DigitalPersona Product Brief

Endpoint Protection with DigitalPersona® Pro

An introductory technical overview to DigitalPersona's suite for Access Management, Data Protection and Secure Communication.

April 2010

DigitalPersona Pro is a leading Endpoint Protection suite for access management, data protection and secure communication. With DigitalPersona Pro, you can deploy and centrally manage multiple solutions for 360° security and compliance without sacrificing efficiency and ease of management.

This document is intended to provide a high-level, technical overview of DigitalPersona Pro's architecture and main functionality.

digitalPersona®

DigitalPersona Pro

Centrally-managed Endpoint Protection

DigitalPersona Pro is the centrally-managed endpoint protection suite for access management, data protection and secure communication.

By integrating multiple technologies into a single solution, DigitalPersona Pro helps your organization achieve:

- **Stronger security**, by deploying and enforcing multiple security solutions that span from biometrics to encryption, and from signature to two-factor authentication for VPN.
- **Improved compliance**, by ensuring protection for data in motion and at rest and tightly controlling access to business resourcing.
- **Higher efficiency**, by allowing for modular deployment of the management configuration that best fits your organization's needs.

Endpoint Protection with DigitalPersona Pro

At-a-glance

- **Access management** – Control access to PCs, networks or applications with strong authentication, security for VPN and Single Sign-On.
- **Data protection** – Protect data at rest even if computers are lost or stolen with pre-boot level security and full disk encryption.
- **Secure communication** – Help employees share information safely with digital signatures and encryption for email and documents.

In addition, DigitalPersona Pro provides the best value in the industry, thus allowing for improved Return on Investment (ROI) and lower Total Cost of Ownership (TCO).

DigitalPersona's technology is validated by industry leaders and chosen by the world's #1 business computer manufacturer as the management solution of choice for the security software preloaded on all its PCs.

Content

The first section provides an introduction to DigitalPersona Pro's structure. The second section provides more insights about Pro Workgroup. The last section is dedicated to Pro Enterprise.

A high level picture of DigitalPersona Pro

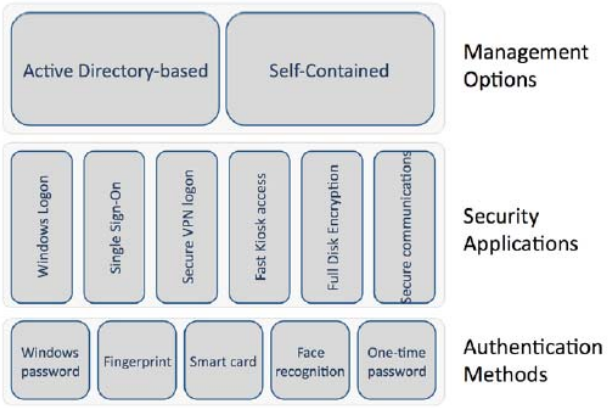
Introduction

DigitalPersona Pro includes multiple modules that can be independently deployed in the organization.

At a very high level there are three different "levels":

- Management options
- Security applications
- Authentication methods

Each of these layers is substantially independent from the others and – depending on your specific system configuration – may adapt to virtually any combination of the others.



At the **MANAGEMENT OPTIONS** level, DigitalPersona Pro allows for two configurations in order to meet your requirements and need for flexibility:

- DigitalPersona Pro Workgroup offers a standalone, self-contained solution that does not require any IT infrastructure.
- DigitalPersona Pro Enterprise leverages the existing Active Directory network for Enterprise-level scalability and maximum integration with your IT infrastructure.

Regardless of the management option you choose, you may be able to centrally control and deploy security policies for a variety of **SECURITY APPLICATIONS**. Examples may include:

- PC access with Windows logon
- Enterprise Single Sign-On
- Multi-factor authentication for existing Virtual Private Networks
- Full Disk Encryption
- Fast access for shared kiosks or computers
- Digital signature and encryption for email and shared documents

As a final component of the DigitalPersona Pro infrastructure, depending on your system configuration you will be able to choose between several **AUTHENTICATION METHODS**.

Based on the security application and the policies set by the IT Manager, users will be prompted to verify their identity with virtually any combination of credentials such as:

- Windows password
- Smart cards
- Fingerprints
- Face recognition
- One-time passwords

This paper focuses on DigitalPersona Pro's management options and provides you with technical insights on how Pro Workgroup and Pro Enterprise work. Refer to dedicated material or contact DigitalPersona for more information on security applications or authentication methods.

Self-contained, out-of-the-box security with Pro Workgroup

DigitalPersona Pro Workgroup is the totally self-contained, out-of-the-box solution for centrally-managed Endpoint Protection.

This section presents a high level overview of how Pro Workgroup works.

Components

Pro Workgroup includes client and server software. On the client side, Pro Workgroup supports

- DigitalPersona Pro Workstation
- HP ProtectTools[1]

Client software runs on Windows® 7, Vista and XP (32 and 64 bit). All versions of these Operating Systems are supported.

The server "package" includes three main components:

- Server software
- Database
- Additional infrastructure needed to allow communication between server and clients.

The server software runs on Windows 7, Vista or Server 2008 (32 and 64 bit). The database is SQL Express 2005. Additional installed elements may include Internet Information Service (IIS) 7 and Windows Communication Foundation (WCF).

Pro Workgroup server automatically installs and configures all necessary components.

[1] Depending on the specific software version, you may need to run an update to make HP ProtectTools fully manageable with Pro Workgroup.

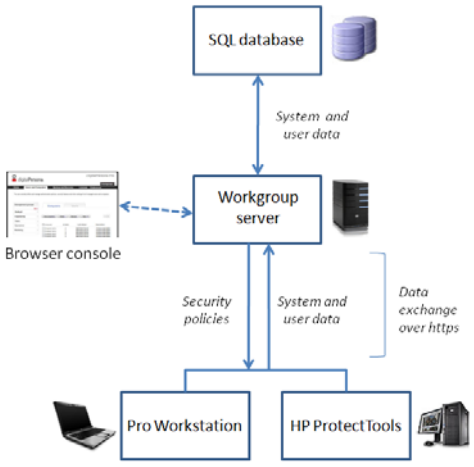


Figure 1 - Pro Workgroup components

Client-server communication

With Pro Workgroup, server and client software communicate over a secure channel to deploy and apply security policies or transmit other relevant system information.

Upon installation of the server software, Pro Workgroup automatically generates a public/private key pair. When computers become managed, the initial key exchange is completed to establish a securely encrypted communication channel.

After installation, client and server software communicate over https. If the server software is properly configured to be accessible through the Internet, this allows managed computers to receive security policies even if they are not connected to the corporate network.

Deployment of security policies

With Pro Workgroup, IT Managers can set and deploy security policies from the server software.

Once the security policies are saved and applied to a specific group, the policies are pulled from managed workstations the next time they contact the server, based on the settings configured by the Administrator.

Policies are then locally applied by the DigitalPersona agent running on the managed workstation; potential issues encountered during the enforcement process are reported as error messages to the server.

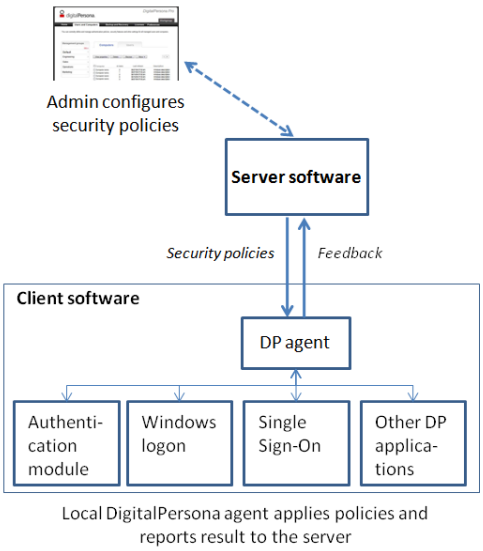


Figure 2 – Policy deployment and enforcement

Access recovery

Pro Workgroup allows for access recovery in case legitimate users are locked out of their computers or employees depart from the company.

To unlock pre-boot and full disk encryption, Pro Workgroup automatically creates a "Recovery" account in the BIOS and Full Disk Encryption modules[2]. When the recovery account is used, the client software informs the server that a recovery was completed. A new password is then generated to allow for tighter security.

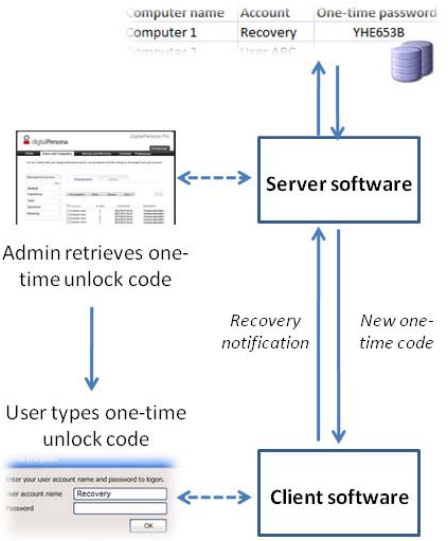


Figure 3 - BIOS and Full Disk Encryption access recovery

In order to allow recovery into Windows, a similar process is completed. The user dictates a security code to the IT Manager in order to unlock a one-time access code. Upon successful recovery, new codes are generated.

Data exchange is initiated as soon as the computer becomes managed. On the local computer, a one-time password is generated and used to encrypt a copy of the Windows password.

Storage of system and user data

When computers become managed and/or when users are added to workstations, dedicated records are created in Pro Workgroup's SQL database.

DigitalPersona Pro Workgroup does not permanently store any user personal, identifiable information, including user passwords or credentials (e.g. fingerprints, etc.). Records in the database only include encrypted information that allow for access recovery.

[2] Support may vary depending on your system configuration.

Integrated, scalable security with Pro Enterprise

DigitalPersona Pro Enterprise is the scalable Endpoint Protection solution that tightly integrates into your existing IT infrastructure.

This section presents a high level overview of how Pro Enterprise works.

Components

Pro Enterprise includes client and server software. On the client side, Pro Enterprise supports

- DigitalPersona Pro Workstation
- HP ProtectTools[3]

Client software runs on Windows® 7, Vista and XP (32 and 64 bit). All versions of these Operating Systems are supported.

The server "package" includes three main components:

- Server software
- Database
- Additional tools used to prepare your environment before installation or for ancillary tasks.

The server software runs on Windows Server 2008 and 2003 (32 and 64 bit). It requires an Active Directory schema extension so that AD can be used as a database of computer and user data. The server software runs on a Domain Controller.

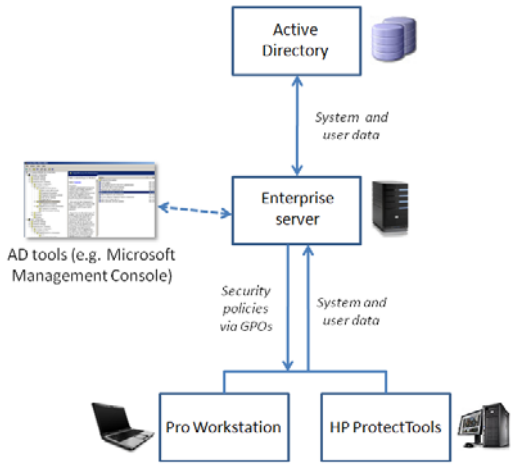


Figure 4 - Pro Enterprise components

Client-server communication

With Pro Enterprise, server and client software communicate securely over an SSL-equivalent channel via DCOM technology and Kerberos mutual authentication.

If the system uses multiple servers, Pro Enterprise generates pairs of public-private keys that allow secure communication between the servers by leveraging industry-standard Public Key Infrastructure (PKI) technology.

Data stored in Active Directory are encrypted and signed to allow for integrity and authenticity, and only accessible to the DigitalPersona service upon an authenticated request.

Deployment of security policies

With Pro Enterprise, IT Managers can set and deploy security policies using Active Directory Group Policy Objects. The Admin can set GPOs using the DigitalPersona snap-in into standard Active Directory tools (e.g. Microsoft Management Console).

[3] Depending on the specific software version, you may need to run an update to make HP ProtectTools fully manageable with DigitalPersona Pro.

Once a new policy is configured, it is automatically distributed via Active Directory replication and according to the cycle set for the forest. Computers that are not connected to the corporate network receive the new policy as soon as they connect.

Policies are then locally applied by the DigitalPersona agent running on the managed workstation; potential issues encountered during the enforcement process are reported as error messages to the server.

Roaming of user data and centralized credential authentication

Pro Enterprise supports roaming of user data across workstations and allows for centralized, server-side authentication of some credentials (e.g. fingerprints).

When DigitalPersona Pro is configured to allow for user data (e.g. passwords for Single Sign-On) roaming, they are securely encrypted and stored in Active Directory. Data is released and then decrypted upon successful user authentication.

Centralized matching of user credentials are processed on the local computer and securely sent to the server. On the server, credentials are matched against the "master" copy stored in Active Directory upon initial user registration. In the case of a successful authentication, a positive confirmation is sent to the client software and encrypted user data is released.

IT Managers can delete user data and credentials in Active Directory without the need to decrypt them, so that privacy is guaranteed even when employees leave the company.

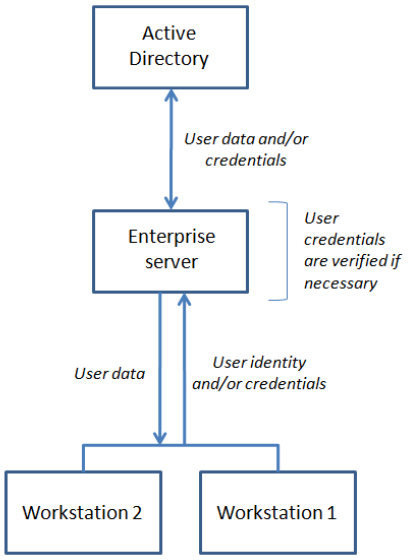


Figure 5 - Data flow with roaming of user data and centralized credential authentication

Access recovery

Pro Enterprise allows for access recovery in case legitimate users are locked out of their computers or employees depart from the company.

The workflow is similar to the one described for Pro Workgroup. The IT Manager initiates the recovery process through standard Active Directory tools.

More questions? Contact us

DigitalPersona is looking forward to hearing from you and answering your questions. Contact your Account Manager or sales@digitalpersona.com to learn more.