HID DigitalPersona®

Flexibilité et commodité quand vous le souhaitez, robustesse et sécurité quand c'est nécessaire

HID DigitalPersona transforme la façon dont une organisation protège l'intégrité des actifs et des applications numériques en fournissant une authentification multi-facteurs (MFA) facile à déployer, à adopter et à gérer qui élimine les processus de sécurité cloisonnés avec un bon rapport coût-efficacité. Conçue pour les organisations sans frontières d'aujourd'hui, cette solution MFA permet une connexion rapide et sécurisée à Windows, aux réseaux et aux applications via la biométrie, les appareils mobiles, les badges d'accès physiques, les cartes à puce et les clés de sécurité - offrant une expérience utilisateur transparente avec la protection la plus forte disponible dans l'industrie.

Alliant sécurité et convivialité, DigitalPersona utilise l'une des plus vastes gammes de méthodes d'authentification et de facteurs de forme de l'industrie, y compris le numéro d'identification personnel (PIN), les mots de passe à usage unique (OTP), les notifications push mobiles, FIDO, PKI, les empreintes digitales et la reconnaissance faciale - permettant une approche de sécurité zéro confiance qui évolue avec les normes de sécurité, les technologies et les réglementations de l'industrie.

CE QUE VOUS SAVEZ

- Mot de passe
- CODE PIN
- Authentification basée sur les connaissances*
- Code d'accès unique*

CE QUE VOUS ÊTES

- Empreinte digitale
- Reconnaissance faciale

CE QUE VOUS AVEZ

- Clés de sécurité**
- Smart Card**
- Cartes d'accès (écrites ou de proximité)
- Appareils Bluetooth (mobile, montre, casques)
- Jetons OTP

Combinaison avec les fonctions MS Windows® natives

OÙ VOUS ÊTES

- Adresse IP
- Réseaux fiables ou non fiables

QUAND VOUS AGISSEZ

Cadre temporel

*Méthodes de récupération

**Technologies prises en charge : PKI, FIDO2, OATH

AVANTAGES CLÉS

Couverture complète

Avec DigitalPersona, les organisations peuvent être assurées qu'elles adoptent une approche holistique de la sécurité d'accès en appliquant un MFA fort à toutes les applications (dans le cloud, personnalisées et héritées), aux systèmes et aux réseaux - tout en sécurisant l'accès pour toutes les identités, y compris les employés, les clients, les fournisseurs et les partenaires.

En plus de la série traditionnelle de facteurs d'authentification - quelque chose que vous avez, quelque chose que vous êtes ou quelque chose que vous savez - DigitalPersona peut être combiné avec les sites et services Microsoft, ajoutant une authentification pour les facteurs de risque contextuels que sont le temps, la vitesse et l'emplacement. Ces derniers couvrent ce que vous faites, où vous êtes et quand vous agissez, ce qui vous permet d'adapter précisément votre exposition au risque à la posture de sécurité optimale pour votre organisation.

Authentification polyvalente

Le large éventail de méthodes et de facteurs d'authentification pris en charge par DigitalPersona élimine à la fois la dépendance et le fardeau des utilisateurs, ce qui permet aux organisations d'adopter les meilleures pratiques d'authentification forte sans compromettre l'expérience et la productivité de l'utilisateur. Cette gamme croissante d'options d'authentification offre une liberté de choix sans précédent qui permet aux organisations de combiner commodité et sécurité, aujourd'hui et à l'avenir.

Déploiement rapide et évolutivité

Déploiement rapide et mise en service en quelques jours. Grâce à sa prise en charge native d'Active Directory®, Azure® AD et Microsoft 365®, DigitalPersona vous permet de vous intégrer facilement à votre infrastructure informatique existante en utilisant les outils et ressources informatiques actuels et d'obtenir une flexibilité en matière de personnel et une réduction des frais généraux initiaux et continus - tout en gagnant en tranquillité d'esprit avec une solution à l'épreuve du temps qui évolue avec les besoins croissants de l'entreprise, les exigences de sécurité et les réglementations de l'industrie.

	HID DIGITALPERSONA
	CARACTÉRISTIQUES
Gestion centralisée	Active Directory – Définition des stratégies de sécurité pour les utilisateurs et les ordinateurs du domaine à l'aide des objets de stratégie de groupe Azure Active Directory – Définition des stratégies de sécurité DigitalPersona pour les utilisateurs et les ordinateurs du domaine
Console d'administration Web	Console d'administration Web des utilisateurs et des authentifiateurs
Authentification à plusieurs facteurs pour la connexion à Windows	**FACTEURS D'AUTHENTIFICATION** **Ce que vous SAVEZ :** Mot de passe Windows, code PIN en tant qu'authentificateurs de connaissances utilisateur **Ce que vous ÊTES :** Empreintes digitales et reconnaissance faciale comme authentificateurs inhérents à l'utilisateur **Ce que vous AVEZ :** Jetons de mot de passe à usage unique (OTP) ; cartes à puce et/ou clés de sécurité (USB-A, USB-C, NFC), telles que HID Crescendo ® avec prise en charge de FIDO2, PKI, OATH ; cartes d'accès physique (PACS) (cartes d'accès sans contact, cartes inscriptibles sans contact, ID mobile) ; dispositifs Bluetooth (mobile, montre, écouteurs) en tant qu'authentificateurs de la possession de l'utilisateur.
Accès au kiosque rapide	Station de travail à utilisateur partagé (« Kiosque ») Contrôle de connexion : Appliquer des politiques d'authentification avancées pour les postes de travail partagés (comme les kiosques sans rendez-vous) où les personnes utilisent leurs identifiants individuels pour déverrouiller Windows et se connecter aux applications. Prise en charge de plusieurs kiosques et des environnements de travail partagés.
Récupération du mot de passe en libre-service	Récupération du mot de passe de l'utilisateur par le biais d'une question posée lors de la connexion à Windows ou d'un portail web en libre-service. Les questions peuvent être créées par les utilisateurs ou prédéterminées par l'administrateur.
Fédération des fournisseurs d'identité	Le fournisseur d'identité (IdP) prend en charge WS-FED et OpenID Connect pour se fédérer à des applications telles que Azure AD pour Microsoft 365, Salesforce, SharePoint et ADFS.
	CLIENTS ET COMPOSANTS
Client DigitalPersona	Se connecte au serveur DigitalPersona pour la connexion, l'inscription, l'authentification et l'application des stratégies Windows
Console DigitalPersona avec inscription des participants	Permet à l'utilisateur de s'inscrire ou de participer à l'inscription pour les outils de bureau et WEB
Plug-in RADISU DigitalPersona	Plug-in RADIUS pour Microsoft Network Policy Server (NPS) afin d'assurer l'accès à distance par le biais de l'authentification électronique (2FA)
Extension ADFS DigitalPersona	Active les capacités d'authentification à plusieurs facteurs pour les utilisateurs qui se connectent à l'aide de Microsoft Active Directory Federation Services (ADFS)
	CARACTÉRISTIQUES TECHNIQUES
Systèmes d'exploitation du logiciel client	Windows 11, Windows 10, Windows 8,1 (mode bureau), Windows Server 2016, 2019, 2022
Système d'exploitation du logiciel serveur	Windows Server 2022, 2019, 2016 et 2012 R2
VDI (Infrastructure de Bureau Virtuel)	RDP, ICA (Citrix), VMWare Horizon, VMWare Blast. REMARQUE : Les protocoles USB de virtualisation et d'authentification varient selon le produit VDI.

hidglobal.com

Amérique du Nord : +1 512 776 9000 | Numéro gratuit : 1 800 237 7769
Europe, Moyen-Orient, Afrique : +353 91 504 900
Asie-Pacifique : +852 3160 9800 | Amérique latine : +52 55 9171 1108
Pour plus de numéros de téléphone internationaux, cliquez ici

2023-05-03-iams-hid-digitalpersona-ds-fr PLT-07180
Part of ASSA ABLOY