TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Whitepaper V2.0.3 / 23.04.2025

HelloID Identity as a Service

Inhoud

Inleiding

Identity & Access Management (IAM)-software speelt al langer een centrale rol in veel IT-omgevingen. Via deze functionaliteit krijgen gebruikers toegang tot hun IT-omgeving en kunnen ze gebruikmaken van hun applicaties en data. Met trends zoals de toenemende digitalisering en verdere cloud-evolutie veranderen ook de eisen aan Identity Management-software. Hieronder schetsen we deze trends en wat ze betekenen voor IAM-functionaliteit.

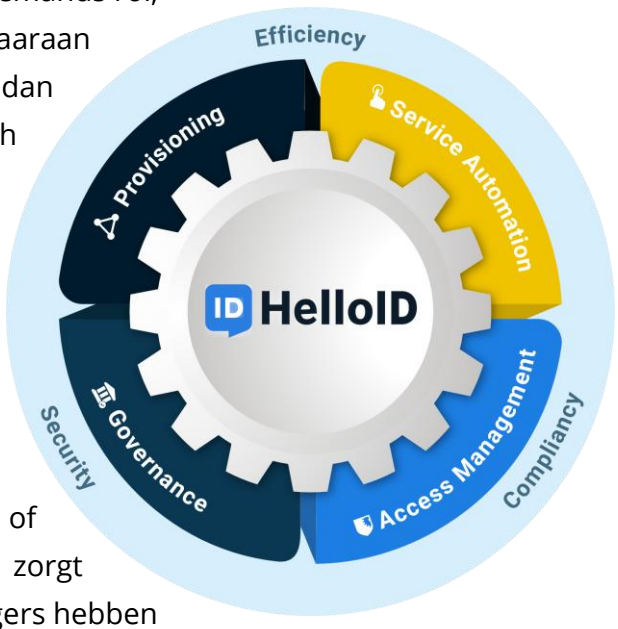
Trend	Gevolg
Veel organisaties zijn recent gestart met de transitie naar de cloud. Basis infrastructuurcomponenten als Exchange, Active Directory en lokale opslag worden omgezet naar Azure, O365 en Teams. Business-applicaties zoals het HR-systeem zijn vaak al eerder naar de cloud gemigreerd. Het eigen datacenter wordt nog een paar jaar aangehouden, maar de infrastructuur wordt uitgefaseerd zodra de afschrijvingstermijn voorbij is.	Identity en Access Management is nu nog vaak on premise. Over een paar jaar hebben organisaties geen lokale infrastructuur meer beschikbaar. De Identity en Access Management-oplossing moet dan ook als dienst (as a Service) beschikbaar zijn. Dit soort systemen worden aangeduid als Identity as a Service (IDaaS).
Data over producten, klanten en medewerkers wordt steeds waardevoller voor organisaties. Toegang tot deze gegevens, tijdig en correct, is cruciaal voor succes. Tegelijkertijd dwingt strengere regelgeving zoals GDPR, AVG en NIS2 organisaties maatregelen te nemen om audits, boetes en reputatieschade te voorkomen.	Voorheen waren semi-geautomatiseerde procedures en enkele scripts voldoende om gegevens te beschermen en te voldoen aan de geldende eisen. Dit wordt echter steeds lastiger. Directie, raad van bestuur en de security officer vragen steeds nadrukkelijker om een organisatiebrede professionele IAM-oplossing.
Verbeteren van de dienstverlening, doorvoeren van bezuinigingen, betere concurrentiepositie, organisaties willen steeds efficiënter werken. Het stroomlijnen van informatie over medewerkers en het tijdig en correct verlenen van toegang tot systemen is hier zeker een onderdeel van.	Organisaties willen medewerkers centraal beheren via een kernregistratiesysteem, waar alle wijzigingen automatisch worden verwerkt. Het IAM-systeem detecteert wijzigingen zoals in- en uitdiensttreding, adres- of afdelingswijzigingen, en verwerkt deze direct naar useraccounts, e-mailadressen, toegangsrechten, licenties en IT-middelen op basis van HR-gegevens zoals functie en afdeling.

Trend	Gevolg
De automatisering binnen organisaties groeit snel, waardoor alles digitaal is geworden. Waar vroeger groepsaccounts nog gangbaar waren, heeft nu iedereen een persoonlijk useraccount. In deze digitale wereld is de juiste verbinding tussen de medewerker en zijn data beslissend voor het succes van de organisatie. Medewerkers moeten op ieder moment, met elk apparaat en vanaf elke locatie, toegang hebben tot de gegevens die ze nodig hebben.	Zonder correcte en snelle toegang is een medewerker niet productief, raakt gefrustreerd en creëert stress bij betrokken afdelingen. Via IDaaS is het mogelijk om alle benodigde resources tijdig en correct te verzorgen. Ook eenvoudig en eenmalig inloggen (SSO) op een veilige manier met een telefoon (2FA) is daar onderdeel van. Medewerker gaat naar één centrale plek en heeft van daaruit toegang tot alle benodigde IT-middelen.
Identity Management-systemen zijn vaak complex te implementeren en te onderhouden. Het is moeilijk te doorgronden wat het systeem doet. Consultants zijn schaars, duur en lastig om op tijd in te plannen.	Organisaties kunnen niet inspelen op markt- en organisatorische veranderingen. Het systeem werkt onbetrouwbaar, is een black box en er komen steeds vaker kritische vragen over de hoge kosten die gemoeid zijn met het systeem.

Met HelloID – de Identity & Access Management-oplossing van Tools4ever – zijn we voorgesorteerd op deze belangrijke ontwikkelingen. Tools4ever biedt Identity as a Service (IDaaS), een volwaardige cloud native oplossing. HelloID automatiseert je volledige Identity-lifecycle en jouw gebruikers krijgen gebruiksvriendelijk én veilig toegang tot hun IT-diensten. Je hoeft niet te investeren in een eigen infrastructuur met hardware, storage en software. De installatie en configuratie zijn letterlijk een kwestie van uren en Tools4ever, een implementatiepartner of de eigen organisatie verzorgt het beheer. De lagere kosten en minimale beheerwerkzaamheden gaan niet ten koste van de controle en veiligheid. Tools4ever-klanten ontvangen vaak complimenten van IT-auditors over de inrichting en werking van HelloID. Bovendien draait de software in maximaal beveiligde Microsoft Azure en Google Cloud-omgevingen, die iedere zes maanden grondig worden gecontroleerd door Deloitte Risk Services. Compliance aan de strenge security-eisen is gewaarborgd. Deze IDaaS-oplossing biedt een gebalanceerd groeipad. HelloID dwingt je niet tot een ‘big bang’ met veel druk op de organisatie en grote risico’s. HelloID is opgesplitst in modulen en de uitrol kan gefaseerd worden uitgevoerd. Als organisatie kan je vrij kiezen met welke modulen je start en welke functies je later wilt activeren. Ook functies weer uitzetten is probleemloos mogelijk.

HelloID omvat de volgende modulen

1. **Provisioning** verzorgt de automatische aanmaak, beheer en eventuele verwijdering van gebruikersaccounts op basis van informatie uit je HR-systeem. Ook beheert Provisioning automatisch de bijbehorende rechten en verdere faciliteiten, afhankelijk van iemands rol en verdere context. Wijzigt iemands rol, dan worden automatisch de rechten daaraan aangepast. En verlaat iemand de organisatie, dan kan het gebruikersaccount automatisch worden gedeactiveerd en verwijderd.



2. **Service Automation** sluit naadloos aan op de module Provisioning. Naast de geautomatiseerde provisioning vanuit het HR-systeem, zijn er altijd 'maatwerk'-serviceverzoeken. Iemand heeft tijdelijk specifieke software nodig voor een project, of rechten tot bepaalde bestanden. Hiervoor zorgt Service Automation. Medewerkers en managers hebben toegang tot een portaal met alle IT-diensten die (tijdelijk) aangevraagd kunnen worden. Wijzigingen worden direct in het netwerk, zonder tussenkomst van IT-medewerkers, doorgevoerd.

3. **Governance** voegt extra mogelijkheden toe aan Provisioning en Service Automation. Waar deze modules de basis leggen voor efficiënt en veilig toegangsbeheer, gaat de Governance module een stap verder. Governance is een oplossing die organisaties helpt om continu controle te houden over gebruikersaccounts en toegangsrechten. Hiermee kun je deze periodiek te evalueren, afwijkingen detecteren en corrigeren, waardoor je nog meer grip krijgt op toegangsbeheer en compliance.

4. **Access Management** beheert veilige én gebruiksvriendelijke toegang van medewerkers tot de verschillende applicaties en gegevens. Gebruikers kunnen zich authentiseren via een login met gebruikersnaam, een wachtwoord en Multi Factor Authenticatie. HelloID biedt na toegang een gebruiksvriendelijk dashboard waarin gebruikers eenvoudig hun applicaties kunnen openen. Dankzij de uitgebreide Single Sign-On functionaliteit volstaat daarbij één klik.

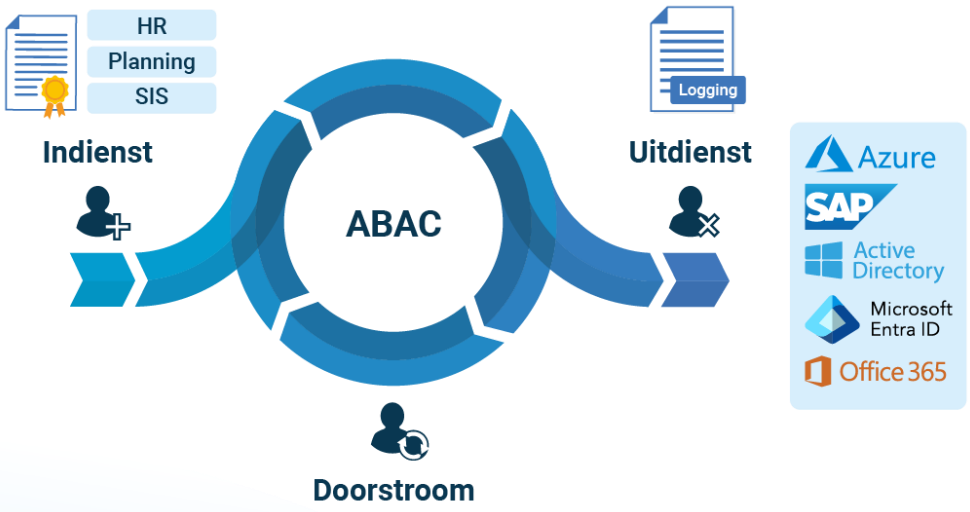
Provisioning

Koppel bron- en doelsystemen voor geautomatiseerd gebruikers- en autorisatiebeheer.

Als organisatie moet je talloze gebruikersaccounts beheren. Van vaste medewerkers, tijdelijke krachten en vaak ook van ketenpartners en klanten. Dat betekent uiteraard dat regelmatig gebruikersaccounts moeten worden aangemaakt of juist verwijderd. Bovendien moeten de accounts voortdurend worden beheerd. Iemands rechten, applicaties en verdere resources zullen veelal afhankelijk zijn van diens rol, afdeling, locatie etc. En bij veranderingen daarin moeten ook die zaken meestal worden aangepast. HelloID Provisioning verzorgt het volautomatisch aanmaken, aanpassen en verwijderen van accounts. Hiermee automatiseren we het volledige in-, door- en uitstroomproces, je gehele 'Identity Lifecycle Management'. Met automatische provisioning maak je jouw medewerkers productiever, bespaar je op routinewerkzaamheden en dure licenties en versterk je jouw IT-beveiliging.

Identity Lifecycle Management

Dankzij HelloID beschikt een nieuwe medewerker op de eerste werkdag over een gebruikersaccount met de bijbehorende toegangsrechten, de benodigde software en andere faciliteiten. Wanneer een medewerker na verloop van tijd doorstroomt naar een andere functie en/of afdeling zorgt het HelloID doorstroomproces dat automatisch diens rechten en licenties worden aangepast. En gaat een medewerker uit dienst? Dan kan HelloID ervoor zorgen dat het account direct wordt geblokkeerd. Ook kan een forward en out of office op de e-mailbox worden gezet en een e-mail naar de manager gestuurd met welke hardware moet worden ingeleverd. Alle eerdere handmatige acties worden nu via HelloID geautomatiseerd.



Provisioning maakt het beheer van gebruikersaccounts eenvoudiger, sneller en veiliger. Niet langer is het beheer van gebruikersaccounts een handmatige, complexe en tijdrovende klus voor de HR- en IT-teams. Terwijl medewerkers er productiever van worden omdat ze altijd direct over de juiste faciliteiten beschikken. Naast gemak en efficiency biedt automatische provisioning ook een krachtige extra beveiligingstool. Binnen veel bedrijven verzamelen medewerkers vaak gaandeweg – zelfs onbedoeld – steeds meer rechten en faciliteiten. Veelal ontbreekt een automatisch proces om rechten weer terug te draaien als iemand ze niet meer nodig heeft. Het komt vaak voor dat oud-medewerkers nog toegang houden tot systemen, met alle bijbehorende risico's.

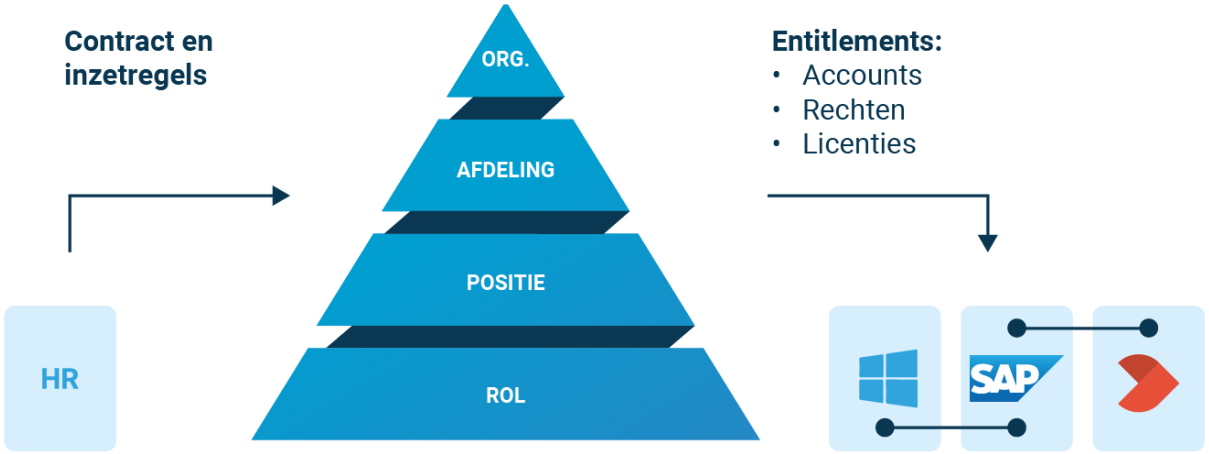
Automatische provisioning garandeert dat iemand steeds alleen dié rechten heeft die voor zijn of haar rol nodig zijn. Bij een functie- of afdelingswijziging worden rechten en licenties, optioneel met een grace-periode, ingenomen. Deze automatische roll-back van rechten en faciliteiten levert ook direct een kostenvoordeel op. Veel bedrijven maken veel nodeloze kosten aan dure licenties en faciliteiten die niet meer gebruikt worden maar wel maandelijks worden gefactureerd. Met HelloID krijg je veel meer grip op deze kosten.

Attribute Based Access Control (ABAC)

Een centraal element van Provisioning wordt gevormd door Attribute Based Access Control. ABAC zorgt dat medewerkers toegang hebben tot de juiste IT-resources die ze nodig hebben om hun werk te kunnen doen. Dus afhankelijk van iemands rol in de organisatie en de bijbehorende werkzaamheden heeft een medewerker specifieke zaken nodig van IT. Via ABAC beleidsregels wordt deze vertaling uitgevoerd. Op basis van de combinatie functie en afdeling worden accounts, rechten, licenties en IT-middelen (laptop, werkplek, telefoon, etc.) uitgeleverd.

Door de verscherping van wet- en regelgeving (zoals AVG, FISMA, HIPAA, SOX, ISO 27001, NEN 7510) is ABAC de laatste jaren steeds belangrijker geworden. ABAC was voorheen vooral het domein van financiële instellingen en grote internationale bedrijven. Tegenwoordig is ABAC ook steeds vaker een eis binnen zorginstellingen, middelgrote bedrijven (300-5000 medewerkers) en andere commerciële organisaties.

Als organisatie wil je volledige grip hebben op wie waar toegang toe heeft. Daarbij zoek je een heldere balans tussen gebruiksvriendelijkheid en informatiebeveiliging. Met te weinig rechten en rechten die te laat worden uitgeleverd belemmer je medewerkers bij hun werk. Met te veel rechten loopt de organisatie grote risico's. Veel organisaties lopen hierbij tegen grenzen aan. Handmatig de rechtenstructuur in kaart brengen en beheren is enorm complex, tijdrovend en omvangrijk. Snel gebruikers aanmaken op basis van copy-user – "Jolanda gaat dezelfde werkzaamheden uitvoeren als Marian" – is weer te eenvoudig. ABAC-functionaliteit zorgt dat u dit beheer naar een volwassen niveau kunt brengen op een praktische en eenvoudige manier.



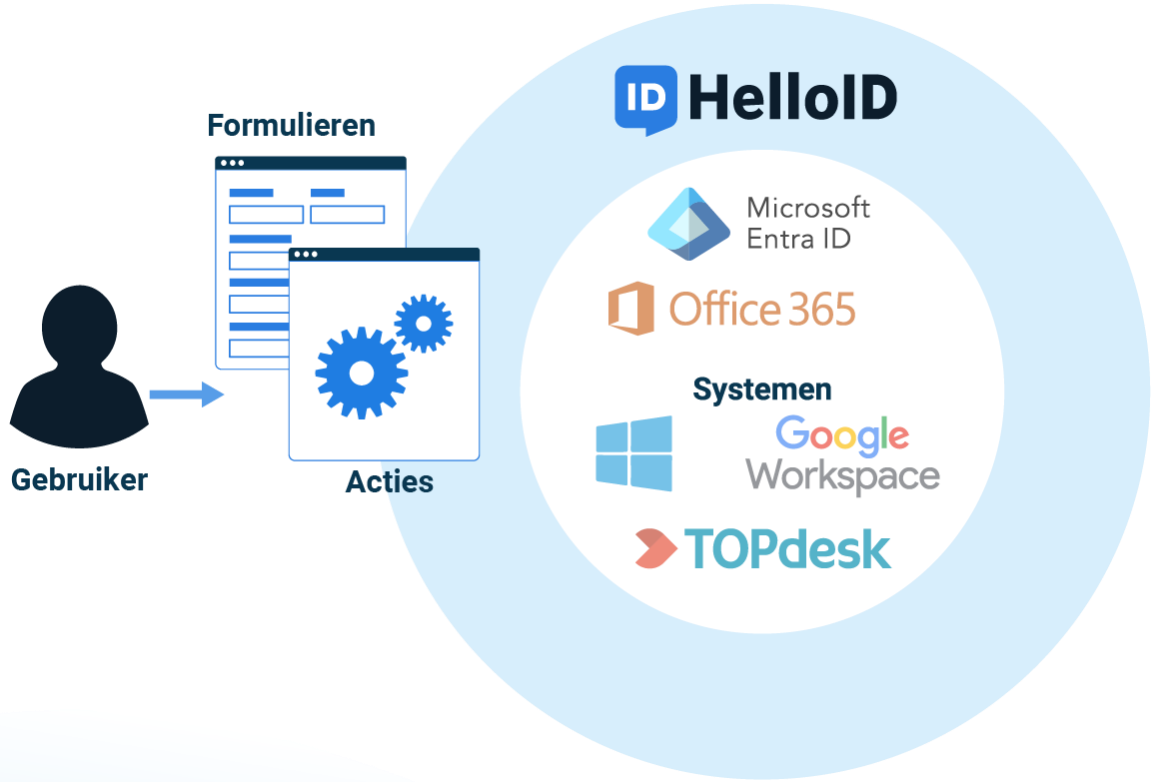
Binnen HelloID implementeren we ABAC via onze 'Business Rules' functionaliteit. Business Rules biedt de mogelijkheid om met een gefaseerde aanpak het rechtenmodel op te bouwen. Business Rules brengt organisaties vanaf het huidige niveau stapsgewijs naar een professioneel platform waarmee ze op een gecontroleerde manier rechten kunnen beheren, zonder dat eerst alle rollen en rechten in kaart gebracht moeten worden. Het bovenstaande diagram geeft een schematisch overzicht van de aanpak van de HelloID Business Rules. Op basis van de contracten en inzetregels wordt per niveau (organisatie, afdeling, functie en rol) van medewerkers bepaald welke toegang (accounts, rechten en licenties) nodig zijn in het netwerk om de werkzaamheden uit te kunnen voeren.

Service Automation

Gestroomlijnde aanvraagprocessen middels helpdesk delegatie, self-service en workflows.

Het Provisioning-proces automatiseert nagenoeg alle IT-gerelateerde wijzigingen. Toch zijn er uitzonderingen, want niet alles wordt geregistreerd in het HR-systeem. Denk aan een medewerker die tijdelijk de werkzaamheden waarneemt van een zieke collega, of een medewerker die wordt ingezet op een project of uitgeleend aan een andere afdeling. Om deze extra taken uit te voeren heeft de medewerker bijvoorbeeld extra toegangsrechten tot dossiers nodig, extra rechten om taken uit te kunnen voeren in SAP, een Microsoft-projectlicentie, lidmaatschap op een distributielijst, lid van een Microsoft Teams site, etc.

In veel bedrijven worden dit soort wijzigingen handmatig afgehandeld door de IT-helpdesk of Functioneel Beheer (FB), wat het duur en tijdrovend maakt. Service Automation automatiseert daarom deze wijzigingen. Via een webinterface kunnen medewerkers zonder IT-kennis en domain admin-rechten zelf veilig wijzigingen in het netwerk doorvoeren. Dit gebeurt via een gedelegeerde schil om het netwerk en alle wijzigingen worden via gedefinieerde scenario's via de HelloID engine in het netwerk uitgevoerd. Volgens exact gedefinieerde stappen, altijd op dezelfde wijze, met een volledige audit-log zonder admin-rechten.



De module Service Automation biedt de volgende voordelen

- Iedereen kan op een veilige en gecontroleerde manier wijzigingen doorvoeren in het netwerk. De helpdesk hoeft niets meer te doen en is niet langer de vertragende factor. Managers hebben direct inzicht in waar hun medewerkers toegang toe hebben en kunnen dit ook direct aanpassen.
- Het is direct zichtbaar wie welke licenties gebruikt, of er niet te veel licenties worden gebruikt en hoeveel licenties nog beschikbaar zijn. Managers zien eenvoudig wat de 'IT-footprint' van hun afdeling is.
- Aan wijzigingen wordt een tijdslimiet gekoppeld. Dit voorkomt ongewenste accumulatie van rechten en licenties. Niet langer worden extra rechten wél aangevraagd maar achteraf nooit of nauwelijks geretourneerd. Dit is zeker een aandachtgebied van auditors en geeft vaak een negatieve beoordeling.
- Moderne en professionele uitstraling naar de organisatie en medewerkers die nieuw in dienst komen;
- HelloID Service Automation is geïntegreerd in verschillende ITSM-platformen (Servicenow, TOPdesk). Hierdoor treden er minimale veranderingen op voor de eindgebruiker en is gebruikersacceptatie hoog, omdat er niet (weer) een nieuw startportaal wordt geïntroduceerd.

Service Automation kan een grote organisatorische impact hebben. Zo krijgen medewerkers en managers een andere en belangrijkere rol in de uitgifte van IT-faciliteiten. Om de implementatie zo eenvoudig mogelijk te laten verlopen kan Service Automation stapsgewijs worden ingevoerd. De onderstaande stappen kunnen doorlopen worden:

Delegatie naar de servicedesk

Dit is vaak de eerste stap. Bij deze stap komen gedelegeerde formulieren beschikbaar voor (non/semi-skilled) servicedeskmedewerkers. Hiermee kunnen werkzaamheden worden gedelegeerd van systeemspecialisten naar deze servicedeskmedewerkers. Het voordeel met Service Automation is dat geen admin-rechten nodig zijn voor het uitvoeren van de wijzigingen. De wijzigingen worden altijd op dezelfde wijze uitgevoerd, er is geen IT-kennis of applicatiekennis nodig voor het uitvoeren van de wijziging en elke wijziging wordt vastgelegd. Service Automation is een 'schil' om het netwerk, elke wijziging wordt gecontroleerd via Service Automation.

Delegatie naar de manager

De delegatie naar de manager is de volgende stap. Technisch gezien is dit een eenvoudige stap omdat de formulieren en acties al gedefinieerd zijn voor de medewerkers van de servicedesk. Vanuit de organisatie is het wel een grote stap omdat meer medewerkers direct met HelloID in aanraking komen. Na deze stap hebben de managers direct inzicht in welke toegangsrechten hun medewerker hebben en welke licenties ze gebruiken. De manager kan vervolgens zelf direct wijzigingen doorvoeren. Ook kan de manager zelf rechten voor een medewerker toevoegen of verwijderen. Er is geen omslachtig proces meer nodig met servicetickets en servicemedewerkers om ze uit te voeren.

Delegatie naar de eindgebruiker

De ultieme selfservice-stap is de delegatie naar de eindgebruiker. Belangrijke voorwaarde hiervoor is de integratie in de al aanwezige selfservice-portalen, zoals TOPdesk of AFAS. Er wordt een goedkeuringsslag toegevoegd, waarin bijvoorbeeld de manager en/of functioneel beheerder de aanvraag beoordeelt voordat deze wordt doorgevoerd. Deze controle voorkomt dat eindgebruikers zaken aanvragen of toegekend krijgen die niet nodig zijn voor de uitoefening van hun functie. Deze controle is voor een manager of licentiemanager veel eenvoudiger dan voor een IT-medewerker. Na goedkeuring verzorgt de Service Automation-module dat de wijzigingen automatisch worden doorgevoerd.

Governance

Grip door continu inzicht in naleving van beleid en het opsporen van afwijkingen.

HelloID Governance breidt de functionaliteiten van Provisioning en Service Automation verder uit. Waar deze modules de basis leggen voor efficiënt en veilig toegangsbeheer, gaat de Governance-module een stap verder. Het helpt je om niet alleen controle te krijgen, maar die ook die te houden.

Als organisatie is het namelijk essentieel om voortdurend inzicht en controle te hebben over de toegangsrechten van gebruikers, zoals medewerkers, tijdelijke krachten en externe partners. Zonder effectief beheer bestaat het risico dat ongeautoriseerde personen toegang krijgen tot gevoelige informatie. Dit kan leiden tot datalekken en andere beveiligingsincidenten. Daarnaast helpt Governance je om te voldoen aan wet- en regelgeving, zoals de AVG, NEN 7510, ISO 27001, Normenkader IBP FO en BIO, waardoor risico's worden beperkt en je organisatie voorbereid is voor de audit.

De module Governance biedt de volgende voordelen:

- **Voorkom ongeautoriseerde toegang**: Identificeer en verwijder ongewenste rechten om je security te versterken.
- **Continu toezicht op toegangsrechten:** Detecteer afwijkingen, herstel deze en stem toegangsrechten voortdurend af op de actuele situatie.
- **Slimme AI-aanbevelingen:** Verminder de werkdruk met proactieve suggesties en verbeterpunten voor de autorisatiematrix en self-serviceproducten.
- **Optimaliseer je auditproces:** zorg voor gestructureerde rapportages die voldoen aan alle auditvereisten.
- **Blijf altijd compliant:** Voldoe aan regelgeving zoals AVG, NEN 7510, ISO 27001, Normenkader IBP FO en BIO.

Wat houdt onze Governance module in?

HelloID Governance voegt extra functionaliteiten toe aan Provisioning en Service Automation, waarmee je voortdurend je beleid kunt evalueren en afwijkingen kunt identificeren en oplossen.

Wat is al beschikbaar?

Niet alle functionaliteiten van HelloID Governance zijn op dit moment al beschikbaar, maar we werken hard aan de verdere ontwikkeling. Stap voor stap voegen we nieuwe mogelijkheden toe, zodat je binnenkort kunt profiteren van alle functionaliteiten van de Governance Module.

Hieronder staat welke functionaliteiten al beschikbaar zijn:

- Reconciliation
- Recertification
- Toxic Policies

De volgende functionaliteiten staan op onze milestone planning, maar zijn nog niet direct beschikbaar:

- Role Mining
- Advanced Role Model
- Product Suggestions
- Advanced Approval Workflows

Provisioning & Governance

✓ Nu beschikbaar!

Reconciliation

Behoud controle over je doelsysteem

De reconciliation-functionaliteit binnen HelloID Governance vergelijkt de gewenste situatie (SOLL) met de actuele situatie (IST) in je doelsystemen. Hierdoor kun je verschillen identificeren, zoals ongewenste of ontbrekende accounts en toegangsrechten, en deze effectief corrigeren. Dit proces helpt bij het opschonen van historische vervuiling en het verbeteren van compliance met regelgeving zoals de AVG/GDPR.

✓ Nu beschikbaar!

Toxic Policies

Voorkom conflicterende rechten

De Toxic Policies-functionaliteit in HelloID helpt conflicterende toegangsrechten binnen je organisatie te identificeren en te verwijderen. Door specifieke regels in te stellen, voorkom je dat gebruikers rechten krijgen die niet gecombineerd mogen worden, zoals dubbele licenties of functies die fraude kunnen faciliteren. Dit verhoogt de beveiliging en voorkomt onnodige licentiekosten.

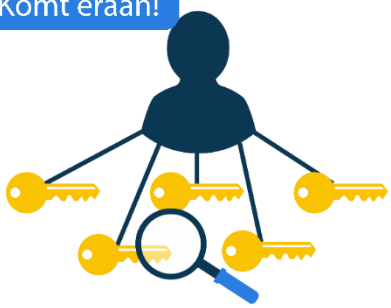
Komt eraan!

Role Mining

Snel een klantgericht autorisatiemodel

Met role mining krijg je snel aanbevelingen voor het opzetten of aanpassen van een autorisatiemodel. Door patroonherkenning van bestaande autorisaties binnen een doelsysteem helpt HelloID je om een model te creëren dat optimaal aansluit bij de behoeften van de organisatie.

Komt eraan!



Advanced Role Model

Hou de controle over je autorisatiemodel

Op basis van patroonherkenning en eerder genomen beslissingen krijg je advies voor het beheer en de optimalisatie van je autorisatiemodel. Dit helpt je om de controle te behouden en verbeteringen door te voeren waar nodig.

Service Automation & Governance

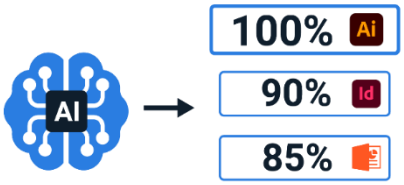
✓ Nu beschikbaar!

Recertification

Valideer self-service producten met periodieke controles

De recertificatie functie binnen HelloID Governance stelt organisaties in staat om periodiek te controleren of gebruikers nog over de juiste self-service producten en toegangsrechten beschikken. Dit proces, ook wel hercertificatie genoemd, helpt voorkomen dat gebruikers onnodige of ongewenste rechten behouden, wat de beveiliging en compliance van de organisatie versterkt.

Komt eraan!



Product Suggestions

AI-aanbevelingen voor efficiëntere workflows

Krijg suggesties op basis van organisatiepatronen om het aanvraagproces te vereenvoudigen, te optimaliseren en beter af te stemmen op de behoeften van gebruikers binnen de organisatie. Door deze aanbevelingen kun je sneller beslissingen nemen en wordt het hele proces efficiënter.

Komt eraan!

Advanced Workflows

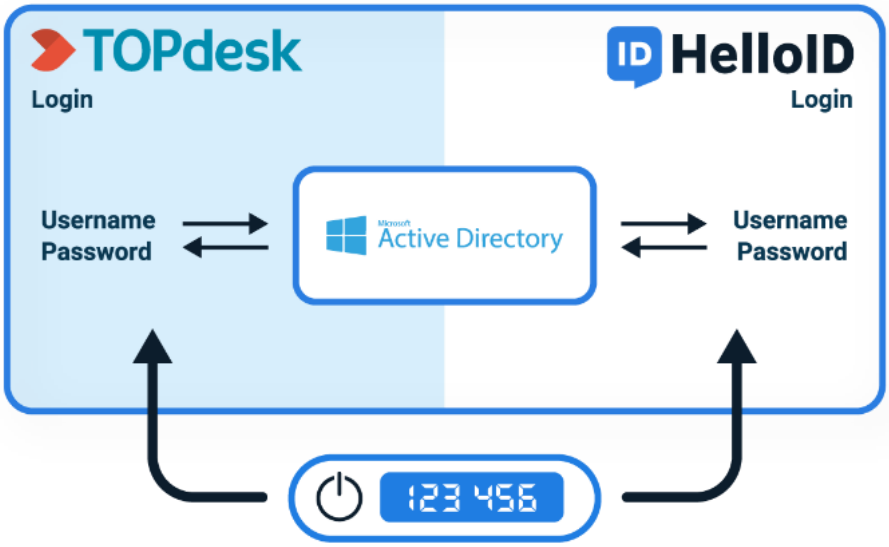
Breid je goedkeuringsproces uit

Met geavanceerde goedkeuringsworkflows krijg je extra opties om het goedkeuringsproces verder aan te passen. Dit kan bijvoorbeeld door een vestigingsmanager te betrekken bij de goedkeuring, zodat deze beter aansluit op de behoeften van de organisatie.

Access Management

Eenvoudige, uniforme, en veilige toegang tot webapplicaties.

Access Management biedt medewerkers, partners en klanten van een organisatie eenvoudig en uniform toegang tot de cloudapplicaties. Authenticatie vindt plaats via een gebruikersnaam met wachtwoord en een two-factor (2FA) naar keuze. De gebruiker krijgt toegang tot een gebruiksvriendelijk dashboard op de laptop, tablet of smartphone. Dat dashboard toont via herkenbare iconen de cloudapplicaties die met één muisklik worden geopend. De eindgebruiker hoeft in een sessie maar een keer in te loggen. HelloID ondersteunt alle gangbare Single Sign-On (SSO) protocollen om gebruikers per cloudapplicatie automatisch te authentiseren. De gebruiker doorloopt hiermee drie onderdelen van HelloID Access Management: 1) de medewerker moet bewijzen dat hij de persoon is die hij claimt te zijn (**Authenticatie**); 2) de gebruiker krijgt een overzicht van de applicaties waar hij toegangsrechten voor heeft (**Dashboard**); 3) de gebruiker kiest een applicatie en komt zonder tussenstap direct in de doelapplicatie, zonder hiervoor opnieuw te hoeven in te loggen (**Single Sign-On**).



Authenticatie

Inloggen van een gebruiker op HelloID gaat in veel gevallen via de Active Directory. HelloID ondersteunt ook andere Identity Providers zoals Azure, Google, SAML, Salesforce en OpenID. Ook kan gebruik worden gemaakt van de login van de lokale HelloID-directory. Deze lokale directory kan gebruikt worden om toegang voor bijvoorbeeld klanten of patiënten van de organisatie te beheren zónder hiervoor deze

gebruikers aan te maken in de Active Directory of een andere Identity Provider. HelloID biedt daarbij 3rd party 2FA-technologie en is kostentechnisch zeer concurrerend (bijvoorbeeld t.o.v. Azure P1). Naast soft of hard tokens en SMS worden ook verschillende one time passwords (OTP's) als tweede factor ondersteund. Afhankelijk van de behoefte van de organisatie biedt HelloID uiteenlopende integratiemogelijkheden.

Dashboard

Na succesvol inloggen krijgen eindgebruikers toegang tot een onlinedashboard. Via iconen heeft de gebruiker direct toegang tot de gekoppelde cloudapplicaties. Welke cloudapplicaties getoond worden is afhankelijk van de rechten van de gebruiker binnen de organisatie. Medewerkers kunnen op basis van hun afdeling, functie, locatie, etc. aan een bepaalde groep binnen HelloID worden gekoppeld. Iedere groep is geautoriseerd voor bepaalde applicaties. Op die manier heeft de beheerder controle over wie toegang krijgt tot welke cloudapplicatie.

Door de integratie met bijvoorbeeld Active Directory (AD) kan de plaatsing van gebruikers in groepen worden gesynchroniseerd met de groepen in de Active Directory. Dit scheelt de beheerders veel werk. Zo bepaalt het lidmaatschap van een bepaalde AD-groep bijvoorbeeld of een medewerker toegang krijgt tot een cloudapplicatie en of daarvoor een 2FA is vereist. Zonder extra beheerhandelingen op HelloID.

De lay-out van het dashboard is verder volledig af te stemmen op de specifieke wensen van de organisatie. Naast een standaardopmaak biedt HelloID mogelijkheden om eigen stylesheets, CSS-koppelingen of links te integreren. Door de end user API is het dashboard eenvoudig te integreren in socialintranettoepassingen als TripTic, Embrace, Google Sites of SharePoint Online.

Single Sign-On (SSO)

Zodra de gebruiker is geauthentiseerd op het HelloID-dashboard is het mogelijk de authenticatie tot andere applicaties automatisch te laten verlopen. Op het HelloID-dashboard heeft de gebruiker een overzicht van beschikbare cloudapplicaties. De authenticatie op de applicatie verloopt via het centrale HelloID-managementportal. Hierbij is het voor de eindgebruiker niet nodig nogmaals in te loggen op de geselecteerde applicatie. Het HelloID-portal onthoudt de gebruiker en verifieert de identiteit van de gebruiker automatisch op het andere systeem (automated login).

Om deze Single Sign-On (SSO) automatisch mogelijk te maken voor de verschillende applicaties ondersteunt HelloID alle bestaande SSO-protocollen zoals: SAML, WS-Fed, HTTP(S) Post, OpenID Connect (OIDC), Basic Authentication, etc.

Over Tools4ever

Tools4ever is een Nederlands softwarebedrijf. We ontwikkelen innovatieve en gestandaardiseerde Identity as a Service (IDaaS)-oplossingen. De hedendaagse IDaaS-oplossingen zijn complex, daarom hebben wij onszelf toegelegd op het ontwikkelen en leveren van IDaaS-oplossingen die eenvoudig te implementeren en beheren zijn. Van 2013 tot en met 2020 hebben we maximaal geïnvesteerd om deze doelstelling te realiseren. HelloID is van scratch opgebouwd waarbij gebruikgemaakt wordt van de modernste softwaretechnieken. De eerste release van HelloID is begin 2020 met veel enthousiasme ontvangen. HelloID is een mooi product waar onze gebruikers blij van worden. We voelen ons verplicht om voor een eerlijke vergoeding, excellente service te verlenen, en te blijven investeren in verdere ontwikkeling van HelloID.

Tools4ever BV
Amalialaan 126C
3743 KJ Baarn
Nederland

Website: tools4ever.nl
Informatie: info@tools4ever.com
Sales: sales@tools4ever.com
Telefoon: +31 (0) 35 54 832 55