



AD Administrator Guide

Copyright© 2014-2019 Crossmatch. All rights reserved. Specifications are subject to change without prior notice. The Crossmatch logo and Crossmatch® are trademarks or registered trademarks of Cross Match Technologies, Inc. in the United States and other countries. DigitalPersona® is a registered trademark of DigitalPersona, Inc., which is owned by the parent company of Cross Match Technologies, Inc. All other brand and product names are trademarks or registered trademarks of their respective owners.

Published/Revised: April 24, 2019 (Software version 3.1.0)

Table of Contents

Introduction	11
Architecture	11
Components	12
Server components	12
Client components	13
Password Manager Admin Tool	14
Authentication and Credentials	14
Upgrading from previous versions	14
Licensing model	14
System Requirements	16
Remote access	17
Support Resources.....	17

SECTION ONE: INSTALLATION

DIGITALPERSONA AD SERVER INSTALLATION	19
Deployment Overview	19
Upgrading from previous versions	19
Migration from DigitalPersona Pro for Enterprise	19
Compatibility	20
Extending the Active Directory Schema	20
Configuring each domain	21
Installing DigitalPersona AD Server	22
Setting up DigitalPersona AD Server for use with DigitalPersona AD Kiosk.....	24
Configuration Steps	24
Configuring Kiosk GPO Settings	24
Creating the OU for the Kiosk	24
Specifying a Shared Account for the Kiosk	25
Adding Shared Account Settings Using GPO	25
Changes Made During Installation	26
Active Directory Containers	26
Published Information	26
DNS Registration	27
Uninstalling DigitalPersona AD Server.....	28
SEPARATE INSTALLATIONS	29
Components included in the product package	29
DigitalPersona AD Administration Tools	29
License Activation Manager	30
Users and Computers Snap-In	30
User Query Snap-in	30
GPMC Extensions	30
Attended Enrollment	31
Separate product packages	31
Web Management Components	31
Password Manager Admin Tool	31
Extended Server Policy Module (ESPM)	31
Guardian ten-print scanner support	32
DigitalPersona Large Scale ID wrapper	32
DigitalPersona CAC/PIV card module	33

Initializing the PIV token	33
Installing the YubiKey Smart Card Minidriver	33
Enrolling the YubiKey Smart Card	34
Additional considerations	34
SECTION TWO: ADMINISTRATION	
ADMINISTRATION OVERVIEW	37
Overview	37
About GPO settings.....	37
ADMINISTRATION TOOLS	38
Overview	38
Attended Enrollment.....	38
Hardware Tokens Management Utility	39
LICENSE ACTIVATION & MANAGEMENT	41
Overview	41
Product Options	41
DigitalPersona License Group Policy Object.....	42
Evaluation license	42
License activation	42
License activation from another computer.....	44
Checking for license updates	47
Displaying license properties.....	48
License deactivation.....	49
License deactivation from another computer.....	50
Releasing user licenses	53
.....	53
ADUC SNAP-INS	54
Users and Computers snap-in	54
User properties	54
User object commands	55
User Query snap-in.....	56
ActiveX control	56
Interactive dialog-based application	59
Command line utility	61
EXTENDED SERVER POLICY MODULE	63
GPMC/GPOE EXTENSIONS	65
Overview	65
Group Policy Object Extensions.....	66
DigitalPersona Client	66
DigitalPersona Server	66
Administrative Templates	67
Implementation Guidelines.....	70
Organizational Units and GPOs	70

GPO behavior	70
Installing Administrative Templates Locally.....	71
POLICIES AND SETTINGS	72
Overview	72
Computer Configuration\Policies\Software Settings.....	73
DigitalPersona Client (Summary)	73
DigitalPersona Client (Detail)	74
Security\Authentication	74
Security\Enrollment	77
Security\SMS	77
Security\SMTP	77
Kiosk Administration	78
DigitalPersona Server	78
Licenses	78
Computer Configuration\Policies\Administrative Templates	79
DigitalPersona (AD LDS) \ General (Summary)	79
DigitalPersona\General (Detail)	80
Attended Enrollment	80
Authentication Devices	80
Event logging	85
DigitalPersona Server (Detail)	86
Credentials verification lockout	86
DigitalPersona Server DNS	87
Identification Server settings	88
DigitalPersona Workstations (Detail)	90
Advanced	90
Caching Credentials	91
Disable Applications	92
Password Manager	92
Quick Actions	92
Browser hardware support	92
User Configuration\Policies\Administrative Templates	93
DigitalPersona (AD LDS) \ Workstations (Summary)	93
Workstations (Detail)	93
Password Manager	93
ATTENDED ENROLLMENT	94
Setting up Attended Enrollment	94
To assign, or remove Register/Delete permissions.....	94
PASSWORD RANDOMIZATION	97
Password Randomization Options	97
DoNotRandomize	97
RandomizeAlways UI	98
MayRandomize UI	99
SINGLE SIGN-ON	101
Configuring Single Sign-On.....	101
Disabling Session Authentication	101
Creating managed logons	101

RECOVERY	102
User recovery	102
Account lockout recovery.....	103
DIGITALPERSONA REPORTS	104
About Reported events.....	105
Setting up DigitalPersona Reports	105
Install and configure DigitalPersona Reports	106
Requirements	106
Upgrading DigitalPersona Reports	106
Installation	106
Reports Server Configuration	107
Configure Active Directory GPO settings	108
Web console features	114
Creating a report	115
Creating a new subscription	116
Adding a report to an existing subscription	117
Bookmarking a report	118
Deleting a report or subscription	118
Troubleshooting steps	118
DIGITALPERSONA EVENTS	119
Overview	119
Credential Management	120
User Management	121
Secret Management	122
Service Management.....	123
Password Manager.....	123
Credential Authentication	124
DNS Registration	124
Deployment	125
OTP Management.....	125
Windows Logon.....	125
Authentication Domain Management	126
UTILITIES	127
DELEGATING PERMISSIONS	128
SMS/SMTP Management.....	128
License management	131
Attended Enrollment.....	133
PASSWORD MANAGER ADMIN TOOL	134
Overview	134
System requirements.....	135
Installation & setup	135
Using Managed logons.....	137
Creating managed logons	137
Creating logons manually	145
Deploying managed logons	146
Creating an extended authentication policy	148

Setting Up a Change Password screen	149
Setting up a Change Password Screen manually	154
Regular Expression syntax	156
Managing logons	158
The Field Catalog.....	160
Tools page.....	161
Password Manager Actions.....	162
User policy settings	162
Logging On	163
Changing passwords.....	163

SECTION THREE: WEB MANAGEMENT

WEB MANAGEMENT COMPONENTS INSTALLATION	165
Installation wizard	165
Prerequisites	165
Installation steps	166
Configuration wizard.....	168
Express Configuration	169
Advanced Configuration	172
Uninstallation	175
ASSIGNING SECURITY OFFICER PERMISSIONS	177
Overview	177
Assigning permissions.....	177
Assigning the OTP Tokens permission.....	179
DIGITALPERSONA IDENTITY SERVER	181
Identity Server features.....	182
Integrated Windows Authentication (IWA)	182
Multi-Factor authentication	182
Forgot password?	182
Unlock account?	183
Identity Server configuration (DigitalPersona IIS Plugin)	184
Installation	184
Configuration details	185
General tab	185
STS options tab	185
Policy tab	185
Step-up policy tab	186
Web Portal tab	188
Additional configuration via .config files	188
policyBypassGroups	188
Configuring STS to work with ADFS	188
Add ADFS Relying Party to STS	189
Create an ADFS Claim Provider trust	189
DIGITALPERSONA WEB ADMINISTRATION CONSOLE	190
Overview	190
Logging in	190
Administration Console features	191

Features summary	191
Search for and filter users	191
Display user details	192
Recover password (user recovery)	192
Unlock the account	193
Manage Credentials	193
Manage Hardware OTP Tokens	193
DIGITALPERSONA WEB ENROLLMENT	195
Overview	195
Accessing Web Enrollment	196
Selecting a user for attended enrollment	196
Self Enrollment and credential management	197
Credential enrollment	197
Password credential	198
Fingerprints credential	199
Cards credential	200
PIN credential	201
One-Time Password credential	202
OTP Enrollment	202
OTP via email enrollment	207
Authentication with a One-Time Password	208
Recovery Questions credential	209
FIDO Key credential	210
Face credential	211
Customizing Web Enrollment	213
To assign, or remove Register/Delete permissions	213
Prohibit domain administrators from enrolling/deleting credentials	214
DIGITALPERSONA APPLICATION PORTAL	216
Overview	216
Adding links to the Application Portal	217
Adding DigitalPersona web applications to the Application Portal	217
Adding third-party applications to the Application Portal	217
Portal verification	217
SECTION FOUR: APPENDICES	
TROUBLESHOOTING	219
How to configure ports used by DigitalPersona for firewall	219
How to troubleshoot fingerprint reader operation	220
Resolving unavailable server or domain issues	221
Addressing fingerprint registration not allowed error	221
Changing Password Manager Data storage limits	222
FIDO Token AppIDs	223
DIGITALPERSONA AD ADFS EXTENSION	228
Installation	228
Selecting and deselecting DigitalPersona credentials	230
.....	231

DIGITALPERSONA NPS PLUGIN	232
Recommended Configuration	232
Using Microsoft NPS as your RADIUS Server	232
Installing Network Policy Server (NPS)	233
Configuring your VPN Server to use the NPS RADIUS server	239
Deploying the DigitalPersona NPS Plugin	239
Configuring the Microsoft VPN Client	239
Configuring the VPN connection	241
Testing the VPN connection using the PAP protocol	242
Testing the VPN connection using the MS-CHAPv2 protocol	242
Using OTP Push Notification with PAP	242
Using OTP Push Notification with MS-CHAPv2	243
Authenticating with OTP Only	243
Configuration required when using CHAP.....	243
Enabling reversible encryption for storing passwords	243
Configuring Microsoft RRAS to support CHAP	245
Configuring Microsoft NPS to support CHAP	245
Configuring Microsoft VPN Client to support CHAP	246
Testing the VPN connection using the CHAP protocol	247
CITRIX SUPPORT	248
Overview	248
Definitions	248
Supported Citrix platforms	248
Integration of Citrix with DigitalPersona components	248
Disabling automatic client updates	249
XenDesktop limitation.....	249
Resolving duplicate DigitalPersona system tray icons.....	249
Resolving missing DigitalPersona system tray icon	249
FINGERPRINT ADJUDICATION AND DEDUPLICATION	251
Overview	251
Identification	251
Enrollment.....	251
Cautions	251
Fingerprint Identifiers.....	252
IDENTIFICATION LIST	253
Introduction	253
Example: Restricting kiosk identification.....	253
CHROME INSTALL VIA GPO	255
Introduction	255
Installation	255
SECURE AND SMALL SENSOR SUPPORT	258
WINDOWS PASSWORD SYNCHRONIZATION TOOL	260

V2.3 TO 3.0 REVISED GPO SETTINGS	261
Computer Configuration/Policies/Software Settings.....	261
Renamed GPOs and settings	261
New containers and settings	261
Security GPO and settings	261
Computer Configuration/Policies/Administrative Templates	262
New Administrative Templates structure	262
New GPOs and settings	262
Relocated and renamed GPOs and settings	263
SCHEMA EXTENSION	266
Introduction	266
Schema extension overview.....	266
Schema objects summary	266
Object structure	267
Schema classes summary	269
Class structure	269
Standard Classes Extensions	270
Schema objects details	271
dp-User-Credentials-Data	271
dp-User-Account-Control	273
dp-User-Private-Data	275
dp-Servers-Data	278
dp-License	280
dp-User-Logon-Policy	282
dp-User-Public-Key	284
dp-User-Payload	287
dp-User-Recovery-Key	289
dp-User-Data-Type	291
dp-Lockout-Time	293
dp-Recovery-Password-Last-Set-Time	295
dp-Recovery-Password	297
dp-Master-Key	300
dp-Omit-Reasons	302
dp-Password-Manager-Data	303
dp-OTP-Key	304
dp-OTP-Length	306
dp-OTP-Time-Interval	308
dp-Servers-Configuration	311
Class details	313
dp-User-Secret	313
dp-Authentication-Servers-Container	315
dp-Service-Configuration	318
dp-Authentication-Service-Connection-Point	320
dp-OTP-Token	323
INDEX	326

THIS CHAPTER PROVIDES A HIGH-LEVEL OVERVIEW OF THE DIGITALPERSONA AD SOLUTION, AND INCLUDES THE FOLLOWING MAJOR TOPICS.

Main topics in this chapter	Page
Introduction	11
Architecture	11
Components	12
Authentication and Credentials	14
Upgrading from previous versions	14
Licensing model	14
System Requirements	16
Remote access	17
Support Resources	17

Details on specific components, modules and features are provided in the various chapters of this Administrator Guide. Additional documentation is provided through the DigitalPersona Client Guide and a series of integrated help files accessed through the various components. Some optional modules will include additional documentation provided with the module.

References to procedures, UI elements and images in this guide are always made to the current version of the product unless another version is specifically referenced. References to, and images of, Microsoft Windows products are to Windows Server 2012 and Windows 7 unless otherwise noted.

Introduction

DigitalPersona AD is an enterprise-level central management solution for composite authentication that enables administrators to manage security and authentication within Active Directory networks including data protection, access management and recovery. It represents an optimal solution to multiple security needs, including:

- Strong Authentication for PC, application and RADIUS logon
- Single Sign-On (SSO) for Enterprise applications

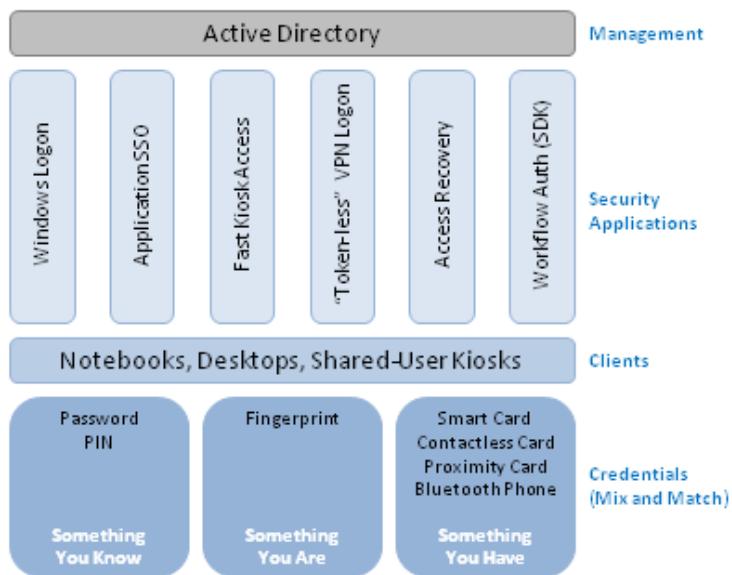
For further information on how DigitalPersona AD can help you solve your security needs, we have white papers, datasheets and case studies on our website at <http://www.crossmatch.com/digitalpersona>

Architecture

The conceptual architecture of DigitalPersona AD consists of four layers.

- *Management* – Provides an Active Directory-based solution for the enterprise; enabling the IT Administrator to configure, deploy and administer security policies throughout the organization.
- *Security Applications* – Provides pluggable applications and features that are managed through the DigitalPersona AD management infrastructure.
- *Clients* - Workstation software installed on notebooks, desktops and shared-user kiosks.

- *Credentials* – Provides support for multiple authentication credentials that may be used in specified combinations for verifying the identity of users accessing managed computers and security applications.



Components

DigitalPersona AD is a client-server product. It consists of server and client components that work within an existing Active Directory environment.

Server components

DigitalPersona AD's server components fulfill four main purposes:

- They allow IT Administrators to manage security and authentication policies via Active Directory Group Policy Objects. For these purposes, DigitalPersona AD includes various GPMC (Group Policy Management Console) extensions, installed under the Software Settings and Administrative Templates nodes, to link product policies and settings to Active Directory containers.
- They provide centralized, server-side authentication of various types of credentials (e.g. fingerprints, smart cards, Bluetooth, one-time passwords etc.). For these purposes, DigitalPersona AD runs authentication services within your domain and receives authentication requests from managed computers.
- They allow centralized backup and roaming of computers' and users' credentials and passwords. For these purposes, DigitalPersona AD uses Active Directory as a database of relevant data.
- They also allow other general administrative tasks, including:
 - Access recovery into locked workstations
 - Deployment of license activation codes.

The main server components of the DigitalPersona AD product are briefly described in the following table, and more fully described in the referenced pages.

Server component	Purpose	Page
DigitalPersona AD Server	Provides domain-wide, centralized administration of DigitalPersona AD clients and enables strong authentication through various credentials and credential combinations	19, 37

Server component	Purpose	Page
DigitalPersona AD Administration Tools	Provide additional tools for administration of various DigitalPersona AD features and utilities including License Activation Manager, GPMC Extensions, Access Recovery and the Password Manager Admin Tool.	29, 35

Client components

The DigitalPersona AD solution supports the following clients.

- *DigitalPersona AD Workstation* - Enforces security and authentication policies on managed Windows computers while providing intuitive access to end-user features and functionality.
- *Attended Enrollment* - Allows an administrator or other delegated individuals to supervise credential enrollment for end-users from one or more centralized locations. Attended Enrollment is an optional component of DigitalPersona AD Workstation, installed by choosing Custom during the DigitalPersona AD Workstation installation.
- *DigitalPersona AD Kiosk* - Provides DigitalPersona features for environments where users log on to a shared, common Windows account on a computer managed by a DigitalPersona AD Server.

NOTE: DigitalPersona clients may be installed individually on computers or deployed through Active Directory GPO, SMS (Systems Management Server) or logon scripts. They cannot be installed through ghosting or imaging technologies.

For installation instructions and complete descriptions of features, see the *DigitalPersona Client Guide*.

DigitalPersona AD Workstation

DigitalPersona AD Workstation is the primary client application for end-users. A clean and intuitive DigitalPersona Console provides the ability to increase both security and convenience through a variety of configurable features; including enrollment and use of multiple credentials for Windows logon. It may be centrally managed by the DigitalPersona AD Server, or installed as a stand-alone product.

DigitalPersona Password Manager is an optional application that integrates with the DigitalPersona Console to provide automated logon to enterprise resources, programs and websites.

For a full description of its features, see the chapter *DigitalPersona Workstation* in the *DigitalPersona Client Guide*.

Attended Enrollment

Attended Enrollment is a feature that allows a delegated user, or a member of a delegated user group, to attend and supervise the enrollment of DigitalPersona AD credentials for other users. This optional component may be selected during a Custom installation of DigitalPersona AD Workstation. It is also included in the DigitalPersona AD Users and Computers Snap-in within the DigitalPersona AD Administration Tools package. Attended Enrollment can add a higher level of security to the implementation and use of DigitalPersona AD.

DigitalPersona AD Kiosk

DigitalPersona AD Kiosk is a client application specifically designed for environments where users need fast, convenient and secure multi-factor identification on workstations shared by multiple users. Although users share a common Windows account, DigitalPersona AD Kiosk provides separately controlled access to resources, applications and data - all centrally managed by the DigitalPersona AD Server.

DigitalPersona Password Manager is an optional application that integrates with the Kiosk's DigitalPersona Console to provide automated logon to enterprise resources, programs and websites.

For a full description of its features, see the chapter *DigitalPersona Kiosk* in the *DigitalPersona Client Guide*.

Password Manager Admin Tool

The Password Manager Admin Tool is a separate application included with the DigitalPersona Premium package, which simplifies and secures access to password-protected software programs and websites through the use of *managed logons* that allow users to identify themselves through the use of any supported credential or combination of credentials specified by the administrator, as defined in the Authentication and Credentials topic above.

Administrators can use the DigitalPersona Password Manager Admin Tool to create managed logons specifying information for logon and change password screens for websites, programs and network resources. These managed logons are then deployed to managed workstations, where they are accessible to the user through the Password Manager application and the mini-dashboard. Managed logons always take precedence over personal logons created by users.

For a full description of its features, see the *Password Manager Admin Tool* chapter.

Authentication and Credentials

The default, and simplest, means of authentication, i.e. making sure that you are a person authorized to access a computer or other resource, is your Windows account name and password. Authentication is generally required in logging on to Windows, accessing network applications and resources, and logging into to websites.

DigitalPersona AD clients provide a means for the IT Administrator to easily setup and enforce strong authentication such as two-factor and multi-factor authentication using a variety of supported credentials.

DigitalPersona AD supports the use of various credentials for authentication, including Windows passwords, fingerprints, smart cards, contactless cards, proximity cards, face, PIN, Bluetooth and One-Time-Passwords.

An additional Self Password Recovery credential may be used solely for recovering access to a managed client computer in place of a forgotten password

Note that by default, user credentials are cached on the local DigitalPersona Workstation client, and *not* cached on a computer running the DigitalPersona Kiosk client. This means that DigitalPersona Workstation users will be authenticated without a connection to the DigitalPersona AD Server, but DigitalPersona Kiosk users will *not* be authenticated if there is no connection to the DigitalPersona AD Server (although caching can be enabled for the Kiosk client if desired).

By default, initial enrollment of end-user credentials is provided through the DigitalPersona Attended Enrollment component, which requires the supervising logged on user to have been previously assigned the permission to enroll Non AD users. See the chapter on *DigitalPersona Attended Enrollment* in the *DigitalPersona Client Guide* for further details.

Upgrading from previous versions

To upgrade from a previous version of this software, refer to the DigitalPersona AD Upgrade Notes available at:

<http://www.crossmatch.com/digitalpersona>

Licensing model

Some features and functionality described in this Administrator Guide are only included in the Premium version of the product or may be separately licensed.

There are three ways that DigitalPersona software is licensed.

- *Perpetual* - allows use of purchased DigitalPersona software for a specified number of users, indefinitely, and includes the first year of support and maintenance.

- *Subscription* - allows use of purchased DigitalPersona software for a specific period and for a specified number of users, and includes support and maintenance.
- *Evaluation* - is automatically activated upon installation and allows use of DigitalPersona software for a limited period of time for up to 10 users.

A DigitalPersona AD license has a single Product Option. Each activated license is shown under the *Licensed product options* heading in the DigitalPersona License GPO within the Group Policy Editor.

DigitalPersona Premium Employee License - Permits the enrollment of user credentials, and subsequent use by a specified number of users with Active Directory accounts.

The specific DigitalPersona AD SKU and/or package you purchased may entitle you to licensing for one or more additional modules or components that are integrated with DigitalPersona AD.

You should have received from Crossmatch, or your authorized reseller, all of the License IDs that are part of the package you purchased. Some modules or optional components may need to be activated individually.

For information on other licensed versions of the product which may be available, and licensing for specific features, contact your Crossmatch Account Manager or Reseller - or visit our website at:

<http://www.crossmatch.com/digitalpersona>.

Licenses may be activated through Active Directory using the License Activation Manager. For more information about DigitalPersona AD license activation, see *License Activation & Management* on page 41.

System Requirements

Product/Component	Minimum Requirements
DigitalPersona AD Server	<ul style="list-style-type: none"> • Microsoft Windows Server 2016, 2012 or 2012 R2 • Active Directory • 12 MB disk space plus 5 KB per user
DigitalPersona AD Workstation, DigitalPersona AD Kiosk and DigitalPersona Attended Enrollment	<p>DigitalPersona AD Workstation, DigitalPersona AD Kiosk and DigitalPersona Attended Enrollment</p> <ul style="list-style-type: none"> • Operating Systems <ul style="list-style-type: none"> • Windows 7 SP1, Windows 8.x (32/64), Windows 10 version 1703 or later (32/64) with 50MB disk space and 100MB during installation. Home editions, Windows 10 S and Windows 10 in S mode are not supported. The Face credential is not available on 32-bit systems. • Windows Embedded Standard 7+ (requires at least 8GB RAM and 64GB HD) • Windows Server 2012, 2012 R2 or 2016 • 50 MB disk space, 100 MB during installation • .NET Framework 4.5 or above • (x86 machines) - Installed automatically by executable if not present, but must be installed manually when pushing MSI through GPO. <ul style="list-style-type: none"> • Microsoft Visual C++ 2013 Redistributable package (x86 version) • Microsoft Visual C++ 2015 Update 2 Redistributable package (x86 version) • (x64 machines) - Installed automatically by executable if not present, but must be installed manually when pushing MSI through GPO. <ul style="list-style-type: none"> • Microsoft Visual C++ 2013 Redistributable package (x86 and x64 versions) • Microsoft Visual C++ 2015 Update 2 Redistributable package (x86 and x64 versions) • Microsoft Internet Explorer*, Google Chrome or Mozilla Firefox browser required in order to create/use Password Manager <i>personal</i> logons or use <i>managed</i> logons***. See the readme.txt file for tested browser versions. • Microsoft Internet Explorer (only) in order to create <i>managed</i> logons** using the optional Password Manager Admin Tool. See the readme.txt file for tested browser versions. • (Versions 2.0.3+) On Windows 8.1, Windows Update KB 2919355 is required. On Windows 7, Windows Update KB 2999226 is required.****
DigitalPersona Web Management Components	<p>DigitalPersona Web Management Components</p> <ul style="list-style-type: none"> • Domain Admin permissions are required for installation. • When all components are installed on the same machine as the DigitalPersona AD Server, requirements are the same as the AD Server plus Windows Web Server (IIS). • To access the Web Administration Console, Web Enrollment or the Application Portal from a device, either the DigitalPersona AD Server or a DigitalPersona client must be installed on the device, and one of the following supported web browsers, with Javascript enabled. See the readme.txt file for supported browser versions. <ul style="list-style-type: none"> • Windows - Internet Explorer (11+), Microsoft Edge, Google Chrome, Firefox. • Mac and iOS - Safari • Android - Google Chrome

Product/Component	Minimum Requirements
DigitalPersona Web Enrollment	<ul style="list-style-type: none"> • Operating Systems <ul style="list-style-type: none"> • Windows 7 SP1, Windows 8.x/10, 32/64-bit (Home and Windows Embedded editions are not supported.) • Windows Server 2012 and later. • .NET Framework 4.5.2 or above • .NET Core Windows Server Hosting bundle • Internet Information Services feature or the Web Server (IIS) Server role

* On Windows 8.1, Password Manager requires that IE is launched from the legacy desktop, not from the Metro UI.

** Personal logons allow end-users to create automated logon to programs, websites and network resources, while managed logons have the same function but are created by an administrator and deployed to end-users. Personal logons are not available on DigitalPersona AD Kiosk.

*** These Windows Updates should resolve any possible 1722 errors.

Remote access

DigitalPersona AD Server includes support for remotely accessing DigitalPersona AD Workstation and DigitalPersona AD Kiosk clients through Windows Terminal Services (including Remote Desktop Connection), and through various Citrix products.

- When DigitalPersona AD Workstation or DigitalPersona AD Kiosk are accessed remotely, the fingerprint reader attached to a local Workstation or Kiosk can be used to access all DigitalPersona AD Workstation or DigitalPersona AD Kiosk features on the remote computer. See *Level of detail in event logs* on page 85. Also see the NOTE below.
- When using DigitalPersona AD Workstation or DigitalPersona AD Kiosk remotely, the remote computer is locked to prevent interruption of your session.
- When completing a Terminal Services session, use "Log Off" to close the session; use "Disconnect" or "Shutdown", or the Close Window icon to leave your session active.
- For additional information on Citrix deployment, see *Citrix Support* on page 248.

NOTE: By default, the Remote Desktop Protocol (RDP) is not enabled on any Microsoft operating system version. The use of Microsoft Remote Desktop entails opening a port in your firewall and thus creates a security vulnerability. For more information on this vulnerability, see the Microsoft Security Bulletin MS05-041 located at:

<https://technet.microsoft.com/en-us/library/security/ms05-041.aspx>

Support Resources

The following resources are provided for additional support.

- Readme files in the root directory of each product package contain late-breaking product information.
- AskPersona.com (<http://askpersona.com>) is a Crossmatch knowledge portal providing answers to many frequently asked questions about our products.
- Maintenance and Support customers will find additional information about technical support resources in their Maintenance and Support confirmation email.
- Online help is included with each component and application.

DigitalPersona documentation is available on our website at:

<https://www.crossmatch.com/company/support/documentation>

Section One: Installation

This section of the DigitalPersona AD Administrator Guide includes the following chapters:

Chapter Number and Title	Purpose	Page
2 - DigitalPersona AD Server Installation	Requirements and procedure for installing the DigitalPersona AD Server.	19
3 - Separate installations	Requirements and procedure for installing additional and separate DigitalPersona AD components.	29

THIS CHAPTER PROVIDES INSTRUCTIONS FOR THE INSTALLATION OF THE DIGITALPERSONA AD SERVER ON A DOMAIN CONTROLLER.

For instructions on uninstalling DigitalPersona AD Server, see page 28.

Deployment Overview

Here is a high-level overview of the steps required for initial deployment of DigitalPersona AD Server on the domain controller for a supported Windows Server network.

Procedure	Page
1. Extend the Active Directory schema to include attributes and classes used by DigitalPersona AD Server. Requires AD Schema Administrator rights. You can view the details of the changes that will be made to the schema by opening the file "dp-schema.ldif" located in the "AD Schema Extension" folder in the product package.	20
2. Configure each domain on which DigitalPersona AD Server will be installed by running DPDomainConfig.exe (located in the folder "AD Domain Configuration" in the product package). Requires AD Domain Administrator rights.	21
3. Install the DigitalPersona AD Server software. Note that this will set firewall rules necessary for the operation of DigitalPersona software.	22
4. Install the DigitalPersona AD Administration Tools. (These may be installed on a separate computer. See page 29 for installation instructions.)	
5. (Optional) Configure DigitalPersona AD for use with DigitalPersona AD Kiosk, if the kiosk client will be used in the domain.	24

Detailed steps for installation of the DigitalPersona AD Server begin on page [Installing DigitalPersona AD Server](#) on page 22.

Upgrading from previous versions

To upgrade from a previous version of this software, refer to the DigitalPersona AD Upgrade Notes available at:

<http://www.crossmatch.com/company/support/documentation>

Migration from DigitalPersona Pro for Enterprise

This version of the software supports migration from DigitalPersona Pro for Enterprise (version 5.5.1 or above). To upgrade to the current version of DigitalPersona Composite Authentication, simply follow the instructions in this chapter, the same as for a new installation.

Note that any configured GPO settings from DigitalPersona Pro will still be in force for any remaining Pro clients. However, these settings will not affect DigitalPersona clients, and new GPO settings will need to be configured for them.

For environments where Pro clients will exist along with the current version of DigitalPersona AD clients, you should maintain a machine with a copy of the Pro Administration Tools in order to manage Pro GPO policies and settings. However if this is not the case, you should be aware that you cannot upgrade an installation of Pro Administration Tools to DigitalPersona AD Administration Tools. You will need to uninstall both Pro Administration Tools and Pro Workstation on the machine and then install DigitalPersona AD Workstation and the DigitalPersona AD Administration Tools.

Migration services and tools are available from our Professional Services team.

Direct upgrades from DigitalPersona Pro for Enterprise versions previous to 5.5.1 are not supported. If you need to upgrade from a version prior to 5.5.1, please contact our Professional Services team.

Also, make sure to review the readme.txt files included with each component in the product package that you are installing.

Compatibility

This version of DigitalPersona AD Server is compatible with the following Crossmatch products:

- DigitalPersona AD Workstation 2.1 and above
- DigitalPersona AD Kiosk 2.1 and above
- DigitalPersona Password Manager Admin Tool 6.0 and above

This release is not compatible with, and requires the uninstallation of, any other Crossmatch products on the same computer.

Extending the Active Directory Schema

Prior to installing DigitalPersona AD Server, the Active Directory schema must be extended to create new attributes for the user object and new classes, as well as to make modifications to existing classes. The Active Directory Schema Extension Wizard automatically handles all of the necessary changes to the schema.

Each schema extension has a schema extension version number that is independent of the Crossmatch product version number. Each Crossmatch product release will identify the schema extension version it requires. This schema extension is global to the Active Directory forest.

If you want to view the script that is used to extend the schema (dp-schema.ldif), it is available in the product package at the following location:

AD Schema Extension\dp-schema.ldif

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

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

You must have Schema Administrator privileges to run the Schema Extension Wizard.

To run the Active Directory Schema Extension Wizard

1. Double-click *DPSchemaExt.exe*, which is located in the Schema Extension folder in the Server installation package, to start the Schema Extension Wizard.
1. 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*.
2. When prompted to proceed with the schema extension, click *Yes*.
3. 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*.
4. If the schema is not writable, the wizard will inform you of this and allow you to make it writable. If this dialog box displays, click *Yes* to make the schema writable and perform the schema extension.

5. The wizard will extend the schema and provide information such as the class and attribute names. To close the wizard, click *Finish*.

Note that during upgrades, warnings will be thrown for all previously existing elements, however this should not affect the actual success of the installation.

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.

Configuring each domain

For each domain on which you plan to install DigitalPersona AD Server, you need to run the DigitalPersona AD Active Directory Domain Configuration Wizard, which configures the required domain-specific data including the necessary cryptographic keys. This includes the following -

- Verifies that the AD schema was extended correctly
- Creates the AD containers required by DigitalPersona
- Creates the DigitalPersona Server encryption keys
- Creates necessary Active Directory Extended Rights
- Creates DigitalPersona Display-Specifiers (required to add our content to ADUC)
- Sets the default DigitalPersona-related security on the AD Domain

Running the wizard requires administrator privileges on the domain controller.

You should run this wizard only once on each domain where DigitalPersona AD Server will be installed.

When installing multiple DigitalPersona AD Servers, it is critical that you run the wizard only once during any replication period, allowing full replication to be completed before going on to run the wizard on the next domain.

Running the wizard a second time during a single replication period will result in corrupted Server data, and any DigitalPersona AD Servers in the domain will be unusable.

After running the Domain Configuration wizard, domain level permissions to enroll/delete fingerprints are reset to the default, i.e. Allow.

To run the DigitalPersona AD Domain Configuration Wizard

1. Double-click *DPPDomainConfig.exe*, which is located in the Domain Configuration folder in the Server installation package.
2. 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*.
3. A warning reminds you not to run this wizard if you have an existing DigitalPersona AD Server installation on this domain. If you are sure there are no other DigitalPersona AD Server installations on the domain you are configuring, check the *I accept that the domain will be configured* box and 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 and click *Save*.
5. When you click *Save*, the wizard performs the changes on the domain.
6. To close the wizard, click *Finish*.

Installing DigitalPersona AD Server

After extending the Active Directory schema and configuring the domain where you will install DigitalPersona AD Server, you are ready to install the software.

Before installing DigitalPersona AD Server, ensure the computer meets the minimum requirements listed on page 16.

WARNING: To avoid possible data loss, wait one data replication cycle after domain configuration before installing DigitalPersona AD Server.

Note also that the installation will set three inbound firewall policies necessary for the operation of DigitalPersona software as follows:

Policy Name	Description
DigitalPersona Authentication Service (Echo Request - ICMPv4-In)	Inbound rule for DigitalPersona Authentication Service to allow Echo Request messages to be sent as ping requests.
DigitalPersona Authentication Service (DCOM-In)	Inbound rule for DigitalPersona Authentication Service to allow remote DCOM activation via the RPCSS service.
DigitalPersona Authentication Service (TCP-In)	Inbound rule for DigitalPersona Authentication Service to allow it to be remotely connected via DCOM.

To install DigitalPersona AD Server

1. Double-click *Setup.exe* to run the DigitalPersona AD Server Installation Wizard, located in the *../Server/DigitalPersona AD Server* folder of the product package.
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 AD Server will be installed. If you want to install the server in the default location, which is *C:\Program Files\DigitalPersona*, click *Next*. Or click *Browse* to specify a new location and then click *Next* to continue.
5. Choose one the following options to indicate the type of installation you want to perform.
 - Typical - Installs the most commonly used features.
 - Custom - Allows selection of which features to install.

Fingerprint Recognition Engine - (Default) Enables fingerprint matching functionality, i.e. fingerprint enrollment, verification and identification. Note that if you plan on installing the Biometric Tokenization Engine or the optional *DigitalPersona Large Scale ID Wrapper*, you should deselect the *Fingerprint Recognition Engine* feature. For further details on the wrapper, see the *DigitalPersona Large Scale ID Wrapper: Installation Guide*.

Biometric Tokenization Engine - (Optional) Creates a tokenized revocable presentation of a fingerprint. It can be used for enrollment and verification but not for identification. Note that this engine does not support deduplication. Also, switching from the Fingerprint Recognition Engine to the Biometric Tokenization Engine will require re-enrollment of all users' fingerprints.

It is critical that the same recognition engine is installed on all DigitalPersona Servers and clients in the AD forest.

6. Click *Next* and then *Install*, to begin installation.
7. During installation, progress is shown until the process is completed.
8. When installation is complete, a final page displays. Click *Finish*.
9. If prompted to do so, reboot the computer.

DigitalPersona AD Server and its associated workstation clients use GPMC extensions, installed under the *Software Settings* and *Administrative Templates* nodes, to link product policies and settings to Active Directory containers. These policies and settings are described in the chapter, [*Policies and Settings*](#) on page 72.

Setting up DigitalPersona AD Server for use with DigitalPersona AD Kiosk

Configuration Steps

Complete the following DigitalPersona AD Server and DigitalPersona AD Kiosk installation and configuration steps in the order shown below. Specific instructions for configuration are described in the following sections and additional pages as referenced.

Complete the following

1. **Install DigitalPersona AD Server.** This includes performing Schema Extension, Domain Configuration and the Server installation as specified on pages 20 and following. If previous versions of DigitalPersona AD Server were installed in the domain, you should run the Domain Configuration Wizard, but should not run the Schema Extension Wizard again in this case.
2. **Install the DigitalPersona AD Administration Tools.** You do not need to install all of the included Administration Tools components. However, the GPMC Extensions component must be installed. See *Administration Tools* on page 29.
3. **Create an OU for each kiosk and assign computers to the kiosk OU.** See *Creating the OU for the Kiosk* on page 24. By default, the entire domain is considered as one kiosk. You may want to set up multiple, separate kiosks.
4. **Assign kiosk permissions.** By default, all domain users are allowed Kiosk permissions. You can restrict identification to specific groups or users by following the instructions in the chapter *Identification List* on page 253. Note that by design, AD Domain Administrator will have access even if not granted permission on an Identification List. However, you can change the permission for the Domain Administrator from Allow to Deny for any specific kiosk.
5. **Create a Shared Account in Active Directory** and specify the account information either by GPO or on individual kiosk computers. See *Kiosk Shared Account Settings* on page 24 and *Adding Shared Account Settings Using GPO* on page 25.
6. **Install DigitalPersona AD Kiosk on kiosk computers.** See the chapter, *DigitalPersona AD Kiosk installation* in the DigitalPersona Client Guide.
7. **Enroll user credentials.** By default, all domain users are allowed to enroll their own credentials. However, you can choose whether you want to supervise the credential enrollment process, or allow users to enroll credentials themselves when they first log on to or unlock a kiosk computer. See the chapter, *Attended Enrollment* in the DigitalPersona Client Guide.

Configuring Kiosk GPO Settings

Perform fingerprint identification on server

The GPO setting *Perform fingerprint identification on server* may be applied and enabled for DigitalPersona AD Kiosk clients that will be using fingerprint credentials. For further details, see *Perform fingerprint identification on server* on page 88.

Kiosk Shared Account Settings

At the kiosk level, whether it is the domain or an OU, you must specify the kiosk Shared Account information. For more information, see *see Adding Shared Account Settings Using GPO* on page 25.

Creating the OU for the Kiosk

When you install DigitalPersona AD Server and DigitalPersona AD Kiosk, the entire domain is considered as one kiosk unless you complete further configuration.

To create multiple kiosks in a domain, or to limit the usage of the kiosk to specific computers only, you should create an organizational unit (OU) for each kiosk and then assign computers to the OU. You might create several kiosks where each kiosk is associated with its own OU. If computers in the same OU are geographically located in different sites, each OU per site is a kiosk.

Specifying a Shared Account for the Kiosk

DigitalPersona AD Kiosk requires an account, known as the Shared Account, that is specified on every kiosk computer. Account information includes the user name, domain name and password for an Active Directory account. You should have one Shared Account per kiosk with a *Password never expires* setting.

You can configure the kiosk Shared Account by supplying the kiosk Shared Account information through GPO settings, as described below.

If the kiosk Shared Account information is distributed through Group Policies settings, all computers that belong to the selected object level in Active Directory, such as OU, Domain, or Site, receive the kiosk Shared Account settings.

DigitalPersona AD Kiosk automatically assigns the “Impersonate a client after authentication” user right to the kiosk Shared Account. This right allows programs that run on behalf of that user to impersonate a client. This right allows DigitalPersona AD Kiosk to authenticate multiple users while using only one logon session for the Shared Account.

Adding Shared Account Settings Using GPO

The Kiosk Workstation Shared Account Settings are provided as part of the GPMC Extensions component of the DigitalPersona AD Administration Tools, a separate installation available in your product package.

You can use the Group Policy Editor to modify DigitalPersona settings. For the Kiosk Shared Account Settings, at the OU level for the kiosk, open the Kiosk Administration node and double-click Kiosk Workstation Shared Account Settings. Specify the following values:

- Kiosk Shared Account user name
- Kiosk Shared Account NetBIOS domain name
- Kiosk Shared Account password

The Shared Account information will be enabled for all computers in the OU.

Assigning Kiosk Permissions

In situations where additional security restrictions are necessary or desirable, you can modify the default permissions to allow or deny specific groups or users from using each kiosk. The default installation permits every domain user to use all kiosks in the domain and no additional configuration is necessary.

For an example of how to restrict identification, see [Identification List](#) on page 253.

Password Manager Admin Tool settings

If you plan on using managed logons with DigitalPersona AD Kiosk, the templates created in the Password Manager Admin Tool must be accessible by the Shared Accounts that are used to access the kiosks. Make sure that the templates are available through GPO settings to the kiosk Shared Account rather than kiosk user accounts.

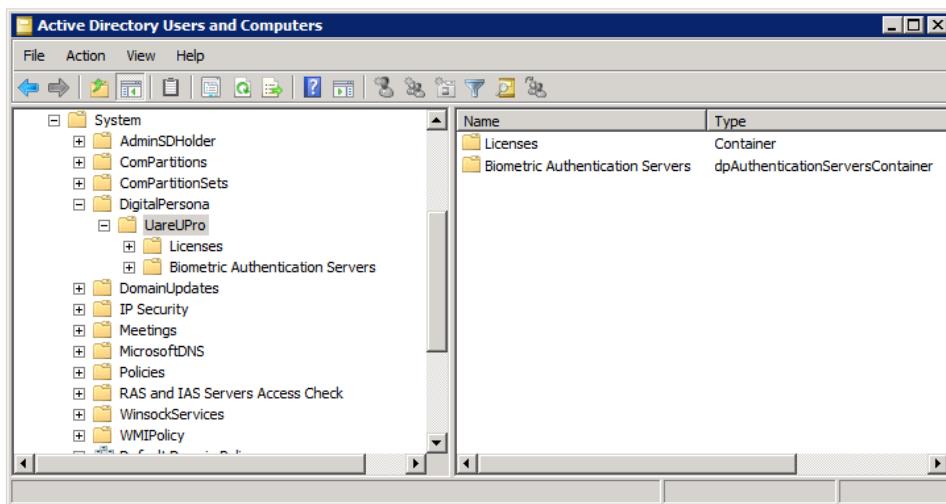
The Password Manager logon functionality is the same as in DigitalPersona AD Workstation except that kiosk users cannot create their own personal logons, but can use managed logons created by the administrator. For more information, on the Password Manager GPO settings, refer to *Policies and Settings* on page 72. For additional information on managed logons, see the Password Manager Application Guide.

Changes Made During Installation

Running the Schema Extension Wizard adds the following data to Active Directory.

Active Directory Containers

The Schema Extension Wizard installs two subcontainers in the Active Directory System container. They contain information administrators can use to verify and administer the DigitalPersona AD Server installation. In the ADUC (Active Directory Users and Computers) Snap-in, ensure that *Advanced Features* is selected from the *View* menu in order to view the System container.



The new containers installed are the BAS (Biometric Authentication Servers) container and the Licenses container.

The Biometric Authentication Servers container provides the objectCategory and objectClass for the BAS.

The Licenses container stores the license files for DigitalPersona AD products.

Published Information

DigitalPersona AD Server publishes its service using the following properties:

- Service Class Name, set to 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 AD Server software.
- Product Version High, set to [current version].
- Product Version Low, set to [current version].
- 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

The use of DNS registration enables DigitalPersona AD Workstations to locate DigitalPersona AD Servers without needing additional local configuration to do so. If your DNS Server supports dynamic registration, DigitalPersona AD Server registers itself with the DNS using the service name, _dpproent.

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

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

DigitalPersona AD Server calculates site coverage based on the availability of other DigitalPersona AD Servers on the domain (as well as sites configured for the domain) and then creates Service Resource Records (SRV RRs) for the domain and sites it covers.

Settings in the DigitalPersona AD Administrative Template govern whether or not DigitalPersona AD Server utilizes dynamic registration. For information on this and other DNS related settings, see pages 87 and following.

Automatic Registration

By default, DigitalPersona AD Server registers itself with DNS every time it starts, is automatically refreshed at specified intervals, and unregisters itself every time it stops.

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

Automatic Registration may be disabled through a GPO setting.

Manual DNS Registration

If your DNS Server does not support dynamic registration, or if dynamic registration is disabled through a DigitalPersona AD GPO setting, an administrator can manually register the DigitalPersona AD Servers by entering the DNS resource records in the format shown above.

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

To manually register a DigitalPersona AD Server in Microsoft DNS

1. Open the DNS console and expand the *Forward Lookup Zone*.
2. In the left pane, select and then 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, set the following values:
 - Service: _dpproent
 - Weight: 100
 - Port Number: 0
 - Host offering this service: domaincomputername.domainname.com
5. Click *OK* to save the settings and return to the main DNS console window.
6. Under the same [domainname], expand the *_sites* key.
7. In the left pane, select and then right-click on *Default-First-Site-Name* and select *Other New Records* from the context menu.
8. Repeat steps 3 through 5 for each DigitalPersona AD server that you want to register.

If the DP Service Resource Records (SRV RRs) are not added, either dynamically or manually, the DigitalPersona AD Workstation will not be able to find the Servers and will perform fingerprint enrollment and authentication locally.

Improving Performance

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

The _dpproent 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

Adding SRV RRs manually

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 AD Server.

Configuring DNS Dynamic Registration

Additional parameters for configuring DNS registration are available in the DigitalPersona AD Administrative Template when added to the governing GPO. These settings are described beginning on page 87.

Uninstalling DigitalPersona AD Server

DigitalPersona AD Server can be uninstalled from the Add/Remove Programs Control Panel in Windows if you have administrator privileges on the domain on which DigitalPersona AD Server is installed. The software is listed as, “DigitalPersona AD Server.”

When you uninstall the Server software, the published information (described in “Published Information” on page 26) and the DNS SRV RRs (described in “DNS Registration” on page 27) are removed.

Although the Add/Remove Programs Control Panel uninstalls DigitalPersona AD Server software, the user data (such as fingerprint credentials and secure application data) and global domain data remain in Active Directory. DigitalPersona provides a DigitalPersona AD Cleanup Wizard to remove this data. See “Utilities” on page 127 for details.

Separate installations

3

THE FOLLOWING OPTIONAL DIGITALPERSONA AD COMPONENTS ARE NOT AUTOMATICALLY INSTALLED AS PART OF EITHER THE DIGITALPERSONA AD SERVER OR CLIENT INSTALLATIONS.

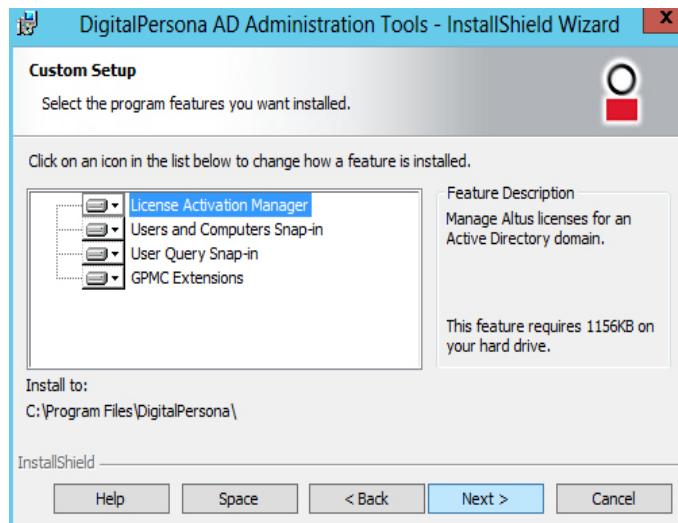
Main topics in this chapter	Page	Main topics in this chapter	Page
Components included in the product package		Components available as a separate module	
DigitalPersona AD Administration Tools	29	Web Management Components	31
License Activation Manager	30	Password Manager Admin Tool	31
Users and Computers Snap-In	30	Extended Server Policy Module (ESPM)	31
User Query Snap-in	30	Guardian ten-print scanner support	32
GPMC Extensions	30	DigitalPersona Large Scale ID wrapper	32
Attended Enrollment	31	DigitalPersona CAC/PIV card module	33

There are two categories of optional components, those included in the DigitalPersona AD product package, and those available as a separate package.

Components included in the product package

DigitalPersona AD Administration Tools

Those tools shown in the following illustration are part of a separate installation package included in the DigitalPersona AD product package.



These Administration Tools may be installed on a single workstation for centralized administration of DigitalPersona AD, or for larger organizations, each tool may be installed on a separate workstation in order to divide the administration of various features among several people.

DigitalPersona AD Workstation must be installed on the computer before the Administration Tools can be installed.

By default, all Administration Tools are installed. Select Custom Setup to deselect any tools you do not wish to install.

License Activation Manager

To install the License Activation Manager

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

For a description of the features available through this component, [see License Activation & Management](#) on page 41.

Users and Computers Snap-In

To install the snap-in

1. Locate and launch the *setup.exe* located in the .\Server\DigitalPersona AD Administration Tools folder of the DigitalPersona AD product package.
2. Select *Complete* or *Custom* installation. To install *only* the Users and Computers Snap-in, select *Custom* and deselect all other administrative tools.
3. Click *Next*, and then click *Install*.

For a description of the features available through this snap-in, see page [54](#).

User Query Snap-in

Use of the User Query Snap-in requires a licensed copy of DigitalPersona AD Workstation, and the logged on user must have domain administrator privileges.

To install the DigitalPersona User Query Snap-in

1. Locate and launch the *setup.exe* located in the .\Server\DigitalPersona AD Administration Tools folder of the product package.
2. Select *Complete* or *Custom* installation. To install *only* the User Query Snap-in, select *Custom* and deselect all other administrative tools.
3. Click *Next*, and then click *Install*.

For a description of the features available through this snap-in, and additional implementations of the tool, see page [56](#).

GPMC Extensions

DigitalPersona AD Server and its associated workstation clients use GPMC/GPOE extensions, installed under the *Software Settings* and *Administrative Templates* nodes, to link product policies and settings to Active Directory containers. These policies and settings are described in the chapter, *Policies and Settings* on page 72.

To install the DigitalPersona GPMC/GPOE Extensions

1. Locate and launch the *setup.exe* located in the .\Server\DigitalPersona AD Administration Tools folder of the package.
2. Select *Complete* or *Custom* installation. To install *only* the GPMC/GPOE Extensions, select *Custom* and deselect all other administrative tools.
3. Click *Next*, and then click *Install*.

For a description of the features available through this component, [see GPMC/GPOE Extensions](#) on page 65.

Attended Enrollment

DigitalPersona Attended Enrollment is an optional feature of the DigitalPersona client software, DigitalPersona AD Workstation. Its installation and features are therefore addressed in the DigitalPersona AD Client Guide. However, there is a small amount of setup that must be performed in Active Directory by an administrator. Instructions for setup are contained in the chapter *Attended Enrollment* beginning on page 94.

Separate product packages

The following security applications and modules are separately installed and may be separately licensed.

Web Management Components

The Web Management Components module contains a collection of components that together enable management of your DigitalPersona environment through a web based interface. For installation instructions and complete details, see *Section Three: Web Management* beginning on page 164.

Password Manager Admin Tool

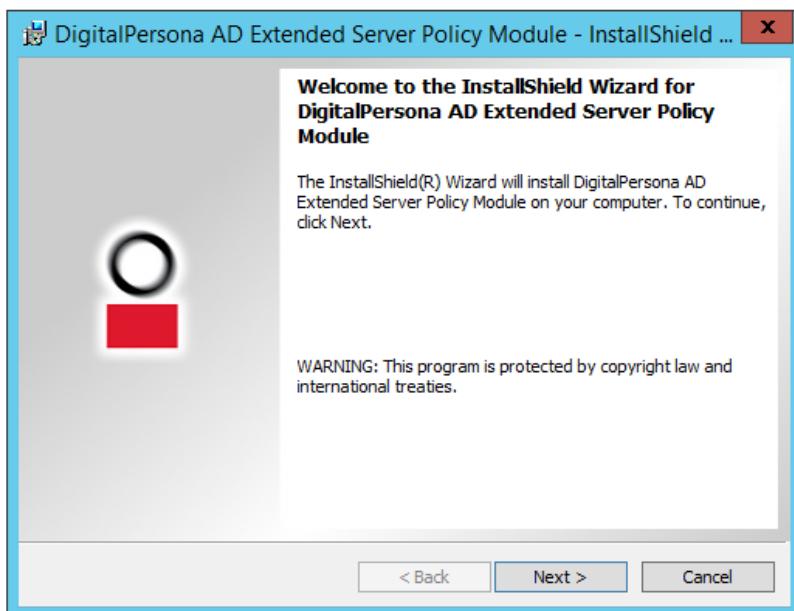
The Password Manager Admin Tool can be used by DigitalPersona AD administrators to create automated *managed* logons for websites, applications and network resources. For complete a detailed product description and installation instructions, see the *Password Manager Admin Tool* chapter beginning on page 134.

Extended Server Policy Module (ESPM)

The DigitalPersona ESPM adds additional per-user policy settings to Active Directory. For a description of these settings, see page 63.

To install the Extended Server Policy Module

1. Copy the package received from Crossmatch, your channel partner or reseller to the computer where DigitalPersona AD Server is installed, or any Active Directory-aware computer that will be used to administer the DigitalPersona AD Server.
2. Launch the installer by clicking setup.exe. Follow the onscreen instructions.



3. Licensing is included in the product purchase. No additional entry of a license number is required.

Guardian ten-print scanner support

In order to use the Guardian family of ten-print scanners with your DigitalPersona product, you will need to install the following:

- A DigitalPersona client (Workstation, Kiosk, Attended Enrollment or Mobile Enrollment)
- DigitalPersona Guardian Support package
- L Scan Essentials (LSE) SDK RunTime component

The DigitalPersona Guardian Support and L Scan Essentials SDK products are available from Crossmatch or your channel partner/reseller.

Both DigitalPersona Guardian Support and the LSE SDK RunTime component must be installed on each computer where the Guardian scanner will be used.

DigitalPersona Large Scale ID wrapper

Requirements

Hardware and software requirements are the same as those specified for the DigitalPersona component using the wrapper, i.e either the DigitalPersona Server or one of the DigitalPersona clients.

WARNING: The following procedure requires the previous installation of the MegaMatcher Accelerator from Neurotechnology.

Installing the Neurotechnology MegaMatcher SDK

Before installing the DigitalPersona Large Scale ID Wrapper, you should have previously installed, configured and activated licenses for the *Neurotechnology MegaMatcher Accelerator* on a dedicated machine. This is generally accomplished through the services of the Crossmatch Solutions Team.

Installing the wrapper on a DigitalPersona Server

1. Install the Neurotec Biometric SDK and ensure that the *Neurotechnology* service is running.
2. Configure the PATH environment to the Neurotechnology SDK Bin folder. For example, if the SDK was installed to the default folder on a 64-bit machine, you would set the PATH environment to:

C:\Program Files (x86)\Neurotechnology\Neurotec Biometric 5.1 SDK\Bin\Win64_x64
3. Install DigitalPersona Server. Choose Custom installation and deselect the *Fingerprint Recognition Engine* component. *Do not activate any DigitalPersona Server licenses at this time.*
4. Install the DigitalPersona Large Scale ID Wrapper.
5. Configure the path to the computer where MegaMatcher Accelerator is installed by creating the following key in the registry.

[HKEY_LOCAL_MACHINE\SOFTWARE\DigitalPersona\NEUROTECH]

Enter the following property values.

"Host"="n.n.n.n" (IP Address of MegaMatcher Accelerator as a string)

"Port"=dword:[command listening port]

"AdminPort"=dword:[administrator command listening port]

Note that by default the value of a dword is hexadecimal, but you would ordinarily be entering the port number as a decimal, so make sure to select *decimal* as the option when creating the key.

6. Restart the DigitalPersona Server.

7. Activate your DigitalPersona Server Licenses.

Installing the wrapper on a DigitalPersona client

1. Install the Neurotec Biometric SDK and ensure that the *Neurotechnology* service is running.
2. Configure the PATH environment to the Neurotechnology SDK Bin folder. For example, if the SDK was installed to the default folder on a 64-bit machine, you would set the PATH environment to:
C:\Program Files (x86)\Neurotechnology\Neurotec Biometric 5.1 SDK\Bin\Win64_x64
3. Install the DigitalPersona client. Choose *Custom* installation and deselect the *Fingerprint Recognition Engine* component.
4. Install the DigitalPersona Large Scale ID Wrapper.
5. Restart the DigitalPersona client.

DigitalPersona CAC/PIV card module

The optional DigitalPersona CAC/PIV card module works with the *YubiKey NEO* USB device to provide multiple authentication credentials, including PIV, OTP and U2F, depending on what applications are installed on the token. Therefore, one YubiKey device can serve the purpose of two or three separate authentication tokens, for example, it can be used as both a Smart Card and a One-Time Password token.

The YubiKey NEO USB dongle with CCID mode enabled supports the Personal Identity Verification (PIV) card interface and can be used with DigitalPersona software, versions 2.3 and above, as a highly secure PKI Smart Card token. For more information, refer to this link: <https://developers.yubico.com/PIV/>.

A significant advantage to this token is that it doesn't require purchase of ActivClient middleware, but instead uses its own downloadable YubiKey PIV minidriver.

Initializing the PIV token

Each YubiKey NEO device must be initialized before distribution to the end-user.

To initialize the YubiKey NEO device

1. Download and install the *YubiKey NEO Manager* application and enable the CCID connection mode. For details, see the following YubiKey document: <https://www.yubico.com/wp-content/uploads/2014/11/NEO-Manager-Quick-Start-Guide.pdf>.
2. Download and install the *YubiKey PIV Manager* application. For details, see the following YubiKey document: https://www.yubico.com/wp-content/uploads/2016/04/YubiKey-PIV-Manager_Users_Guide_April04_2016.pdf.
3. Use the *YubiKey PIV Manager* to initialize the YubiKey device. This will include
 - Creating a new PIN
 - Creating a self-signed authentication certificate and a pair of 2048-bit RSA asymmetric keys.

Installing the YubiKey Smart Card Minidriver

The YubiKey Smart Card Minidriver (version 3.3.1.5 or above) must be installed on each DigitalPersona client machine where the YubiKey device will be used.

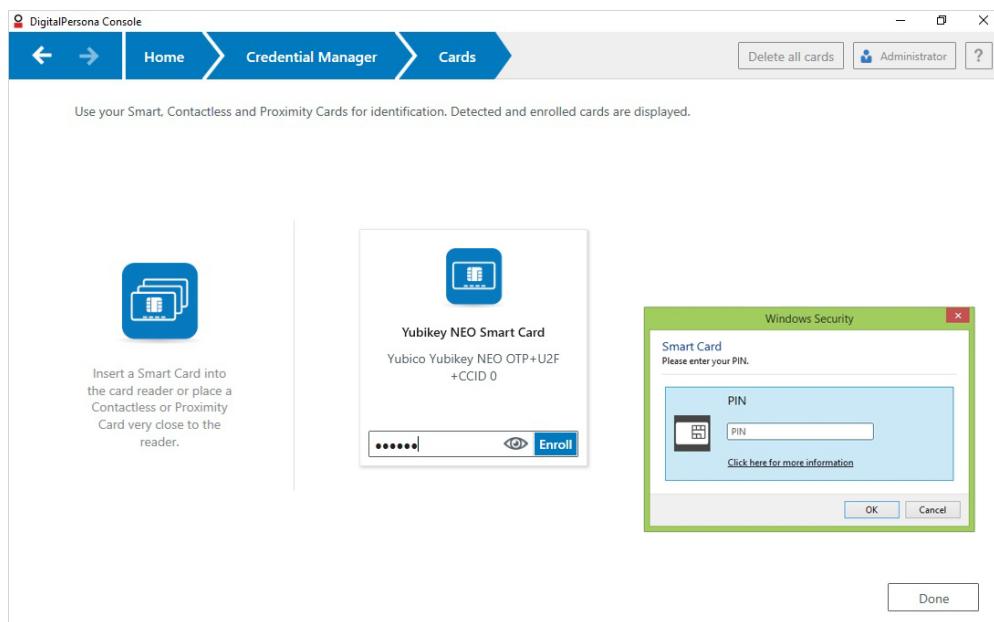
The Minidriver is available through Microsoft Windows Update, or can be downloaded directly from the Yubico website at <https://www.yubico.com/support/knowledgebase/categories/downloads/>. For additional details about the driver, see the following YubiKey document: https://www.yubico.com/wp-content/uploads/2017/10/YubiKey_Smart_Card_Minidriver_User_Guide_10_2017_RevA.pdf.

Note that ActivClient PKI client's PIV minidriver can be used with the YubiKey NEO, however it is not recommended since Windows logon will not be supported and other errors may occur. The YubiKey Smart Card Minidriver should be installed manually to replace the ActivClient PIV minidriver.

Enrolling the YubiKey Smart Card

The previously initialized YubiKey Smart Card is enrolled in the same manner as any other supported Smart Card, on the *Cards* page of the *DigitalPersona Credential Manager*, within the DigitalPersona clients, from DigitalPersona Attended Enrollment and from DigitalPersona Web Enrollment.

When using an empty YubiKey Smart Card with version 3.3.1.5 of the Minidriver, the keys created by the PIV Manager might be not available to the DigitalPersona software. In this case, a new key pair is created on the card during an initial enrollment. This will cause a second request for the card PIN to be displayed by Windows, which may sometimes be hidden behind the window currently in focus (as shown in the following image).



Additional considerations

The YubiKey Smart Card PKCS11 module (libykcs11-1.dll) installed with the August 2017 version of the YubiKey PIV Manager should not be used on the same computer as the YubiKey Smart Card Minidriver.

Older YubiKey devices featuring a contactless MiFare interface can be used in with DigitalPersona software, however the YubiKey NEO does not support MiFare. Use of the YubiKey NEO in CCID connection mode (for PIV) will cause the MiFare interface on the older device to fail irretrievably.

Section Two: Administration

Section Two of the DigitalPersona AD Administrator Guide includes the following chapters.

Chapter Number and Title	Purpose	Page
4 - Administration overview	Describes the types of tools and utilities available for administration of DigitalPersona AD.	37
5 - Administration Tools	Describes the DigitalPersona AD Administration Tools, a collection of administrative tools for managing your DigitalPersona software.	38
6 - License Management	Describes the types of licenses available, the license activation process, and the information provided to administrators for managing their licenses.	41
7 - ADUC Snap-ins	Describes the user properties settings, user object commands and computer object commands that are added to Active Directory by the installation of the ADUC Users and Computers Snap-in.	54
8 - Extended Server Policy Module	Describes a separately purchased and installed server module that adds additional per user policies to the DigitalPersona tab in the AD user Properties tab.	63
9 - GPMC/GPOE Extensions	Describes use of the DigitalPersona Group Policy Object extensions that enable configuration of DigitalPersona AD policies and settings.	65
10 - Policies and Settings	Defines the policies and settings that govern DigitalPersona AD Servers and clients.	72
11 - Attended Enrollment	Describes a feature available through a Custom install of the DigitalPersona Client that enables an assigned user or group to supervise enrollment of user credentials.	94
12 - Password Randomization	Describes how to configure Password Randomization options through .xml files associated with DigitalPersona clients.	97
13 - Single Sign-On	Describes how to implement a Single Sign-On (SSO) policy in the enterprise.	101
14 - Recovery	Describes the user and computer recovery options made available through DigitalPersona AD.	102
15 - DigitalPersona Reports	Describes DigitalPersona Reports, a tool for aggregating and reporting on DigitalPersona AD events generated by DigitalPersona AD Server and clients.	104
16 - DigitalPersona Events	Lists and describes the events that DigitalPersona AD writes to the Windows Event log.	119
17 - Utilities	Describes additional utilities provided within the DigitalPersona AD product package.	127

Chapter Number and Title	Purpose	Page
18 - Delegating permissions	Describes how to delegate permissions for performing various administrative tasks within the DigitalPersona AD environment.	128
19 - Password Manager Admin Tool	Describes use of the Password Manager Admin Tool to create and administer Managed Logons.	134

THIS CHAPTER PROVIDES AN OVERVIEW OF THE FEATURES, COMPONENTS, TOOLS AND UTILITIES PROVIDED FOR THE ADMINISTRATION OF DIGITALPERSONA AD SERVER AND CLIENTS.

Overview

DigitalPersona provides a full complement of features, tools and utilities to assist the administrator in managing various aspects of the product, as well as expanding the functionality of the product.

Some of these tools and utilities are included in the product packages for either DigitalPersona AD Server or DigitalPersona AD Workstation. Others are available as separate modules, which may be obtained from your Crossmatch Account Manager or product Reseller.

The following chapters in this section describe the administrator tools available to the DigitalPersona administrator.

About GPO settings

Most of the settings that govern the features and behavior of the DigitalPersona AD solution are controlled through Active Directory GPO settings (see Policies and Settings on page 72). Additional settings and behaviors may be configured through Microsoft's ADSI Editor and through custom *VBS*cript scripts.

We strongly recommend managing all DigitalPersona policies through a separate OU linked to an Organizational Unit (OU), and avoiding making any changes to the "Default Domain Policy."

However, note that GPO settings that are left "Not Configured" in Active Directory may be configured by the local administrator by installing the GPMC Extensions feature from the Administration Tools component to a computer. Local settings that are configured will then be effective for all users on the specific computer.

Whenever a setting is configured (enabled or disabled) in Active Directory, the local administrator cannot modify the setting at the local computer.

For this reason – especially if the needs specific to your environment require you to provide end users with local administrative rights – Crossmatch strongly recommends IT Administrators explicitly configure each desired setting in Active Directory, rather than relying on default behaviors associated with the unconfigured state.

About credentials

FIDO Keys

If FIDO Key credentials will be used with DigitalPersona Web Components, i.e. Identity Provider, Web Administration Console or Web Enrollment, the Web Management Components module should be installed and configured prior to any user enrolling a FIDO Key credential. If a FIDO Key credential is enrolled through the DigitalPersona Workstation User Console, prior to the successful configuration of the Web Management Components, the credential will not roam and cannot be managed through Web Enrollment or used to authenticate to any DigitalPersona web-based component,

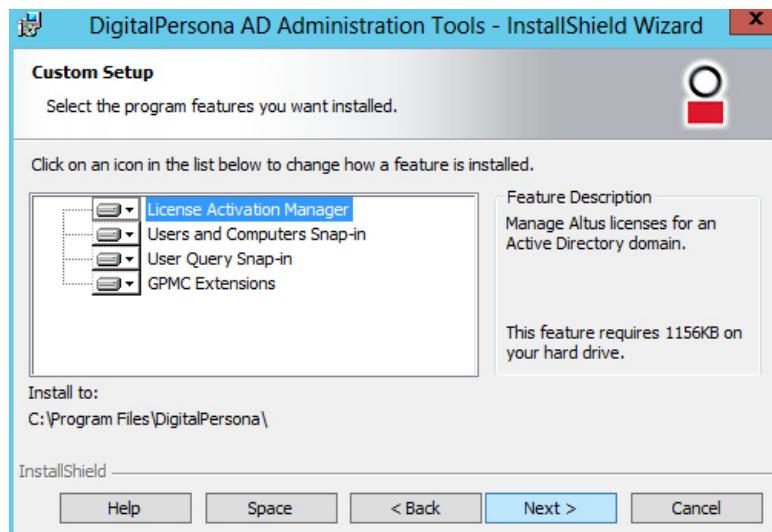
Bluetooth credentials

Enrollment of the Bluetooth credential is not supported in Web Enrollment.

THIS CHAPTER DESCRIBES THE ADMINISTRATION TOOLS THAT ARE PROVIDED TO ASSIST THE ADMINISTRATOR IN MANAGING THE DIGITALPERSONA AD INSTALLATION.

Overview

Those tools shown in the illustration below are part of a separate installation package included in the DigitalPersona AD product package. These Administration Tools may be installed on a single workstation for centralized administration of DigitalPersona AD, or for larger organizations, each tool may be installed on a separate workstation in order to divide the administration of various features among several people.



CAUTION: The Administration Tools should not be installed on a computer until after the *DigitalPersona Active Directory Domain Configuration Wizard* has been run.

To install the DigitalPersona AD Administration Tools, do one of the following.

- Locate and double-click the setup.exe file located in the DigitalPersona AD Administration Tools directory of the product package. Follow the instructions in the installer wizard. Select **Custom** to choose which tools to install. Press the down arrow to select installation options for a component.
- For silent installation, use the syntax shown below to install all tools or remove those you do not want to install. For example, to install only the Attended Enrollment Tool:

```
msiexec /i setup.msi ADDLOCAL=ALL REMOVE=LicenseControlManager,UsersComputersSnapin,UserQuerySnapin
```

For descriptions of the separate components, see the following chapters, *License Activation & Management* on page 41 and *ADUC snap-ins* on page 54.

Attended Enrollment

DigitalPersona Attended Enrollment is an optional feature of the DigitalPersona client software, DigitalPersona AD Workstation. Its installation and features are therefore addressed in the DigitalPersona AD Client Guide. However, there is a small amount of setup that must be performed in Active Directory by an administrator. Instructions for setup are contained in the chapter "*Attended Enrollment*" beginning on page 94.

Hardware Tokens Management Utility

The Hardware Tokens Management Utility is a Windows command line utility copied to the target machine as part of a DigitalPersona Administration Tools installation. The utility imports a vendor-supplied XML file containing information about a set of hardware tokens that will be enrolled by users for generating One-Time Passwords. It can also be used to query information about the tokens and their users.

In order to use Time-based One-Time Password algorithm (TOTP) hardware tokens for the generation of One-Time Passwords, the serial numbers of these hardware tokens must first be registered with the DigitalPersona Server by using the *Hardware Tokens Management Utility*.

Note that the utility must be run from an elevated command prompt.

To run the *Hardware Tokens Management Utility*

1. Open an elevated command prompt by right-clicking any Command Prompt shortcut on the Windows Start menu (located by default in the Accessories folder) and selecting *Run as administrator*.
2. In the Command Prompt window, run *DPOTPMgr.exe* using the following syntax and parameters.

By default, DPOTPMgr.exe is located in the following folder after installation of the DigitalPersona Administration Tools: C:\Program Files\DigitalPersona\Bin. Navigate to the folder where the file is located or enter the full path name to the file.

Example:

```
C:\Program Files\DigitalPersona\Bin\DPOTPMgr.exe /i /f tokenfilename /u MYDOMAIN\username
```

Note that although the internal file format must be PKSC, the actual file extension may be PKSC, xml or there may be no extension.

Syntax

```
DPOTPMgr.exe [/i] [/f <FileName>] [/u <UserName> [/?]
```

Parameters

Parameter	Description
/i	Specifies import mode. The default mode is informational.
/f <FileName>	Identifies the name of the file to be imported.
/u <UserName>	<UserName> Provides information about OTP tokens which are enrolled by a specific user. NOTE: Name should be provided in SAM compatible format. For example: MYDOMAIN\myusername
/?	/? Displays help for this command.

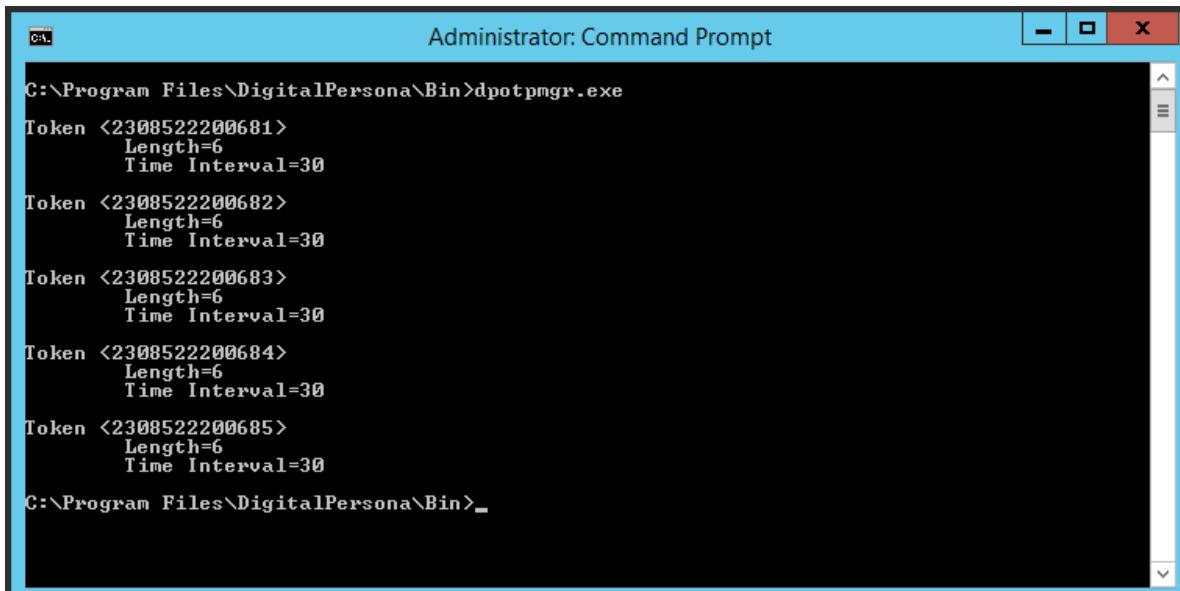
Examples

```
DPOTPMgr.exe /i /f C:\temp\2308522200681-2308522200685.xml
```

The above example imports registration information for OTP tokens from an XML file provided by the hardware token vendor.

```
DPOTPMgr.exe
```

The above query example returns information about all hardware OTP tokens registered in the DigitalPersona instance, as shown below.



A screenshot of an Administrator Command Prompt window titled "Administrator: Command Prompt". The window shows the output of the command "dpotpmgr.exe". The output lists five tokens, each with a unique identifier (length 6) and a time interval of 30 seconds.

```
C:\>Program Files\DigitalPersona\Bin>dpotpmgr.exe
Token <2308522200681>
    Length=6
    Time Interval=30
Token <2308522200682>
    Length=6
    Time Interval=30
Token <2308522200683>
    Length=6
    Time Interval=30
Token <2308522200684>
    Length=6
    Time Interval=30
Token <2308522200685>
    Length=6
    Time Interval=30
C:\>Program Files\DigitalPersona\Bin>_
```

DPOTPMgr.exe /u MYDOMAIN\myusername

The above query example returns information about any hardware OTP tokens enrolled by a specific user.

THIS CHAPTER DESCRIBES ACTIVATION AND MANAGEMENT OF DIGITALPERSONA LICENSES.

Main topics in this chapter	Page
Product Options	41
DigitalPersona License Group Policy Object	42
Evaluation license	42
License activation	42
License activation from another computer	44
Checking for license updates	47
Displaying license properties	48
License deactivation	49
License deactivation from another computer	50
Releasing user licenses	53

Overview

Activation and management of DigitalPersona licenses is provided through a series of intuitive wizards for activating, deactivating and refreshing DigitalPersona licenses. These actions may also be initiated through a Command Line Interface, by executing the file *DPLicActivator.exe*. Help for the parameters and flags, as well as a short description of the activation process, is available by executing *DPLicActivator.exe help*.

There are three ways that DigitalPersona software is licensed.

Perpetual - allows use of purchased DigitalPersona software for a specified number of users, indefinitely, and includes the first year of support and maintenance.

Subscription - allows use of purchased DigitalPersona software for a specific period and for a specified number of users, and includes support and maintenance.

Evaluation - is automatically activated upon installation and allows use of DigitalPersona software for a limited period of time for up to 10 users.

IMPORTANT: Any activation of DigitalPersona licenses (from the Licenses GPO on the DigitalPersona AD Server or when using a License Transfer file for remote license management), requires access to the following URL: <https://solo.digitalpersona.com>. This URL is also accessed when verifying licenses from the link in the Active Directory Group Policy Management Editor *License Properties* dialog for the DigitalPersona AD Server.

For air-gapped environments, when initially launching the License Manager, it is critical that the computer is connected to the internet, but **does not** have access to a DigitalPersona Server. After a Request Transfer file has been generated, the License Manager should be run again on the DigitalPersona Server to be licensed. See detailed steps in the following section, *License activation from another computer*.

Product Options

A DigitalPersona AD license has a single Product Option. Each activated license is shown under the *Licensed product options* heading in the DigitalPersona License GPO (shown below).

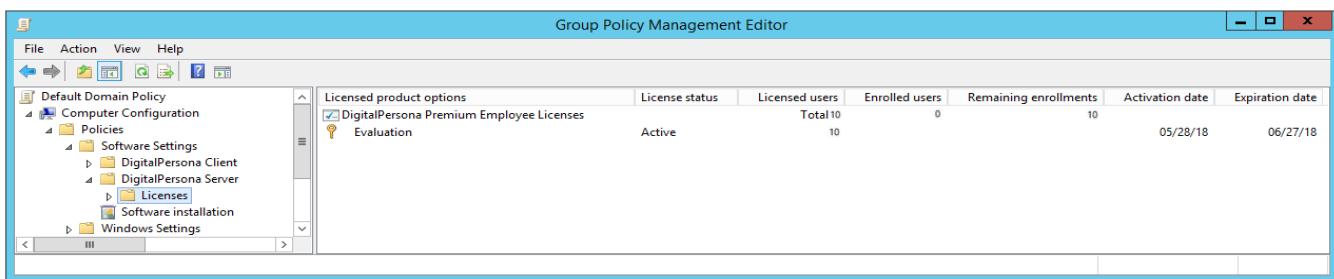
DigitalPersona Premium Employee License - Permits the enrollment of user credentials, and subsequent use by a specified number of users with Active Directory accounts.

DigitalPersona License Group Policy Object

The DigitalPersona License Group Policy Object is installed automatically as part of the DigitalPersona Administration Tools. It provides an Active Directory-based means of activating and managing your DigitalPersona licenses, as well as providing detailed information about the licenses and their use.

- If the DigitalPersona Server was installed on a member server (i.e. not a domain controller), you may need to add the Group Policy Management feature in order to see or edit DigitalPersona group policies.
- In order to view and edit DigitalPersona group policies, you will need to install the DigitalPersona Administration Tools.

After installation of the DigitalPersona Administration Tools, the DigitalPersona *Server* object can be accessed through the Group Policy Management Editor and used to activate, deactivate and refresh licenses for the DigitalPersona solution.



Evaluation license

Your DigitalPersona solution comes with a 30-day Evaluation License for 10 users. Upon product activation with a purchased license, the evaluation license is hidden. If all licenses are deactivated, the Evaluation license will redisplay.

License activation

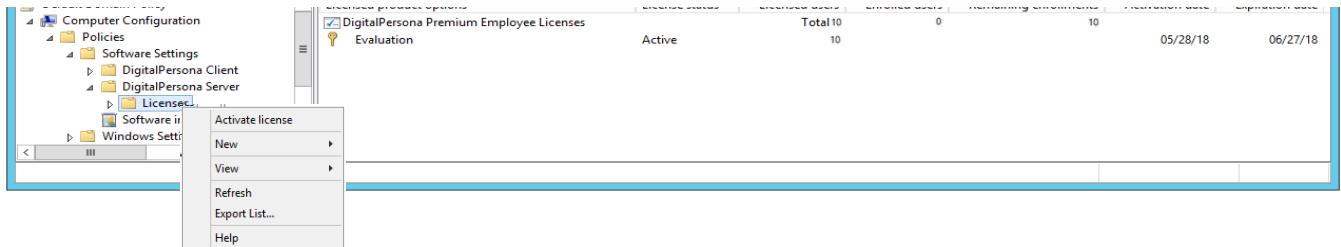
The DigitalPersona user license is issued with a unique License ID and password. The license may be activated, deactivated or refreshed through various wizards launched through the Active Directory Group Policy Management Editor on the computer where the DigitalPersona Server is installed.

If you need to activate a license for a DigitalPersona Server that is not connected to the internet, see the topic *License activation from another computer* below.

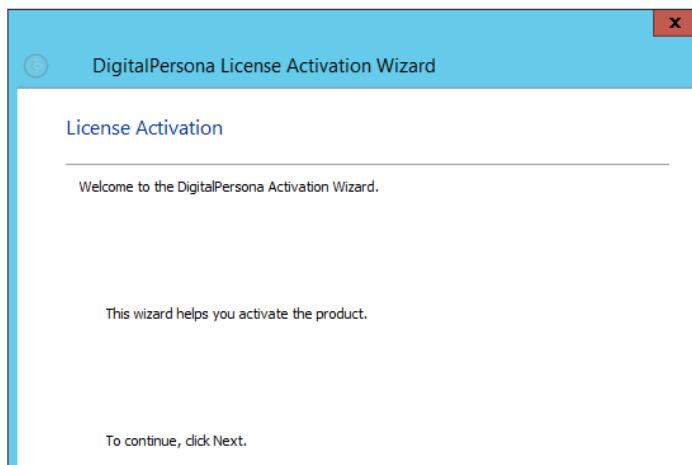
In most cases, you will activate your DigitalPersona Servers over the internet through Active Directory and the DigitalPersona Activation wizard.

To activate a DigitalPersona user license

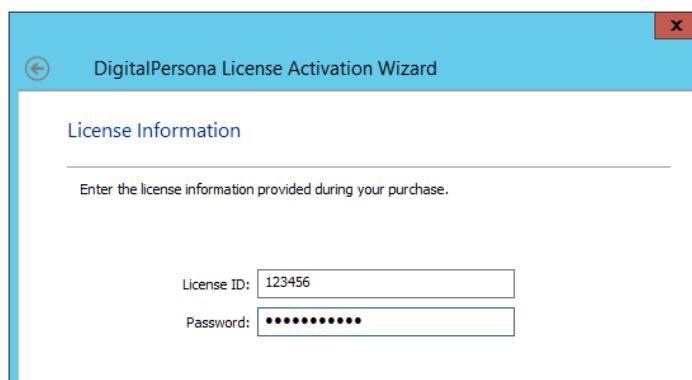
1. In the Group Policy Management Editor, navigate to: *Computer Configuration, Software Settings, DigitalPersona Server, Licenses*.
2. Right-click on *Licenses* and select *Activate license*.



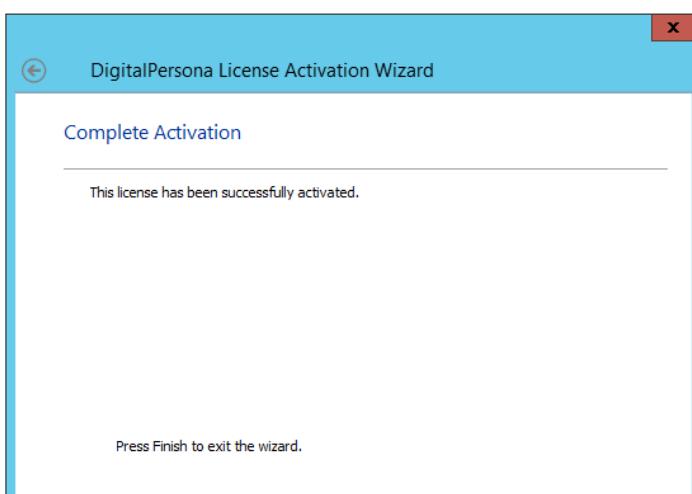
3. When the DigitalPersona Activation Wizard displays, click *Next*.



4. Enter the license information provided during the purchase of your DigitalPersona software.



5. If the license information is valid and the wizard is able to contact the activation server, the license will be activated.



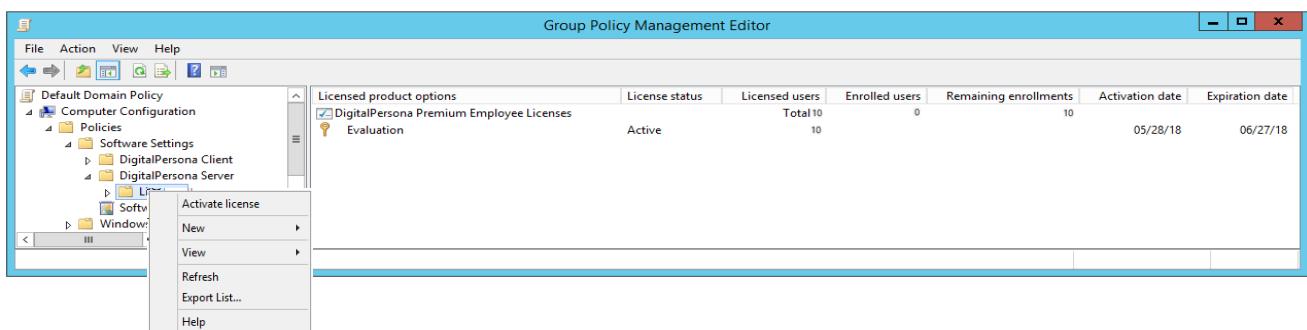
License activation from another computer

If your DigitalPersona Server does not have access to the internet, you can activate it remotely through the use of any computer that has internet access. *Installation of the Group Management Console and the DigitalPersona Administration Tools are required on the computer used for remote activation.*

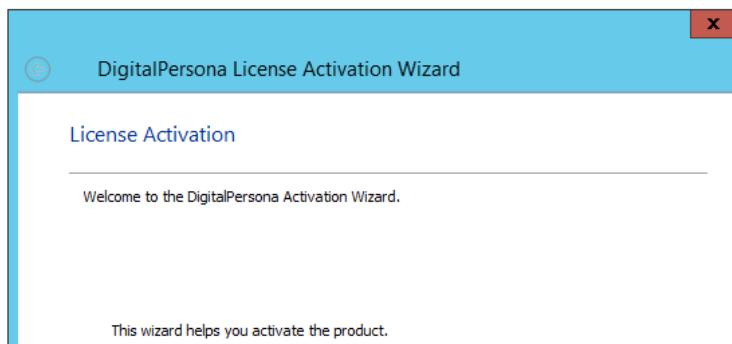
To remotely activate your DigitalPersona license

On your DigitalPersona Server,

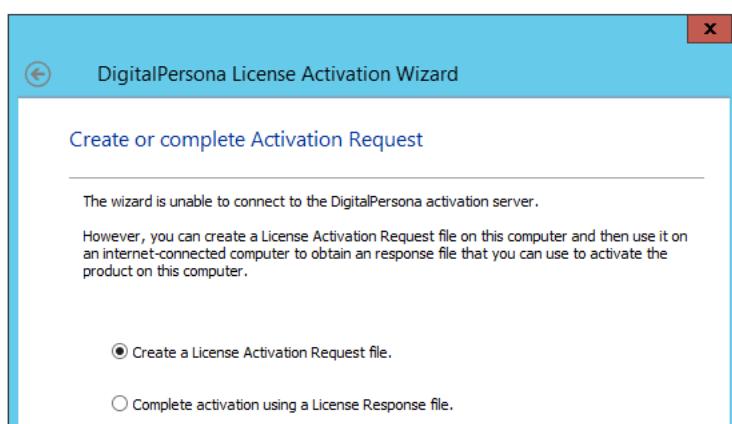
1. In the Group Policy Management Editor; navigate to *Computer Configuration, Policies, Software Settings, DigitalPersona Server, Licenses*.
2. Right-click on *Licenses* and select *Activate license*.



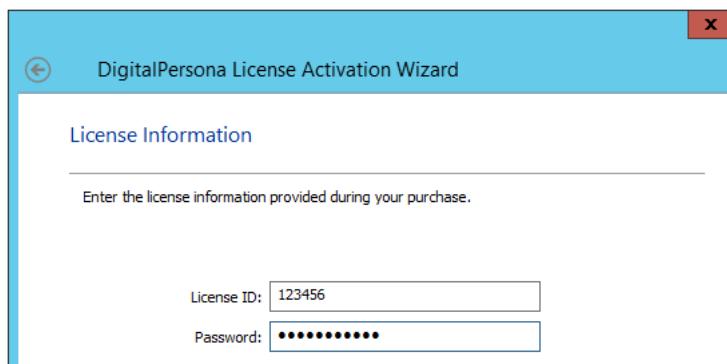
3. When the DigitalPersona License Activation Wizard displays, click *Next*.



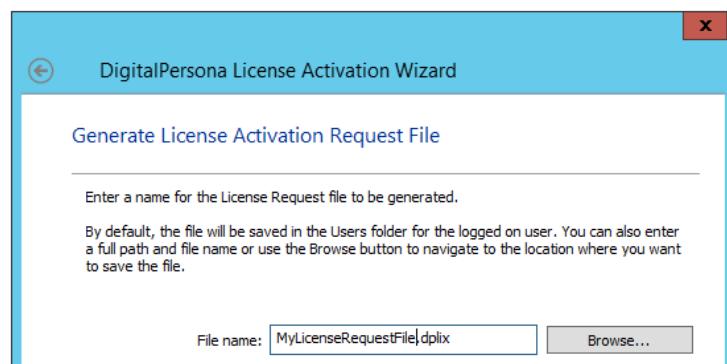
4. On the *Create or complete Activation Request* page, select *Create a License Activation Request file*.



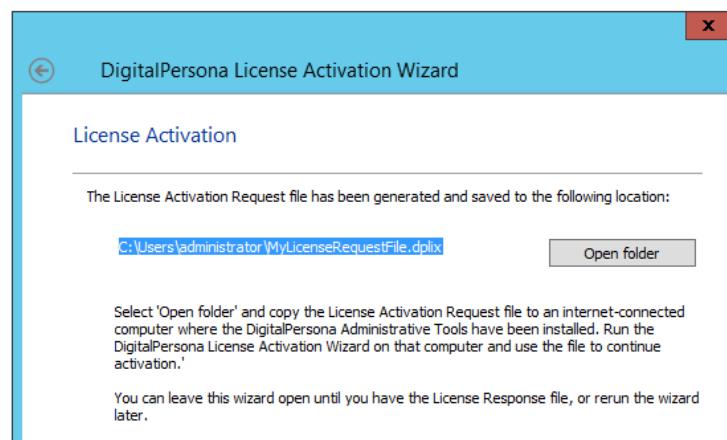
5. On the *License Information* page, enter the license information provided during your purchase.



6. On the *Generate License Activation Request file* page, enter a name for the file to be generated.



By default, the file will be saved in the Users folder of the logged on user. You can also enter a full path and file name or use the *Browse* button to navigate to the location where you want to save the file.



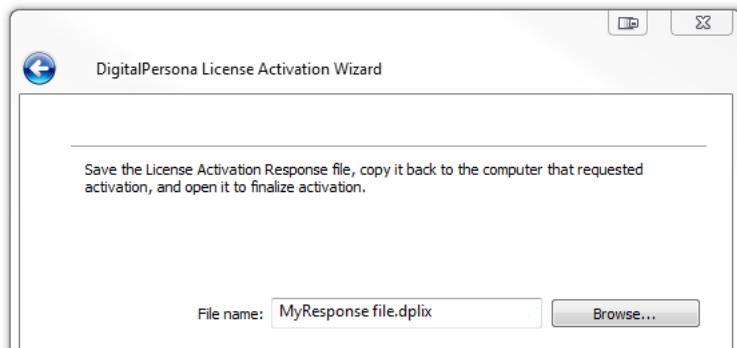
7. Copy the resulting *License Activation Request (.dplix) file* to a shared directory or device that can be accessed from a computer with an internet connection and the DigitalPersona Administrative Tools installed.

You can leave this wizard open until you have the License Activation Response file, or rerun the wizard later.

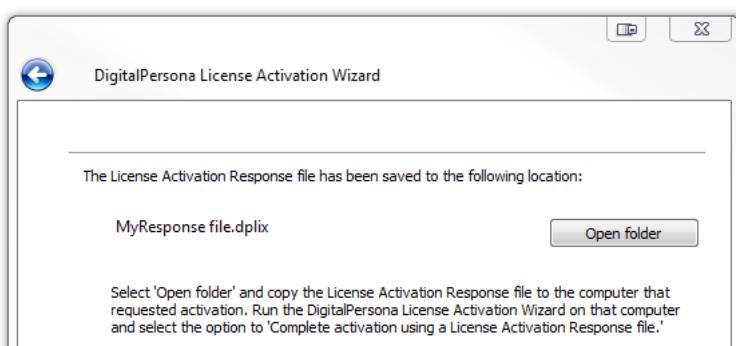
On an internet-enabled computer

8. Install *DigitalPersona Administrative Tools* (if not previously installed).
9. Navigate to, and double-click the License Activation Request file generated in step 6 above.
10. The *DigitalPersona License Activation Wizard* will launch. Click *Next*.

- Enter a name for the License Activation Response file to be generated.



By default, the file will be saved in the Users folder of the logged on user. You can also enter a full path and file name or use the *Browse* button to navigate to the location where you want to save the file.



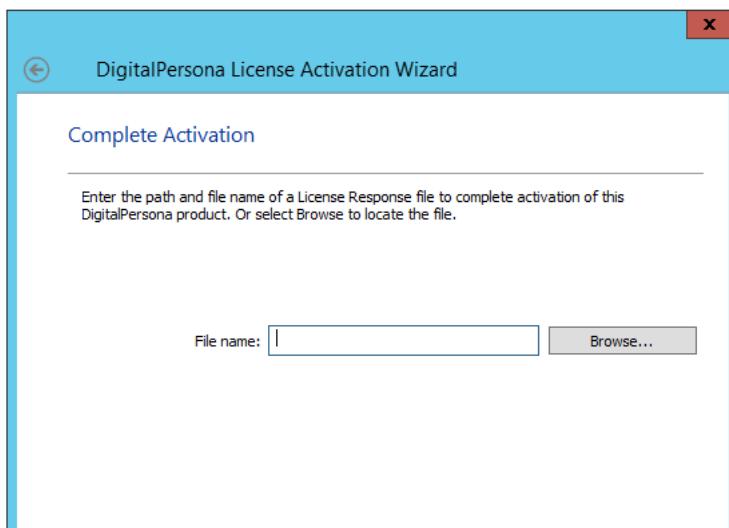
- Click *Next* and then click *Finish* to close the wizard.

- Copy the response file back to the DigitalPersona Server machine.

On the DigitalPersona Server

- If you have left the wizard open, click *Next*.

- On the *Complete Activation* page, enter the path and file name of the *License Activation Response* file to complete activation of your DigitalPersona product. Or select *Browse* to locate the file.



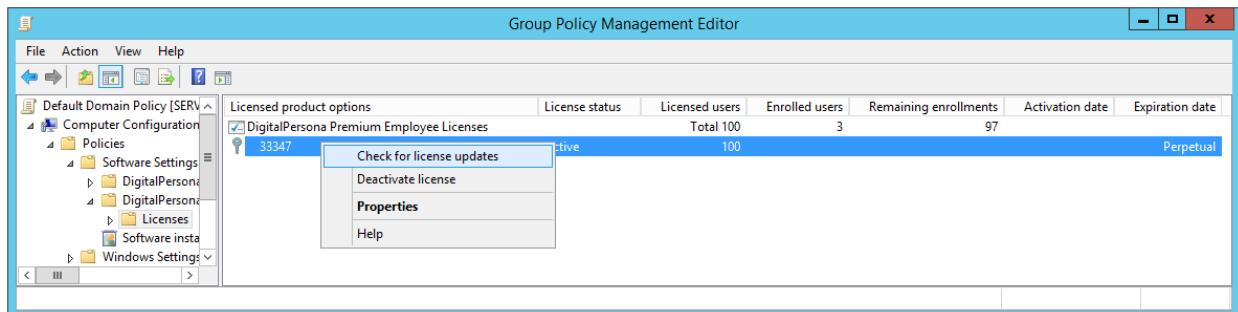
- Enter the path to, or Browse to, the location of the *License Activation Response* file (specified in step 11 above). Click *Next*.

- Upon successful activation, the final page of the wizard displays. Click *Finish* to close the wizard.

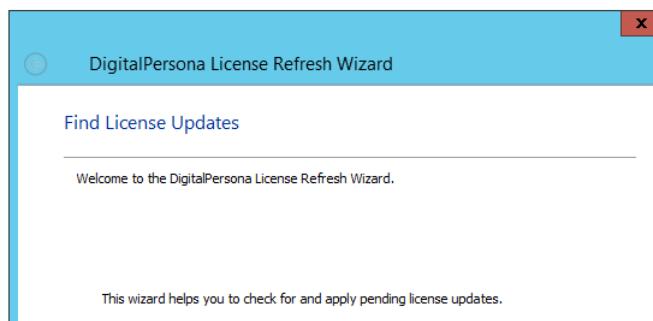
Checking for license updates

To check for updates to your licenses

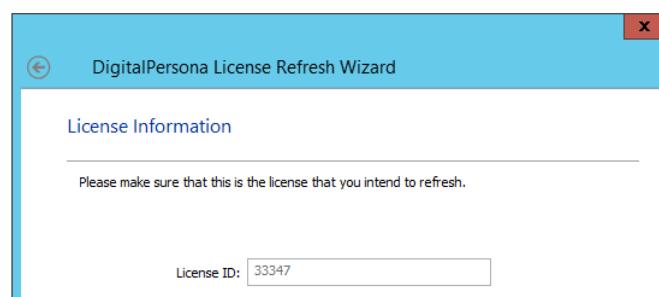
1. In the Group Policy Management Editor; navigate to *Computer Configuration, Policies, Software Settings, DigitalPersona Server, Licenses.*
2. Right-click on a license and select *Check for license updates.*



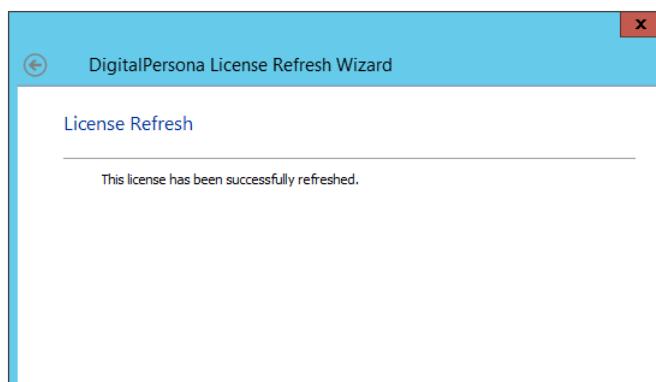
3. When the DigitalPersona License Refresh Wizard displays, click *Next.*



4. On the *License Information* page, check to make sure that the License ID identifies the license that you are refreshing.

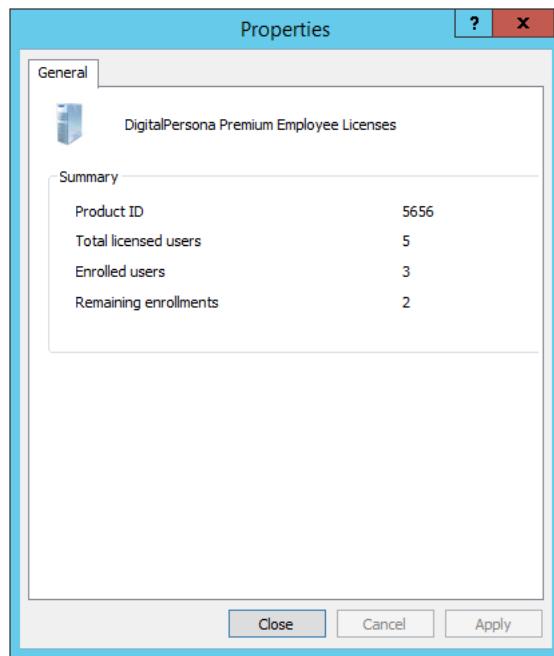


5. Once the license has been successfully refreshed, click *Finish* to close the wizard.

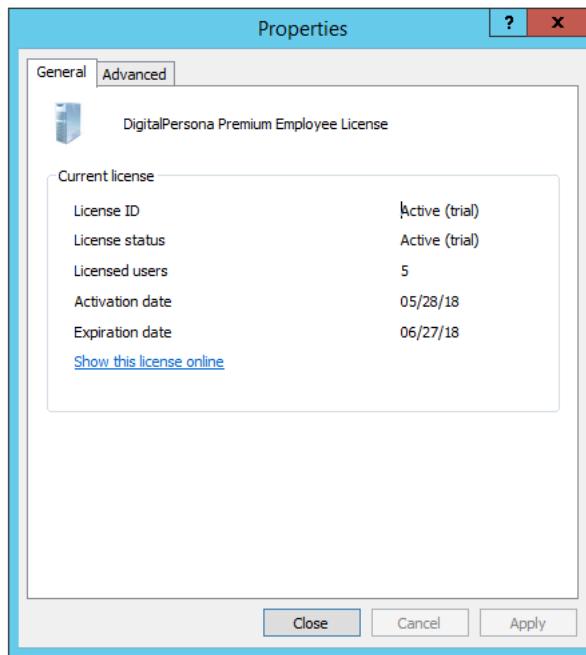


Displaying license properties

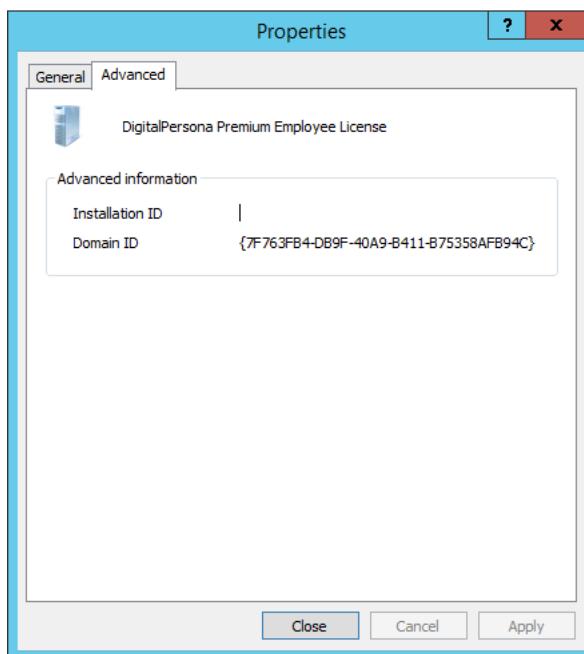
To display a summary of license information for all DigitalPersona licenses installed on this machine, right click anywhere on the *Licensed product option* line and select *Properties*.



To display detailed information for a specific license, right click on the license and select *Properties*.



To display advanced information for a specific license, right click on the license and select *Properties*. Then select the *Advanced* tab.



License deactivation

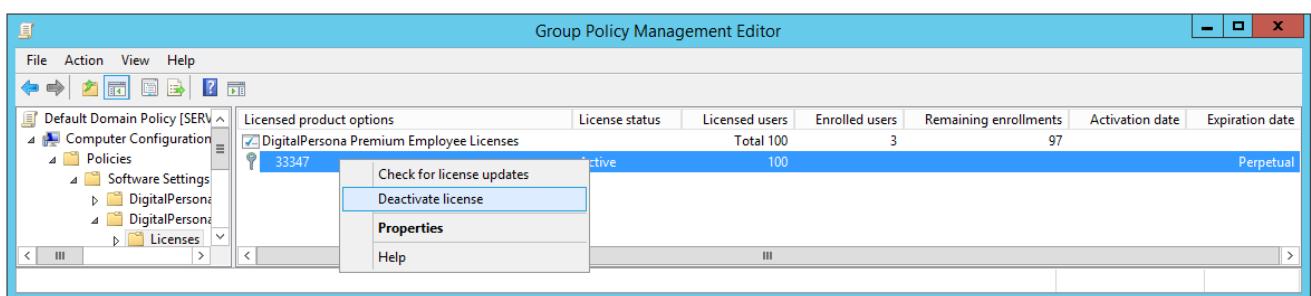
Your DigitalPersona license may be deactivated through the *DigitalPersona Deactivation Wizard*, launched through the Active Directory Group Policy Management Editor on the computer where the DigitalPersona Server is installed.

If your DigitalPersona Server is not connected to the internet, see the topic *License deactivation from another computer* below.

In most cases, you will deactivate your DigitalPersona Server license over the internet through Active Directory and the DigitalPersona Deactivation wizard.

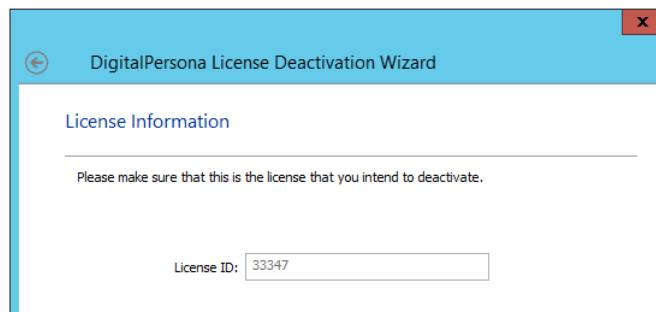
To deactivate a DigitalPersona license

1. In MMC, navigate to: *Computer Configuration*, *Software Settings*, *DigitalPersona Server*, *Licenses*.
2. Right-click on *Licenses* and select *Deactivate license*.

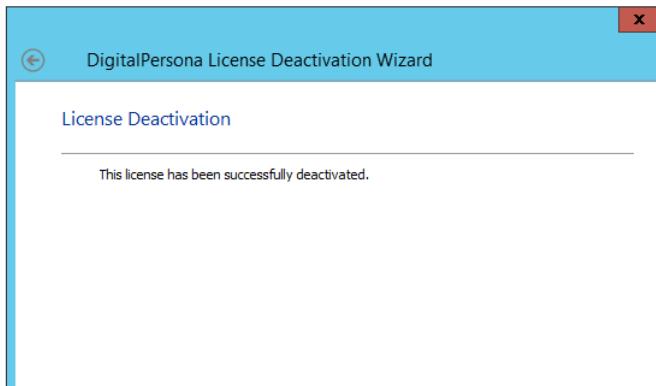


3. In the *License Deactivation Wizard*, click *Next*.

- On the *License Information* page, check to make sure that the License ID identifies the license that you intend to deactivate.



- Once the license has been successfully refreshed, click *Finish* to close the wizard.



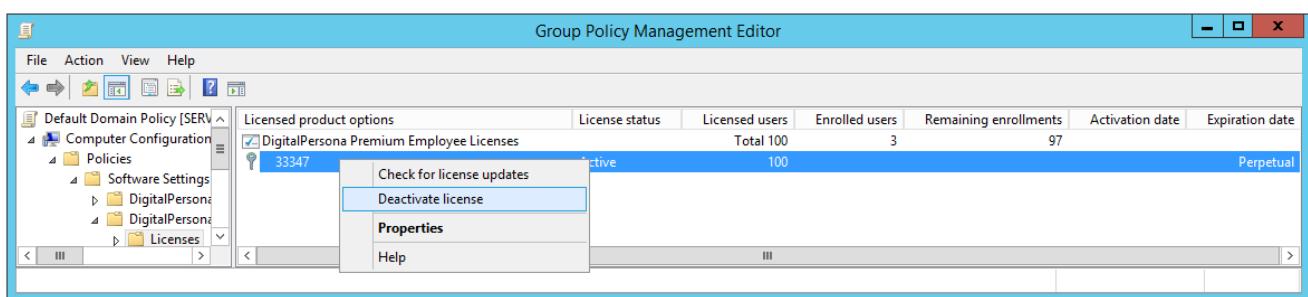
License deactivation from another computer

If your DigitalPersona Server does not have access to the internet, you can deactivate it remotely through the use of any computer that has internet access. *Installation of the Group Management Console and the DigitalPersona Administration Tools are required on the machine.*

To remotely deactivate your DigitalPersona license

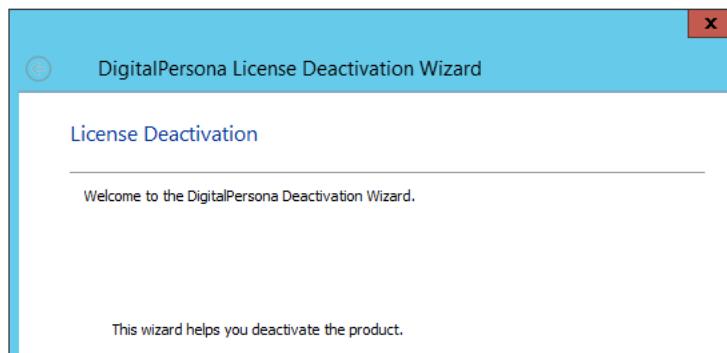
On your DigitalPersona Server,

- In the Group Policy Management Editor, navigate to *Computer Configuration, Policies, Software Settings, DigitalPersona Server, Licenses*.
- Right-click on *Licenses* and select *Deactivate license*.

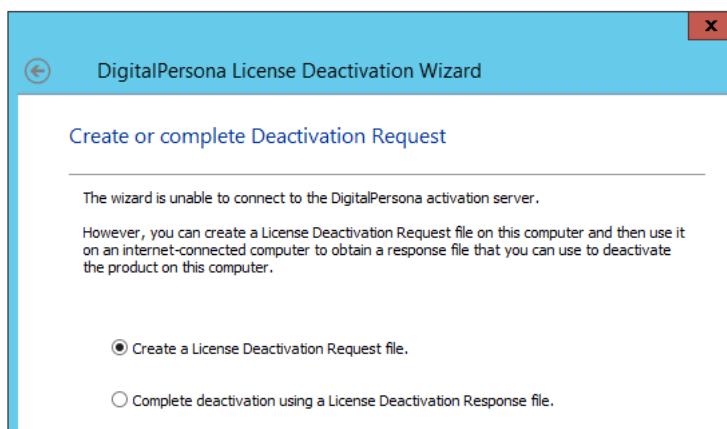


License deactivation from another computer

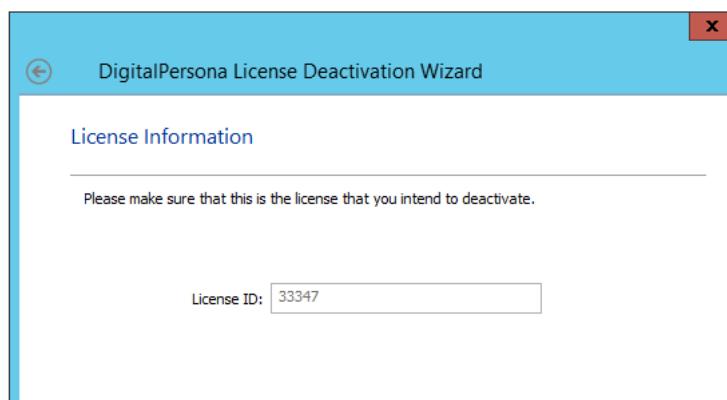
- When the DigitalPersona License Deactivation Wizard displays, click *Next*.



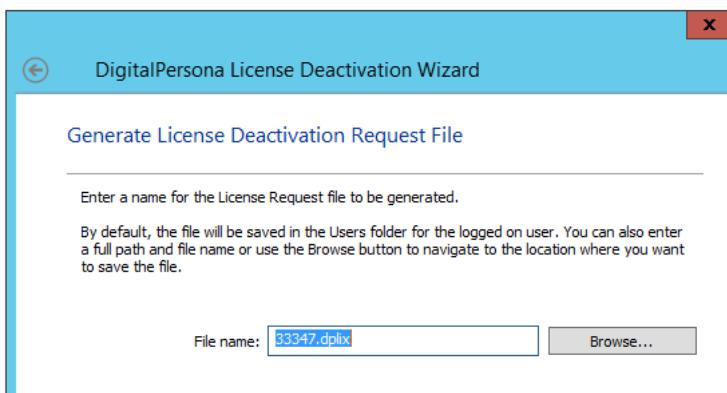
- On the *Create or complete Deactivation Request* page, select *Create a License Deactivation Request file*.



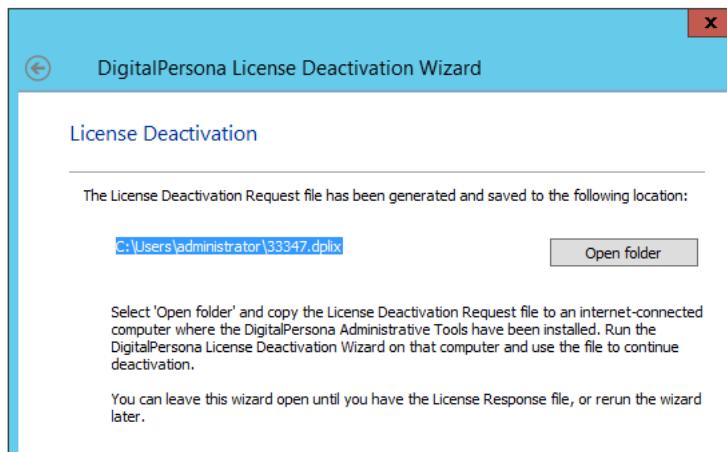
- On the *License Information* page, verify that the License ID identifies the license that you want to deactivate.



- On the *Generate License Deactivation Request File* page, enter a name for the License Request file to be generated.



By default, the file will be saved in the Users folder of the logged on user. You can also enter a full path and file name or use the *Browse* button to navigate to the location where you want to save the file.

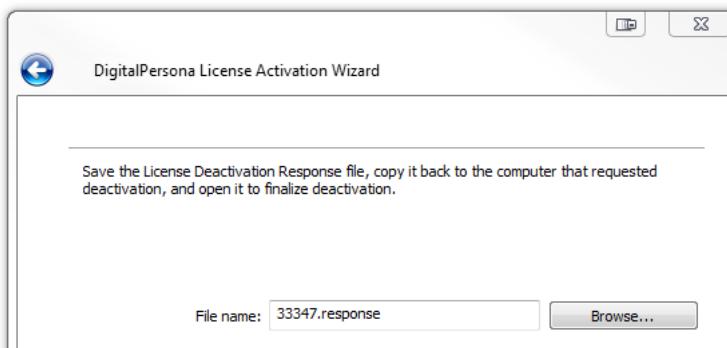


7. Copy the resulting *License Deactivation Request (.dplix) file* to a shared directory or device that can be accessed from a computer with an internet connection and the DigitalPersona Administrative Tools installed.

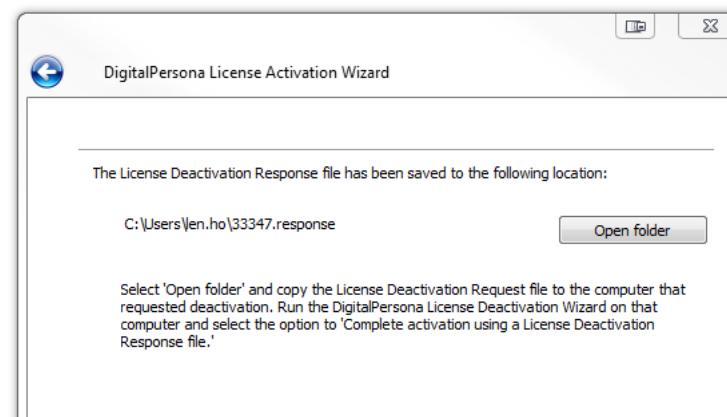
You can leave this wizard open until you have the License Deactivation Response file, or rerun the wizard later.

On an internet-enabled computer

8. Install *DigitalPersona Administrative Tools* (if not previously installed).
9. Navigate to, and double-click, the *License Deactivation Request* file generated in step 6 above.
10. The *DigitalPersona License Deactivation Wizard* will launch. Click *Next*.
11. Enter a name for the file to be generated and click *Next*.

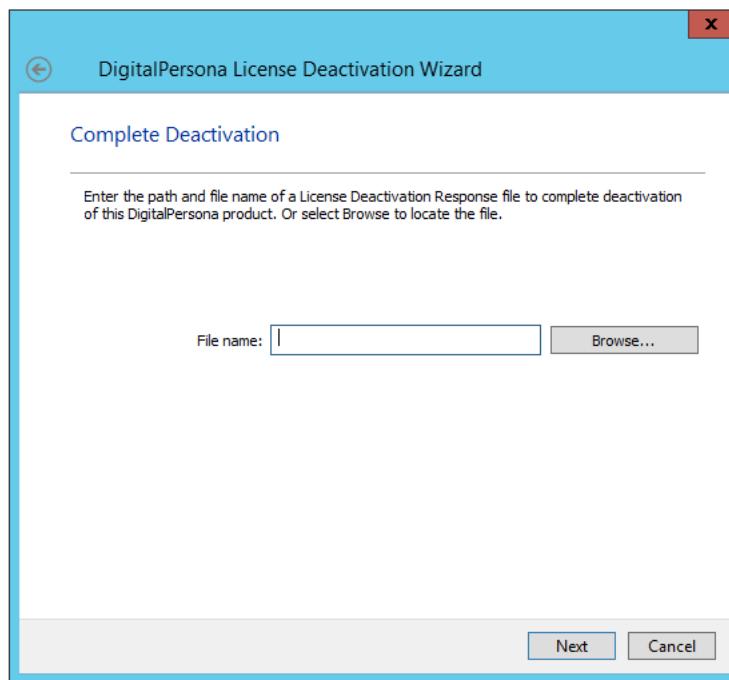


By default, the file will be saved in the Users folder of the logged on user. You can also enter a full path and file name or use the *Browse* button to navigate to the location where you want to save the file.



On the DigitalPersona Server

12. If you have left the wizard open, click *Next*.
13. On the *Complete Deactivation* page, enter the path and file name of the *License Deactivation Response* file to complete deactivation of your DigitalPersona license. Or select *Browse* to locate the file. Then click *Next*.



14. Upon successful deactivation, the final page of the wizard displays. Click *Finish* to close the wizard.

Releasing user licenses

You can release the DigitalPersona license associated with a specific user back to the license pool through the Delete License command in the DigitalPersona ADUC Snap-in. See the *ADUC snap-ins* chapter for further details.

THIS CHAPTER DESCRIBES TWO SNAP-INS TO ADUC (ACTIVE DIRECTORY USERS AND COMPUTERS), THE USERS AND COMPUTERS SNAP-IN AND THE USER QUERY TOOL SNAP-IN.

Main topics in this chapter	Page
Users and Computers snap-in	54
User Query snap-in	56

The ADUC snap-ins described below are part of the DigitalPersona AD Administration Tools component. For installation instructions, see *DigitalPersona AD Administration Tools* on page 29.

Users and Computers snap-in

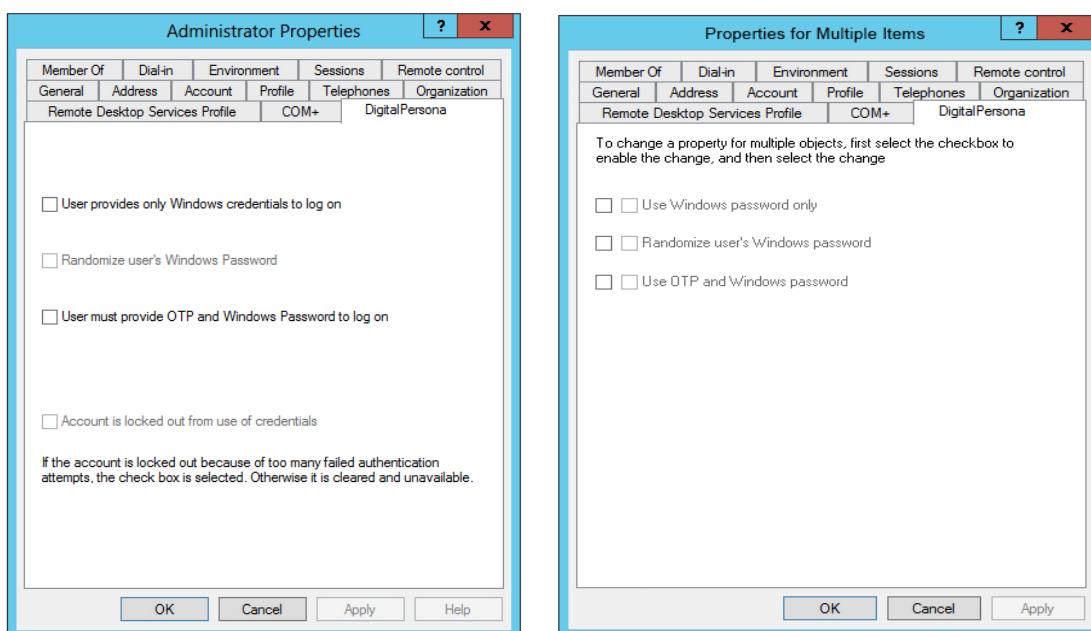
The DigitalPersona Users and Computers snap-in adds a new DigitalPersona tab to the User Properties page enabling additional administrative functions and adds several DigitalPersona commands to the user and computer object context menus. For installation instructions, see page 30.

User properties

DigitalPersona provides the administrator with several Basic user properties that define settings or behaviors that can be applied to a single user, multiple selected users, groups or OUs. These properties are located on the Properties dialog for the selected Active Directory user. Additional user properties are available through a separate product, the Extended Server Policy Module (ESPM) described on page 63. Note that these user properties override any conflicting computer policies.

To access the DigitalPersona Basic user properties:

1. In the Users and Computers console, open the *Users* folder.
2. Right-click on the desired user(s), group(s) or OU, select *Properties* and click the *DigitalPersona* tab.
3. Make any desired changes to the user properties, as listed below. Note that when more than one object (user, group or OU) has been selected, the DigitalPersona tab UI changes slightly as shown below.



4. When making changes to multiple objects, follow the steps below.

- To disable a property setting for multiple users, select the leftmost checkbox for the setting and click *Apply*. Do NOT select the second checkbox.
- To enable a property setting for multiple users, select both checkboxes for the setting and click *Apply*.

Settings

- User provides only Windows credentials to log on

When this option is set, the user will not be subject to any logon policy from DigitalPersona AD. Users will be able to logon with password or smart card as defined by the Windows logon settings. By default this setting is turned off.

- Randomize user's Windows Password

Enable this setting to randomize a user's Windows Password. This will block them from using their Windows Password to verify their identity, and a fingerprint or other authorized and enrolled credential must be used instead.

When this option is set, DigitalPersona AD changes the user password to a random value when you click OK on this dialog box. *This user will no longer be able to access any domain resources unless they have an alternative supported and enrolled credential - even computers where DigitalPersona AD software is not installed.*

Warning - Do not enable password randomization with incompatible logon authentication policies, such as "Fingerprint and Password," as users will be unable to log on or enroll new credentials (since enrollment requires entering their Windows Password). Also, this property should not be used in combination with the Active Directory policy "User must change password on next logon," since users will be unable to change their password, and therefore unable to logon.

This option is not available for accounts with administrative privileges.

- *Account is locked out from use of fingerprint credentials*

If the user account is locked out due to too many failed authentication attempts, this checkbox will be selected. Otherwise it will be unselected. Note that this setting cannot be manually selected, i.e. used by an administrator to *lock* an account.

For instructions on unlocking an account, see below.

Unlocking accounts after failed logon attempts

You can unlock an account that has been locked out of fingerprint authentication due to the user reaching the threshold number for failed authentication attempts. You must have permissions to access the user account. When an account is unlocked by an administrator, the account becomes immediately available for 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 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* tab.
3. Click the *Account is locked out from use of credentials* 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.

User object commands

Installation of DigitalPersona AD adds the following new commands to the context menu for a user in the Active Directory Users and Computers console.

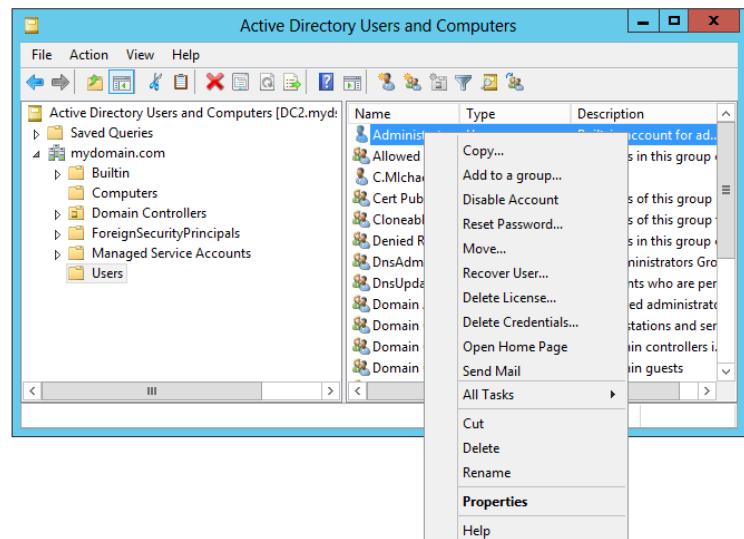
Recover User - Enables recovery of the user's access to their Windows account through a one time access code available through a link on the Windows logon screen.

Delete License - Use this command to release the DigitalPersona license associated with this user back to the license pool.

The use of this command will delete all of the selected user's DigitalPersona credentials and other user data stored in Active Directory.

You should note the following behavior.

- The license will be released within a few minutes after the user logs off from their computer.
- The ability for a user to log on using their Windows password is not affected by deleting the license.
- Due to cached credentials on the client computer, the user will still be able to use their enrolled credentials to log on to the computer after the license is deleted. But the cache will be cleared after the log on with any enrolled credential (except Windows password) and the user will need to re-enroll their credentials in order to continue to use them with the DigitalPersona software.
- The first time a user tries to save a new Password Manager logon after their license has been deleted, they will receive an error, *Data cannot be saved. If this persists, contact your administrator.* The next time they attempt to do so, the message should not appear and the data should be saved successfully.
- After a license has been deleted, a user's first attempt to re-enroll their credentials through the user dashboard, or an administrator's attempt to do so through the Attended Enrollment wizard, may fail. Closing and re-opening the user dashboard or Attended Enrollment wizard should resolve the issue.



Delete Credentials - Use this command to delete specific enrolled credentials for selected users. A dialog displays where you can select the credentials to be deleted. This does not release the associated DigitalPersona user license.

User Query snap-in

The DigitalPersona AD User Query snap-in is a component within the DigitalPersona AD Administration Tools. These tools are a separate installation and are located in the DigitalPersona AD Administration Tools folder of your product package. This tool provides a means for the administrator to query the DigitalPersona AD user database for information about DigitalPersona AD users and to perform certain operations and to set values associated with a selected user.

It has three separate implementations, as described in the following topics.

- ActiveX control (page 56)
- Interactive dialog-based application (page 59)
- Command line utility (page 61)

The User Query Tool must be installed on a computer running a licensed copy of DigitalPersona AD Workstation, and the logged on user must have domain administrator privileges. Once installed, the Interactive dialog-based application can be run from the Start menu by clicking DigitalPersona, User Query Tool.

ActiveX control

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

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

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

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

- Lock user account
- Set user logon policy
- Delete specific authentication credentials
- Delete user Secrets

The DigitalPersona AD User Query Tool ActiveX control provides two interfaces that can be implemented through Visual Basic or Java script.

IDPUserQueryControlInterface

This interface is used to return licensing information and create an instance of the DPUserControl object described in the next section.

```
[object,
uuid(4AC9BCDA-7C6F-4919-A885-D533CBA447DF),
dual,
nonextensible,
helpstring("IDPUserQueryControl Interface: "),
pointer_default(unique)

]

valuesActiveX control
interface IDPUserQueryControl : IDispatch
{
[proptget, id(1), helpstring("Returns number of licenses installed.")]
    HRESULT NumberOfLicensesInstalled([out, retval] LONG* pVal);
[proptget, id(2), helpstring("Returns number of licenses used.")]
    HRESULT NumberOfLicensesUsed([out, retval] LONG* pVal);
[id(3), helpstring("Creates an instance of DPUserControl object based on user
DN.")]
    HRESULT GetUser([in] BSTR UserDN, [out,retval] IDispatch** ppUser);
};
```

IDPUserControl

The IDPUserControl is used to get or set a number of different user properties.

```
[object,
uuid(C6AAB663-EA2A-4195-940F-1C56C5736924),
dual,
nonextensible,
helpstring("IDPUserControl Interface: "),
pointer_default(unique)

]
```

```

interface IDPUserControl : IDispatch{
    [propget, id(1), helpstring("Returns a flag that indicates if the account
        is locked because of intruder detection.")]
    HRESULT IsAccountLocked([out, retval] VARIANT_BOOL* pfIsAccountLocked);
    [propput, id(1), helpstring("Sets a flag that indicates if the account is
        locked because of intruder detection.")]
    HRESULT IsAccountLocked([in] VARIANT_BOOL fIsAccountLocked);
    [propget, id(2), helpstring("Returns a user account control value.")]
    HRESULT AccountControl([out, retval] LONG* pVal);
    [propput, id(2), helpstring("Sets a user account control value.")]
    HRESULT AccountControl([in] LONG newVal);
    [propget, id(3), helpstring("Returns a user logon policy value.")]
    HRESULT LogonPolicy([out, retval] LONG* pVal);
    [propput, id(3), helpstring("Sets a user logon policy value.")]
    HRESULT LogonPolicy([in] LONG newVal);
    [propget, id(4), helpstring("Returns a flag that indicates if the specific
        authentication token is enrolled.")]
    HRESULT IsTokenEnrolled([in] BSTR TokenID, [out] VARIANT_BOOL*
        pfIsTokenEnrolled);
    [propget, id(5), helpstring("Returns a flag that indicates fingerprints
        enrolled mask.")]
    HRESULT FingerprintMask([out, retval] LONG* pVal);
    [propget, id(6), helpstring("Returns user recovery password.")]
    HRESULT RecoveryPassword([in] BSTR EncryptedPassword, [out, retval]
        BSTR* pVal);
    [id(7), helpstring("Deletes specific authentication token credentials.")]
    HRESULT DeleteToken([in] BSTR TokenID);
    [id(8), helpstring("Deletes enrolled fingerprints.")]
    HRESULT DeleteFingerprints(void);
    [id(9), helpstring("Deletes user Secrets.")]
    HRESULT DeleteSecrets(void);
    [id(10), helpstring("Returns date and time of first fingerprint
        enrollment.")]
    HRESULT FingerprintFirstEnrollmentTime([out, retval] DATE* pVal);
    [id(11), helpstring("Returns date and time of last fingerprint
        enrollment.")]
    HRESULT FingerprintLastEnrollmentTime([out, retval] DATE* pVal);
    [propget, id(12), helpstring("Returns a flag that indicates if the specific
        authentication token is enrolled.")]
    HRESULT IsTokenEnrolledEx([in] BSTR TokenID, [in] BSTR Prefix, [out]
        VARIANT_BOOL* pfIsTokenEnrolled);
    [propget, id(13), helpstring("Returns a flag that indicates if license
        taken by this user.")]
    HRESULT IsLicenseTaken([out, retval] VARIANT_BOOL* pfIsLicenseTaken);
    [id(14), helpstring("Clear license by deleting all DigitalPersona data for
        this user.")]
    HRESULT ClearLicense(void);
};


```

Sample VB Script

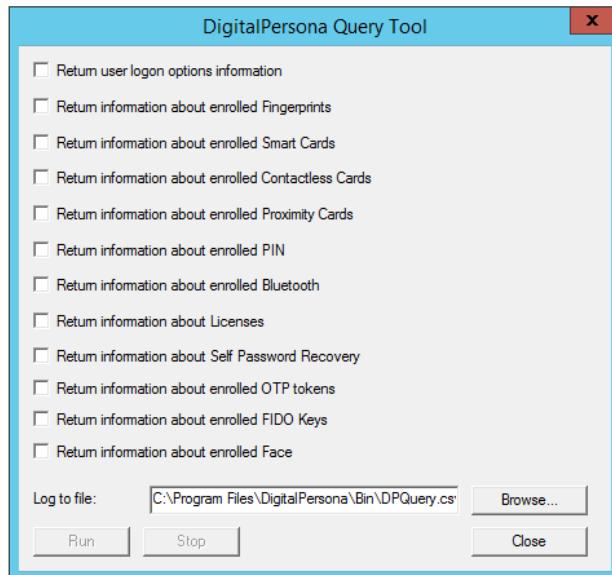
This is a sample of a VB script that returns the date and time of the first and last fingerprint enrollments for a user.

```
Dim objUser
Set objQueryControl = CreateObject("DPUserQuery.DPUserQueryControl")
Set objUser = objQueryControl.GetUser("cn=testuser,CN=Users,DC=testdomain,DC=COM")
wscript.echo objUser.FingerprintFirstEnrollmentTime
wscript.echo objUser.FingerprintLastEnrollmentTime
```

Interactive dialog-based application

To run the interactive dialog-based application:

1. From the *Start* menu, select *All Programs*, *DigitalPersona*, *User Query Tool*.
2. In the application dialog that displays, select the type of information you would like to display.
3. Optionally, *Browse* to the location where you want to save the resulting log file.
4. Click the *Run* button.
5. The file is saved as a .csv file with the default name of DPQuery.csv, which can be opened in Notepad or programs like Microsoft Excel and other spreadsheet programs.



DPQuery.csv format

The file resulting from the use of either the Interactive User Query Tool described above, or the command line interface User Query Tool is illustrated below and described more fully in the table that follows.

DPQuery.csv - Notepad	
File	Edit
User Name,Display Name,User Type,Logon Options,Fingerprints,Smart Cards,Contactless Cards,Proximity Cards,Bluetooth,PIN,Licenses,Self Password Recovery,OTP,FIDO Key,Face	
"Administrator","Administrator","DigitalPersona AD User",0,1,NO,NO,NO,NO,YES,YES,NO,NO,NO,NO	
"Guest","Guest","DigitalPersona AD User",0,N/A,N/A,N/A,N/A,N/A,NO,NO,N/A,N/A,N/A	
"mikelyc","mikelyc","DigitalPersona AD User",0,1,NO,NO,NO,NO,YES,YES,NO,NO,NO,NO	
"krbtgt","krbtgt","DigitalPersona AD User",0,N/A,N/A,N/A,N/A,N/A,NO,NO,N/A,N/A,N/A	
"jon.doe","Jon Doe","DigitalPersona AD User",0,0,NO,NO,NO,NO,NO,NO,NO,NO,NO,NO,NO	
"DP_ACCESS","DP_ACCESS","DigitalPersona AD User",0,0,NO,NO,NO,NO,NO,NO,NO,NO,NO,NO,NO	
"John.Doe","John A. Doe","DigitalPersona AD User",0,0,NO,NO,NO,NO,YES,YES,NO,NO,NO,NO	
Total number of users - 7.	
Total number of licenses used - 3.	
Total number of Employee licenses used - 3.	
Total number of Customer Facing licenses used - 0.	
LicenseID,ProductID,Status,Activation Date,Expiration Date,Licensed Users	
33347,5656,0,N/A,NO,100	
Total number of users with fingerprints enrolled - 2.	
Total number of users with smart cards enrolled - 0.	
Total number of users with contactless cards enrolled - 0.	
Total number of users with proximity cards enrolled - 0.	
Total number of users with Bluetooth enrolled - 0.	
Total number of users with PIN enrolled - 3.	
Total number of users with Self password Recovery enrolled - 0.	
Total number of users with OTP enrolled - 0.	
Total number of users with FIDO Keys enrolled - 0.	
Total number of users with Face enrolled - 0.	

Column	Description
User Name	Name of the user being reported against.
Display Name	Display Name of the user being reported against.
User Type	Type of user, i.e. Administrator or DigitalPersona AD User.
Logon Options	0 - No logon option is set. 1 - User provides only Windows credentials to log on. 2 - Randomize user's Windows Password. 4 - User must provide Fingerprint and PIN to log on. 8. - Account is locked out from use of fingerprints credentials.
Fingerprints	Number of fingerprints enrolled by the user.
Smart Cards	YES or NO. Indicates whether this credential has been enrolled by the specified user.
Contactless Cards	YES or NO. Indicates whether this credential has been enrolled by the specified user.
Proximity Cards	YES or NO. Indicates whether this credential has been enrolled by the specified user.
Bluetooth	YES or NO. Indicates whether this credential has been enrolled by the specified user.
PIN	YES or NO. Indicates whether this credential has been enrolled by the specified user.
Licenses	YES or NO. Indicates whether a DigitalPersona User license is being utilized by the specified user.
Self Password Recovery	YES or NO. Indicates whether the Self Password Recovery questions have been answered by the specified user.
OTP	YES or NO. Indicates whether this credential has been enrolled by the specified user.
FIDO Key	YES or NO. Indicates whether this credential has been enrolled by the specified user.
Face	YES or NO. Indicates whether this credential has been enrolled by the specified user.

Additionally, the following totals are provided at the end of the file.

Total number of users

Total number of Employee licenses used

Total number of Customer Facing licenses used

License ID, Product ID, Status, Activation Date, Expiration Date, Licensed Users

Total number of users with fingerprints enrolled

Total number of users with smart cards enrolled
 Total number of users with contactless cards enrolled
 Total number of users with proximity cards enrolled
 Total number of users with Bluetooth enrolled
 Total number of users with PIN enrolled
 Total number of users with Self Password Recovery enrolled
 Total number of users with OTP enrolled
 Total number of users with FIDO Keys enrolled
 Total number of users with Face enrolled

Command line utility

The User Query Tool command line utility must be run from an elevated command prompt.

To run the User Query Tool command line utility

1. Open an elevated command prompt by right-clicking any Command Prompt shortcut on the Windows Start menu (located by default in the Accessories folder) and selecting *Run as administrator*.
2. In the Command Prompt window, enter *DPQuery.exe* using the following syntax and parameters.

Syntax

```
DPQuery.exe [-noui] [-dn="BaseDN"] [-out="FileName"] [-ac] [-fp] [-sc] [-cc] [-pc]
[-bt] [-pin] [-lic] [-rec]
```

Parameters

Parameter	Description
-noui	Run utility silently with no graphical interface, writing results to the DPQuery.csv file in the [Installation path]Bin folder, where the default location would be “C:\Program Files\DigitalPersona\Bin.” If -noui is not used, the UI shown on page 59 displays.
-dn=“BaseDN”	Sets the Distinguished Name of the search base for the query. If missing, the DN of the domain name that the computer belongs to will be used as the search base.
-out=”FileName”	Identifies the path and file name for the output log file. If missing, the file DPQuery.csv will be created in the directory containing the utility.
-fp	Add information about the number of fingerprints enrolled for each user in a query.
-ac	Add information about user account control flags like password randomization.
-sc	Add information about smart cards enrolled for each user in a query.
-cc	Add information about contactless cards enrolled for each user in a query.
-pc	Add information about proximity cards enrolled for each user in a query.
-bt	Add information about Bluetooth credentials enrolled for each user in a query.
-pin	Add information about PINs enrolled for each user in a query.
-lic	Add information about licenses utilized for each user in a query.

Parameter	Description
-rec	Add information about Self Recovery Password enrolled for each user in a query.
-otp	Add information about OTP credentials enrolled for each user in a query.
-utf	Add information about FIDO Key credentials enrolled for each user in a query.
-face	Add information about Face credentials enrolled for each user in a query.

Examples

Return license information on all users

```
DPQuery.exe -noui -dn="CN=Users, DN=DigitalPersona, DN=com" -lic
```

The example query below returns information about users in the Users OU of the DigitalPersona domain, and includes account control flags (defined above) and information about enrolled fingerprints.

```
DPQuery.exe -noui -dn="CN=Users, DN=DigitalPersona, DN=com" -ac -fp
```

The example query below returns information about users in the Users OU of the DigitalPersona domain, and includes information about enrolled smart cards, contactless cards and One-Time Password credentials.

```
DPQuery.exe -noui -dn="CN=Users, DN=DigitalPersona, DN=com" -sc -cc -pc -otp
```

Extended Server Policy Module

8

THIS CHAPTER DESCRIBES THE DIGITALPERSONA AD EXTENDED SERVER POLICY MODULE, AN OPTIONAL COMPONENT AVAILABLE FOR YOUR DIGITALPERSONA LDS SERVER.

The DigitalPersona AD Extended Server Policy Module (ESPM) is a separately purchased and installed server module that adds additional per user policies configurable through the *DigitalPersona Users and Computers snap-in*, part of the *DigitalPersona AD Administration Tools* component.

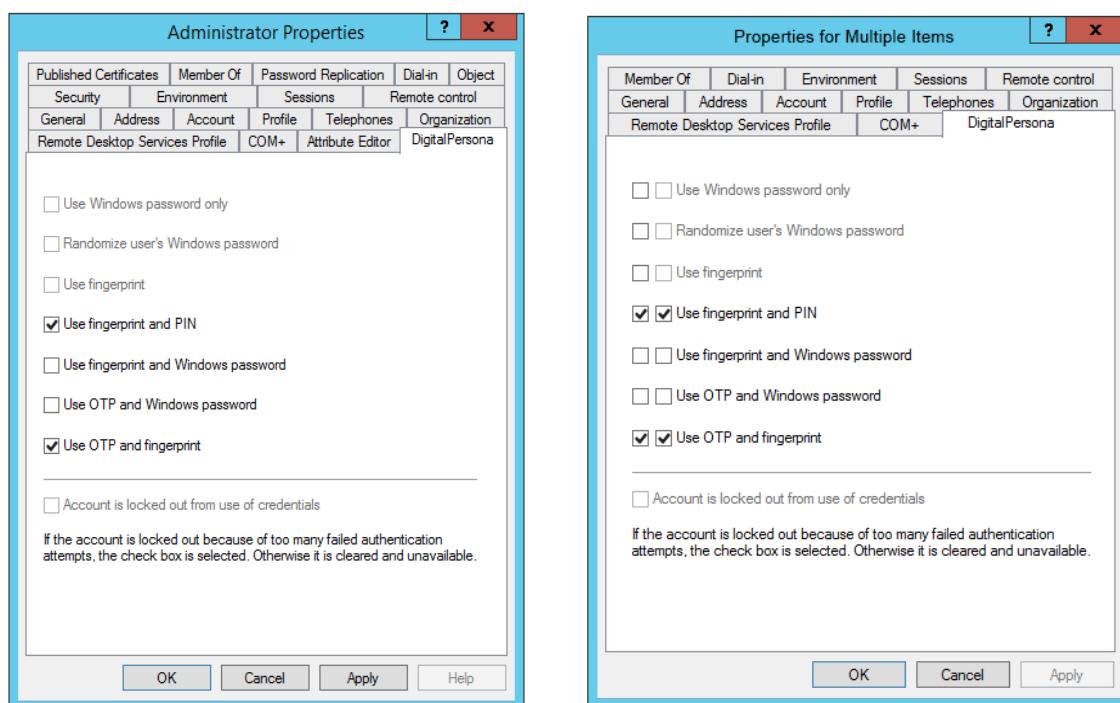
This module requires the previous installation of the *DigitalPersona Users and Computers snap-in*, part of the *DigitalPersona AD Administration Tools* component.

This module provides additional user policies that may be used to manage the credential combinations used for Windows logon. They do not affect the use of DigitalPersona credentials for authentication when used with personal or managed logons to websites, applications and network resources, but only log on to Windows.

Without the ESPM, the following user policies are available for DigitalPersona users.

- Use Windows password only
- Randomize user's Windows password
- Use OTP and Windows password

Installation of the ESPM adds the following additional user policy settings to the *User Properties* dialog. Note that when more than one object (user, group or OU) has been selected, the DigitalPersona tab UI changes slightly as shown below.



When making changes to multiple objects, follow the steps below.

- To disable a property setting for multiple users, select the leftmost checkbox for the setting and click *Apply*. Do NOT select the second checkbox.
- To enable a property setting for multiple users, select both checkboxes for the setting and click *Apply*.

Settings

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

- Use fingerprint and PIN
- The user must provide a PIN whenever a fingerprint is used to log on, to unlock the computer or to change their Windows password. The fingerprint PIN option adds another level of security to logging on with a fingerprint.
- Use fingerprint and Windows Password
- The user must verify their identity with their fingerprint credential in addition to Windows authentication (a smart card or password according to the Windows policy setting).
- Use OTP and fingerprint
- The user must verify their identity with their fingerprint credential in addition to using the OTP credential.

Note that some user policies (such as ‘Use Windows password only’ and ‘Use fingerprint’) will cause conflicting policies to be greyed out and unavailable to select. Those policies defining credential combinations, such as ‘Use fingerprint and PIN’ and ‘Use OTP and fingerprint’ will allow the user to authenticate with any credential combination that is selected, i.e. creates an OR policy.

•

THIS CHAPTER DESCRIBES DIGITALPERSONA EXTENSIONS TO THE MICROSOFT GROUP POLICY MANAGEMENT CONSOLE AND GROUP POLICY MANAGEMENT EDITOR.

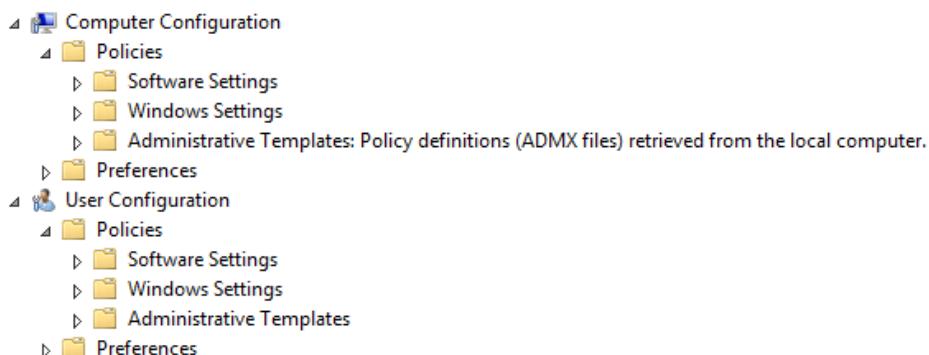
Main topics in this chapter	Page
Group Policy Object Extensions	66
Administrative Templates	67
Implementation Guidelines	70
Installing Administrative Templates Locally	71

Overview

DigitalPersona creates a number of extensions that are visible in the Group Policy Management Console (read-only) and the Group Policy Management Editor. This chapter describes these extensions from the viewpoint of the GPO Editor, since that is where they can be enabled and configured or disabled.

There are three child nodes under the Computer Configuration and User Configuration parent nodes in the Group Policy Object Editor namespace.

- Software Settings
- Windows Settings
- Administrative Templates



DigitalPersona settings are located in the Software Settings and Administrative Templates nodes.

- The *Software Settings* node contains extension snap-ins that extend the Computer Configuration node and the User Configuration node.
- The *Administrative Templates* node contains registry-based policy settings, and are extended by using administrative template (.adm/.admx) files.

These DigitalPersona policies and settings are described in detail in the chapter, [Policies and Settings](#).

The Group Policy Object Extensions and the Administrative Templates are installed automatically as part of the DigitalPersona AD Administrative Tools.

Adding an administrative template to a container applies the DigitalPersona policies and settings to the computers and users in that container. For instructions on installing the Client Administrative Template locally, see the topic [Installing Administrative Templates Locally](#) on page 71.

Additional extensions or templates may be provided as new components are released, and will be specified in the Readme.txt file for each component.

Group Policy Object Extensions

DigitalPersona uses the following Group Policy Object Extensions under the *Software Settings* node. They are installed automatically as part of the DigitalPersona Administrative Tools.

DigitalPersona Client

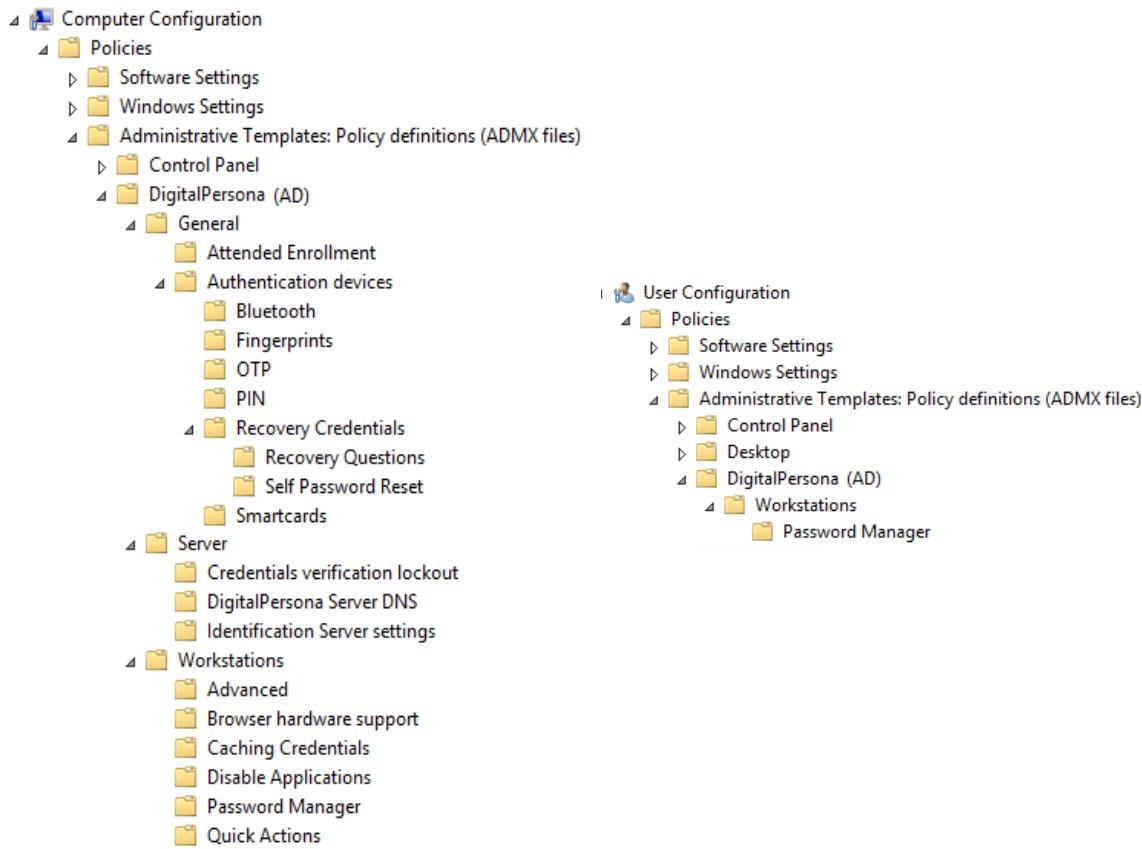
Security		
Authentication	Logon Authentication Policy	
	Enhanced Logon Authentication Policy	
	Session Authentication Policy	
	Kiosk Session Authentication Policy	
	Enrollment Policy	
	SMS Configuration	
SMTP	SMTP Configuration	
Kiosk Administration		
	Allow automatic logon using Shared Kiosk Account	
	Logon/Unlock with Shared Account Credentials	
	Prevent users from logging on outside of a Kiosk session	
	Kiosk Workstation Shared Account Settings	
	Kiosk Unlock Script	

DigitalPersona Server

Node	Setting
Licenses	None (Used for license management)

Administrative Templates

DigitalPersona uses the following Administrative Templates installed under the *Computer Configuration/Policies/Administrative Templates* node. They are installed automatically as part of the DigitalPersona AD Administrative Tools.



Note that when installing Administrative Templates, corresponding .adml (language) files for each template need to be located in the language subfolder where the template is stored.

DPCA_AD_Root.admx	Creates a root-level folder and categories for all DigitalPersona products, and if not already present, is installed automatically with any DigitalPersona product.
DPCA_AD_General.admx	Creates these settings under the following node: Computer Configuration/Policies/Administrative Templates/ DigitalPersona
	Attended Enrollment
	Authentication of the user being enrolled
	Security officer authentication
	Require to complete or omit credential
	Authentication devices
	Bluetooth

Fingerprints		
OTP		
PIN		
Recovery Credentials		
	Recovery Questions	
	Self Password Reset	
	Allow users to reset their Windows passwords	
	Path to DigitalPersona Secure Token Server (STS)	
	Smartcards	
	Lock the computer upon smart card removal	
	Event logging	
	Level of detail in event logs	
DPCA_AD_DesktopApps.admx	Creates these settings under the following node: Computer Configuration/Policies/Administrative Templates/ DigitalPersona	
	Workstations	
	Advanced	
	Do not launch the Getting Started wizard upon logon	
	Identification Server domain	
	Compatibility with Microsoft Fingerprint support	
	Allow DigitalPersona client to use DigitalPersona Server	
	Show Taskbar icon	
	Allow VPN-less access	
	Browser hardware support	
	Allow Localhost Loopback	
	Localhost Loopback Origins	
	Caching Credentials	
	Cache user data on local computer	
	Maximum size of identification list	
	Disable Applications	
	Prevent Password Manager from running	
	Quick Actions	
	Credential	

		Ctrl+Credential
		Shift+Credential
DPCA_AD_PasswordManager.admx	Creates these settings under the following node: Computer Configuration/Policies/Administrative Templates/DigitalPersona/Workstations	
	Display password complexity popup	
	Creates these settings under the following node: User Configuration/Policies/Administrative Templates/DigitalPersona/Workstations	
	Allow creation of personal logons	
	Managed logons	
DPCA_AD_OneTouchLock.admx	Creates these settings under the following node: Computer Configuration/Policies/Administrative Templates/DigitalPersona/Workstations	
	One Touch Lock	
	Note that when installed by itself, the setting does not show up under Administrative Templates, but can be accessed from the <i>All Settings</i> node under Administrative Templates.	
DPCA_AD_Servers.admx	Creates these settings under the following node: User Configuration/Policies/Administrative Templates/DigitalPersona/Server	
	Credentials verification lockout	
		Allow users to unlock their Windows account using DigitalPersona Recovery Questions
		Account lockout duration
		Reset account lockout counter after
		Account lockout threshold
	DigitalPersona Server DNS	
		Automated site coverage by DigitalPersona Server Locator DNS SRV records
		Refresh interval of DigitalPersona Server DNS records
		Sites covered by DigitalPersona Server Locator DNS SRV records
		Priority set in DigitalPersona Server Locator DNS SRV records
		Weight set in DigitalPersona Server Locator DNS SRV records
		Register DigitalPersona Server Locator DNS SRV records for domain

		Dynamic registration of DigitalPersona Server Locator DNS SRV records
DPCA_AD_IDServer.admx		Creates these settings under the following node: User Configuration/Policies/Administrative Templates/DigitalPersona/Server
		Identification Server settings
		Perform fingerprint identification on server
		Restrict identification to a specific list of users

Implementation Guidelines

Before you add any Administrative Templates to your GPOs, give some thought to your Active Directory structure, where GPOs are placed, and which GPOs the Administrative Templates should be added to.

Policy configuration needs will vary from network to network and specific policy recommendations are beyond the scope of this guide. You may want to refer to Microsoft's documentation on Group Policy Object configuration for more information.

Organizational Units and GPOs

Although the use and configuration of organizational units and GPOs varies widely among corporations, we have provided some general guidelines for structuring Active Directory organizational units.

- There are two key factors in deciding how to structure your network:
 - How you group your users and computers, and
 - Where the DigitalPersona AD GPOs are set.

For example, if users and computers are to be grouped according to authentication policies, you should group them into separate OUs (Organizational Units) and then set specific GPOs for each OU.

- However, when authentication policies within organizational units vary, as they often do among department heads and subordinates, then you should group your users and/or computers into child organization units reflecting the necessary authentication needs.

Structuring your organizational units based on authentication policies is the easiest way to administer DigitalPersona.

1. Plan your network structure by identifying the settings you intend to configure.
2. Determine whether to apply the settings to all users and computers in a site or domain, or just to the users and computers in an organizational unit.
3. Create the organizational units required to implement your design.
4. Add the respective users and computers to the organizational units.

GPO behavior

Here are a few guidelines to keep in mind when configuring DigitalPersona GPOs.

- If a GPO setting is not configured, the default value set in the software is used.
- If a superior (higher-level) GPO has a value for a setting and a subordinate GPO has a conflicting value for that setting, the setting in the subordinate is used.

- If a GPO has a value for a setting and a subordinate (lower-level) container has the GPO setting with no value, the setting in the superior (high-level) GPO is used.
- GPOs can only be applied to the three Active Directory containers: sites, domains and organizational units; not to 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.

The DigitalPersona GPO settings apply only to computers with DigitalPersona software installed on them. In very basic Active Directory deployments, one can simply make a specific DigitalPersona GPO, linked at the domain, and set the DigitalPersona Server and DigitalPersona Workstation settings here for all users and computers alike.

Installing Administrative Templates Locally

For local administration of a DigitalPersona AD Workstation or Kiosk, the following Administrative Templates can be added to the local policy object of any computer running the client by using the Microsoft Management Console (MMC) Group Policy Editor.

- DPCA_AD_General.admx
- DPCA_AD/DesktopApps.admx
- DPCA_AD_PasswordManager.admx
- DPCA_AD_OneTouchLock.admx

To add the Administrative Templates locally

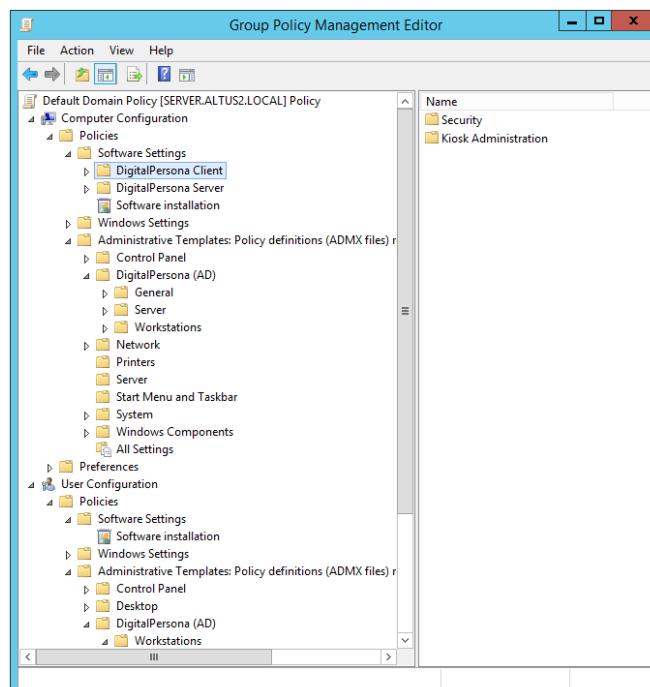
1. On the Start menu, click *Run*. Type `gpedit.msc` and press *Enter* to launch the Group Policy Editor.
2. Right-click the Administrative Templates folder and select *Add/Remove Templates* on the Administrative Templates folder shortcut menu.
3. Click the *Add* button on the Add/Remove Templates dialog box and then locate and select the desired Administrative Templates from the default administrative templates directory.
4. Click *Close*.

THIS CHAPTER DESCRIBES THE POLICIES AND SETTINGS AVAILABLE THROUGH ACTIVE DIRECTORY TO MANAGE THE BEHAVIOR OF THE DIGITALPERSONA SERVER AND CLIENTS.

Main topics in this chapter	Page
Computer Configuration\Policies\Software Settings	73
DigitalPersona Client	73
DigitalPersona Server	78
Computer Configuration\Policies\Administrative Templates	79
DigitalPersona AD)	79
General	79
Server	86
Workstations	90
User Configuration\Policies\Administrative Templates	93
DigitalPersona	93
Workstations	93

Overview

DigitalPersona provides a comprehensive set of Active Directory-based policies and settings used for licensing, configuring and administering the DigitalPersona AD Server and its clients. These policies and settings are implemented through DigitalPersona AD GPMC extensions and the User Query Tool. They are available as separate components installed through the DigitalPersona AD Administration Tools, which is included in your product package. See page 88 for a description of the GPMC Extensions and page 81 for information about the User Query Tool.



Note that the structure shown above and described in this chapter is from Windows Server 2012. Minor variations in the structure framework may exist in other versions of Windows Server, and in previous versions of this software.

The Workstation administrative template, installed through the GPMC Extensions component, may also be added to a local policy object on a standalone workstation without access to Active Directory. See the *DigitalPersona Workstation Installation* chapter in the DigitalPersona Client Guide for further details.

In Active Directory, the DigitalPersona AD GPMC Extensions component adds DigitalPersona policies and settings to the *DigitalPersona Client* and *DigitalPersona Server* nodes under Computer Configuration/Policies/Software Settings, and adds additional policies and settings for the DigitalPersona Client under the Computer Configuration/Policies/Administrative Templates, and User Configuration/Policies/Administrative Templates nodes.

Installed computer policies and settings can then be accessed through the Active Directory Group Policy Management Editor.

Local administrators can access the DigitalPersona AD Workstation settings from the Microsoft Management Console (MMC), after installing the GPMC Extensions component of the DigitalPersona AD Administration Tools, which contains the required administrative templates.

Each setting can be accessed in the Group Policy Management Editor (or MMC) by navigating to the desired setting and selecting Edit from the context menu.

GPO settings have three states: enabled, disabled and not configured.

By default, all settings are **not** configured. To override the default settings of DigitalPersona AD, each setting must be changed to enabled or disabled and, in some cases, additional parameters must be supplied.

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 AD GPOs without concern for disrupting DigitalPersona AD functionality on a computer.

The following pages describe the policies and settings made available in Active Directory through the DigitalPersona GPMC Extensions component. The information is organized according to major Active Directory nodes, categories and subcategories mirroring their locations in the GPME policy tree. Summary tables list each policy and setting, and reference the page number where a full description is provided.

Computer Configuration\Policies\Software Settings

During installation of the DigitalPersona AD Administration Tools, the following nodes are created under the Computer Configuration\Policies\Software Settings node.

DigitalPersona Client (Summary)

These settings can be found at the following location:

Computer Configuration\Policies\Software Settings\DigitalPersona Client.

They are used to configure and govern DigitalPersona clients.

Category	Subcategory	Setting	Page
Security	Authentication	Logon Authentication Policy	74
		Enhanced Logon Authentication Policy	75

Category	Subcategory	Setting	Page
		Session Authentication Policy	76
		Kiosk Session Authentication Policy	76
Enrollment		Enrollment Policy	77
SMS		SMS Configuration	77
SMTP		SMTP Configuration	77
Kiosk Administration			
		Allow automatic logon using Shared Kiosk Account	78
		Logon/Unlock with Shared Account Credentials	78
		Prevent users from logging on outside of a Kiosk session	78
		Kiosk Workstation Shared Account Settings	78
		Kiosk Unlock Script	78

DigitalPersona Client (Detail)

These settings can be found at the following location:

Computer Configuration\Policies\Software Settings\DigitalPersona Client.

They are used to configure and govern DigitalPersona clients.

Security\Authentication

Logon Authentication Policy

The Logon Authentication Policy defines the credentials and/or credential combinations needed for authentication and logon to Windows. By default, all supported credentials are listed on the tab.

- If enabled, only the specified credentials, in the specified combinations, can be used for authentication.
- If disabled or not configured, any Primary credential can be used for authentication.

Primary and Secondary credentials

For the purposes of Logon authentication, DigitalPersona credentials are defined as *Primary* and *Secondary* credentials. Primary credentials are considered stronger (more secure) than Secondary credentials, and include the following:

- Password
- Fingerprint
- Smart cards
- Contactless card
- One-Time Password
- Face (Requires a separate Face Authentication License. Not supported in web-based components.)
- FIDO Key

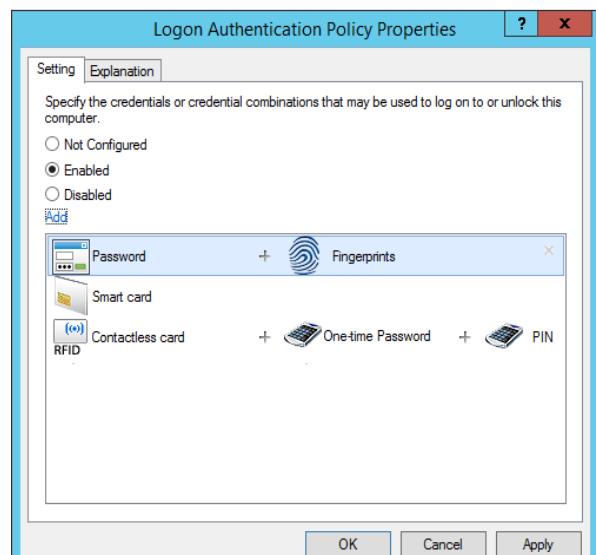
Secondary credentials can only be used in combination with a Primary credential. They are:

- Proximity card
- PIN
- Bluetooth device

When selecting credentials to be used for the Logon Authentication Policy, the first credential must be a Primary credential. Additional (optional) credentials may be either Primary or Secondary credentials.

To add a credential or credential combination to the list

- Enable the policy.
- Click the *Add* link just below the configuration buttons.
- Click *Apply*.



To edit a credential or credential combination

- Click the credential or credential combination and edit it using the dropdown lists provided.
- Click *Apply*.

To delete a credential or credential combination

- Click on the X that appears to the right of the item when hovering over it with your mouse.
- Click *Apply*.

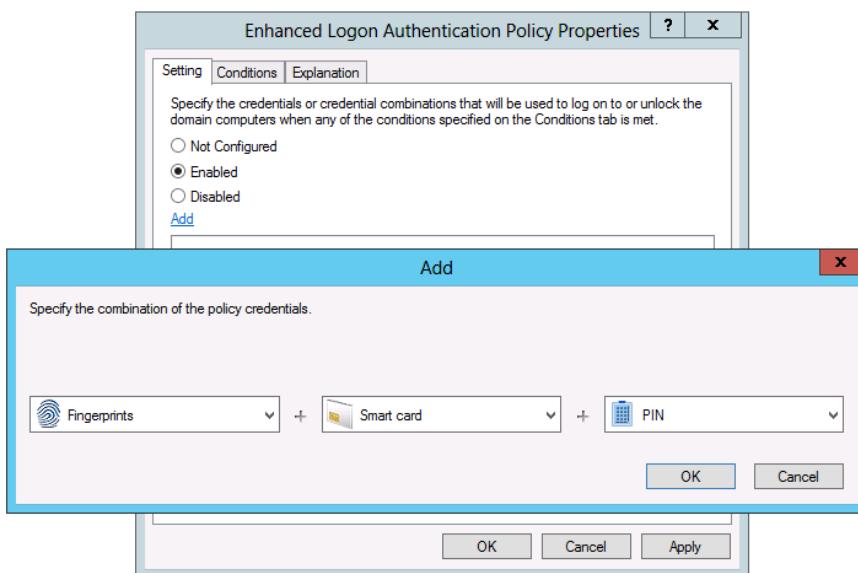
Enhanced Logon Authentication Policy

The Enhanced Logon Authentication Policy specifies the credentials or credential combinations that will be used to log on to or unlock domain computers when any of the conditions specified on the Conditions tab are met. Note that this policy has no effect on DigitalPersona Kiosk clients.

- If enabled, and credentials are defined by clicking the *Add* button; then whenever the conditions selected on the Conditions tab are met, logon authentication will require the credentials or credential combinations specified in this policy. Note that when the specified conditions are met, this policy replaces the *Logon Authentication Policy* in force.
- If disabled or not configured, the standard *Logon Authentication Policy* remains in force.

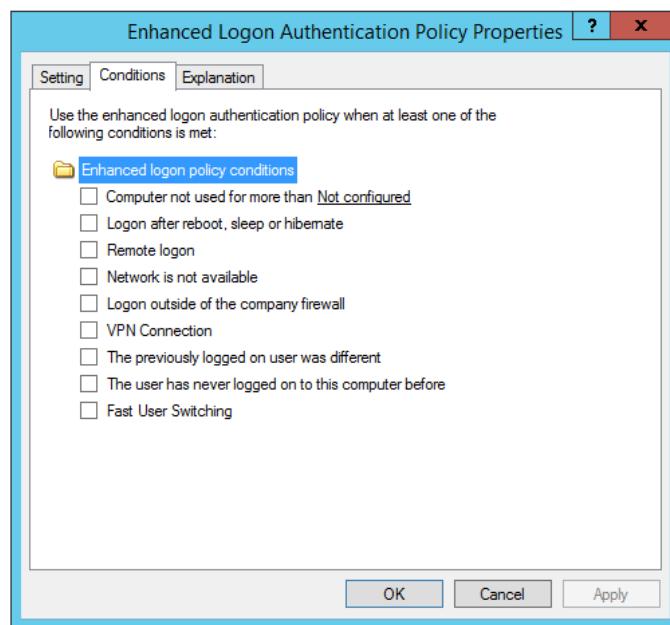
To configure the Enhanced Logon Authentication Policy

1. Select *Enabled* and click the *Add* link in order to specify the required credential(s). See the previous topic *Primary and Secondary credentials* for details on permitted credential combinations.



Note that the Face credential requires a separate Face Authentication License and is not supported in web-based components.

2. Specify any conditions that must be met for this policy to be applied.



Session Authentication Policy

The Session Authentication Policy defines the credentials needed to access Security applications during a Windows session. By default, all supported credentials are listed on the tab. See the previous topic *Primary and Secondary credentials on page 74* for details on permitted credential combinations.

Note that the Face credential requires a separate Face Authentication License and is not supported in web-based components.

- If enabled, only the specified combination of credentials in the Policy can be used for authentication.
- If disabled, the user is not prompted to authenticate by DigitalPersona security applications during the Windows session. This configuration provides Single Sign-on functionality. The user logs on to Windows, and gains access to all security applications without being prompted to authenticate for each application.
- If not configured, credentials will be controlled by local GPOs. However, credential enrollment will still require authentication.

To edit or delete a credential from the list

- Click the arrow that appears to the right of the credential.

To add a credential to the list

- Click *Add* at the top of the list.

Kiosk Session Authentication Policy

The Kiosk Session Authentication Policy defines the credentials that may be used to access Security applications during a DigitalPersona Kiosk session.

By default, all supported credentials are listed on the tab. Note that the Face credential requires a separate Face Authentication License and is not supported in web-based components.

See the previous topic *Primary and Secondary credentials on page 74* for details on permitted credential combinations.

- If enabled, only the specified combination of credentials in the Policy can be used for authentication.
- If disabled or not configured, credentials will be controlled by local GPOs.

To edit or delete a credential from the list

- Click the arrow that appears to the right of the credential.

To add a credential to the list

- Click *Add* at the top of the list.

Security\Enrollment

Enrollment Policy

The Enrollment Policy specifies the credentials that may be used for enrollment in the User Console, Attended Enrollment and Web Enrollment applications. By default, all supported credentials are initially listed on this tab.

- If enabled, only the specified credentials may be enrolled and only those credentials' tiles are displayed in the UI.
- If disabled or not configured, any installed and supported credentials may be used, except for Face.

To use the Face credential, the policy must be enabled and the Face credential selected. All other credentials that you want to be available for enrollment must also be selected.

Note that the Face credential requires a separate Face Authentication License and is not supported in web-based components.

Security\SMS

SMS Configuration

SMS Configuration specifies the API values and Sender Addresses assigned by the Nexmo Gateway and is required for operation of DigitalPersona's OTP via SMS credential. A previously created Nexmo account is required.

- If enabled, and valid values are entered in the fields provided, SMS authentication will be shown on the logon screen. The API Key assigned by Nexmo is required.
- If disabled or not configured, SMS authentication is not shown on the logon screen.

Nexmo API Key

Enter the API Key assigned by Nexmo.

Nexmo API Secret

Enter the API Secret assigned by Nexmo.

Nexmo Sender Addresses

Enter one or more semicolon-delimited alphanumeric strings to be used as Sender Addresses (also called SenderID) by the Nexmo SMS Gateway. There are country specific limitations for sender addresses; for example, alphabetic characters are not allowed in the United States. Country specific restrictions are described here:

<https://help.nexmo.com/hc/en-us/sections/200622473-Country-Specific-Features-and-Restrictions>.

- If more than one Sender Address is specified, the SMS will be sent with a Sender Address selected randomly from the list.
- If no Sender Address is specified, a default Sender Address of 'NXSMS' will be used.

Security\SMTP

SMTP Configuration

Specify the SMTP server parameters for an account to be used by the password reset and OTP through email features for sending email to the user. Note that these features are separately enabled through the additional GPO settings *Allow sending OTP through email* and *Allow users to reset their Windows passwords*.

When enabled, the following fields are mandatory:

SMTP Server - Hostname only supported

Email Address - Used to login to SMTP Server

Email Password - Used to login to SMTP Server

To validate the SMTP server parameters entered, enter an *Incoming Email Address* and click *Test Settings*. A test email will be sent to the specified address.

- If enabled and valid SMTP parameters are entered, the specified SMTP server will be used.
- If disabled or not configured, password reset and OTP through email features will not be successful.

Kiosk Administration

Settings that define DigitalPersona Kiosk policies are stored in the following location.

Computer Configuration\Policies\Software Settings\DigitalPersona Client\Kiosk Administration

Allow automatic logon using Shared Kiosk Account

Determines whether the automatic logon feature is enabled.

- If enabled, automatic logon uses the Kiosk Shared Account to log users on to the computer when the Windows operating system starts up. The Log On to Windows dialog box is not displayed.
- If disabled or not configured, the automatic logon is disabled.

CAUTION: The automatic logon setting will allow any user to access a Windows session without interactive authentication when the Kiosk computer is restarted.

Logon/Unlock with Shared Account Credentials

- If enabled, any user who knows the user name and password for the shared account that Kiosk uses can use those credentials to log on to or unlock the computer.
- If disabled or not configured, the shared account credentials cannot be used to log on to or unlock the computer.

Prevent users from logging on outside of a Kiosk session

- If enabled, only those with administrator privileges are able to log on to any Kiosk workstation controlled by the GPO.
- If disabled or not configured, users can log on to the Kiosk workstations as a local user outside of the Kiosk session.

Kiosk Workstation Shared Account Settings

In order for a DigitalPersona Kiosk workstation to function correctly, this setting must be enabled and the Windows shared account information (user name, domain and password) specified. For further details, see “[Specifying a Shared Account for the Kiosk](#)” on page 25.

- If enabled, you can specify Windows shared account information for the governed kiosks.
- If disabled or not configured, Kiosk workstations affected by the GPO will not be operable.

Kiosk Unlock Script

Specifies a script file to run whenever a Kiosk session is unlocked by a new user.

By default, the script file should be located in the directory shown below on the Domain Controller or you can specify the full path to a shared folder containing the script file.

%systemroot%\sysvol\sysvol\domain_DNS_name\scripts

DigitalPersona Server

This server setting can be found at the following location.

Computer Configuration\Policies\Software Settings\DigitalPersona Server.

Licenses

This setting provides a way to activate, de-activate and refresh DigitalPersona licenses.

- To add a license for a DigitalPersona Server, right-click the **License** node and select *Activate*. Follow the instructions given in the DigitalPersona Activation wizard.
- To view detailed information about a license, right-click on the license and select *Properties*.
- To refresh license information, right-click the **License** node and select *Check for license updates*. Follow the instructions given in the DigitalPersona Activation wizard.
- To deactivate a license, right-click the **License** node and select *Deactivate*. Follow the instructions given in the DigitalPersona Activation wizard.
- For complete information on adding and managing your DigitalPersona AD licenses, see the *License Activation and Management* chapter.

Computer Configuration\Policies\Administrative Templates

During installation of the DigitalPersona AD or LDS Administration Tools, the following nodes and settings are created under the Computer Configuration\Policies\Administrative Templates node.

DigitalPersona (ADILDS) \ General (Summary)

These settings are used to configure and govern general features of the DigitalPersona software.

Category	Subcategory	Setting name	Page
Attended Enrollment		Authentication of the user being enrolled	80
		Security Officer authentication	80
		Require to complete or omit credential	80
Authentication Devices			80
	Bluetooth	Lock computer when your phone is out of range	80
		Silent authentication	80
	Face	Use Infrared Cameras for Face Recognition	81
		Face Verification	81
	Fingerprints	Redirect fingerprint data	81
		Fingerprint enrollment	81
		Fingerprint verification	82
	OTP	Allow sending OTP through email	82
		Time-Based OTP Validation Window	82
		Push Notification Server API Key	83
		Push Notification Server Tenant ID	83
		Custom SMS or Mail Message	83
	PIN	PIN enrollment	83
	Recovery	Recovery Questions	83
	Credentials	Enable Recovery Questions	83
		Allow Recovery Questions for Windows Logon	84
		Self Password Reset	84
		Path to DigitalPersona Secure Token Server (STS)	84
	Smartcards	Lock the computer upon smart card removal	85
Event logging		Level of detail in event logs	85

DigitalPersona\General (Detail)

Attended Enrollment

Authentication of the user being enrolled

Specify the occasions when a user enrolling credentials through Attended Enrollment must authenticate.

- If enabled, the user being enrolled must authenticate only on those occasions selected in the Options area.

Options are:

- Upon starting to enroll any credential
 - At the end of the enrollment process, before saving data.
- If disabled or not configured, the user needs to authenticate only once during the enrollment session.

Note that this policy has no effect if the *Session Authentication Policy* GPO is disabled.

Security Officer authentication

Specify the occasions when the Security Officer supervising Attended Enrollment must authenticate.

- If enabled, the Security Officer must authenticate upon those occasions selected in the Options area.

Options are:

- When application starts
 - Every time when saving any credential
 - Every time when omitting a credential enrollment
 - Every time when deleting any credential
 - At the end of enrollment, before saving data
- If disabled or not configured, the Security Officer needs to authenticate only when starting Attended Enrollment.

Note that this policy has no effect if the *Session Authentication Policy* GPO is disabled.

Require to complete or omit credential

Require that all specified credentials must either be enrolled or explicitly omitted.

- If enabled, the user must complete the enrollment of all specified credentials or a Security Officer must explicitly approve the omission of any unenrolled credential.
- If disabled or not configured, enrollment of all specified credentials is not required and omitting a credential does not need Security Officer approval.

Note that this policy has no effect if the *Session Authentication Policy* GPO is disabled.

Authentication Devices

Note that the Face and FIDO Key authentication devices (credentials) cannot be used over RDP or within a Citrix environment.

Bluetooth

Lock computer when your phone is out of range

Configure whether or not the computer locks when enrolled Bluetooth device goes out of range.

- If enabled, the computer locks when enrolled Bluetooth device goes out of range.
- If disabled or not configured, the computer does not lock when enrolled Bluetooth device goes out of range.

Silent authentication

- If enabled or not configured, when Bluetooth credentials are allowed for authentication by the Logon or Session Policy in force, authentication will be attempted with the previously used Bluetooth credential immediately upon entry to a logon screen.
- If disabled, selection of a specific Bluetooth credential is required for authentication.

Face

Use Infrared Cameras for Face Recognition

Specifies whether an infrared camera can, or must, be used for Facial Recognition.

- If this setting is enabled and the “Use only infrared cameras for Face recognition” checkbox is *not* checked, any IR camera connected to the computer can be used for Facial Recognition. If an IR camera is mounted on the front panel of the computer, it will be used by default. If no IR camera is found, any camera can be used.
- If enabled and the "Use only infrared cameras for Face recognition" option *is* checked, users without an IR camera connected to their computer cannot use Facial Recognition. If any IR camera is found, it can be used for Facial Recognition. If an IR camera is mounted on the front panel of the computer, it will be used by default.
- If disabled or not configured, any camera connected to the computer can be used for Facial Recognition.

Face Verification

Configure the False Accept Rate (FAR).

The False Accept Rate is the probability of receiving a false acceptance decision when comparing the faces of different people.

- If enabled, you can select one of the following FAR values:
 - Medium (1 in 10,000)
 - Medium High (1 in 100,000) - Recommended
 - High (1 in 1,000,000)

For example: if you select Medium High, on average, one false acceptance will occur when a face is compared against a hundred thousand other faces.

The higher the setting, the lower the chance of receiving a false acceptance. However, at the High setting, the system may reject legitimate faces.

- If disabled or not configured, the value of 1 in 100,000 FAR is used.</string>

Fingerprints

Redirect fingerprint data

Configure whether or not to allow the client computer to redirect fingerprint data to a remote Terminal Services session.

- If enabled, clients can send fingerprint data to a remote computer. This configuration must be enabled to support fingerprint authentication on a remote desktop.
- If disabled or not configured, fingerprint data redirection is not allowed.

When an administrator changes this setting, only new connections display the behavior specified by the new setting. Sessions that were initiated before the change must log off and reconnect to be affected by the new setting.

- The *Do not compress fingerprint data for redirection* checkbox specifies whether to compress fingerprint data on the client computer before redirecting it to the Terminal Services session.
 - If checked, fingerprint data is not compressed on the client computers before sending to the Terminal Server.
 - If not checked, fingerprint data is compressed on the client computers before sending to the Terminal Server.

When an administrator changes this setting, only new connections display the behavior specified by the new setting. Sessions that were initiated before the change must log off and reconnect to be affected by the new setting.

Fingerprint enrollment

Configure settings related to fingerprint enrollment.

- Set the minimum number of enrolled fingerprints

This setting requires that the user enroll at least the specified number of fingerprints.

Enrolling just one fingerprint increases the probability of not being able to authenticate. Enrolling several fingerprints will increase the probability of false acceptance.

If disabled or not configured, the minimum number of fingerprints required for enrollment is 1.

- Set the maximum number of enrolled fingerprints:

This setting restricts the number of fingerprints that a user can enroll. Enrolling several fingerprints will increase the probability of false acceptance.

If disabled or not configured, the maximum number of fingerprints allowed for enrollment is 10.

Fingerprint verification

Configure settings related to fingerprint verification.

- If enabled, allows you to set the False Accept Rate for the fingerprint verification.
- If disabled or not configured, a FAR setting of Medium High (1 in 100,000) is used.

Set the False Accept Rate

The False Accept Rate (FAR) is the probability of receiving a false acceptance decision when comparing fingerprints scanned from different fingers.

When this setting is enabled, you can select one of the following FAR values:

- Medium (1 in 10,000)
- Medium High (1 in 100,000) - Recommended
- High (1 in 1,000,000)

For example: if you select Medium High, on average, one false acceptance will occur when a fingerprint is compared against one hundred thousand fingerprints scanned from different fingers.

The higher the setting, the lower the chance of receiving a false acceptance. However, at the High setting, the system may reject legitimate fingerprints.

NOTE: The FAR is set on a per verification basis. When matching a fingerprint against the fingerprints of multiple users (identification), the internally used FAR is automatically adjusted to maintain the same effective FAR that was selected for one match.

OTP

Allow sending OTP through email

Specify whether to allow sending the user a One-Time Password through email. Requires also entering valid SMTP server information in the SMTP Configuration GPO.

- If enabled, the option to send the user a One-Time Password through email is shown in the UI.
- If disabled or not configured, this option is not shown in the UI.

Time-Based OTP Validation Window

Specifies a validation system acceptance delay for OTP validation in minutes.

Time differences between the TOTP validation server and a client device generating an OTP token can result in a mismatch of the OTP, and subsequent login failure. This is due to the fact that the validation server compares the timestamp when the OTP was generated with the timestamp when it is received. Although the duration of validity of a specific OTP may vary for specific devices, this window is generally plus or minus 30 seconds, for a total window of one minute. In some cases, due to network latency, or inaccurate clocks on lower-end OTP hardware devices, the gap between the originating timestamp and receiving timestamp may be more than the validation window.

This setting allows the administrator to specify a longer validation window. Note that the value indicates the total window, for example a window of 2 minutes would extend the validation window for 1 minute before and after the receiving timestamp.

- If enabled, you can specify a validation window of between 1 and 20 minutes. Be aware that a longer validation window increases the time that the data may be vulnerable to attack.
- If not configured, the validation window defaults to 1 minute.

Push Notification Server API Key

Specifies the user's unique identification key on the Crossmatch Push Notification Server.

- If enabled, and a valid API Key is entered, OTP Push Notification is shown on the logon screen. The API Key is provided in an email from the CPNS Team when a tenant account is created on the Crossmatch Push Notification Server.
- If disabled or not configured, Push Notification will not be shown on the logon screen.

Push Notification Server Tenant ID

Specifies the user's unique identifier on the Crossmatch Push Notification Server.

- If enabled, and a valid Tenant ID is entered, Push Notification is shown on the logon screen. The Tenant ID is provided in an email from the CPNS Team when a tenant account is created on the Crossmatch Push Notification Server.
- If disabled or not configured, Push Notification will not be shown on the logon screen.

Custom SMS or Mail Message

Specifies a string to be used as the SMS or email message sent to the user. Requires a previously created Nexmo SMS account.

- If enabled, this message will be sent each time the SMS or email OTP feature is used. You can specify a custom message with a limit of 140 characters. The message must also include the variable placeholder %s representing the code that will be sent in the message. For example, “Enter the following code to logon: %s”.
- If disabled or not configured, the default message will be sent. The default message is “Use the DigitalPersona Verification Code %s.”

PIN

PIN enrollment

Configure settings related to enrollment of a user PIN.

- If enabled, you can specify the minimum and maximum length of the user PIN.
- If disabled or not configured, the minimum length of the user PIN is 4 and the maximum length is 12.

Note that requiring longer PINs increases security by making it more difficult to try all possible combinations of numbers to discover a user's PIN.

Recovery Credentials

Recovery Questions

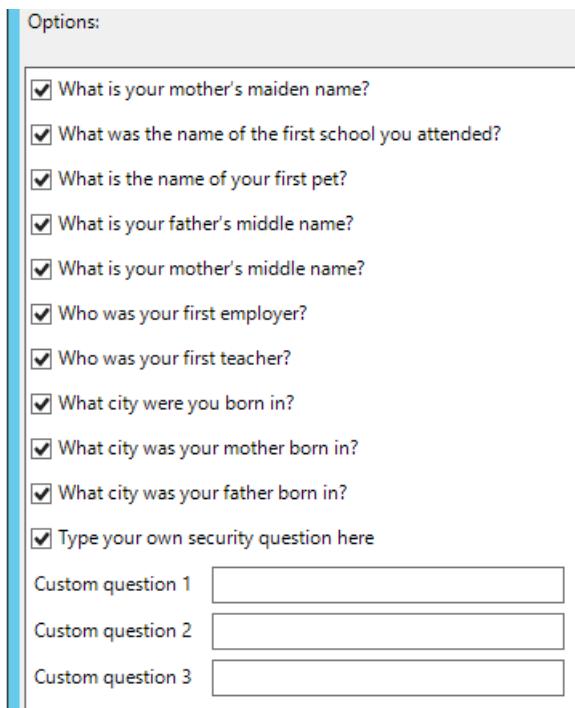
Enable Recovery Questions

Recovery Questions is a recovery feature that allows users to gain access to the computer in the event that they are unable to authenticate with the required credentials.

- If enabled or not configured, users will be able to use Recovery Questions to log on.
- If disabled, Recovery Questions functionality is not available to users.

Once enabled, the administrator can select or deselect from the provided list those questions that will be available to the user. There are also options for the users to be able to type their own security question during enrollment of the

credential, and for the administrator to define up to three custom questions to be included in the Recovery Questions to be answered during credential enrollment.



Allow Recovery Questions for Windows Logon

Specifies whether users can bypass the current Logon Policy after using their Recovery Questions at Windows logon or simply set their Windows Password.

- If enabled or not configured, users may use their Recovery Questions at Windows logon to reset their Windows password and bypass the current Logon Policy.
- If disabled, users may use their Recovery Questions at Windows logon to reset their Windows password only.

Self Password Reset

Allow users to reset their Windows passwords

Specify whether users are allowed to reset their Windows password using DigitalPersona *Recovery Questions* or the *Forgot password?* link on the Identity Provider (STS) page.

- If enabled and the above conditions are met, users are allowed to reset their Windows password using *Recovery Questions* or the *Forgot password?* link.
- If disabled or not configured, or the conditions specified below are not met, users will not be able to reset their Windows password using *Recovery Questions* or the *Forgot password?* link and their Windows password can only be reset by the domain administrator.

Conditions

- For Recovery Questions, the *Enable Recovery Questions* setting must be enabled, and Recovery Questions must be specified in the *Enrollment Policies* GPO.
- For Forgot Password?, the *Path to DigitalPersona Secure Token Server (STS)* GPO must be enabled and the path to the server must be valid.

Path to DigitalPersona Secure Token Server (STS)

Specify the path (URL) to the DigitalPersona Secure Token Server (STS).

For example: <https://server.domain/dppassivests>.

This path is required when the *Forgot password?* link has been enabled on the Identity Server (STS) page through the *Allow users to reset their Windows passwords* GPO.

- If enabled, and a valid URL is entered, the *Forgot Password?* link can be used to obtain an email that can be used to reset a user's Windows password.
- If disabled or not configured, or an invalid URL is entered, the *Forgot password?* link will not function correctly.

Smartcards

Lock the computer upon smart card removal

Configure whether or not the computer locks upon removing the smart card from the smart card reader.

- If enabled, the computer locks upon removing the smart card from the smart card reader. The computer will lock only if the smart card was used to log on to Windows.
- If disabled or not configured, the computer does not lock upon removing the smart card from the smart card reader.

Event logging

Level of detail in event logs

Determines whether DigitalPersona logs events such as credential enrollment and authentication attempts in the Windows Event Log.

There are three levels of event logging:

- Errors
 - Auditing
 - Details
- If enabled, DigitalPersona logs events on the specified level.
 - If disabled or not configured, events are logged on the Auditing level and Status Events are not logged.
- Each higher level includes all previous levels. Events are logged on the computer where the event occurred.

For most normal tasks it is enough to set the level to Auditing. This would cover all events related to logon, authentication, credential management and user management. Setting the level to Detail will fill the log file quickly.

Log Status events

Note that logging of Status Events is not enabled by default, and must be separately enabled by selecting the *Log Status Events* checkbox. Status events provide information about the state of various policies and components on client computers. They are logged on configurable intervals and generally used when events are remotely collected.

DigitalPersona\Server (Summary)

The policies and settings in this table are implemented through AD Administrative Templates and are used to configure the behavior of a DigitalPersona Server.

Category	Setting name	Page
Credentials verification lockout		
	Allow users to unlock their Windows account using DigitalPersona Recovery Questions	86
	Account lockout duration	86
	Reset account lockout counter after	86
	Account lockout threshold	87
DigitalPersona Server DNS		
	Automated site coverage by DigitalPersona Server Locator DNS SRV records	87
	Refresh interval of DigitalPersona Server DNS records	87
	Sites covered by DigitalPersona Server Locator DNS SRV records	87
	Priority set in DigitalPersona Server Locator DNS records	88
	Weight set in DigitalPersona Server Locator DNS records	88
	Register DigitalPersona Server Locator DNS records for domain	88
	Dynamic registration of DigitalPersona Server Locator DNS records	88
Identification Server settings		
	Perform fingerprint identification on server	88
	Restrict identification to a specific list of users	89

DigitalPersona Server (Detail)

Credentials verification lockout

Allow users to unlock their Windows account using DigitalPersona Recovery Questions

Configure whether or not users are allowed to unlock their Windows account using DigitalPersona Recovery Questions.

- If enabled, users are allowed to unlock their account.
- If disabled or not configured, users are not allowed to unlock their account. User accounts can only be unlocked by the domain administrator.

Account lockout duration

Configure the number of minutes an account is locked out before automatically being unlocked. To specify that the account will be locked out until the administrator explicitly unlocks it, set the value to 0. The Account lockout duration must be greater than or equal to the reset time.

- If enabled, you can set a value between 1 and 99999 minutes.
- If disabled or not configured, the duration of the lockout is 30 minutes.

Reset account lockout counter after

Configure the number of minutes that must elapse after a failed credential verification attempt before the account lockout counter is reset to 0. The reset time must be less than or equal to the Account lockout duration.

- If enabled, you can set a value between 1 and 99999 minutes.
- If not configured, the counter is reset after 5 minutes.

Account lockout threshold

Configure the number of failed credential verification attempts that causes a user account to be locked out. The lockout applies to verification of all credentials except the Windows password, which is governed by the Windows lockout policy.

A user cannot access a locked out account using any credential (except their Windows password) until it is reset by an administrator or until the account lockout duration has expired.

- If enabled, you can set a value between 1 and 999 failed fingerprint verification attempts, or you can specify that the account will never be locked out to fingerprint verification by setting the value to 0.
- If disabled or not configured, the account will never be locked out due to failure of fingerprint verification.

DigitalPersona Server DNS

Automated site coverage by DigitalPersona Server Locator DNS SRV records

Configure whether or not DigitalPersona will dynamically register DigitalPersona Server Locator site-specific SRV records for the closest sites where no DigitalPersona Server for the same domain exists. These DNS records are dynamically registered by the DigitalPersona Server, and used by DigitalPersona clients to locate a DigitalPersona AD Server.

- If enabled, the computers to which this setting is applied dynamically register DigitalPersona AD Server Locator site-specific DNS SRV records for the closest sites where no DigitalPersona AD Server for the same domain exists.
- If disabled or not configured, the computers will not register site-specific DigitalPersona AD Server Locator DNS SRV records for any other sites but their own.

Refresh interval of DigitalPersona Server DNS records

Configure the refresh interval of DigitalPersona Server Locator DNS resource records for computers to which this setting is applied. These DNS records are dynamically registered by the DigitalPersona Server and are used by DigitalPersona clients to locate a DigitalPersona Server. This setting may be applied only to computers using dynamic update.

Computers configured to perform dynamic registration of DigitalPersona AD Server Locator DNS resource records periodically re-register 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 re-registration is required so that the authoritative DNS servers (which are configured to automatically remove stale records) will recognize these records as current and preserve them 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 DigitalPersona AD Server Locator DNS records to longer than the refresh interval of the DNS zones may result in unwanted deletion of DNS resource records.

- If enabled, allows you to specify a refresh interval longer than the default value of 1800 seconds (30 minutes).
- If disabled or not configured, computers use the default value.

Sites covered by DigitalPersona Server Locator DNS SRV records

Configure the sites for which the domain DigitalPersona Server registers site-specific DigitalPersona AD Server Locator DNS SRV resource records. These records are in addition to the site-specific SRV records registered for the site where DigitalPersona Server resides, and in addition to the records registered by a DigitalPersona AD Server configured to register DigitalPersona Server Locator DNS SRV records for those sites without an DigitalPersona AD Server that are closest to it.

The DigitalPersona AD Server Locator DNS records are dynamically registered by DigitalPersona AD Server, and they are used by DigitalPersona AD clients to locate a DigitalPersona Server. An Active Directory site is one or more well-connected TCP/IP subnets that allow administrators to configure Active Directory access and replication.

- If enabled, configures the sites covered by the DigitalPersona AD Server Locator DNS SRV records. Specify the site 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 disabled or not configured, no site-specific SRV records will be registered.

Priority set in DigitalPersona Server Locator DNS records

Configure the Priority field in the SRV resource records registered by DigitalPersona AD Server to which this setting is applied. These DNS records are dynamically registered by DigitalPersona AD Server and are used by DigitalPersona AD Workstation to locate a DigitalPersona Server.

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.

- If enabled, configures the Priority in the DigitalPersona AD Server Locator DNS SRV resource records. Specify a value between 0 and 65535.
- If disabled or not configured, computers use a default priority of 0.

Weight set in DigitalPersona Server Locator DNS records

Configure the Weight field in the SRV resource records registered by the DigitalPersona Server to which this setting is applied. These DNS records are dynamically registered by the DigitalPersona Server, and they are used to locate a DigitalPersona Server.

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 record's 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.

- If enabled, configures the Weight in the DigitalPersona Server Locator DNS SRV records. Specify a value between 0 and 65535.
- If disabled or not configured, computers use a default weight of 100.

Register DigitalPersona Server Locator DNS records for domain

Configure whether or not DigitalPersona will dynamically register the DigitalPersona Server Locator domain-specific SRV records for the domain it belongs to. The DNS records are dynamically registered by DigitalPersona Server, and they are used by the DigitalPersona Workstation to locate a DigitalPersona Server.

- If enabled or not configured, computers dynamically register DigitalPersona Server Locator domain-specific DNS SRV records.
- If disabled, computers will not register the domain-specific DigitalPersona Server Locator DNS SRV records for the domain they belong to and register only site-specific records.

Dynamic registration of DigitalPersona Server Locator DNS records

Configure whether or not dynamic registration of DigitalPersona Server Locator DNS resource records is enabled. These DNS records are dynamically registered by the DigitalPersona Server and are used by DigitalPersona clients to locate a DigitalPersona Server.

- If enabled or not configured, computers will dynamically register DigitalPersona Server Locator DNS resource records through dynamic DNS update-enabled network connections.
- If disabled, computers will not register DigitalPersona Server Locator DNS resource records.

Identification Server settings

Perform fingerprint identification on server

Specifies whether fingerprint identification is performed on the DigitalPersona AD Server or against the local computer cache.

- If enabled or not configured, fingerprint identification requests are directed to a DigitalPersona AD Server, where the provided fingerprint data is compared to the data for every user with enrolled fingerprints in the Active Directory domain. Note that after enabling this setting, you will need to wait about 15 minutes before identification is available - or you can restart the DigitalPersona Server to refresh the settings.
- If disabled, fingerprint identification requests are processed on the local computer, where the provided fingerprint data is compared to the data for every user with enrolled fingerprints in the local computer cache.

The default is “not configured.” Note that the default of *not configured* for this setting has the opposite effect from the same setting in the previous DigitalPersona Pro software where not configured resulted in fingerprint identification requests being processed on the local computer.

Restrict identification to a specific list of users

Allow restricting identification to a specific list of users with permissions for the computer where the identification request originates.

- If enabled, you can define a list of users who can participate in identification, and then assign this list to a specific computer or set of computers.
- If disabled or not configured, identification is performed against all domain users.

For details on how to define this list of users, see the topic “[Identification List](#)” on page 253.

DigitalPersona Workstations (Summary)

These settings are used to configure and govern features specific to DigitalPersona workstations.

Category	Setting name	Page
Advanced		
	Do not launch the Getting Started wizard upon logon	90
	Identification Server domain	90
	Compatibility with Microsoft fingerprint support	90
	Allow DigitalPersona client to use DigitalPersona Server	91
	Show Taskbar icon	91
	Allow VPN-less access	91
Caching Credentials		
	Cache user data on local computer	91
	Maximum size of identification list	91
Disable Applications		
	Prevent Password Manager from running	92
Password Manager		
	Display password complexity popup	92
Quick Actions		92
Browser hardware support		92

DigitalPersona Workstations (Detail)

Advanced

Do not launch the Getting Started wizard upon logon

- If enabled, the DigitalPersona User Console and the Getting Started page do not start automatically after user logon.
- If disabled or not configured, the DigitalPersona User Console and the Getting Started page starts automatically after user logon.

Identification Server domain

Specifies the name of the domain where a DigitalPersona ID Server is hosted. Computers attempting to identify a user based on their fingerprint credentials will send the query to this domain.

- If enabled, and a DNS domain name is entered, queries are sent to the specified domain.
- If not configured or disabled, queries are sent to the domain that the computer belongs to.

Compatibility with Microsoft fingerprint support

For Quick Actions to work, the DigitalPersona client software must always maintain an exclusive connection to the fingerprint reader. This exclusivity prevents other software from using the reader, including Microsoft's built-in fingerprint support.

This setting enables or disables those Quick Actions that have a fingerprint credential as a component (called *Finger Actions*), thus allowing or disallowing use of the fingerprint reader in other applications.

- If enabled, Finger Actions are disabled. Other fingerprint software can use the fingerprint reader whenever the DigitalPersona software does not require exclusive use for authentication and fingerprint enrollment.
- If disabled or not configured, Finger Actions may be used, but other fingerprint software (including Microsoft Windows) cannot use the fingerprint reader.

Note that if either the DigitalPersona *Verify Your Identity* dialog or DigitalPersona fingerprint enrollment process is running, it will use the fingerprint reader exclusively, but other applications can use the fingerprint reader as soon as they finish.

Allow DigitalPersona client to use DigitalPersona Server

- If enabled or not configured, DigitalPersona clients will attempt to contact a DigitalPersona Server to obtain services.
- If disabled, DigitalPersona clients will not attempt to contact a DigitalPersona Server, and will use cached data.

Show Taskbar icon

- If enabled or not configured, a Taskbar icon is displayed on managed workstations.
- If disabled, the Taskbar icon is not shown.

Allow VPN-less access

Specifies the URL for VPN-less access.

This feature allows logon to Windows and access to other resources when users are outside of their corporate network without a VPN connection.

- If enabled and a valid URL to the DigitalPersona Web Proxy is entered, the web proxy will be used.
- If disabled or not configured, VPN-less access will not be available.

Requires installation and valid configuration of the DigitalPersona Web Management Components.

Caching Credentials

Cache user data on local computer

Determines whether user data for domain users are cached on the local computer.

- If enabled or not configured, user data (fingerprint templates and secure application data) of domain users is cached locally on the computer. This provides domain users the ability to use their fingerprints when a DigitalPersona Server cannot be located. This is a convenient but less secure option.
- If not enabled, users may only use fingerprints when a DigitalPersona Server is accessible.

The data of local users is always stored on the local computer.

Maximum size of 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.

- If enabled, 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 100; the minimum is 0.
- If disabled or not configured, the default value of 10 is used.

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 from the list, a user can still use their cached credentials (if enabled), but they must type their user name and domain manually.

If DigitalPersona is deployed in a networked environment, 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 Server.

Disable Applications

Prevent Password Manager from running

- If enabled, the Password Manager application is not available.
- If disabled or not configured, the Password Manager application is available.

Password Manager

Display password complexity popup

- If enabled or not configured, the password complexity popup displays when modifying logon profile protected fields.
- If disabled, the popup is not displayed.

Quick Actions

Settings: Credential, Ctrl+Credential, Shift+Credential

Specifies administrator-defined Quick Actions (DigitalPersona Workstation only) that are performed automatically when a user presents an authorized and enrolled credential, or credential plus the Ctrl or Shift keys.

- If enabled, the administrator can specify the Quick Action to be performed by the DigitalPersona client.
- If disabled, no Quick Action will be performed for the selected credential and Ctrl or Shift keys combination on the DigitalPersona client.
- If not configured, the default or user specified Quick Action will be performed on the DigitalPersona client.

For each credential or credential combination, select one of the Quick Action options to be performed by the DigitalPersona client as explained below.

Password Manager Action – If the active window is associated with a personal or managed logon, stored logon data will be filled in. If there is no associated logon, and “Allow creation of personal logons” is enabled or not configured, the User Training Tool displays.

Lock Workstation – Locks the computer.

Browser hardware support

Allow Localhost Loopback

Configures whether to allow client computers to use Localhost Loopback from their web browsers.

Some product features require communication between a client’s web browser and a locally attached hardware device such as a fingerprint reader. DigitalPersona uses a web service named ‘Localhost Loopback’ for this purpose.

Be aware that enabling this feature does involve some security risk where malicious websites may be able to communicate with hardware on the local machine.

- If enabled or not configured, Localhost Loopback is enabled.
- If disabled, Localhost Loopback is disabled. Features such as fingerprint or smart card authentication will not work within client web browsers.

Localhost Loopback Origins

Specifies origins for which Localhost Loopback will be enabled.

Be aware that enabling this feature does involve some security risk where malicious websites may be able to communicate with hardware on the local machine.

- If enabled, the administrator can specify those websites for which Localhost Loopback will be enabled by entering the website origins in a semicolon-delimited format, i.e. www.crossmatch.com;www.mydomain.com. Localhost Loopback will be enabled only for specified websites and disabled for all other websites.

- If disabled or not configured, Localhost Loopback will be enabled for all websites.

User Configuration\Policies\Administrative Templates

DigitalPersona (AD|LDS) \ Workstations (Summary)

During installation, DigitalPersona places a folder under the *User Configuration\Policies\Administrative Templates\DigitalPersona [AD|LDS]\Workstations* folder containing policies and settings that may be applied to users.

The policies and settings in this table only affect users on supported DigitalPersona clients.

Category\Subcategories	Setting name	Page
Password Manager	Allow creation of personal logons	93
	Managed logons	93

Workstations (Detail)

Password Manager

Allow creation of personal logons

Allows users to create and use personal logons for websites and programs.

- If enabled or not configured, creation of personal logons by users is allowed.
- If disabled, creation of personal logons by users is not allowed.

Managed logons

Configure settings for managed logons that govern access to account data and the deployment of logons to users.

If enabled, the options listed below can be configured.

If disabled or not configured managed logons will not be available to users.

Options

- *Allow users to view managed logon passwords:* If this option is selected, users are allowed to view their managed logon passwords after verifying their identity. If unselected, users are not allowed to view managed logon passwords.
- *Allow users to edit account data:* If this option is selected, users can edit their account data. If unselected, users cannot edit account data.
- *Allow users to add account data:* If this option is selected, users can add to their account data. If unselected, users cannot add new account data.
- *Allow users to delete account data:* If this option is selected, users can delete their account data. If unselected, users cannot delete account data.
- *Path(s) to the managed logons folder(s):* When the setting is enabled, managed logons located in the specified folder are copied to all DigitalPersona computers that have this setting applied. Multiple folders may be specified by separating the paths with a pipe (|) character . If no valid path is specified, managed logons will not be available to users.

THIS CHAPTER PROVIDES INSTRUCTIONS FOR SETTING UP THE ATTENDED ENROLLMENT FEATURE OF THE DIGITALPERSONA AD WORKSTATION CLIENT.

Attended Enrollment is a feature that allows a delegated user, or a member of a delegated user group, to attend and supervise the enrollment of DigitalPersona credentials for other users. This functionality is an optional feature that can be selected through a Custom installation of the DigitalPersona AD Workstation client. Instructions for installation and a full description of tasks that may be performed through Attended Enrollment are covered in the DigitalPersona Client Guide. However, the following instructions cover set up and maintenance of Attended Enrollment functionality by the DigitalPersona administrator.

Setting up Attended Enrollment

By default, Attended Enrollment may be performed by any user with domain administrator privileges, and end-users may also enroll and modify their own credentials from their DigitalPersona workstation. If this is the desired behavior for your environment, no further setup is necessary.

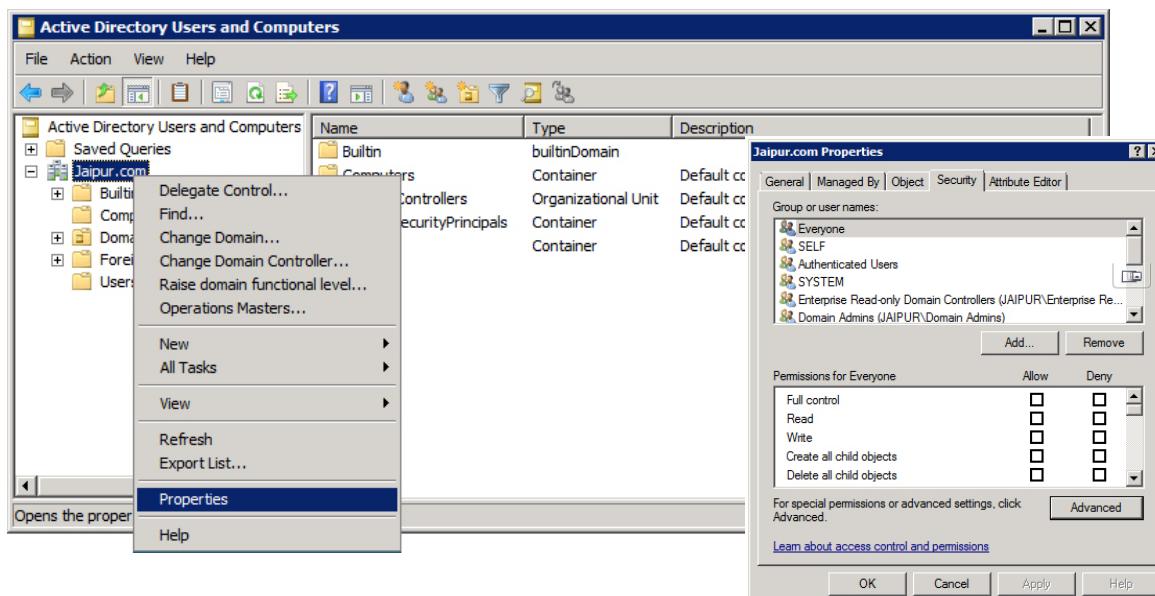
In some scenarios, you may want to delegate authority for attended enrollment to another user or user group and prohibit end-users from enrolling or modifying their own credentials.

Use the following steps to

- Assign enroll/delete credentials permission to a user or group so that they may supervise Attended Enrollment.
- Remove the enroll/delete credentials permission from all users. Note that in this case, you should *remove* the permission, not *Deny* the permission.
- Create a user or group that will supervise Attended Enrollment.

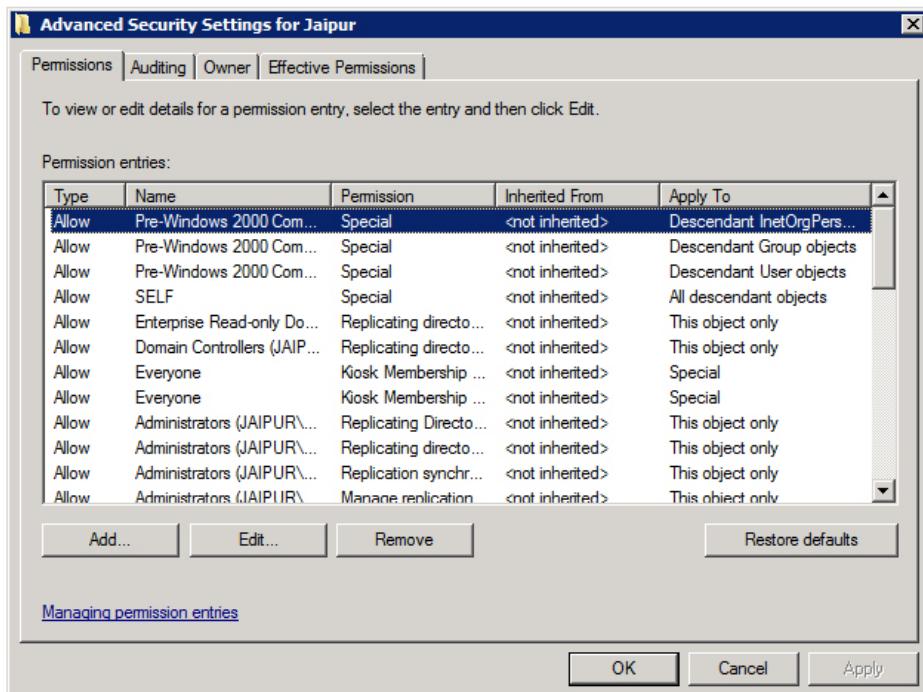
To assign, or remove Register/Delete permissions

1. Open Active Directory Users and Computers.
2. On the View menu, select Advanced Features.
3. As necessary, create a new AD Security Group for those who will be supervising Attended Enrollment.
4. Right-click the AD Domain Root and then click Properties.



To assign, or remove Register/Delete permissions

5. On the **Security** tab, click **Advanced** to view all of the permission entries.



6. Do one or more of the following:

- To assign new permissions
 - Click **Add**. Then type the name of the group, computer, or user that you wish to assign the permission, and click **OK**.
 - In the Permission Entry for *ObjectName* dialog box, on the Object and Properties tabs, select *Descendant User objects* from the *Apply to* drop-down menu.
 - Double-click the **Register/Delete Fingerprint (Digital Persona)*** permission entry, and as appropriate, select either *Allow* or *Deny*.
- To remove the **Register/Delete Fingerprint** permission from an object or attribute, select the permission entry, and then click **Remove**.

* Although the permission is titled “Register/Delete Fingerprint,” it actually applies to all DigitalPersona credentials.

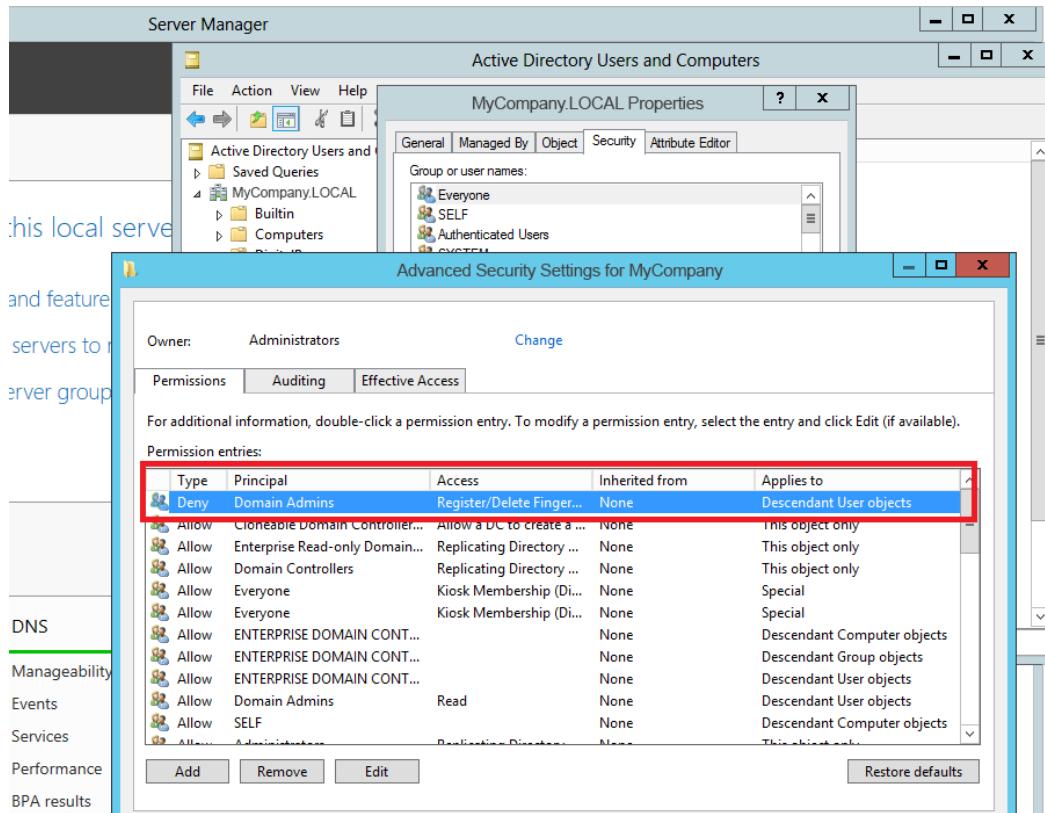
To prohibit domain administrators from enrolling/deleting credentials

1. Open Active Directory Users and Computers.
2. On the View menu, select **Advanced Features**.
3. Right-click the **AD Domain Root** and then click **Properties**.

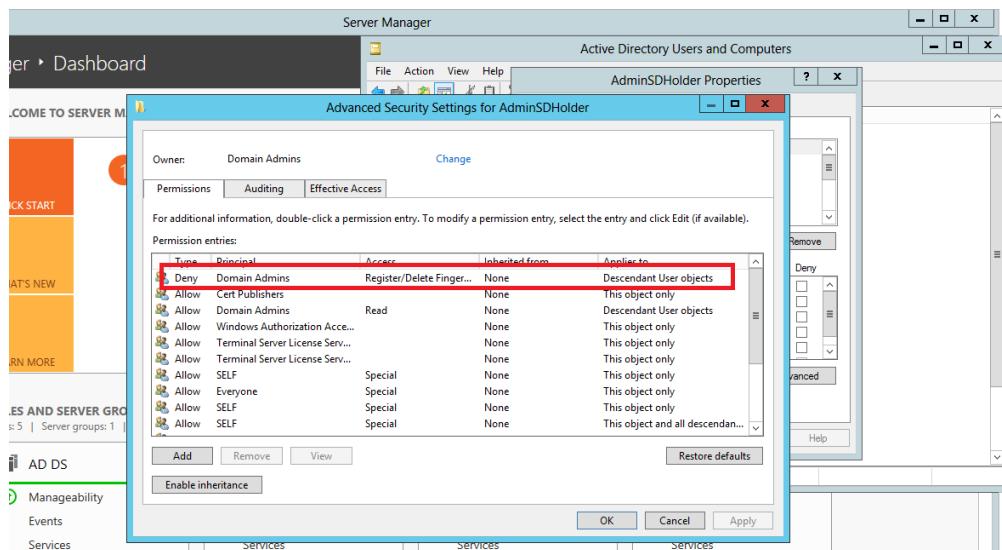
Remove the **Register/Delete Fingerprint (DigitalPersona)** permission from the *Self* object. Although the permission is titled “Register/Delete Fingerprint,” it actually applies to all DigitalPersona credentials.

To assign, or remove Register/Delete permissions

4. Set the permission for the **Register/Delete Fingerprint (DigitalPersona)** entry to *Deny* for the Domain Admins Group.



5. Navigate to [Domain root]\System\AdminSDHolder. Right-click on AdminSDHolder and select *Properties*.
 6. Set the permission for the **Register/Delete Fingerprint (DigitalPersona)** entry to *Deny* for AdminSD Holder.



THIS CHAPTER DESCRIBES THE BUILT-IN PASSWORD RANDOMIZATION FEATURE OF THE DIGITALPERSONA ATTENDED ENROLLMENT COMPONENT.

By default, the Password Randomization feature of DigitalPersona Attended Enrollment is set to *MayRandomize*, which means that the person authorized to enroll users through Attended Enrollment can randomize, unrandomize and re-randomize the user's DigitalPersona password through the Attended Enrollment UI.

However, this behavior can be changed through a setting/element in the *DigitalPersona.Altus.Enrollment.exe.config*, located in the Bin subdirectory within the folder where DigitalPersona Attended Enrollment is installed. By default, this is C:\Program Files\DigitalPersona\Bin.

DigitalPersona Attended Enrollment is an optional feature of DigitalPersona AD Workstation, and is not installed as part of the standard installation. To install it, you must choose *Custom* during the installation and select the *Attended Enrollment* feature.

See the *DigitalPersona Client Guide* for installation instruction and complete *Attended Enrollment* feature details.

Password Randomization Options

The Password Randomization setting is specified in the associated xml file for DigitalPersona Attended Enrollment as described above.

This element can specify one of the following three values.

- DoNotRandomize
- RandomizeAlways
- MayRandomize

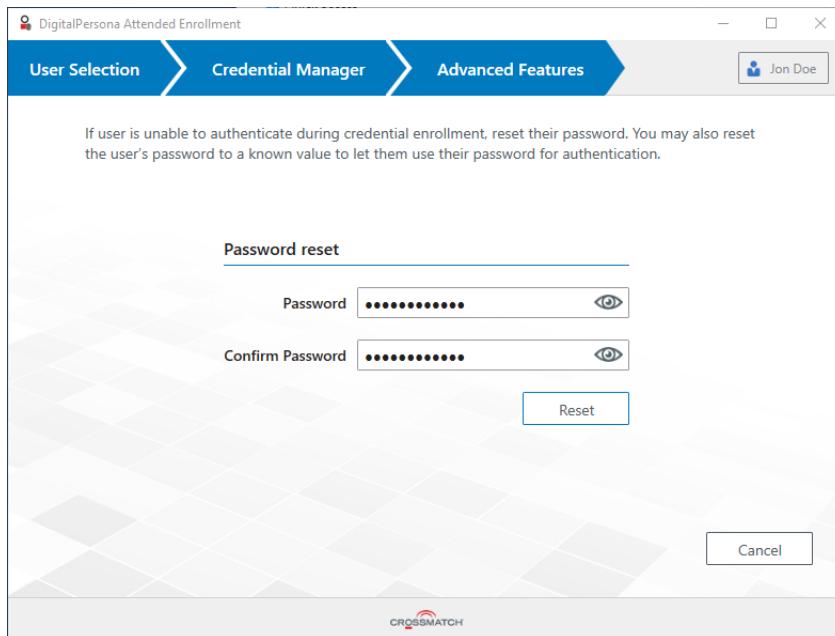
DoNotRandomize - (Default) Passwords are not randomized, and the UI elements for password randomization are not displayed. Passwords cannot be randomized during credential enrollment or from the DigitalPersona Advanced Features page as shown on the following page. Behavior of password entry during enrollment is as described previously in this guide for DigitalPersona Attended Enrollment.

RandomizeAlways - Passwords are randomized automatically. Some UI elements relating to password randomization are displayed. However, the UI does not allow changing passwords during enrollment or changing a randomized password to a non-randomized password or re-randomizing a password. See *RandomizeAlways UI* on page 97.

MayRandomize - Passwords are not randomized automatically, but UI elements for randomization are displayed and may be selected during user enrollment. See *MayRandomize UI* on page 99.

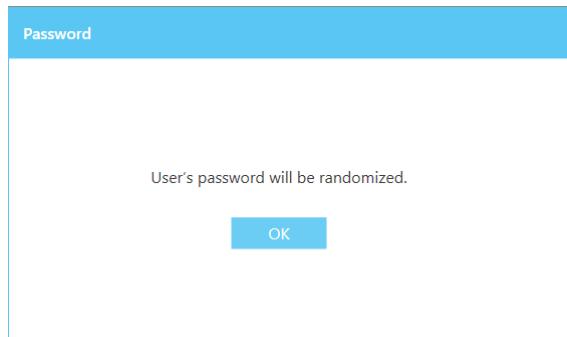
DoNotRandomize

When DoNotRandomize is specified in the configuration file, randomizing the user password is not allowed and the Credential Manager's Advanced Features page displays as shown below, without randomize password UI elements.



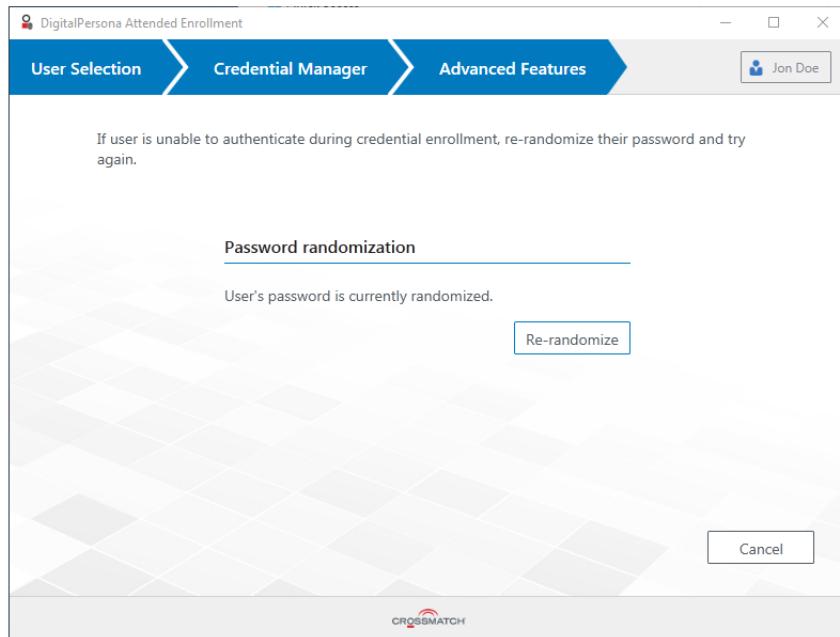
RandomizeAlways UI

When *RandomizeAlways* is specified, instead of asking the user to enter a password during prior to credential enrollment, the software instead displays a message that the user's password will be randomized.



Secondly, clicking the Password tile's *Change* link on the Credential Manager page will display a message that the password cannot be changed because it is randomized.

Finally, on the DigitalPersona Advanced Features page (accessed by the Advanced button on the Credential enrollment page), the *Re-randomize* button displays, providing the means to re-randomize a user's password.



To re-randomize a user's password

- Click *Re-randomize*.

Note that this operation does not require the user's authentication.

MayRandomize UI

When *MayRandomize* is specified, the DigitalPersona Advanced Features page displays UI elements allowing the administrator to reset (randomize, un-randomize or re-randomize the user's password).

The name of the button on the page will change depending on whether the password is currently randomized or not.

If the user is unable to authenticate during credential enrollment, re-randomize or reset user's password. You also may reset the user's password to known value to let the user use the password for authentication.

To reset user's password, enter and confirm the new password.

To randomize or re-randomize user password, press Generate random password.

Generate random password

Reset

Advanced Features

Each tile menu

Advanced Features

Password

Password strength: Good

If user is unable to authenticate during credential enrollment, reset or re-randomize their password. You may also reset the user's password to a known value to let them use their password for authentication.

Password reset

Confirm Password

Reset

Advanced Features

User Selection > Credential Manager > Advanced Features

Jon Doe

Randomize

CROSSMATCH

The officer supervising the enrollment may choose whether or not to randomize the password for each user being enrolled. When password randomization is not desired, the user password may be entered on the screen as described previously in this guide.

If the password is randomized, clicking the *Change* link on the Credential Manager's Password tile for the user displays a message that the password cannot be changed because it is randomized.

To randomize a user's password

- Click *Randomize*.

To reset (un-randomize) a user's password

1. Enter and confirm a new password.

2. Click *Reset*.

To re-randomize the user's password

- Click *Re-randomize*.

Note that the above operations do not require the user's authentication, and that by default, the Attended Enrollment application is configured with the setting *MayRandomize* enabled.

If a user's property in AD is set to 'Randomize User's Windows password,' and credentials are then enrolled through Attended Enrollment, their password will be set to a known value (i.e. un-randomized) during the enrollment process and the 'Randomize User's Windows password' setting in AD will be disabled (unchecked). To re-randomize the user's password, select *Re-randomize* on the *Advanced Features* page.

THIS CHAPTER DESCRIBES THE SINGLE SIGN ON FEATURE IN DIGITALPERSONA AD.

Single Sign-On (SSO) is a feature of DigitalPersona Composite Authentication AD that allows IT administrators to simplify user logon to DigitalPersona Security Applications and enterprise applications; including traditional Windows applications, websites and web applications, terminals, and Citrix or similar software thin client solutions, without needing to modify existing processes.

Single Sign-On supports multiple authentication credentials in configurable combinations in order to provide the utmost flexibility in customizing the feature to your environment.

Configuring Single Sign-On

Configuration of Single Sign-On requires two steps.

1. Disable the Session Authentication Policy setting for the computers where you want to implement SSO.
2. Create managed logons for any resources that you want users to be able to access during a Windows session without needing to provide additional authentication. These logons must have their *Start Authentication Immediately* property set to *Yes* when they are created by the administrator.

Disabling Session Authentication

In Active Directory, disable Session Authentication for the OU (or domain) where you want to use SSO.

1. In the Group Policy Management Editor, click *Session Authentication Policy* at the following location: Computer Configuration/Policies/Software Settings/DigitalPersona/Security/Authentication.
2. On the *Session Policy* tab, select *Disabled*.

Creating managed logons

In order to implement SSO, the managed logon for each resource that will be part of SSO must include use of the *Start Authentication Immediately* setting.

When creating a managed logon for a resource,

- On the Logon Screen Properties page of the Logon Screen Wizard, choose *Yes* for the *Start Authentication Immediately* setting.

Note that this must be used in conjunction with disabling the Session Authentication Policy in order to create a SSO experience. If the Session Authentication Policy is not disabled, authentication will start immediately, but the user will still be prompted for additional authentication.

The process of creating managed logons is covered in the chapter [Password Manager Admin Tool](#) on page 134.

THIS CHAPTER DESCRIBES RECOVERY OPTIONS PROVIDED BY DIGITALPERSONA COMPOSITE AUTHENTICATION AD.

DigitalPersona AD provides full recovery options to administrators for enabling users to regain access to their Windows user accounts and computers.

This chapter includes the following main topics.

Main topics in this chapter	Page
User recovery	102
Account lockout recovery	103
Account lockout recovery	103

User recovery

Installation of DigitalPersona AD or the DigitalPersona ADUC Snap-in adds the Recover User command to Active Directory's context menu for a user in the Active Directory Users and Computers console. This command enables recovery of the user's access to their Windows account by a one time access code available through a link on the Windows logon screen.

To recover a user

DigitalPersona AD provides a means to easily recover access to a computer where a user is unable to access their account, and needs one-time access to the pre-boot environment and their Windows account.

Step	User or DigitalPersona software	Administrator
1.	The user contacts a helpdesk person or DigitalPersona Administrator and provides their Windows user account name.	
2.		The administrator locates the user in Active Directory, right-clicks the user and selects <i>Recover User</i> , which launches the <i>Recover access</i> wizard.
3.		The administrator transmits the displayed Recovery account name and password to the user. This will enable them to authenticate at the pre-boot level. Upon use, this password is automatically changed.
4.	The user enters the provided information, gaining access to the computer at the pre-boot level.	
5.	At the Windows logon screen, the user clicks their user tile. On their user tile screen, they click the <i>One time access</i> link.	
6.	The user transmits the displayed Security Key to the administrator.	
7.		The administrator clicks <i>Next</i> , enters the Security Code and clicks <i>Next</i> again.

Step	User or DigitalPersona software	Administrator
8.	DigitalPersona displays a One time access code which is transmitted to the user. It does not expire, but can only be used once.	
9.	The user types the One time access code and clicks <i>OK</i> , gaining access to their Windows account.	

Account lockout recovery

When a user exceeds the permissible number of authentication attempts (as defined in the Windows security policy) with a fingerprint credential, they are automatically locked out of their account. A locked out account cannot be used until it is reset by an administrator or until the account lockout duration has expired.

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.

To unlock a Windows user account

1. Ensure that you have the required permissions to modify the user account.
2. In Active Directory for Users and Computers, right-click on the user name and select Properties.
3. Click the DigitalPersona tab.
4. Clear the *Account is locked out for fingerprint authentication* checkbox. This checkbox is for unlocking accounts and cannot be used by an administrator to lock an account. If the account is unlocked, the checkbox is disabled.
5. Click OK to close the dialog box and save the changes.

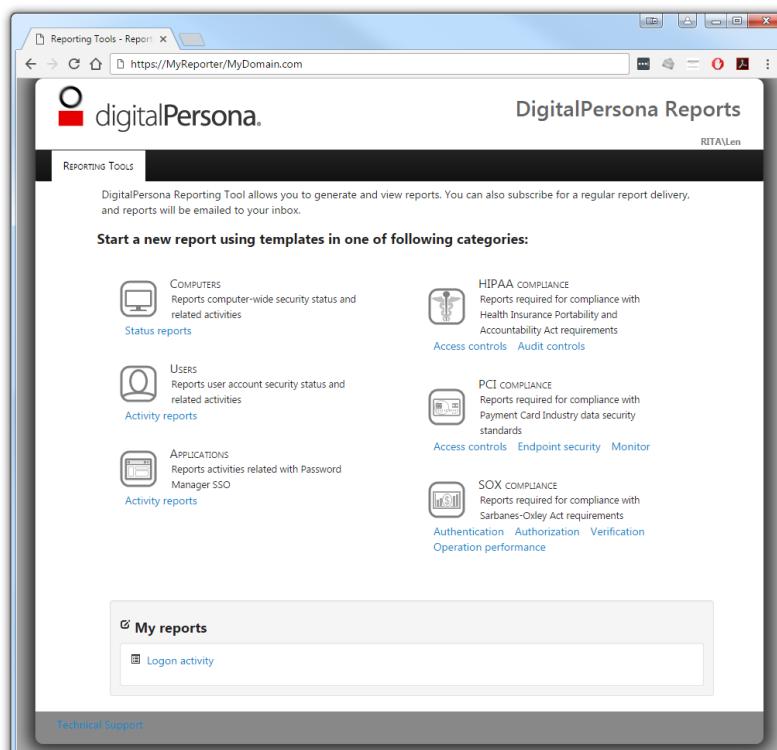
The administrator can choose to set less strict lockout settings by reducing the lockout duration time or reducing the counter reset time through Windows security settings.

DigitalPersona Reports 15

THIS CHAPTER DESCRIBES DIGITALPERSONA REPORTS, AN ADD-ON COMPONENT FOR THE DIGITALPERSONA SOLUTION.

Main topics in this chapter	Page
About Reported events	105
Setting up DigitalPersona Reports	105
Install and configure DigitalPersona Reports	106
Configure Active Directory GPO settings	108
Web console features	114
Creating a report	115
Creating a new subscription	116
Adding a report to an existing subscription	117
Bookmarking a report	118
Deleting a report or subscription	118
Troubleshooting steps	118

DigitalPersona Reports, an add-on component to the DigitalPersona solution, provides a wide-variety of pre-configured template-based reports for managers, administrators and auditors, including detailed information on managed computers, users, SSO events and specific reports addressing HIPAA, PCI and SOX compliance.



About Reported events

Once DigitalPersona Reports has been setup and configured, all events generated by DigitalPersona clients will be forwarded to a designated *Collector* computer via the *Windows Event Forwarding* mechanism.

The *DigitalPersona Report Event import* task, which runs every fifteen minutes on the hour, parses the forwarded events and writes them to a SQL database. Events can then be viewed through the DigitalPersona Reports web console (see page [114](#)).

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

There are some events that are **not** automatically written to the local Windows Event log. Logging of these events requires additional configuration through selection of the *Log Status Events* checkbox of the *Level of detail in event logs* GPO setting. These events provide information about the state of various policies and components on client computers. The interval at which status events are reported can also be configured through the GPO. Logging status events at small time intervals may consume system resources and fill up your Forwarded Events log very quickly.

All logged DigitalPersona client events are written to the local Windows Event Log with a root name of “DigitalPersona > Altus.” The channel name includes the name of the component that logs the events. Currently, the following Component names are defined:

Component name	Description
Core	A general log for all DigitalPersona component events not assigned to a more specific channel.
Logon	User logon/logoff and lock/unlock events.
Password Manager	Managed logon events created by the use of the Password Manager application.

Future components may provide their own channel names, creating a separate Component log under “DigitalPersona>Altus.”

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

Event logging happens on the client workstation/kiosk whether or not event forwarding to the Collector computer has been enabled and set up. If the *DigitalPersona Reports Event Forwarding* setting has been enabled, then events are forwarded to the “Forwarded Events Log” folder on the computer where DigitalPersona Reports is installed. The events are logged in the Event Viewer > Windows Log > Forwarded Events folder.

Setting up DigitalPersona Reports

If installing on Windows Server 2012 R2, ensure that .NET 3.5 has been previously installed.

Setting up DigitalPersona Reports, consists of the following high-level tasks. Each task is described in more detail in the following sections.

- Install and configure DigitalPersona Reports.
- Configure Active Directory GPO settings for event forwarding.
- Enable JavaScript in the web browser used to access the DigitalPersona Reports web console. (In Internet Explorer, this setting is called “Active Scripting.”)

Install and configure DigitalPersona Reports

Requirements

DigitalPersona Reports should be installed on a computer that is a member of the domain and meets the following requirements.

- The computer is not a domain controller.
- It is running Windows Server 2012 or /2012 R2 (32/64-bit)
- The computer name must not include underscores, for example TEST_0250.

Installation on a computer that also hosts a DigitalPersona Server is not recommended.

Upgrading DigitalPersona Reports

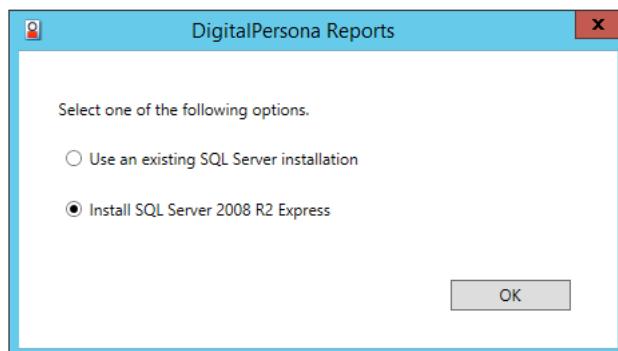
When upgrading from a previous version of DigitalPersona Reports, you should deactivate or unlink all GPOs that have been applied to DigitalPersona Reports before upgrading. You should do this regardless of whether you are installing over the previous installation or uninstalling the previous version before installing the newer version. After installation, reactivate the GPOs.

- Deactivate/unlink Reports GPOs
- Run gpupdate /force
- Reboot system
- Install new version
- Activate/link Reports GPOs
- Run gpupdate /force
- Reboot system

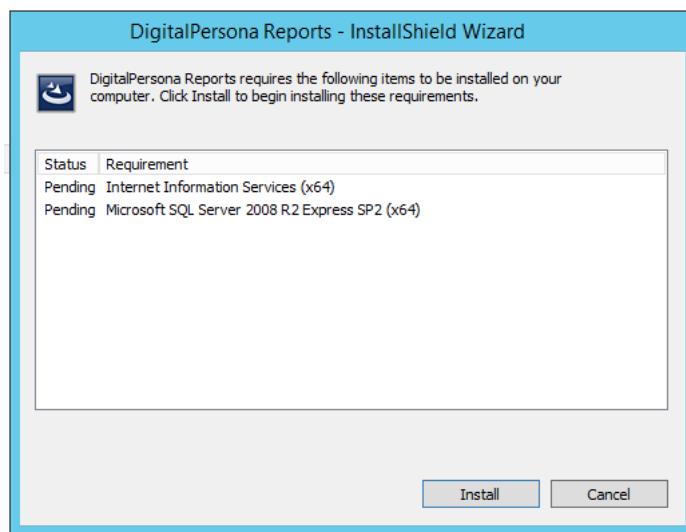
Installation

The installation file for DigitalPersona Reports is located in the *DigitalPersona Reports* directory of your DigitalPersona product package. Be sure to check the included *readme.txt* file for any updated information prior to installing DigitalPersona Reports.

1. Start the installation wizard by launching **setup.exe**.
2. Follow the onscreen instructions.
 - a. You will be prompted to either use an existing SQL Server 2008 instance (if no other instances of SQL Server RTM, R2 SP1, Express RTM or R2 SP1 Express are detected), or to install SQL Server 2008 R2 Express Edition. Select the appropriate choice for your environment.



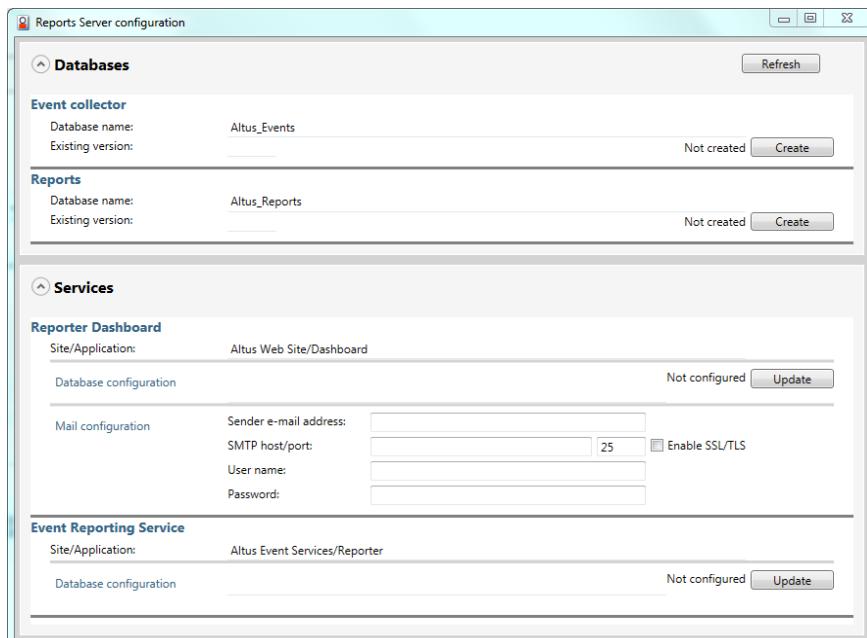
- b. A prompt will display asking you to install Internet Information Services (if not previously installed) and SQL Server 2008 R2 Express SP2 (if selected in the previous step). Click *Install*.



- c. Reboot when prompted to do so. Installation will resume after the reboot.
- d. If you chose to install SQL Server Express Edition in step a. above, follow the onscreen prompts for installation.
- e. The DigitalPersona Reports software will then install.
- f. The installation will place a shortcut to the DigitalPersona Reports web console on your desktop.
- g. On the last page of the wizard, click *Finish*.

Reports Server Configuration

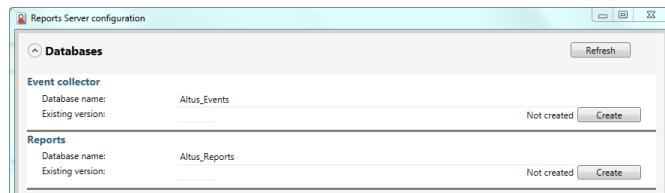
The Reports Server Configuration Tool is launched automatically after the installation of DigitalPersona Reports finishes.



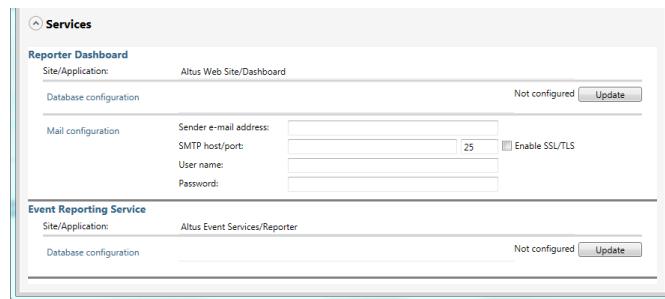
The Reports Server Configuration Tool provides a central place to

- Connect to the SQL server (existing or newly installed)

- Create or upgrade databases ("Altus_Events" for collecting events, and Altus_Reports for reporting queries and mailing subscriptions)

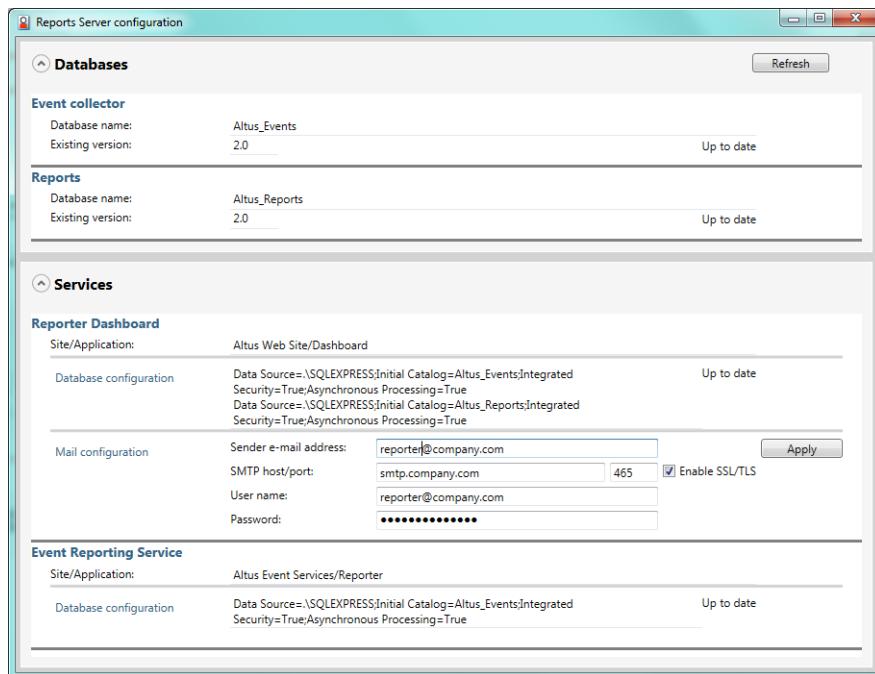


- Configure web services to use those databases



- Setup mailing configuration to enable sending reports by e-mail

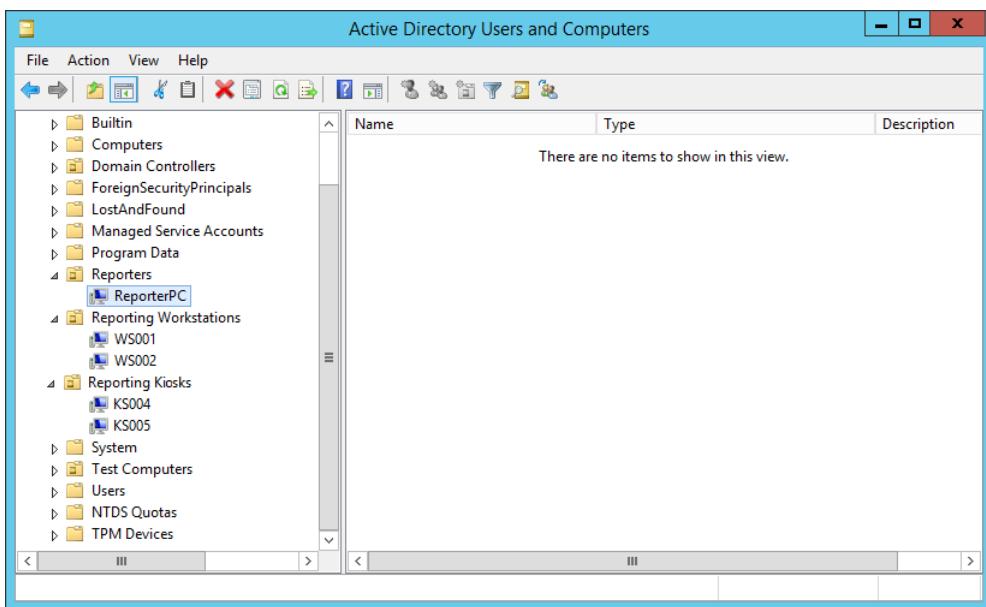
The image below shows an example of a completed Reports Server configuration.



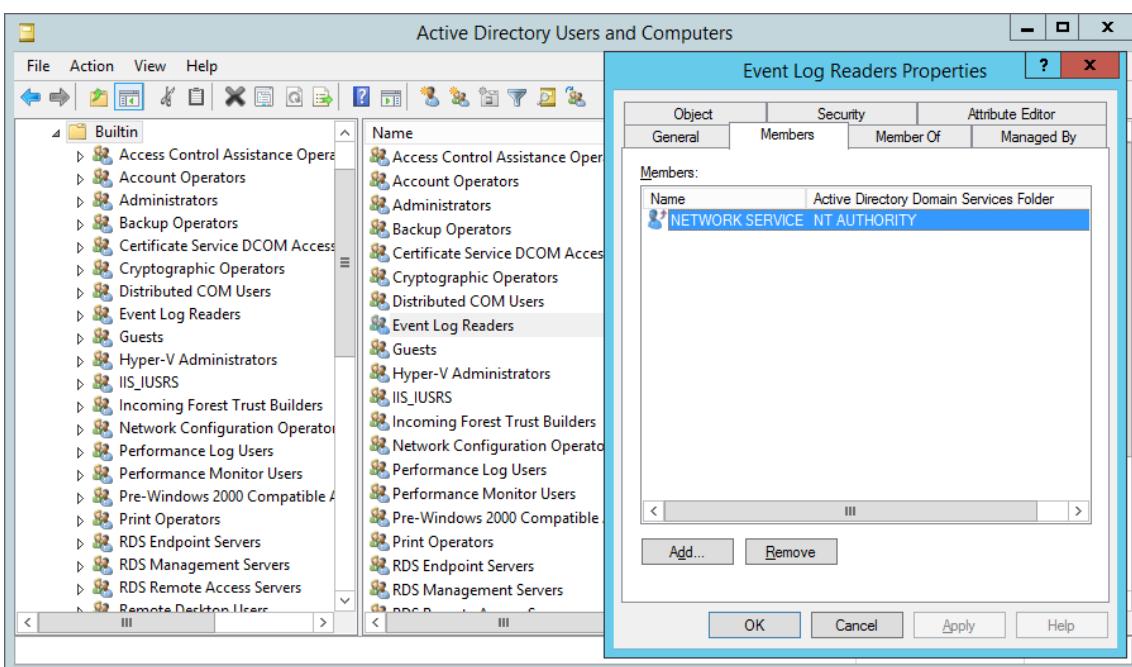
Configure Active Directory GPO settings

In Active Directory Users and Computers

1. Configure Active Directory. As a best practice, DigitalPersona Reports and DigitalPersona clients should be located in separate OUs linked with an appropriate policy.



2. On the domain controller, make the “NT AUTHORITY/Network Service” built-in account a member of the *EventLogReaders* group. This will allow WinRM to read event logs.



- In ADUC, navigate to <yourdomain>\Builtin\Event Log Readers.
- Right-click on *Event Log Readers* and select *Properties* from the shortcut menu. Then select the *Members* tab.
- Select *NETWORK SERVICE* and click *Add*.

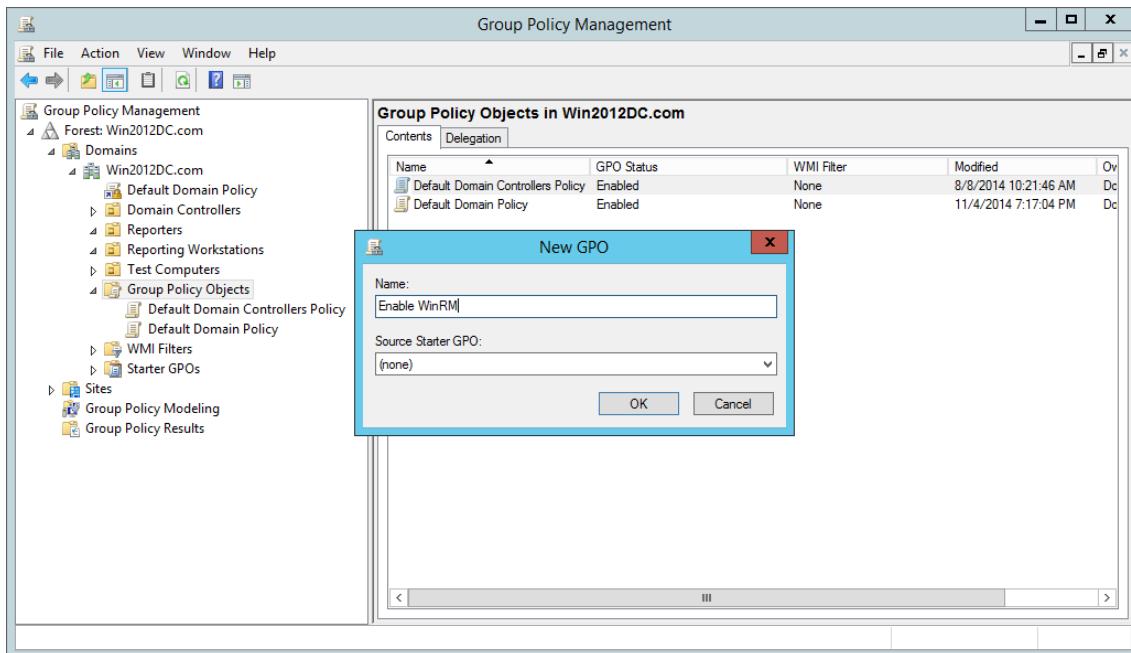
Import GPOs from GPO backup

1. Using the following steps to create new empty GPOs and give them meaningful names such as:

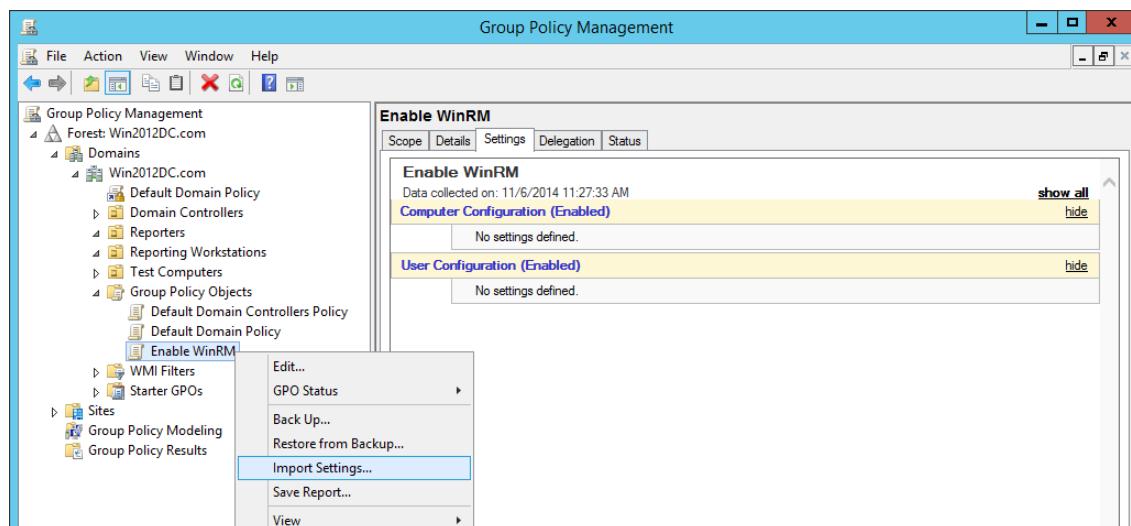
- Enable WinRM
- Enable DigitalPersona Event Forwarding

Setting up DigitalPersona Reports

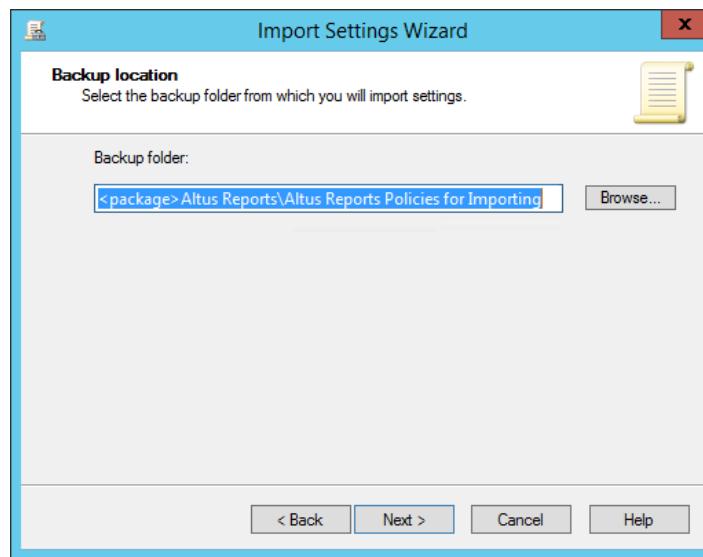
- Enable DigitalPersona Audit Event Logging (Optional, sets level of Event reporting to Audit level detail)



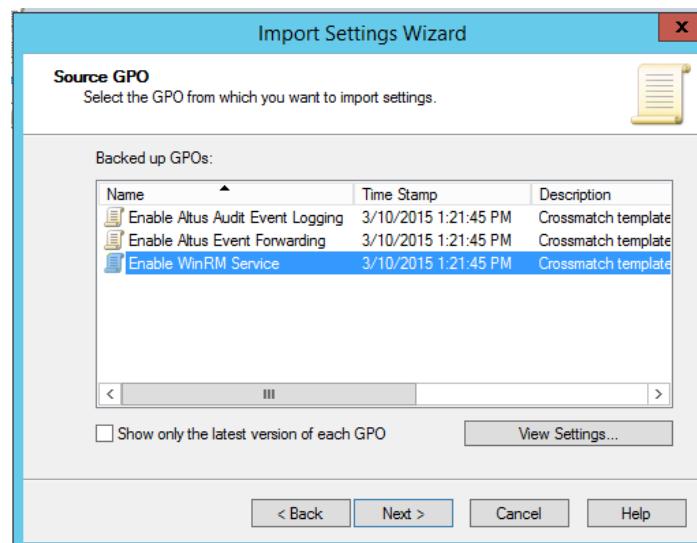
- Import GPO: right-click on the new GPO and select *Import settings* to start the *Import Settings wizard*.



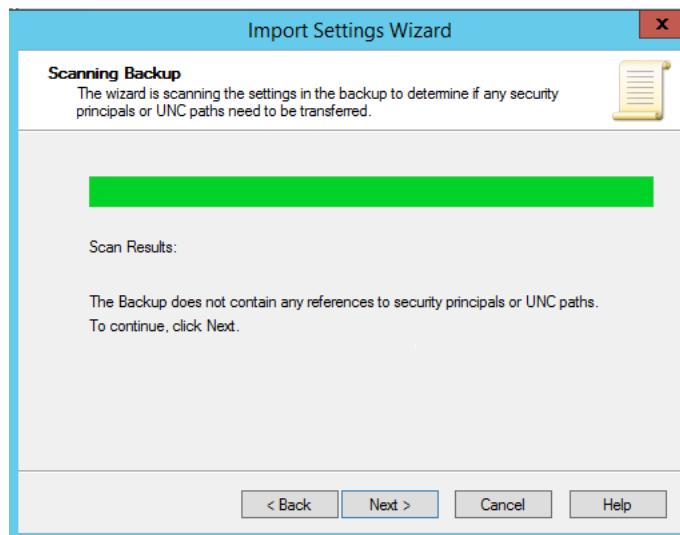
- i. On the *Backup Location* page, select the *DigitalPersona Reports Policies for Importing* folder described above.



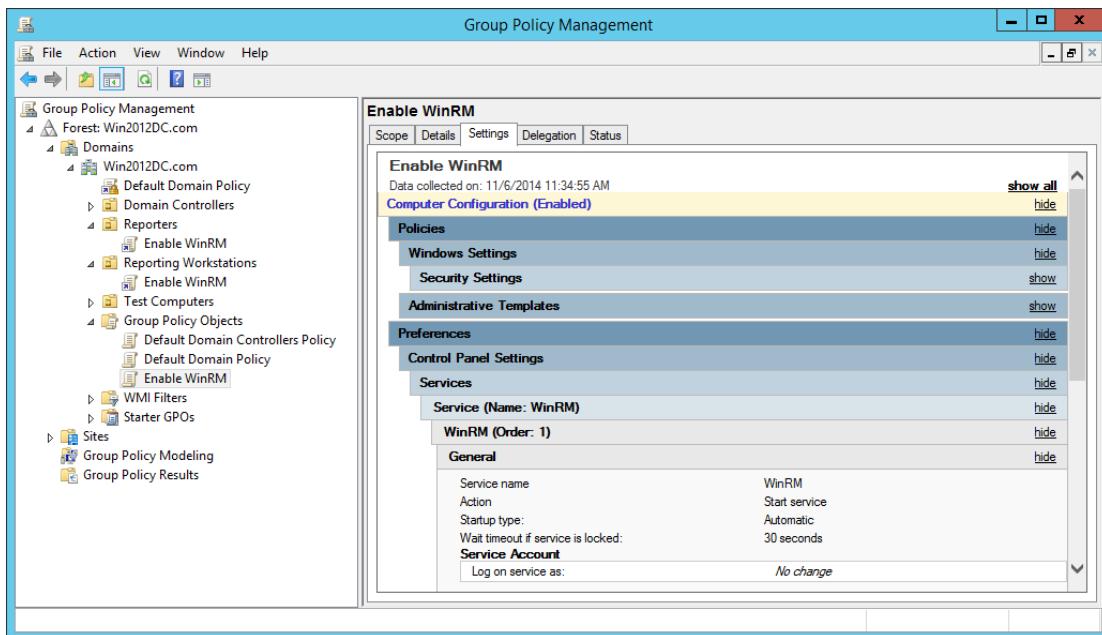
- j. On the *Source GPO* page, choose the corresponding DigitalPersona GPOs and proceed to the end of the wizard.



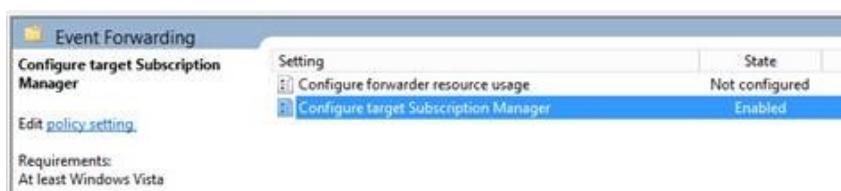
- k. On the *Scanning Backup* page, click *Next*. On the final page, click *Finish* to close the wizard.



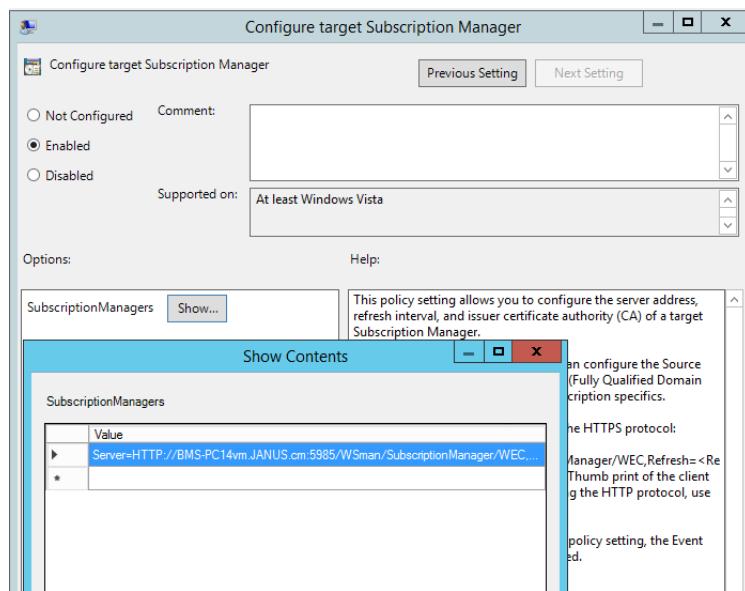
- l. In the GPO, check the *Settings* tab to make sure that the settings were imported.



2. Repeat steps *a* through *l* for each DigitalPersona GPO listed at the beginning of step 1.
3. Configure the *target Subscription Manager* URI.
- Configure the *target Subscription Manager* URI.
 - Right-click on the *Enable DigitalPersona Event Forwarding* GPO created above, and then double-click on the *Configure target Subscription Manager* setting.



- c. In the *Configure target Subscription Manager* window, click *Show*. Then, in the *Show Contents* window, replace *ReporterPC.company.com* with the appropriate Fully-Qualified Domain Name (FQDN) of the DigitalPersona Reports computer.



Example:

Default string - *Server=http://ReporterPC.Company.com:5985/wsman/SubscriptionManager/WEC,Refresh=10*
 Updated string - *Server=http://{ReportServerFQDN}:5985/wsman/SubscriptionManager/WEC,Refresh={interval}*

where

{ReportServerFQDN} is the fully-qualified domain name of the Reports machine,

{interval} is the time interval in seconds between updates to subscriptions. Note that it is not an event collection interval. The default value is 10 seconds.

For more about Windows Event Forwarding, see the following Microsoft articles.

<https://docs.microsoft.com/en-us/advanced-threat-analytics/configure-event-collection>

<https://blogs.msdn.microsoft.com/canberrapfe/2015/09/21/diy-client-monitoring-setting-up-tiered-event-forwarding/>

4. Link the GPO to the corresponding OU (or setup Security Filtering):
 - a. Apply these GPOs to all OUs with reporting workstations and all OUs with reporting kiosks.
 - Enable WinRM
 - Enable DigitalPersona Event Forwarding
 - Enable DigitalPersona Audit Event Logging GPO (Optional, for audit-level detailed event reporting)
 - b. Apply this GPO to DigitalPersona Reports
 - Enable WinRM
5. After the GPOs are applied,
 - a. Verify the following on reporting workstations, kiosks and on the DigitalPersona Reports computer.
 The *Windows Remote Management* service is running.
 - b. Verify the following on reporting workstations and kiosks.
 The *Event Forwarding* service is running and events are appearing in the *Forwarded Events* event log.

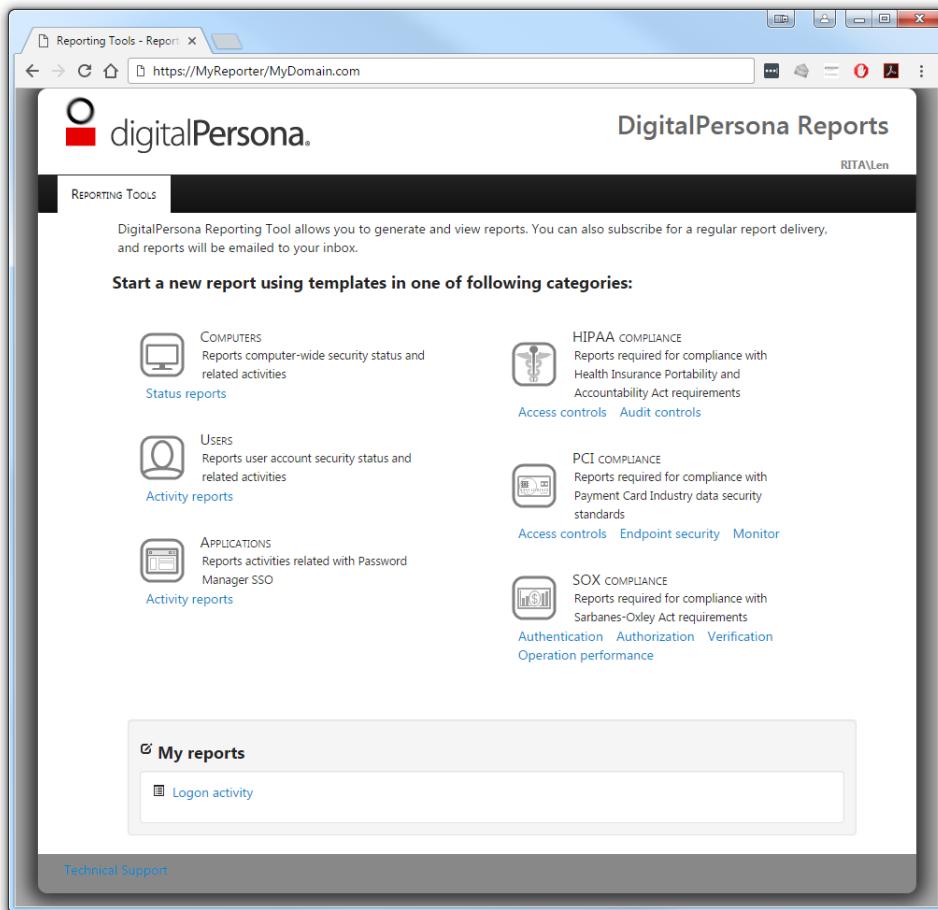
See the *Troubleshooting steps* topic at the end of this chapter (page 118) if you experience problems with the Event forwarding setup.

Web console features

The DigitalPersona Reports web console allows you to generate, view and schedule reports based on the activity and status events generated by DigitalPersona clients.

Reports can be created ad hoc for specific one-time needs, or scheduled (subscribed to) for email delivery on a regular timetable.

DigitalPersona Reports also provides a powerful assortment of pre-configured templates for quickly and easily creating various types of reports as shown in the illustration below, including HIPAA, PCI and SOX compliant reports.



The URL for accessing the DigitalPersona Reports web console (after initial installation and configuration) is

<https://<hostname>/Dashboard/Reports>

The DigitalPersona Reports web console supports the following web browsers.

- Internet Explorer
- Google Chrome
- Mozilla Firefox

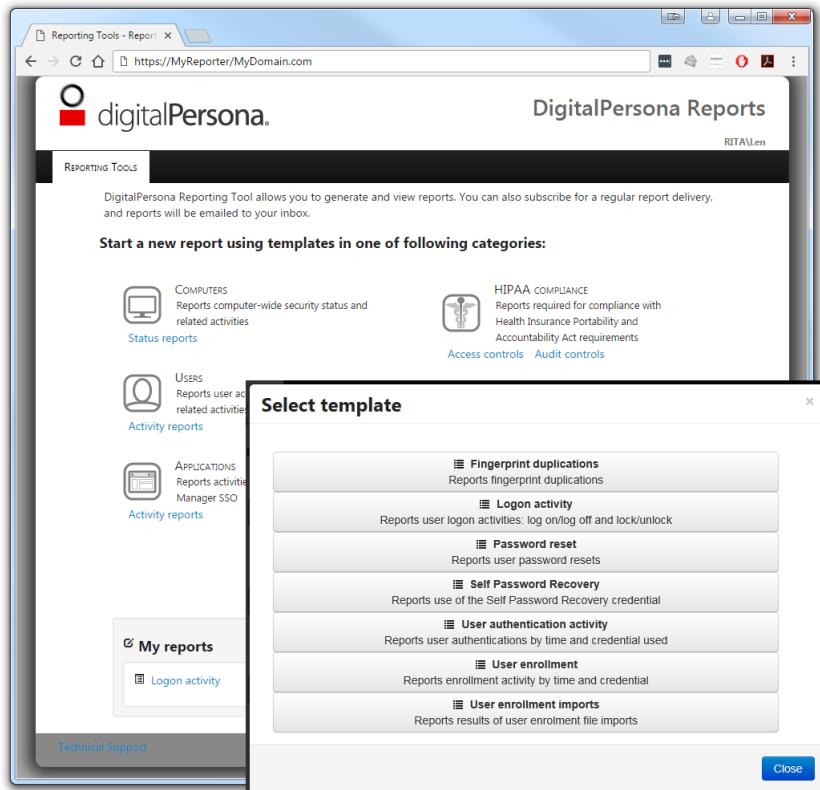
See the *readme.txt* file within the DigitalPersona Reports folder of your product package for a current list of supported browser versions.

Note that when creating or editing reports, you must click the **Save** or **Run Now** buttons to save any new or modified information.

Creating a report

To create a new report

1. On the main DigitalPersona Reports page, click a report type under one of the listed categories.
2. Within the report type, select a pre-defined report template.



3. By default, the report name and description are prepopulated with the given template name and description. Click on the name or description to use your own name and/or description for the report.
4. Select from the available parameters to build the query for your report. Parameters will vary for different reports.

This screenshot shows the configuration page for a 'User authentication activity' report. The URL in the browser is <https://MyReporter/MyDomain.com/Dashboard/Reports/Queries/Edit/c018f2db-4a4f-4ce1-8r>. The page header includes the DigitalPersona logo and 'DigitalPersona Reports'. Below the header, there's a breadcrumb trail 'Home / User authentication activity'. There are three buttons at the top: 'Back', 'Save', and 'Run now'. A note says 'This report is not a part of any subscription. To start receiving this report by email on a regular basis, create a new subscription.' A 'User authentication activity' section contains a description 'Reports user authentications by time and credential used'. A large 'Query' section at the bottom contains the following fields:

- 'End date': A date input field set to '5/19/2017'.
- 'Report data for previous': A dropdown menu set to 'day'.
- 'Computer name': An input field.
- 'User account': An input field.
- 'Activity result': A dropdown menu set to 'All'.

5. In the image above, the *End Date* would be the last date you want included in the report. Select from the *Limit Data* by dropdown to indicate how far back you would like to report data from, i.e. an *End Date* of today and a *Limit Data* by selection of “*End Date - 1 day*” would give you data from the beginning of yesterday (00”00”00) to the current time today. When scheduling a report, you will enter the date ranges to be used for the subscriptions.
6. (Optional) To report on data for all DigitalPersona managed computers, leave the Computer name field blank. To report on data for a single DigitalPersona managed computer, enter the computer name.
7. To run the report, click *Run now*.

Note that data entered in the fields on this form is *not* automatically saved as you move from field to field. If you close a tab or browser window before Saving or Running a report your data will be lost.

Creating a new subscription

A subscription is a way of automatically running a report on a regular basis. Subscriptions can be created from one or more reports that are then scheduled to be run at regular intervals. They may be created either during the initial definition of the report, or later, by opening a report and clicking one of the links available to create a new subscription or to add the report to an existing subscription (see page 117).

To create a new subscription from a report

1. From the previously created report’s page, click *Create a new subscription* (see previous image).
2. Enter a name for the subscription and (optionally) a description. Then click *Create*.

Create a new subscription

Name: Len's Logon Policy Report

Description: Logon Policy Report for weekly staff mtg

Create

3. Enter the email address that you want the report to be sent to. You can also enter multiple email addresses, separated by semicolons.

E-mail settings

Mail to: Type an e-mail address

CC: Type an e-mail address

BCC: Type an e-mail address

Subject: Len's Logon Policy Report

Schedule

Enabled

From: MM/DD/YYYY To: MM/DD/YYYY

Time: 00:00

4. Enter a subject for the email that recipients will receive when they get the report.
5. By default, the subscription is enabled. To disable the subscription, i.e. stop the report from running, deselect the *Enabled* checkbox.

6. Enter the beginning date and time and the ending date for the subscription. The report(s) in this subscription will be run beginning on the *From* date and time until the *To* date.
7. Configure the following parameters used to determine how often the report(s) are to be run.
 - By default, the report(s) will be run daily during the time period selected in step 6 above. Click one of the following links to specify more advanced parameters.
 - *Specific months* - To run only in specified months, deselect any months (during the dates entered in steps 6) when the report should *not* be run.
 - *Specific weeks* - To run only during specified weeks within those months selected, deselect any weeks (during the dates entered in steps 6) when the report should *not* be run.
 - *Specific week days* - To run only during specified days of the week within those weeks selected, deselect any week days (during the dates entered in steps 6) when the report should *not* be run.

Specific months					
<input checked="" type="checkbox"/> January	<input checked="" type="checkbox"/> February	<input checked="" type="checkbox"/> March	<input checked="" type="checkbox"/> April	<input checked="" type="checkbox"/> May	<input checked="" type="checkbox"/> June
<input checked="" type="checkbox"/> July	<input checked="" type="checkbox"/> August	<input checked="" type="checkbox"/> September	<input checked="" type="checkbox"/> October	<input checked="" type="checkbox"/> November	<input checked="" type="checkbox"/> December
Specific weeks					
<input checked="" type="checkbox"/> 1st	<input checked="" type="checkbox"/> 2nd	<input checked="" type="checkbox"/> 3rd	<input checked="" type="checkbox"/> 4th	<input checked="" type="checkbox"/> last	
Specific week days					
<input checked="" type="checkbox"/> Sunday	<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday		
<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input checked="" type="checkbox"/> Saturday	<input type="checkbox"/> Last		

8. For example, to run the report for a year (as defined in the above image), at 8 am on the first Monday in March, deselect all months except March, select *1st* for Specific weeks and deselect all days except Monday.
9. Click the *Reporting Tools* tab to return to the main DigitalPersona Reports page. Your new subscription will be listed under *My subscriptions*.

Adding a report to an existing subscription

To add a report to an existing subscription

1. From the main DigitalPersona Reports page, click the report that you want to add.
2. Click *add report to an existing subscription*.
3. Select the subscription that you want to add the report to.

4. The report will be added to the selected subscription.

Editing a subscription

To edit a subscription

1. From the main DigitalPersona Reports page, click the subscription you want to revise.
2. Click one of the reports in the subscription to edit the query details.
3. Revise subscription details as required. Changes are saved automatically.

Bookmarking a report

To bookmark a report

1. On the main DigitalPersona Reports page, hover over the name of the report.
2. Click the bookmark  icon.

Deleting a report or subscription

To delete a report

- On the main DigitalPersona Reports page, hover over the name of the report or subscription. Click the X that displays to the right of the report or subscription name.

Troubleshooting steps

If you are having trouble getting DigitalPersona Reports to function properly, please check the following items.

1. Is the Windows Remote Management service running on both the DigitalPersona Reports and DigitalPersona client machines?
2. Is the Windows Event Collector service running on the DigitalPersona Reports machine?
3. Are there any errors in the “Microsoft\Windows\EventCollector” or “Microsoft\Windows\Eventlog-ForwardingPlugin” event logs?
4. Are there any events in the “Forwarded Events” channel on the DigitalPersona Reports machine?
5. Is there an “Reports event import” task in the Windows Task Scheduler, and can you confirm that it executes periodically by looking in the task History tab?
6. Do you see a “ForwardedEvent.bookmark” file created in the “%ProgramFiles%\DigitalPersona\bin\” folder?

THIS CHAPTER DESCRIBES THE EVENTS THAT DIGITALPERSONA COMPONENTS WRITE TO THE WINDOWS EVENT LOG WHEN SIGNIFICANT ACTIVITIES OCCUR.

Overview

DigitalPersona AD components write events to the Windows Event Log when significant activities occur, along with a date and time stamp indicating when they occurred.

All of the following DigitalPersona events are logged by default (depending on the logging level being viewed) - except for those that report the *status* of applications, components or devices. Status events are identified in the following pages by the designation (Status event) after the event name.

Activity events are classified into the following categories, with a range of event IDs that begin with the ID number shown below.

Description	ID	Page
Credential Management	256	120
User Management	512	121
Secret Management	768	122
Service Management	1024	123
Password Manager	1536	123
Credential Authentication	2048	124
DNS Registration	2304	124
Deployment	4096	125
OTP Management	4358	125
Windows Logon	4864	125
Authentication Domain Management	5632	126

Events are listed in tables under each category in the following sections. For each event, information is shown indicating where the event is logged (on the DigitalPersona AD Server or on a client workstation) and what level of logging an event is reported at. For example, if an event is shown as logged on the workstation (Wks) at the D (Details) level, it will not be written to the log unless the Detail level is specified in the *Level of detail in event logs* GPO setting governing that computer (see page 85).

Note that error levels are inclusive, i.e. the Audit level includes all Error level messages, and the Details level includes all Audit and Error level messages.

Credential Management

Task Category: 256

The following events may be generated during credentials management.

Event	ID	Level	
		Srvr	Wks
Failed to enroll credential	259	-	A
Credential enrolled	260	-	A
Failed to unenroll credential	261	-	A
Credential unenrolled	262	-	A
Failed to recover user record	263	-	E
Failure of user credential consistency check	272	-	E
Fingerprint credentials cache is cleared. User: <UserName>*	277	-	E
Duplicate fingerprint found**	278	E	-
Credential enrolled (Attended Enrollment)***	281	-	A
Failed to enroll credential (Attended Enrollment)***	288	-	E
Credential deleted (Attended Enrollment)***	289	-	A
Failed to delete credential (Attended Enrollment)***	259	-	E

Level: E = Error, A - Audit, Dt = Details

* This event is logged after fingerprints have been matched locally but not found on the server three times in a row. DigitalPersona then clears the client's fingerprint credentials cache.

** Duplicate fingerprint found - After a fingerprint is enrolled, it may take up 5 minutes for the fingerprint to be added to the identification set. Therefore, a duplicate fingerprint enrolled within that 5 minute window may not trigger the *Duplicate fingerprint found* event. See additional details in the table on the next page and in the [Fingerprint Adjudication and Deduplication](#) chapter on page 251.

*** Events marked above as (Attended Enrollment) include a hidden TransactionId parameter in event parameters allowing tracking of a single attended enrollment activity.

Duplicate fingerprint found

This topic further defines the Duplicate Fingerprint found event listed in the above table.

The Duplicate fingerprint found event includes the following details:

User, Fingerprint, Duplicate User, Duplicate fingerprint

Example:

Duplicate fingerprint found.

User: Engineering\JSmith

Fingerprint: 3

Duplicate user: Sales\GBush

Duplicate fingerprint: 9

Fingerprint and Duplicate fingerprint enumerate a user's fingers as follows.

Finger	#
Left pinky finger	0
Left ring finger	1
Left middle finger	2
Left index finger	3
Left thumb	4
Right thumb	5
Right index finger	6
Right middle finger	7
Right ring finger	8
Right pinky	9

User Management

Task Category: 512

The following events may be generated during user management, as well as during import and export of user enrollment data.

Event	Level		
	ID	Srvr	Clntr
Cannot update User Account Control Flags	527	-	E
User Account Control Flags were updated	528	A	-
User account was unlocked	529	A	-
User password was randomized	530	A	-
User added to the database	531	A	-
Cannot add Altus User to the database	532	E	-
User deleted from the database	533	A	-
Cannot delete Altus User from the database	534	E	-
User account was unlocked using Password Reset	535	A	E
User record is created and opened for attended enrollment.	537	-	A
Cannot create user record for attended enrollment.*	544	-	E
User record is opened for attended enrollment.*	545	-	A
Cannot open user record for attended enrollment.*	546	-	E
User record is closed after attended enrollment.*	547	-	A

Event	Level		
	ID	Srvr	Clnt
Cannot close user record after attended enrollment.*	548	-	E
User attribute is queried.	549	-	A
Failed to query a user attribute.	550	-	E
User attribute is updated.	551	-	A
Failed to update a user attribute.	552	-	E
User enrollment data is exported to a file.	553	-	A
Failed to export user enrollment data to a file.	560	-	E
User enrollment data file is imported.	561	-	A
Failed to import user enrollment data file.	562	-	E
Failed to import user enrollment data record.	563	-	E

Level: E = Error, A - Audit, Dt = Details

* Events include a hidden TransactionId parameter in event parameters allowing tracking of a single attended enrollment activity.

Secret Management

Task Category: 768

The following events may be generated during Secret management.

Event	Level		
	ID	Srvr	Clnt
Failure of %1 secure application data consistency check	769	E	E
Failed to delete secure application data	770	E	E
Secure application data deleted	771	A	A
Failure to release secure application data	772	E	E
Secure application data released	773	A	A
Failure of secure application data signature check	774	E	E
Failed to store secure application data	775	E	E
Secure application data stored	776	A	A
Failed to synchronize secure application data	779	E	-
Secure application data is synchronized*	780	A	-

Level: E = Error, A - Audit, Dt = Details

* Event 780 is logged on the Server when Password Manager data, which was modified offline, is synced to the DigitalPersona Server. We allow modification of Password Manager data offline, i.e. when a workstation is not

connected to the server, and then when the workstation is reconnected to the server, the data is synced and this event is logged.

Service Management

Task Category: 1024

The following events may be generated during the management of system operations.

Event	Level		
	ID	Srvr	Clnt
Failed to start DigitalPersona Authentication Service	1029	E	E
DigitalPersona Authentication Service started	1030	A	A
DigitalPersona Authentication Service stopped	1031	A	A
Failed to reset DigitalPersona Authentication Service configuration parameter	1032	A	A
DigitalPersona Authentication Service configuration parameter reset	1033	A	A
Failed to update DigitalPersona Authentication Service configuration parameter	1034	A	A
DigitalPersona Authentication Service configuration parameter updated	1035	A	A
DNS registration of the server failed - Client workstations will not be able to locate the server.	1041	E	-
Removal of DNS record failed.	1042	E	-
Remote DNS server cannot be reached.	1043	E	-
No remote DNS servers available.	1044	E	-

Level: E = Error, A - Audit, Dt = Details

Password Manager

Task Category: 1536

These events are generated when personal or managed logons are used, or logon account data is modified.

Event	Level (Workstation)		
	ID	Personal	Managed
CRC check failure in %1.	1548	Dt	A
Logon created	1549	Dt	A
Logon modified	1550	Dt	A
Logon deleted	1551	Dt	A
Password change has been canceled by user	1552	Dt	Dt
Fillin was performed	1553	Dt	A

Event	ID	Level (Workstation)	
		Personal	Managed
Account data could not be modified	1554	E	E
Account data was successfully modified.	1555	Dt	A
Account data was successfully entered.	1556	Dt	A
Account data was successfully deleted.	1557	Dt	A

Level: E = Error, A - Audit, Dt = Details

Credential Authentication

Task Category: 2048

The following events may be generated during the authentication of credentials.

Event	ID	Level	
		Srvr	Clnt
Account is locked for fingerprint verification.	2051	E	-
User account is locked.	2053	E	-
Authentication failure.	2054	A	-
Authenticated successfully.	2055	Dt	-
User password was reset.	2056	Dt	-
Failed to identify user.	2057	A	-
User identified.	2058	Dt	-

Level: E = Error, A - Audit, Dt = Details

DNS Registration

Task Category: 2304

The following events may be generated during DNS registration.

Event	ID	Level	
		Srvr	Clnt
Registration of the server failed. (Clients will not be able to locate the server.)	2306	E	-
Removal of DNS record failed.	2307	E	-
Remote server cannot be reached.	2308	-	E
No remote servers available.	2309	-	E

Level: E = Error, A - Audit, Dt = Details

Deployment

Task Category: 4096

The following events may be generated during license management operations.

Event	Level		
	ID	Srvr	Clnt
The service is licensed for %1 users. (No more users can be registered at this time because the license quota has been exceeded.)	4097	E	-
The service is licensed for %1 users. (%2 users are already registered.%n The license quota is nearly exceeded.)	4098	A	-
License activation status	4104	-	-
Computer set to Standard mode.	4105	-	A
User license uninstalled.	4112	-	A
User license installed.	4113	-	A
Failed to install user license(s).	4114	-	E
Software installed.	4130	A	-
Software uninstalled.	4131	A	-
List of product(s):	4145	-	-
Applications enabled.	4146	-	-

Level: E = Error, A - Audit, Dt = Details

OTP Management

Task Category: 4358

The following events may be generated during OTP management.

Event	Level		
	ID	Srvr	Clnt
PKSC file is imported.	4359	A	-
Hardware OTP token record is created.	4361	A	-
Level: E = Error, A - Audit, Dt = Details			

Windows Logon

Task Category: 4864

The following events may be generated during Logon operations.

Event	Level		
	ID	Srvr	Clnt
Credentials verified for logon	4865	-	A
Credentials verified for unlock	4866	-	A
Credentials verified for kiosk logon	4867	-	A
Credentials verified for kiosk unlock	4868	-	A
Computer locked	4869	-	A
User (%1) logged off	4870	-	A
Kiosk computer locked	4871	-	A
Kiosk user logged off	4872	-	A
There is a problem with the Kiosk Shared Account	4873	-	E

Level: E = Error, A - Audit, Dt = Details

Authentication Domain Management

Task Category: 2048

These Status events may be generated at specified intervals by selecting *Log Status events* within the *Level of detail in event logs* setting (see page 85). Status events provide information about the state of various policies on client computers.

Event	Level		
	ID	Srvr	Clnt
Logon Policy for Users (Status event)	5649	*	-
Logon Policy for Administrators (Status event)	5650	*	-
Session Policy for Users (Status event)	5651	*	-
Session Policy for Administrators (Status event)	5652	*	-
Logon Policy (Status event)	5653	*	-
Session Policy (Status event)	5654	*	-

Level: E = Error, A - Audit, Dt = Details

* The logging of Status events is not enabled by default, and must be explicitly enabled by selecting the *Log Status Events* checkbox.

THIS CHAPTER DESCRIBES THE UTILITIES PROVIDED WITH YOUR DIGITALPERSONA SERVER

Your DigitalPersona Server includes the following utilities.

Cleanup Wizard

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

DigitalPersona provides the DigitalPersona Cleanup Wizard to remove this data. However, if you are planning to reinstall DigitalPersona AD Server, you may want to retain the user data. The Cleanup Wizard is located in the Server Tools\Cleanup folder of the DigitalPersona AD Server product package.

This wizard provides full cleanup of all DigitalPersona AD data. For removal of individual user data, see *Delete License* on page 56.

Warning: Existing DigitalPersona AD Servers may stop working when the Cleanup Wizard is run.

To run the DigitalPersona Cleanup Wizard

1. Double-click **DPCleanup.exe** to launch the DigitalPersona Cleanup Wizard.
2. When the installer runs, you are prompted to choose the type of cleanup you want to perform:
 - *Delete DigitalPersona user data* - This option removes all DigitalPersona data associated with users on the domain, such as fingerprint credentials and secure application data. If you choose to delete DigitalPersona user data, all users in the domain must enroll their fingerprints again.
 - *Cleanup all DigitalPersona data* - This option removes both DigitalPersona data associated with users on the domain and global data. If you choose this option, you must reinstall all DigitalPersona AD Servers on the domain and run the Active Directory Domain Configuration Wizard again.
3. When prompted to proceed with the removal of DigitalPersona 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 AD Group Policy Objects.

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

Running the DigitalPersona Clean Up Wizard will render all DigitalPersona AD Servers on the domain inoperable. To restore the DigitalPersona AD Server functionality after performing a full cleanup, run the Active Directory Domain Configuration Wizard again, as described in *Configuring each domain* on page 21, and then reinstall the DigitalPersona AD Server.

THIS CHAPTER DESCRIBES STEPS THAT CAN BE FOLLOWED TO DELEGATE PERMISSIONS FOR PERFORMING VARIOUS ADMINISTRATIVE TASKS WITHIN THE DIGITALPERSONA AD ENVIRONMENT.

This chapter includes the following main topics.

Main topics in this chapter	Page
SMS/SMTP Management	128
License management	131
Attended Enrollment	133

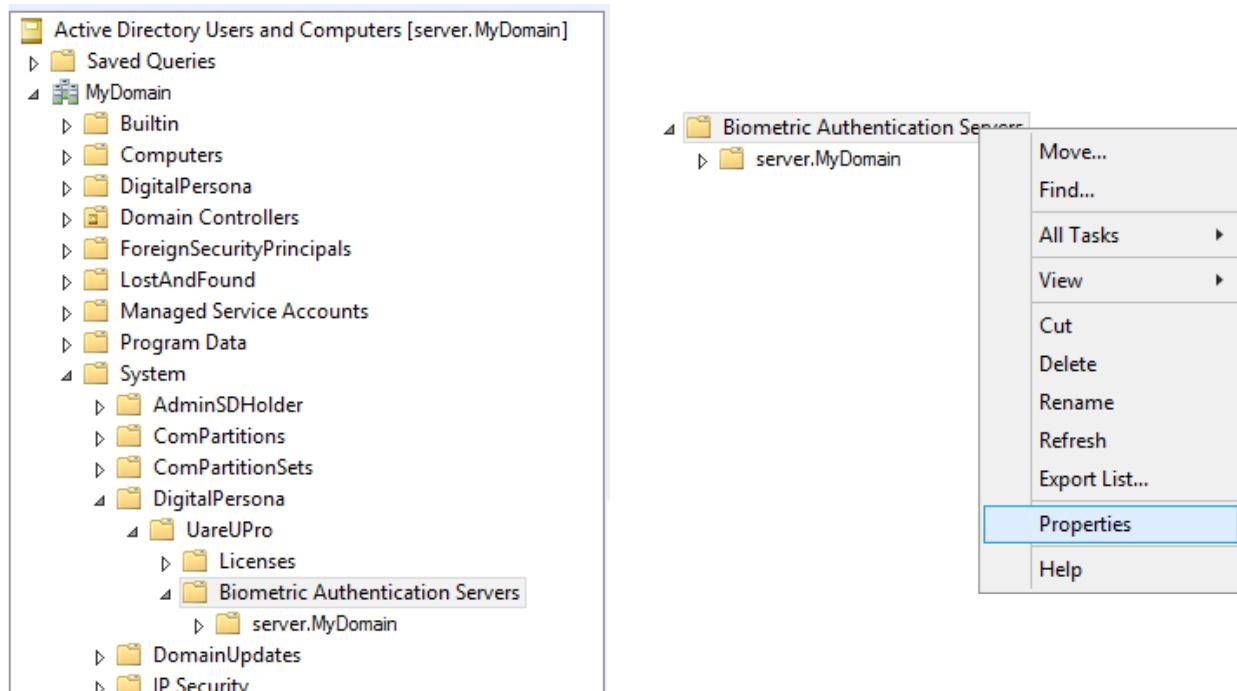
SMS/SMTP Management

In order to manage the SMS or SMTP settings provided through DigitalPersona GPOs, the following permissions can be assigned to a user or group.

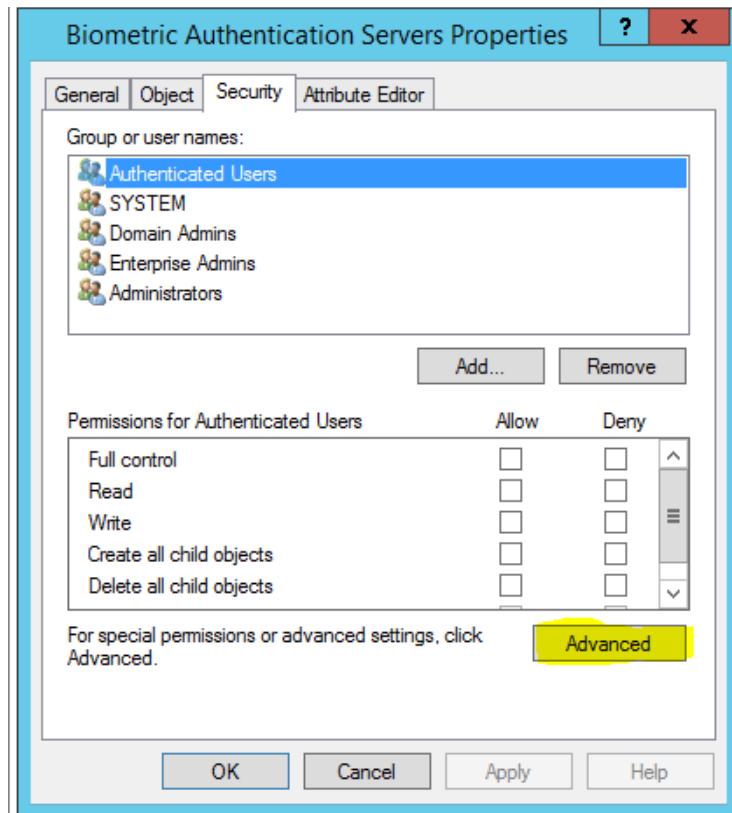
- Read dpServersConfiguration
- Write dpServersConfiguration

Follow the steps given below to add the above permissions to a user or group.

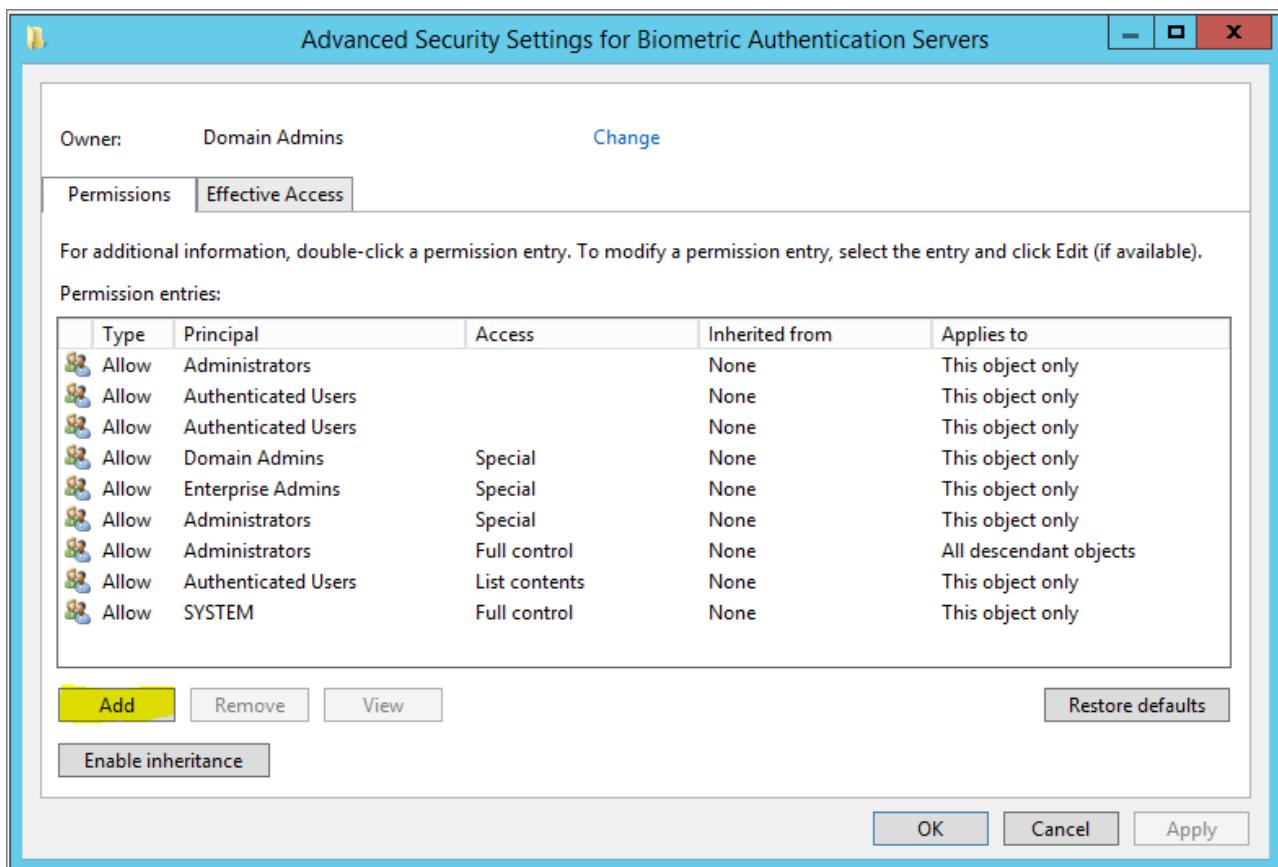
1. Open Active Directory Users and Computers and navigate to the *Biometric Authentication Servers* container.



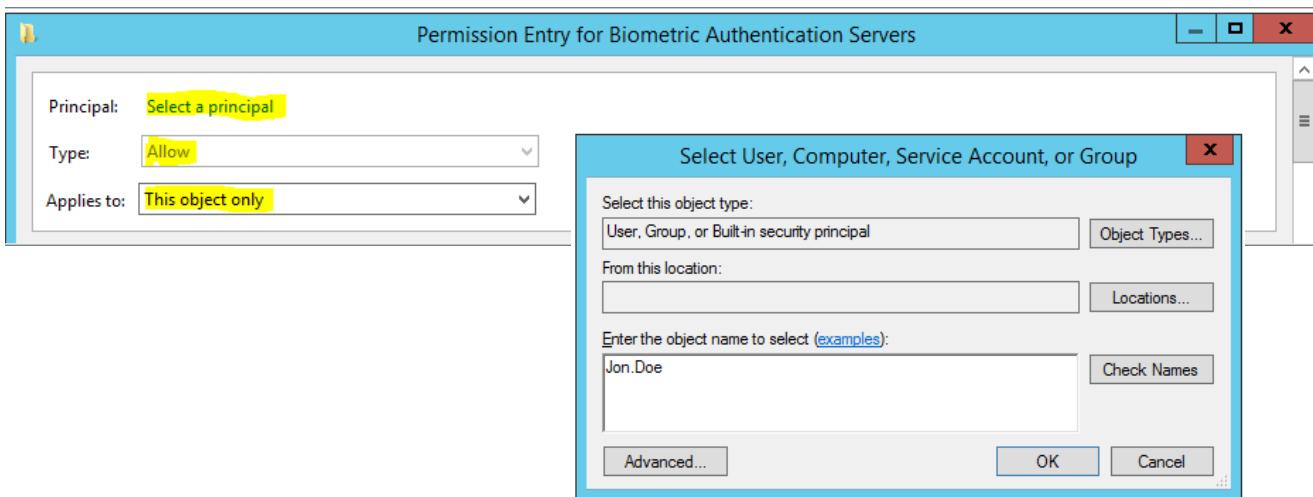
2. Right click on the *Biometric Authentication Servers* container and select *Properties* to display the *Biometric Authentication Servers Properties* dialog.



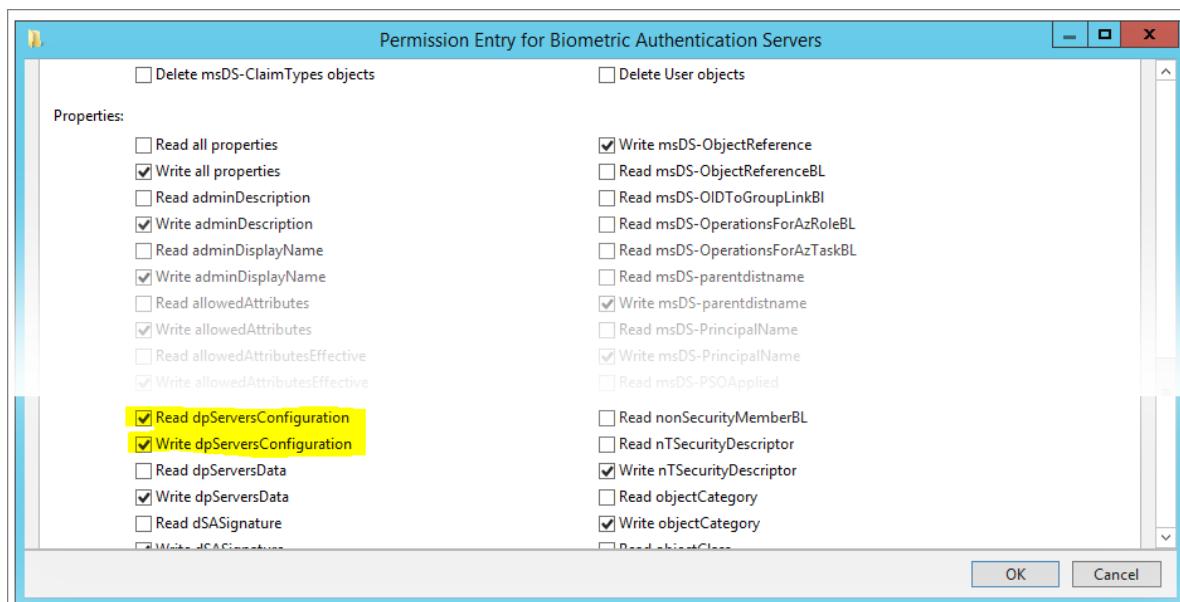
- In the *Biometric Authentication Servers Properties* dialog, select the *Security* tab and click the *Advanced* button to display the *Advanced Security Settings for Biometric Authentication Servers* dialog.



4. In the *Advanced Security Settings for Biometric Authentication Servers* dialog, click *Add* to display the *Permission Entry for Biometric Authentication Servers* dialog.



5. In the *Permission Entry for Biometric Authentication Servers* dialog, click *Select a principal*.
6. Enter the User, Group or Built-in security principal that you want to delegate SMS setting management to. Click *Check Names* and then click *OK* to close the dialog and return to the previous screen.
7. Ensure that the *Type* is *Allow* and the *Applies to* value is *This object only*.
8. In the lower portion of the *Permission Entry for Biometric Authentication Servers* dialog, scroll down to and select the following properties.
- Read dpServersConfiguration
 - Write dpServersConfiguration



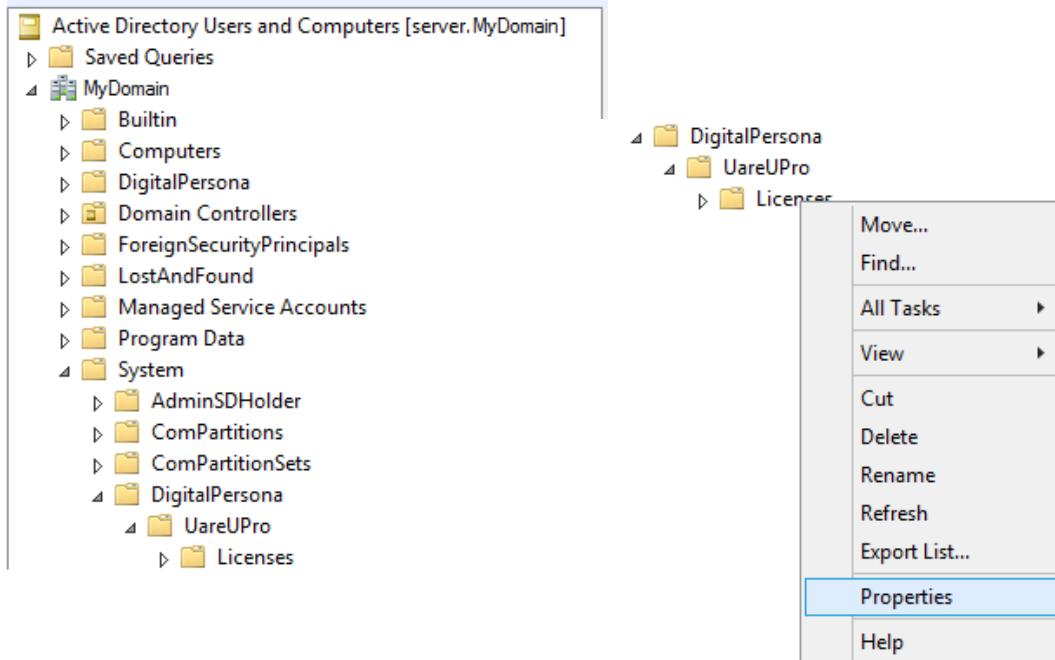
Click *OK* to apply the permissions and close the dialog.

License management

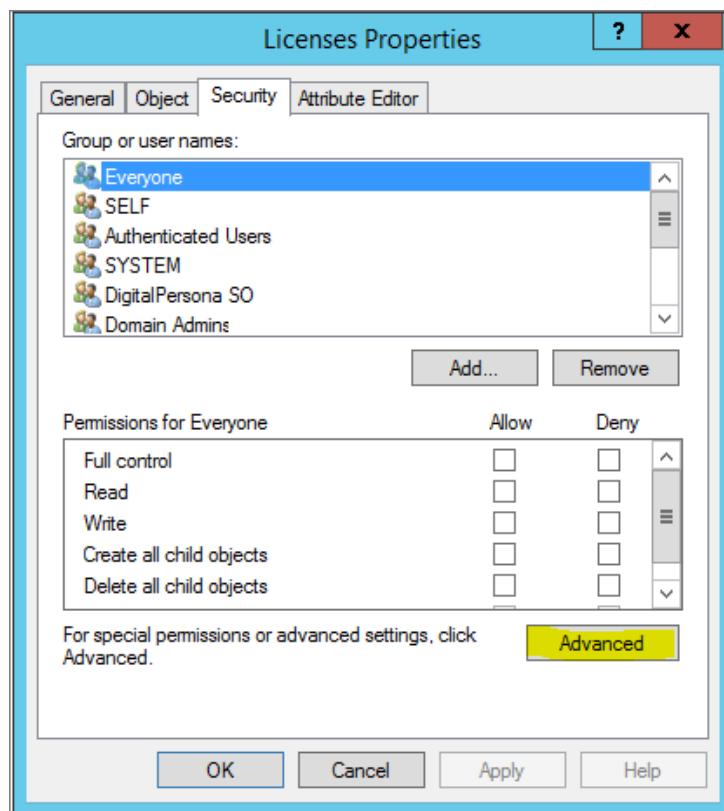
In order to view and manage DigitalPersona Licenses, grant *Full Control* of the ADUC *Licenses* container to the User, Group or Built-in security principal that you want to manage your DigitalPersona licenses.

Follow the steps given below to grant the required permission to a User, Group or Built-in security principal.

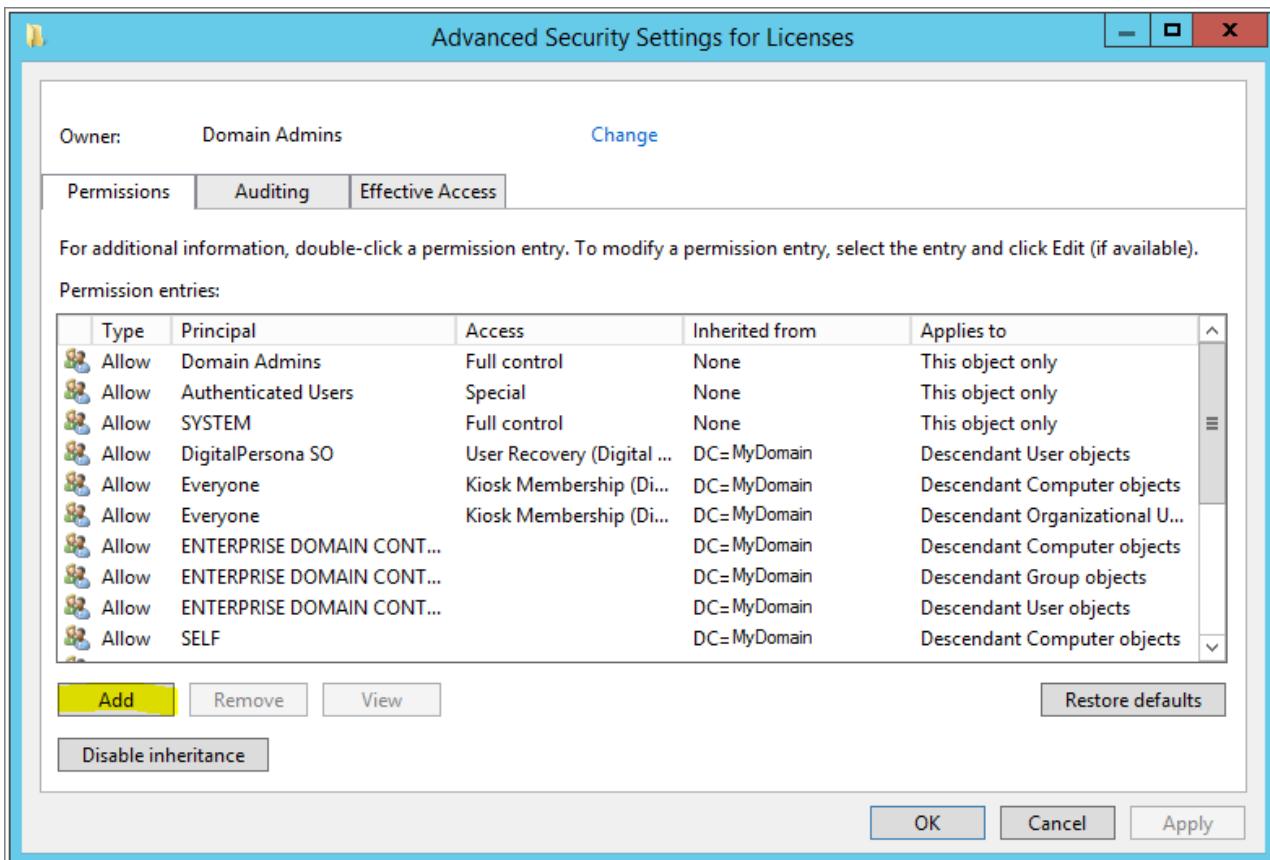
1. Open Active Directory Users and Computers and navigate to the *Licenses* container.



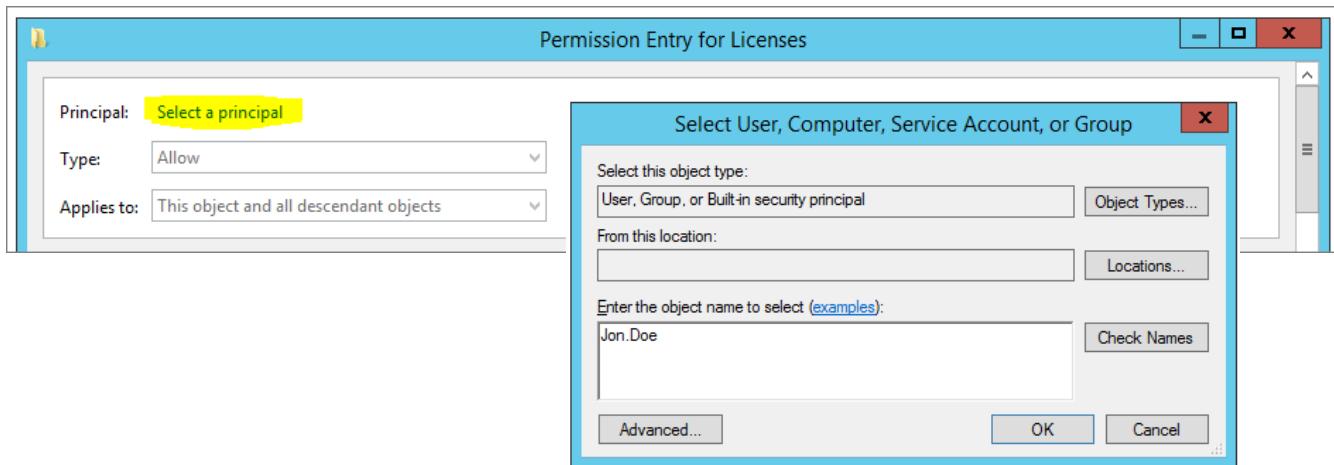
2. Right click on the *Licenses* container and select *Properties* to display the *Licenses Properties* dialog.



3. In the *Licenses Properties* dialog, select the *Security* tab and click the *Advanced* button to display the *Advanced Security Settings for Licenses* dialog.

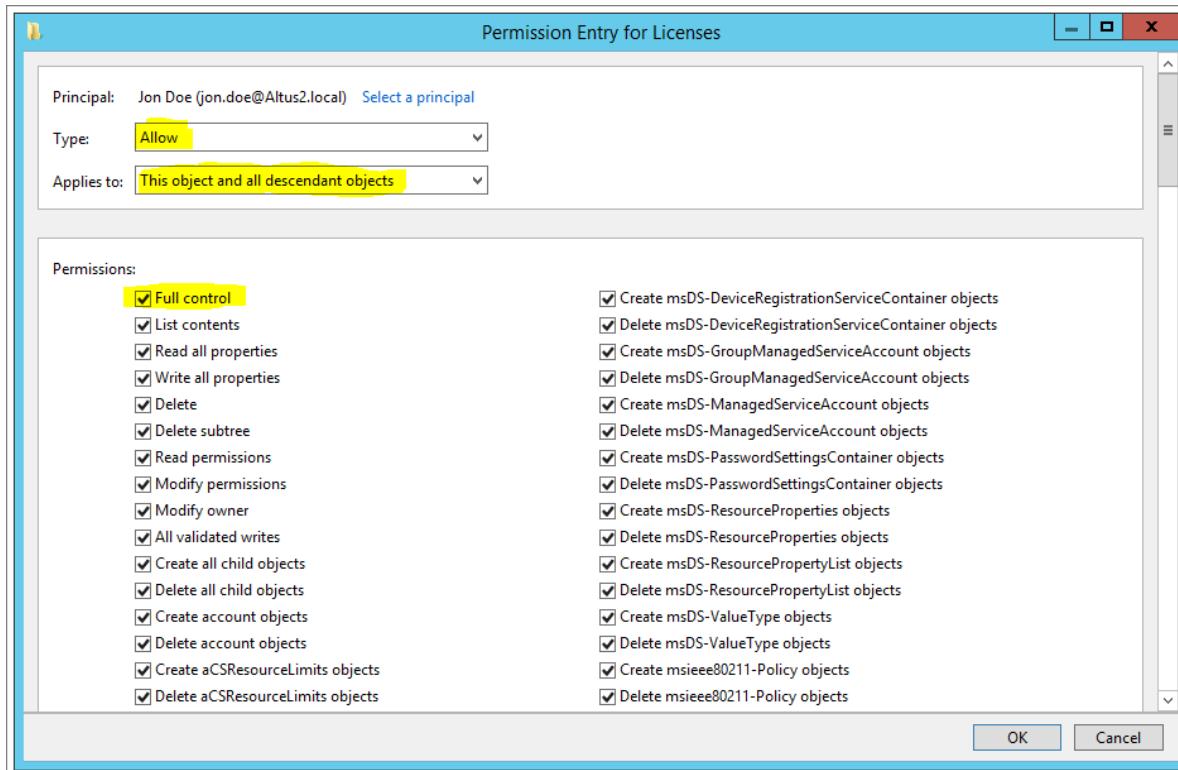


4. In the *Advanced Security Settings for Licenses* dialog, click *Add* to display the *Permission Entry for Licenses* dialog.



5. In the *Permission Entry for Licenses* dialog, click *Select a principal*.
6. Enter the User, Group or Built-in security principal that you want to delegate License management to. Click *Check Names* and then click *OK* to close the dialog and return to the previous screen.
7. Ensure that the *Type* is *Allow* and the *Applies to* value is *This object and all descendant objects*.

8. In the lower portion of the *Permission Entry for Licenses* dialog, select *Full Control*.



9. Click *OK* to apply the permissions and close the dialog.

Attended Enrollment

For instructions on delegating responsibility for Attended Enrollment, see the chapter *Attended Enrollment* beginning on page 94.

THIS CHAPTER DESCRIBES THE PASSWORD MANAGER ADMIN TOOL, AN OPTIONAL COMPONENT OF DIGITALPERSONA COMPOSITE AUTHENTICATION PREMIUM THAT ADMINISTRATORS CAN USE TO CREATE MANAGED LOGONS FOR WEBSITES, PROGRAMS AND NETWORK RESOURCES.

Main topics in this chapter	Page
Overview	116
System requirements	135
Setting up the Password Manager Admin Tool	135
Using Managed logons	137
Creating managed logons	137
Creating logons manually	145
Deploying managed logons	146
Creating an extended authentication policy	148
Setting Up a Change Password screen	149
Setting up a Change Password Screen manually	154
Regular Expression syntax	156
Managing logons	158
The Field Catalog	160
Tools page	161

The Password Manager Admin Tool enables administrators to provide controlled access to websites, programs and network resources by adding a variety of authentication mechanisms (such as password, smart/proximity/contactless card or fingerprint) to their logon and change password screens. The DigitalPersona Password Manager Admin Tool is an optional DigitalPersona component, which may be part of your purchased product package, or can be acquired separately through Crossmatch or your authorized reseller.

Overview

Setting up a managed logon screen is as simple as specifying attributes (such as the user name, password, the submit button and other required fields) in a logon for the website or program. The DigitalPersona Password Manager Admin Tool also provides many configurable options for defining and reusing information for logon and change password screens.

The change password process can also be automated and controlled, by specifying constraints such as the minimum and maximum password length, letters or numbers only, and other format restrictions.

These managed logons can then be automatically deployed to computers where the Password Manager application is installed and which are being managed by a DigitalPersona Server.

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

- The Password Manager icon displays on screens that have had managed logons created for them.
- The user is guided through the process of logging on or changing their password.



Each time that a user accesses the “trained” website, program or network resource, the Password Manager icon shown below is displayed in the upper left corner of the screen (Internet Explorer) or to the right of the first recognized entry field (Chrome), indicating that they can use any of their enrolled credentials to log on.



Password Manager Icon for Internet Explorer



Password Manager Icon for Internet Explorer as displayed on Change Password screens



Password Manager Icon for Chrome



Password Manager Icon for Chrome as displayed on Change Password screens

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

System requirements

Installation of the DigitalPersona Password Manager Admin Tool requires the previous installation of a DigitalPersona Workstation client and the DigitalPersona Password Manager application. (Versions of the DigitalPersona Workstation client prior to 2.0.3 include the Password Manager application.)

Although Microsoft Internet Explorer is not required prior to installation, it is required in order to create managed logons with the tool. They cannot be created using other browsers.

Installation & setup

To install the DigitalPersona Password Manager Admin Tool

1. Locate and launch the setup.exe located in the *Password Manager Admin Tool* folder within the software package you were provided.
2. Follow the onscreen instructions.
3. Once installation is complete, set up the tool by following the instructions in the next topic.

Setting up the Password Manager Admin Tool

Before using the Password Manager Admin Tool, you will need to set it up.

Managed logons are organized in shared folders created and maintained through the DigitalPersona Password Manager Admin Tool.

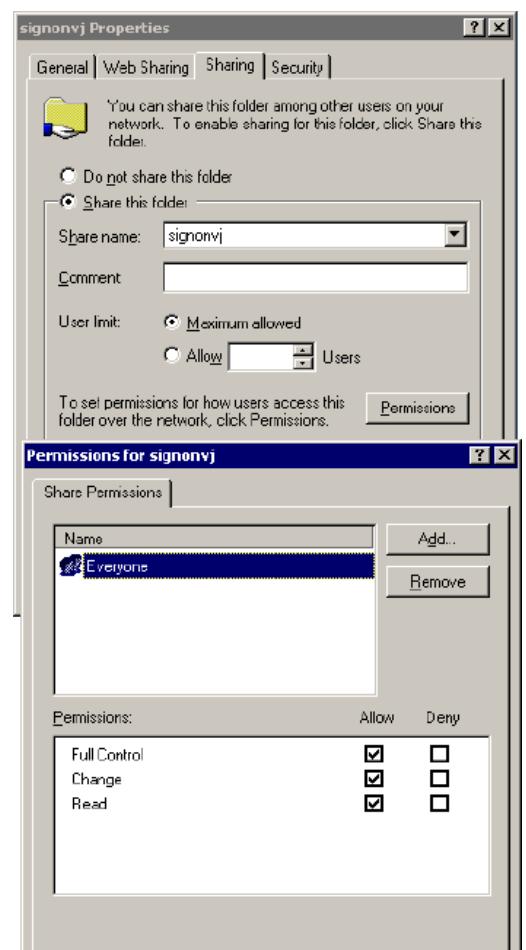
The folder should be created on a shared network drive accessible to the DigitalPersona server in order to make the logons available for deployment. However, the folder may be created on a local drive for initial testing and later copied to a shared drive. Folders are created and managed from the Logons tab in the Password Manager Admin Tool.

Create a shared network folder

Create a shared folder on the network drive to store the Password Manager Admin Tool managed logons and then assign appropriate permissions to the folder's users.

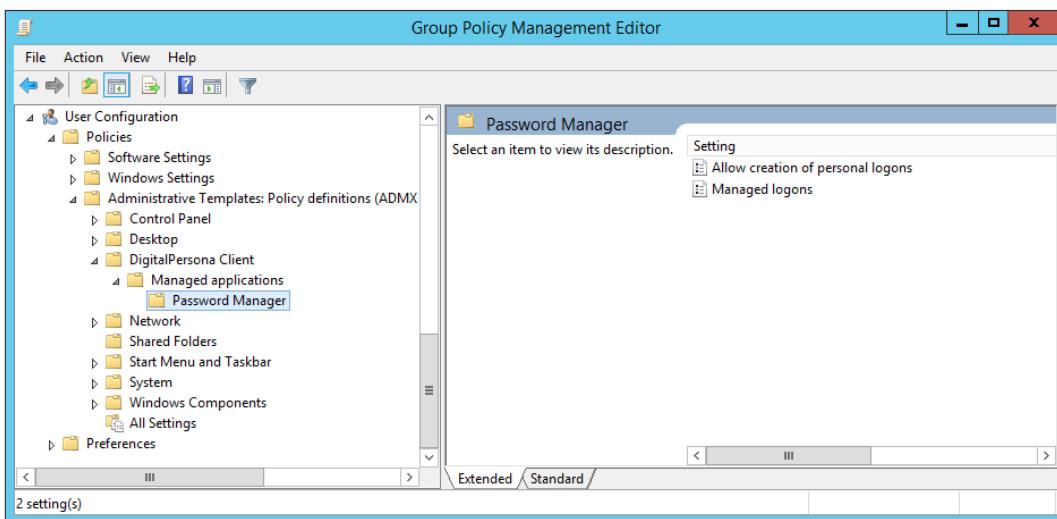
The folder should be created on a shared network drive accessible to the DigitalPersona Server in order to make the logons available for deployment. However, the folder may instead be created on a local drive for initial testing and then later copied to a shared drive.

1. Create a folder on the server/computer where you will store the managed logons.
2. Share the folder that you just created to allow users to access it.
3. Right click on the folder and click on *Properties* in the context menu.
4. Click on the *Sharing* tab.
5. Verify the permissions by clicking on the *Permissions* button.



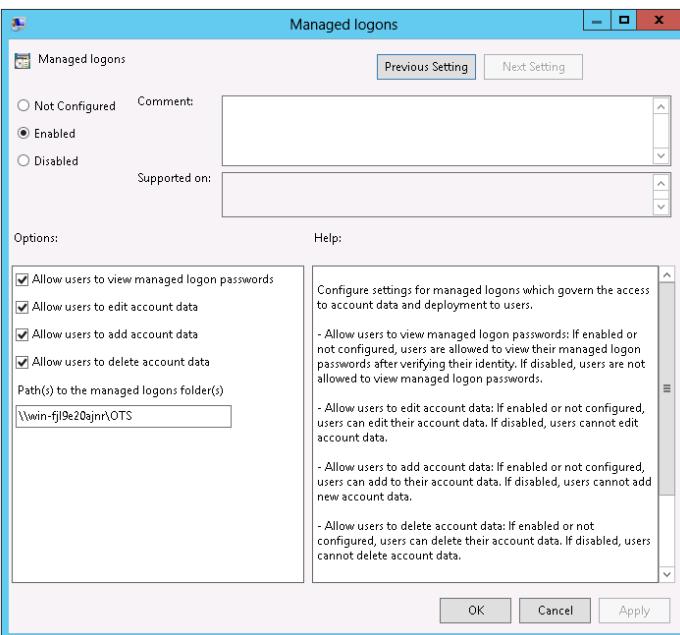
Set up the GPO policy

1. The Workstation Administrative Template, DPAltusClient (admx/adm) file must be added to the Active Directory Computer Configuration folder in the Administrative Templates folder of the Group Policy Management Editor. For further details on administrative templates, see the chapter *Install the Administrative Templates* in your DigitalPersona Administrator Guide.
2. Open the GPO where the DigitalPersona template was added.
3. Go to User Configuration\Administrative Templates\DigitalPersona Client>Password Manager.



4. Double click on *Managed logons* (in the right pane).

- Click on *Enabled* to enable this policy. The default setting is "Not Configured."



- Specify the path to the shared folder that you created in the previous section. To specify multiple folders, you can use the pipe (|) character.
- The new setting will be applied to all DigitalPersona clients during the usual refresh interval or the next time they restart Windows.

Using Managed logons

Managed logons are used to store attributes such as the user name, password, the submit button, and other required fields and screen information for Logon and Change Password screens.

These managed logons are stored in a shared folder specified in a GPO setting in Active Directory. From there they can be deployed to specific groups of users managed by the server. Users of the companion product, Password Manager, on computers managed by DigitalPersona, will then automatically have access to the managed logons.

- Managed logons are downloaded to client computers as soon as they are set up to be managed, and at intervals specified by the administrator.
- Note that credentials entered by the user for a website or program do not roam on the network, and are only available on the computer where they were entered.
- When users connect to the domain through a VPN, there will be a period of 30 minutes from their login to the current Windows session before their managed logons will be shown on the Managed Logons tab of the DigitalPersona Console, Password Manager page. They must be connected to the domain (through VPN) before the 30 minutes is up in order to gain access to their managed logons.

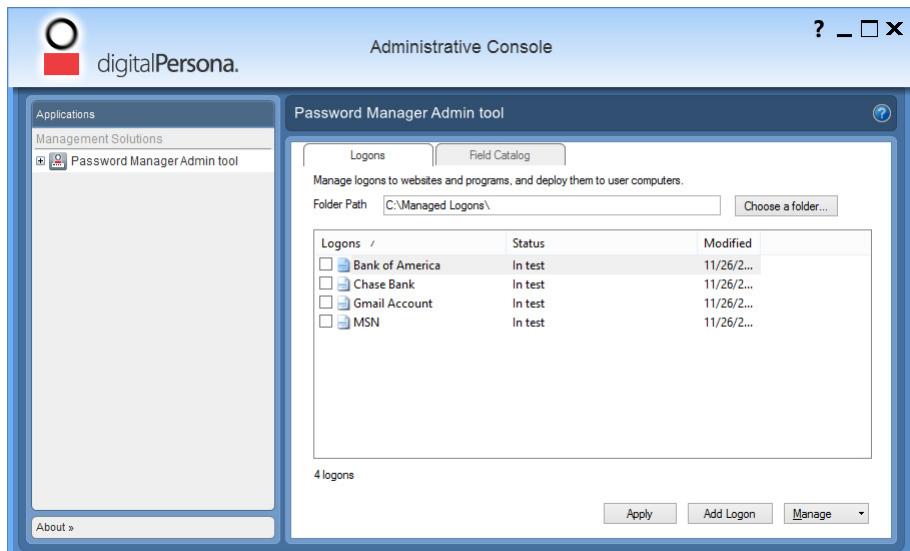
The Password Manager Admin Tool includes intuitive wizards that will guide you through the few steps necessary to automatically create a managed logon and an optional change password screen for most websites and programs. For more complex screens, there is also a manual mode that provides more sophisticated options for matching the logon or change password process to non-standard screens.

Creating managed logons

Password Manager Admin Tool managed logons are used to store attributes such as the user name, password, the submit button, and other required fields and screen information for Logon and Change Password screens.

To create a managed logon for a logon screen:

1. Launch the Password Manager Admin Tool. The following screen displays.

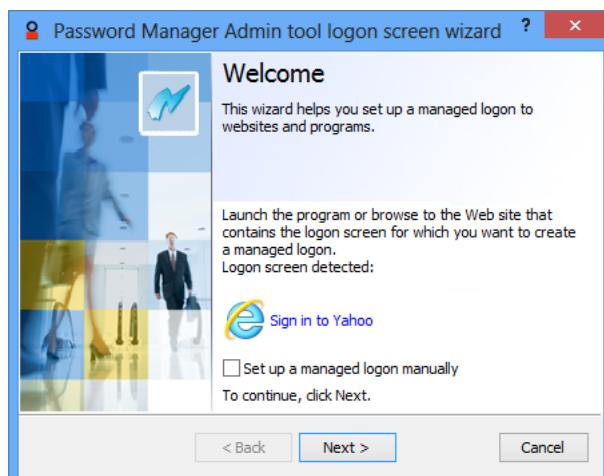


2. On the Logons tab, select *Choose a folder*.
3. In the *Choose a folder* dialog, select a previously created folder, or specify a path to a folder. Or choose *Browse for folder* to navigate to a folder or create a new one. This can be a local folder for testing, or a shared network folder where managed logons are made available to DigitalPersona Workstation or Kiosk users. Then click *Choose*.
4. Click *Add Logon*. The Password Manager Admin Tool Logon Screen wizard launches.
5. Launch the logon screen for the password-protected website or program.

Troubleshooting tip - If an error message *No input fields* displays in the wizard, it may indicate that you are inadvertently attempting to create a logon from a Windows session other than the one where the Password Manager Admin Tool is running. For example, right-clicking on an application and selecting the *Run as different user* option would run the application in a separate Windows session where it could not be accessed by the Password Admin Tool.

A resource used to create the logon must be in the same Windows session that the Password Manager Admin Tool is running in. So, when creating logons for applications that require elevated privileges (i.e. such as Domain Admin), they must be created in a Windows session where the logged on user has the same, or higher, privileges.

6. On the first page of the wizard, confirm that the logon screen has been detected and verify the title of the logon screen. Click *Next*.

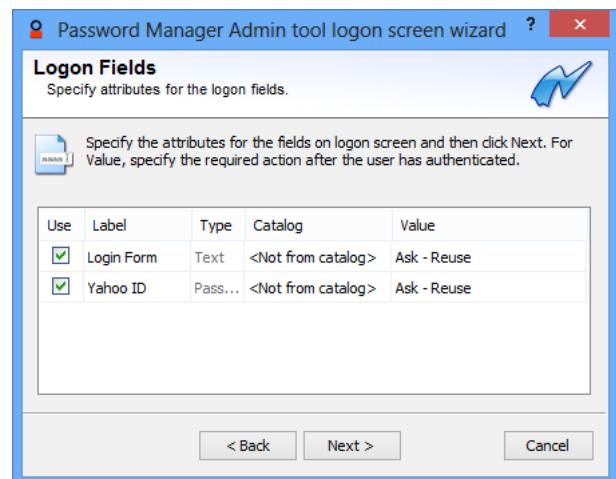
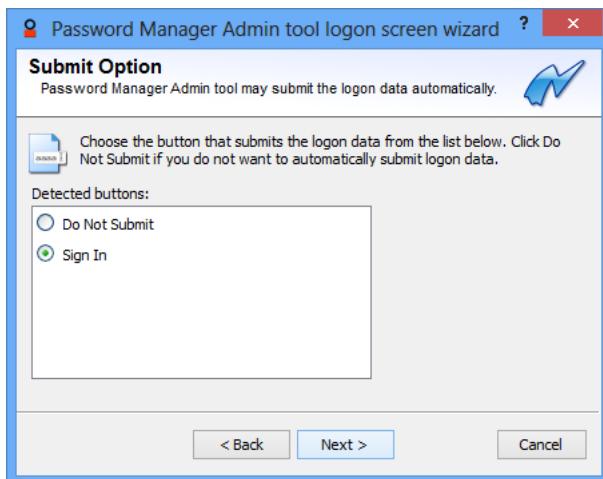


For websites or programs that are difficult for the wizard to detect automatically, such as terminal emulator programs, you can create a logon manually by selecting *Set up a managed logon manually*. This provides additional control for specifying the fields and keystrokes required for logon. Further details on manual creation can be found at *Creating logons manually on page 145*.

- The *Logon Fields* page displays all the fields on the logon screen, using the nearest label to identify each field.

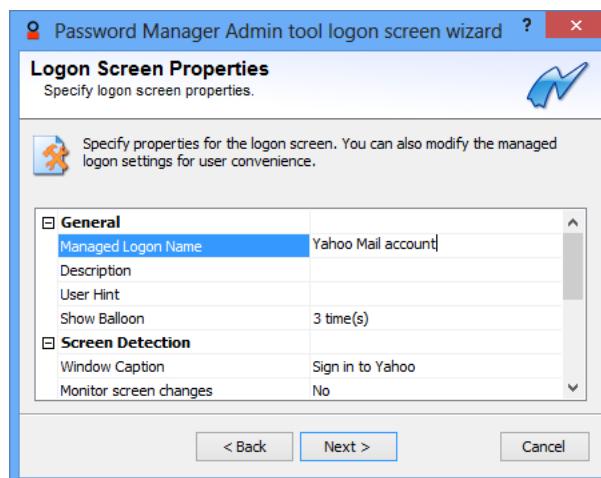
Select which fields are required for logon, set their desired attributes (see page - 140) and values (see page - 141) and then click *Next*.

- On the *Submit Option* page, choose the button that submits the logon data.



- You can edit the button labels by clicking the label and typing a new name.
- If you want the user to manually submit the logon data, select Do Not Submit.

- Click *Next* to display the *Logon Screen Properties* page, where you can view and modify the various properties (see page - 142) for detailed descriptions of the Logon Screen properties.

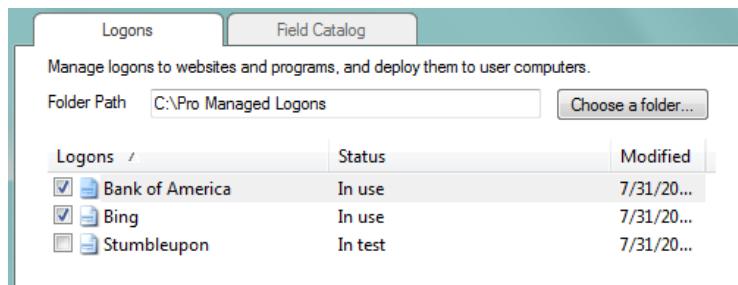


- Click *Next*, and then click *Finish* to create the logon and close the wizard.
- In the Administrative Console's Logon tab, click *Apply* to save your changes to the server.

You do not have to click *Apply* after making *each* change, but be aware that you *do* need to click *Apply* before any new logons or changes to logons will be saved to the server.

To deploy managed logons:

1. Check the boxes next to logons to change their status from In Test to In Use. Only logons with an "In Use" status will be visible to your end-users.



2. Click *Apply*.
3. After a managed logon is deployed to a computer, the Password Manager icon on the user's screen indicates that the user should add their account credentials to the logon. Afterwards, any time the user launches the resource, they can log in by simply verifying their identity with any enrolled credential.

Notes:

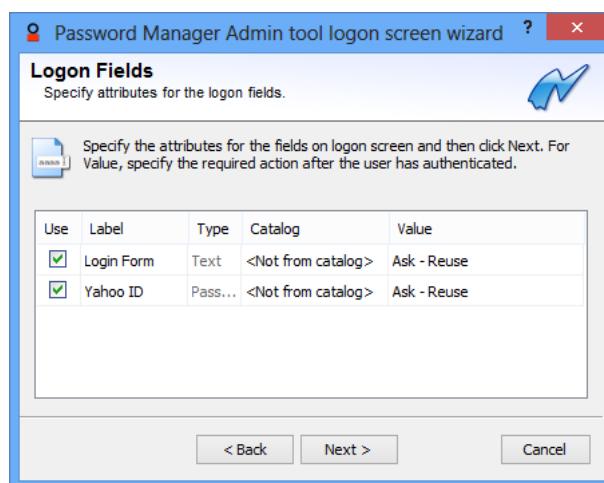
Logons created by the administrator (also called *managed* logons) take precedence over any personal logons created for the same screen by the application. The personal logon will no longer be able to be used to log on, but can be opened from the *Personal tab* by right-clicking the logon and selecting *Edit* (or selecting the logon and then choosing *Edit* from the *Manage* button) in order to retrieve your account information.

If more than one administrator is using the Password Manager Admin Tool at the same time, they should make sure not to make changes to logons at the same time, as only the last applied changes will be deployed.

See Also: [Creating logons manually](#) on page 145.

Logon Fields attributes

Logon Fields attributes are used in the Logon Screen Wizard during the creation of managed logons and Change Password screens.

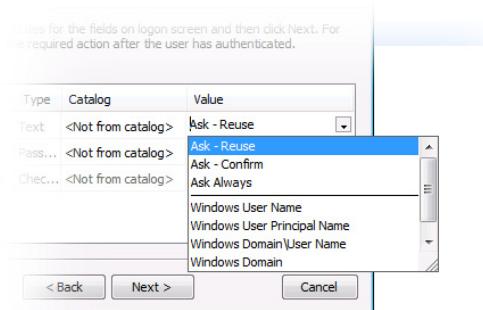


Column headings specify the attributes for each field on a Logon Screen or Change Password screen.

Field	Description
Use	Check the <i>Use</i> checkbox 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 website logon page. Leave these unchecked.
Label	If the label for a field shown on the Login Credentials dialog is not intuitively related to the corresponding field on the logon screen, you can type a new label. 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. <i>Password</i> hides the password on the logon screen so it cannot be viewed. <i>Text</i> displays readable text.
Catalog	For added convenience, you can create specifications for frequently used fields using the Field Catalog tab. The Field Catalog is a collection of frequently-used fields and their specifications. If the field is in the Field Catalog, you can click and then choose it from the dropdown list. The specified data will be filled in automatically. To add a field to the Field Catalog, see page 160.
Value	Type a value for the logon field or use the Value dropdown menu (see next section) to indicate a value specified by the user or provided by the program. A typed value is stored in the logon in clear (unencrypted) text and is shared by all of those using the logon.

Values

Logon Field and Password Field values are used on the Logon Fields page of the Logon Screen Wizard during the creation of managed logons and Change Password screens.



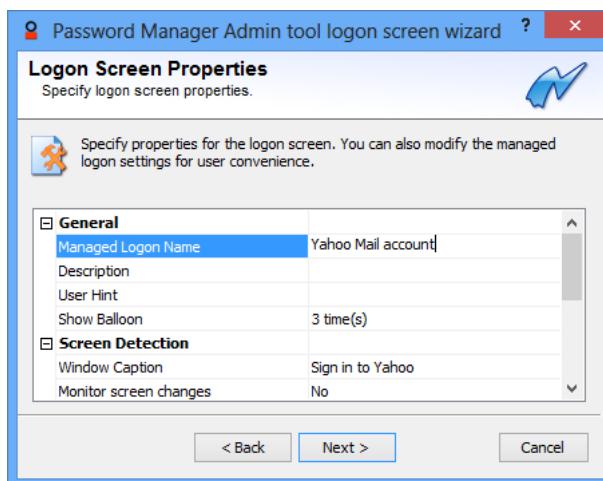
A Value dropdown menu provides a list of options for specifying values to be supplied by the user or automatically by Password Manager. The available options vary depending on the type of field selected.

Option	Description
Ask-Reuse	Prompts the user to enter a value for a logon field the first time they use the logon. This value is automatically submitted for them on each subsequent logon without prompting the user again.
Ask-Confirm	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.

Option	Description
Ask Always	Prompts the user to enter a value for a logon field each time they use the logon.
Windows User Name	Password Manager provides the Windows user name.
Windows User Principal Name	Password Manager provides the user name and domain values in UPN format. Example: [user name]@[domain].
Windows Domain\ User Name	Password Manager provides the domain of the user followed by a backslash and the user name. Example: [domain]\[user name].
Windows Domain	Password Manager provides the user domain name only.
Windows E-Mail Address	Password Manager provides the registered E-Mail address for the Windows user account currently logged on.
Windows User Password	Password Manager provides the password used for Windows logon.
Write Only	Always prompts a user for the value.

Logon properties

In the Logon Screen Wizard, both Logon Screens and Change Passwords Screens have associated Properties pages where you can edit the properties for the screen.



Category	Property	Description
General	Managed Logon Name	The name of the logon.
	Description	Can be used to enter optional information about the managed logon that is only viewable on the Password Manager Admin Tool Logons tab. By default, this column is hidden. To display the column, right click anywhere in the column headings area and select <i>Description</i> .

Category	Property	Description
	User Hint	Type a message to be displayed when the managed logon is used. For example, a custom prompt to type values for the logon fields. To add more detailed user assistance, type a URL that a user can click to be directed to a web page.
	Show Balloon	(Logon screens only) Once this managed logon is created and deployed, a balloon tip will automatically display (up to three times) when the user accesses the logon screen. Use this setting to select how many times the balloon is displayed.
Screen Detection	Window Caption	<p>Title of the screen as detected by the wizard; used to match the managed logon to the specified screen.</p> <p>If portions of the window caption will change, you can use wildcards (*) at the beginning, middle or end of the caption. Only one wildcard can be used per caption. The portion of the string that does not change will be used to recognize the screen.</p> <p>For example:</p> <ul style="list-style-type: none"> *Some Application Login Some Company*Login My Bank Login*
	Monitor screen changes	<p>When enabled, Password Manager continually monitors the title bar, URL and content of the specified web page for changes that may affect the logon. When disabled, only the title bar and the URL are monitored.</p> <p>For example, if a page were using frames, and a link in one frame changes another frame in the page in such a way that it changes to a logon page, with this setting on, the change is recognized and appropriate action taken. With the setting disabled, the change would not be recognized.</p> <p>Use of this setting is resource intensive, and it is disabled by default.</p>

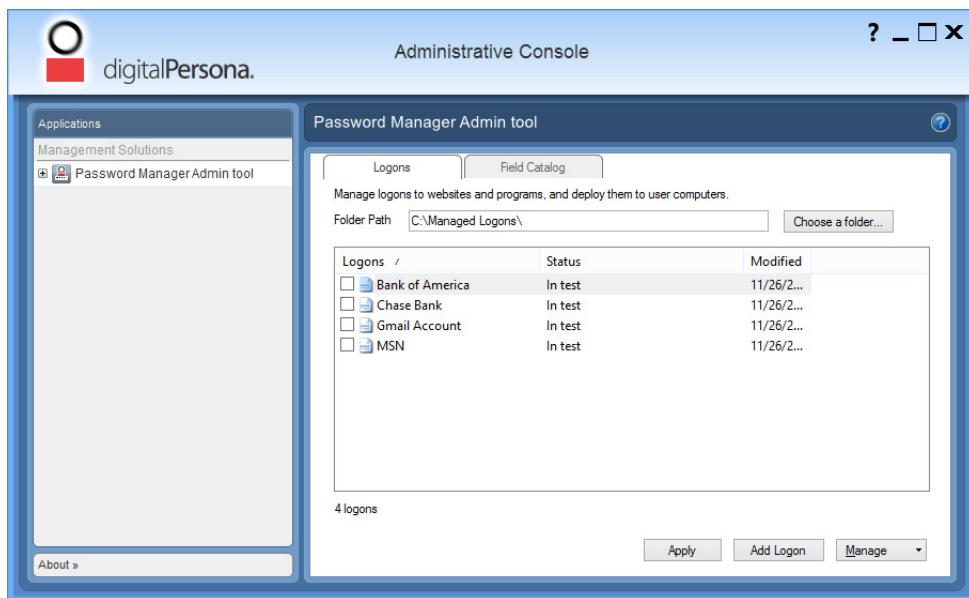
Category	Property	Description
	URL	<p>Used by Password Manager to recognize a website screen. The URL information in the logon is matched to the URL in the screen. If multiple websites have the same title or if portions of the URL change, which can be the case for websites that redirect traffic for load balancing, then specify the portion of the URL to match. The dropdown menu allows you to specify the type of matching to perform on the URL. The options are:</p> <p><i>Do Not Match</i> - This is the default. URL matching will not be performed.</p> <p><i>String Match</i> - Matches the exact string displayed.</p> <p><i>Wildcard Match</i> - Matches a displayed string utilizing an asterisk (*) to represent the portion of the URL that may change.</p> <p><i>Regular Expression</i> - Matches a displayed string constructed as a regular expression (See “Regular Expression syntax” on page 156).</p> <p><i>Case Sensitive</i> - Ignore case when matching.</p> <p><i>Restore Defaults</i> - Return to the default URL settings.</p>
	Extended Match	<p>Displayed only when creating a logon for a program, not a website.</p> <p>Click the button next to the <i>Extended Match</i> field and select any labels that should be used for matching when recognizing the screen. Click the checkbox next to the labels to use.</p> <p>After making selections and clicking <i>OK</i>, you can select the type of matching to perform by selecting it from the dropdown list. The options are the same as those listed above for the URL.</p>
Authentication	Start Authentication Immediately	If set to <i>Yes</i> , the user is prompted for their credential immediately after the logon screen displays. The default setting is <i>No</i> .
	Lock out logon fields	If set to <i>Yes</i> , the user is prevented from typing data in the logon fields. The default setting is <i>No</i> .
Password Manager icon	Location ID	Identifies the location selected in the Location field (below) so that it can be shared with other logon screens.
	Location	From the dropdown menu, select the initial location where the Password Manager icon will appear on the logon screen. The default is the top left corner of the screen.

Creating logons manually

If the Password Manager Admin Tool does not detect fields automatically in websites and programs, you can create a managed logon for a logon screen by manually specifying the fields. Creating logons manually can include using additional controls besides specifying fields and field contents, such as adding keystrokes, forcing delays between actions, and specifying the positions of fields.

To create a logon manually for a logon screen:

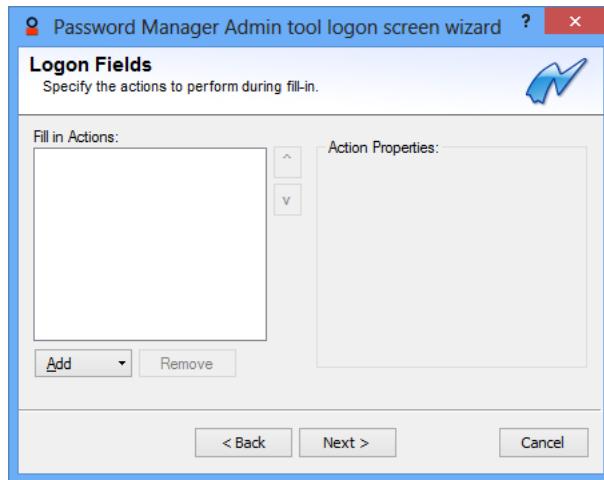
- From within the Administrative Console, launch the Password Manager Admin Tool.



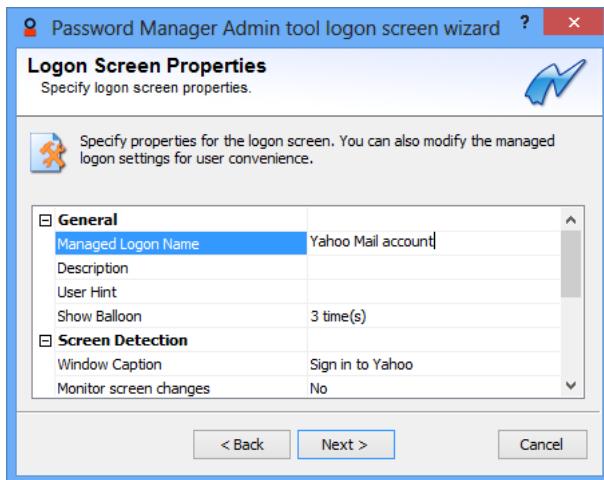
- On the Logons tab, select *Choose a folder*. Click one of the recently used locations, or specify a path and click *Browse for folder* to add a folder to the list. Then click *Choose*.
- Click *Add Logon*. The Password Manager Admin Tool Logon wizard starts.
- Launch the logon screen for the password-protected website or program.
- On the first page of the wizard, confirm that the logon screen has been detected and verify the title of the logon screen.
- Select *Set up a managed logon manually* and then click *Next*.



7. On the *Logon Fields* page, click *Add* and select an action (see page 147) from the dropdown menu.



8. Add additional actions as required. If necessary, use the arrow buttons to modify the order in which the actions are performed.
9. Click **Next** to display the *Logon Screen Properties* page, where you can view and modify the various properties (page - 142) for the logon screen.



10. Click *Next*, and then click *Finish* to create the logon and close the wizard.

11. In the Administrative Console's Logon tab, click *Apply* to save your changes to the server.

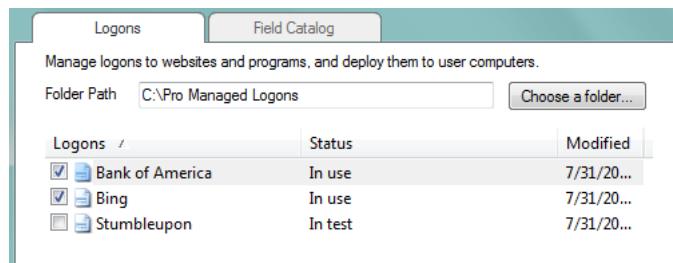
You do not have to click *Apply* after creating *each* logon or making every change, but you do need to click *Apply* before any new logons or changes to logons will be saved to the server.

See Also: Creating managed logons on page 137.

Deploying managed logons

To deploy managed logons:

1. Check the boxes next to logons to change their status from In Test to In Use. Only logons with an "In Use" status will be visible to users.

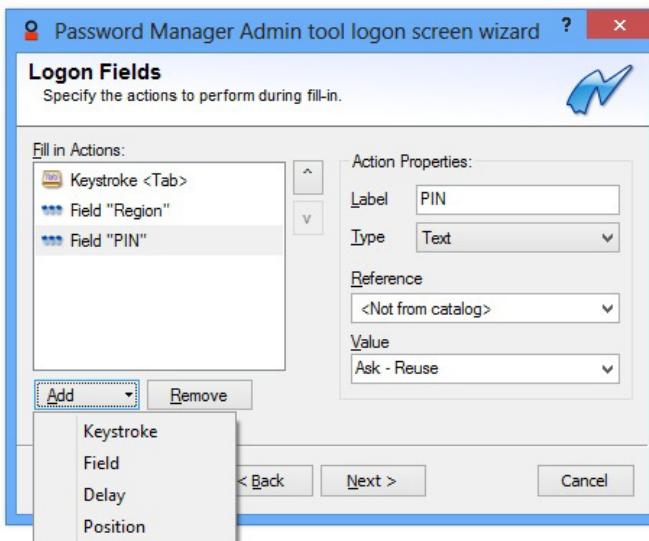


2. Click *Apply*.

After a managed logon is deployed to a computer, the Password Manager icon on the screen indicates to the user that they can add their account data to the logon. Afterwards, they will be able to automatically fill in their credentials simply by verifying their identity with any enrolled credential.

Logon Fields actions

Logon Fields actions are used when creating logons manually in the the Password Manager Admin Tool Logon Screen Wizard and the the Password Manager Admin Tool Change Password Screen Wizard.



An Actions dropdown menu provides a list of actions that are used to build a script for those logon and change password screens that cannot be automatically configured by the Password Manager Admin Tool.

Action	Description
Keystroke	This sequence of keys will be placed in the keyboard buffer. Keystroke properties are: Key - Select the main key to be entered. Repeat - Specify the number of times the key sequence is entered. Shift, Control, Alt - Optionally, select one of these keys in combination with the main key. You may specify the exact use of a Generic , Left or Right key as well.

Action	Description
Field	<p>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.</p> <p>Type - Select the type of field, either text or password. Choosing password hides the password on the logon screen; choosing text displays readable text.</p> <p>Reference - Optionally, select a field previously defined on the Field Catalog tab.</p> <p>Value - Type a value for the logon field or use the dropdown menu to indicate a value specified by the user or provided by the program. If you type a value for the logon field, it is stored in the logon in clear (unencrypted) text and is shared by all users using the logon.</p>
Delay	Specify how many seconds to wait before the next action in the list is performed.
Position	<p>Specify a location where the system will perform a mouse click. Position is measured from the top left corner of the client window area.</p> <p>Client X - Type a number of pixels for the X axis position for the action.</p> <p>Client Y - Type a number of pixels for the Y axis position for the action.</p> <p> Instead of typing X and Y coordinates, you can drag the target icon to the actual logon screen field to specify the position. When you release the target icon at the location you want to specify, the Client X and Y positions will be captured.</p>

Creating an extended authentication policy

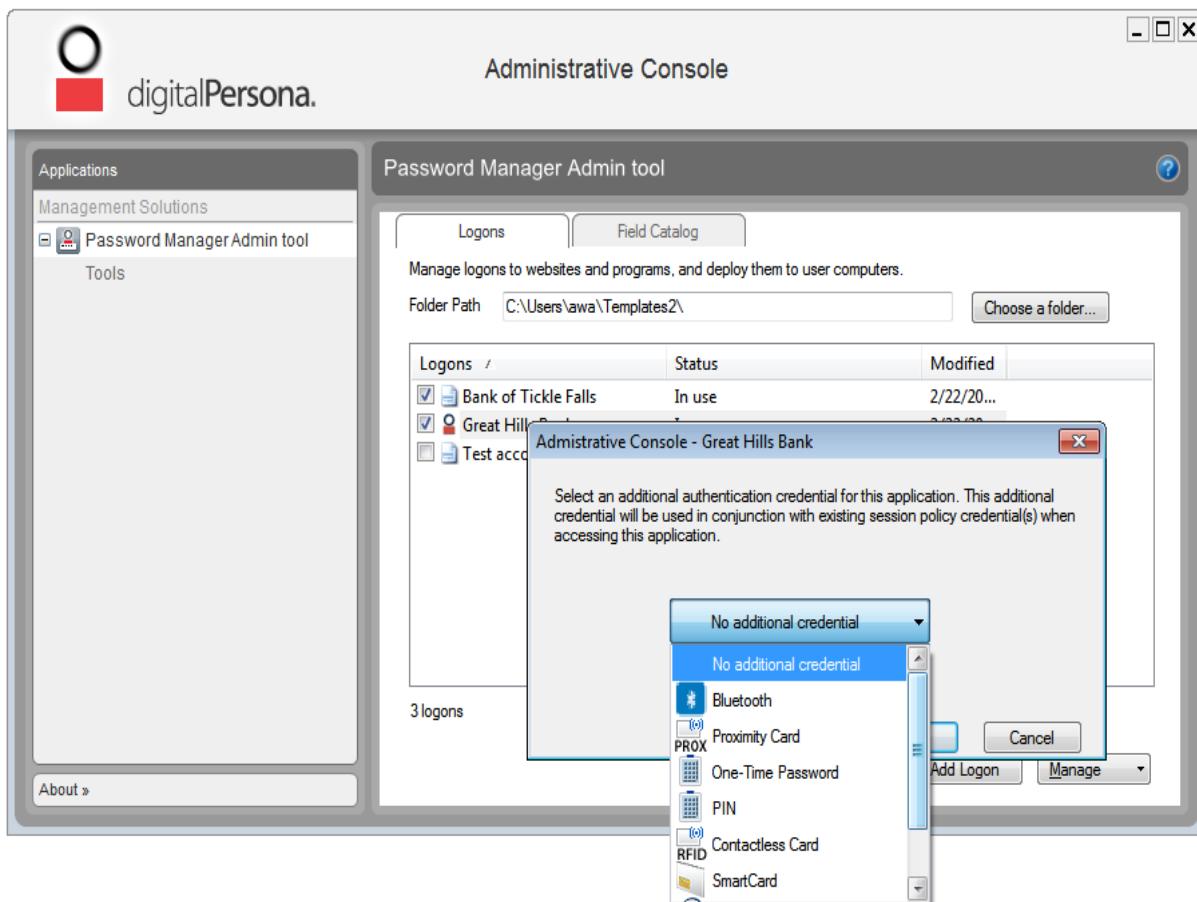
The authentication credentials required for users to access resources (websites, programs, etc.) through managed logons is defined by the DigitalPersona Session Authentication Policy.

However, an additional second factor can be defined for specific resources as necessary by creating an extended authentication policy in the Password Manager Admin Tool.

To create an extended authentication policy

1. Create or select a managed logon for the resource.
2. Click the *Manage* button.
3. From the context menu, select *Edit, Extended authentication policy*.

4. Select the credential(s) to use as a second authentication factor for this resource.



5. Click *OK*.

Examples

- Session Policy is "Fingerprint or Password," and extended policy is "PIN."
- User may authenticate with "Fingerprint + PIN" or "Password + PIN."
- Session Policy is "Fingerprint or Password," and extended policy is "PIN, Bluetooth."
- User may authenticate with "Fingerprint + PIN" or "Password + PIN" or "Fingerprint + Bluetooth" or "Password + Bluetooth."

Any session policy elements already having two factors will not be changed. If none are selected, the session authentication policy will be used as is.

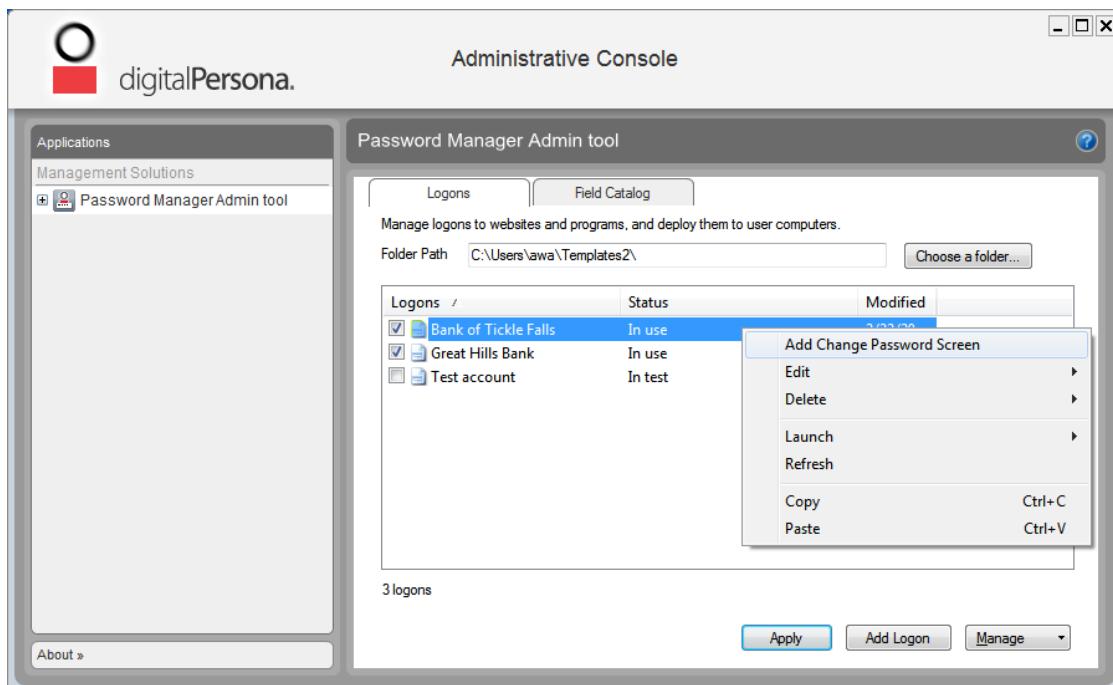
Setting Up a Change Password screen

By managing a change password screen, you can specify the fields required by the application for changing passwords, implement password policies and automate the entire process for the end user.

To set up a Change Password Screen automatically:

1. Launch the password-protected website or program for which you want to set up a Change Password Screen. Move to that site's or program's Change Password screen.
2. In the Password Manager Admin Tool, select the logon for that website or program.

3. Right-click to display that logon's context menu, then click *Add Change Password Screen*. The the Password Manager Admin Tool Change Password Screen wizard starts.



4. On the first page of the wizard, confirm that the correct screen has been detected. Click *Next*. The wizard displays the Change Password Screen Fields page.
5. Select all fields on the page that are relevant to the change password process, and click *Next*.

Option Heading	Description
Use	Check the Use check box for each field used for password change. If some of the fields displayed by the wizard are not relevant for password change (i.e., a search field on a website change password page), leave those fields unchecked.
Label	If the label for a field is not intuitively related to the corresponding field on the change password screen, enter a new label name in this field. The labels are displayed when users are prompted to type a value for the field.
Catalog	By default, specifies values for fields based on those used in the associated Logon screen. For example, the password used at logon is re-used during the Change Password process. Use the Catalog dropdown menu to change these values as needed.
Value	Specifies the value for this field. For Old Password, the value should be Ask-Reuse. For New Password and Repeat New Password fields, the value should be Write Only.

6. On the Password Policy page, optionally, click (...) to specify changes to the password policy. The password policy defined in the wizard should generally be the same as that used on the website or in the program. The default is none.
7. Click *Next*, and on the Submit Selection page, select the button used to submit the password data. Or select *Do Not Submit* to fill in the data but not submit it.
8. Click *Next* to display the Change Password Screen Properties page. Modify any of the listed properties (see below) to customize behavior of the Change Password screen.
9. On the *Setup Complete* page, click *Finish* to close the wizard.

10. Click *Apply* to save your changes to the server.

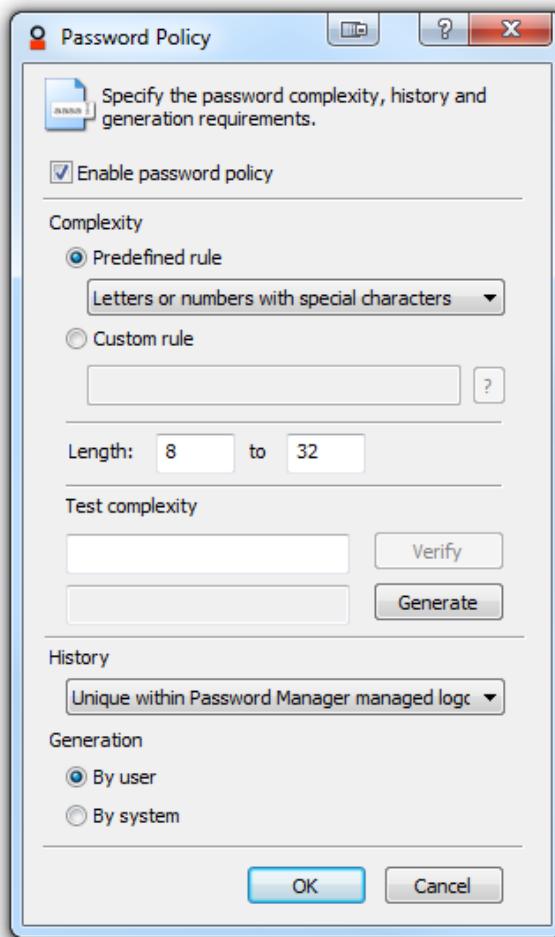
You do not need to click *Apply* after creating making every change, but you do need to click *Apply* to save any changes that you have made.

Managed change password screens are deployed at the same time as the managed logons that they are associated with. After they are deployed, they will display the *Change Password* icon, indicating that the user should verify their identity to begin the change password process.

See Also: Creating logons manually on page 145.

Password policies

Password policies for passwords that are generated by the Password Manager Admin Tool or entered by a user at a Change Password screen are enabled and defined in the the *Password Policy* dialog.



Here, you can also verify proposed passwords against specified password complexity requirements.

Option	Description
Enable password policy	When enabled: If the password is entered by the user, it will be verified by Password Manager and must conform to the password complexity requirements defined in this dialog. If the password is generated by the system, it will be generated according to the specified complexity requirements.
Complexity	

Option	Description
Predefined rule	<p>The password must conform to the predefined rule selected from the dropdown menu. These include:</p> <p>Letters and numbers - allows any combination of letters and/or numbers.</p> <p>Numbers only - allows numbers only.</p> <p>Letters only - allows letters only.</p> <p>Letters or numbers with special characters - passwords must contain at least one number or letter and at least one special character. Special characters include !"#\$%&()'*,.-./:;<=>?[\\]^_`{ }~@. Spaces are not allowed.</p> <p>Letters or numbers with at least one number - passwords may contain either letters or numbers with at least one number.</p>

Option	Description
Custom rule	<p>Enter a pattern for verifying or generating a password using the following notation:</p> <p>A = UPPERCASE LETTERS, i.e. A through Z</p> <p>a = lowercase letters, i.e. a through z</p> <p>d = digits, i.e. 0 through 9</p> <p>s = special characters, i.e. !"#\$%&'()*+,-./;?:@[\]^_`{ }~</p> <p>() = Use the enclosed indicators in random order.</p> <p>For example: (asd) would require or generate a password with a lower case letter, a special character and a digit in any order, i.e. b\$3, #1f or 0z! But the use of asd without the parentheses would always have a lowercase character first, a special character second and then a number.</p> <p>[] = Define a custom character set i.e. [abcdef] would limit the user to only those letters in the specified position.</p> <p>For example: A custom rule of [abcd]ds would generate only passwords with a, b, c or d in the first position, a digit in the second position and a special character in the third position.</p> <p>{n,m} Define a range of acceptable occurrences of the previously indicated character set.</p> <p>For example: d{2,4}a{(2,)s{3}} indicates 2 to 4 digits followed by 2 or more lower case letters and 3 special characters.</p> <p>Note that when there is a comma but no upper range defined, as in {2,}, then the upper limit is only constrained by the maximum length of the password as specified in the field described below.</p> <p>When only one value is specified - without the comma, as in {3}, then the lower and upper range are the same, i.e. in this case, exactly 3 special characters.</p> <p>~ = Prevent two identical consecutive characters</p> <p>For example: This symbol would prevent passwords such as abCCd or fkiq&33.</p> <p>& = Prevent a character being in the same position as in the most recent password</p> <p>For example: This symbol would prevent using the password abc3def if the most recent previous password was dar3feg.</p>
Length	Select the minimum and maximum length for the password. Note that any custom rule defined must fall within the range between the minimum and maximum lengths specified here.

Option	Description
Test Complexity	<p>This area includes two fields and buttons which can be used to verify that a specific password meets the defined complexity requirements or generate a new password that will meet the requirements.</p> <p><i>Verify</i> - Enter a password in the text field to the left of the Verify button and it will be verified against the defined complexity rule.</p> <p><i>Click</i> the Generate button and the system will generate a password that conforms to the defined complexity requirements and display it in the field to the left of the button.</p>
History	<p>From this dropdown menu, you can select additional password constraints relating to the history of the password.</p> <p><i>None</i> - No other constraints are applied to the password contents.</p> <p><i>Different than the Windows password</i> - The new password must be different than the current Windows password.</p> <p><i>Unique within Password Manager managed logons</i> - The new password must be different from any other password associated with this managed logon for a specified user account.</p> <p><i>Different than the current password</i> - The new password must be different than the current password for this website or program</p> <p>Note that the History constraints are not applied when verifying or generating passwords within this dialog, but only on an actual Change Password screen.</p>
Generation	<p><i>By User</i> - Password Manager does NOT provide password information to a Change Password screen and the user has the option to log on by entering their password or another allowed credential. If a password is used, it is verified against the defined complexity rules.</p> <p><i>By System</i> - Password Manager generates the password automatically. An alternate credential must be used to log on.</p>

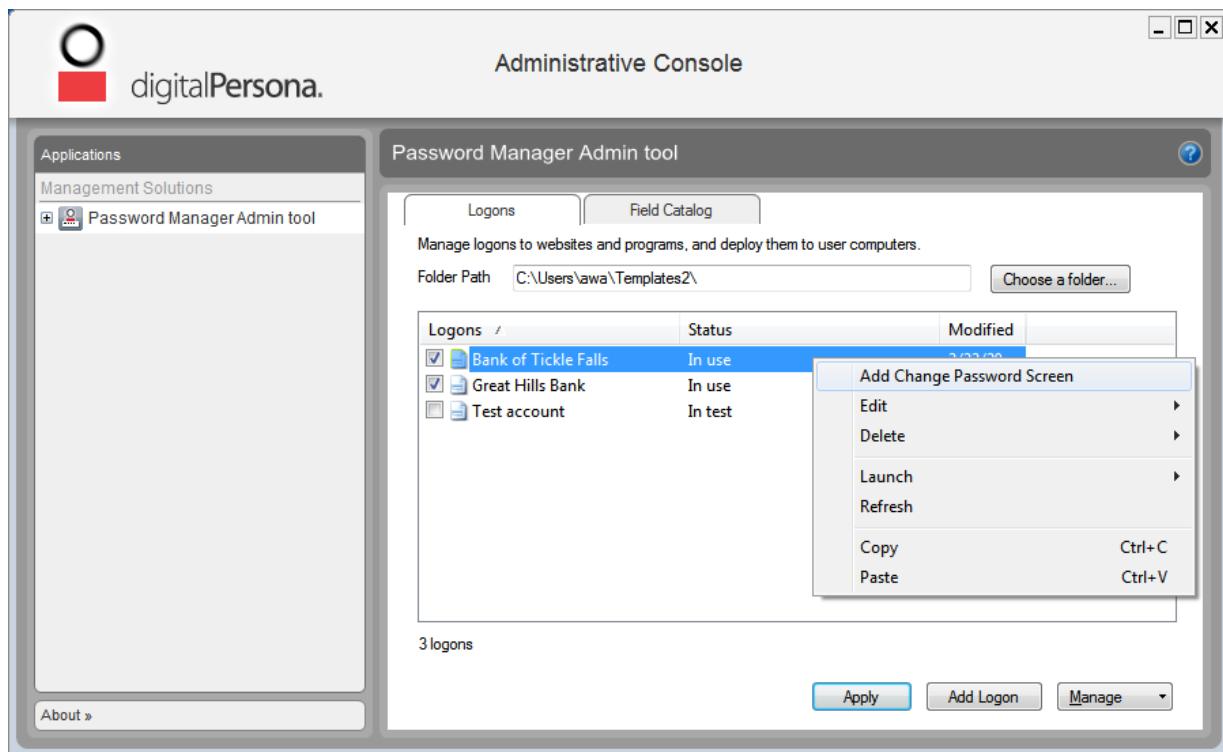
Setting up a Change Password Screen manually

If the Password Manager Admin Tool does not detect fields automatically in Change Password screens, you can manually specify the fields and actions required. Creating a Change Password screen manually allows you to include additional controls such as adding keystrokes, forcing delays between actions, and specifying positions of fields.

To set up a Change Password screen manually

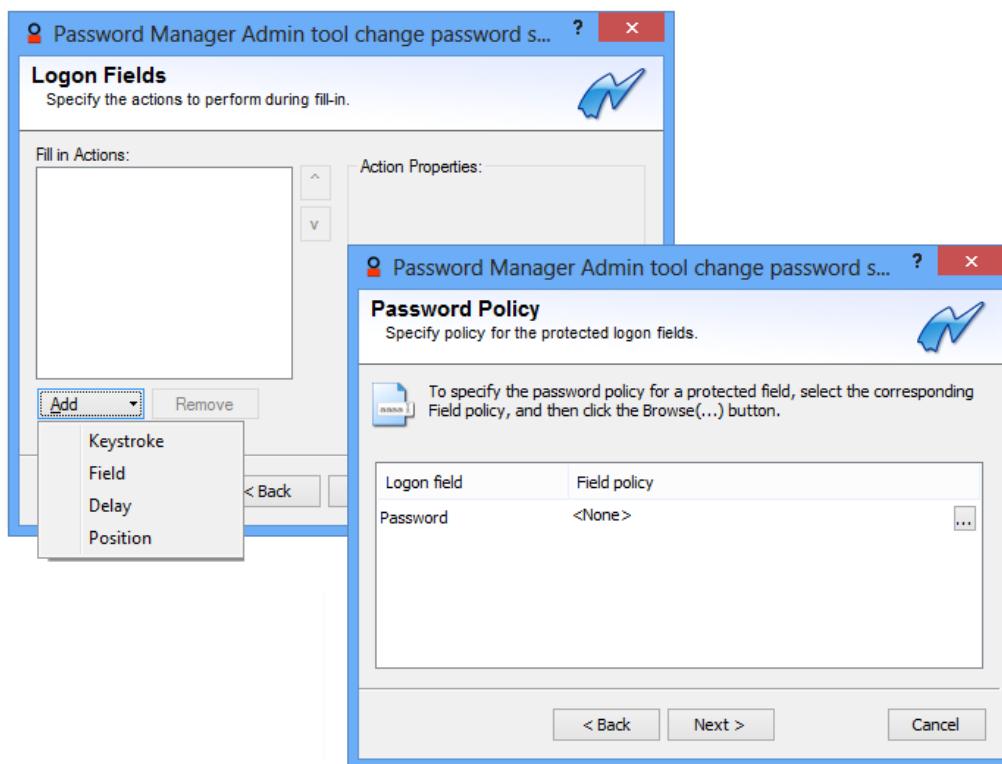
1. Launch the password-protected website or program for which you want to set up a Change Password Screen. Move to that site's or program's Change Password screen.
2. In the Password Manager Admin Tool, select the logon for that website or program.

3. Right-click to display that logon's context menu, then click *Add Change Password Screen*.



The Password Manager Admin Tool Change Password Screen Wizard starts.

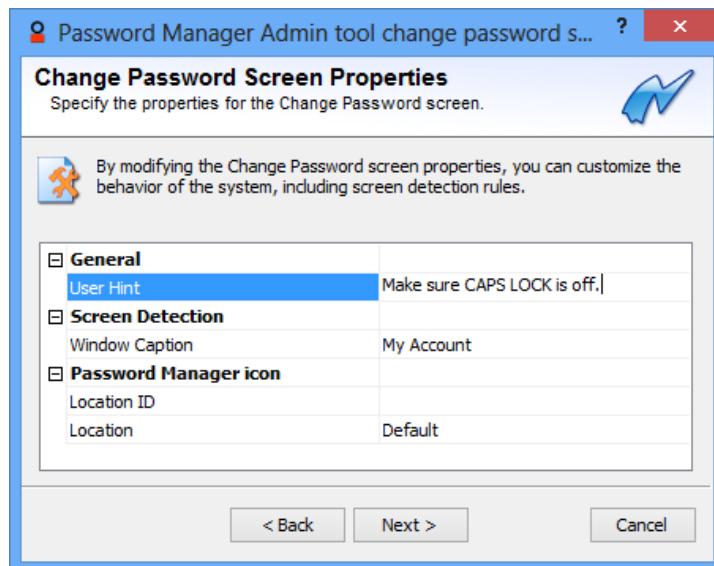
4. On the first page of the wizard, confirm that the correct screen has been detected. Select *Set up change password screen manually*. Click *Next*.
5. On the *Logon Fields* page, click *Add* and select an action from the dropdown menu.



For example, you might study a Change Password screen and discover that it takes nine presses of the tab key to get to the first input field (Change Password).

You could choose Keystroke, select the Tab key, and specify "Repeat 9 times" to get the user where they need to be; or you could choose to use the Position action to place the cursor in the right location to change the password.

6. Add additional actions as required. If necessary, use the arrow buttons to modify the order in which the actions are performed.
7. On the Password Policy page, optionally, click (...) to specify changes to the password policy. The password policy defined in the wizard should generally be the same as that used on the website or in the program. The default is *None*.
8. Click *Next* to display the Change Password Screen Properties page. Modify any of the listed properties to customize behavior of the Change Password screen.



9. On the *Setup Complete* page, click *Finish* to close the wizard.

10. Click *Apply* to save your changes to the server.

You do not need to click *Apply* after making every change, but you do need to click *Apply* to save any changes that you have made.

Managed change password screens are deployed at the same time as the managed logons that they are associated with. After they are deployed, they will display the *Change Password* icon, indicating that the user should verify their identity to begin the change password process.

Regular Expression syntax

Both Logon Screens and Change Passwords Screens can use regular expressions in the URL field of the Properties page to define the part of a URL that should be matched when determining if the page has changed.

A regular expression is a text string used to create a logon for matching certain characters, or a series of characters, within another text string.

In a regular expression, most characters are treated as literals, i.e. they match only themselves ("a" matches "a", "(bc" matches "(bc", etc). The exceptions are called metacharacters (MC in the table below).

MC	Description
.	Matches any single character

MC	Description
[]	<p>Matches a single character that is contained within the brackets. For example, [abc] matches "a", "b", or "c". [a-z] matches any lowercase letter. These can be mixed: [abcq-z] matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [a-cq-z].</p> <p>The '-' character should be literal only if it is the last or the first character within the brackets: [abc-] or [-abc]. To match an '[' or ']' character, the easiest way is to make sure the closing bracket is first in the enclosing square brackets: [][ab] matches '[', '[', 'a' or 'b'.</p>
[^]	Matches a single character that is not contained within the brackets. For example, [^abc] matches any character other than "a", "b", or "c". [^a-z] matches any single character that is not a lowercase letter. As above, these can be mixed.
^	Matches the start of the line (or any line, when applied in multiline mode)
\$	Matches the end of the line (or any line, when applied in multiline mode)
()	Defines a "marked subexpression". What the enclosed expression matched can be recalled later. See the next entry, \n. Note that a "marked subexpression" is also a "block."
\n	Where n is a digit from 1 to 9; matches what the nth marked subexpression matched. This construct is theoretically irregular and has not been adopted in the extended regular expression syntax.
*	A single character expression followed by "*" matches zero or more copies of the expression. For example, "[xyz]*" matches "", "x", "y", "zx", "zyx", and so on.
\n*	<p>Where n is a digit from 1 to 9, matches zero or more iterations of what the nth marked subexpression matched. For example, "\(\(a.\)\)c\1*" matches "abcab" and "abcabab" but not "abca".</p> <p>An expression enclosed in "\(" and "\)" followed by "*" is deemed to be invalid. In some cases (e.g. /usr/bin/xpg4/grep of SunOS 5.8), it matches zero or more iterations of the string that the enclosed expression matches. In other cases (e.g. /usr/bin/grep of SunOS 5.8), it matches what the enclosed expression matches, followed by a literal "*".</p>
{x,y}	Match the last "block" at least x and not more than y times. For example, "a\{3,5\}" matches "aaa", "aaaa" or "aaaaa".
+	<p>The + operator will match the preceding atom (a single character, a marked sub-expression, or a character class) one or more times, for example the expression a+b will match any of the following:</p> <p>ab aaaaaaaaab</p> <p>But will not match: b</p>
	<p>The operator will match either of its arguments, so for example: abc def will match either "abc" or "def".</p> <p>Parenthesis can be used to group alternations, for example: ab(d ef) will match either of "abd" or "abef".</p>

MC	Description
?	The ? operator will match the preceding atom (a single character, a marked sub-expression, or a character class) zero or one times, for example the expression ca?b will match any of the following: cb cab But will not match: caab

Managing logons

The Password Manager Admin Tool makes managing logons easy. Most management features can be accessed through either of two means available on the Logons tab:

- Right-click on a logon to display the shortcut menu for that logon
- Select a logon and click *Manage* to display available commands for that logon.

After making any changes to your managed logons, remember that they need to be deployed before they can be seen and used by the end user (see *Deploying managed logons on page 146*).

The following logon management features are described in this section.

Feature	Page
Editing logons	158
Deleting logons	159
Deploying logons	159
The Field Catalog	160
Finding logons	161
Finding duplicate logons	162
Finding logons with enhanced authentication policies	162

Editing logons

To edit a logon:

1. Select a logon to edit and click *Manage*.
2. Click *Edit* and select from the following options: *Logon Screen*, *Change Password Screen* or *Extended Authentication Policy*.
3. In the corresponding wizard, make any desired changes to the logon. For details on specific wizard pages, see one of the following topics:

Reference	Page
Logon Fields attributes	140
Values	141
Logon properties	142
Logon Fields actions	147

Reference	Page
Password policies	151

4. When editing is complete, click *Finish* to exit the wizard.
5. Click *Apply* to save your changes to the server.

You do not need to click *Apply* after making *each* change, but be aware that you *do* need to click *Apply* before any changes to logons will be saved.

Deleting logons

To delete a logon:

1. On the *Logons* tab, select the folder that contains the logon you want to delete.
2. Select a logon to remove and click *Manage*, or just right-click the logon to display the shortcut menu.
3. Click *Delete*. Then click *All Screens* to delete the logon and any associated Change Password screens, or click *Change Password Screen* to delete only the Change Password screen.
4. Click *Apply* to save your changes to the server.

You do not need to click *Apply* after making every change, but you do need to click *Apply* to save any changes that you have made.

Deploying logons

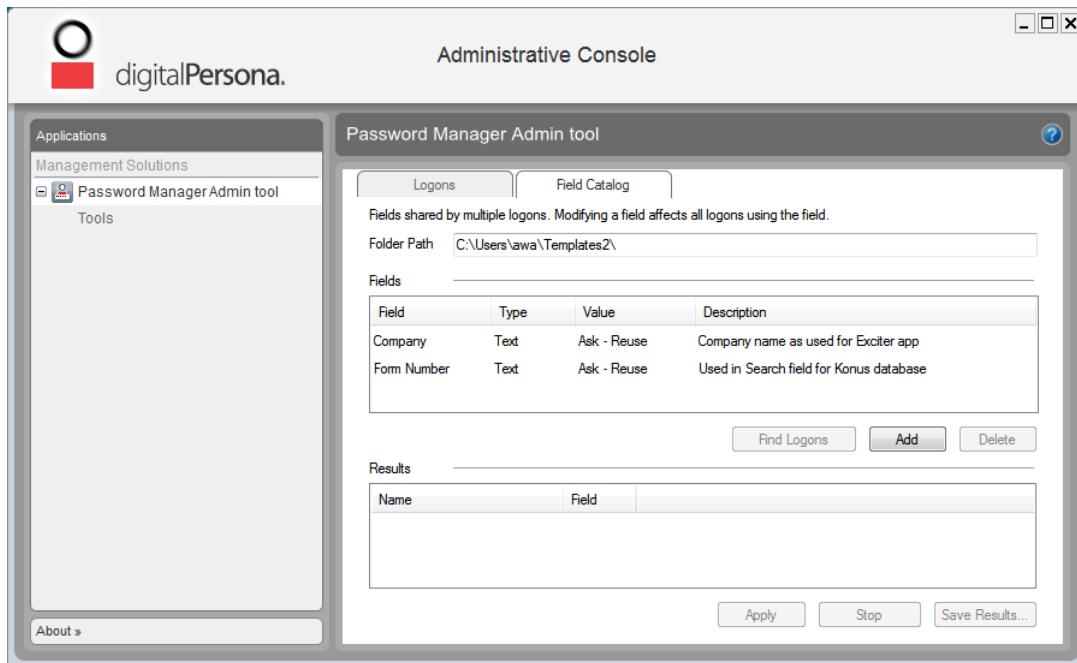
To deploy managed logons:

1. Check the boxes next to logons to change their status from *In Test* to *In Use*. Only logons with an *In Use* status will be visible to users.
2. Click *Apply*.

After a managed logon is deployed to a computer, the Password Manager icon on the screen tells the user that they can fill in the requested account data by verifying their identity with the required credentials.

The Field Catalog

You can use the Field Catalog to store logon field values and attributes that can be reused in creating managed logons for logon screens that share common fields.



By storing frequently used logon fields in the catalog, you can add commonly used fields to additional logons without setting values or attributes each time. Later changes made to fields in the catalog will then also be propagated to all logons that use the field.

Managing shared fields in the Field Catalog

To add a field to the Field Catalog:

1. On the Field Catalog tab, click *Add* to create a new field in the table.
2. In the *Field* column, type a name for the field you are adding to the catalog.
3. Specify the type of the field by selecting *Password* or *Text* in the *Type* dropdown list.
4. Specify the value of the field (see page 141) from the *Value* dropdown menu.
5. Add any comments related to this field in the *Description* text box.

To delete a field from the Field Catalog:

1. On the Field Catalog tab, select a field.
2. Click *Delete*.

Example: Use of Field Catalog for password

To use a field from the Field Catalog for a password:

1. Add a field to the catalog, and select *Password* as the type (see previous topic).
2. Create a managed logon manually (see page 145).
3. On the Logon Fields page of the wizard, from the *Add* dropdown menu, select *Field*.
4. In the Action Properties area, enter a label for the field.

5. From the Type dropdown menu, select *Password*.
6. From the Reference dropdown menu, select the name of the field that you added in step 1 above.
7. Continue creation of the logon as described in step 9 of *Creating logons manually* on page 146.

Finding fields in logons

You can search for managed logons that contain fields selected from the Field Catalog.

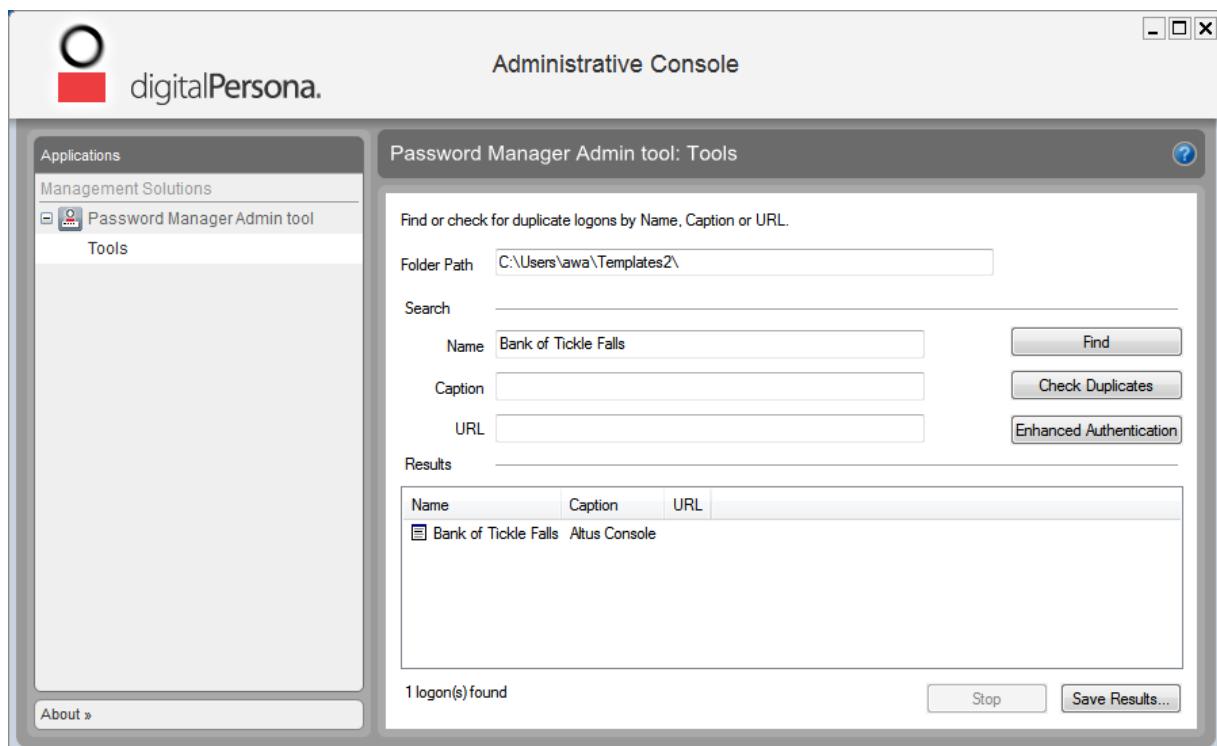
To search for logons that contain selected fields:

1. On the *Field Catalog* tab, select the fields to search for and click *Find Logons* to display the search results.
2. Optionally, click *Save Results* to save the results to an HTML file.

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

Tools page

Use the Tools page to search for logons, or check for duplicate logons.



Finding logons

To search for logons

1. On the Tools page, enter a logon Name, Caption or URL in one of the associated text fields to search for it. Use ? or * wild cards to indicate individual or multiple characters.
2. Click *Find* to display the search results.
3. (Optionally) Click *Stop* to cancel the search.
4. In the Results area, right-click on any of the displayed logon names to display a shortcut menu with options to edit or delete the duplicate managed logon.

5. (Optionally) Click **Save Results** to save the results to an HTML file.

Finding Duplicate Logons

Duplicate logons are multiple copies of logons for a single logon or change password screen.

To search for duplicate logons

1. On the Tools page, click *Check Duplicates*.
2. (Optionally) Click *Stop* to cancel the search.
3. Optionally) Click *Save Results* to save the results to an HTML file.

In the Results area, right-click on any of the displayed logon names to display a shortcut menu with options to edit or delete the duplicate managed logon.

Finding logons with enhanced authentication policies

To list all logons that have associated enhanced authentication policies

1. On the Tools page, click *Enhanced Authentication*.
2. (Optionally) Click *Stop* to cancel the search.
3. In the Results area, right-click on any of the displayed logon names to display a shortcut menu with options to edit or delete the duplicate managed logon.
4. Optionally, click *Save Results* to save the results to an HTML file.

Password Manager Actions

Password Manager Actions are operations that may be performed when any assigned DigitalPersona Hot Key combinations are pressed, or a specified credential or credential combination is presented.

Password Manager Actions may be assigned to the DigitalPersona Hot Key, credential or credential combination through the Quick Actions policy setting on the DigitalPersona Server.

The Password Manager Action that will be performed depends on the context. One of the following operations will be performed, in the listed order of preference.

1. When the active window is a website, program or other resource associated with a previously created personal or managed logon - trained fields will be filled in with user account data.
2. If the active window does not have a previously created personal or managed logon - The Create Logon dialog is displayed allowing creation of a personal logon for the resource. This action also requires that the “Allow creation of personal logons” policy setting in Active Directory must be enabled or not configured.

User policy settings

The following Active Directory policy settings are available in Active Directory on the DigitalPersona Server and apply to DigitalPersona AD users only.

Allow creation of personal logons - When enabled, allows users to create personal logons. However, when managed logons and personal logons are created for the same screen, only the managed logon is functional.

Managed Logons - When enabled, the following options can be configured.

- Allow users to view managed logon passwords - When selected, allows users to see passwords when providing account data. By default, passwords are hidden.
- Allows users to edit account data - Enabled by default.

- Allow users to add account data - Enabled by default.
- Allow users to delete account data - Enabled by default.
- Path(s) to the managed logons folder(s) - Must be enabled and a folder path entered in order to deploy managed logons to specified computers.

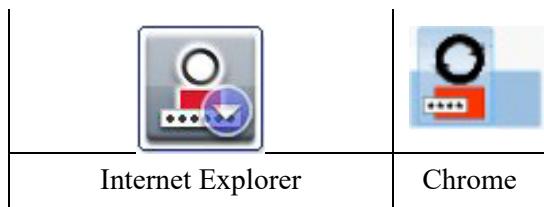
These settings can be configured in the Group Policy Management Editor under the node User Configuration\Policies\Administrative Templates\DigitalPersona Client\Managed Applications\Password Manager. More detailed explanations are provided on the Explain tab for each of the settings and in the *Policies and Settings* chapter of the DigitalPersona Administrator Guides.

Logging On

After creating managed logons and deploying them, users will then be able to launch a logon screen and verify their identity with their specified credentials.

Logon screens that have a logon created for them display the Password Manager icon on the screen.

Depending on the attributes defined by the logon administrator, the logon process may vary.



A user can be automatically logged on, with all fields populated and submitted, simply by verifying their identity. The user may need to supply information for required fields the first time they use the logon, but be automatically logged on subsequently.

If the user has set up multiple sets of account data, they will be prompted to select the account they wish to log on to in the *Choose Logon Account* dialog box.

Changing passwords

After creating logons and deploying them to users, managed password screens display the Change Password icon on the screen. After verifying their identity, the user is asked to provide an old password, a new password and to confirm the new password.

Depending on the logon attributes, the change password process may vary.

- The user can be allowed to choose a new password with or without constraints on the password content.
- A new random password can be automatically generated, in which case the user must log on with alternate credentials.

Section Three: Web Management

Section Three of the DigitalPersona AD Administrator Guide includes the following chapters:

Chapter Number and Title	Purpose	Page
20 - Web Management Components installation	Provides instructions on installation and configuration of the Web Management Components.	165
21 - Assigning Security Officer permissions	Provides details on the permissions available for assignment to Security Officers.	177
22 - DigitalPersona Identity Server	Describes the DigitalPersona Identity Server.	181
23 - DigitalPersona Web Administration Console	Describes the DigitalPersona Web Administration Console.	190
24 - DigitalPersona Web Enrollment	Describes the DigitalPersona Web Enrollment application.	195
25 - DigitalPersona Application Portal	Describes the DigitalPersona Application Portal.	216

THIS CHAPTER DESCRIBES HOW TO INSTALL, CONFIGURE AND UNINSTALL THE WEB MANAGEMENT COMPONENTS.

Main topics in this chapter	Page
Installation wizard	165
Prerequisites	165
Installation steps	166
Configuration wizard	168
Express Configuration	169
Advanced Configuration	172
Uninstallation	175

The Web Management Components module contains a collection of components that together enable management of your DigitalPersona environment through a web based interface. The following components are included.

- DigitalPersona Web Access Management (previously DigitalPersona Confirm)
- DigitalPersona Secure Token Service
- DigitalPersona Web Administration Console
- DigitalPersona Web Enrollment
- DigitalPersona Web Application Portal

This module works in conjunction with, and requires previous installation and configuration of at least the DigitalPersona AD Server and the DigitalPersona AD Administration Tools. If the optional DigitalPersona Extended Server Policy Module (ESPM) will be used, it must be installed on the same machine as these components. For system requirements, see the table beginning on page 17.

Installation wizard

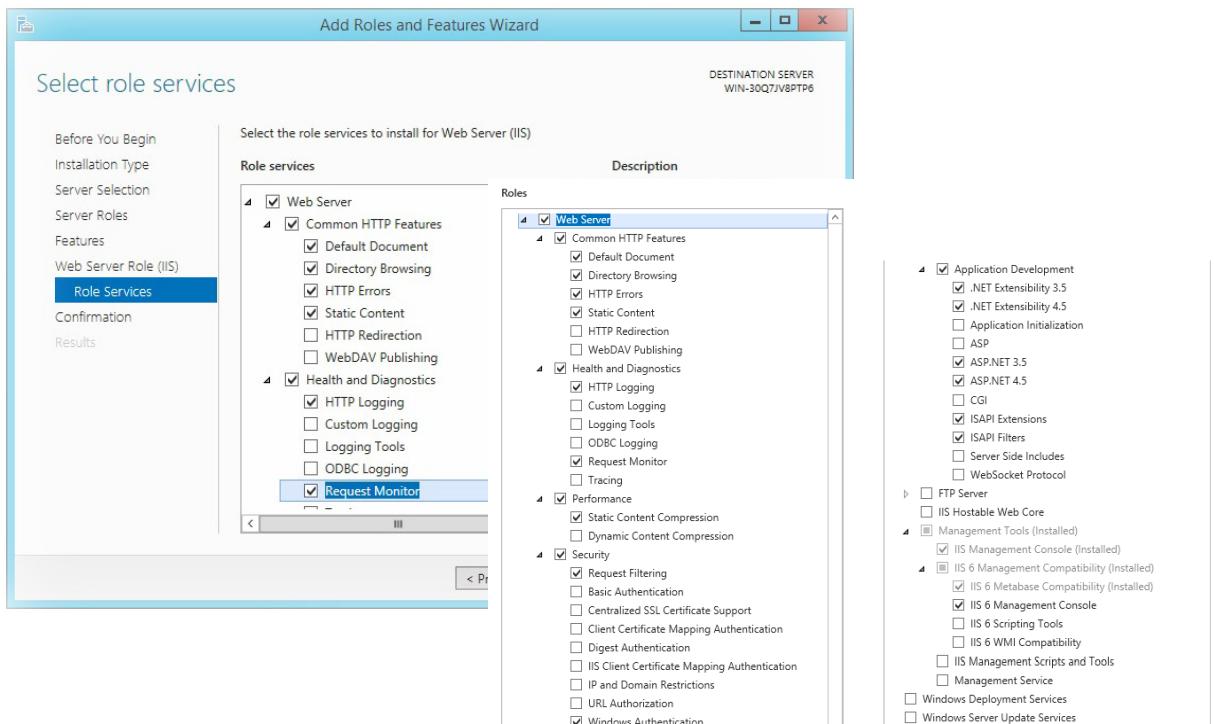
Note that a valid SSL certificate should be imported to the target machine before running the DigitalPersona AD Web Management Components Wizard.

The Web Management Components installation wizard provides both an Express Configuration, for installation of all components on the same IIS website, and an Advanced Configuration, that installs each separate web application on its own site. Also, Express Configuration requires the use of a wildcard SSL certificate, while Advanced Configuration may be used with either a wildcard SSL certificate or separate SSL certificates for each component.

Prerequisites

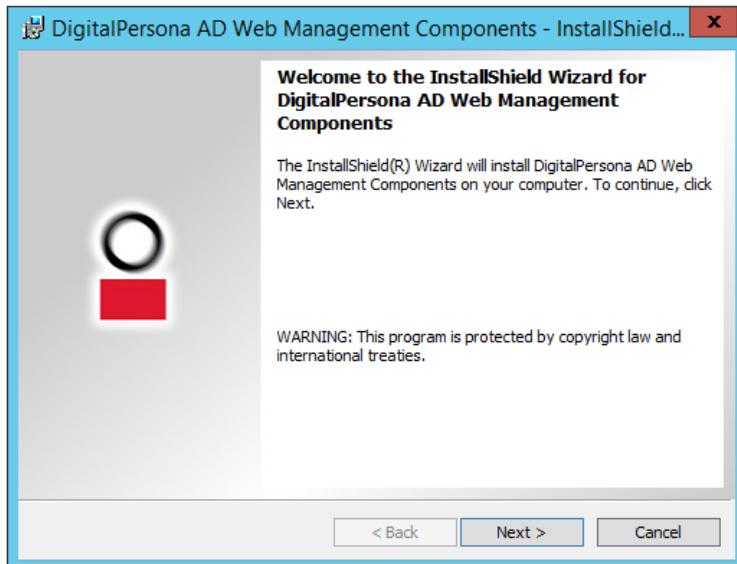
- A valid SSL certificate must be imported to the target machine *before* running the DigitalPersona AD Web Management Components Wizard.
- If Windows Web Server (IIS) has not been previously added to the machine, it will be added by the wizard, and a reboot may be required in order to continue.
- When Windows Web Server has been previously installed, ensure that the following features have been installed
- .NET 4.5 Framework features: ASP.NET, HTTP Activation and TCP Port Sharing.

- Web Server role services, including those shown in the following images.

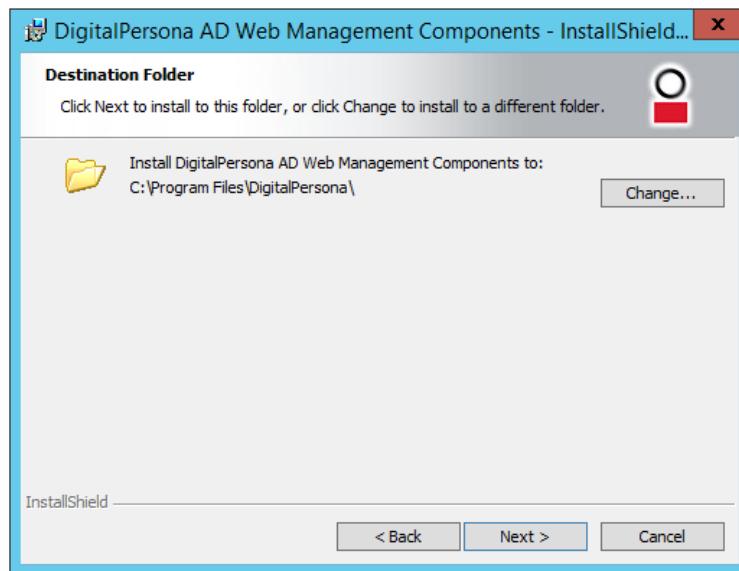


Installation steps

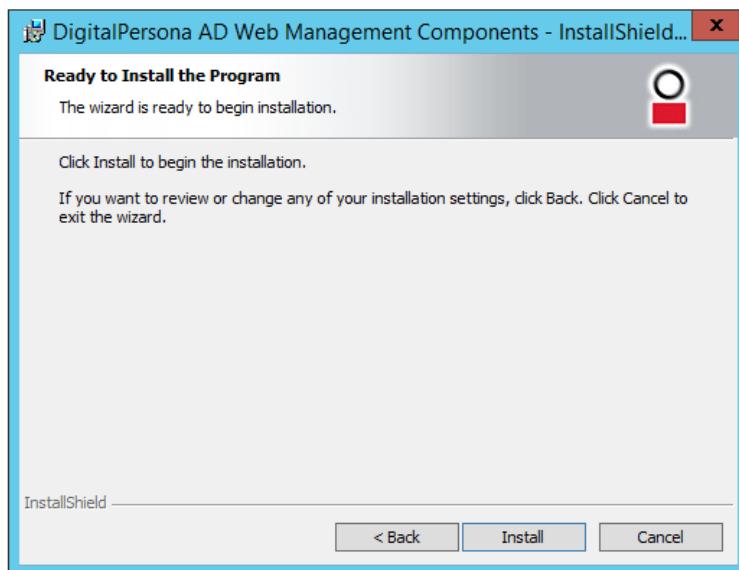
1. Locate and launch the *setup.exe* located in the *DigitalPersona AD Web Management Components* folder within the product package. The *DigitalPersona AD Web Management Components Wizard* displays.



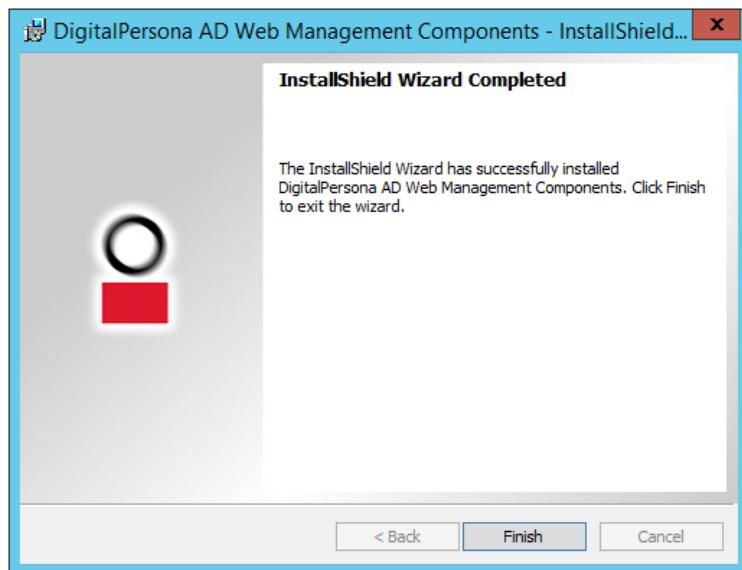
2. On the *Welcome* page, click *Next*. Then on the *License Agreement* page, accept the agreement and click *Next*.



3. On the *Destination Folder* page, click *Next*. If this is the first DigitalPersona product being installed on this machine, there will also be a *Change* button which allows you to change the installation directory. Additional DigitalPersona product installations may remove this button in order to ensure that associated products are installed to the same directory.



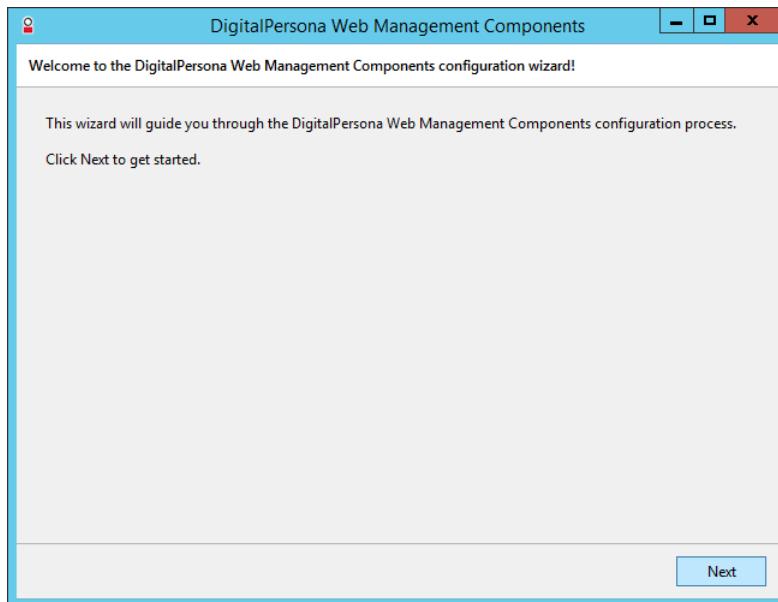
4. On the *Ready to Install the Program* page, click *Install*.



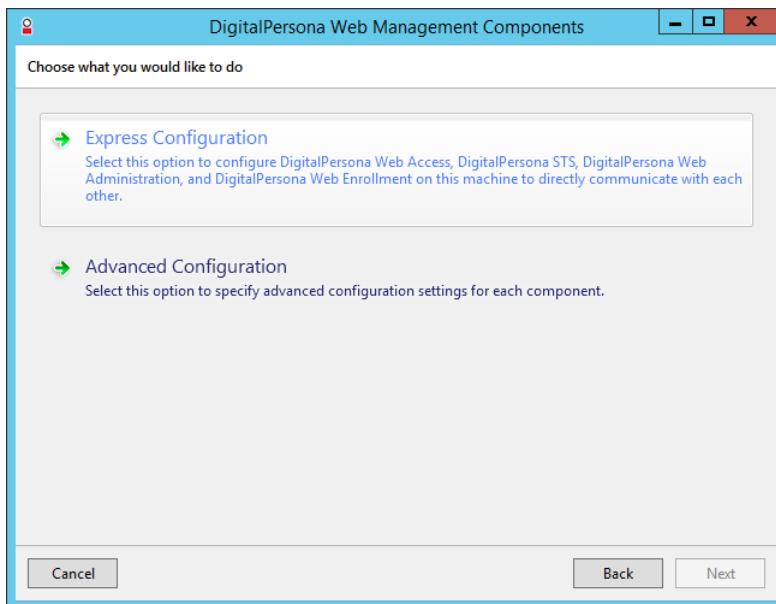
5. On the *InstallShield Wizard completed* page, click *Finish*.

Configuration wizard

Immediately following the completion of the installation wizard, a configuration wizard displays to guide you through the configuration process.



1. Click *Next* to begin the configuration process.

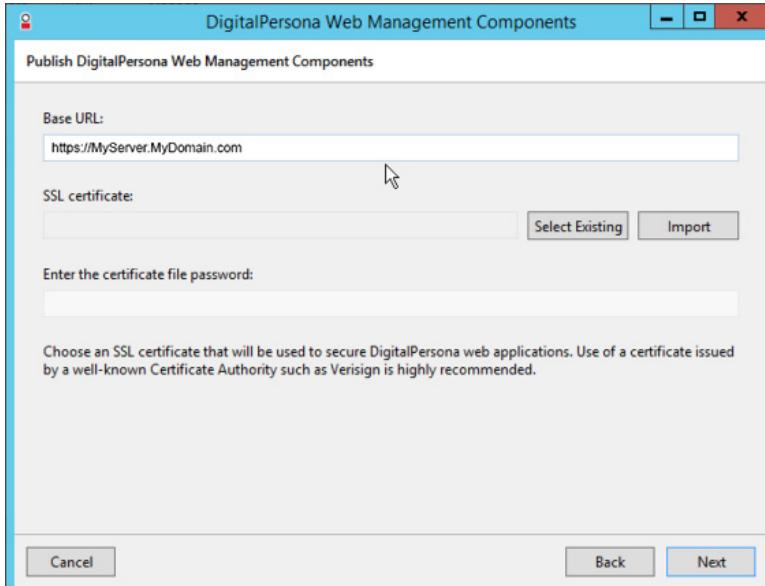


2. Select the type of configuration you wish to use.

- *Express Configuration* - to install all components on this machine and configure them for direct communication.
- *Advanced Configuration* - to create and configure separate websites for each component.

Express Configuration

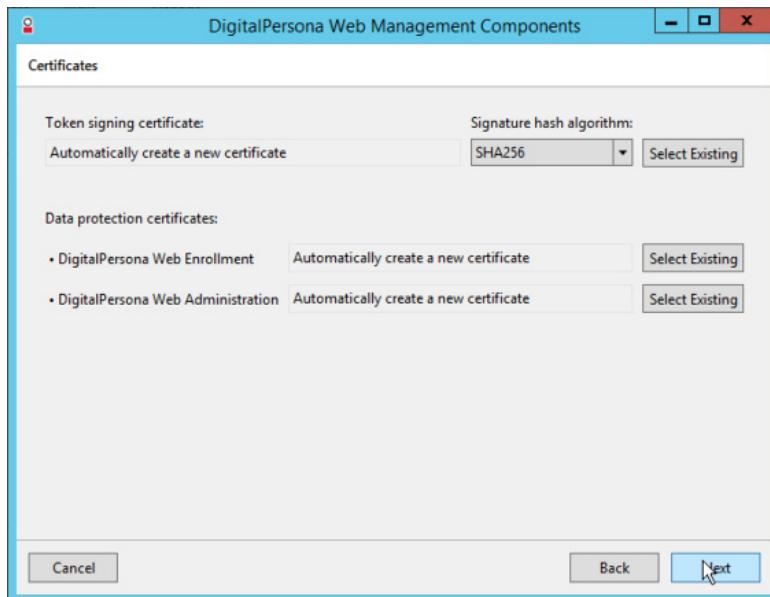
3. For *Express Configuration*, continue with the following steps. For *Advanced Configuration*, skip to the topic *Advanced Configuration* on page 172.



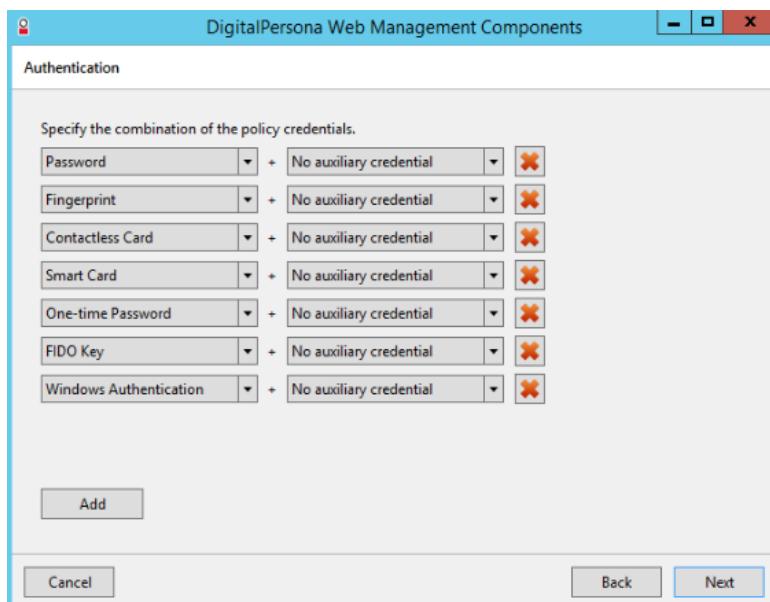
4. Confirm that the Base URL is correct.
5. Under *SSL Certificate*, click *Select Existing* to choose an existing SSL certificate or click *Import* to locate and import a .pfx certificate file. Make sure that the Base URL specified above matches the subject in the SSL certificate being selected or imported. Note that an SSL certificate from the Domain Certificate Authority or a

Global CA is highly recommended. Use of a self-signed certificate will cause invalid certificate warnings and may have additional unanticipated effects.

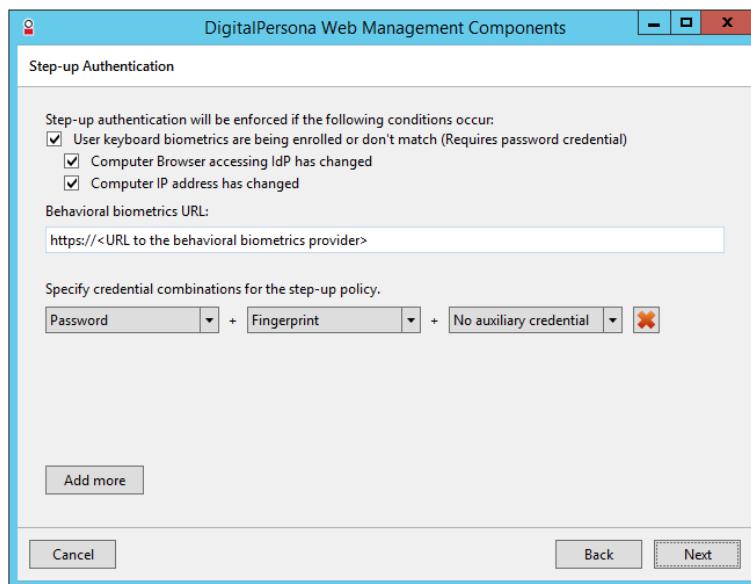
6. If the certificate is password protected, enter the password for the certificate.
7. On the *Certificates* page, you can accept the defaults and allow DigitalPersona to automatically create the required certificates, or choose *Select Existing* to use a certificate of your own for token signing and/or data protection.



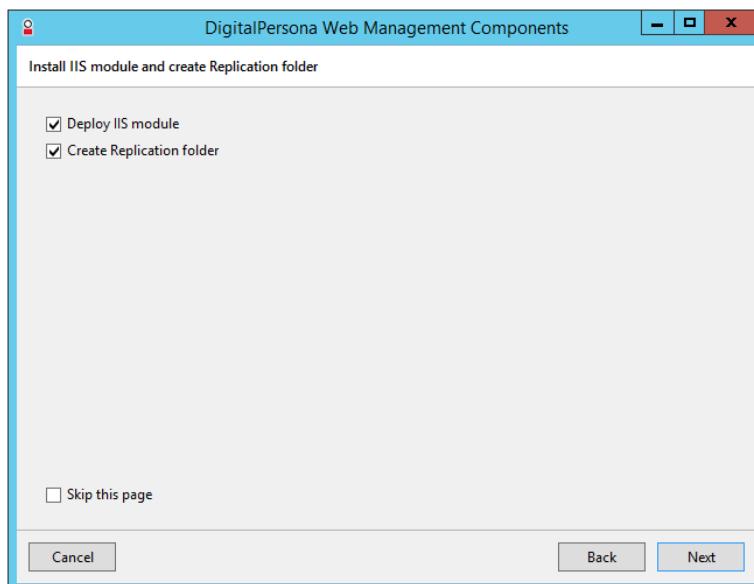
8. Click *Next*.
9. On the *Authentication* page, specify each credential or credential combination that may be used to authenticate a user's identity when accessing web applications through the DigitalPersona Identity Server. Select additional credentials or combinations from the available dropdown menus. Click *Add* to insert an additional line or click the associated X to delete a line. Click *Next*.



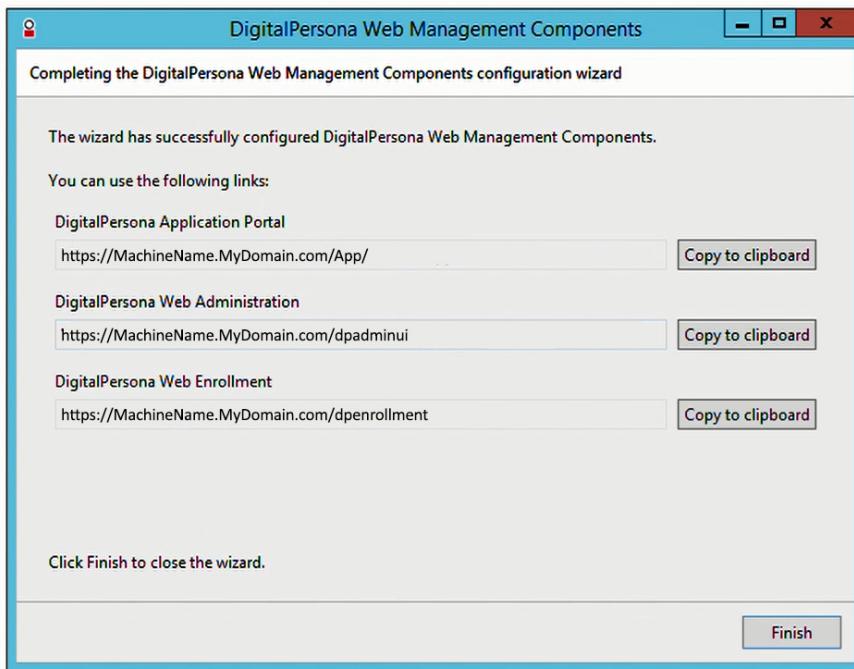
10. The *Step-up Authentication* page enforces step-up authentication for the DigitalPersona Identity Server when any of the selected conditions occur.



- Select the desired conditions for step-up authentication.
 - Enter the URL to the behavioral biometrics server provided to you during implementation. Click *Next*.
 - Specify up to three credentials that will be required for authentication when the step-up conditions occur.
 - To add additional credential combinations, click *Add more*.
11. Click *Next*. For more about step-up authentication, see the topic *Identity Server configuration (DigitalPersona IIS Plugin)* on page 184.
12. On the following page, accept the default if you want to deploy the DigitalPersona Configuration IIS module and create a Replication folder. For additional information on the module, see *Identity Server configuration (DigitalPersona IIS Plugin)* on page 184. You can also *Skip this page* if you do not intend to install or use the IIS module.



13. On the *Apply configuration* page, verify what actions will be performed during configuration, and any parameters shown and then click *Next*.



14. On the final page, the URLs to the three resulting web applications are shown. Click the *Copy to clipboard* button next to a URL to copy it to the clipboard so that you can open it in a supported browser. You may also want to create shortcuts to these pages for distribution to users. After testing the URLs and your ability to log in to the web applications, click *Finish* to close the wizard.

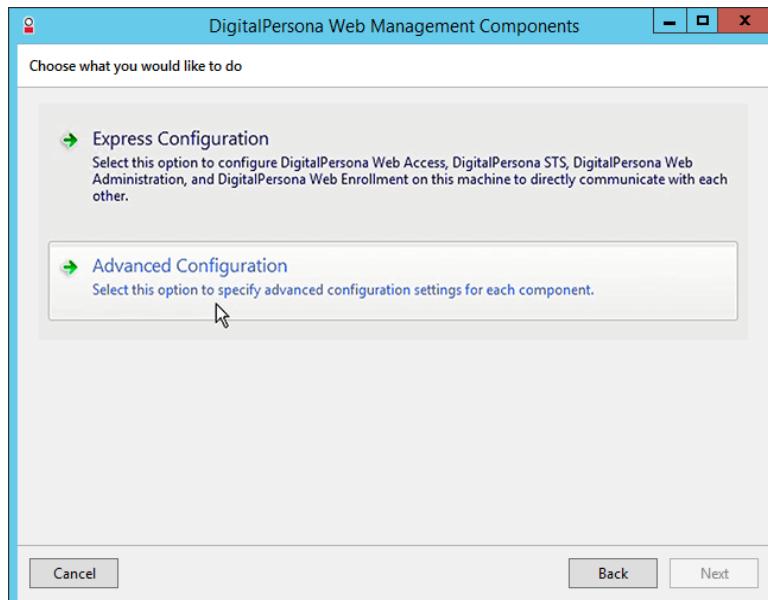
15. For *Express configuration*, stop here.

Advanced Configuration

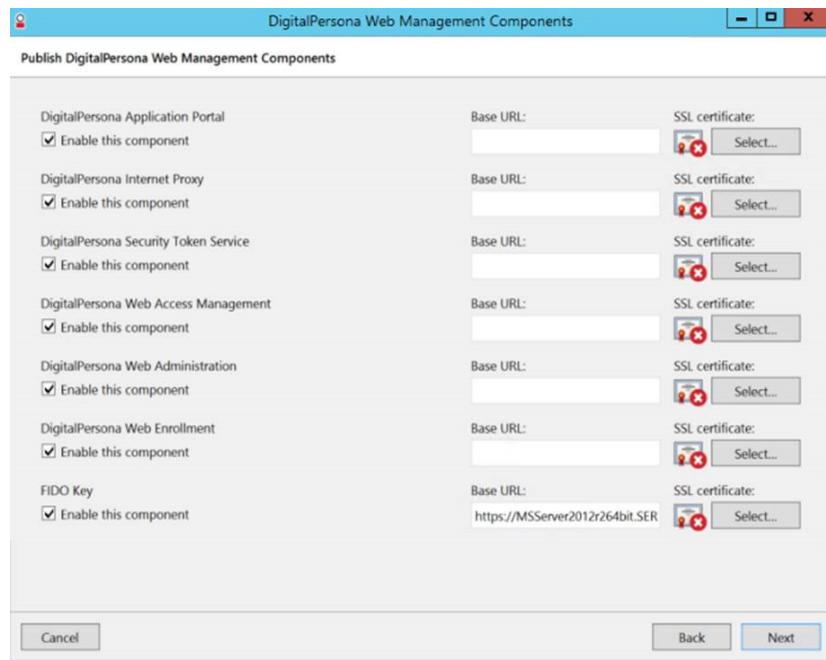
Advanced Configuration is used to create separate websites in IIS for each DigitalPersona web application.

This section continues from the screen in the DigitalPersona Web Management Components Configuration wizard where *Advanced Configuration* is selected.

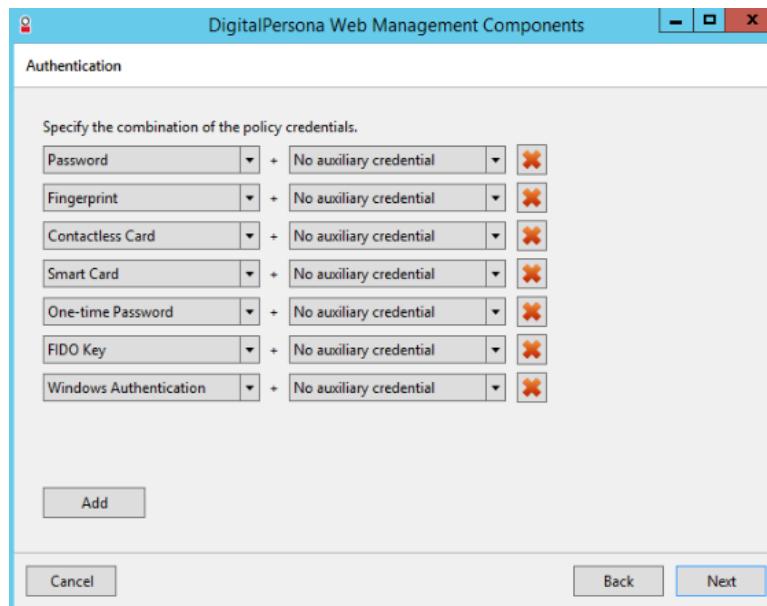
1. Ensure that you have created DNS records for each web management component.



2. After selecting *Advanced Configuration*, click *Next*.
3. Unselect any components that you do not want to configure.

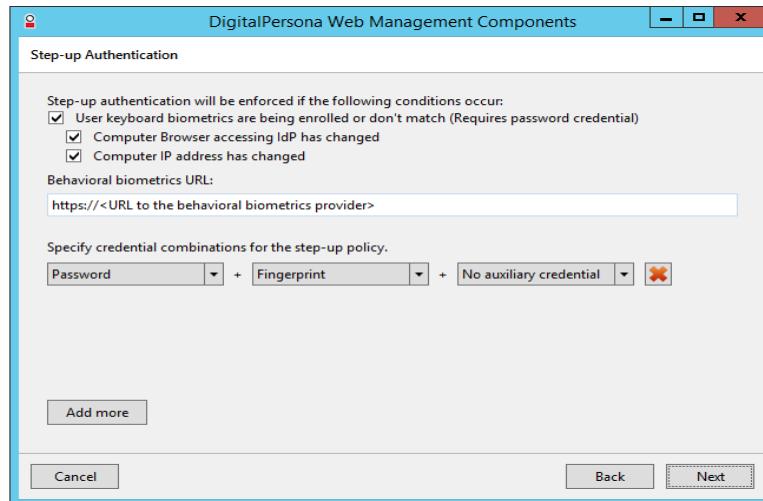


4. Ensure that the Base URLs for any selected components match the DNS records created in step 1 above.
5. Select an SSL certificate for each selected component. Wildcard certificates or separate certificates for each component can be used. Click *Next*.

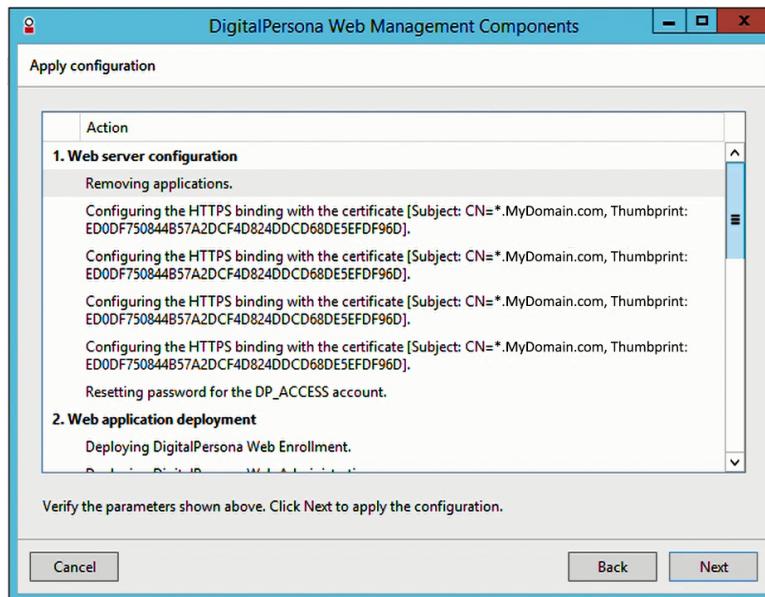


6. On the *Authentication* page, specify each credential or credential combination that may be used to authenticate a user's identity through the DigitalPersona Identity Server. Select additional credentials or combinations from the available dropdown menus. Click *Add* to add another element or click the X to the right of a line to delete that element.

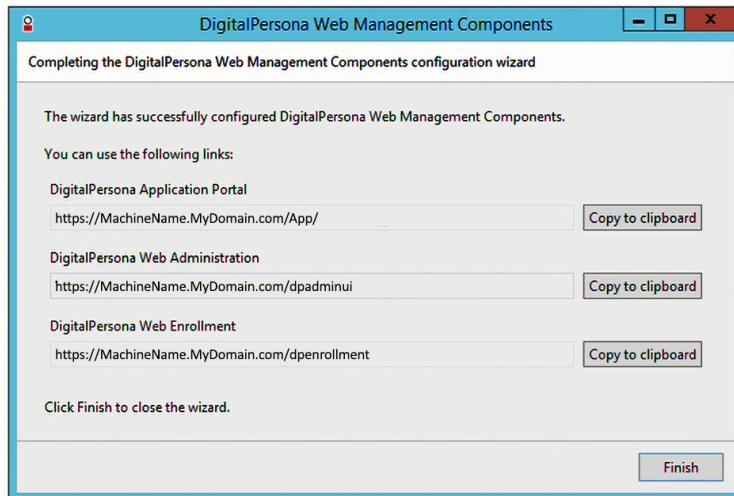
7. Click *Next* to continue.



8. The *Step-up Authentication* page enforces step-up authentication for the DigitalPersona Identity Server when any of the selected conditions occur.
- Select the desired conditions for step-up authentication.
 - Enter the URL to the behavioral biometrics server provided to you during implementation.
 - Specify up to three credentials that will be required for authentication when the step-up conditions occur.
 - To add additional credential combinations, click *Add more*.
9. Click *Next*. For more about step-up authentication, see the topic *Identity Server configuration (DigitalPersona IIS Plugin)* on page 184.



10. On the *Apply configuration* page, verify the actions and parameters listed and click *Next*.

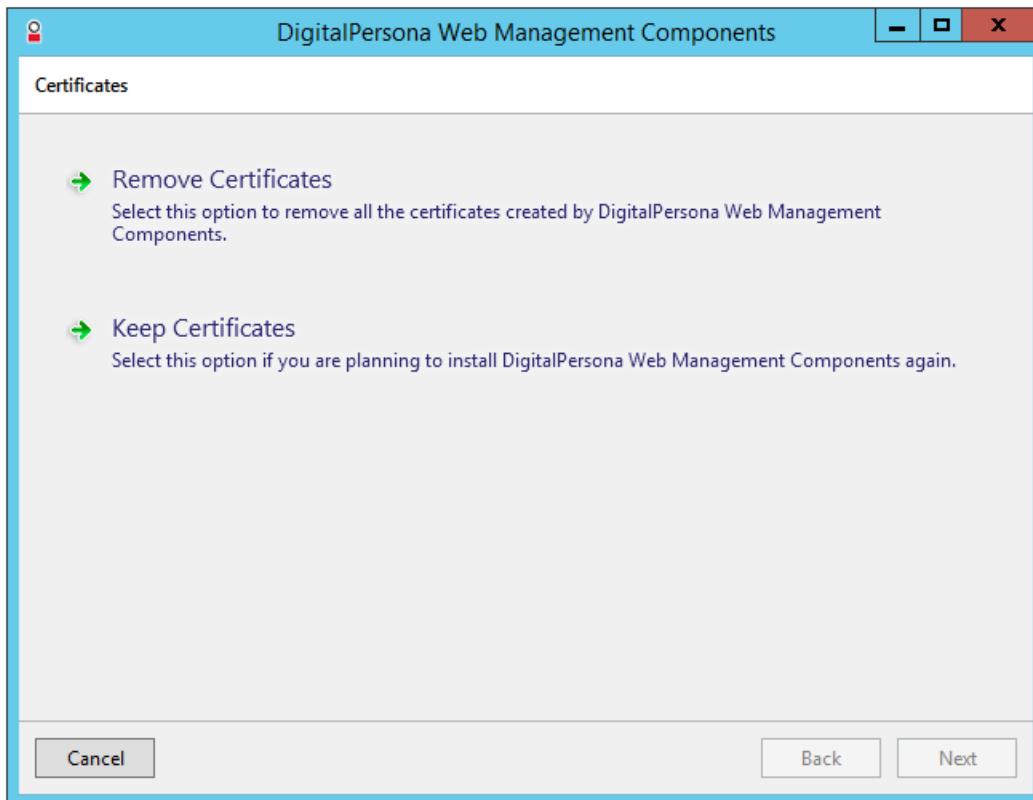


11. On the final page, the URLs to the three resulting web applications are shown. (Although there are five components, there are only three web applications.) Click the button next to a URL to copy it to the clipboard so that you can open it in a supported browser. You may also want to create shortcuts to these pages for distribution to users. After testing the URLs and your ability to log in to the web applications, click *Finish* to close the wizard.
12. For *Advanced configuration*, stop here.

Uninstallation

The DigitalPersona Web Management Components can be uninstalled using the Windows Control Panel.

During uninstallation, a dialog displays that allows you to remove any certificates that were created automatically by the DigitalPersona Configuration wizard.



If you choose to remove the certificates created by DigitalPersona

- When upgrading, new certificates will have to be created, either automatically or manually.
- For deployments of DigitalPersona SSO for Office 365, you will need to update the federation setting to Azure.

If you choose to keep the certificates created by DigitalPersona

- When upgrading, the saved certificates will be used
- For deployment of DigitalPersona SSO for Office 365, no changes will need to be made.

THIS CHAPTER DESCRIBES HOW TO ASSIGN THE NECESSARY PERMISSIONS THAT WILL ALLOW DELEGATION OF SECURITY OFFICER FUNCTIONS TO A DELEGATED USER OR GROUP.

Overview

Within the DigitalPersona AD solution, the Security Officer, or other delegated user(s) or groups can be assigned the necessary permissions to supervise Attended Enrollment through the Attended Enrollment or Web Enrollment applications. Note that a Security Officer group is not created automatically, but if desirable, must be created manually in Active Directory.

Additionally the same or different user(s) or group(s) can be granted specific permission to

- Enroll and manage DigitalPersona credentials
- Recover user passwords
- Unlock user Windows accounts
- Omit required credentials during Attended Enrollment
- Import OTP token seed files

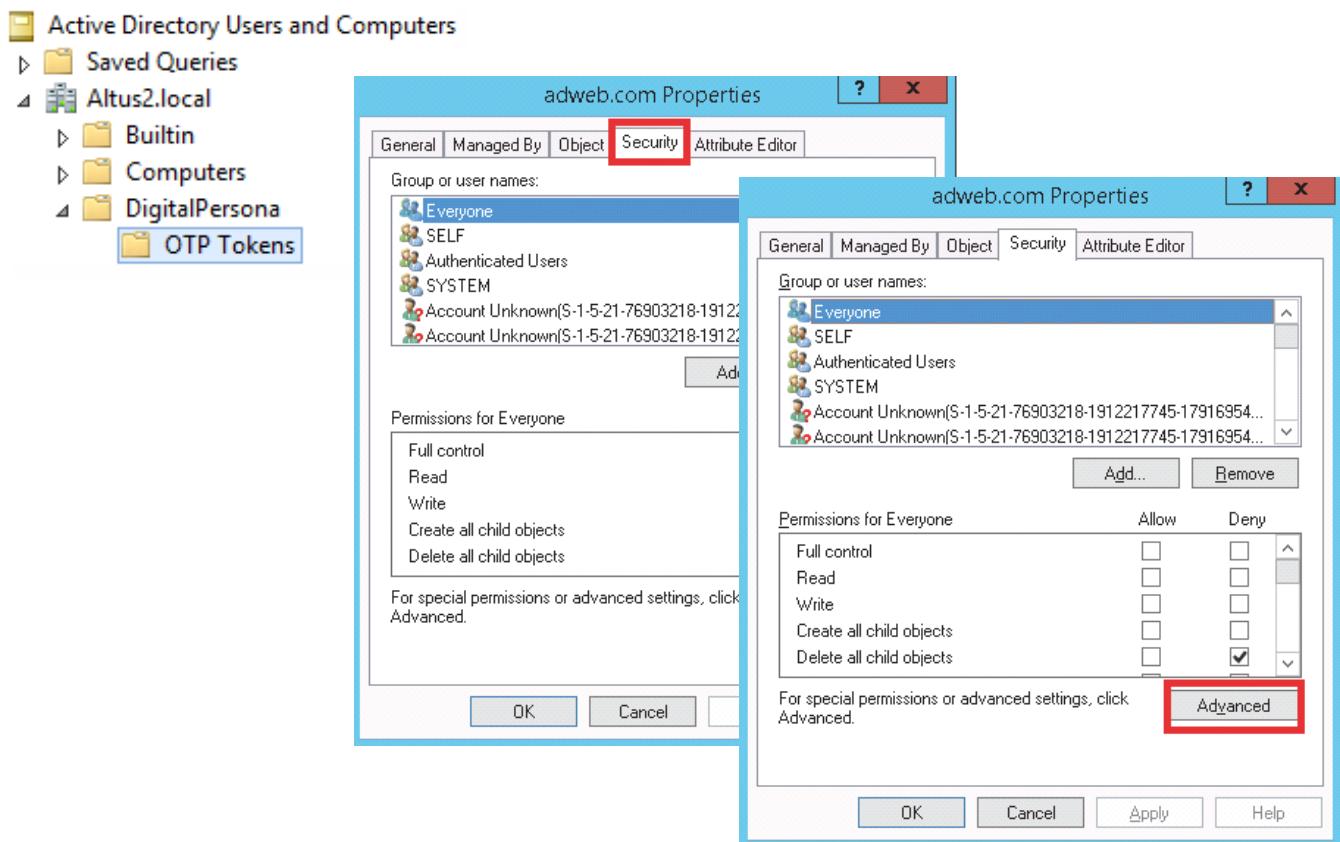
The following table lists the Windows permissions and properties which must be assigned in order to enable each of the above functions.

Permitted task	Windows permission/property	Applies to
Enroll/manage credentials	Register/Delete Fingerprint (DigitalPersona)	Descendant User objects
Recover user's Windows password	User Recovery (DigitalPersona) Reset Password	Descendant User objects
Unlock account that is locked due to invalid DigitalPersona credentials	Write dpLockout Time	Descendant User objects
Omit required credentials	Write dpOmitReasons	Descendant User objects
Import hardware OTP token seed file	Create dpOTPToken Objects Delete dpOTPToken Objects Write all properties	Descendant User objects Descendant User objects Descendant dpOTPToken objects

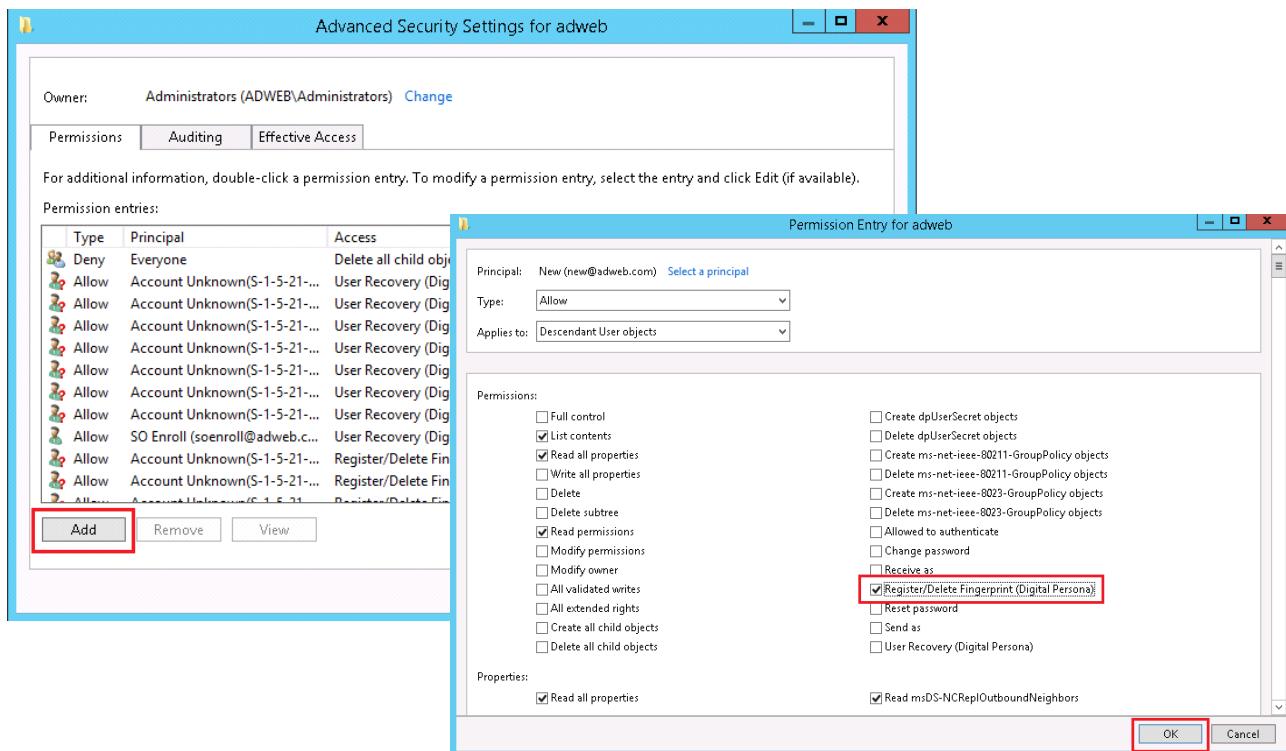
Assigning permissions

The following steps apply to all the available DigitalPersona permissions that may be assigned to Security Officers, except for the *OTP Tokens* permission, which is handled a bit differently and described on page 179.

1. Launch the *Active Directory Users and Computers* snap-in.
2. From the *View* menu, select *Users, Contacts, Groups, and Computers as containers* and *Advanced Features*.
3. Right-click on the OU, group or user that you want to assign specific permission to and select *Properties*.
4. In the *Properties* dialog, click the *Security* tab.
5. Near the bottom of the dialog, click *Advanced*.



- In the *Advanced Security Settings* dialog, click *Add*.



- In the *Permission Entry* dialog, select a Principal, i.e. a user or group.
- From the *Applies to* dropdown menu, select *Descendant User Objects*.

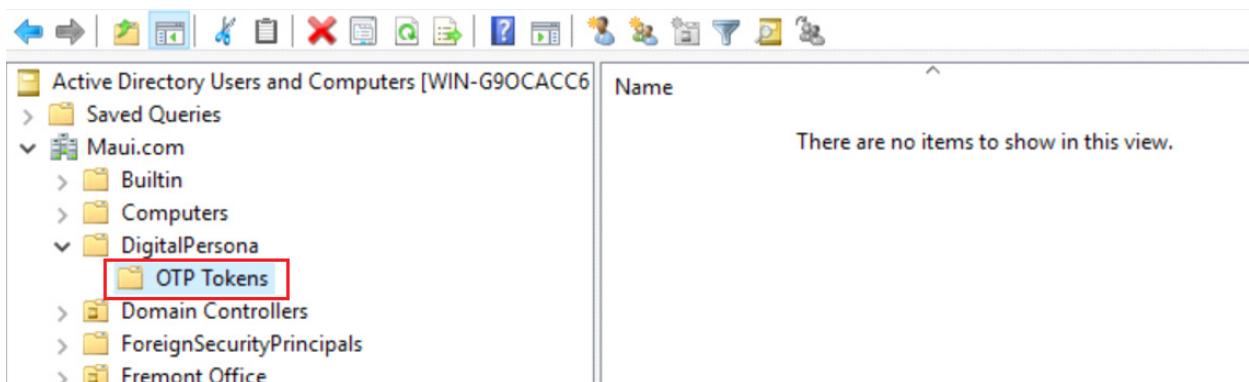
9. Select one or more of the following permission and properties that you want to assign to this Principal.

- Register/Delete Fingerprint (DigitalPersona)
- User Recovery (DigitalPersona) Reset Password
- Write dpLockout Time
- Write dpOmitReasons

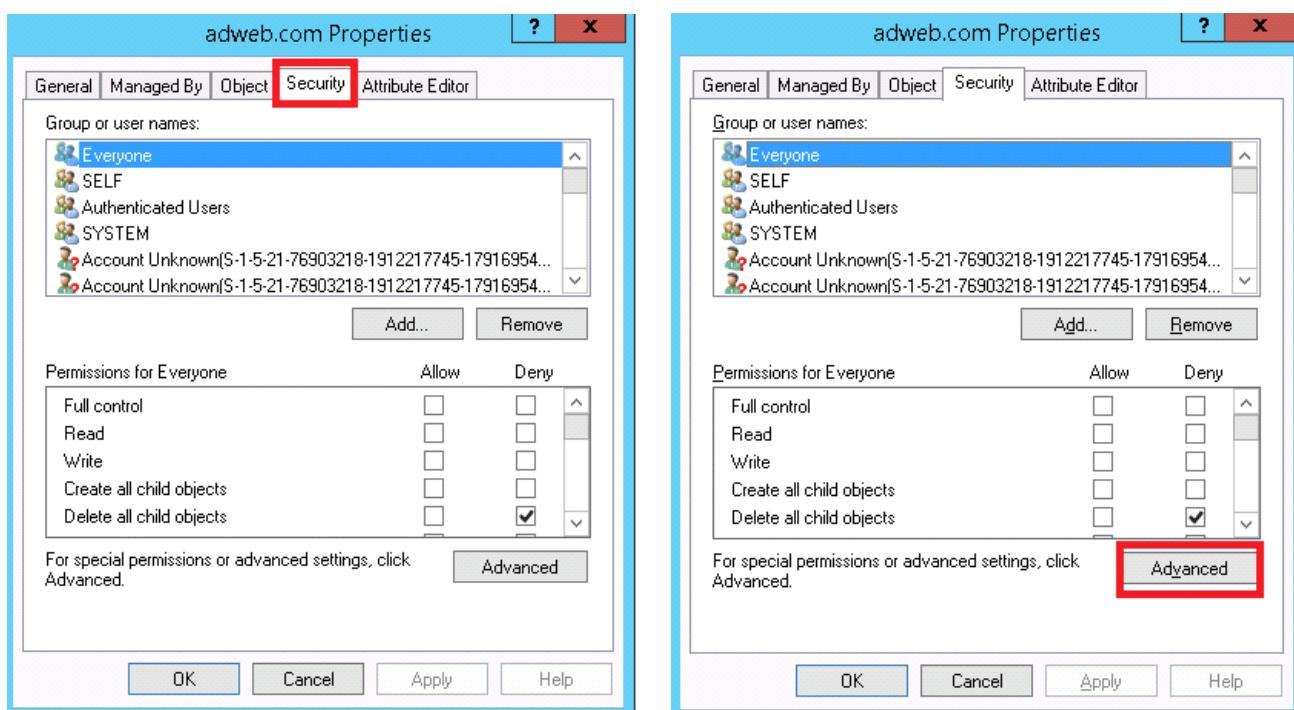
Assigning the OTP Tokens permission

The following steps apply only to assigning the *OTP Tokens* permission, as is handled a bit differently than the other permissions described in this chapter.

1. Launch the *Active Directory Users and Computers* snap-in.
2. From the *View* menu, select *Users, Contacts, Groups, and Computers as containers* and *Advanced Features*.
3. Expand the *DigitalPersona* node, right-click on *OTP Tokens* and select *Properties*.

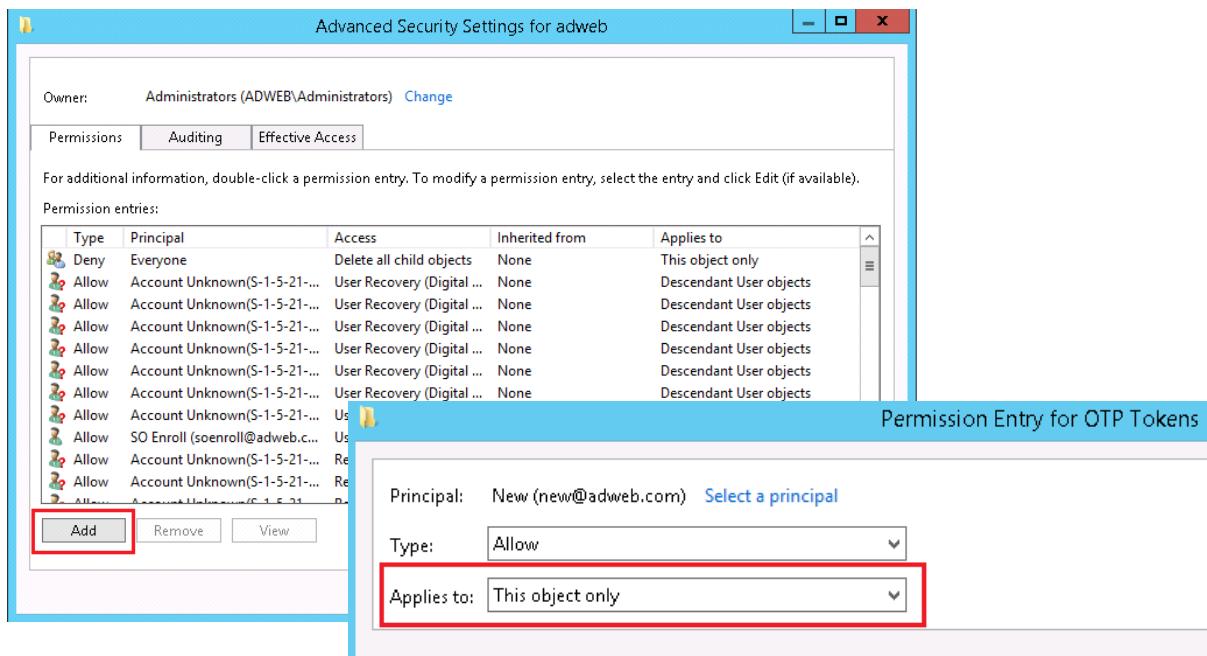


4. In the *Properties* dialog, click the *Security* tab.
5. Near the bottom of the dialog, click *Advanced*.



Assigning the OTP Tokens permission

6. In the *Advanced Security Settings* dialog, click *Add*.



7. In the *Permission Entry* dialog, select a Principal, i.e. a user or group.
8. From the *Applies to* dropdown menu, select *This object only*.
9. Select the following permissions.
- Write all properties
 - Create dpOTPToken objects
 - Delete dpOTPToken objects

THIS CHAPTER DESCRIBES THE DIGITALPERSONA IDENTITY SERVER AND ITS FEATURES.

Main topics in this chapter	Page
Identity Server features	182
Integrated Windows Authentication (IWA)	182
Multi-Factor authentication	182
Forgot password?	182
Unlock account?	183
Supported credentials	183
Identity Server configuration (DigitalPersona IIS Plugin)	184
Installation	184
Configuration details	185
General tab	185
STS options tab	185
Policy tab	185
Step-up policy tab	186
Web Portal tab	188
Additional configuration via .config files	188
Configuring STS to work with ADFS	188

The DigitalPersona Identity Server is used to identify and authenticate users logging in to DigitalPersona web applications such as the Web Administration Console, Web Enrollment and the Application Portal. It is also used as part of the DigitalPersona Office365 integration solution.

The figure consists of three parts. The left side shows two separate log-in pages for the 'DigitalPersona - Identity Server'. The top one is for 'DigitalPersona Web Administration' and the bottom one is for the 'DigitalPersona Application Portal'. Both pages feature a 'Domain\Username' input field and a 'PASSWORD LOGIN' button. The right side shows a single 'DigitalPersona - Identity Server' log-in page. This page includes a 'Domain\Username' input field and a 'PASSWORD LOGIN' button. Below these are several circular icons representing different authentication methods: a key icon for 'PASSWORD', a fingerprint icon for 'FINGERPRINTS', a face icon for 'FACE', a card icon for 'CARDS', and a USB drive icon for 'FIDO KEY'. At the bottom of this section are four smaller icons: a smartphone for 'ONE-TIME PASSWORD', a smartphone with a signal for 'SEND SMS', an envelope for 'SEND EMAIL', and a smartphone with a push notification icon for 'SEND PUSH NOTIFICATION'. The overall background has a faint watermark of a network or mesh pattern.

When presented with this webpage for the first time, if no other credentials have been enrolled yet, the user enters their domain and user name in the format *Domain\Username* or *username@domain* and clicks the arrow to the right of the password field.

- Once credentials are enrolled, users can select which credential to use by clicking one of the credential tiles and submitting the specified credential.
- The system will remember the last used credential and automatically select that credential the next time the user visits the page. If a combination of credentials is required, any additional credentials will be requested automatically after authentication with a previous credential.
- When an Enhanced Logon Policy is triggered, the user will first see tiles for any credentials required by the standard Logon Policy. Once a credential is authenticated, tiles for any additional credentials required by the Enhanced Logon Policy will be displayed.

Identity Server features

Integrated Windows Authentication (IWA)

When Integrated Windows Authentication is selected as the single credential for logon to the DigitalPersona Identity Server and a user launches any federated application accessed through the DigitalPersona Identity Server (from a domain-joined computer where a DigitalPersona Workstation or DigitalPersona Lite Client is installed), and if no additional credentials are specified in an authentication policy, they will be automatically logged on without the need for further authentication.

Additionally, any federated applications accessed through the internal network will not need further authentication.

If there are additional credentials specified for authentication to the Identity Server, the user will automatically be authenticated with their Windows credentials and will only need to submit the additional credential. For example, if the authentication policy for the Identity Server is set to require *Windows Authentication* and *Fingerprint* credentials, the user will simply need to scan their fingerprint.

Note that if a policy includes IWA as a factor and Step-up authentication is enabled, then any additional factors defined for step-up authentication will always be required since there is no trackable user behavior available to complete training by the step-up authentication feature.

Multi-Factor authentication

One of the primary benefits of the DigitalPersona solution is the easy implementation of multi-factor authentication (MFA), i.e. requiring more than one credential in order to log on to web-based services protected by the DigitalPersona Identity Server.

When DigitalPersona MFA is enabled and you have logged on for the first time, the system will remember which credentials you have used to log on with, and the sequence they were used in. For example, if you used your Windows Password first and your fingerprints second, the next time you go to log on, you will not have to select these, but will automatically be presented with the UI necessary to authenticate with those credentials in that order.

Forgot password?

If a user has forgotten their password and cannot log in to the Identity Provider, they can click the *Forgot password?* link to have a link emailed to them which will enable them to reset their password.

- Upon clicking the link, the user will be asked for their user name.
- After entering their user name, an email will be sent to the email address associated with their Active Directory account.
- The user clicks on the link provided in the email and is directed to a page where they can provide the answers to their previously enrolled Recovery Questions.

- Upon successfully answering their Recovery Questions, they are presented with a *Password Reset* page, where they can reset their password.

In order to use this feature, the following four GPOs must be enabled.

- Allow users to reset their Windows password* - If this GPO is not enabled or not configured, the *Forgot password?* link will not be shown on the Identity Provider login page.
- Enable Recovery Questions* - This GPO is enabled by default, but if disabled, the link will be displayed but users will not be able to reset their password from this page with this feature.
- Path to DigitalPersona Secure Token Server (STS)* - This must be enabled and a valid URL to the DigitalPersona STS Server entered in order for the system to send the password reset link to the user.
- SMTP Configuration* - This must be enabled and properly configured in order for the system to send the password reset link to the user.

Of course, users must have previously enrolled their Recovery Questions as well.

Unlock account?

If a user account has been locked out from too many failed password attempts, they can click the *Unlock account?* link on the Identity Provider login page to unlock their account. They will be asked for their user name and the answers to their previously enrolled Recovery Questions.

Note that this will *not* unlock the user's account if the account has been locked due to failed authentication attempts with other DigitalPersona credentials. For this type of account lock, use the *Unlock the account* button in the Web Administration Console.

Upon successfully answering their Recovery Questions, the user's account will be unlocked.

In order to use this feature, the following two GPOs must be enabled.

- Allow users to unlock their Windows account using DigitalPersona Recovery Questions* - If this GPO is not enabled or not configured, the *Unlock account?* link will not be shown on the Identity Provider login page.
- Enable Recovery Questions* - This GPO is enabled by default, but if disabled, the link will be displayed but users will not be able to unlock their account with it.

Of course, users must have previously enrolled their Recovery Questions as well.

Supported credentials

Credential	IE	Edge	Chrome	Firefox	Safari	iOS	Android	Comments
Password	Y	Y	Y	Y	Y	Y	Y	
Fingerprint	Y	Y	Y	Y	N	N	N	
Cards	Y	Y	Y	Y	Y	Y	Y	Smart, Contactless and Proximity Cards
OTP	Y	Y	Y	Y	Y	Y	Y	SMS, Email and Push Notification
PIN	Y	Y	Y	Y	Y	Y	Y	
FIDO	N	N	Y	Y	Y	N	N	
Face	N	Y	Y	Y	Y	Y*	Y**	* Face credential requires iOS11+ and the Safari browser. ** Face requires Android 7.0+ and the Chrome or Firefox browser.

Credential	IE	Edge	Chrome	Firefox	Safari	iOS	Android	Comments
Recovery Questions	Y	Y	Y	Y	Y	Y	Y	
Integrated Windows Authentication	Y	Y	Y	Y	Y	N	N	The device must be domain-joined.

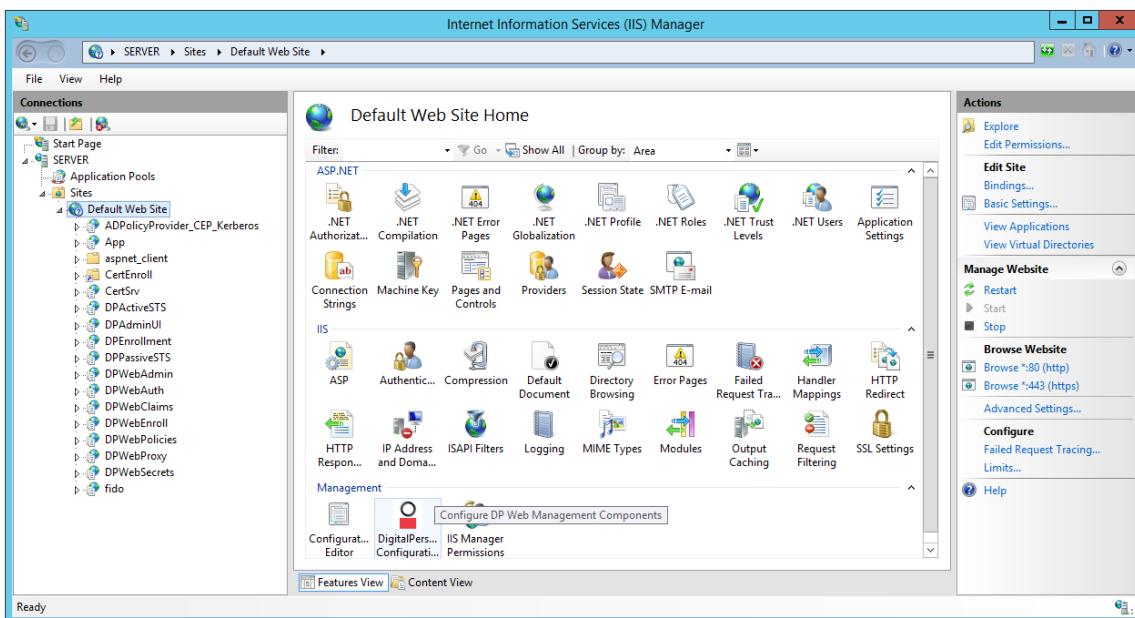
Note that if all credentials required by the logon policy in force are not supported on the browser and/or the device being used to access the Identity Server, the following error message will be displayed.

Your browser or device does not support the required credentials, or they are not configured. Please contact your administrator.

Identity Server configuration (DigitalPersona IIS Plugin)

Configuration of the DigitalPersona Identity Server is accomplished through the DigitalPersona Configuration IIS Plugin, a Digitalpersona component that provides configuration of the DigitalPersona Web Management Components through the Microsoft Information Services (IIS) Manager.

Once installed, its icon will be displayed under the *Management* area for the *Default Website*.



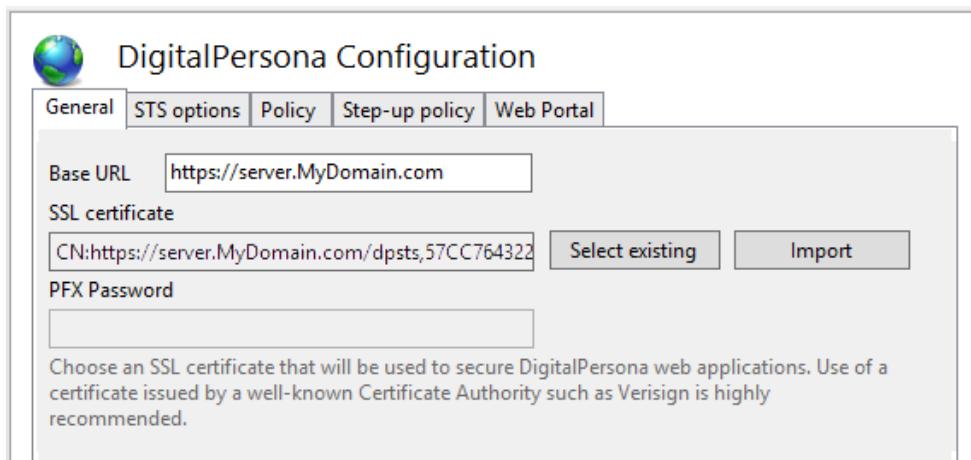
Installation

The DigitalPersona Configuration IIS plugin is installed by default as part of the DigitalPersonsa Web Management Components configuration wizard.

Configuration details

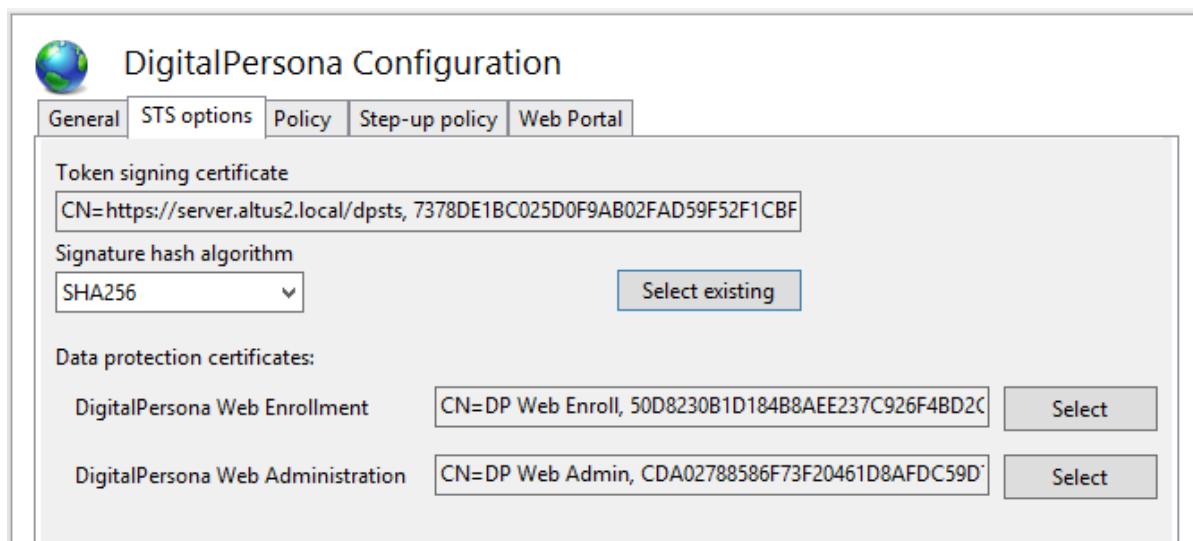
General tab

On the *General* tab, you can configure the Base URL for your DigitalPersona Server, and specify the token-signing and SSL certificates used by DigitalPersona. If the appropriate certificate is not automatically chosen, click the *Select existing* button to choose a previously created certificate stored on this computer or click *Import* to import a credential.



STS options tab

On the STS options tab, you can select the required STS certificates for token signing and data protection. If the certificates are not automatically chosen, click the *Select existing* or *Select* button to choose a previously created certificate.



Policy tab

On the Policy tab, you can specify each credential or credential combination that may be used to authenticate a user's identity when accessing web applications through the DigitalPersona Identity Server. Select additional credentials or

combinations from the available dropdown menus. Click *Add* to insert an additional line or click the associated **X** to delete a line.

Specify the combination of the policy credentials		
Password	+	No Auxiliary Credential
Fingerprint	+	No Auxiliary Credential
Face	+	No Auxiliary Credential
Contactless Card	+	No Auxiliary Credential
Smart Card	+	No Auxiliary Credential
One-time Password	+	No Auxiliary Credential
FIDO Key	+	No Auxiliary Credential
Add		

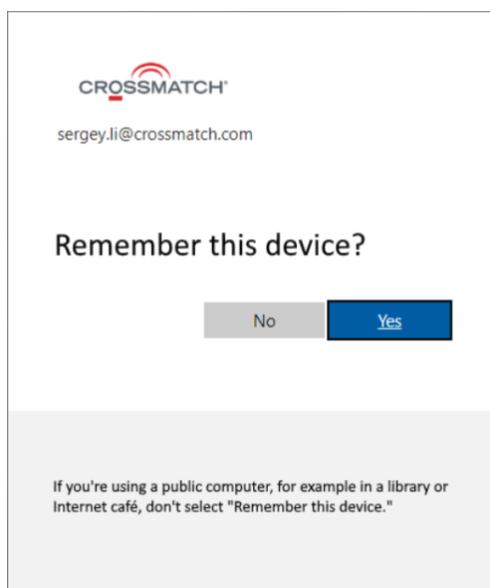
Step-up policy tab

On the *Step-up policy* tab, you can specify step-up authentication for the DigitalPersona Identity Server that is enforced when any of the selected conditions occur.

Step-up authentication will be enforced if the following conditions occur:					
<input checked="" type="checkbox"/> User keyboard biometrics are being enrolled or don't match (Requires password credential)					
<input checked="" type="checkbox"/> Computer Browser accessing IdP has changed					
<input checked="" type="checkbox"/> Computer IP address has changed					
Specify credential combinations for the step-up policy.					
Add					
Password	+	Fingerprint	+	No Auxiliary Cred	X

- Select the desired conditions for step-up authentication.
 - *User keyboard biometrics are being enrolled or don't match* - analyzes keyboard use and enforces step-up authentication when usage pattern deviates from historical data. Applies only to Password field. Enter the URL to the behavioral biometrics server provided to you during implementation.
 - *Computer Browser accessing IdP has changed* - Whenever the user accesses the Identity Server from a new browser, step-up authentication is enforced. Users will be prompted to *Remember this device*, immediately

after authentication of their credentials. The prompt will be in the form of a dialog box that looks like the following image.



- *Computer IP address has changed* - Whenever a user accesses the Identity Server from an untrusted or unknown IP address, step-up authentication will be enforced. The system will first check whether the IP address is within a specified trusted range. If it is, no step-up authentication is needed. If the IP address is *not* within the trusted range, the system will check the last five IP addresses that the user accessed the Identity Server from. If the current IP address matches one of them, no step-up authentication is required. If *not*, step-up authentication is enforced.

The trusted IP address range is specified by the administrator in the web.config file located at:

C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPSService\app.config

The information is added to the <AltusConfirm> node in the following format.

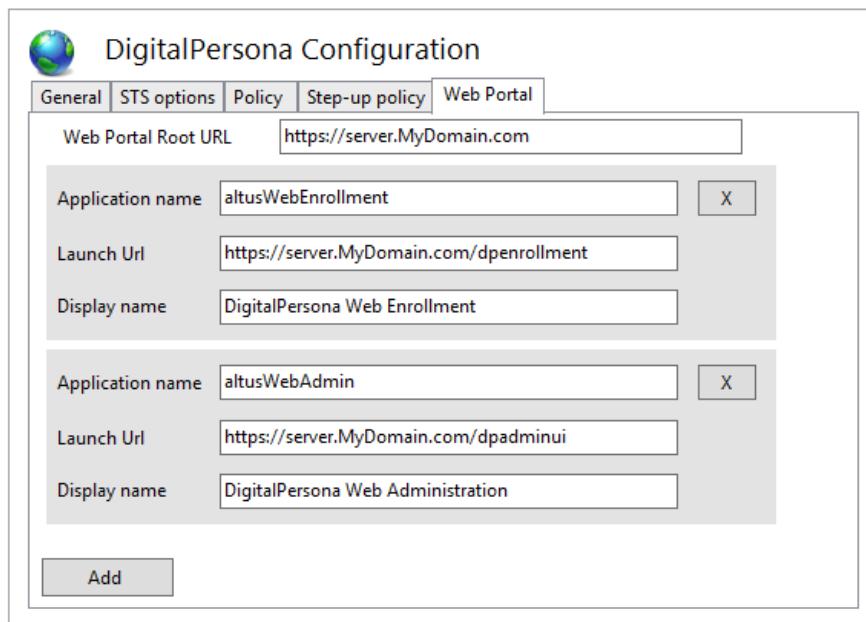
```
<TrustedIPs>
  <add StartAddress="192.168.56.102" EndAddress="192.168.56.199" />
<TrustedIPs>
```

Multiple ranges can be specified. To limit access to a single IP address, make the StartAddress and EndAddress the same.

- Specify up to three credentials that will be required for authentication when the step-up conditions occur. To add additional credential combinations, click *Add*.

Web Portal tab

On the *Web Portal* tab, you can enter the root URL for the DigitalPersona Web Portal as well as specify any web applications to be displayed on the DigitalPersona Web Portal.



Additional configuration via .config files

policyBypassGroups

The purpose of the `policyBypassGroups` setting is to provide a whitelist of *active logons* (service accounts with no UI) AD groups that can bypass the MFA policy currently in force when accessing various federated third-party applications (such as Office 365) that would otherwise require Multi-Factor Authentication. *Passive logons* (users that are presented with the Identity Server UI) will still be under enforcement of the authentication policy in force.

To create a `BypassGroups` policy

1. Open the `web.config` file from the following default location.

C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPActiveSTS

2. Create a new key/value pair in the `appSettings` section using the following format, where the value consists of the desired comma-delimited AD groups.

```
<appSettings>
...
<add key="policyBypassGroups" value="SomeADGroup1, SomeADGroup2" />
</appSettings>
```

Configuring STS to work with ADFS

In order to add DigitalPersona Identity Server (STS) features to ADFS, you need to establish a Claim provider trust. This is accomplished through the following procedure.

Add ADFS Relying Party to STS

1. Locate the PassiveSTS *web.config* file. You can find it at the following location on your DigitalPersona Server (after installation of the Web Management Components).

C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPPassiveSTS\web.config

2. Open the file with your favorite text editor and find the following section.

```
<add Realm="http://adfs.domain.com/adfs/services/trust" DisplayName="DigitalPersona ADFS Relying Party"
    ReplyUrl="https://adfs.domain.com/adfs/ls" TokenType="urn:oasis:names:tc:SAML:1.0:assertion"
    AllowPolicyOverride="false">
    <ClaimMappings>
        <add key="sub" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier" />
        <add key="name" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" />
        <add key="amr" value="http://schemas.microsoft.com/claims/authnmethodssreferences" />
        <add key="dom" value="http://www.crossmatch.com/altus/claims/user_domain" />
        <add key="uid" value="http://www.crossmatch.com/altus/claims/original_id" />
        <add key="http://www.crossmatch.com/altus/claims/web_auth_jwt" />
        <add key="http://www.crossmatch.com/altus/claims/auth_policy" />
        <add key="wan" value="http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname" />
        <add key="group" value="http://schemas.xmlsoap.org/claims/Group" />
        <add key="upn" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" />
        <add key="role" value="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" />
        <add key="oper" value="http://www.crossmatch.com/altus/claims/operation" />
        <add key="ad_guid" value="http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID" />
        <add key="mail" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" />
        <add key="sid" value="http://schemas.microsoft.com/ws/2008/06/identity/claims/principalsid" />
    </ClaimMappings>
</add>
```

3. Replace *adfs.domain.com* within the first and second lines with the machine name and domain where AD FS is installed.
4. Save the file.

Create an ADFS Claim Provider trust

1. Locate the PowerShell script *DPCA STS Script.ps1*. You can find it at the following location on your DigitalPersona Server (after installation of the Web Management Components).

C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPPassiveSTS\DPCA STS Script.ps1

2. Open the file with your favorite text editor and find the following section.

```
$sts_metadata_url = 'https://sts.domain.com/dppassivests/wsfed/metadata'

$transform_rules = @"
@RuleTemplate = "PassThroughClaims"
@RuleName = "Pass Through Name Identifier"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"]
=> issue(claim = c);

@RuleTemplate = "PassThroughClaims"
@RuleName = "Pass Through Name"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"]
=> issue(claim = c);
```

3. Replace *sts.domain.com* within the machine name and domain where STS was installed.
4. Save the file.
5. Run the script on your ADFS server.

THIS CHAPTER DESCRIBES THE DIGITALPERSONA WEB ADMINISTRATION CONSOLE AND ITS FEATURES.

Topic	Page	Topic	Page
Logging in	190	Recover password (user recovery)	192
Administration Console features	191	Unlock the account	193
Features summary	191	Manage Credentials	193
Display user details	192	Manage Hardware OTP Tokens	193

Overview

The DigitalPersona Web Administration Console provides a convenient web based way to administer DigitalPersona users. From the console, an administrator can manage DigitalPersona users and the most common user policies. Additional user settings and policies can be configured in Active Directory.

The DigitalPersona Web Administration Console can be accessed through any of the web browsers listed in the system requirements on page 17 as long as it has JavaScript enabled. When accessing the console remotely, only credentials (such as Passwords and OTP) that do not require attached hardware (fingerprint and card readers, for example) can be used to log on to the console, unless a DigitalPersona client (such as DigitalPersona Workstation, Kiosk or Lite Client) is also installed on the machine.

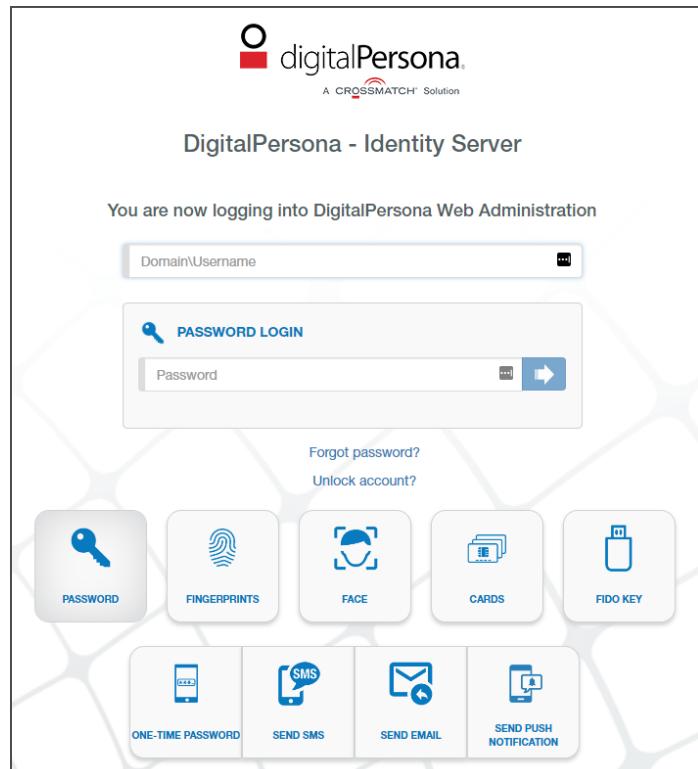
Logging in

Any domain user can log in to the DigitalPersona Administration Console, although specific Windows permissions (as described in *Assigning Security Officer permissions* beginning on page 177) must be assigned to the user (or the user's group) in order to make any changes. Domain administrators do not need additional permissions to make changes.

To log on to the console

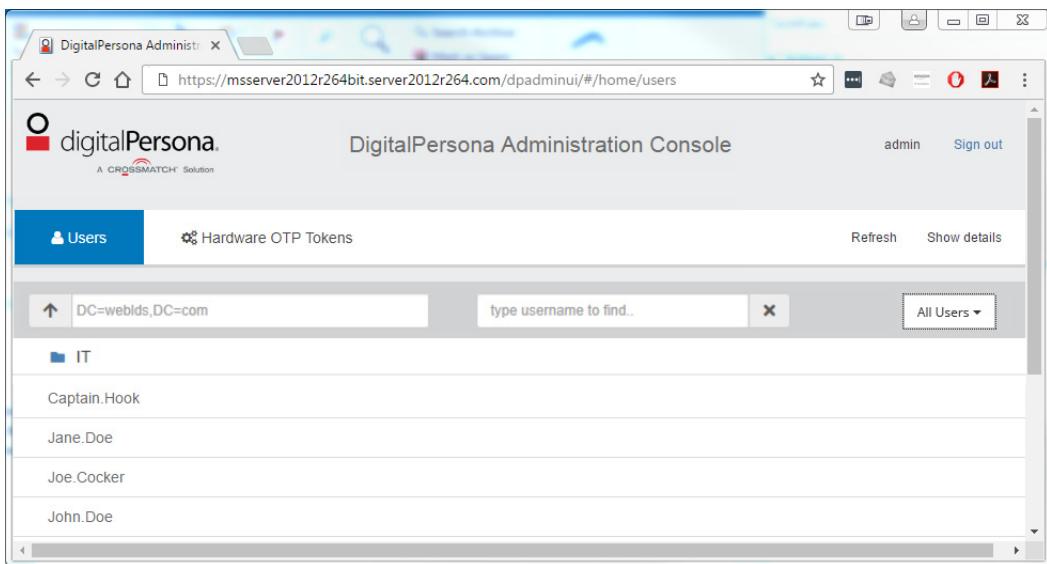
- On the DigitalPersona Identity Server webpage, enter your domain\username and password, or select one of the displayed tiles to use a different previously enrolled authentication credential.
- If a multi-factor authentication policy is in effect, the tile for the next required credential will become highlighted after successful authentication with the first one, and any fields necessary for use of the credential will be displayed. The system will learn your most used credentials and suggest them in the order you generally use them.

Note that the specific credential tiles that appear on the Identity Server page and any combination of credentials that may be required to log in are configurable by the DigitalPersona Administrator.



See *Identity Server configuration (DigitalPersona IIS Plugin)* on page 184 for details.

Administration Console features



The following sections describe the features available through the DigitalPersona Administration Console.

Features summary

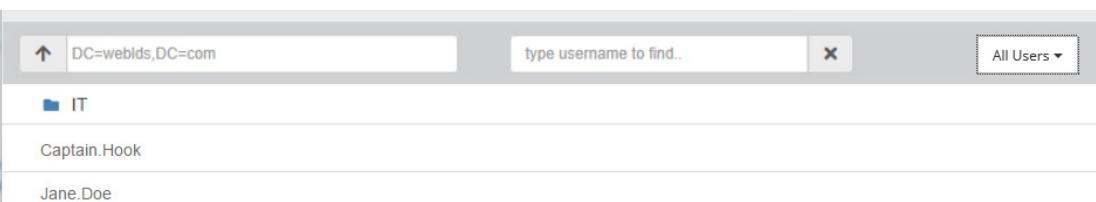
Through the console, the administrator can perform the following activities. Further details are provided in the sections that follow.

- Search for and filter users
- Display User Details including the credentials enrolled for each user
- Remove a user's credentials
- Recover a user's password
- Unlock a user account
- Manage user credentials
- Manage hardware OTP tokens

Additionally, the types of credentials displayed, and the policies specifying which credentials or credential combinations are required for authentication or log in to the DigitalPersona Web Administration Console (through the DigitalPersona Identity Server) may be specified through the DigitalPersona IIS module plug-in. See *Identity Server configuration (DigitalPersona IIS Plugin)* on page 184 for details.

Search for and filter users

Use the Search field and Users drop down menu to search for and filter users by their status., i.e. All Users, Disabled Users or Locked Users. Click on an OU to display users within that Organizational Unit or the Up arrow to view a parent OU.



Note that users are listed by their Windows Display Name and therefore cannot be searched by their SAM account name.

Display user details

Most of the user properties and settings are accessed from the *Details* panel, which by default is hidden when first logging into the console. This panel displays user details, properties, credentials and task buttons. It also indicates whether any credentials required during Attended Enrollment were omitted and shows the reason the administrator provided for their omission.

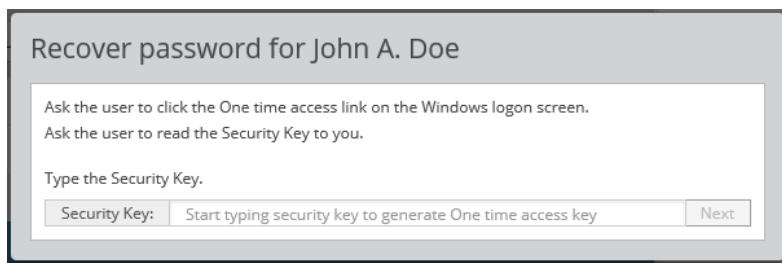
To open the *Details* panel, select a user and click *Show details*. When details are being displayed, *Show details* changes to *Hide details*.

Recover password (user recovery)

The DigitalPersona Administration console provides assisted access to a user's Windows account, with minimal involvement of the DigitalPersona Administrator or Helpdesk personnel, through the recovery link provided on the Windows logon screen when DigitalPersona Workstation or Kiosk are installed on the machine.

To recover a user's Windows access

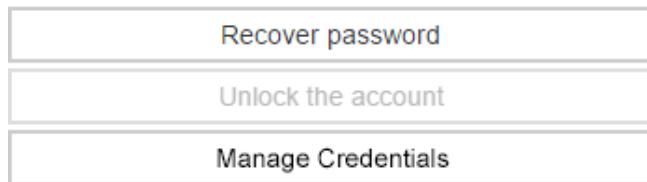
- 1 On the *Users* tab of the DigitalPersona Administration Console, select the user and click *Recover password* to display the following dialog.



- 2 Ask the user to click the *Can't access your account* link (Windows 7) or *Options/One-time access code* button (Windows 8 and above) on the Windows logon screen.
- 3 The user will read the Security Key displayed on the screen.
- 4 A DigitalPersona administrator or designated person types the Security Key into the User recovery window and clicks *Next*.

Unlock the account

The *Unlock the account* button is used to unlock the account of a user whose account has been locked because of too many failed authentication attempts using DigitalPersona credentials. If the user's account is not locked, this button is disabled.



Once the account is locked, the button becomes active, and pressing it will unlock the specified user's account.

Note that this cannot be used to unlock an account that has been locked by Windows due to excessive failed attempts at entering a Windows Password. In this case, use the *Unlock account?* link on the DigitalPersona Identity Server page.

Manage Credentials

To manage the credentials of a selected user

1. Select a user.
2. If user details are not shown, click *Show details*.
3. Click the *Manage Credentials* button.
4. The Web Enrollment application is displayed, where you can enroll and manage the user's credentials. See the *Web Enrollment* chapter for further details.

Manage Hardware OTP Tokens

In order to use hardware-based OTP tokens, you must import seed files provided by the hardware vendor to the DigitalPersona Server.

To import OTP hardware token seed files

1. Select the *Hardware OTP Tokens* tab (see image below).
2. The file format must be PKSC, although the actual file extension may be PKSC, xml or there may be no extension.
3. If the file is protected by an encryption key or a password, select the appropriate radio button and enter the encryption key or password provided by the token vendor.
4. Click *Import*.

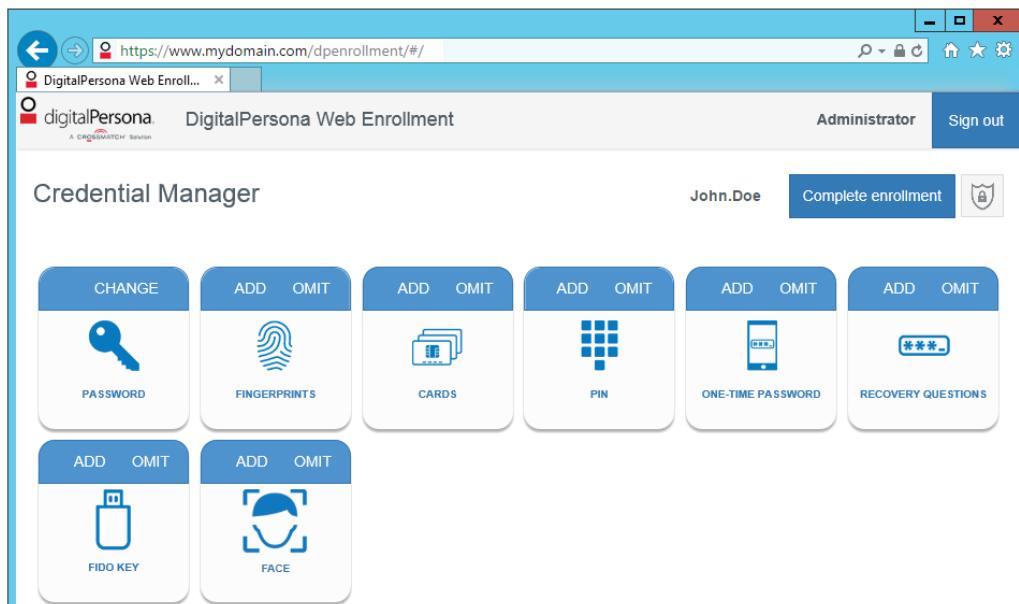
The screenshot shows the DigitalPersona Administration Console interface. At the top, there is a navigation bar with links for 'Users' and 'Hardware OTP Tokens'. The 'Hardware OTP Tokens' link is highlighted in blue, indicating it is the active page. On the left side, there is a sidebar with the digitalPersona logo and a 'CHOSDAWATCH Solution' section. The main content area is titled 'Hardware OTP Token Management' and contains instructions about importing device seed files. It includes fields for 'Device seed file:' (with a 'Browse' button), 'File protection:' (with radio buttons for 'Not encrypted', 'Encryption Key protected', and 'Password protected'), and two input fields for 'Enter preshared key' and 'Enter password'. A large 'Import' button is located at the bottom right of this section. At the very bottom of the page, there is a horizontal navigation bar with arrows for navigating between pages.

THIS CHAPTER DESCRIBES DIGITALPERSONA WEB ENROLLMENT, AN OPTIONAL COMPONENT FOR ENROLLING DIGITALPERSONA CREDENTIALS.

Main topics in this chapter	Page
Accessing Web Enrollment	196
Selecting a user for attended enrollment	196
Self Enrollment and credential management	197
Credential enrollment	197
Password credential	198
Fingerprints credential	199
Cards credential	200
PIN credential	201
One-Time Password credential	202
Recovery Questions credential	209
FIDO Key credential	210
Face credential	211
To assign, or remove Register/Delete permissions	213
Prohibit domain administrators from enrolling/deleting credentials	214

Overview

DigitalPersona Web Enrollment is a web based application that provides both attended (supervised) and unattended (self) enrollment and management of DigitalPersona credentials. It is compatible with most web browsers on popular desktop and mobile platforms. See the System Requirements on page 17 for details.



DigitalPersona Web Enrollment is an optional component included in the DigitalPersona Web Management Components package. For instructions on installing the package, see *Web Management Components* on page 62.

By default, Web Enrollment is configured to allow both attended enrollment and self enrollment by end users. Domain Administrators, DigitalPersona Administrators and Local Administrators on the machine where the Web Management Components package was installed are automatically assigned permissions to enroll other users.

Note that the UI is slightly different depending on whether a user is self-enrolling their credentials or enrollment is attended.

- Attended enrollment - If the *Require enrolling or omitting each credential GPO* is enabled, each tile displays both an *Add* and an *Omit* label. All displayed credentials must either be enrolled or specifically omitted with a reason given for the omission.
- Self-enrollment - There is no *Omit* label, since the UI does not require specific credentials to be enrolled.



Additional persons or groups can be assigned the *Register/Delete Fingerprint (DigitalPersona)* permission to enroll other users as well, and permission can be removed from any of the default groups. Note that the *Register/Delete Fingerprint (DigitalPersona)* permission actually affects all DigitalPersona credentials, not just fingerprints. The ability for end-users to enroll and manage their own credentials can also be disabled (See page 213.)

In order to use DigitalPersona Web Enrollment to enroll credentials that require a peripheral device (such as a fingerprint or card reader) a DigitalPersona client must also be installed on the same (Windows) computer, for example, DigitalPersona Workstation, DigitalPersona Kiosk, or DigitalPersona Lite Client.

Use of the One-Time Password (OTP) Push Notification or SMS features with the One-Time Password credential requires the administrator to create an account on the Crossmatch Push Notification Server (see page 204) and then enable and configure the OTP GPO in Active Directory (see page 3).

Accessing Web Enrollment

Access to Web Enrollment is through a URL created during installation and provided on the final page of the Web Management Components installation wizard. Navigating to the URL will first display the DigitalPersona Identity Server page for authentication, and upon successful authentication will then open the Web Enrollment application.

Prior to enrolling any credentials, users can log in with the Active Directory account name and password. Once additional credentials have been enrolled, they can use any of those credentials or credential combinations to log in (as specified by any authentication policy in force).

Selecting a user for attended enrollment

Any domain user with the *Register/Delete Fingerprint (DigitalPersona)* privilege assigned can select a user for web credential enrollment or modification either from within the DigitalPersona Web Administration Console (described in the previous chapter) or directly from the DigitalPersona Web Enrollment component.

To select a user for credential enrollment or modification

1. After authentication through the DigitalPersona Identity Server, enter the name of the user to manage. As soon as the first character of the name is entered, the *Manage user* button is enabled.

2. Click *Manage user*.
3. The *Credential Manager* page displays.

Self Enrollment and credential management

To self enroll, i.e. to manage a user's own credentials through DigitalPersona Web Enrollment

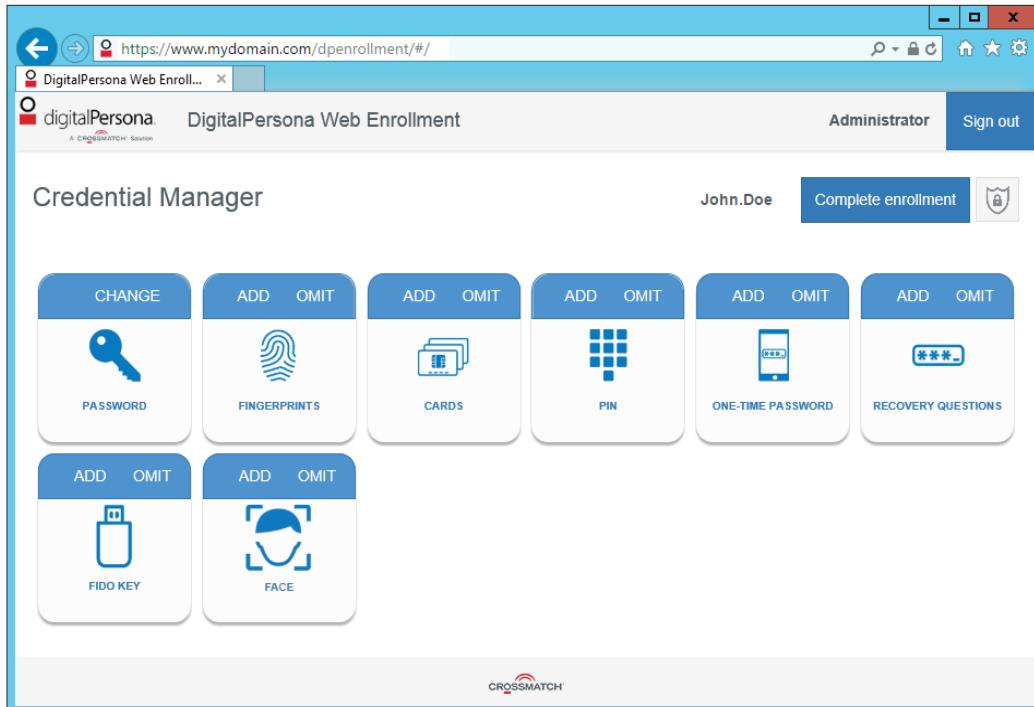
1. Navigate to the URL provided for Web Enrollment.
2. After authentication through the DigitalPersona Identity Server, click the *Self Enrollment* button.

The screenshot shows a web form titled "Self enrollment". It contains a text input field for specifying a user's name and a separate input field for a username. A large blue button at the bottom is labeled "Manage user".

3. The *Credential Manager* page displays.

Credential enrollment

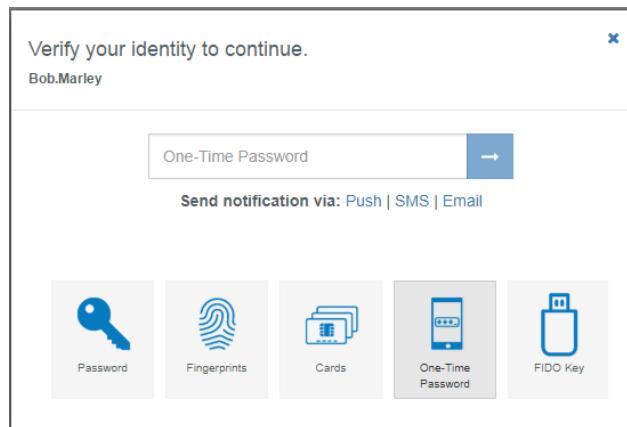
Once a user is either selected by an administrator or logged in (if self-enrolling), the *Credential Manager* page displays.



The Credential Manager page is the central location within Web Enrollment where a user's credentials can be enrolled and managed. Note that a Bluetooth credential is not available during Web Enrollment. This is because Bluetooth enrollment pairs the associated device directly with the machine where it is being enrolled, and most users will not be using a Bluetooth device to authenticate on the Web Enrollment machine.

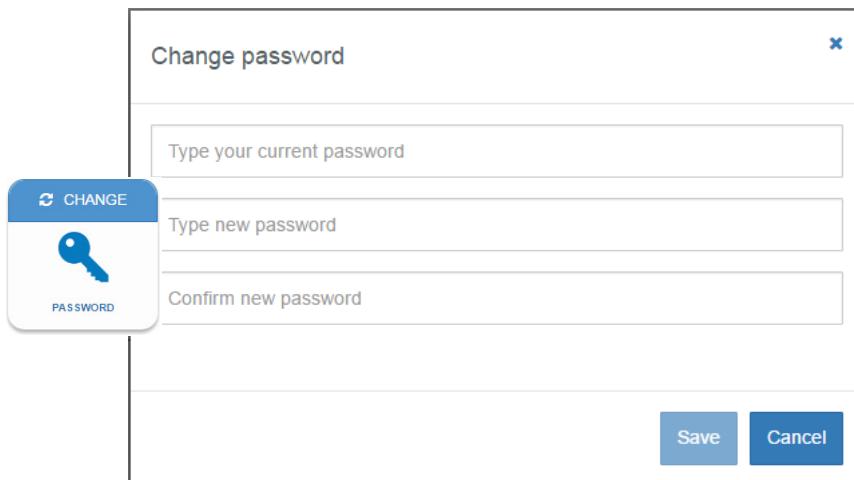
The tiles on the page, representing credentials and other information that may be captured by DigitalPersona in relation to a specific user, give access to pages where this information may be provided. Once a credential has been enrolled, the word ADD will be replaced with CHANGE.

The first time, within a browser session, that a user clicks a credential tile, they will be asked to verify their identity by submitting a previously enrolled credential. This may be their password or any other DigitalPersona credential that has been enrolled for their account.



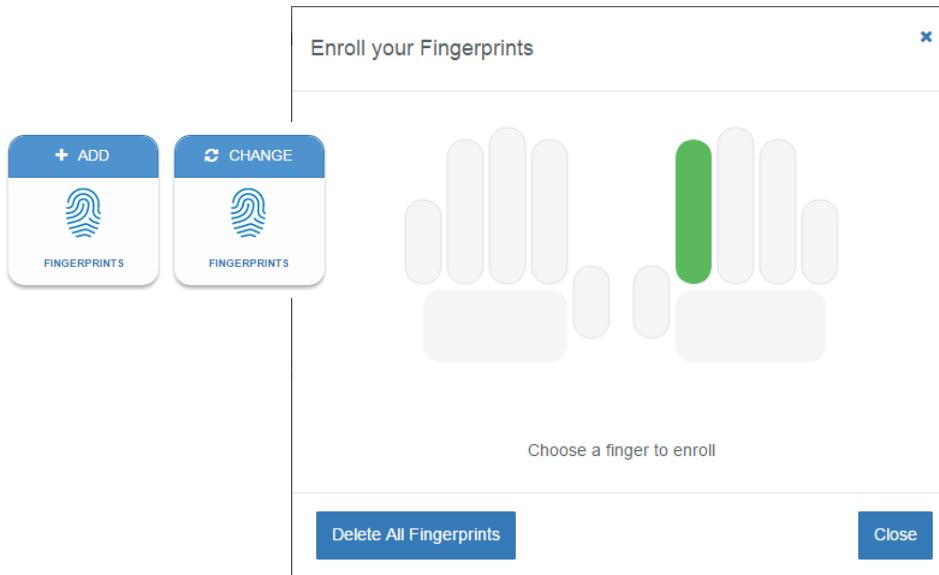
Password credential

The *Password* tile launches the *Change password* window, where a user can change their Windows password by entering their current password, and then creating and confirming a new password.



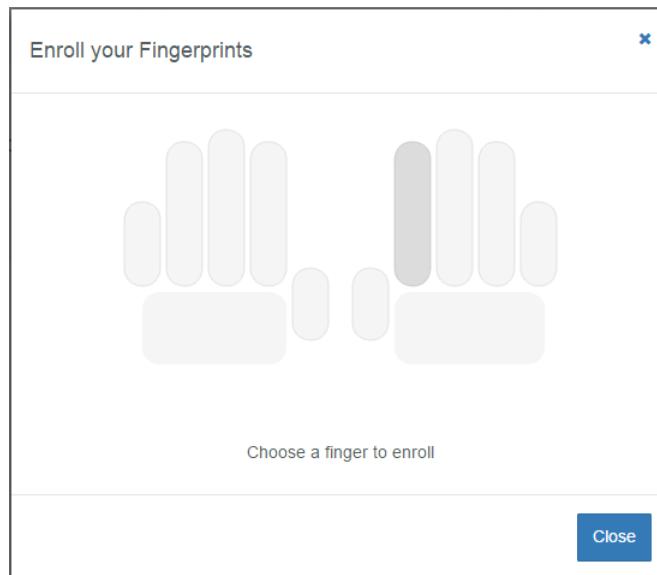
Fingerprints credential

If there is a supported fingerprint reader or ten-print scanner built into or connected to your computer, you can enroll and manage a user's fingerprints. Select the Fingerprints tile to display the Fingerprints page, where you can enroll a user's fingerprints credential.

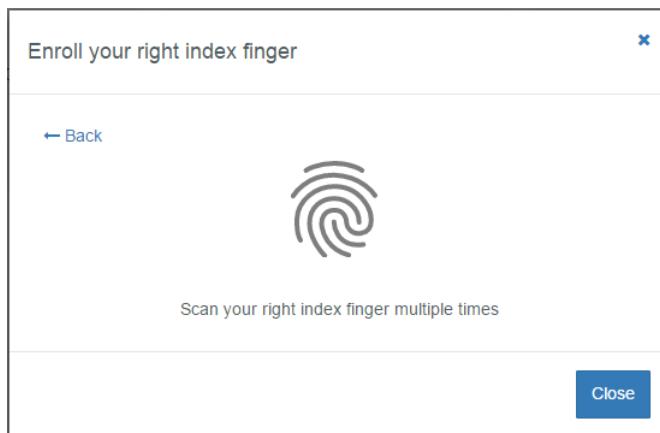


To enroll a fingerprint

1. Click the *Fingerprints* tile to display the *Enroll your Fingerprints* window.
2. Select a finger in the displayed hand image.



- Scan the selected finger as many times as necessary to enroll the fingerprint. Successful scans will show a temporary blue background on the fingerprint icon.



- When an adequate number of images have been captured, this window will close automatically and the *Enroll your Fingerprints* window will redisplay.
- Click *Close* to return to the Credential Manager page.

WARNING: When using the default DigitalPersona Fingerprint Engine, if any fingerprint being enrolled during this session, prior to clicking *Save*, is found to be a duplicate of an existing fingerprint for another user, *the other user's matched fingerprint will be deleted* and the current user's pending fingerprints will not be saved. An error message will display: The fingerprint cannot be enrolled. Contact your administrator for more information.

To delete a single fingerprint

- Click any highlighted finger.
- Confirm the deletion by clicking *OK* in the message box that displays.

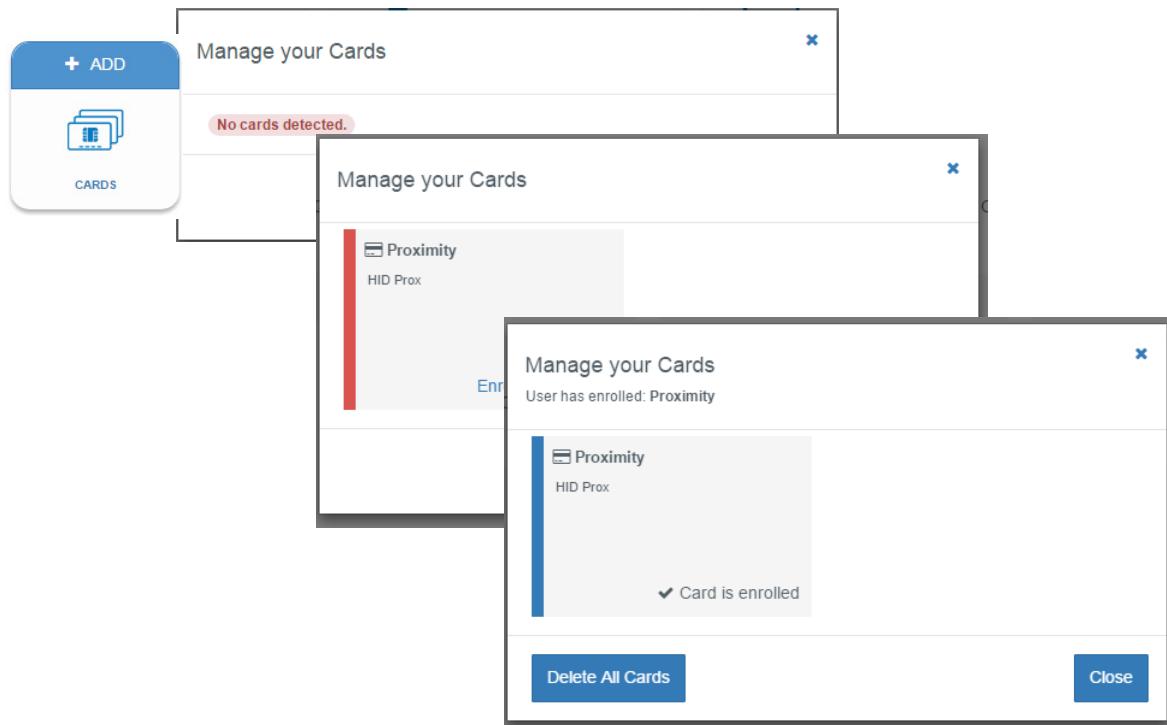
To delete the entire fingerprint credential

- Once the credential has been enrolled, a *Delete All Fingerprints* button is added to the *Enroll your fingerprints* window.
- Click *Delete All Fingerprints* and then click *OK* in the message box that displays to confirm the deletion.

Cards credential

This tile provides a means for enrolling a user's Smart, or Proximity Card credential.

Note that Smart Cards require separate middleware (ActiveClient and ActiveClient hotfix) installation on the enrollment machine. Contactless Cards are not supported in Web Enrollment.



To enroll a Smart Card or Proximity Card credential

1. Click *Add* or *Change* on the *Cards* tile to display the *Manage your Cards* window.
2. Insert a Smart Card into a built-in or attached card reader, or place a Proximity Card very close to the reader.
3. Click *Enroll this card*. Then click *Close*.

To delete all enrolled cards, click *Delete All Cards*. Individual enrolled cards cannot be deleted separately.

PIN credential

This tile provides a means for enrolling a user's PIN credential.

To enroll a PIN credential

1. Click the PIN tile to display the PIN window.
2. Enter and confirm a four-digit PIN.
3. Click *Save*.

One-Time Password credential

A One-Time Password (OTP) credential uses an automatically generated time-sensitive numeric code for authentication.

The OTP credential can be used for authentication to the DigitalPersona Identity Server, for providing access to the DigitalPersona Administration Console, DigitalPersona Web Enrollment and the DigitalPersona Application Portal, as well as for verifying one's identity when enrolling or managing one's credentials.

A QR Code scanner app on your device will greatly simplify the enrollment process for the software-based tokens, by automating the entry of required account information, although manual entry of the information is also possible.

The verification code may be generated in one of the following ways.

Authenticator app - A software token is generated by a special authenticator app on a user's mobile device, and the resulting time-sensitive code is used for authentication.

OTP Push Notification - A software token is generated by DigitalPersona and sent to a mobile device where the user can Accept or Deny its use for authentication. This feature is only available through the DigitalPersona authentication app. Although generation of the OTP is supported in third party authentication apps, Push Notification is only available through the DigitalPersona app.

OTP via SMS - A software token is generated by DigitalPersona, and a time-sensitive code that can be used for authentication is sent to a mobile device through SMS.

Hardware token - A dedicated hardware device generates a time-sensitive code used for authentication. The hardware token must be an OATH-compliant TOTP (Time-based One-Time Password) device.

OTP via email - A software token is generated by DigitalPersona, and a time-sensitive code that can be used for authentication is sent to the user's email address. By default, this option is not configured (and therefore unavailable to users), but can be enabled by the administrator through the *Allow sending OTP code over email* GPO setting. Also a valid SMTP server must be specified during configuration of the DigitalPersona Web Management Components package.

OTP Enrollment

The steps in the enrollment of an OTP credential differ slightly based on the type of OTP credential described above.

Authenticator app and Push Notification

Enrollment of an OTP credential to be used with an authenticator app will also automatically include the ability to make use of OTP Push Notification, but only if the DigitalPersona administrator has installed and configured the Crossmatch Push Notifications Server. Also, the associated *OTP* GPO setting must be enabled and configured by a DigitalPersona administrator as described in the chapter *Policies and Settings* on page 72.

However, during enrollment, you may choose *not* to use OTP Push Notification by selecting *Decline* on the *Push Authentication* page. If both the authenticator app and OTP Push Notification are enrolled, you can use either one for authentication.

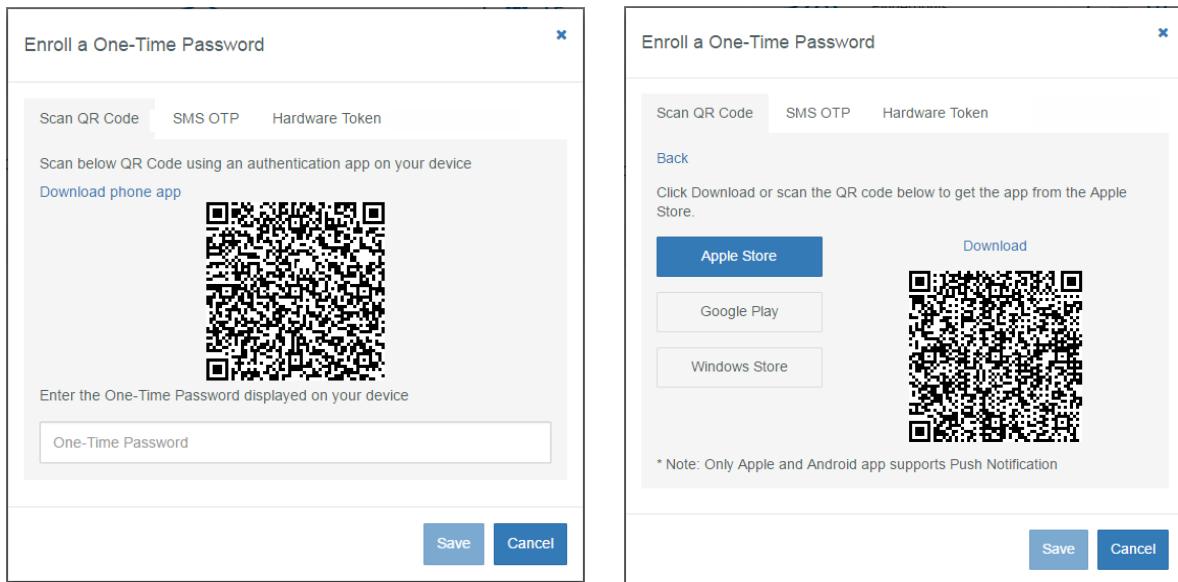
From a link in the One-Time Password window, you can download an OTP authentication app from various platform-centric app stores, and then enroll the OTP credential for use with the authenticator app (and OTP Push Notification, if configured and in the DigitalPersona app only) by scanning the QR Code shown on the screen or by manually entering the information required to create a DigitalPersona account in the authentication app.

The steps to enrolling a software-based OTP token to be used with an authenticator app or OTP Push Notification are:

- Download an authenticator app.
- Setup a DigitalPersona account on your device.
- Sign in to the DigitalPersona app
- Enroll the credential in the DigitalPersona Console

Download an authenticator app

- From the *Enroll a One-Time Password* window, click the *Download phone app* link to display the QR Code for downloading and installing an authentication app for your device. The windows will display a new QR Code for downloading the app and a means to choose which app store to download it from.



- Select your device's app store, and then scan the QR code provided or click the corresponding *Download* link.

The *DigitalPersona* app is currently available in the Apple Store and on Google Play. For the Windows mobile platform, the Microsoft and Google *Authenticator* apps provide nearly identical functionality, although setup and enrollment steps may vary slightly.

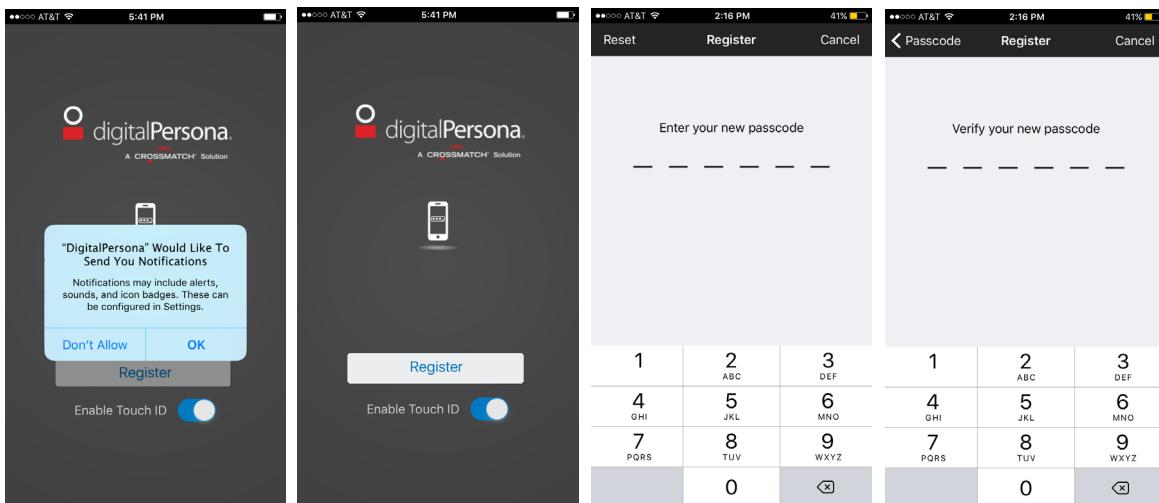
- Scanning the QR code with a QR Code scanner app on your device is the simplest procedure. It will automatically open your device's default web browser and display the product page for the selected Authenticator app so that you can download and install the app.
- Clicking the *Download* link shown above the QR Code will open the selected app store in your computer's default browser. Some app stores may require signing in and/or downloading the app and copying it to your device.

The instructions that follow are for the DigitalPersona app as installed on an iPhone. Instructions for the use of other authentication apps and devices may differ slightly.

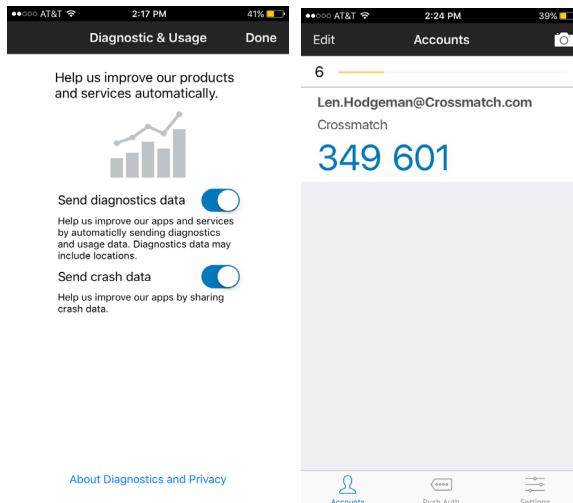
Set up a DigitalPersona account on your device

- Launch the authentication app on your device. The first time the app is launched, the *Register* screen displays. Click *OK* to allow the DigitalPersona app to send you notifications. Then click *Register*.

- Enter and verify a six-digit passcode.



- On the Diagnostic and Usage page, accept the defaults or tap an option to deselect it.

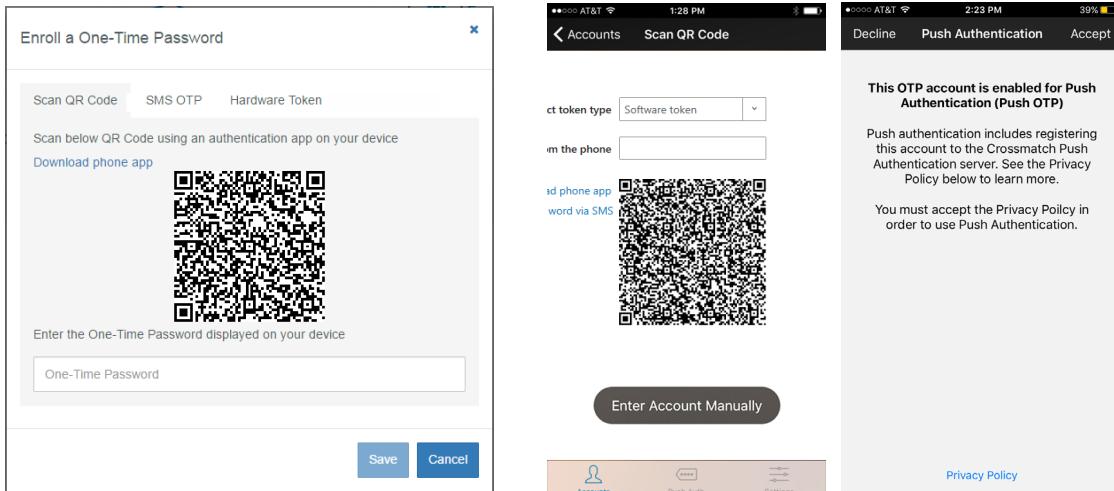


- On the *Accounts* screen, click the Plus sign (+). You will be asked for permission to access your device's camera. Tap *OK* if you want to use the camera to scan the QR Code for automatically creating your DigitalPersona Mobile account. If you click *Don't Allow*, you will need to enter account information manually.
- You can create the required account on your device *automatically* by scanning the QR Code displayed in the *Enroll a One-Time Password* window, or by entering the account data *manually*.

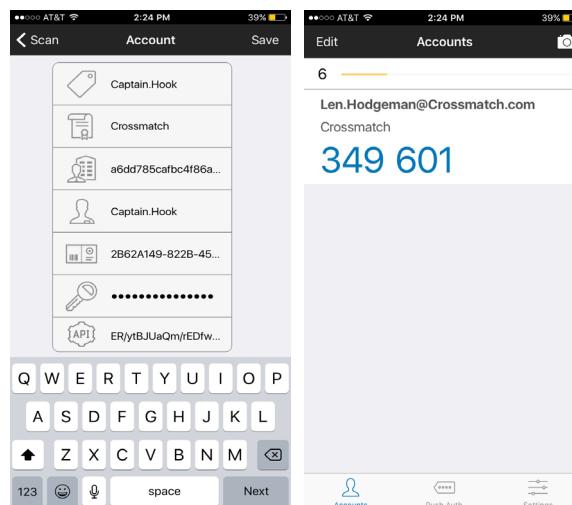
Account creation

- From the *Scan QR Code* tab, scan the displayed QR code. Do not scan the QR code that was used to download the app.

If the Crossmatch Push Authentication Server has been previously setup by your DigitalPersona Administrator, Push Authentication will be automatically enabled for your device once you choose to *Accept* the associated Privacy Policy. If you choose to *Decline* the Privacy Policy, Push Authentication will not be enabled.



- Once the account information is displayed, tap *Save*. The DigitalPersona Mobile account will be created and the *Accounts* screen displayed with the new account and your first One-Time Password shown.



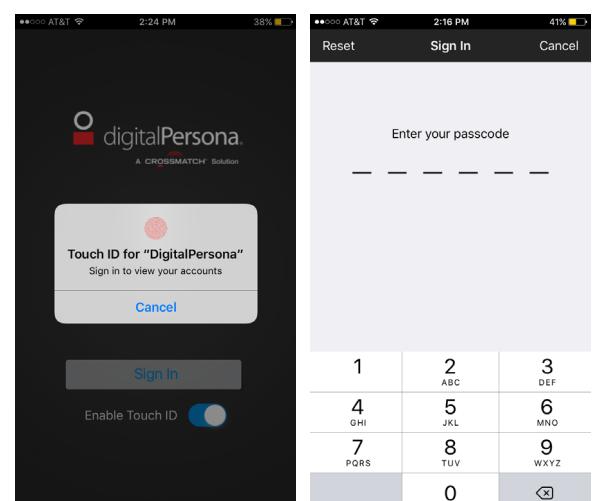
Manual account creation

Manual account creation is not available in version 3.0 and above.

Sign in to the DigitalPersona Mobile app

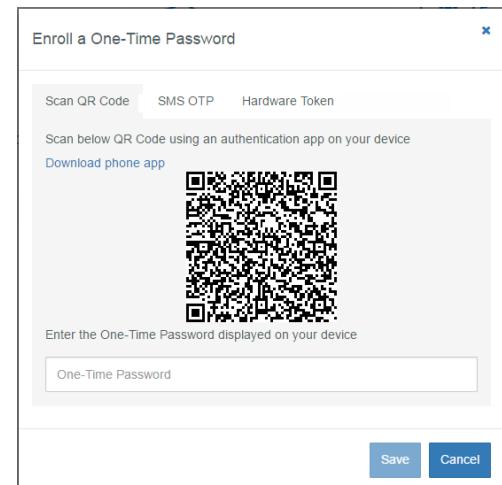
Once you have registered as described in the previous pages, you can sign in to the app as follows.

- Launch the DigitalPersona app.
 - Sign In.
- Fingerprint enabled devices - You can enable fingerprint authentication to the DigitalPersona Mobile app by selecting *Enable TouchID* on the Sign In screen or later in the DigitalPersona Mobile Settings. Then touch the fingerprint sensor to sign in.
 - Non-fingerprint enabled devices - Tap *Sign In* and then enter your six-digit DigitalPersona Mobile passcode.



Enroll the OTP credential

1. On your computer, open the *Enroll a One-Time Password* window.
2. On your device, sign in to the DigitalPersona Mobile app.
3. On your computer, at the bottom of the window, enter the six-digit One-Time Password displayed in the app and click *Save*.



SMS OTP

On the Credential Manager, One-Time Password page, you can enroll an OTP credential that will transparently generate a time-sensitive code that is sent to your mobile device and display a notification asking you to Allow or Deny its use for authentication.

Note that the OTP displayed in the authentication app changes every 30 seconds and the code on a hardware token device generally changes every 30 to 60 seconds, depending on the manufacturer and any optional configuration (using the *SMS GPO*) by the administrator.

Enrollment of the SMS delivery feature requires that a DigitalPersona administrator has previously created a Nexmo (<https://www.nexmo.com>) account and entered Nexmo account information into the OTP setting on the DigitalPersona Server, as described on page 82 in the *Policies and Settings* chapter.

To enroll the OTP via SMS credential

1. In the *Enroll One-Time Password* window, click the *SMS OTP* tab.
2. Enter the number (country code and full phone number) for the mobile device where you would like to receive a One-Time Password through SMS delivery.
3. Click the arrow next to the phone number field.
4. You will receive an SMS message on your mobile device containing a six-digit One-Time Password.
5. On your computer, enter the One-Time Password into the *One-Time Password* field and click *Save*.
6. The *Credential Manager* page will re-display and the One-Time Password tile will now show a *Change* caption, indicating that a One-Time Password credential has been successfully enrolled.

OTP hardware token

On the Credential Manager, One-Time Password page, you can enroll a hardware token as a DigitalPersona credential. The hardware device can then be used to generate a code for authentication. Note that hardware tokens must be OATH compliant TOTP (Time-based One-Time Password) devices.

The screenshot shows a software interface titled 'Enroll a One-Time Password'. At the top, there are three tabs: 'Scan QR Code', 'SMS OTP', and 'Hardware Token', with 'Hardware Token' being the active tab. Below the tabs, there are two input fields: 'Enter the serial number of your hardware token' and 'Enter the One-Time Password displayed on your device'. At the bottom right are two buttons: 'Save' and 'Cancel'.

Typical hardware tokens



To enroll an OTP credential using a hardware token

1. From the *Enroll a One-Time Password* window, select the *Hardware Token* tab.
2. Enter the serial number for your hardware token, which is usually found on the back of the device. Note that a vendor supplied seed file that is associated with a specific set of hardware tokens must have been previously imported to the DigitalPersona Server before the hardware token can be enrolled. (See the topic *Hardware Tokens Management Utility* in your DigitalPersona Administrator Guide.)
3. Activate your hardware device. On some hardware tokens, you will simply need to press a button to do so, on others you will need to enter a preselected PIN to display the valid code on your device.
4. Enter the verification code displayed on your device and click *Save*.

OTP via email enrollment

If enabled by the administrator, a software token is generated by DigitalPersona, and a time-sensitive code that can be used for authentication is sent to the user's Active Directory email address. By default, this option is not configured (and therefore unavailable to users), but can be enabled by the administrator through the *Send OTP by email* GPO. Also a valid SMTP server must be specified during configuration of the DigitalPersona Web Management Components package or through the *SMTP Configuration* GPO setting.

Once enabled, the option to have a One-Time Password sent to the user's email address is automatically available (enrolled) upon completing the enrollment of any of the other types of OTP credentials described above.

NOTE: In order to authenticate using OTP via SMS or OTP via email, the user's workstation must be able to connect to the DP Server, either within the network, through a VPN or using the VPN-less (web proxy) feature which is enabled through the *Allow VPN-less access* GPO.

Authentication with a One-Time Password

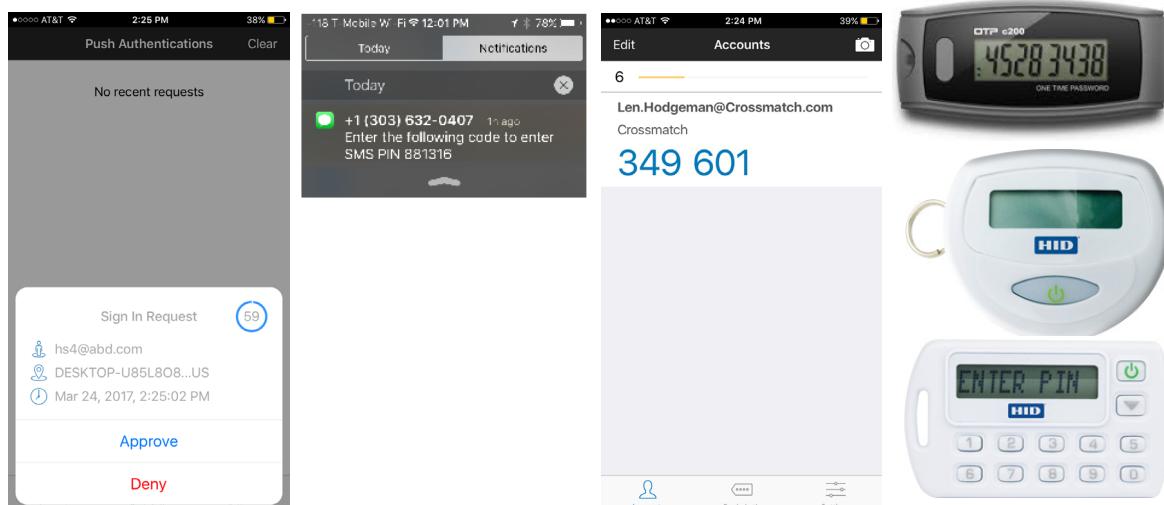
To authenticate with your One-Time Password

1. Do one of the following, depending on where you are authenticating from.

- At Windows logon, select *Sign-in options* and then select the *One-Time Password* (or OTP) tile to display *One-Time Password* options.
- On the *DigitalPersona Identity Server* or *Verify your Identity* screen, select the *One-Time Password* (or OTP) tile.

2. You can use an OTP credential in any of the following ways.

- Select *Send push notification* to send a One-Time Password to your enrolled mobile device allowing you to Approve or Deny authentication.
- Select *Send SMS* to send an SMS message to your enrolled mobile device with a One-Time Password that you can enter on your computer for authentication.
- Launch your previously registered authentication app on your mobile device and enter the resulting One-Time Password into the entry field on your computer.
- Activate the display on an enrolled hardware token, and enter the displayed One-Time Password on your computer.



3. In most cases, enter your One-Time Password into the One-Time Password field on your computer screen and select the arrow button. When using push notification, you do not need to enter the code on your computer, as tapping *Approve* or *Deny* on your mobile device automatically authenticates to your computer.
4. Note that the OTP displayed in the authentication app changes every 30 seconds and the code on a hardware token device generally changes every 30 to 60 seconds, depending on the manufacturer and any optional configuration by your administrator.

To change or delete your OTP credential

1. Once the credential has been enrolled, the word *CHANGE* will display beneath the OTP tile.
2. On the Credential Manager page, click *CHANGE*.
3. Confirm that you want to delete the current OTP credential and enroll a new credential.
4. Enroll the new OTP credential, or click *Cancel* to return to the Credential Manager page without enrolling a new OTP credential.

Recovery Questions credential

The Recovery Questions credential allows a DigitalPersona user to regain access to their Windows account by answering a series of questions that have been previously configured.

Enroll Recovery Questions

1	Select a question
Type your answer	
2	Select a question
Type your answer	
3	Select a question
Type your answer	

+ ADD

RECOVERY QUESTIONS

Enroll Recovery Questions

1	What is your mother's maiden name?
Pocahontas	
2	What was the name of the first school you attended?
Hard Knocks High	
3	What is the name of your first pet?
Alfred	

Save Cancel

To set up a user's Recovery Questions

1. Click the Recovery Questions tile to display the Recovery Questions window.

2. The user selects their questions from those available from the dropdown menus, and enters their unique answers. They can also write their own Custom questions by selecting the *Custom question* from the menu.

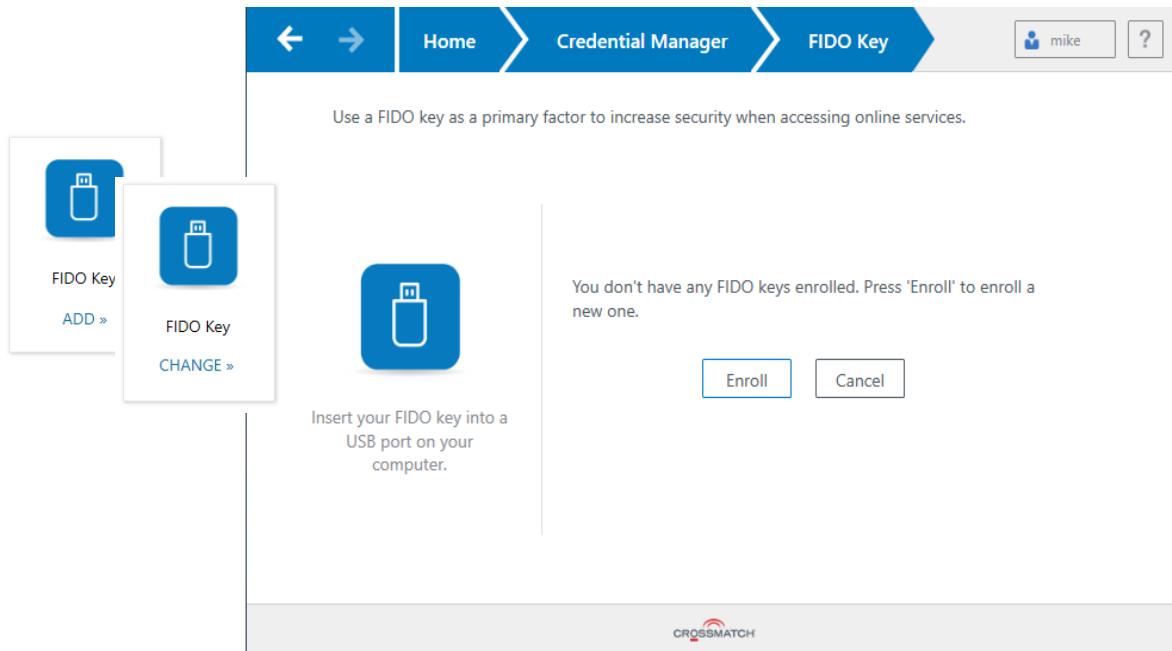
FIDO Key credential

The FIDO Key credential uses a FIDO USB key for authentication. The FIDO Key page is where FIDO keys are enrolled and managed.

IMPORTANT: If FIDO Keys will be used with DigitalPersona Web Components, i.e. Identity Provider, Web Administration Console or Web Enrollment, they should be enrolled through Web Enrollment, and not through the DigitalPersona Workstation User Console. FIDO Keys enrolled through the User Console will not work with DigitalPersona's Web Components.

To enroll or manage a FIDO Key credential

1. In the *Credential Manager*, click *ADD or CHANGE* on the FIDO Key tile.
2. The FIDO Key page displays.



To enroll a FIDO key as a DigitalPersona credential

1. Click *ADD*.
2. On the *FIDO Key* page, insert a FIDO key into an available USB port and choose *Enroll*.
3. Depending on the type of FIDO key being used, activate it through one of the following actions.
 - Tap the sensor on the device.
 - Press a button on the device.
 - Remove and reinsert the device.

To change the FIDO key being used as a credential

1. Choose *CHANGE* on the FIDO Key tile.
2. On the *FIDO Key* page, select *Re-Enroll*.
3. Tap, press the button on, or re-insert your FIDO key.

Upon successful enrollment, the *Credential Manager* page redisplays.

To delete this credential

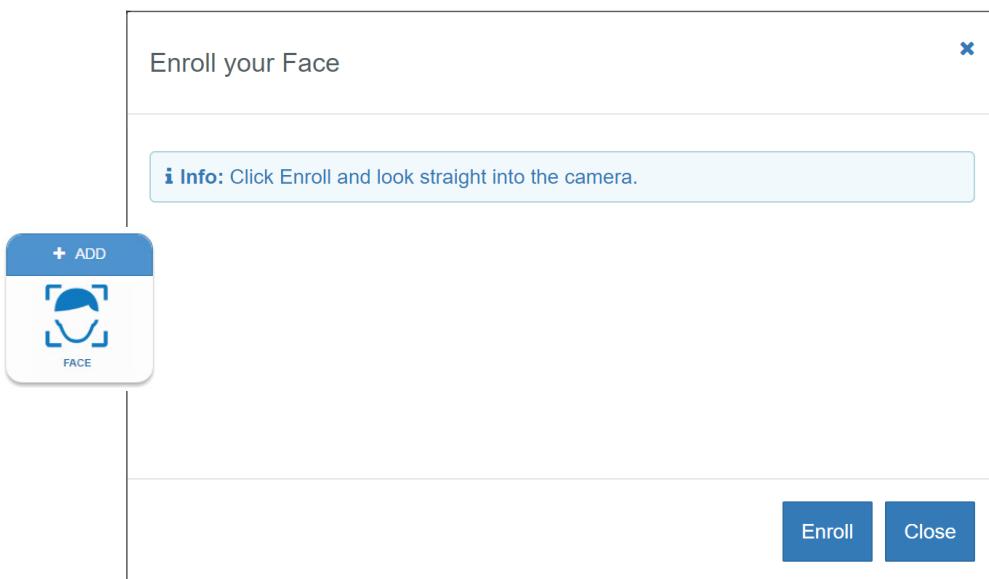
1. Choose *CHANGE* on the FIDO Key tile.
2. On the *FIDO Key* page, in the upper right, click *Delete Credential*. In the confirmation dialog, click *Delete*.

Face credential

This tile provides a means for enrolling a user's Face credential. Note that the Face credential is not supported on 32-bit versions of Windows, and is not enabled by default. In order to use this credential:

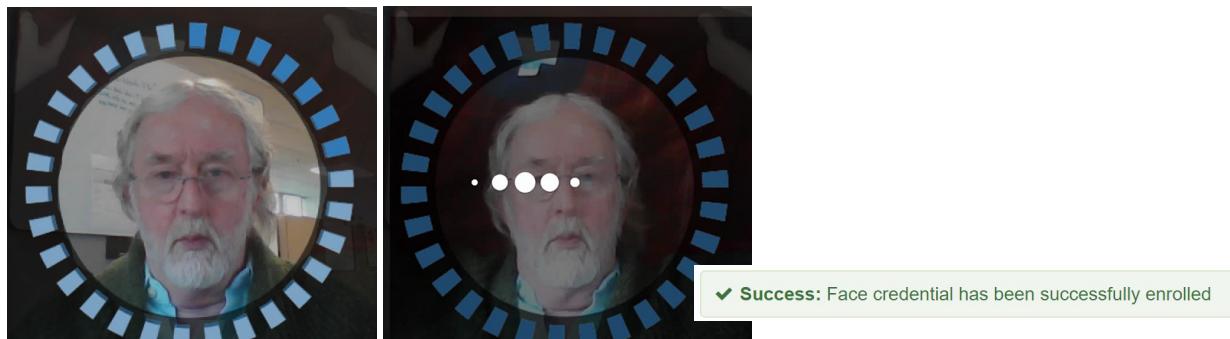
- A separate Face credential license must be purchased and installed on the same machine as the DigitalPersona Server.
- The Enrollment GPO must be enabled and the Face credential selected.

- Your computer must have a built-in or connected camera to enroll a Face credential.



To enroll a Face credential

1. Click the Face tile to display the *Enroll your Face* dialog.
2. If multiple cameras are available, select a camera from the dropdown list that will be displayed.
3. Click *Enroll* and look straight into the camera.
4. Wait until the system completes capturing your image. When successful, the process should look like this.



5. During the capture process, various messages may appear if the lighting is not adequate, you are too near or too far away, or when multiple faces are detected.

To change your Face credential

1. Once your Face credential has been enrolled, the label on the Face tile will be 'CHANGE.'
2. Click CHANGE.
3. In the *Delete Credential* dialog, click *OK* to delete your current credential.
4. The following message displays: *The credential has been successfully removed.*
5. You can now re-enroll your Face credential.

To delete your Face credential

1. Click CHANGE on the Face tile.

2. In the *Delete Credential* dialog, click *OK* to delete your current credential.
3. The following message displays: *The credential has been successfully removed.*
4. Click *Close*.

Note: Enrollment of your Face credential using an IR (infrared) camera in bright daylight is not recommended. If the camera being used to enroll your Face credential is an IR camera, and it is being used in bright daylight, the Face credential will still be enrolled, but the image shown after enrollment may be too dark to see any features.

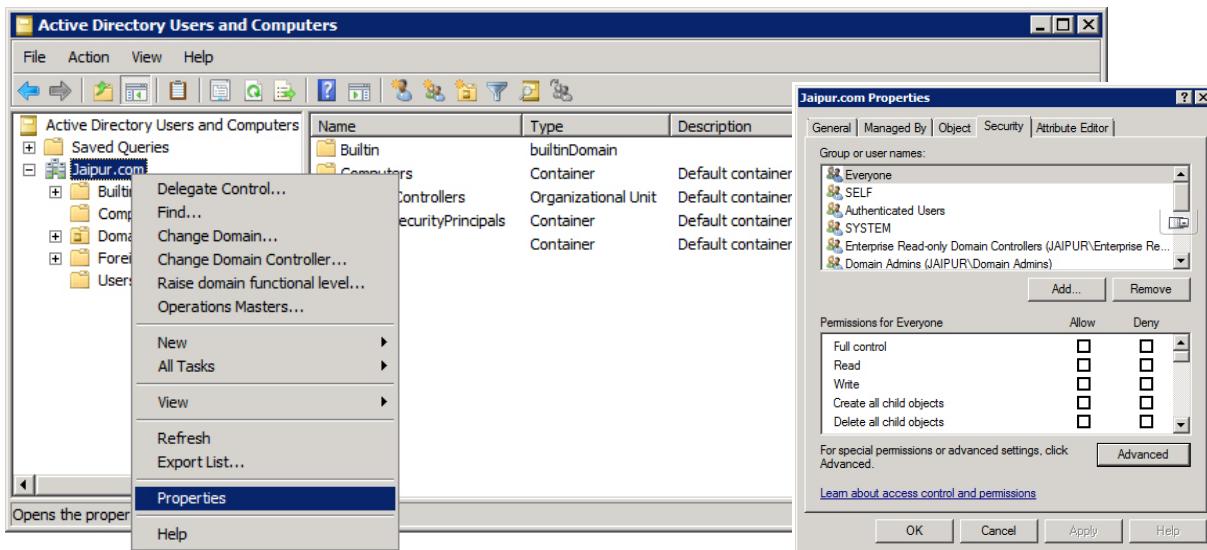
Customizing Web Enrollment

Use the following steps to

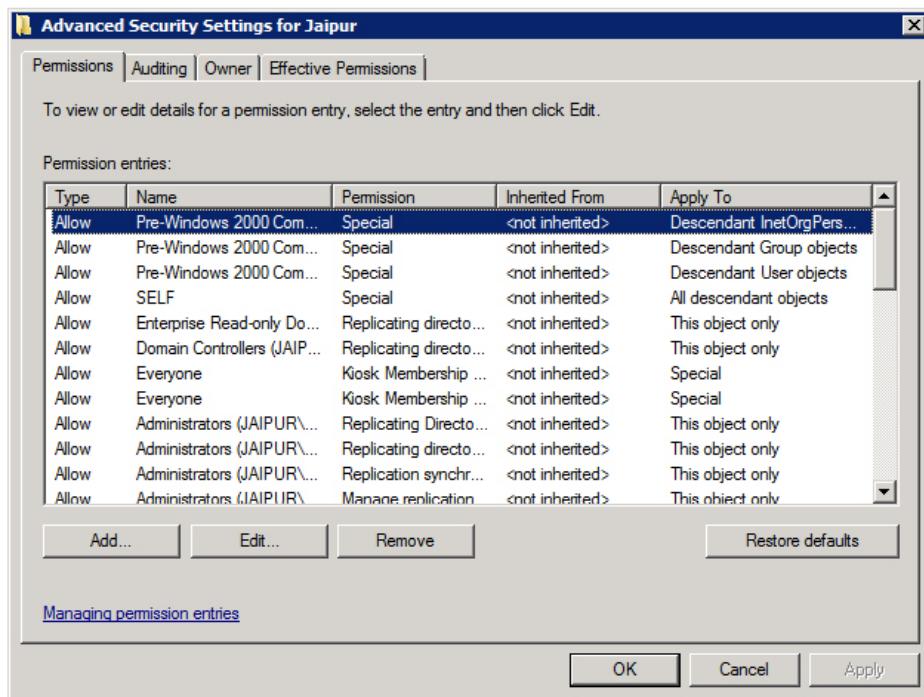
- Assign enroll/delete credentials permission to a user or group so that they may supervise Web Enrollment.
- Remove the enroll/delete credentials permission from all users. Note that in this case, you should *remove* the permission, not *Deny* the permission.
- Create a user or group that will supervise Web Enrollment.
- Prohibit domain administrators from enrolling users.

To assign, or remove Register/Delete permissions

1. Open Active Directory Users and Computers.
2. On the View menu, select **Advanced Features**.
3. As necessary, create a new AD Security Group for those who will be supervising Web Enrollment.
4. Right-click the **AD Domain Root** and then click **Properties**.



5. On the **Security** tab, click **Advanced** to view all of the permission entries.



6. Do one or more of the following:

- To assign new permissions
 - Click **Add**. Then type the name of the group, computer, or user that you wish to assign the permission, and click **OK**.
In the Permission Entry for *ObjectName* dialog box, on the Object and Properties tabs, select *Descendant User objects* from the *Apply to* drop-down menu.
 - Double-click the **Register/Delete Fingerprint (DigitalPersona)*** permission entry, and as appropriate, select either *Allow* or *Deny*.
- To remove the **Register/Delete Fingerprint** permission from an object or attribute, select the permission entry, and then click **Remove**.

* Although the permission is titled “Register/Delete Fingerprint,” it actually applies to all DigitalPersona credentials.

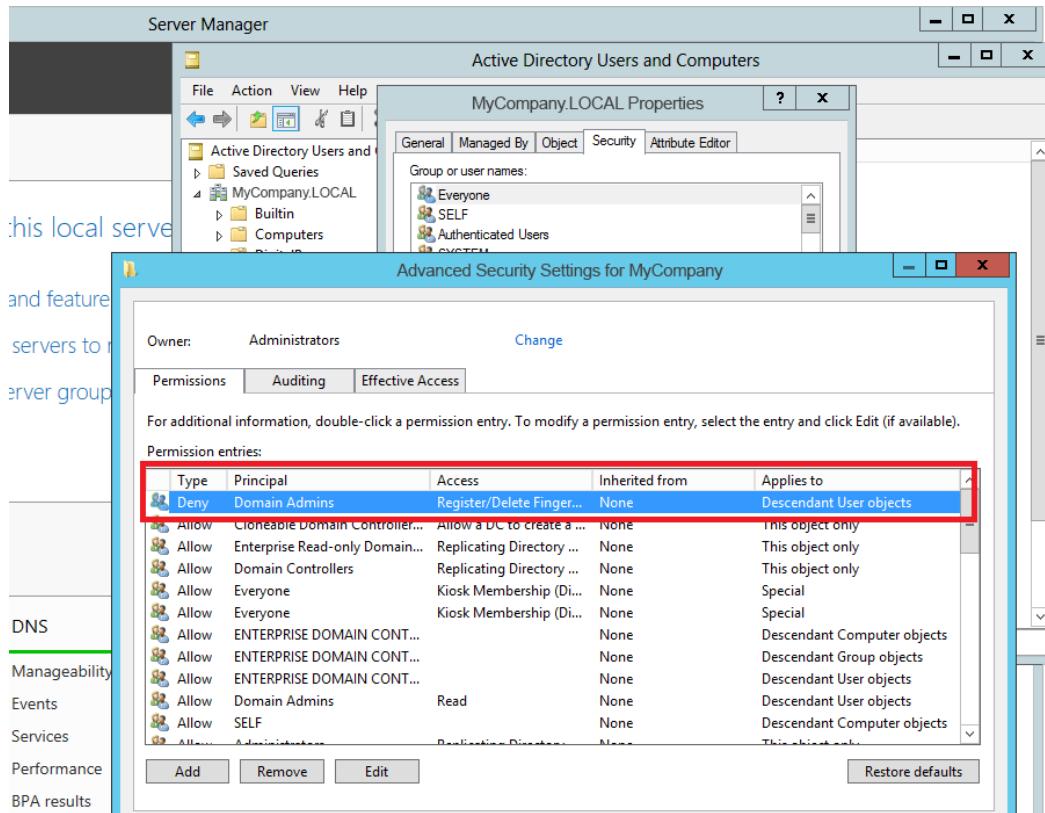
Prohibit domain administrators from enrolling/deleting credentials

To prohibit domain administrators from enrolling/deleting credentials

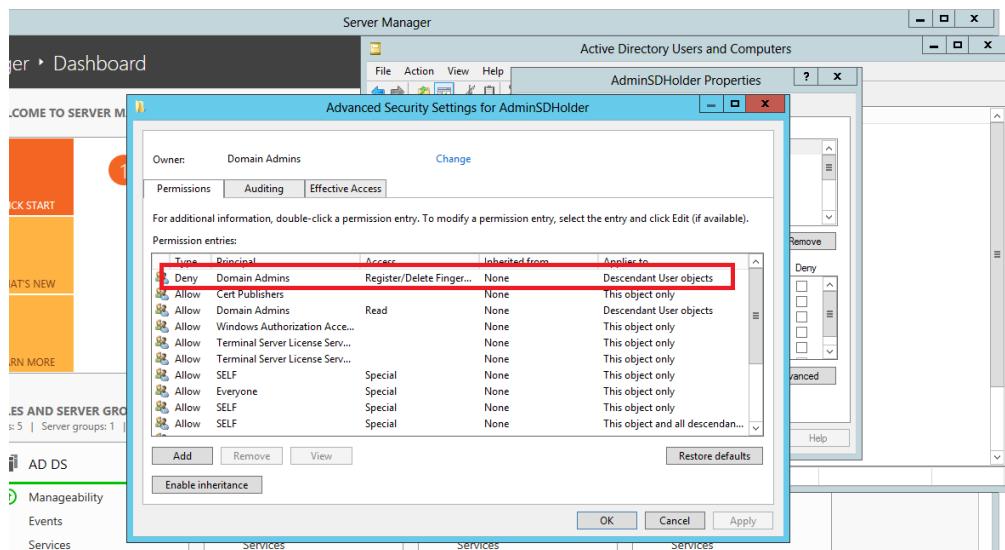
1. Open Active Directory Users and Computers.
2. On the View menu, select **Advanced Features**.
3. Right-click the **AD Domain Root** and then click **Properties**.

Remove the **Register/Delete Fingerprint (DigitalPersona)** permission from the *Self* object. Although the permission is titled “Register/Delete Fingerprint,” it actually applies to all DigitalPersona credentials.

4. Set the permission for the **Register/Delete Fingerprint (DigitalPersona)** entry to *Deny* for the Domain Admins Group.



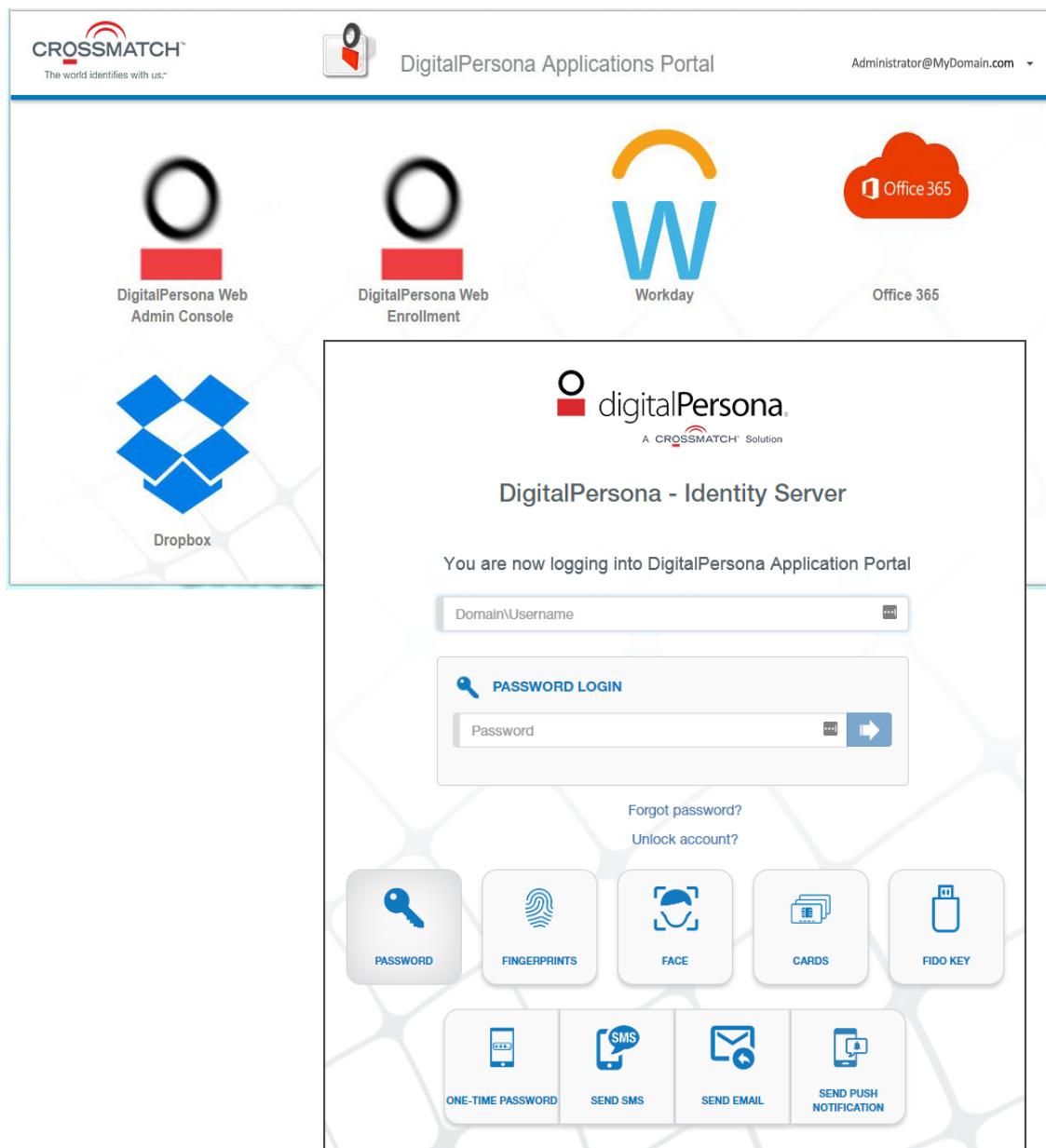
5. Navigate to [Domain root]\System\AdminSDHolder. Right-click on AdminSDHolder and select *Properties*.
 6. Set the permission for the **Register/Delete Fingerprint (DigitalPersona)** entry to *Deny* for AdminSD Holder.



THIS CHAPTER DESCRIBES DIGITALPERSONA APPLICATIONS PORTAL AND ITS CONFIGURATION

Overview

The DigitalPersona Application Portal is an optional DigitalPersona module, included in the DigitalPersona Web Management Components package, that provides web-based single sign-on to applications through the use of claims-aware SAML tokens.



Sign on to the Application Portal is provided through the DigitalPersona Identity Server, further described on page 240. To install the DigitalPersona Application Portal, select it from the component choices available in the DigitalPersona Web Management Components Installation Wizard. The last page of the wizard will contain a URL for the application portal.

The general process for adding links to additional applications is described below. Specific additional instructions for configuring any specific application are unique to the application and must be provided by the application vendor.

Adding links to the Application Portal

Once the Application Portal has been installed and access to it has been verified, locate the Portal.config. By default this will be the location of the file.

C:\Program Files\DigitalPersona\Web Management Components\DP App Portal\App

Editing this file requires Administrator privileges. You should backup the file before editing, and you may want to copy the file to the desktop for editing to avoid warnings about insufficient rights, and then copy it back to the original location.

For your convenience, icons and application names for common DigitalPersona and 3rd party applications have been provided in this file. However, the correct URL for each application needs to be entered in the portal.config file.

Adding DigitalPersona web applications to the Application Portal

Add the URLs for the DigitalPersona Administration Console and DigitalPersona Web Enrollment shown on the final page of the Web Management Components Installation Wizard.

Examples:

```
<add name="DPWebAdmin" url="https://webadmin.MyDomain.com/dpadminui" description="DigitalPersona Web Admin Console" />  
<add name="DPWebEnroll" url="https://webenroll.MyDomain.com/dpadminui" description="DigitalPersona Web Enrollment" />
```

Adding third-party applications to the Application Portal

The structure for adding third party applications to the Application Portal is the same for third-party applications. However, the process for enabling an application for SSO is often complex and is unique to each application. For assistance in this process, please contact our Professional Services.

Portal verification

Navigate to the Application Portal link provided on the last page of the DigitalPersona Web Components Installation Wizard. If everything is set up correctly, your browser will be redirected to the DigitalPersona Identity Server logon page. After successful logon, the browser will be redirected back to the Application Portal page, with a list of

Section Four: Appendices

Section Four of the DigitalPersona AD Administrator Guide includes the following chapters:

Chapter Number and Title	Purpose	Page
26 - Troubleshooting	Addresses common questions or issues relating to DigitalPersona software, and how to troubleshoot and resolve them.	219
27 - DigitalPersona AD ADFS Extension	Describes the optional DigitalPersona ADFS Extension, which adds fingerprint and OTP authentication methods (DigitalPersona credentials) to an ADFS environment.	228
28 - DigitalPersona NPS Plugin	Describes the optional DigitalPersona component used to add composite authenticated VPN to the enterprise network.	232
29 - Citrix Support	Describes DigitalPersona support for the Citrix virtualization platform.	248
30 - Fingerprint Adjudication and Deduplication	Provides details on adjudication and deduplication.	251
31 - Identification List	Provides steps for creating an identification list.	253
32 - Chrome install via GPO	Provides steps for creating an identification list.	255
33 - Secure and small sensor support	Provides a description of DigitalPersona's support for secure and small sensors.	258
34 - Windows Password Synchronization Tool	Describes the Windows Password Synchronization Tool, which protects against user passwords in the DigitalPersona database becoming out of sync with the user's current password as stored in Active Directory	260
35 - v2.3 to 3.0 Revised GPO settings	Provides details on changes made to the DigitalPersona GPO structure, containers and settings.	261
36 - Schema extension	Provides details on changes made to the Active Directory schema by DigitalPersona AD.	266

THIS CHAPTER ADDRESSES COMMON QUESTIONS OR ISSUES RELATING TO DIGITALPERSONA SOFTWARE, AND HOW TO TROUBLESHOOT AND RESOLVE THEM.

Topic	Page
How to configure ports used by DigitalPersona for firewall	219
How to troubleshoot fingerprint reader operation	220
Resolving unavailable server or domain issues	221
Addressing fingerprint registration not allowed error	221
Changing Password Manager Data storage limits	222
FIDO Token AppIDs	223

How to configure ports used by DigitalPersona for firewall

Issue

The DigitalPersona client console fails to open. This may be due to interrupted communication between the DigitalPersona Server and the client through the firewall due to dynamically assigned ports.

Resolution

DigitalPersona uses Microsoft's DCOM for calls between our server and clients. By default, DCOM assigns ports dynamically from the TCP port range of 1024 through 65535. You can open all the specified ports, or you can configure the range by using Component Services.

Before following the steps below, you should familiarize yourself with the following topics.

- *Using Distributed COM with Firewalls (<http://go.microsoft.com/fwlink/?LinkId=46088>)*
- *How to configure RPC dynamic port allocation to work with firewalls (<https://support.microsoft.com/en-us/help/154596/how-to-configure-rpc-dynamic-port-allocation-to-work-with-firewalls>).*

To configure the range of ports used by DigitalPersona

1. In the registry on each DigitalPersona Server, navigate to the following key.

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet

2. Under the Internet key, add the values "Ports" (MULTI_SZ), "PortsInternetAvailable" (REG_SZ), and "UseInternetPorts" (REG_SZ).

3. Set the value of *Ports* to the range that you want to open for DCOM communication.

4. Set *PortsInternetAvailable* to *Y*.

5. Set *UseInternetPorts* to *Y*.

For example, the new registry key appears as follows:

Ports: REG_MULTI_SZ: 5000-6000

PortsInternetAvailable: REG_SZ: Y

UseInternetPorts: REG_SZ: Y

6. Restart the server.

How to troubleshoot fingerprint reader operation

Issue

An officially supported fingerprint reader is not working with a properly installed DigitalPersona client.

Resolution

Troubleshooting steps will vary depending on several factors, as outlined below.

Fingerprint reader	Comment
U.are.U 4500	Drivers for this Crossmatch U.are.U external fingerprint reader are automatically installed as part of the DigitalPersona Workstation or Kiosk installation. The driver can be reinstalled from this directory: <i>C:\Windows\DPDrv</i> .
U.are.U 5xxx	The 5xxx series of U.are.U external fingerprint readers is technically not a driver, but rather a code library enabling DigitalPersona support for the U.are.U 5xxx series of fingerprint readers. It is not installed automatically. The library can be found in the <i>\Drivers\UareU_5100_5160_5200_5300</i> folder within the DigitalPersona product package. After installation, the reader will be listed in the Device Manager as <i>PC camera</i> with Microsoft shown as the provider.
Other non-U.are.U	Drivers are provided (but not automatically installed) for the following non-U.are.U fingerprint readers. Egistec, Eikon, MINI, and Validity FDG-100, VFS201, VFS451, VFS471, VFS491, VFS495. The drivers can be found in the <i>\Drivers</i> folder within the DigitalPersona product package. Additional drivers may be added from time to time.
WBF Windows Biometric Framework	Any WBF-compatible reader should work with DigitalPersona when running on a Windows 8 or Windows 10 machine. In some cases, you may have to use Windows Update to download the correct WBF driver for the specific reader, or download it from the vendor's website.

Note that you may have to find and remove conflicting drivers or application software in order to allow the fingerprint reader to communicate with DigitalPersona. Possible sources of conflict that should be removed include: HP Protect Tools, HP Personal, Dell Personal, DigitalPersona Personal and the Wave Embassy Trust suite.

Resolving unavailable server or domain issues

Issue

The following two errors may indicate that either DNS cannot resolve the _srv_dpproent records which the client is looking for to resolve and start the process, or the client is unable to contact the DNS server.

- There are currently no logon servers to process the request (0x8007501)
- An error occurred. We can't sign you in with this credential because your domain isn't available

Resolution

To address this issue, you need to confirm that the srv record can be resolved correctly, and restart the DNS Server.

One way to confirm that the srv record is being resolved correctly by the DNS server is to open PowerShell or the command line, and run the following commands.

Nslookup

Set type-all

_dpproent._tcp.domainname.com

_uareuidsvr._tcp.domainname.com

Addressing fingerprint registration not allowed error

Issue

When attempting to enroll fingerprints, one of the following error messages displays.

Fingerprint Registration is not allowed. Contact your system administrator.

Error Access Denied (0x8007005)

This is most often the result of a user being moved from one OU to another, which causes the *Allow Inheritable permissions from parent to propagate to this object and all child objects. Include these with entries explicitly defined here.* checkbox to become automatically un-checked.

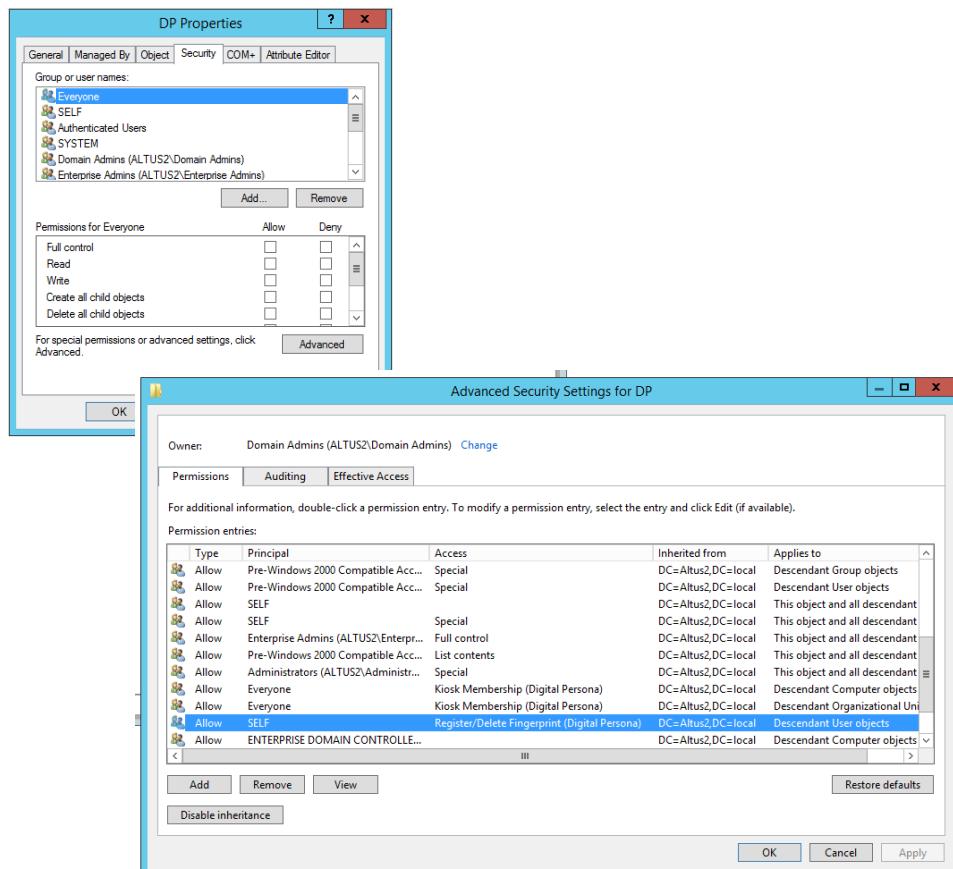
Resolution

Checking this item and waiting a few moments before attempting to enroll the user's fingerprints should resolve this issue.

If it is necessary to *not* have inheritance to user or OU objects, the *Register/Delete Fingerprint* permission can be added directly via the object or parent object's security tab in AD Users and Computers.

Changing Password Manager Data storage limits

To view the Advanced Security Settings, from the ADUC menu, select *View > Advanced Features*. Then right-click on the object and select *Properties*. Click the *Security* tab and then the *Advanced* button.



When mandatory attended fingerprint registration has been set up, users (via AD's SELF) will *not* have this permission on their own user objects, but the permission will be instead applied to the attended fingerprint user(s) and or group(s).

Changing Password Manager Data storage limits

Issue

DigitalPersona version 2.1+ - If you receive the following error message, *Cannot save logon due to attribute size limitation. Contact your administrator*, then the storage space allotted in Active Directory for storing Password Manager data may have been exceeded.

Previous versions - When it appears that logon data is not being saved, for instance if changes are reverting to previously entered information, this may indicate that the Password Manager storage space allotment has been exceeded.

Resolution 1 - Clear dp-Password-Manager-Data rangeUpper value by script

Requirements

- PowerShell with Active Directory module installed on a domain controller
- User with Schema Master role assigned

Procedure

- Copy 'dpPasswordManagerData_rangeUppe.ps1' to a local directory.
- Sign the provided script, or temporarily allow running unsigned scripts using 'Set-ExecutionPolicy Unrestricted' in the PowerShell console.

3. Right-click the file and select "Run in PowerShell."
4. When prompted to confirm the action, type "Y" for Yes.
5. You may run the script again to verify that the value was cleared, or check the value through ADSI Edit.

Note that this script changes only the dp-Password-Manager-Data rangeUpper value. You may also want to change the dp-Password-Manager-Data rangeUpper value using the procedure below.

Resolution 2 - Change Password Manager Data values manually

Requirements

- User with Schema Master role assigned
- ADSI Edit (part of the Windows Server Support Tools)

Procedure

1. Make the following change on the domain controller where your DigitalPersona Server is installed.
2. Navigate to *%Program Files%\Support Tools*, and then double-click *adsiedit.msc*.
3. Expand the Schema, and then click *CN=Schema,CN=Configuration,DC=domain_name,DC=com*
4. In the Details pane, right-click *CN=dp-Password-Manager-Data*, and then click *Properties*.
5. Double-click *rangeUpper*.
6. Type a new appropriate upper range for the attribute. If a significant number of logons are being created or modified on a regular basis, you may want to consider doubling the current value.
7. Click *OK*.
8. Repeat steps 4 through 6 with *dp-User-Private-Data*.
9. Click *OK* again.

FIDO Token AppIDs

When a FIDO Key credential is enrolled through the User Console of the DigitalPersona Workstation, no FIDO Token AppID is saved on the DigitalPersona Server.

FIDO tokens register their keys (AppIDs) for a specific application, which is usually a URL. FIDO clients must verify that the AppID belongs to the requesting application ,and that the keys are issued for the claimed AppID, which is added to the set of the signed data the token creates.

However, it is possible that an application may be represented by a real app on an Android or iOS gadget, in which case the URL does not apply. Also, it may be possible that a Web app uses multiple URLs, or one Relying Part uses multiple apps on different systems, etc. All the above cases are supported by FIDO by using concept of *TrustedFacets*.

The official description of Trusted Facets can be found here: <https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-appid-and-facets-v1.2-ps-20170411.html>

In short, AppID can represent a URL from which a JSON – encoded list of trusted URL origins and Android/iOS applications (“FacetIDs”) can be downloaded and used by the client application to verify that the AppID is indeed trusted before passing AppID to the Fido Token.

There are quite strict rules as what can be placed in the list of the URLs in the “trustedFacets” which are documented in the above document link. For Android and iOS apps, the “FacetID” is basically constructed by obtaining signature of the application package. This is out of scope for this document, but it seems it can be easily added when we have Android and iOS applications using the same AppID as Web applications. For other OS (i.e. Windows) the document does not specify any scheme, but it mentions that something similar can be used.

Restrictions on the Web FacetIDs within TrustedFacets are the following: Only URLs with matching public DNS suffixes plus one extra label are trusted. Public DNS suffix can be received from the official list at https://publicsuffix.org/list/public_suffix_list.dat. For practical reasons, any subdomain of the company domain may be trusted if we host the AppID JSON file one level below the company domain, like <https://fido.crossmatch.com/AppID> or <https://www.crossmatch.com/fido/AppID>.

HTTPS is mandatory, the path beyond the server address is irrelevant.

The following are examples from the Trusted facets document mentioned above.

AppID Example 1

".com" is a public suffix. "<https://www.example.com/appID>" is provided as an AppID. The body of the resource at this location contains:

```
{
  "trustedFacets": [
    {
      "version": { "major": 1, "minor": 0 },
      "ids": [
        "https://register.example.com", // VALID, shares "example.com" label
        "https://fido.example.com", // VALID, shares "example.com" label
        "http://www.example.com", // DISCARD, scheme is not https:
        "http://www.example-test.com", // DISCARD, "example-test.com" does not match
        "https://www.example.com:444" // VALID, port is not significant
      ]
    }
}
```

For this policy, "<https://www.example.com>" and "<https://register.example.com>" would have access to the keys registered for this AppID, and "<https://user1.example.com>" would not.

AppID Example 2

"hosting.example.com" is a public suffix, operated under "example.com" and used to provide hosted cloud services for many companies. "<https://companyA.hosting.example.com/appID>" is provided as an AppID. The body of the resource at this location contains:

```
{
  "trustedFacets": [
    {
      "version": { "major": 1, "minor": 0 },
      "ids": [
        "https://register.example.com", // DISCARD, does not share "companyA.hosting.example.com" label
        "https://fido.companyA.hosting.example.com", // VALID, shares "companyA.hosting.example.com" label
        "https://xyz.companyA.hosting.example.com", // VALID, shares "companyA.hosting.example.com" label
        "https://companyB.hosting.example.com" // DISCARD, "companyB.hosting.example.com" does not match
      ]
    }
}
```

For this policy, "<https://fido.companyA.hosting.example.com>" would have access to the keys registered for this AppID, and "<https://register.example.com>" and "<https://companyB.hosting.example.com>" would not as a public-suffix exists between these DNS names and the AppID's.

Notes

Be aware that each FIDO U2F token may need to be re-enrolled every time the FIDO AppId changes. For instance, if you deploy app-id.json into <https://win-erepv5i4qub.ldsdemo.com/Fido/app-id.json> and later decide to move it to another server. You would have two options:

1. Re-enroll all registered FIDO U2F devices.
2. Create an HTTP redirect:

from <https://win-erepv5i4qub.ldsdemo.com/Fido>
 into <https://newhost.virgo.com/Fido>.

More information on redirects can be found here: <https://docs.microsoft.com/en-us/iis/configuration/system.webserver/httpredirect/>

Check the FIDO specification for guidance on implementing the redirect.

Excerpt - If the server returns an HTTP redirect (status code 3xx) the server must also send the HTTP header FIDO-AppID-Redirect-Authorized: true and....."

3. Depending on the installation sequence, i.e. a DigitalPersona desktop client and/or the DP Web Management Components, follow the steps in one of the following procedures.

When Web Management Components are installed first or along with a DigitalPersona client

At the end of the Web Management Components Configuration Wizard, a file named *app-id.json* is created at a location similar to this: <https://fido.company-domain-name.com/fido/app-id.json>. The URL is recorded in the DigitalPersona Server store under the name "FidoAppID", and this AppID is used by each web server and desktop client during FIDO enrollment and authentication.

The default content of this file is similar to the following, where company-domain-name.com will be replaced with the actual company domain name.

```
{
  "trustedFacets": [
    {
      "version": { "major": 1, "minor": 0 },
      "ids": [
        "https://sts.company-domain-name.com",
        "https://webenrollment.company-domain-name.com",
        "dPCA:<?AD/LDS domain/installation guid?>"
      ]
    }
}
```

Note that part of the URL "company-domain-name.com" must be the same in all facets within the JSON file and in the URL of the JSON file.

The URL of the JSON file (<https://fido.company-domain-name.com/fido/app-id.json>) will be used as the AppID. It will be saved on the DigitalPersona Server using the interface WebGetSettingsEx under the name "U2F\AppId", from which any interested party can read it to use with the Fido tokens.

HTTPS call to get the JSON file

Protocol

HTTPS

Method

GET

URL

<https://fido.company-domain-name.com/fido/app-id.json>

Headers

Content-Type: application/fido.trusted-apps+json

Response

In case of success, the response code is 200. Otherwise the appropriate code must be returned. If the file is not found, the code is 404. The response body is the content of the file.

When only a DigitalPersona desktop client is installed

If a DigitalPersona desktop client is installed without the Web Management Components, no Fido Token AppID is saved in the DigitalPersona Server store and a default hard-coded AppID is used for all FIDO token enrollments. Re-enrollment will be needed if the DigitalPersona Web Management Components are later installed.

Manually adding an AppID value to the server store

You can add an AppID (URL of a future app-id.json file) in the DigitalPersona Server store, and it should work fine even if the actual file is not found at that URL.

1. Modify Web Management Components Configuration Wizard to do the following:

- a. Update the file "C:\Program Files\DigitalPersona\Web Management Components\DP Web SDK\app-id.json" with the list of configured host names.

Express configuration sample

app-id.json in *Express* Configuration

```
{
  "trustedFacets": [
    {
      "version": {
        "major": 1,
        "minor": 0
      },
      "ids": [
        "https://win-erepv5i4qub.ldsdemo.com"
      ]
    }
  ]
}
```

Advanced configuration sample

app-id.json in *Advanced* Configuration

```
{
  "trustedFacets": [
    {
      "version": {
        "major": 1,
        "minor": 0
      },
      "ids": [
        "https://webenroll.virgo.com",
        "https://sts.virgo.com"
      ]
    }
  ]
}
```

- b. Ensure in the Configuration Wizard that all URLs used for STS and Web Enrollment share "public DNS suffixes plus one extra label."
- c. Add a Fido application under the Default Web Site and point it to "c:\Program Files\DigitalPersona\Web Management Components\DP Web SDK\app-id.json"

Note that the FIDO AppId will be <Web Management Components Host>\Fido\app-id.json - i.e. if the Web Components were installed on win-erepv5i4qub.ldsdemo.com then AppId for both Basic and Advanced configuration will be https://win-erepv5i4qub.ldsdemo.com\Fido\app-id.json

- d. Store the FIDO AppId into the Digitalpersona server Web*Settings interface under name the name "U2F\AppId".

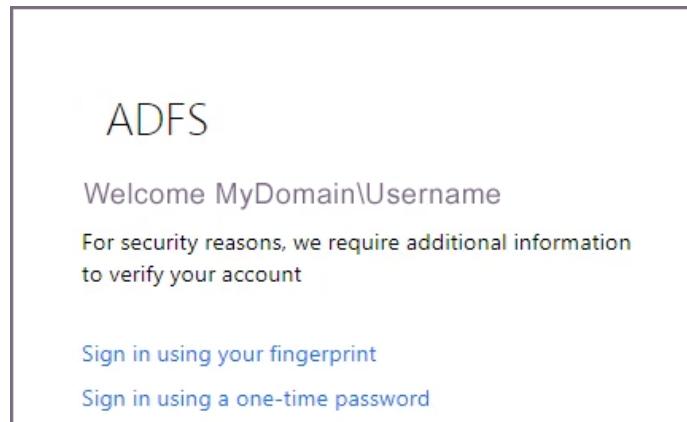
You may pass null in the jwt parameter of WebSetSettingsEx if you want DPCA to use the Windows Interactive user token for authentication.

```
HRESULT WebSetSettingsEx(
    [in] BSTR JWT,                                // Caller credentials
    [in] int Type,                                // Settings type
    [in] BSTR Settings);                          // List of settings to be set
```

- e. Store the FIDO AppId under the U2F\AppId name in the <appSettings> section of the following files.
 - c:\Program Files\DigitalPersona\Web Management Components\DP STS\DPPassiveSTS\web.config
 - c:\Program Files\DigitalPersona\Web Management Components\DP STS\DPActiveSTS\web.config
 - c:\Program Files\DigitalPersona\Web Management Components\DP Web Enroll\DPEnrollment\Web.config
- 2. Modify the Enrollment page of the Web Enrollment app to get the FIDO AppId from its U2F\AppId setting on the server.
- 3. Modify the Authentication page in the STS web server to get the FIDO AppId from the base64url encoded handshake data returned by the Continues authentication call.
- 4. Modify the Authentication page in Enrollment to get the FIDO AppId from the base64url encoded handshake data returned by Continues authentication call.
- 5. Modify the desktop FIDO authentication token to get the Fido AppID from the WebGetSettings interface and use it in enrollment and authentication.

THIS CHAPTER DESCRIBES THE ADFS EXTENSION FOR THE DIGITALPERSONA AD SOLUTION.

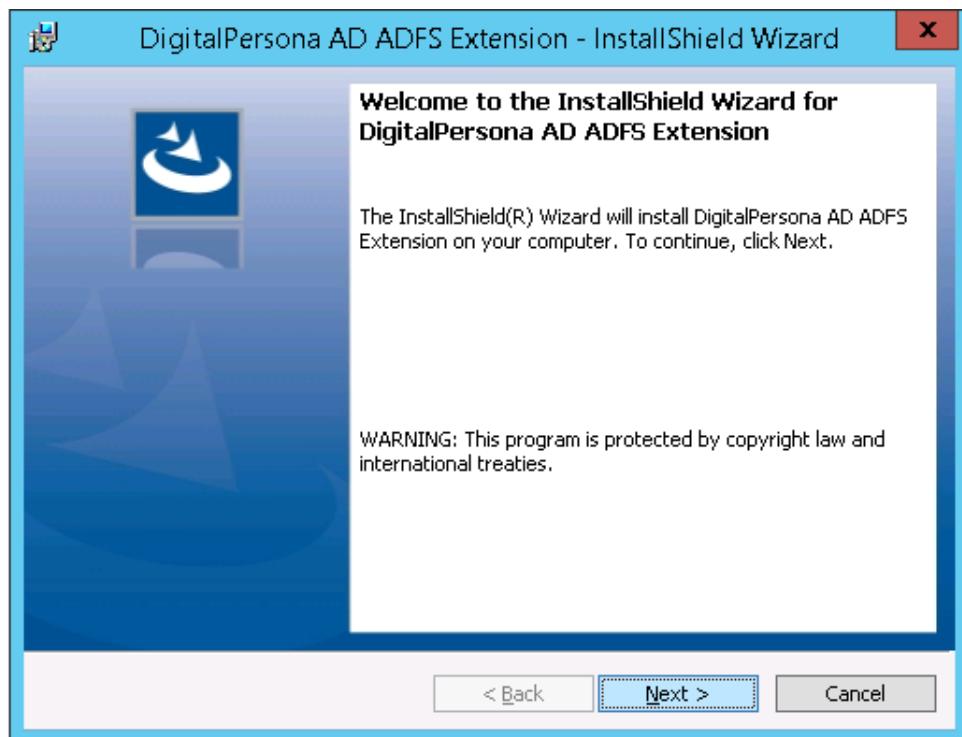
The DigitalPersona ADFS Extension adds fingerprint and OTP authentication methods (DigitalPersona credentials) to an ADFS environment.



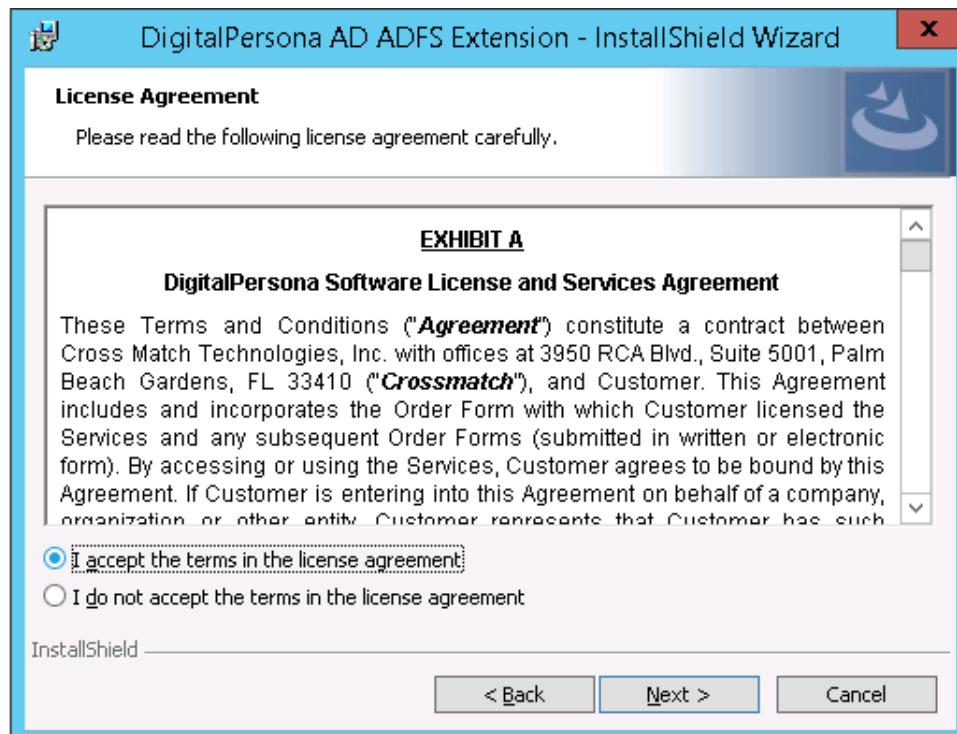
Installation

To install the DigitalPersona ADFS Extension

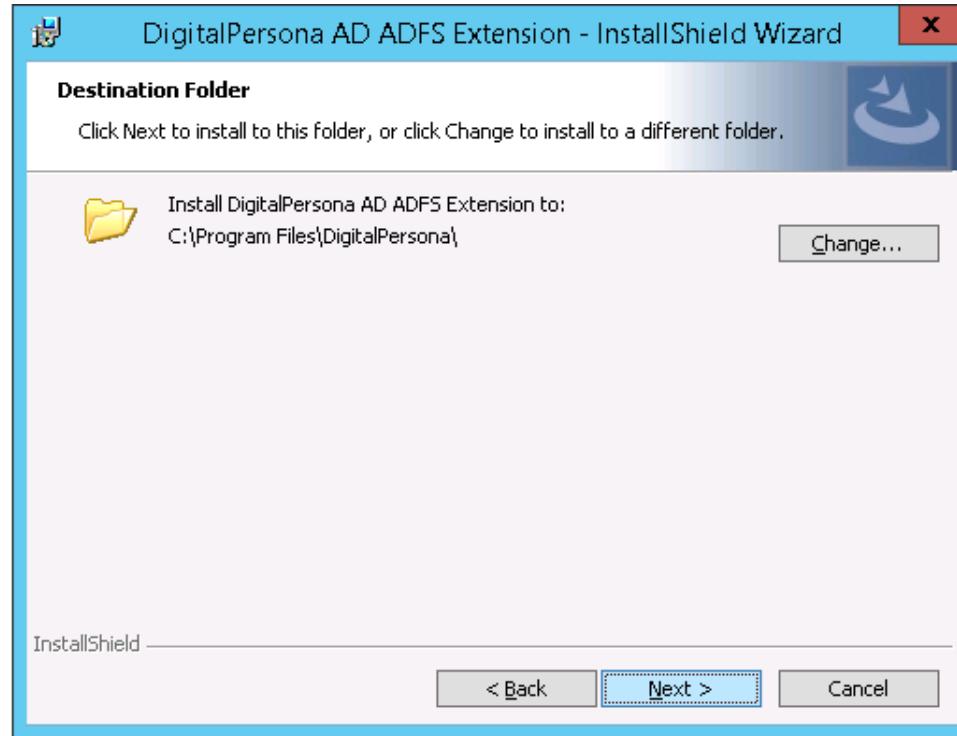
1. Launch the installation wizard by running the *DigitalPersona ADFS Extension.exe* file. Click *Next*.



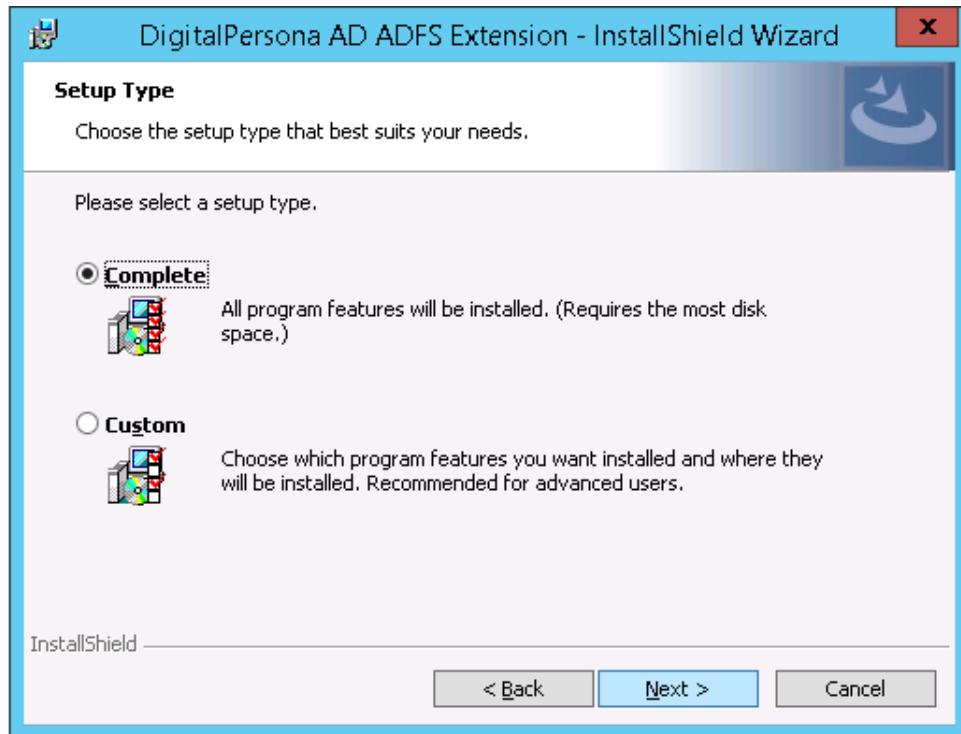
- Accept the license agreement. Click *Next*.



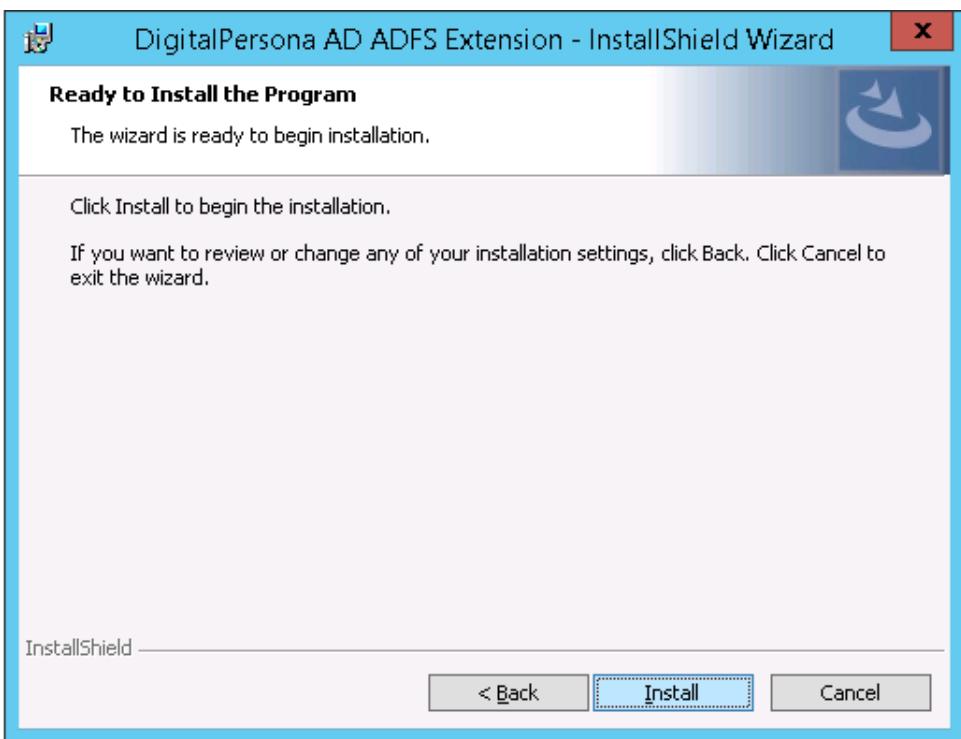
- Accept the default destination folder, or click *Change* to install to a different folder. Then click *Next*.



- Accept the default *Setup Type* of *Complete*, and click *Next*.



5. On the *Ready to Install the Program* page, click *Install* to begin the installation.



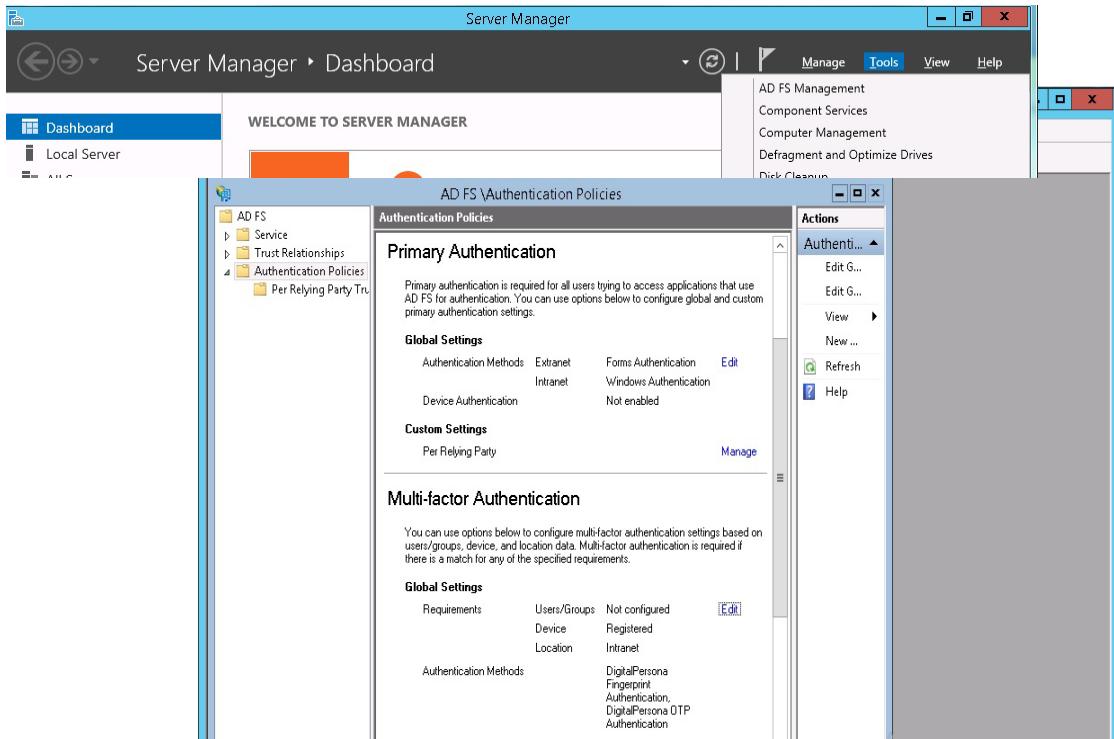
6. When installation is completed, on the final page of the wizard, click *Finish*.

Selecting and deselecting DigitalPersona credentials

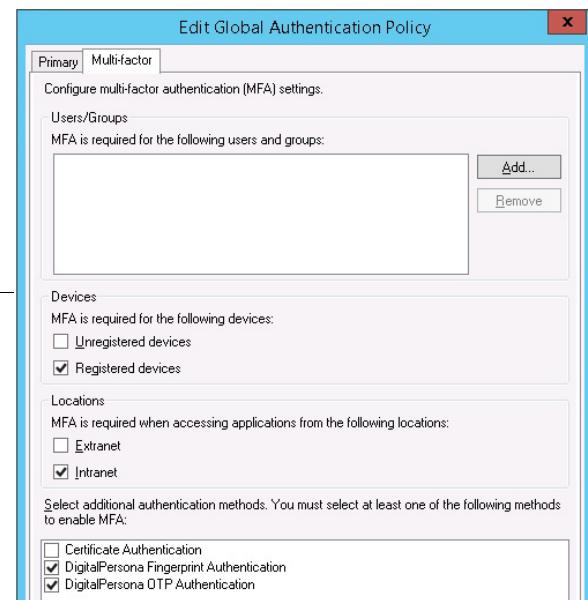
With the DigitalPersona AD ADFS Extension installed, you can select or deselect additional DigitalPersona credentials for AD FS authentication through the AD FS Management Console.

To select or deselect DigitalPersona credentials

1. From the Server Manager, select *Tools*, then select *AD FS Management*.
2. In the AD FS Management Console, select *Authentication Policies*.



3. Scroll down to the *Multi-factor Authentication* section.
To the right of the *Global Settings* area, click *Edit*.
4. In the *Edit Global Authentication Policy* dialog, select or deselect additional DigitalPersona credentials for multi-factor authentication.



THIS CHAPTER DESCRIBES THE DIGITALPERSONA NPS PLUGIN, AN OPTIONAL COMPONENT AVAILABLE FOR YOUR DIGITALPERSONA PREMIUM SOLUTION THAT PROVIDES INTEGRATED DIGITALPERSONA COMPOSITE AUTHENTICATION FOR YOUR RADIUS VPN.

Main topics in this chapter	Page
Recommended Configuration	232
Using Microsoft NPS as your RADIUS Server	232
Installing Network Policy Server (NPS)	233
Configuring your VPN Server to use the NPS RADIUS server	239
Deploying the DigitalPersona NPS Plugin	239
Configuring the Microsoft VPN Client	239
Testing the VPN connection using the PAP protocol	242
Testing the VPN connection using the MS-CHAPv2 protocol	242
Using OTP Push Notification with PAP	242
Using OTP Push Notification with MS-CHAPv2	243
Authenticating with OTP Only	243
Configuration required when using CHAP	243
Enabling reversible encryption for storing passwords	253
Configuring Microsoft RRAS to support CHAP	254
Configuring Microsoft NPS to support CHAP	255
Configuring Microsoft VPN Client to support CHAP	256
Testing the VPN connection using the CHAP protocol	257

Note regarding Password Manager managed logons and VPN: When connecting to your domain through a VPN, there will be a period of 30 minutes from your login to the current Windows session before managed logons will be shown on the Managed Logons tab. You must be connected to the domain (through VPN) before the 30 minutes is up in order to gain access to your managed logons.

Recommended Configuration

The following sections describe setting up your VPN using the DigitalPersona VPN extension and the MS-CHAPv2 or PAP protocols. If you need to use the CHAP protocol, see the section *Configuration required when using CHAP* beginning on page 243 before performing the procedures in this section.

Using Microsoft NPS as your RADIUS Server

To take advantage of DigitalPersona composite authentication, you will need to deploy the Microsoft Network Policy Server (NPS) and configure your VPN solution to use NPS as the RADIUS server for authentication.

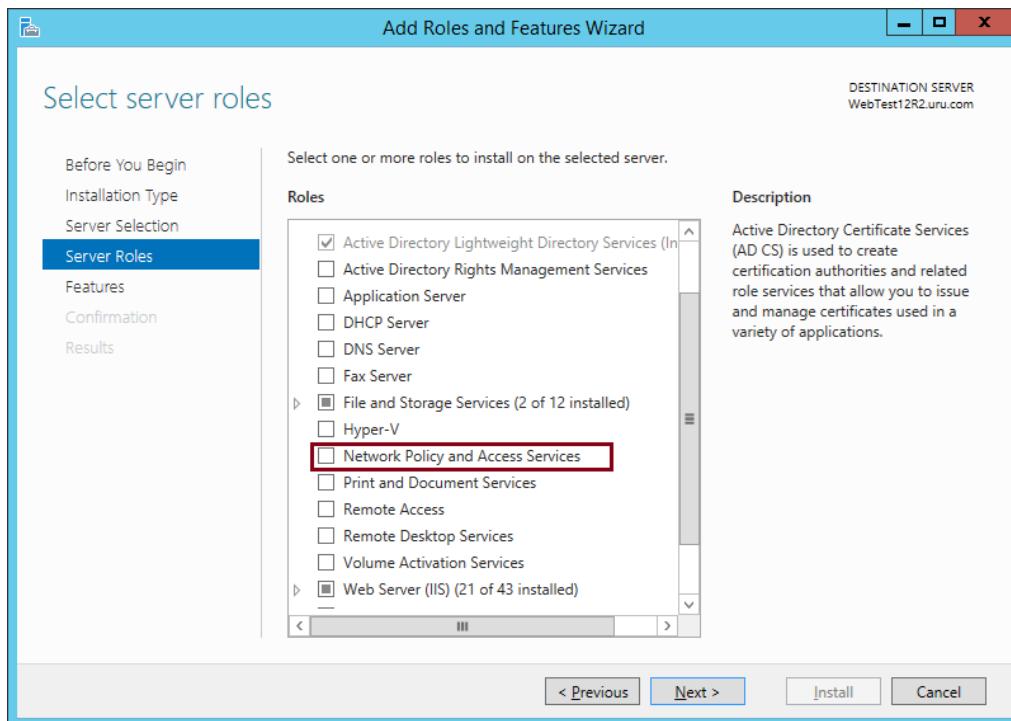
NPS is a server role of Windows Server 2012 R2 and later that performs authentication, authorization, and accounting for wireless, authenticating switch, and remote access dial-up and virtual private network (VPN) connections.

The following procedure assumes that a VPN Remote Access Server has been previously deployed, configured and is operational in your environment. This chapter deals only with setting up NPS as your RADIUS server and deploying the DigitalPersona NPS Plugin on Windows Server 2012 R2, although later versions should be similar.

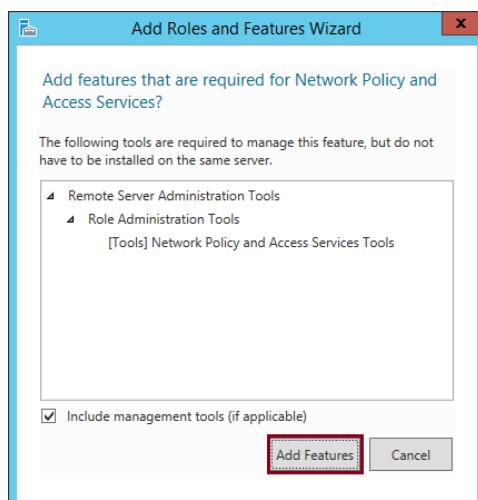
Installing Network Policy Server (NPS)

To install NPS

1. Open the Server Manager console Dashboard and click Add Roles and Features.
2. Select *Role-based or feature-based installation* and click *Next*.
3. On the Select destination server page, choose *Select a server from the server pool*. Select your server and click *Next*.
4. On the *Select server roles* page, select *Network Policy and Access Services* and click *Next*.

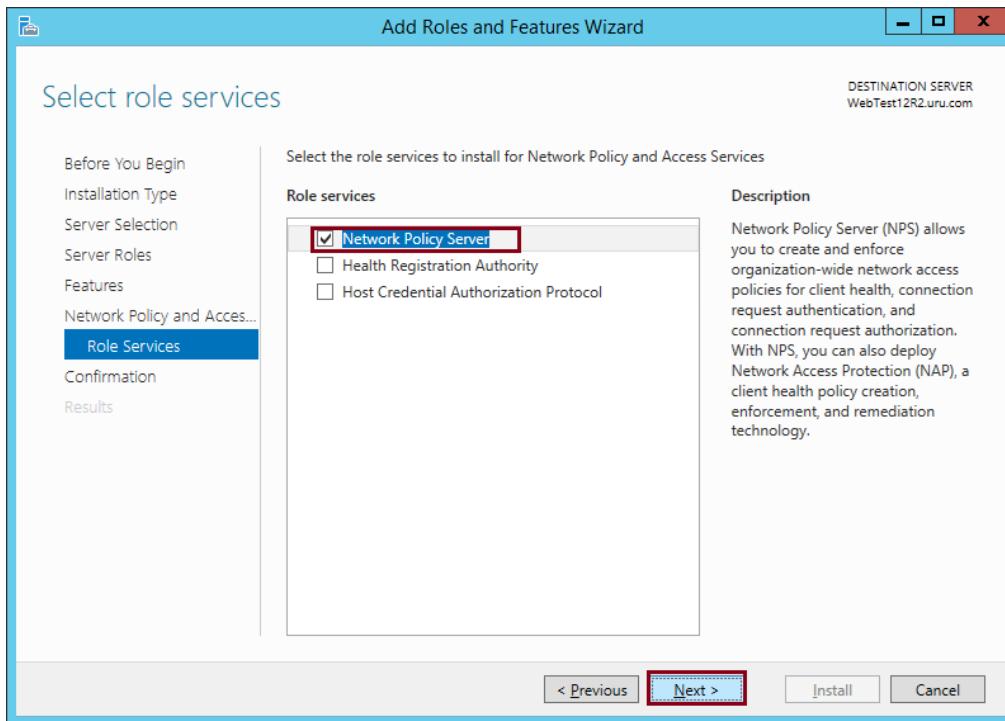


5. On the *Add Features* dialog, click *Add Features*.

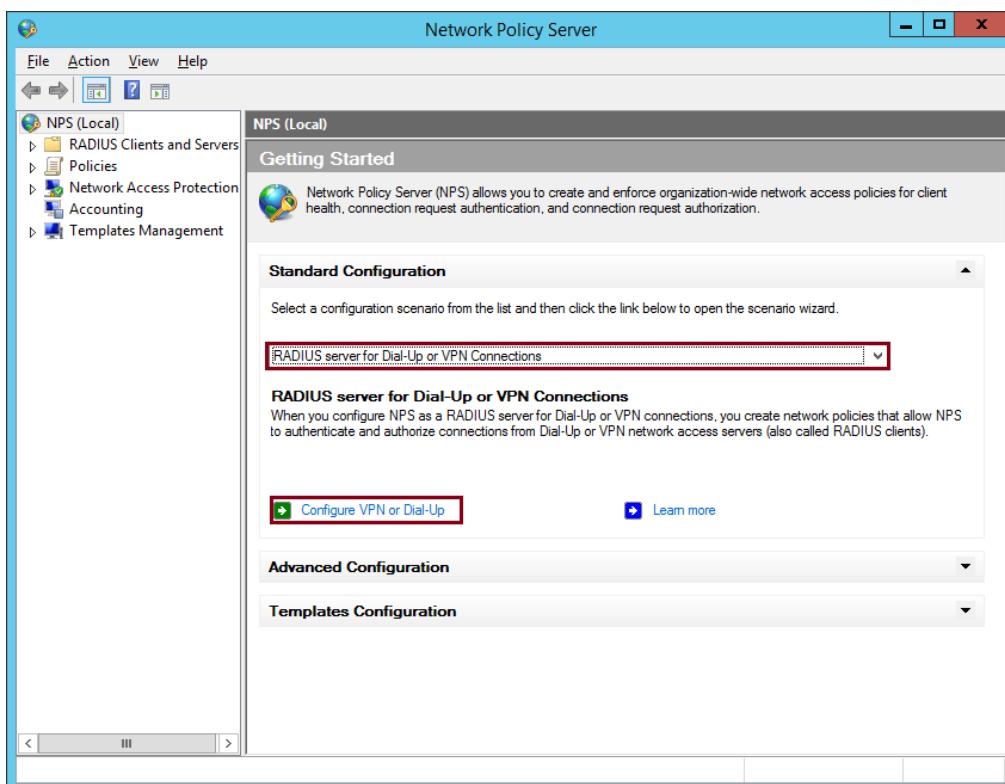


6. Click *Next*.
7. On the *Select Features* page, click *Next*.
8. On the *Network Policy and Access Services* page, click *Next*.

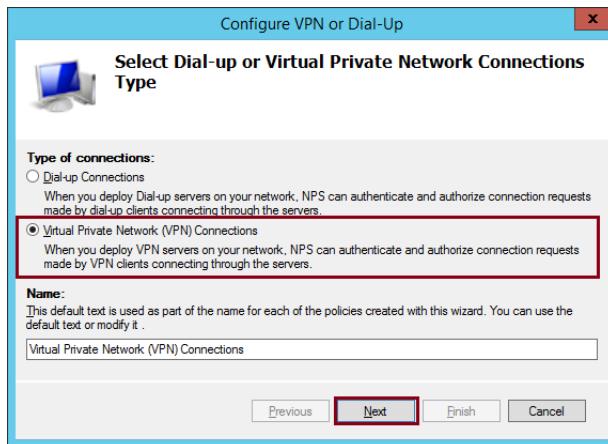
9. On the *Select role services* page, *Network Policy Server* should be automatically selected. Click *Next*.



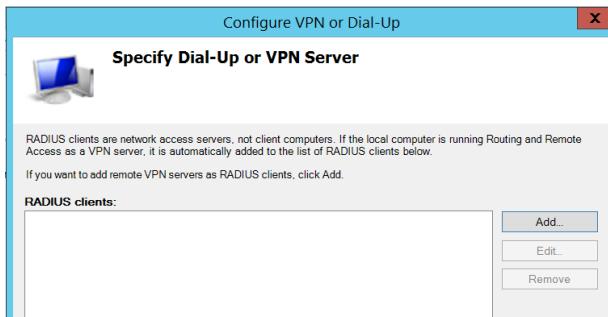
10. On the *Confirm Installation Selections* page, click *Install*.
 11. On the *Installation Results* page, review your installation results, and then click *Close*.
 12. Open the NPS console from the Administrative Tools menu on the server.
 13. On the *Getting Started* page, select *RADIUS server for Dial-Up or VPN Connections* from the dropdown menu and then click *Configure VPN or Dial-Up*.



14. On the first page of the *Configure VPN or Dial-Up* wizard, select **Virtual Private Network (VPN) Connections**. Use the default *Name* for the policies to be created or modify it as desired. Then click *Next*.

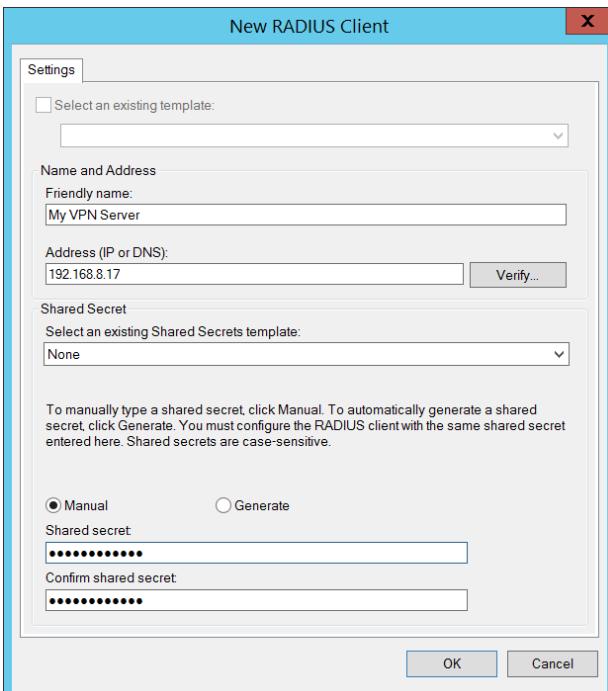


15. On the *Specify Dial-Up or VPN Server* page, click *Add*.

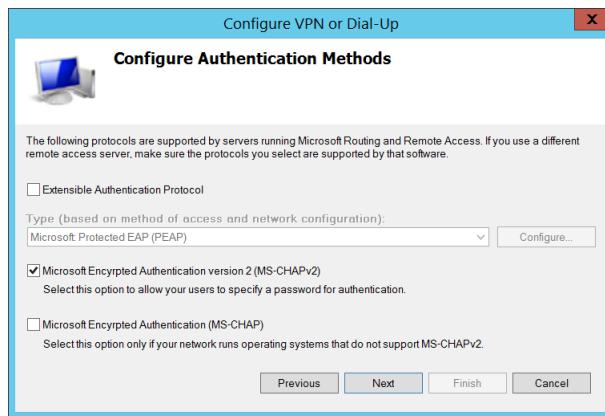


16. On the *New Radius Client* page, type a *Friendly name* for the new RADIUS client and then enter the IP or DNS address of the VPN Server. Note that a RADIUS client is a network access server (VPN server), not a client computer. If the local computer is running Routing and Remote Access as a VPN server, it is automatically added to the list of RADIUS clients in the page's list of clients.

17. Click *Verify* to ensure that a connection can be made to the DNS server you specified.



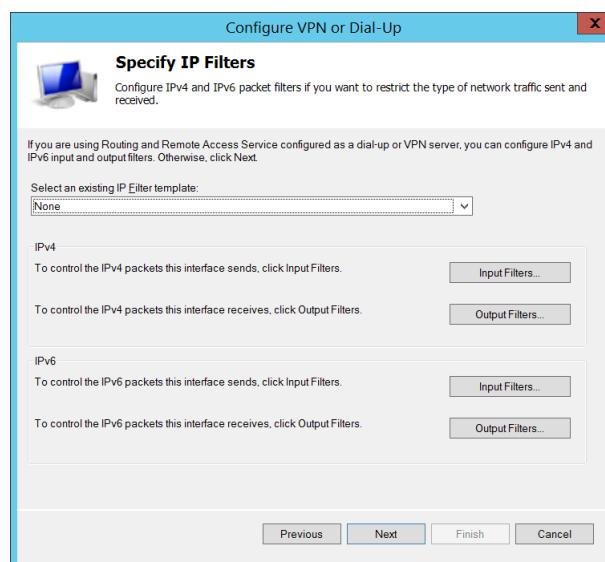
18. Select *Manual*, then enter and confirm the *Shared secret* (password) you want to use for the connection and click *OK*.
19. On the *Configure Authentication Methods* page, select *Microsoft Encrypted Authentication version 2 (MS-CHAPv2)* and click *Next*.



20. On the *Specify User Groups* page, accept the default to allow all users to access this VPN connection, or click *Add* to select groups that may be allowed or denied access based on the network policy Access Permission setting. Then click *Next*.



21. On the *Specify IP Filters* page, you can configure IPv4 and IPv6 packet filters to restrict the type of network traffic sent and received. If you are using Routing and Remote Access Service as a dial-up or VPN server, you can configure IPv4 and IPv6 input and output filters to restrict the type of network traffic sent and received. Otherwise, click *Next*.

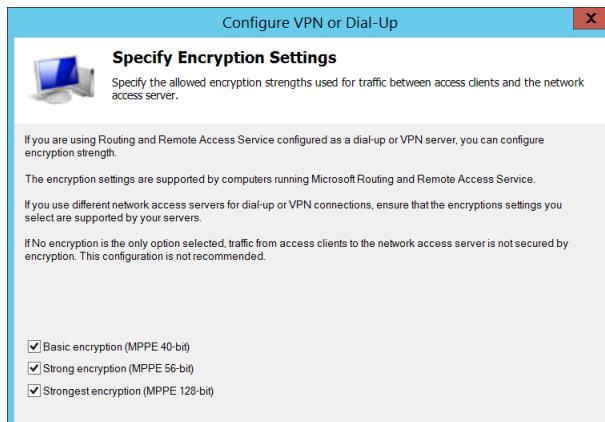


22. On the *Specify Encryption Settings* page, you should specify the allowed encryption strengths used for traffic between access clients and the network access server, and then click *Next*.

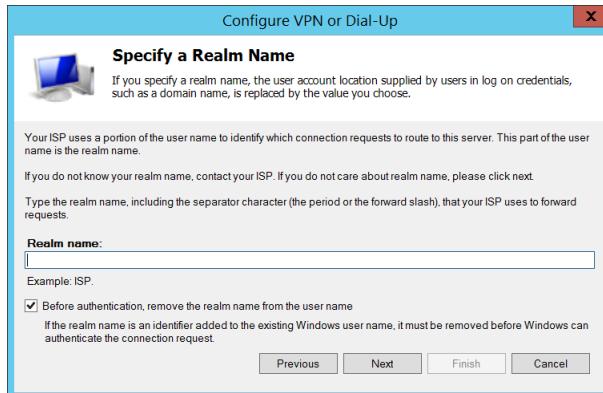
If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can select any (or all) of the listed encryption strengths on the page.

If you use different network access servers for dial-up or VPN connection, ensure that the encryption settings that you select are supported by your servers.

Unencrypted communication from access clients to the network access server is not recommended.



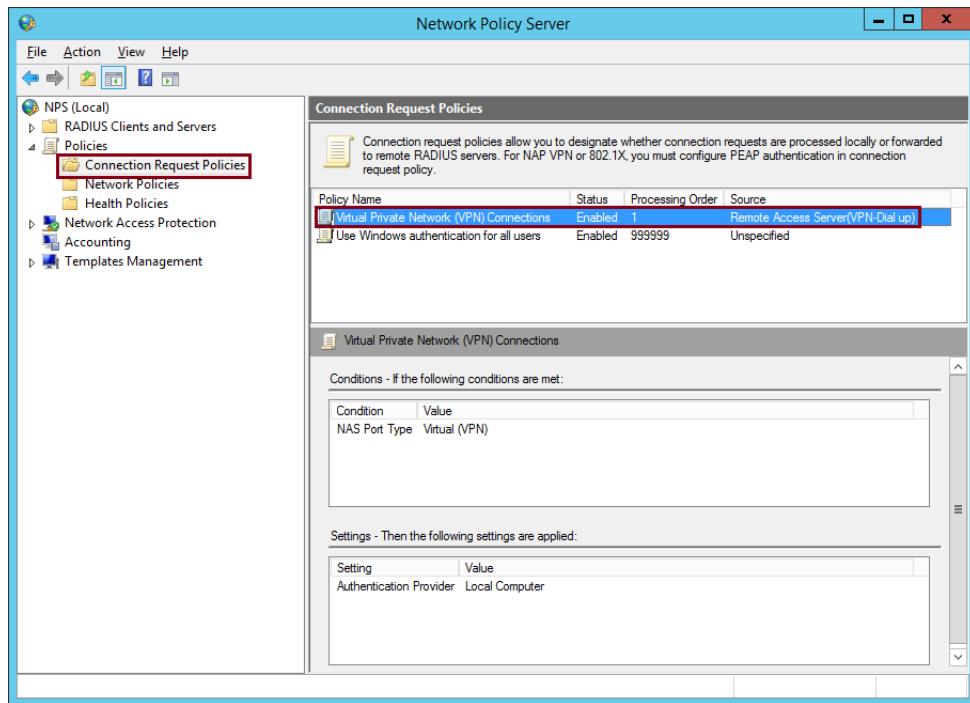
23. On the *Specify a Realm Name* page, optionally specify a realm name. If you specify a realm name, the user account location supplied by users in logon credentials (such as a domain name) is replaced by the value you specify. Click *Next*.



24. On the *Completing ...* page, click *Finish*.



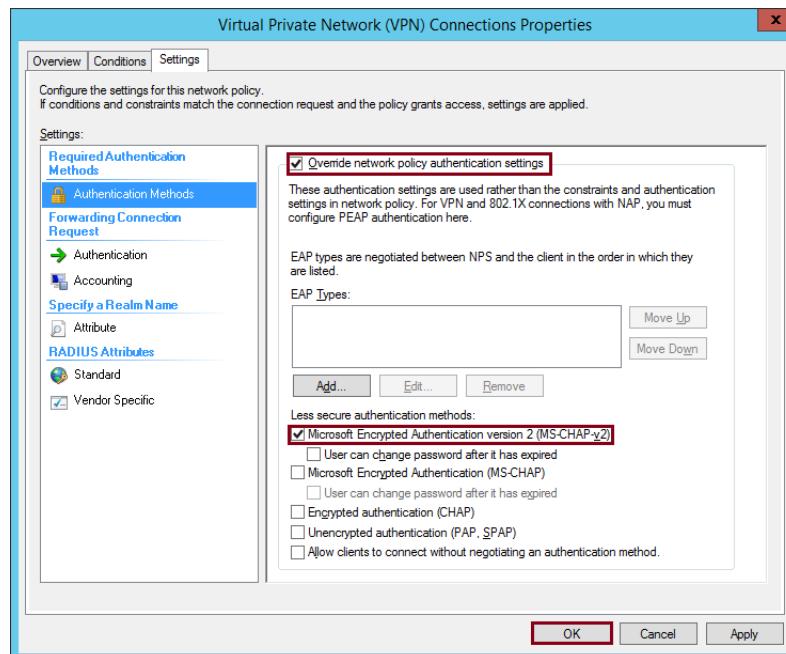
25. Once the installation is complete, return to the NPS console. In the left panel, under *Policies*, select *Connection Request Policies*. Then, in the main panel, double-click *Virtual Private Network (VPN) Connections* to display its *Properties* page.



26. On the *Properties* page, click the *Settings* tab and in the left panel, select *Authentication Methods*.

27. In the main panel, select the following items.

- Override network policy authentication settings
- Select one of the following options
 - Microsoft Encrypted Authentication version 2 (MS-CHAP v2)
 - Unencrypted authentication (PAP, SPAP)



28. Click *OK*. This completes installation and configuration of your NPS RADIUS server.

Configuring your VPN Server to use the NPS RADIUS server

You need to configure your VPN Server to use RADIUS Authentication. The actual configuration steps will depend on the specific VPN server you are using and is beyond the scope of this chapter. Review the configuration instructions for RADIUS Authentication in the documentation for your VPN server.

The following general instructions indicate the minimal information that must be configured.

1. The *IP or DNS address* of the VPN server must specify the NPS server you configured in the previous section (step 16 on page 235).
2. The *Shared secret* must be the same as that specified in step 18 on page 236.
3. You must use the Microsoft Encrypted Authentication version 2 (MS-CHAP v2) authentication methods in your VPN server.

Deploying the DigitalPersona NPS Plugin

Install the DigitalPersona NPS Plugin on the same server as the NPS server and restart the machine.

To install the DigitalPersona NPS Plugin

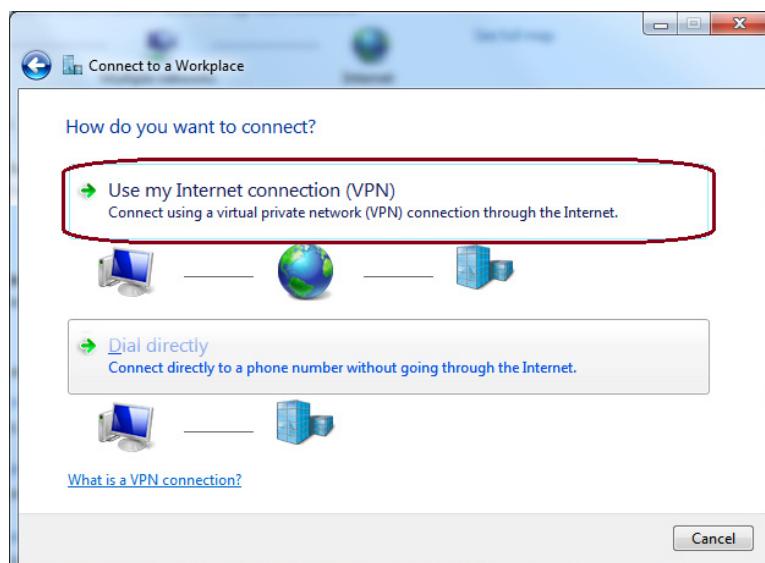
1. Make sure that the NPS service is running.
2. Launch the DigitalPersona NPS Plugin installer by double-clicking the *Setup.exe* file.
3. Accept the *End User License Agreement*.
4. Follow the onscreen instructions.

Configuring the Microsoft VPN Client

The following is an example of configuring the Microsoft VPN Client on a Windows 7 machine. Configuration of other VPN clients should use the same values, although the actual steps and UIs may be different.

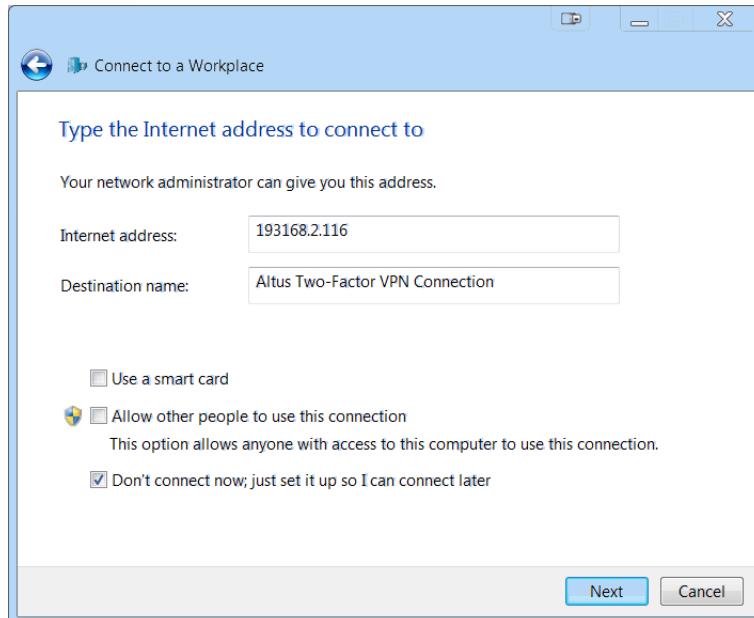
To configure the Microsoft VPN Client

1. Open the *Network and Sharing Center*.
2. Under *Change your network settings*, select *Setup a new connection or network*.
3. On the *Choose a connection* page, select *Connect to a workplace* and click *Next*.
4. On the *How do you want to connect* page, select *Use my Internet connection (VPN)*.

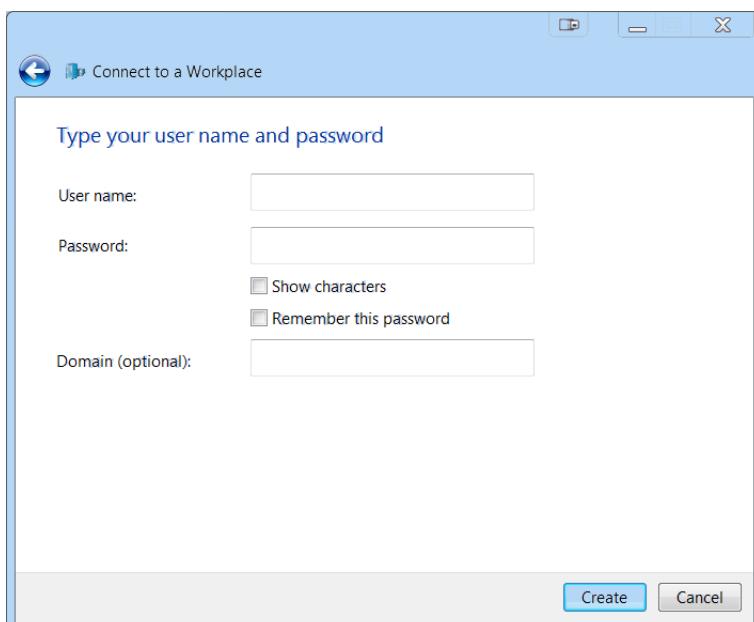


5. On the *Type the Internet address to connect to* page, perform the following:

- Internet Address: Enter the IP address or URL to your RRAS server.
- Destination Name: Enter a name for the new VPN connection.
- Select *Don't connect now, just set it up so I can connect later*.
- Click *Next*.



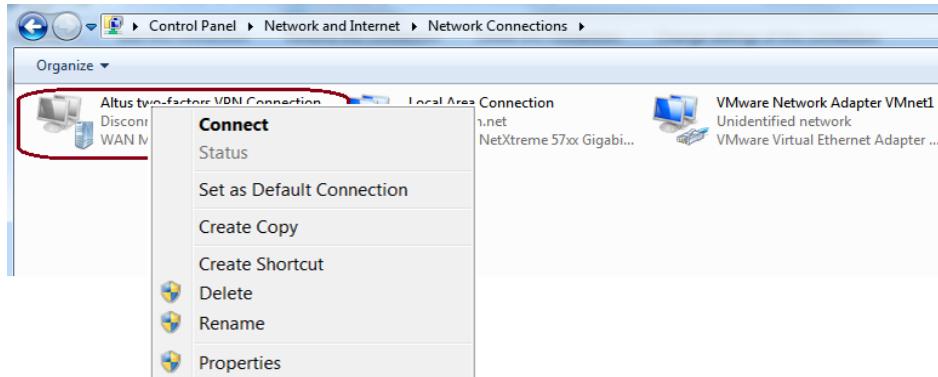
6. On the following page, do not fill in any fields, simply click *Create*.



7. Once the VPN connection has been created, it needs to be configured.

Configuring the VPN connection

1. In the Control Panel, select *Network Connections*. Right-click the connection and select *Properties*.



2. On the *Properties* dialog, select the *Security* tab. From the Type of VPN dropdown menu, select the VPN type. The following VPN types are supported:

- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol with IPSEC (L2TP/ IPSEC)
- Secure Socket Tunneling Protocol (SSTP)

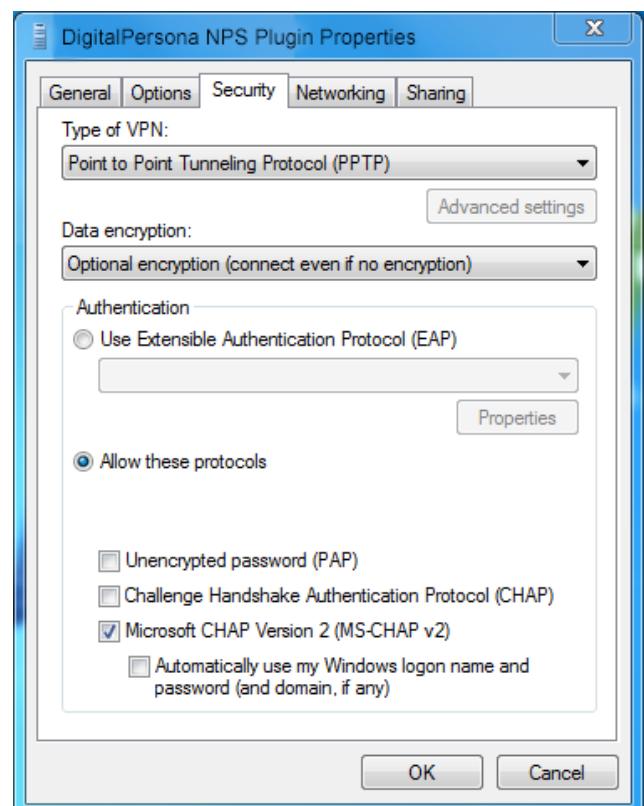
3. From the *Data encryption* dropdown menu, select *Optional encryption (connect even if no encryption)*.
4. Under *Allow these protocols*, select **only one** of the following protocols.

- Unencrypted password (PAP) - If PAP is selected, using PPTP as the VPN type is *not* recommended.
Although PAP is a simple, fast and quite reliable method, it does have a security drawback. PAP sends the user password to the VPN server in clear text and has no ability to encrypt the VPN communication channel after successful authentication.

Therefore it should only be used on top of VPN types that can pre-encrypt the communication channel, such as L2TP/IPsec (better) or SSTP (best).

- Microsoft CHAP Version 2 (MS-CHAP v2).

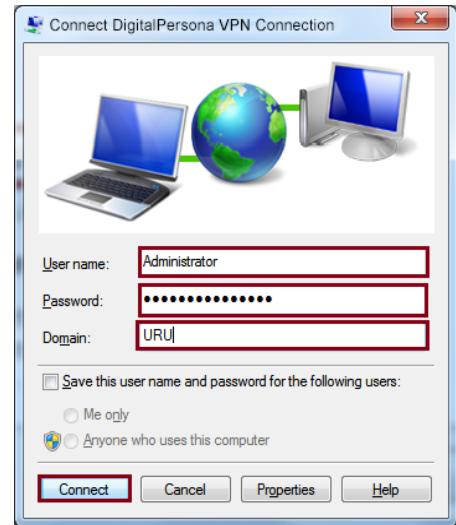
5. Click *OK* to finish the configuration.



Testing the VPN connection using the PAP protocol

To test your VPN connection using the *Unencrypted password (PAP)* protocol, use the following steps.

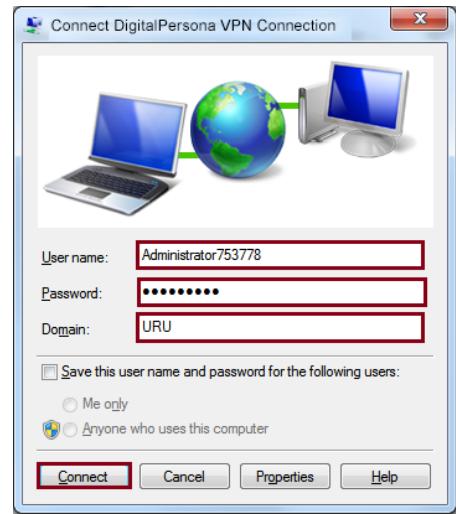
1. In the Control Panel, select *Network Connections*. Right-click on the VPN connection and select *Connect*.
2. Fill in the *Connect* dialog as explained below.
 - User name: For AD users, enter the Windows user account name or the user UPN name. For Non AD users, enter the user account name.
 - Password: Enter the user password and the OTP code, separated by a comma. For example, if the user password is aaaAAA123 and the OTP code is 753778, enter aaaAAA123,753778.
 - Domain: For AD users, enter the AD Domain name in the NETBIOS form. For Non AD users, leave the field blank.
3. Click *Connect*.



Testing the VPN connection using the MS-CHAPv2 protocol

To test your VPN connection using the *Microsoft CHAP version 2 (MS-CHAP v2)* protocol, use the following steps.

1. In the Control Panel, select *Network Connections*. Right-click on the VPN connection and select *Connect*.
2. Fill in the *Connect* dialog as explained below.
 - *User name*: (AD users only) Enter the Windows user account name and the OTP code, separated by a comma. For example, if the Windows user name is *Administrator* and the OTP code is 753778, enter *Administrator,753778*. UPN names and DigitalPersona LDS Non AD users are not supported.
 - *Password*: Enter the Windows password for the account.
 - *Domain*: Enter the AD Domain name in the NETBIOS format.
3. Click *Connect*.



Using OTP Push Notification with PAP

To use OTP Push Notification when using the PAP protocol

1. In the Control Panel, select *Network Connections*. Right-click on the VPN connection and select *Connect*.
2. Fill in the *Connect* dialog as explained below.
 - *User name*:
 - AD users - Enter the Windows user account name or UPN name.
 - Non AD Users - Enter the DigitalPersona Non AD account name
 - *Password*: Enter the user password, comma, and the word push.
 - Example - *MyPassword#123,push*
 - *Domain*:
 - AD users - Enter the AD Domain name in the NETBIOS form.
 - Non AD Users - Leave this field blank.

3. Click *Connect*.

Using OTP Push Notification with MS-CHAPv2

To use OTP Push Notification when using the MS-CHAPv2 protocol

1. In the Control Panel, select *Network Connections*. Right-click on the VPN connection and select *Connect*.
2. Fill in the *Connect* dialog as explained below.
 - *User name*:
 - AD users - Enter the Windows user account name,comma,push. Note that UPN names are not supported for this protocol.
 - Example: *MyUserName,push*
 - Non AD Users - Are not supported for this protocol.
 - *Password*: Enter the user's Windows password. Non AD Users are not supported for this protocol.
 - *Domain*: Enter the AD Domain name in the NETBIOS form.
3. Click *Connect*.

Authenticating with OTP Only

To authenticate to your VPN connection through OTP (One-Touch Password) only, perform the following.

1. On the machine where NPS (Network Policy Server) is installed, launch *regedit*.
2. Navigate to the following registry key.
HKEY_LOCAL_MACHINE\SOFTWARE\DigitalPersona\Policies\Default\TOTP
3. Create a new DWORD Value named *VPNAllowOTPOnly* with a value of 1.

Configuration required when using CHAP

Enabling reversible encryption for storing passwords

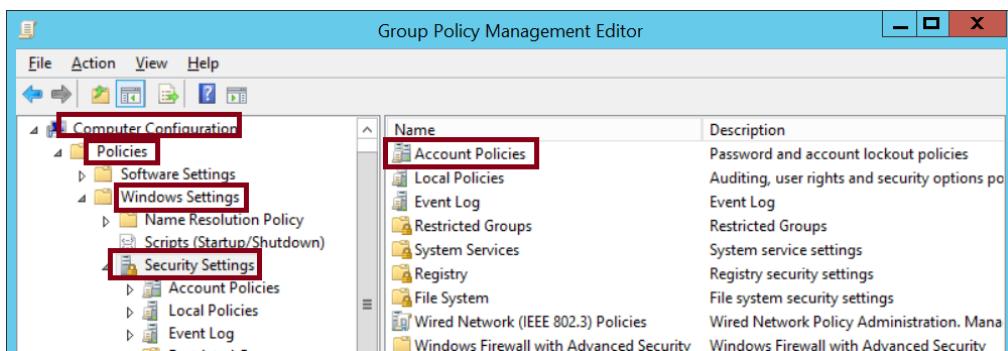
To use the CHAP protocol with the DigitalPersona NPS Plugin, the *Store password using reversible encryption* Password Policy must be enabled. See [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773343\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773343(v=ws.10)) for details.

To allow reversible encryption complete the following steps.

1. Open the Group Policy Management Editor.
2. Open the Default Domain Policy for editing.

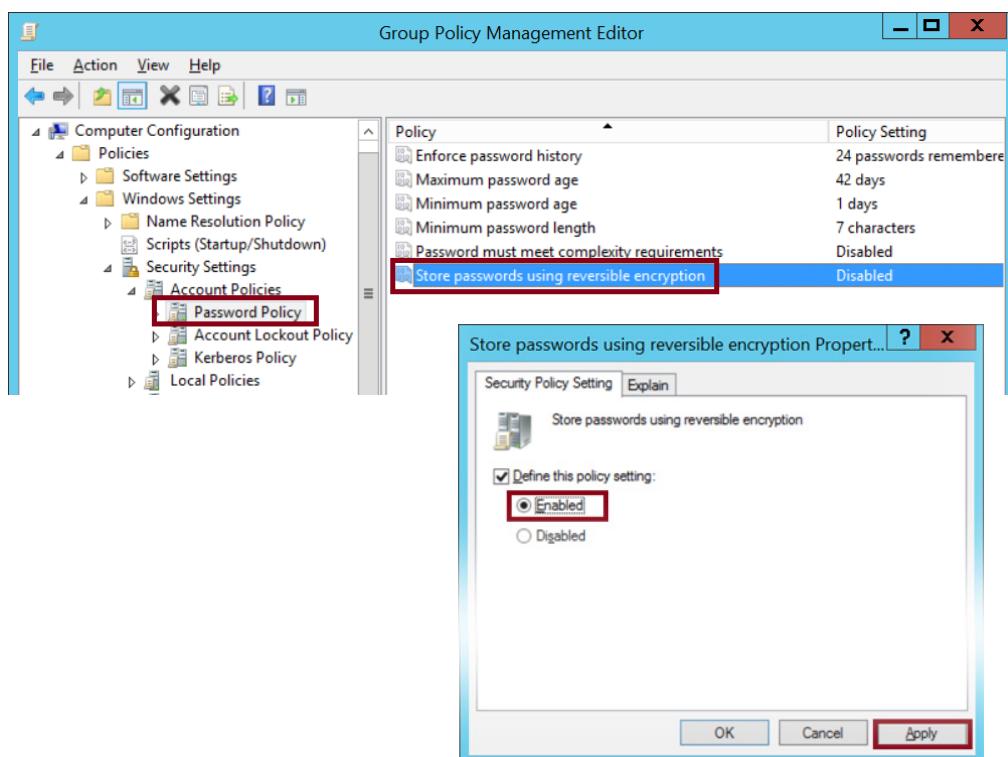
Configuration required when using CHAP

3. Navigate to Computer Configuration|Policies|Windows Settings|Security Settings|Account Policies.



4. Open *Password Policy* and double-click *Store password using reversible encryption*.

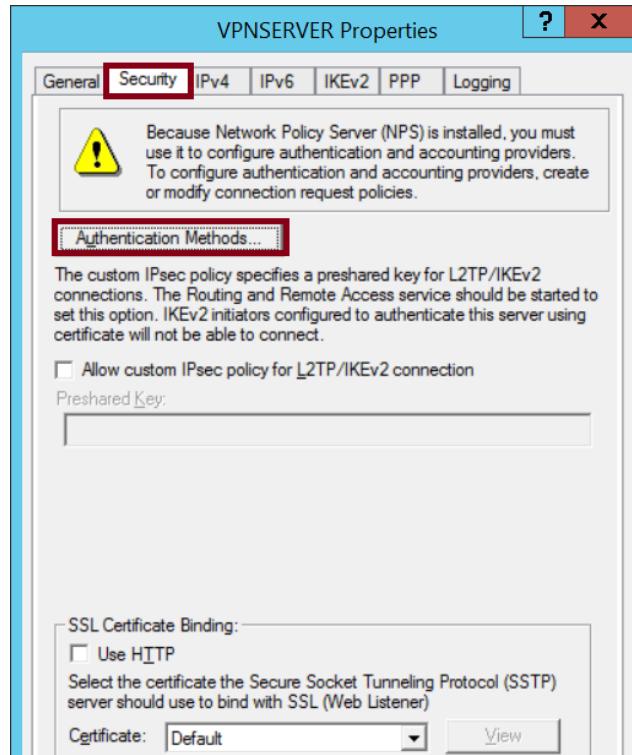
5. Enable the policy and click *Apply*.



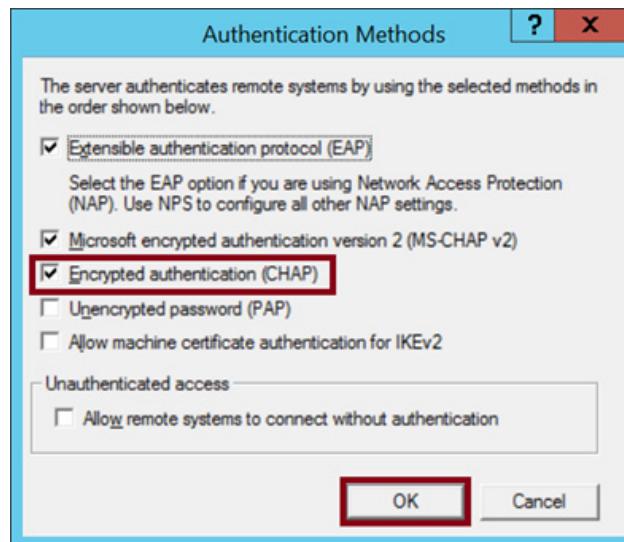
Now storing passwords using reversible encryption is allowed but all passwords stored in AD are still stored using irreversible encryption so CHAP will not work yet. To make it work users MUST change their passwords;

Configuring Microsoft RRAS to support CHAP

1. In RRAS configuration choose "Security" tab and click on "Authentication Methods...";



2. Make sure "Encrypted authentication (CHAP)" is checked and click "OK".

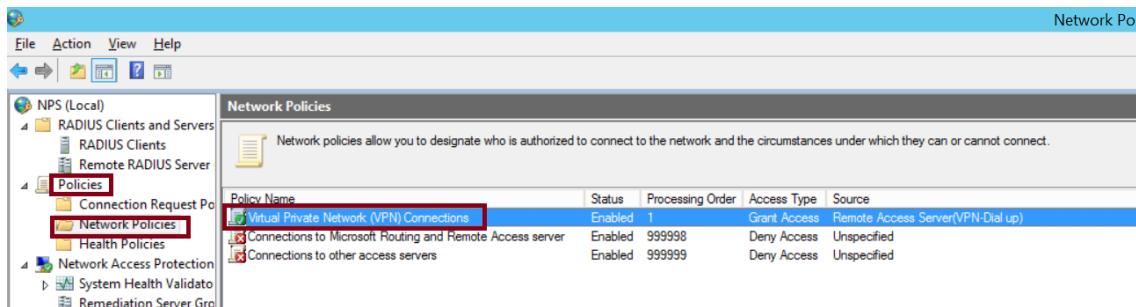


Configuring Microsoft NPS to support CHAP

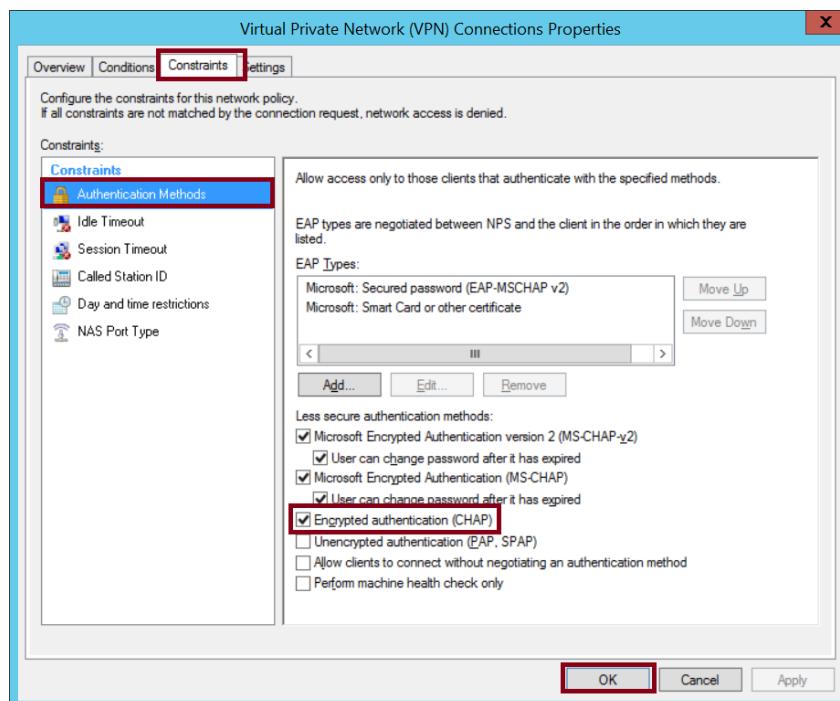
1. Open NPS Configuration;

Configuration required when using CHAP

2. Go to Policies|Network Policies|Virtual Private Network (VPN) Connections.



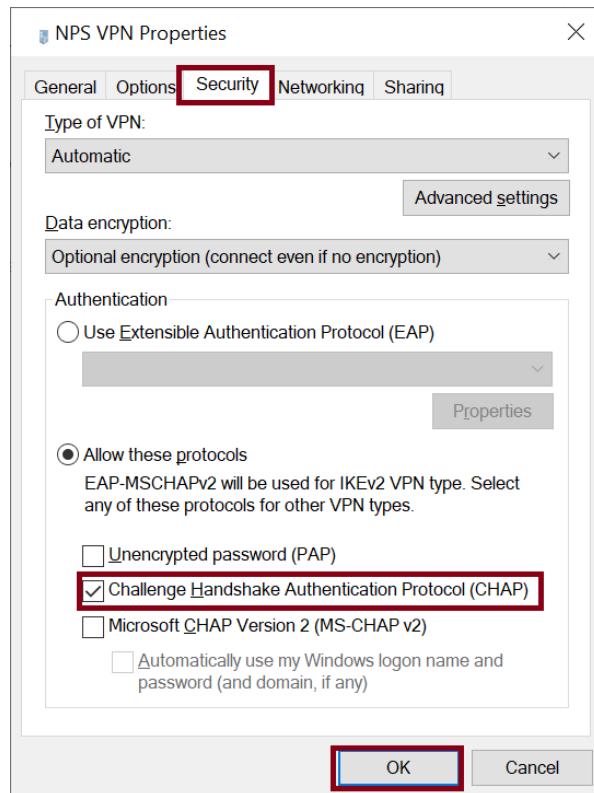
3. Click the *Constraints* tab, then select *Authentication Methods*. Ensure that *Encrypted Authentication (CHAP)* is checked and click *OK*.



Configuring Microsoft VPN Client to support CHAP

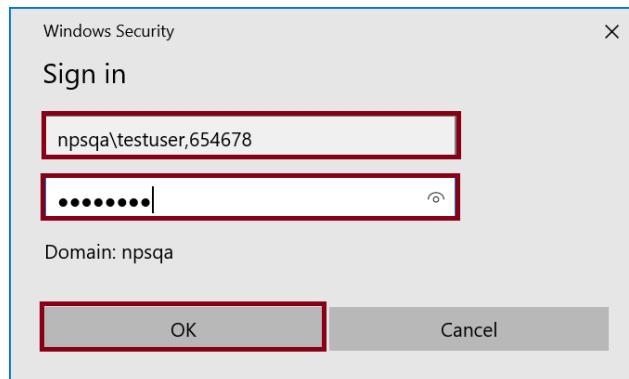
1. Open VPN Client configuration.

- Click on the *Security* tab. Make sure only *Challenge Handshake Authentication Protocol (CHAP)* is checked and click *OK*;



Testing the VPN connection using the CHAP protocol

- Choose your VPN connection and click *Connect*.
- In the connection dialog, enter your login credentials.



- User name - Enter in the following format: *user account name,OTP code*. For example if user name is *domain\user* and the OTP code is *654678*, enter *domain\user,654678*. Note that UPN names are not supported.
- Password - Enter your Windows password.

- Then click *OK*.

THIS CHAPTER PROVIDES INFORMATION ABOUT DIGITALPERSONA'S SUPPORT FOR DEPLOYMENT IN THE CITRIX ENVIRONMENT.

Main topics in this chapter	Page
Definitions	248
Supported Citrix platforms	248
Integration of Citrix with DigitalPersona components	248
Disabling automatic client updates	249
XenDesktop limitation	249

Overview

This chapter describes the built-in support for Citrix products provided with our DigitalPersona Workstation and Kiosk components

Definitions

XenApp enables launching a Citrix published application or entire desktop, hosted on a XenApp server in a data center, from anywhere, using your desktop computer, laptop, tablet or even a mobile phone.

XenDesktop uses the same technology, but provides each user with a unique (not shared) instance of the desktop operating system with any Citrix published applications.

Citrix Receiver is the Citrix local client that provides shared, encrypted access to the a Citrix published application or desktop, without needing to configure or launch a separate VPN client.

Supported Citrix platforms

DigitalPersona Workstation and DigitalPersona Kiosk may be installed and run on the Citrix XenApp and XenDesktop virtualization platforms.

At the time of release, support for the Citrix platform includes

- Citrix XenApp 7.5 and above
- Citrix XenDesktop 7.5 and above
- Citrix Receiver 3.4.0 and above

For updated information on supported versions and clients, see the *readme.txt* file provided with the DigitalPersona product package.

Integration of Citrix with DigitalPersona components

The following instructions assume that Citrix has been installed, configured and tested in the environment prior to installing the DigitalPersona client.

- To integrate the DigitalPersona components with Citrix, simply install a DigitalPersona client component on the Citrix server and on the client computer.
- If Citrix was not present prior to installing the DigitalPersona client, the files necessary to support Citrix will not be included as part of the component installation. You must run the DigitalPersona client installer and select *Repair* in order to enable Citrix support and then reboot the computer in order for the changes to take effect.

Disabling automatic client updates

It is possible that a Citrix update to the client could interfere with DigitalPersona functionality. To prevent this from happening, you may want to disable the automatic updating of clients from either the client or server machine.

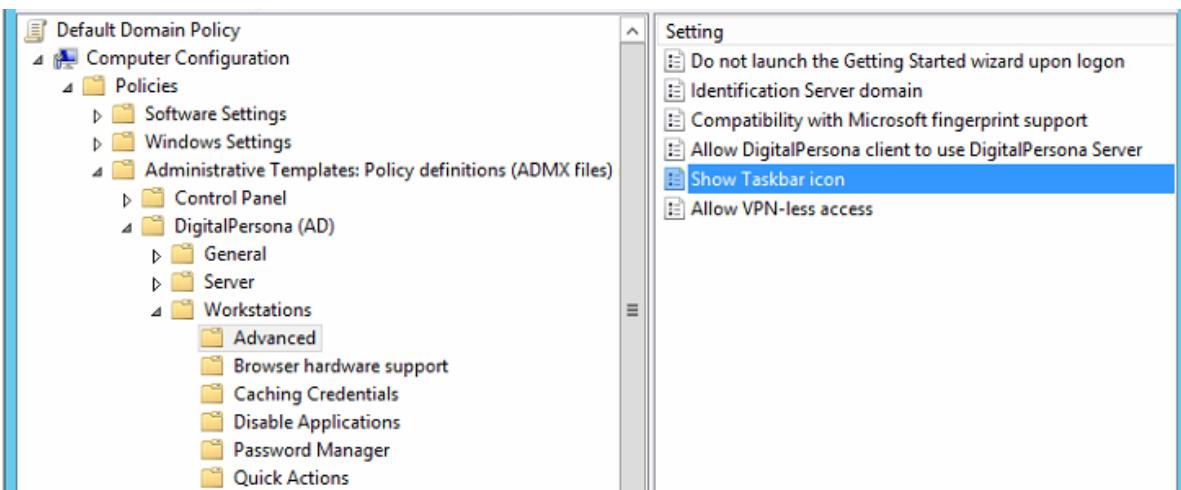
XenDesktop limitation

Due to the nature of XenDesktop's Credential Provider implementation, it is not possible to support using DigitalPersona credentials to log on to XenDesktop. After logging on to XenDesktop, DigitalPersona credentials may be used to log on to websites, applications and network resources through the DigitalPersona Password Manager application.

Resolving duplicate DigitalPersona system tray icons

In some cases, two DigitalPersona icons may be displayed in the system tray on the DigitalPersona Workstation. To resolve this issue, on the XenApp server, set the *Show taskbar icon* setting to *disabled*. The setting is located at the following location in the Policy Editor.

Computer configuration > Policies > AdministrativeTemplate Policy definitions > DigitalPersona Client > General Administration.



Resolving missing DigitalPersona system tray icon

A missing DigitalPersona system tray icon may be an indication that DpAgent failed to load, most probably due to recent changes in Citrix XenApp that disables systray agents by default. Password Manager relies on the systray agent to indicate that DpAgent has been loaded.

Caution! The following procedure requires you to edit the registry. Using Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Ed

To stop Citrix from disabling systray agents

1. On the XenApp server, open the registry and search for the setting *SeamlessFlags* or navigate to the setting at HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\wfshell\TWI.
2. If the setting doesn't exist, create the *SeamlessFlags* setting with a type of REG_DWORD and set its Hexadecimal value to 0x20, which will disable the *Disable Systray Agent* flag.

3. If the setting already exists, add the value 0x20 to any previous (Hexadecimal) value contained in the setting.

Example: To use two flags with values of 0x1 and 0x200, add them for a result of 0x201, i.e. the hexadecimal value for SeamlessFlags would be $0x1 + 0x200 = 0x201$.

More detailed information is available on the Citrix support site at the following URL.

https://support.citrix.com/content/dam/supportWS/kA460000000Cc9BCAS/Seamless_Configuration.pdf

This Citrix document provides additional background information on the SeamlessFlags setting and lists all of the available flags and their corresponding values.

If you need to create a registry flag on many servers, it might be worthwhile to create it first on one server, then export the registry key as a .Reg file, which can then be easily distributed to the other servers. To export a .Reg file from the Regedit file menu, select *Export*.

THIS CHAPTER DESCRIBES THE DIGITALPERSONA ADJUDICATION PROCESS USED TO IDENTIFY DUPLICATE FINGERPRINTS DURING ENROLLMENT.

Overview

Adjudication and deduplication is a process of identifying and processing situations where one or more users have fingerprints that are significantly similar. This feature is associated with the DigitalPersona Fingerprint Engine, and is not available when the Biometric Tokenization Engine is used.

During fingerprint identification and during fingerprint enrollment, if the matching score between a fingerprint being enrolled and one existing in the DigitalPersona database for another user is higher than the specified threshold, the result of the query is treated as a genuine match. This is called a false accept.

Setting the FAR (false accept rate) policy setting higher can mitigate this somewhat (see the *Fingerprint verification* setting in the *Policies and Settings* chapter), but it also has the effect of increasing the FRR (false reject rate) whereby some genuine users are not matched when presenting a fingerprint. So there is always a tradeoff between the FAR and the FRR.

When a duplicate is identified, what happens next depends on whether identification or enrollment is being performed.

Identification

The default DigitalPersona client behavior is to perform identification locally first through the local cache, and if it fails (and a connection to the DigitalPersona Server is available) identification is attempted on the server. If multiple candidates are found, the response is a no match and an error message is written to the appropriate event log. Note that possible duplicates are *not* deleted. You can also disable local caching for domain users via GPO (see the *Cache user data on local computer* setting).

Enrollment

When a user enrolls a fingerprint that is a duplicate of a fingerprint already in the DigitalPersona database, the following events occur.

- The fingerprint data (template) for the finger being enrolled will be discarded.
- The record (template) for the matched fingerprint will be deleted from the database. This means that the original user of the matched fingerprint will no longer be able to authenticate with that finger and may need to enroll another finger to meet any minimum number of enrolled fingerprints defined by the Fingerprint Enrollment policy in force.
- A message displays, *The fingerprint cannot be enrolled. Contact your administrator for more information.*
- The DigitalPersona Administrator is notified by the system writing two *duplicate fingerprint found* events to the event log on the DigitalPersona AD Server. One event with the new enrollee name and the number of the finger being enrolled, and another with the same information for the matched fingerprint.

The administrator needs to review the event log on a regular basis and follow up to determine the cause of the duplication. In most cases, they should delete the duplicate fingerprints from the database and re-enroll them.

Cautions

Note that whenever a fingerprint is enrolled, it may take a few minutes for it to be added to the identification set. Therefore, enrolling a duplicate fingerprint within that timespan may not trigger the duplicate fingerprint found event, since the first fingerprint may not have been added to the identification set yet.

Even after a duplicate fingerprint has been identified, when local caching is enabled (the default), the original user may in some cases be able to continue using their fingerprint for authentication and identification, for example when providing User Name+Fingerprint. In most cases, upon successful logon, the cache will be refreshed and that original user's duplicated fingerprint will no longer be valid.

Fingerprint Identifiers

In events written to the event log, fingerprints and duplicate fingerprints are identified using the numbers in the following table.

Finger	#
Left pinky finger	0
Left ring finger	1
Left middle finger	2
Left index finger	3
Left thumb	4
Right thumb	5
Right index finger	6
Right middle finger	7
Right ring finger	8
Right pinky finger	9

THIS CHAPTER DESCRIBES USE OF AN IDENTIFICATION LIST WITH DIGITALPERSONA COMPOSITE AUTHENTICATION AD.

Introduction

By default, all domain users are granted Kiosk access. However, DigitalPersona AD provides the capability to restrict identification to a specific list of users with permissions for the computer where the identification request originates.

To restrict identification

- Enable the *Restrict identification to a specific list of users* GPO setting (see page 89).
- Remove the default domain-level permission that includes all domain users in the identification list.
- Assign Allow or Deny permissions to the OU or computers.

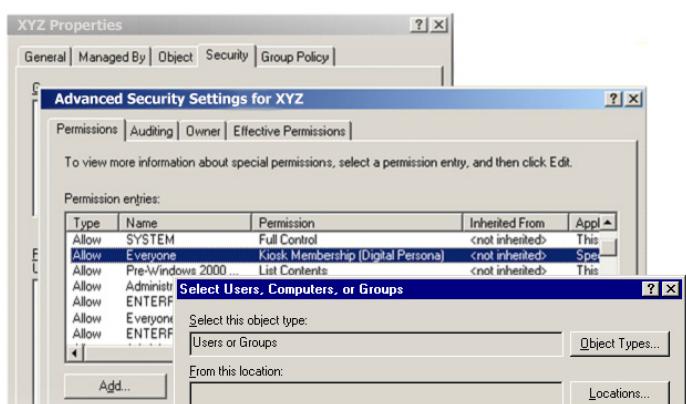
Note that this restriction applies to all supported credentials.

Also, since the Kiosk rights have to be read from the DigitalPersona AD Server to see whether or not there is a restriction, if the Kiosk is unable to reach an DigitalPersona AD Server, all users are assumed to be “restricted” and will be rejected, except for those users who have previously logged onto the Kiosk and are therefore cached on the client.

Example: Restricting kiosk identification

The following procedure assumes that a kiosk has already been created and that required Shared Account information has been entered. See *Kiosk Shared Account Settings* on page 24.

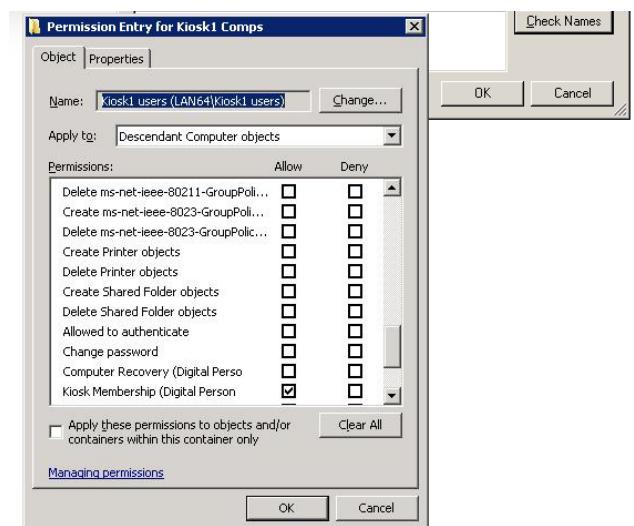
1. In the AD Users and Computers console menu, check the View menu to make sure that *Advanced Features* is on (has a check mark next to it).
2. Remove the default *domain-level* Kiosk Membership permission that allows everyone in the domain to be identified through the built-in ID Server.
 - Right-click on the domain and select *Properties*. On the *Security* tab, click the *Advanced* button
 - Within the *Advanced Security Settings* dialog, in the list of permissions, locate the permission *Allow\Everyone\Kiosk Membership (DigitalPersona)*, and click *Remove* to delete it.
3. Locate (or create) and select the OU or container object that you want to configure the membership for.
4. Ensure that all kiosk computers that you want to use this identification list for are shown within the container. Add kiosk computers as necessary.
5. If you are not using a previously defined user group for the identification list, create a new user group object and add the desired users to the group.
6. Right-click on the kiosk container and select *Properties*. On the *Security* tab, click the *Advanced* button.
7. Set Allow or Deny permissions as desired.
8. In the Advanced Security Settings dialog, click *Add* to display the *Permission Entry* dialog (see illustration on next page).
9. Click the *Select a principal* link to display the *Select Users, Computers or Groups* dialog. Then Enter the name of the group (or specific user) that you want to define permissions for and click *OK*.



Example: Restricting kiosk identification

10. Choose the permission type (Allow or Deny) from the *Type* dropdown menu.
11. In the *Applies To* drop-down list, select *Descendant Computer objects*.
12. Select *Kiosk Membership (DigitalPersona)*. Then click *OK*.

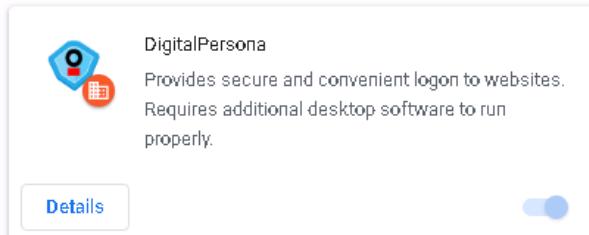
In most cases, it is preferable to manage permissions at the group level rather than on a user-by-user level. Note that a Deny permission always has precedence over any Allow permissions for a specific group or user.



THIS CHAPTER DESCRIBES THE PROCEDURE FOR FORCING INSTALLATION OF THE DIGITALPERSONA CHROME EXTENSION VIA GPO.

Introduction

The following instructions describe how to use a Policy Template to force installation of the DigitalPersona Extension for Google Chrome on Windows computers. The extension enables DigitalPersona Password Manager features within the Google Chrome browser.



IT administrators can set Chrome policies to install the DigitalPersona Chrome extension on their corporate-managed computers. This Chrome extension is installed on computers silently and users will not be able to uninstall it.

There are two types of policy templates available, ADMX and ADM. You'll want to verify which template type you can use on your network (ADM templates are designed for Windows XP and Windows Server 2003, whereas ADMX templates are for Windows Vista onwards.). These templates show which registry keys you can set to configure Chrome, and what the acceptable values are. Chrome looks at the values set in these registry keys to determine how to act.

Installation

1. Download Google Chrome templates and documentation from the following location:

https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip

2. Unpack the downloaded zip file.
3. From within the unzipped *Policy_Templates* folder, open the *Windows* folder and then the *.admx* folder (or *.adm* folder if your target computers are Windows XP or Windows Server 2003).

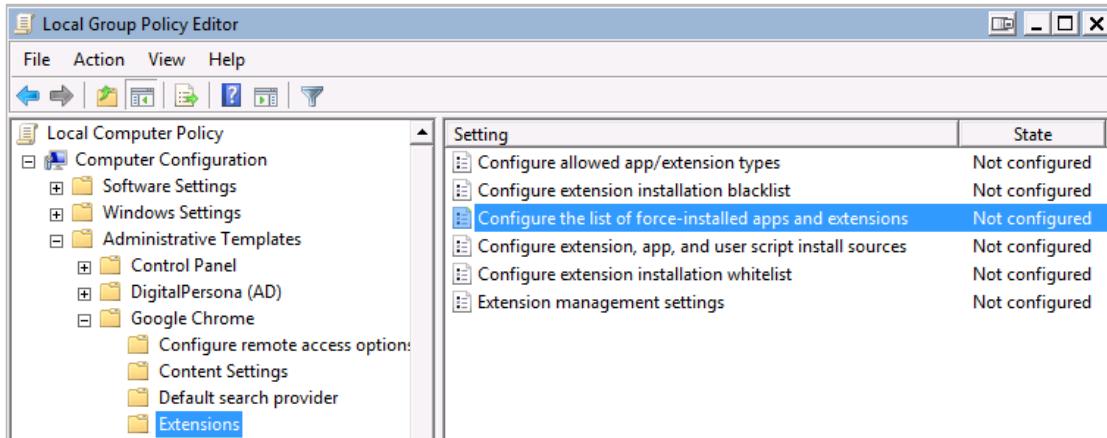
A screenshot of a Windows File Explorer window. The left pane shows a tree view of folders: "policy_templates", "chromeos", "common", "windows", "adm", "admx", "examples", "Previous", and "Read Me". The "admx" folder is selected and highlighted with a blue border. The right pane displays a list of files and folders under "admx".

Name	Date modified	Type
th-TH	3/5/2019 10:05 AM	File folder
tr-TR	3/5/2019 10:05 AM	File folder
uk-UA	3/5/2019 10:05 AM	File folder
vi-VN	3/5/2019 10:05 AM	File folder
zh-CN	3/5/2019 10:05 AM	File folder
zh-TW	3/5/2019 10:05 AM	File folder
<input checked="" type="checkbox"/> chrome.admx	3/5/2019 10:05 AM	ADMX File
<input type="checkbox"/> google.admx	3/5/2019 10:05 AM	ADMX File

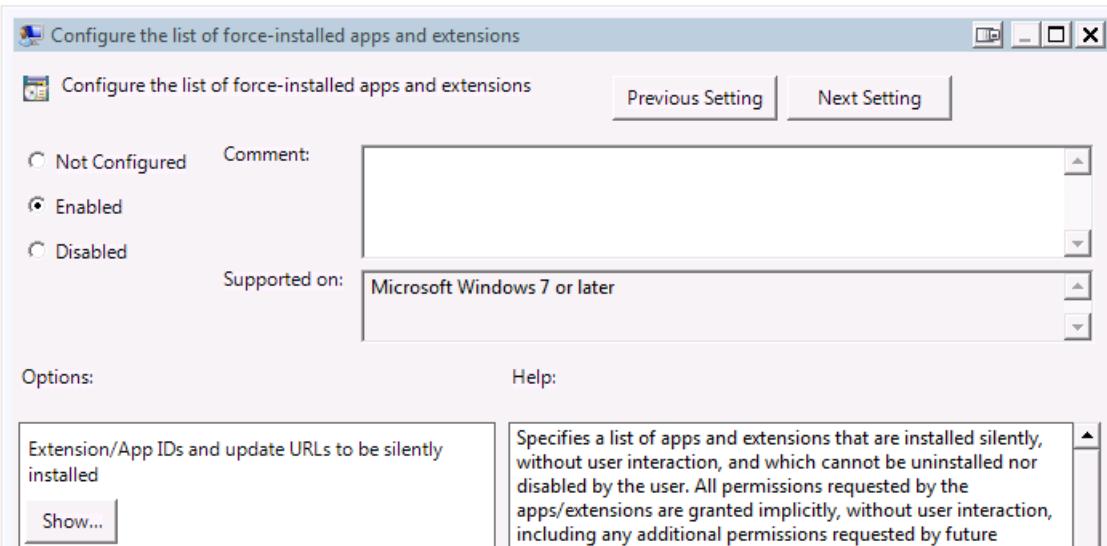
4. Copy the *chrome.admx* file and the relevant locale (*.adml*) file from the folder for your locale, i.e. *en-US* for the United States, to the folder where policy definitions on your computer are stored. This is usually *C:\Windows\PolicyDefinitions*). For Windows XP or Windows Server 2003, just copy the *chrome.adm* file from the folder for your locale.
5. Launch the Local Group Policy Editor.

To launch the Local Group Policy Editor, click on the *Start* button, type *Run* and press *Enter* to open the *Run* window. Type *gpedit.msc* and click *OK* to open the Local Computer Policy Editor.

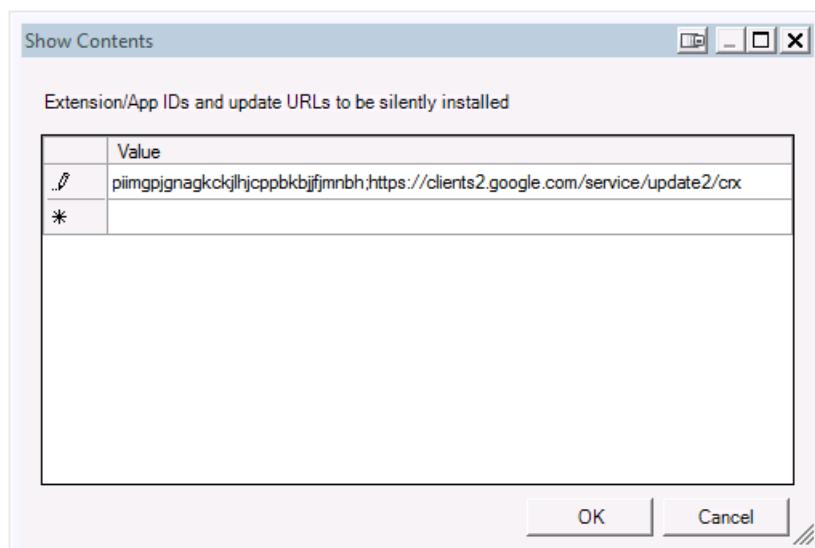
- Navigate to the following folder: *Local Computer Policy\Computer Configuration\Administrative Templates\Google Chrome\Extensions*.



- Double-click *Configure the list of force-installed apps and extensions* to open a dialog of the same name.



- Select the *Enabled* radio button and then click *Show...* to display the *Show Contents* dialog.



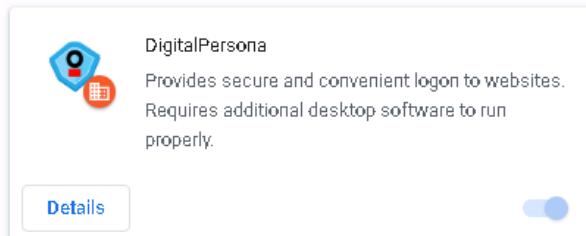
9. Copy and paste the following string into the text field and then click *OK*.

piimgpjqnagkckjlhjcppbkjjfjmnbh;https://clients2.google.com/service/update2/crx

10. In the *Configure the list of force-installed apps and extensions* dialog, click *Apply* and then *OK* to close the dialog.

11. Close the Local Group Editor.

12. You can verify that the installation was successful by typing chrome://extensions/ in your Chrome browser and ensuring that the DigitalPersona extension has been installed and enabled.



THIS CHAPTER DESCRIBES DIGITALPERSONA'S SUPPORT FOR SECURE FINGERPRINT SENSORS AND CERTAIN SMALL SENSORS.

WBF fingerprint reader support

DigitalPersona supports most WBF (Windows Biometric Framework) readers. It does so by using the WBF driver to get an image, and then using the DigitalPersona Fingerprint Engine to create a fingerprint template for matching, and finally storing the fingerprint template in the centralized DigitalPersona database. The fingerprint can then be used from any DigitalPersona workstation or from DigitalPersona web services and from the DigitalPersona Identity Provider (STS).

However, there are some fingerprint readers where the DigitalPersona Fingerprint Engine cannot be used.

For the types of fingerprint readers and sensors described below, the administrator should choose to store biometric data locally rather than remotely **during the installation** of DigitalPersona Workstation.

Secure fingerprint readers

For ‘secure’ fingerprint readers, defined as those which do not allow an image to leave the reader hardware, the actual template creation, matching and storage must be done by the reader hardware instead of the DigitalPersona Fingerprint Engine. Consequently, the template cannot be stored in the DigitalPersona database, and the fingerprint credential doesn’t roam, i.e. is not automatically available for authentication to other computers in the domain. This also means that fingerprints

- Can only be used on the computer where the fingerprints were originally enrolled.
- Cannot be used for web services or Office 365 integration through the Access Management API.
- Is not available within the DigitalPersona SSO for Office 365 product (because STS uses the DigitalPersona web services).

If during installation, the default choice to store biometric data remotely was selected, this behavior can be changed manually on the machine using the secure reader in order to allow full use of the WBF driver. Other DigitalPersona credentials will still roam and be stored on the DigitalPersona Server. However, a user wishing to have their fingerprint credential available on another computer will have to re-enroll the credential on the other machine (one that does not have this setting disabled).

Small form factor sensors

Certain small form factor sensors, such as those built into some mobile devices, tablets, laptops and accessories (such as the Surface Pro 4 Type Cover with Fingerprint ID or the Lenovo T460), also cannot use the DigitalPersona Fingerprint Engine for template creation or matching and therefore must be stored locally.



Overriding the CredentialsRoaming policy

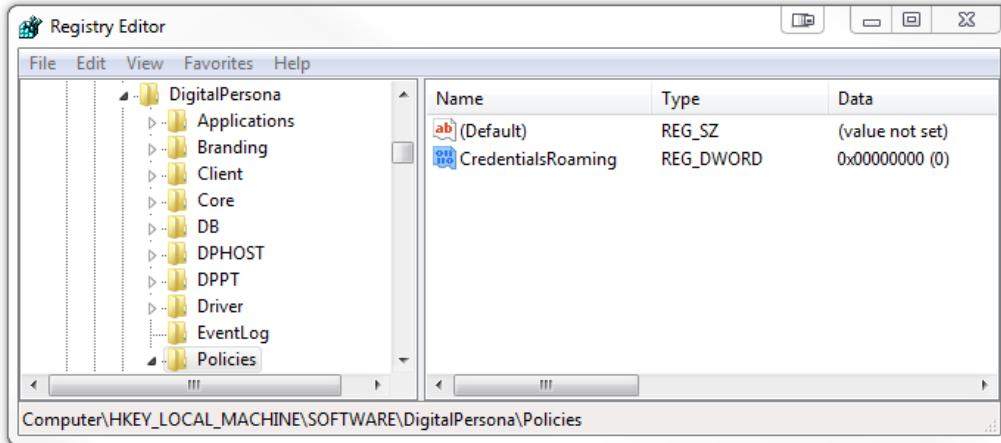
Complete the following steps to override the default *CredentialsRoaming* policy setting (which actually only affects roaming of fingerprints) in order to support the use of Microsoft’s WBF driver for fingerprint matching and storage on the computer.

Note that any fingerprints enrolled on the computer can then only be used for authentication on the computer where they were originally enrolled and do not roam.

To override the default credential roaming policy setting

1. Back up your registry!
2. Create a new registry entry (DWORD (32-bit Value) in the following location

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\DigitalPersona\Policies



3. Set the value to "0".
4. Close the Registry Editor.
5. Reboot the computer *twice*. Once will not be adequate.

THIS CHAPTER DESCRIBES THE PURPOSE USE AND LOCATION OF THE WINDOWS PASSWORD SYNCHRONIZATION TOOL.

Purpose

The purpose of the Windows Password Synchronization Tool (previously the Altus Windows Password Filter) is to resolve, and protect against, the situation where the Windows Password stored in the DigitalPersona database becomes out of sync with the user's current password as stored in Active Directory.

Background

When a user initially identifies themselves through the DigitalPersona software, either through self-enrollment within the DigitalPersona Console, or through Attended Enrollment, their Windows password is stored in the DigitalPersona database. When they change their Windows password through the DigitalPersona credential provider (at the logon screen) or through one of the DigitalPersona clients, their new password is stored in the DigitalPersona database and all is well.

If, on the other hand, their Windows password is changed outside of the DigitalPersona software, for instance through a non-DigitalPersona credential provider, the password is not stored in the DigitalPersona database and becomes unsynchronized, resulting in the inability for the user to authenticate within any of the DigitalPersona components.

Solution

The Windows Password Synchronization Tool, residing on the enterprise's domain controllers, intercepts all password change requests within the domain, and ensures that the new passwords are written to the DigitalPersona database.

It is critical that the tool be installed on all domain controllers in the domain.

Location

The Windows Password Synchronization Tool is part of the Altus 2.0.3 release, as well as the DigitalPersona Premium 2.1 and above releases. It is located in the '<ProductName> Windows Password Synchronization' folder.

This chapter explains the differences between the Group Policy Object containers and settings in versions 2.3 and 3.0 of the DigitalPersona solution.

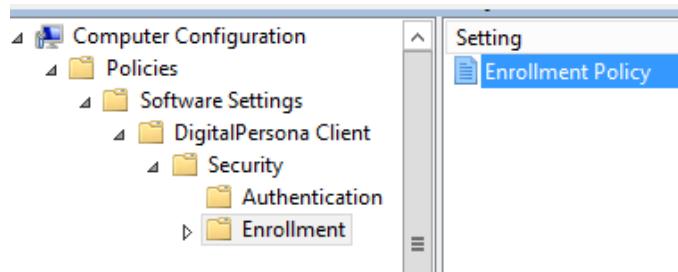
Version 3.0 of the DigitalPersona solution includes a significant reorganization of the containers and policy settings governing the software (compared to version 2.3), as well as several new, revised and renamed containers and policy settings, described below as they appear in the Windows Group Policy Editor. For complete descriptions of each setting, refer to the *Policies and Settings* chapter beginning on page 72.

These changes will be discussed in two sections, in accordance with the two primary Policy containers, *Software Settings* and *Administrative Templates*.

Computer Configuration/Policies/Software Settings

Renamed GPOs and settings

Self Enrollment Policy - This policy, located in the *DigitalPersona Client/Security/Enrollment* GPO, has been renamed to *Enrollment Policy*.



New containers and settings

Security GPO and settings

The *Security* GPO includes two new settings.

SMS

This new GPO consists of a single new setting, *SMS Configuration*, which includes three configurable values that were previously located in the *Administrative Templates/DigitalPersona AD Client/Authentication Devices|OTP* GPO.

These values are

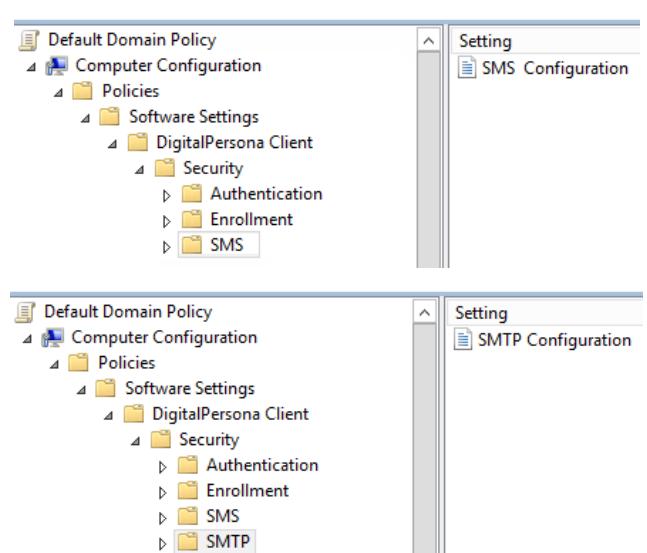
- Nexmo API Key
- Nexmo API Secret
- Nexmo Sender Addresses

SMTP

This new GPO consists of a single new setting, *SMTP Configuration*, which includes four required values for configuring the email account to be used with the new *Password Reset* feature.

These values are

- SMTP Server
- Port
- Email Address



- Email Password

Additionally, a field is provided for entering an *Incoming Email Address* and a *Test Settings* button, which can be used to confirm that the designated SMTP Server is working.

Computer Configuration/Policies/Administrative Templates

New Administrative Templates structure

Within the Computer Configuration/Policies/Administrative Templates container, the structure has been changed significantly, both at the topmost DigitalPersona level (as shown below) and at successive levels as shown in the images that follow.

Previous high-level structure

- ▷ DigitalPersona AD Client
- ▷ DigitalPersona AD Server

New high-level structure

- ▷ DigitalPersona (AD)
 - ▷ General
 - ▷ Server
 - ▷ Workstations

Previous expanded structure

- ▷ DigitalPersona AD Client
 - ▷ Authentication Devices
 - Bluetooth
 - Fingerprints
 - OTP
 - PIN
 - Smart cards
 - ▷ Event logging
 - DigitalPersona Reports
 - ▷ General Administration
 - Quick Actions
 - ▷ Managed applications
 - Disable Applications
 - Password Manager
 - ▷ Security
 - Settings
- ▷ DigitalPersona AD Server
 - ▷ Authentication Devices
 - Fingerprints
 - PIN
 - Credentials verification lockout
 - DigitalPersona Server DNS
 - Event logging
 - Identification Server settings
 - Windows Password Reset

New expanded structure

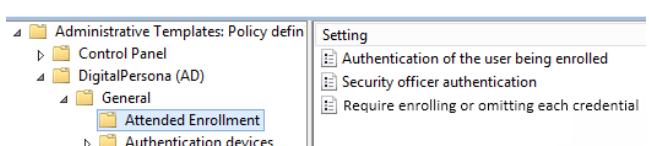
- ▷ DigitalPersona (AD)
 - ▷ General
 - Attended Enrollment
 - Authentication devices
 - Bluetooth
 - Fingerprints
 - OTP
 - PIN
 - ▷ Recovery Credentials
 - Recovery Questions
 - Self Password Reset
 - Smartcards
 - Event logging
 - ▷ Server
 - Credentials verification lockout
 - DigitalPersona Server DNS
 - Identification Server settings
 - ▷ Workstations
 - Advanced
 - Browser hardware support
 - Caching Credentials
 - Disable Applications
 - Password Manager
 - Quick Actions
 - DigitalPersona Reports

New GPOs and settings

Attended Enrollment

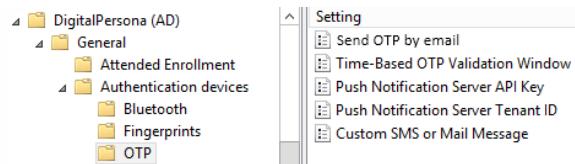
The *Attended Enrollment* GPO is new, and includes the following new settings (previously configured using XML files), which apply to both the Attended Enrollment application, and the Web Enrollment application when used for attended enrollment.

- Authentication of the user being enrolled
- Security Officer authentication
- Require enrolling or omitting each credential



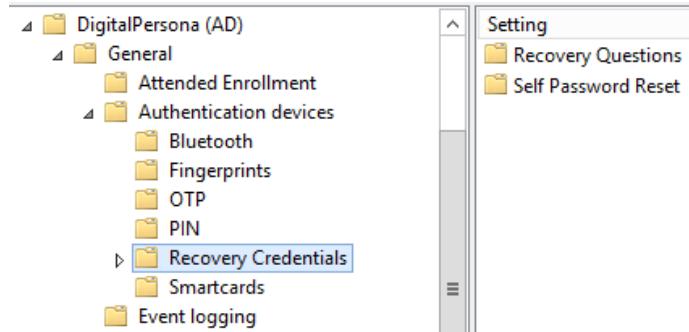
Send OTP by email

This setting is new, supporting the new ability for an AD User to choose to have their One-Time Password sent to them by email.



Recovery Credentials

This GPO is new, and includes two new GPOs, *Recovery Questions* and *Self Password Reset*.



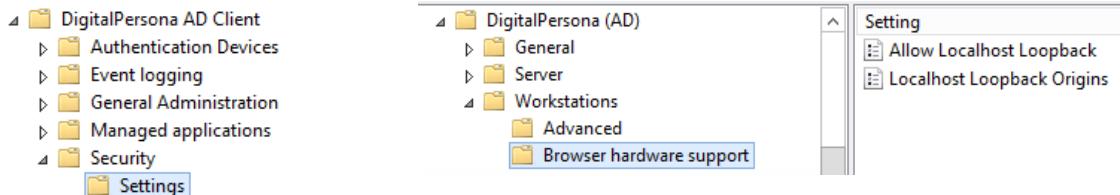
Recovery Questions - includes the *Enable Recovery Questions* setting, moved from the previous Security/Settings.

Self Password Reset - renamed from the previous *Windows Password Reset* GPO and moved from the DigitalPersona AD Server container to this location. It includes the following settings:

- Allow users to reset their Windows passwords (moved from previous *Windows Password Reset*)
- Path to DigitalPersona Secure Token Server (STS)

Browser hardware support

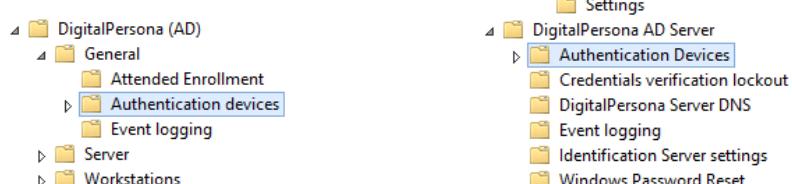
This GPO is new, and includes two settings previously located in the *DigitalPersona AD Client/Security/Settings* containers, *Allow Localhost Loopback* and *Localhost Loopback Origins*.



Relocated and renamed GPOs and settings

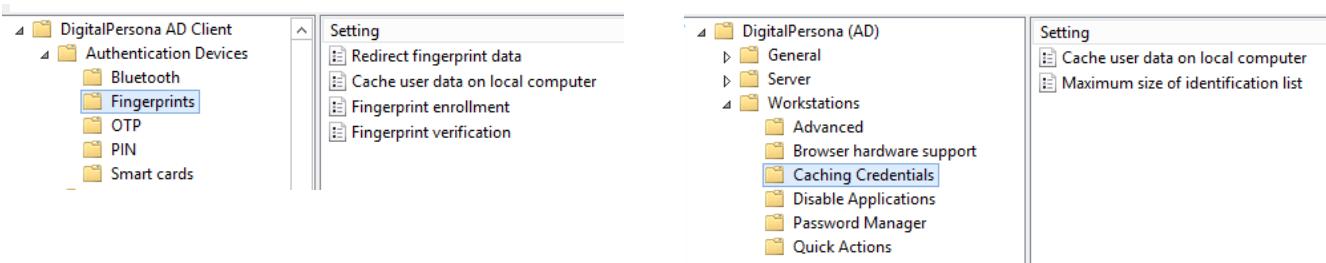
Authentication Devices

Previously there were *Authentication Devices* GPOs under both the Client and Server containers. They have been combined into one GPO, which includes the previous settings for both Server and Client, and which is now located in the *DigitalPersona AD/General* container.



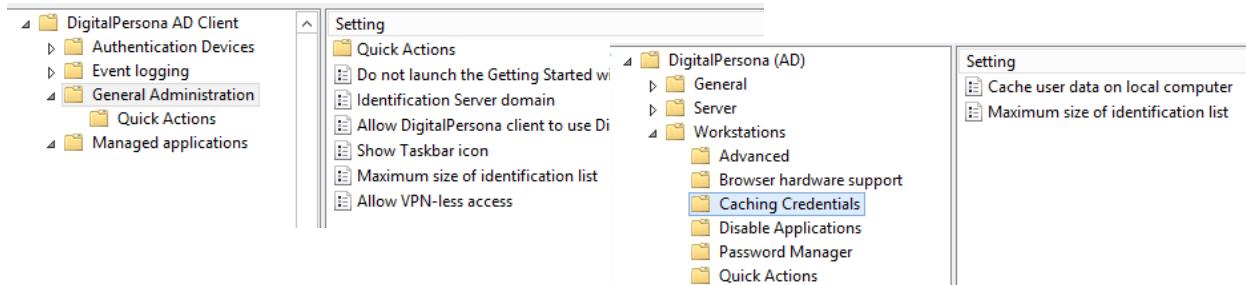
Cache user data on local computer

This setting was previously located within the *DigitalPersona AD Client/Authentication Devices/Fingerprint* GPO, and has been relocated to the *DigitalPersona AD/Workstations/Caching Credentials* GPO.



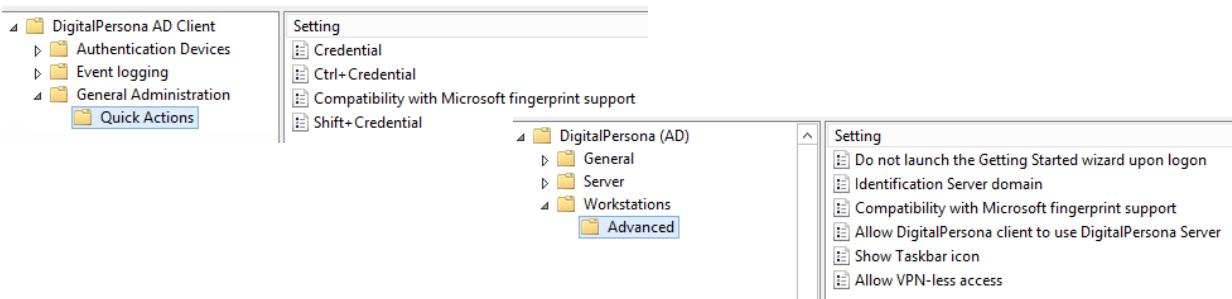
Maximum size of identification list

This setting was previously located within the *DigitalPersona AD Client/General Administration* GPO, and has been relocated to the *DigitalPersona AD/Workstations/Caching Credentials* GPO.



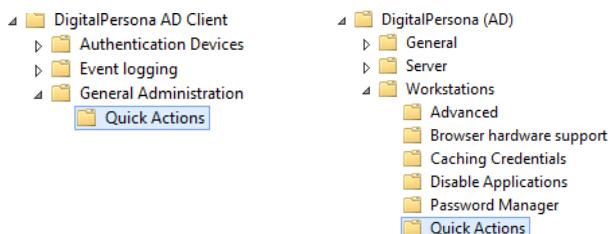
Compatibility with Microsoft fingerprint support

This setting was previously located within the *DigitalPersona AD Client/General Administration/Quick Actions* GPO, and has been relocated to the *DigitalPersona AD/Workstations/Advanced* GPO.



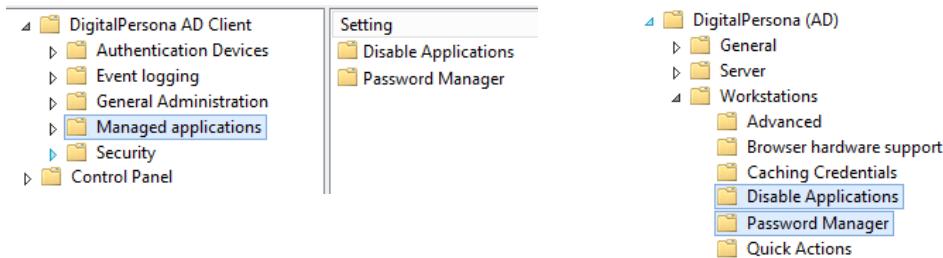
Quick Actions

This GPO was previously located within the *DigitalPersona AD Client/General Administration* container, and has been relocated to the *DigitalPersona AD/Workstations* GPO.



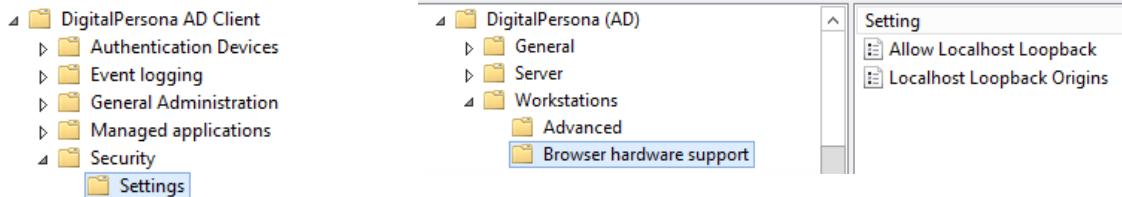
Managed Applications

This GPO, previously located within the *DigitalPersona AD Client* container, has been deleted. The *Disable Applications* and *Password Manager* GPOs have been relocated to the *DigitalPersona AD/Workstations* container.



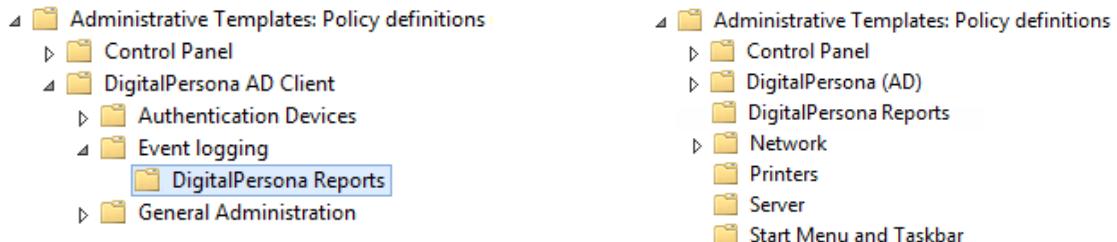
localhost settings

Two settings, *Allow Localhost Loopback* and *Localhost Loopback Origins*, previously in the *DigitalPersona AD Client/Security/Settings* GPO, have been relocated to the *DigitalPersona AD/Workstations/Advanced/Browser hardware support* GPO.



DigitalPersona Reports

This GPO, and the *Event Logging* container above it, previously in the *DigitalPersona AD Client* container, has been removed as it is no longer being used. The functionality has been replaced by the process of importing the DigitalPersona Reports GPOs described in the *DigitalPersona Reports* chapter beginning on page 104.



THIS CHAPTER DESCRIBES THE SCHEMA EXTENSION MADE TO THE ACTIVE DIRECTORY DATABASE IN ORDER TO SUPPORT THE OPERATION OF DIGITALPERSONA COMPOSITE AUTHENTICATION AD.

Main topics in this chapter	Page
Schema extension overview	266
Schema objects details	271
Class details	313

Introduction

This schema extension is version 5. The schema extension version number is independent of the DigitalPersona AD product version number. Each DigitalPersona AD product release will identify the schema extension version it requires.

The schema extension creates new attributes for the user object, creates new classes and makes changes to some existing classes (adding links), as shown in the following tables.

The Microsoft naming conventions are followed. The name prefix registered with Microsoft is “dp.” The Microsoft-generated OID base is 1.2.840.113556.1.8000.651.

For the full, detailed specifications, see Technical Bulletin 1006B, Schema Extension Specifications.

This document is intended to be used for reference purposes only, and may be superseded at any time by a new version.

Schema extension overview

Schema objects summary

The following schema objects are created in the Active Directory database.

Object	Description
dp-User-Credentials-Data	Stores fingerprint registration templates for the user.
dp-User-Account-Control	Specifies the flags to control fingerprint credentials behavior for the user.
dp-User-Private-Data	Stores the application secure data of the user.
dp-Servers-Data	Stores configuration data for all authentication servers in a particular domain.
dp-License	Stores the license for all servers in the Active Directory forest.
dp-User-Logon-Policy	Stores user logon policy information.
dp-User-Public-Key	Stores the user's public key.
dp-User-Payload	Stores the user's unified key data.
dp-User-Recovery-Key	Stores the user's recovery key.

Object	Description
dp-User-Data-Type	Stores the type of the user data stored in the dp-User-Private-Data attribute.
dp-Lockout-Time	Stores the date and time (UTC) that this account was locked out. This value is stored as a large integer that represents the number of 100 nanosecond intervals since January 1, 1601 (UTC). A value of zero means that the account is not currently locked out.
dp-Recovery-Password-Last-Set-Time	Stores data indicating the last time that the Recovery Password was set.
dp-Recovery-Password	Stores the computer's recovery password.
dp-Master-Key	Stores the computer's hard drive encryption key.
dp-Omit-Reasons	Stores the reasons credentials are omitted during an attended enrollment.
dp-Password-Manager-Data	Stores Password Manager data.
dp-Key	Stores the Time-based OTP key.
dp-OTP-Length	Stores the number of digits required in OTP code.
dp-OTP-Time-Interval	Stores the time interval for Time-based OTP.
dp-Servers-Configuration	Stores configuration information (settings) shared by all DigitalPersona Servers.

Object structure

Attribute property	Description
adminDisplayName	Display name of this object for use in directory service administrative tools.
adminDescription	Description of this object for use in directory service administrative tools
cn	Common name.
LDAPDisplayName	The name used by LDAP clients to refer to the object's class.
attributeID	A unique OID that identifies the attribute.
objectClass	The class of which this object is an instance.
objectCategory	Reference to an object class or one of its superclasses, which is used when searching for this object.
schemaIDGUID	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.

Attribute property	Description
attributeSyntax	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
oMSyntax	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
isSingleValued	TRUE means that the attribute has a single value, FALSE means that the attribute can have multiple values.
attributeSecurityGUID	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
searchFlags	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects.
showInAdvancedViewOnly	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell
systemFlags	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSFLAG_ENUM enumeration in ADSI Reference.
systemOnly	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

Schema classes summary

Class	Description
dp-Authentication-Servers-Container	Object Class Container for Authentication Server objects.
dp-User-Secret	Object Class used to represent application secure data of user (i.e. user encryption key).
dp-Service-Configuration	Object Class used to represent global configuration information such as schema version and license.
dp-Authentication-Service-Connection-Point	Object Class used to represent Authentication Server. The class contains information about the Authentication Server version, service principal name, binding information etc.
dp-OTP-Token	Object Class used to represent Hardware OTP tokens.

Class structure

Class Property	Description
adminDisplayName	Display name of this object for use in directory service administrative tools.
adminDescription	Description of this object for use in directory service administrative tools.
cn	Common name.
LDAPDisplayName	The name used by LDAP clients to refer to the object's class.
objectClass	The class of which this object is an instance.
objectCategory	Reference to an object class or one of its superclasses, which is used when searching for this object.
objectClassCategory	1 means structural classes. 2 means abstract classes. 3 means auxiliary classes
defaultObjectCategory	Object-Category used in queries for objects of this class.
rDNAttID	Attribute name used as the Relative Distinguished Name (RDN) for this class.
subClassOf	Immediate superclass of this class.
systemAuxiliaryClass	Auxiliary classes that this class inherits from.
governsID	A unique OID identifying the class.

Class Property	Description
schemaIDGUID	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
defaultSecurityDescriptor	The default security descriptor for new instances of this class.
defaultHidingValue	TRUE means that new object instances are hidden in the Administrative snap-ins and the Windows shell, FALSE covers all other situations.
showInAdvancedViewOnly	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in the Normal View of the Users and Computers snap-in and in the Windows shell.
systemPossSuperiors	Structural classes that can be containers of instances of this class. For the complete set of classes that can contain this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above.
systemOnly	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.
systemMustContain	Mandatory attributes that MUST be present on instances of this class. For the complete set of mandatory attributes for this class, you must, in addition to any values shown on the left, include those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.
systemMayContain	Optional attributes that may be present on instances of this class. For the complete set of optional attributes for this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.

Standard Classes Extensions

The following Active Directory classes are extended in the Active Directory Database to support DigitalPersona Composite Authentication AD.

User Class

mayContain: dp-User-Account-Control
dp-User-Credentials-Data

dpUserLogonPolicy
 dpUserPublicKey
 dpUserPayload
 dpUserRecoveryKey
 dpLockoutTime

Computer Class

mayContain:

- dpRecoveryPasswordLastSetTime
- dpRecoveryPassword
- dpMasterKey

Schema objects details

dp-User-Credentials-Data

Stores fingerprint registration templates for the user. The size of DigitalPersona fingerprint data depends on the number of fingerprints registered to a maximum 6.5 KB.

Attribute property	Value	Description
adminDisplayName	dp-User-Credentials-Data	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Credentials-Data	Description of this object for use in directory service administrative tools.
Cn	dp-User-Credentials-Data	Common name.
LDAPDisplayName	dpUserCredentialsData	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.1	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.

Attribute property	Value	Description
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	128	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper		The maximum value or length of an attribute.

Attribute property	Value	Description
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-User-Account-Control

Specifies the flags that control fingerprint credentials behavior for the user.

Size of DigitalPersona data: 4 bytes.

Attribute property	Value	Description
adminDisplayName	dp-User-Account-Control	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Account-Control	Description of this object for use in directory service administrative tools.
Cn	dp-User-Account-Control	Common name.
LDAPDisplayName	dpUserAccountControl	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.15	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.

Attribute property	Value	Description
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.9	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	2	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	<p>TRUE means that the attribute has a single value.</p> <p>FALSE means that the attribute can have multiple values.</p>
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	<p>TRUE means that the attribute is replicated to the global catalog.</p> <p>FALSE means that the attribute is not included in the global catalog.</p>

Attribute property	Value	Description
SearchFlags	0	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-User-Private-Data

Stores the user's secure application data.

Size of DigitalPersona data: Varies, depending on the type and size of the user Secrets saved. Potentially there is no limit. Usually it is around 530 bytes. OTS Secrets: Approximately 520 bytes + application logon data. Each application logon data consists of the account name + password + 18 bytes.

Attribute property	Value	Description
adminDisplayName	dp-User-Private-Data	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Private-Data	Description of this object for use in directory service administrative tools.
Cn	dp-User-Private-Data	Common name.
LDAPDisplayName	dpUserPrivateData	The name used by LDAP clients to refer to the object's class.
AttributelD	1.2.840.113556.1.8000.651.2	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).

Attribute property	Value	Description
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	0	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	131072	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-Servers-Data

Stores configuration data for all authentication servers in particular domain.

Size of DigitalPersona data: 1KB.

Attribute property	Value	Description
adminDisplayName	dp-Servers-Data	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Servers-Data	Description of this object for use in directory service administrative tools.
Cn	dp-Servers-Data	Common name.
LDAPDisplayName	dpServersData	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.10	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).

Attribute property	Value	Description
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	128	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	32768	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.

Attribute property	Value	Description
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-License

Stores license information for all DigitalPersona Servers in the Active Directory forest.

Size of DigitalPersona data: 0 (Not currently used – provided for future extension).

Attribute property	Value	Description
adminDisplayName	dp-License	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-License	Description of this object for use in directory service administrative tools.
Cn	dp-License	Common name.
LDAPDisplayName	dpLicense	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.14	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.

Attribute property	Value	Description
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	0	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	32768	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.

Attribute property	Value	Description
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-User-Logon-Policy

Stores the user's logon policy information.

Attribute property	Value	Description
adminDisplayName	dp-User-Logon-Policy	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Logon-Policy	Description of this object for use in directory service administrative tools.
Cn	dp-User-Logon-Policy	Common name.
LDAPDisplayName	dpUserLogonPolicy	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.16	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID	e667KO53BEyWMiMRqj3t4 A==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.

Attribute property	Value	Description
AttributeSyntax	2.5.5.9	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	2	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	<p>TRUE means that the attribute has a single value.</p> <p>FALSE means that the attribute can have multiple values.</p>
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	<p>TRUE means that the attribute is replicated to the global catalog.</p> <p>FALSE means that the attribute is not included in the global catalog.</p>
SearchFlags	0	<p>An integer value whose least significant bit indicates whether the attribute is indexed.</p> <p>The four bit flags in this value are:</p> <ul style="list-style-type: none"> 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects

Attribute property	Value	Description
showInAdvancedViewOnly	FALSE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-User-Public-Key

Stores the user's public key.

Attribute property	Value	Description
adminDisplayName	dp-User-Public-Key	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Public-Key	Description of this object for use in directory service administrative tools.
Cn	dp-User-Public-Key	Common name.
LDAPDisplayName	dpUserPublicKey	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.17	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.

Attribute property	Value	Description
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	<p>TRUE means that the attribute has a single value.</p> <p>FALSE means that the attribute can have multiple values.</p>
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	<p>TRUE means that the attribute is replicated to the global catalog.</p> <p>FALSE means that the attribute is not included in the global catalog.</p>

Attribute property	Value	Description
SearchFlags	0	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	131072	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-User-Payload

Stores the user's unified key data.

Attribute property	Value	Description
adminDisplayName	dp-User-Payload	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Payload	Description of this object for use in directory service administrative tools.
Cn	dp-User-Payload	Common name.
LDAPDisplayName	dpUserPayload	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.18	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).

Attribute property	Value	Description
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	128	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	32768	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.

Attribute property	Value	Description
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-User-Recovery-Key

Stores the user's recovery key.

Attribute property	Value	Description
adminDisplayName	dp-User-Recovery-Key	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Recovery-Key	Description of this object for use in directory service administrative tools.
Cn	dp-User-Recovery-Key	Common name.
LDAPDisplayName	dpUserRecoveryKey	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.19	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.

Attribute property	Value	Description
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	128	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	32768	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.

Attribute property	Value	Description
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-User-Data-Type

Stores the type of the user data stored in the dp-User-Private-Data attribute.

Attribute property	Value	Description
adminDisplayName	dp-User-Data-Type	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Data-Type	Description of this object for use in directory service administrative tools.
Cn	dp-User-Data-Type	Common name.
LDAPDisplayName	dpUserDataType	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.20	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.

Attribute property	Value	Description
AttributeSyntax	2.5.5.9	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	<p>TRUE means that the attribute has a single value.</p> <p>FALSE means that the attribute can have multiple values.</p>
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	<p>TRUE means that the attribute is replicated to the global catalog.</p> <p>FALSE means that the attribute is not included in the global catalog.</p>
SearchFlags	0	<p>An integer value whose least significant bit indicates whether the attribute is indexed.</p> <p>The four bit flags in this value are:</p> <ul style="list-style-type: none"> 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects

Attribute property	Value	Description
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-Lockout-Time

Stores the date and time (UTC) that this account was locked out. This value is stored as a large integer that represents the number of 100 nanosecond intervals since January 1, 1601 (UTC). A value of zero indicates that the account is not currently locked out.

Attribute property	Value	Description
adminDisplayName	dp-Lockout-Time	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Lockout-Time	Description of this object for use in directory service administrative tools.
Cn	dp-Lockout-Time	Common name.
LDAPDisplayName	dpLockoutTime	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.21	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.

Attribute property	Value	Description
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.16	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	65	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	<p>TRUE means that the attribute has a single value.</p> <p>FALSE means that the attribute can have multiple values.</p>
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	<p>TRUE means that the attribute is replicated to the global catalog.</p> <p>FALSE means that the attribute is not included in the global catalog.</p>
SearchFlags	0	<p>An integer value whose least significant bit indicates whether the attribute is indexed.</p> <p>The four bit flags in this value are:</p> <ul style="list-style-type: none"> 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects

Attribute property	Value	Description
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-Recovery-Password-Last-Set-Time

Stores data indicating the last time that the Recovery Password was set.

Attribute property	Value	Description
adminDisplayName	dp-Recovery-Password-Last-Set-Time	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Recovery-Password-Last-Set-Time	Description of this object for use in directory service administrative tools.
Cn	dp-Recovery-Password-Last-Set-Time	Common name.
LDAPDisplayName	dpRecoveryPasswordLastSetTime	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.22	A unique OID that identifies the attribute.

Attribute property	Value	Description
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.16	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
oMSyntax	65	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.

Attribute property	Value	Description
SearchFlags	0	<p>An integer value whose least significant bit indicates whether the attribute is indexed.</p> <p>The four bit flags in this value are:</p> <ul style="list-style-type: none"> 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
SystemFlags	0	<p>An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory.</p> <p>For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.</p>
SystemOnly	FALSE	<p>TRUE means that only Active Directory can modify the class of this object.</p> <p>FALSE means users can make the modification as well.</p>

dp-Recovery-Password

Stores the computer's recovery password.

Attribute property	Value	Description
adminDisplayName	dp-Recovery-Password	Display name of this object for use in directory service administrative tools.

Attribute property	Value	Description
AdminDescription	dp-Recovery-Password	Description of this object for use in directory service administrative tools.
Cn	dp-Recovery-Password	Common name.
LDAPDisplayName	dpRecoveryPassword	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.23	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.

Attribute property	Value	Description
SearchFlags	128	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	32768	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-Master-Key

Stores a computer's hard drive encryption key.

Attribute property	Value	Description
adminDisplayName	dp-Master-Key	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Master-Key	Description of this object for use in directory service administrative tools.
Cn	dp-Master-Key	Common name.
LDAPDisplayName	dpMasterKey	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.24	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).

Attribute property	Value	Description
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	128	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	32768	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.

Attribute property	Value	Description
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-Omit-Reasons

Stores the reasons credentials are omitted during attended enrollment.

Attribute property	Value	Description
adminDisplayName	dp-Omit-Reasons	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Omit-Reasons	Description of this object for use in directory service administrative tools.
Cn	dp-Omit-Reasons	Common name.
LDAPDisplayName	dpOmitReasons	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.29	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID	zKGWRTmm6U6DVvYunGc Pw==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.12	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
oMSyntax	64	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.

Attribute property	Value	Description
IsSingleValued	FALSE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
rangeUpper	32768	The maximum value or length of an attribute.

dp-Password-Manager-Data

Stores Password manager data.

Attribute property	Value	Description
adminDisplayName	dp-Password-Manager-Data	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Password-Manager-Data	Description of this object for use in directory service administrative tools.
Cn	dp-Password-Manager-Data	Common name.
LDAPDisplayName	dpPasswordManagerData	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.300	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID	WubMEBRH1ECmVdJsZGPZLw==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.12	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.

Attribute property	Value	Description
OMSyntax	64	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
attributeSecurityGUID	Not set	An optional GUID that identifies the attribute as a member of an attribute set (also known as a property set).
rangeUpper	131072	The maximum value or length of an attribute.

dp-OTP-Key

Stores the Time-based OPT key

Attribute property	Value	Description
adminDisplayName	dp-OTP-Key	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-OTP-Key	Description of this object for use in directory service administrative tools.
Cn	dp-OTP-Key	Common name.
LDAPDisplayName	dpOTPKey	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.33	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID	GpxNxP/ 1L0SmME0QEBI9Mw==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.

Attribute property	Value	Description
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	4	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags	128	An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	32768	The maximum value or length of an attribute.

Attribute property	Value	Description
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-OTP-Length

Stores the number of digital required in the OTP code.

Attribute property	Value	Description
adminDisplayName	dp-OTP-Length	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-OTP-Length	Description of this object for use in directory service administrative tools.
Cn	dp-OTP-Length	Common name.
LDAPDisplayName	dpOTPLength	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.35	A unique OID that identifies the attribute.

Attribute property	Value	Description
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID	C6XUG7q5akWi7Wpxwf9IHA==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.9	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	2	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.
SearchFlags		An integer value whose least significant bit indicates whether the attribute is indexed. The four bit flags in this value are: 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects

Attribute property	Value	Description
rangeUpper		The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSFLAG_ENUM enumeration in ADSI Reference.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

dp-OTP-Time-Interval

Stores the time interval for Time-based OTP.

Attribute property	Value	Description
adminDisplayName	dp-OTP-Time-Interval	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-OTP-Time-Interval	Description of this object for use in directory service administrative tools.
Cn	dp-OTP-Time-Interval	Common name.
LDAPDisplayName	dpOTPTimeInterval	The name used by LDAP clients to refer to the object's class.

Attribute property	Value	Description
AttributeID	1.2.840.113556.1.8000.651.36	A unique OID that identifies the attribute.
ObjectClass	Attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID	fBCb5mFA6EaqnP2rXeSTNw==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.9	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	2	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.

Attribute property	Value	Description
SearchFlags		<p>An integer value whose least significant bit indicates whether the attribute is indexed.</p> <p>The four bit flags in this value are:</p> <ul style="list-style-type: none"> 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper		The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	<p>TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell.</p> <p>FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.</p>
SystemFlags	0	<p>An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory.</p> <p>For more information, see ADS_SYSETMFLAG_ENUM enumeration in ADSI Reference.</p>
SystemOnly	FALSE	<p>TRUE means that only Active Directory can modify the class of this object.</p> <p>FALSE means users can make the modification as well.</p>

dp-Servers-Configuration

Stores configuration information (settings) shared by all DigitalPersona Servers.

Attribute property	Value	Description
adminDisplayName	dp-Servers-Configuration	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Servers-Configuration	Description of this object for use in directory service administrative tools.
Cn	dp-Servers-Configuration	Common name.
LDAPDisplayName	dpServersConfiguration	The name used by LDAP clients to refer to the object's class.
AttributeID	1.2.840.113556.1.8000.651.38	A unique OID that identifies the attribute.
ObjectClass	attribute-Schema	The class of which this object is an instance.
ObjectCategory	Attribute-Schema	Reference to an object class or one of its superclasses, which is used when searching for this object.
SchemaIDGUID	y7u2s3vp0UuWC/l+j1vKqA==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
AttributeSyntax	2.5.5.10	An OID of the syntax. The combination of the attributeSyntax and oMSyntax properties determines the syntax of an attribute.
OMSyntax	1	Syntax of this attribute as defined by the XAPIA XOM (X/Open Object Model) specification.
IsSingleValued	TRUE	TRUE means that the attribute has a single value. FALSE means that the attribute can have multiple values.
isMemberOfPartialAttributeSet	FALSE	TRUE means that the attribute is replicated to the global catalog. FALSE means that the attribute is not included in the global catalog.

Attribute property	Value	Description
SearchFlags		<p>An integer value whose least significant bit indicates whether the attribute is indexed.</p> <p>The four bit flags in this value are:</p> <ul style="list-style-type: none"> 1 = Index over attribute only 2 = Index over container and attribute 4 = Add this attribute to the Ambiguous Name Resolution set, used together with 0x0001 8 = Preserve this attribute in the tombstone object for deleted objects
rangeUpper	131072	The maximum value or length of an attribute.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
SystemFlags	0	An integer value that contains flags that define additional properties of this object. Category 1 classes or attributes have the 0x10 bit set by the system and cannot be set by users. They are shipped with Active Directory. For more information, see ADS_SYSETMFLAG_ENUM enumeration in Microsoft's Active Directory Service Interfaces Reference .
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

Class details

dp-User-Secret

This class represents the user Secret object that stores the secure application data (i.e. encryption keys) for the user.

Class property	Value	Description
adminDisplayName	dp-User-Secret	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-User-Secret	Description of this object for use in directory service administrative tools.
Cn	dp-User-Secret	Common name.
LDAPDisplayName	dpUserSecret	The name used by LDAP clients to refer to the object's class.
ObjectClass	ClassSchema	The class of which this object is an instance.
ObjectCategory	ClassSchema	Reference to an object class or one of its superclasses, which is used when searching for this object.
ObjectClassCategory	1	1 means structural classes. 2 means abstract classes. 3 means auxiliary classes.
defaultObjectCategory	dp-User-Secret	Object-Category used in queries for objects of this class.
rDNAttID	cn	Attribute name used as the Relative Distinguished Name (RDN) for this class.
subClassOf	Top	Immediate superclass of this class.
systemAuxiliaryClass		Auxiliary classes that this class inherits from.
governsID	1.2.840.113556.1.8000.651.5	A unique OID identifying the class.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.

Class property	Value	Description
defaultSecurityDescriptor	D:(A;;RPWPCRCCDCLCLOR CWOWDSDDTSW;;;;DA) (A;;RPWPCRCCDCLCLORC WOWDSDDTSW;;;;SY) (A;;RPLCLORC;;;;AU) S:(AU;SAFA;WDWOSDDTW PCRCCDCSW;;;;WD)	The default security descriptor for new instances of this class.
defaultHidingValue	TRUE	TRUE means that new object instances are hidden in the Administrative snap-ins and the Windows shell. FALSE covers all other situations.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
systemPossSuperiors	User	Structural classes that can be containers of instances of this class.
		For the complete set of classes that can contain this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.

Class property	Value	Description
systemMustContain		Mandatory attributes that MUST be present on instances of this class. For the complete set of mandatory attributes for this class, you must, in addition to any values shown on the left, include those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.
systemMayContain	dpUserPrivateData dpUserDataType	Optional attributes that may be present on instances of this class. For the complete set of optional attributes for this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.

dp-Authentication-Servers-Container

Container for Authentication Server objects.

Class property	Value	Description
adminDisplayName	dp-Authentication-Servers-Container	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Authentication-Servers-Container	Description of this object for use in directory service administrative tools.
Cn	dp-Authentication-Servers-Container	Common name.
LDAPDisplayName	dpAuthenticationServersContainer	The name used by LDAP clients to refer to the object's class.

Class property	Value	Description
ObjectClass	ClassSchema	The class of which this object is an instance.
ObjectCategory	ClassSchema	Reference to an object class or one of its superclasses, which is used when searching for this object.
ObjectClassCategory	1	1 means structural classes. 2 means abstract classes. 3 means auxiliary classes.
defaultObjectCategory	dp-Authentication-Servers-Container	Object-Category used in queries for objects of this class.
rDNAttID	cn	Attribute name used as the Relative Distinguished Name (RDN) for this class.
subClassOf	Container	Immediate superclass of this class.
systemAuxiliaryClass		Auxiliary classes that this class inherits from.
governsID	1.2.840.113556.1.8000.651.11	A unique OID identifying the class.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
defaultSecurityDescriptor	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY) (A;;CCDCLC;;;;DA) (A;;CCDCLC;;;;EA) (A;;CCDCLC;;;;BA) (A;CIIO;RPWPCRCCDCLCLORCWOWDSDDTSW;;;;BA) (OA;;RP;BF9679E5-0DE6-11D0-A285-00AA003049E2;;;;AU) (OA;;RP;26D97369-6070-11D1-A9C6-0000F80367C1;;;;AU) (A;;LC;;;;AU)	The default security descriptor for new instances of this class.

Class property	Value	Description
defaultHidingValue	TRUE	TRUE means that new object instances are hidden in the Administrative snap-ins and the Windows shell. FALSE covers all other situations.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
systemPossSuperiors	Container	Structural classes that can be containers of instances of this class. For the complete set of classes that can contain this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.
systemMustContain		Mandatory attributes that MUST be present on instances of this class. For the complete set of mandatory attributes for this class, you must, in addition to any values shown on the left, include those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.

Class property	Value	Description
systemMayContain	dpServersData dpServersConfiguration userCertificate	Optional attributes that may be present on instances of this class. For the complete set of optional attributes for this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.

dp-Service-Configuration

Class that represents global configuration information (i.e. schema version, license).

Class property	Value	Description
adminDisplayName	dp-Service-Configuration	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Service-Configuration	Description of this object for use in directory service administrative tools.
Cn	dp-Service-Configuration	Common name.
LDAPDisplayName	dpServiceConfiguration	The name used by LDAP clients to refer to the object's class.
ObjectClass	ClassSchema	The class of which this object is an instance.
ObjectCategory	ClassSchema	Reference to an object class or one of its superclasses, which is used when searching for this object.
ObjectClassCategory	1	1 means structural classes. 2 means abstract classes. 3 means auxiliary classes.
defaultObjectCategory	dp-Service-Configuration	Object-Category used in queries for objects of this class.
rDNAttID	cn	Attribute name used as the Relative Distinguished Name (RDN) for this class.

Class property	Value	Description
subClassOf	Top	Immediate superclass of this class.
systemAuxiliaryClass		Auxiliary classes that this class inherits from.
governsID	1.2.840.113556.1.8000.651.12	A unique OID identifying the class.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
defaultSecurityDescriptor	D:(A;;RPWPCRCCDCLCLOR CWOWDSDDTSW;;;DA) (A;;RPWPCRCCDCLCLORC WOWDSDDTSW;;;SY) (A;;RPLCLORC;;;AU) S:(AU;SAFA;WDWOSDDTW PCRCCDCSW;;;WD)	The default security descriptor for new instances of this class.
defaultHidingValue	TRUE	TRUE means that new object instances are hidden in the Administrative snap-ins and the Windows shell. FALSE covers all other situations.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
systemPossSuperiors	Container	Structural classes that can be containers of instances of this class. For the complete set of classes that can contain this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above.

Class property	Value	Description
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.
systemMustContain		Mandatory attributes that MUST be present on instances of this class. For the complete set of mandatory attributes for this class, you must, in addition to any values shown on the left, include those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.
systemMayContain	AppSchemaVersion dpLicense	Optional attributes that may be present on instances of this class. For the complete set of optional attributes for this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.

dp-Authentication-Service-Connection-Point

This class represents the Authentication Server. It provides information about Authentication Server (i.e. version, service principal name, binding information).

Class property	Value	Description
adminDisplayName	dp-Authentication-Service-Connection-Point	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-Authentication-Service-Connection-Point	Description of this object for use in directory service administrative tools.

Class property	Value	Description
Cn	dp-Authentication-Service-Connection-Point	Common name.
LDAPDisplayName	dpauthenticationServiceConnectionPoint	The name used by LDAP clients to refer to the object's class.
ObjectClass	ClassSchema	The class of which this object is an instance.
ObjectCategory	ClassSchema	Reference to an object class or one of its superclasses, which is used when searching for this object.
ObjectClassCategory	1	1 means structural classes. 2 means abstract classes. 3 means auxiliary classes.
defaultObjectCategory	dp-Authentication-Service-Connection-Point	Object-Category used in queries for objects of this class.
rDNAttID	cn	Attribute name used as the Relative Distinguished Name (RDN) for this class.
subClassOf	ServiceConnectionPoint	Immediate superclass of this class.
systemAuxiliaryClass		Auxiliary classes that this class inherits from.
governsID	1.2.840.113556.1.8000.651.13	A unique OID identifying the class.
SchemaIDGUID		A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
defaultSecurityDescriptor	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA) (A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY) (A;;RPLCLORC;;;AU) S:(AU;SAFA;WDWOSDDTWPCRCCDCSW;;;WD)	The default security descriptor for new instances of this class.
defaultHidingValue	TRUE	TRUE means that new object instances are hidden in the Administrative snap-ins and the Windows shell. FALSE covers all other situations.

Class property	Value	Description
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
systemPossSuperiors	Container	Structural classes that can be containers of instances of this class. For the complete set of classes that can contain this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above.
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.
systemMustContain		Mandatory attributes that MUST be present on instances of this class. For the complete set of mandatory attributes for this class, you must, in addition to any values shown on the left, include those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.

Class property	Value	Description
systemMayContain	AppSchemaVersion	Optional attributes that may be present on instances of this class.
	MarshalledInterface	For the complete set of optional attributes for this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.
	Vendor	
	VersionNumber	
	VersionNumberHi	
	VersionNumberLo	

dp-OTP-Token

Class that represents the hardware Time-based OTP token.

Class property	Value	Description
adminDisplayName	dp-OTP-Token	Display name of this object for use in directory service administrative tools.
AdminDescription	dp-OTP-Token	Description of this object for use in directory service administrative tools.
Cn	dp-OTP-Token	Common name.
LDAPDisplayName	dpOTPToken	The name used by LDAP clients to refer to the object's class.
ObjectClass	ClassSchema	The class of which this object is an instance.
ObjectCategory	ClassSchema	Reference to an object class or one of its superclasses, which is used when searching for this object.
ObjectClassCategory	1	1 means structural classes. 2 means abstract classes. 3 means auxiliary classes.
defaultObjectCategory	dp-OTP-Token	Object-Category used in queries for objects of this class.
rDNAttID	cn	Attribute name used as the Relative Distinguished Name (RDN) for this class.

Class property	Value	Description
subClassOf	device	Immediate superclass of this class.
systemAuxiliaryClass		Auxiliary classes that this class inherits from.
governsID	1.2.840.113556.1.8000.651.034	A unique OID identifying the class.
SchemaIDGUID	YWQM2TgaD0OrjtJX3lL4vg==	A GUID that uniquely identifies this object. You can use this string value in an ACE to control access to objects of this object.
defaultSecurityDescriptor	D:(A;;RPWPCRCCDCLCLOR CWOWDSDDTSW;;;DA)(A;;R PWPCRCCDCLCLORCWOW DSDDTSW;;;SY) (A;;RPLCLORC;;;AU)S:(AU;SAFA;WDWOSDDTWPCRCCDCSW;;;WD)	The default security descriptor for new instances of this class.
defaultHidingValue	TRUE	TRUE means that new object instances are hidden in the Administrative snap-ins and the Windows shell. FALSE covers all other situations.
showInAdvancedViewOnly	TRUE	TRUE means that the object will appear in the Advanced View of the Users and Computers snap-in only, but not in the Windows shell. FALSE means that the object will appear in Normal view of the Users and Computers snap-in and the Windows shell.
systemPossSuperiors	Container	Structural classes that can be containers of instances of this class. For the complete set of classes that can contain this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above.

Class property	Value	Description
SystemOnly	FALSE	TRUE means that only Active Directory can modify the class of this object. FALSE means users can make the modification as well.
systemMustContain		Mandatory attributes that MUST be present on instances of this class. For the complete set of mandatory attributes for this class, you must, in addition to any values shown on the left, include those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.
systemMayContain	dpOTPKey dpOTPLength dpOTPTimeInterval	Optional attributes that may be present on instances of this class. For the complete set of optional attributes for this class, you must include, in addition to any values shown on the left, those inherited from its superclasses as listed in the subClassOf attribute above and/or those derived from any of its auxiliary classes as specified in the systemAuxiliary attribute above and as inherited from its superclasses.

Standard Classes Extensions

User Class:

mayContain: dp-User-Credentials-Data, dp-User-Account-Control.

Symbols

dpproent SRV RR 27
uareupro SRV RR
— DNS Console path 28
modifying Priority and Weight settings 28
.config files 188

Numerics

0x8007005 error 221
0x8007501 error 221

A

account is locked out from use of fingerprint credentials setting 55
Account lockout duration (setting) 86
threshold (setting) 87, 103
account lockout 102
Active Directory containers 26
Biometric Authentication Servers container 26
Active Directory Domain Configuration Wizard 21
Active Directory Schema Extension Wizard 20
adding a change password screen 149
adding a change password screen manually 154
Adjudication process 251
Administration Tools
Cleanup Wizard 127
Administrative Templates 23, 30, 31, 38, 67
DPCA_AD/DesktopApps.admx 68
DPCA_AD/General.admx 67
DPCA_AD/IDServer.admx 70
DPCA_AD/OneTouchLock.admx 69
DPCA_AD>PasswordManager.admx 69
DPCA_AD/Root.admx 67
DPCA_AD/Servers.admx 69
ADUC Snap-in 54
Advanced Configuration, Web Management Components 172
Allow Altus client to use Altus Server (setting) 91
Allow Recovery Questions for Windows Logon 84
Allow use of personal logons (setting) 93
Allow users to add account data 93
Allow users to delete account data 93
Allow users to edit account data 93
Allow users to view managed logon passwords 93
Allow VPN-less access 91
Allow VPN-less access (setting) 91
Application Portal 216

Attended Enrollment 31

Attended Enrollment, setting up 94
attributes 141

Authentication Server Object Name property 26
authenticator app 203
Automated site coverage by Altus Server Locator DNS SRV records (setting) 87

automatic account creation 204
automatic DNS registration 27

B

Biometric Authentication Servers container 26
Bluetooth 80

C

CAC/PIV card module 33
Cache user data on local computer 91
can't open client console 219
Cannot save logon due to attribute size limitation 222
change password screen 149
changes made during installation 26
checking for license updates 47
Citrix Receiver 248
Citrix support 248
Cleanup Wizard 127
client-outside-the firewall. *See* Allow VPN-less access 91
configure domain 21
configure ports used by DigitalPersona for firewall 219
configuring
DigitalPersona AD Server GPO settings 24
OUs for kiosks 24
settings for DigitalPersona Kiosk 24
configuring DNS dynamic registration 28
console fails to open 219
creating an extended authentication policy 148
Credential Authentication events 124
Credential Management events 120
credentials report 56
CredentialsRoaming registry setting 258
Custom SMS Message, Nexmo 83

D

deactivating your license 49
Deduplication 251
delay 148
Delegating permissions for SMS/SMTP management 128
Delete Credentials command 56

- Delete License command **53, 56**
Delete user license **53**
delete user license **56**
deploy managed logons **140, 146, 151, 156, 159**
Deployment events **125**
DigitalPersona
 Application Portal **216**
 Identity Server **181**
 Kiosk **13**
 Lite Client **196**
 Mobile app **203**
 Web Administration Console **190**
 Workstation **13**
DigitalPersona AD Server
 Active Directory containers **26**
 installation overview **19**
 installing software **22**
 published information **26**
 uninstalling **28**
DigitalPersona CAC/PIV card module **33**
displaying license properties **48**
DNS Console path **28**
DNS Registration **27**
DNS Registration events **124**
Do not launch the Getting Started wizard upon logon
 (setting) **90**
domain isn't available **221**
domain, configuring for DigitalPersona AD Server **21**
download an authenticator app **203**
DPCA_AD/DesktopApps.admx **68**
DPCA_AD/General.admx **67**
DPCA_AD/IDServer.admx **70**
DPCA_AD/OneTouchLock.admx **69**
DPCA_AD/PasswordManager.admx **69**
DPCA_AD/Root.admx **67**
DPCA_AD/Servers.admx **69**
Dynamic registration of Altus Server Locator DNS
 records (setting) **88**
dynamically assigned ports **219**
- E**
- Error Access Denied **221**
ESPM **63**
events
 Credential Authentication **124**
 Credential Management **120**
 Deployment **125**
 DNS Registration **124**
 Password Manager **123**
 Secret Management **122**
 Service Management **123**
- System **123**
User Management **121**
Windows Logon **125**
Express Configuration, Web Management
 Components **169**
extend the Active Directory schema **20**
extended authentication policy **148**
Extended Server Policy Module **63**
- F**
- field catalog **160**
finding duplicate logons **162**
finding fields in logons **161**
finding logons **161**
Fingerprint credentials cache is cleared **120**
fingerprint registration not allowed error **221**
- G**
- ghosting **13**
GPMC/GPOE Extensions **65**
GPO
 implementation guidelines **70**
Group Policy Object Extensions **66**
- H**
- hardware OTP token seed files, import **193**
- I**
- identification list, maximum size **91**
Identity Server **181**
imaging **13**
implementation guidelines **70**
import Hardware OTP Token seed files **193**
improving performance **28**
installing
 ADUC User Properties Snap-in **30**
 DigitalPersona AD Server **22**
Installing Administrative Templates Locally **71**
- K**
- kiosk permissions **25**
Kiosk Session Authentication Policy **76**
- L**
- Level of detail in event logs (setting) **85**
license activation **42**
license activation from another computer **44**
license deactivation **49**
license deactivation from another computer **50**
License Group Policy Object **42**
license report **56**

- License Transfer file **41**
- License, delete/recover **53**
- license, delete/recover **56**
- Lite Client **196**
- Lock the computer on smart card removal (setting) **83, 85**
- locked account **55**
- locked computer **102**
- Log Status Events **85, 126**
- logon field values **141**
- logon fields **143**
- logon fields attributes **141**
- M**
 - manage Hardware OTP Tokens **193**
 - managed logons **137**
 - Managed logons (setting) **93**
 - manual DNS registration **27**
 - maximum size of identification list **91**
 - migration **19**
 - modifying
 - DNS Priority setting **28**
- N**
 - Nexmo
 - Custom SMS Message **83**
 - Sender Addresses **83**
 - no logon servers available **221**
- O**
 - onfiguring the DigitalPersona Identity Server **184**
 - online help **17**
 - OTP **82**
 - OTP only authentication (NPS VPN Plugin) **243**
 - OTP Push Notification Support (NPS Plugin) **242**
- P**
 - password field values **141**
 - Password Manager events **123**
 - password policies **151**
 - Path(s) to the managed logons folder(s) **93**
 - PIV card support **33**
 - policies
 - DigitalPersona client **73, 74**
 - DigitalPersona Server **93**
 - policyBypassGroups **188**
 - ports used by DigitalPersona **219**
 - prerequisites for DigitalPersona SAML SSO Portal **216**
 - Prevent Password Manager from running (setting) **92**
 - Priority set in Altus Server Locator DNS records (setting) **88**
 - Product Compatibility **17**
- R**
 - randomize user's Windows Password **55**
 - recover password **102**
 - Recover user license **53**
 - recover user license **56**
 - recovery
 - from account lock **103**
 - user **102**
 - Recovery Questions **86**
 - refresh license **47**
 - Register Altus Server Locator DNS records for domain (setting) **88**
 - regular expression syntax **156**
 - releasing user licenses **53**
 - remote license activation **44**
 - remote license deactivation **50**
 - removing DigitalPersona AD data **127**
 - Reset account lockout counter after (setting) **86**
- S**
 - schema
 - Active Directory Schema Extension Wizard **20**
 - extending **20**
 - schema extension
 - class details **313**
 - class structure **269**
 - details **271**

- overview 266
 schema classes summary 269
 schema object structure 267
 schema objects details 270
 schema objects overview 266
 standard classes extensions 325
 Schema Version Number property 26
 second authentication factor 149
 Secret Management events 122
 Self Password Reset 84
 Service Class GUID property 26
 Service Class Name property 26
 Service Management events 123
 Service Principal Name property 26
 Service Resource Records
 _dpproent SRV RR 27
 adding manually 28
 format 27
 Session Authentication Policy 76
 Set the False Accept Rate 82
 Set the maximum number of enrolled fingerprints 82
 Set the minimum number of enrolled fingerprints 82
 set up a DigitalPersona account on your device 203
 setting up
 a change password screen 149
 a change password screen manually 154
 a logon screen 137
 setting up a logon screen 137
 setting up Attended Enrollment 94
 settings
 DigitalPersona AD client (user) 93
 DigitalPersona AD Server 93
 DigitalPersona client 73, 74
 Shared Accounts, specifying 25
 SMS/SMTP Management
 Delegating permissions 128
 specifying Shared Accounts 25
 Status events 105
 Status Notifier events 85, 126
 support
 online help 17
 readme file 17
 System events 123
- T**
- target icon 148
 to unlock a locked account 55
 Tools page 161
 troubleshooting 219
- U**
- unavailable domain 221
 unavailable server 221
 uninstalling
 DigitalPersona AD Server 28
 unlocking locked accounts 55
 Upgrading from previous versions 14
 upgrading from Previous Versions 19
 User Context Menu commands 55, 103
 user license delete/recover 56
 User license, delete/recover 53
 User Management events 121
 User must provide Fingerprint and PIN to log on 63
 User must provide Fingerprint and Windows Password to log on 64
 user object commands 55
 User provides only Windows credentials to log on 55
 User Query snap-in 56
 ActiveX control 56
 command line utility 56
 interactive application 56
 user recovery 102
 using DigitalPersona AD Cleanup Wizard 127
- V**
- values 141
 Vendor Name
 published information property 26
 VPNAallowOTPOnly registry setting 243
 VPN-less access (setting) 91
- W**
- Web Administration Console 190
 Web Management Components 165
 Advanced Configuration 172
 Command line installation 175
 Configuration wizard 168
 Express Configuration 169
 installation 165
 prerequisites 165
 web.config file 188
 Weight set in Altus Server Locator DNS records (setting) 88
 Windows E-Mail Address 142
 Windows Logon events 125
- X**
- XenApp 248
 XenDesktop 248