

DigitalPersona[®] Pro Enterprise

Quick Start Guide
5.x



DATA PROTECTION • REMOTE ACCESS • SECURE COMMUNICATION • STRONG AUTHENTICATION • ACCESS RECOVERY • SINGLE SIGN-ON

DigitalPersona® Pro Enterprise

DigitalPersona Pro Enterprise is the centrally-managed Endpoint Protection suite for Access Management, Data Protection and Secure Communications.

It allows companies to control and enforce multiple security applications through a single control point; and can provide solutions including Strong Authentication, Single Sign-On (SSO), Secure VPN access, and Access Recovery.

DigitalPersona Pro Enterprise provides convenient and secure central administration, easily scaling to over one hundred thousand users. The product is tightly integrated with Windows Active Directory and can be deployed without the need for professional services.

This Quick Start Guide provides an overview of the DigitalPersona Pro Enterprise solution and describes the major features of its components. Additional resources are listed at the end of this guide. The DigitalPersona Pro Enterprise Administrators Guide and Application Guides are located on our website at <http://www.digitalpersona.com/products/material>.

Note that some features may be specific to certain product editions. Procedures and screen images are from Microsoft Windows Vista. Actual steps and visual appearance may be slightly different on other versions of Windows.

Feature Overview

The DigitalPersona Pro Enterprise solution includes the following core components and features. (Some features are optional add-on modules)

- Pro Enterprise Server - is used to centrally configure and manage installations of DigitalPersona Pro Workstation and the HP ProtectTools suite preloaded on many Hewlett-Packard business notebooks and desktops. It is installed on a domain controller and is automatically connected to by installed clients.
- Pro Workstation - includes an end-user dashboard for local access to installed security applications and an Administrative Console where the local administrator can pre-configure applications for users of the computer. Use of the console can be disabled through a GPO setting in Active Directory.
- Credential Manager and Password Manager - are built-in core applications providing multi-factor authentication capabilities with Single Sign-On to Windows, websites and programs.
- DigitalPersona Defender VPN module - Supports authentication to RADIUS-based VPNs using OATH-compliant One Time Password (OTP) tokens. To use hardware tokens or smartphone tokens, Defender can be used by itself without the Pro Enterprise client. For generation of the OTP on the client, Password Manager Pro and a supported Pro Enterprise client are required. Additional information on this product is available from your DigitalPersona partner or on our website at <http://www.digitalpersona.com/enterprise>.
- Password Manager Admin Tool - enables administrators to provide controlled access to network resources, programs and websites by adding any of a variety of authentication mechanisms (such as password, smart card, fingerprints or Defender-compatible VPN tokens) to their managed logon and change password screens.

- Administration Tools - a set of programs and utilities for administrating and licensing DigitalPersona Pro Enterprise components and applications.
- Fast Connect - a feature enabling SSO (Single-Sign-On) through DigitalPersona Pro Workstation or Kiosk to Published Applications and Desktops on XenApp and XenDesktop.

Make sure and check the DigitalPersona Pro website at <http://www.digitalpersona.com/enterprise> for additional applications that may be available.

Getting Started

System requirements

Minimum system requirements for installation of the DigitalPersona Pro Enterprise Server and Workstation are shown below.

| Product/Component | Minimum Requirements |
|--------------------------------------|---|
| DigitalPersona Pro Enterprise Server | Windows Server 2008 R2 (32/64-bit) or Windows Server 2003 SP2 (32/64-bit) or Windows SBS 2003 SP2 Active Directory 12 MB disk space plus 5Kper user |
| DigitalPersona Pro Workstation | Windows Server 2008 R2 (32/64-bit) or Windows Server 2003 SP2 (32/64-bit) or Windows 7/Vista (32/64-bit) or Windows XP Professional SP3 (32/bit)* Home editions of Windows 7/Vista/XP are not supported. 30 MB disk space, 60 MB during installation Microsoft Internet Explorer 6-9, Chrome 11+ or Firefox 4+ to create/use Password Manager <i>personal</i> † logons or use <i>managed</i> † logons Microsoft Internet Explorer 6-9 to create <i>managed</i> † logons using Password Manager <i>Pro</i> |

* Also supported: Windows XP Embedded, Windows Embedded Standard 2009 and Windows Embedded Standard 7, with dependencies as documented in the DigitalPersona Pro Enterprise Administrator's Guide.

† Personal logons allow end-users to create automated logon to programs, websites and network resources. Managed logons have the same function but are created by an administrator and deployed to end-users.

Server installation

Although the DigitalPersona Pro Workstation can be used as a standalone product without centralized management by a DigitalPersona Pro Enterprise Server, it is most commonly used in conjunction with the Enterprise Server.

The DigitalPersona Pro Enterprise Server should be installed prior to installing any instances of the Pro Workstation. Otherwise, domain users of Pro Workstation will need to enroll their credentials again and re-enter any Password Manager logon data after the server is installed.

The following instructions indicate the simplest common installation scenario: installation on a domain controller running Windows 2008 Server.

The following must also be true.

- No other installations of DigitalPersona Pro Enterprise Server exists in the domain
- The Pro clients that will be used with the Enterprise Server are on the same domain
- Active Directory has been properly configured and tested on your network. Note that the installation will extend your Active Directory schema. Specific details on the schema extensions are available upon request from our Technical Support department.

To install the DigitalPersona Pro Enterprise Server -

- 1 Run the Active Directory Schema Extension wizard (DPSchemaExt.exe) in the “AD Schema Extension” folder of the Pro Enterprise Server software package. You must have Schema Administrator privileges. to run the Schema Extension Wizard.

The Active Directory Schema Extension Wizard must be run from the schema master domain controller, or the data may not replicate fast enough to allow the wizard to continue. If the data is not replicated fast enough, the wizard will terminate, and you should then wait one replication cycle before running the wizard again.

After the schema extension, and again after configuring your domains, you must wait for Active Directory schema replication to be completed. The amount of time this takes will depend on the complexity of your Active Directory structure.

- 2 Run the Active Directory Domain Configuration wizard by launching DPDomainConfig.exe in the “Domain Configuration” folder of the Pro Enterprise Server software package.
- 3 Run the Pro Enterprise Server Installation wizard by launching Setup.exe in the “Pro Enterprise Server” folder of the software package.

Licensing

Prior to installing DigitalPersona User Licenses, the Pro Server software must be installed, and the DigitalPersona License Activation Manager must be installed on a computer in the same domain.

Installing License Activation Manager

The DigitalPersona Pro License Activation Manager is used to activate licenses for DigitalPersona Pro Enterprise Server, Enterprise Packages and Pro Enterprise clients, for versions 5.2 and above.

You may also select to install additional Administration Tools at this time. See page 12 for a brief description of the tools, or the Administration Tools chapter in the DigitalPersona Pro Enterprise Administrator Guide for a more detailed description.

To install the License Activation Manager

- 1 Locate and launch the **setup.exe** located in the Pro Enterprise Server\Pro Administration Tools folder of the DigitalPersona Pro Enterprise product package.
- 2 Select **Complete** or **Custom** installation. To install *only* the License Activation Manager, select Custom and deselect all other administration tools.
- 3 Click **Next**, and then click **Install**. Follow the onscreen instructions.

License activation

The Pro Server User Licenses are applied to the domain, site or OU that will encompass users of the DigitalPersona software.

Licenses for Pro Servers without an internet connection may also be activated from another computer with an internet connection (see further details in the Administrator Guide.)

Pro Enterprise Server activation

In most cases, you will activate your Pro Enterprise Servers over the internet through Active Directory and the DigitalPersona Activation wizard.

To activate a DigitalPersona Pro Enterprise Server license

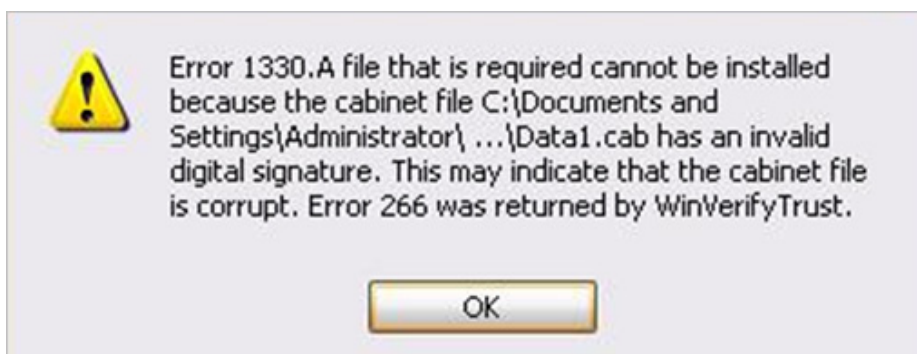
- 1 In the Group Policy Management Editor, navigate to [domain, site or OU], Computer Configuration, Policies, Software Settings, DigitalPersona Pro Enterprise Server, Licenses.
- 2 Right-click on **Licenses** and select **Add license**.
- 3 When the DigitalPersona Activation wizard displays, click **Next**.
- 4 Select the option **I want to activate the software over the Internet**.
- 5 Browse to the License Activation (.dplic) file provided with your purchase.
- 6 Click **Next**. Upon successful activation, a confirmation dialog will display.

Pro Enterprise Client Suite installation

- 1 In the Client folder of the software package, run Setup.exe.
- 2 Click **Next**.
- 3 Select the product to install. Note that only one of these product can be installed on a computer.
 - DigitalPersona Pro Workstation for Enterprise, or
 - DigitalPersona Pro Kiosk for Enterprise
- 4 If you need to install third party drivers for fingerprint or card readers, click the Third Party Drivers button and select the appropriate drivers for your hardware and operating system. Note that DigitalPersona does not provide drivers for Authentec fingerprint readers. There is a link for downloading these drivers. The suggested driver for Authentec fingerprint readers is AT9.
- 5 On the confirmation page you will see a list of items to be installed.
- 6 Click **Install** to begin the installation.
- 7 Successful installation requires the presence of a VeriSign Primary PCA Root Certificate (G5). If your system does not have this certificate, the installation will fail. If it does, see the next topic, *Install VeriSign Primary PCA Root Certificate*, and then restart the installation.
- 8 After installation is finished, you will need to restart the computer. After the restart, installation of any third-party drivers will be started automatically.

Install VeriSign Primary PCA Root Certificate

Note that this is only required if the DigitalPersona Pro client installation fails due to the following error.



- 1 To install a VeriSign Primary PCA Root Certificate
- 2 Go to <http://www.verisign.com/support/roots.html> and click the *Download a root package* link.
- 3 Unzip the downloaded file and open the *Generation 5 (G5) PCA* folder.
- 4 Launch the file *VeriSign Class 3 Public Primary Certification Authority - G5.cer*.
- 5 Select *Install Certificate*.

- 6 In the Certificate Import Wizard, select *Place all certificates in the following store*, and browse to the *Trusted Root Certification Authorities* store.
- 7 Click *Next* and then click *Finish*.

Policy Settings

DigitalPersona Pro Enterprise provides complete centralized management of the Pro Enterprise Server and all managed client workstations through Active Directory Group Policy Object settings.

In Active Directory, each setting includes a complete description of its purpose and use on the Explain tab. Additionally, a complete list and description of these settings, as well as an alphabetical listing, are available in the DigitalPersona Pro Enterprise Administrator Guide.

Configuration of these settings is provided through the Group Policy Management Editor and a collection of .adm\admx files (Administrative Templates). These templates may be installed onto any Active Directory aware computer in the domain from the DigitalPersona Pro Administration Tools component.

Pro Workstation

The DigitalPersona Pro Workstation is one of the available client components of the DigitalPersona Pro Enterprise solution, providing centrally managed endpoint protection. It is generally used in an enterprise environment with DigitalPersona Pro Server, but can also be used separately from the Enterprise Server.

Multi-factor logon to Windows

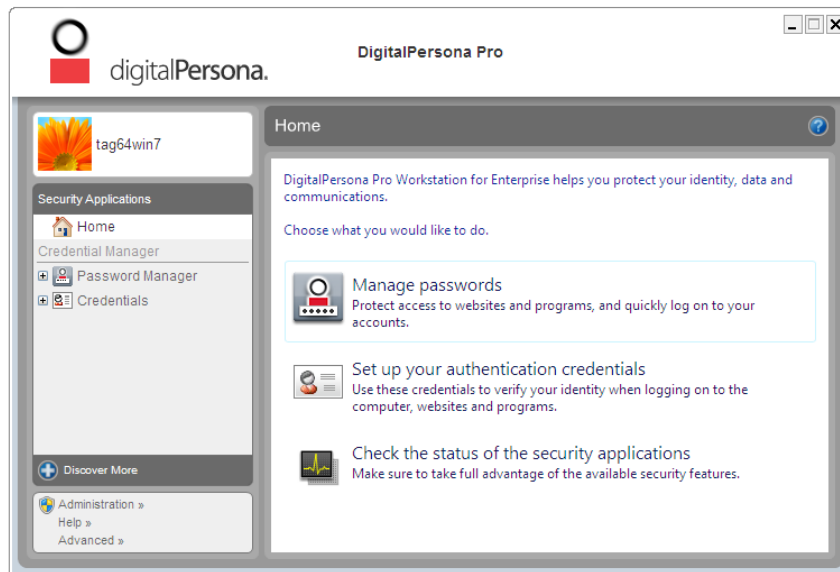
DigitalPersona Pro Workstation adds administrator configured multi-factor authentication to the Windows logon experience, allowing the replacement of passwords with any supported credential or combinations of credentials. The end-user is prompted for the required credentials according to the logon settings implemented by the administrator, and guided through the process of logging on to Windows without needing to know specific details of policy implementation.

Password Randomization

This feature can be used to completely replace use of Windows Passwords with specified credentials that must be used to log on to Windows, even on computers where DigitalPersona Pro is not installed.

Workstation dashboard

The Pro Workstation dashboard is the central location for easy access to Pro Workstation features, applications, and settings.



To open the dashboard

- Click **Start, All Programs, DigitalPersona, DigitalPersona Pro.**

Major features of the dashboard include:

- **Credentials** - Provides a means to enroll and modify credentials used to verify your identity.
- **Password Manager** - Allows the end-user to create automated *personal* logons to their favorite websites and programs, replacing their passwords with a single credential such as a fingerprint, smart card or facial recognition, or multi-factor authentication as defined by the administrator. Use can also be restricted to *managed* logons created by DigitalPersona Password Manager Pro.
- **Backup and Restore** - Allows you to back up or restore DigitalPersona Pro Workstation data.

Additional dashboard features, such as setting general workstation and device-specific preferences are described in the DigitalPersona Pro Enterprise Administrator Guide.

Enrolling your credentials

DigitalPersona Pro Workstation can use your current Windows password for authentication, or use multiple or alternate credentials specified by the administrator. Depending on a computer's hardware and software configuration, the following additional credentials may be available.

- Fingerprints

- PIN
- Bluetooth
- Smart Cards, Proximity Cards and Contactless Cards
- Facial recognition

Prior to using any of these credentials, they must be set up and enrolled. Setup will vary for hardware and software devices, and may require installation of drivers provided with the hardware. See the DigitalPersona Pro Administrator Guide for full details including a list of supported card readers and cards.

To enroll a credential

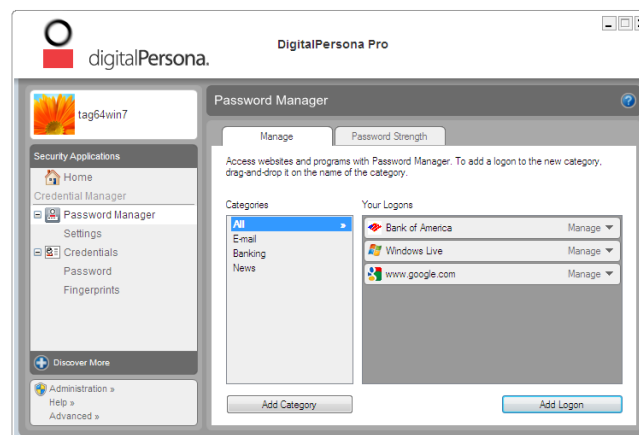
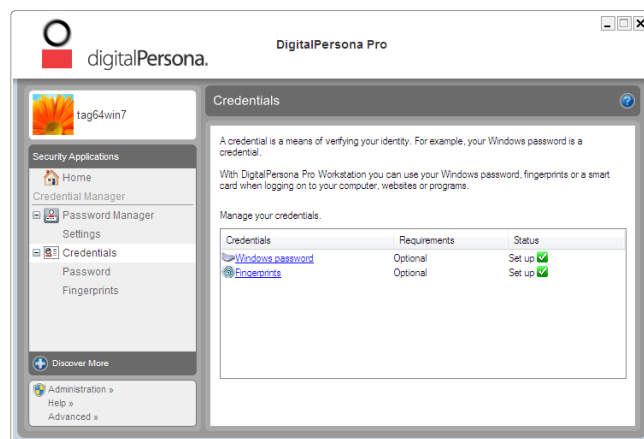
- 1 Open the DigitalPersona Pro dashboard.
- 2 Click **Credentials**.
- 3 Click the credential you want to enroll.
- 4 Follow the onscreen instructions.

Creating logons

Using DigitalPersona Password Manager, a built-in security application, you can use your preferred credential to logon to websites and programs.

By creating *logons* for each site or program, you can then use a single password, fingerprint or other credential instead of having to remember (or write down!) dozens or hundreds of logon/password combinations.

To create a Password Manager logon



- 1 Launch the logon screen for a website or program.

- 2 Open the DigitalPersona Pro dashboard.
- 3 Click the Password Manager topic.
- 4 On the **Manage** tab, click **Add Logon**.
- 5 Enter your logon data.

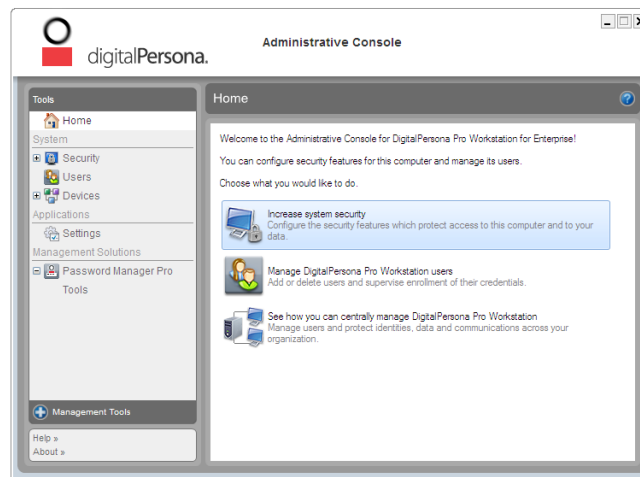
For more information on the features of Password Manager, see the online help provided within the application and the Password Manager Application Guide.

Additional security applications

Additional security applications that integrate with the DigitalPersona Pro dashboard may be available for download from the DigitalPersona website.

Workstation Administrative Console

Local administration of Pro Workstation on a computer is provided through the Pro Enterprise Administrative Console.



The console can be launched from Start, All Programs, DigitalPersona Pro, or from the Pro Enterprise dashboard. Access to the console can be prohibited with a GPO setting available through the Pro Enterprise Server. In any conflict between local settings and GPO settings, the GPO setting always takes precedence.

Using the console, the local administrator has access to the following features and functions.

- Device management - Specify settings for supported authentication devices.
- Applications settings - Set computer-wide and application-specific settings including enabling and disabling installed Pro Workstation applications such as Password Manager or Windows Logon Security.

- Central management - Additional management tools may be available and can be downloaded directly from our website through the Central Management link in the lower-left corner of the console.

The Administrative Console also provides a foundation for additional Pro Enterprise administrative plug-ins which may be included in your specific solution, or ordered separately, such as the DigitalPersona Password Manager Admin Tool (see page 17).

Additional administration components

In addition to the numerous GP and Administrative Console settings available for customizing and managing the behavior of DigitalPersona Pro Enterprise and its clients, there are two further types of administration components provided.

- DigitalPersona Pro Administration Tools - A separate installable package that provides additional Active Directory-based tools including the License Activation Manager, the Users and Computers Snap-in, Attended Enrollment Tool, the User Query Tool and the DigitalPersona Pro Active Directory Administrative Templates.
- Administrative Console plug-ins - Individual components available to extend the administrative features of Pro Enterprise and allow for delegation of specific administrative functions, such as the creation of managed logons with the Password Manager Admin Tool.

For a more complete description of these tools, see the Administrative Tools section of the DigitalPersona Pro Enterprise Administrators Guide and the Password Manager Application Guide.

Administration Tools

The components of the DigitalPersona Administration Tools package are described in the following sections. These tools are separately installed.

CAUTION: The Administration Tools should not be installed prior to running the DigitalPersona Pro Enterprise Domain Configuration Wizard (which is usually done as part of the initial installation process). When installing the DigitalPersona Pro Administration Tools on systems where Pro Enterprise 5.0.x or 5.1.x were previously installed, the current version of the Domain Configuration Wizard must be run prior to installing the Administration Tools.

- 1 In the Client folder of the software package, run Setup.exe.
- 2 Click Next.
- 3 Select the product to install.
 - Pro Administration Tools, or
 - Remote License Tool
4. Click **Install** to begin the installation.

License Activation Manager

License Activation Manager is a component of the DigitalPersona Pro Administration Tools. It is an Active Directory-based administration tool for installing and managing User Licenses for DigitalPersona Pro Enterprise Server. This tool may be installed on the domain controller where DigitalPersona Pro Enterprise Server is installed, or on any computer in the domain. When installed on a workstation, it requires one of the following - depending on the Windows Server version running on the domain controller.

- If Windows Server 2008, install Microsoft Remote Server Administration Tools (available from the Microsoft Download Center).
- If Windows Server 2003, install Windows Server 2003 Administration Tools Pack (adminpak.msi).

ADUC Snap-ins

The DigitalPersona Users and Computers snap-in adds a new tab to the User Properties page enabling additional administrative functions; and adds several DigitalPersona commands to the user and computer object context menus.

Users and Computers Snap-in

The Users and Computers Snap-in is a component of the DigitalPersona Pro Administration Tools. It adds a new tab to the User Properties page enabling additional administrative functions. It also adds several DigitalPersona commands to the user and computer object context menus.

User properties define settings or actions that apply to a specific user, such as deleting fingerprints, attended credential enrollment and recovery from lockout of a user's Windows account.

Computer object commands allow recovery of access to a specific computer - for example due to lockout at the drive encryption level - and backing up the master encryption key for any encrypted drives on a computer.

This snap-in is automatically installed to the console during the installation of Pro Enterprise Server, and can also be added manually to any Active Directory aware computer.

User Query Tool snap-in

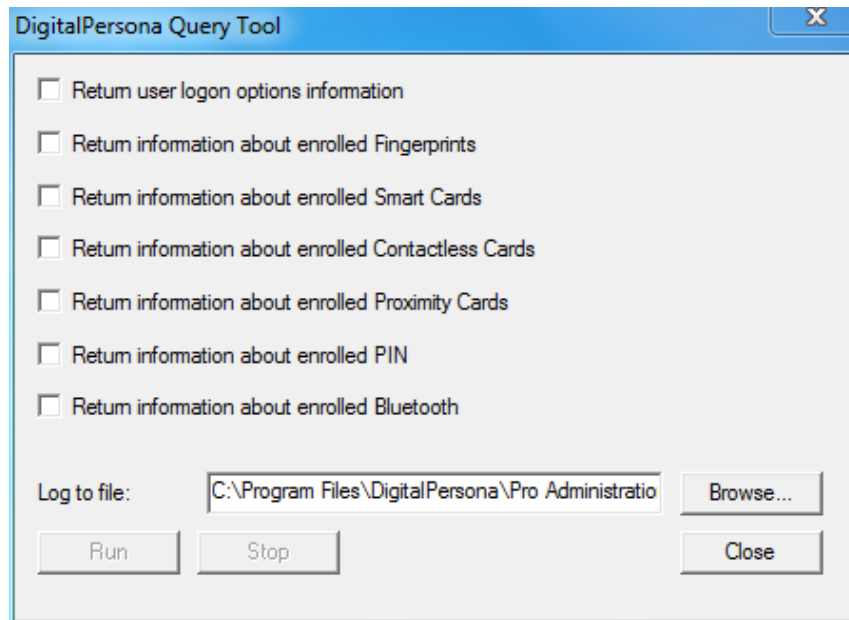
The DigitalPersona Pro User Query Tool snap-in is a component of the DigitalPersona Pro Administration Tools. This tool provides a means for the administrator to query the Pro Enterprise user database for information about DigitalPersona Pro users and to perform certain operations and to set values associated with a selected user.

It has three separate implementations; an ActiveX control, an Interactive dialog-based application and a Command Line utility.

The User Query Tool must be installed on a computer running a licensed copy of DigitalPersona Pro Workstation, and the logged on user must have domain administrator privileges.

To run the interactive dialog-based application:

- 1 On the Start menu, point to **All Programs, DigitalPersona Pro, User Query Tool**.



- 2 In the application dialog, select the type of information you would like to display and enter or browse to the location where you want to save the resulting log file.
- 3 Click the **Run** button.
- 4 The file is saved as a .csv file, which can be opened in programs like Microsoft Excel or other spreadsheet programs.

The ActiveX control provides the most functionality, including performing operations against the user record and setting certain flags and values. The dialog-based and CLI applications are reporting tools only.

Examples of the types of query information that can be accessed by the ActiveX control are:

- Number of installed licenses
- Number of licenses used
- Number of enrolled credentials for each user
- Types of credentials enrolled for each user
- Number of users utilizing managed logons
- Dates of first and last fingerprint enrollment

Additionally certain operations may be performed against the DigitalPersona user database through the ActiveX control, such as:

- Lock user account

- Set user logon policy
- Delete specific authentication credentials
- Delete user secrets

For further information on the ActiveX control and the Command Line utility, see the DigitalPersona Pro Enterprise Administrator Guide.

Attended Enrollment Tool

The Attended Enrollment Tool is a component of the DigitalPersona Pro Administration Tools. It can be used to add a higher level of security to the implementation and use of DigitalPersona Pro Enterprise.

With attended enrollment, a designated user (or member of a designated user group) is assigned the permission to supervise the credential enrollment process of other users. Users are prohibited from enrolling or managing their own credentials.

On the computer where the Attended Enrollment Tool will be used -

- Install DigitalPersona Pro Workstation for Enterprise in Roaming mode.
- Install the Attended Enrollment Tool component from the DigitalPersona Pro Administration Tools folder of your product package.
- Additional steps necessary to set up Attended Enrollment prior to use are defined in the online help and the DigitalPersona Pro Enterprise Administration Guide.

GPMC extensions

DigitalPersona Pro Enterprise Server and its associated workstation clients use Group Policy Management Console (GPMC) extensions, installed under the *Software Settings* and *Administrative Templates* nodes, to link product policies and settings to Active Directory containers.

The GPMC Extensions component includes several Administrative Templates and additional extensions such as the Authentication Policy and Kiosk Administration extensions.

Adding an Administrative Template to a container applies the DigitalPersona Pro Enterprise policies and settings to the computers and users in that container.

Each setting includes a complete description of its purpose and use on the Explain tab. Additionally, a complete list and description of these settings, as well as an alphabetical listing, are available in the DigitalPersona Pro Enterprise Administrator Guide.

Authentication Policy Editor

The Authentication Policy Editor provides access to two of the most commonly used Pro Enterprise policies. They can be found at: [domain, site or OU], Computer Configuration, Policies, Software Settings, DigitalPersona Pro Client, Security, Authentication.

The Logon Authentication Policy defines the credentials that end-users may provide when logging on to Windows. By default, all supported credentials are listed and any of the credentials or credential combinations may be used for authentication.

The Session Authentication Policy defines the credentials that end-users may provide when accessing Security applications and features during a Windows session. By default, all supported credentials are listed and any of the credentials or credential combinations may be used for authentication.

- To edit or delete a credential from either policy, click the arrow that appears to the right of the credential.
- To add a credential to the list, click **Add** at the top of the list.

Each setting includes a complete description of its purpose and use on the Explain tab. Additionally, a complete list and description of these settings, as well as an alphabetical listing, are available in the DigitalPersona Pro Enterprise Administrator Guide.

Extended Server Policy Module

The Extended Server Policy Module (ESPM) is a separately purchased and installed server module that adds additional per user policies to the DigitalPersona tab in the AD user Properties dialog.

These extended policies provide additional settings associated with the use of biometric credentials such as fingerprints.

Included settings are:

User may only log on with Fingerprint credential

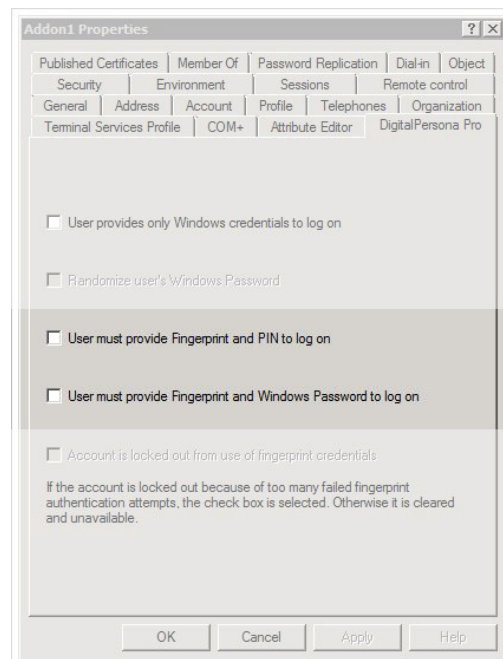
The user must verify their identity with a fingerprint credential in order to log on to Windows. No other credentials can be used, except for supported recovery options such as Self Password Recovery.

User must provide Fingerprint and PIN to log on

The user must provide a PIN whenever a fingerprint is used to log on, to unlock the computer or to change their Windows password. The fingerprint PIN option adds another level of security to logging on with a fingerprint.

User must provide Fingerprint and Windows Password to log on

The user must verify their identity with their fingerprint credential in addition to Windows authentication (a smart card or password according to the Windows policy setting).



Administrative Console Plug-ins

Password Manager Admin Tool

The Password Manager Admin Tool, an optional plug-in to the DigitalPersona Pro Enterprise Administrative Console, enables administrators to provide controlled access to network resources, programs and websites by adding any of a variety of authentication mechanisms (such as password, smart card, fingerprints or Defender-compatible VPN tokens) to their logon and change password screens. These *managed logons* can then be automatically deployed to computers where the Password Manager application is installed and which are being managed by a DigitalPersona Pro server.

Setting up a logon screen can be as simple as specifying attributes (such as the user name, password, the submit button and other required fields) in a managed logon for the website or program. The change password process can also be automated by specifying details such as whether the password can be changed by the user at will, or must be changed at prescribed intervals, and any additional password format restriction.

The Password Manager Admin Tool also provides many configurable options for defining and reusing information for logon and change password screens.

Before using The Password Manager Admin Tool, you will need to set it up for your network. This consists of creating a shared network folder and enabling the “Managed Logons” setting for the GPO governing the DigitalPersona Pro clients that you wish to deploy the managed logons to. For instructions on these steps, see The Password Manager Admin Tool chapter in the DigitalPersona Pro Enterprise Administrator Guide.

Creating managed logons

To create a managed logon

- 1 Launch the logon screen for a website or program.
- 2 Open the DigitalPersona Pro Administrator Console.
- 3 Click Password Manager Admin Tool in the navigation panel.
- 4 On the **Logons** tab, choose a folder where the managed logons are to be stored. This location must be accessible to computers where users will be using the logons.
- 5 Click **Add Logon**.
- 6 The Password Manager Admin Tool Logon Screen wizard displays. Follow the onscreen instructions to specify logon fields, attributes, values and properties. See the Password Admin Tool online help or the Password Manager Admin Tool Application Guide for detailed instructions.

Deploying managed logons

To deploy managed logons:

The GPO setting, **path to the managed logons folder**, must be enabled on the Pro Enterprise Server, and you must have entered the path to the shared folder where the managed logons are stored, i.e. the folder that was created or selected by clicking the **Choose folder** button.

1. In the Password Manager Admin Tool, on the Logons page, check the boxes next to specific logons to change their status from *In Test* to *In Use*. (See illustration on previous page.) Only logons with an "In Use" status will be visible to users.
3. Click **Apply**.



After managed logons are deployed, a Password Manager icon on the screen tells the user that they can fill in the requested account data by verifying their identity with the required credentials. For more information on the Password Manager Admin Tool and Password Manager, see the DigitalPersona Pro Admin Tool Application Guide.

After managed logons are created and deployed, they are made available to computers managed by DigitalPersona Pro after their next restart, or after a specified time interval as configured by the Pro administrator.

Depending on the settings applied by the administrator, the user may be prompted for account data, such as user name, password, and other information during the first logon. During subsequent logons, the account data is provided by Password Manager after the user's identity is confirmed by supplying the credentials required by the Session Authentication Policy in effect.

The Password Manager Admin Tool is included in certain Pro Server packages, and is also available as an optional add-in from your DigitalPersona Account Manager or product Reseller. Detailed documentation is provided in the online help available from within the product.

DigitalPersona Defender VPN module

The DigitalPersona Defender module provides generation and validation of One Time Passwords that support most RADIUS-based VPNs, such as CISCO and Juniper; and that can be used with any method or device that is based on OATH-compliant one-time passwords.

This one-time-password can be automatically generated on the user's PC, typically upon successful authentication using one of the strong identity methods that DigitalPersona Pro supports. The OTP can then be used with Password Manager Pro as an additional factor required for logging in to corporate VPNs through managed logons deployed by the administrator.

This feature requires separate installation of DigitalPersona Defender, an optional server product providing token-based two-factor authentication to network, website, and application-based resources. Additional information on this product is available from your DigitalPersona partner or our website at <http://www.digitalpersona.com/enterprise>.

Event Logging and Auditing

DigitalPersona Pro logs activity events and (optionally) status events to the Windows Event Log on the server, client and in some cases both computers. These events can be forwarded to a designated collector computer and reported on through DigitalPersona Reporter, a separately installed event collection, analysis and reporting component.

Administrators can view, sort, and export all local events from the Windows Event Viewer, or view forwarded events from the Windows Event Viewer “Forwarded Events” log on the collector computer. This assists administrators in meeting compliance requirements for Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA.

For further details on DigitalPersona Reporter, see the corresponding chapter in the DigitalPersona Pro Enterprise Administrator Guide, available at

<http://www.digitalpersona.com/products/material>.

Additional Resources

Use the following resources for additional information about this product:

- The DigitalPersona Pro Enterprise Administrator Guide and associated Application Guides can be found on our website at:

<http://www.digitalpersona.com/products/material>.

- The Readme.txt file containing last minute information is included in the product package.
- AskPersona.com (<http://www.askpersona.com>) is a DigitalPersona Knowledge Portal providing answers to many frequently asked questions about our enterprise and consumer products.
- DigitalPersona Maintenance and Support customers will find additional information about technical support resources in their Maintenance and Support confirmation email.

Online Help is available for all enterprise and consumer products, and can be accessed from within each product.

This guide and the software it describes are furnished under license as set forth in the applicable End User License Agreement (the “EULA”) located in the product package; are furnished for informational use only, and are subject to change without notice.

© 1996-2012 DigitalPersona, Inc. All Rights Reserved. DigitalPersona, the DigitalPersona logo, U.are.U and One Touch are trademarks of DigitalPersona, Inc. registered in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.

Published: 11/02/2012 (5.4.0)