Administrator Guide

DigitalPersona® Pro

for Active Directory

Version 3.2.0

digitalPersona.

DigitalPersona, Inc.

© 2005 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.

U.are.U®, DigitalPersona® and One Touch® are registered trademarks of DigitalPersona, Inc.

Windows, Windows 2000, Windows 2003 and Windows XP are registered trademarks of Microsoft Corporation. All other trademarks are property of their respective owners.

This DigitalPersona Pro for Active Directory Administrator Guide and the software it describes are furnished under license as set forth in the Installation Software screen “License Agreement.” 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. This document is subject to the DigitalPersona LIMITED WARRANTY and other general provisions set forth in the Appendix of this manual.

Should you have any questions concerning this document, or if you need to contact DigitalPersona for any other reason, write to:

DigitalPersona, Inc., 720 Bay Road, Suite 100, Redwood City, CA 94063 USA

Table of Contents

1 Introduction **1**

About this Guide 1

Requisite Knowledge 2

Support Resources 3

Typographic Conventions 3

Notational Conventions 4

Naming Conventions 4

Your Feedback Requested 5

2 Product Overview **7**

DigitalPersona Pro for Active Directory Software and Hardware 7

Fingerprint Reader 7

Workstation Software 8

Administering DigitalPersona Pro Workstation 8

Server Software 9

DigitalPersona Pro Concepts and Terminology 9

Fingerprints 9

Fingerprint Registration 10

Fingerprint Verification 10

Fingerprint Identification 10

Credentials 10

Authentication 11

Cached Credentials 11

Identification List 11

Deploying DigitalPersona Pro 12

DigitalPersona Pro Workstation with Pro Server Support 12

DigitalPersona Pro Workstation without Pro Server 13

Deployment Recommendations 14

Steps for Deploying DigitalPersona Pro 14

Server Deployment Recommendations 15

Informing End Users before Deployment 15

Fingerprint Registration Options 16
Implementing Stronger Security Settings in Stages 16
Workstation Installation and Connecting the Reader 17
Deploying One Touch SignOn Templates 17
Security Recommendations and Multi-credential Settings 17
Increasing Password Security 20

3 Installing DigitalPersona Pro Server 21

Installing DigitalPersona Pro Server 21
Step 1: Extending the Active Directory Schema 21
Step 2: Configuring a Domain for DigitalPersona Pro Server 23
Step 3: Installing DigitalPersona Pro Server Software 24
Uninstalling DigitalPersona Pro Server 25
Deleting DigitalPersona Pro Data from Active Directory 25
Changes Made During Installation 27
Active Directory Containers 27
Published Information 28
DNS Registration 29

4 Administering DigitalPersona Pro 33

Administration Overview 33
Implementing DigitalPersona Pro Policies 33
Changing GPO Settings 34
Adding DigitalPersona Pro Administrative Templates 35
Configuring DigitalPersona Pro Settings 38
DigitalPersona Pro Settings 38
Fingerprint Management 39
Fingerprint Logon to Windows 2000, XP and Server 2003 42
Fingerprint Logon to Windows 98 or Me or NT 42
Server Connection Settings 45
Biometric Authentication Service (BAS) Locator 45
Log Events 49
One Touch SignOn 49

DigitalPersona Pro User Properties in Active Directory 49
Windows Logon Options 50
Unlocking Accounts after Failed Logon Attempts 51
Deleting Single User Credentials using ADSI Edit Tool 52
Logging and Auditing 52
Auditing Using the Windows Event Viewer 53
Filtering DigitalPersona Pro Events in Event Viewer 53
Finding DigitalPersona Pro Events with Event Viewer 53
Notes for Windows 98 and Me Computers 54
Administering Pro Workstation on Windows 98 and Me 54
Configuring Settings on Local Computers 54
Configuring Settings on Remote Computers 55

5 Using Administration Tools 57

Using DigitalPersona Pro Workstation for Administrator Tasks 57
One Touch SignOn 57
Setting Up Logon Screens with One Touch SignOn 58
Creating Containers 59
Creating Templates 61
Creating Templates Manually 65
Adding Change Password Screens to Templates 69
Two-Factor Authentication and Other Policies 72
Using Field Catalogs 73
Finding Templates 74
Finding Redundant Templates 74
Finding Fields in Templates 75
Configuring One Touch SignOn 75
Deploying One Touch SignOn Templates 77
Deploying Templates Locally 77
Logging On with One Touch SignOn 78
Changing Passwords with One Touch SignOn 80

Using Attended Fingerprint Registration 80
Assigning Permissions to Perform Attended Registration 80
Registering User Fingerprints 82
Deleting Fingerprints with Attended Registration 83

6 Installing DigitalPersona Pro Workstation 85
Installing DigitalPersona Pro Workstation 85
Customizing a DigitalPersona Pro Workstation Installation 87
Uninstalling DigitalPersona Pro Workstation 87
Remote Installation and Uninstallation 87
Installation Using the Command Prompt 88

7 Using DigitalPersona Pro Workstation 91
Logging on after Installation 91
DigitalPersona Pro Feedback 92
Fingerprint Prompt Feedback 92
Fingerprint Scan Acquisition Feedback 93
Fingerprint Recognition Feedback 93
Reader Not Found Feedback 93
Managing Fingerprint Credentials 94
Registering Fingerprints 95
Deleting Registered Fingerprints 98
One Touch Logon 99
Logon Policies 100
Cached Credentials and the Identification List 101
Using Smart Cards for Logon 102
Using Fingerprint PINs 103
Changing Your Windows Password 105
Using One Touch Unlock 107
Using One Touch Unlock on Windows 98/Me 107
One Touch Internet 109
Logging On to Web Sites and Programs 109
Creating Fingerprint Logons 110
Editing Fingerprint Logons for Web Sites and Programs 112

Using the One Touch Menu 113
Create Fingerprint Logon 114
Quick Links 114
Help 114
Properties 115
Reader Icon and Menu 115
Lock Computer 115
Properties 116
Help 116
About 116
Hide Icon 116
Configuring DigitalPersona Pro Workstation 116
Quick Actions 117
Show Fingerprint Reader Icon on the Taskbar 118
Show Fingerprint Recognition Animation 118
Enable Visual Feedback for Fingerprint Scan 118
Enable Sound Feedback for Fingerprint Scan 118
One Touch Menu 119
Fingerprint Reader Usage and Maintenance 119
Proper Fingerprint Reader Usage 119
Cleaning the Reader 120

8 Troubleshooting 123

Reader Troubleshooting 123
Reader Does Not Light Up During Installation or Restart 123
Reader Light Went Out When In Use 124
Reader Does Not Blink When Touched 125
Software Does Not Respond When Reader Is Touched 125
Reader Blinks Constantly 125
One Touch Programs Troubleshooting 125
One Touch Logon Troubleshooting 125
One Touch Internet and OTS Troubleshooting 126
Installation Troubleshooting 127
Using the Diagnostic Center 127

Running the Diagnostic Center 128
Collecting Trace Files for Troubleshooting 128
Common Issues Found 130

9 Appendix A 131

Event Log Specifications 131
User Authentication Events 131
Secure Application Data Released 131
Secure Application Data Denied 132
User Management Events 133
User Record Added 133
Record Add Failed 133
User Record Updated 134
User Record Update Failed 135
User Record Deleted 135
User Record Delete Failed 136
User Record Consistency Failed 136
User Secret Consistency Failed 137
User Record Signature Check Failed 138
User Secure Signature Check Failed 138
User Account Locked Out 139
DNS Registration Events 139
DNS Update Disabled 139
DNS Registration Failed 140
DNS Unregistration Failed 141
DigitalPersona Name Translation Failed 141
Logon Events 142
User Logged In 142
User Logon Failed 142
GINA Password Logon 143
GINA Unlock 143
GINA Register PIN 144
GINA Change PIN 144

GINA Smart Card Unlock 144
GINA Fingerprint PIN Registration Canceled 145

10 Appendix B 147

Configuring DigitalPersona Pro Workstation Settings 147
Configuring the One Touch Menu Content 147
Configuring Quick Actions 148

11 Appendix C 149

Limited Warranties and Warranty Service 149
General Provisions 151
Regulatory Information 152

Introduction 1

The DigitalPersona® Pro for Active Directory Administrator Guide describes the installation, configuration and use of the DigitalPersona Pro for Active Directory Server and Workstation software.

About this Guide

This chapter describes the requisite knowledge an administrator of DigitalPersona Pro software must possess in order to use this guide and the product. It also explains technical support options and describes the conventions used in this guide.

Following is a description of the remaining chapters:

Chapter 2, Product Overview, describes DigitalPersona Pro Server and DigitalPersona Pro Workstation software and hardware and provides a feature comparison of deployment scenarios. It also introduces key product and security concepts to administer and use the software. It provides deployment process recommendations and security considerations.

Chapter 3, Installing DigitalPersona Pro Server, contains detailed instructions for deploying and installing the Server software, including system requirements and any special considerations to be made before performing the installation. It provides additional instructions and considerations for uninstalling DigitalPersona Pro software.

Chapter 4, Administering DigitalPersona Pro, provides guidelines and instructions for administering DigitalPersona Pro Servers and Workstations using Active Directory administration tools for domain-wide administration or the Microsoft Management Console for local administration.

Chapter 5, Using Administration Tools, provides instructions for using One Touch SignOn to create fingerprint logons for Web sites and programs and to deploy them to users. It also describes how to register users through Attended Fingerprint Registration.

Chapter 6, Installing DigitalPersona Pro Workstation, contains detailed instructions for installing the Workstation software and hardware, including system requirements and any special considerations to be made before

performing the installation. It provides additional instructions and considerations for uninstalling DigitalPersona Pro software.

Chapter 7, Using DigitalPersona Pro Workstation, introduces the primary functionality of DigitalPersona Pro Workstation software, such as logging on, registering and deleting fingerprints, using the One Touch Menu and the reader icon menu and configuring DigitalPersona Pro properties. It describes the changes made to a computer when DigitalPersona Pro Workstation software is installed. It also describes how to secure your desktop with One Touch Unlock and how to use One Touch Internet to log on to Web sites and programs with your fingerprint.

Chapter 8, Troubleshooting, provides helpful information to assist you with using both DigitalPersona Pro Server and Workstation software. Tips for using the U.are.U Reader are also included. It describes how to use the Diagnostic Center for identifying and resolving configuration and connection issues.

Requisite Knowledge

To use DigitalPersona Pro Server and Workstation software, you must possess the skills and knowledge described in this section.

A domain administrator must have knowledge of and experience with the Windows 2000 or Server 2003 and its administrative tools to administer DigitalPersona Pro Server. Specifically, you must be able to define and work with key Active Directory concepts, including, but not limited to, group policy objects, containers, sites, domains and Organizational Units. You must also be able to use the standard Active Directory administration tools, such as the Active Directory for Users and Computers console and the Group Policy Editor.

If you are administering DigitalPersona Pro locally, you should understand how to use the Microsoft Management Console (MMC) to manage computer properties. Instructions for using MMC to configure a DigitalPersona Pro Workstation locally are provided as well as descriptions of each configurable property.

End users of DigitalPersona Pro for Active Directory Workstation must possess basic computer and network operation skills, such as logging on to a computer and using context menus, the taskbar and a Web browser.

Support Resources

In addition to this guide, the following resources are provided for additional support to both users of DigitalPersona Pro Server and Workstation:

- A Readme file is provided on both the DigitalPersona Pro Server and Workstation installation CD root directories. Each file contains last-minute information about DigitalPersona Pro.
- The DigitalPersona Web site (http://www.digitalpersona.com) provides an online technical support form in the Support section. You can describe your issue and include your contact information and a technical support representative will contact you by e-mail or phone.
- E-mail support is available at `techsupport@digitalpersona.com`.
- Phone support can be reached at (877) 378-2740 in the U.S. only. Outside the U.S., call +1 650-474-4000.
- Online help is included with DigitalPersona Pro Workstation installations. It is accessible from various dialog boxes that appear during the use of the software and from the One Touch Menu, as described in "Help" on page 114.

Typographic Conventions

The following typographic conventions are used in this guide:

- `Courier` indicates text that is typed by the user.
  Example:
  "Type `http://www.digitalpersona.com/` in the Address text box."
  You would only type "http://www.digitalpersona.com/" and would not type any surrounding text.
- Text in **`Courier bold`** and surrounded by brackets **`[ ]`** indicates information that is always supplied by you and will vary depending on a particular circumstance.

Example:
"Type `http://` **`[your company Web site URL]`** / in the Address text box."
You would type "http://", then type your company Web site URL—not the words "[your company Web site URL]"—and then "/".
It is also used to display information that is dynamically generated by DigitalPersona Pro.

Notational Conventions

The following notational conventions are used in this guide to call attention to information of special importance:

Note
A note highlights information that may help you better understand the text and its concepts.

Warning
A warning advises you that failure to take or avoid a specific action could result in your inability to complete the required tasks or will cause undesired results in the use of the software or hardware.

Naming Conventions

For brevity and easier reading of this guide, the following naming conventions are used to describe the DigitalPersona Pro for Active Directory Server and Workstation software and hardware:

- DigitalPersona Pro Server, Pro Server and Server sometimes replace the full product name, DigitalPersona Pro for Active Directory Server. In this guide, these terms always refer to the Active Directory version—not any other version of DigitalPersona Pro Server software.
- DigitalPersona Pro Workstation, Pro Workstation and Workstation are sometimes used instead of the full name, DigitalPersona Pro for Active

Directory Workstation. They always refer to the Active Directory version of DigitalPersona Pro when used in this guide.

- Reader—in both upper and lower case—is always used without the preceding U.are.U. It replaces the full product name, U.are.U Reader.

Your Feedback Requested

The information in this guide has been thoroughly reviewed and tested. If you find errors or have suggestions for future publications, contact DigitalPersona at:

720 Bay Road, Suite 100
Redwood City, California 94063 USA
(650) 474-4000
(650) 298-8313 FAX

Product Overview 2

DigitalPersona Pro combines the security of fingerprint authentication with the simplicity and convenience of Single Sign-On (SSO). The DigitalPersona Pro fingerprint authentication software combined with the U.are.U® Fingerprint Reader, instantly verifies the identity of authorized users. Users can conveniently log on to Windows computers, Microsoft networks, password-protected programs and Web sites by providing their fingerprint with a touch of a finger. DigitalPersona Pro provides central administration and scales to over one hundred thousand users. The product is tightly integrated with Windows Active Directory and can be deployed without the need for professional services.

DigitalPersona Pro for Active Directory can be deployed in a variety of scenarios and environments. The type of deployment you choose will depend on the features you require.

This chapter describes the features and benefits of the product to help you determine the best deployment for your environment. It also introduces key product and security concepts that you should become familiar with before installing and using DigitalPersona Pro for Active Directory.

DigitalPersona Pro for Active Directory Software and Hardware

DigitalPersona Pro for Active Directory includes workstation software with the U.are.U Reader and server software.

Fingerprint Reader

The DigitalPersona U.are.U Fingerprint Reader is an optical scanner for fingerprints used with DigitalPersona Pro. DigitalPersona Pro Workstation is the client software that works with the U.are.U Reader to read the fingerprint scan for authentication, also known as fingerprint logon. You may have a U.are.U Reader or a keyboard or device with an embedded U.are.U Reader.

Workstation Software

The DigitalPersona Pro for Active Directory Workstation software provides fingerprint logon functionality for Windows computers. It includes the following applications:

- **One Touch Logon** increases security and convenience by adding fingerprint authentication to the Windows logon procedure. One Touch Logon allows users to log on to Windows with a fingerprint in addition to, or as an alternative to, their Windows credentials, such as a password or a smart card. One Touch Logon replaces the standard Windows logon dialog box. One Touch Logon guides users through providing the required credentials to log on to Windows. It also allows users to quickly lock and unlock their computers using the credentials specified by the logon settings.
- **One Touch SignOn** simplifies and secures access to password-protected, third-party software programs and Web sites. Users just touch the reader to automatically and securely provide data for logon fields, such as user name and password fields, on any Web site or program logon screen. Administrators use the One Touch SignOn Administration Tool and application policy settings to create and deploy the One Touch SignOn templates specifying information for the logon screens.
- **One Touch Internet** provides end users with many of the capabilities of One Touch SignOn for their personal Web accounts through the easy-to-use wizard.

Administering DigitalPersona Pro Workstation

The DigitalPersona Pro Workstation software has several configurable properties, which can be accessed with the standard Active Directory administration tools when deployed with DigitalPersona Pro Server, or the Microsoft Management Console for local administration. The end user can also configure some Workstation properties to customize the user experience.

Server Software

DigitalPersona Pro Server provides domain-wide administration for networked DigitalPersona Pro Workstations. Server software features include:

- **Full integration with Active Directory Administration (Windows 2000, 2003).** DigitalPersona Pro Server allows you to use the Active Directory administration tools to modify a number of settings. For example, with the Active Directory Group Policy Editor, you can create Group Policy Objects that control the security level for fingerprint matching, as well as specify credential requirements for logon settings and more. You apply a Group Policy Object to computers to configure them. The computers themselves require no additional configuration to use the DigitalPersona Pro Server for authentication. DigitalPersona Pro includes fault tolerance and load balancing by using the DNS locator service of Active Directory to automatically and transparently locate all available servers and then choose one for authentication.
- **High-level security architecture.** DigitalPersona Pro Server builds on the trust relationship established by Windows 2000, 2003 to provide a secure infrastructure for server-client communication. PKI technology is used to encrypt data and secure communications between the workstation and server.
- **Centralized credential and application databases.** DigitalPersona Pro Server extends the Active Directory schema to store DigitalPersona Pro data. User data is replicated through the entire network, allowing a known user to use a fingerprint on any DigitalPersona Pro Workstation connected to a DigitalPersona Pro Server.

DigitalPersona Pro Concepts and Terminology

DigitalPersona Pro introduces several key concepts that you are required to be familiar with and understand to use or administer DigitalPersona Pro.

Fingerprints

Fingerprints provided through the fingerprint reader are transformed into highly compressed and digitally encoded mathematical representations of fingerprint features. The mathematical representations are created whenever a user places a

finger on the reader, for example, when logging on, and encoded with a one-way algorithm that cannot be reversed to recreate the scan of that fingerprint. Fingerprint scans are never stored; they are discarded after the mathematical representation is created.

Fingerprint Registration

Fingerprint registration is the process of creating a registration template, which is derived from four fingerprint scans acquired by the reader and stored in the user database for future use during authentication and identification. A fingerprint for which a registration template was created is referred to as a registered fingerprint.

Fingerprint Verification

Fingerprint verification is the process of verifying that the template derived from the fingerprint scan acquired by the reader during authentication and identification and the registration templates are from the same finger. Unlike registration templates, the template created during fingerprint verification, called a verification template, is discarded after it is used for matching.

Fingerprint Identification

Fingerprint identification is the process of identifying a user out of a set of users by fingerprints. It is performed with only a fingerprint, and not a user name, by matching the verification template to all registration templates in the set of users.

Credentials

Credentials are a set of information used to gain access to your Windows account or a password protected Web site or program. Windows credentials can include a combination of a user name, password, fingerprint, fingerprint PIN, or smart card. Web site and program credentials can include a combination of fingerprint and password.

Authentication

Authentication is the process of proving identity, by providing one or more credentials that attest to your identity. User authentication is a critical component of security. DigitalPersona Pro uses fingerprint recognition as the method of authentication and identification.

Cached Credentials

DigitalPersona Pro user data can be cached on any computer where a user logs on. The cached user data is used for local authentication when a DigitalPersona Pro Server is unavailable. Refer to "Cache Domain User Data on Local Computer" on page 43.

For example, if a user wants to log on to a domain and the computer is either disconnected from the network or the network is down, then the authentication can be performed locally using the cached credentials. All DigitalPersona Pro cached credentials are encrypted for security and privacy with the local key of the DigitalPersona Pro Workstation.

Identification List

The identification list contains an administrator-specified number of user accounts. It is used in conjunction with cached credentials to identify a user by their fingerprint and, as an added convenience, frees them from typing their user name and domain at Windows logon.

Users are added to the identification list in the order they log on. The most recent user to log on is added to the top of the list. If the list has exceeded its capacity, the least recent user to log on is removed from the list when another user logs on. If a user is already on the list and logs on again, they are moved from their original position on the list and placed on top.

Once removed, a user can still use their cached credentials (if enabled), but they must type their user name and domain manually. If DigitalPersona Pro is deployed in a networked environment with Pro Server support, it performs identification locally out of the set of users in the identification list and then, for added security, confirms the user identity using the DigitalPersona Pro Server.

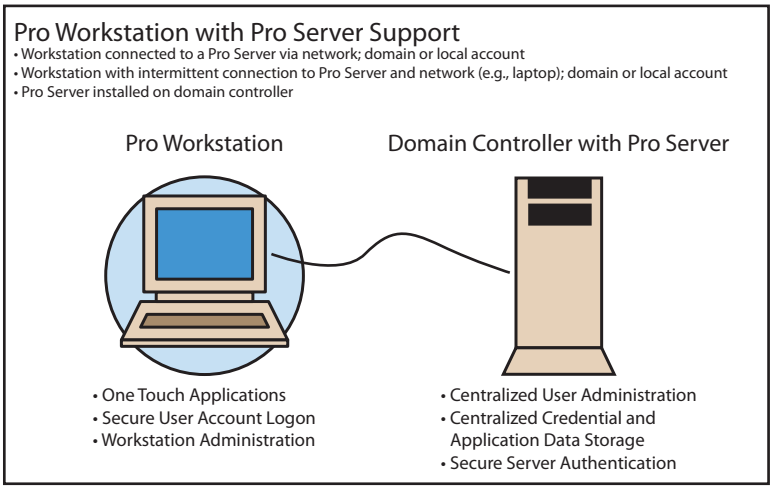
The number of users stored in the identification list is determined by the value of the "Maximum Size of Identification List" GPO setting, as described on page 44.

Deploying DigitalPersona Pro

DigitalPersona Pro can be deployed in any scenario, from a stand-alone computer to a networked computer with DigitalPersona Pro Server support. Deployment scenarios and their differences are described in the next sections.

DigitalPersona Pro Workstation with Pro Server Support

For enterprise-wide deployment, DigitalPersona Pro Workstation can be installed on a network computer connected to a domain controller that has DigitalPersona Pro Server installed. Computers can be periodically connected to and disconnected from the network, such as a laptop computer.



Using a DigitalPersona Pro Workstation with Pro Server support is the most comprehensive deployment of DigitalPersona Pro because you can take

advantage of both the Workstation and Server features of DigitalPersona Pro for Active Directory.

In addition to the One Touch applications for the Workstation, this deployment allows you to administer DigitalPersona Pro with Active Directory administration tools and provides the high-level security architecture and user roaming features.

DigitalPersona Pro Workstation without Pro Server

If you install DigitalPersona Pro on a computer connected to a domain without DigitalPersona Pro Server support or on a computer configured to perform authentication locally, you have all the features provided by the DigitalPersona Pro Workstation software as described in "Workstation Software" on page 8.

The table below compares the features available for DigitalPersona Pro Workstations with and without Pro Server support:

Deployment Scenario	DigitalPersona Pro Features					
	Centralized User Administration	Centralized User Credential Data Storage	Secure Server Authentication	One Touch SignOn and One Touch Internet	Secure Windows Logon	Workstation Administration
Workstation with Pro Server support	X	X	X	X	X	X
Workstation without Pro Server support				X	X	X

Deployment Recommendations

As the administrator, you should carefully consider your options and create a plan before starting deployment. The following sections describe the basic steps and decisions required for deployment and provides general guidelines and recommendations. Your specific solution may vary based on your own needs and requirements.

Steps for Deploying DigitalPersona Pro

The following steps and decision making process are recommended when planning for deployment:

1 Plan for the number of Pro Servers and Pro Workstations to be installed in your deployment. In larger deployments, it is recommended to have enough servers installed to provide service to the first set of users. Continue to test performance to make sure that enough servers are installed as each set of users is added. Smaller organizations may decide to deploy all users at the same time.

2 Deploy Pro Servers, which includes performing an Active Directory schema extension, domain configuration and installation of the DigitalPersona Pro Server software to support the first set of users.

3 Test the DigitalPersona Pro Workstation deployment on a single computer and set the options that the end users will use. Test the GPO settings set in Active Directory and confirm the intended effects for users.

4 Inform and educate end users on the deployment process and the tasks that you want them to complete.

5 If using attended fingerprint registration, register user fingerprints from the test DigitalPersona Pro Workstation. Attended registration requires a supervising user and the end user to be present to register the user's fingerprints. See "Using Attended Fingerprint Registration" on page 80 for more information.

6 Install DigitalPersona Pro Workstation for the first set of users. Users should be separated into sets either by department or geography or some other grouping. The first set of users should be a small test group to make sure you

have implemented settings as intended. Later, other sets of users can be added in stages.

7 Create and deploy One Touch SignOn templates for fingerprint logon to Web sites and programs.

8 Connect fingerprint readers to computers. Instruct users on which order to complete install, hardware connection, and fingerprint registration as needed.

Server Deployment Recommendations

DigitalPersona Pro Server software provides a replicated storage of user data in Active Directory, central administration of user data, and user and computer policies (GPO) to configure the DigitalPersona Pro system. Pro Server provides the security of fingerprint verification on a domain controller. You must decide whether you will deploy DigitalPersona Pro Workstation in a standalone mode, or in conjunction with DigitalPersona Pro Servers.

You can test in the standalone mode and then choose to move to a server deployment later. In this case, all Pro user data on the standalone computer is lost when connected to DigitalPersona Pro Server. Fingerprints must be registered again and user account data for fingerprint logons must be provided again. Organizations that intend to implement a server deployment should also test in a server environment.

To decide how many DigitalPersona Pro Servers must be installed, it is recommended to assign 1000 users per server if the majority of users log on at approximately the same time of day. You can assign up to 2000 users per server if users log on over a longer period of time, for example, due to different work shifts or hours. It is also recommended to install a minimum of two servers per domain or site to ensure continuous service if one server is unavailable.

Informing End Users before Deployment

Deployment will be most effective and flow smoothly if you inform your users about the new user experience before DigitalPersona Pro Workstation is installed on their computers. Users need instructions on what to do when they view the DigitalPersona Pro Welcome screen to log on to Windows and when

the Fingerprint Registration Wizard launches. You may need to provide additional instructions to users based on your implementation such as:

- Logging on with a password just as they did before DigitalPersona Pro Workstation was installed until the fingerprint reader is connected by an IT representative.
- Logging on with registered fingerprints after fingerprints are registered if the fingerprint reader is already connected.

Warning

Make sure that you do not enable restrictive logon settings based on fingerprints until users have successfully registered fingerprints.

Let users know that their fingerprint images will not be stored. Instead, fingerprints are converted into binary data and then stored. This data cannot be reverted to actual fingerprint images.

Fingerprint Registration Options

You can allow users to register their own fingerprints from their computers or you can require that fingerprint registration is attended by an administrator. With attended registration, a designated user must be logged on to supervise the fingerprint registration process of other users. You can set permissions so that the users cannot modify the registered fingerprints. For more information on using attended fingerprint registration, see "Using Attended Fingerprint Registration" on page 80.

Implementing Stronger Security Settings in Stages

For large enterprise deployments, you might want to implement less strict security settings while users adopt the new process of registering fingerprints and using fingerprints to log on. During this time, you can configure a setting allowing a fingerprint or a password for log on to Windows. This allows users to register their fingerprints and to start using them, for example, over a two week period.

Afterwards, you can transition to more strict settings to make fingerprints required for logon. You can increase security settings by changing the settings in the DigitalPersona Pro GPO. You may also randomize user passwords which prevents users from logging on to Windows without providing fingerprints.

If you find that users have not registered fingerprints, you can either complete attended fingerprint registration with the users, or you can choose to extend the open registration period. In this case, continue to inform the users that they will not be able to log on if they do not register their fingerprints before a specific date.

For a discussion on the DigitalPersona Pro logon settings, see "Security Recommendations and Multi-credential Settings" on page 17.

Workstation Installation and Connecting the Reader

Smaller companies may want users to install the hardware. Larger companies may use a representative from the IT department to install the hardware. To install software locally, the user must have administrative privileges on the local computer.

Deploying One Touch SignOn Templates

The administrator for One Touch SignOn can decide how much control to maintain over the templates for Web sites and programs. Templates can be created and deployed using GPO settings. The ability for users to make changes to account data or create their own fingerprint logons can be limited or disabled. If a lower level of control is more appropriate, editing, adding and deleting settings for account data can remain enabled.

Security Recommendations and Multi-credential Settings

You can configure logon settings that require more than one type of credential to log on. Possible credentials for Windows logon include fingerprint, password or smart card. The multi-credential logon settings are configured using the Multi-credential Logon to Windows in the GPO. DigitalPersona Pro does not provide

any setting to control the use of the smart card for the Windows logon and will apply the Windows policies.

For local area network users, allowing the fingerprint to be used instead of the password, while also accepting the password as an option, is recommended as a starting logon setting. A simple way to require two-factor authentication, to increase security without compromising user convenience, is to require a fingerprint PIN in addition to a fingerprint. This is the recommended setting for remote users. For more information on fingerprint PINs, see "Using Fingerprint PINs" on page 103.

While users adapt to the new fingerprint policies, you might want to begin with more flexible logon settings. For example, a policy may be set strictly at the beginning of deployment that requires the user to use a fingerprint. If the user cancels out of the Fingerprint Registration Wizard, then the next time the user tries to log on to Windows, the user will be unable to log on. If users have not registered their fingerprints, they will need to contact an administrator to register their fingerprints. If you allow a fingerprint or a password to log on as part of an initial phase, users can continue working as they learn to adopt the new policies.

To provide a more convenient logon process for multi-credential logons, you can choose to allow the fingerprint to unlock the smart card instead of requiring users to type the PIN for the smart card.

All Multi-credential Logon to Windows settings are available as GPO settings. User specific settings are available to override all GPO settings, with the exception of Fingerprint is allowed to unlock the smart card, which is available as GPO only.

The table below shows all the possible combinations of credentials that can be implemented using the DigitalPersona Pro policies and the Windows policy for the smart card.

	Windows Policy	DigitalPersona Policies		
Logon Requirements	**Smart card is required for interactive logon**	**User must provide a fingerprint to log on**	**Password is not allowed for log on**	**User cannot use fingerprint to log on to Windows**
Fingerprint OR Smart card			X	
Fingerprint AND Smart card	X	X	X	
Fingerprint AND (Smart card OR Password)		X		
Smart card OR Password				X
Fingerprint OR Smart card OR Password				
Fingerprint only *			X	
Fingerprint OR Password *				
Fingerprint AND Password *		X		
Password only *				X

* available only if you do not deploy the smart card

Deploying a smart card requires that the smart card reader is connected to the computer and the proper smart card reader drivers are installed. Smart cards are supported on Windows XP and 2000.

Because of Windows settings for smart cards, the following combinations are not possible:

- Smart card AND Password
- Fingerprint AND Smart card AND Password

For descriptions of each setting, see “Multi-credential Logon to Windows” on page 42.

The following table shows the settings available for configuration and indicates whether the setting applies to all users on a computer, to a specific user or both.

Settings in the GPO apply to all users, local and network. Per user settings apply to domain users. You cannot configure settings on the user level for local users.

Setting	Computer GPO	User Properties	Default Value
User must provide a fingerprint to log on	X	X	Fingerprint is optional.
Password is not allowed for log on	X	X	The password is allowed.
PIN is required when a fingerprint is provided	X	X	The PIN is not required.
Fingerprint is allowed to unlock the smart card	X		The fingerprint is not allowed to unlock the smart card.
User cannot use fingerprint to log on to Windows		X	Fingerprint is allowed for Windows logon.

Increasing Password Security

Security-conscious users should take additional measures to decrease the likelihood of unauthorized access to their computers. Suggestions in this manual are specific to DigitalPersona Pro only and do not represent a complete list of security measures. All users should create secure passwords for Windows accounts and applications.

Refer to the Microsoft Web site for more information about securing your computer from unauthorized access. The Microsoft Web site also contains more information on creating secure passwords.

Installing DigitalPersona Pro Server 3

This chapter provides instructions for the local installation of DigitalPersona Pro Server on a domain controller. It also describes the process of uninstalling DigitalPersona Pro Server software.

If you are installing DigitalPersona Pro Server software, you should read the chapter in its entirety. If you are installing DigitalPersona Pro Workstation, refer to "Installing DigitalPersona Pro Workstation" on page 85 and "Remote Installation and Uninstallation" on page 87.

Installing DigitalPersona Pro Server

The following steps are required to install DigitalPersona Pro Server for Active Directory on a Windows 2000 or 2003 network:

1. Extend the Active Directory schema to include attributes and classes used by DigitalPersona Pro Server, as described in "Step 1: Extending the Active Directory Schema" on page 21.
2. Configure one or more domains on which DigitalPersona Pro Server will be installed to set up global data and server security for the domain, as described in "Step 2: Configuring a Domain for DigitalPersona Pro Server" on page 23.
3. Install the DigitalPersona Pro Server software on the domain controllers of the configured domains, as described in "Step 3: Installing DigitalPersona Pro Server Software" on page 24.

Note

You must wait for Active Directory schema replication to complete after both extending the schema and configuring the domain.

The remainder of this section provides instructions for performing the necessary steps to install DigitalPersona Pro Server software.

Step 1: Extending the Active Directory Schema

The Active Directory schema must be extended to use DigitalPersona Pro Server. Changes to the schema include the creation of new attributes including attributes for the user object and new classes, as well as modifications to existing classes. Only if absolutely necessary, future updates of DigitalPersona Pro for

Active Directory may introduce other schema extensions. The DigitalPersona schema extension wizard version number is independent of the DigitalPersona Pro version number.

Warning

The schema extension is global to the Active Directory forest, not just a single domain. Also, schema changes cannot be rolled back in Active Directory.

To extend the Active Directory schema, make sure that you have schema administration privileges and then run the Schema Extension Wizard.

Note

You should run this wizard from the schema master domain controller. If you run it from a different domain controller, the data may not replicate fast enough to allow the wizard to run. If the data is not replicated and you attempt to run the wizard, it will terminate automatically. You should then wait one replication cycle before running the wizard again.

To run the Active Directory Schema Extension Wizard

1. Double-click DPSchemaExt.exe, which is located in the AD Schema Extension folder on the Server installation CD, to start the Schema Extension Wizard.
2. Read the terms and conditions on the License Agreement page. If you agree with them, select I accept the license agreement and then click Next.
3. When prompted to proceed with the schema extension, click Yes.
4. Next, specify a location and name for the log file generated by the Schema Extension Wizard in the Save Log File As dialog box. Then, click Save.
5. If the schema is not writable, the wizard will inform you and will allow you to make it writable. If this dialog box displays, click Yes to make the schema writable and perform the schema extension.
6. The wizard will extend the schema, while providing the specifics of the schema extension, such as the class and attribute names. To close the wizard, click Finish.

The name of each new attribute and class added to the Active Directory schema follows Microsoft naming conventions. The names are assigned a “dp” prefix, which is registered with Microsoft.

The OID base, generated by Microsoft, is 1.2.840.113556.1.8000.651.

Step 2: Configuring a Domain for DigitalPersona Pro Server

For each domain on which you will install DigitalPersona Pro Server, make sure you have administrator privileges on the domain controller and then run the DigitalPersona Pro Active Directory Domain Configuration Wizard. This wizard configures the domain-specific data for DigitalPersona Pro, including the cryptographic keys.

You should run this wizard only once.

Warning

Active Directory replicates the domain-specific data. User data could be erased in the unlikely situation that the wizard is run more than once before data is fully replicated in an environment with multiple Pro Servers or multiple domain controllers.

To run the DigitalPersona Pro Active Directory Domain Configuration Wizard

1 Double-click DPDomainConfig.exe, which is located in the AD Domain Configuration folder on the Server installation CD.
2 A warning reminds you not to run this wizard if you have an existing DigitalPersona Pro Server installation on this domain.

Warning

If you run this wizard on a domain with an existing DigitalPersona Pro Server installation, DigitalPersona Pro data will be unusable and cryptographic keys will be invalidated.

If you are sure there are no other DigitalPersona Pro Server installations on the domain you are configuring, click Yes.

3 Read the license agreement that displays and, if you agree to the terms and conditions, select I accept the license agreement and then click Next.
4 In the Save Log File As dialog box, specify a file name and folder path for the log file generated by the wizard. Then, click Save.
5 When you click Save, the wizard performs the necessary changes on the domain.
6 To close the wizard, click Finish.

Step 3: Installing DigitalPersona Pro Server Software

After a domain controller is configured to run DigitalPersona Pro Server, you can install the DigitalPersona Pro Server software.

Before installing the Server software, make sure that the domain controller meets the following hardware and software requirements:

- Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, or Windows 2003 Server
- Active Directory
- High-encryption (128-bit) capability. If this capability is not installed, use the instructions provided below.
- 10 MB of free hard disk space

If your domain controller is not high-encryption (128-bit) capable, install Microsoft Windows 2000 High Encryption (128-bit) Capability which is available for download from Microsoft. Because high encryption capability is built into Windows XP, 2003 and the latest service packs for Windows 2000, you do not need to install high encryption pack on these operating systems.

To install Microsoft Windows 2000 High Encryption (128-bit) Capability on your domain controller

1 Double-click ENCPACK.exe to launch the installer.
2 When prompted to continue with the installation of Microsoft Windows 2000 high-encryption (128-bit) capability, click Yes.
3 To finish the installation, restart the computer.

In addition to the hardware and software requirements, there are two conditions that must be met before you can install the Server:

- You must have administrator privileges on the domain controller.
- No other DigitalPersona products are installed.

To install DigitalPersona Pro Server software

1 Double-click Setup.exe, which is located in the Install folder on the Server installation CD, to run the DigitalPersona Pro Server Installation Wizard.
2 When the wizard opens, click Next.
3 Read the terms and conditions on the License Agreement page. If you agree with them, select the I accept the license agreement button and then click Next.
4 On the next page, you can specify the folder in which DigitalPersona Pro Server will be installed. If you want to install DigitalPersona Pro in the default location, `C:\Program Files\DigitalPersona\`, click Next; otherwise, click Browse to specify a new location and then click Next to continue.
5 The wizard will install the Server software. To close the wizard, click Finish.

When DigitalPersona Pro Server is installed, several changes are made to Active Directory. For more information, see "Changes Made During Installation" on page 27.

Uninstalling DigitalPersona Pro Server

If you have administrator privileges on the domain on which Pro Server is installed, you can remove the Server software using the Add/Remove Programs Control Panel in Windows. The Server software is listed as, "DigitalPersona Pro Server for Active Directory version **`[version number]`**."

When you uninstall the Server software, the published information (described in "Published Information" on page 28) and the DNS SRV RRs (described in "DNS Registration" on page 29) are removed.

Deleting DigitalPersona Pro Data from Active Directory

Although the Add/Remove Programs Control Panel uninstalls DigitalPersona Pro Server software, the user data—such as fingerprint credentials and secure application data—and global domain data remain in Active Directory.

DigitalPersona provides the DigitalPersona Pro Cleanup Wizard to remove this data. If you are planning to reinstall DigitalPersona Pro software, you may want to retain the user data.

Note
You must have administrative privileges in order to run this wizard on a domain controller.

Note
This wizard provides full cleanup of DigitalPersona Pro data. For removal of individual user data, see "DigitalPersona Pro User Properties in Active Directory" on page 49.

To use the DigitalPersona Pro Cleanup Wizard to remove Pro data from Active Directory

1 Double-click DPCleanup.exe to launch the DigitalPersona Pro Cleanup Wizard, which is located on the Server installation CD in the AD Clean Up folder in the Administration Tools folder.
2 When the installer runs, you are prompted to choose the type of clean up you want to perform:
   - **Delete DigitalPersona Pro user data.** This option removes all DigitalPersona Pro data associated with users on the domain, such as fingerprint credentials and secure application data. If you choose to delete DigitalPersona Pro user data, all users must register their fingerprints again.
   - **Full clean up.** This option removes both DigitalPersona Pro data associated with users on the domain and global data. If you choose full clean up, you must reinstall all DigitalPersona Pro Servers on the domain and run the Active Directory Domain Configuration Wizard. See "Step 2: Configuring a Domain for DigitalPersona Pro Server" on page 23.
3 When prompted to proceed with the removal of DigitalPersona Pro data, click Yes.
4 Choose a location and name for the log file generated during the data removal process.

The wizard will then remove the data from Active Directory; however, you must manually remove any DigitalPersona Pro Group Policy Objects.

Warning

Data changes take time to propagate in Active Directory. Do not configure a domain for DigitalPersona Pro Server or install Server software until all changes made by the removal of domain global data are replicated throughout the domain.

Running the DigitalPersona Pro Clean Up Wizard renders all Pro Servers inoperable on the domain. To restore the Pro Server functionality after performing a full cleanup, run the Active Directory Domain Configuration Wizard again, as described in "Step 2: Configuring a Domain for DigitalPersona Pro Server" on page 23, and then reinstall Pro Server. Otherwise, you only need to register all user fingerprints again.

Changes Made During Installation

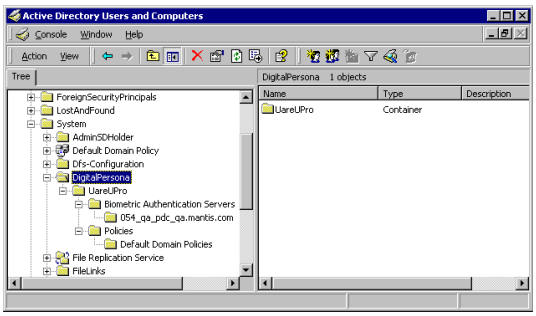
This section describes changes made during the server installation.

Active Directory Containers

The DigitalPersona Pro Server installs subcontainers in the System container of Active Directory. They contain information administrators can use to verify DigitalPersona Pro Server installation and to administer it.

The two containers are the Policies container and the Biometric Authentication Servers container.

Containers added to the System container by DigitalPersona Pro Server



The Policies container—located under **[domain name]**/`System/DigitalPersona/UareUPro/Policies`—contains all the Policy Objects created for use with DigitalPersona Pro, as described in "Administering DigitalPersona Pro" on page 33.

The Biometric Authentication Servers container provides the class name of the Server.

In addition to these containers, the following data is added to the Service container:

- Service Configuration Container Name, set to Biometric Authentication Server.
- Service Version Object Name, set to basVersion.

Published Information

DigitalPersona Pro Server publishes its service using the following properties:

- Service Class Name, set to Biometric Authentication Service.
- Service Class GUID, set to {EFE03FEC-2A6C-4DFB-9B56-E3BC77F32D7F}.
- Vendor Name, set to DigitalPersona.
- Product Name, set to UareUPro.
- Product GUID, set to {48F74E29-1CC0-468F-A0A0-8236628A5170}.
- Authentication Server Object Name, the DNS name of the host computer.

- Service Principal Name, a unique name identifying the instance of a service for a client.
- Schema Version Number, the version of the Active Directory schema extension.
- Product Version Number, the version of DigitalPersona Pro Server software.
- Product Version High, set to 1.
- Product Version Low, set to 0.
- Keywords for searching the server are Service Class GUID, Vendor Name, Product Name and Product GUID. The keyword values are the same as the property values listed in this section.

The Server publishes its service in compliance with the Active Directory Service Connection Point specifications.

DNS Registration

DigitalPersona Pro Server is registered in the DNS in compliance with Microsoft NetLogon service and uses the service name, _uareupro.

The format of the DNS resource records for DigitalPersona Pro Server is:

- `_uareupro._tcp.[domain] 600 IN SRV 0 100 0 [server name]`
- `_uareupro._tcp.[site name]._sites.[domain] 600 IN SRV 0 100 0 [server name]`

Pro Server calculates site coverage based on availability of other DigitalPersona Pro Servers on the domain—as well as sites configured for the domain—and then registers SRV RRs for the domain and sites it covers.

Manual Registration

After running the Pro Server setup, the administrator can manually register a Pro Server by entering the DNS resource records in the format shown above.

Note

You can view the default values of settings created during Pro Server setup by opening U.are.UPro.DNS in Notepad. It is located in the DigitalPersona\bin folder under the Program Files folder.

To manually register a Pro Server

1 Open the DNS console and click on the Forward Lookup Zone.
2 Right-click on `[domainname]`, and select Other New Records in the context menu.
3 In the Resource Record Type dialog box, click on Service Location, and then click the Create Record button.
4 In the New Resource Record dialog, apply the following values:
   - Service: `_uareupro`
   - Weight: `100`
   - Port Number: `0`
   - Host offering this service: `domaincomputername.domainname.com`
5 Click OK.This returns you to the main DNS console window.
6 Under the same `[domainname]`, click on the _sites key.
7 Right-click on Default-First-Site-Name and select Other New Records from the context menu.
8 Repeat steps 3 through 5.

Improve Performance

The Priority and Weight settings can be modified to achieve better response time and load-balancing on the _uareupro.Properties dialog box, which is accessible by double-clicking _uareupro in the DNS Console.

The _uareupro SRV RRs can be found in the following paths in the DNS Console:

- DNS/**[DNS server]**/Forward Lookup Zones/**[domain]**/_tcp
- DNS/**[DNS server]**/Forward Lookup Zones/**[domain]**/sites/**[site name]**/_tcp

If your DNS does not support dynamic registration, you will have to add these SRV RRs manually. For your convenience, these entries are stored in a file, UareUPro.DNS, which is located in the folder in which you installed DigitalPersona Pro Server.

Warning

If the SRV RRs are not added, the DigitalPersona Pro Workstation will not be able to find the Servers and will perform fingerprint registration and authentication locally.

Configuring DNS Dynamic Registration

Administrators of networks and local computers can configure if and where the fingerprint authentication service will update the DNS resource records, assuming that the DNS Server supports automatic registration.

Automatic Registration

The Pro Server automatically registers itself in the DNS server if allowed to do so in the GPO.

- Value: `"UseDynamicDns"`
- Type: `REG_DWORD`
- Default: `enable`

Automatic registration occurs every time DigitalPersona Pro Server starts. Registration is automatically refreshed at specified intervals. Registration is removed every time DigitalPersona Pro Server stops.

Note

When DigitalPersona Pro Server unregisters itself, it removes only the records it has created during automatic registration. Records entered by the administrator will be unaffected.

Warning

When DigitalPersona Pro Server updates the DNS records, it first removes all its records before registering itself again according to the current GPO settings. In the case where there is only one Pro Server covering the site for load-balancing, there is a very brief period (a few milliseconds) during which there are no server records in the DNS server. If DigitalPersona Pro Workstation attempts to locate a Pro Server during that period, it will not find

the server. It will perform fingerprint registration and authentication locally, until the computer refreshes its Pro Server cached information the next time it performs registration or authentication, or every two hours at a minimum.

Automatic registration is always performed on the DNS server covering the site to which the Pro Server belongs. In addition, the following configurations are available using GPO settings.

Description	Value	Type	Default
A Pro Server record is added to the domain where the server resides if enabled in the GPO.	"UseDomainRecord"	REG_DWORD	enable
Pro Server calculates site coverage automatically and adds itself to all sites if enabled in the GPO.	"AutoSiteCoverage"	REG_DWORD	disable
Pro Server adds itself to the sites specified in the GPO.	"SiteCoverage"	REG__SZ	empty
Pro Server updates the DNS registration every time it starts and after the interval defined in the GPO. The use of refresh intervals occurs when site coverage is calculated automatically. In this case, changes in the site structure, site costs and addition/ deletion of Pro Servers will be addressed automatically, at every fresh interval.	"DnsRefreshInterval"	REG_DWORD	30 mins

Administering DigitalPersona Pro 4

This chapter provides an overview of DigitalPersona Pro administration for administrators of an Active Directory network. In addition, administration instructions are provided for local administrators of DigitalPersona Pro Workstations. Whether you are administering an entire network or a single computer, you should read the entire chapter.

Administration Overview

Domain administrators use Group Policy Objects (GPO) in Active Directory to administer DigitalPersona Pro. To import DigitalPersona Pro policies, the DigitalPersona Pro Administrative Template is added to a GPO using the Group Policy Editor, where the settings can then be modified. The GPO is then linked to one or more of the three Active Directory containers (domains, sites and Organizational Units) to apply these settings to users and computers, as appropriate.

A local administrator of a DigitalPersona Pro Workstation also uses the DigitalPersona Pro Administrative Template, but adds it to a local computer policy object using the Microsoft Management Console (MMC), where DigitalPersona Pro settings for that computer can be modified.

Implementing DigitalPersona Pro Policies

Policy configuration will vary from network to network and recommendations are beyond the scope of this guide. Refer to Microsoft documentation on GPO configuration for more information. A few rules to remember when configuring DigitalPersona Pro GPOs include:

- If a GPO setting is not configured, the default value set in the software is used.
- The value of a child GPO setting is ignored when the same setting in the parent is not configured.
- If a parent GPO has a value for a setting and the child does not, the parent setting is used.
- If a parent GPO has a value for a setting and the child has the same value for that setting, that setting is used.

- If a parent GPO has a value for a setting and the child GPO has a conflicting value for that setting, the setting in the child is used.

In addition, there are some guidelines when linking GPOs to containers:

- GPOs can only be applied to the three Active Directory containers: sites, domains and Organizational Units; not users or computers.
- A single GPO can be applied to one or more containers.
- A GPO affects all users and computers in the container—and subcontainers—it is applied to.

Network configuration varies widely among corporations, but some guidelines for structuring Organizational Units are provided.

Grouping user and computer permissions and authentication policies and placement of the DigitalPersona Pro GPOs are the two key factors in structuring your network.

For example, if users and computers can be grouped according to authentication policies, you would group them into separate Organizational Units and set specific GPOs for each. When authentication policies within Organizational Units vary, as they often do among department heads and subordinates, then you would group those users and computers into a child Organization Unit.

Structuring your Organizational Units based on authentication policies when possible is the easiest way to administer DigitalPersona Pro. You should plan your network structure by identifying the settings you intend to configure and determining whether to apply the settings to users and computers in a site or domain, or just to users and computers in an Organizational Unit. Then, create the Organizational Units required to implement your design and add the respective users and computers to them.

Changing GPO Settings

To make changes to GPO settings, domain administrators make changes to the GPO settings using the Group Policy Editor, and local administrators can use MMC.

On the network, by default, changes made to existing GPOs may take as long as 90 minutes to refresh with a 30 minute offset. GPOs applied to computers are refreshed during this time, as well as when the computer is restarted. GPOs applied to users are refreshed every 90 minutes and when the user logs on or off. You can use the standard Windows methods of enforcing refresh of DigitalPersona Pro GPOs without concern for disrupting DigitalPersona Pro functionality on a computer.

Adding DigitalPersona Pro Administrative Templates

If you are a domain administrator, add the DigitalPersona Pro Administrative Template to a GPO using the Group Policy Editor, which is accessible from several Active Directory administrative tools, for example, Active Directory for Users and Computers.

There are three .adm files to install:

- DigitalPersonaProWks.adm should be added in GPO (including local GPO) for computers running Windows 2003, 2000 and XP, and DigitalPersona Pro Workstation version 3.2.
- DigitalPersonaProSvr.adm should be added in GPO for Domain Controllers for DigitalPersona Pro Server version 3.2.

Note

DigitalPersonaPro98-NT.adm should be added in GPO (including local GPO) for computers running Windows 2003, 2000 and XP, and DigitalPersona Pro Workstation version 3.1 and earlier, and also for all computers running Windows NT 4.0, 98 and Me and versions of DigitalPersona Pro Workstation from 3.0 and up.

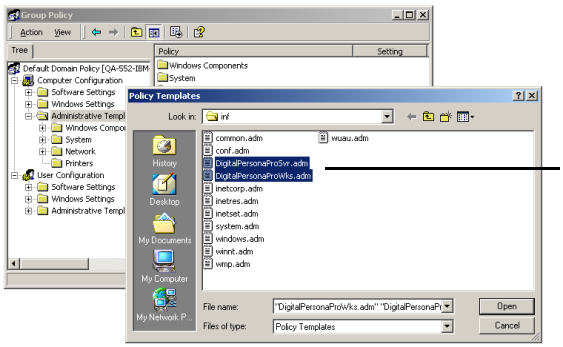
Note

Windows 98/Me administrators should skip this section and proceed to "Administering Pro Workstation on Windows 98 and Me" on page 54.

The ADM files, DigitalPersonaProSrv.adm and DigitalPersonaProWks.adm, must be added to the Computer Configuration folder, which is located in the Administrative Templates folder in the Group Policy Editor tree. The ADM files are located on the hard drive on which the operating system is installed. The folder path is:

`%system root%\inf\`

When the ADM files are added, a DigitalPersona Pro folder is listed in `Computer Configuration/Administrative Templates`.



Import the DigitalPersona Pro ADM files to add Pro settings to Active Directory

For every GPO you create, you must add the ADM files to incorporate DigitalPersona Pro settings and functionality.

When you add the ADM files to a GPO, you can use the Group Policy Editor to modify DigitalPersona Pro settings, as described in “Configuring DigitalPersona Pro Settings” on page 38.

Local DigitalPersona Pro Workstation administrators must create a local computer policy on the computer and add the DigitalPersona Pro ADM files using MMC.

To create a local computer policy object and add the Pro ADM files with MMC

1 On the Start menu, click Run. Type `MMC` and press Enter to launch the Microsoft Management Console.

2 On the Add/Remove Snap-in dialog box, click Add to open the Add Standalone Snap-in dialog box.
3 Locate and select the Group Policy item listed in the Available Standalone Snap-ins table and then click Add.
4 Accept the default setting of Local Computer in the Group Policy Object text box by clicking Finish.
5 Click Close on the Add Standalone Snap-in dialog box, then click OK on the Add/Remove Snap-in dialog box to add the local computer policy object.
6 To add the DigitalPersona ProWks.adm file to the local computer policy object, display the Administrative Templates folder by clicking the plus sign next to Local Computer Policy and then Computer Configuration.
7 Click Add/Remove Templates on the Administrative Templates folder context menu.
8 Click the Add button on the Add/Remove Templates dialog box and then locate and select the DigitalPersonaPro ADM file located in the following path:
`%system root%\inf`
9 Click Close.

The DigitalPersona Pro Administrative Template is added to both Administrative Templates folders in the Computer Configuration and User Configuration trees and the settings are accessible from the Setting table.

DigitalPersona Pro settings can be accessed in the Group Policy Editor and MMC by clicking Properties on the context menu of each setting and then clicking the Policy tab on the Properties dialog box.

For a description of each setting, refer to "Configuring DigitalPersona Pro Settings" on page 38.

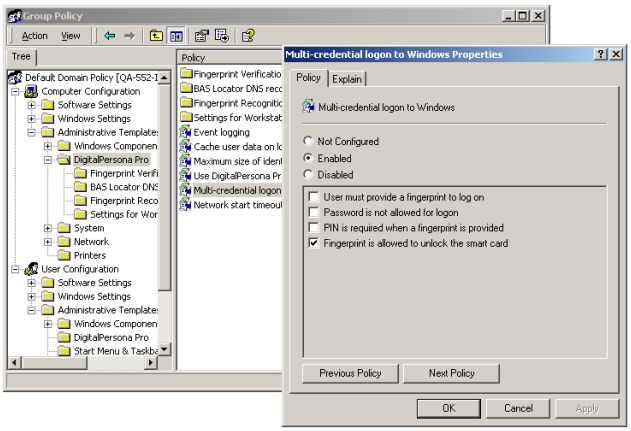
Note
If you are upgrading from a previous version and you added the Administrative Templates without uninstalling, you will see an additional folder for the most recent BAS Locator settings. Always apply your changes to the latest version of the settings.

Configuring DigitalPersona Pro Settings

GPO settings have three states: enabled, disabled and not configured. By default, all settings are not configured. To override the default settings of DigitalPersona Pro, each setting must be changed to enabled or disabled and, in some cases, additional parameters must be supplied.

All computer policy settings are accessible to domain administrators in the Group Policy Editor tree from the path:

`Computer Configuration/Administrative Templates/DigitalPersona Pro`



For local administrators, the path is the same, but is instead accessible from MMC, as described in “Adding DigitalPersona Pro Administrative Templates” on page 35.

DigitalPersona Pro Settings

Following are descriptions of the function of each setting and its configuration options.

Fingerprint Management

The following fingerprint management settings are included in the server and workstation templates.

False Accept Rate Used in Fingerprint Verification

This setting specifies the False Accept Rate for fingerprint verification. The False Accept Rate (FAR) is the mathematical probability (1:*n*) of two different fingerprints being falsely matched.

Note

To estimate the likelihood of false rejects and false accepts, DigitalPersona recommends following the guidelines described in "Best Practices in Testing and Reporting Performance of Biometric Devices: Version 2.01," by A. J. Mansfield and J. L. Wayman, NPL Report CMSC 14/02, 2002, defining a transaction as three verification attempts and assuming a single comparison of a verification template against a single registration template. False Reject Rates and False Accept Rates are only probabilistic estimates and not indicators of actual performance in a given deployment. Visit the DigitalPersona Web site (http://www.digitalpersona.com) for more information.

The value of *n*, which is specified in the Value: (one in) text box, indicates the likelihood of false fingerprint verification. The higher the value of *n*, the less likely a fingerprint will be falsely accepted as verified. For example, setting *n* to 10,000 indicates that it is probable that one in every 10,000 fingers will be falsely accepted as verified; setting *n* to 100,000 sets the probability to one in 100,000.

Particularly high values of *n* may cause false rejection of fingerprints from the same finger.

If this setting is not configured, the default value of one in 100,000 is used. The maximum value for *n* is one in 1,000,000; the minimum is one in 1,000. 1,000, 10,000 and 100,000 are the only values available to Windows 98, Me and NT users.

Maximum Number of Fingerprints

This setting determines the maximum number of fingers that a user can register. The value for this setting specified in the Maximum Number of Fingerprints Per User text box influences both the speed of authentication and the probability of false accepts. For example, the more fingerprints a user registers, 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 register a maximum of two fingers.

The maximum and default value is ten registered fingers. The minimum value is zero.

Failed Logon Account Lockout

This setting specifies that the user account is locked after a specified number of failed fingerprint validation attempts. The DigitalPersona Pro account lockout does not affect the Microsoft account lockout and is managed separately. For users to log on by fingerprint, both lockout settings must be unlocked. If users are only locked out from using fingerprints, they can still log on to Windows by typing their passwords.

To unlock a locked user account, see "Unlocking Accounts after Failed Logon Attempts" on page 51.

Note

If a lockout policy is applied on the domain, users must type their user names when logging in to specify which account to use because the identification list cannot be accessed.

The following table describes the settings.

Setting	Description	Default Value
Account lockout duration	Length of time account is locked until user can attempt to log on again	30 minutes
Account lockout threshold	Number of failed attempts allowed before the account is locked	0 (do not lock out)
Reset account lockout counter after	Length of time for counter to track number of failed attempts	5 minutes

Each Authentication Server in the domain maintains individual lockout counters per user account. When an account is locked out due to failed fingerprint attempts, the following occurs:

- The Logon dialog displays the account locked out message.
- The locked account information is replicated during the next replication interval in Active Directory.
- A record is added to the DigitalPersona Pro event log.

Computers do not lock out cached accounts of the domain users inside the user session. For instance, when accessing the One Touch Menu, the fingerprint is validated against cached information and not on the server.

XTF Templates

This setting determines whether the Extended Template Format (XTF) or Basic Template Format (BTF) is used for fingerprint registration templates. XTF is the default template format. XTF provides improved recognition performance, especially for users with poor quality fingerprints. BTF template size is less than 550 bytes, and XTF template size is about 1.5 kb. XTF is recommended. If you have space constraints, then BTF can be used. If enabled, BTF is used. If not configured, XTF is used.

Fingerprint Logon to Windows 2000, XP and Server 2003

The following logon credentials settings are included in the workstation Administrative Template.

Multi-credential Logon to Windows

The logon settings determine the credentials required to log on to Windows. The default settings allow a fingerprint or a password or a smart card for logon. The following is the list of settings in DigitalPersona Pro for logon to Windows XP and 2000:

- **User must provide a fingerprint to log on**
  The user must verify the fingerprint credential in addition to the Windows authentication (smart card or password according to the Windows policy setting).
- **Password is not allowed for log on**
  The user is not allowed to log on to Windows with the password. In this case, the fingerprint or the smart card, if available, must be used instead.
  When this option is set at the user level, DigitalPersona Pro will randomize the Windows password preventing the specific user to log on with a password from any computer on the network. If the user has administrative privileges, this option is not available.
- **PIN is required when a fingerprint is provided**
  When this option is enabled, the user must provide a PIN code whenever the fingerprint is used to log on, to unlock the computer or to change the Windows password. The fingerprint PIN option provides additional security to the logon with the fingerprint. See “Using Fingerprint PINs” on page 103.
- **Fingerprint is allowed to unlock the smart card**
  When this option is enabled, the user can use the fingerprint to unlock the smart card instead of typing the PIN for the smart card.

Fingerprint Logon to Windows 98 or Me or NT

When enabled, one of four authentication policies can be applied by clicking the policy on the “Windows Logon Authentication Policy” drop-down menu. Below

is a list of each policy as they appear on the menu, followed by a description of their function:

- **Fingerprint or Password.** Allows the user to provide either a registered fingerprint or a password—but not both—to log on to the computer.
- **Fingerprint only.** Requires the user to provide a registered fingerprint to log on. The user cannot use their password.
- **Password only.** The user must use their password to log on; they cannot use any registered fingers.
- **Fingerprint and Password.** Requires the user to provide both a registered fingerprint and a password to log on.

If the setting is not configured, the default policy is "Fingerprint or Password."

Cache Domain User Data on Local Computer

This setting determines if domain user credentials are cached on DigitalPersona Pro Workstations. When enabled, domain users can log on to Windows using cached credentials when the computer is disconnected from the network or the Pro Server is unavailable. You can select the Store user data on computer check box.

Note

In a network with DigitalPersona Pro Server deployed, if a domain user is disconnected from the network or Pro Server is unavailable, any changes to credentials and application data will be lost when the computer is reconnected to a Pro Server.

Warning

If cached credentials are disabled and the logon policy is "Fingerprint only" or "Fingerprint and Password" (as described in "Multi-credential Logon to Windows" on page 42), the user will not be able to log on to the computer if it is disconnected from the network.

If this setting is not configured, cached credentials are enabled by default. Windows 98 and Me users must select “yes” or “no” to indicate whether the cache is enabled or disabled.

If not selected, domain users may only use fingerprints when the Authentication server is available which might be slower but provides higher security. If selected, user data is cached locally on the computer. In this case, users can continue to work on the computer if the network is disconnected, but it is less secure.

Refer to “Cached Credentials” on page 11 for more information on cached credentials.

Maximum Size of Identification List

You can specify the maximum number of users the identification list can hold on a particular computer. Type the number of users in the Maximum size of identification list text box. While the number of credentials that can be cached is virtually unlimited, the maximum number of users that can be added to the identification list is 20; the minimum is 0. If this setting is not configured, the default value of 5 is used.

Refer to “Identification List” on page 11 for more information about the identification list.

Warning

When setting the logon policy for Pro Workstations, be aware of the following:

- Certain combinations policy settings may temporarily prevent a user from logging on to their computer if the “Fingerprint only” and “Fingerprint and Password” policy are applied.
- Do not select a logon authentication policy requiring the user to type a password if password randomization has been enabled for that user.

If cached credentials are disabled and the logon policy is “Fingerprint only” or “Fingerprint and Password” the user will not be able to log on to the computer if it is disconnected from the network.

Server Connection Settings

The following server connections settings are included in the workstation Administrative Template.

Use Remote Authentication Server

The Use Remote Authentication Server setting determines whether DigitalPersona Pro Workstation will use DigitalPersona Pro Server for fingerprint registration and authentication or perform these operations locally instead.

When enabled, Pro Workstation will look for an available Pro Server for authentication. If disabled, Pro Workstation will always perform authentication locally, whether a Pro Server is accessible or not. If this setting is not configured, the Pro Server is always used for authentication. Windows 98 and Me users must select “yes” or “no” on the drop-down menu to use this setting.

Network Start Timeout

This setting specifies the amount of time in milliseconds a computer will wait for an IP address assignment from the network. In most cases, this is not necessary and the value can be set to 0; however, in situations where a computer or network may be slow to respond, increase the wait time to compensate.

Note
This setting is not available to Windows 98/Me users.

The number of milliseconds is specified in the Network Start Timeout (milliseconds) text box. The maximum amount is 120,000 milliseconds. If not configured, the default value of 0 is used.

Biometric Authentication Service (BAS) Locator

BAS Locator settings allow registration of Biometric Authentication Service (BAS) Locator DNS records. These DNS records are dynamically registered by BAS and are used by DigitalPersona Pro Workstation to locate BAS. The

following BAS Locator settings are included in the server Administrative Template.

Dynamic Registration of BAS Locator DNS Records

This setting determines if BAS performs dynamic registration of Biometric Authentication Service (BAS) Locator DNS resource records. If you enable this setting, computers to which this setting is applied dynamically register BAS Locator DNS resource records through dynamic DNS update-enabled network connections. If you disable this setting, computers will not register BAS Locator DNS resource records. If this setting is not configured, computers will dynamically register BAS Locator DNS resource records.

Refresh Interval of BAS Locator DNS Records

This setting specifies the Refresh interval of Biometric Authentication Service (BAS) Locator DNS resource records for computers to which this setting is applied. These DNS records are dynamically registered by BAS and are used by DigitalPersona Pro Workstation to locate BAS. This setting may be applied only to computers using dynamic update. Computers configured to perform dynamic registration of BAS Locator DNS resource records periodically reregister their records with DNS servers, even if their records' data has not changed. If authoritative DNS servers are configured to perform scavenging of the stale records, this reregistration is required to instruct the DNS servers configured to automatically remove stale records that these records are current and should be preserved in the database.

Warning

If the DNS resource records are registered in zones with scavenging enabled, the value of this setting should never be longer than the Refresh Interval configured for these zones. Setting the Refresh interval of BAS Locator DNS records to longer than the Refresh interval of the DNS zones may result in unwanted deletion of DNS resource records.

To specify the Refresh interval of BAS records, select Enabled, and then specify a value larger than 1800. This value specifies the Refresh Interval of BAS

records in seconds. For example, the value 3600 is 60 minutes. If this setting is not configured, computers use default value of 1800 seconds.

Weight Set in BAS Locator DNS SRV Records

This setting specifies the Weight field in the SRV resource records registered by Biometric Authentication Service (BAS) to which this setting is applied. These DNS records are dynamically registered by BAS, and they are used to locate BAS. The Weight field in the SRV record can be used in addition to the Priority value to provide a load-balancing mechanism where multiple servers are specified in the SRV records Target field and set to the same priority. The probability with which the DNS client randomly selects the target host to be contacted is proportional to the Weight field value in the SRV record. To specify the Weight in the BAS Locator DNS SRV records, select Enabled, and then specify a value. The range of values is 0 to 65535. If this setting is not configured, computers use a default weight of 100.

Priority Set in BAS Locator DNS SRV Records

This setting specifies the Priority field in the SRV resource records registered by Biometric Authentication Service (BAS) to which this setting is applied. These DNS records are dynamically registered by BAS and are used by DigitalPersona Pro Workstation to locate BAS. The Priority field in the SRV record sets the preference for target hosts specified in the SRV record Target field. DNS clients that query for SRV resource records attempt to contact the first reachable host with the lowest priority number listed. To specify the Priority in the BAS Locator DNS SRV resource records, select Enabled, and then specify a value. The range of values is 0 to 65535. If this setting is not configured computers use default value of 0.

Automated Site Coverage by BAS Locator DNS SRV Records

This setting determines whether Biometric Authentication Service (BAS) will dynamically register BAS Locator site-specific SRV records for the closest sites where no BAS for the same domain exists. These DNS records are dynamically registered by BAS, and they are used by DigitalPersona Pro Workstation to locate BAS. If this setting is enabled, the computers to which this setting is

applied dynamically register BAS Locator site-specific DNS SRV records for the closest sites where no BAS for the same domain exists. If you disable this setting, the computers will not register site-specific BAS Locator DNS SRV records for any other sites but their own. If this setting is not configured, computers will not register site-specific BAS Locator DNS SRV records for any other sites but their own.

Sites Covered by BAS Locator DNS SRV Records

This setting specifies the sites for which the domain Biometric Authentication Service (BAS) register the site-specific BAS Locator DNS SRV resource records. These records are registered in addition to the site-specific SRV records registered for the site where BAS resides, and records registered by a BAS configured to register BAS Locator DNS SRV records for those sites without a BAS that are closest to it. The BAS Locator DNS records are dynamically registered by BAS, and they are used to locate BAS. An Active Directory site is one or more well-connected TCP/IP subnets that allow administrators to configure Active Directory access and replication. To specify the sites covered by the BAS Locator DNS SRV records, select Enabled, and then specify the sites names in a space-delimited format. The site names have the following format, in which the <site name> component must be present and the <priority> and <weight> components are optional. The <priority> and <weight> components must be a numeric string value. <site name>:<priority>:<weight>

If this setting is not configured, no site-specific SRV records will be registered.

Register BAS Locator DNS SRV Record for Domain

This setting determines whether Biometric Authentication Service (BAS) will dynamically register BAS Locator domain-specific SRV record for the domain it belongs to. The DNS records are dynamically registered by BAS, and they are used by DigitalPersona Pro Workstation to locate BAS. If this setting is enabled, the computers to which this setting is applied dynamically register BAS Locator domain-specific DNS SRV records. If you disable this setting, computers will not register the domain-specific BAS Locator DNS SRV records for the domain they belong to and register only site-specific records. If this setting is not

configured, computers will register domain-specific BAS Locator DNS SRV records for the domain they belong to.

Log Events

This setting enables DigitalPersona Pro Server and Workstation event logging in the Windows Event Log. Windows event logging must also be enabled to use this setting. Logged events are accessible from the Windows Event Viewer. This setting in included in the server and workstation Administrative Templates.

If this setting is not configured, DigitalPersona Pro events are logged in the Windows Event Log.

For information on how events are logged and a detailed description of each event, refer to “Event Log Specifications” on page 131.

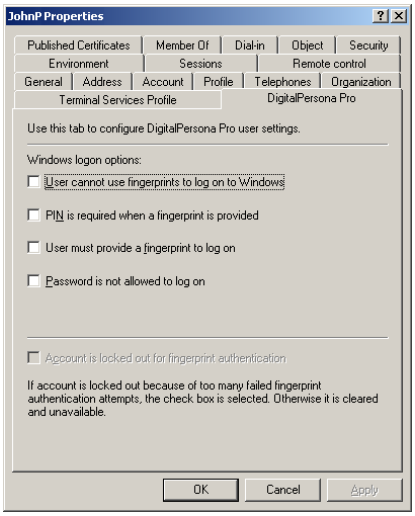
One Touch SignOn

One Touch SignOn settings are described in “Configuring One Touch SignOn” on page 75. One Touch SignOn settings are included in the workstation Administrative Template.

DigitalPersona Pro User Properties in Active Directory

Installation of DigitalPersona Pro Server adds the DigitalPersona Pro tab to the User Properties settings of the Active Directory Users and Computers console. You may want to apply user properties to increase the overall level of security for your network while maintaining flexible options for individual users. For example, you can set a higher multi-credential requirement for all users in an organization, but then, for a particular user who may be having problems with fingerprint registration, you can specify fewer logon credentials in the User Properties. User Properties override the computer policies.

To access these properties, launch the Active Directory Users and Computers console and open the Users folder. Right-click on a specific user name, select Properties and click the DigitalPersona Pro tab. User properties allow you to configure fingerprint logon settings and restore the use of fingerprints for a user after the account has been locked due to failed fingerprint attempts.



Windows Logon Options

These settings at the user level are turned off by default.

- **User cannot use fingerprints to log on to Windows**
  When this option is set, the user will not be subject to any logon policy from DigitalPersona Pro. Users will be able to logon with password or smart card as defined by the Windows logon settings.
- **PIN is required when a fingerprint is provided**
  When this option is enabled, the user must provide a PIN code whenever the fingerprint is used to log on, to unlock the computer or to change Windows password. The fingerprint PIN option provides additional security to the logon with the fingerprint. See “Using Fingerprint PINs” on page 103.
- **User must provide a fingerprint to log on**
  The user must verify the fingerprint credential in addition to the Windows authentication (smart card or password according to the Windows policy setting).

- **Password is not allowed for log on**
  The user is not allowed to log on to Windows with the password. In this case, the fingerprint or the smart card, if available, must be used instead.
  When this option is set, DigitalPersona Pro changes the user password to a random value when you click OK on this dialog box. This prevents the specific user from logging on with a password from any computer on the network, even those where the Pro software is not installed. This setting can be used to enforce a Fingerprint only policy because the user will not know the randomized password and will have to use their fingerprint to log on.

Note
This option is not available for accounts with administrative privileges.

Warning
Do not enable password randomization with incompatible logon authentication policies, such as "Fingerprint and Password," as users will be unable to log on.

Unlocking Accounts after Failed Logon Attempts

You can unlock an account that is locked for fingerprint authentication because the user has reached the failed fingerprint attempts threshold number. You must have permissions to access the user account. When an account is unlocked by an administrator, the account becomes immediately available for fingerprint authentication from all computers, or after the next replication interval if there are multiple domain controllers.

The administrator can choose to set less strict lockout settings by reducing the the lockout duration time or reducing the counter reset time.

To unlock a locked account

1 In Active Directory for Users and Computers, right-click on the user name, and select Properties.
2 Click the DigitalPersona Pro tab.

3 Click the Account is locked out for fingerprint authentication check box to unselect it. This check box is for unlocking accounts and cannot be checked by an administrator to lock an account. If the account is unlocked, the check box is disabled.
4 Click OK to close the dialog box and save the changes.

Deleting Single User Credentials using ADSI Edit Tool

As an alternative method for removing Pro user credential data from Active Directory for a single user, use the ADSI Edit tool, which is included with Windows 2000 and 2003 Server.

To remove individual Pro user credential data from Active Directory with ADSI Edit

1 On the Start menu, point to Programs, Windows 2000 Support Tools, Tools and then click ADSI Edit.
2 In the tree on the ADSI Edit tool, locate the user profile and, on its context menu, click Properties.
3 On the Select a property to view drop-down menu, click dpUserCredentialsData.
4 Click the Clear button to remove the user credential data.

Logging and Auditing

All authentication and user record modification events are logged in the Windows Event Log. You can view which users have accessed networked computers, password-protected applications, Web sites as well as failure to access these items. Logged events show when events occurred. Administrators can view, sort, and export all log events from the Event Viewer. This aids administrators in securing data and networks for meeting compliance requirements for Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA.

For a list of events and the logs that events are stored in, see “Event Log Specifications” on page 131.

Auditing Using the Windows Event Viewer

The Windows Event Viewer is used to view logged DigitalPersona Pro events. In this section, instructions are provided for viewing DigitalPersona Pro event logs, as well as filtering and finding events specific to DigitalPersona Pro.

Filtering DigitalPersona Pro Events in Event Viewer

You can specify a filter that limits the type of information the Event Viewer displays to only DigitalPersona Pro events.

To filter DigitalPersona Pro events in the Event Viewer

1 To launch the Event Viewer, click Start, point to Programs, point to Administrative Tools and then click Event Viewer.
2 In the console tree, right-click the log containing the specific DigitalPersona Pro events you want to view and then click Properties.
3 Click the Filter tab.
4 Use the Filter tab to specify the criteria to filter DigitalPersona Pro events with, such as the event ID and category. Use “DigitalPersona Pro audit” as the event source.
5 Click OK to display the DigitalPersona Pro events matching the criteria you specified in the Event Viewer.

Finding DigitalPersona Pro Events with Event Viewer

You can use the Event Viewer to search for DigitalPersona Pro events. This may be useful when you are viewing large logs.

To find a specific DigitalPersona Pro event

1 Click Start, point to Programs, point to Administrative Tools and then click Event Viewer to launch it.
2 On the View menu, click Find.
3 Type the search criteria (specifying, “DigitalPersona Pro Audit,” as the event source) in the dialog box and click Find Next.
The events matching the search criteria you specified are displayed in the Event Viewer.
4 Click Close when you are finished.

Notes for Windows 98 and Me Computers

The following sections apply to Windows 98 and Windows Me computers only.

Administering Pro Workstation on Windows 98 and Me

DigitalPersona Pro running on Windows 98 or Me is administered from the System Policy Editor. It is available as a download from the Microsoft Web site and is also located on the Windows 98 and Me installation CDs. The name of the file is, "poledit98." A copy of this file can be found on the DigitalPersona Pro for Workstation CD in the folder:

`Redistr\Poledit for Win98`.

To add the DigitalPersona Pro Administration Template to the System Policy Editor

1 Launch the System Policy Editor and, on the Options menu, click Policy Template.
2 On the Policy Template Options dialog box, click the Add button.
3 Use the Open Template File dialog box to locate and select the file, "DigitalPersonaPro98-NT.adm," which is located in the Windows INF folder.
4 When the file is added to the Current Policy Template(s) table, click OK.

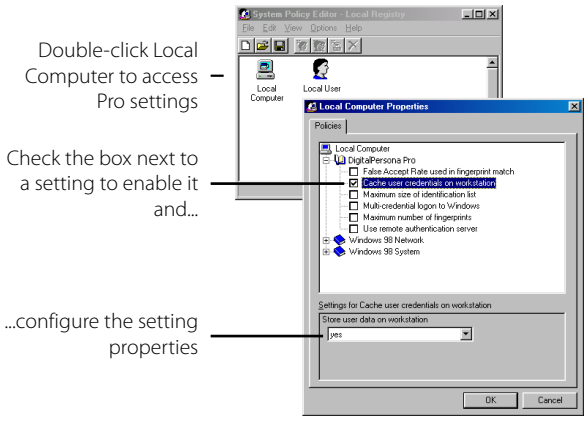
You can now configure DigitalPersona Pro settings, as described in "Configuring Settings on Local Computers" on page 54.

Configuring Settings on Local Computers

Windows 98/Me users configure Pro settings using the System Policy Editor.

To configure DigitalPersona Pro settings using the System Policy Editor on Windows 98/Me

1 Launch the System Policy Editor and, on the File menu, click Open Registry.
2 Double-click the Local Computer icon to open the Local Computer Properties dialog box.
3 Click the plus sign next to DigitalPersona Pro to display all of the DigitalPersona Pro settings.
4 To configure a setting, click its name and use the controls on the area below the tree.



Proceed to “Configuring DigitalPersona Pro Settings” on page 38 for more information about each setting.

Configuring Settings on Remote Computers

You can also apply DigitalPersona Pro settings to a domain of Windows 98/Me computers using poledit98 on the Windows 2000 domain server by performing the following steps:

- Require all Windows 98 and Me computers to validate from the network before logging on.
- Create a policy file using poledit98 and the DigitalPersona Pro Administrative Template file.
- Place the policy file on the Windows 2000 domain server to enforce policy settings.

You can require Windows 98 and Me computers on a Windows 2000 domain to validate from the network before logging on using poledit98.

To use poledit98 to modify Windows 98/Me computer domain logon properties

1 Launch poledit98 on the Windows 2000 domain server and, on the File menu, click Open Registry.
2 Double-click Local Computer.

3 On the Local Computer Properties dialog box, navigate to Windows 98 Network, and then select Logon and then select the Require validation from network for Windows access checkbox.

Note
Windows 98 and Me users will not be able to log on using the Default user when this option is enabled.

4 Click OK to close the dialog box and then click Save to save your changes.

Next, you must create a policy file using poledit98 following the same instructions provided in "Administering Pro Workstation on Windows 98 and Me" on page 54. You must then configure the policy, as described in "Configuring Settings on Local Computers" on page 54.

Finally, to enforce the policy settings on the Windows 98 and Me computers, locate the config.pol file and move it to the NETLOGON folder on the Windows 2000 domain server.

Using Administration Tools 5

This chapter describes administration tools that can be used to implement higher security and more control over deployment. It describes how to set up and deploy One Touch SignOn templates to manage Web site and program access. Additionally, it describes how to implement attended registration for users. Administration tools are installed separately by running the setup.exe in the Administration Tools folder on the DigitalPersona Pro Workstation CD.

Using DigitalPersona Pro Workstation for Administrator Tasks

For server implementations where a higher level of administrative maintenance is required, you can install DigitalPersona Pro Workstation and the DigitalPersona Pro Administration Tools on a computer to do the following:

- Implement fingerprint logon for Web sites and programs using One Touch SignOn.
- Register users by attended fingerprint registration.

One Touch SignOn

One Touch SignOn allows administrators to control access to a Web site or program by adding fingerprint authentication to logon screens while simplifying logon for the end users. The administrator specifies the attributes for the logon screen in a template, such as the user name, password, the submit button and other fields. The administrator can also automate the process of changing passwords, by adding the attributes of the change password screen to the template for the Web site or program.

Templates contain the specifications for a logon screen and a change password screen for a particular Web site or program. Templates are stored in folders, called containers in the One Touch SignOn Administration Tool, and are deployed to DigitalPersona Pro Workstations using the One Touch SignOn Group Policy Object or any other file deployment tool.

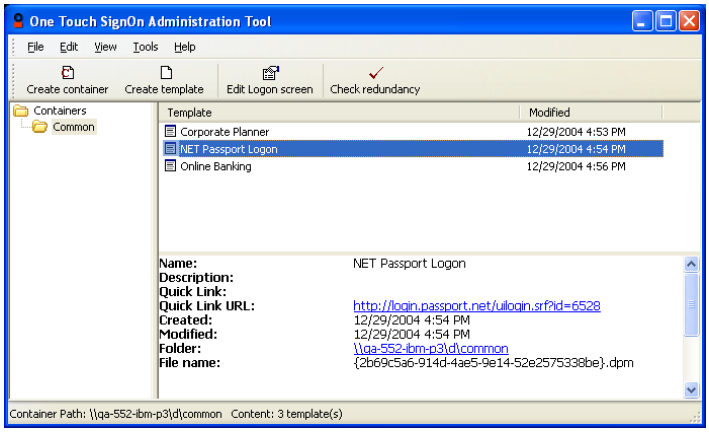
After templates are deployed to a computer, One Touch SignOn recognizes that logon or change password screens are fingerprint-enabled by using the attributes specified in the templates. Then, a DigitalPersona icon appears on the Web site

or program title bar indicating that the user can log on by fingerprint. The user is guided through the process of logging on or changing the password with One Touch SignOn. Depending on the settings applied by the administrator, the user may be prompted for account data, such as user name, password, and other information during the first logon. After the first logon, the account data is provided by One Touch SignOn after the user identity is confirmed with a fingerprint.

The One Touch SignOn Administration Tool is used to create and manage the templates for password-protected Web sites and programs.

Setting Up Logon Screens with One Touch SignOn

The One Touch SignOn Administration Tool is used to create templates for logon screens which are shared by multiple users. One Touch SignOn Administration Tool also allows you to provide specifications for change password screens. By setting up a change password screen with the One Touch SignOn Administration Tool, you can automate the process of changing passwords and shield password information from users.



The following summarizes the steps for setting up a template for a logon screen:

- **Launch the One Touch SignOn Administration Tool.** To launch the One Touch SignOn Administration Tool, from the Start menu, point to Programs (or All Programs), DigitalPersona Pro and then click One Touch SignOn Administration Tool.
- **Create a container.** You must create a container, or use an existing one, to store the templates. Creating a container in the One Touch SignOn Administration Tool requires that you specify a folder on a network drive.
- **Create a template.** Browse to a Web site or launch a program that you want to specify a logon screen for. The One Touch SignOn Wizard guides you through the process of specifying logon screen attributes. Instructions are provided in Creating Templates. To expedite the process of creating templates, use the Field Catalog to store and retrieve recurring logon fields.

To deploy templates through Active Directory, and make them accessible to DigitalPersona Pro users, see "Deploying One Touch SignOn Templates" on page 77.

Note

Other file deployment methods can be used. However, this guide provides only instructions for using GPO settings and the Group Policy Editor.

Creating Containers

In the One Touch SignOn Administration Tool, you use containers to organize your OTS templates. Containers are associated with Windows folders on a network drive. When you create a container, you specify a path to a folder on a shared network drive where the templates will be stored. You must create at least one container before you can create OTS templates.

To create a new container in the One Touch SignOn Administration Tool

1. In the One Touch SignOn Administration Tool, click Create Container on the toolbar to display the New Container dialog box.
2. Type a name for the container in the Name text box and specify the path of a folder on a shared network drive in the Path text box. The template files will

be stored in this folder. To specify a path using the standard Windows file browser dialog box, click the Browse button.

3 Click OK to create the container.

When a container is created, you can add templates for a logon screen and a change password screen. For more information, see "Creating Templates" on page 61 and "Adding Change Password Screens to Templates" on page 69.

Editing Containers

You can rename a container. You cannot change the folder associated with a container. If you must change the container folder, delete the container and create a new one.

To edit the name of container

1 Click Properties on the context menu of the container.
2 Type a new name.
3 Click OK.

Deleting Containers

You can delete containers in the One Touch SignOn Administration Tool. When you delete a container, the container and all templates in the container are removed from the One Touch SignOn Administration Tool. However, the folder associated with the container is not removed. When you delete a container, you can choose whether or not to delete the template files in the folder.

To delete a container

1 Click the container to delete.
2 Select Delete Container from the context menu or press the Delete key.
3 You are prompted to confirm that you want to delete the container. If you also want to delete all the templates in the Windows folder used for the container, click the Delete all templates in the selected container check box, and click Yes.

Note

If you delete a container and its templates, you must either update the corresponding One Touch SignOn GPO by pointing to a new container or delete the GPO.

Creating Templates

The Logon Screen Wizard helps you to create templates for logon screens. Open the logon screen for a Web site or program, and then click Create template in the One Touch SignOn Administration Tool. The Logon Screen Wizard launches. The wizard detects the fields on the logon screen. You can specify which fields are required for logon and what type of information should be provided in the fields.

For logon screens that are difficult for the wizard to detect automatically, you can create a template manually. When you create a template manually, you have additional controls for specifying fields and keystrokes required for logon. It is recommended to attempt to create templates automatically before creating templates manually. See "Creating Templates Manually" on page 65 for more information.

You can also add change password screens to templates as described in "Adding Change Password Screens to Templates" on page 69.

To set up a logon screen with One Touch SignOn

1 Launch the password-protected Web site or program and go to the logon screen for which you want to create a template.
2 In the One Touch SignOn Administration Tool, select the container you want to add a template to and then click Create template on the toolbar.
3 When the One Touch SignOn Logon Screen Wizard launches, confirm that the title of the logon screen is accurately displayed on the first page. Then click Next.
4 When you click Next, the Logon Fields page displays all the fields on the logon screen, using the nearest label to identify each field. On this page, indicate which fields are required for logon, as well as several other attributes, which are described below:
   - **Use.** Check the Use check box for each field used for log on. Some fields discovered by the wizard may not be relevant to log on, such as a search field on a Web site logon page. Leave these unchecked.

- **Label.** If the label for a field is not intuitively related to the corresponding field on the logon screen, type a new label name in this field. The labels are displayed when users are prompted to type a value for a logon field.
- **Type.** The type of field, either text or password, is displayed in the Type text box. This value is not editable. Password hides the password on the logon screen so it cannot be viewed. Text displays readable text.
- **Catalog.** For added convenience, you can create specifications for frequently used fields using the Field Catalog Editor. If the field is in the Field Catalog, you can click and then choose it from the drop-down list. Its specifications will be provided automatically by One Touch SignOn.
- **Value.** Type a value for the logon field or use the Value drop-down menu to indicate a value specified by the user or provided by One Touch SignOn.

Note
If you type a value for the logon field, it is stored in the template in clear (unencrypted) text and is shared by all users using the template.

There are several options on the Value drop-down menu, which allow you to specify values that must be provided by the user or by One Touch SignOn. The first three options can be used if you require the user to provide information at logon:

- **Ask-Reuse** prompts the user to enter a value for a logon field the first time they use the template for logon. This value is automatically submitted for them on each subsequent logon without prompting the user again.
- **Ask-Confirm** also prompts the user to enter a value for a logon field the first time they use it. However, on subsequent logons, the value is automatically entered and they are then prompted to confirm this value or change it.
- **Ask Always** prompts the user to enter a value for a logon field each time they use the template.

For a text field, the next options allow you to specify values which are provided by One Touch SignOn:

- **Windows User Name** provides the Windows user name.

- **Windows User Principal Name** provides the user name and domain values in UPN format: [user name]@[domain]
- **Windows Domain\User Name** provides the domain of the user, followed by a backslash and the user name.
- **Windows Domain** provides the user domain name.
- **Windows E-mail Address** provides the email address stored in Active Directory for the user.

For a password field, you can specify the following value which is provided by One Touch SignOn:

- **Windows User Password** provides the password used for Windows logon.

5 Click Next and, on the Submit Option page, choose a button from the list that submits the logon data. You can type a new button name by typing over the current name. If you want the user to submit the logon data, click Do Not Submit. Click Next to continue.

6 The Logon Screen Template Properties page allows you to view and modify the following properties of the logon screen template:

In the General category:

- **Template** is the name of the template.
- **Description** contains information about the template and is viewable in the One Touch SignOn Administration Tool.
- **User Hint** allows you to type a message that is displayed when a user uses the template for logon, such as when users are prompted to type values for logon fields. For additional user assistance, if you type a URL in the User Hint field, a user can click it to be directed to a Web page that you created to provide custom instructions for logon.
- **Show Balloon** is the number of times a balloon will be displayed on the fingerprint-enabled logon screen to inform the user they can touch the reader to log on.

In the Quick Link category:

- **Quick Link Name** is the name of the Quick Link, if the template was created for a Web site, and appears in the One Touch Menu for accessing Web sites set up for fingerprint logon. Users touch the reader to display the

One Touch Menu, point to Quick Links and then click the fingerprint logon title that corresponds to the Web site they want to access. Internet Explorer is launched automatically and is pointed to the Web site.

- **Quick Link URL** is the URL the Quick Link points to.

In the Screen Detection category:

- **Window Caption** is the title of the logon screen as detected by the wizard. The caption information in the template is used by One Touch SignOn to recognize the logon screen by matching the window caption in the logon screen. If portions of the window caption change, specify the portion of the window caption to match and represent the changing portion of the caption with special characters, such as *. The invariant portion of the string will be used to recognize the logon screen.
- **URL** is used by One Touch SignOn to recognize a Web site logon screen. The URL information in the template is matched to the URL in the logon screen. If multiple Web sites have the same title or if portions of the URL change, which can be the case for Web sites that redirect traffic for load balancing, then specify the portion of the URL to match. The drop-down menu allows you to specify the type of matching to perform on the URL.
- **Extended Match** If you are creating a template for a program, and not a Web site, you can click the button next to the Extended Match field. Select labels that should be used for matching when recognizing the screen. Click the check box next to labels to use. After making selections and clicking OK, you can select the type of matching to perform by selecting it from the drop-down list.

In the Authentication category:

- **Start Authentication Immediately.** If set to Yes, the user is prompted for a fingerprint logon immediately after the logon screen displays. The default setting is No.
- **Lock out logon fields.** If set to Yes, the user is prevented from typing data in the logon fields. The default setting is No.

7 Click Next, and then click Finish, to create the template and close the wizard.

When a template is created for a Web site or program and deployed to a computer, a DigitalPersona icon, as well as a balloon that instructs the user to touch the reader to log on, is displayed in the title bar.
For more information on deploying templates, see "Deploying One Touch SignOn Templates" on page 77.

Creating Templates Manually

If One Touch SignOn does not detect fields automatically in your Web site and program logon screens, you can create a template for a logon screen by manually specifying the fields. Creating templates manually includes using additional controls besides specifying fields and field contents, such as adding keystrokes, forcing delays between actions, and specifying positions of fields.

To create a template manually for a logon screen

1 Launch the password-protected Web site or program and go to the logon screen for which you want to create a template.
2 In the One Touch SignOn Administration Tool, select the container you want to add a template to and then click Create template on the toolbar.
3 When the One Touch SignOn Logon Screen Wizard launches, confirm that the title of the logon screen is accurately displayed on the first page and select the Set up template manually check box. Then click Next.
4 When you click Next, the Logon Fields page displays an empty Fill in Actions list.
5 Click Add and select an action from the drop-down menu. Each action type has its own properties. You can add several actions to the list in the order in which they will be executed during logon.

   Keystroke. This key sequence of one or more keys will be placed in the keyboard buffer.

   - **Key.** You can select keys such as Tab, Enter, Left arrow, Spacebar or Page Up. The Tab key is the default.
   - **Repeat.** Specify a number of times the key sequence is entered.
   - **Shift, Control, Alt.** You can check **Generic**, **Left** or **Right** to simulate pressing one or more of these keys in addition to the key you selected. You

can specify if the key is from the left or right side of the keyboard if necessary.

Field. You can define a field and its type.

- **Label.** Type a label name for the corresponding field on the logon screen. The labels are displayed when users are prompted to type a value for a logon field.
- **Type.** Select the type of field, either **text** or **password**, in the Type text box. Choosing password as the type hides the password on the logon screen so it cannot be viewed. Choosing text displays readable text.
- **Catalog.** For added convenience, you can create specifications for frequently used fields using the Field Catalog Editor. If the field is in the Field Catalog, you can click and then choose it from the drop-down list. Its specifications will be provided automatically by One Touch SignOn.
- **Value.** Type a value for the logon field or use the Value drop-down menu to indicate a value specified by the user or provided by One Touch SignOn.

Note

If you type a value for the logon field, it is stored in the template in clear (unencrypted) text and is shared by all users using the template.

There are several options on the Value drop-down menu, which allow you to specify values that must be provided by the user or by One Touch SignOn. The first three options can be used if you require the user to provide information at logon:

- **Ask-Reuse** prompts the user to enter a value for a logon field the first time they use the template for logon. This value is automatically submitted for them on each subsequent logon without prompting the user again.
- **Ask-Confirm** also prompts the user to enter a value for a logon field the first time they use it. However, on subsequent logons, the value is automatically entered and they are then prompted to confirm this value or change it.
- **Ask Always** prompts the user to enter a value for a logon field each time they use the template.

For a text field, the next options allow you to specify values which are provided by One Touch SignOn:

- **Windows User Name** provides the Windows user name.
- **Windows User Principal Name** provides the user name and domain values in UPN format: [user name]@[domain]
- **Windows Domain\User Name** provides the domain of the user, followed by a backslash and the user name.
- **Windows Domain** provides the user domain name.
- **Windows E-mail Address** provides the email address stored in Active Directory for the user.

For a password field, you can specify the following value which is provided by One Touch SignOn:

- **Windows User Password** provides the password used for Windows logon.

Delay. You can specify how many seconds to wait before the next action in the list is performed.

Position. Using this action, you can specify a location where One Touch SignOn will perform a mouse click. Position is measured from the top left corner of the client window area.

- **Client X.** Type a number of pixels for the X axis position for the action.
- **Client Y.** Type a number of pixels for the Y axis position for the action.
- **Target icon.** You can click and drag the target icon to the actual logon screen field to specify the position. Drop the target icon on the location you want to specify. When you drop the target icon, the Client X and Y positions are updated with the target location.

6 Click **Next** to continue.

7 The **Logon Screen Template Properties** page allows you to view and modify the following properties of the logon screen template:

In the General category:

- **Template** is the name of the template.
- **Description** contains information about the template and is viewable in the One Touch SignOn Administration Tool.

- **User Hint** allows you to type a message that is displayed when a user uses the template for logon, such as when users are prompted to type values for logon fields. For additional user assistance, if you type a URL in the **User Hint** field, a user can click it to be directed to a Web page that you created to provide custom instructions for logon.
- **Show Balloon** is the number of times a balloon will be displayed on the fingerprint-enabled logon screen to inform the user they can touch the reader to log on.

In the Quick Link category:

- **Quick Link Name** is the name of the Quick Link, if the template was created for a Web site, and appears in the One Touch Menu for accessing Web sites set up for fingerprint logon. Users touch the reader to display the One Touch Menu, point to Quick Links and then click the fingerprint logon title that corresponds to the Web site they want to access. Internet Explorer is launched automatically and is pointed to the Web site.
- **Quick Link URL** is the URL the Quick Link points to.

In the Screen Detection category:

- **Window Caption** is the title of the logon screen as detected by the wizard. The caption information in the template is used by One Touch SignOn to recognize the logon screen by matching the window caption in the logon screen. If portions of the window caption change, specify the portion of the window caption to match and represent the changing portion of the caption with special characters, such as *. The invariant portion of the string will be used to recognize the logon screen.
- **URL** is used by One Touch SignOn to recognize a Web site logon screen. The URL information in the template is matched to the URL in the logon screen. If multiple Web sites have the same title or if portions of the URL change, which can be the case for Web sites that redirect traffic for load balancing, then specify the portion of the URL to match. The drop-down menu allows you to specify the type of matching to perform on the URL.

In the Authentication category:

- **Start Authentication Immediately** If set to **Yes**, the user is prompted for a fingerprint logon immediately after the logon screen displays. The default setting is **No**.

8 You can specify additional logon screen matching to help One Touch SignOn recognize the screen.

9 Click **Next**, and then click **Finish**, to create the template and close the wizard.

Adding Change Password Screens to Templates

To set up a change password screen with One Touch SignOn, use the One Touch SignOn Change Password Screen Wizard. With it, you can specify the fields required by the application for changing passwords, implement password policies and even automate the entire process for the end user.

If a template was defined manually, you cannot add a change password screen to the template.

To set up a change password screen with the One Touch SignOn Change Password Screen Wizard

1 Launch the Web site or program and then go to the change password screen.

2 In the One Touch SignOn Administration Tool, select the template for the Web site or program and click Add Change Password Screen on its context menu.

3 When the One Touch SignOn Change Password Screen Wizard launches, make sure that the title of the change password screen is displayed and then click Next.

4 On the Change Password Fields page, select all fields relevant to the change password process, such as fields requesting old and new passwords, and then indicate their value on the Value Type drop-down menu, such as Old Password, New Password or Not a Password. Click Next when you are finished.

5 Indicate the policy to apply to new password entry and syntax on the Password Policy page. The options are:

- **Password is provided by user** will allow the user to specify the new password when changing their password for the Web site or program.

- **Password is generated automatically** will generate a randomized password for the user. By selecting this, you can ensure that the user can only log on with a fingerprint.

6 Check Use Password Policy to specify the syntax, character length and constraints on new passwords.

Note
The password policy applied in the wizard should be synchronized with that of the Web site or program.

If you checked Use Password Policy, select one of the options from the drop-down list to define the contents of the password:

- **Letters and numbers** allows any combination of letters and numbers.
- **Letters only** allows letters only.
- **Numbers only** allows numbers only.
- **Letters with special characters** allows passwords that contain at least one number or at least one letter, and at least one special character is required. Special characters include symbols such as !\"#$%&'()*+,-./ :;<=>?[\\]^_`{|}~@. Spaces are not allowed in passwords.
- **Letters with at least one number** allow passwords containing at least one letter character and at least one number.

Select the constraints to place on the password contents. The options are:

- **None.** No other constraints are applied to the password contents.
- **Different from Windows password.** The new password must be different from the current Windows password.
- **Different from any password.** The new password must be different from any current password for Windows or fingerprint-enabled Web sites or programs.
- **Different from current password.** The new password must be different from the current password for this Web site or program.

Specify a minimum and maximum number of characters for the password.

7 Click Next and, on the Submit Selection page, choose a button to submit the change password data from the list. Click Next again.

The Change Password Screen Properties page displays various attributes that allow you to configure the change password screen template. In addition, you can provide users with instructions for using One Touch SignOn to change their password. Each field, such as User Hint, Window Caption and URL, is described in "Creating Templates" on page 61.

8 If you are adding a change password screen for a program, and not a Web site, on the next page, you can select labels that should be used for matching when recognizing the screen. Select the check box next to labels to use. You can select the type of matching to perform by selecting it from the drop-down list.

9 Click Next, and then click Finish, to save the change password screen specifications to the template.

Change password screens set up with One Touch SignOn display a DigitalPersona icon in the title bar, as well as a balloon telling the user to touch the reader to begin the change password process.

Editing Templates

A logon screen setup can be edited in the OTS Administration Tool.

To edit a template

1 Select the container that includes the template.

2 Select a template to edit.

3 Do one of the following:

Click Edit Logon Screen on the toolbar button.

Click Edit on the context menu of the template and then click Logon Screen.

If you have already added a change password screen, you can select it for editing instead of the logon screen. Templates are not required to include a change password screen.

4 When the One Touch SignOn Logon Screen Wizard launches, edit the settings described in "Creating Templates" on page 61.

5 Click Next to continue with the wizard. Click Finish to exit the wizard.

Deleting Templates

Logon screen setups cannot be deleted without deleting the entire template, including any change password screen setup.

To delete a template

1 In the One Touch SignOn Administration Tool, select the container that includes the template.
2 Click Delete on the context menu of the template, and then click All Screens to delete the template or click Change Password Screen to delete only this screen from the template.

Two-Factor Authentication and Other Policies

Various authentication policies, specifically, fingerprint and password, fingerprint or password, and fingerprint only, can be applied to the logon process with the One Touch SignOn Logon Screen Setup Wizard. Following is a list of each authentication policy, with instructions for implementing them when setting up a logon screen with the One Touch SignOn Logon Screen Setup Wizard:

- **Fingerprint and password.** Choose Ask Always as the value of the password field on the Logon Fields page and enable the Start authentication immediately and Lock out logon fields options on the Logon Screen Templates Properties page. When a user accesses the logon screen, they are immediately presented with a fingerprint authentication screen and are unable to bypass it because the logon fields are locked out. Once they submit a registered fingerprint, they are prompted by One Touch SignOn to type their password.
- **Fingerprint only.** Enable the Start authentication immediately and Lock out logon fields options on the Logon Screen Templates Properties page. When a user accesses the logon screen, they are required to touch the reader with a registered finger and are unable to bypass fingerprint authentication until they do. Once they submit a registered fingerprint, they are logged on, assuming that the password value has already been specified in the template

or by the user the first time they logged on via use of the Ask-Reuse option on the Logon Fields page.

Password only is the default authentication policy for all password-protected Web sites and applications that do not use One Touch SignOn. A fingerprint or password policy applies to OTS-enabled logon screens that allow a user to either type their password manually or touch the reader to automatically provide it.

Using Field Catalogs

The Field Catalog of a container stores logon field values and attributes to expedite the process of creating templates for logon screens that share common fields. By storing frequently used logon fields in the catalog once, you can add the same field to several templates without entering its value or attributes each time. In addition, changes made to fields in the Field Catalog are propagated to all templates that use the field. Each container has only one Field Catalog.

To add a field to a field catalog for a container

1 In the One Touch SignOn Administration Tool, select a container and select Field Catalog on the Tools menu.
2 On the Field Catalog Editor, click Add to create a new field in the table.
3 In the Field text box, type a name for the field you are adding to the catalog.
4 Specify the type of the field by selecting Password or Text in the Type drop-down list.

5 Specify the value of the field on the Value drop-down menu. See "Creating Templates" on page 61 for a description of each value.
6 Add any comments related to this field in the Description text box, and then click OK to close the Field Catalog Editor.

Finding Templates

You can search for templates in specific containers.

To find templates in the One Touch SignOn Administration Tool

1 Select Find Template on the Tools menu.
2 The name, caption and URL fields are available for a pattern-matching search. Select the containers to search in from the list and click Find.
3 The search results display in the dialog.
4 You can save the results of the search by clicking Save. Specify a location and file name to save the results.

The results are saved as an HTML table that includes the template name, file name and container.

Finding Redundant Templates

You can search for redundant templates, which are multiple templates created for a single logon or change password screen.

To search for redundant templates

1 Click Check redundancy on the toolbar.
2 Select the containers to search in from the list and click Check.
The search results display in the dialog.
3 You can save the results of the search by clicking Save. Specify a location and file name to save the results.

The results are saved as an HTML table that includes the container, template name, caption, screen type, created date, modified date and file name.

Finding Fields in Templates

You can search for templates that contain certain fields defined in the Field Catalog of a container. You can select fields from a Field Catalog.

To search for templates that contain certain fields

1 Select the container that uses the Field Catalog you want to use.
2 Select Field Usage from the Tools menu.
3 Select the fields from the Field Catalog and click Find.
The search results display in the dialog.
4 You can save the results of the search by clicking Save. Specify a location and file name to save the results.

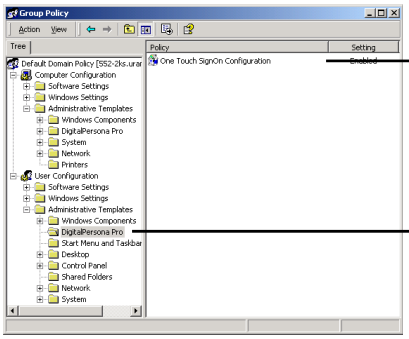
The results are saved as an HTML table that includes the caption, template name, created date, modified date and file name.

Configuring One Touch SignOn

Settings in the One Touch SignOn GPO can impact the way users can use templates for a password-protected Web site or program. Each GPO setting and a description is provided below. By default, all options are enabled.

One Touch SignOn GPOs can be configured using the Group Policy Editor. The policy settings are found in the following path:

`User Configuration/Administrative Templates/DigitalPersona Pro`



Double-click to configure One Touch SignOn properties

One Touch SignOn properties are listed in User Configuration

Note

If you are upgrading an existing installation of DigitalPersona Pro to include support for One Touch SignOn, you must add the DigitalPersona Pro ADM file

again, as described in "Adding DigitalPersona Pro Administrative Templates" on page 35, to access One Touch SignOn settings.

With the DigitalPersona Pro folder selected, double-click One Touch SignOn Configuration to access these GPO settings:

- **Show clear text passwords.** Enable this option to show password field values to the end user when they are prompted to provide a password.
- **Allow users to edit account data.** When enabled, this option permits end users to change the values of logon screen fields by clicking the reader icon located in the title bar of the logon screen.
- **Allow users to add account data.** This option allows end users to add account data fields for Web sites and applications from their computers.
- **Allow users to delete account data.** Allows end users to remove account data from a template.
- **Log One Touch SignOn events, Log account modification events and Log OTS start/stop events.** These settings allow you to specify which events are logged when generated by One Touch SignOn. Event logging is described in detail in "Auditing Using the Windows Event Viewer" on page 53.
- **Path to the container of templates.** Specify the path to the container in the Container Path field to provide access to the templates it contains for DigitalPersona Pro Workstation users. The container path is determined when creating a new container, as described in "Creating Containers" on page 59. You can add multiple paths, which are separated by the vertical bar character, |.

Deploying One Touch SignOn Templates

To make templates accessible by computers running DigitalPersona Pro Workstation, you can add the One Touch SignOn Group Policy Object (GPO) to Active Directory or apply the GPO locally.

Templates can be accessed from a shared network drive. You specify the path to the shared folder in the Active Directory user GPO using the Path to the

container of templates setting. One Touch SignOn will copy templates from the shared folder to the user computers as specified by the policy.

You can also copy templates to the computer and configure the GPO on the computer to find the templates locally. The templates can be stored in any folder as long as the Path to the container of templates setting in the GPO specifies that folder. This is useful for testing your templates before deploying them on the network.

Deploying Templates Locally

Administrators may want deploy a template on a local computer to test OTS templates on a Pro Workstation before distributing it to other computers on a network or, if a computer does not have access to the container the template is stored in, administrators can add the template directly to the computer using the default OTS template folder installed by OTS. The path is:

[hard drive]:\Documents and Settings**[user name]**\Application Data\DigitalPersona\OTS\Templates

Administrators can also deploy templates to networked computers without configuring the OTS GPO by placing the templates in the default OTS template folder installed by OTS on a network server. The network server path is:

[network server ID or hard drive]:\Documents and Settings**[user name]**\Local Settings\Application Data\DigitalPersona\OTS\Templates

Note

In both cases, the template settings will not take effect until the user logs out and then logs in again or a local template is created or edited using either the One Touch Internet or One Touch SignOn tools.

Logging On with One Touch SignOn

After creating templates and deploying them to users, users can launch the logon screen and touch the fingerprint reader with a registered finger to log on. If a Quick Link was defined in the template, users can select the Quick Link from

the One Touch Menu to launch the Web site logon screen. Quick Links only display in the One Touch Menu after the user has visited them and provided a fingerprint logon to logon.

Logon screens that have a template created for them display a DigitalPersona icon in the title bar and a balloon informing the user to log on with a fingerprint.

A balloon indicates that the Web site or program is set up for fingerprint logon

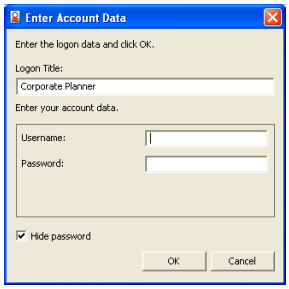
Depending on the template attributes, the logon process may vary. For example, the user can be automatically logged on by touching the reader. The fields can be automatically populated and submitted.

In other cases, the user is prompted to choose a set of account data or provide logon field values. If the user has set up multiple sets of account data, the user is prompted to select an account in the Select Account Data dialog box. The user must click the name of the account to use and click OK to log on.

When the user is prompted to type values for logon fields, the Enter Account Data dialog box displays. This dialog box displays when the user has required fields where the values are not yet specified. In the dialog box, the user can provide the appropriate values for the fields and click OK to log on.

Providing Logon Field Values

If the template contains logon field values that are provided by the end user, the Logon Field Values dialog box opens, listing each field needing a value and allowing the user to enter them before logging on.

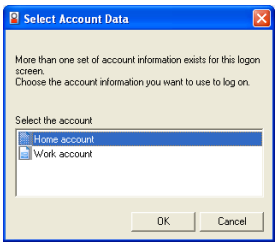


The appearance of this dialog box is dependent on the Value attribute, such as Ask- Reuse, Ask-Confirm or Ask Always, for fields in a template.

If the Show Password Values in Fields option in the GPO is enabled or not configured, the user can click the “Show passwords during editing” button to display the password as they edit it. Otherwise, the characters in the password are replaced with a bullet.

Choosing an Account

If a logon screen is set up for multiple accounts, the Select Account Data dialog box is displayed, prompting the user is prompted to select the set of account data they want to use to log on.



When the user selects the set of account data, they can click OK to log on.

Providing Multiple Credentials

Two-factor authentication—as well as other authentication policies—can be applied to logon screens, which may require the user to first provide a registered fingerprint and then a password, for example. Two-factor authentication and implementing authentication policies with One Touch SignOn is described in "Two-Factor Authentication and Other Policies" on page 72.

Changing Passwords with One Touch SignOn

Change password screens that have a template created for them display a DigitalPersona icon in the title bar and a balloon informing the user to provide a fingerprint. The user is asked to provide the old password, a new password and to confirm the new password. Depending on the template attributes, the change password process may vary. For example, the user can be allowed to choose a new password with or without constraints on the password complexity.

In other cases, the new password is generated automatically by the system. In this case, the user must log on with a fingerprint.

Using Attended Fingerprint Registration

To provide a higher level of security, some organizations might want to implement attended registration for users or groups of users. With attended registration, a designated user must be logged in to supervise the fingerprint registration process of other users. After users have been registered using attended registration, users are prevented from registering other fingerprints or delete fingerprints from their own account.

This secure implementation is performed by assigning registration permissions to a supervising user or user group and then by removing the permissions for all users to register themselves.

Assigning Permissions to Perform Attended Registration

The user designated to perform attended registration for other users must have permission to register and delete user fingerprints. The Register/Delete Fingerprint permission can be granted at the single user, organizational unit or domain level. You cannot assign this permission at the user group level. The

supervising user can be an individual user or belong to a user group. Then, remove the permission for users to register themselves.

To assign permissions for an organizational unit or domain to the supervising user

1 In Active Directory for Users and Computers, select the domain or organizational unit to be registered through attended registration by the supervising user.
2 Right-click and select Properties.
3 Click the Security tab.
4 Click the Advanced button.
5 Click Add and add the supervising user or group to the users who have permissions to this account. Then click OK.
6 Click the Edit/View button.
7 Select User Objects from the Apply onto drop down list.
8 In the Permissions list, select the Allow check box for the Register/Delete Fingerprint (DigitalPersona) permission.
9 Click OK to close dialog and save changes.

To assign permissions for a single user to the supervising user

1 In Active Directory for Users and Computers, select the user name to be registered through attended registration.
2 Right-click and select Properties.
3 Click the Security tab.
4 Click the Add button.
5 Select the supervising user or group who will have register and delete fingerprints permission to this account.
6 Click Add and OK.
7 In the Permissions list, select the Allow check box for the Register/Delete Fingerprint (DigitalPersona) permission.
8 Click OK.

Applying permissions for one user at a time is not efficient and most organizations will prefer to apply permissions on an organizational unit or domain.

You can remove permissions for users to register themselves at the organizational or domain level. The domain level is the simplest level to remove the permission for all users.

To remove permissions at the domain level for users to register themselves

1 In Active Directory for Users and Computers, select the domain.
2 Right-click and select Properties.
3 Click the Security tab and click the Advanced button.
4 In the Permissions list, select the Allow SELF Register/Delete Fingerprint permission.
5 Click the Remove button.
6 Click OK.

Registering User Fingerprints

DigitalPersona Pro Workstation must be installed on the computer where registration is performed. The currently logged-in user must have permission to register fingerprints for the user account being registered.

To register a user

1 Make sure you have installed the Administration tools.The Attended Fingerprint Registration Tool is included with the DigitalPersona Pro Administration tools and is installed separately from the Pro Workstation for Active Directory CD.
2 From the Start menu, point to Programs, then DigitalPersona Pro, and then select Attended Fingerprint Registration Tool to run the Attended Fingerprint Registration Tool and provide the user name and the domain of the user to register.

The Attended Fingerprint Registration Wizard starts.

Note

If the account of the supervising user does not have the Register/Delete Fingers permission for the user being registered, the Access Denied message displays when registered fingerprints are saved.

3 Type the user name and select the domain. Then click Next.

4 Follow the Attended Fingerprint Registration Wizard instructions to register the user's fingerprints.

The user being registered must provide the user password or fingerprint to continue through the Registration Wizard. This requirement prevents the supervising user from registering the incorrect person's fingerprints for the user account. For more information on registering fingerprints, see "Registering Fingerprints" on page 95.

Deleting Fingerprints with Attended Registration

If a user is not allowed to delete fingerprints, the supervising user can use the Attended Fingerprint Registration Tool to delete registered fingers. The registered user must be present to provide the password or fingerprint.

You can also delete registered fingerprints from Active Directory for Users and Computers. Select the user, right-click, and select All Tasks, and then select Delete Fingers.

Installing DigitalPersona Pro Workstation 6

This chapter describes the installation and configuration required for setting up DigitalPersona Pro Workstation on a client computer in a network environment. It is recommended to install and configure DigitalPersona Pro Servers before setting up DigitalPersona Pro Workstation.

Installing DigitalPersona Pro Workstation

Before installing DigitalPersona Pro Workstation, make sure your system meets the following minimum requirements:

- Windows XP Professional, Windows 2003, Windows NT, Windows 2000, Windows Me, Windows 98
- 45 MB of free hard disk space
- 128-bit encryption capability (for Windows 98, Me, NT and 2000 only), as described in "Step 2: Configuring a Domain for DigitalPersona Pro Server" on page 23
- Active Directory Client for Windows 98 installed on Windows 98/Me computers. The installer is located on the DigitalPersona Pro installation CD in `Redistr\Active Directory Client for Win98` folder.

If your system meets the above requirements, proceed with the installation of DigitalPersona Pro Workstation for Active Directory.

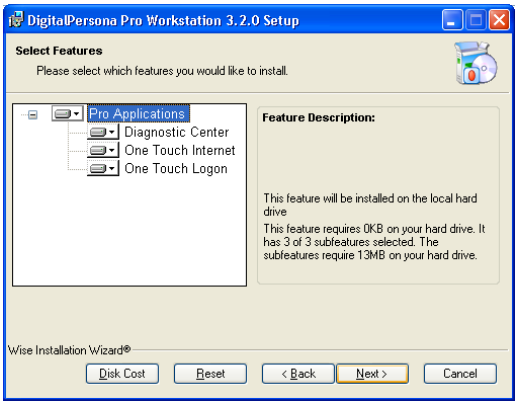
To install DigitalPersona Pro Workstation for Active Directory

1. Insert the DigitalPersona Pro Workstation for Active Directory CD in your CD-ROM drive.
2. If the installation wizard does not start automatically, locate and double-click the Setup.exe file to run the DigitalPersona Pro Workstation for Active Directory Installation Wizard.
3. When the installer runs, click Next to proceed with installation.
4. Read the terms and conditions on the License Agreement page. If you agree with them, select the I accept the license agreement button and then click Next.
5. On the next page, you can specify the folder that DigitalPersona Pro will be installed in. If you want to install DigitalPersona Pro in the default location,

`C:\Program Files\DigitalPersona\`, click Next; otherwise, click Browse to specify a new location and then click Next to continue.

6 Choose one the following options to indicate the type of installation you want to perform:

- **Complete.** Click Next for the Complete installation, which installs the One Touch Applications and the Diagnostic Center. Then, click Next.
- **Custom.** Click Custom and then click Next to specify the options to install. Select an installation option on the drop-down menu if you do not want to install it. You can also check how much disk space a particular installation will require by clicking Disk Cost. To return the installation option settings to the default settings, click Reset. When you are finished, click Next to proceed.



Note

On Windows 98, One Touch Internet is not available.

7 When you click Next, the installer begins installing DigitalPersona Pro on your computer.

8 Connect the reader when prompted. The installer puts the necessary driver files on your hard drive to use the reader with DigitalPersona Pro.

9 When installation is finished, click Finish to close the installer. Click Yes when prompted to restart the computer.

After the computer restarts, and at every subsequent restart, the Workstation software automatically uses the default DNS Server to locate all DigitalPersona Pro Servers for the domain and its site. If more than one Pro Server is found, the Workstation will choose the Pro Server for authentication that offers the most efficient connectivity. If no Pro Servers are found, DigitalPersona Pro Workstation will perform authentication locally.

When you are finished with installation, proceed to "Logging on after Installation" on page 91, which describes the changes made to the user account logon process and how to register fingerprints for authentication.

Customizing a DigitalPersona Pro Workstation Installation

To customize an existing installation of DigitalPersona Pro Workstation, you can add or remove One Touch Applications using the Add or Remove Programs Control Panel. Follow the on-screen instructions in the Control Panel for adding the One Touch Applications. By default, all applications are installed.

Uninstalling DigitalPersona Pro Workstation

The DigitalPersona Pro Workstation software is removed using the Add or Remove Programs Control Panel. The Workstation software is listed as "DigitalPersona Pro Workstation for Active Directory version **`[version number]`**."

Note

You must have local administrative privileges to modify installations on the computer.

Remote Installation and Uninstallation

The installers for both DigitalPersona Pro Server and Workstation use Microsoft Windows Installer (MSI) technology, which allows administrators to remotely install or uninstall DigitalPersona Pro software using Active Directory administration tools, or other software deployment tools.

This section provides remote installation and uninstallation instructions and guidelines for using Active Directory administration tools.

To install DigitalPersona Pro software remotely using Active Directory administration tools

1 Launch the Active Directory Users and Computers administration tool.
2 On the context menu of a site, domain or Organizational Unit, click Properties and then click the Group Policy tab.
3 Create a new Group Policy Object, or select an existing one, and click Edit to launch the Group Policy Editor.
4 In the tree, select one of the following folders:
- For a computer-based policy, select `Computer Configuration/Software Settings/Software Installation`.
- For a user-based policy, select `User Configuration/Software Settings/Software Installation`.

5 Click Properties on the context menu of the Software Installation folder to open the Software Installation Properties dialog box
6 On the General tab, specify the default software distribution location in the Default package location text box.
   This must be a location on the network that is accessible by the domain controller or computer on which you want to install the DigitalPersona Pro software.
   Also, specify the settings for all other options, such as new package and installation user interface options. Click OK.
7 Right-click the right pane on the Group Policy Editor, point to New and then click Package.
8 On the Deploy Software dialog box, select the appropriate deployment option and click OK.
9 After setup is complete, assign the appropriate computers and users to Active Directory containers to which the installation GPO is associated with.

Installation Using the Command Prompt

DigitalPersona Pro Workstation software can also be installed and uninstalled using MSI via the command prompt.

The format of the `msiexec` command is shown below and is followed by a description of the command line options, parameters and values it uses:

`msiexec /i setup.msi INSTALLDIR=`**`[directory]`** `ADDLOCAL=`**`[software]`** `REMOVE=`**`[software]`** `/qn`

Command Line Options

There is one required command line option and one optional:

- `/i` indicates that MSI will be used to install DigitalPersona Pro software. It is immediately followed by the folder path and name of the .msi file (setup.msi for DigitalPersona Pro Workstations and Servers) that contains the software to install.

Note
Both the command line option and .msi file are required.

- `/qn` hides the user interface when installing the software on the computer, allowing a "silent install." If used, it is placed at the end of the command line. This command line option is not required; however, it is recommended by DigitalPersona for deploying software in the enterprise.

Parameters

Three parameters indicate where the software should be installed on the computer, as well as what components should be included or removed:

- `INSTALLDIR` is an optional parameter used to indicate where DigitalPersona Pro software components should be installed on the target computer. It is optional and, if a folder is not specified, defaults to: `C:\Program Files\DigitalPersona`
- `ADDLOCAL` and/or `REMOVE` indicate which DigitalPersona Pro software components to install or uninstall. They can be used together or interchangeably; only one is required. Each command is followed by values specified in the next section.

ADDLOCAL and REMOVE Parameter Values

The table below lists all the recommended `ADDLOCAL` and `REMOVE` parameter values and provides a description of each:

Parameter Value	Description
`All`	Installs all DigitalPersona Pro software components or removes all the components already installed.
`Logon`	Installs or removes One Touch Logon
`One_Touch_Internet`	Installs or removes One Touch Internet

Following are a few rules when using these parameters and their values:

- Individual software components cannot be installed unless the `All` value was used with the `ADDLOCAL` parameter first.

To install DigitalPersona Pro Workstation software for the first time while omitting one or more software components, use `ADDLOCAL=ALL`, followed by the `REMOVE` parameter with each software component you do not want to install separated by a comma.

Using DigitalPersona Pro Workstation 7

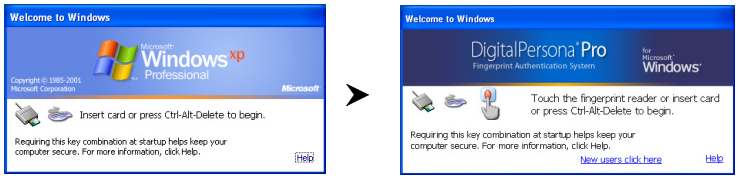
Each administrator and end user of DigitalPersona Pro Workstation should acquire the basic skills for using DigitalPersona Pro and be aware of the changes the Workstation software makes on a computer.

This chapter describes these changes and provides instructions for registering fingers, modifying Workstation properties and using the One Touch Menu and the reader icon menu.

DigitalPersona Pro Workstation provides secure and convenient access to your Windows user accounts, as well as your accounts for Web sites and applications. This chapter describes the One Touch Logon application, which provides fingerprint authentication for Windows user account logon, and One Touch SignOn, which provides fingerprint authentication for Web site and application logon.

Logging on after Installation

After you install DigitalPersona Pro Workstation with the One Touch Logon application, the standard Windows logon dialog box is replaced with the One Touch Logon dialog box.



Before you can use the fingerprint authentication functionality of DigitalPersona Pro, you must first log on and register a fingerprint. When the One Touch Logon dialog box displays, press Ctrl-Alt-Delete and log on with your password.

Note

Windows 98 and Me users cannot press Ctrl-Alt-Delete; instead, they must click the provided link on the logon dialog box.

After logging on, the Fingerprint Registration Wizard launches, allowing you to register your fingers for use with the DigitalPersona Pro Workstation. Refer to "Managing Fingerprint Credentials" on page 94 for instructions on using the Fingerprint Registration Wizard to register fingerprints.

For a more detailed description of subsequent logons using One Touch Logon, read "One Touch Logon" on page 99.

DigitalPersona Pro Feedback

DigitalPersona Pro Workstation provides visual and/or audio feedback for several events, which are described in the next four sections.

Fingerprint Prompt Feedback

DigitalPersona Pro applications can display a graphic of a finger touching the reader to prompt you to place a registered finger on the reader.

A finger pointing to the reader prompts you to touch the reader

A finger touching the reader indicates you may lift your finger

When you are prompted for a registered fingerprint at a logon screen on a DigitalPersona Pro-enabled application, the first graphic is displayed. When the second graphic is displayed, you may lift your finger from the reader.

These graphics will be preceded by a reader with an hour glass next to it until DigitalPersona Pro is ready to use the reader to acquire a fingerprint scan.

The hour glass indicates that DigitalPersona Pro is not ready to accept a fingerprint

When the hour glass graphic is replaced by the fingerprint prompt graphic, you may place a registered finger on the reader.

Fingerprint Scan Acquisition Feedback

Once the reader acquires a scan of your fingerprint, a sound is played and an animation displays, which consists of a series of circles that quickly expand from the center of the screen outward.

Using the DigitalPersona Pro Properties dialog box, you can specify whether the sound plays, as described in "Enable Sound Feedback for Fingerprint Scan" on page 118, and whether the animation displays, as described in "Enable Visual Feedback for Fingerprint Scan" on page 118, when a fingerprint scan is acquired.

Fingerprint Recognition Feedback

DigitalPersona Pro indicates whether the acquired fingerprint scan is recognized as a registered fingerprint. If the fingerprint scan is recognized, it displays a graphic of a check mark on the right side of the reader and finger. If it is not, the graphic displays a question mark instead of a check mark.

Indicates a successful scan of your fingerprint

Indicates the fingerprint was not recognized

The DigitalPersona Pro Properties dialog box allows you to specify whether this animation displays, as described in "Show Fingerprint Recognition Animation" on page 118.

Reader Not Found Feedback

A graphic that consists of a reader with a red X over it displays on the logon screen, desktop and notification area on the taskbar if the reader is not connected or installed.

Icon in notification area

Icon in logon screen

It is displayed on the desktop if the Show Fingerprint Recognition Animation property is enabled on the DigitalPersona Pro Properties dialog box, as described in "Show Fingerprint Recognition Animation" on page 118.

Managing Fingerprint Credentials

Fingerprints are used by DigitalPersona Pro to provide a convenient way to submit your account information to log on to Windows, Web sites and programs. Instead of typing your account information at a logon screen, you simply touch the fingerprint reader with your finger and DigitalPersona Pro enters your account information for you.

In order to use fingerprints for logging on to Windows, Web sites and programs, you must first register fingerprints using the Fingerprint Registration Wizard, which creates a template for each fingerprint and stores it in the user database. Your administrator determines how many fingerprints you can register and if you can delete or change registered fingerprints.

When you touch the reader with a registered finger, DigitalPersona Pro compares the scanned fingerprint to the fingerprint templates stored in the user database to verify your identity. When verified, your user name and password are provided for log on.

Note
Your settings might prevent you from registering and deleting fingerprints. If your administrator sets the maximum number of registered fingerprints to zero, you are prevented from registering fingerprints and any existing registered fingerprints are deleted.

Note
If a Pro Server is not found, you will have the option to store your fingerprint credentials in the local cache. Locally cached credentials will be discarded should a Pro Server become available. You cannot modify your server-based credentials when the Pro Server is unavailable.

If you installed One Touch Logon, the Fingerprint Registration Wizard launches automatically the first time you log on after installation of DigitalPersona Pro. You may also launch it by pressing Ctrl-Alt-Delete, clicking the Manage

Fingerprints button and selecting Register Fingerprints from the drop-down menu.

If you did not install One Touch Logon and you have no registered fingers, you can launch the Fingerprint Registration Wizard by placing a finger on the reader. You can also right-click the reader icon—located in the notification area on the taskbar—and then click Fingerprint Registration Wizard.

Registering Fingerprints

The Fingerprint Registration Wizard guides you through the process of registering fingerprints. If you are not permitted to register fingerprints, it may be because of your settings implemented by your administrator.

If you have not registered fingerprints yet, and One Touch Logon is installed, the Fingerprint Registration Wizard launches automatically after logging on. It is recommended to register fingerprints the first time that the Fingerprint Registration Wizard displays because your administrator may have implemented logon settings that require you to provide a fingerprint the next time you log on.

Note

You must have a Windows user account and be logged on to that account to register your fingerprints.

In order to successfully register one fingerprint, that fingerprint must be scanned four times by the fingerprint reader. Refer to "Fingerprint Reader Usage and Maintenance" on page 119 for guidelines on how to correctly place your fingers on the fingerprint reader.

To register fingerprints using the Fingerprint Registration Wizard

1 During your Windows session, launch the Fingerprint Registration Wizard by doing one of the following:
   - For Windows XP and 2000 users, press Ctrl-Alt-Delete and click Manage Fingerprints. Select Fingerprint Registration from the drop-down menu and click OK.

- For Windows NT 4.0 users, press Ctrl-Alt-Delete and click Register Fingerprints.
- For Windows 98 and Me users, on the Start menu, point to All Programs, point to DigitalPersona Pro and then click Fingerprint Registration Wizard.
- For users who have not installed One Touch Logon, on the Start menu, point to All Programs, point to DigitalPersona Pro and then click Fingerprint Registration Wizard.

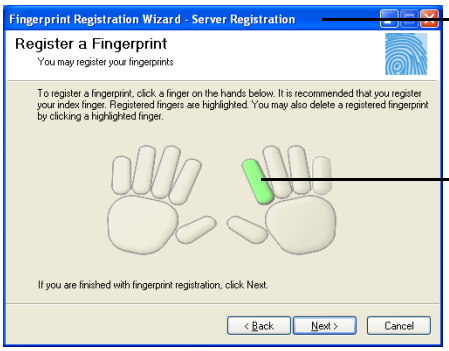
2 Click Next. If registered fingerprints will be saved in the user database on your computer instead of in Active Directory, you are prompted to confirm that you want to save your fingerprints locally only. This prevents you from using your registered fingerprints from another computer. Click Yes to confirm, or click No and contact your administrator for guidance.

3 When prompted, verify your identity, either by typing your Windows password if you do not have any registered fingerprints or by touching the reader with any registered finger.

4 An outline of two hands is displayed. Fingers that are already registered are highlighted in green. Click the finger you want to register on the outline.

Note

Clicking a green highlighted finger deletes the associated registered fingerprint.

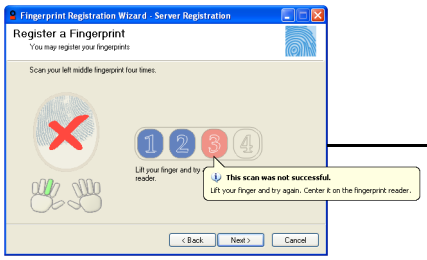


The title bar indicates local or server storage of fingerprint credentials

Fingers highlighted in green are already registered

5 When you have selected a finger to register, you are prompted to place that finger on the reader four times. The Fingerprint Registration Wizard provides feedback indicating the quality of each fingerprint scan. If the fingerprint scan is not of an acceptable quality, you are prompted to touch the reader again. When you have provided four good fingerprint scans, the fingerprint is successfully registered and is highlighted in green on the outline.

Fingerprint scan was successful



Fingerprint scan was not successful

6 Click Next or select another finger to register by clicking a finger that is not highlighted on the outline.

Note

The number of fingers you can register is determined by the value of the Maximum Number of Fingers setting, as described on page 40. If the settings allow, it is recommended that you register two fingers, preferably the index finger of both hands.

7 If you only registered one fingerprint, you may be prompted to register another. Registering two or more fingers ensures that, in the event you cannot use one registered finger, you can use the other.
Click Yes to register another fingerprint or click No to close the prompt.
8 Click Finish to exit the wizard and save your changes.

The fingerprint credentials you added with the Fingerprint Registration Wizard are now DigitalPersona Pro registered fingerprints.

Deleting Registered Fingerprints

You can use the Fingerprint Registration Wizard to delete any fingerprints that you have previously registered. If you are not permitted to delete fingerprints, it may be because of your settings implemented by your administrator.

To delete registered fingerprints using the Fingerprint Registration Wizard

1 Launch the Fingerprint Registration Wizard by doing one of the following:
   - For Windows XP, 2000 and NT 4.0 users, press Ctrl-Alt-Delete and click Manage Fingerprints. Then select Register Fingerprints in the drop-down box.
   - For Windows NT 4.0 users, press Ctrl-Alt-Delete and click Register Fingerprints.
   - For Windows 98 and Me users, on the Start menu, point to All Programs, point to DigitalPersona Pro and then click Fingerprint Registration Wizard.
   - For users who have not installed One Touch Logon, on the Start menu, point to All Programs, point to DigitalPersona Pro and then click Fingerprint Registration Wizard.
2 Click Next. If changes to registered fingerprints will be saved in the user database on your computer instead of in Active Directory, you are prompted to confirm that you want to make changes to your fingerprints locally only. These changes will not be applied to Active Directory. Click Yes to confirm, or click No and contact your administrator for guidance.
3 When prompted to verify your identity, touch the reader with any registered finger.

4 An outline of two hands is displayed with your registered fingers highlighted in green. Click the highlighted finger that represents the registered fingerprint you want to delete.

Note
Clicking a finger which is not highlighted starts the registration of that finger.

5 When prompted, click Yes to delete the registered fingerprint. Otherwise, click No if you do not want to delete that fingerprint.
6 Click Next or select another finger to delete.

Note
If your settings allow, it is recommended that you register two fingers, preferably the index finger of both hands. If you are prompted to register another fingerprint, click Yes to continue registration or click No to close the prompt and proceed to the last page of the wizard.

7 Click Finish to exit the wizard and save your changes. Canceling or closing the dialog box does not save your changes.

One Touch Logon

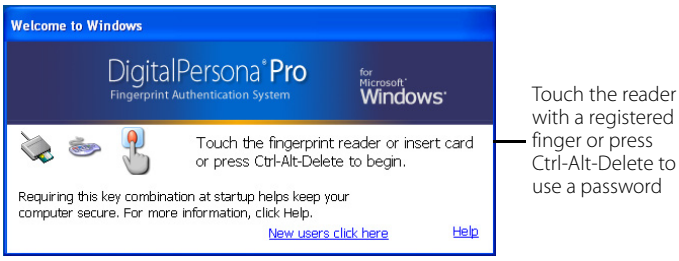
One Touch Logon allows users to use any registered fingerprint, or a fingerprint and the Windows password or a smart card, to log on to Windows user accounts. It replaces the standard Windows logon dialog box and prompts users for their credentials according to the logon policy implemented by the administrator of the computer, as well as cached credentials and identification list settings. Although these factors may affect the logon process, One Touch Logon guides users through the process of authenticating to their user account with DigitalPersona Pro, making it unnecessary to burden them with the specifics of policy implementation.
The three factors that determine how users are prompted for credentials when they log on with One Touch Logon—the logon policy applied to a computer and

cached credentials and identification list settings—are explained in the next two sections.

Logon Policies

One Touch Logon first uses the logon policy applied to the computer (as described in "Multi-credential Logon to Windows" on page 42) to determine which credentials are needed to log on, such as registered fingerprints or passwords. It then uses cached credentials and identification list settings to determine the rest of the logon process, as described in "Cached Credentials and the Identification List" on page 101.

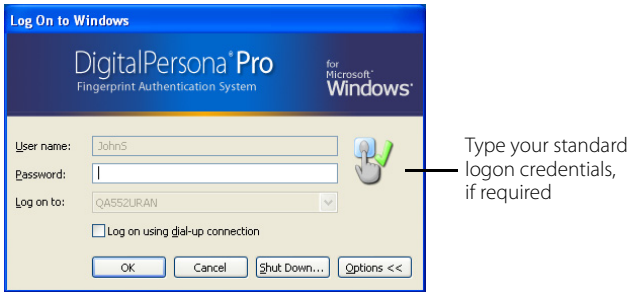
If a logon policy requires a registered fingerprint, One Touch Logon will prompt the user to place a registered finger on the reader. The user can place a registered finger on the reader or press Ctrl-Alt-Delete.



Note

Windows 98/Me users must click the provided link instead of Ctrl-Alt-Delete.

If required, they are also prompted for their Windows logon password.



This dialog box is similar to the standard Windows logon dialog box, on which a user types their user name, password and domain to authenticate. Depending on the Windows local security policy applied to the computer, this may be the only screen a user sees when logging on. If cached credentials and identification list settings permit, the user name and domain may be automatically provided, requiring the user to provide only a password.

When a fingerprint only policy is applied to the computer, then the user is only prompted for a registered fingerprint; a password only policy prompts the user for their standard logon credentials.

If either a fingerprint or password is required, the user is prompted for a registered fingerprint. They can provide their password instead of a registered fingerprint by pressing Ctrl-Alt-Delete; however, if the user provides a registered fingerprint, they are not prompted for their password and are logged on.

Cached Credentials and the Identification List

In any scenario where a user is prompted for a registered fingerprint and cached credentials and the identification list are enabled, One Touch Logon attempts to perform user identification by searching for their cached credentials and the user data on the identification list.

If the credentials are cached, but the user is not on the identification list, they are prompted to press Ctrl-Alt-Delete and provide their user name and domain before they can log on—regardless of the logon policy. The user, however, may

try using their registered fingerprint two more times before they are advised to log on by typing their account information manually.
If the credentials are cached and the user is on the identification list, they are immediately logged on if the policy requires a fingerprint only or either a fingerprint or password. If required, they are also prompted for a password before logging on; the user name and domain are automatically provided for them.

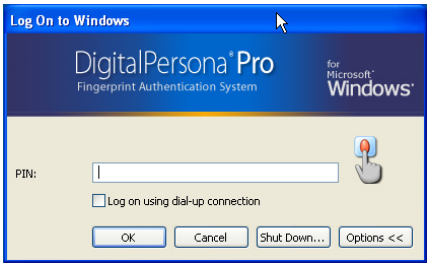
Using Smart Cards for Logon

If you have a smart card reader connected to your computer, the Welcome screen includes instructions for using a smart card. If you are required to log on with a smart card, you must insert the smart card into the smart card reader first, before providing any other credentials, such as a fingerprint. Your settings cannot require you to provide both a smart card and a password for logon.

Smart card users are required to type a PIN to access the smart card, also known as a user PIN. This PIN is provided with your smart card package. Smart cards are supported only on Windows XP and 2000.

To use a smart card to log on

1 Insert the smart card into the smart card reader first, even if you must provide a fingerprint as one of your credentials.
The PIN dialog box displays requesting the PIN to access the smart card.



2 Type the user PIN for the smart card and click OK.

If your logon settings implemented by your administrator allow you, you can touch the fingerprint reader with a registered finger instead of typing the PIN for the smart card.

Using Fingerprint PINs

The administrator may require that users type a short sequence of characters, known as a fingerprint PIN, each time they use a fingerprint to log on, unlock the computer, or change your Windows password. This provides an additional level of security. Logon settings with fingerprint PINs are supported only on Windows XP and 2000. Logon settings are managed by your administrator.

You must register a fingerprint before you can register a fingerprint PIN. If your logon settings require a fingerprint PIN, you will be prompted to register a fingerprint PIN the first time you log on using a registered fingerprint. Fingerprint PINs are only used with fingerprints to log on, unlock the computer, or change the Windows password. They are not used for fingerprint logons to Web sites and programs or to unlock smart cards.

Registering Fingerprint PINs

When you create a fingerprint PIN, you can choose any sequence of four to six numbers or letters. Make sure that you remember this code, or you may not be able to log on. The Register Fingerprint PIN dialog box displays automatically after you log on to Windows using a fingerprint if your logon settings require you to provide a fingerprint PIN in addition to a fingerprint.

You must register a fingerprint PIN when the Register Fingerprint PIN dialog box displays. If you click Cancel, you will be prevented from logging in with a fingerprint.

To register a fingerprint PIN

1 Type a new fingerprint PIN in the New fingerprint PIN text box and then type it again in the Confirm fingerprint PIN text box.

2 Click OK to save the fingerprint PIN.

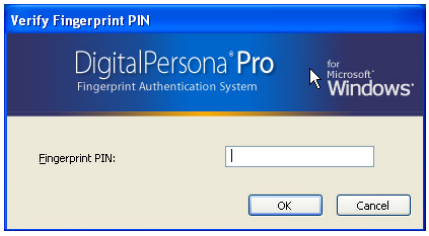
3 After you register your fingerprint PIN, you can change your fingerprint PIN at any time.

Using Fingerprint PINs

After you register a fingerprint PIN, you will be prompted to type the fingerprint PIN after each time you use a fingerprint to log on, unlock the computer, or change the Windows password. The Verify Fingerprint PIN dialog box displays each time the fingerprint PIN is required. The fingerprint PIN is not required when you use fingerprint logons to Web sites or programs, or when you unlock a smart card with a fingerprint.

To use a fingerprint PIN

1 When the Verify Fingerprint PIN dialog box displays, type your fingerprint PIN and click OK.



Changing Fingerprint PINs

You can change your fingerprint PIN at any time during your Windows session. You must type the current PIN and then type a new code of four to six characters.

To change a fingerprint PIN

1 Press Ctrl-Alt-Delete to display the Windows Security dialog box.
2 Click the Manage Fingerprints button and then select Change Fingerprint PIN from the drop-down box.
3 On the Change Fingerprint PIN dialog box, type your current fingerprint PIN in the Old Fingerprint PIN text box.
4 Type a new fingerprint PIN in the New Fingerprint PIN text box and then type it again in the Confirm New Fingerprint PIN text box.
5 Touch the reader with a registered fingerprint for verification.
A green check mark displays on the reader icon in the dialog box when the fingerprint is successfully verified.
6 Click OK to change your current fingerprint PIN to the new one you specified.

Changing Your Windows Password

The process of changing your Windows password on Windows XP and Windows 2000 is very similar to that of computers without DigitalPersona Pro.

To change your Windows password

1 Press Ctrl-Alt-Delete to display the Windows Security dialog box.
2 Click the Change Password button.
3 On the Change Windows Password dialog box, type your current password in the Old Password text box. You can also touch the reader with a registered

fingerprint. If your identity is verified, One Touch Logon provides the current password in the Old Password text box.

4 Type a new password in the New Password text box and then type it again in the Confirm New Password text box.
5 Click OK to change your current password to the new one you specified.

Changing Your Windows Password on Windows NT

The process of changing your Windows password on Windows NT 4.0 is very similar to that of computers without DigitalPersona Pro.

To change your Windows password

1 Press Ctrl-Alt-Delete to display the Windows Security dialog box.
2 Click the Change Password button.
3 On the Change Windows Password dialog box, type your current password in the Enter Old Password text box. You can also select the Enter old password with fingerprint check box to be prompted for a registered fingerprint. If your identity is verified, One Touch Logon provides the current password in the Old Password text box.
4 Type a new password in the New Password text box and then type it again in the Confirm New Password text box.
5 Click OK to change your current password to the new one you specified.

Changing Your Password with One Touch Logon on Windows 98/Me

If you are running Windows 98 or Me, you must change your Windows password using the standard method, i.e., the Users Control Panel. Refer to Windows Help for instructions.

Warning

Win 98 and Me users who log on both locally and to a domain must use the same password for the local and domain logon account.

In addition to One Touch Logon and One Touch SignOn, DigitalPersona Pro Workstation includes One Touch Unlock and One Touch Internet. This chapter provides instructions for using them.

Using One Touch Unlock

To lock your computer, double-click the fingerprint reader icon or click Lock Computer on the fingerprint reader icon context menu. The reader icon is located in the notification area on the taskbar.

When your computer becomes locked, One Touch Unlock replaces the standard Windows Computer Locked dialog box. One Touch Unlock guides you through providing the required credentials to unlock your computer. The required credentials depend on the logon settings implemented by your administrator. You can also press Ctrl-Alt-Delete to type your account information and provide the required credentials.

Note

This feature is only available if One Touch Logon is installed.

Using One Touch Unlock on Windows 98/Me

If you are running Windows 98 or Me, you can lock your computer by double-clicking the fingerprint reader icon or click Lock Computer on the fingerprint reader icon context menu. The reader icon is located in the notification area on the taskbar. To unlock a Windows 98 or Me computer, you must supply the same credentials required by the logon settings. In addition, you can display any Windows screen saver when the computer is locked.

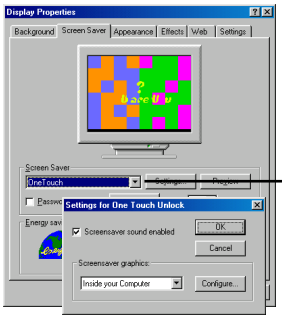
To activate One Touch Unlock with screen saver functionality on Windows 98 and Me

1 Right-click anywhere on the desktop and then click Properties. On the Display Properties dialog box, click the Screen Saver tab.

2 To activate the One Touch Unlock screen saver, click One Touch Unlock on the Screen Saver drop-down menu.

3 To choose which screen saver to display when the computer is locked, click Settings.

4 In the Settings for One Touch Unlock dialog box, choose a screen saver in the Screen Saver Graphics drop-down menu.



Select OneTouch to activate a screen saver with One Touch Unlock; click Settings to configure

Choose (and configure) the screen saver that displays when One Touch Unlock is activated

5 If the screen saver you choose has options to configure, you can click Configure.

6 If you choose the DigitalPersona screen saver, the option, Screen saver sound enabled, is in the Settings for One Touch Unlock dialog box and cannot be accessed by clicking Configure.

7 When you are finished, click OK. Then, click Apply on the Display Properties dialog box and then click OK again to save your changes.

Note

Because a "preview" version of the screen saver is displayed, some screen savers might not display as expected.

One Touch Internet

One Touch Internet provides fingerprint logon to password-protected Web sites. With it, you will not have to remember or type your user name or password for a Web site logon screen.

Setting up a logon screen requires that you provide your logon data the first time to create a fingerprint logon. Then, on subsequent logons, you only need to browse to the Web site and touch the reader with a registered finger. One Touch Internet automatically enters your user name and password in the logon screen text boxes. It can also be configured to submit your credentials for you by clicking the Submit button, or another equivalent button.

Internet Explorer users can access fingerprint-enabled Web accounts from the One Touch Menu. Just touch the reader to display the menu, point to Quick Links and then click the logon screen setup for the Web site you want to access. Internet Explorer will be launched automatically and your logon data will be submitted for you.

Logging On to Web Sites and Programs

Fingerprint logons can be created by you and your administrator. If you and your administrator created fingerprint logons for the same Web site or program, the fingerprint logon created by your administrator is used. In this case, DigitalPersona Pro prompts you to delete the fingerprint logon you created.

You can log on to a fingerprint-enabled logon screen by doing one of the following:

- Type the URL in a Web browser or launch the program that contains the logon screen for which you have created a fingerprint logon. The logon screen will display a DigitalPersona icon in the title bar of the Web browser or program, indicating that you can touch the reader with any registered finger to log on to the specific Web site or program.

A balloon indicates that the Web site or program is set up for fingerprint logon

Note
If you created more than one account for the Web site or program, you are prompted to choose the account data you want to use to log on.

- If you have a Quick Link for a Web site, point to Quick Links on the One Touch Menu, and then click the fingerprint logon title that corresponds to the Web site you want to access. If you configured the fingerprint logon to submit your account information automatically, you are immediately logged on.
- If required fields were left blank in the account data when the fingerprint logon was created, the Enter Account Data dialog box displays. Type the required data in the fields and click OK to log on.

Creating Fingerprint Logons

Creating a fingerprint logon requires you to enter your account data with DigitalPersona Pro once. Then, on subsequent logons, you only need to browse to the Web site, or launch the program, and touch the reader with any registered finger. DigitalPersona Pro automatically enters your user name and password and any other necessary account data in the appropriate logon screen text boxes and, if configured, submits your account data.

Your administrator may have already created fingerprint logons for you. If so, you should use the fingerprint logons from your administrator instead of creating your own.

To create a fingerprint logon for a Web site or program

1 Open the logon screen of the Web site or program.
2 Touch the reader with any registered finger and click Create Fingerprint Logon on the One Touch Menu.

Note
If Create Fingerprint Logon is not on the One Touch Menu, your administrator has not installed this feature on your computer.

3 The title of the logon screen displays on the Create Fingerprint Logon dialog box. Click Continue.
4 In the Logon Title text box, the title of the Web site uniquely identifies the logon screen in the Fingerprint Logon Manager and the Quick Links submenu on the One Touch Menu. You can type a different title in the text box.
5 Check Display in Quick Link list to add the fingerprint logon to the Quick Links submenu on the One Touch Menu.

Note
Quick Links are for Web sites only and not for programs.

6 DigitalPersona Pro determines logon fields and displays them in the Logon Information area. Type the appropriate account data in the corresponding text box for each field required for logon. For example, in the Password text box, you would type the password you use to access the Web site or program. If a field required for logon is not displayed in the Logon Information area, click Choose Fields to select the additional fields.

Note
As you point to each logon field in the Logon Information area, the corresponding field on the logon screen is highlighted, such as a text box and drop-down menu.

7 Select the button from the logon screen that is used to submit the account data. DigitalPersona Pro may recognize multiple buttons on some Web sites or programs. You may choose to submit your account data yourself each time you log on to the Web site or program by selecting Do Not Submit.
8 Click OK to create the fingerprint logon.

The DigitalPersona icon on the logon screen title bar of the Web site or program indicates that touching the reader with any registered finger will log you on to the Web site or program. You may add more than one account for a Web site or program.

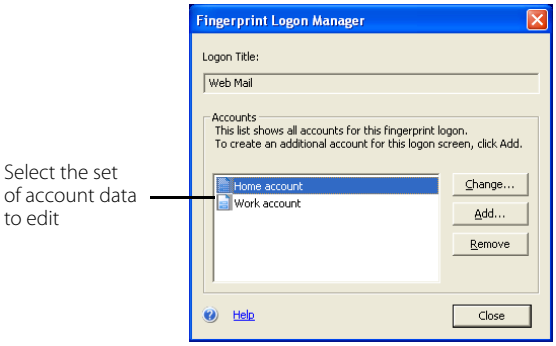
Editing Fingerprint Logons for Web Sites and Programs

You can add, change or remove fingerprint logons for Web sites and programs using the Fingerprint Logon Manager. To access it, browse to the Web site or launch the program and click the DigitalPersona icon, which is located in the title bar.

Note

When you want to make changes to a fingerprint logon for a Web site, do not use a Quick Link to browse to the Web site logon screen if the fingerprint logon is set up to automatically submit your logon information. Instead, browse to the Web site manually and click the DigitalPersona icon on the title bar.

If a fingerprint logon was created by your administrator, you are only allowed to add and delete account data. You cannot delete the fingerprint logon.



The following describes the Fingerprint Logon Manager functions:

- **Change.** To modify the account data entered by a fingerprint logon, select the account and then click Change. On the Edit Fingerprint Logon dialog box, edit your existing account data in the appropriate text boxes and click OK. You can also change the fingerprint logon title and Quick Link settings.
- **Add.** To add additional account data to the fingerprint logon for a Web site or program, click the Add button on the Fingerprint Logon Manager. This will

launch the Create Fingerprint Logon dialog box. Specify the additional account data for the logon screen as described in Creating a Fingerprint Logon. When logging on to the Web site or program using DigitalPersona Pro, you will be prompted to choose the account data you want to use.

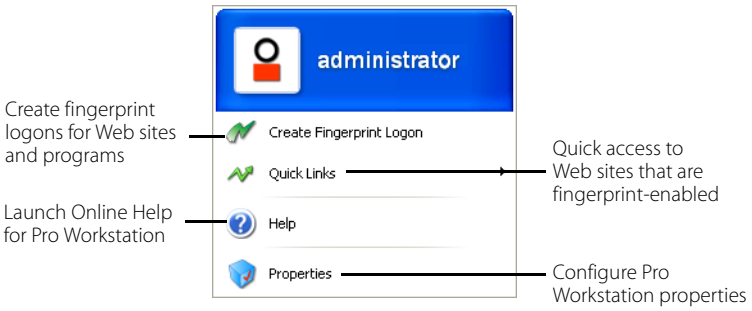
Note
When logging on the Web site, you will now be prompted to choose the set of account data before you can log on.

- **Remove.** To remove a fingerprint logon, select the title of the fingerprint logon in the list on the Fingerprint Logon Manager and click Remove. If you remove the last account for a fingerprint logon, the fingerprint logon is deleted. You can delete the account data of a fingerprint logon created by your administrator, but you cannot delete the actual fingerprint logon.

Note
If there are multiple sets of account data for a logon screen, other logon screen data—such as the submit button—is not deleted until you delete all sets.

Using the One Touch Menu

When enabled, the One Touch Menu provides fast and convenient access to the personal One Touch applications, settings and help. To enable and configure the One Touch Menu, refer to "Quick Actions" on page 117. To display the One Touch Menu, place a registered finger on the reader.



The next sections describe each item on the One Touch Menu.

Create Fingerprint Logon

The Create Fingerprint Logon menu item launches the Fingerprint Logon Wizard, which guides you through the process of setting up your personal Web site logon screens, as described in "One Touch Internet" on page 109.

This item appears on the One Touch Menu only if One Touch Internet is installed.

Quick Links

Point to Quick Links to display the One Touch SignOn and the One Touch Internet logon data you created for Web sites browsed by Internet Explorer. Click a Quick Link to launch the associated password-protected Web site. Your account data will also be submitted.

For more information on One Touch SignOn and creating profiles for Web sites, refer to "Setting Up Logon Screens with One Touch SignOn" on page 58.

Help

Clicking Help launches the Online Help file for DigitalPersona Pro Workstation for Active Directory. It contains step-by-step instructions for using various product features, including use of the One Touch applications.

Properties

Click Properties to configure DigitalPersona Pro on your computer, as described in "Configuring DigitalPersona Pro Workstation" on page 116.

Reader Icon and Menu

When you install DigitalPersona Pro Workstation for Active Directory, a reader icon is placed in the notification area on the taskbar. It displays the connectivity status of the reader and provides convenient access to various functions.

There are two different icons used to display the connectivity status of the reader:

- When the reader is connected and the driver is installed, the reader icon appears.
- If the reader is not plugged in, a red X is displayed over the reader icon.

Indicates the reader is connected and the driver is installed

Indicates the reader is disconnected or the driver is not installed

The reader icon also provides a context menu containing various Pro functions.

Each menu item is described in the next sections.

Lock Computer

Lock Workstation locks your computer while you are away from your desk and allows you to unlock it using the logon policy applied to the computer. You can also double-click the reader icon to lock your computer.

Properties

Click Properties to configure DigitalPersona Pro on your computer, as described in "Configuring DigitalPersona Pro Workstation" on page 116.

Help

Identical to the function of the Help menu item on the One Touch Menu, clicking Help launches Online Help for DigitalPersona Pro Workstation.

About

Click About to get the version number of the DigitalPersona Pro Workstation software.

Hide Icon

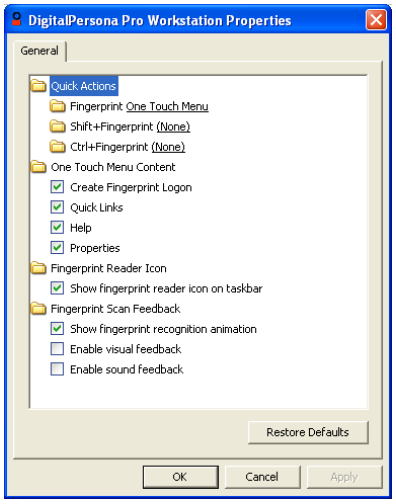
To hide the reader icon, click Hide Icon. To display the icon again, use the DigitalPersona Pro Properties dialog box, as described in "Show Fingerprint Reader Icon on the Taskbar" on page 118.

Note

On Windows 98 and Me, you can also launch the Fingerprint Registration Wizard from the reader icon context menu.

Configuring DigitalPersona Pro Workstation

You can edit various Workstation properties using the DigitalPersona Pro Properties dialog box. To open it, click the reader icon in the notification area and then click Properties.



When you modify the properties, click OK to implement the new settings and close the dialog box.

The DigitalPersona Pro Properties dialog box contains several folders. The following sections describe each property that can be configured for DigitalPersona Pro.

Quick Actions

In the Quick Actions folder, you can assign actions to be performed when touching the fingerprint reader and when touching the reader while pressing a key. The actions that you can assign are:

- None
- Create a fingerprint logon
- Display this Help file
- View the One Touch Menu
- Open the Properties dialog box
- View the Quick Links submenu

You can assign actions to:

- **Fingerprint.** The default setting is to view the One Touch Menu.
- **Ctrl + Fingerprint.** The default setting is None.
- **Shift + Fingerprint.** The default setting is None.

Show Fingerprint Reader Icon on the Taskbar

When checked, the fingerprint reader icon is displayed in the notification area on the taskbar, which is described in "Reader Icon and Menu" on page 115.

Show Fingerprint Recognition Animation

Select this option to display an animation indicating when a fingerprint has been scanned. It indicates that you may lift your finger from the reader and also shows a finger touching the reader whenever the user places a finger on the reader. A green check mark indicates a successful scan. A red question mark indicates an unsuccessful scan.

Enable Visual Feedback for Fingerprint Scan

This option displays an animation on the desktop, which consists of a series of circles that quickly expand from the center of the screen outward, when a fingerprint scan is acquired by the reader.

For more information about visual and audio feedback when a fingerprint scan is acquired, refer to "Fingerprint Scan Acquisition Feedback" on page 93.

Enable Sound Feedback for Fingerprint Scan

Check Enable Sound Feedback for Scan Capture to play a sound when the reader acquires a fingerprint scan. It indicates that you may lift your finger from the reader. Different sounds are played for successful and unsuccessful scans. You may select different sounds from Control Panel.

Refer to "Fingerprint Scan Acquisition Feedback" on page 93 for more information about visual and audio feedback when a fingerprint scan is acquired by the reader.

One Touch Menu

In the One Touch Menu folder, the following menu items are added to the One Touch Menu if the check box is selected:

- **Create Fingerprint Logon.** Displays the Create Fingerprint Logon dialog box.
- **Quick Links.** Displays the list of Quick Links.
- **Help.** Displays this Help file.
- **Properties.** Displays the Properties dialog box.

Fingerprint Reader Usage and Maintenance

This section provides reader usage and maintenance guidelines, which are intended to maximize fingerprint registration and authentication performance.

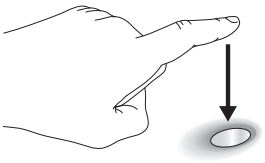
Proper usage of the reader during fingerprint registration and authentication, as well as a well-maintained reader, is crucial to achieving optimal fingerprint recognition performance.

The next section, "Proper Fingerprint Reader Usage" describes the proper way to use the reader to register fingerprints and authenticate using them. It is followed by reader maintenance instructions, provided in "Cleaning the Reader" on page 120.

Proper Fingerprint Reader Usage

To reduce the number of false rejects, you must place a finger on the reader correctly when registering fingerprints and authenticating.

During both processes, you must place the pad of your finger—not the tip or the side—in the center of the oval window of the reader in order to maximize the area of the finger that touches the reader window.



Place the entire pad of your finger squarely on the sensor window

Apply even pressure. Pressing too hard will distort the scan; pressing too lightly will produce a faint, unusable scan. Do not "roll" your finger.

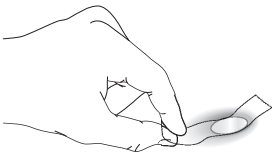
To complete the fingerprint scan, hold your finger on the reader until you see the reader light blink. This may take longer if the skin is dry. When the light blinks and, if configured, a sound plays, you may lift your finger.

If the reader is capturing your fingerprint scan as indicated by the reader blink, but DigitalPersona Pro consistently rejects it, you may need to reregister that finger by first deleting it and then registering it again, as described in "Managing Fingerprint Credentials" on page 94.

Cleaning the Reader

The condition of the reader window has a large impact on the ability of the reader to obtain a good quality scan of a fingerprint. Depending on the amount of use, the reader window may need to be cleaned periodically.

To clean it, apply the sticky side of a piece of adhesive cellophane tape on the window and peel it away.



Under heavy usage, the window coating on some readers may turn cloudy from the salt in perspiration. In this case, gently wipe the window with a cloth (not paper) dampened with a mild ammonia-based glass cleaner.

Reader Maintenance Warnings

There are several things you should never do when cleaning or using the reader:

- Do not pour the glass cleaner directly on the reader window.
- Do not use alcohol-based cleaners.
- Never submerge the reader in liquid.

- Never rub the window with an abrasive material, including paper.
- Do not poke the window coating with your fingernail or any other item, such as a pen.

The fingerprint reader is for indoor home or office use only.

Troubleshooting 8

This chapter provides assistance to users having difficulty using the One Touch programs, being authenticated with your fingerprint, or the U.are.U Reader.

Reader Troubleshooting

This section contains reader troubleshooting tips for a variety of symptoms.

Reader Does Not Light Up During Installation or Restart

If the reader does not light up during installation or restart after installation of DigitalPersona Pro, try the following:

- Ensure the reader is connected directly to a USB port on the computer—not a USB hub.
- Connect the reader to another USB port on the same computer.

If neither step resolves the issue, try any of the options in the three sections:

Reinstall USB Driver

Reinstalling the USB driver for the reader sometimes corrects the problem.

To reinstall the USB driver for the reader

1 Log on using your Windows password.
2 On the Start menu, point to Settings and click the Control Panel. Click the Hardware tab and then the Device Manager button.
3 Expand the Biometric item in the table and click Uninstall on the context menu of the UareU 4000 Fingerprint Device listing.
4 Unplug the reader.
5 Locate the UsbDPFp.sys file (C:\WINNT\System32\drivers) and delete it.
6 Plug the reader in again. The installation wizard should automatically launch, locate the reader driver software and install it.

Note

If the wizard prompts you to locate the driver, point to the DpDrv folder in the Windows root folder.

7 Restart the computer.

Test Ports with Second Reader

If available, take a working reader from another computer and plug it in your computer. If it works, the original reader may be faulty; if not, the USB controller may be configured improperly (see "Check USB Controller Configuration" on page 124).

In addition, you can also try plugging the original reader in a USB port on another computer to verify whether the reader is faulty or the computer on which you are trying to install it.

Check USB Controller Configuration

Your computer must be configured to use USB devices. This section guides you through the process of verifying this functionality.

To check the USB controller configuration on your computer

1. On the Start menu, point to Settings and click Control Panel. Then, click System.
2. Click the Hardware tab and then the Device Manager button to verify that "Universal Serial Bus controller" is listed as an entry.
3. If the entry exists, click the plus sign (+) next to Universal Serial Bus controller and verify that icons for USB Root Hub and USB Port are present.
4. If none of the entries or icons are visible or if they have exclamation marks or red X's through them, you must contact the manufacturer of your computer to acquire the necessary software to support USB devices.

Reader Light Went Out When In Use

If the reader light is no longer lit after the reader has been in use for some time, try these steps to determine the source of the problem:

- Unplug the reader and then plug it in again. Check the USB cable connection to ensure a secure fit.
- Connect the reader to a different USB port on your computer to verify that the first USB port is working properly.
- Connect the reader to a different computer to see if the reader is malfunctioning.

If the reader functions on another USB port or computer, the first USB port is faulty. If the reader works on another computer—but not on the first one—check the USB controller configuration, as described in "Check USB Controller Configuration" on page 124.

Reader Does Not Blink When Touched

If the reader light is on, but does not blink when touched, unplug the reader and then plug it in again. If this does not correct the problem, try cleaning the reader, as described in "Cleaning the Reader" on page 120.

Software Does Not Respond When Reader Is Touched

If the reader light is on and it blinks when touched but the fingerprint is not scanned, unplug the reader and then plug it in again. If this does not correct the problem, try cleaning the reader, as described in "Cleaning the Reader" on page 120. If these steps do not correct the problem, try restarting your computer.

Reader Blinks Constantly

If the reader light blinks constantly, the reader window may need cleaning. Follow the instructions in "Cleaning the Reader" on page 120.

One Touch Programs Troubleshooting

The following sections describe remedies for issues you may encounter with the One Touch programs of DigitalPersona Pro Workstation.

One Touch Logon Troubleshooting

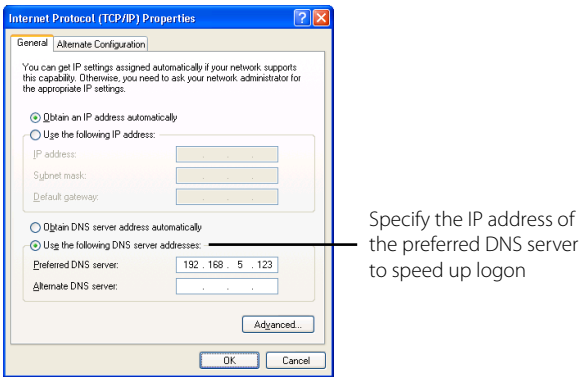
If logon seems particularly slow, it may be because the computer is spending excess time looking for the DNS server. In this case, you can speed up authentication by manually specifying the preferred DNS IP address.

To manually specify the preferred DNS IP address on a DigitalPersona Pro Workstation

1 Locate the My Network Places icon on the desktop and click Properties on its context menu.
2 On the Network Connections dialog box, locate the Local Area Connection icon and click Properties on its context menu.

3 Select Internet Protocol (TCP/IP) on the Local Area Connection Properties dialog box and then click the Properties button.

4 Select the Use the following DNS server addresses radio button and type the IP address of the DNS server in the Preferred DNS server text box.



5 Close all dialog boxes to save your changes.

One Touch Internet and OTS Troubleshooting

Following are issues you may encounter when using One Touch SignOn and One Touch Internet:

- Due to the design of a particular Web site or program, One Touch SignOn and One Touch Internet may not be able to save certain logon credentials. You can try to create a template manually which may overcome the issue. If you still have problems, you should report the problem to DigitalPersona to attempt to engineer a solution or workaround to the problem.
- A submit button may not be found when setting up a logon screen that uses a non-standard method for submitting forms. In this case, you will have to manually submit logon data by clicking the submit button on the Web page after One Touch SignOn or One Touch Internet fills in the field values.
- If a Quick Link is not working properly, ensure you have entered the Web page title in the logon screen setup exactly as it appears on the Web page.

Also, verify that the URL specified in the logon screen setup is correct. Some Web pages redirect users to a temporary URL that expires after one-time use. If the logon screen you set up with One Touch SignOn or One Touch Internet redirects users to temporary and unique URLs, for example, with Microsoft's Hotmail, you will have to manually type the URL in the logon profile instead of using the URL One Touch SignOn assigns by default.

Installation Troubleshooting

See the DigitalPersona Web site for more updates at http://www.digitalpersona.com/support.htm.

Using the Diagnostic Center

If you encounter issues when trying to install or run DigitalPersona Pro, you can use the Diagnostic Center to help identify issues. The Diagnostic Center is a utility that detects potential configuration issues and server connections before and after installation. The Diagnostic Center can determine missing files or incompatible versions of files. It can test connections to servers and check to make sure that DigitalPersona Pro services are running. When you run the diagnostics, a list of items found displays.You can click items in list to display details on issues and how to resolve them.

For more complex cases where the diagnostics do not identify any issues but a problem still exists, you can turn on tracing to create trace files while reproducing the problem. You can collect the trace files to send to DigitalPersona Technical Support. Trace information is not displayed or analyzed by the Diagnostic Center.

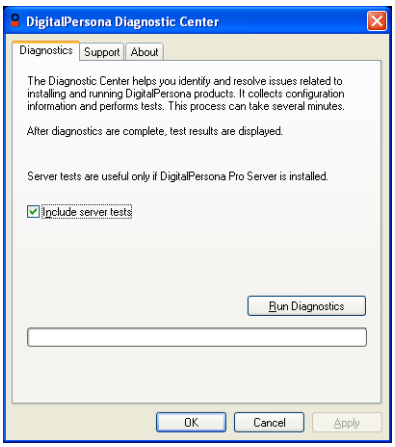
The Diagnostic Center is installed as part of the DigitalPersona Pro Server and Workstation installations.

Running the Diagnostic Center

You can run the diagnostic tests at any time to receive information on your current environment and DigitalPersona Pro installation.

To run the Diagnostic Center

1 Double-click DpDiagCt.exe, which is located in the DigitalPersona\bin folder under the Program Files folder.
The Diagnostic Center dialog displays.



2 On the Diagnostics tab, select the check box to include server connection tests if your deployment includes Pro Servers.
3 Click the Run Diagnostics button.
The progress of the diagnostic test is displayed in a progress bar.
The Diagnostic Center Results dialog displays.
4 Click items in the list for more information and how to resolve issues.

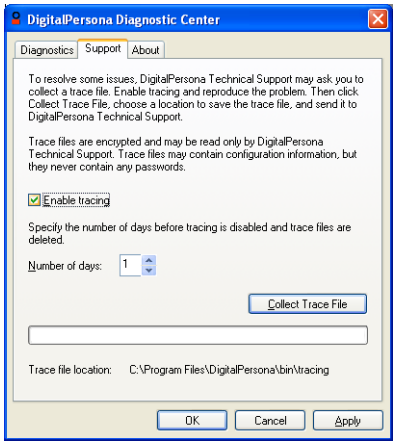
Collecting Trace Files for Troubleshooting

If no issues are found by running the diagnostics, you can turn on tracing, reproduce the problem, and send the trace files to DigitalPersona Technical Support to investigate the problem.

To collect trace files

1 Click the Support tab.

2 Select the Tracing is enabled check box.



3 Specify a number of days to collect the tracing information. This might vary from one to many days depending on the issue. Setting a number of days prevents the trace files from becoming so large that your hard drive becomes full.

4 Reproduce the problem by repeating the steps that lead up to the issue.

5 After the issue is reproduced, click the Collect trace files button.
The trace files are saved in a .zip file. You can attach the .zip file to an email and send it to DigitalPersona Technical Support.

6 After the trace files are collected and sent to DigitalPersona, turn off tracing by unchecking the check box. The trace files are deleted from your hard drive. Tracing is automatically turned off after the number of days you specified.

Common Issues Found

Types of issues or information found by running the diagnostics include:

- Software information
- Product version numbers
- DigitalPersona Pro Server information such as server connection status and which server connection was last established
- OTS template names and date created
- GPO settings
- Key error logging and tracking
- Fingerprint reader information such as connection status, reader model and hardware version, serial number, driver version
- USB controller information

Appendix A

Event Log Specifications

There are four categories of DigitalPersona Pro events, which are logged in the Windows Event Log.

The following table lists each event category, ID range and the logs they can be found in:

Category	Event IDs	Windows Event Log	Page
User Authentication	1000-1099	Security Log	131
User Management	1100-1199	Security and System Logs	133
DNS Registration	1200-1299	System Log	139
Logon Events	1400-2006	System Log	142

You can view DigitalPersona Pro events in the Event Viewer and use it to filter and search for these events.

Refer to “Logging and Auditing” on page 52 for instructions on filtering and searching for DigitalPersona Pro events in the Windows Event Viewer.

Following are the listings and descriptions of each event category and event that is logged.

User Authentication Events

User Authentication events are logged when DigitalPersona Pro software requests secure application data for a particular user.

Secure Application Data Released

This event is logged when an application using DigitalPersona Pro for authentication releases secure application data. It occurs when the user is prompted for a registered finger and the fingerprint scan is acquired and recognized as a registered finger.

Description
Secure application data **[data]** for Pro User **[name]**, (Fingerprint: **[number of finger]**), was released.

Event ID
1003

Type
Audit success

More Information
[data] is the name the application gives to the secure application data. **[name]** is the full user name of the user, for example, domain\user. The number of the registered finger is supplied as an integer, ranging from zero to nine. Zero represents the left pinkie finger; nine, the right pinkie finger.

Secure Application Data Denied

This event is logged when a user is prompted to authenticate by an application using DigitalPersona Pro, but the acquired fingerprint scan was not recognized as a registered finger.

Description
Secure application data **[data]** for Pro User **[name]** was denied.

Event ID
1002

Type
Audit fail

More Information
[data] is the name the application gives to the secure application data and can be: S.MainSystemLogon or U.OTS ProtectedStorage. **[name]** is the full user name of the user, for example, domain\user. If this event is logged frequently, it may indicate that a user is having difficulty using the reader or attempts are being made to gain unauthorized access to the network.

User Management Events

User Management events are logged when a user record is created, updated or deleted.

User Record Added

This event is logged after a user successfully registers a finger on a DigitalPersona Pro Workstation and cached credentials are enabled or not configured.

Description

A record was added to the database for Pro User GUID **`[GUID]`**.

User name: **`[name]`**

Domain: **`[domain]`**

Modified by: **`[acting domain]\[acting user]`**

Event ID

1101

Type

Audit success

More Information

Specifies the user account and domain for which the registered finger was added, unless the user who added the registered finger to the account is different from the user the finger was registered for. The event also indicates the user, and the domain they belong to, from which the event originated in the Modified by field (format: NT Authority\System).

Record Add Failed

An attempt to add a record for a user failed, which may be due to a logon policy conflict or insufficient database write permission.

Description

A user record could not be added to the Pro database.

Event ID
1102

Type
Audit fail

More Information
Other supplied information includes the user name and domain that the record could not be added to, as well as the user name and domain the event was originated by. The error message generated by Windows is also displayed.

User Record Updated

This event is logged when a user modifies secure application data or adds or deletes registered fingers.

Description
The record was updated for Pro User GUID: **[GUID]**

User name: **[name]**

Domain: **[domain]**

Modified by: **[acting domain]****[acting user]**

Description: **[description]**

Event ID
1103

Type
Audit success

More Information
The user name and domain is supplied for both the user the data was modified for (User name and Domain fields) and the user who performed the modification in the Modified by field. **[description]** lists the portion of the user record that was updated. Possible values are “Security Descriptor Updated,” “Secret **[secret name]** Added”, “Secret **[secret name]** Replaced”, “Password

Added" and "Fingerprint **[number]** Added." [secret name] is the name of the application in which the secure data resides: S.MainSystemLogon or U.OTS ProtectedStorage. The number of the registered finger is supplied as an integer, ranging from zero to nine. Zero represents the left pinkie finger; nine, the right pinkie finger.

User Record Update Failed

This event is logged when a user attempts to modify secure application data or register or delete fingers, but does not have sufficient write privileges to the database or the DigitalPersona Pro settings conflict with the attempted operation, for example, a user tries to register more fingers than allowed by the "Maximum Number of Fingers a User Can Register" property, as described on 40.

Description

The user record was not updated for Pro User GUID **[GUID]**.

Event ID

1104

Type

Audit fail

More Information

The user name and domain is specified for both the user to which the record belongs, as well as the user who attempted to modify the record. The error generated by Windows is also displayed.

User Record Deleted

This event indicates that a user record was deleted.

Description

The record was deleted for Pro User GUID **[GUID]**.

Event ID
1105

Type
Audit success

More Information
The event indicates the user and domain to which the deleted record belonged, as well the user name and domain of the user who deleted the record.

User Record Delete Failed

An attempt to delete a user record failed.

Description
The user record was not deleted for Pro User GUID `[GUID]`.

Event ID
1106

Type
Audit fail

More Information
The user name and domain of the user the record belongs to is displayed, as well as the user name and domain the delete request was originated by. The Windows error generated by the failed delete request is also displayed.

User Record Consistency Failed

This event is logged when a consistency check between the Pro User GUID and the AD User GUID fails. It suggests network tampering or an attempt to comprise security.

As a security measure, DigitalPersona Pro associates user credentials to a user by cryptographically binding the user GUID (sometimes referred to as the Pro User GUID) to credential data, which is also bound to the Active Directory User

GUID. The cryptographic key for the Pro User GUID must be the identical to the key for the Active Directory User GUID or this error event is logged.

In another case, the consistency check will fail if an administrator modifies Pro user data in Active Directory without using a Pro Workstation.

Description

The consistency check for user credential data failed. The Pro User GUID `[GUID]` bound to the credentials failed to match the AD User GUID `[GUID]`.

Event ID

1113

Type

Error

User Secret Consistency Failed

This event is logged when a consistency check between the Pro User GUID and the AD User GUID fails. It suggests network tampering or an attempt to comprise security.

As a security measure, DigitalPersona Pro associates secure user application data to a user by cryptographically binding the user GUID (sometimes referred to as the Pro User GUID) to the secure application data, which is also bound to the Active Directory User GUID. The cryptographic key for the Pro User GUID must be the identical to the key for the Active Directory User GUID or this error event is logged.

In another case, the consistency check will fail if an administrator modifies Pro user data in Active Directory without using a Pro Workstation.

Description

The consistency check for secure application data `[data]` failed. The Pro User GUID `[GUID]` bound to the secure application data failed to match the AD User GUID `[GUID]`.

Event ID
1114

Type
Error

User Record Signature Check Failed

This event is logged when the cryptographic signature of credential data could not be verified.

Description
The signature of the credential data could not be verified.

Event ID
1115

Type
Error

More Information
The name of the user and the Pro User GUID is displayed.

User Secure Signature Check Failed

This event is logged when the cryptographic signature of the secure application data could not be verified.

Description
The signature of the secure application data could not be verified.

Event ID
1116

Type
Error

More Information

The Pro user GUID, user name and the name of the secure application data is displayed.

User Account Locked Out

This event is logged when the user attempted to log on to Windows with an unrecognized fingerprint more than the specified number of times allowed in the GPO.

Description

The user account is locked out.

Event ID

1117

Type

Error

More Information

The Pro user GUID and user name is displayed.

DNS Registration Events

DNS Registration events are logged when the Pro Server software fails to register or remove DigitalPersona Pro registration records from the Active Directory DNS server.

DNS Update Disabled

When an administrator disables DNS registry updates on the DNS Server—and the Pro Server attempts to write SRV RRs to the DNS registry—this event is logged. As a result of disabled DNS registry updates, the Pro Server will not register DNS records and any computer that connects to it will not be able to use the Pro Server for authentication.

Description
Registration of the DNS record was not performed because Dynamic DNS updates were disabled. Client computers will not be able to find the server.

Event ID
1201

Type
Warning

More Information
The name of the server is displayed, as well as the names of the domain and site it belongs to.

DNS Registration Failed

This event is logged when the Pro Server is unable to register SRV RRs with the DNS server. It can occur when Pro Server attempts to register records during DNS server refresh, installation and restart, as well as when the network connection or the DNS server itself is down. Other factors that may generate this error event include insufficient permissions to update the DNS server and a DNS server that does not support dynamic updates.

Description
Registration of the server failed. Client computers will not be able to find the server.

Event ID
1202

Type
Error

More Information
The name of the server, as well as the names of the domain and site it belongs to, is displayed. The Windows error generated by the attempt to register with a DNS server is also displayed.

DNS Unregistration Failed

This event is logged when DigitalPersona Pro Server failed to unregister. The problem must be resolved by manually removing the DNS record. In some cases, restarting and stopping the server can solve the problem.

Description

Removal of DNS record failed.

Event ID

1203

Type

Error

More Information

The name of the Pro Server affected by this event is displayed, as well as the name of the domain and site it belongs to. The Windows error generated by this event is also displayed.

DigitalPersona Name Translation Failed

This event is logged when domain name cannot be resolved and it can prevent Pro Workstations from working properly.

Description

The domain name could not be resolved in namespace `[namespace]`.

Event ID

1301

Type

Warning

More Information

The name of the Pro Server affected by this event is displayed, as well as the name of the domain and site it belongs to. The Windows error generated by this event is also displayed.

Logon Events

User Logged In

This event is logged when DigitalPersona Pro Server failed to unregister. Workstations will not be able to find this server. The problem must be resolved by registering the server manually.

Description

User logged in, name: **`[name]`**, domain: **`[domain]`**, finger used: **`[finger]`**

Event ID

1401

Type

Audit success

More Information

The name of the user is displayed, as well as the name of the domain and the finger used.

User Logon Failed

This event is logged when DigitalPersona Pro Server failed to unregister. Workstations will not be able to find this server. The problem must be resolved by registering the server manually.

Description

User logged in, name: **`[name]`**, domain: **`[domain]`**

Event ID

1402

Type

Error

More Information

The name of the user is displayed, as well as the name of the domain.

GINA Password Logon

This event is logged when DigitalPersona Pro a user logs on to Windows.

Description

Password: **`[Yes/No]`**, Fingerprint: **`[Yes/No]`**, Smartcard: **`[Yes/No]`**, Fingerprint PIN: **`[Yes/No]`**

Event ID

2001

Type

Audit success

More Information

The password, fingerprint, smart card and fingerprint PIN display Yes if used and No if not used for logon.

GINA Unlock

This event is logged when a DigitalPersona Pro user unlocks a locked Windows computer.

Description

Password: **`[Yes/No]`**, Fingerprint: **`[Yes/No]`**, Smartcard: **`[Yes/No]`**, Fingerprint PIN: **`[Yes/No]`**

Event ID

2002

Type

Audit success

More Information

The password, fingerprint, smart card and fingerprint PIN display Yes if used and No if not used for unlocking the computer.

GINA Register PIN

This event is logged when a DigitalPersona Pro user registers a fingerprint PIN.

Description

A new Fingerprint PIN has been registered

Event ID

2003

Type

Audit success

GINA Change PIN

This event is logged when a DigitalPersona Pro user changes the fingerprint PIN.

Description

The Fingerprint PIN has been changed.

Event ID

2004

Type

Audit success

GINA Smart Card Unlock

This event is logged when a DigitalPersona Pro user uses a fingerprint to unlock the smart card instead of using the smart card PIN.

Description

The fingerprint was used to unlock the smartcard: **`[Yes/No]`**

Event ID

2005

Type

Audit success

More Information

The fingerprint displays Yes if used and No if not used for unlocking the smart card.

GINA Fingerprint PIN Registration Canceled

This event is logged when a DigitalPersona Pro user begins to register a fingerprint PIN and then cancels the registration process.

Description

The fingerprint PIN registration was canceled.

Event ID

2006

Type

Audit success

Appendix B

Configuring DigitalPersona Pro Workstation Settings

After installation of DigitalPersona Pro, administrators can override the default DigitalPersona Pro Properties settings in the Windows Registry for One Touch Menu content and Quick Actions.

Warning

Editing registry settings may damage your system. Before making changes, back up your data. Use the Last Known Good Configuration startup option if you encounter problems after making changes to the registry.

Instructions in the next two sections are provided to configure the One Touch Menu and Quick Actions using the Windows Registry.

Note

Changes made to the settings in the registry do not take precedence over local configuration by end users.

Configuring the One Touch Menu Content

You can use the Windows Registry Editor to modify registry keys for the One Touch Menu, export the new settings in a .reg file and import those settings on the target machines, which determines what menu items are displayed.

To configure the One Touch Menu menu content

1 Launch the Windows Registry Editor.

2 In the Registry Editor, navigate to the following key:
`HKEY_LOCAL_MACHINE\SOFTWARE\DigitalPersona\Applications\OTAppSettings\MenuContent`
The following keys—all with a default value of 1—are listed:
- **Help.** Launches the online help for DigitalPersona Pro.
- **OTI.** Displays the menu item, “Create Fingerprint Logon,” in the One Touch Menu and launches the Fingerprint Logon Wizard.

- **Properties.** Opens the DigitalPersona Pro Properties dialog box. See "Configuring DigitalPersona Pro Workstation" on page 116.
- **QuickLinks.** Allows end users to access fingerprint-enabled Web sites and applications from the One Touch Menu, as described in "One Touch Internet" on page 109.
- **Registration.** Launches the Fingerprint Registration Wizard, which is described in "Managing Fingerprint Credentials" on page 94. The One Touch Menu item displays as "Fingerprint Registration Wizard" only if One Touch Logon is installed.

3 To remove an item from the One Touch Menu, set the corresponding key value to 0. To add an item, set the key to 1.

Configuring Quick Actions

The procedure for modifying Quick Actions settings is similar to the One Touch Menu registry configuration. Using the Windows Registry Editor, you can specify the Quick Actions that correspond with a DigitalPersona Pro feature.

To configure Quick Actions in the Windows Registry

1 Launch the Windows Registry Editor.

2 In Registry Editor, navigate to the following registry key:
`HKEY_LOCAL_MACHINE\SOFTWARE\DigitalPersona\Applications\OTAppSettings\QuickActions`
The key value finger has a default value of None.

3 Select a Quick Action feature by setting the value to 1 of the following strings:
- Help
- Lock Workstation
- OTI (to access One Touch Internet)
- OTMenu (to access One Touch Menu)
- Properties
- QuickLinks

Appendix C

Limited Warranties and Warranty Service

The DigitalPersona Pro for Active Directory System (the "SYSTEM") you acquired may include: the U.are.U Reader, (the "READER"); and the DigitalPersona Pro for Active Directory Workstation and DigitalPersona Pro for Active Directory Server software, the software embedded in the READER and their associated media, printed material and "online" or electronic documentation (the "SOFTWARE PRODUCT"). The SOFTWARE PRODUCT is licensed, not sold, as set forth in the Installation Software screen "License Agreement."

LIMITED WARRANTY; LIMITATION OF REMEDIES

The warranties provided by DigitalPersona in this statement of limited warranty apply only to SYSTEMS you originally purchased from DigitalPersona or an authorized reseller for your personal or business use, and not for resale.

DigitalPersona warrants that the SOFTWARE PRODUCT will perform substantially in accordance with the applicable documentation and that its media will be free from defects in material and workmanship for a period of ninety (90) days from the date of original purchase. DigitalPersona does not warrant that use of the SOFTWARE PRODUCT will be uninterrupted or error-free. DigitalPersona warrants that the READER will be free from defects in materials and workmanship for a period of one (1) year from the original date of purchase.

If you discover an error or defect covered under this limited warranty, DigitalPersona's sole obligation, and your exclusive remedy, shall be, at DigitalPersona's option, either (a) to return the price paid, if any; or (b) to replace the SOFTWARE PRODUCT or the READER using new or remanufactured components. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Any replacement of the READER will be warranted for the remainder of the original warranty period.

Warranty Service. To obtain your remedy under this warranty you must deliver the defective product and the original sales receipt to the place of purchase. For purchases made directly from DigitalPersona, you must first contact DigitalPersona Customer Service and obtain a Return Merchandise Authorization (RMA) number before returning the product to DigitalPersona. You must pre-pay shipping charges to return the product to DigitalPersona and insure the shipment or accept the risk of loss or damage during shipment. DigitalPersona shall not be responsible for any returned product that is not packaged properly or is returned without a valid and visible RMA number.

Product Failures Not Covered By This Warranty. This warranty covers defects in manufacturing that arise during normal use and proper care in an office environment. It does not cover damage caused by any misuse, improper maintenance, including physical abuse to the SOFTWARE PRODUCT or to the READER (for example, but not limited to, cuts or scratches to the READER window), or use of corrosive, abrasive, or improper cleaning materials, or any misapplication, improper modifications or repair, activity intended to circumvent the security devices incorporated into the READER or SOFTWARE PRODUCT, criminal activity, moisture, shipping, or high voltage surges from external sources such as power lines or other connected equipment. This warranty also does not apply to any product with an altered or defaced serial number. Opening the READER automatically voids this warranty.

Disclaimer of Warranties. EXCEPT FOR THE FOREGOING LIMITED WARRANTY, DIGITALPERSONA MAKES NO OTHER EXPRESS OR IMPLIED WARRANTIES TO THE MAXIMUM EXTENT PERMITTED BY LAW AND SPECIFICALLY DISCLAIMS THE WARRANTIES OF QUALITY, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS WITH REGARDS TO THE SYSTEM AS WELL AS ANY PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. IF SUCH DISCLAIMER OF ANY IMPLIED WARRANT IS NOT PERMITTED BY LAW, THE DURATION OF ANY SUCH IMPLIED WARRANTIES IS LIMITED TO 90 DAYS FROM THE DATE OF DELIVERY. SOME JURISDICTIONS DO NOT

ALLOW SUCH EXCLUSIONS OR LIMITATIONS, SO THEY MAY NOT APPLY TO YOU. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Provisions

Limitation on Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL DIGITALPERSONA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, GOODWILL, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, BREACH OF COMPUTER SECURITY SYSTEMS OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITYTO USE THE SYSTEM EVEN IF DIGITALPERSONA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. DIGITALPERSONA DOES NOT GUARANTEE THAT THE SYSTEM WILL MEET ALL YOUR REQUIREMENTS OR ALL REQUIREMENTS OF THE SOFTWARE OR HARDWARE WITH WHICH IT INTERACTS. IN NO EVENT WILL DIGITALPERSONA'S LIABILITY FOR ANY CLAIM, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, EXCEED THE PURCHASE PRICE OF THE SYSTEM PAID BY YOU. Some jurisdictions do not allow these exclusions or limitations, so such exclusions or limitations may not apply to you. The above limitations will not apply in case of personal injury in countries other than U.S.A. and Canada only if and to the extent that such limitations are expressly prohibited by applicable law.

Reverse Engineering. You may not reverse engineer, de-compile, or dis-assemble the SYSTEM in whole or in part; nor shall you attempt to recreate the source code from the object code of the SOFTWARE PRODUCT. Any other activity regarding the form or substance of the SYSTEM will be allowed only to the extent such activity is expressly permitted by applicable law.

Export Controls. You agree that you will not directly or indirectly export the SYSTEM and related technical data in violation of Export Administration regulations of the U.S. Department of Commerce and other applicable laws. You further agree that you will not export, re-export, divert or transfer the SYSTEM (a) into, or to a national or resident of any country to which the United States has embargoed goods, (b) or to anyone included in the U.S. government List of Specially Designated Nationals, the Table of Denial Orders, the Entity List, (c) or to anyone involved in the manufacturing and proliferation of weapons in violation of U.S. applicable laws. By using the SYSTEM you are representing and warranting that you are not located in, or under the control of, or a national resident of any such country or on any such lists, or involved in any such activity.

U.S. Government Rights. If you are an agency or instrumentality of the United States Government, the Software and Documentation included in the SOFTWARE PRODUCT are "commercial computer software" and "commercial computer software documentation," and pursuant to FAR 12.212 or DFARS 227.7202, and their successors, as applicable, use, reproduction and disclosure of the Software and Documentation are governed by the terms of the End User License Agreement.

Regulatory Information

Any changes or modifications not expressly approved by DigitalPersona could void your authority to operate this equipment.

The U.are.U Fingerprint Reader has been tested and found to comply with the limits for a Class B digital device under Part 15 of the Federal Communications Commission (FCC) rules, and it is subject to the following conditions: a) It may not cause harmful interference, and b) It must accept any interference received, including interference that may cause undesired operation.

This device conforms to emission product standards EN55022(B) and EN50082-1 of the European Economic Community and AS/NZS 3548 Class B of Australia and New Zealand.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus as set out in the radio interference regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de Classe B prescrites dans le règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Index

Symbols

_uareupro SRV RR 29
  DNS Console path 30
  modifying Priority and Weight settings 30

A

About menu item 116
Active Directory containers 27
  Biometric Authentication Servers container 28
  Policies container 28
Active Directory Domain Configuration Wizard 23
Active Directory Domain Configuration Wizard, configuring a domain with 23
Active Directory Schema Extension Wizard 22
ADM file 35
  adding in MMC 36
  adding to a GPO 35
  viewing settings in MMC 37
administration, Pro Workstation 8, 33
attended registration
  deleting fingerprints 83
  permissions required 80
  using 80
auditing, using Windows Event Viewer 52
Authentication Server Object Name property 28
authentication, defined 11

B

BAS Locator settings 45
Biometric Authentication Servers container 28
  Server Version Object Name 28
  Service Configuration Container Name 28

C

Cache User Credentials on the Workstation property setting 43
cached credentials
  defined 11
  in One Touch Logon 101
changing policy configurations 34
changing your Windows password 105, 107
cleaning the reader 120
Cleanup Wizard 26
collecting trace files 128
conventions
  typographic 3
conventions used in this guide 4

D

deleting registered fingers 98
deploying OTS templates 77
deployment
  Pro Server overview 12
  recommendations 14
Diagnostic Center, using 127
DNS Record Removal event 141
DNS Registration 29
DNS Registration events 139
  DNS Record Removal 141
  DNS Registration Failed 140
  DNS Update Disabled 139
DNS Registration Failed event 140
DNS Update Disabled event 139
domain, configuring for Pro Server 23

E

Enable sound feedback for scan capture property 118
Enable visual feedback for scan capture property 118
event feedback 92
  fingerprint prompt feedback 92
  fingerprint recognition feedback 93
  fingerprint scan acquisition feedback 93
event logs
  DNS Record Removal event 141
  DNS Registration category 139
  DNS Registration Failed event 140
  DNS Update Disabled event 139
  Record Add Failed event 133
  Secure Application Data Denied event 132
  Secure Application Data Released event 131
  specifications 131
  User Authentication category 131
  User Management category 133
  User Record Added event 133
  User Record Consistency Failed event 136
  User Record Delete Failed event 136
  User Record Deleted event 135
  User Record Signature Check Failed event 138
  User Record Update Failed 135
  User Record Updated 134
  User Secret Consistency Failed event 137
  User Secure Signature Check Failed event 138
extending the Active Directory schema 22

F

Failed logon attempt lockout settings 40
False Accept Rate policy setting 39

FAR 39
filtering Pro events in the Windows Event Viewer 53
finding Pro events in the Windows Event Viewer 53
finger verification, defined 10
fingerprint credentials
  deleting 98
  managing 94
  registering 95
fingerprint identification, defined 10
fingerprint PINs, using 103
fingerprint prompt feedback 92
fingerprint recognition feedback 93
fingerprint registration, defined 10
fingerprint scan acquisition feedback 93
fingerprint templates
  defined 9
  registration template 10

G

GPO
  adding the ADM file 35
  changing policy configurations 34
  configuring policy settings 38
  implementing policies 33

H

Help menu item 114, 116
Hide Icon menu item 116

I

identification list
  defined 11
  in One Touch Logon 101
implementing policy configurations 33
increasing password security 20
installation, logging on after 91
installing
  Microsoft Windows 2000 High Encryption (128-bit) Capability 24
  Pro Server overview 21
  Pro Server software 24
  Pro Workstation overview 85
  Pro Workstation software 85

K

key concepts 14
  authentication 11
  cached credentials 11
  finger verification 10
  fingerprint identification 10
  fingerprint registration 10
  fingerprint templates 9
  identification list 11
keywords, published information 29

L

Lock Computer menu item 115
locking a computer 107
Log Events policy setting 49
logon policies
  in One Touch Logon 100
Logon Policy policy setting
  Fingerprint and Password option 43
  Fingerprint only option 43
  Fingerprint or Password option 43
  Password only option 43

M

managing fingerprint credentials 94
Maximum Number of Fingers a User Can Register policy setting 40
Maximum Size of Identification List policy setting 44
Microsoft Windows 2000 High Encryption (128-bit) Capability
  installing 24
MMC
  adding the Pro ADM file 36
  viewing ADM file settings 37
Multi-credential Logon to Windows policy setting 42

N

Network Start Timeout policy setting 45

O

One Touch Logon
  Cached Credentials 101
  changing Windows password with 105, 107
  Identification List 101
  logon policies 100
  overview 8, 99
One Touch Menu 113
  Help 114
  Properties 115
  Quick Links 114
One Touch SignOn
  adding change password screens 69
  Administration Tool 58
  creating containers 59
  creating templates 61
  creating templates manually 65
  deploying templates 77
  overview 8
One Touch Unlock 107
online help 3
overview
  One Touch Logon 8, 99
  One Touch SignOn 8
  One Touch Unlock 107
  Pro Workstation 7

P

permissions for attended registration 80
Policies container 28
policy settings 38
  Account Lockout 40
  False Accept Rate 39
  Log Events 49
  Maximum Number of Fingers a User Can Register 40
  Maximum Size of Identification List 44
  Multi-credential Logon to Windows 42
  Network Start Timeout 45
  Use Remote Authentication Server 45
Pro
  administration summary 33
  configuring policy settings 38
  event feedback 92
  key concepts 14
  removing data 25
Pro ADM file
  accessing settings in MMC 37
Pro Server
  Active Directory containers 27
  deployment overview 12
  installation overview 21
  installing software 24
  overview 9
  published information 28
  system requirements 24
  uninstalling 25
Pro User Properties in Active Directory 49
Pro Workstation
  administration overview 8, 33
  custom installation 87
  increasing security 20
  installation overview 85
  installing 87
  locking 107
  overview 7
  properties 116
  system requirements 85
Product GUID property 28
Product Name 28
Product Version High property 29
Product Version Low property 29
Product Version Number property 29
Properties menu item 115
property settings
  Cache User Credentials on the Workstation 43
published information 28
  Authentication Server Object Name property 28
  keywords 29
  Product GUID property 28
  Product Name 28
  Product Version High property 29
  Product Version Low property 29

Product Version Number 29
Schema Version Number property 29
Service Class GUID property 28
Service Class Name property 28
Service Principal Name property 29
Vendor Name property 28

Q

Quick Links menu item 114

R

reader
cleaning 120
touching 119
troubleshooting 123
reader icon, indicating connectivity status 115
reader menu
About 116
Help 116
Hide Icon 116
Lock Computer 115
Properties 116
Readme file 3
Record Add Failed event 133
registering fingers 95
registration template, defined 10
removing Pro data 25, 26
requisite knowledge 2

S

schema
Active Directory Schema Extension Wizard 22
extending 21
Schema Version Number property 29
Secure Application Data Denied event 132
Secure Application Data Released event 131
Service Class GUID property 28
Service Class Name property 28
Service Configuration Container Name 28
Service Principal Name property 29
Service Resource Records
_uareupro SRV RR 29
adding manually 30
format 29
Service Version Object Name 28
Show finger recognition animation property 118
Show Reader icon on the taskbar property 118
smart cards, using for logon 102
support 3
DigitalPersona Web site 3
online help 3
system requirements
Pro Server software 24
Pro Workstation 85

T

touching the reader 119
trace files, collecting 128
typographic conventions 3

U

uninstalling
  Pro Server 25
  Pro software remotely 87
  Pro Workstation 87
unlocking locked accounts 51
Use Remote Authentication Server policy setting 45
User Authentication events 131
  Secure Application Data Denied 132
  Secure Application Data Released 131
User Management events 133
  Record Add Failed 133
  User Record Added 133
  User Record Consistency Failed 136
  User Record Delete Failed 136
  User Record Deleted 135
  User Record Signature Check Failed 138
  User Record Update Failed 135
  User Record Updated 134
  User Secret Consistency Failed 137
  User Secure Signature Check Failed 138
user properties settings 49
User Record Added event 133
User Record Consistency Failed event 136
User Record Delete Failed event 136
User Record Deleted event 135
User Record Signature Check Failed event 138
User Record Update Failed event 135
User Record Updated event 134
User Secret Consistency Failed event 137
User Secure Signature Check Failed event 138
users, attended registration 80
using
  attended registration 80
  Diagnostic Center 127
  fingerprint PINs 103
  smart cards 102
  Windows Event Viewer 53
using Pro Cleanup Wizard 26

V

Vendor Name
  published information property 28

W

Windows Event Viewer
filtering Pro events 53
finding Pro events 53
using 53