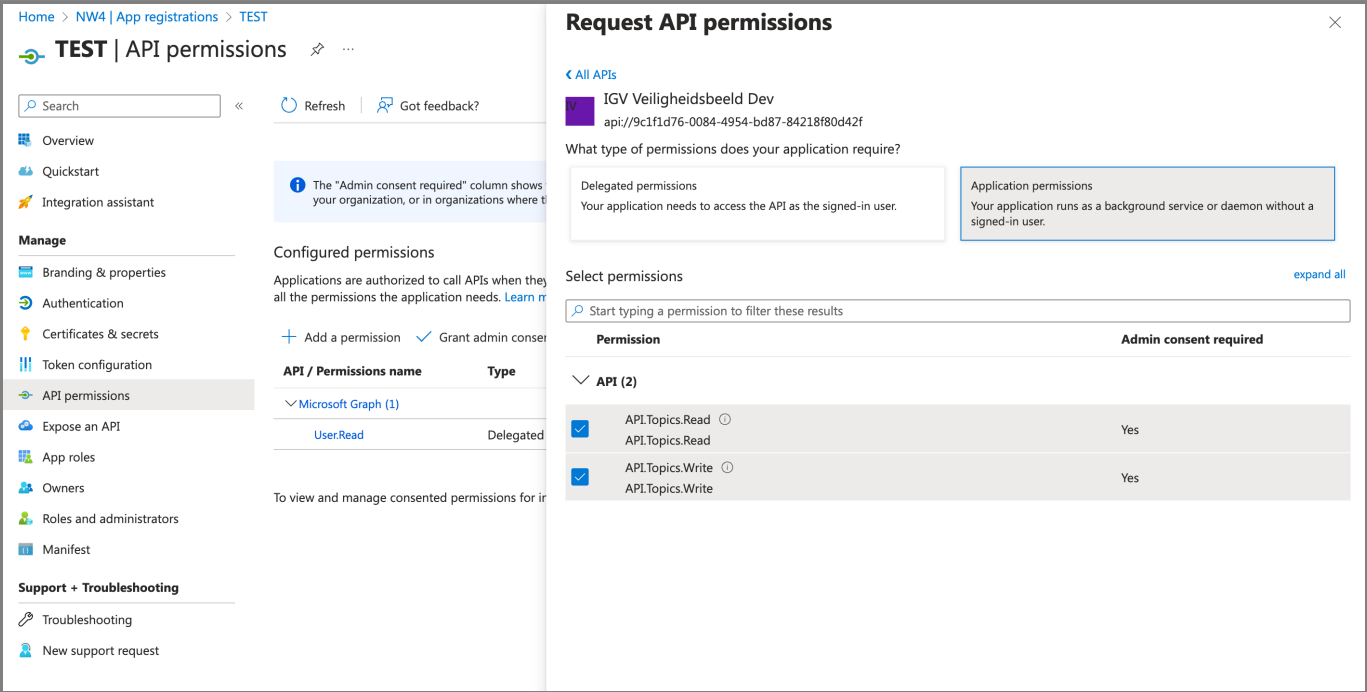
Applications that expose permissions are shown below

Name	Application (client) ID
IGV Admin Test	592b0e5e-e3e1-47b0-aa64-ecd51e3f0d72
IGV Admin Dev	ac7e700f-030d-449c-ae2b-001c454cd8f5
IGV Veiligheidsbeeld Staging	29c42d24-43ab-43c9-9804-e596def31235
IGV Portal Dev	d05fe4f6-1520-48ab-bf21-34b6ee7defbd
IGV Admin	be77f878-bce7-4367-9451-7dc7243e821e
IGV Portal	e6a54f5a-449e-4dcc-8a42-0219a81d69e1
IGV Portal Test	d931a1ef-4c14-49df-af75-a77fc1ec09a4
IGV Veiligheidsbeeld Dev	9c1f1d76-0084-4954-bd87-84218f80d42f

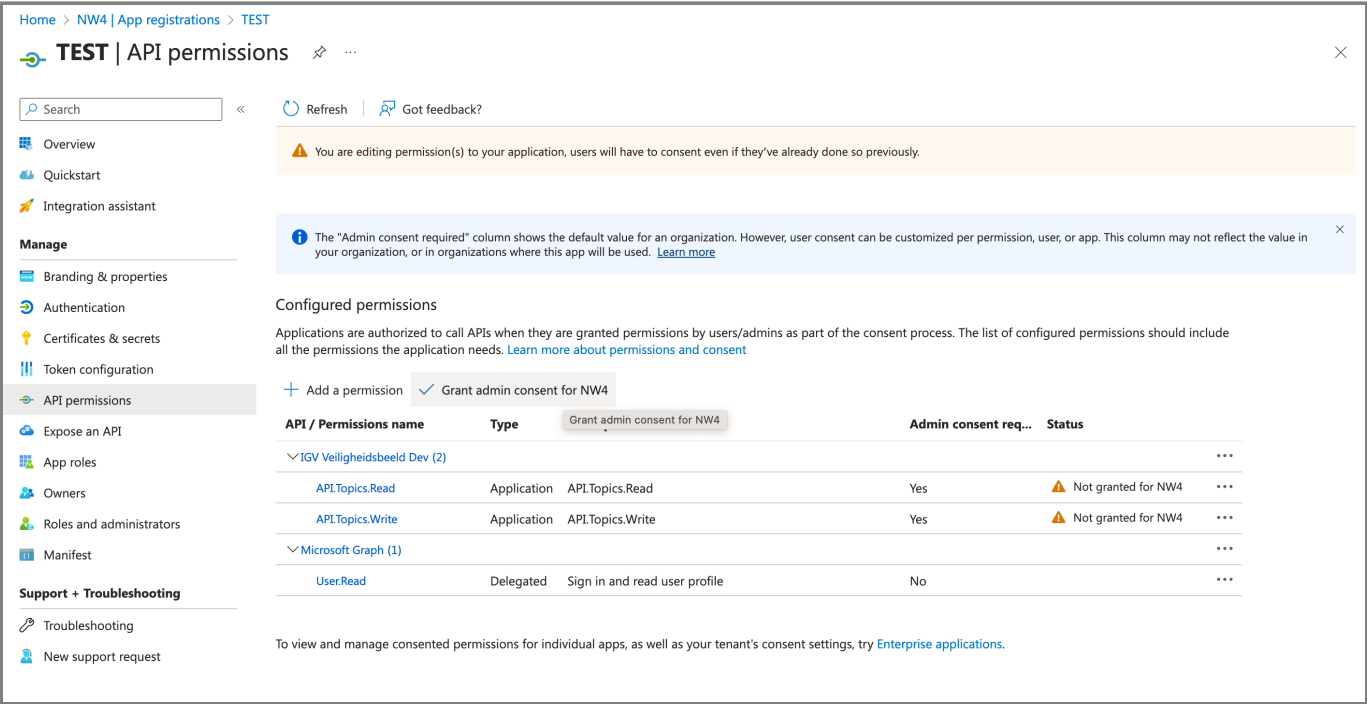
Kies voor 'Application permissions' en voeg de rechten toe die de client nodig gaat hebben:

- **API.Topics.Read** voor het ophalen van de topics
- **API.Topics.Write** voor het bewerken en verwijderen van topics

2 / 7



Vervolgens moet er nog toestemming gegeven worden om de rechten daadwerkelijk toe te wijzen, dit kan via de knop 'Grant admin consent':



Vanaf dit moment kan er een token opgehaald worden uit naam van de nieuwe client applicatie die gebruikt kan worden om de Veiligheidsbeeld API aan te roepen.

Authenticatie

Authenticatie met de Veiligheidsbeeld API gaat via een **Bearer** token. Deze kan opgehaald worden via het Azure AD OAuth2 endpoint:

POST <https://login.microsoftonline.com/{tenantId}/oauth2/v2.0/token>

Hierbij moet `{tenantId}` vervangen worden door het ID van de tenant waarin het Veiligheidsbeeld (en de client applicatie) staan.

Als body (met type `x-www-form-urlencoded`) moeten parameters meegestuurd worden die aangeven om welke applicatie het gaat, en met welke applicatie gecommuniceerd gaat worden:

Parameter	Waarde
<code>client_id</code>	Het client ID van de client applicatie
<code>client_secret</code>	Het client secret dat aangemaakt is voor de client applicatie
<code>scope</code>	<code>api://{api_client_id}/.default</code> , waarbij <code>{api_client_id}</code> vervangen moet worden door het client ID van de Veiligheidsbeeld applicatie (dus niet de client)
<code>grant_type</code>	<code>client_credentials</code>

Dit endpoint geeft een response met daarin een `access_token`, die waarde moet als `Authorization` header in de vorm `Bearer {access_token}` meegestuurd worden met requests naar de Veiligheidsbeeld API.

Beschikbare endpoints

Op dit moment zijn er externe endpoints beschikbaar voor het ophalen en bewerken van topics.

Ophalen alle topics

De lijst van alle beschikbare topics kan opgehaald worden via het volgende endpoint:

`GET /api/external/topics`

De response bestaat uit een lijst van objecten met (een aantal van) de waardes van een topic:

```
[
  {
    "id": "43988a39-d270-40f2-a875-c440d49eedf0",
    "title": "Verkeer",
    "isActive": true,
    "slug": "verkeer",
    "shortDescription": "Zwarte zaterdag",
    "rawContent": "<h1>Verkeer</h1><h2>Files</h2><p>Er staan weer eens  
veel files.</p><h2>Boeren</h2><p>Er rijden boze boeren op de A58.</p>",
    "subTopics": [],
    "currentThreatLevel": 2,
    "maxThreatLevel": 4,
    "creationTime": "2023-05-04T07:24:12.399412Z",
    "lastModificationTime": "2023-05-04T07:24:12.399412Z"
  },
  {
    "id": "07695849-0786-4c81-b336-c81f6976a555",
    "title": "Weer",
```

```
    "isActive": true,
    "slug": "weer",
    "shortDescription": "Lekker zomerweertje",
    "rawContent": "<h1>Weer</h1><h2>KNMI</h2><p>Het KNMI geeft geen  
waarschuwingen</p>",
    "subTopics": [],
    "currentThreatLevel": 1,
    "maxThreatLevel": 5,
    "creationTime": "2023-05-02T07:24:12.399412Z",
    "lastModificationTime": "2023-05-02T08:56:12.399412Z"
  }
]
```

Ophalen van een topic

Op basis van de slug die in elk topic te vinden is kan deze ook los opgehaald worden door de slug achter de URL van het vorige endpoint te zetten:

GET /api/external/topics/{slug}

De response bestaat uit een object met (een aantal van) de waardes van een topic:

```
{
  "id": "43988a39-d270-40f2-a875-c440d49eedf0",
  "title": "Verkeer",
  "isActive": true,
  "slug": "verkeer",
  "shortDescription": "Zwarte zaterdag",
  "rawContent": "<h1>Verkeer</h1><h2>Files</h2><p>Er staan weer eens veel  
files.</p><h2>Boeren</h2><p>Er rijden boze boeren op de A58.</p>",
  "subTopics": [],
  "currentThreatLevel": 2,
  "maxThreatLevel": 4,
  "creationTime": "2023-05-04T07:24:12.399412Z",
  "lastModificationTime": "2023-05-04T07:24:12.399412Z"
}
```

Bewerken van een topic

Met dit endpoint kan een enkel topic aangepast worden. Het is mogelijk om o.a. de beschrijving, het dreigingsniveau en de volledige HTML-inhoud aan te passen. Dit kan d.m.v. het volgende endpoint (waarbij {id} vervangen wordt door het ID van het topic dat aangepast moet worden):

PUT /api/external/topics/{id}

Als body moet het topic object meegestuurd worden, zonder id, creationTime of lastModificationTime:

```
{
  "title": "Verkeer",
  "isActive": true,
  "slug": "verkeer",
  "shortDescription": "Alles rustig",
  "rawContent": "<h1>Verkeer</h1><h2>Files</h2><p>Er staan bijna geen files.</p><h2>Boeren</h2><p>De boze boeren zijn weer weg.</p>",
  "currentThreatLevel": 1,
  "maxThreatLevel": 4
}
```

De response is het bijgewerkte topic, met dezelfde vorm als bij het endpoint waarmee topics opgehaald worden.

Nieuwe rollen toevoegen

Als er nieuwe features aan de externe API toegevoegd worden, moeten er mogelijk nieuwe permissies toegevoegd worden. Deze moeten toegevoegd worden in de API en in de Azure portal. Daarna kunnen de permissies via de Azure portal ook echt toegewezen worden aan de juiste client applicaties.

Code

Voeg een extra rol toe aan de `ExternalClientRoles`:

```
public static class ExternalClientRoles
{
    public static class Topics
    {
        public const string Read = "API.Topics.Read";
        public const string Write = "API.Topics.Write";

        public const string MyNewPermission = "API.Topics.NewPermission";
    }
}
```

Voeg in `Startup.cs` een extra policy toe waar op gecheckt kan worden:

```
services.AddAuthorization (options => {
    ...

    options.AddPolicy (ExternalClientRoles.Topics.MyNewPermission, policy
=> policy.Requirements.Add (new HasRoleRequirement
(ExternalClientRoles.Topics.MyNewPermission)));
});
```

Voeg de nieuwe check toe aan een endpoint d.m.v. het `[Authorize]` attribute:

```
[Authorize (Policy = ExternalClientRoles.Topics.MyNewPermission)]
public async Task<string> GetNewValue (Guid id)
{
    ...
}
```

Azure Portal

Een nieuwe permissie aan de API client toevoegen kan door een nieuwe app role te definiëren.

Open de 'App registrations' pagina en navigeer naar de detailpagina van de Veiligheidsbeeld applicatie.

Op de pagina 'App roles' kan een nieuwe app role toegevoegd worden:

Home > NW4 | App registrations > IGV Veiligheidsbeeld Dev

IGV Veiligheidsbeeld Dev | App roles

Search

Create app role | Got feedback?

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

New support request

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
API.Topics.Read	Read topics from external client	Applications	API.Topics.Read	bbb86f30-4a59-49a2-...	Enabled
API.Topics.Write	Modify topics from external client	Applications	API.Topics.Write	aaa86f30-4a59-49a2-8...	Enabled
WriteCategories	Can manage categories	Users/Groups	WriteCategories	a77cd719-0cf6-4fd6-9...	Enabled
WriteTopics	Can create update and delete topics	Users/Groups	WriteTopics	f9c54ac2-78dc-4b5b-9...	Enabled
ReadTopics	Can read topics	Users/Groups	ReadTopics	f4a7e480-1b83-498e-...	Enabled
Beheerder	Beheerder rol Rechten: Lees en schrijf...	Users/Groups	Beheerder	2b13ea27-c273-4dc6-...	Disabled
Admin	Admin rol Rechten: Lees- schrijf cate...	Users/Groups	Admin	74cd18a4-3a18-4705-...	Enabled
Meldkamer	Meldkamer rol rechten: meldkamert...	Users/Groups	Meldkamer	1c686f30-4a59-49a2-8...	Enabled

Kies bij het formulier dat verschijnt onder 'Allowed member types' voor 'Applications'.

Vul als 'Value' de naam in die in de code gebruikt wordt (bijv. `API.Topics.NewPermission` uit het voorbeeld)

Het is ook mogelijk om de app roles direct toe te voegen via de 'Manifest' pagina.