L’identité comme un Service

(IDaaS)

Les trois meilleures idées sur :

- Automatisation des comptes et des permissions
- Self-service pour les collaborateurs et les managers
- Contrôle de conformité continu grâce à l'IA

TOOLS4EVER

Sommaire

Introduction

Les logiciels de gestion des identités et des accès (IAM) jouent depuis longtemps un rôle clé dans les environnements informatiques. L'identification, l'authentification et l'autorisation garantissent que les utilisateurs ont le bon accès au bon moment. Mais le rôle de la gestion des identités évolue. Ces changements sont dus à la croissance des services cloud, à la nouvelle réglementation des données, à l'automatisation croissante et au travail à distance. Ci-dessous, nous décrivons ces tendances.

Tendances

Les organisations font la transition vers le cloud. L'infrastructure traditionnelle comme Exchange, Active Directory et le stockage local est en cours de migration vers Entra ID, O365. Les systèmes RH et autres applications métier sont généralement les premiers à migrer. Les entreprises ne maintiennent leurs centres de données existants que jusqu'à la fin de la période d'amortissement.

Les données deviennent de plus en plus précieuses, mais aussi plus réglementées.
Les informations sur les produits, les clients et les employés sont plus importantes que jamais. Un accès rapide, complet et correct est essentiel. Dans le même temps, des lois et réglementations strictes (par exemple, la RGPD) imposent des changements coûteux et de grande envergure. Les organisations doivent éviter les audits non souhaités, la publicité négative et les éventuelles amendes.

L'automatisation et l'augmentation de l'efficacité sont aujourd'hui des priorités absolues. Mais des goulots d'étranglement persistent dans le cycle de vie de l'utilisateur. Les entreprises réduisent les inefficacités et automatisent les flux de travail manuels dans la mesure du possible, mais les équipes de gestion les plus intelligentes ont trouvé une piste d'amélioration supplémentaire : la rationalisation du processus de création de compte utilisateur et de gestion des d'accès.

Conséquences

La gestion des identités et des accès (IAM) est encore généralement assurée par des solutions sur site (on-premises). Dans quelques années, les organisations ne disposeront plus d'infrastructure locale.
La solution de gestion des identités et des accès devra donc être disponible sous forme de service (as a Service). Ce type de systèmes est appelé « Identity as a Service » (IDaaS).

Les mesures de sécurité et de conformité d'audit doivent être mises en œuvre au niveau le plus bas. Il y a cinq ans, des procédures semi-automatisées et quelques scripts suffisaient pour être conforme. Les comptes et les mots de passe partagés étaient encore courants, mais plus maintenant. La direction, les conseils d'administration et les responsables de la sécurité réalisent les avantages liés à la sécurité et à la conformité des solutions professionnelles IDaaS.

Les solutions IDaaS incluent désormais le provisionning des comptes utilisateurs.
Dans le passé, les RH ou les chefs de service soumettaient des tickets de support relatifs aux nouvelles arrivées/mobilités/départ et le service informatique créait/modifiait ou désactivait les comptes à la main.
Aujourd'hui, les solutions IDaaS surveillent automatiquement les données de la RH et propagent les changements nécessaires sur tous les systèmes cibles en limitant significativement les actions manuelles.

Tendances	Conséquences
Le télétravail a fait exploser les anciens périmètres du réseau. Les collaborateurs ont besoin d'accéder à leurs applications et données à tout moment, avec n'importe quel dispositif et depuis n'importe quel endroit. Cela crée à la fois de nouveaux risques mais aussi de nouvelles opportunités.	**Les modèles « Zéro Trust Security »**, ancrés dans la gestion des identités, sont l'avenir. Les procédures de fourniture de droits d'accès sont renforcées et appliquées à chaque étape de manière transparente. La vieille menace de « rupture de périmètre » est atténuée. Grâce à IDaaS, toutes les ressources sont fournies en toute sécurité et à temps. L'accès aux applications d'authentification unique (SSO), associé à l'authentification multifacteur (MFA) en est la première étape.
Les anciens systèmes IAM « boîte noire » sont devenus inacceptables. Chaque année, la maintenance des logiciels traditionnels de gestion des identités on-premises devient plus difficile et plus coûteuse. Peu de personnes dans l'organisation les comprennent et encore moins peuvent les gérer. Les consultants spécialisés sont lents, rares et onéreux.	**Les organisations ont besoin de solutions IDaaS** développées activement et maintenues par des experts. Un logiciel moderne permet une adaptation rapide aux changements du marché et de l'organisation. Les équipes de développement sont plus réactives aux demandes de fonctionnalités des clients. Un support d'experts est fourni en interne, avec des structures de coûts transparentes et prévisibles

Avec HelloID - Solution d'identité en tant que service (IDaaS) de Tools4ever, nous sommes en avance sur ces développements importants. HelloID est une application cloud native à part entière. Elle automatise l'ensemble du cycle de vie des identités de votre organisation. Vos utilisateurs bénéficient d'un accès simple et sécurisé à leurs services informatiques. Vous êtes soulagés du fardeau de maintenir une infrastructure de stockage, de matériel et de logiciels locaux coûteux.

L'installation et la configuration sont effectuées en quelques jours. Vous décidez qui gérera la solution : Tools4ever, en interne, ou via un prestataire habituel que vous aurez choisi et que nous formerons gratuitement.

Avec HelloID, il n'y a pas de compromis entre économies de coûts et sécurité. Les auditeurs informatiques félicitent fréquemment nos clients pour leurs excellentes évaluations de conformité. Toutes les instances HelloID s'exécutent dans un environnement Azure à sécurité maximale, qui est soigneusement audité/vérifié par Deloitte Risk Services tous les six mois. La conformité de la sécurité est garantie également au travers de notre certification ISO27001.

HelloID ne vous oblige pas à un scénario d'adoption « big bang » avec de gros risques et de fortes pressions. HelloID est divisé en modules et le déploiement se déroule par étapes. Vous êtes libre de commencer avec le ou les modules de votre choix.

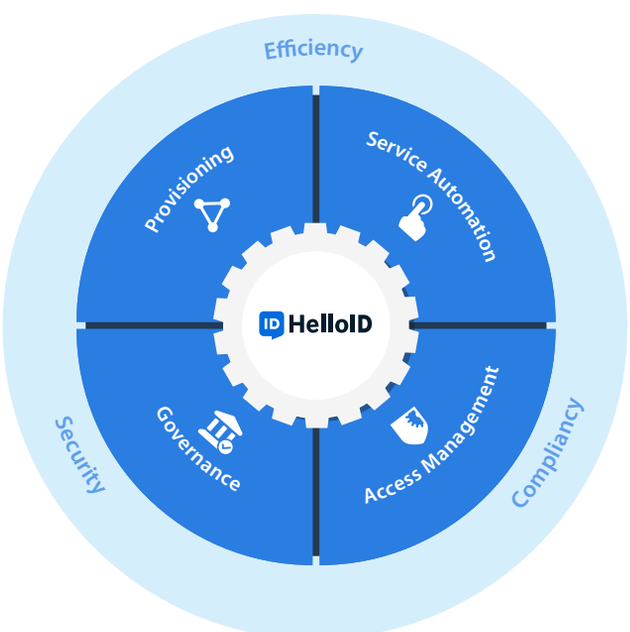
HelloID comprend les modules suivants :

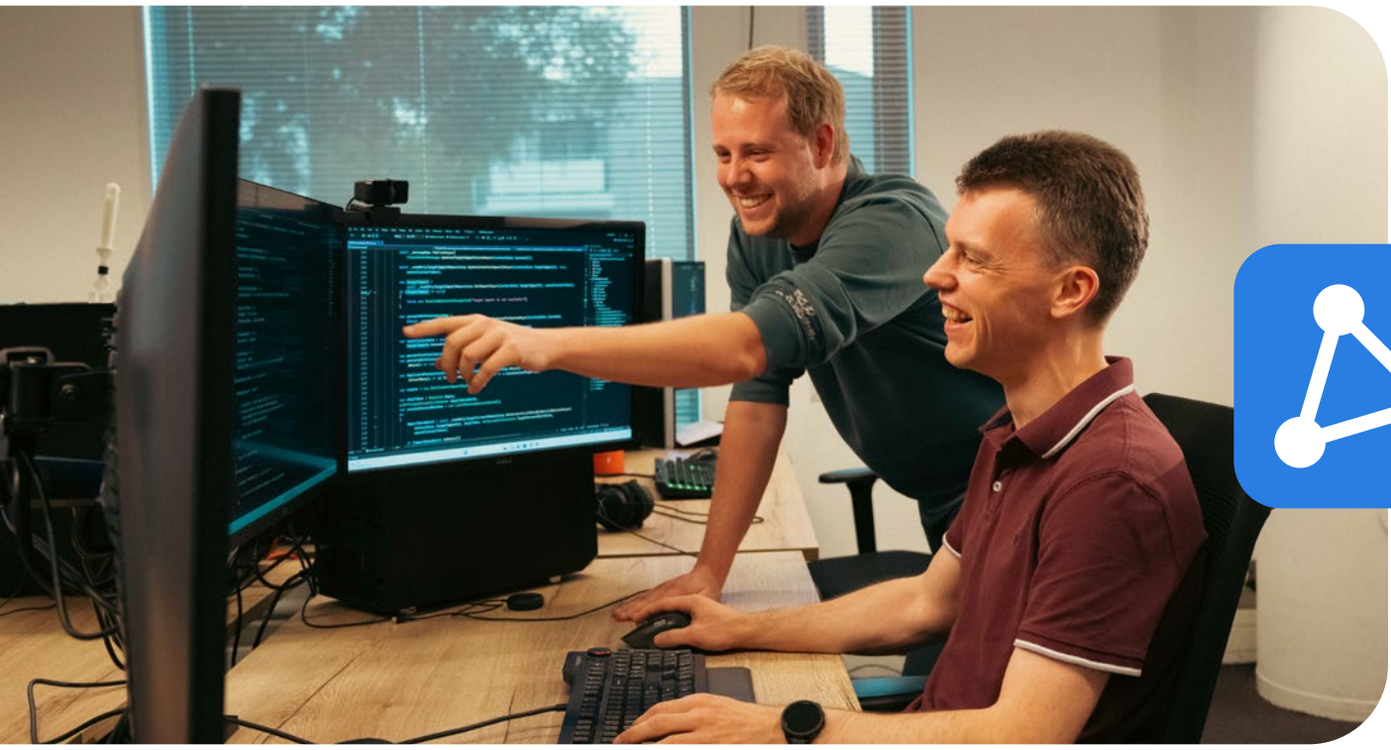
1. Provisioning crée, gère et supprime automatiquement les comptes utilisateurs dans un nombre illimité de systèmes cibles, en fonction des informations sources de votre système RH. Il attribue automatiquement des droits, des autorisations et d'autres ressources en fonction du contexte. Le terme générique que nous utilisions est « droits ». Chaque fois que le contexte d'un utilisateur est modifié, ses droits sont ajustés en conséquence. Par exemple, lorsqu'une personne quitte l'organisation, tous ses droits sont automatiquement révoqués, y compris ses comptes. Cela se produit sans aucune intervention manuelle.

2. Service Automation se connecte de manière transparente avec Provisioning. Inévitablement, il y a des demandes ponctuelles qui ne peuvent pas être anticipées dans les règles métier du Provisioning. Par exemple, un utilisateur a temporairement besoin d'une application spécifique ou d'un partage de fichiers. L'automatisation des services comble cette lacune. Les employés et les responsables remplissent simplement un formulaire Web et HelloID s'occupe du reste. La prise en charge complète de PowerShell permet à chaque tâche d'être automatisée dans toute la mesure du possible. Les modifications sont effectuées directement dans le réseau, sans intervention du personnel informatique.

3. Governance ajoute des fonctionnalités supplémentaires au Provisioning et au Service Automation. Alors que ces modules constituent la base d'une gestion des accès efficace et sécurisée, le module de gouvernance va encore plus loin. La gouvernance est une solution qui aide les organisations à contrôler en permanence les comptes utilisateurs et les droits d'accès. Elle vous permet de les évaluer périodiquement, de détecter et de corriger les anomalies, ce qui vous donne encore plus de contrôle sur la gestion des accès et la conformité.

4. Access Management gère l'accès sécurisé et convivial des employés aux différentes applications et données. Les utilisateurs peuvent s'authentifier via un identifiant, un mot de passe et une authentification multifactorielle. Après l'accès, HelloID offre un tableau de bord convivial dans lequel les utilisateurs peuvent facilement ouvrir leurs applications. Grâce à la fonctionnalité étendue d'authentification unique, un seul clic suffit.





Provisioning

Connectez les systèmes source et cible pour une gestion automatisée des utilisateurs et de leurs autorisations.

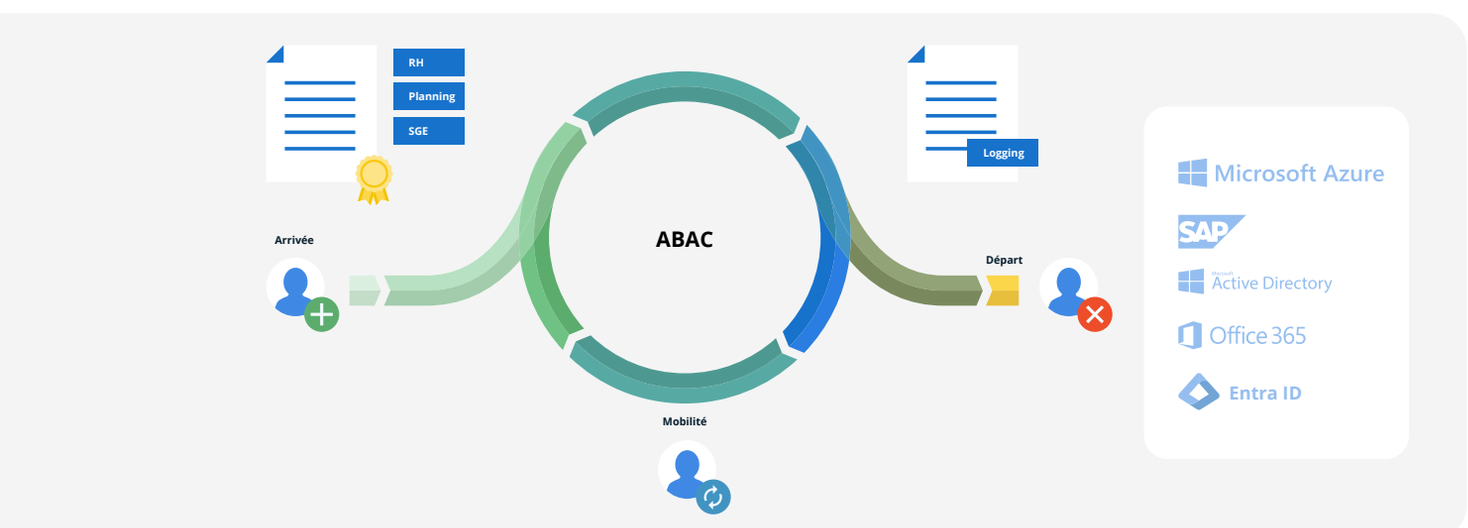
Gestion du cycle de vie des identités

En tant qu'organisation, vous devez gérer un grand nombre de comptes utilisateurs. Ceux des collaborateurs permanents, des intérimaires et aussi ceux des prestataires externes. Cela signifie que des comptes utilisateurs doivent être créés, modifiées et/ou supprimés régulièrement. Les droits, les applications et les autres ressources d'une personne dépendent généralement de son rôle, de son service, de son lieu de travail, etc. Et lorsque ces éléments changent, les droits d'accès doivent généralement être modifiés. HelloID Provisioning assure la création, la modification et la suppression des comptes de manière entièrement automatisées. Nous automatisons ainsi l'ensemble du processus d'entrée, de mobilité et de départ. Grâce au provisioning automatique, vous rendez vos collaborateurs plus productifs, vous économisez sur les tâches routinières et les licences coûteuses et vous renforcez votre sécurité informatique.

Grâce à HelloID, dès son premier jour de travail, un nouveau collaborateur dispose d'un compte utilisateur avec les droits d'accès correspondants et les logiciels nécessaires à son activité. Lorsqu'un collaborateur change de fonction et/ou de service au fil du temps, le processus de transfert HelloID veille à ce que ses droits et licences soient automatiquement modifiés. Et si un collaborateur quitte l'entreprise, HelloID peut alors veiller à ce que son compte soit immédiatement neutralisé. Il est également possible de mettre en place un transfert et une absence du bureau sur la boîte mail et d'envoyer un e-mail au responsable pour lui indiquer le matériel à restituer. Toutes les actions manuelles précédentes sont désormais automatisées via HelloID.

Le provisioning simplifie, accélère et sécurise la gestion des comptes utilisateurs. Ces gestes ne se font plus de manière manuelle, complexe et chronophage par les équipes RH et informatiques. Il permet aux collaborateurs d'être plus productifs, car ils disposent toujours immédiatement des ressources dont ils ont besoin. Outre la commodité et l'efficacité, le provisioning automatique offre également un outil de sécurité supplémentaire puissant. Dans de nombreuses entreprises, les employés accumulent souvent, même involontairement, de plus en plus de droits et de fonctionnalités. Il n'existe généralement pas de processus automatique permettant de révoquer les droits lorsqu'une personne n'en a plus besoin. Il arrive souvent que d'anciens collaborateurs et même prestataires externes conservent l'accès aux systèmes, avec tous les risques que cela comporte.

Le provisionnement automatique garantit que chaque personne dispose uniquement des droits nécessaires à l'exercice de ses fonctions. En cas de changement de fonction ou de service, les droits et licences sont retirés, éventuellement avec une période de grâce. Ce retrait automatique des droits et des ressources se traduit également par un avantage financier immédiat. De nombreuses entreprises engagent des dépenses inutiles pour des licences et des services coûteux qui ne sont plus utilisés, mais qui sont facturées chaque mois. HelloID permet de mieux maitriser ces coûts.

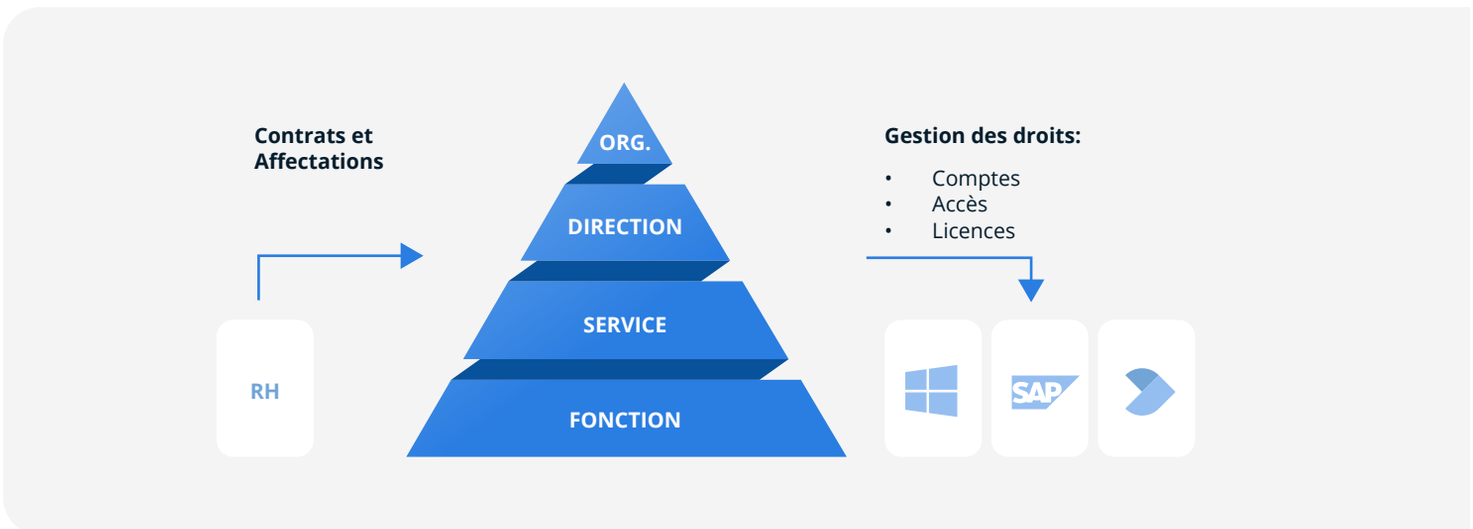


Attribute Based Access Control (ABAC)

HelloID Provisioning utilise la méthodologie de contrôle d'accès basé sur les attributs. L'ABAC fournit une manière structurée et progressive de créer des règles métier.
Celles-ci pilotent le processus de provisioning.
À l'aide des règles de gestion, une « matrice » est créée. Elle fait des références croisées entre les attributs de contexte et les droits nécessaires. Les attributs peuvent inclure des fonctions, des contrats, des services ou tout autre facteur pertinent.
Chaque attribut est mis en correspondance avec ses droits associés. Ensuite, les attributs sont « empilés » du bas vers le haut pour mettre en place des profils organisationnels.
La plupart du temps, ce travail peut être effectuée avant le déploiement du Provisioning. Cela catapulte immédiatement la matrice ABAC à environ 80% de résultat. Les 20% restants (règles détaillées) sont remplies au fil du temps. De cette manière, vous pouvez implémenter le provisioning avec une approche par étapes. Vous transformez progressivement le processus actuel de votre organisation en une automatisation complète du cycle de vie, sans avoir à planifier chaque détail à l'avance.

L'approche ABAC est une amélioration majeure par rapport aux méthodologies de provisioning traditionnelles. Par exemple, la cartographie manuelle non structurée est extrêmement complexe et prend du temps. Paradoxalement l'approche « modèle basée sur un utilisateur » du genre « Bernard fera le même travail que Nathalie » est trop simple.

Auparavant, l'ABAC n'était utilisé que pour les grandes institutions financières et les sociétés internationales. Mais il s'est démocratisé ces dernières années en raison de nouvelles lois et réglementations (par exemple, le RGPD, FISMA, HIPAA, SOX, NIS, NIS2). C'est désormais une pratique courante, voire obligatoire, pour les établissements de santé, les entreprises de taille moyenne (300 à 5000 salariés) et autres organisations privées.



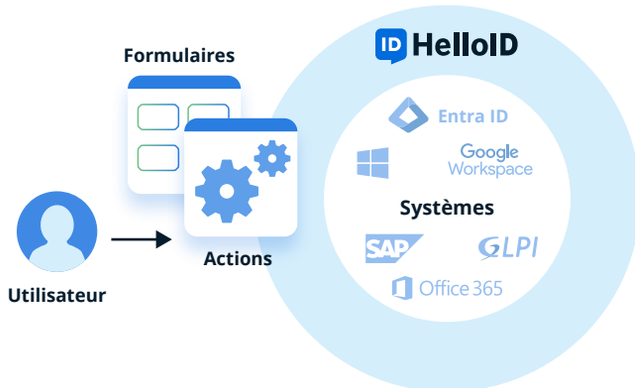
Service Automation

Rationalisez le processus de demande grâce à la délégation au service support, au libre-service et aux workflows.

Le processus de provisioning automatise pratiquement toutes les modifications liées à l'informatique. Il existe toutefois des exceptions, car tout n'est pas enregistré dans le système RH. Prenons l'exemple d'un collaborateur qui remplace temporairement un collègue malade, ou d'un employé affecté à un projet ou détaché dans un autre service. Pour accomplir ces tâches supplémentaires, le collaborateur a besoin, par exemple, de droits d'accès supplémentaires aux dossiers, de droits supplémentaires pour pouvoir effectuer des tâches dans SAP, d'une licence Microsoft Project, d'une adhésion à une liste de distribution, d'une adhésion à un canal Microsoft Teams, etc.

Dans de nombreuses entreprises, ce type de modifications est traité manuellement par le service d'assistance informatique ou la gestion fonctionnelle, ce qui rend le processus coûteux et fastidieux.

Service Automation automatise donc ces modifications. Grâce à une simple interface web, les collaborateurs sans connaissances informatiques ni aucun droit d'administration sur les systèmes, peuvent eux-mêmes apporter des modifications au réseau en toute sécurité. Cela se fait via une couche déléguée et toutes les modifications sont effectuées dans le réseau via des scénarios définis dans le moteur HelloID. Toutes ces actions sont exécutées avec régularité, précision, et bien sûr avec un journal d'audit complet.



Le module Service Automation offre les avantages suivants :

- Les utilisateurs peuvent apporter eux-mêmes des modifications prédéfinies dans le réseau, de manière sûre et contrôlée. Le Helpdesk est libéré de tâches à faible valeur ajoutée.
- Les changements se produisent immédiatement, car aucune file d'attente de tickets n'est impliquée.
- Les responsables ont un aperçu immédiat des ressources allouée à leurs collaborateurs, y compris les licences et les coûts. Des modifications directes peuvent être apportées si besoin.
- Des limites de temps de procession empêchent l'accumulation indésirable de droits et de licences.
- L'organisation projette une image moderne et professionnelle, notamment auprès des nouveaux collaborateurs.
- Les plates-formes ITSM telles que ServiceNow, GLPI ou EasyVista sont intégrées de manière transparente. Cela augmente l'adhésion des utilisateurs finaux au service en réduisant le nombre de portails séparés que les utilisateurs doivent apprendre à utiliser.

Délégation auprès des utilisateurs finaux

Le Service Automation peut avoir un impact organisationnel considérable. Elle confère ainsi aux collaborateurs et aux managers un rôle différent et plus important dans la distribution des équipements informatiques. Afin de faciliter au maximum la mise en œuvre, la Service Automation peut être introduite progressivement. Les étapes suivantes peuvent être suivies :

Délégation auprès du service d'assistance (Helpdesk)

La première étape consiste à déléguer les tâches des spécialistes système au personnel du service desk. Cela produit immédiatement un gain en efficacité. Le personnel du service desk non ou semi-technique prend en charge des tâches qui n'étaient auparavant possibles que pour les spécialistes système. La clé de cette approche est qu'aucun droit d'administrateur n'est requis. Les formulaires délégués garantissent que seules les tâches spécifiquement autorisées sont disponibles. Par exemple, un formulaire délégué peut réinitialiser les mots de passe Active Directory, attribuer des appartenances à des groupes ou exécuter toute tâche PowerShell personnalisée sur le réseau. Aucune connaissance informatique ou applicative n'est requise et chaque changement est enregistré dans des journaux détaillés.

Délégation auprès des managers

La deuxième étape consiste à déléguer davantage les formulaires mise à disposition lors de l'étape (1). Cette fois, les formulaires éligibles sont délégués du Service Desk aux gestionnaires. Il s'agit d'une étape simple, car à ce stade, les formulaires ont déjà été créés.

C'est à cette étape que davantage d'utilisateurs entrent en contact direct avec HelloID. Les managers ont désormais un aperçu immédiat des droits de leurs collaborateurs.

Ils peuvent apporter des modifications immédiates sans impliquer le personnel informatique. Les processus de ticket encombrants sont totalement éliminés.

La dernière étape consiste à déléguer les formulaires éligibles des gestionnaires aux utilisateurs finaux eux-mêmes. Les utilisateurs finaux sont autorisés à demander directement les ressources nécessaires à leur activité, telles que des applications logicielles spécifiques.

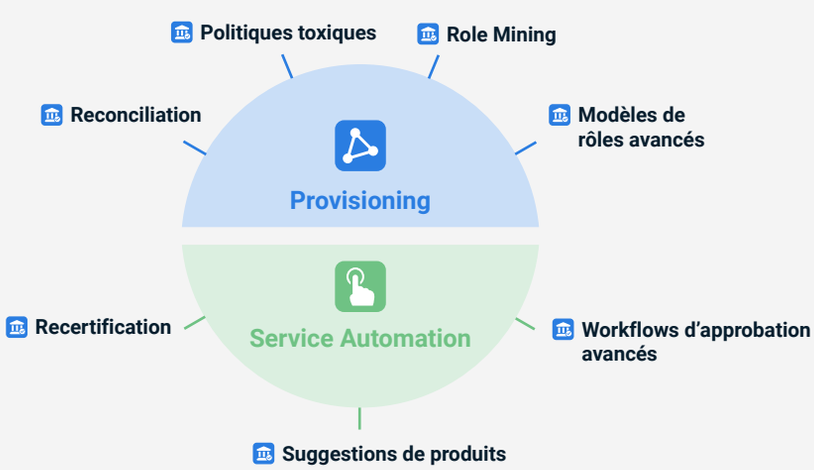
Lorsqu'un utilisateur soumet une demande via un formulaire, son responsable est averti et peut approuver ou refuser la demande. Cette vérification est beaucoup plus facile pour le responsable direct ou le gestionnaire de licence d'un utilisateur que pour un agent du service informatique. C'est l'avantage du modèle de délégation descendante. Après approbation, le module Service Automation livre automatiquement le produit s'il s'agit d'un article numérique. Si le produit est un article physique, les notifications nécessaires sont envoyées via l'outil d'ITSM (EasyVista, GLPI, JIRA, ServiceNow etc.)

Les managers ont désormais un aperçu immédiat des droits de leurs collaborateurs. Ils peuvent apporter des modifications immédiates sans impliquer le personnel informatique.

Governance

La maîtrise grâce à une visibilité continue sur le respect des politiques et la détection des anomalies.

HelloID Governance étend d'avantage les fonctionnalités de Provisioning et Service Automation. Alors que ces modules constituent la base d'une gestion des accès efficace et sécurisée, le module Governance va encore plus loin. Il vous aide non seulement à prendre le contrôle, mais aussi à le conserver.
En tant qu'organisation, il est en effet essentiel d'avoir en permanence une vue d'ensemble et un contrôle sur les droits d'accès des utilisateurs, tels que les employés internes, les intérimaires, les partenaires externes etc. Sans une gestion efficace, il existe un risque que des personnes non autorisées aient accès à des informations sensibles. Cela peut entraîner des fuites de données et d'autres incidents de sécurité. En outre, la gouvernance (via le module Governance) vous aide à vous conformer aux lois et réglementations, telles que le RGPD, NIS, NIS2, la norme ISO 27001, ce qui limite les risques et prépare votre organisation à l'audit.



Le module Governance offre les avantages suivants :

- **Empêcher tout accès non autorisé** : identifier et supprimer les droits indésirables afin de renforcer votre sécurité.
- **Surveiller en continue des droits d'accès** : détecter les anomalies, les corriger et adapter en permanence les droits d'accès à la situation actuelle.
- **Obtenir des recommandations intelligentes basées sur l'IA** : réduction de la charge de travail grâce à des suggestions proactives et des points d'amélioration pour la matrice d'autorisation et les produits en libre-service.
- **Optimiser le processus d'audit** : la garantie de générer facilement et rapidement des rapports structurés qui répondent à toutes les exigences d'audit.
- **Rester toujours conforme** : respectez les réglementations telles que le RGPD, la norme ISO 27001, le cadre normatif NIS et NIS2, etc.

Que comprend notre module Governance?

HelloID Governance ajoute des fonctionnalités supplémentaires aux modules provisioning et Service Automation, vous permettant d'évaluer en permanence votre politique, d'identifier les écarts et de les résoudre.

Qu'est-ce qui est déjà disponible?

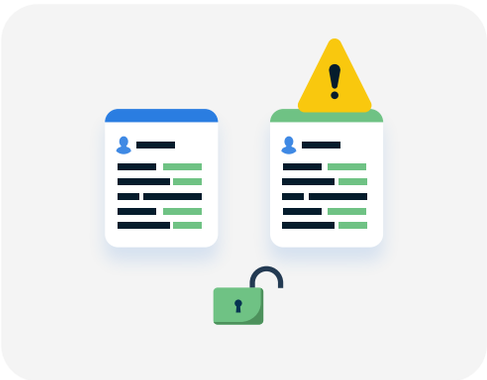
Toutes les fonctionnalités de HelloID Governance ne sont pas encore disponibles, mais nous travaillons d'arrache-pied à leur développement. Nous ajoutons progressivement de nouvelles fonctionnalités afin que vous puissiez bientôt profiter pleinement de ce module.
Vous trouverez ci-dessous les fonctionnalités déjà disponibles :

- Réconciliation
- Recertification
- Politiques Toxiques

Les fonctionnalités suivantes figurent dans notre planning des étapes importantes, mais ne sont pas encore disponibles immédiatement :

- Role Mining
- Modèle de rôles avancés
- Suggestion de produits
- Workflows d’approbation avancés

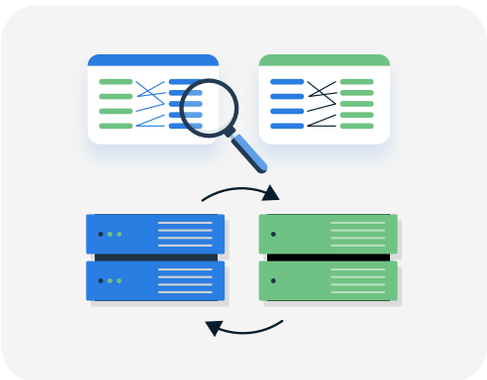
Provisioning et Governance



Réconciliation

Gardez le contrôle sur vos systèmes cible

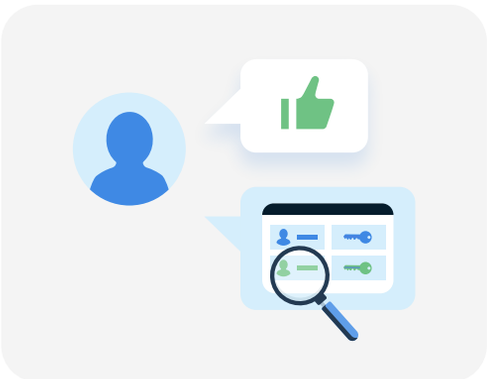
La fonctionnalité de réconciliation de HelloID Governance compare la situation souhaitée (à la situation actuelle dans vos systèmes cibles. Cela vous permet d'identifier les différences, telles que les comptes et les droits d'accès indésirables ou manquants, et de les corriger efficacement. Ce processus aide à nettoyer les données historiques polluées et à améliorer la conformité avec les réglementations telles que le RGPD.



Politiques Toxiques

Évitez les conflits de droits

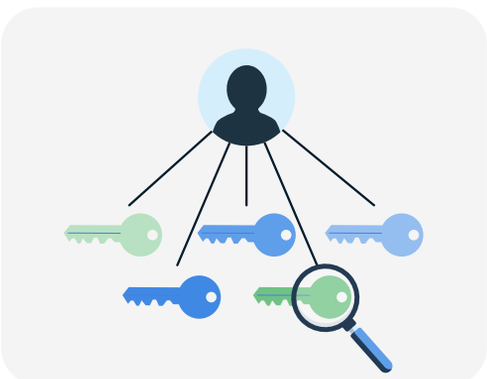
La fonctionnalité « Toxic Policies » de HelloID vous aide à identifier et à supprimer les conflits de droits d'accès au sein de votre organisation. En définissant des règles spécifiques, vous évitez que les utilisateurs obtiennent des droits qui ne peuvent être combinés, tels que des licences doubles ou des fonctions susceptibles de faciliter la fraude. Cela renforce la sécurité et évite des frais de licence inutiles.



Role Mining

Un modèle d'autorisations rapidement orienté client

Le « Role Mining » permet d'obtenir rapidement des recommandations pour la mise en place ou l'adaptation d'un modèle d'autorisation. Grâce à la reconnaissance des modèles d'autorisations existants dans un système cible, HelloID vous aide à créer un modèle qui répond de manière optimale aux besoins de l'organisation.

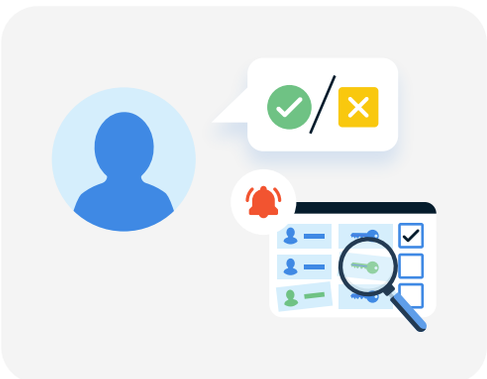


Modèles de rôles avancés

Gardez le contrôle sur votre modèle d'autorisation

Sur la base de la reconnaissance des modèles et des décisions prises précédemment, vous recevez des conseils pour la gestion et l'optimisation de votre modèle d'autorisation. Cela vous aide à garder le contrôle et à apporter des améliorations si nécessaire.

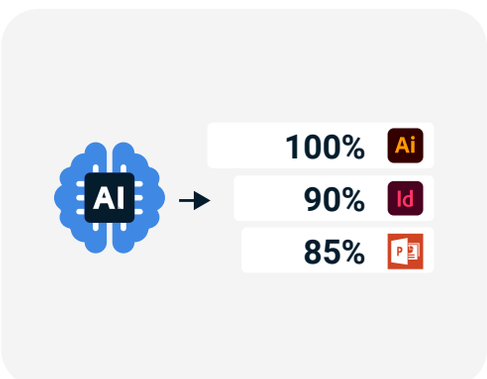
Service Automation et Governance



Recertification

Validez les produits en libre-service grâce à des contrôles périodiques

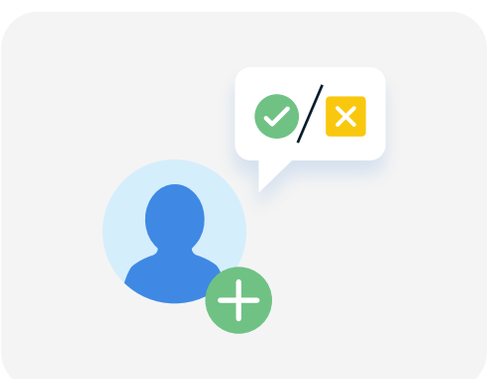
La fonction de recertification du module HelloID Governance permet aux organisations de vérifier périodiquement si les utilisateurs disposent toujours des produits en libre-service et des droits d'accès appropriés. Ce processus, permet d'éviter que les utilisateurs conservent des droits inutiles ou indésirables, ce qui renforce la sécurité et la conformité de l'organisation.



Suggestions de Produits

Recommandations IA pour des workflow plus efficaces

Obtenez des suggestions basées sur les modèles opérationnels afin de simplifier et d'optimiser le processus de demande, et de mieux l'adapter aux besoins des utilisateurs au sein de l'organisation. Ces recommandations vous permettent de prendre des décisions plus rapidement et rendent l'ensemble du processus plus efficace.



Workflows Avancés

Élargissez votre processus d'approbation

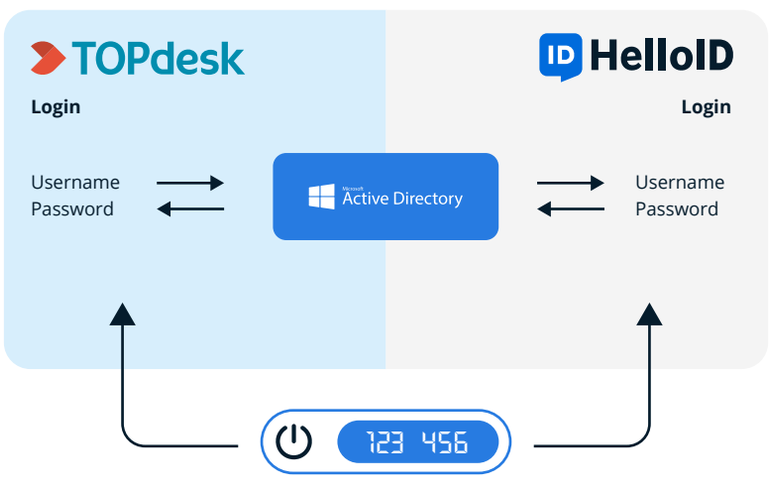
Les workflows d'approbation avancés vous offrent des options supplémentaires pour personnaliser davantage le processus d'approbation. Vous pouvez par exemple impliquer un responsable d'établissement dans le processus d'approbation afin de mieux répondre aux besoins de l'organisation.

Access Management

Accès simple, uniforme et sécurisé aux applications Web.

Le module de gestion des accès, Access Management, offre aux collaborateurs internes, partenaires et clients d'une organisation un accès simple et uniforme aux applications cloud. L'authentification s'effectue à l'aide d'un nom d'utilisateur et d'un mot de passe, ainsi que d'une authentification à deux facteurs (2FA) au choix. L'utilisateur a accès à un tableau de bord convivial sur son ordinateur portable, sa tablette ou son smartphone. Ce tableau de bord affiche, à l'aide d'icônes reconnaissables, les applications cloud qui s'ouvrent d'un simple clic. L'utilisateur final ne doit se connecter qu'une seule fois par session. HelloID prend en charge tous les protocoles Single Sign-On (SSO) courants pour authentifier automatiquement les utilisateurs par application cloud. L'utilisateur passe ainsi par trois étapes de HelloID Access Management :

1. L'utilisateur doit prouver qu'il est bien la personne qu'il prétend être (authentification)
2. L'utilisateur obtient un aperçu des applications auxquelles il a accès (tableau de bord)
3. L'utilisateur choisit une application et accède directement à l'application cible, sans étape intermédiaire et sans avoir à se reconnecter c'est le principe du Single Sign-On.



Authentification

Dans la plupart des cas, la connexion d'un utilisateur à HelloID s'effectue via Active Directory on Entra ID. HelloID prend également en charge d'autres fournisseurs d'identité tels que Google, SAML, Salesforce et OpenID. Il est également possible d'utiliser des comptes locaux d'HelloID. Ces comptes locaux peuvent par exemple, être utilisés pour gérer l'accès des clients ou des personnes externes à l'organisation, sans avoir à créer ces utilisateurs dans Active Directory ou un autre fournisseur d'identité. HelloID propose une technologie 2FA tierce et est très compétitif en termes de coûts (par exemple par rapport à Azure P1). Outre les jetons logiciels ou physiques et les SMS, différents mots de passe à usage unique (OTP) sont également pris en charge comme deuxième facteur. En fonction des besoins de l'organisation, HelloID offre diverses possibilités d'intégration.

Tableau de bord

Une fois connectés, les utilisateurs finaux ont accès à un tableau de bord en ligne. Des icônes leur permettent d'accéder directement aux applications cloud associées. Les applications cloud affichées dépendent des droits de l'utilisateur au sein de l'organisation. Les employés peuvent être associés à un groupe spécifique dans HelloID en fonction de leur service, de leur fonction, de leur emplacement, etc. Chaque groupe est autorisé à utiliser certaines applications. De cette manière, l'administrateur contrôle qui a accès à quelle application cloud.
Grâce à l'intégration avec Active Directory (AD), par exemple, l'affectation des utilisateurs dans des groupes peut être synchronisé avec les groupes dans Active Directory. Cela facilite considérablement le travail des administrateurs. Ainsi, l'appartenance à un certain groupe AD détermine, par exemple, si un employé a accès à une application cloud et si une authentification à deux facteurs (2FA) est requise pour cela. Sans opérations de gestion supplémentaires dans HelloID.

Single Sign-On (SSO)

L'authentification sur l'application s'effectue via le portail de gestion central HelloID. L'utilisateur final n'a donc pas besoin de se reconnecter à l'application sélectionnée. Le portail HelloID mémorise l'utilisateur et vérifie automatiquement son identité sur l'autre système (connexion automatisée).

HelloID prend en charge tous les protocoles SSO existants tels que : SAML, WS-Fed, HTTP(S) Post, OpenID Connect (OIDC), Basic Authentication, etc.

A propos de Tools4ever

Tools4ever est un éditeur de logiciels dont le siège social se trouve aux Pays-Bas. Spécialiste en gestion des identités et des accès depuis 1999, nous développons à présent des solutions d'identité en tant que service (IDaaS) innovantes et standardisées. Les solutions IDaaS actuelles sont complexes, c'est pourquoi nous nous sommes consacrés au développement et à la fourniture de solutions IDaaS faciles à mettre en œuvre et à gérer. De 2013 à 2020, nous avons investi dans ce sens afin d'atteindre cet objectif.

HelloID est construit à partir de zéro en utilisant notre longue expérience et des techniques logicielles de pointe. La première version de HelloID a été reçue avec beaucoup d'enthousiasme début 2020. HelloID est un beau produit qui rend nos utilisateurs heureux. Nous sommes fiers de fournir un excellent service pour un modèle économique équitable et vertueux. Nous continuons à investir massivement dans le développement de HelloID avec une équipe de professionnels qui s'agrandit de jour en jour.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Tools4ever South Europe

Adresse C/ Ramon Turró 169 A
08005 Barcelone
Espagne

Info sesales@tools4ever.com
Support frsupport@tools4ever.com