

DigitalPersona® Pro Workgroup

Version 1.0

Administrator Guide



digitalPersona.

© 2010 DigitalPersona, Inc. All Rights Reserved.

All intellectual property rights in the DigitalPersona software, firmware, hardware and documentation included with or described in this guide are owned by DigitalPersona or its suppliers and are protected by United States copyright laws, other applicable copyright laws, and international treaty provisions. DigitalPersona and its suppliers retain all rights not expressly granted.

DigitalPersona® is a trademark of DigitalPersona, Inc. registered in the United States and other countries. Windows, Windows Server 2003/2008, Windows Vista and Windows XP are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

This DigitalPersona Pro Workgroup Administrator Guide and the software it describes are furnished under license as set forth in the “License Agreement” screen that is shown during the installation process.

Except as permitted by such license, no part of this document may be reproduced, stored, transmitted and translated, in any form and by any means, without the prior written consent of DigitalPersona. The contents of this manual are furnished for informational use only and are subject to change without notice. Any mention of third-party companies and products is for demonstration purposes only and constitutes neither an endorsement nor a recommendation. DigitalPersona assumes no responsibility with regard to the performance or use of these third-party products. DigitalPersona makes every effort to ensure the accuracy of its documentation and assumes no responsibility or liability for any errors or inaccuracies that may appear in it.

Feedback

We welcome your feedback on any errors, omissions, or suggestions for future improvements. You may contact us at:

- TechPubs@digitalpersona.com
- DigitalPersona, Inc.
720 Bay Road, Suite 100
Redwood City, California 94063 USA
- Tel: (650) 474-4000
- Fax: (650) 298-8313

Document Revised: 4/8/2010 (Software version 1.0)

Table of Contents

- 1 Introduction 1**
 - Chapter Overview 1
 - Glossary 2
 - Recommended Skill Set 4
 - Support Resources 4

- 2 Solution Overview 5**
 - Solution overview 5
 - Product line 5
 - Pro Workgroup server 6
 - DigitalPersona Pro Workstation for Workgroup 6
 - DigitalPersona Pro Workgroup Add-on 7
 - Password Manager Pro 7
 - Full Disk Encryption 7
 - Feature overview 8
 - Managing computers 8
 - Managing users 8
 - Configuration & deployment 8
 - Security Model 8
 - Licensing 9
 - Product Compatibility 10

- 3 Installation & Deployment 11**
 - System Requirements 11
 - Planning 12
 - Support 13
 - Installation 14
 - Server installation 14
 - Internet access to Pro Workgroup 15
 - Client Installation 16
 - Deployment 16
 - Setting up computers to be managed 16
 - Creating & Deploying Managed Logons 17
 - Backup 17
 - Uninstallation 18

Table of Contents

4 Policies and Settings	19
5 Pro Workgroup Events	21
Session operations	21
Workstation operations	21
Group operations	24
User and Storage operations	25
License operations	27
Privileged user operations	28
Installation package operations	30
6 Index	32

DigitalPersona Pro Workgroup is the central management solution for Endpoint Protection, including data protection, access management and secure communications.

With DigitalPersona Pro Workgroup, you can securely and conveniently manage, organize and recover access to computers running a compatible Pro Workgroup client, such as DigitalPersona Pro Workstation for Workgroup or HP ProtectTools.

Groups can be created based on your organizational structure and your security needs. Group settings are centrally configured and automatically deployed to client computers at intervals specified by the administrator. You can also provide access to users who are locked out of their computers.

The DigitalPersona Pro Workgroup Administrator Guide provides information that an administrator will need to know in order to understand, plan for, install and deploy the solution in your enterprise.

Detailed descriptions of specific features contained in the server and client components are included in their respective help systems, and are not duplicated in this guide.

Chapter Overview

Chapter 1, *Introduction*, provides a general orientation to the DigitalPersona Pro Workgroup solution, its terminology, and the contents of this Administrator Guide.

Chapter 2, *Solution Overview*, is a high-level introduction to DigitalPersona Workgroup, its components, features and security structure.

Chapter 3, *Installation & Deployment*, lists system requirements, discusses deployment considerations and scenarios, and describes changes made to your system during installation. Instructions are given for installation of the Pro Workgroup server and associated clients.

Chapter 4, *Policies and Settings*, provides a complete description of all available policies and settings that can be applied to groups of managed computers.

Chapter 5, *Pro Workgroup Events*, describes each event generated by Pro Workgroup, what data is reported and the level of detail available.

Glossary

administrator account

In this document, unless otherwise specified, refers to the Pro Workgroup administrator, not a local Windows Administrator account.

authentication

DigitalPersona Pro Workgroup allows an administrator to set authentication policy for a group of computers.

When a Pro Workgroup server is unavailable, such as when a laptop is disconnected from the network, the authentication policy is retrieved from a local cache on the computer. The authentication policy can be modified by a Pro Workgroup administrator using settings available through the Pro Workgroup web console (see “Policies and Settings” on page 19).

credentials

Credentials are a set of information used to gain access to your computer, Windows account or to a password protected website or program. Credentials may include a combination of a user name, password, fingerprint, fingerprint PIN, smart card or facial recognition.

group

A collection of managed computers sharing identical Pro Workgroup settings.

logon

Account data for a website, program or password change screen that allows a user to logon by using specific credentials as specified by the Pro Workgroup administrator. There are two types of logons, personal logons and managed logons. See separate glossary entries.

managed logon

A logon (see above) created using Password Manager Pro, which can then be deployed to all managed computers. The term logon is generally used, except when specifically referring to logons created by an administrator with Password Manager Pro (managed logons) as contrasted with those created by an end-user (personal logons). When both managed and personal logons exist for the same program or website, the personal logon is disabled and only the managed logon may be used for access to the specified program or website. See also: personal logon.

managed computer - Any computer running a compatible Pro Workgroup client, such as DigitalPersona Pro Workstation for Workgroup or HP ProtectTools 6.0 (with Pro Workgroup Add-on installed), that has been set up to be managed by Pro Workgroup.

managed user - Any Windows user (local or domain) who has an account on a managed computer.

One time access - A link on a user's Windows tile screen that provides a means for recovering access to their Windows account. This link is available only on computers managed by Pro Workgroup.

Password Manager

A security application included with Pro Workgroup compatible clients that allows users to create their own personal logons for programs and websites. These logons may be used to launch the program or website and automatically fill in required account data after verify their identity with whatever credentials may be specified by the Pro Workgroup administrator.

Password Manager Pro

An optional module that plugs into the Administrative Console of compatible workstation clients that enables the creation, administration and management of logons for password-protected software programs and websites. Users simply verify their identity by supplying required credentials to securely provide data for logon fields, such as user name and password, on any website or program logon screen.

Administrators use the Password Manager Pro application to create and deploy the managed logons. End-users access the logons through the Password Manager application and replication of the logons is handled through the Pro Workgroup server.

personal logon

A logon created by an end-user with the Password Manager application. The term logon is generally used, except when contrasting logons created by an end-user (personal logons) with those created by an administrator with Password Manager Pro (managed logons). See also: managed logons.

recover computer - Provide a means for users to access their computer when they are locked out at the pre-boot level.

recover user - Provide a means for users to access their user account when they are locked out at the pre-boot level and/or their Windows account.

secret

Application specific user data that is stored securely on the Pro Workgroup server. The secret is released to a requesting application upon successful verification of the user's identity, and used to log on to programs and websites for which logons have been created.

settings

Defined authentication policies, security features and other configuration options managed by Pro Workgroup.

web console - A web application used to administer Pro Workgroup server and manage its groups, computers and users.

Recommended Skill Set

To fully and effectively utilize the information contained in this guide, we recommend that you possess the minimum skills and knowledge defined below.

Administrators

DigitalPersona Workgroup provides an out-of-the box solution that assumes only general knowledge of client-server application installation and familiarity with basic Windows operations. This administrator guide aims to provide you with any additional information you may need to operate and manage the Pro Workgroup environment. Help systems included with both the server and client applications provide more detailed explanations of specific features and functions.

Workstation End Users

End users of DigitalPersona Pro Workgroup clients should possess basic computer and network operation skills, such as logging on to a computer and using the taskbar, shortcut menus and a Web browser.

Support Resources

In addition to this guide, the following resources are provided for additional support to users of DigitalPersona Pro Workgroup:

- Readme files are provided in the root directory of the product package for each product. These files often contain late-breaking information about the product.
- AskPersona.com (<http://askpersona.com>) is a DigitalPersona Knowledge Portal providing answers to many frequently asked questions about our products.
- DigitalPersona Maintenance and Support customers will find additional information about technical support resources in their Maintenance and Support confirmation email.
- Online help is included with each component of the product. Context-sensitive help is accessible from various pages, menus and dialog boxes that appear during the use of the software.

This chapter provides a high-level overview of the DigitalPersona Pro Workgroup solution. For a more comprehensive description of specific features and functions, please see the help system available with each product.

DigitalPersona Pro Workgroup is an out-of-the-box central management solution for Endpoint Protection, including data protection, access management and secure communications.

You can use it to organize computers in groups based on your organization and your security needs, without the need to install and configure Microsoft Active Directory. Group settings are stored in a SQL database located on the server where they can be centrally configured and automatically deployed to client computers. You can also provide access to users who are locked out of their computers or Windows accounts.

Product line

The DigitalPersona Pro Workgroup product line includes the following products.

Component	Description	Page
DigitalPersona Pro Workgroup server	Provides central management of security policies and settings for computers with compatible clients.	6
DigitalPersona Pro Workstation for Workgroup	Provides endpoint protection features which can be customized to achieve a good balance of security and convenience, as well as administrative functions.	6
DigitalPersona Pro Workgroup Add-on	A simple to install plug-in for HP ProtectTools Security Manager 5.x, which enables centralized management by DigitalPersona Pro Workgroup.	7
DigitalPersona Password Manager Pro	An administrative tool used to create managed logons for websites and applications for deployment to computers managed by DigitalPersona Pro Workgroup.	7
Full Disk Encryption	A plug-in that provides complete data protection by encrypting your computer hard drive.	7

Each of the products listed above are described in the following pages. Additional plug-ins may be available. Contact your DigitalPersona partner or reseller for further information, or go to our website at: <http://www.digitalpersona.com/pro-workgroup>.

Pro Workgroup server

The DigitalPersona Pro Workgroup server is used to centrally manage groups of computers with compatible client software installed. All computers in a group share identical security settings, which are configured from the server and applied to each computer in the group. Settings are refreshed at intervals specified by the Pro Workgroup administrator.

- The Pro Workgroup server is administered through a browser-based console installed with the server and automatically set up as a dedicated fully-functional intranet website. The DigitalPersona Pro Workgroup web console provides an intuitive interface for managing server features, member computers and their users, and their associated policies and settings.

Additionally, the server product includes a command-line utility, the DigitalPersona Pro Workgroup Setup Tool (DPWGSTool.exe), that can be used to create a new SSL certificate for Pro Workgroup or to create a DigitalPersona Pro Workgroup Setup (MSI) file.

- MSI files can be run locally or remotely on each computer that is to be managed by Pro Workgroup, or automatically through GPOs and other software deployment tools.

The Setup file created with this tool will require the name and password of a Pro Workgroup administrator when it is run.

This same type of Setup file can also be created from the **Administration, Deployment** tab of the DigitalPersona Pro Workgroup web console. Also, on this tab, you can create additional types of Setup files for deployment by a specifically designated person or for silent deployment.

- DigitalPersona Pro server uses Microsoft SQL Server 2008 Express for storing DigitalPersona Pro Workgroup settings and data.

See Chapter 3, *Installation & Deployment*, for specific system requirements, installation procedure and deployment scenarios.

DigitalPersona Pro Workstation for Workgroup

DigitalPersona Pro Workstation for Workgroup provides the following features:

- **Dashboard** - A central location for managing your security applications.
- **Mini-dashboard** - Quick access to Password Manager logons for programs and websites.
- **Credential Manager** - increases both security and convenience by providing alternative and multi-factor credentials in addition to or in place of passwords used for Windows log on. Credentials required for access to managed computers are specified at the group level by the administrator through the Pro Workgroup web console.

- **Password Manager** - provides end users with the ability to create personal logons for access to programs and websites. Administrators can also create managed logons (using Password Manager Pro) that are then deployed to workstations, superceding any personal logons created for the same program or website.
- **Discover more** - Additional security applications may be available to plug in new features to DigitalPersona Pro Workstation for Workgroup. The ability to discover these applications and install them may be regulated through a setting on the DigitalPersona Pro Workgroup web console.

DigitalPersona Pro Workgroup Add-on

The DigitalPersona Pro Workgroup Add-on is included in the solution package, and used to enable workstations with HP ProtectTools Security Manager (v5.04 or above) installed to be managed with Pro Workgroup.

Simply execute the setup file on the workstation to enable this functionality.

Password Manager Pro

Password Manager Pro simplifies and secures access to password-protected software programs and websites through the use of managed logons that allow end-users to identify themselves through the use of such mechanisms as fingerprints, smart cards and facial recognition in addition to, or instead of passwords.

Administrators use the DigitalPersona Password Manager Pro application to create managed logons specifying information for program or website logon and change password screens. These are then deployed to managed workstations, where they are accessible through the Password Manager application and the mini-dashboard. Managed logons always take precedence over personal logons created by end users.

Full Disk Encryption

Full Disk Encryption (FDE) provides complete data protection by encrypting your computer hard drive.

An easy-to-use, intuitive user interface makes encrypting a computer's hard drive a simple matter of point and click. The plug-in enables Pro Workgroup administrators to activate and deactivate full disk encryption, manage FDE users and backup a unique encryption key to a USB connected storage drive for recovery in case of a forgotten password.

Feature overview

DigitalPersona Pro Workgroup enables centralized security management of compatible workstations and their users.

Managing computers

DigitalPersona Pro Workgroup provides the ability to manage security policies and settings for groups of computers without the need for Active Directory. It provides a browser-based console for administering both computers and users, as well as the ability to remotely grant one-time access to managed computers and Windows accounts.

Managing users

When a workstation becomes managed by DigitalPersona Pro Workgroup, all current and future users of the computer (both local and domain) will become managed users after their next logon to Windows. This means that security policies and settings configured for the group this computer belongs to will apply to all current users of the workstation. Additionally, Pro Workgroup can be used to recover access to a computer or Windows account when users are locked out. (See the Pro Workgroup server help file for recovery procedures.).

Configuration & deployment

Policies and settings for a group are configured through the DigitalPersona Pro Workgroup web console. All policies and settings are described in the topic “Policies and Settings” on page 19.

Group policies and settings are deployed to managed workstations at intervals defined on the Settings tab for the group.

Security Model

DigitalPersona Pro Workgroup utilizes the Windows Communication Foundation (WCF), a Microsoft communication infrastructure that was designed to create distributed applications that address today’s security needs. Internet Information Services 7 is used to host the WCF for the Pro Workgroup server. Each workstation client uses a WCF proxy.

Installation of the DigitalPersona Pro Workgroup server includes generation of a self-signed certificate and creation of an .MSI file used to install the certificate (and necessary connection information) onto client workstations that are to be managed.

All communication between the Pro Workgroup server and managed clients is signed and encrypted in WCF running over the http protocol.

During client setup, each client workstation is also assigned a very long password that is used to authenticate it during each communication with the server.

Configuration information, policies and settings and logon data are stored in an SQL Express database on the server (by default, located on the same machine where IIS is running), and is not directly accessible from the outside.

The web console used to administer the server uses https and SSL to secure the traffic between the web browser and the server. Each communication event is also logged to the SQL database. Events, data written and their level of detail, are provided in Pro Workgroup Events beginning on page 21.

Licensing

Overview

The DigitalPersona Pro Workgroup solution includes the following licensed features:

- Client licenses - Five client workstations (seats) may be managed with DigitalPersona Pro Workgroup right out of the box. Additional client licenses may be purchased from your DigitalPersona partner or reseller, or directly from our ecommerce site. For more information about client licenses, see digitalpersona.com/pro-workgroup.
- Password Manager - This security application, used to create personal logons for programs and websites, is included as part of all Pro Workgroup compatible clients.

Optional modules

These optional modules are separately licensed:

- **Password Manager Pro** - Create managed logons for automatic deployment to computers, enabling users to logon on specified programs and websites using credentials specified by the administrator. This security application is a plug-in to the workstation client's Administrative Console. For more information, see digitalpersona.com/pro-workgroup.

License Purchase & Activation

You may purchase and activate additional client licenses or licenses for optional modules from the Administration tab in the DigitalPersona Pro Workgroup web console.

Purchase - Click the **Buy More** link and follow the onscreen instructions. License information required for activation may vary depending on the type of license purchased and the manner in which it is purchased.

Activation - Click **Activate** and follow the onscreen instructions.

Product Compatibility

DigitalPersona Pro Workgroup server 1.x

- Requires compatible workstation software on each computer to be managed. See “System Requirements” on page 11 for a list of compatible client software.
- Cannot coexist with the following DigitalPersona products
 - DigitalPersona Pro Server for Active Directory
 - DigitalPersona Pro Workstation
 - DigitalPersona Pro Kiosk
 - DigitalPersona Pro Kiosk for ID Server
 - DigitalPersona Personal

DigitalPersona Pro Workstation for Workgroup

- Requires a properly installed and configured instance of the DigitalPersona Pro Workgroup server and a working connection to the server.
- Cannot coexist with the following DigitalPersona products
 - DigitalPersona Pro Server for Active Directory
 - DigitalPersona Pro Workstation
 - DigitalPersona Pro Kiosk
 - DigitalPersona Pro Kiosk for ID Server
 - DigitalPersona Personal
 - HP ProtectTools Security Manager

DigitalPersona Pro Workgroup Add-on

- Requires HP ProtectTools Security Manager 5.0
- Cannot coexist with the following DigitalPersona products
 - DigitalPersona Pro Server for Active Directory
 - DigitalPersona Pro Workstation
 - DigitalPersona Pro Kiosk
 - DigitalPersona Pro Kiosk for ID Server
 - DigitalPersona Personal

This chapter provides instructions for installing and deploying DigitalPersona Workgroup, and addresses the following topics:

Topic	Page
System Requirements	11
Installation	14
Planning	12
Support	13
Backup	17
Uninstallation	18

System Requirements

Before beginning the installation of DigitalPersona Pro Workgroup components, ensure that each target system meets the following minimum requirements.

Pro Workgroup server

- One of the following operating systems:
 - Windows Server 2008 (32 or 64-bit), any edition
 - Windows 7 (32 or 64-bit), any edition
 - Windows Vista (32 or 64-bit), any edition
- User must have administrative privileges

Pro Workstation for Workgroup

- One of the following operating systems:
 - Windows 7 (32 or 64-bit), any edition
 - Windows Vista (32 or 64-bit), any edition
 - Windows XP (32-bit), any edition
- Microsoft .NET Framework 3.5 or later
- User must have administrative privileges for installation and setup
- HP ProtectTools Security Manager is NOT installed on the computer

Pro Workgroup Add-on

- One of the following operating systems:
 - Windows 7 (32 or 64-bit)
 - Windows Vista (32 or 64-bit)
 - Windows XP (32-bit)

* Windows XP, Vista, and Windows 7 Home editions are not supported.
- HP ProtectTools Security Manager 5.04 or above
- User must have administrative privileges for installation and setup

Password Manager Pro

- One of the following operating systems:
 - Windows 7 (32 or 64-bit), any edition
 - Windows Vista (32 or 64-bit), any edition
 - Windows XP (32-bit), any edition
- Microsoft .NET Framework 3.5 or later
- Internet Explorer 6 or above
- User must have administrative privileges for installation and setup
- One of the following Pro Workgroup clients
 - DigitalPersona Pro Workstation for Workgroup
 - HP ProtectTools 5.04 or above with Pro Workgroup Add-on

Always check the readme file included with your installation package for the latest information on the product.

Planning

We have made planning for and deploying DigitalPersona Pro Workgroup as simple and straightforward as possible. However, a comprehensive design, a well-formed deployment plan, and a well-informed deployment staff will help to ensure a successful implementation.

Whatever the size of the deployment, it is critical to spend some time designing an implementation that will meet your organization's needs, provide a straightforward deployment plan, and allow you to allocate the necessary hardware and personnel resources.

In designing your DigitalPersona Pro Workgroup solution, you will want to take into account many factors, including your security needs, performance requirements, levels of administration, and the amount of control that you want to allow the end user to have with certain features like

personal and managed logons, multi-factor authentication and access to the client Administrative Console.

Deploying DigitalPersona Pro Workgroup includes configuring settings that affect the way that authentication operates in your specific environment, including multi-factor authentication. The level of security that you require is up to you, and is quite easily implemented through the included Pro Workgroup server and web console.

The information provided in this chapter is not intended to take the place of the services of a professional systems architect or analyst, and should not be construed as advice or recommendations addressing your specific situation.

Support

Evaluation Support

During your evaluation of this DigitalPersona product, support is available through our Sales Engineering Team at 1-650-474-4042

Technical Support

AskPersona.com (<http://askpersona.com>) is a Pro Knowledge Portal providing answers to many frequently asked questions about Pro Server, Workstation and Kiosk.

DigitalPersona Maintenance and Support customers will find additional information about technical support resources to them in their Maintenance and Support confirmation email.

Professional Services

DigitalPersona Professional Services can discuss options ranging from initial onsite consulting to completely outsourcing all or part of the design, deployment and installation process as well as customizing the software.

For Professional Services, please contact your DigitalPersona Account Manager or product Reseller.

Installation

DigitalPersona Pro Workgroup is optimized for a straightforward out-of-the-box installation on your company intranet. It automatically creates a website where you can access its web console to administer the Pro Workgroup server and managed computers, and a default Setup (MSI) file that can be used to setup computers to be managed.

Server installation

The DigitalPersona Pro Workgroup installation wizard will guide you through the steps necessary to install the solution for access within your corporate network. If you are planning on accessing the Pro Workgroup server from the internet, see the section immediately following this one, beginning on page

Note that the following installation creates a fully functioning web server and SQL database. These should be included in your company strategy for updating and backing up the underlying Windows software such as Internet Information Services and the MS SQL database.

1. Ensure that the computer meets the minimum requirements for the Pro Workgroup server listed on page 11.
2. Open the self-extracting (.exe) product package. The Installation wizard will guide you through the installation process.
3. This list of actions performed during the installation may help you judge the installation progress, which should take between 30 to 60 minutes, depending on the performance of the target computer.
 - Enable required Windows features
 - Install Microsoft .NET Framework 3.5.1
 - Install Windows Installer 4.5
 - Enable and configure IIS (Internet Information Services) 7
 - Install and start the Windows Process Activation Service
 - Install and configure MS SQL Server 2008 Express
 - Create and install server and SSL certificates, configure ACLs.
 - Create DigitalPersona website directories and configure ACLs
 - Create website for Pro Workgroup server web administration
 - Configure registry information and set ACLs
 - Open ports 8000 (HTTP) and 443 (HTTPS) to inbound traffic
 - Test installation using a PING utility

4. In addition to the installation and configuration of the software, you will be asked to perform the following steps:
 - Create a username and password for the Pro Workgroup administrator.
 - Back up the private keys and certificate to a password-protected encrypted file.
 - Save a Pro Workgroup Setup (Connection.msi) file, that can be used to transfer required connection information to a client computer. This file can also be created from the Pro Workgroup web console, or by running the DPWGS Tool included with the product package.
5. Once the installation is complete, you can use the generated setup file to connect compatible clients to the server. You can access the Pro Workgroup web console locally through the https protocol using a web browser by simply entering the name of the computer where you installed the Pro Workgroup server, i.e. https://<computer name>.

Internet access to Pro Workgroup

If the administrator wants to manage computers that will be accessing the Pro Workgroup server from the internet. they need to take the following information into account.

- Computers both inside and outside the company will use the same connection string to access the Pro Workgroup server, i.e. an internet URL such as https://<computer name>.<domain>.
- You will need to add a DNS record for the Pro Workgroup server.
- Configure your firewalls and DMZ zones according to the latest recommended Internet security standards. This should include at least the following -
 - a. If IP Address translation is used, configure the IP Address translation.
 - b. If the Workgroup Server IP Address is visible from the Internet -
 - i. Install SQL Server from the Workgroup Server to another computer
 - ii. Move the database to that computer and connect the SQL server to it.
 - iii. Change the connection string on the Workgroup server to connect to the new database.
 - c. Installing an SSL certificate from some global certificate authority is highly recommended.

Also, when setting up computers to be managed by Pro Workgroup, you cannot use the Default Setup (MSI) file created during the server installation and available from the Deployment tab of the web console. You must create a new Setup file from the Web Console or by using the DigitalPersona Pro Workgroup Setup Tool (DPWGSTool.exe), specifying the domain in addition to the computer name which is automatically populated when creating the file through the web console. For example: Pro-Server.mydomain.com.

Client Installation

Each computer that is to be managed by DigitalPersona Pro Workgroup must have one of the following compatible clients installed on it.

- **DigitalPersona Pro Workstation for Workgroup** - This client application natively supports management by DigitalPersona Pro Workgroup. No further installation is required. However, see the following topic, “Setting up computers to be managed.”
- **HP ProtectTools 5.x** - Computers with preloaded HP ProtectTools 5.x software can be made compatible with DigitalPersona Pro Workgroup by installing the DigitalPersona Pro Workgroup Add-on upon each workstation to be managed. This add-on is included in the DigitalPersona Pro Workgroup package. Simply copy the add-on to the workstation, launch it and follow the instructions in the wizard.

Deployment

Setting up computers to be managed

Each computer that is to be managed by the Pro Workgroup server must first be set up to work with the server. This may be done manually on each computer, or through various automated deployment mechanisms.

The Pro Workgroup Setup (.MSI) file is used to set up computers which will be managed by Pro Workgroup and provides necessary connection information as well as installing the server's public certificate in a client's certificate storage.

As part of the installation of the Pro Workgroup server, a default Pro Workgroup Setup file was created, and saved to a location specified at the time of installation.

- The same file can also be downloaded from the Administration, Deployment tab of the Pro Workgroup web console, or by running the DPWG Setup Tool (DPWGSTool.exe) on the server. This tool can be found in your product package, but is not installed by default on the server.
- The Default Setup file created during installation, or downloaded from the web console will require entry of a Pro Workgroup administrator credentials when being run.

You can also create new Pro Workgroup Setup files from the web console Administration, Deployment tab. When creating a setup file from the Deployment tab, you can choose whether it can only be deployed by a Pro Workgroup administrator, must be deployed by a specifically designated user, or can be run silently by anyone.

To start managing a computer with Pro Workgroup

1. Run the Pro Workgroup Setup file on each computer to be managed, or deploy the setup file through an automated deployment mechanism.
2. Follow the onscreen instructions. This will include selecting a group to add the computer to.

You may also create a new group using the default settings, which can be changed later using the web console.

3. After completing the wizard and closing the client's Administrative Console, by default the console can then only be opened by a Pro Workgroup administrator. This behavior may be changed by the administrator as desired. (See “Policies and Settings” on page 19.)

To stop managing a computer

- Uninstall “DigitalPersona Pro Workgroup Connection” from the Windows Control Panel, or rerun the original Pro Workgroup Setup (MSI) file that was used to start managing the computer.

To create a Pro Workgroup Setup file

1. On the Deployment tab, click **New**.
2. Follow the instructions provided on the screen.

To download a Pro Workgroup Setup file

- Click a file name in the Setup file list.

Creating & Deploying Managed Logons

DigitalPersona Password Manager Pro is an optional module that allows administrator to create logons for specific programs and websites and then deploy these “managed logons” to workstations managed by DigitalPersona Pro Workgroup. For further information on DigitalPersona Password Manager Pro, see one of the following references -

- Password Manager Pro on page 7
- Password Manager Pro Administrator Guide
- Online help provided with the program.

Backup

The simplest backup strategy would be to create a duplicate image, or “ghost” of an entire partition or drive where Pro Workgroup is installed. This would include the configuration-dependent license key, and enable the easiest reinstallation path. Note that information about

member computers will not be current if they have become managed or unmanaged since the image was made.

You can stop managing a computer by uninstalling the DigitalPersona Pro Workgroup Setup (MSI) file on any affected workstations, or start managing it by running the Setup file.

Uninstallation

Note that in order to facilitate maintenance and possible re-installation of DigitalPersona Pro Workgroup, certain actions and states are NOT reversed during uninstallation.

- Internet Information Services features enabled during the installation remain enabled after uninstallation.
- The Microsoft SQL Server 2008 Express database created during the installation and used by DigitalPersona Pro Workgroup is not uninstalled.

The following policies and settings can be set on the **Computers and Users, Settings tab** of the Pro Workgroup web console. They can be set (or copied) for each group of managed computers, and will be deployed to computers in the group at the interval specified in the associated interval setting (listed below).

Setting	Description
<i>Security - Features</i>	
Protect access to the computer	Require logon prior to starting Windows. Applies only to computers with built-in Pre-boot logon capabilities.
Protect Windows accounts	Protect Windows accounts using strong authentication.
<i>Security - Authentication</i>	
Logon policy	Specify the credentials needed to access the computer, decrypt the hard drive and log on to Windows.
Session policy	Specify the credentials needed to access client security applications during the Windows session.
<i>Security - Settings</i>	
Allow One Step logon	Allow users to log on to Windows automatically after pre-boot authentication.
Allow SpareKey	Allow users to log on to Windows using HP SpareKey, overriding the Logon authentication policy in effect.
<i>Devices - Fingerprint reader</i>	
Set the False Accept Rate	<p>Adjust the sensitivity of the fingerprint scan. Reduce this setting to minimize false acceptance. The False Accept Rate (FAR) is the mathematical probability (1:n) of false fingerprint verification.</p> <p>The higher the value of <i>n</i>, the less likely a fingerprint will be falsely accepted as verified. Particularly high values of <i>n</i> may cause false rejection of fingerprints from the same finger.</p> <p>The False Accept Rates is only a probabilistic estimate. Actual performance may vary in a given deployment.</p>
Set the minimum number of enrolled fingerprints	Select the minimum number of fingerprints that must be enrolled during the fingerprint enrollment process when it is required.

Setting	Description
Set the maximum number of enrolled fingerprints	<p>Select the maximum number of fingerprints that must be enrolled during the fingerprint enrollment process when it is required.</p> <p>This setting determines the maximum number of fingers that a user can enroll. The value for this setting influences both the speed of authentication and the probability of false accepts. For example, the more fingerprints a user enrolls, the more time it takes to authenticate or identify the user. Also, more comparisons increase the likelihood of false acceptance of the fingerprint. To increase security and maximize server efficiency, users should be allowed to enroll a maximum of two fingers.</p>
<i>Devices - Smart card</i>	
Lock the computer upon smart card removal	Prevent access to a computer when a smart card used is removed.
<i>Applications - Settings</i>	
Do not launch the Getting Started wizard upon logon	Prevent the Getting Started wizard from launching when a user logs on to the computer.
<i>Client - Administration</i>	
Do not allow users to run administration tools	Do not allow users to configure settings with the Administrative Console and the Setup wizard.
Do not prompt to authenticate with Pro Workgroup to run administration tools	Allow users to run the Administrative Console and the Setup wizard without logging on to Pro Workgroup.
Set the level of details for event logging	Select the level of details that you want to be written to the DigitalPersona Pro Workgroup event log.
Set interval for refreshing settings	Select the interval at which client computers obtain settings from the Workgroup server.
<i>Client - Software updates</i>	
Enable the Discover more button	Allow users to discover and add new client security applications by clicking the Discover more button.
Allow running auto updates on the computer	Allow client security applications to automatically download and install software updates.

DigitalPersona Pro Workgroup writes the following events an SQL database. Third party tools such as Crystal Reports can be used to view and report on the records in the database.

The events are classified into the following categories.

Description	Page
Session operations	21
Workstation operations	21
Group operations	24
User and user storage operations	25
License operations	27
Privileged user operations	28
Installation package operations	30

The following tables list all Pro Workgroup events by task category, providing an event name and ID, description, the data logged and the logging level for each event.

Session operations

These events are generated during session operations

Event (Event ID)	Description	Data	Level
Session opened. (0x101)	Session opened. Initiated by: <client name>	Event ID, Timestamp, Client ID	Detailed Full Detailed

Workstation operations

The following events are generated during workstation operations.

Event (Event ID)	Description	Data	Level
Workstation added to managed pool. (0x201)	Workstation added to managed pool. Workstation: <group name>\ <workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID)	Audit Detailed Full Detailed

Event (Event ID)	Description	Data	Level
Workstation addition to managed pool failed. (0x202)	Workstation added to managed pool failed. Workstation: <group name>\ <workstation name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID), Error code, Error description	Error Audit Detailed Full Detailed
Workstation removed from managed pool. (0x203)	Workstation removed from managed pool. Workstation: <workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID),	Audit Detailed Full Detailed
Workstation removal from managed pool failed. (0x204)	Workstation removal from managed pool failed. Workstation: <workstation name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID), Error code, Error description	Error Audit Detailed Full Detailed
Workstation modified. (0x205)	Workstation modified. Workstation: <group name>\ <workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID),	Audit Detailed Full Detailed
Workstation modification failed. (0x206)	Workstation modification failed. Workstation: <group name>\ <workstation name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID), Error code, Error description	Error Audit Detailed Full Detailed
Workstation recovered. (0x207)	Workstation recovered. Workstation: <group name>\ <workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID),	Audit Detailed Full Detailed

Event (Event ID)	Description	Data	Level
Workstation recovery failed. (0x208)	Workstation recovery failed. Workstation: <group name>\<workstation name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID), Error code, Error description	Error Audit Detailed Full Detailed
Workstation assigned to group. (0x209)	Workstation assigned to group. Workstation: <group name>\<workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID),	Audit Detailed Full Detailed
Workstation assignment to group failed. (0x20a)	Workstation assignment to group failed. Workstation: <group name>\<workstation name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Workstation ID (as Subject ID), Error code, Error description	Error Audit Detailed Full Detailed
Workstations enumerated. (0x20d)	Workstations enumerated. Initiated by: <user name>	Event ID, Timestamp, Client ID	Full Detailed
Workstation enumeration failed. (0x20e)	Workstation enumeration failed. Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Error code, Error description	Error Audit Detailed Full Detailed

Group operations

The following events are generated during group operations.

Event	Description	Data	Level
Group created. (0x301)	Group created. Group: <group name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Group ID (as Subject ID),	Audit Detailed Full Detailed
Group creation failed. (0x302)	Group creation failed. Group: <group name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Group ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
Group deleted. (0x303)	Group deleted. Group: <group name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Group ID (as Subject ID),	Audit Detailed Full Detailed
Group deletion failed. (0x304)	Group deletion failed. Group: <group name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Group ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
Group modified. (0x305)	Group modified. Group: <group name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Group ID (as Subject ID),	Audit Detailed Full Detailed
Group modification failed. (0x306)	Group modification failed. Group: <group name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Group ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
Groups enumerated. (0x307)	Groups enumerated. Initiated by: <user name>	Event ID, Timestamp, Client ID	Full Detailed

Event	Description	Data	Level
Group enumeration failed. (0x308)	Group enumeration failed. Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Error code, Error description	Error Audit Detailed Full Detailed
Group settings modified. (0x309)	Group settings modified. Group: <name> Initiated by: <user name>	Event ID, Timestamp, Client ID, Group ID (as Subject ID)	Audit Detailed Full Detailed

User and Storage operations

The following events are generated during User and Storage operations.

Event	Description	Data	Level
User created. (0x401)	User created. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name>	Event ID, Timestamp, Client ID, User ID (as Subject ID),	Audit Detailed Full Detailed
User creation failed. (0x402)	User creation failed. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
User deleted. (0x403)	User deleted. User: <name> Initiated by: <user name>	Event ID, Timestamp, Client ID, User ID (as Subject ID),	Audit Detailed Full Detailed
User deletion failed. (0x404)	User deletion failed. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
User modified. (0x405)	User modified. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name>	Event ID, Timestamp, Client ID, User ID (as Subject ID),	Audit Detailed Full Detailed

Event	Description	Data	Level
User modification failed. (0x406)	User modification failed. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
Users enumerated. (0x407)	Users enumerated. Workstation: <group name>\ <workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID	Full Detailed
User enumeration failed. (0x408)	User enumeration failed. Workstation: <group name>\ <workstation name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Error code, Error description	Error Audit Detailed Full Detailed
User storage created. (0x409)	User storage created. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name>	Event ID, Timestamp, Client ID, User ID (as Subject ID), Storage Name	Audit Detailed Full Detailed
User storage creation failed. (0x40a)	User storage creation failed. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Storage Name, Error code, Error description	Error, Audit Detailed Full Detailed
User storage deleted. (0x40b)	User storage deleted. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID, User ID (as Subject ID), Storage Name	Audit Detailed Full Detailed
User storage deletion failed. (0x40c)	User storage deletion failed. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Storage Name, Error code, Error description	Error, Audit Detailed Full Detailed

Event	Description	Data	Level
User storage modified. (0x40d)	User storage modified. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name>	Event ID, Timestamp, Client ID, User ID (as Subject ID), Storage Name	Audit Detailed Full Detailed
User storage modification failed. (0x40e)	User storage modification failed. User: <name> Workstation: <group name>\ <workstation name> Initiated by: <Initiating user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Storage Name, Error code, Error description	Error, Audit Detailed Full Detailed
User storage enumerated. (0x40f)	User storage enumerated. Workstation: <group name>\ <workstation name> Initiated by: <user name>	Event ID, Timestamp, Client ID, User ID (as Subject ID)	Full Detailed
User storage enumeration failed. (0x410)	User storage enumeration failed. Workstation: <group name>\ <workstation name> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Full Detailed

License operations

The following events are generated during license operations.

Event	Description	Data	Level
License activated. (0x501)	License activated. Type: <license type> ID: <license ID> Number of workstations: <number> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, License Type, License ID	Audit Detailed Full Detailed
License activation failed. (0x502)	License activation failed. Type: <license type> ID: <license ID> Number of workstations: <number> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, License Type, License ID, Error code, Error description	Error, Audit Detailed Full Detailed

Event	Description	Data	Level
License transfer in. (0x503)	License transferred in. Type: <license type> ID: <license ID> Initiated by: <user name>	Event ID, Timestamp, Client ID, License Type, License ID	Audit Detailed Full Detailed
License transfer in failed. (0x504)	License transfer in failed. Type: <license type> ID: <license ID> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, License Type, License ID, Error code, Error description	Error, Audit Detailed Full Detailed
License transfer out. (0x505)	License transferred out. Type: <license type> ID: <license ID> Initiated by: <user name>	Event ID, Timestamp, Client ID, License Type, License ID	Audit Detailed Full Detailed
License transfer out failed. (0x506)	License transfer out failed. Type: <license type> ID: <license ID> Initiated by: <user name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, License Type, License ID, Error code, Error description	Error, Audit Detailed Full Detailed

Privileged user operations

The following events are generated during the creation and management of privileged users.

Event	Description	Data	Level
Privileged user created. (0x601)	Privileged user created. Initiated by: <user name> User: <name>	Event ID, Timestamp, Client ID, User ID (as Subject ID)	Audit Detailed Full Detailed
Privileged user creation failed. (0x602)	Privileged user creation failed. Initiated by: <user name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed

Event	Description	Data	Level
Privileged user deleted. (0x603)	Privileged user deleted. Initiated by: <user name> User: <name>	Event ID, Timestamp, Client ID, User ID (as Subject ID)	Audit Detailed Full Detailed
Privileged user deletion failed. (0x604)	Privileged user deletion failed. Initiated by: <user name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
Privileged user modified. (0x605)	Privileged user modified. Initiated by: <user name> User: <name>	Event ID, Timestamp, Client ID, User ID (as Subject ID)	Audit Detailed Full Detailed
Privileged user modification failed. (0x606)	Privileged user modification failed. Initiated by: <user name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, License Type, License ID, Error code, Error description	Error, Audit Detailed Full Detailed
Privileged user's password changed. (0x607)	Privileged user's password changed. Initiated by: <user name> User: <name>	Event ID, Timestamp, Client ID, User ID (as Subject ID)	Audit Detailed Full Detailed
Privileged user's password change failed. (0x608)	Privileged user's password change failed. Initiated by: <user name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Audit Detailed Full Detailed
Privileged user unlocked. (0x609)	Privileged user unlocked. Initiated by: <user name> User: <name>	Event ID, Timestamp, Client ID, User ID (as Subject ID)	Audit Detailed Full Detailed
Privileged user unlock failed. (0x60a)	Privileged user unlock failed. Initiated by: <user name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, User ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed

Event	Description	Data	Level
Privileged users enumerated. (0x60b)	Privileged users enumerated. Initiated by: <user name>	Event ID, Timestamp, Client ID	Full Detailed
Privileged users enumeration failed. (0x60c)	Privileged user enumeration failed. Initiated by: <user name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Error code, Error description	Error, Audit Detailed Full Detailed

Installation package operations

The following events are generated during the creation and management of product installation packages (also called Pro Workgroup Setup (MSI) files).

Event	Description	Data	Level
Interactive installation package could not be created. (0x701)	Interactive installation package could not be created. Initiated by: <user name> Group: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Group ID (as Subject ID), Error code, Error description	Error, Audit Detailed Full Detailed
Interactive installation package has been created. (0x702)	Interactive installation package has been created. Initiated by: <user name> Group: <name>	Event ID, Timestamp, Client ID, Group ID (as Subject ID),	Audit Detailed Full Detailed
Delegated installation package could not be created. (0x703)	Delegated installation package could not be created. Initiated by: <user name> Group: <name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Group ID (as Subject ID), User ID (as Param1), Error code, Error description	Error, Audit Detailed Full Detailed
Delegated installation package has been created. (0x704)	Delegated installation package has been created. Initiated by: <user name> Group: <name> User: <name>	Event ID, Timestamp, Client ID, Group ID (as Subject ID), User ID (as Param1),	Audit Detailed Full Detailed

Event	Description	Data	Level
Silent installation package could not be created. (0x705)	Silent installation package could not be created. Initiated by: <user name> Group: <name> User: <name> Error: <error description> (<error code>)	Event ID, Timestamp, Client ID, Group ID (as Subject ID), User ID (as Param1), Error code, Error description	Error, Audit Detailed Full Detailed
Silent installation package has been created. (0x706)	Silent installation package has been created. Initiated by: <user name> Group: <name> User: <name>	Event ID, Timestamp, Client ID, Group ID (as Subject ID), User ID (as Param1),	Audit Detailed Full Detailed

Index

A

ACL **14**

Active Directory, defined **4**

authentication **2**

B

backup **17**

C

chapter overview **1**

Credentials **6**

credentials, defined **2**

D

deployment planning **12**

designated user **16**

DigitalPersona Pro Workstation for Workgroup **16**

DPWGSTool.exe **16**

G

group **2**

Group operations **24**

H

HP ProtectTools **16**

I

installation scenario **14**

L

License operations **27, 28**

local installation of Pro Workstation **11**

logon **2**

M

managed computer **2**

managed logon **2**

managed user **3**

O

One time access **3**

online help **4**

open ports **14**

P

Password Manager **3**

Password Manager Pro **3**

Planning & Deployment **12**

ports 800 and 443 **14**

privileged user operations **28**

Pro Workgroup client system requirements **11, 12**

Product Compatibility **10**

R

recommended skill set **4**

requisite knowledge **4**

S

setting up computers to be managed **16**

silent installation **16**

SQL Express database **18**

support **4**

 during evaluation **13**

 online help **4**

 Professional Services **13**

 readme file **4**

System **11**

system requirements **10, 11**

U

uninstallation **18**

User and Storage operations **25**

W

web console URL **15**