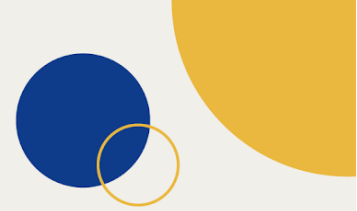


De BHV App User synchronisation via Microsoft Azure

Through automatic user synchronization, accounts in the StandBy BHV app are updated daily (by default during the night) based on your Microsoft Azure group. When you add or remove someone from this group, the account in StandBy is automatically adjusted. This manual provides the necessary details for activation, the available synchronization options, the data we use, and the required Azure configuration.

Requirements	2
Data to be collected for Standby	2
Synchronisation configuration	3
Create (New user):	3
Delete (From Azure group):	3
Exceptions (Retention-whitelist):	3
Data used by StandBy	4
Configuration in Microsoft Azure	5
Stap 1: Configure group	5
Stap 2: Create App-registration	6
Stap 3: Add Permissions & Grant Admin Consent	7
Stap 4: Create Client Secret	9
Stap 5: Execute Admin Consent URL	10
How does Synchronisation work in practise?	10
Next Steps	11
Providing data	11
Testing	11
Synchronisation	11



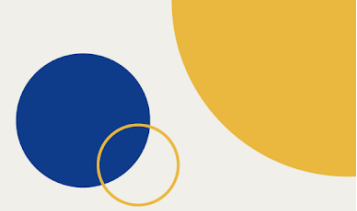
Requirements

- A **Microsoft Azure environment** (at least one environment/tenant).
- An **Azure Group** in which all individuals who require a StandBy BHV account are added.
- The permissions to create and configure a **'daemon app'** (an app with background permissions) within the Azure environment, as well as grant administrative permissions for it.
- The permissions to grant one-time **'admin consent'** for the application.

Data to be collected for Standby

To enable the linking of user data, after completing the steps outlined below, the following information must be provided to StandBy Solutions:

- Tenant ID
- Group ID ('object ID')
- App ID ('object ID')
- App Client ID
- App Client Secret
- At least one contact person / department (name and email address) who can be contacted if there are issues with credentials at a later stage (such as an expired API secret).



Synchronisation configuration

By default, user synchronization will be executed once per day between 00:00 and 06:00 during the night.

Create (New user):

- Users automatically receive the 'BHV' role and are linked to the primary location(s).
- Users immediately receive an activation email containing instructions and the app download link.

Delete (From Azure group):

- The account and associated data are immediately removed from StandBy.
- Users receive an email confirming that app access has been revoked.

Exceptions (Retention-whitelist):

- System accounts can be placed on a 'whitelist' so that they are never automatically removed, even if they disappear from Azure.

Please note: This module synchronizes users only once upon creation or deletion in Azure. No interim updates take place (such as changes to email address or phone number). This is *not* a Single Sign-On (SSO) module.



Data used by StandBy

StandBy Solutions performs user synchronization every night. During this process, all users who are members of the specified group in Microsoft Azure are retrieved.

The following fields are retrieved via the Microsoft Graph API:

id, **businessPhones**, **mail**, **mobilePhone**, officeLocation, **givenName**, **surname**, accountEnabled, createdAt, **employeeId**

The following fields are used and stored within StandBy by default:

- **givenName** and **surname** used to construct the username (both required).
- **mail**: Used to link to the StandBy account and inform the user about their new account (as well as other StandBy application-specific email notifications depending on the selected modules/configuration) (required).
- **employeeId**: Used to uniquely identify users. Based on this ID, StandBy determines whether a user should be created, maintained, or removed (required).
- **mobilePhone**: Used as the phone number if available in the API response. Otherwise, the system checks (only) the first phone number in **businessPhones**. If no phone numbers are found, none is stored in StandBy.

If the API fails to respond or returns incomplete required data for any reason, no mutations are performed on the StandBy side.

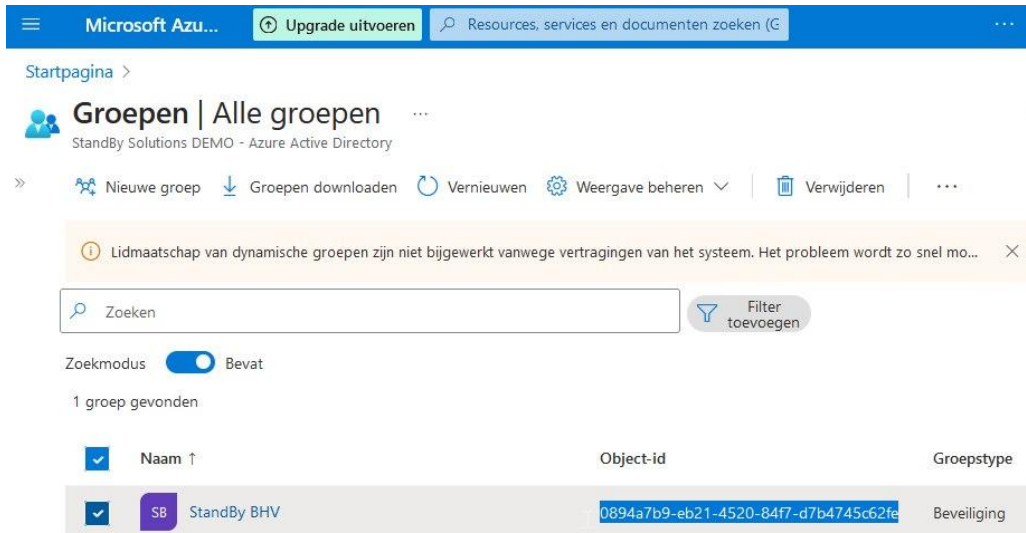
Optional fields:

- **officeLocation**: Can be custom-mapped to automatically assign a user's Azure location to the appropriate location(s) within the StandBy app.
- **accountEnabled**: Can be used to automatically remove disabled Azure accounts. (**accountEnabled** = **false**) From StandBy, even if they remain in the Azure group.
- **createdDateTime**: Used by StandBy to analyze and resolve potential synchronization issues.



Configuration in Microsoft Azure

Step 1: Configure group



Startpagina > Microsoft Azure > Upgrade uitvoeren > Resources, services en documenten zoeken (G)

Groepen | Alle groepen

StandBy Solutions DEMO - Azure Active Directory

Nieuwe groep | Groepen downloaden | Vernieuwen | Weergave beheren | Verwijderen

Lidmaatschap van dynamische groepen zijn niet bijgewerkt vanwege vertragingen van het systeem. Het probleem wordt zo snel mo...

Zoeken

Filter toevoegen

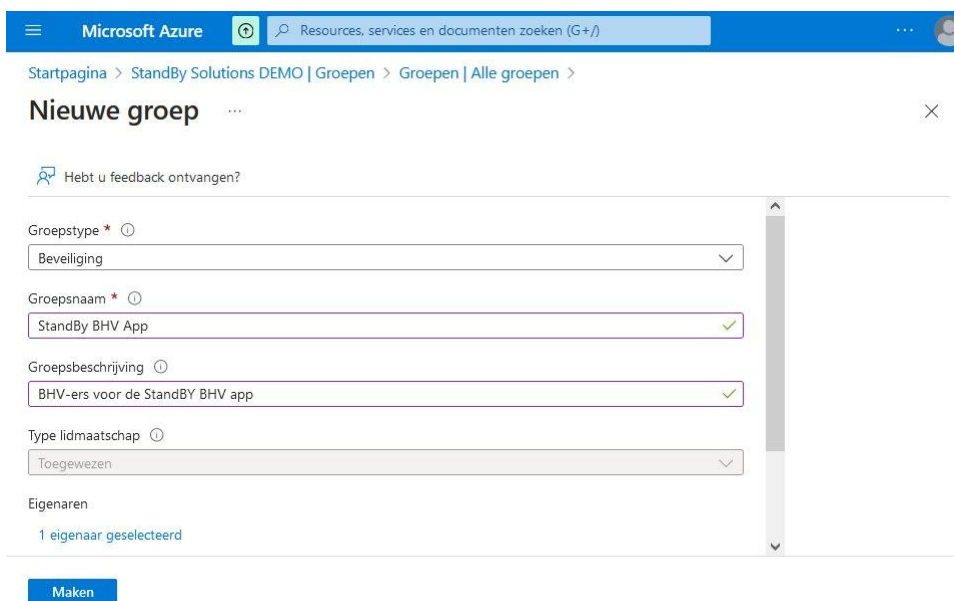
Zoekmodus: Bevat

1 groep gevonden

Naam ↑	Object-id	Groepstype
SB StandBy BHV	0894a7b9-eb21-4520-84f7-d7b4745c62fe	Beveiliging

Create a new group or select an existing group containing Emergency Response Officers (BHV personnel) to synchronize with StandBy.

1. In Microsoft Azure, navigate to: Home > Azure Active Directory > Groups > All groups.
2. Select one of the following options:
 - o **Existing group:** Copy the *Object ID* from the table for the BHV group and save it.
 - o **New group:** Click New group, define the group details (optionally add owners/members directly), and click Create. Then copy the *Object ID*.



Startpagina > StandBy Solutions DEMO | Groepen > Groepen | Alle groepen >

Nieuwe groep

Hebt u feedback ontvangen?

Groepstype * ①
Beveiliging

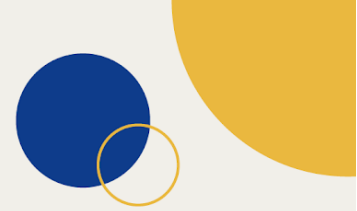
Groepsnaam * ①
StandBy BHV App

Groepsbeschrijving ①
BHV-ers voor de StandBY BHV app

Type lidmaatschap ①
Toegewezen

Eigenaren
1 eigenaar geselecteerd

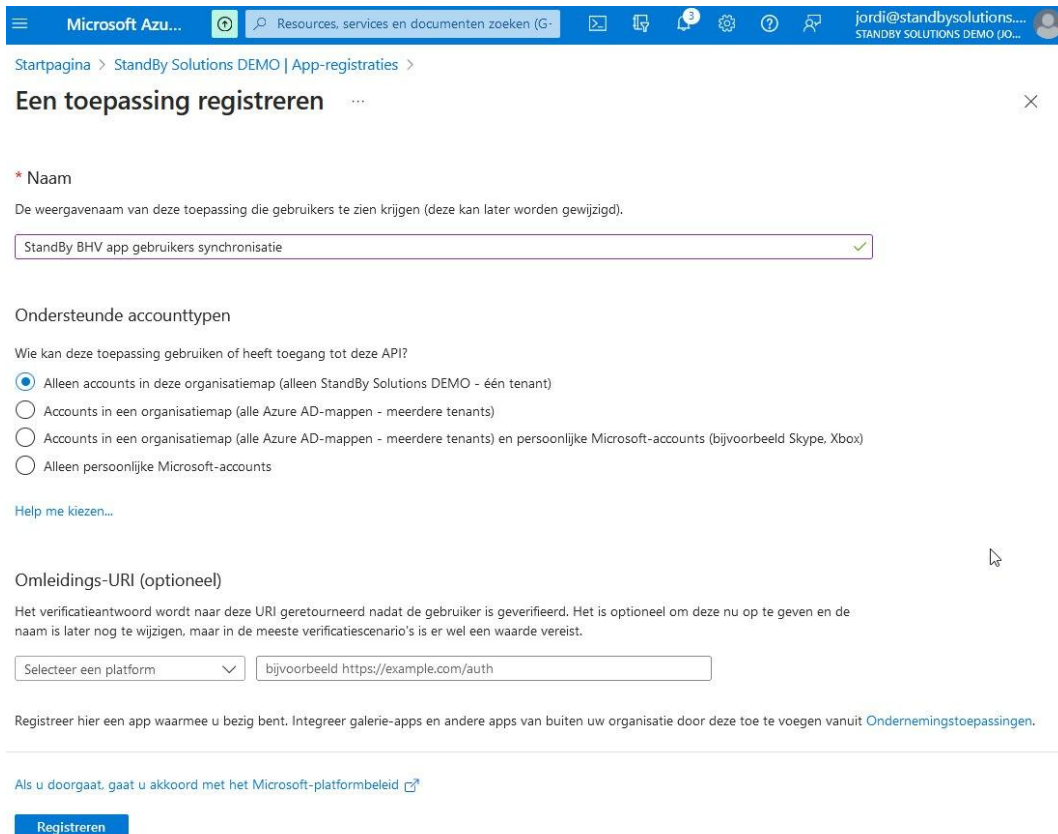
Maken



Step 2: Create App-registration

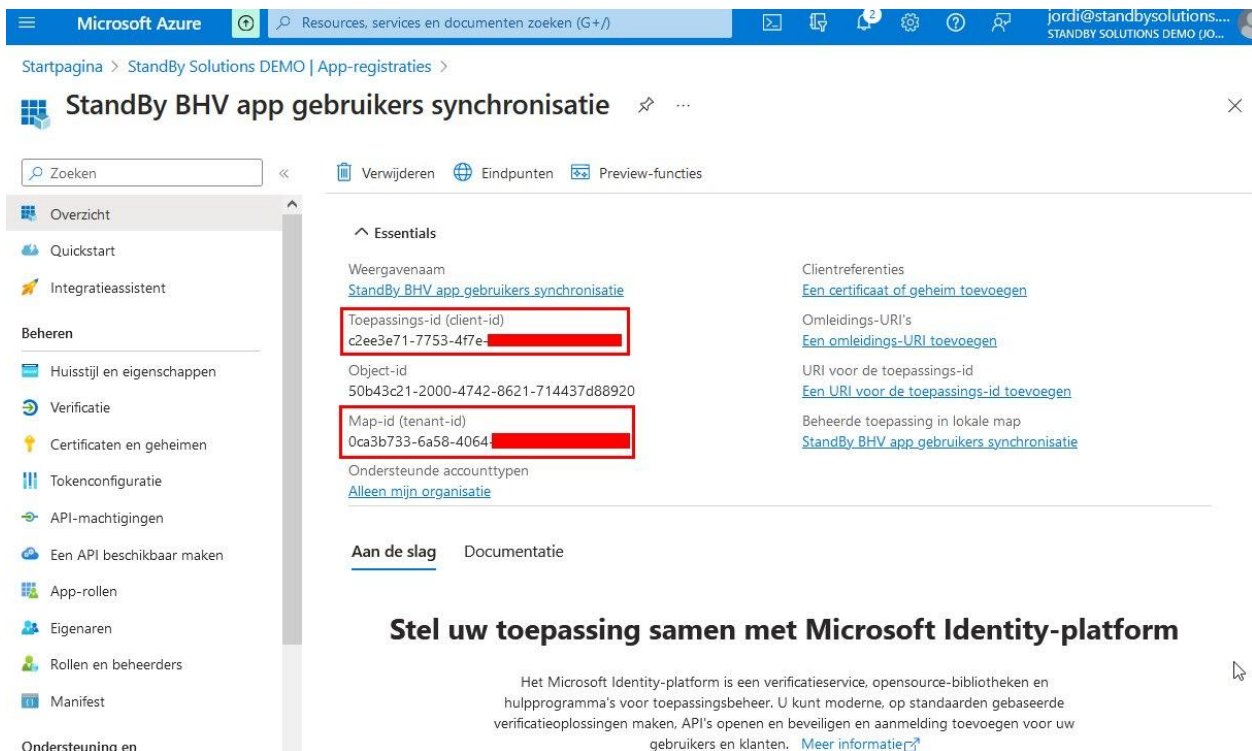
Create a new application and grant the necessary permissions to provide StandBy with access to user data.

1. Navigate to: Home > Azure Active Directory > App registrations.
2. Click New registration at the top left.



The screenshot shows the 'Een toepassing registreren' (Register an application) page in the Microsoft Azure portal. The breadcrumb trail is 'Startpagina > StandBy Solutions DEMO | App-registraties >'. The page title is 'Een toepassing registreren'. Below the title, there is a section for '* Naam' (Name) with a description: 'De weergavenaam van deze toepassing die gebruikers te zien krijgen (deze kan later worden gewijzigd)'. The input field contains 'StandBy BHV app gebruikers synchronisatie'. Below this is a section for 'Ondersteunde accounttypen' (Supported account types) with the question 'Wie kan deze toepassing gebruiken of heeft toegang tot deze API?'. There are four radio button options: 'Alleen accounts in deze organisatiemap (alleen StandBy Solutions DEMO - één tenant)' (selected), 'Accounts in een organisatiemap (alle Azure AD-mappen - meerdere tenants)', 'Accounts in een organisatiemap (alle Azure AD-mappen - meerdere tenants) en persoonlijke Microsoft-accounts (bijvoorbeeld Skype, Xbox)', and 'Alleen persoonlijke Microsoft-accounts'. Below this is a section for 'Omleidings-URI (optioneel)' (Optional redirect URI) with a description: 'Het verificatieantwoord wordt naar deze URI geretourneerd nadat de gebruiker is geverifieerd. Het is optioneel om deze nu op te geven en de naam is later nog te wijzigen, maar in de meeste verificatiescenario's is er wel een waarde vereist.' There is a dropdown menu for 'Selecteer een platform' and an input field for the URI containing 'bijvoorbeeld https://example.com/auth'. At the bottom, there is a note: 'Registreer hier een app waarmee u bezig bent. Integreer galerie-apps en andere apps van buiten uw organisatie door deze toe te voegen vanuit Ondernemingstoepassingen.' and a button labeled 'Registreren'.

3. Fill in the details:
 - o **Name:** Enter a recognizable name (e.g., 'StandBy BHV app user synchronization').
 - o **Supported account types:** Select *Accounts in this organizational directory only (Single tenant)*. (If managing multiple tenants, ensure the correct tenant containing the BHV group is selected).
 - o **Redirect URI:** Can be left blank.
4. Click Register.
5. Copy and save the following values:
 - o Application (client) ID
 - o Object ID (this is the App ID)
 - o Directory (tenant) ID

StandBy BHV app gebruikers synchronisatie

Essentials

Weergavenaam: [StandBy BHV app gebruikers synchronisatie](#)

Toepassings-id (client-id): **c2ee3e71-7753-4f7e-...**

Object-id: 50b43c21-2000-4742-8621-714437d88920

Map-id (tenant-id): **0ca3b733-6a58-4064-...**

Ondersteunde accounttypen: [Alleen mijn organisatie](#)

Clientreferenties: [Een certificaat of geheim toevoegen](#)

Omleidings-URI's: [Een omleidings-URI toevoegen](#)

URI voor de toepassings-id: [Een URI voor de toepassings-id toevoegen](#)

Beheerde toepassing in lokale map: [StandBy BHV app gebruikers synchronisatie](#)

Stel uw toepassing samen met Microsoft Identity-platform

Het Microsoft Identity-platform is een verificatieservice, opensource-bibliotheken en hulpprogramma's voor toepassingsbeheer. U kunt moderne, op standaarden gebaseerde verificatieoplossingen maken, API's openen en beveiligen en aanmelding toevoegen voor uw gebruikers en klanten. [Meer informatie](#)

Stap 3: Add Permissions & Grant Admin Consent

To ensure StandBy can read the correct group and user data, specific Microsoft Graph API permissions are required.



API-machtigingen aanvragen

Een API selecteren

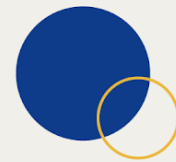
Microsoft-API's API's die in mijn organisatie worden gebruikt Mijn API's

Veelgebruikte Microsoft-API's

Microsoft Graph

Profiteer van de enorme hoeveelheid gegevens in Office 365, Enterprise Mobility + Security en Windows 10. Open Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner en meer via één eindpunt.

1. From the overview page of the newly created application, navigate to API permissions.



Geconfigureerde machtigingen

Toepassingen zijn gemachtigd om API's aan te roepen wanneer ze zijn gemachtigd door gebruikers/beheerders als onderdeel van het goedkeuringsproces. De lijst met geconfigureerde machtigingen moet alle machtigingen bevatten die nodig zijn voor de toepassing. [Meer informatie over machtigingen en toestemming](#)

+ Een machtiging toevoegen

☒ Beheerderstoestemming verlenen voor StandBy Solutions DEMO

Naam API/machtigingen	Type	Beschrijving	Beheerderstoestemming verlenen voor StandBy Solutions DEMO	Status
▼ Microsoft Graph (5)				
Directory.Read.All	Toepassing	Read directory data	Ja	⚠ Niet toegekend voor Sta... ***
Group.Read.All	Toepassing	Read all groups	Ja	⚠ Niet toegekend voor Sta... ***
GroupMember.Read.All	Toepassing	Read all group memberships	Ja	⚠ Niet toegekend voor Sta... ***
User.Read	Gedelegeerd	Aanmelden en gebruikersprofiel lezen	Nee	***
User.Read.All	Toepassing	Read all users' full profiles	Ja	⚠ Niet toegekend voor Sta... ***

- Click Add a permission and select Microsoft Graph API.
- Select Application permissions and add the following permissions:
 - Directory.Read.All
 - Group.Read.All
 - GroupMember.Read.All
 - User.Read (*mogelijk standaard al toegevoegd*)
 - User.Read.All
- Click the button Grant admin consent for [tenant] and confirm the action.

[Bevestiging voor beheerderstoestemming verlenen](#)

StandBy BHV app gebruikers synchronisatie | API-machtigingen

»  Vernieuwen |  Hebt u feedback ontvangen?

Bevestiging voor beheerderstoestemming verlenen.

Wilt u toestemming verlenen voor de aangevraagde machtigingen voor alle accounts in StandBy Solutions DEMO? Met deze actie worden bestaande beheerderstoestemmingrecords van de toepassing bijgewerkt zodat deze overeenkomen met de onderstaande gegevens.

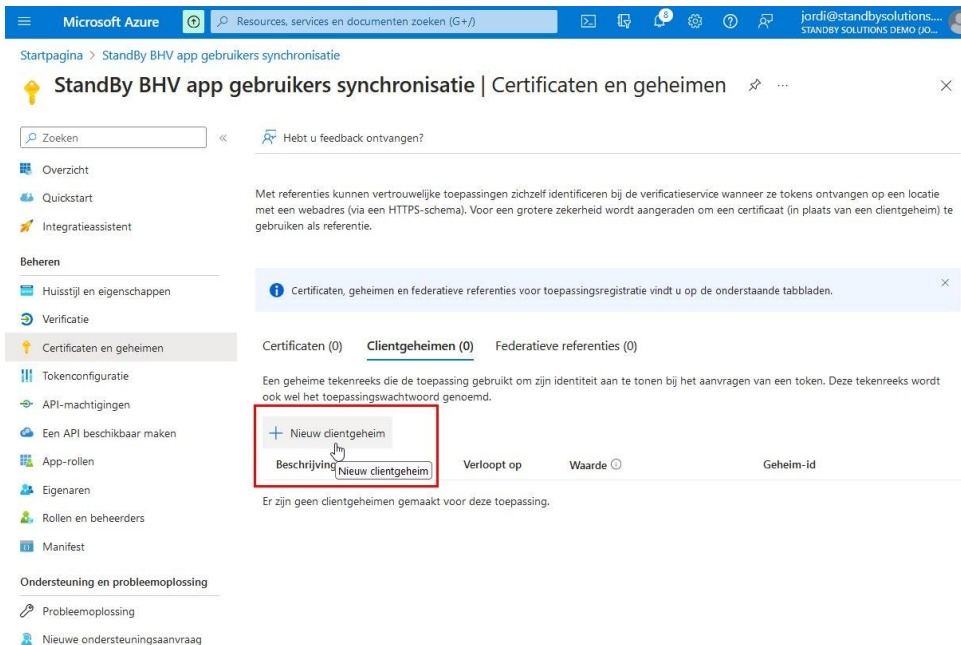
- Verification: Once granted, a green checkmark will appear next to all permissions in the *Status* column ('Granted for [tenant]').



Stap 4: Create Client Secret

Create a set of 'client secrets' to grant StandBy authorized access to the application.

1. Navigate to: Certificates & secrets > 'Client secrets' tab.
2. Click New client secret



The screenshot shows the Azure portal interface. The left sidebar contains navigation links for 'Overzicht', 'Quickstart', 'Integratieassistent', 'Beheren', 'Huisstijl en eigenschappen', 'Verificatie', 'Certificaten en geheimen' (selected), 'Tokenconfiguratie', 'API-machtigingen', 'Een API beschikbaar maken', 'App-rollen', 'Eigenaren', 'Rollen en beheerders', 'Manifest', 'Ondersteuning en probleemoplossing', 'Probleemoplossing', and 'Nieuwe ondersteuningsaanvraag'. The main content area is titled 'StandBy BHV app gebruikers synchronisatie | Certificaten en geheimen'. It shows a tab for 'Clientgeheimen (0)'. A red box highlights the '+ Nieuw clientgeheim' button. Below the button, there is a table with columns 'Beschrijving', 'Verloopt op', 'Waarde', and 'Geheim-id'. A message at the bottom states: 'Er zijn geen clientgeheimen gemaakt voor deze toepassing.'

3. Enter a description (e.g., 'StandBy BHV App') and set the expiration duration to 730 days (24 months).



The screenshot shows the 'Een clientgeheim toevoegen' form. It has two input fields: 'Beschrijving' with the value 'StandBy BHV App' and 'Verloopt op' with a dropdown menu set to '730 dagen (24 maanden)'. At the bottom, there are two buttons: 'Toevoegen' and 'Annuleren'.

4. Click Add. Immediately copy the Value of the new client secret.

ATTENTION: This value is visible only at the moment of creation. Once you leave the page, the full value can no longer be viewed or recovered.



Certificaten (0) **Clientgeheimen (1)** Federatieve referenties (0)

Een geheime tekenreeks die de toepassing gebruikt om zijn identiteit aan te tonen bij het aanvragen van een token. Deze tekenreeks wordt ook wel het toepassingswachtwoord genoemd.

+ Nieuw clientgeheim

Beschrijving	Verloopt op	Waarde ⓘ	Naar het klembord kopiëren d
StandBy BHV App	1-5-2025	638 [redacted] CR0sj.P ... f1601710-cc28-4206-b3d0-c4f38ec68890	 

Step 5: Execute Admin Consent URL

Grant final approval via the constructed Admin Consent URL.

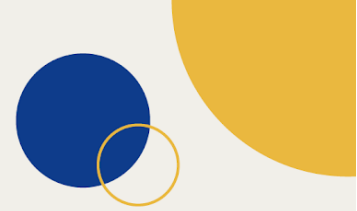
1. Construct the URL using your specific parameters:

https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id={client-id}

2. Open this URL in a browser and grant consent. (Any messages displayed immediately after granting consent can be safely ignored).

How does Synchronisation work in practise?

- **Nightly Processing:** Synchronization is automatically executed daily between 00:00 and 06:00 during the night.
- **Automatic Invitations:** New users added to the Azure group are created with the 'BHV' role and immediately receive an email with instructions on downloading the app.
- **Data Security:** Removed users receive a confirmation email stating that their account and associated data have been permanently deleted from StandBy.



Next Steps

Providing data

Send the collected information (Tenant ID, Client ID/Secret, Group ID) securely to your designated contact person at StandBy Solutions.

- **Contact Person:** Include the name and email address of a designated contact person or department responsible for managing potential credential issues (such as an expiring secret).

Security Notice: Treat this dataset with the same confidentiality as an administrative password; it grants direct access to user data.

Testing

StandBy Solutions will test the connection via the Microsoft Graph API and communicate the results or any error messages directly back to you.

Synchronisation

The activation date and initial (manual) synchronization will be scheduled in consultation. Please keep the following points in mind prior to activation:

- **Key Renewal:** Well before the expiration date (within 2 years, ideally 30-60 days prior), generate new keys in Azure and email them to support@standbysolutions.nl.
- **Existing Accounts:** Critical or shared accounts must be flagged in StandBy prior to activation to prevent them from being automatically deleted during synchronization.
- **Communication & IT:** Ensure that Emergency Response Officers (BHV personnel) are notified about the incoming activation email and that your IT department has implemented the required 'Technical Requirements' to guarantee email deliverability.