



SOC Team
Zwarte Woud 2
3524 SJ Utrecht
Telefoon 030 252 3004
Email soc@ggdghor.nl



Onboarding account provider – Checklist

Aansluiten nieuwe account provider via GGDGHOR TIH

Versie: 0.3

Opdrachtgever	Peter de Koning	Manager SOC GGD GHOR
Auteur	M. Hoogenraad	IAM GGD GHOR

Rapportnummer	
Classificatie	Intern
Status	Voorlopig
Datum	28 april 2021
File Naam	Onboarding Account provider – Technisch IAM

Concept versie 0.01

Inhoud

1. Inleiding	4
1.1. Scope en doelgroep	4
1.2. Rollen en verantwoordelijkheden	4
1.3. Review of audit door het SOC.....	4
2. Proces onboarding account provider	5
2.1. Fase 1: Wijzigingsaanvraag / Intake	5
2.2. Wijzigingsaanvraag autorisatie	6
2.3. Fase 2: Uitvoering	6
2.4. Implementatie autoriseren.....	6
2.5. Communicatie regie	6
2.6. Bijlage A: Account provider checklist voor de intake.....	7

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
0.1	28-04-2021	Michiel Hoogenraad	Initiële opzet	Concept
0.2	10-05-2021	Michiel Hoogenraad	Aanpassingen na review	Concept
0.3	12-05-2021	Marc Rietbergen	Aanpassingen proces en checklist	Concept

Gecontroleerd door

Versie	Datum	Naam	Functie
0.1	06-05-2021	Marc Rietbergen Enrico Lammens Mick Lemmerman	IAM-Specialist IAM-Specialist IAM-Specialist

Geautoriseerd door

Versie	Datum	Naam	Functie
		Peter de Koning	Manager SOC

Gerelateerde documenten

Documenttitel	Omschrijving

Volgende review en/of herziening, plus accordering (tenzij eerdere update)

Datum	Functie voor bewaking
01-06-2021	Manager SOC

1. Inleiding

Met dit document wil GGD GHOR het technisch onboarden van nieuwe Account Provider (hierna te noemen AP) structureren en zorgdragen dat relevante informatie op de juiste plaats worden opgeslagen.

Dit document biedt informatie en een checklist voor het toevoegen van nieuwe AP aan de GGD-GHOR IAM oplossing, The Identity Hub (hierna te noemen TIH) om gebruik te maken van één of meerdere applicaties welke via de TIH ontsloten zijn.

1.1. Scope en doelgroep

Dit document is van toepassing op **alle** APs die door GGDGHOR worden ontsloten via TIH

De doelgroep bestaat uit de projectleiders van de aan te sluiten AP en de technische projectmedewerkers van de APs.

Dit document beschrijft het onboardingsproces van een AP in termen van activiteiten en verantwoordelijkheden tussen het GGDGHOR IAM team, de APs en de projectleider voor de aansluiting.

1.2. Rollen en verantwoordelijkheden

Het IAM team van GGD GHOR is verantwoordelijk voor de inhoud van dit document.

Het IAM-team is verantwoordelijk voor het correct uitvoeren van de handelingen conform dit document.

1.3. Review of audit door het SOC

Desgewenst kan het SOC een review of audit uitvoeren op de AP.

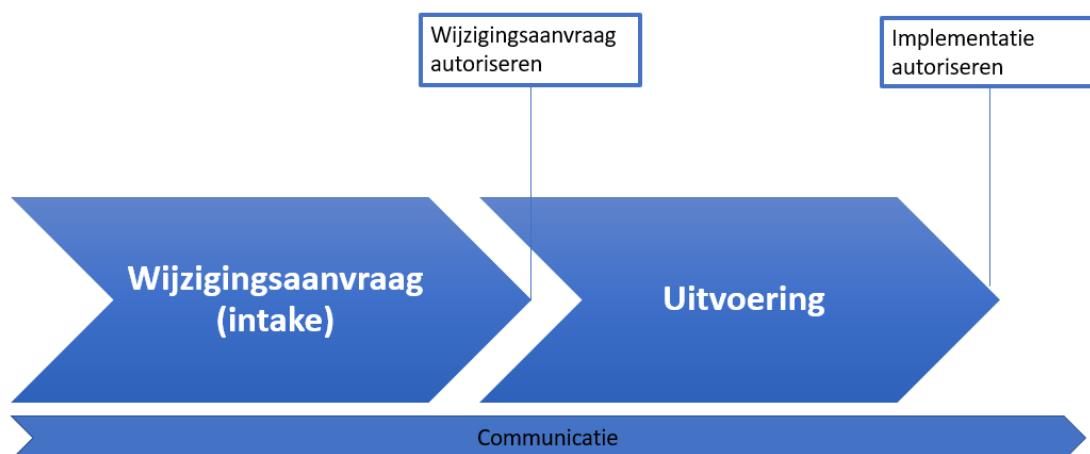
Het IAM-team onderhoudt dit document en communiceert deze naar de betrokken medewerkers van het IAM-team en projectmedewerkers.

2. Proces onboarding account provider

Het onboarding proces voor een AP wordt door een lid van het IAM Team gecoördineerd. Het proces start met een TOPdesk wijzigingsaanvraag. Een projectmanager of IAM-teamlid maakt een wijzigingsaanvraag aan. Dit teamlid is dan ook de coordinator van de wijziging. De aanvraag wordt concreet gemaakt tijdens de intake fase, waar de nodige informatie wordt verzameld om de haalbaarheid te beoordelen. Na de intake wordt het wijzigingsverzoek gehonoreerd (geautoriseerd) of afgewezen. Indien geautoriseerd gaat men verder met de uitvoering.

Processtappen voor onboarding applicatie

Het proces is conform het standaard wijzigingsproces van TOPdesk
De stappen binnen het proces zijn:



2.1. Fase 1: Wijzigingsaanvraag/ Intake

Er wordt een TOPdesk wijzigingsaanvraag namens een opdrachtgever geregistreerd. De eerste stap is om het wijzigingsverzoek te beoordelen op de volledigheid en correctheid van de informatie. Er wordt een checklist doorgenomen (zie Bijlage A). Een medewerker van het IAM-team neemt contact op met de aanmelder en contactpersoon van de AP en neemt het proces door en de context rondom de aansluiting van de nieuwe AP.

Randvoorwaarden

- De aanvrager is een geautoriseerd persoon binnen de GGDGHOR, bijvoorbeeld een informatiemanager of projectleider.
- De aanvrager levert de contactgegevens aan van de nieuwe account provider en moet aangeven welke applicaties de AP gaat gebruiken (binnen de scope van het project).

Deliverable

- Het AP checklist van IAM (Zie bijlage A) is volledig ingevuld
- Bevestiging naar de aanmelder dat het wijzigingsverzoek compleet en correct is en naar de volgende fase (Vorbereiding) overgaat.

2.2. **Wijzigingsaanvraag autorisatie**

Nadat de intake is gedaan rapporteert de uitvoerder aan de aanvrager. Dit is een GonoGO moment. Kan de AP worden aangesloten dan wordt de wijziging geautoriseerd en start de Fase 2: Uitvoering.

2.3. **Fase 2: Uitvoering**

In de uitvoerfase wordt de AP aangesloten samen met de ICT beheerder en het IAM team van GGDGHOR. De uitvoering bestaat minimaal uit de onderstaande activiteiten

1. **Maken voorlopige planning:** Stem de planning af met de projectleider en de AP. Maak de activiteiten aan in TOPdesk aan de hand van de voorlopige planning.
2. **Technische aansluiting:** Aanmaken van accountprovider op de GGDGHOR tenant.
3. **Test technische aansluiting:** Test aanmelden op TIH
4. **Pilot applicatie aansluiting:** In overleg wordt een applicatie gekoppeld aan de nieuw accountprovider en een kleine pilot groep van eindgebruikers. Aandachtpunten zijn:
 - i) Het aanmaken van AD security groepen.
 - ii) lid maken van pilot medewerkers.
 - iii) Het configureren van de claimmappings (gebruik de standaard excel bestand.
 - iv) Publiceren aangepaste URL applicatie indien van toepassing op de werkplek.
 - v) Instructies voor het eerste keer aanmelden met 2FA van TIH.
5. **Go-Live:** In deze fase gaat de account provider live voor 1 applicatie. Betreft het meerdere applicaties dan worden stap 4 en 5 herhaald. Afhankelijk van de complexiteit kunnen er meerdere applicatie 1 een keer ontsloten worden.
6. **Nazorg:** Tijdens de nazorg staat het IAM op 'standby' om de servicedesk te ondersteunen.

Deliverable

- Een aangesloten AP aan TIH

2.4. **Implementatie autoriseren**

Is de wijziging succesvol afgerond dan vindt er een decharge plaatst. Administratief gezien wordt de implementatie in TOPdesk geautoriseerd door de aanvrager.

2.5. **Communicatie regie**

De regie van communicatie rondom het project wordt gedaan door de projectleider in afstemming met de AP.

2.6. **Bijlage A: Account provider checklist voor de intake**

Deze checklist is noodzakelijk voor de juiste aansluiting aan de IAM oplossing, TIH, van GGDGHOR. Op basis van onderstaande gegevens kan de AP aangesloten worden met onder andere de volgende standaarden: SAML, OAuth 2.0, OpenID Connect.

Gegevens van de aanmelder/projectleider

#	Item	Antwoord
1	Naam	
2	Functie	
3	Telefoon	
4	Email	
5	Naam GGD	
6	/ Naam Partner	

Gegevens van de informatiemanager (van GGDGHOR):

#	Item	Antwoord
1	Naam	
2	Functie	Informatiemanager
3	Telefoon	
4	Email	@ggdghor.nl

Gegevens van de contactpersonen van de AP (functioneel en/of technisch)

#	Item	Functioneel	Technisch	Projectleiding
1	Naam			
2	Functie			
3	Telefoon			
4	Email			

Account provider readiness

#	Item	Omschrijving	Antwoord
1	Naam	Naam van de AP	
2	Omschrijving	Soort organisatie	
3	Image URL		
4	SSO Methode	SAML/OAuth/OIDC	
5	ADFS of Azure AD of andere IDP?	Beschik de AP over een ADFS of Azure infrastructuur of een andere IDP (bijvoorbeeld een HelloID) waarmee TIH kan koppelen.	
6	Aantal medewerkers	Hoeveel gebruikers gaan via de TIH ontsloten?	
7	Persoonlijk account	Beschikken alle medewerkers over een persoonlijk account?	
8	Smartphone gebruik	Beschikken alle medewerkers over een smartphone voor het gebruik van een Authenticator App? Authenticatie via TIH vereist namelijk een Authenticator App die op een smartphone gebruikt dient te worden.	
9	Aansluiting op app	Welke applicaties wil de AP gaan gebruiken? Naam van applicatie en het aantal gebruikers per applicatie vermelden	
10	Koppeling met HR	Bestaat er een koppeling tussen het HR pakket en de AD/AAD? Zo ja, welke?	
11	Naamconventie	Wat is de naamconventie van de inlognamen? Naamgeving UPN, Primaire Emailadres en weergave naam bijvoorbeeld UPN = <1e letter roepnaam>.<geboortnaam>@<upn suffix>.nl UPN = gelijk aan Email	
12	Certificaat	Wordt er gebruik gemaakt van een self signed certificaat? Dit wordt namelijk niet geaccepteerd vanuit GGD GHOR.	

Tip! Voor meer informatie over de AP ga naar [Account Providers | Documentation \(theidentityhub.com\)](https://theidentityhub.com)