DigitalPersona Pro Enterprise

DigitalPersona Pro Enterprise is a strong, multi-factor authentication and access management solution. Administered via 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, Multi-Factor Authentication.** Mix and match authentication credentials (passwords, biometrics, cards, phones, etc.) for both Windows and applications to reliably know who’s doing what.

- **Single Sign-On (SSO).** Reduce the exploding costs and burdens of complying with new password mandates. Retain control of access with optional secondary authentication.

- **Access control for cloud/enterprise apps.** Hide passwords from users to prevent access to business data from uncontrolled devices.

- **Emergency access recovery.** Prevent lockouts when credentials are lost, stolen or forgotten (IT-assisted and self-service).

- **No changes to existing applications.** Add strong authentication and SSO on top of your existing applications in minutes.

- **Central Management of notebooks, desktops, kiosks.** Control access to individual PCs, shared-user workstations, applications and networks from a common console.

- **Integration with Active Directory group policies.** Create, deploy and monitor security policies for your domain accounts and organizations using familiar AD Group Policies and tools.

- **Workflow authentication inside custom apps.** Build strong authentication into custom applications with an easy-to-use SDK.

---

**Easy to Deploy and Manage**

DigitalPersona Pro Enterprise makes it practical and cost-effective to use multi-factor authentication to secure access to enterprise applications from 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, DigitalPersona Pro Enterprise lets you quickly create, deploy, enforce and monitor security policies across your domain.

**Multi-Factor Security that’s Flexible**

DigitalPersona Pro Enterprise enables strong, multi-factor security to be tailored to the needs of different groups of users. You can mix and match authentication credentials to follow industry best practices for combining something users know (password or PIN), something they are (fingerprint) and something they have (smart card, contactless card, proximity card or Bluetooth phone).

---

**Extensible Platform**

DigitalPersona Pro Enterprise provides a powerful, consistent platform for securing access to applications throughout your business. With it, you can add strong authentication on top of password-based applications as needed, without having to modify the apps. With DigitalPersona Pro Enterprise, you can address today’s pressing needs and seamlessly scale up to handle more users and more applications as your requirements grow.
Key Features of DigitalPersona Pro Enterprise

**Centralized Management**
- **Active Directory** – set security policies for domain users and groups using Group Policy Objects (GPOs).
- **Notebooks, desktops and kiosks** – secure access to individual PCs and shared-user workstations from a common console.
- **Reporting** – monitor and document enforcement of security policies.

**Multi-Factor Authentication**
- **Multi-credential authentication** – mix and match authentication credentials: Windows Password, PIN, Fingerprint, 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 enforcement** – require combinations of credentials to address growing compliance mandates.
- **Roaming** – store user credentials centrally for automatic use on multiple computers.
- **Attended enrollment** – require a supervisor’s permission when users enroll or change credentials.

**Windows Logon**
- **PC logon control** – enforce multi-factor authentication policies for PC logon.
- **Domain password randomization** – enforce use of strong authentication by preventing users from knowing their password.
- **Thin clients** – use a variety of credentials in Citrix XenApp, Microsoft Terminal Services and VMware View environments.

**Application Logon**
- **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.
- **No changes to apps** – provide single sign-on and enforce strong authentication without modifying underlying applications.
- **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.

**Single Sign-On (SSO)**
- **Fast, IT-configured application logon** – set up logon processes for enterprise applications in minutes; no user action required.
- **Optional secondary authentication** – require users to prove that they are the person at the computer when launching enterprise 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.
- **Fast user switching** – switch among users quickly when accessing applications from shared Windows accounts.

**Token-less 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.

**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).

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