



HID DigitalPersona® Premium

La bonne combinaison de facteurs





Authentification composite

La bonne combinaison de facteurs, au bon moment



CE QUE VOUS SAVEZ

Mot de passe
PIN
Questions de récupération de compte



QUI VOUS ÊTES

Empreinte
Reconnaissance faciale



CE QUE VOUS AVEZ

Cartes à puces
Tokens USB
Carte sans contact
Carte de proximité
Dispositifs Bluetooth
Mots de passe uniques
Clé FIDO U2F
Apple® Watch



CE QUE VOUS FAITES

Dynamique de frappe



OÙ VOUS ÊTES

Localisation GPS
Adresse IP
Protocole IWA (Integrated Windows Authentication)



À QUEL MOMENT

Cadre temporel

Pour que leur sécurité soit effective, les entreprises s'efforcent de faire adhérer les utilisateurs à des politiques d'authentification complexes. Elles doivent se libérer de cette trop grande dépendance à l'égard du facteur humain. DigitalPersona propose une solution « human-proofed » : celle-ci assure systématiquement le niveau de sécurité adéquat en se basant sur la plus large sélection de facteurs d'authentification possible. Avec DigitalPersona, vous disposez de la meilleure des protections avec une expérience utilisateur fluide et positive.



Points forts

Ne négliger aucune variable

En plus des facteurs traditionnels d'authentification ("ce que vous avez", "ce que vous êtes" et "ce que vous savez"), DigitalPersona propose une authentification fondée sur plusieurs facteurs de risques contextuels : le temps, la vitesse, le lieu et le comportement. Ces critères permettent de prendre en compte ce que vous faites, où vous êtes et quand vous agissez, pour définir un degré d'exposition au risque et mettre en place des mesures de sécurité adaptées.

Couverture complète

Assurer une couverture complète est enfin possible. DigitalPersona prend en charge TOUTES vos applications, y compris le web, le cloud, Windows, les mobiles, VDI et le VPN. DigitalPersona inclut même les applications mainframe existantes, qui continuent à jouer un rôle essentiel dans les environnements informatiques de nombreuses organisations. Employés, clients, fournisseurs et partenaires : avec DigitalPersona, tous sont couverts, sans exception.

Solution « Human-proofed »

Grâce au large éventail de facteurs d'authentification proposés par DigitalPersona, les entreprises peuvent mettre en place une politique d'authentification renforcée sans craindre de dysfonctionnement lié à un manque de coopération des utilisateurs.

Grâce aux nombreuses options d'authentification proposées, votre organisation n'est plus contrainte de suivre une voie prédéterminée : vous pouvez trouver le juste équilibre entre confort d'utilisation et protection, en fonction de vos objectifs de sécurité spécifiques.

Adaptabilité rapide

Avec DigitalPersona, vous pouvez vous appuyer sur votre infrastructure informatique existante pour obtenir un déploiement plus rapide que celui proposé par les autres solutions du marché. Les entreprises peuvent ainsi être opérationnelles en quelques jours, plutôt qu'en quelques semaines, ou en quelques mois. DigitalPersona fournit une prise en charge native pour Active Directory®, Azure® AD et Office 365®, pour vous permettre de mettre à profit votre expertise Microsoft®. Le travail de gestion est également simplifié : aucun outil propriétaire n'est nécessaire pour administrer votre système. L'implémentation de DigitalPersona est réalisée au prix de perturbations minimales. Cette solution vous offre une flexibilité totale en termes de ressources humaines et minimise vos investissements et dépenses. Elle se base sur une architecture extensible et durable, conçue pour s'adapter facilement aux nouveaux facteurs d'authentification, dès leur apparition.



Version Premium : composants-clés

Modules clients

Identification DigitalPersona pour Windows	<ul style="list-style-type: none"> Fournit une connexion rapide et sécurisée aux différents appareils Inclut les politiques comportementales et contextuelles fondées sur la prévention des risques
Client DigitalPersona Console DigitalPersona avec inscription, moteur de gestion et composants de base	<ul style="list-style-type: none"> Connexion au serveur DigitalPersona pour les enregistrements, les authentifications et l'application des politiques Fournit des outils pour les enregistrements utilisateurs
Client d'inscription DigitalPersona Mobile	<ul style="list-style-type: none"> Possibilité d'enregistrement délégué (attended enrollment) sur plateforme mobile Windows pour l'enregistrement d'utilisateurs en mode déconnecté
Gestionnaire de mots de passe DigitalPersona	<ul style="list-style-type: none"> Applique une AMF renforcée pour Windows, le web et les applications héritées L'AMF déverrouille le nom d'utilisateur/mot de passe pour remplir les formulaires d'authentification Inclut la randomisation des mots de passe et la réinitialisation en libre-service
Portail SSO SAML DigitalPersona	<ul style="list-style-type: none"> Permet l'intégration d'applications en utilisant le protocole SAML Fournit un portail SSO via navigateur pour accéder aux applications compatibles SAML
API de gestion des accès DigitalPersona	<ul style="list-style-type: none"> SDK d'authentification multifacteurs pour l'intégration d'applications personnalisées SDK natif - les interfaces incluent C, Java et .NET Interface de services web - pour l'intégration avec les applications web Plus besoin d'une authentification par mot de passe

MODUS SERVEURS

Base de données et moteur de politiques de serveur (AD ou LDS)	<ul style="list-style-type: none"> Crée, distribue et applique les politiques d'authentification multifactorielle Sert de répertoire central pour les identifiants des utilisateurs
Extension VPN RADIUS DigitalPersona	<ul style="list-style-type: none"> Fournit une authentification à deux facteurs pour l'accès à distance
Fournisseurs d'identité SAML DigitalPersona	<ul style="list-style-type: none"> Permet aux utilisateurs de s'authentifier auprès d'un fournisseur d'identité (IdP) et d'accéder ensuite aux applications sans authentification supplémentaire



Options d'intégration Premium

Pour assurer une prise en charge de toutes vos applications, cette version Premium vous offre de nombreuses options d'intégration : intégration native, SAML ou encore notre propre gestionnaire de mots de passe, leader du secteur.

SSO (SAML)

- Intégration des applications compatibles SAML
- Portail d'applications SSO pour les plateformes Windows et mobile
- Possibilité pour les clients de supprimer tous les mots de passe

API de gestion des accès

- La gestion complète par API de DigitalPersona permet une intégration avancée
- Évolutivité optimale pour les services on-prem et cloud

Gestion des mots de passe

- Superposition pratique et sécurisée d'applications d'authentification
- Possibilité pour les clients de provisionner rapidement des applications sans modifier le code source

Identification Windows

- Intégration prête à l'emploi avec l'identification Windows
- Prise en charge de tous les facteurs, y compris les facteurs contextuels et les facteurs de risque
- Jusqu'à 3-FA, toute combinaison possible



WEB



CLOUD



MOBILES



SERVEURS

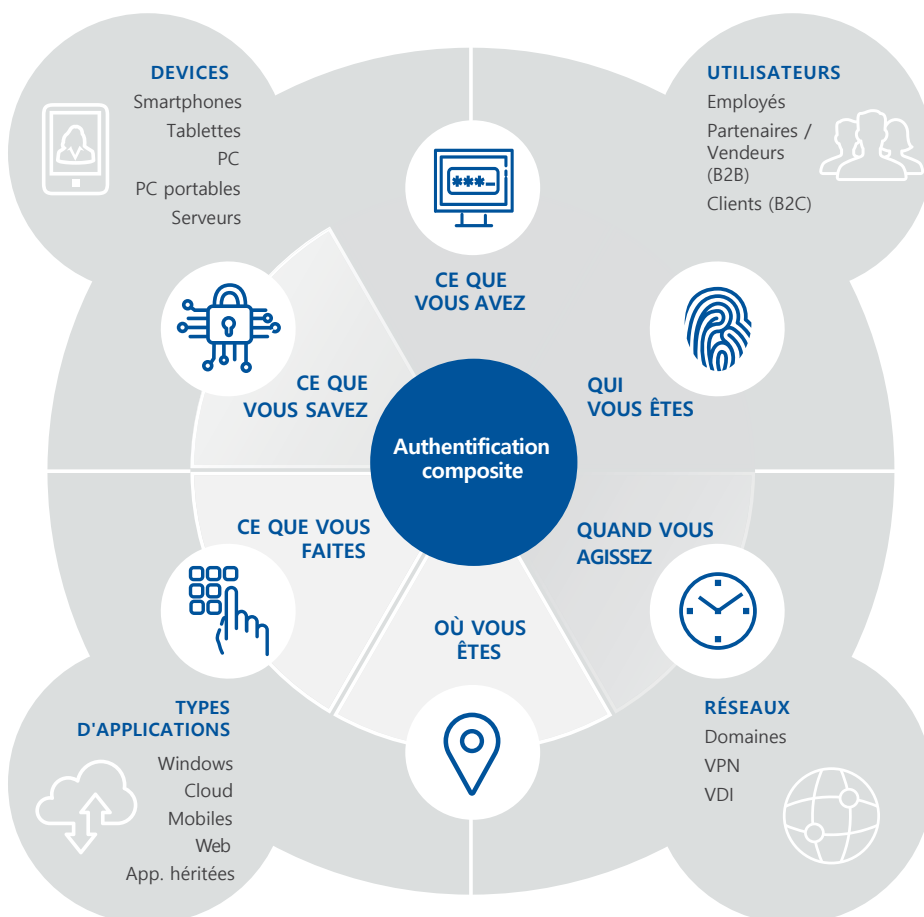


WINDOWS



DigitalPersona fait la différence

DigitalPersona vous offre une approche complète permettant d'optimiser la sécurité de chaque application, chaque utilisateur, à chaque instant. Cette solution révolutionne l'authentification et offre des niveaux de protection inédits garantissant l'identité numérique de vos employés, clients et partenaires, pour protéger l'accès aux réseaux, aux applications et aux données.





Fonctionnalités et spécifications Premium

Console d'administration web	Administration des utilisateurs DigitalPersona LDS et AD à partir de l'infrastructure backend de DigitalPersona LDS
Authentification composite pour la connexion à Windows	<p>Facteurs d'authentification :</p> <p>Savoir : mots de passe Windows, PIN, questions de récupération de comptes</p> <p>Avoir : OTP, cartes sans contact (cartes mémoire HID iCLASS, MIFARE Classic 1k, 4k et mini cartes mémoire) et Seos, cartes à puce (compatibles PKCS11 et CSP), cartes de proximité (HID 125 kHz) et appareils Bluetooth. Tokens. Clés FIDO U2F, Apple Watch, FIDO2 ex : clé HID Crescendo, carte C2300</p> <p>Être : Empreintes digitales, authentification du visage, lecteurs Lumidigm®</p> <p>Faire : Dynamique de frappe</p> <p>Où : Adresse IP, IWA (<i>Integrated Windows Authentication</i>)</p> <p>Quand : Cadre temporel</p>
SSO (<i>Single Sign-On</i>)	<p>Gestion de mots de passe – Fournit une signature unique et applique une authentification renforcée sans altérer les applications concernées.</p> <p>SAML - Authentification fédérée SSO, portail d'applications SSO accessible depuis les PC Windows, Mac et appareils mobiles</p>
Politique d'authentification par application	Politiques par application - Ajout d'identifiants supplémentaires pour des applications spécifiques
Accès rapide aux kiosques	Contrôle des accès aux postes de travail partagés (« kiosques ») : Application de politiques d'authentification avancées pour les postes de travail partagés sur lesquels chaque employé utilise ses propres identifiants pour déverrouiller Windows et se connecter à des applications. Prise en charge de plusieurs environnements de kiosques sous Citrix/RDP
Récupération autonome des mots de passe	Si un utilisateur oublie son mot de passe, il peut utiliser son PC pour répondre à une série de questions prédéfinies (gestion centralisée par le service informatique)
Rapports	Gestion, visualisation et programmation de rapports d'activité et d'état préconfigurés pour les utilisateurs et applications, depuis un emplacement centralisé
Système d'exploitation logiciel client	Windows 10®, Windows 8.1® (mode desktop), Windows 7® (32- and 64-bit), Windows Embedded Standard® 2009 (nécessite .NET 4.5), Windows Server® 2008, 2012, 2016, et 2019 et Linux (choisir des clients légers)
Systèmes d'exploitation logiciel serveurs	Windows Server 2019, 2016, 2012 et 2012 R2, Windows Server 2008 R2 (64-bit)
Mobiles	Portail d'application SSO accessible depuis les appareils mobiles. IntSDK pour l'intégration des applications mobiles via les services web natifs iOS et Android™.
Navigateurs	Internet Explorer® versions 8-11, Chrome® dernière version, Firefox®, Edge Chromium
VDI (Virtual Desktop Infrastructure)	XenApp (serveur) 6.5, XenDesktop 6.2 et 7, Receiver et Online; Plug-In 11 et 12, VMWare View et VMWare Horizon

Amérique du nord : +1 512 776 9000 • Gratuit : 1 800 237 7769
• Europe, Moyen Orient, Afrique : +44 1440 714 850
• Asie Pacifique: +852 3160 9800 • Amérique latine : +52 55 9171 1108

© 2020 HID Global Corporation/ASSA ABLOY AB. Tous droits réservés. HID, HID Global, le logo HID Blue Brick, le design de la chaîne, HID Mobile Access®, iCLASS SE® et Seos® sont des marques ou des marques déposées de HID Global ou de ses concédants/fournisseurs aux États-Unis et dans d'autres pays et ne peuvent être utilisés sans autorisation. Toutes les autres marques commerciales, marques de service et noms de produits ou de services sont des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

2020-07-28-iams-digitalpersona-premium-br-en

PLT-04486

Une marque du groupe ASSA ABLOY

ASSA ABLOY



hidglobal.com