HID DigitalPersona® Premium

Flexibility and convenience when wanted,
Strength and security where needed

Overview

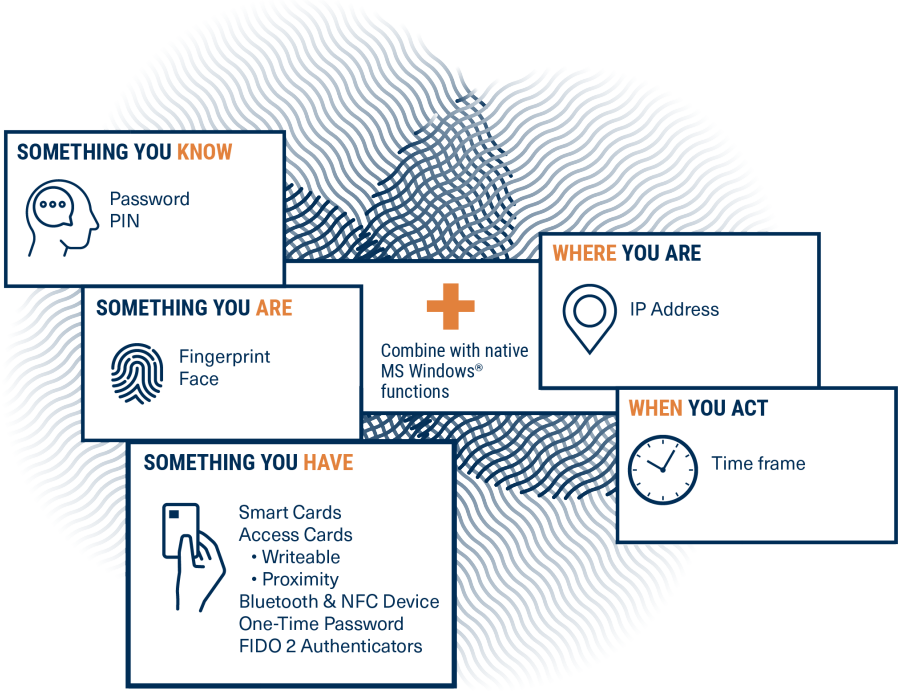
HID DigitalPersona®, a key element within HID Global's multi-factor authentication portfolio, transforms the way IT professionals protect the integrity of their digital organization by going beyond traditional two-factor and multi-factor authentication. Building upon the fast and secure Windows® Logon and VPN access found in DigitalPersona Logon for Windows, Premium adds advanced integration options to secure all applications, systems, and networks. Additional client and server components included in Premium are SSO, Access Management API and Password Manager modules. Premium offers the ability to deploy the optimal set of authentication factors for every user, application, device and network — moment by moment. It accomplishes this while uniquely serving IT through unparalleled ease of integration and ongoing maintenance.

DIGITALPERSONA® BENEFITS:

- Complete Coverage
- Versatile Authentication
- Rapid Adaptibility

Breadth of Authentication

Full protection requires organizations to eliminate their dependence on the ability of humans to adhere to complex authentication policies. DigitalPersona provides the right level of security through the broadest possible selection of authentication factors delivering a completely frictionless user experience and the strongest protection available in the industry.



Key Benefits

COMPLETE COVERAGE

In addition to the traditional set of authentication factors — something you have, something you are, or something you know — DigitalPersona may be optionally combined with Microsoft Sites and Services adding authentication for the contextual risk factors of time, velocity, and location. The latter cover what you do, where you are and when you act, allowing you to precisely match your risk exposure to the optimal security posture for your organization. Supporting applications such as websites, cloud, Windows, mobile, VDI and VPN, DigitalPersona goes beyond contemporary applications to include legacy mainframe apps, which continue to play a vital role in many organization's computing environments. Moreover, DigitalPersona ensures secure access for all your identities from employees to customers, vendors, and partners with flexible authentication configured for your security needs.

VERSATILE AUTHENTICATION

DigitalPersona's widest array of authentication factors eliminate both the reliance and burden on users enabling organizations to lead with strong authentication postures without fear of compromise due to lack of user compliance. The range of authentication options means you are never forced down a predetermined path. With this unprecedented freedom of choice, organizations can balance usability and protection based on specific security goals.

RAPID ADAPTIBILITY

With DigitalPersona, you can leverage your existing IT infrastructure and deploy more quickly than other solutions on the market today. Organizations are typically up and running in days — not weeks or months. DigitalPersona also provides native support for Active Directory, Azure AD and Office 365, enabling you to leverage your existing Microsoft expertise. Administration is simplified: no proprietary tools are needed to learn, manage or administer the system.

You can implement with minimal disruption, total staffing flexibility and both lower up-front and on-going overhead costs. DigitalPersona provides peace of mind through extensible architecture, designed to easily accommodate new authentication factors as they emerge.

Premium Key Components

CLIENT MODULES	
DigitalPersona Logon for Windows	• Provides fast and secure device logon
DigitalPersona Client DigitalPersona Console with Enrollment, Policy Engine and Core	• Connects to DigitalPersona server for enrollment, authentication and policy enforcement • Provides tools for user enrollment
DigitalPersona Password Manager	• Enforces strong MFA for Windows, web and legacy apps • MFA unlocks username/password to fill in authentication forms • Includes password randomization and self-serve reset
DigitalPersona SSO Portal	• Allows for app integration using OpenID Connect or WS-Fed protocols • Provides browser-based SSO Portal for accessing OpenID Connect or WS-Fed enabled apps
DigitalPersona Access Management API	• MFA authentication SDK for custom app integration • Native SDK - interfaces include C#, Java and .NET • Web services interface – for integration with web apps • Eliminates the need for password-based authentication

ACCESS SERVER MODULES	
DigitalPersona Server Policy Engine and DB (AD or LDS)	• Creates, distributes, and enforces MFA policies • Acts as a central repository for user credentials
DigitalPersona RADIUS VPN Extension	• Provides two-factor authentication for remote access
DigitalPersona Identity Provider	• Allows users to authenticate at an identity provider (IdP) and then access apps without additional authentication
DigitalPersona ADFS Extension	• Enables multi-factor authentication capabilities for users logging on using Microsoft Active Directory Federation Services (ADFS)

Premium Integration Options

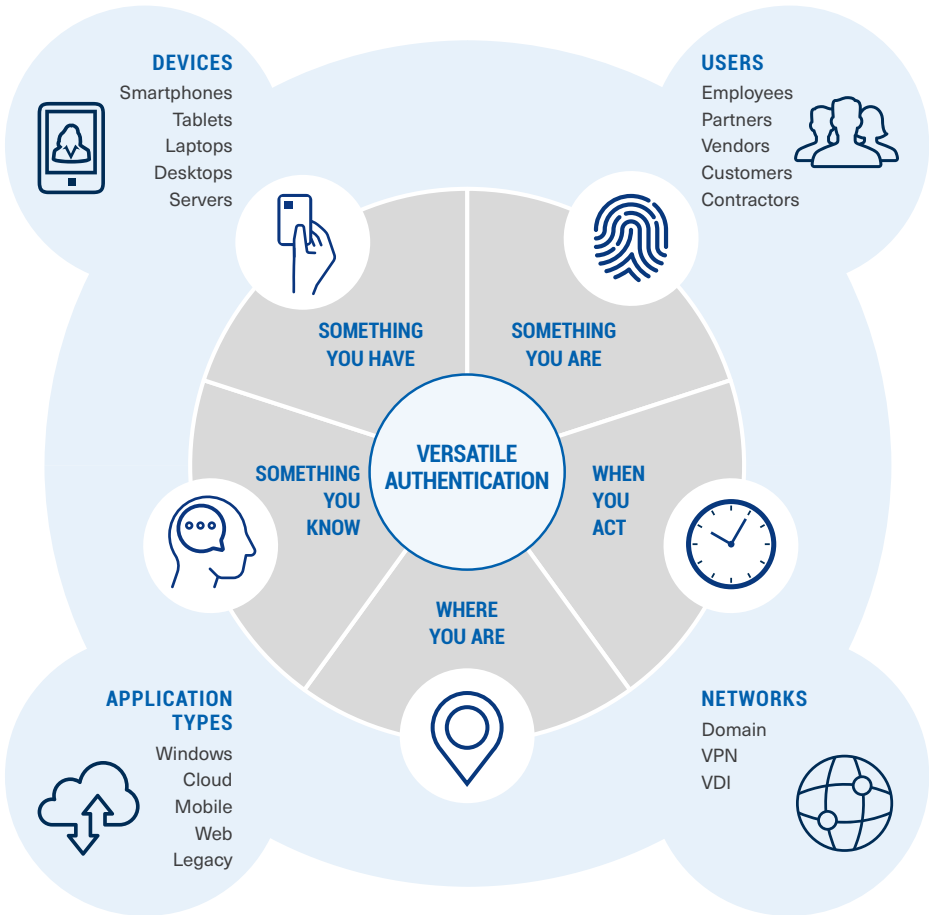
A rich array of integration options – helps to ensure that all applications are covered.

WEB SSO	ACCESS MANAGEMENT API	PASSWORD MANAGER	WINDOWS LOGON
• Integration of OpenID Connect or WS-Fed enabled applications • SSO application portal on both Window and mobile platforms • Customers option to remove all passwords	• Comprehensive DigitalPersona API management enables tightly integrated implementation • Full scalability across on-premise and cloud services	• Secure and convenient authentication application overlay • Allows customers to quickly provision apps without modifying source code	• Out of the box integration with Windows logon • Up to 3-FA, any combination

web cloud mobile server windows

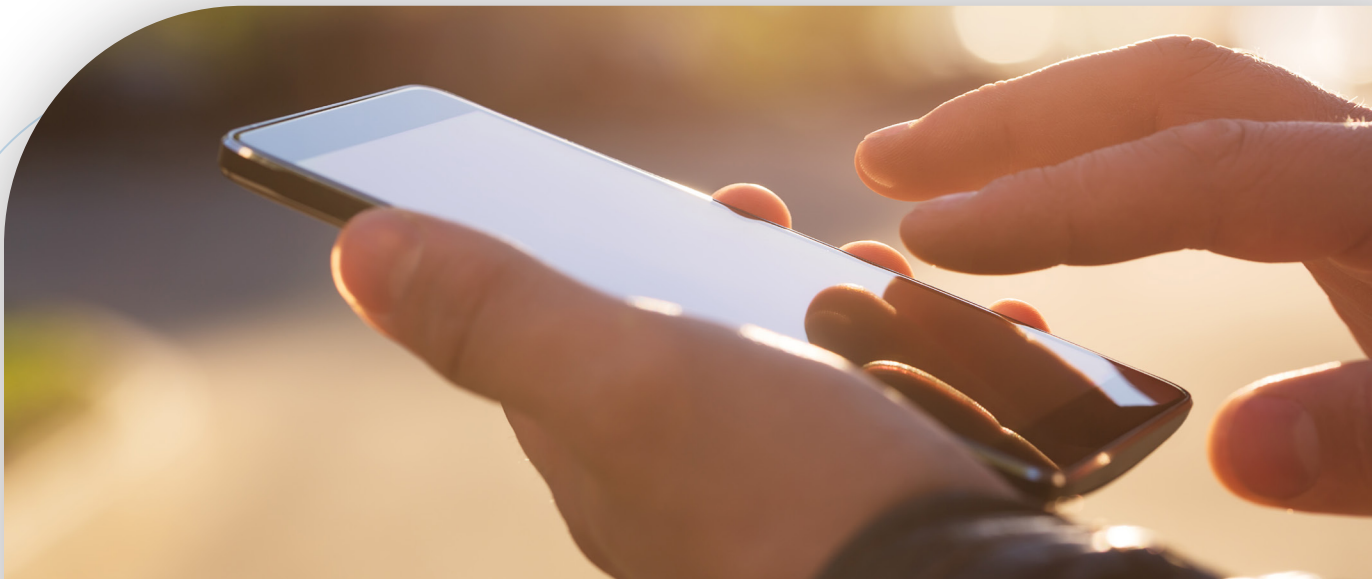
The DigitalPersona Difference

The most complete way to optimize security for every app, every user, every time. DigitalPersona transforms authentication and provides entirely new levels of protection ensuring identity-focused zero trust security for your employees, customers and partners, as well as protecting access to networks, applications and data.



Premium Features and Specifications

Web Administration Console	Web based user and authenticator management console
Multi-factor Authentication for Windows Logon	**Authentication Factors:** **Something you KNOW:** Windows Password, PIN as user knowledge authenticators **Something you ARE:** Fingerprint, Face Recognition biometrics as user inherent authenticators **Something you HAVE:** One Time Password (OTP) tokens; Smart credentials (Smart Cards, Security Keys USB-A and USB-C) with support for FIDO2, PKI, OATH; PACS credentials (Contactless Cards, Contactless Writeable Cards, Mobile ID); Bluetooth and NFC Devices as user possession authenticators
Policy Management	Workstation and user level configuration of needed authentication factors
SSO (Single Sign-On)	**Password Manager –** Provides Single Sign-On and enforces strong authentication without modifying underlying applications **OpenID Connect and WS-Fed –** Federated identity SSO, SSO application portal accessible from Windows PC, Mac and mobile devices
Per Application Authentication Policy	**Per Application Policy –** adds additional authentication credential to specified applications
Fast Kiosk Access	**Shared-User Workstation ("Kiosk") Logon Control:** Enforce versatile authentication policies for shared workstations i.e., kiosks, where users may present credentials to unlock Windows and log into applications.
Self-Service Password Recovery	Forgotten password challenge questions defined by user or centrally managed by administrator
Client Software Operating System	Windows 11, Windows 10®, Windows 8.1® (desktop mode), Windows Embedded Standard® 2009 (requires .NET 4.5), Windows Server® 2016, 2019 and Linux (select thin clients)
Server Software Operating System	Windows Server 2022, 2019, 2016, 2012 and 2012 R2
Mobile	SSO application portal accessible from mobile device. DigitalPersona mobile app available for iOS and Android utilizing OATH OTP and Push Notification services
Browsers	Internet Explorer® versions 8-11, Chrome® latest version, Firefox®, Edge Chromium
VDI (Virtual Desktop Infrastructure)	RDP, ICA (Citrix), VMWare Horizon, VMWare Blast. NOTE: USB Virtualization and Authenticator Protocols vary by VDI product.
Azure Active Directory	Supports a wide variety of Authentication Factors (Password, Fingerprint, Contactless ID, Contactless writable card, Face, FIDO2, Push Notification, SMS, PIN, Bluetooth, OTP, Security Questions) for Azure Active Directory domain-joined machines



hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2021-11-10-iams-digitalpersona-premium-br-en
PLT-04486

Part of ASSA ABLOY