



# DigitalPersona® Pro Enterprise

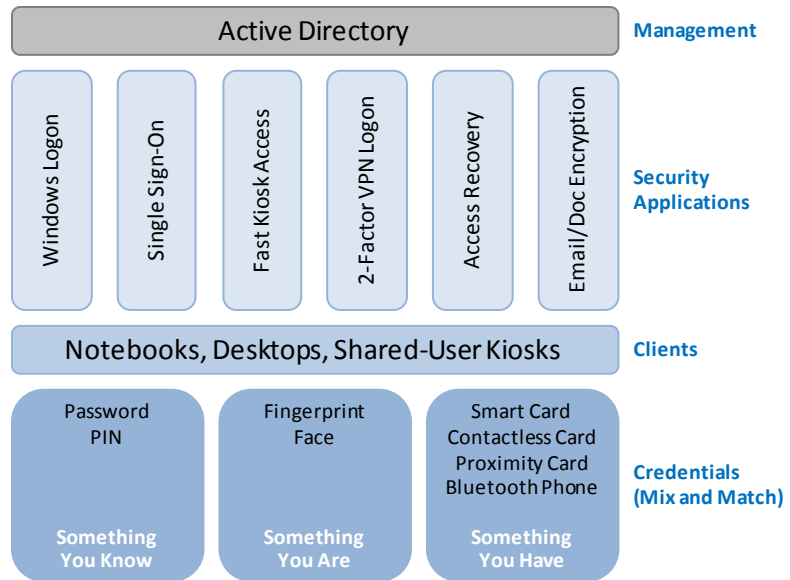
Authentication and Access Management  
centrally-managed via Active Directory

## DigitalPersona Pro Enterprise

DigitalPersona Pro Enterprise is an authentication and access management suite that is administered through Active Directory. It secures user access to data, applications, computers and networks in industries such as healthcare, financial services and government. DigitalPersona Pro Enterprise gives organizations a cost-effective way to increase security and simplify compliance.

- **Strong Authentication.** Centrally control access to notebooks, desktops and shared workstations, as well as applications and networks, from a single management console.
- **Multi-factor protection.** Mix and match authentication credentials (passwords, biometrics, cards, phones, etc.) to reliably know who's doing what. Randomize passwords to prevent users from accessing business data from uncontrolled devices.
- **Single Sign-On (SSO).** Reduce the exploding costs and burdens of complying with new password mandates without changes to your enterprise applications.
- **Emergency access recovery.** Prevent lockouts when credentials are lost, stolen or forgotten (IT-assisted and self-service).
- **“Token-less” VPN security.** Get multi-factor security for VPN access without having to carry special token hardware.
- **Integration with Active Directory.** Create, deploy and monitor security policies for your domain accounts and organizations using familiar AD Group Policies and tools.
- **Modular platform.** Start with the solutions you need today and add new capabilities as your requirements grow.

## DigitalPersona Pro Enterprise



## Easy to Deploy

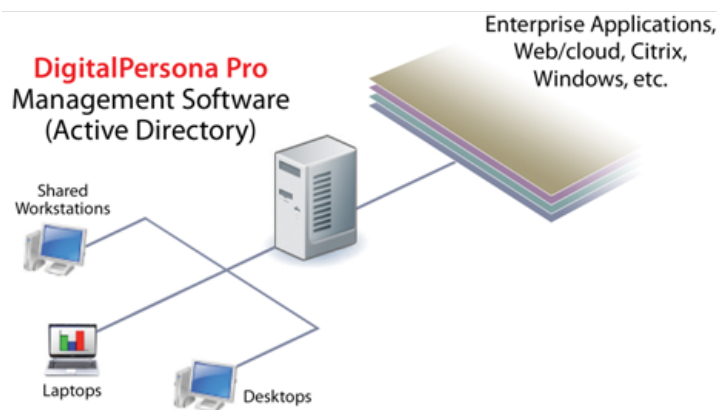
DigitalPersona Pro Enterprise gives you advanced authentication and access management for securing your notebooks, desktops and “kiosk-style” shared workstations. It takes advantage of your Active Directory infrastructure for high scalability and fault tolerance without requiring any special server hardware. Using familiar Group Policy tools and snap-ins, DigitalPersona Pro Enterprise makes it easy to create, deploy, enforce and monitor security policies across your domain groups and accounts.

## Flexible Multi-Factor Security

DigitalPersona Pro Enterprise gives you the ability to deploy true, multi-factor security that can be easily tailored to the needs of different groups of users. You can mix and match authentication credentials, allowing you to follow industry best practices for combining something users **know** (password or PIN), something they **are** (fingerprint or face recognition) and something they **have** (smart card, contactless card, proximity card or Bluetooth phone).

## Extensible Platform

DigitalPersona Pro Enterprise provides a powerful, consistent platform for security applications. It helps you address pressing issues in a way that scales up as your needs evolve.



# Key Features of DigitalPersona Pro Enterprise

## Centralized Management

- **Active Directory** – set security policies for domain users and groups using Group Policy Objects (GPOs).
- **Reporting** – monitor and document enforcement of security policies.

## Strong Authentication

- **Multi-credential authentication** – mix and match authentication credentials: Windows Password, PIN, Fingerprint, Face, Contactless Cards (HID iCLASS memory cards; HID Crescendo C700 PKI cards; MIFARE Classic 1k, 4k and mini memory cards), Smart Cards (PKCS11 and CSP-compatible), Proximity Cards (HID 125 kHz) and Bluetooth Phones.
- **Multi-factor security** – require combinations of credentials to address growing compliance mandates.
- **Attended enrollment** – require a supervisor’s permission when users enroll or change credentials.
- **Password randomization** – enforce use of strong authentication by preventing users from knowing their password.

## Windows Logon

- **PC logon control** – enforce advanced authentication policies for PC logon.
- **Roaming** – store user credentials centrally for automatic use on multiple computers.
- **Thin clients** – use a variety of credentials in Citrix, Microsoft Terminal Services and VMware environments.

## Single Sign-On (SSO)

- **Application logon control** – enforce advanced authentication policies for logging into applications on the Web or cloud, on Citrix servers, in terminal emulators and on Windows.
- **Non-intrusive** – provide single sign-on and enforce strong authentication without modifying underlying applications.
- **Optional secondary authentication** – require users to prove that they are the person at the computer when launching enterprise applications.
- **Fast, IT-configured application logon** – set up logon processes for enterprise applications in minutes; no user action required.
- **Application password randomization** – prevent users from being able to log into applications (esp. remote Cloud/Web or Citrix apps) from uncontrolled devices by automatically generating passwords during Change Password operations.

## 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.
- **Fast user switching** – switch among users quickly when accessing applications from shared Windows accounts.

## 2-Factor VPN Logon

- **Network logon control** – secure access to VPNs, Microsoft Outlook Web Access (OWA) and other RADIUS-compatible applications with OATH-based one-time passwords (OTPs).
- **Token-less operation** – link use of one-time passwords to other authentication credentials (e.g., use fingerprint and Bluetooth phone) to avoid the need to carry or type in OTP codes.
- **Tokens** – use traditional one-time password tokens (key fobs and soft tokens on smartphones) for access from other devices.

## Access Recovery

- **IT-assisted recovery** – avoid lockouts due to forgotten passwords; no network or Internet connection required.
- **Self-service recovery** – give users the ability to get into their PC by answering questions (which can be customized by IT to avoid use of personal information); no network or Internet connection required.

## Email/Documents Encryption

- **Digital signature** – securely sign email messages and documents (Office and PDF) to prevent tampering and forging.
- **Encryption** – cryptographically secure email messages and documents (Office and PDF) to help prevent data breaches.
- **Centralized enforcement** – set policies requiring use of digital signatures or encryption.

## System Requirements

### Client Software & Operating System

- **DigitalPersona Pro Workstation for Enterprise** or **DigitalPersona Pro Kiosk**.
- **HP ProtectTools 5.04** or later.
- **Windows 7** (32- & 64-bit), **Windows Vista** (32- & 64-bit), **Windows XP SP3** (32-bit).

### Server Operating System

- **Windows Server 2003** (32- & 64-bit), **Windows Server 2008** and **R2** (32- & 64-bit).

### Browsers

- **Internet Explorer** versions 7-9, **Firefox** versions 4-10.

DigitalPersona reserves the right to modify its products and specifications. Contact DigitalPersona for current detailed information on supported fingerprint readers, card readers, one-time password tokens and thin client platforms.



DigitalPersona, Inc.  
720 Bay Road  
Redwood City, CA 94063  
USA

Tel: +1 650.474.4000  
Fax: +1 650.298.8313  
info@digitalpersona.com  
www.digitalpersona.com

© 2012 DigitalPersona, Inc. All rights reserved.  
DigitalPersona® is a trademark of DigitalPersona, Inc. registered in the U.S. and other countries. All other brand and product names are trademarks or registered trademarks of their respective owners. MC-118-020212