HID DigitalPersona® Premium

The Right Mix of Factors

Overview

HID's DigitalPersona® transforms the way IT executives protect the integrity of the digital organization by going beyond traditional two-factor and multi-factor authentication. DigitalPersona Premium builds on the fast and secure Windows® Logon and VPN access found in DigitalPersona Logon for Windows, adding advanced integration options to secure all applications, systems and networks. Additional client and server components included in Premium are SSO (SAML), 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.

BENEFITS

- Closes Every Gap
- Complete Coverage
- Human-proofed
- Rapid Adaptibility

Composite Authentication

The Right Mix of Factors, Moment by Moment

WHAT YOU KNOW

Password

PIN

Recovery Questions

WHO YOU ARE

Fingerprint

Face Recognition

WHAT YOU HAVE

Smartcards and USBs

Contactless Card

Proximity Card

Bluetooth Device

One-Time Password

Apple Watch®

FIDO U2F Key

WHAT YOU DO

Keystroke

Swipe

WHERE YOU ARE

GPS Location

IP Address

IWA – Integrated Windows Authentication

WHEN YOU ACT

Time Frame

Full protection requires organizations to eliminate their dependence on the ability of humans to adhere to complex authentication policies. DigitalPersona offers a human-proofed solution that delivers 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

Closes Every Gap

In addition to the traditional set of authentication factors– what you have, are and know – DigitalPersona offers authentication for the contextual risk factors of time, velocity, location and behavior. 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.

Complete Coverage

Complete coverage is finally possible. DigitalPersona supports ALL your applications, including web, cloud, Windows, mobile, VDI and VPN. DigitalPersona goes beyond contemporary applications to include even legacy mainframe apps, which continue to play a vital role in many organization's computing environments. And with DigitalPersona, ALL your constituencies are covered – employees, customers, vendors and partners.

Human-proofed

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're 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 ongoing overhead costs. DigitalPersona's extensible architecture also provides peace of mind. DigitalPersona is 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 • Includes behavioral and contextual risk-based policies
DigitalPersona Client DigitalPersona Console with Enrollment, Policy Engine and Core	• Connects to Altus server for enrollment, authentication and policy enforcement • Provides tools for user enrollment
DigitalPersona Mobile Enrollment Client	• Offers strong attended enrollment on a Windows mobile platform to onboard users in disconnected mode
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 SAML SSO Portal	• Allows for app integration using SAML protocol • Provides browser-based SSO Portal for accessing SAML 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
	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 SAML Identity Provider	• Allows users to authenticate at an identity provider (IdP) and then access apps without additional authentication

Premium Integration Options

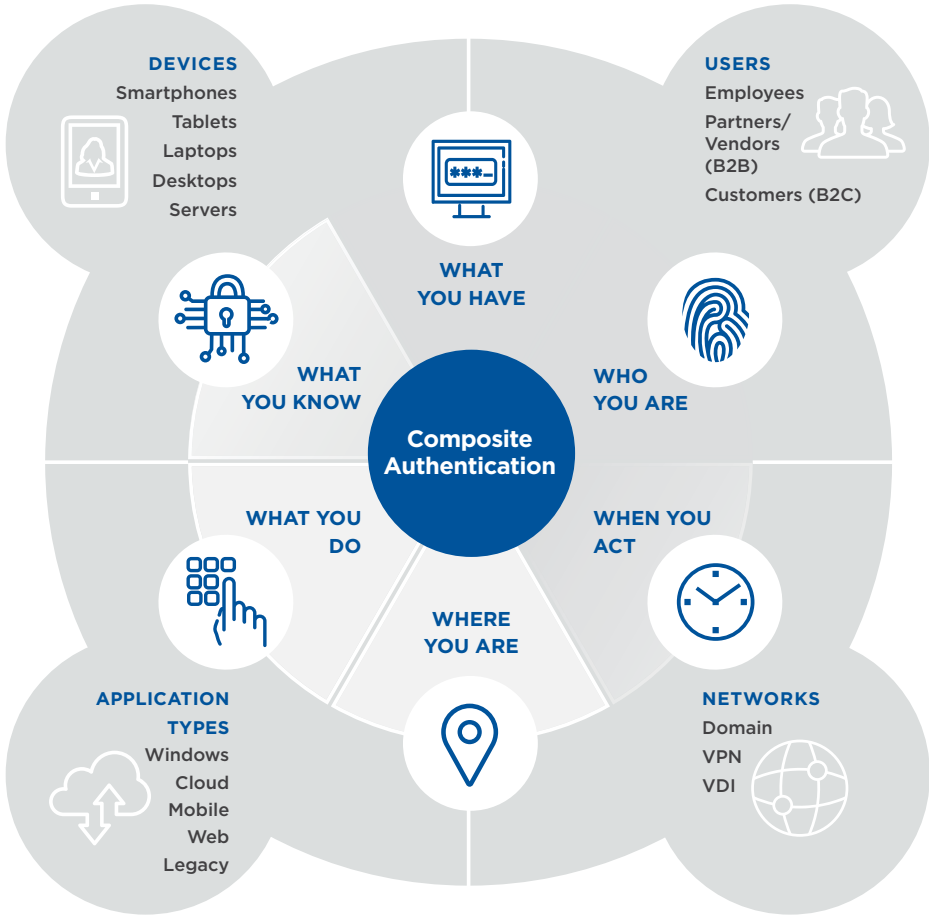
A rich array of integration options – from native integration to SAML to our own industry-leading password manager – helps to ensure that all applications are covered.

SSO (SAML)	Access Management API	Password Manager	Windows Logon
• Integration of SAML 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 • Includes all factors including contextual and risk-based • 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 the digital identity of employees, customers and partners, as well as protecting access to networks, applications and data.



Premium Features and Specifications

Web Administration Console	Administer DigitalPersona LDS and AD users with the DigitalPersona LDS backend infrastructure
Composite Authentication for Windows Logon	**Authentication Factors:** ▪ **Know:** Windows password, PIN, recovery questions ▪ **Have:** OTP, contactless cards (HID iCLASS memory cards, MIFARE Classic 1k, 4k and mini memory cards), smart cards (PKCS11 and CSP-compatible), proximity cards (HID 125 kHz) and Bluetooth devices; Apple Watch; FIDO U2F Key ▪ **Are:** Fingerprint, face recognition ▪ **Do:** Keystroke, swipe ▪ **Where:** GPS location, IP address, Integrated Windows Authentication (IWA) ▪ **When:** Time frame, Geo-velocity
SSO (Single Sign-On)	**Password Manager –** Provides Single Sign-On and enforces strong authentication without modifying underlying applications **SAML –** 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 specific applications
Fast Kiosk Access	Shared-User Workstation (“Kiosk”) Logon Control: Enforce advanced authentication policies for shared workstations (such as walk-up kiosks) where people use their individual credentials to unlock Windows and log into applications. Support for multiple kiosk environments under Citrix/RDP
Self-Service Password Recovery	If users forget their passwords, they can access their PC by answering a set of predefined questions (this can be customized and centrally managed by IT)
Reports	Generate, view and schedule preconfigured activity and status reports for users and applications from a centralized location
Client Software Operating System	Windows 10®, Windows 8.1® (desktop mode), Windows 7® (32- and 64-bit), Windows Embedded Standard® 2009 (requires .NET 4.5), Windows Server® 2008 and 2012 and Linux (select thin clients)
Server Software Operating System	Windows Server 2012 and 2012 R2, Windows Server 2008 R2 (64-bit)
Mobile	SSO application portal accessible from mobile device. Mobile Access SDK for mobile app integration using: Web Services from iOS and Android™ native wrapper over Web Services on Android mobile devices
Browsers	Internet Explorer® versions 8-11, Chrome® latest version, Firefox®
VDI (Virtual Desktop Infrastructure)	XenApp (server) 6.5, XenDesktop 6.2 and 7, Receiver and Online Plug-In 11 and 12, VMWare View and VMWare Horizon

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 5081 1650

2019-05-23-iams-digitalpersona-premium-br-en PLT-04486

An ASSA ABLOY Group brand

ASSA ABLOY

hidglobal.com