Enterprise Single Sign-On with DigitalPersona® Pro

An introductory technical overview to the DigitalPersona solution for centrally-managed Enterprise Single Sign-On.

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 Single Sign-On solution works.

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 Single Sign-On module works.

Replacing passwords for web and application logon

Introduction

With DigitalPersona Pro, IT can centrally manage logon into web and enterprise applications such as ERP systems, portals, etc.

At a very high level, managing access to enterprise applications includes two steps:

- "Training" DigitalPersona Pro's Single Sign-On module to recognize application logons.

- Defining how employees authenticate when logging on to managed applications.

Training the system to recognize applications

DigitalPersona Pro's Single Sign-On module, Password Manager Pro, is capable of recognizing enterprise applications' logon screens.

Depending on the type of application, DigitalPersona Pro "scrapes" the logon screen to locate the logon fields. For example, DigitalPersona Pro is capable of automatically recognizing fields in web applications by analyzing the html code of the logon page.


With the same approach, DigitalPersona Pro locates elements such as "Submit" buttons or other input fields that may be relevant for logging on, such as check boxes.

DigitalPersona Pro is capable of automatically interpreting the vast majority of enterprise applications. For the few that do not allow any form of automatic "discovery", DigitalPersona Pro provides IT Managers with a simple yet powerful scripting tool. Using this tool, sometimes referred to as "Manual mode", IT Managers can help the software identify a relevant starting point on the logon page (e.g. the position of the "username" field) and then navigate the page from there by repeating a series of actions – e.g. entering keystrokes.
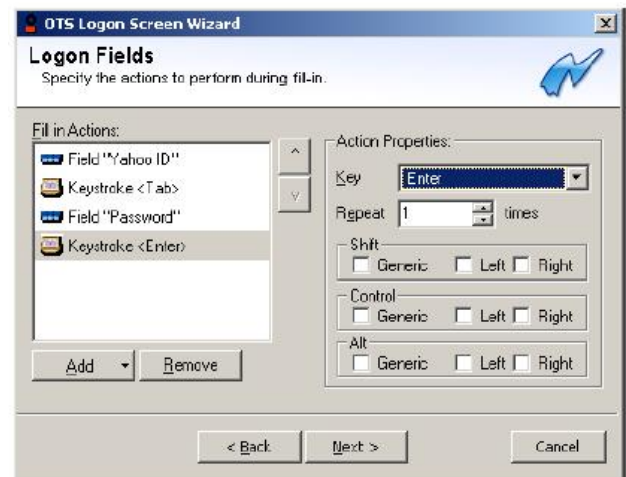
Regardless of how the system recognizes a given application, the output of the "training" process is an XML file, sometimes referred to as a "logon template". To allow managed computers and users to use single sign-on to log on to the managed application, IT Managers deploy the templates to managed workstations using DigitalPersona Pro's policies.
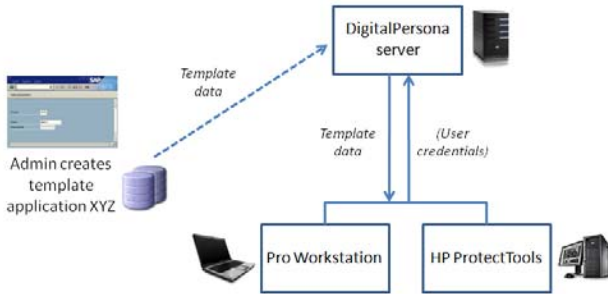
Defining user authentication

Once an application is enabled with DigitalPersona Pro's Single Sign-On module, IT Managers can leverage this powerful tool to replace standard, password-based logon with their preferred authentication policy. In fact, when users try to log on to managed applications, they will be prompted to authenticate based on the policy chosen by the Administrator.

IT Managers can choose from a broad range of policies, ranging from no authentication (i.e. Single Sign-On) to 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.

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.