DigitalPersona Product Brief

Two-Factor VPN Authentication with DigitalPersona® Pro

An introductory technical overview to the DigitalPersona solution for Two-Factor VPN Authentication.

July 2010

DigitalPersona Pro is a leading Endpoint Protection suite for access management, data protection and secure communication. With DigitalPersona Pro, IT Managers can strengthen the security of existing Virtual Private Networks by adding strong authentication based one-time passwords.

This document is intended to provide a high-level, technical overview of how DigitalPersona's Two-Factor VPN Authentication solution works.

DigitalPersona Pro

Centrally-managed Endpoint Protection

DigitalPersona Pro is a 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 resources.
- **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 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

This document provides a high level introduction to how DigitalPersona Pro's Two-Factor VPN Authentication module works.

Strengthening authentication for VPN access

Introduction

With DigitalPersona Pro, you can improve the security of existing Virtual Private Networks by adding one-time password authentication upon user logon.

DigitalPersona Pro supports most RADIUS-based VPNs, such as Cisco®, Juniper®, etc.

At a high level, adding two-factor authentication to an existing VPN solution requires the following steps:

- IT Managers have to provide users with the means to generate the one-time-password
- Users have to provide the one-time password together with their VPN logon credentials
- The one-time password has to be validated "in real time" when a user tries to log on

Generating one-time passwords

DigitalPersona Pro supports a variety of methods for users to generate the one-time password required at VPN logon.

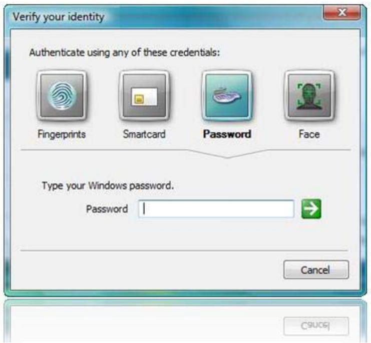
DigitalPersona Pro's Two-Factor Authentication module supports virtually any device or method that is based on OATH-compliant one-time passwords. OATH-based one-time passwords are adopted by the vast majority of the token manufacturers and players in the Two-Factor Authentication market.

A typical example of supported devices include dedicated hardware tokens, of the type users typically carry attached to their key fobs. Leading token providers such as Vasco® or Quest® use OATH-compliant algorithms to generate the one-time password in their devices.

In addition, DigitalPersona Pro lets users use a broad set of smartphones as one-time password generating devices. On those devices, the one-time code is typically generated by a dedicated application that runs on the phone operating system. Examples of supported smartphones include:

- BlackBerry®
- iPhone®
- Windows® Mobile® smartphones
- Palm® smartphones

Finally, DigitalPersona Pro allows Administrators to configure the system so that the one-time password is automatically generated on the user's PC, typically upon successful user authentication using some form of strong identity methods that DigitalPersona Pro supports.


Verify your identity

Authenticate using any of these credentials:

Type your Windows password.

Password

For example, IT Managers may leverage the fingerprint readers that come built-in on many laptops and require users to provide their password AND swipe their finger in order to submit their own VPN credentials and a one-time password generated "on-the-fly".

Overall, DigitalPersona Pro offers market-leading flexibility in the deployment and configuration of methods users can leverage to generate and provide the one-time password. This allows Administrators to choose the configuration that best fits their needs and their organization's preferences in terms of balance between security and usability.

Submitting one-time passwords

DigitalPersona Pro supports different user experiences that largely depend on the one-time password generation system the IT Manager chooses to deploy.

With dedicated tokens or smartphones, users are typically prompted to type the one-time password on a dedicated dialog box that appears during the VPN logon process.

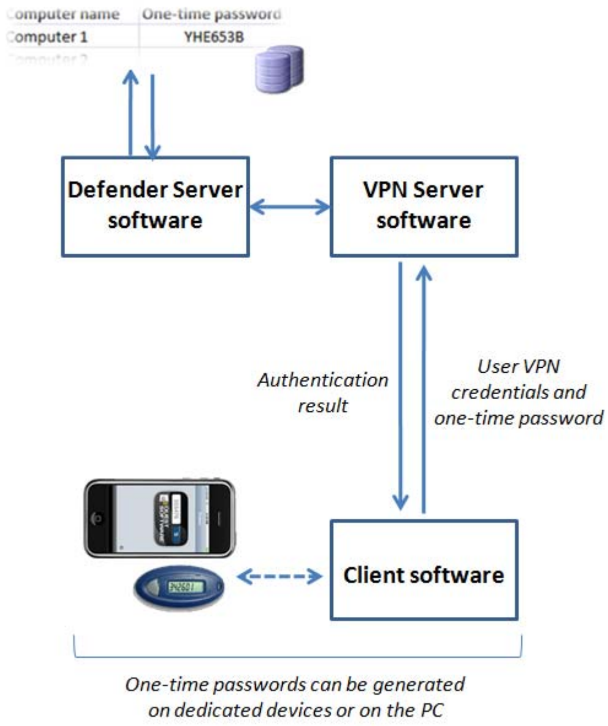
When the one-time password is automatically generated on the user's computer, the IT Manager can leverage DigitalPersona Pro's Password Management functionality to require user authentication (e.g. with password and fingerprints, or any other combination of supported credentials) and then automatically submit VPN credentials and the one-time password.

Validating one-time passwords

The security value of adding one-time passwords to VPN systems largely depends on the fact that the one-time password is validated "on-the-fly" during the user logon process.

Regardless of whether it is automatically generated on the user's computer and then submitted, or manually typed by the user based on the output of a smartphone application or a hardware token, the one-time password is sent from the managed computer to the Virtual Private Network system together with the user's credentials.

Digitalpersona Pro's RADIUS plug-in routes the one-time password to the DigitalPersona Defender Security Server for validation. The Defender server validates the one-time password by tying it to the user for which the authentication request was submitted.



In the case of a successful one-time password validation, a positive confirmation is provided to the VPN that then verifies the VPN user credentials. Upon successful authentication, the corresponding feedback is sent to the client and the secure communication channel is established.

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.