

**Document Classificatie: Internal use**

Versie: **1.1** / Status: **Published**

Gepubliceerd op: 8-2-2022

Documentnummer: 84272

Paginnummer: 1 van 21

Handleiding: Single Sign-on



## Handleiding Inregelen Single Sign On



Centix B.V

Tasveld 1B

3417 XS MONTFOORT

Tel: +31 348-471040

Fax: +31 348-475036

Email: [support@centix.com](mailto:support@centix.com)

Website: [www.centix.com](http://www.centix.com)

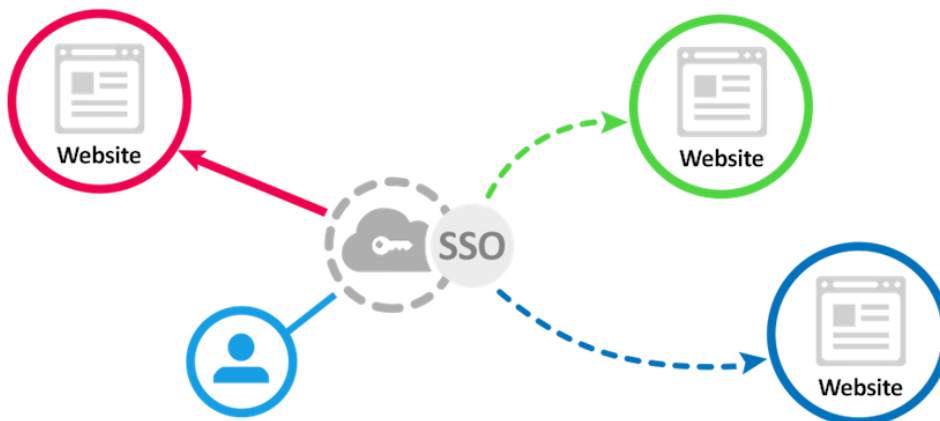


## Inhoud

1. Introductie .....	3
2. Inregelen Single Sign On .....	4
2.1. Inregelen Centix applicatie bij identity provider .....	4
2.1.1 Nieuwe applicatie toevoegen in OKTA .....	4
2.1.2 Nieuwe applicatie toevoegen in Azure Active Directory .....	7
2.2 Inregelen identity provider in Centix .....	10
2.2.1 Relatie uitwisselen .....	11
2.2.2 Beveiligingsgroep instellen .....	12
2.2.3 Aanmaken en migreren bestaande gebruikers .....	12
2.2.4 Foutpagina's instellen .....	13
2.2.5 Gegevensuitwisseling(provisioning) .....	13
2.3 Details provider .....	14
2.3.1 Gekoppelde gebruikers .....	14
2.3.2 Overzicht identity providers .....	15
3. Gebruikers markeren voor Single Sign On .....	15
4. Inloggen met identity provider .....	16
4.1 Inloggen met nieuwe gebruiker .....	16
4.2 Inloggen met bestaande Centix gebruiker (migratie) .....	17
5. Verwijderen Single Sign on van een gebruiker .....	18
5.1 Verwijderen van Single Sign On .....	18
5.2 Verwijderen van Single Sign On van gemigreerde gebruiker .....	18
5.3 Verwijderen van Single Sign On van niet gemigreerde (nieuwe) gebruiker .....	18
6. Foutmeldingen .....	20
7. Bijzonderheden .....	21
7.1 Inloggen via identity provider (Okta) .....	21

## 1. Introductie

Single Sign On is ontwikkeld op basis van de behoefte om met accounts binnen de organisatie in te kunnen loggen in Centix. Een dergelijke vergelijking is een Google of Facebookaccount welke gebruikt wordt om bij verschillende andere applicaties in te kunnen loggen, u gebruikt echter maar één inlogaccount, waardoor het niet nodig is om opnieuw inloggegevens aan te maken.



Naast het gemak om met één account in te kunnen loggen kan Single Sign On ook gefaciliteerd worden om alleen medewerkers met bepaalde bevoegdheden te laten inloggen in Centix. Hiervoor is het gebruik van een **identity provider** noodzakelijk.

Een identity provider verzorgt het registreren van medewerkers van de organisatie waarna er rechten per applicatie ingesteld kunnen worden. Door de medewerkers aan te maken in een programma als **Okta** of **Microsoft Azure identity** is het mogelijk om de medewerkers toegang te geven tot bepaalde applicaties.

Centix B.V ondersteunt alleen identity providers met het type OpenID Connect (Niet te verwarren met OpenID). OpenID Connect ondersteunt ook het inloggen met Single Sign On op mobiele devices.

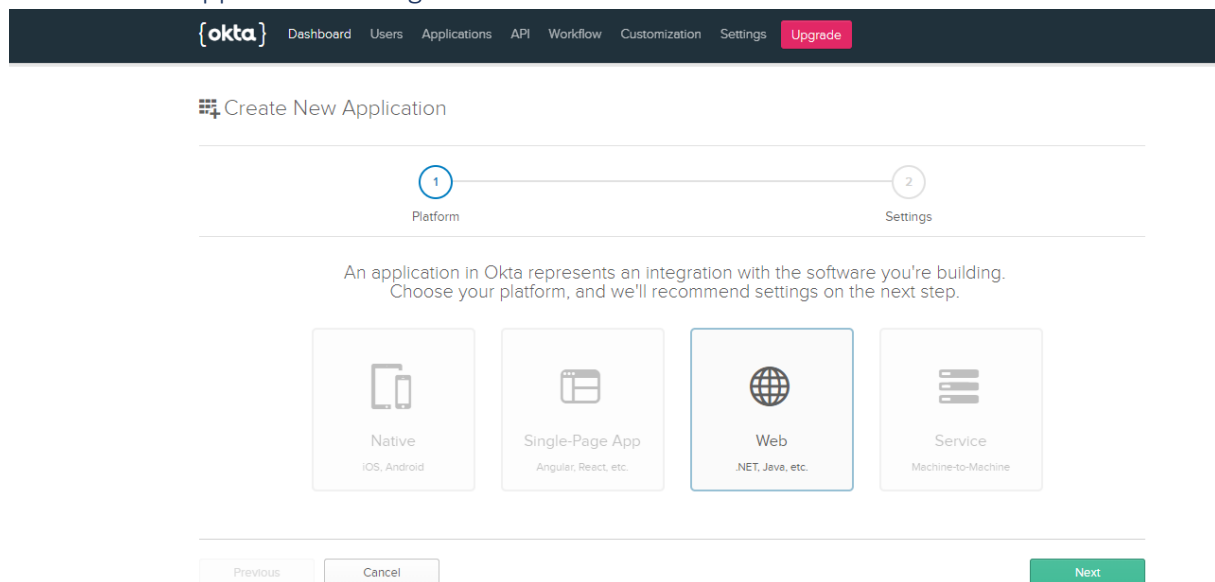
## 2. Inregelen Single Sign On

Om gebruik te kunnen maken van Single Sign On is het belangrijk dat de identity provider met Centix kan communiceren. Het instellen van een identity provider dient zowel in Centix als bij de identity provider zelf gedaan te worden.

### 2.1. Inregelen Centix applicatie bij identity provider

Om gebruik te kunnen maken van Single Sign on is het nodig om tussen Centix en de **identity provider** gegevens uit te wisselen. Door in het systeem van de **identity provider** een “**vertrouwde applicatie**” toe te voegen weet de **identity provider** dat deze applicatie gebruikt mag worden door de medewerkers binnen de organisatie. Centix dient daarom eerst geregistreerd worden bij de desbetreffende **identity provider**.

#### 2.1.1 Nieuwe applicatie toevoegen in OKTA



Na het registreren van een vertrouwde applicatie wordt er vaak gevraagd om een aantal gegevens. De volgende gegevens worden door de **identity provider** gevraagd:

- **Naam:** De naam van de desbetreffende applicatie
- **Domein:** Het (sub)domein waar de applicatie op draait
- **Redirect URI:** De locatie binnen Centix waar de gebruiker naartoe wordt gestuurd als hij is ingelogd bij de identity provider. Vb. <https://mijnbedrijf.com/mvc/oidc/authorize>
- **Grant type:** Centix ondersteunt alleen de **Authorization code**.

Create New Application



We use these default values for our web app samples. Edit them to fit your needs. All these settings can be changed at any time.

APPLICATION SETTINGS

Name: Centix

Base URIs (Optional): https://centix.com

Login redirect URIs: https://centix.com/mvc/oidc/authorize

Logout redirect URIs: + Add URI

Group assignments (Optional): Everyone

Grant type allowed:

- Client acting on behalf of itself:  Client Credentials
- Client acting on behalf of a user:  Authorization Code,  Refresh Token,  Implicit (Hybrid)

Quick Start Guides

- Node.js
- Java
- .NET
- PHP

Door een **group assignment** toe te voegen aan de applicatie is het mogelijk bepaalde afdelingen of medewerkers toegang te geven tot de applicatie middels Single Sign On. Wanneer de gebruiker niet tot de bepaalde groep hoort krijgt deze de melding dat de medewerker niet genoeg rechten heeft om in te mogen loggen.

Na het opslaan van de vertrouwde applicatie bij een identity provider wordt er een uniek ID en een wachtwoord voor de applicatie aangemaakt. Deze gegevens heeft Centix nodig om gebruik te kunnen

**Document Classificatie: Internal use**

Versie: **1.1** / Status: **Published**

Gepubliceerd op: 8-2-2022

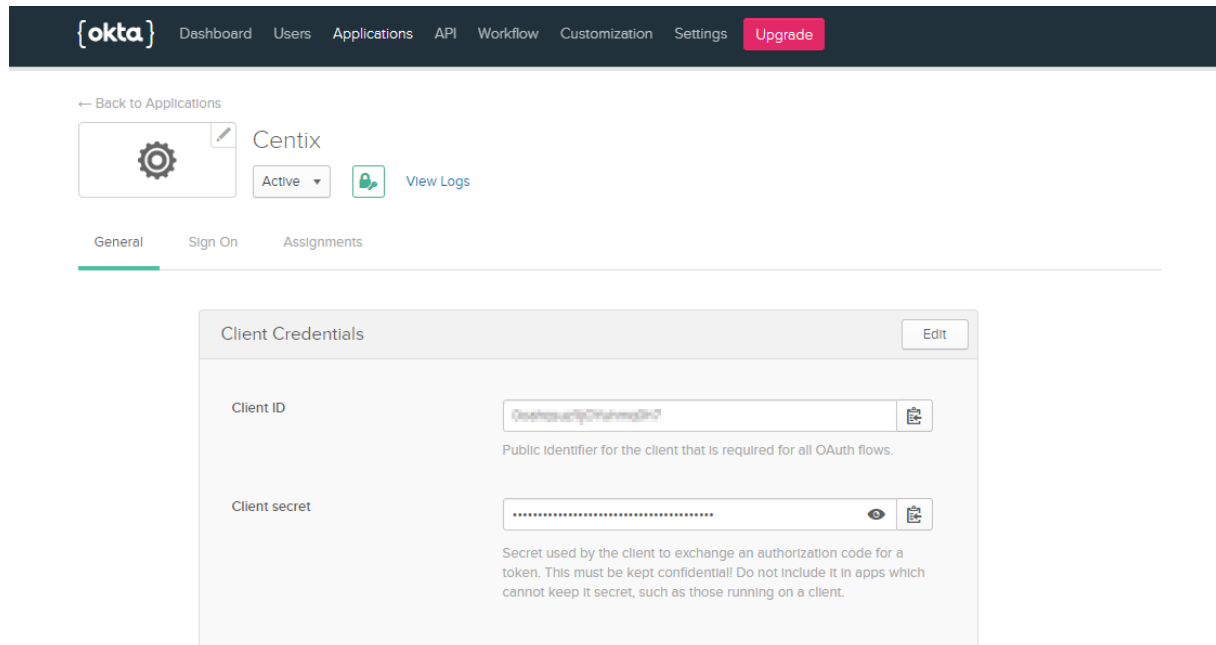
Documentnummer: 84272

Paginnummer: 6 van 21

Handleiding: Single Sign-on



maken van de identity provider. Het ID en wachtwoord zijn niet voor publicatie en dienen beveiligd te zijn.



Het inregelen van de vertrouwde applicaties is een taak voor de klant, het is belangrijk dat de juiste type **domain**, **redirect URI** en **het Grant type** worden ingevoerd. Deze worden als volgt ingevoerd:

**Domain:** het domein van de Centix configuratie. Vb. *https://mijnbedrijf.centix.com*

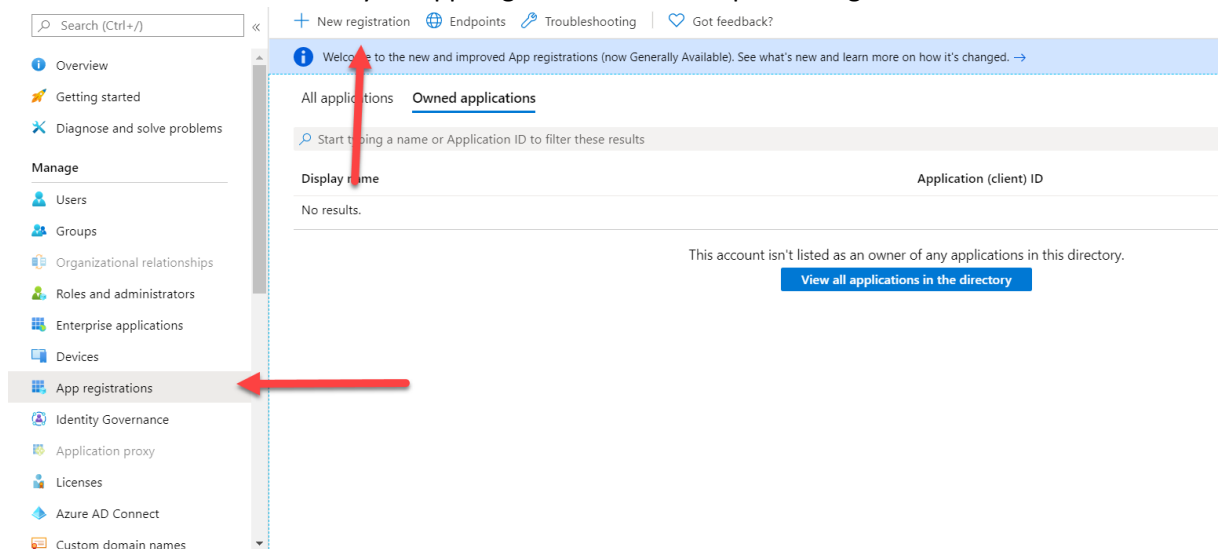
**Redirect URI:** domein + /mvc/oidc/authorize. Vb. *https://mijnbedrijf.centix.com/mvc/oidc/authorize*

**Grant type:** Is altijd ingesteld op Authorization code

Wanneer deze gegevens zijn ingesteld, zal de **identity provider** een sub domein van Centix toestaan om in te loggen met de gebruikers in zijn systeem. De volgende stap is de **identity provider** te registreren in Centix zodat Centix de **identity provider** 'vertrouwd'.

## 2.1.2 Nieuwe applicatie toevoegen in Azure Active Directory

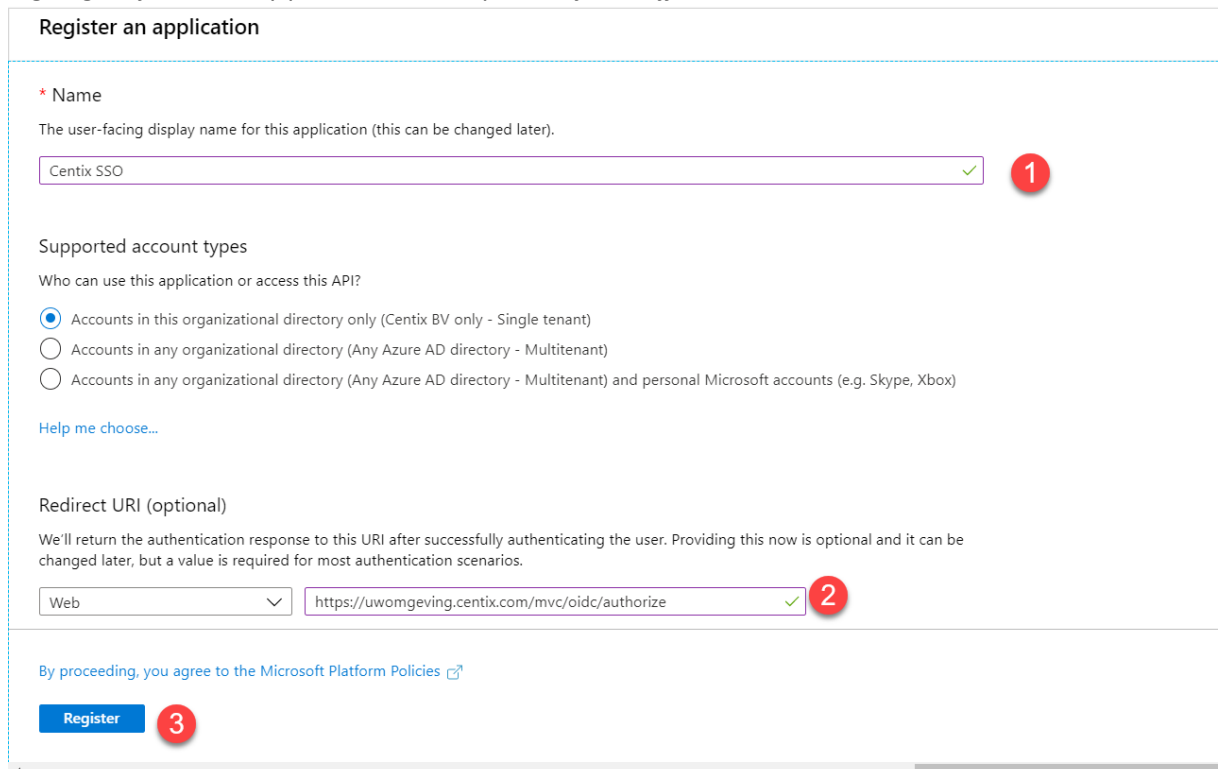
### 1. Ga naar Azure Active Directory → App Registrations en klik op 'New registration'



### 2. Voer de volgende gegevens in en klik op 'Register'

**Name:** De naam van de desbetreffende applicatie

**Redirect URI:** De locatie binnen Centix waar de gebruiker naartoe wordt gestuurd als hij is ingelogd bij de identity provider. Vb. <https://mijnbedrijf.centix.com/mvc/oidc/authorize>



**Register an application**

\* Name  
The user-facing display name for this application (this can be changed later).  
Centix SSO ✓ 1

Supported account types  
Who can use this application or access this API?  
 Accounts in this organizational directory only (Centix BV 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)  
[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 https://uwomgeving.centix.com/mvc/oidc/authorize ✓ 2

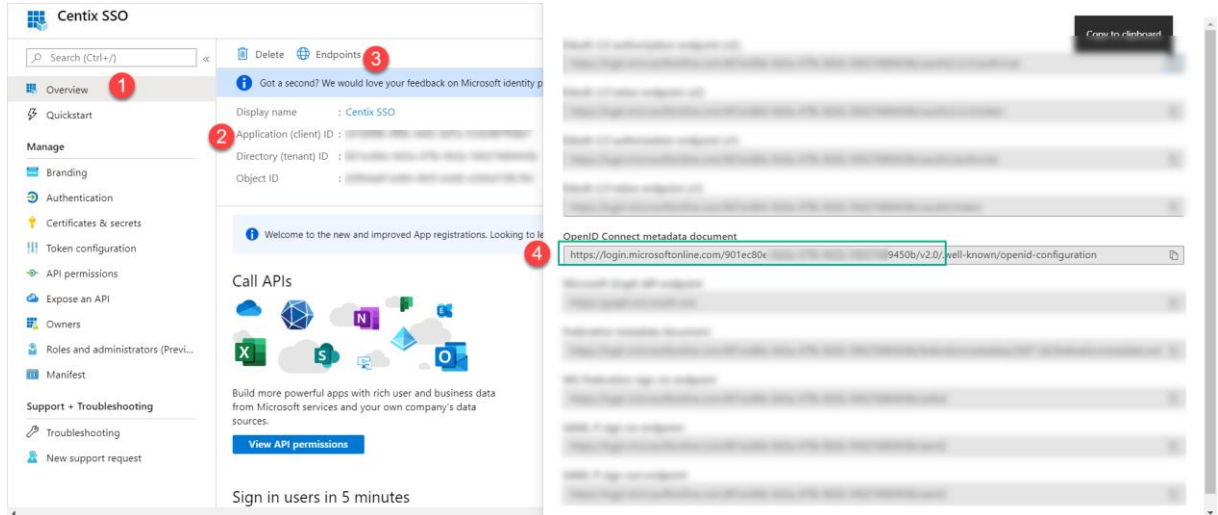
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register 3

3. Verzamel onderstaande informatie:

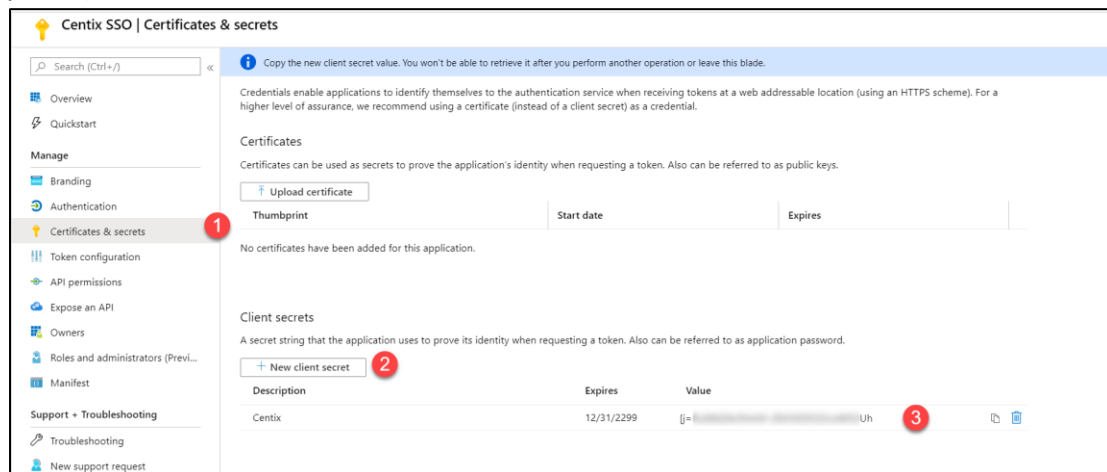
**Client ID:** Dit betreft Application (client) ID (Zie 2)

**Autorisatie Server URL:** Dit betreft het eerste deel van het OpenID endpoint (zie 3 en 4 → groene markering) Vb. <https://login.microsoftonline.com/{TenantID}/v2.0>



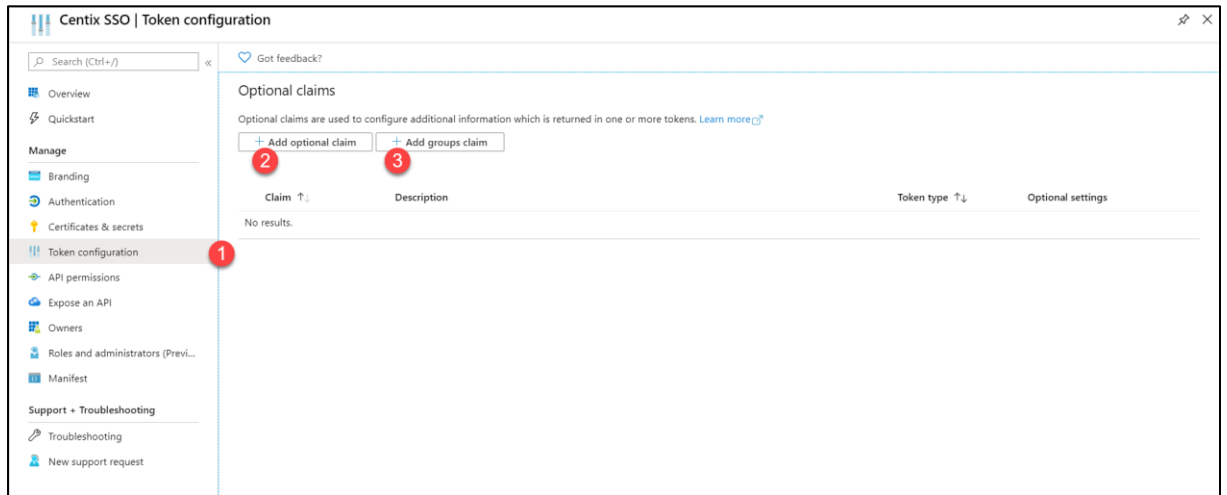
4. Maak een Client Secret aan.

Ga naar Certificates & Secrets en klik op 'New client secret' en bewaar de **Client Secret** (zie punt 3).



5. Voeg indien nodig nog extra claims toe (optioneel)

Afhankelijk van de inrichting kan het nodig zijn om extra claims toe te voegen. Het kan hier bijvoorbeeld gaan om claims ten behoeve van relatiebeperkingen en/of beveiligingsrollen.



## 2.2 Inregelen identity provider in Centix

Nadat Centix als 'vertrouwde applicatie' is ingesteld bij de **identity provider** zijn de volgende gegevens gegenereerd:

**ClientID:** Het ID van Centix zodat de identity provider de Centix applicatie kan herkennen.

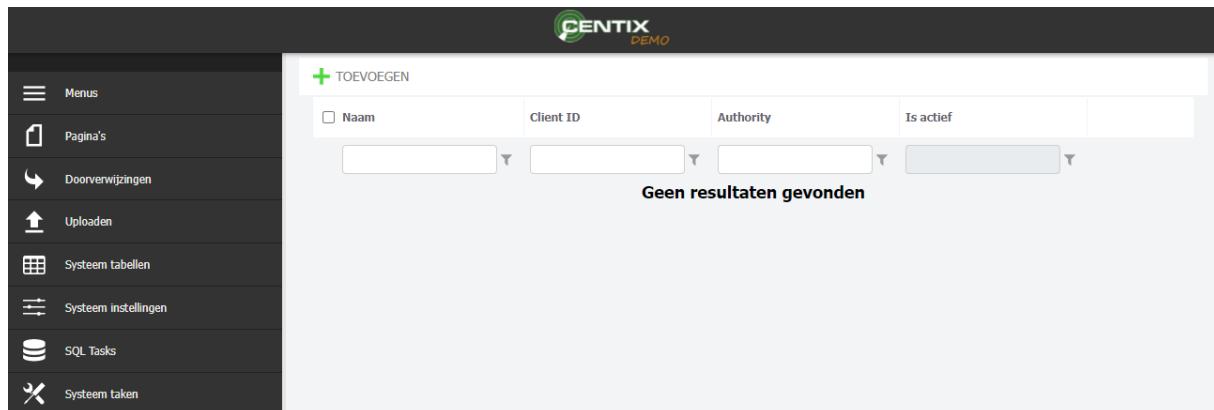
**Client secret:** Het wachtwoord van Centix

Zowel het ClientID als het Client secret wachtwoord zijn nodig om de **identity provider** in Centix in te regelen.

Via het admin panel → systeemtaken → identity providers kan de identity provider worden ingesteld. Om bij de juiste pagina te komen kan ook de volgende URL worden gebruikt:

<https://mijnbedrijf.centix.com/admin/systemtasks/identityproviders>

Op deze pagina kunnen de identity providers toegevoegd worden.



<input type="checkbox"/>	Naam	Client ID	Authority	Is actief
Geen resultaten gevonden				

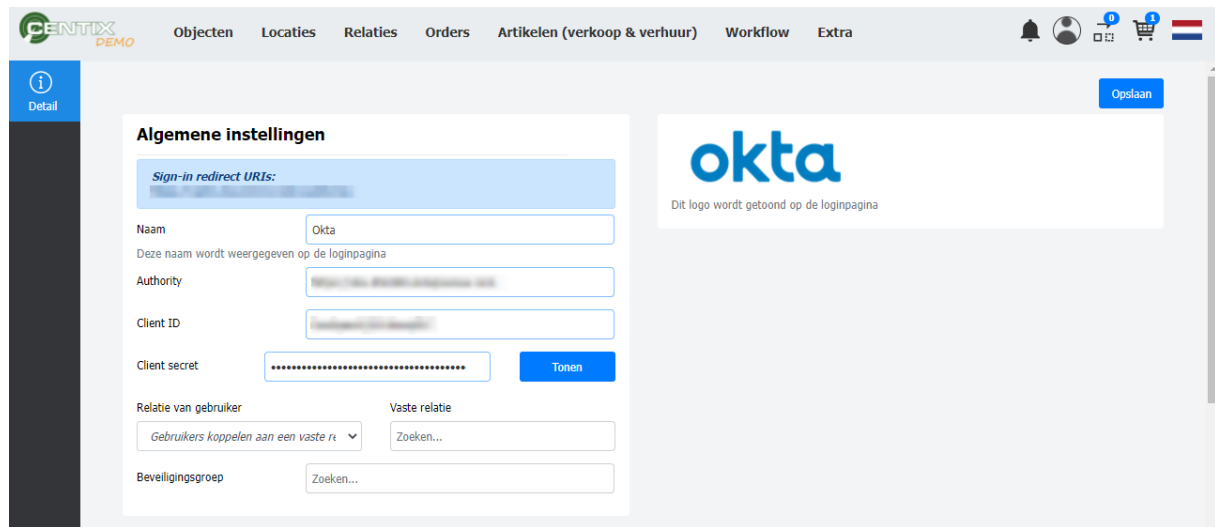
De volgende gegevens zijn benodigd om de **identity provider** in te voeren:

**Provider naam:** De naam van de **identity provider**, deze wordt alleen in het inlogscherf getoond.

**Authorisatie server url:** Deze wordt aangeleverd door de identity provider. Aan de hand van deze url worden alle benodigde gegevens om te koppelen tussen de provider en Centix opgevraagd.

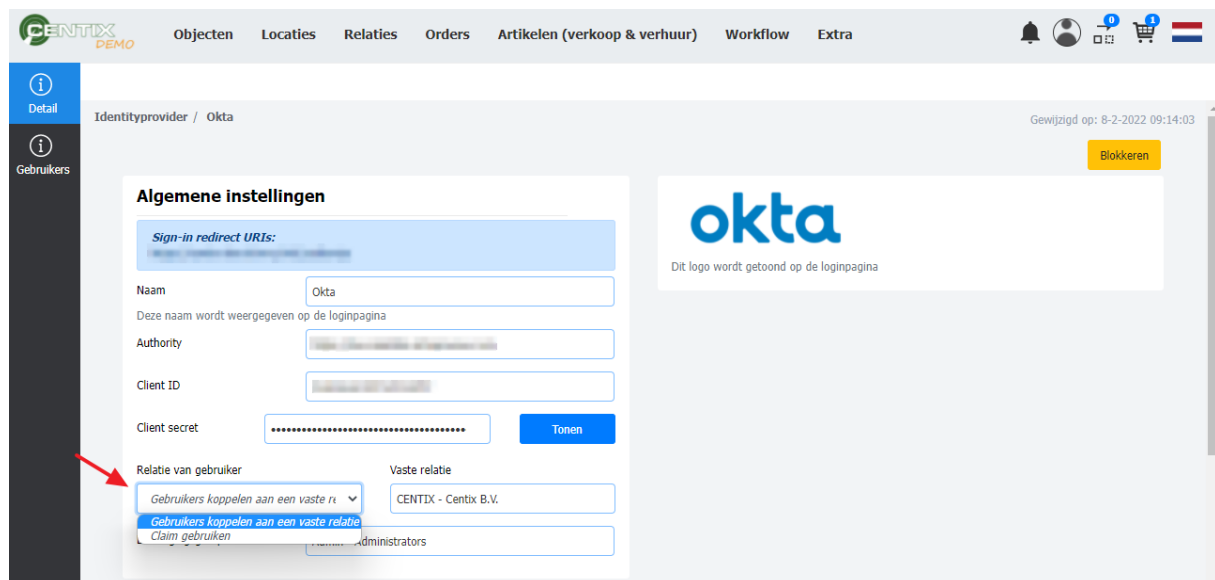
**ClientID en Client secret:** Deze gegevens worden automatisch gegenereerd door de **identity provider**

**Logo:** Het logo komt in het inlogscherf zodat gebruikers hierop kunnen klikken om in te loggen.



### 2.2.1 Relatie uitwisselen

Naast dat er in Centix persoonsgegevens nodig zijn om een gebruiker aan te maken, wordt een gebruiker ook altijd gekoppeld aan een relatie. Bij een aantal identity providers is het mogelijk om een organisatie te koppelen aan de gebruiker. Deze organisatie kan gekoppeld worden aan de gebruiker in Centix.

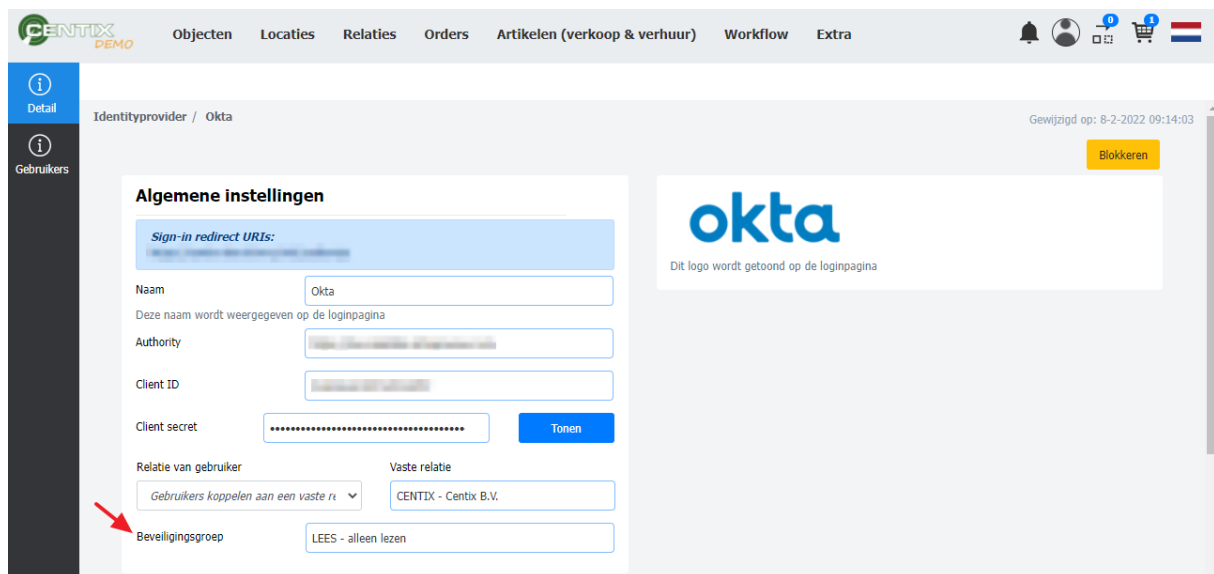


Als er geen mogelijkheid bestaat om de relatie vanuit de identity provider te gebruiken dan kan er een vaste relatie gebruikt worden om deze te koppelen aan de Single Sign On gebruiker. De standaard relatie kan later aangepast worden in het personendetail.

### 2.2.2 Beveiligingsgroep instellen

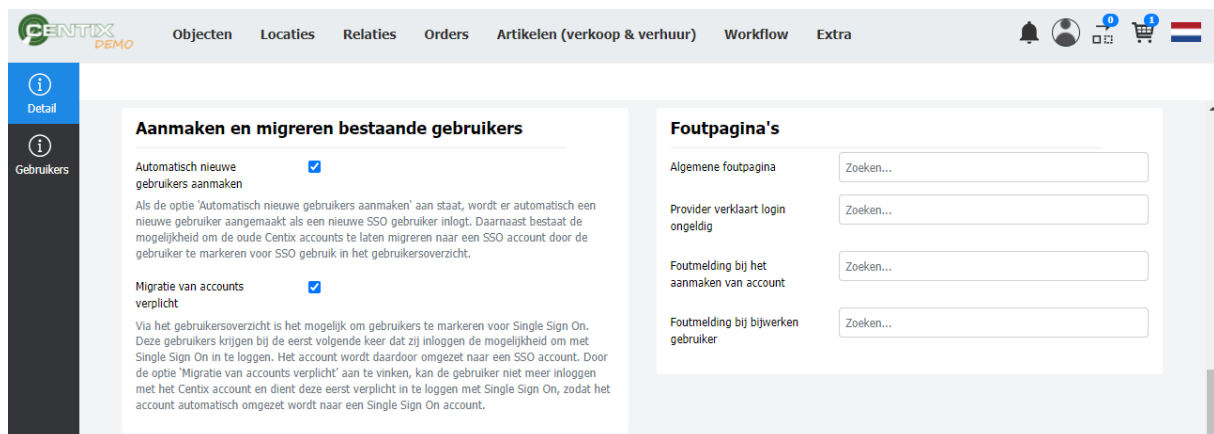
Naast een relatie wordt er altijd een systeemrol aan een gebruiker gekoppeld om te bepalen in welke schermen de gebruiker mag komen en wat hij mag doen in Centix.

Daarom dient een standaard gebruikersrol ingesteld te worden, deze wordt toegekend als een nieuwe Single Sign On gebruiker aangemaakt wordt. Het aanpassen van een beveiligingsrol kan achteraf in het personendetail.



### 2.2.3 Aanmaken en migreren bestaande gebruikers

In Centix wordt de mogelijkheid gegeven om het aanmaken van nieuwe gebruikers en de migratie van bestaande gebruikers in te stellen.



Hiervoor bestaan twee instellingen:

#### **Automatisch nieuwe gebruikers aanmaken**

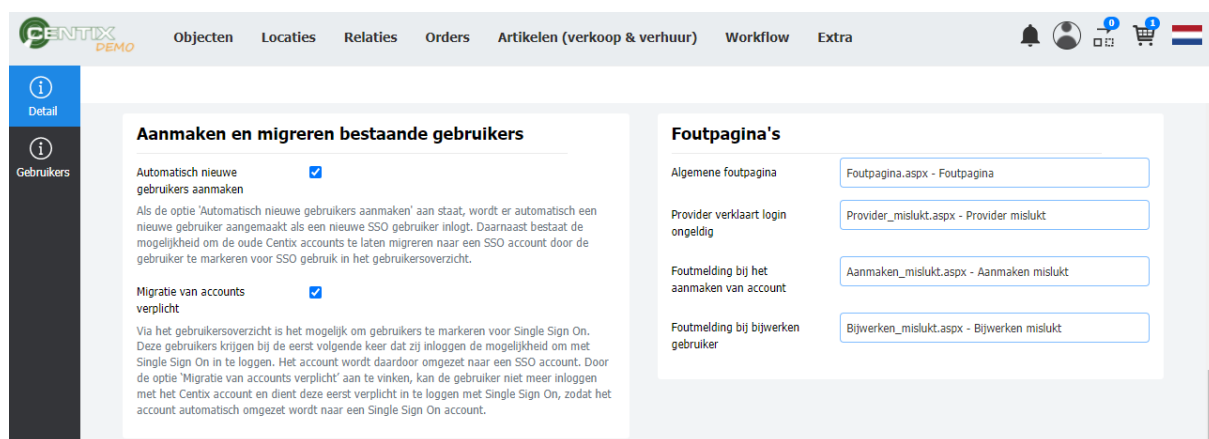
Bij het aanzetten van deze instelling worden automatisch nieuwe gebruikers aangemaakt wanneer deze nog niet in Centix bestaat en de gebruiker voor het eerst inlogt. Als deze instelling aanstaat kan de beheerder Centix gebruikers markeren zodat het Centix account wordt omgezet naar een Single Sign On account als de gebruiker inlogt. Hiervoor dient het account gemigreerd te worden.

### Migratie van accounts verplicht

Daarnaast bestaat de optie om het omzetten van een Centix account naar een Single Sign On account verplicht te maken, door de instelling 'migratie van accounts verplicht' aan te zetten kan een gebruiker niet meer inloggen zonder de migratie af te ronden. De gebruiker kan alleen in Centix inloggen door de migratie af te ronden en de wizard niet wegglikken.

### 2.2.4 Foutpagina's instellen

Om eenvoudiger fouten op te sporen en te bepalen waarom een gebruiker niet kan inloggen zijn een viertal foutpagina's in te stellen. Deze pagina's kunnen zelf aangemaakt worden via het admin panel → pagina's.



De volgende foutpagina's zijn in te stellen:

- Algemene foutpagina
- Provider verklaart login ongeldig
- Foutmelding bij het aanmaken van account
- Foutmelding bij bijwerken gebruiker

### 2.2.5 Gegevensuitwisseling(provisioning)

Als een medewerker voor het eerst inlogt wordt er in Centix automatisch een gebruiker aangemaakt. De gegevens, die gebruikt worden om een account aan te maken, worden vanuit de **identity provider** door Centix overgenomen.

In de sectie **gegevens koppelen** worden op basis van de gekozen identity provider de standaard velden(claims) gekozen die uit de **identity provider** worden gehaald, in Centix is een lijst beschikbaar gesteld met standaard velden die overgenomen kunnen worden om een gebruiker aan te maken. Deze velden komen overeen met de velden die de identity provider gebruikt om de gebruikers te registreren.

Voor elk benodigd gegeven biedt Centix een lijst met opties, dit is de lijst met de namen van de invoervelden die de **identity provider** over een gebruiker beschikbaar stelt. Afhankelijk van de identity provider zijn deze veldnamen standaard ingevuld. Wanneer dit niet zo is, kunnen deze gegevens door middel van de lijst worden ingesteld.

## Document Classificatie: Internal use

Versie: 1.1 / Status: Published

Gepubliceerd op: 8-2-2022

Documentnummer: 84272

Paginnummer: 14 van 21

Handleiding: Single Sign-on



Staat de juiste gegeven niet in de lijst? Door middel van de knop 'claim toevoegen' kan de gegeven worden toegevoegd aan de lijst.

Als de gegeven goed zijn ingesteld wordt bij het inloggen automatisch de persoonsgegevens van de gebruiker gebruikt om een persoon aan te maken in Centix.

A screenshot of the 'Gegevens koppelen' (Link data) form in the Centix system. The form is located in the 'Detail' view of the 'Gebruikers' (Users) section. It has a green 'Claim toevoegen' (Add claim) button at the top right. Below the button is a paragraph of text explaining that this form is used to link user data to a claim. The form contains five input fields, each with a dropdown menu: 'Voornaam' (First name) with 'name', 'Tussenvoegsel' (Middle name) with 'middle\_name', 'Achternaam' (Last name) with 'family\_name', 'E-mailadres' (Email address) with 'email', and 'Gebruikersnaam' (Username) with 'preferred\_username'. The left sidebar shows 'Detail' and 'Gebruikers' options.

## 2.3 Details provider

Na het instellen van de identity provider wordt deze automatisch op actief gezet zodat gebruikers voortaan met Single Sign On in kunnen loggen. De identity provider kan eventueel worden geblokkeerd door links bovenin op 'blokkeren' te klikken.

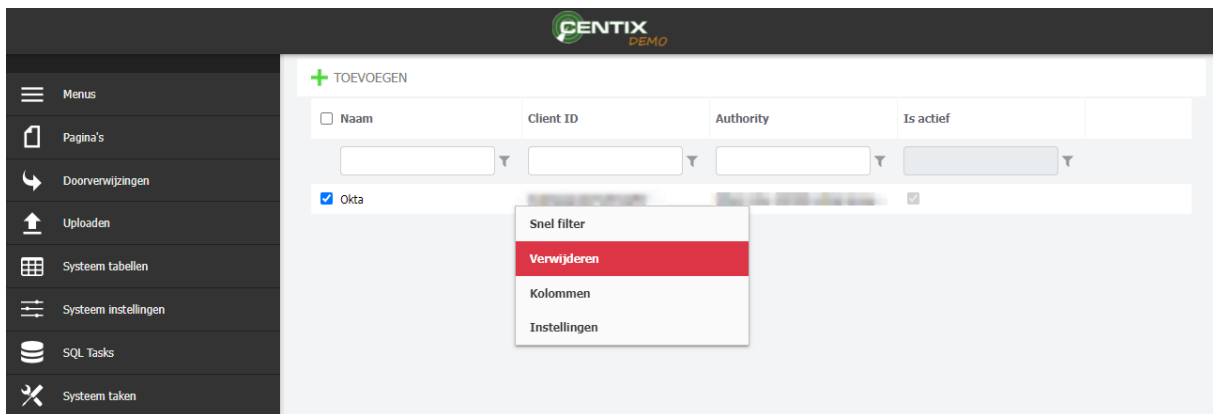
### 2.3.1 Gekoppelde gebruikers

In het detail van de identity provider is een tabblad beschikbaar gesteld om de gekoppelde gebruikers in te zien. Vanaf dit tabblad kunnen gebruikers ook ontkoppeld of verwijderd worden. Gebruikers welke gemarkeerd zijn voor het gebruik van SSO maar nog niet zijn gemigreerd worden niet in dit tabblad getoond.

A screenshot of the 'Identityprovider / Okta' details page in the Centix system. The page shows a list of linked users. At the top, there is a search bar with 'Actief' selected and a 'Zoeken...' (Search) button. Below the search bar is a table with columns: 'Gebruikersnaam' (Username), 'Laatste login' (Last login), 'Identity provider naam' (Identity provider name), 'Geblokkeerd' (Blocked), 'Systeembeveiliging groep' (System security group), 'Is beperkte gebruiker' (Is limited user), and 'Object beperking' (Object restriction). The table contains one row of data: 'SSO gebruiker', '8-2-2022', 'Okta', '否' (No), 'LEES', 'Is', and 'Eigenaar'. The left sidebar shows 'Detail' and 'Gebruikers' options. The top navigation bar includes 'Objecten', 'Locaties', 'Relaties', 'Orders', 'Artikelen (verkoop & verhuur)', 'Workflow', and 'Extra'. The top right corner shows a notification bell, a user profile icon, a shopping cart icon, and a flag icon.

### 2.3.2 Overzicht identity providers

In het overzicht identity providers is het mogelijk om de bestaande identity providers te bekijken toe te voegen of te verwijderen. Het verwijderen van een identity provider is alleen toegestaan als er geen gebruikers zijn gekoppeld of gemarkeerd zijn.

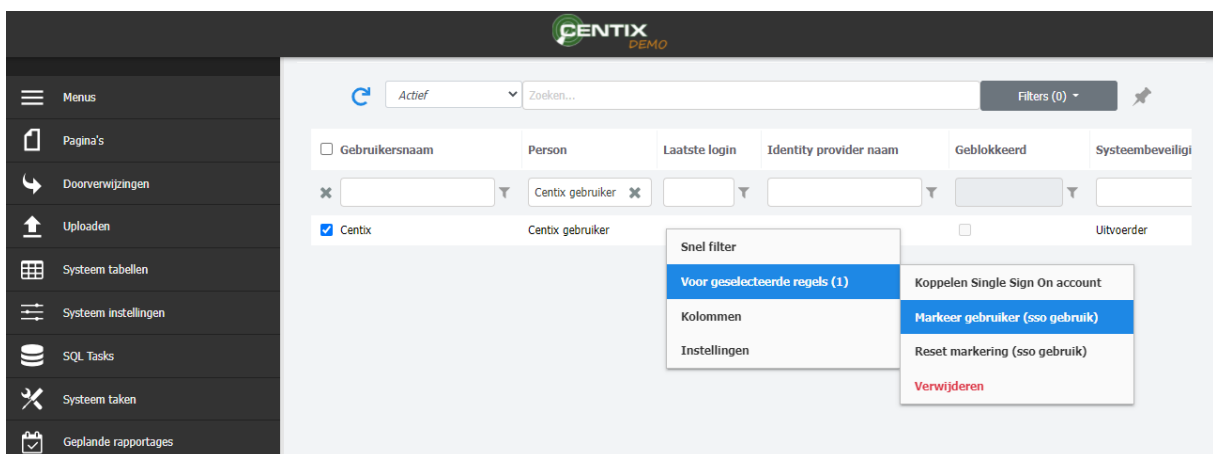


## 3. Gebruikers markeren voor Single Sign On

Het markeren van de gebruikers kan via het gebruikersoverzicht, te benaderen via het admin panel [\[?\]](#) systeemtaken gebruikers of via de volgende URL:

<https://mijnbedrijf.centix.com/admin/systemtasks/users>

Door de gebruiker aan te vinken → rechtermuisknop → voor geselecteerde regels → Markeer gebruiker (SSO gebruik) kan de gebruiker gemarkeerd worden om de volgende keer het account te laten migreren.



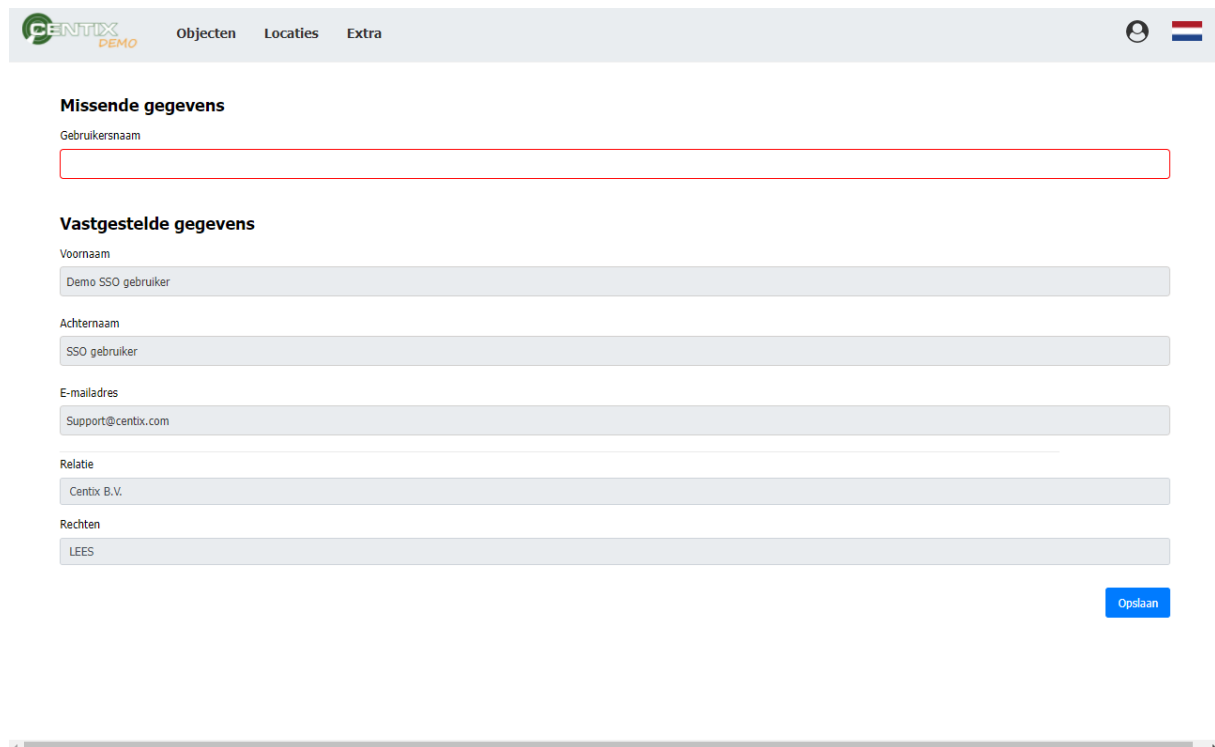
## 4. Inloggen met identity provider

Wanneer een identity provider aangemaakt is en deze is geactiveerd geeft Centix de mogelijkheid om in te loggen via deze identity provider. Wanneer hierop geklikt wordt, wordt de gebruiker doorgestuurd naar de juiste provider om in te loggen.

### 4.1 Inloggen met nieuwe gebruiker

Als Centix geen bestaande gebruiker in het systeem heeft staan en de identity provider het vinkje 'automatisch nieuwe gebruikers aanmaken' aan heeft staan dan wordt automatisch een nieuwe gebruiker aangemaakt. Als er een claim wordt gemist, zoals bijvoorbeeld de gebruikersnaam dan komt de gebruiker in een scherm om alsnog de gemiste claim in te kunnen vullen.

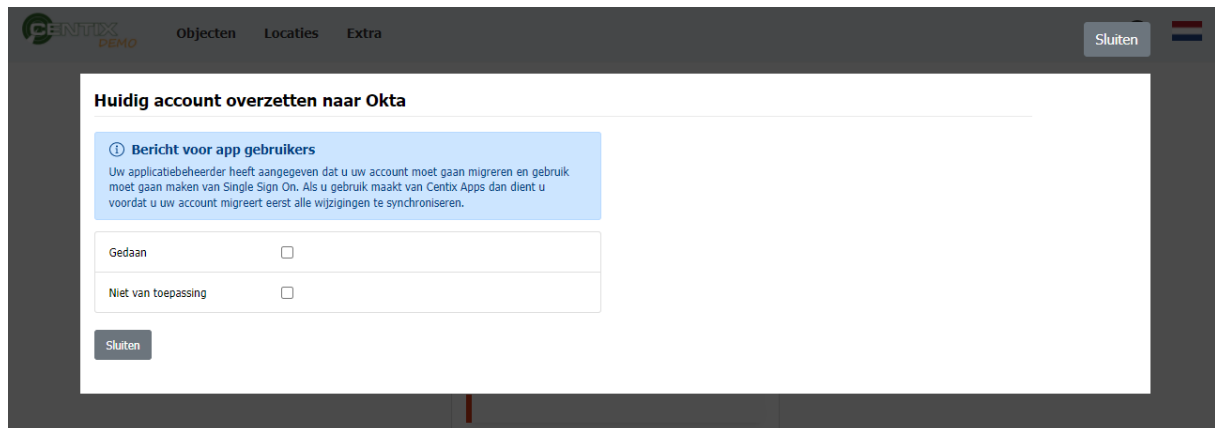
Nadat de missende claim ingevuld is wordt de gebruiker automatisch ingelogd.



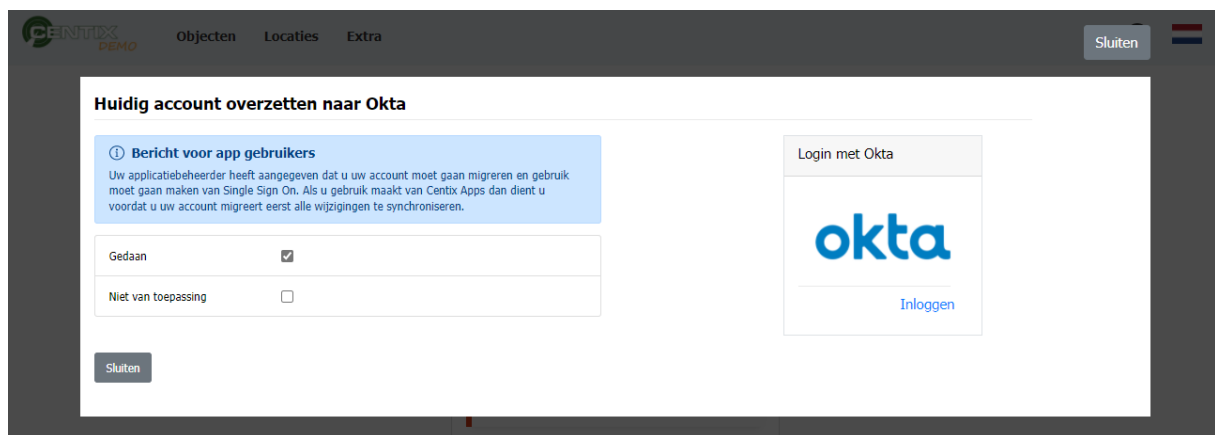
The screenshot shows a web interface for creating a user. At the top, there is a navigation bar with the Centix logo and the text 'CENTIX DEMO', 'Objecten', 'Locaties', and 'Extra'. On the right side of the navigation bar, there are icons for a user profile and the Dutch flag. Below the navigation bar, the form is titled 'Missende gegevens' (Missing data) and 'Vastgestelde gegevens' (Fixed data). The 'Missende gegevens' section contains a single text input field for 'Gebruikersnaam' (Username). The 'Vastgestelde gegevens' section contains several text input fields: 'Voornaam' (First name) with the value 'Demo SSO gebruiker', 'Achternaam' (Last name) with the value 'SSO gebruiker', 'E-mailadres' (Email address) with the value 'Support@centix.com', 'Relatie' (Relationship) with the value 'Centix B.V.', and 'Rechten' (Rights) with the value 'LEES'. A blue 'Opslaan' (Save) button is located at the bottom right of the form.

## 4.2 Inloggen met bestaande Centix gebruiker (migratie)

Logt een gebruiker in met het bestaande Centix account maar is deze gemarkeerd als Single Sign On account dan krijgt de gebruiker de optie om het account te migreren. De gebruiker krijgt eerst een waarschuwing, app gebruikers dienen eerst de app te hebben gesynchroniseerd.



Als de gebruiker aan heeft gegeven dat dit gedaan is, of niet van toepassing is komt het logo van de Identity provider tevoorschijn en kan men inloggen met de Identity provider.



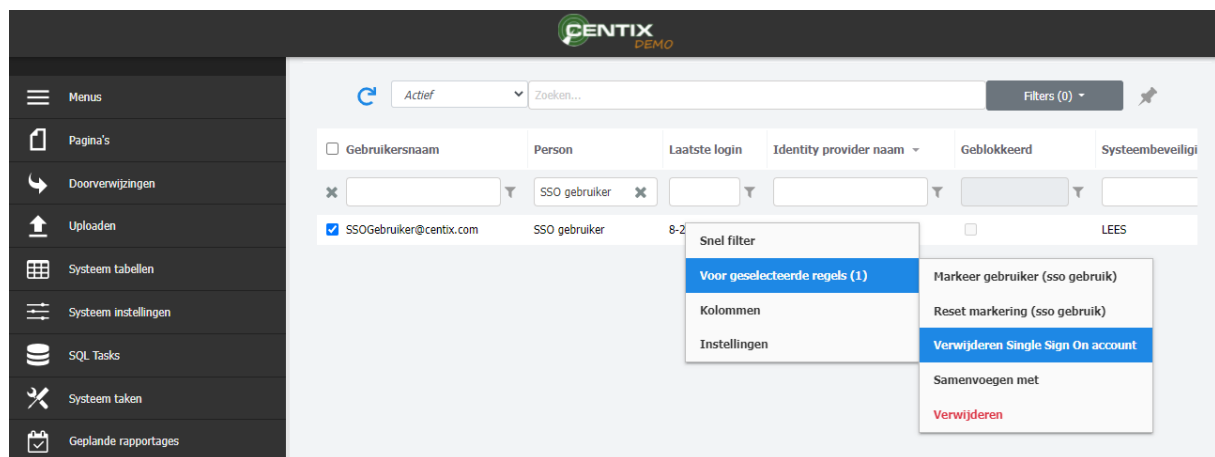
Na het inloggen met de identity provider is de gebruiker gemigreerd en kan deze gebruiker voortaan alleen nog inloggen via de identity provider.

## 5. Verwijderen Single Sign on van een gebruiker

Als een gebruiker geen gebruik meer mag maken van Single Sign On dan kan dit van het account worden verwijderd. Het verwijderen van Single Sign On op de gebruiker wordt gedaan via het gebruikersoverzicht, te benaderen via admin panel → systeem taken → gebruikers, via de volgende URL: <https://mijnbedrijf.centix.com/admin/systemtasks/users> of via het gebruikerstabblad in het detail van de identity provider.

### 5.1 Verwijderen van Single Sign On

De Single Sign On verwijderen kan op verschillende plekken. Echter is de basis hetzelfde. Vink de gebruiker aan → rechtermuisknop → voorgeselecteerde regels → verwijderen Single Sign On account.



The screenshot shows the CENTIX DEMO admin interface. On the left is a dark sidebar menu with options like 'Menu', 'Pagina's', 'Doorverwijzingen', 'Uploaden', 'Systeem tabellen', 'Systeem instellingen', 'SQL Tasks', 'Systeem taken', and 'Geplande rapportages'. The main area displays a table of users. The table has columns: 'Gebruikersnaam', 'Person', 'Laatste login', 'Identity provider naam', 'Geblokkeerd', and 'Systeembeveiliging'. One user is selected: 'SSOGebruiker@centix.com' with 'SSO gebruiker' as the person and '8-2' as the last login. A context menu is open over this row, showing options: 'Snel filter', 'Voor geselecteerde regels (1)', 'Kolommen', 'Instellingen', 'Markeer gebruiker (sso gebruik)', 'Reset markering (sso gebruik)', 'Verwijderen Single Sign On account' (highlighted), 'Samenvoegen met', and 'Verwijderen'.

Door de gebruiker volledig te verwijderen wordt ook meteen het Single Sign On account verwijderd. Echter is dit niet te adviseren omdat bijvoorbeeld status logs aan de gebruiker gekoppeld zijn. Het advies is daarom om de gebruiker te blokkeren en de Single Sign On van het account te verwijderen.

### 5.2 Verwijderen van Single Sign On van gemigreerde gebruiker

Wanneer de Single Sign On wordt verwijderd van een gemigreerde gebruiker dan wordt de gebruiker teruggezet naar het oude Centix account. Na het verwijderen kan de gebruiker weer inloggen met de oude Centix inloggegevens.

### 5.3 Verwijderen van Single Sign On van niet gemigreerde (nieuwe) gebruiker

Als de Single Sign On van een niet gemigreerde, dus nieuw aangemaakte gebruiker wordt verwijderd dan blijft de gebruiker bestaan. Dit om ervoor te zorgen dat er geen gegevens verloren gaan. In het persoonsdetail zal daarom ook een gebruikersnaam en een wachtwoord te zien zijn.

**Document Classificatie: Internal use**

Versie: 1.1 / Status: **Published**

Gepubliceerd op: 8-2-2022

Documentnummer: 84272

Paginnummer: 19 van 21

Handleiding: Single Sign-on



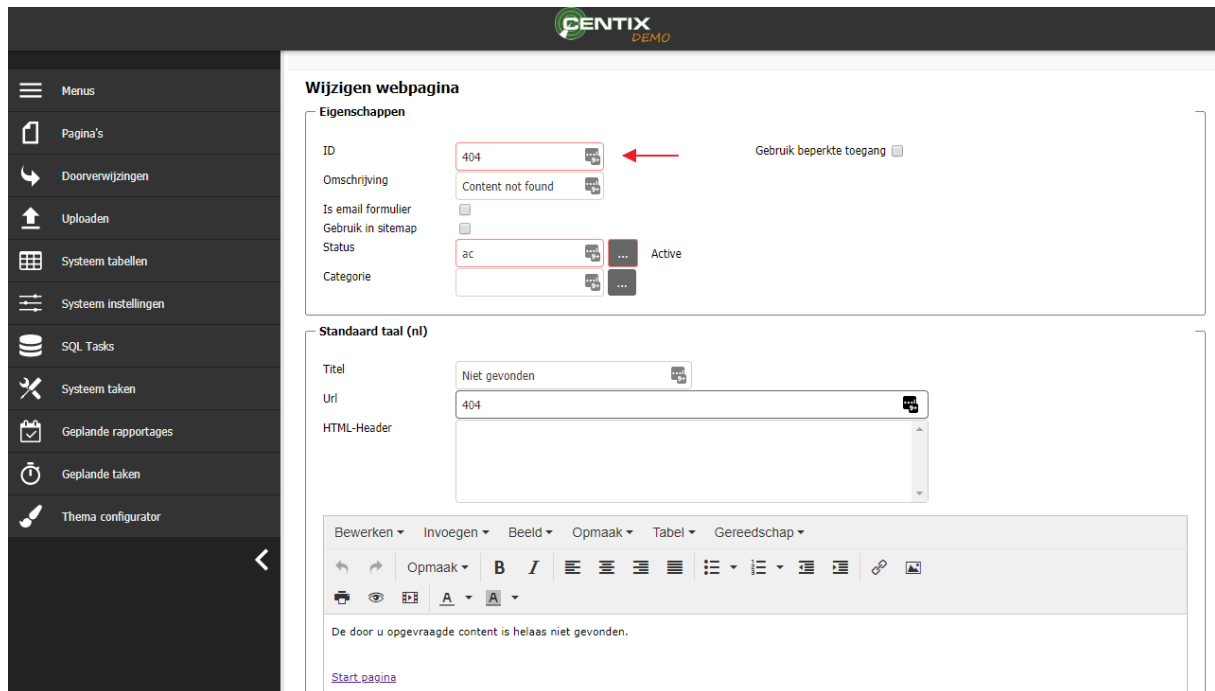
The screenshot shows the 'Persoon detail / CENTIX-SSO' page in the CENTIX system. The interface includes a top navigation bar with menu items like 'Objecten', 'Locaties', 'Relaties', 'Orders', 'Artikelen (verkoop & verhuur)', 'Workflow', and 'Extra'. A left sidebar contains navigation options: 'Detail', 'Relaties', 'Handteke...', 'Profiel', 'Locatie gebruikers', 'Beveiliging' (highlighted), 'Email profiel', and 'Gebruikersinstellingen'. The main content area is divided into several sections:

- Gebruikersnaam:** SSO gebruiker
- Domeinnaam:** (empty field)
- Wachtwoord:** (masked with dots)
- Herhaal wachtwoord:** (masked with dots)
- Windows authenticatie:**
- Geblokkeerd:**
- Systeemrol:** LEES - alleen lezen
- Gebruiker met beperkte rechten:** De gebruiker is lid van een 'view' beveiligingsrol.
- Relatie beperking:** Eigenaar
- Object beperking:** Eigenaar
- Locatie beperking:** Eigenaar
- Workflow beperking:** Contactpersoon
- Nieuwe gebruikersaanvraag beperking:** Eigenaar
- Factuur beperking:** Geassocieerde personen
- Order beperking:** Geassocieerde personen
- Startpagina:** Zoeken...
- Laatste login:** 8 / 2 / 2022

Het wachtwoord wat bij de niet gemigreerde gebruiker staat is een automatisch gegenereerd wachtwoord welke niet te achterhalen valt. Men kan hier zelf een wachtwoord invullen of deze laten resetten door de wachtwoord vergeten knop op de login pagina.

## 6. Foutmeldingen

Centix heeft een lijst met foutmeldingen die kunnen optreden gegenereerd. Wanneer een Centix pagina wordt aangemaakt met deze foutcodes als ID zal bij de betreffende foutcode deze pagina geopend worden.



**C3000** = Algemene foutmelding

**C3001** = Cookies zijn missend, zal waarschijnlijk alleen voorkomen wanneer hackers cookies manipuleren.

**C3002** = Provider is niet actief

**C3003** = De provider heeft de gebruiker door gestuurd maar Centix beoordeelt het verzoek als ongeldig, in de logs is de reden terug te vinden.

**C3004** = Er is een error binnen Centix opgetreden bij het inloggen.

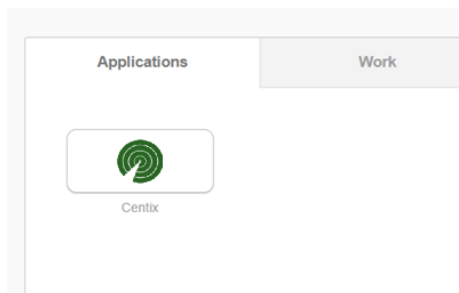
**C3005** = De provider bestaat niet meer.

## 7. Bijzonderheden

In de bijzonderheden worden uitzonderingen of extra's uitgelegd die mogelijk zijn met het inregelen van Single Sign On in Centix.

### 7.1 Inloggen via identity provider (Okta)

Het kan zijn dat de wens niet speelt om in te loggen via de Centix pagina maar liever inlogt via de identity provider. De gebruiker krijgt dan een overzicht met opties binnen zijn homepagina van de identity provider met de applicaties waar hij op in kan loggen.



Wanneer de gebruiker op Centix klikt wordt deze meteen doorgestuurd en ingelogd. Om dit mogelijk te maken dienen er een aantal dingen in de applicatie Okta ingesteld te worden:

Login initiated by	Either Okta or App
Application visibility	<input checked="" type="checkbox"/> Display application icon to users <input type="checkbox"/> Display application icon in the Okta Mobile app
Login flow	<input checked="" type="radio"/> Redirect to app to Initiate login (OIDC Compliant) <input type="radio"/> Send ID Token directly to app (Okta Simplified)
Initiate login URI	<a href="https://centix.com/mvc/oidc/ldp">https://centix.com/mvc/oidc/ldp</a>

Als initiate login URI wordt de volgende opzet gebruikt: <https://mijnbedrijf.centix.com/mvc/oidc/ldp>