DigitalPersona Product Brief

Full Disk Encryption with DigitalPersona® Pro

An introductory technical overview to the DigitalPersona solution for encryption of data at rest.

April 2010

DigitalPersona Pro is the leading Endpoint Protection suite for access management, data protection and secure communication. With DigitalPersona Pro, IT managers can centrally control password management, strong authentication and single sign-on throughout the organization.

This document is intended to provide a high-level, technical overview of how DigitalPersona's Full Disk Encryption works.

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 signature and encryption for email and documents.

In addition, with DigitalPersona Pro you can achieve all of this at a cost-effective price, 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 of their PCs.

Content

This document provides a high level introduction to how DigitalPersona Pro's Full Disk Encryption module works.

Securing data with full disk encryption

Introduction

With DigitalPersona Pro, IT can enforce data protection with Full Disk Encryption.

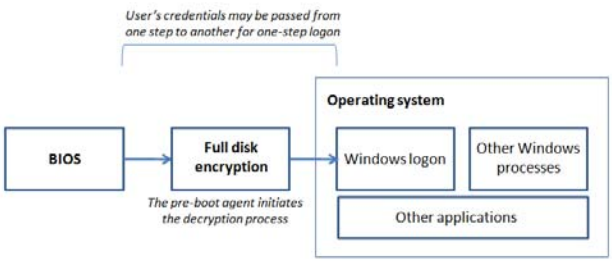
At a very high level, managing Full Disk Encryption includes three main activities:

- Encrypting hard drives
- Defining user authentication, how users are allowed to decrypt data
- Recovering access to locked PCs or drives for emergencies

Encrypting hard drives

When it comes to protecting data, Full Disk Encryption is recognized in the industry as a new "standard of due care". Only solutions that encrypt the entire hard disk, in fact, can help protect the system with minimum or no dependency on users' behavior and in case computers are lost or stolen.

Drive Encryption for DigitalPersona Pro helps protect customer data and other mission critical information by encrypting all sectors of the hard drive, including empty space or areas used by the Operating System for booting up. DigitalPersona Pro uses AES encryption with 256 bit key length.



Pre-boot level functionality implies that users need to authenticate before the Operating System starts. One-step logon functionality is available for an improved user experience.

Once the Operating System is up and running, other applications can be started as well. Drive Encryption continuously monitor the user's activity to decrypt "on-the-fly" additional sectors of the hard disk that might need to be accessed. This allows for tighter security and for faster operations, because the computer does not need to go through a full encryption or decryption every time the system is being used.

Defining user authentication

Once Drive Encryption is active, IT Managers can choose how users are required to verify their identity when logging on to the system. Since this operation substantially initiates the decryption process, many organizations find particularly important to have strong authentication policies in place.

IT Managers can choose from a broad range of policies, including multi-credential authentication with methods such as biometrics or smart cards. Each

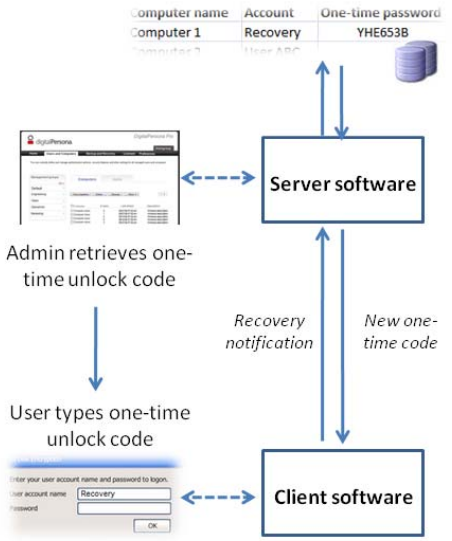
option provides unique characteristics and user experiences and should correspond to the balance between security and convenience IT Managers deem appropriate for the organization. Availability of specific authentication methods in pre-boot may depend on the specific hardware configuration available on each computer.

When the user authenticates successfully, the "master encryption key" used to initiate the decryption process is released and used to decrypt the disk. This key is never stored permanently on the hard disk, thus offering a higher level of protection over some file-level encryption solutions.

Access recovery

DigitalPersona Pro 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, DigitalPersona Pro automatically creates a "Recovery" account in the BIOS and Full Disk Encryption modules[1]. When the recovery account is used, the client software informs the server that a recovery was completed. A new one-time password is then set in place for future use.



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.

DigitalPersona Pro also provides a last resort recovery options in case hard drives are damaged (e.g. the Master Boot Record is corrupted) and users cannot boot from them. Using special recovery tools and treating the encrypted hard drive as an external storage device, IT can temporarily get access to the encrypted information and export data in a safe location.

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.

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