

# DigitalPersona<sup>®</sup> Pro Workgroup

Version 5.1

## Administrator Guide



digitalPersona.

© 2010-2011 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 7, Windows Vista and Windows XP are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

This document 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](mailto: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: 6/30/2011 (Software version 5.1.0)

# Table of Contents

- 1 Introduction ..... 6
  - Chapter Overview ..... 6
  - Glossary ..... 7
  - Recommended Skill Set ..... 9
  - Support Resources ..... 9
  
- 2 Solution Overview ..... 11
  - Product line ..... 11
    - Pro Workgroup server ..... 12
    - DigitalPersona Pro Workstation for Workgroup ..... 12
    - DigitalPersona Pro Workgroup Add-on ..... 13
    - Password Manager Pro ..... 13
    - Full Disk Encryption ..... 13
  - Feature overview ..... 14
    - Managing computers ..... 14
    - Managing users ..... 14
    - Configuration & deployment ..... 14
    - Security Model ..... 14
    - Licensing ..... 15
  - Product Compatibility ..... 16
  
- 3 Installation & Deployment ..... 18
  - System Requirements ..... 18
  - Planning ..... 19
  - Support ..... 20
  - Installation ..... 21
    - Server installation ..... 21
    - Creating a Setup file ..... 22
    - Internet access to Pro Workgroup ..... 23
    - Client Installation ..... 23
    - Deployment ..... 24
      - Setting up computers to be managed ..... 24

## Table of Contents

Creating & Deploying Managed Logons .....	25
Backup .....	26
Uninstallation .....	26
Optional installations .....	26
Drive Encryption .....	26
Privacy Manager Pro .....	27
Password Manager Pro .....	28
4 Administration & Licensing .....	29
Overview .....	29
Account administration .....	30
Licensing .....	32
Software license administration .....	32
Client Setup and Deployment .....	34
Client license activation .....	35
Activating licenses through a proxy .....	36
5 Managing computers and users .....	37
Managing groups .....	37
Configuring settings .....	38
Setting up client computers .....	39
Manage computers .....	40
Managing users .....	42
Manage applications .....	43
6 Policies and Settings .....	44
7 DigitalPersona Reporter .....	50
Overview .....	50
Event logs and channels .....	51
Setting up DigitalPersona Reporter .....	51
Available reports .....	53
Running Reports .....	55
8 Activity Events .....	56

## Table of Contents

Server Events .....	57
Workstation Events .....	62
Drive Encryption Events .....	68
Reporter events .....	69
9 Status Events .....	71
10 Utilities .....	74
DigitalPersona Workgroup Setup Tool .....	74
Disconnect Utility .....	75
11 Appendix .....	76
Troubleshooting Workgroup server installation .....	76
12 Index .....	77

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 you, the 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 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, *Administration & Licensing*, includes information on managing Pro Workgroup administrator accounts, licensing of Pro Workgroup Server and client components, and setting up client computers to be managed by Pro Workgroup.

Chapter 5, *Managing computers and users*, gives step-by-step procedures for managing Pro Workgroup groups, computers, users applications and settings.

Chapter 6, *Policies and Settings*, provides a complete description of all available policies and settings that can be applied to groups of managed computers.

Chapter 7, *DigitalPersona Reporter*, describes the built-in reporting capabilities of DigitalPersona Pro Workgroup.

Chapter 8, *Activity Events*, describes each event generated by Pro Workgroup, what data is reported and the levels of detail that are available.

Chapter 9, *Status Events*, describes optionally-generated events that can keep you informed of the status of various features and components of DigitalPersona Pro Workgroup.

Chapter 10, *Utilities*, describes various utilities included in the DigitalPersona Pro Workgroup solution.

## 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 44).

### **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://www.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.	12
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.	12
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.	13
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.	13
Full Disk Encryption	A plug-in that provides complete data protection by encrypting your computer hard drive.	13

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.
- **Central Management**- provides easy access to information about DigitalPersona Pro and centralized management of DigitalPersona Pro Workstation clients. This menu item may be hidden through a setting on the Computers and Users/General tab of 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 and manage FDE users. An optional feature to backup a unique encryption key to a USB connected storage drive for recovery in case of a forgotten password may be enabled by the administrator.

## 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 44.

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 Activity Events beginning on page 56.

## Licensing

### *Overview*

The DigitalPersona Pro Workgroup solution includes the following licensed features:

- Software 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 through a link in the Pro Workgroup web console that launches our ecommerce site.
- 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 about DigitalPersona Pro Workgroup licenses, see

<http://www.digitalpersona.com/enterprise/products/pro-workgroup>.

### *License Purchase, deployment and activation*

You may purchase and deploy additional client licenses or licenses for optional modules from the Administration tab in the DigitalPersona Pro Workgroup web console. A Customer Service Portal provides you with additional information about your licenses such as the number of activations remaining.

**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.

**Activations left** - Click this link to access the DigitalPersona Customer Service portal.

**Deploy** - Click **Deploy** 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 18 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, uninstalling and deploying DigitalPersona Workgroup and additional optional components. This includes the following topics.

<b>Topic</b>	<b>Page</b>
System Requirements	18
Installation	21
Planning	19
Support	20
Backup	26
Uninstallation	26
Optional installations	26

## 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 (managed client for HP ProtectTools 5.x only)

- 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://www.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 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.

- We strongly recommend installing the Pro Workgroup server on a clean, dedicated machine. If you must share the machine with an existing instance of IIS and additional web sites, see “Troubleshooting Workgroup server installation” on page 76.
- If you are planning on accessing the Pro Workgroup server from the internet, see the section immediately following this one, beginning on page 23.

*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 18.
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 file (Connection.msi), that can be used to transfer required connection information to a client computer. For further information on the Setup file, see the topic *Creating a Setup file* below.
  5. Once the installation is complete, you can use the generated setup file to connect compatible clients to the server.
  6. 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>.

## Creating a Setup file

The default Setup file (connection.msi) created during Pro Workgroup Server installation, and shown on the Administration/Deployment tab of the Pro Workgroup web console requires use of a Pro Workgroup administrator logon and password when it is run.

The setup file can also be created through the Pro Workgroup web console, by clicking **New** on the Administration/Deployment tab.

A command line utility for creating a setup file is also available in the DigitalPersona\ Workgroup Server\bin folder on the server after installation.

Creating a new Setup file provides the following options

- Designated user - Allows you to create credentials (name and password) for a designated user that can be used to run the resulting setup file.
- Silent - Allows creation of a setup file that does not require any credentials to run.

To create a setup file for managing Pro Workgroup through the internet, create the file through the web console. When prompted for the Server name, enter the Pro Workgroup Server's internet address.

## Internet access to Pro Workgroup

By default, the Pro Workgroup Server is not visible from the internet and cannot be accessed from the internet.

However, if the administrator wants the flexibility to manage Pro Workgroup Server and clients from the internet, they can do so. Here are general guidelines to follow for allowing internet access for Pro Workgroup.

- 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.

You cannot use the default Connection file (`connection.msi`) shown on the Web Console's Administration/Deployment tab to set up computers to be managed by Pro Workgroup. See the previous topic on *Creating a new Setup file*.

## 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. Installation is straightforward. Simply launch the `Setup.exe` included in the Pro Workgroup Workstation folder of the product package. Also 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 44.)

To stop managing a computer, use one of the following procedures.

- **Connection available** - If a connection is available to the Pro Workgroup Server that the computer is managed by, 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.
- **Connection unavailable** - If the computer is unable to connect to the Pro Workgroup Server, run the Disconnect Utility (DPWGDisconnect.exe) with the Unmanage parameter. The file is available in the Tools directory of the product package.

Example: `dpwgdisconnect /Unmanage`

This will place the computer in local management mode. However, the computer should then be manually deleted from the list of managed computers in the Pro Workgroup Server web console.

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 (page 13)

- 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 Server, 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.

## Optional installations

The following optional DigitalPersona Pro Workgroup components are *not* automatically installed as part of either the DigitalPersona Pro Workgroup Server or client installations.

They following components may be available depending on the DigitalPersona Pro solution being installed.

## Drive Encryption

You must have administrative rights to install this product on supported operating systems.

### System Requirements

- DigitalPersona Pro Workstation for Enterprise
- 120 MB hard disk space

- One of the following operating systems: Windows 7 (32/64 bit), Windows Vista (32/64 bit) or Windows XP (32 bit). Home editions of these operating systems are not supported.

To install Drive Encryption:

1. In the Drive Encryption product package, run **DPFVE.exe**.
2. Follow the onscreen instructions.

## Privacy Manager Pro

Privacy Manager Pro consists of two subcomponents: Privacy Manager (the end-user application), and the Privacy Manager AdminTool (which provides central manageability through DigitalPersona Pro Enterprise). Each is installed separately.

### Privacy Manager installation

You must have administrative rights to install this product on supported operating systems.

#### System Requirements

- One of the following operating systems: Windows 7 (32/64 bit), Windows Vista (32/64 bit) or Windows XP (32 bit). Home editions of these operating systems are not supported.
- 10 MB hard disk space (20MB during installation)
- Microsoft Outlook 2003, 2007 or 2010 and a valid email account

To install Privacy Manager:

1. In the Privacy Manager Pro product package, run **Setup.exe** (located in the Privacy Manager folder).
2. Follow the onscreen instructions.

### Privacy Manager AdminTool installation

You must have administrative rights to install this product on supported operating systems. The installation adds a Windows Administrative Template to Active Directory, and should be installed on the computer where administrative tasks will be performed.

#### System Requirements

- One of the following operating systems:
  - Windows Server 2003 (32/64 bit) or Windows 2008 (32/64 bit) and Active Directory
  - Windows 7 (32/64 bit) or Windows Vista (32/64 bit) or Windows XP (32 bit) with Remote Administration Tools and Active Directory access

To install the Privacy Manager AdminTool

- Launch the Setup.exe file located in the product package. For a silent mode installation, you can run `Setup.exe /s/v" /qn"` at the command line.

## Password Manager Pro

You must have administrative rights to install this product on supported operating systems.

### System Requirements

- One of the following operating systems: Windows 7 (32/64 bit), Windows Vista (32/64 bit) or Windows XP (32 bit). Home editions of these operating systems are not supported.
- One of the following DigitalPersona clients already installed:
  - DigitalPersona Pro Workgroup Add-On 5.00 for HP ProtectTools
  - DigitalPersona Pro Workstation for Workgroup 5.00
  - DigitalPersona Pro Enterprise Add-On 5.50 for HP ProtectTools
  - DigitalPersona Pro Workstation for Enterprise 5.00
- 10 MB hard disk space (20MB during installation)
- Internet Explorer (6/7/8) or Mozilla Firefox (3.5/3.6/4) Note that creation of (managed) logons within Password Manager Pro, to be deployed to users of the Password Manager application, requires Internet Explorer 6, 7 or 8. Personal (non-managed) logons may be created/modified and used by the end-user of the *Password Manager* application in either Internet Explorer (6/7/8) or Mozilla Firefox (3.5/3.6/4)

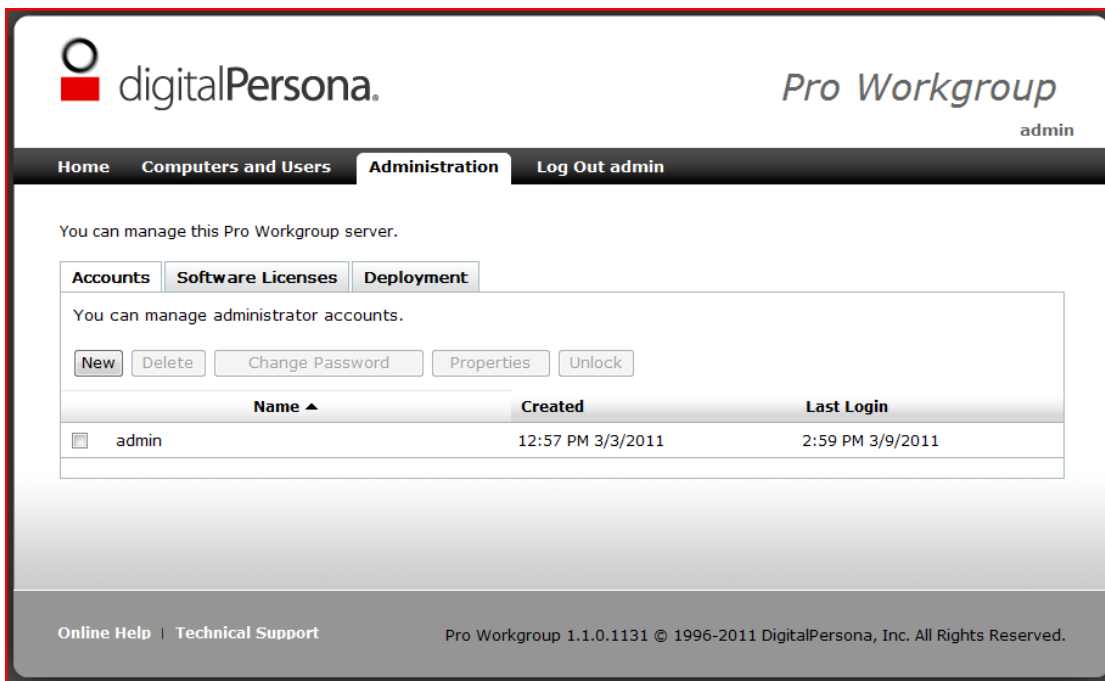
To install Password Manager Pro:

1. In the Password Manager Pro product package, run **Setup.exe**.
2. Follow the onscreen instructions.

## Overview

DigitalPersona Pro for Active Directory provides a full complement of tools and features for administering and managing various aspects of your deployment as well as expanding the functionality of the product. Note that the features and functionality of DigitalPersona Pro Workgroup as described in this Administrator Guide are available through licensing the Ultimate version of the product. Some features may not be present in other versions.

DigitalPersona Pro Workgroup provides administration capabilities on the Administration tab of the DigitalPersona Pro Workgroup web console.

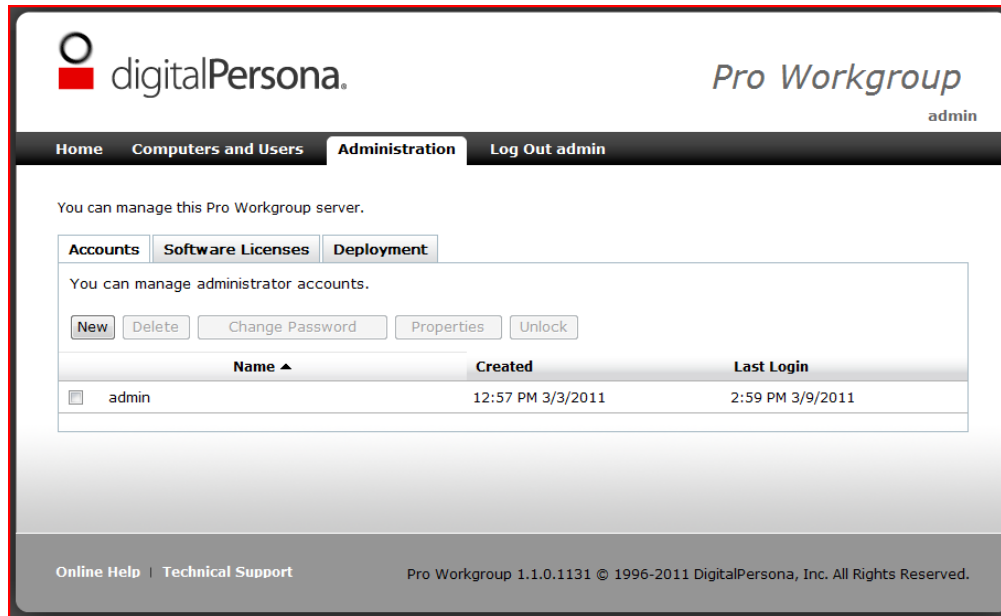


The Administration tab provides the following administrative features through its included subtabs.

Administrative feature	Click on this subtab	Page
Account administration	Accounts	30
Software license administration	Software licenses	32
Client Setup & Deployment	Deployment	34

## Account administration

Administration of the administrator accounts for the server is done on the Accounts subtab.



Account administration includes the following tasks.

To add an administrator

- 1 Click **New**.
- 2 Type the name of the new administrator and a password. Then confirm the password.
- 3 Type their email address (optional).

To delete an administrator

- 1 Select an administrator.
- 2 Click **Delete**.
- 3 Click **OK** to confirm.

To change administrator's password

- 1 Select an administrator.
- 2 Click **Change password**.

3 Enter and confirm a new password.

4 Click **OK**.

To unlock an administrator account

For security purposes, Pro Workgroup server will lockout an administrator account after 5 unsuccessful login attempts. The account must then be unlocked on the computer where Pro Workgroup server is installed.

1 On the Pro Workgroup server, open the Windows **Control Panel**.

2 In the left panel, expand the Select Administrative Tools, **Internet Information Services** node.

3 Expand the **Sites** folder, and select **DigitalPersona Workgroup Server**.

4 Double-click the **.NET Users** icon.

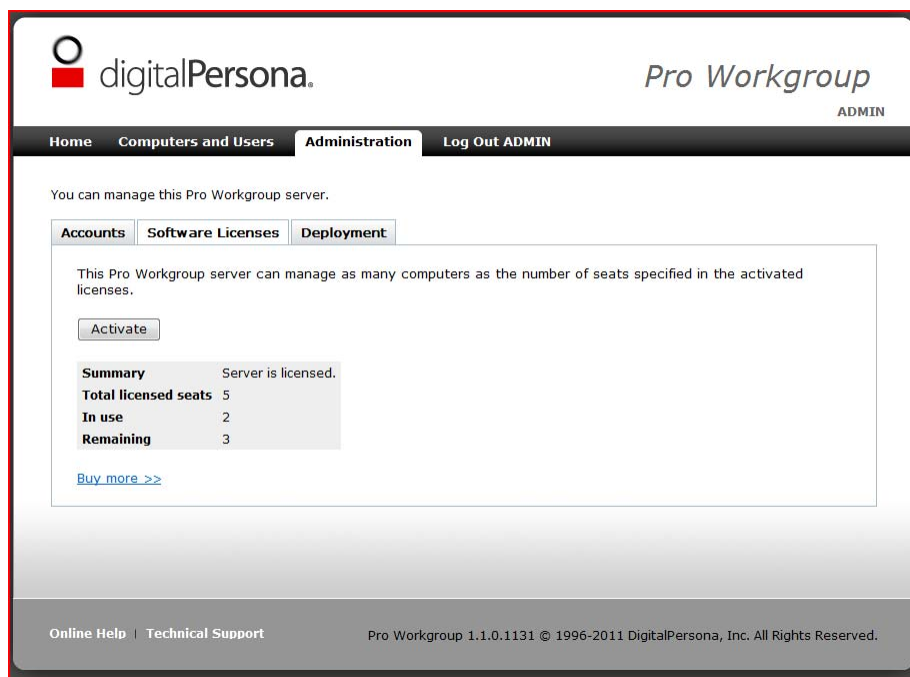
5 Right-click the name of the locked-out user and select **Unlock**.

## Licensing

Server (user), Security Application and feature licenses may be activated through the DigitalPersona Pro Workgroup web console. Security Application and feature licenses may also be activated on individual workstations through the DigitalPersona Activation Wizard, accessed through the dashboard About dialog.

### Software license administration

The Software Licences tab is used to monitor, purchase and activate your Pro Workgroup Server software licenses.



All DigitalPersona Pro Workgroup versions include a builtin five-seat Software license. Additional Software licenses may be purchased from the Administration/Software Licenses tab in the DigitalPersona Pro Workgroup web console, or directly from our website at

<http://www.digitalpersona.com/enterprise/products/pro-workgroup>.

To activate new Software licenses

- 1 In the Pro Workgroup Server web console, navigate to the Administration/Software Licenses tab.

## 2 Click **Activate**.

Follow the onscreen instructions to activate your Software license. Note that you may choose to activate your license online (requiring an internet connection), or from another computer with an internet connection.

Software license administration includes the following tasks.

To purchase additional licenses

### 1 Click **Buy more**.

### 2 Follow the onscreen instructions.

To activate a license

### 1 Click **Activate**.

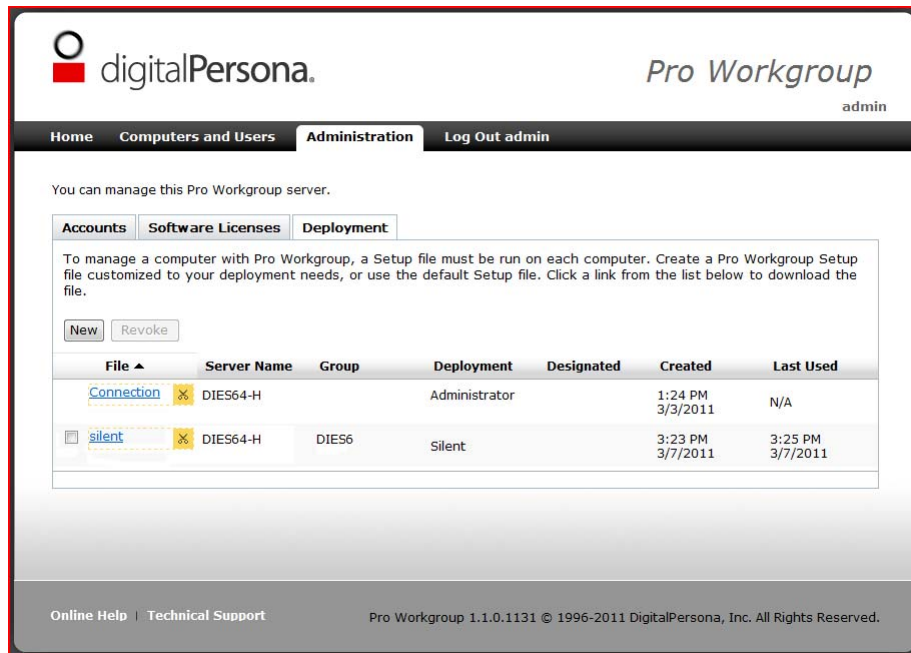
### 2 Follow the instructions provided on screen. Note that you may choose to activate your license online (requiring an internet connection), or from another computer with an internet connection.

The screenshot shows a dialog box titled "Activate software license". At the top, there is a progress bar with three steps, the first of which is highlighted in green and labeled "Step 1". Below the progress bar, the text reads "Activate the software license for this server" and "Choose how you would like to activate this license." There are three input fields: "License ID", "Password", and "Activation type". The "Activation type" dropdown menu is open, showing "Online" (selected) and "From a different computer". There are "Next" and "Cancel" buttons at the bottom right.

**Note:** Pro Workgroup server can manage as many computers as the number of seats specified in the activated licenses. You should check the licenses page occasionally to ensure that you are maintaining an adequate supply of product licenses.

## Client Setup and Deployment

The Deployment tab is used to create a Pro Workgroup Setup file that is used to deploy license and connection information to computers you wish to manage by Pro Workgroup. During the creation of the file, you can choose whether the file can only be deployed by a Pro Workgroup administrator, by a specifically designated user, or silently.



To manage a computer with Pro Workgroup, a Setup file must be run on each computer. Create a Pro Workgroup Setup file customized to your deployment needs, or use the default Setup file (Connection.msi).

To create a Pro Workgroup Setup file

- 1 Click **New**.
- 2 Follow the instructions provided on screen.

To download a Pro Workgroup Setup file

- Click a file name in the Setup file list.
- The URL for a setup file can also be copied to the Windows clipboard by clicking the Copy icon next to the file name. This URL may then be launched on the client computer to download and run the Setup file.

For additional information on Setup files, see “Setting up client computers” on page 39.

## Client license activation

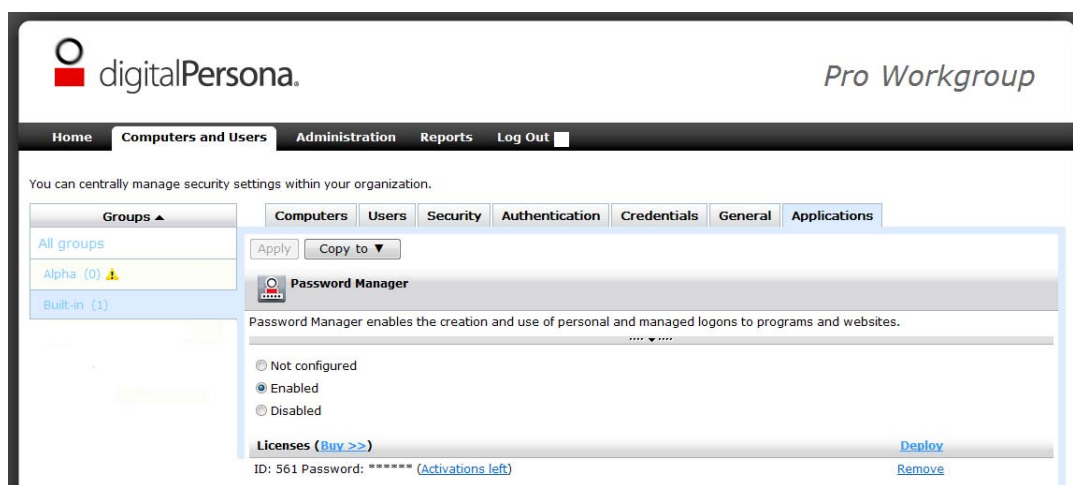
Your DigitalPersona Pro Workgroup licenses may be deployed through the Pro Workgroup web console. Client (and optional Pro Security Applications) licenses for individual workstations will be activated as the workstations access the Pro Workgroup Server.

Licenses may also be individually activated at the workstation if circumstances require it, using the DigitalPersona Activation Wizard. This wizard can be accessed from the About dialog on Pro 5.1 clients or from a dialog that is displayed whenever an unlicensed client or security application is accessed.

DigitalPersona Pro Security applications and features requiring licensing may vary depending on the version of Pro Workgroup that you have installed.

To deploy Pro Workgroup licenses

- 1 In the Pro Workgroup Server web console, click the **Computers and Users** tab and select a group.
- 2 Click the **Applications** subtab. Under the section for the application or feature that you want to license, click **Deploy**.



- 3 Enter the License ID and password that you received with your purchase.

Licenses may be applied multiple times to different groups as long as the total number of workstations does not exceed the number specified in the license.

You can monitor the number of activations available for a licensed component by clicking the *Activations Left* link.

### Activating licenses through a proxy

Application and feature licenses are activated automatically and transparently when a workstation connects to Pro Workgroup Server, but only if the workstation has an internet connection.

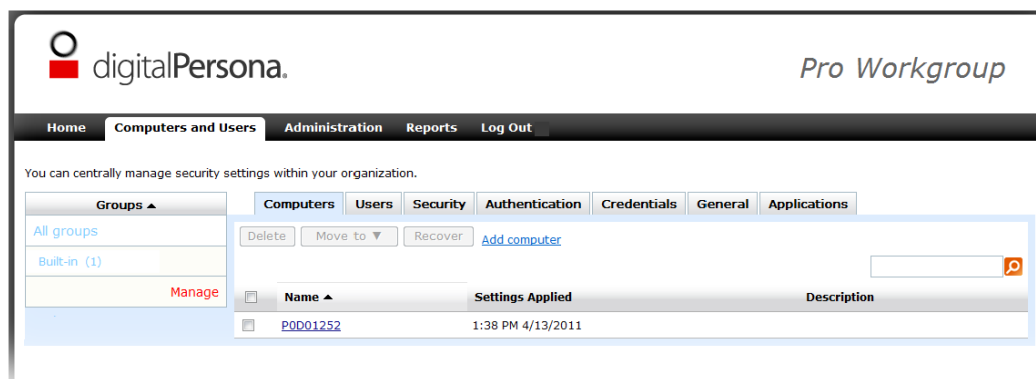
Workstations that do not have an internet connection may be activated locally by proxy, i.e. from another computer.

To activate a license by proxy

- 1 In the Pro Workstation for Workgroup dashboard, click **About**.
- 2 Right-click the application or feature that you want to activate and choose **Activate product now**.
- 3 Click **Next**, and on the following screen, select **I want to activate the software from another computer**.
- 4 The DigitalPersona Activation Wizard will guide you through the following steps:
  - Entering the License ID and password.
  - Saving the activation link to a file (leave the wizard open)
  - Opening the file on a different computer that has internet access
  - Entering the generated registration code in the wizard on the computer being licensed.

For further details on licensing including other licensed versions of the product which may be available, and licensing for specific features, contact your DigitalPersona Account Manager or Reseller.

Use the Computers and Users tab to manage groups, member computers and their users, and DigitalPersona Pro security applications.



Managed computers share identical settings specified on the Pro Workgroup server, and obtain those settings upon each restart or at an interval specified on the server.

This chapter contains the following topics.

Topic	Page
Managing groups	37
Configuring settings	38
Setting up client computers	39
Manage computers	40
Managing users	42
Manage applications	43

## Managing groups

In Pro Workgroup, groups are used to centrally configure computers. A built-in sample group is created during installation. You can modify and use this group or add your own. Each computer can only belong to one group.

To create a group

1. On the Computers and Users tab, click **Manage Group**. Then click **New**.

2. Type a group name and description. Then click **Create**.

#### Edit group details

1. On the Computers and Users tab, click **Manage Group**.
2. Select a group.
3. Type a group name and description. Then click **Create**.

#### Delete a group

1. On the Computers and Users tab, click **Manage Group**.
2. Select a group. Then click **Delete**.

#### Search for a computer or user, or filter the list of computers or users

1. On the Computers and Users tab, select a group or select **All Groups**.
2. Enter a search string in the search field and click the Search button. [insert image]

To administer the computers, users and settings for a group, click the group name in the Group panel on the left.

## Configuring settings

Settings are separately configured for each defined group of computers. All computers assigned to the group have identical settings, such as authentication policies, security features, etc.

Settings are configured through the various subtabs of the Computers and Users tab.

#### To configure settings

1. In the Group panel, select a group.
2. Click one of the settings tabs.
3. Configure settings as you want them applied to computers in this group. You can also click **Copy** to copy settings to another group.
4. Click **Apply**. Computers in the group will obtain these settings the next time they connect to Pro Workgroup server.

#### To copy settings from this group to another group

- Click **Copy To** and select the group that you want to copy these settings to.

## Setting up client computers

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

- DigitalPersona Pro Workstation for Workgroup - This client natively supports management by Pro Workgroup.
- HP ProtectTools Security Manager 5.x - This software, with the addition of the DigitalPersona Pro Workgroup Add-on, can be managed by Pro Workgroup. The add-on is included in the Pro Workgroup product package. Simply copy the add-on to the workstation, launch it and follow the instructions in the wizard.
- HP ProtectTools Security Manager 6.0 - This client requires an update, available as a download from the internet, in order to be managed by Pro Workgroup.

Additionally, each computer must be setup to connect with the Pro Workgroup 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.
- The URL for a setup file can also be copied to the Windows clipboard by clicking the Copy icon next to the file name. This URL may then be launched on the client computer to download and run the Setup file.

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 on the Settings tab.

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.

If the computer is unable to connect to the Pro Workgroup server that the computer is managed by, you can use the Disconnect Utility (DPWGDisconnect.exe) to disconnect the computer from being managed by the Pro Workgroup server. See “Disconnect Utility” on page 75.

To create a Pro Workgroup Setup file

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

You can also create a Pro Workgroup Setup file from the command line on the server. See “DigitalPersona Workgroup Setup Tool” on page 74.

To download a Pro Workgroup Setup file

- Click a file name in the Setup file list.

## Manage computers

Computers that are part of a group, can be managed from the Pro Workgroup web console, Computers and Users tab.

All computers to be managed must first be set up (see page 39), which includes adding each computer to a predefined group.

*To delete a computer from a group*

Note that this has the same effect as stopping a computer from being managed, accomplished from the local computer’s About dialog.

1. Select one or more computers. Click **Delete**.
2. Click **OK** to confirm.

*To move a computer to a different group*

1. Select one or more computers.
2. Click **Move**.
3. Select a different group from the dropdown menu.
4. Click **OK** to confirm.

*To recover a computer*

One of the advantages of managing computers with Pro Workgroup is the ability to easily recover access to a computer where a user has been locked out during pre-boot or drive encryption authentication.

*To recover from a pre-boot lockout*

1. The user contacts your helpdesk for assistance in recovering from a pre-boot lockout. A Pro Workgroup administrator assists them in recovering their user access.
2. The administrator locates their computer in a group, and clicks **Recover** to launch the Computer recovery wizard.
3. The administrator transmits the displayed Recovery account name and password to the user. This will enable them to authenticate at the pre-boot level. Upon use, this password is automatically changed.

**Note:** To display details about the computer, and a list of its users, click the computer name.

*To recover a backup key for a supported Drive Encryption application:*

1. From the Pro Workgroup web console, **Computers and Users tab**, select the desired computer.
2. On the **Computers** tab, click **Recover**.
3. In the **Recover computer** dialog, click **Download Recovery key**.

The procedure for use of the Drive Encryption Recovery (backup) key will vary depending on the specific Drive Encryption application as described in the application's Administrator Guide or help file.

## Managing users

When a computer starts being managed by Pro Workgroup, all of its users are added to Pro Workgroup. Any new Windows users created on the computer become managed users when the computer connects to Pro Workgroup immediately following their first authentication using Pro Workgroup client software. When a computer stops being managed, all its users are removed from Pro Workgroup.

Users are managed on the Computers and Users tab.

To recover a user

Easily recover access to a computer where a user is unable to access their account, and needs one time access to the pre-boot environment and their Windows account.

1. The user contacts your helpdesk and provides their Windows user account name. A Pro Workgroup administrator assists them in recovering their user access.
2. The administrator, on the Computers and Users tab, clicks the **User** subtab, selects the name of the user and clicks **Recover** which launches the **Recover access** wizard.
3. The administrator transmits the displayed Recovery account name and password to the user. This will enable them to authenticate at the pre-boot level. Upon use, this password is automatically changed.
4. The user enters the provided information, gaining access to the computer at the pre-boot level.
5. At the Windows logon screen, the user clicks their user tile. On their user tile screen, they click the **One time access** link.
6. The user transmits the displayed Security Key to the administrator.
7. The administrator clicks **Next**, enters the Security Code and clicks **Next** again.
8. Pro Workgroup displays a One time access code which is transmitted to the user.
9. The user types the One time access code and clicks **OK**, gaining access to their Windows account.

## Manage applications

Use the Applications tabs to purchase and manage Security Application licenses, including enabling and configuring application-specific settings.

To display the Applications tab

- Click Computers and Users, and select a group. Click the **Applications** tab.


To purchase application licenses

- On the Applications tab, click **Buy**.

To add a license

- On the Applications tab, click **Import**. Enter your license ID and password and click **OK**.

To enable, disable and configure applications

- Under the specific section for an application, select one of the following options: Not Configured, Enabled or Disabled. Configure any available settings for your environment.
- For an explanation of a setting, click the Help button next to the setting. 

Settings are also described in the DigitalPersona Pro Workgroup Administrator Guide, available on our website at <http://www.digitalpersona.com/products/material>.

To copy settings from this group to another group

- Click **Copy To** and select the group that you want to copy these settings to.

The following policies, settings and behaviors can be configured on the various subtabs of the **Computers and Users** tab within the Pro Workgroup web console. They can be configured (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).

Tab	Setting	Description
<b>Security</b>	Enable multi-credential authentication in Windows logon	<p>Configures whether or not the multi-factor authentication feature is enabled in Windows logon.</p> <p>If enabled, users are allowed to log on to Windows only if they are authenticated according to the multi-factor Logon Authentication Policy in effect.</p> <p>If disabled, the multi-factor Logon Authentication Policy in effect is not enforced, and the standard Windows logon is used.</p> <p>If not configured, multi-factor authentication is enabled on Pro Workstations and disabled on HP ProtectTools.</p>
	Drive Encryption	<p>If enabled, all hard drives on computers in the selected category will be encrypted.</p> <p>If disabled, encryption will not be available.</p> <p>If not configured, policy may be set by the computer's local administrator.</p>
	Enable multi-credential authentication in HP BIOS	<p>Configures whether or not multi-factor authentication is enabled at the BIOS level on specific models of HP computers. Refer to the HP documentation for a specific model for further information.</p> <p>If enabled, users are authenticated at the BIOS using the Logon Authentication policy in effect.</p> <p>If disabled, or not configured, the standard Windows logon is used, and the Logon Authentication policy in effect is not used for authentication at the BIOS.</p>
<b>Authentication</b>	Logon Authentication Policy	<p>Configure the credentials needed to access the computer, decrypt the hard drive, and log on to Windows.</p> <p>If enabled, only the specified authentication devices, in the specified combination, can be used for authentication.</p> <p>If disabled or not configured, any of the installed authentication devices can be used for authentication.</p>

Tab	Setting	Description
	Session Authentication Policy	<p>Configure the credentials needed to access Pro security applications during the Windows session.</p> <p>If enabled, only the specified combination of credentials in the Policy can be used for authentication.</p> <p>If disabled, the user is not prompted to authenticate by the Pro or Hewlett-Packard ProtectTools security applications during the Windows session. This configuration provides Single Sign-on functionality. The user logs on to Windows, and gains access to all security applications without being prompted to authenticate for each application.</p> <p>If not configured, any of the installed authentication devices can be used for authentication.</p>
	Enable One Step Logon	<p>One Step Logon simplifies the logon process when multi-factor authentication is enabled at both pre-boot and Windows logon.</p> <p>If enabled or not configured, authentication is required at pre-boot only, and users are automatically logged on to Windows.</p> <p>If disabled, authentication may be required multiple times.</p>
<b>Credentials</b>	SpareKey	<p>SpareKey is a recovery feature that allows users to gain access to the computer in the event that they are unable to authenticate with the required credentials.</p> <p>If enabled, users will be able to use SpareKey to log on. Once enabled, administrators can choose the options available to the user when setting up their SpareKey; such as predefined questions, custom questions or user specified passphrases.</p> <p>If disabled or not configured, users will not be able to use their SpareKey to log on.</p>

Tab	Setting	Description
	Fingerprint enrollment	<p>Configure settings related to fingerprint enrollment.</p> <p>Minimum number of enrolled fingerprints - Select the minimum number of fingerprints that must be enrolled during the fingerprint enrollment process when it is required.</p> <p>Maximum number of fingerprints - 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>
	Fingerprint verification	<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>
	Lock the computer on smart card removal	<p>Configure locking behavior of the computer upon smart card removal.</p> <p>If enabled, the computer locks upon removing the smart card from the smart card reader. The computer will lock only if the smart card was used to log on to Windows.</p> <p>If disabled or not configured, the computer does not lock upon removing the smart card from the smart card reader.</p>
<b>General</b>	Set interval for refreshing settings	<p>Configure the settings refresh interval for clients.</p> <p>If enabled, you can specify the interval at which client computers obtain settings from the Pro Workgroup Server.</p> <p>If disabled or not configured, the default interval of 1 hour is used.</p>

Tab	Setting	Description
	Local administration	<p>Configure permissions for running the Administrative Console and the Setup wizard.</p> <p>If enabled, specifies whether or not local administrators are allowed to run these administrative tools, and whether they need to authenticate as a Pro Workgroup administrator to do so.</p> <p>If disabled or not configured, local administrators are allowed to run these tools after authentication as a Pro Workgroup administrator.</p>
	DigitalPersona Reporter Event Forwarding	<p>Configures forwarding of Pro Workstation events to DigitalPersona Reporter via Windows Event Forwarding.</p> <p>If enabled, Pro events are forwarded.</p> <p>If disabled, or not configured, Pro events are not forwarded.</p>
	Level of detail in event logs	<p>Determines whether DigitalPersona Pro logs events, such as fingerprint registration and authentication attempts, in the Windows Event Log.</p> <p>If enabled, DigitalPersona Pro logs events on the specified level.</p> <p>If disabled or not configured, events are logged at the Auditing level and status events are not logged.</p> <p>There are four levels of event logging: Errors, Auditing, Details and Fine Details. Each higher level includes all previous levels. Normally, the Auditing level provides sufficient detail, covering all logon, authentication, fingerprint management, and user management events, etc. Higher levels can fill the log file very quickly.</p> <p>Status events provide information about the state of several important systems on the computer. They are logged on configurable intervals and generally used when events are remotely collected.</p> <p>Events are logged on the computer where they occur.</p>
	Allow running auto updates on the computer	<p>If enabled or not configured, automatic updates for DigitalPersona products are allowed on client computers.</p> <p>If disabled, automatic updates for DigitalPersona products are not allowed on client computers.</p>

Tab	Setting	Description
	Enable the Central Management menu item	If enabled or not configured, the Central Management menu item is shown in the user dashboard.
	Do not launch the Getting Started wizard upon logon	If enabled, the DigitalPersona Pro dashboard and the Getting Started page do not start automatically after user logon.  If disabled or not configured, the DigitalPersona Pro dashboard and the Getting Started page start automatically after user logon.
<b>Applications</b>	Password Manager	<p>If this setting is enabled or not configured, Password Manager supports both personal and managed logons. You may then configure the following behaviors.</p> <p><i>Allow creation of personal logons</i> - Allows users to create personal logons for websites and programs.</p> <p><i>Allow users to view managed logon passwords</i> - If enabled or not configured, users are allowed to view their managed logon passwords after verifying their identity. If disabled, users are not allowed to view managed logon passwords.</p> <p><i>Allow users to edit account data</i> - If enabled or not configured, users can edit their account data. If disabled, users cannot edit their account data.</p> <p><i>Allow users to add account data</i> - If enabled or not configured, users can add to their account data. If disabled, users cannot add to their account data.</p> <p><i>Allow users to delete account data</i> - If enabled or not configured, users can delete their account data. If disabled, users cannot delete account data.</p> <p>If this setting is disabled, Password Manager is removed from the client dashboard.</p>

Tab	Setting	Description
	Privacy Manager Suite	<p>Privacy Manager provides centrally-managed encryption capabilities for Microsoft Office documents.</p> <p>If this setting is enabled or not configured, Privacy Manager encryption is allowed. You may then configure the following behaviors.</p> <p><i>Allow use of third-party certificates</i> - If disabled, any certificate having signature, encryption and email protection capabilities is allowed. If disabled or not configured, only special Comodo-issued certificates can be used and only those certificates are displayed in the Certificate Manager and Trusted Contacts Manager.</p> <p><i>Disable encryption in Microsoft Office</i> - If enabled, users are prevented from using Privacy Manager encryption capabilities in Microsoft Office. If disabled or not configured, Privacy Manager encryption capabilities are available.</p> <p><i>Disable encryption in Microsoft Outlook</i> - If enabled, users are prevented from using Privacy Manager encryption capabilities in Microsoft Outlook. If disabled or not configured, Privacy Manager encryption capabilities are available.</p> <p>If this setting is disabled, Privacy Manager encryption is not allowed.</p>

DigitalPersona Reporter is a separately installed event collection, analysis and reporting component for DigitalPersona Pro Enterprise and DigitalPersona Pro Workgroup. Although the basic functionality is the same in both products, there are slight differences in architecture and setup. This chapter describes the DigitalPersona Pro Workgroup version.

## Overview

The capability to forward activity and status events generated by DigitalPersona Pro clients to a designated *Collector* computer via the Windows Event Forwarding mechanism is built into DigitalPersona Pro and HP ProtectTools 5.1 and later clients.

Forwarded events can be viewed in the Windows Event Viewer *Forwarded Events* log on the Collector computer, where they can be parsed, analyzed and reported on through DigitalPersona Reporter or various 3rd-party tools.

DigitalPersona Reporter also automatically transfers these events to a SQL database, where they can be used to generate customized reports. The transfer can be disabled, if necessary, by removing the ReportEventImport task in the Windows Task Scheduler on the Collector computer.

All DigitalPersona Pro client *activity* events are automatically logged into the local Windows Event Viewer Event Log with a root name of “DigitalPersona.” Each DigitalPersona Pro application and subsystem has its own sub-log.

*Activity* events are logged whenever a designated activity occurs on the client. For a complete listing and description of all activity events, see chapter 8 beginning on page 50.

*Status* events, by default, are not written to the local Windows Event log, but must be separately enabled. This is accomplished by selecting the *Log Status Events* checkbox of the *Level of detail in event logs* setting on the *General* subtab of the *Computers and Users* tab in the web console. Status events (see page 71) provide information about the state of various policies and components on client computers. The interval at which status events are reported can also be configured.

## Event logs and channels

The names of the event logs created on the client computer will be slightly different depending on the Windows version and the DigitalPersona component.

- On Windows XP, all events are written into the Windows Event Log with the name “DigitalPersona Pro” or “HP ProtectTools” depending on the installed client.
- On Windows Vista and later, events are logged into separate channels in the Microsoft Windows Event Log. Company and Product are defined for all products as follows:

DP products: “DigitalPersona\Pro”

HP products: “HP\HP ProtectTools”

The Component part of the channel name is the actual component that logs the events. Currently, the following Component names are defined:

- “Core” (for DigitalPersona components) or “Security Manager” (for supported HP client) – general log for all events not reported under another specific channel
- “Logon” – user logon/logoff and lock/unlock events
- “Password Manager” – Managed logon events
- “Drive Encryption” - Drive Encryption events
- “Privacy Manager” - Reserved for future use. No events are currently logged under this channel.

Future components may provide their own channel names, creating a separate Component log under “DigitalPersona-Pro” or “HP-HP ProtectTools” respectively.

Currently, all the events are written into the “Operational” log under the Component folder

Event logging occurs on the client workstation. If the “DigitalPersona Reporter Event Forwarding” setting (on the Computers and Users \General tab of the Pro Workgroup server web console) has been enabled, then events are also forwarded to the “Forwarded Events Log” folder on the computer where the DigitalPersona Pro Workgroup server resides. They will be located in the Event Viewer\Windows Log\Forwarded Events folder.

## Setting up DigitalPersona Reporter

Setting up DigitalPersona Reporter includes the following tasks:

- 1 Verifying the license status of Pro Workgroup Server and clients.
- 2 Configuring Reporter settings for event forwarding in the DigitalPersona Pro Workgroup web console
- 3 Installing and configuring DigitalPersona Reporter on the Pro Workgroup server.

## Verifying license status

DigitalPersona Pro Workgroup events will only be forwarded from licensed clients. Client licenses can be verified on the Computers and Users tab of the web console.

## Configuring Reporter settings

Configure the following Pro Workgroup settings for any specified group of clients from which events will be forwarded.

- 1 Enable the “DigitalPersona Reporter Event Forwarding” setting, located on the Computers and Users/ General tab of the DigitalPersona Pro Workgroup web console.
- 2 Enable and configure the “Level of detail in event logs” setting, located on the Computers and Users/ General tab of the DigitalPersona Pro Workgroup web console. Optionally, check the “Log status events” checkbox and adjust the interval at which status events are collected.
- 3 Click OK to close the dialog.

## Installing DigitalPersona Reporter

**NOTE:** Reporter requires that Digitalpersona Pro Workgroup server 1.1 or above has been previously installed. Reporter is **not** compatible with Pro Workgroup server 1.0.

*If a DigitalPersona client is also installed on the same computer as Digitalpersona Reporter, events from this client cannot be included in the Windows Forwarded Events Log or in any reports produced by DigitalPersona Reporter.*

DigitalPersona Reporter may be installed on any domain member except the domain controller. Supported operating systems are:

- Windows Server 2008 Enterprise Edition (32/64-bit)
- Windows Server 2008 R2 Standard Edition (64-bit)
- Windows Server 2008 Standard Edition SP2 (32/64-bit)
- Windows 7 Professional (32/64-bit)

The installation file for DigitalPersona Reporter is located in the root directory of the DigitalPersona Reporter product package.

- 1 Start the installation wizard by launching **setup.exe**.
- 2 Follow the onscreen instructions. The following steps will be performed.
  - Creation of Reporter tables in the DigitalPersona Pro Workgroup instance of SQL Server 2008 R2 RTM Express
  - Installation and configuration of Crystal Reports Basic Runtime 2008
  - Installation of DigitalPersona Pro queries

- Addition of a Windows Task Scheduler job (ReporterEventImport)
  - Configuration, in the Windows Event Viewer, of a subscription to the DigitalPersona Reporter Collector, and configuration of the Forwarded Events log for the source computers
- 3 After the installation wizard is finished, you may want to manually run the ReporterEventImport task mentioned above in order to begin populating the Reporter database. By default, the task is scheduled to run once daily at midnight.

## Available reports

DigitalPersona Reporter provides the following built-in reports .

Report	Description
Disk Encryption Status	The Disk Encryption Status report tells you which computers have their hard drives protected with full disk encryption.
Windows/Domain Security Policy Status	The Operating System Security Policy Status report lists users logging on to their Windows and/or Domain account by using DigitalPersona Pro.
Logon Authentication Policy Status	The Logon Authentication Policy Status report specifies which authentication policy users are required to fulfill when logging on to their computers.
Session Authentication Policy Status	The Session Authentication Policy Status report specifies which authentication policy users are required to fulfill when logging on to managed applications, including applications set up for Password Management/Single Sign-On.
IT-assisted Access Recovery	The IT-assisted Access Recovery activity report shows whether users have recovered access to the computer via IT-assisted recovery leveraging one-time passwords. IT-assisted Access Recovery events include both recovery at the computer level (i.e. BIOS and/or Disk Encryption) and at the operating system level (i.e. Windows and/or Domain).
Self-service Access Recovery	The Self-service Access Recovery activity report shows whether users recovered access to a computer using the Sparekey functionality.
Credential Enrollment	The Credential Enrollment activity report specifies which authentication credentials users enrolled, such as Windows passwords, fingerprints, smart cards or other supported authentication methods.
Computer Logon	The Computer Logon activity report shows which users logged on to managed computers, including the credentials they used for authentication.

<b>Report</b>	<b>Description</b>
Password Manager Logon	The Password Manager Logon activity report shows which users logged on to applications managed with Password Manager, including the credentials they used for authentication (e.g. two-factor authentication, Single Sign-On).
Password Manager Account Setup	The Password Manager Account Setup activity report shows which users registered their logon credentials for applications managed with Password Manager, so that they can subsequently access those applications using the Session Authentication Policy applicable to them.
Password Manager Credentials Change	The Password Manager Credentials Change activity report shows which users changed their credentials, such as username and password, to access applications managed with Password Manager.
License Status	The License Status report shows whether or not licenses for managed applications are active.
License Activation	The License Activation activity report lists all successful and unsuccessful attempts to activate licenses for managed applications.
Last Server Connection	The Last Server Connection reports shows the last time managed computers checked with the server for policy updates.
All Pro Workgroup Server events	View all DigitalPersona Pro status and activity events collected from the Workgroup Server.
Computer Management	The Computer Management activity reports shows which computers were added to the pool of managed computers, and whether the operation was successful.

## Running Reports

DigitalPersona Pro Workgroup reports are run from the Reporter tab of the Pro Workgroup web console.

The screenshot shows the DigitalPersona Pro Workgroup Reporter web console. The interface includes a navigation menu with options like Home, Computers and Users, Administration, Reports (selected), and Log Out admin. Below the navigation, there is an introductory text explaining the purpose of the reports. A table lists various reports with their names and descriptions.

Name	Description
<a href="#">Disk Encryption Status</a>	The Disk Encryption Status report tells you which computers have their hard drives protected with full disk encryption.
<a href="#">Windows/Domain Security Policy Status</a>	The Operating System Security Policy Status report lists users logging on to their Windows and/or Domain account by using DigitalPersona Pro.
<a href="#">Logon Authentication Policy Status</a>	The Logon Authentication Policy Status report specifies which authentication policy users are required to fulfill when logging on to their computers.
<a href="#">Session Authentication Policy Status</a>	The Session Authentication Policy Status report specifies which authentication policy users are required to fulfill when logging on to managed applications, including applications set up for Password Management/Single Sign-On.
<a href="#">IT-assisted Access Recovery</a>	The IT-assisted Access Recovery activity report shows whether users have recovered access to the computer via IT-assisted recovery leveraging one-time passwords. IT-assisted Access Recovery events include both recovery at the computer level (i.e. BIOS and/or Disk Encryption) and at the operating system level (i.e. Windows and/or Domain).
<a href="#">Self-service Access Recovery</a>	The Self-service Access Recovery activity report shows whether users recovered access to a computer using the Sparekey functionality.
<a href="#">Credential Enrollment</a>	The Credential Enrollment activity report specifies which authentication credentials users enrolled, such as Windows passwords, fingerprints, smart cards or other supported authentication methods.
<a href="#">Computer Logon</a>	The Computer Logon activity report shows which users logged on to managed computers, including the credentials they used for authentication.
<a href="#">Password Manager Logon</a>	The Password Manager Logon activity report shows which users logged on to applications managed with Password Manager, including the credentials they used for authentication (e.g. two-factor authentication, Single Sign-On).
<a href="#">Password Manager Account Setup</a>	The Password Manager Account Setup activity report shows which users registered their logon credentials for applications managed with Password Manager, so that they can subsequently access those applications using the Session Authentication Policy applicable to them.
<a href="#">Password Manager Credentials Change</a>	The Password Manager Credentials Change activity report shows which users changed their credentials, such as username and password, to access applications managed with Password Manager.
<a href="#">License Status</a>	The License Status report shows whether or not licenses for managed applications are active.
<a href="#">License Activation</a>	The License Activation activity report lists all successful and unsuccessful attempts to activate licenses for managed applications.
<a href="#">Last Server Connection</a>	The Last Server Connection reports shows the last time managed computers checked with the server for policy updates.
<a href="#">All Pro Workgroup Server events</a>	View all DigitalPersona Pro status and activity events collected from the Workgroup Server
<a href="#">Computer Management</a>	The Computer Management activity report shows requests to start or stop managing computers and whether the operations were successful.

At the bottom of the interface, there are links for Online Help and Technical Support, and a copyright notice: Pro Workgroup 1.1.0.1300 © 1996-2011 DigitalPersona, Inc. All Rights Reserved.

To run a report, click the report name. In the Filtering Options pop-up window, select any desired criteria to specify the focus of the report.

Reports may be exported to one of several formats by clicking the Export button in the upper left corner of the report. Supported formats include PDF, Word, Excel, RTF and others.

DigitalPersona Pro Workgroup writes the following events to an SQL database where they can be analyzed through a built-in Reporter feature (See “DigitalPersona Reporter” on page 50). Third party tools such as Crystal Reports can also be used to view and report on the records in the database.

Activity events are classified into the following categories and subcategories.

Component	Description	Page
Server*	Session operations	57
	Workstation operations	57
	Group operations	58
	User and user storage operations	59
	License operations	60
	Privileged user operations	60
	Installation package operations	61
Workstation	Credential Management	62
	User Management	62
	Secret Management	63
	Systems, Services, Settings and User Sessions	64
	External components	65
	Password Manager	65
	Fingerprint match	65
	License Management	66
	OTP Management	66
	Logon events	67
Workstation for Workgroup operations	67	
Reporter	Reporter operations	68

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

\* Note that Pro Workgroup Server events are generated by Pro Workgroup Server itself and stored in the server's internal event logging database. These events reflect activity on the Workgroup Server. If the Pro Workgroup Server is uninstalled, the Server event logging database will be deleted, and all the stored server events will be removed.

## Server Events

### *Session operations*

These events are generated during session operations.

ID	Event	Level	
		Srvr	Wks
257	Session opened.	-	Dt
258	Session closed.	-	Dt

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

### *Workstation operations*

The following events are generated during workstation operations.

ID	Event	Level	
		Srvr	Wks
513	Workstation added to managed pool.	-	A
514	Workstation added to managed pool failed.	-	E
515	Workstation removed from managed pool.	-	A
516	Workstation removal from managed pool failed.	-	E
517	Workstation modified.	-	A
518	Workstation modification failed.	-	E
519	Workstation recovered.	-	A
520	Workstation recovery failed.	-	E
521	Workstation assigned to group.	-	A
522	Workstation assignment to group failed.	-	E

ID	Event	Level	
		Srvr ----	Wks
523	Workstation settings retrieved.	-	A
524	Workstation settings retrieval failed.	-	E
525	Workstations enumerated.	-	Fd
526	Workstation enumeration failed.	-	E

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

### **Group operations**

The following events are generated during group operations.

ID	Event	Level	
		Srvr ----	Wks
769	Group created.	-	A
770	Group creation failed.	-	E
771	Group deleted.	-	A
772	Group deletion failed.	-	E
773	Group modified.	-	A
774	Group modification failed.	-	E
775	Groups enumerated.	-	A
776	Group enumeration failed.	-	E
777	Group settings modified.	-	A
778	Group settings modification failed.	-	E
779	Group settings retrieved.	-	A
780	Group settings retrieval failed.	-	E

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

***User and Storage operations***

The following events are generated during User and Storage operations.

ID	Event	Level	
		Srvr	Wks
1025	User created.	-	A
1026	User creation failed.	-	E
1027	User deleted.	-	A
1028	User deletion failed.	-	E
1029	User modified.	-	A
1030	User modification failed.	-	E
1031	Users enumerated.	-	Fd
1032	User enumeration failed.	-	E
1033	User storage created.	-	A
1034	User storage creation failed.	-	E
1035	User storage deleted.	-	A
1036	User storage deletion failed.	-	E
1037	User storage modified.	-	A
1038	User storage modification failed.	-	E
1039	User storage enumerated.	-	Fd
1040	User storage enumeration failed.	-	E

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**License operations**

The following events are generated during license operations.

ID	Event	Level	
		Srvr	Wks
1281	License activated.	-	A
1282	License activation failed.	-	E
1283	License transferred in.	-	A
1284	License transfer in failed.	-	E
1285	License transferred out.	-	A
1286	License transfer out failed.	-	E

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**Privileged user operations**

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

ID	Event	Level	
		Srvr	Wks
1537	Privileged user created.	-	A
1538	Privileged user creation failed.	-	E
1539	Privileged user deleted.	-	A
1540	Privileged user deletion failed.	-	E
1541	Privileged user modified.	-	A
1542	Privileged user modification failed.	-	E
1543	Privileged user's password changed.	-	A
1544	Privileged user's password change failed.	-	E
1545	Privileged user unlocked.	-	A
1546	Privileged user unlock failed.	-	E

ID	Event	Level	
		Srvr ----	Wks
1547	Privileged users enumerated.	-	Fd
1548	Privileged user enumeration failed.	-	E

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

### ***Installation package operations***

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

ID	Event	Level	
		Srvr ----	Wks
1793	Interactive installation package could not be created.	-	E
1794	Interactive installation package has been created.	-	A
1795	Delegated installation package could not be created.	-	E
1796	Delegated installation package has been created.	-	A
1797	Silent installation package could not be created.	-	E
1798	Silent installation package has been created.	-	A

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

## Workstation Events

### *Credential Management*

These events may be generated during credentials management.

ID	Event	Level	
		Srvr	Wks
257	Authentication failure.	-	A
258	Authenticated successfully.	-	Dt
259	Failed to enroll credential.	-	A
260	Credential enrolled.	-	A
261	Failed to unenroll credential.	-	A
262	Credential unenrolled.	-	A
263	Payload recovery has failed.	-	E
264	Failed to set payload recovery.	-	Fd
265	Payload recovery set.	-	Fd
266	Payload recovered successfully.	-	Fd

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

### *User Management*

These events may be generated during user management.

ID	Event	Level	
		Srvr	Wks
513	Failed to add user to authentication domain.	-	A
514	User added to authentication domain.	-	Dt
515	Failed to remove user from authentication domain.	-	A
516	User removed from authentication domain.	-	Dt
517	Failed to set user credentials.	-	A

ID	Event	Level	
		Srvr	Wks
518	User credentials set.	-	Dt
519	Failed to set user policy.	-	A
520	User policy set.	-	Dt
521	Failed to update user information.	-	A
522	User information updated.	-	Dt
523	Failed to identify user.	-	A
524	User identified.	-	Dt
525	Failure of user credential consistency check.	-	E
526	Failure of user credential signature check.	-	E
529	User account was unlocked.	Dt	-
531	Pro User added to the database.	A	-
532	Cannot add Pro User to the database.	E	-
533	Pro User deleted from the database.	A	-
534	Cannot delete Pro User from the database.	E	-

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

### ***Secret Management***

These events may be generated during secret management.

ID	Event	Level	
		Srvr	Wks
769	Failure of %1 secure application data consistency check.	E	E
770	Failed to delete secure application data.	E	E
771	Secure application data deleted.	A	A
772	Failure to release secure application data.	E	E
773	Secure application data released.	A	A

ID	Event	Level	
		Srvr ----	Wks
774	Failure of secure application data signature check.	E	E
775	Failed to store secure application data.	E	E
776	Secure application data stored.	A	A
777	Failure to release secure application data.	E	-
778	Secure application data released.	A	-

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

### ***Systems, Services, Settings and User Sessions***

These events may be generated during the management of system operations.

ID	Event	Level	
		Srvr ----	Wks
1025	Failed to activate authentication domain.	-	A
1026	Authentication domain activated.	-	A
1027	Failed to deactivate authentication domain.	-	A
1028	Authentication domain deactivated.	-	A
1029	Failed to start BAS.	E	E
1030	BAS started.	A	A
1031	BAS stopped.	A	A
1032	Failed to reset BAS configuration parameter.	A	A
1033	BAS configuration parameter reset.	A	A
1034	Failed to update BAS configuration parameter.	A	A
1035	BAS configuration parameter updated.	A	A
1036	Fingerprint reader connected (%1 reader(s) available.)	-	Fd
1037	Fingerprint reader disconnected. (%1 reader(s) remaining.)	-	Fd

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**External components**

These events may be generated during the management of external components.

ID	Event	Level	
		Srvr	Wks
1285	Failed to change user password.	-	E
1286	User password changed.	-	A
1289	Workstation has been unregistered.	-	A

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**Password Manager**

These events may be generated during the Password Manager operations.

ID	Event	Level	
		Srvr	Wks
1544	Initial Fillin was performed.	-	Dt
1545	Fillin was performed.	-	A
1546	Account data could not be modified	-	E
1547	Account data was successfully modified.	-	A

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**Fingerprint match**

These events may be generated during the fingerprint matching operations.

Event	ID	Level	
		Srvr	Wks
One-to-one fingerprint match failed	2049	A	-
One-to-many fingerprint match failed	2050	A	-
Account is locked for fingerprint verification.	2051	A	-

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**License Management**

These events may be generated during license management operations.

ID	Event	Level	
		Srvr ----	Wks
4097	The service is licensed for a %1 number of users. (No more users can be registered at this time because the license quota has been exceeded.)	A	-
4098	The service is licensed for a %1 number of users. (%2 users already registered.%n License quota is nearly exceeded.)	A	-
4099	License is not valid.	-	E
4100	License activated.	-	A
4101	License activation failed.	-	E
4102	License deactivated.	-	A
4103	License deactivation failed.	-	A
4104	License activation status.	-	A

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**OTP Management**

These events may be generated during One Time Password operations.

ID	Event	Level	
		Srvr ----	Wks
4353	One Time Password is provisioned	-	A
4354	Failed to provision the One Time Password	-	E
4355	One Time Password is generated	-	A
4356	Failed to generate the One Time Password	-	E
4357	One Time Password is deleted	-	A
4358	Failed to delete the One Time Password	-	E

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**Logon events**

These events may be generated during Logon operations.

ID	Event	Level	
		Srvr ----	Wks
4865	Credentials verified for log on	-	A
4866	Credentials verified for unlock	-	A
4869	Computer unlocked	-	A
4870	User logged off	-	A

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

**Workstation for Workgroup operations**

These events are generated on the local workstation during workstation operations.

ID	Event	Level	
		Srvr ----	Wks
1287	Workstation has been registered in the workgroup.	-	A
1288	Failed to register workstation in the workgroup.	-	E
1289	Workstation has been unregistered.	-	A
1290	Failed to unregister workstation.	-	E
1291	Workstation failed to connect to the workgroup server.	-	A
1292	Workgroup Administrator is logged on.	-	A
1295	Workstation settings have been synchronized.	-	A
1296	Workstation failed to synchronize settings.	-	E

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

## Drive Encryption Events

Task Category: 5146

These events may be generated during Drive Encryption operations.

Event	ID	Level	
		Srvr	Wks
Centrally managed settings cannot be applied	5147	-	Dt
Drive encryption will attempt to stop according to centrally managed settings	5148	-	Dt
Drive encryption will attempt to start according to centrally managed settings	5149	-	Dt
Drive encryption is up-to-date with centrally managed settings	5150	-	Dt
Drive encryption Scheduler task is about to be removed	5151	-	Dt
Drive encryption Scheduler task is set up.	5152	-	Dt
Drive encryption task failed to set up.	5153	-	Dt
Drive encryption Scheduler task will attempt to run in 1 minute.	5154	-	Dt
Drive encryption Scheduler task will attempt to run now.	5155	-	Dt
Drive encryption Scheduler task has started.	5156	-	Dt
Drive encryption Scheduler task has completed.	5157	-	Dt
Drive encryption Scheduler task is going to reboot or shutdown computer.	5158	-	Dt
Drive encryption Scheduler task notified user to reboot or shutdown computer.	5159	-	Dt
Drive encryption Scheduler authentication domain is not installed.	5160	-	Dt
Drive encryption Scheduler license is not activated.	5161	-	Dt
Delayed activation Scheduler task has started.	5162	-	Dt
Delayed activation Scheduler task has completed.	5163	-	Dt
Delayed activation Scheduler task is set up.	5164	-	Dt
Delayed activation Scheduler task failed to set up.	5165	-	Dt

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

## Reporter events

These events are generated on the Collector computer during DigitalPersona Reporter operations.

---

ID	Event
5377	Event Collector for workgroup successfully configured.
5379	Event Collector for workgroup removed.
5382	Event Source for workgroup successfully configured.
5383	Event Source disabled.
5384	Event Collector for workgroup failed to configure.
5386	Event Collector for workgroup failed to be removed.
5389	Event Source for workgroup failed to configure.
5390	Event Source failed to disable.
5391	Command line utility output.
5392	Failed to install certificate.
5393	Failed to recreate sever certificate.
5394	Server certificate recreated.
5395	Failed to create certificate request.
5396	Failed to parse certificate request.
5397	Failed to create certificate.
5398	Failed to setup certificate response.
5399	Failed to accept certificate response.
5400	Failed to acquire authorization key.
5401	Failed to find Certificate Authority certificate.
5402	Failed to find host certificate.
5403	Failed to install certificate.
5404	Certificate installed.

---

---

ID	Event
5405	Failed to create root certificate.
5406	Root certificate successfully created.
5407	Failed to apply subscription parameters.
5408	Failed to create Scheduler Task.
5409	Scheduler Task created.
5410	Failed to delete Scheduler Task.
5411	Scheduler Task deleted.
5412	Failed to fire status event.
5413	Status events fired.

---

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

---

DigitalPersona Pro Workgroup can query its client applications and report on various aspects of their status to the Windows Event Log, along with a date and time stamp indicating when the status was reported.

These are called *status* events. For *activity* events, see Chapter 8 beginning on page 56.

These status events are listed below in Event ID sequence.

By default, this reporting of status events is not enabled.

To begin reporting status events to the Windows Event Log

- 1 On the Computers and Users tab of the Pro Workgroup web console, enable the *Level of detail in event logs* setting. Optionally, set the desired level of detail.
- 2 Enable the *Log status events* checkbox. Optionally, change the reporting interval for status events.

Event ID	Description	Data returned
4610	Logon Policy for Administrators Generated by DP Pro Workstation for Workgroup and HP ProtectTools Security Manager	<Policy Data in the form of> Multi factor OR Password Yes Fingerprint(s) Yes Smartcard Yes Spare key Yes
4609	Logon Policy for Users Generated by DP Pro Workstation for Workgroup and HP ProtectTools Security Manager	<Policy Data in the form of> Multi factor OR Password Yes Fingerprint(s) Yes Smartcard Yes Spare key Yes
4612	Session Policy for Administrators Generated by DP Pro Workstation for Workgroup and HP ProtectTools Security Manager	<Policy Data in the form of> Multi factor OR Password Yes Fingerprint(s) Yes Smartcard Yes Spare key Yes

Event ID	Description	Data returned
4611	Session Policy for Users Generated by DP Pro Workstation for Workgroup and HP ProtectTools Security Manager	<Policy Data in the form of> Multi factor OR Password Yes Fingerprint(s) Yes Smartcard Yes Spare key Yes
4613	Logon Policy Generated by DP Pro Workstation and DP Pro Kiosk	<Policy Data in the form of> Multi factor OR Password Yes Fingerprint(s) Yes Smartcard Yes Spare key Yes
4614	Session Policy Generated by DP Pro Workstation and DP Pro Kiosk	<Policy Data in the form of> Multi factor OR Password Yes Fingerprint(s) Yes Smartcard Yes Spare key Yes
4615	Authentication Domain Activation Status Generated by DP Pro Workstation, Workstation for Workgroup, DP Pro Kiosk and HP ProtectTools Security Manager	<Domain activation status in the form of> OS Active FVE Inactive BIOS Inactive
4616	Applications Enabled Generated by DP Pro Workstation, Workstation for Workgroup, DP Pro Kiosk and HP ProtectTools Security Manager	<Application list in the form of> PrivacyManager Enabled PTDAM Enabled

## Chapter 9 - Status Events

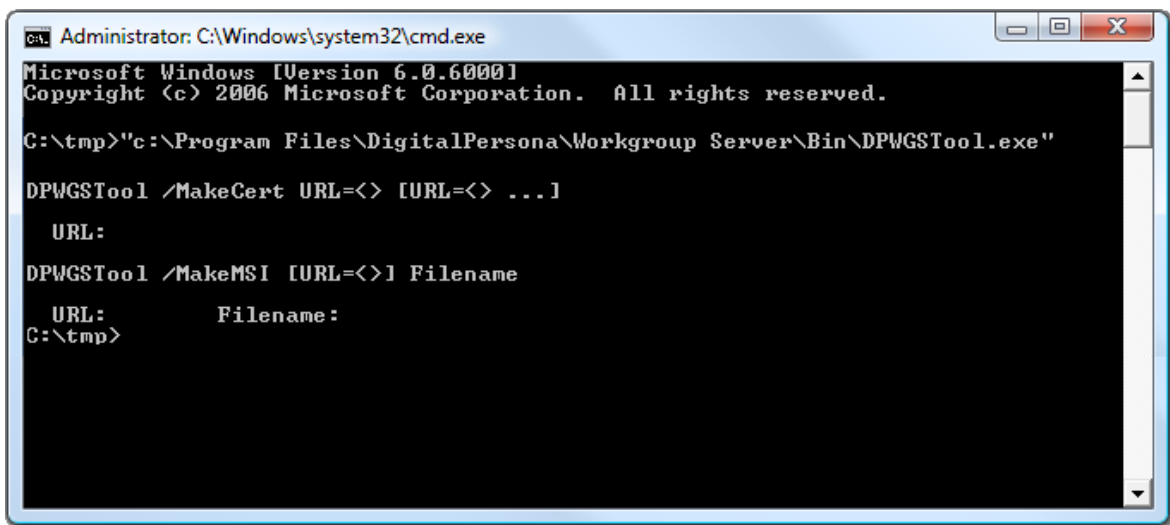
Event ID	Description	Data returned
4617	License Activation status Generated by DP Pro Workstation, Workstation for Workgroup, DP Pro Kiosk and HP ProtectTools Security Manager	<List of products and their license activation status, with details (i.e. # of units)>  PrivacyManager Activated Workstation Not Activated File Crypto N/A
5128	Encrypted Drives using Software Encryption	<Partitions in the form of>  C: Encrypted or C: Encrypting (% Encrypted)  D: Decrypted or C: Decrypting (% Decrypted)
5129	Encrypted Drives using Hardware Encryption Generated only for workstations where hardware encryption is supported in the firmware.	<Physical Drives in the form of>  0(C:,D:) Encrypted 0(C:,D:): Encrypting (% Encrypted)  0(C:,D:) Decrypted 0(C:,D:): Decrypting (% Decrypted)

## DigitalPersona Workgroup Setup Tool

The DigitalPersona Pro Workgroup Setup Tool (DPWGSTool.exe) is a command line utility that can be used to create a new SSL certificate for Pro Workgroup or to create a DigitalPersona Pro Workgroup Setup (MSI) file. You will need to create a new SSL certificate when making your Pro Workgroup server available at other than the default intranet address.

This utility can be found in the DigitalPersona\ Workgroup Server\bin folder on the server after Pro Workgroup Server has been installed.

Running DPWGSTool without parameters will list the available parameters and their syntax.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\tmp>'c:\Program Files\DigitalPersona\Workgroup Server\Bin\DPWGSTool.exe'
DPWGSTool /MakeCert URL=<> [URL=<> ...]
URL:
DPWGSTool /MakeMSI [URL=<>] Filename
URL:      Filename:
C:\tmp>
```

### To create a new Pro Workgroup SSL certificate

- 1 Open a Windows Command prompt.
- 2 Run DPWGSTool with the /MakeCert parameter.

Examples: DPWGSTool /MakeCert URL=mydomain.com

DPWGSTool /MakeCert URL=mydomain.com URL=mydomain2.com

DPWGSTool /MakeCert URL=mydomain.com URL=ServerMachineName

### To create a Pro Workgroup Setup file

- 1 Open a Windows Command prompt.
- 2 Run DPWGSTool with the /MakeMSI parameter.

Example: DPWGSTool /MakeMSI URL=hostname AnyFileName

Note that there are no quotation marks surrounding the URL, and there should be no space between the equal (=) sign and the URL. Also, you do not need to add an extension to the file name that you provide, as the resulting file will automatically include an .msi extension.

Setup files can also be created through the DigitalPersona Pro Workgroup web console. See also “Client Setup and Deployment” on page 34 and “Setting up client computers” on page 39.

## Disconnect Utility

If a network connection is available to the Pro Workgroup Server that the computer is managed by, you should not use the Disconnect Utility; but instead should uninstall “DigitalPersona Pro Workgroup Connection” from the Windows Control Panel on the client computer, or rerun the original Pro Workgroup Setup (MSI) file that was used to start managing the computer.

When it is necessary to stop managing a computer that is unable to connect to the Pro Workgroup Server, you can run the Disconnect Utility (DPWGDisconnect.exe) with the Unmanage parameter. The file is available in the Tools directory of the product package.

Example: `dpwgdisconnect /Unmanage`

This will place the computer in local management mode. However, the computer should then be manually deleted from the list of managed computers in the Pro Workgroup Server web console.

## Troubleshooting Workgroup server installation

If you have installed Pro Workgroup server on a machine with pre-existing IIS applications, you may have one of the following issues:

- 1 Pre-existing applications under the Default Web Site, or with http binding, no longer function
- 2 The Pro Workgroup web console cannot be accessed.

### To resolve issue #1 -

- 1 Open Internet Information Services (IIS) Manager, select the Default Web Site and double-click Modules.
- 2 In the Modules panel, select “Digital Persona redirect,” and in the Actions list, click “Remove.”

### To resolve issue #2 -

- 1 Select a pre-existing website with https binding
- 2 Right-click on the website and select “Add Applications.”
- 3 In the Add Application dialog, enter “wgadmin” as an alias.
- 4 Select “DigitalPersona Workgroup Server” as an application pool. Browse to “C:\Program Files\DigitalPersona\Administration” for the Physical path.
- 5 Click “OK.”
- 6 Navigate to the “https://<server name>/wgadmin” URL in order to access the Pro Workgroup web console.
- 7 Optionally, you may want to update the desktop shortcut to point to the correct URL for the web console.

# Index

## A

ACL **22**  
activation by proxy **36**  
Active Directory, defined **9**  
Applications settings **48**  
Applications tab **43**  
authentication **7**  
Authentication settings **44**

## B

backup **26**

## C

chapter overview **6**  
create a group **37**  
Credential Management events **62**  
credentials **12**  
    defined **7**  
    settings **45**

## D

deployment planning **19**  
designated user **24**  
DigitalPersona Pro Workstation for Workgroup **23**  
display the Applications tab **43**  
DPWGSTool.exe **24**

## E

events  
    Credential Management **62**  
    External components **65**  
    Fingerprint match **65**  
    Group operations **58**  
    Installation package **61**  
    License Management **66**  
    Logon **67**  
    OTP Management **66**  
    Password Manager **65**  
    Privileged user **60**  
    Reporter **69**  
    Secret Management **63**  
    Server **57**

Session operations **57**  
Status **71**  
Systems, Services, Settings and User Sessions **64**  
User and Storage **59**  
User Management **62**  
Workstation **62**  
Workstation for Workgroup **67**  
Workstation operations **57**

## G

General settings **46**  
group **7**  
Group operations events **58**

## H

HP ProtectTools **23**

## I

Installation package events **61**  
installation scenario **21**  
installing  
    DigitalPersona Defender **26**  
    DigitalPersona Pro Enterprise Add-on **26**  
    Drive Encryption **27**  
    Password Manager Pro **28**  
    Privacy Manager Pro **27**

## L

Level of detail in event logs **47**  
License events **60**  
license management **29**  
License operations **60**  
local installation of Pro Workstation **18**  
logon **7**

## M

managed computer **8**  
managed logon **7**  
managed user **8**  
managing computers and users **37**

## O

One time access **8**  
online help **10**  
open ports **22**

## P

Password Manager **8**  
Password Manager Pro **8**  
Planning & Deployment **19**  
ports 800 and 443 **22**  
Privileged user events **60**  
privileged user operations **60**  
Pro Workgroup client system requirements **18, 19**  
Product Compatibility **16**  
proxy activation **36**  
purchase application licenses **43**

## R

recommended skill set **9**  
recover a backup key **41**  
recover a computer **41**  
requisite knowledge **9**

## S

Security settings **44**  
Server Events **57**  
Session operations events **57**  
setting up computers to be managed **24**  
silent installation **24**  
SQL Express database **26**  
Status events **50, 71**  
support **9**

- during evaluation **20**
- online help **10**
- Professional Services **20**
- readme file **9**

System **18**  
system requirements **16, 18**

- Drive Encryption **26**
- Password Manager Pro **28**
- Privacy Manager AdminTool **27**

Privacy Manager Pro **27**

## U

uninstallation **26**  
User and Storage events **59**  
User and Storage operations **59**

## W

web console URL **22**  
Workstation events **62**  
Workstation operations events **57**