TOOLS4EVER

Livre blanc V2.0 / 04 09 2023

HelloID Security

Ce Livre blanc explique comment Tools4ever sécurise sa solution HelloID.

Sommaire

Gestion sécurisée des utilisateurs et des autorisations 1

Plateforme cloud HelloID 2

Architecture 2

Responsabilité partagée 3

Responsabilité de Tools4ever 3

Responsabilité du client 3

Mesures de sécurité 3

Datacenters fournis par des leaders internationalement reconnus 4

Données stockées en toute sécurité dans l'Espace économique européen (EEE) 4

Haute disponibilité et continuité du service 4

Sauvegardes automatisées 5

Chiffrement, vérification et certificats HelloID 5

Bases de données séparées et cryptées 5

Communication sécurisée sur Internet 5

Utilisation d'une URL personnalisée 5

Connexion sécurisée à l'infrastructure locale via l'agent HelloID 6

Installation, vérification et communication 7

Directory Agent 7

Provisioning Agent 7

Service Automation Agent 8

Authentification et autorisation 8

Authentification via l'annuaire cloud HelloID 8

Authentification via des tiers 8

Droits et rôles granulaires 9

Connexion aux systèmes cibles 9

Stockage des données à caractère personnel 9

Rapports et journalisation 10

Accès des données de journalisation 10

Durée de conservation des données 10

Protocole en cas de violation des données 11

Sécurité physique et politique d'autorisation chez Tools4ever 11

Normes et certifications 11

Gestion sécurisée des utilisateurs et des autorisations

Tools4ever est un éditeur de logiciels néerlandais, leader sur le marché de la gestion des identités et des accès (IAM). Depuis 1999, Tools4ever aide les organisations à gérer leurs utilisateurs et leurs autorisations de manière efficace et sécurisée : Tools4ever développe des logiciels aussi bien pour les PME-PMI à partir de 300 utilisateurs que pour les grandes multi-nationales comptant plus de 200 000 utilisateurs. Plus de 5 000 clients totalisant au moins 10 millions d'utilisateurs font confiance aux solutions IAM de Tools4ever.

De l'installation on-premises vers une solution Cloud

Tools4ever a traduit plus de 20 ans de connaissances et d'expertise avec deux générations de solutions IAM on-premises en une plateforme IAM moderne et sécurisée basée sur le cloud : HelloID.
HelloID est disponible dans le cloud en tant qu'Identity-as-a-Service (IDaaS) depuis 2015. Les solutions IAM traditionnelles sont complexes et nécessitent des consultants spécialisés pour chaque changement, alors que HelloID met la puissance de la gestion des identités et des accès entre les mains de nos clients et partenaires. Le service est toujours disponible, régulièrement mis à jour, enrichi de nouvelles fonctionnalités et la sécurité est toujours maintenue au plus haut niveau.

Priorité à la protection de la vie privée, à la sécurité de l'information et à la conformité

Des lois et réglementations plus strictes (AVG/RGPD, notification obligatoire des violations de données) et des lignes directrices en matière de sécurité de l'information (ISO 2700x, BIO, NEN 7510, IBP) obligent les organisations à prendre des mesures en matière de protection de la vie privée et de sécurité de l'information. L'IAM est une discipline de la cybersécurité qui aide les organisations à fournir aux bonnes personnes les autorisations et les accès appropriés au bon moment. Pour parvenir à ce résultat, la solution IAM elle-même travaille avec un grand nombre de données sensibles relatives à la vie privée. Lors de la sélection d'un logiciel de sécurité, il est donc important de se poser les questions suivantes :

- Comment déterminer qui peut y avoir accès, à quoi et de quelle manière ?
- Comment les liens sont-ils créés avec d'autres systèmes et applications ? Quelles sont les données partagées par le biais des liens ? Comment les connexions sont-elles sécurisées ?
- Comment et quelles données sont stockées ? Comment sont-elles codées ? Quel contrôle avons-nous sur nos données ? Comment nous assurons-nous que ces données ne peuvent pas fuir à l'extérieur de l'organisation ?
- Comment déterminons-nous et contrôlons-nous qui effectue quelles actions ? Comment réagissons-nous en cas d'activité suspecte ?

La sécurité de la solution et du stockage des données (personnelles) sont des priorités importantes chez Tools4ever. C'est pourquoi nous avons investi dans des ressources appropriées et des contrôles pour protéger nos clients. Avec HelloID, vous pouvez être sûr que :

- **Vos données sont protégées.** – Nous protègeons les informations confidentielles de nos clients.
- **Vous avez un accès continu à nos services.** – Nos services sont disponibles sans interruption et nous prenons des mesures proactives pour réduire les risques de sécurité susceptibles de perturber la continuité.
- **La sécurité de vos informations est conforme aux normes et à la législation.** – Nous nous conformons à la législation, aux meilleures pratiques et aux normes de l'industrie.

Ces trois principes sont au cœur de notre démarche : nous nous efforçons constamment d'améliorer les contrôles existants et de mettre en œuvre de nouvelles mesures de réduction des risques.

Dans ce document, nous vous expliquons en détail comment Tools4ever garantit la sécurité des données et la protection de la vie privée dans les modules de Provisioning et de Service Automaiton de HelloID.

Plateforme cloud HelloID

HelloID est une plateforme cloud composée de trois modules qui fonctionnent aussi bien de manière indépendante qu'intégrée les uns aux autres. En fonction des besoins en gestion des utilisateurs, des autorisations, de l'accès et en libre-service, les modules peuvent être activés ou désactivés.

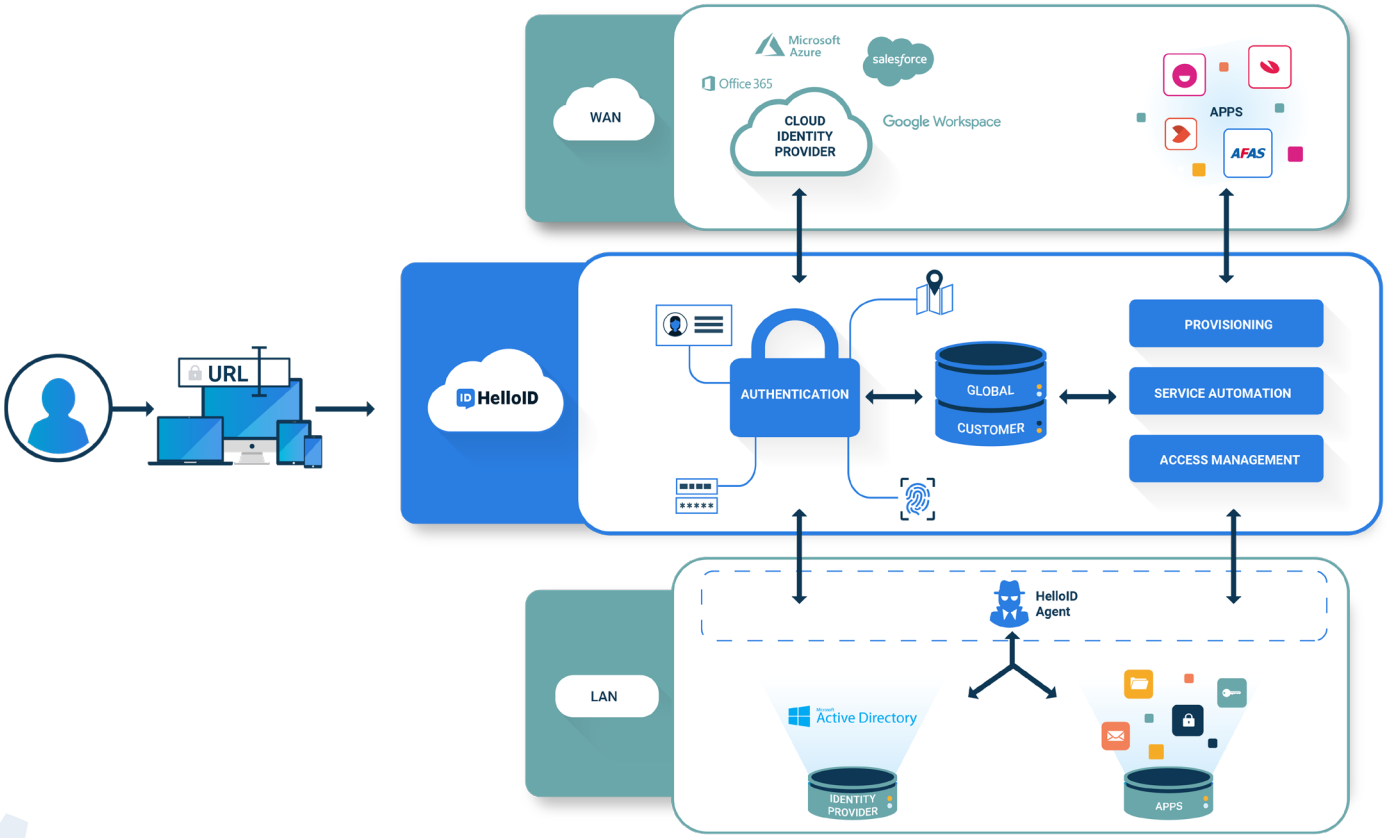
- **Provisioning**
  Gestion automatisée des comptes utilisateurs et des autorisations associées, en fonction du cycle de vie de l'identité, grâce à une liaison entre les systèmes "sources" et "cibles".

- **Service Automation**
  Utilisation de formulaires en libre-service et de formulaires délégués pour traiter de manière structurée, standardisée et automatisée les modifications qui ne peuvent pas être effectuées à partir d'un système source.

- **Access Management**
  Accès sécurisé et convivial au tenant µHelloID avec éventuellement une authentification à 2 facteurs, et en suivant des règles d'accès défini et conditionnelles.

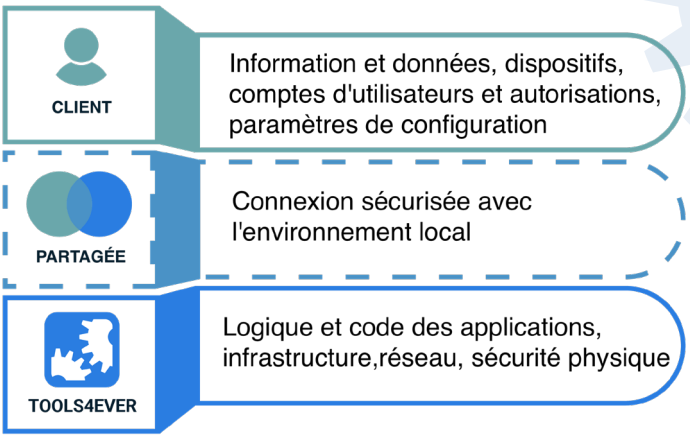
Architecture

L'architecture HelloID est composée de plusieurs composants partagés et distincts. Le schéma ci-dessous donne un aperçu des principaux composants et de leurs interactions. Les informations sont toujours cryptées, qu'elles soient en mouvement ou temporairement stockées. Le niveau de sécurité varie en fonction de chaque composant et dépend de l'impact, du risque et du besoins technique.



Responsabilité partagée

Lorsqu'il s'agit d'une solution SaaS comme HelloID, il est essentiel de comprendre la responsabilité partagée en matière de sécurité de l'information. Le modèle de responsabilité partagée définit les acteurs et leurs responsabilités : Celles de Tools4ever en tant que fournisseur SaaS, celles du client et des ces utilisateurs finaux et enfin celle qui est partagée.



Responsabilité de Tools4ever

Tools4ever est responsable de la sécurité de la plateforme HelloID, y compris la sécurité physique, la sécurité de l'application elle-même et de l'infrastructure sous-jacente. De plus, Tools4ever est responsable de l'accessibilité du service et fournit des mécanismes pour protéger les données au sein de HelloID. Les mesures de sécurité mises en place et fournies par Tools4ever sont détaillées dans le chapitre suivant : Mesures de sécurité.

Responsabilité du client

Le client reste toujours propriétaire de ces propres données. Par conséquent, il est responsable de la sécurisation des données stockées dans HelloID contre un accès non autorisé, de la garantie l'exactitude des données et de la protection contre les actes malveillants. Cela inclut notamment l'application d'une politique d'authentification robuste, la gestion correcte des utilisateurs et de leurs autorisations, ainsi que l'examen des journaux disponibles dans HelloID.

Mesures de sécurité

La façon dont nous concevons, développons et maintenons nos solutions est basée sur dix principes importants. Ces principes de Sécurité par Conception, tels que définis par l'OWASP, constituent la base de notre approche :

1	**Minimiser la surface d'attaque**	Notre objectif en matière de développement sécurisé est de réduire le risque global en réduisant ce que l'on appelle la "surface d'attaque". Chaque fonctionnalité ajoutée à une application ajoute un risque à l'application dans son ensemble.
2	**Sécuriser les paramètres par défaut**	Nous fournissons par défaut une expérience utilisateur aussi sécurisée que possible. Il appartient à l'utilisateur de l'application de réduire le niveau de sécurité par défaut en fonction de ses besoins.
3	**Principe du moindre privilège**	Par défaut, les comptes disposent des droits minimums requis pour exécuter les processus métier nécessaires. Il s'agit non seulement des droits des utilisateurs, mais aussi des exigences minimales en matière de limites de CPU, de mémoire, de réseau et de système de fichiers.
4	**Principe de la défense en profondeur**	Même lorsque seul un contrôle serait raisonnable, nous préférons avoir plusieurs contrôles pour aborder les risques de différentes manières. Ce principe peut rendre les vulnérabilités graves extrêmement difficiles à exploiter, les rendant ainsi moins probables.
5	**Sécurité en cas d'échec**	L'application peut échouer dans l'exécution de ses processus pour diverses raisons. Cependant, le résultat de cette défaillance détermine si une application est sécurisée ou non. Tous les composants de HelloID sont conçus pour échouer de manière sécurisée.

6	**Par défaut, ne pas faire confiance aux services tiers**	Les tiers ont généralement des politiques et des procédures de sécurité différentes des nôtres. C'est pourquoi nous n'accordons pas une confiance aveugle aux systèmes externes et traitons tous les systèmes externes de la même manière.
7	**Séparation des fonctions**	Il s'agit d'un élément essentiel de la sécurité du déroulement des opérations. Par exemple, les administrateurs ne devraient normalement pas être des utilisateurs.
8	**Pas de sécurité par obscurité**	Dans notre vision, la sécurité des systèmes importants ne doit pas dépendre uniquement du fait de cacher les détails. Nous considérons cela comme une sécurité faible.
9	**Simplifier le code**	Notre approche privilégie un code simple plutôt que des approches trop complexes. Nous n'utilisons pas de doubles négations ou d'architectures complexes, sauf en cas d'absolue nécessité.
10	**Résoudre correctement les problèmes de sécurité**	Lorsqu'un problème de sécurité est identifié, il est important de le reproduire dans un environnement de un test afin de comprendre la cause profonde du problème. Lorsque des modèles de conception sont utilisés, il est probable que le problème de sécurité soit répandu dans toutes les "bases de code". Il est donc essentiel de développer la bonne solution sans avoir recours à des solutions de contournement ou de repli.

Datacenters fournis par des leaders internationalement reconnus

HelloID est hébergé sur les plateformes cloud Microsoft Azure et Google Cloud. Nos partenaires Microsoft et Google sont internationalement reconnus comme des leaders mondiaux dans le domaine de l'Infrastructure-as-a-Service (IaaS). Ils ont mis en place des infrastructures en cloud qui répondent pleinement aux exigences mondiales et locales. Les services résistent aux irrégularités et aux attaques malveillantes en protégeant l'infrastructure aux niveaux physique, réseau, hôte, application et données. Des directives de sécurité et des processus opérationnels stricts sont appliqués. Ces services font également l'objet d'une surveillance proactive permanente et des tests de pénétration sont effectués.

Données stockées en toute sécurité dans l'Espace économique européen (EEE)

Microsoft Azure et Google Cloud disposent de centres de données dans le monde entier, répartis par région. La distinction entre les régions nous permet de placer chaque portail HelloID dans la région souhaitée. HelloID utilise actuellement des centres de données dans deux régions : l'Espace économique européen (EEE) et l'ouest des États-Unis. Par défaut, les données de nos clients et partenaires Français sont uniquement stockées dans l'Espace économique européen. Tools4ever répond ainsi aux exigences de l'AVG en matière de localisation des données sensibles.

Haute disponibilité et continuité du service

La disponibilité de la plateforme HelloID est garantie à 99,90 % par an. Ceci est rendu possible, entre autres, par les mesures prises par nos hébergeurs concernant la réplication des données dans la région, les services de sauvegarde et la redondance des installations d'alimentation, de réseau et de refroidissement.

La disponibilité et les performances de HelloID sont constamment surveillées. Les informations sur la disponibilité actuelle et historique, la maintenance (planifiée) et les incidents sont accessibles au public via la page de statut HelloID. Inscrivez-vous pour recevoir les mises à jour de statut, vous serez ainsi informé par e-mail en cas d'incidents.

Sauvegardes automatisées

Tools4ever effectue des sauvegardes automatisées de toutes les bases de données. Les données sont conservées pendant 30 jours. En cas d'incident, il est possible de restaurer la base de données à des

intervalles de 4 heures via la récupération à un instant donné (PITR), ce qui signifie qu'il est possible de restaurer les données à n'importe quel moment au cours des 30 derniers jours dans l'intervalle spécifié. L'utilisation de la récupération à un instant donné (PITR) signifie que les données peuvent être récupérées avec une perte minimale, voire nulle.

Chiffrement, vérification et certificats HelloID

Les certificats garantissent à la fois l'identité et le chiffrement sécurisé d'un site web, d'un individu, d'une organisation, d'un appareil, d'un utilisateur ou d'un serveur. Dans HelloID, le chiffrement est appliqué à différentes couches.

Bases de données séparées et cryptées

Tools4ever propose une solution SaaS multi-tenant évolutive avec HelloID. L'interface utilisateur et les API limitent l'accès aux seules données auxquelles le portail client est autorisé. Les données sont logiquement séparées dans différentes bases de données qui sont cryptées avec des clés de cryptage AES 256 bits. La base de données générale HelloID contient les paramètres de configuration globale et les données du portail. Toutes les configurations spécifiques au client et les données de l'utilisateur sont stockées par portail dans une base de données dédiée au client. Les données de cette base sont cryptées avec leur propre clé de cryptage. Avec cette configuration, tous les locataires sont isolés les uns des autres et il n'y a aucun risque d'accès croisé aux portails ou de contamination des données.

Communication sécurisée sur Internet

La communication sur Internet doit toujours être sécurisée. Le serveur web HelloID communique avec les composants via Internet en utilisant HTTPS. Le niveau de chiffrement est TLS 1.2, avec un chiffrement AES 256 bits.



Utilisation d'une URL personnalisée

Par défaut, votre organisation a accès à son propre sous-domaine : "organisationname.helloid.com", qui donne accès à HelloID. Vous pouvez également remplacer l'URL de HelloID par votre propre nom de domaine afin d'accroître la reconnaissance de votre organisation. Les noms de domaine courants sont, par exemple, "login.organisationname.com" ou "helloid.organisationname.com". Comme la communication avec HelloID se fait via HTTPS, vous avez besoin d'un certificat PFX. Il peut s'agir d'un certificat wildcard ou d'un certificat de domaine pour l'URL demandée. Le lien entre HelloID et le domaine est validé à l'aide d'un enregistrement CNAME.

Si vous souhaitez utiliser votre propre nom de domaine, il est recommandé de le configurer immédiatement après la création du portail. Modifier l'URL ultérieurement peut affecter le fonctionnement des fournisseurs d'identité, de l'authentification unique et des connexions à l'environnement local.

Connexion sécurisée à l'infrastructure locale via l'agent HelloID

La configuration par défaut de HelloID est entièrement basée sur le cloud. Pour les organisations qui fonctionnent entièrement en mode cloud, HelloID fonctionne donc également sans composants sur site. Cependant, un « agent » local optionnel est nécessaire lorsque HelloID doit interagir avec des ressources locales telles qu'un annuaire Active Directory, le système de fichiers ou une base de données. L'agent HelloID se compose d'un ensemble de trois services Windows installés dans le réseau de votre organisation. Ces services Windows permettent la communication avec les différents modules HelloID.

Vous pouvez installer plusieurs agents pour l'équilibrage de charge et la séparation des tâches. Lorsque plusieurs agents sont installés, ils sont regroupés en pools d'agents. Lorsqu'une tâche sur site est lancée, elle est envoyée à un pool d'agents, qui détermine ensuite quel agent HelloID dans ce pool est disponible et adapté pour exécuter la tâche. Chaque pool d'agents nécessite au moins un agent HelloID pour fonctionner.

Installation, vérification et communication

L'agent HelloID est donc un "intermédiaire" qui échange des données et effectue des actions localement. La communication sur l'internet doit toujours être sécurisée. Un processus en trois étapes garantit une communication sécurisée entre le tenant cloud HelloID et l'agent installé localement.

Installation

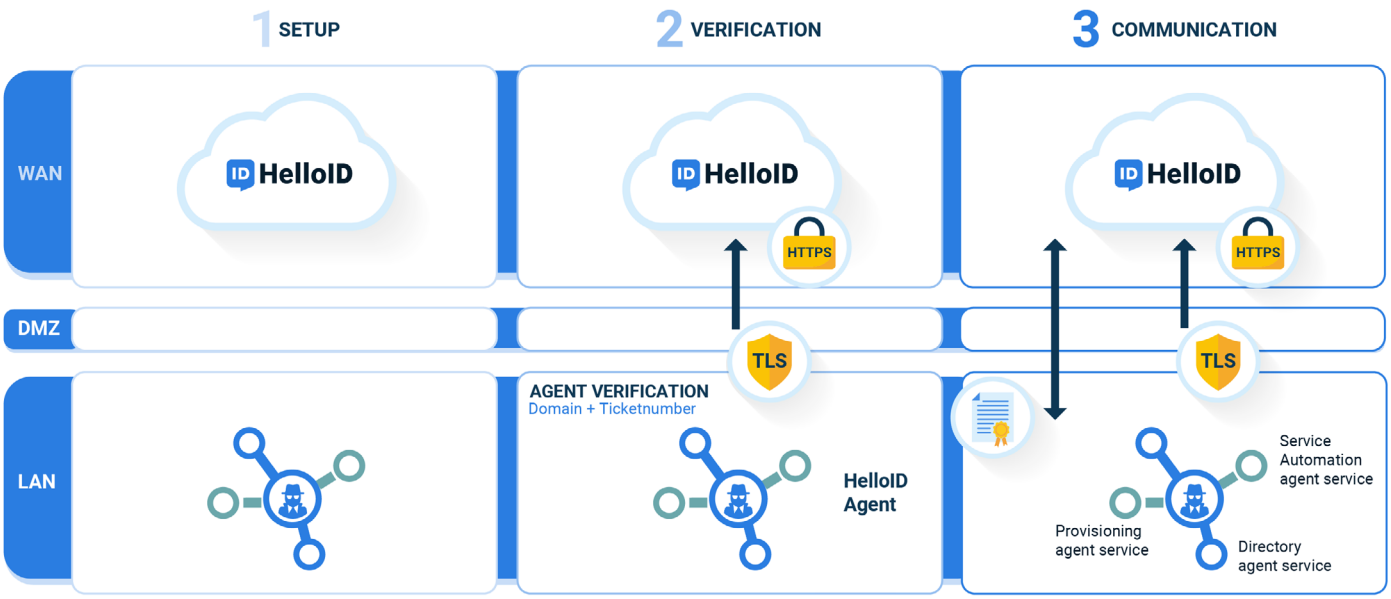
L'Agent HelloID communique avec les composants via Internet en utilisant HTTPS. Le niveau de cryptage est TLS 1.2, AES avec un cryptage de 256 bits. L'Agent HelloID peut être installé sur n'importe quel serveur dans le domaine qui a un accès HTTPS au tenant HelloID. Pour éviter les conflits avec la politique de sécurité locale, il est généralement installé sur un serveur qui n'est pas un contrôleur de domaine. Les services de l'agent s'exécutent avec un compte de domaine ayant des droits d'administrateur local. L'utilisation d'un compte local peut entraîner des problèmes de connexion pour les utilisateurs finaux et des échecs de tâches de synchronisation. Sans droits d'administrateur local, l'agent ne peut pas être mis à jour automatiquement.

Vérification

Le processus de vérification garantit que votre portail HelloID ne fait confiance qu'à la bonne instance de l'agent. Lors de l'installation de l'agent, HelloID génère un numéro de ticket OTP. Ce numéro ne peut être utilisé qu'une seule fois, et seulement dans les 10 minutes suivant sa création. L'administrateur de HelloID fournit ce numéro à l'agent. Un certificat partagé est généré sur la base d'une combinaison de l'OTP, de l'URL du portail et du GUID de l'agent. Ce certificat valide ensuite toute tentative de communication entre HelloID et l'agent. Si le certificat ne correspond pas ou si le GUID de l'agent est modifié, la communication est impossible. Si le certificat ou l'agent est copié ou déplacé, la confiance est immédiatement révoquée. Cette procédure de vérification ne peut être effectuée que par les administrateurs de HelloID autorisés à ajouter des agents. Pour une sécurité maximale, aucun autre scénario n'est autorisé.

Communication

L'Agent HelloID fonctionne exclusivement dans une seule direction, la communication se faisant uniquement du réseau local vers le portail HelloID. Il n'exécute que les actions préparées par le portail HelloID et ne peut pas envoyer de commandes au portail. Lorsque l'agent répond à une demande, HelloID vérifie l'adresse IP d'origine. Si celle-ci ne correspond pas à l'adresse IP utilisée lors de la vérification, la commande est rejetée et la confiance est immédiatement révoquée. Aucune ouverture de port firewall spéciale ou configuration DMZ n'est nécessaire. L'agent communique via le port TCP standard 443.



Directory Agent

Le "Directory Agent" est un service chargé d'exécuter des tâches locales liées à l'authentification sur le tenant HelloID via l'Active Directory pour permettre :

- l'authentification des utilisateurs dans HelloID lors de l'utilisation d'Active Directory comme fournisseur d'identité.
- La synchronisation des comptes utilisateurs d'Active Directory vers HelloID.

Le "Directory Agent" utilise HTTPS avec une technique de "*long polling*". Chaque demande reste ouverte pendant 30 secondes. Pendant cet intervalle, le service répond toutes les cinq secondes avec cinq processus d'interrogation simultanés. La plupart des demandes sont traitées en moins d'une seconde. Toutes les communications sont cryptées à l'aide de certificats HelloID via TLS 1.2. Chaque demande est vérifiée par rapport au certificat et au GUID de l'agent.

Provisioning Agent

Le "Provisioning Agent" est un service responsable des tâches sur site liées au module de Provisionnement de HelloID, telles que:

- Récupération de données à partir de systèmes sources locaux tels que des bases de données RH
- La gestion des comptes utilisateurs et des droits dans les systèmes cibles locaux tels que Active Directory et NTFS, ainsi que dans les fichiers CSV, les bases de données SQL et Oracles

Le "Provisioning Agent" utilise des Websockets sécurisés pour maintenir une communication ouverte, presque en temps réel, avec le tenant HelloID. Une requête HTTPS initiale vers le portail HelloID est transformée en une connexion WebSocket sécurisée. Le WebSocket est recyclé toutes les trois heures et dispose d'un "heartbeat" de 60 secondes pour vérifier si la connexion doit rester ouverte. Toutes les communications sont cryptées par des certificats HelloID via TLS 1.2. Chaque demande est vérifiée sur la base du certificat et du GUID de l'agent. Ce service est optimisé pour la communication en temps quasi réel, la stabilité et la performance pour les demandes en masse.

Service Automation Agent

L'Agent "Service Automatisation" (SA) est un service chargé de toutes les tâches liées au module d'Automatisation de Service de HelloID. Cela inclut notamment :

- L'exécution de scripts PowerShell dans le but de remplir des sources de données.
- L'exécution d'actions sur site pour les tâches programmées, les demandes en libre-service approuvées et les formulaires délégués.

L'agent "Service Automation" partage les caractéristiques de sécurité de l'agent de Provisioning. Ce service est optimisé pour un temps de réponse rapide afin d'offrir une expérience fluide à l'utilisateur. Les tâches préparées à partir du portail en libre-service et des formulaires délégués sont prises en charge et exécutées presque instantanément.

Authentification et autorisation

L'authentification consiste à vérifier l'identité d'un utilisateur pour s'assurer qu'il est bien celui qu'il prétend être. L'authentification en tant qu'utilisateur ou administrateur sur la plateforme HelloID se fait par l'intermédiaire d'un ou plusieurs fournisseurs d'identité. Un fournisseur d'identité (IDP) est un système dans lequel les informations relatives à l'identité sont gérées. Pour l'authentification primaire à l'application HelloID, HelloID supporte deux types de fournisseurs d'identité :

- Annuaire cloud HelloID
- Fournisseur d'identité tiers

Plusieurs fournisseurs d'identité peuvent être actifs en même temps. Dans la pratique, HelloID est souvent lié à un IDP tiers tel que (Azure) Active Directory ou Google Workplace. L'annuaire cloud de Helloid permet à votre organisation de donner accès à des tiers sans qu'il soit nécessaire de leur créer un compte utilisateur dans Active Directory.

Authentification via l'annuaire cloud HelloID

Lors de l'authentification, l'utilisateur est identifié via l'annuaire cloud intégré à HelloID. Cette identification se fait avec un nom d'utilisateur et un mot de passe. Ces informations de compte sont stockées dans le cloud, le mot de passe étant stocké de manière chiffrée. Les administrateurs HelloID de votre organisation peuvent surveiller la complexité et la sécurité des comptes utilisateurs locaux HelloID en configurant une politique de mot de passe. Ils peuvent, par exemple, exiger une certaine robustesse du mot de passe, basée sur des critères tels que la longueur et la complexité, ou exclure les mots de passe courants. Afin d'apporter une couche de sécurité supplémentaire, en plus du mot de passe, une seconde authentification peut être requise. HelloID prend en charge l'authentification à deux facteurs (2FA) par SMS, e-mail, mots de passe à usage unique (OTP) via des jetons logiciels et/ou matériels, et peut s'intégrer avec des clients Radius.

Authentification via des tiers

Dans de nombreux cas, les utilisateurs se connectent à HelloID par l'intermédiaire d'un fournisseur d'identité tiers tel qu'Active Directory. L'utilisation d'un Active Directory local nécessite également des composants locaux sous la forme d'un agent HelloID et d'un serveur web IIS. Cependant, HelloID prend également en charge l'authentification de cloud à cloud via des fournisseurs d'identité tels qu'Azure, Google Workforce et Salesforce. Avec ces fournisseurs d'identité, aucun identifiant de connexion n'est synchronisé, mais l'authentification se fait via un "secret partagé" avec des normes industrielles telles que SAML, WS-Federation et OpenID Connect. Les utilisateurs peuvent se connecter avec les identifiants de connexion gérés dans l'IDP et la tierce partie valide leur exactitude à chaque demande d'authentification.

Droits et rôles granulaires

Après l'authentification d'un utilisateur, ses rôles déterminent les parties de HelloID auxquelles il est autorisé à accéder. Un rôle est un ensemble de droits et de privilèges qui peuvent être attribués à un ou plusieurs utilisateurs. Par défaut, certains rôles de base sont disponibles dans HelloID, mais des rôles d'utilisateur spécifiques à l'organisation peuvent également être définis. Les actions qui peuvent être effectuées par rôle peuvent être affinées en fonction du système CRUD (Create, Read, Update, Delete).

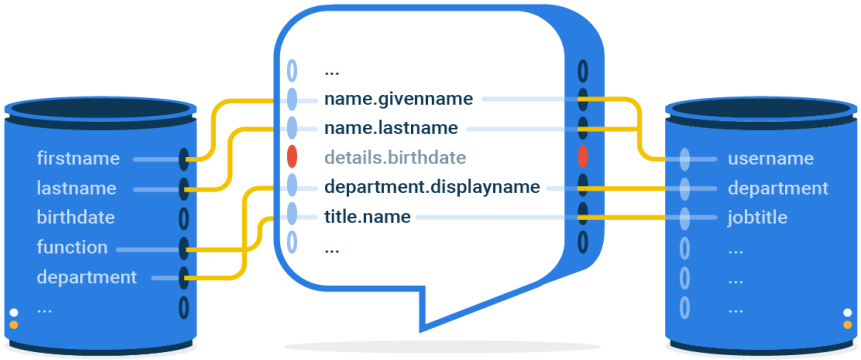
D'une part, cela détermine les actions qu'un utilisateur est autorisé à effectuer. Par exemple, il est possible de configurer qu'une personne ayant un rôle d'administrateur est autorisée à modifier et à supprimer un rapport, tandis qu'une personne ayant un rôle de gestionnaire ne peut que le consulter. D'autre part, cela permet de déterminer quels composants sont visibles par les utilisateurs d'un même rôle. Chaque composant de l'interface utilisateur de HelloID peut être activé ou désactivé par rôle afin que votre organisation puisse décider quelles fonctionnalités peuvent être utilisées. L'attribution d'un rôle peut être effectuée manuellement par un administrateur, mais les rôles peuvent également être attribués en fonction des groupes dans l'annuaire local de HelloID ou du fournisseur d'identité tiers.

Connexion aux systèmes cibles

Avec HelloID Provisioning, la création et la gestion des comptes utilisateurs, des autorisations sur le réseau et les applications sont automatisées au maximum grâce à une connexion à un système source. Le module HelloID Service Automation s'intègre parfaitement à HelloID Provisioning. En plus du provisioning automatisée à partir du système RH, il y aura toujours des demandes de service "spécifiques" occasionnelles. Ces modifications ponctuelles peuvent être automatisées avec le module Service Automation. L'Agent HelloID assure la synchronisation avec les systèmes source et cibles locaux. Pour les applications cloud, la connectivité s'effectue entièrement depuis le cloud. HelloID peut s'interfacer avec les API et les services web des applications sources et cibles via des protocoles tels que SOAP/XML, REST/JSON, SCIM et ODBC. Les connexions sur Internet sont établies via HTTPS..

Stockage des données à caractère personnel

Tools4ever traite les données à caractère personnel de ses clients afin de fournir les services demandés. Une distinction est faite entre les données à caractère personnel qui sont minimalement nécessaires au fonctionnement des modules HelloID aquis et les données à caractère personnel que le client souhaite traiter. Par défaut, HelloID ne traite pas les données classées comme "données personnelles spéciales".



Vous trouverez ci-dessous les données minimales requises pour chaque module :

- **Provisioning** - Il faut au moins les informaitons d'identité (prénom, nom de famille, nom préféré) et les données relatives au contrat (numéro de matricule, poste, service, organisation, dates d'entrée dans le service et de sortie du service) pour gérer les utilisateurs et leurs autorisations.

- **Service Automation** - requiert à minima le nom de connexion (Login) et le nom d'affichage pour s'authentifier sur le portail.

- **Access Management** - comme pour le module Service Automation, il requiert à minima le nom de connexion (Login) et le nom d'affichage pour s'authentifier sur le portail

En tant que client, vous pouvez juger par vous-même si Tools4ever est autorisé à traiter des données supplémentaires. Grâce au "mappeur d'attributs" de HelloID, les administrateurs peuvent laisser les consultants de Tools4ever et de ses partenaires configurer les données des systèmes liés qui seront ou non traitées et/ou stockées dans la base de données HelloID. Ce mappage configurable garantit que la base de données HelloID reste toujours conforme aux politiques de confidentialité et de sécurité de votre organisation.

Rapports et journalisation

La génération de rapports et la journalisation sont des composants de base de toute politique de sécurité, requises à la fois par la législation et la réglementation, ainsi que par les directives en matière de sécurité de l'information. HelloID enregistre tous les événements importants. La journalisation offre une visibilité sous forme de journal d'audit pour suivre l'utilisation de l'environnement HelloID. Elle permet d'identifier les éventuels risques en matière de sécurité. Toutes les actions effectuées dans et par HelloID sont enregistrées dans Elastic Report, offrant ainsi des fonctionnalités étendues pour la génération de rapports.

Voici quelques exemples de données journalisées pour chaque module :

- **Provisioning**
  Toutes les actions effectuées concernant la création, l'activation, la mise à jour, le déplacement, la désactivation et la suppression de comptes, ainsi que l'octroi et le retrait d'autorisations, sont enregistrées pour chaque système et chaque personne. Les événements de modifications de configuration des règles métier sont également enregistrées.

- **Service Automation**
  Pour les produits en libre-service, les informations relatives à la demande et au workflow d'approbation sont stockées. Pour les formulaires délégués, toutes les données saisies dans le formulaire ainsi que les actions réalisées lors de la soumission du formulaire sont stokées.

Accès des données de journalisation

Les données d'Elastic peuvent être affichées via les fonctions de reporting intégrées ou utilisées en conjonction avec des outils propriétaires de business intelligence (BI) tels que PowerBI. Toutes les données de journalisation d'Elastic sont disponibles en temps quasi réel et peuvent être lues via des API REST. L'utilisation de l'authentification via une clé API HelloID garantit que seules les personnes autorisées peuvent consulter les données de journalisation.

Durée de conservation des données

Au sein de HelloID, les périodes de conservation sont différenciées entre les données stockées par le client dans la plateforme et l'enregistrement (d'audit). Les données relatives à l'utilisateur et à la configuration sont conservées pendant toute la durée du contrat. En cas de résiliation du contrat HelloID, les données sont conservées pendant 3 mois au maximum et sont ensuite automatiquement effacées.

HelloID conserve les journaux d'audit interne pendant 30 jours. À l'expiration de cette période de conservation, les journaux, y compris la sauvegarde, sont supprimés. Les journaux d'audit accessibles via la plateforme de reporting Elastic sont conservés pendant un an. Après cette période, ces données, y compris les sauvegardes, sont supprimées. Si la loi et les règlements exigent que les données soient conservées plus longtemps, vous pouvez les exporter vers votre propre outil de rapport, d'archivage ou d'audit via les API disponibles à cet effet. De cette manière, votre organisation a un contrôle total sur la période de conservation de l'enregistrement (d'audit)..

Protocole en cas de violation des données

En cas de violation de données, le protocole de violation de données est activé pour assurer que les clients sont informés des incidents. Après avoir découvert un incident de sécurité ou une violation de données, Tools4ever informe ses clients dans les 24 heures. Tools4ever envoie cette notification par e-mail à la personne de contact au sein de votre organisation. Tools4ever ne signale pas la violation directement à l'AP (Autorité de protection des données) ou aux parties concernées.

Sécurité physique et politique d'autorisation chez Tools4ever

Les bureaux de Tools4ever sont sécurisés de plusieurs manières. À l'intérieur et autour du bâtiment, entre autres, il y a une surveillance par caméra et l'accès aux locaux est limité par des jetons RFID liés à des individus. Pour les salles de serveurs, de stockage et d'électricité, entre autres, des formes supplémentaires de sécurité d'accès sont appliquées.

Tools4ever applique une politique stricte en matière de traitement des données des clients. Des accords de confidentialité ont été conclus avec les employés et ceux-ci n'ont accès qu'aux données strictement nécessaires à leur fonction. Une authentification à deux facteurs est utilisée pour accéder aux systèmes et aux applications. Tools4ever encourage la sensibilisation, l'éducation et la formation en matière de protection de la vie privée et de sécurité de l'information. Des responsables de la sécurité formés à la politique de l'information et à la sécurité informatique contrôlent la conformité et mettent régulièrement à jour les mesures de sécurité.

Normes et certifications

La plateforme HelloID est hébergée sur les solutions Microsoft et Google Infrastructure-as-a-Service (IaaS). Ces deux fournisseurs sont internationalement reconnus pour les normes de sécurité très élevées qu'ils respectent et, sur la base de l'accord de niveau de service conclu avec les deux parties, la sécurité de notre plateforme est garantie. En outre, HelloID, en tant que solution IDaaS, vous aide, en tant que client, à vous conformer à diverses normes et certifications de sécurité de l'information (spécifiques au secteur). Tools4ever considère également qu'il est important que les normes établies par l'industrie du logiciel soient respectées et que nos systèmes, processus et procédures soient examinés structurellement par des tiers externes et indépendants.

OWASP

Les principes de la sécurité par conception définis par l'OWASP (Open Web Application Security Project) constituent la base de notre approche.

Microsoft Gold Partner

Tools4ever bénéficie d'un partenariat Microsoft Gold de longue date (plus de 20 ans) et possède une expertise spécifique en matière de sécurité dans le cadre de la suite de produits Microsoft.

ISO 27001

Tools4ever est certifié ISO 27001. Cela implique que Tools4ever a mis en place un système de gestion de la sécurité de l'information efficace. Concrètement, cela signifie que nous développons des logiciels de manière sécurisée et contrôlée, et que nous prenons des mesures appropriées en cas de risques potentiels ou d'incidents de sécurité. En 2022, nous avons également obtenu la certification SOC 2.

Deloitte.

Deloitte Risk Services réalise deux fois par an des tests de pénétration en black box et gray box. Le rapport d'observations fourni par Deloitte est traité en haute priorité par notre service de développement et les recommandations sont mises en œuvre le cas échéant, ou des réponses sont apportées de manière appropriée par Tools4ever.

TOOLS4EVER

Adresse	Tools4ever France 10-12 Bd Marius Vivier Merle 69003 Lyon
Téléphone	+33 4 78 95 37 98
Site web	Tools4ever.fr
Sales	frsales@tools4ever.com
Support	frsupport@tools4ever.com