



DigitalPersona Product Brief

Full Disk Encryption with DigitalPersona® Pro

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

December 2010

DigitalPersona Pro is a leading centrally-managed suite of security solutions that protects data and controls access to PCs and applications. It simplifies management of solutions like disk encryption, strong authentication, single sign-on, and more thus helping achieve compliance and lower security-related IT costs.

This document is intended to provide a high-level, technical overview of how DigitalPersona Pro's Drive 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.

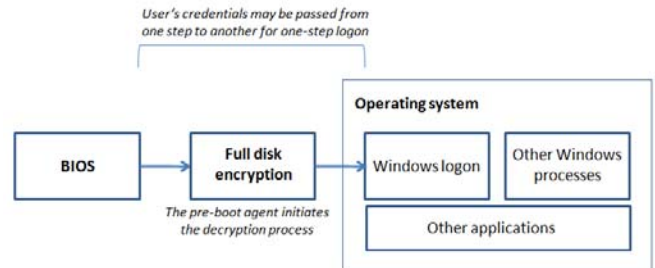
DigitalPersona Pro's Drive Encryption module helps protect customer data and other mission critical information by encrypting all sectors of the hard drive, including empty space or areas used by the Operating System for booting up.

DigitalPersona Pro uses AES encryption with 256 bit key length, in accordance with the recommendation of the National Institute for Standards and Technology (NIST) and deemed appropriate for government-level Top Secret information.

The encryption status of managed PCs is reported within DigitalPersona Pro's auditing and reporting modules to satisfy regulators and auditors.

Computer	Encryption status
Computer name 1	Encrypted
Computer name 2	Encrypted

DigitalPersona Pro requires pre-boot authentication for drive encryption, thus making sure users authenticate before the OS starts up. 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 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 unlocks the drive key, many organizations find it particularly important to have strong authentication policies in place.

With DigitalPersona Pro, 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.



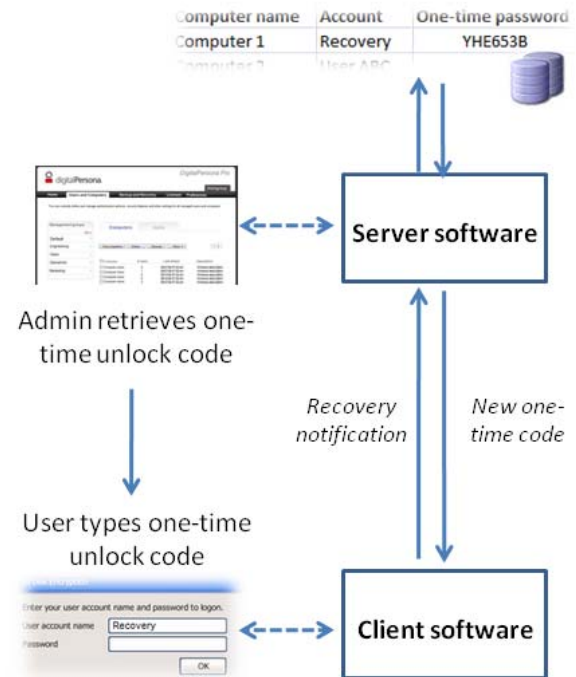
When the user authenticates successfully, the “master encryption key” used to unlock the drive is released. This key is never stored permanently on the hard disk, thus offering a higher level of protection over some file-level encryption solutions.

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 on managed PCs and assigns a random, secret password to it. 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.



DigitalPersona Pro also provides a last resort recovery options in case hard drives are damaged 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.

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.