HelloID

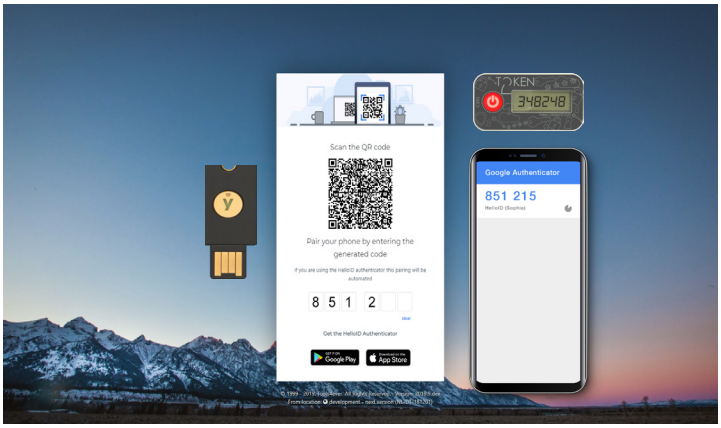
Module Access Management

Les utilisateurs perdent du temps à se connecter à l'ensemble de leurs applicatons ?

Ils oublient régulièrement leurs mots de passe et ne peuvent donc plus se connecter ?

Le service de support est surchargé par le grand nombre de tickets de réinitialisation de mot de passe ?

HelloID résout ces situations !



De nos jours, les personnes à la maison ont souvent un environnement informatique plus convivial qu'au bureau. Ils peuvent facilement accéder à toutes leurs applications depuis n'importe quel appareil, n'importe où dans la maison et en un seul clic. Tools4ever apporte la même facilité d'utilisation à l'entreprise avec HelloID Access Management, pour un faible investissement. Les utilisateurs de l'entreprise peuvent accéder à un tableau de bord convivial via HelloID avec une seule connexion. Ils peuvent ensuite ouvrir leurs applications cloud en un seul clic partout et depuis n'importe quel appareil.

Travailler en toute sécurité, efficacement et facilement avec HelloID

HelloID est un portail qui avec un nom d'utilisateur et un mot de passe donne un accès rapide à toutes les applications. Les utilisateurs n'ont plus besoin de se souvenir de différents noms d'utilisateur et mots de passe et n'ont plus à les saisir à chaque fois qu'ils changent d'application. L'authentification unique (SSO) rend leur travail beaucoup plus agréable et efficace. La charge de travail du service informatique est également considérablement réduite, car beaucoup moins de demandes de réinitialisation de mot de passe sont reçues. Il est possible également de réinitialiser le mot de passe via HelloID Access Management en cas d'oubli.

Étant donné que l'accès aux applications par les utilisateurs se fait au travers du portail, une gestion totale sur l'accès et les droits peut être réalisée par application. Il est possible de choisir des options de sécurité supplémentaires natives dans HelloID telle que l'authentification à deux facteurs (2FA).

HelloID enregistre tous les évènements afin de permettre d'obtenir des rapports de qui utilise quelles applications, à quelle heure et à partir de quel endroit. Cela permet de devenir par conséquant automatiquement conforme aux normes telles que BIO, ISO27001, NEN 7510 et GDPR / AVG.

Un tremplin pour faire avancer l'innovation informatique

HelloID Access Management offre aux employés, partenaires et éventuellement aux clients, un accès simple et uniforme aux applications cloud. La connexion d'un utilisateur à HelloID se fait dans de nombreux cas via Active Directory. HelloID prend également en charge les fournisseurs d'identité utilisant SAML, LDAP et Azure. Par défaut, on se connecte à HelloID Access Management avec un nom d'utilisateur et un mot de passe. Il est également possible d'utiliser des cartes avec un code QR pouvant simplifier la procédure de connexion, par exemple pour les étudiants et autres groupes d'utilisateurs spécifiques. La carte est scannée et HelloID identifie automatiquement l'utilisateur en fournissant l'accès aux applications et aux données.

Un espace de travail numérique convivial

HelloID Access Management est parfaitement intégré dans les portails des principales solutions de gestion d'intranet social et de gestion d'incidents. À cette fin, Tools4ever collabore activement avec des fournisseurs tels que TOPdesk, AFAS, SharePoint, EasyVista, etc. L'intégration de l'intranet avec la fonctionnalité de gestion des accès, crée un portail numérique unique pour les employés. Après s'être connecté à l'intranet social, l'utilisateur accède à un portail personnel avec des informations, des outils de communication et via le Widget HelloID, ses propres applications et dossiers de données qui peuvent être ouvert en un clic, comme nous en avons l'habitude à la maison.

Vérification supplémentaire avec authentification à deux facteurs (2FA)

Il arrive dans certains cas, que l'on ne souhaite pas que les utilisateurs puissent se connecter uniquement avec un nom d'utilisateur et un mot de passe, mais en réquierant une vérification supplémentaire. HelloID Access Management propose gratuitement diverses méthodes 2FA (FIDO, Push to verify, SMS, e-mail, etc.), et s'intègre également de manière transparente avec les applications gratuites Authenticator de Microsoft et Google. De plus, les méthodes et jetons 2FA déjà en place peuvent être réutilisés. Si différentes méthodes 2FA sont utilisées dans la situation existante pour diverses applications, il est possible facilement de réduire cela à une seule méthode commune avec HelloID. En fonction du département, du lieu, de l'heure et du dispositif, il est possible de définir des règles d'accès pour le portail ou des applications spécifiques. Cela permet de choisir de manière granulaire le niveau d'authentification correct pour chaque scénario.

Le respect des lois et réglementations

Les lois et réglementations de plus en plus strictes dans le domaine des audits et de la sécurité exigent que l'accès et l'utilisation des applications cloud soient suivis et rendus transparents. Avec HelloID Access Management, le processus d'authentification est automatiquement surveillé. Les rapports fournissent un aperçu de qui a accédé à quoi, à quelle heure et à partir de quel endroit. Cela fournit non seulement une image détaillée du processus d'authentification, mais montre également les tentatives de connexion à partir d'adresses IP suspectes. Les menaces potentielles peuvent être identifiées à temps pour prendre des contre-mesures. Cela rend le processus d'authentification transparent, contrôlable et adaptable.

Éviter un enchevêtrement de méthodes d'authentification

Au vu, entre autres, des directives ISO et NEN, de plus en plus de fournisseurs de logiciels choisissent de mieux protéger la porte de leur application et de désactiver les possibilités de mise sur liste blanche (autoriser l'accès depuis le bureau de l'organisation). En pratique, cela signifie que chaque application applique ses propres méthodes et systèmes d'authentification. HelloID Access Management peut agir comme un hub central. Cela signifie que les utilisateurs peuvent toujours se connecter via un seul et même processus.