TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Livre Blanc

Gestion des Identités en tant que Service (IDaaS)

Table des matières

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	Conséquences
Les organisations font la transition vers le cloud. L'infrastructure traditionnelle comme Exchange, Active Directory et le stockage local est en cours de conversion vers Azure, O365 et Teams. Les systèmes RH et autres applications métier sont généralement les premiers systèmes à migrer. Les entreprises ne maintiennent leurs centres de données existants que jusqu'à la fin de la période d'amortissement.	**Les systèmes IAM sur site sont en cours de remplacement par des logiciel IDaaS (Identity as a Service).** Dans quelques années, la plupart des entreprises n'auront plus leur propre infrastructure informatique sur site. Les services cloud offriront une meilleure disponibilité, des coûts inférieurs et des mises à jour transparentes.
Les données deviennent de plus en plus précieuses, mais aussi plus réglementées. Les données sur les produits, les clients et les employés sont plus précieuses 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.	**Les mesures de sécurité et de conformité d'audit doivent être mises en œuvre au niveau le plus bas : L'Identité.** Il y a cinq ans, des procédures semi-automatisées et quelques scripts suffisaient pour se conformer. Les comptes et les mots de passe partagés étaient encore courants. 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.
L'automatisation et l'efficacité sont 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 un avantage supplémentaire : la rationalisation du processus de création de compte utilisateur et de gestion des d'accès.	**Les solutions IDaaS complètes incluent désormais le provisionning des comptes utilisateurs.** Dans le passé, les RH soumettaient des tickets de support pour les nouvelles recrues et le service informatique créait leurs comptes à la main. Aujourd'hui, les solutions IDaaS surveillent automatiquement les données RH et propagent les changements nécessaires sur tous les systèmes cibles. Les comptes utilisateur, adresses e-mail, droits d'accès, licences logicielles et autres ressources sont automatiquement provisionnés sans intervention manuelle.
Le télétravail a fait exploser les anciens périmètres du réseau. Les employés ont besoin d'accéder à leurs applications et données à tout moment, avec n'importe quel appareil et depuis n'importe quel endroit. Cela crée à la fois de nouveaux risques et de nouvelles opportunités.	**Les modèles « Zero Trust Security », ancrés dans la gestion des identités, sont l'avenir.** La 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) est la première étape.
Les anciens systèmes IAM « boîte noire » sont devenus intolérables. Chaque année, la maintenance des logiciels traditionnels de gestion des identités sur site devient plus difficile et plus coûteuse. Peu de personnes dans l'organisation les comprennent et encore moins peuvent les gérer. Les consultants sont lents, rares et chers.	**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 soutien d'experts est fourni en interne, avec des structures de coûts transparentes et prévisibles

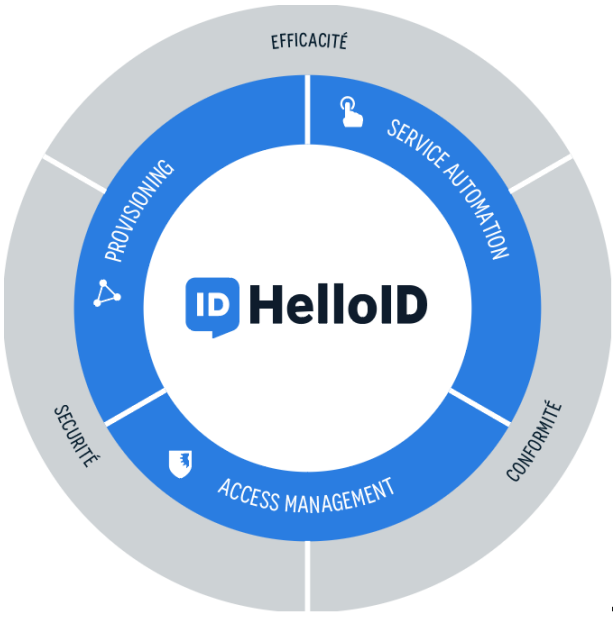
Avec HelloID - Solution d'identité en tant que service (IDaaS) de Tools4ever, nous sommes en avance sur ces développements importants. HelloID est une application cloud native à part entière. Elle automatise l'ensemble du cycle de vie des identités de votre organisation. Vos utilisateurs bénéficient d'un accès simple et sécurisé à leurs services informatiques. Vous êtes soulagé du fardeau de maintenir une infrastructure de stockage, de matériel et de logiciels locaux coûteux. L'installation et la configuration sont effectuées en quelques heures. Vous décidez qui gérera la solution : Tools4ever, l'un de nos partenaires d'implémentation de confiance, ou votre propre organisation.

Avec HelloID, il n'y a pas de compromis entre économies de coûts et de sécurité. En fait, 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 vérifié par Deloitte Risk Services tous les six mois. La conformité de la sécurité est garantie.

De plus, nous vous proposons un chemin de croissance équilibré. HelloID ne vous oblige pas à un scénario d'adoption « big bang » avec de gros risques et de fortes pressions. Au lieu de cela, HelloID est divisé en modules. Le déploiement se déroule par étapes. Vous êtes libre de commencer avec le ou les modules de votre choix. Si nécessaire, les modules actifs peuvent être désactivés sans perturber les autres modules.

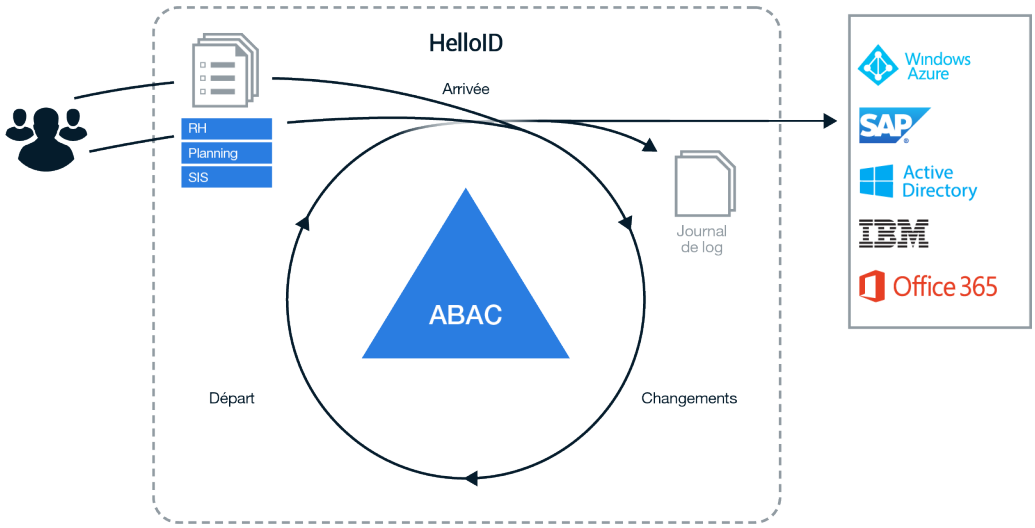
HelloID comprend les modules suivants :

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 utilisons 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 aune 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 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. **Access Management** fournit un accès facile et sécurisé aux applications et aux données. Les utilisateurs s'authentifient via le fournisseur d'identité approprié, généralement associé à une authentification multifacteur. Les applications sont ensuite accessibles via un tableau de bord convivial. La prise en charge complète du protocole d'authentification unique (SSO) signifie que presque toutes les applications sont accessibles en un seul clic.



Provisioning

Les comptes d'utilisateurs doivent être créés, activés, mis à jour et désactivés régulièrement. Cela peut inclure plusieurs types de comptes, y compris des employés permanents et temporaires, des sous-traitants, des prestataires et même des clients. Outre un compte d'annuaire « principal » (généralement Active Directory), chaque utilisateur a besoin de comptes dans d'autres systèmes cibles. Les droits d'accès, les applications et les autres ressources, doivent ensuite être gérés dans tous les systèmes. HelloID Provisioning s'occupe de tout. Il automatise l'ensemble du processus d'entrée, de mobilité interne et de sortie. C'est ce qu'on appelle la « gestion du cycle de vie des identités ».



Avec HelloID, les nouveaux employés reçoivent leurs comptes, leurs droits d'accès et d'autres ressources dès le premier jour. Le travail de routinier de gestion du ou des comptes de l'utilisateur tout au long de son cycle de vie est minimisé. Les droits sont automatiquement modifiés en réponse aux changements de contexte tels que les mobilités, les changements de service, les promotions, etc.

Un employé quitte l'entreprise ? HelloID peut bloquer le compte immédiatement. Des actions de suivi telles que la suppression de boîtes aux lettres et de répertoires personnels peuvent être planifiées pour des semaines ou des mois dans le futur. Vous pouvez même configurer des actions d'anticipation, comme rappeler à un responsable de récupérer l'ordinateur portable d'un employé partant. Cette suppression automatique des droits crée des économies immédiates. L'inventaire des ressources est suivi avec précision et les licences coûteuses sont recyclées. Les abonnements aux logiciels inutilisés peuvent être identifiés et annulés.

Le provisionnement automatique offre de puissants avantages en matière de sécurité. Les employés accumulent souvent progressivement (et involontairement) de plus en plus de droits d'accès. Il n'y a souvent pas de processus structuré pour récupérer les droits inutilisés ou expirés. Les anciens employés peuvent même conserver l'accès aux comptes de l'entreprise, ce qui crée des risques de violation massifs. Avec HelloID, vous pouvez vous assurer que vos utilisateurs ont toujours exactement les droits nécessaires, ni plus, ni moins. Les périodes de grâce garantissent des transitions fluides.

Le provisionning rend la gestion des comptes utilisateur plus facile, plus rapide et plus sécurisée. La gestion des comptes utilisateurs n'est plus une tâche manuelle, complexe et chronophage pour les RH et l'informatique. Les employés deviennent immédiatement plus productifs. Les goulots d'étranglement d'accès appartiennent au passé.

Attribute Based Access Control (ABAC)

HelloID Provisioning utilise la méthodologie de contrôle d'accès basé sur les attributs. ABAC fournit une manière structurée et progressive de créer des règles métier. Celles-ci pilotent le processus de provisionnement.

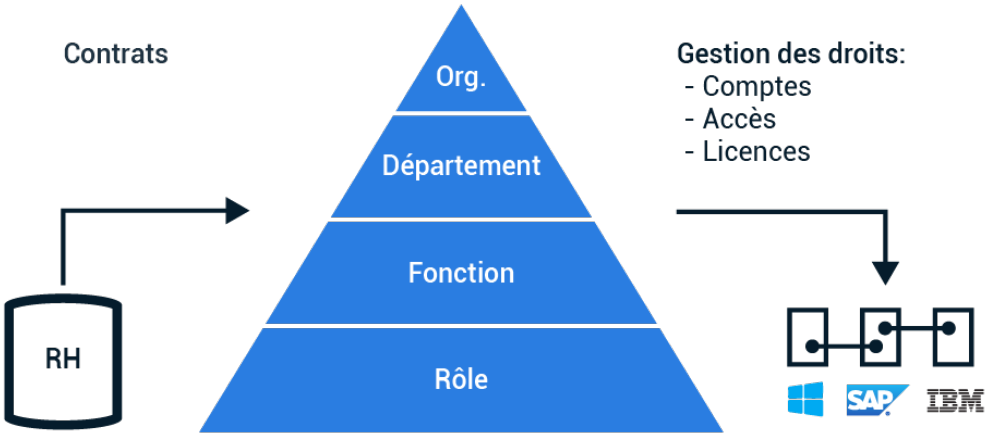
À l'aide des règles de gestion, une « matrice » est créée. Elle fait des références croisées entre les attributs de contexte et les droits nécessaires. Les attributs peuvent inclure des rôles, des contrats, des départements ou tout autre facteur pertinent. Chaque attribut est mis en correspondance avec ses droits correspondants. Ensuite, les attributs sont « empilés » de bas en haut pour développer des profils d'emploi organisationnels.

La part du lion de ce travail peut être effectuée avant le déploiement de Provisioning. Cela catapulte immédiatement la matrice ABAC à environ 80% d'achèvement. Les 20% restants (règles détaillées) sont remplis au fil du temps. De cette manière, vous pouvez implémenter l'approvisionnement avec une approche par étapes. Vous transformez progressivement l'approche actuelle 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 d'approvisionnement traditionnelles. Par exemple, la cartographie manuelle non structurée est extrêmement complexe et prend du temps. Paradoxalement l'approche « modèle basé sur un utilisateur » du genre « Kim fera le même travail que Wendy » est trop simple.

Auparavant, ABAC n'était utilisé que pour les grandes institutions financières et les sociétés internationales. Mais ABAC s'est démocratisé ces dernières années en raison de nouvelles lois et réglementations (par exemple, GDPR, FISMA, HIPAA, SOX, NEN7510). 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 commerciales.

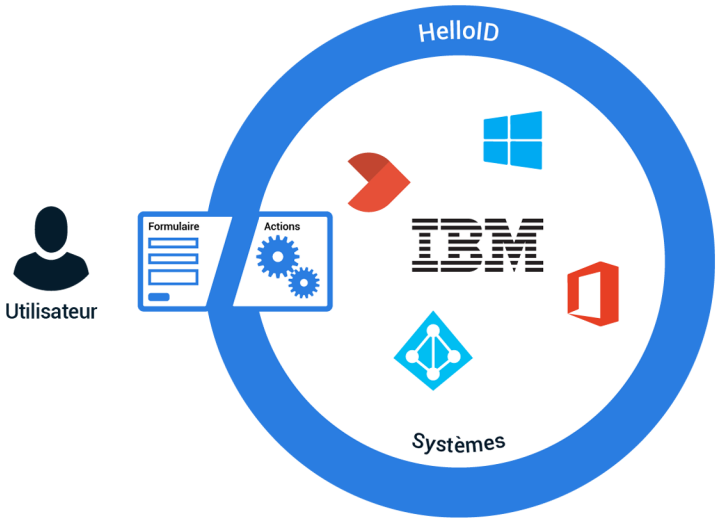
Le diagramme ci-dessous fournit une vue d'ensemble schématique des règles métier HelloID. Les attributs de contexte déterminent les droits nécessaires à chaque niveau - organisation, service, poste et rôle individuel.



Service Automation

Le processus de provisioning automatise presque tous les changements informatiques liés aux utilisateurs. Cependant, il y a toujours des exceptions. De nombreuses fonctions commerciales dépendent de données et de décisions qui ne sont pas enregistrées dans le système source RH de l'entreprise. Pensez à un employé qui remplace temporairement un collègue absent ou à un employé qui collabore avec un autre service. Dans ces cas, les employés auront besoin de droits temporaires. Peut-être auront t'ils besoins de droits dans SAP, d'une application cloud, d'une licence de projet, d'une appartenance à une liste de distribution, d'une appartenance à un site Microsoft Teams, etc.

La plupart des entreprises gèrent ces changements via le center de support informatique ou les gestionnaires fonctionnels. Mais cela coûte cher et prend du temps. Service Automation automatise ces changements. À l'aide de simples formulaires Web appelés « formulaires délégués », les employés sans connaissances informatiques ni droits d'administrateur de domaine peuvent apporter des modifications au réseau en toute sécurité. Cela se produit via un Shell délégué, dans lequel le moteur HelloID exécute des tâches prédéfinies. Ces tâches sont toujours exécutées de la même manière, avec un journal d'audit complet.



Avec HelloID Service Automation :

- Des utilisateurs de confiance peuvent apporter 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 de leurs employés, 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 et EasyVista sont intégrées de manière transparente. Cela augmente l'adhésion des utilisateurs finaux au service en réduisant le nombre de portails séparés que les employés doivent apprendre à utiliser.

Service Automation peut être mise en œuvre étape par étape. À chaque étape, les tâches déléguées éligibles sont poussées « vers le bas ». Chaque demande et décision d'approbation se produit au niveau le plus bas possible.

Délégation au service desk

La première étape consiste à déléguer les tâches des spécialistes système au personnel du centre de services. 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 aux managers

La deuxième étape consiste à déléguer davantage les formulaires développés à 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'employés entrent en contact direct avec HelloID. Les managers ont désormais un aperçu immédiat des droits de leurs employés. Ils peuvent apporter des modifications immédiates sans impliquer le personnel informatique. Les processus de ticket encombrants sont totalement éliminés.

Délégation aux utilisateurs finaux

La dernière étape consiste à déléguer les formulaires éligibles des gestionnaires aux utilisateurs finaux eux-mêmes. Une condition préalable importante pour cette étape est l'intégration des portails en libre-service existants, tels que EasyVista ou tout autre système ITSM. Les utilisateurs finaux sont autorisés à demander directement les ressources nécessaires à leur travail, 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 employé 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.

Access Management

Le module de gestion des accès de HelloID offre à vos employés, partenaires et clients un accès simple et uniforme aux applications cloud. L'authentification s'effectue via une combinaison nom d'utilisateur / mot de passe et une méthode à deux facteurs (2FA) de votre choix.

Les utilisateurs peuvent accéder au tableau de bord de l'application HelloID depuis leur ordinateur portable, tablette ou smartphone. Les applications cloud sont répertoriées sous forme de vignettes simples et reconnaissables, qui sont lancées d'un simple clic de souris. Single Sign-On (SSO) connecte automatiquement l'utilisateur aux applications lancées, sans requérir à un écran de connexion supplémentaire.

La gestion des accès est un processus en trois étapes :

1. L'utilisateur prouve qu'il est 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 lance directement une application, sans avoir à se reconnecter (**Single Sign-On**).

Ces trois étapes sont décrites ci-dessous.

Authentification

Le plus souvent, Active Directory est utilisé pour authentifier les utilisateurs dans HelloID. Mais, d'autres fournisseurs d'identité tels qu'Azure AD, Google G Suite et Salesforce sont également pris en charge.

Des comptes locaux, non liés à un fournisseur d'identité, peuvent également être créés. C'est un moyen utile d'accorder l'accès aux clients, partenaires, patients ou autres invités de l'organisation. Les utilisateurs locaux peuvent se connecter à HelloID et accéder aux ressources sans avoir de compte dans le système d'annuaire de l'organisation.

HelloID offre une technologie 2FA complète et son coût est très compétitif (par exemple, par rapport à Azure P1). Les facteurs pris en charge comprennent le push-to-verify, les jetons et clés de sécurité, les e-mails, les SMS et les mots de passe à usage unique (OTP) traditionnels. Une variété d'autres options d'intégration sont également possibles, y compris l'intégration Radius.

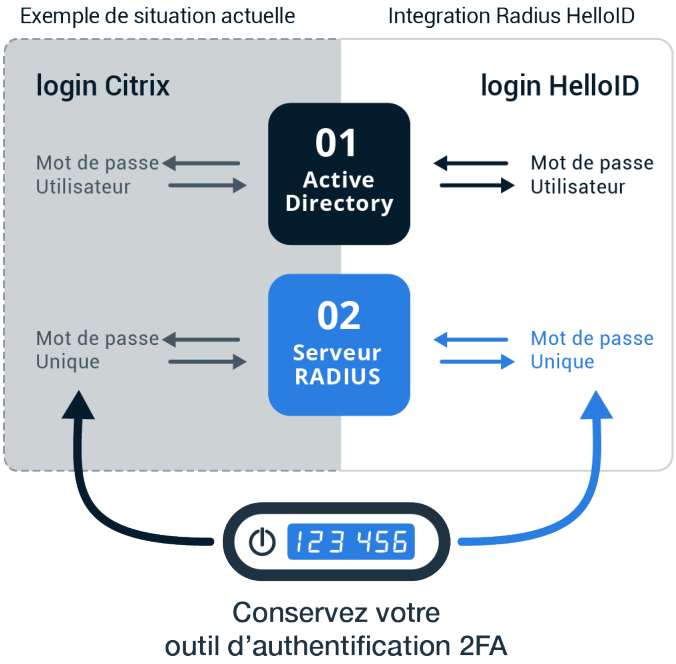


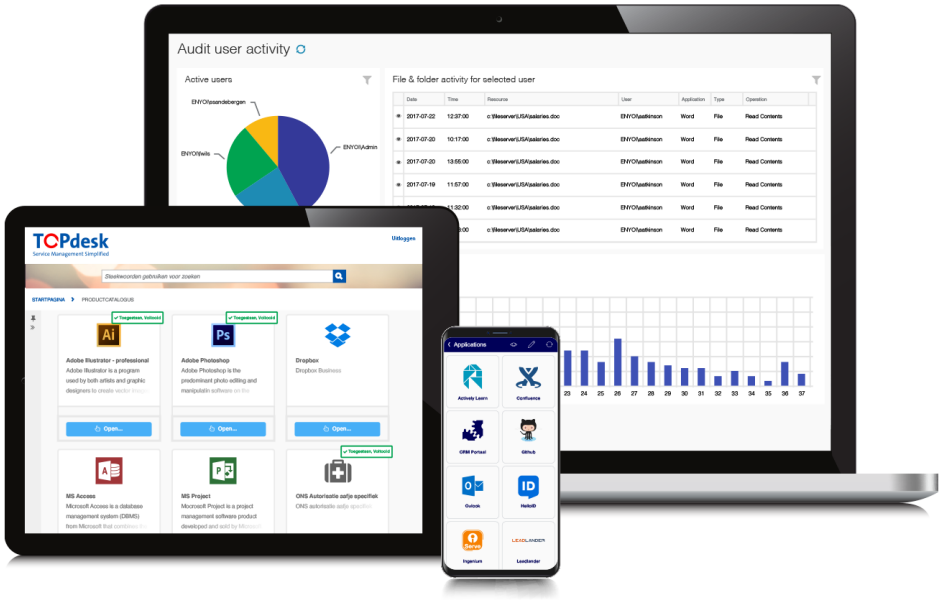
Tableau de bord

Une fois connectés, les utilisateurs finaux sont envoyés au tableau de bord de l'application. Les vignettes graphiques offrent un accès en un clic aux applications cloud de l'**o**rganisation.

Les appartenances aux groupes HelloID déterminent les applications disponibles. Les employés sont ajoutés aux groupes en fonction du service, du poste, de l'emplacement, etc. Cela vous donne une manière organisée de contrôler qui a accès à quelles applications cloud. L'appartenance à un groupe peut même être utilisée pour contrôler si une application en particulier nécessite une couche supplémentaire de 2FA.

Pour rendre le contrôle d'accès encore plus facile, les appartenances aux groupes peuvent être directement synchronisées à partir d'Active Directory ou d'autres systèmes d'annuaire. Cela économise beaucoup de travail aux administrateurs. Par exemple, un groupe AD peut être mappé directement sur un groupe HelloID.

L'aspect et la présentation du tableau de bord peuvent être personnalisés en fonction des besoins spécifiques de votre organisation. La mise en page par défaut peut être modifiée via des feuilles de style personnalisées, un couplage CSS ou des liens. L'API de l'utilisateur final facilite l'intégration du tableau de bord dans des applications intranet sociales telles que TripTic, Embrace, a & m impact, Workplace365, Motivo, Google Sites ou SharePoint Online.



Single Sign-On (SSO)

Une fois l'utilisateur authentifié, il est possible d'automatiser l'authentification auprès d'autres applications via l'authentification unique (SSO). HelloID transmet les informations d'identification de l'utilisateur via le protocole SSO approprié lorsque l'utilisateur lance une application. L'utilisateur n'a pas besoin de se reconnecter, sauf si des exigences supplémentaires ont été définies (par exemple, une deuxième couche 2FA).

HelloID prend en charge tous les protocoles SSO standard, notamment : OpenID Connect, SAML, WS-Federation, HTTP (S) Post et authentification de base, etc. Un plug-in de navigateur couvre les cas extrêmes pour les applications qui ne prennent pas en charge un protocole standard.

À propos de Tools4ever

Tools4ever est une société 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 des techniques logicielles de pointe. La première version de HelloID a été reçue avec beaucoup d'enthousiasme début 2015. 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

T4E.FR

Adresse 10-12 Bd Marius Vivier Merle
69003 LYON
FRANCE

Standard + 33 4 78 95 37 98
Fax + 33 4 78 95 38 37

Sales frsales@tools4ever.com
Support frsupport@tools4ever.com

TOOLS4E SOUTH EUROPE

Adresse Ramon Turró 169
08008 BARCELONE
ESPAGNE

Standard + 34 622 213 732

Sales sesales@tools4ever.com
Support frsupport@tools4ever.com