HID DigitalPersona

LDS Administrator Guide

November 11, 2019

Table of Contents

POLICIES AND SETTINGS 118

PASSWORD RANDOMIZATION 140

SINGLE SIGN-ON 145

AUTHORIZATION MANAGER (AZMAN) 146

SECTION THREE: WEB MANAGEMENT

SECTION FOUR: APPENDICES

TROUBLESHOOTING 280

DIGITALPERSONA ADFS EXTENSION 289

DIGITALPERSONA NPS PLUGIN 294

CITRIX SUPPORT 311

FINGERPRINT ADJUDICATION AND DEDUPLICATION 314

Solution Overview 1

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

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.

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

The Challenge: Assured Identity

Identity assurance is a challenge in today's digital, mobile and highly connected world. Transactions no longer require a cash register, knowledge workers no longer need to be in the same facility to collaborate, and citizens do not have to stand in long lines at service centers to update passports, driver's licenses and national IDs. With such a mobile and digital society, how do organizations assure their authentication solution meets today's identity challenge?

DigitalPersona Identity Solutions

DigitalPersona offers biometric identity assurance solutions to meet today's authentication needs. Our solutions reflect a deep understanding of biometrics technology and the rapidly changing environments in which they are deployed.

For over 20 years, organizations have relied on DigitalPersona to provide secure multi-factor authentication and access management to PCs, Web and Windows applications and networks for users in a Microsoft Active Directory environment.

To address these same security and identity requirements for users outside of Active Directory, DigitalPersona offers the DigitalPersona LDS Solution as described below.

The DigitalPersona LDS Solution

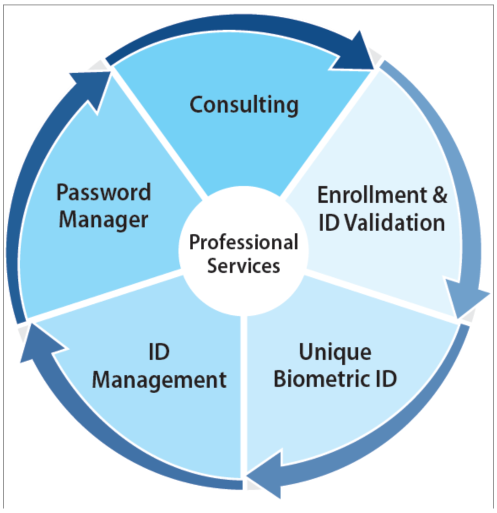
The DigitalPersona LDS Solution provides a modular framework that delivers identity assurance through a strong multi-factor authentication client and server in a Windows platform, leveraging fingerprint biometrics, PKI Smart cards, Contactless cards, Bluetooth devices and more. It enables Service Providers to establish and subsequently authenticate employees in real-time over their Intranet or VPN.

DigitalPersona LDS is an end-to-end, biometrics-focused solution platform that provides a non-repudiable identity from enrollment to authentication, customized to your environment.

Our HID Global consulting and professional services offerings allow you to customize the core features of DigitalPersona to meet your specific needs. Our Solutions team will guide you throughout the entire process from defining the policies and security rules to customizing the DigitalPersona platform, as well as initial deployment and training.

The DigitalPersona LDS Solution provides -

- Strong identity assurance with biometrics
- Composite authentication
- Flexible platform
- Custom integration and deployment via professional services
- Leveraging of existing IT infrastructure
- Highly scalable
- Standards compliant
- Support of Windows endpoints
- Offline enrollment with data synchronization



For further information on how HID DigitalPersona can help you solve your security needs, we have white papers, datasheets and case studies on our website at https://www.hidglobal.com/products/software/activid/digitalpersona-software.

Components

DigitalPersona LDS is a client-server product, comprised of the DigitalPersona Server components (including various administrative tools and utilities) and associated DigitalPersona clients: DigitalPersona LDS Workstation (including DigitalPersona Attended Enrollment) and DigitalPersona LDS Kiosk.

Server components

The DigitalPersona Server components fulfill four main purposes:

- They allows IT Administrators to manage security and authentication policies via Active Directory Group Policy Objects and other non-AD functions. For these purposes, the DigitalPersona Server 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, as well as various Snap-ins and server-based utilities.
- They provide centralized, server-side authentication of various types of credentials (e.g. Fingerprints, access cards, Bluetooth devices etc.). For these purposes, DigitalPersona runs authentication services within a 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 LDS also 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 LDS product are briefly described in the following table, and more fully described in the referenced pages.

Server component	Purpose	Page
DigitalPersona LDS Server	Provides centralized administration of DigitalPersona clients and enables strong authentication through various credentials and credential combinations	23
DigitalPersona LDS Administration Tools	Provides additional tools for administration of various DigitalPersona features and utilities including License Management and GPMC Extensions (with DigitalPersona Administrative Templates).	69, 92

Client components

The DigitalPersona LDS solution supports the following clients:

- *DigitalPersona LDS Workstation* - Enforces security and authentication policies on managed Windows computers while providing intuitive access to end-user features and functionality.
- *DigitalPersona 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 LDS Workstation, installed by choosing Custom during the DigitalPersona LDS Workstation installation.
- *DigitalPersona LDS Kiosk* - Provides DigitalPersona features for environments where users log on to a shared, common Windows account on a computer managed by a DigitalPersona LDS Server.

NOTE: DigitalPersona LDS 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 LDS Workstation

DigitalPersona LDS 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 LDS Server, or installed as a stand-alone product.

DigitalPersona Password Manager is an optional feature of the DigitalPersona Workstation client 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*.

DigitalPersona LDS Kiosk

DigitalPersona LDS 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 the Kiosk application uses a single Windows account, each DigitalPersona user logs in to Kiosk with their own DigitalPersona credentials, gaining separately controlled access to resources, applications and data.

DigitalPersona Password Manager is an optional feature of the DigitalPersona Kiosk client 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 component 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 DigitalPersona 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 in to websites.

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

- Password
- Fingerprint
- PKI Smart cards
- Contactless Writable cards
- Contactless ID cards (when enabled as a single (Primary) credential by GPO. See the *Allow the use of Contactless ID cards as a single (Primary) credential* setting on page *132)*.
- 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:

- Contactless ID card (except when enabled as Single (Primary) by GPO. See the *Allow the use of Contactless ID cards as a single (Primary) credential* setting on page *132)*.
- PIN
- Bluetooth device

An additional Password Recovery credential may be used solely for recovering access to a managed client computer when other credentials fail, are forgotten or are unavailable.

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 Server, but DigitalPersona Kiosk users will *not* be authenticated if there is no connection to the DigitalPersona 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 role of DigitalPersona Security Officer. See the chapter on *Attended Enrollment* in the *DigitalPersona Client Guide* for further details.

PKI Smart Cards

For Customer who would like to use PKI Smart Cards for DigitalPersona Windows Logon or to log in to services federated with the DigitalPersona Identity Provider (including DigitalPersona Web Administration Console and DigitalPersona Web Enrollment), the cards must be initialized outside of the DigitalPersona platform and have a Windows Logon Certificate provisioned on the card.

To use PKI Smart Cards, you must have a PKI infrastructure as part of your environment. Setting up this environment is beyond the scope of this guide, however, you may find the following link helpful.

https://blogs.msdn.microsoft.com/edutech/certificate-services/configure-server-2012-ca-for-smartcard-authentication/

Note that PKI card support in DigitalPersona 3.2 is not compatible with our previously used Smart Card solution in DigitalPersona 3.1 and earlier versions. Cards enrolled using DigitalPersona 3.1 cannot be used with a DigitalPersona 3.2 client, and cannot be used when a DigitalPersona 3.1 client communicates with a DigitalPersona 3.2 server, unless there is a Windows Logon Certificate on the card.

Adjudication and deduplication

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

Upgrading from previous versions

To upgrade from a previous version of this software, refer to the *DigitalPersona AD and LDS Upgrade Notes* available at: https://www.hidglobal.com/products/software/activid/digitalpersona-software.

Licensing model

The DigitalPersona features and functionality included with your product configuration may be included in your license, or may require additional licensing. See your authorized reseller or HID Global representative for further licensing details.

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.

The following Licensed product options are available for the HID DigitalPersona LDS solution.

DigitalPersona Premium Employee License - Permits the enrollment of user credentials, and subsequent use by a specified number of users. These users may be AD users or Non AD users.

DigitalPersona Customer Facing License - Permits the enrollment of user credentials and subsequent use by a specified number of Non AD users only.

Face authentication - Permits enrollment and use of the Face credential by licensed users.

*Behavioral keystroke*s - Permits enrollment and use of the Behavioral keystrokes feature for licensed users.

The specific DigitalPersona SKU and/or package you purchased may entitle you to licensing of one or more additional modules or components that are integrated with your DigitalPersona software. Some modules or optional components may need to be activated individually.

You should have received from HID Global or your authorized reseller all of the License IDs that are part of the solution you purchased. Contact the appropriate representative with any questions you may have.

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

https://www.hidglobal.com/products/software/activid/digitalpersona-software.

Licenses may be activated through Active Directory using the included License Activation Manager. For more information about DigitalPersona license activation, see *License Activation & Management* on page *76*.

System Requirements

Product/Component	Minimum Requirements
DigitalPersona Server	• Microsoft Windows Server 2016, 2012/2012 R2 or 2008 R2 • .NET Framework 4.5.1 or above • 12 MB disk space plus 5K per user
DigitalPersona LDS Workstation, DigitalPersona LDS Kiosk and DigitalPersona Attended Enrollment	• Operating Systems • 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 and 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. • 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. • 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*, Microsoft Edge**, Google Chrome or Mozilla Firefox browser required in order to create/use Password Manager *personal* logons or use *managed* logons***. See the readme.txt file for tested browser versions. • Microsoft Internet Explorer (only) in order to create *managed* logons*** using the optional Password Manager Admin Tool. See the reademe.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	• When all components are installed on the same machine as the DigitalPersona LDS Server, requirements are the same as the LDS Server plus Windows Web Server (IIS). • To access the Web Administration Console, Web Enrollment or the Application Portal from a device, either the DigitalPersona LDS 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.

Product/Component	Minimum Requirements
	- Windows - Internet Explorer (11+), Microsoft Edge**, Google Chrome or Firefox. - Mac and iOS - Safari - Android - Google Chrome
DigitalPersona Web Enrollment	- Operating Systems - 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.

** Microsoft Edge is only supported in versions based on the Chromium engine.

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

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

Remote access

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

- When DigitalPersona Workstation or DigitalPersona Kiosk are accessed remotely, the fingerprint reader attached to a local Workstation or Kiosk can be used to access all DigitalPersona Workstation or DigitalPersona Kiosk features on the remote computer. See *Redirect fingerprint data* on page *112.* Also see the NOTE below.
- When using DigitalPersona Workstation or DigitalPersona 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 311.

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 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.

Support Resources

- The Customer Support Knowledgebase provides answers to many frequently asked questions about our products.
- For software updates and patches, visit http://downloads.crossmatch.com/.
- 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.
- HID DigitalPersona documentation is available on our website at: https://www.hidglobal.com/documents.

Section One: Installation & Setup

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

Chapter Number and Title	Purpose	Page
2 - “DigitalPersona LDS Server Installation & Setup”	Requirements and procedures for installing and configuring Microsoft Active Directory Lightweight Directory Services (AD LDS) and DigitalPersona LDS Server.	23
3 - “Separate installations”	Requirements and procedures for installing additional and separate components compatible with the DigitalPersona LDS solution.	69

DigitalPersona LDS Server Installation & Setup 2

THIS CHAPTER PROVIDES INSTRUCTIONS FOR INSTALLING THE DIGITALPERSONA LDS SERVER AS WELL AS FOR COMPLETING THE TASKS NECESSARY TO PREPARE WINDOWS SERVER FOR THE INSTALLATION, INCLUDING ADDING THE AD LDS ROLE TO WINDOWS SERVER, SETTING UP AND CONFIGURING THE AD LDS SERVICE TO WORK WITH THE DIGITALPERSONA SOLUTION AND SETTING UP THE WINDOWS AUTHORIZATION MANAGER SNAP-IN.

Instructions for uninstalling DigitalPersona Server are also included at the end of this chapter, on page 68.

Deployment Overview

Here is a high-level overview of the steps required for initial deployment of DigitalPersona Server.

Procedure	Page
Add Server roles and features	24
Set up a unique instance of AD LDS	29
Configure the AD LDS service	34
Install DigitalPersona LDS Server	37
Activate the DigitalPersona Server License	45
Define the authorization store name	47
Configure additional servers (Recommended)	49
Command line Installation	65
Published information	66
Configuration for use with DigitalPersona LDS Kiosk (Optional)	66
Uninstalling DigitalPersona LDS Server	68

HID Global strongly recommends installing at least two instances of DigitalPersona LDS Server for load balancing and failover protection.

Detailed instructions for installation begin on the next page.

Upgrading from Previous Versions

To upgrade from a previous version of this software, refer to the *DigitalPersona AD and LDS Upgrade Notes* available at: https://www.hidglobal.com/products/software/activid/digitalpersona-software.

Note that DigitalPersona LDS licenses will need to be deleted and reapplied after the upgrade.

Compatibility

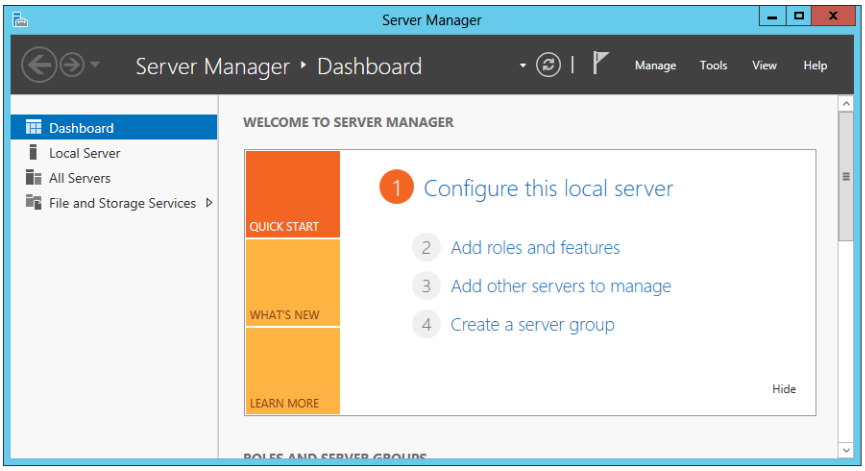
DigitalPersona Server is not compatible with any other DigitalPersona products except the associated components released with the current version of this software.

Add Server roles and features

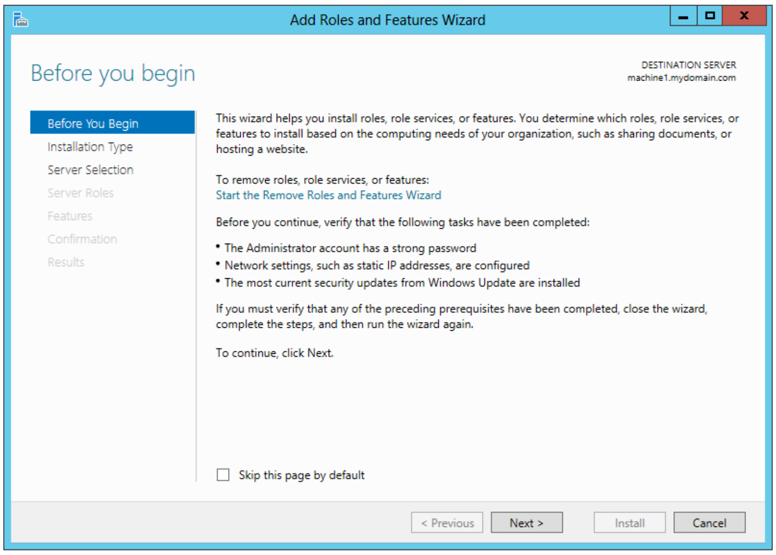
Before installing DigitalPersona LDS Server, there are a few roles and features that need to be added to the default installation of Windows Server.

To add the Windows Server roles and features necessary to support installation of DigitalPersona LDS Server

1. In Windows Server, open the Server Manager and select *Dashboard*.
2. Under *Configure this local server*, click *Add roles and features*.



3. On the *Before you begin* page of the Add Roles and Features Wizard, verify that you have completed the prerequisite tasks before continuing. Then click *Next*.



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

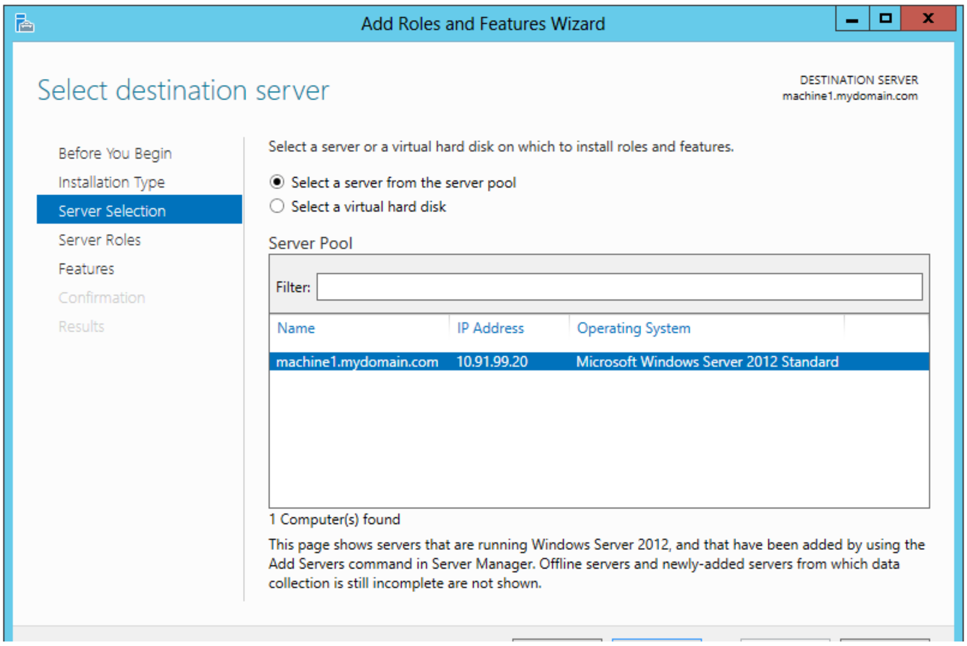
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Add Server roles and features

4. On the *Select installation type* page, select *Role-based or feature-based installation*. Then click *Next*.
5. On the *Select destination server* page, choose *Select a server from the server pool*. Then click *Next*.



Select destination server

DESTINATION SERVER
machine1.mydomain.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

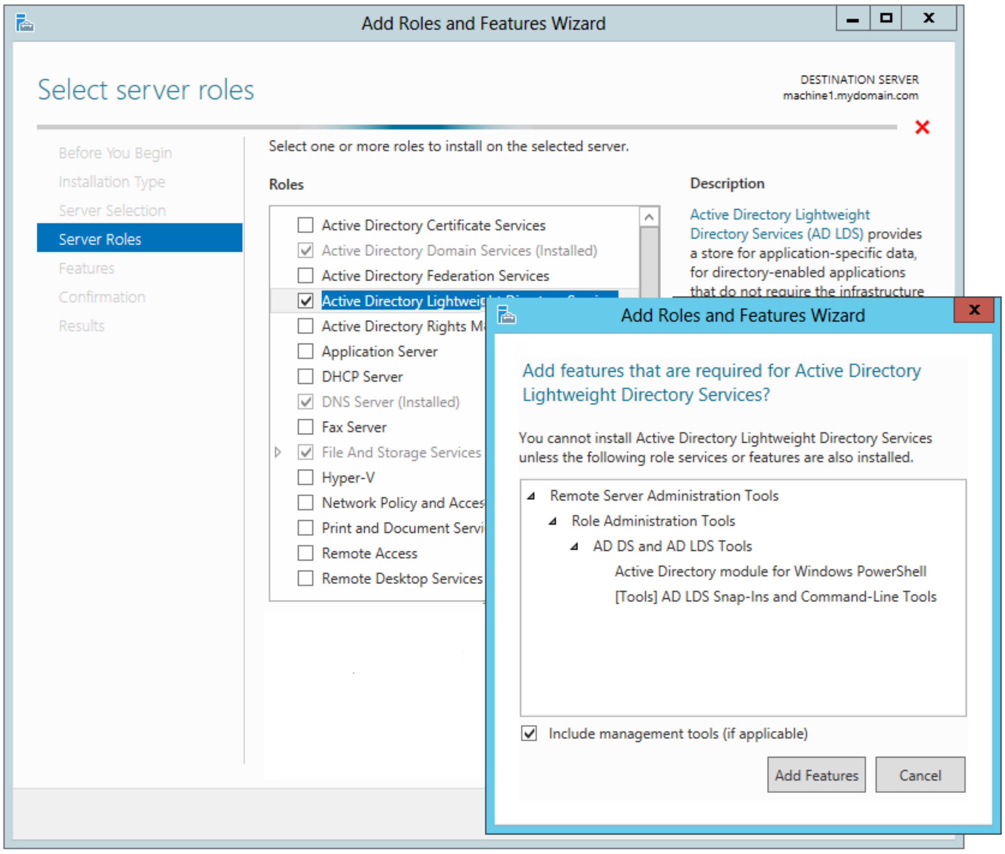
Filter:

Name	IP Address	Operating System
machine1.mydomain.com	10.91.99.20	Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

6. On the *Select server roles* page, in addition to the roles selected by default, ensure that the *Active Directory Lightweight Directory Services role* is included. Selecting this role will pop up a dialog for additional features required for AD LDS. Click *Add Features*.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
machine1.mydomain.com

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☑ Active Directory Lightweig
- ☐ Active Directory Rights M
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☑ File And Storage Services
- ☐ Hyper-V
- ☐ Network Policy and Acces
- ☐ Print and Document Servi
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure

Add Roles and Features Wizard

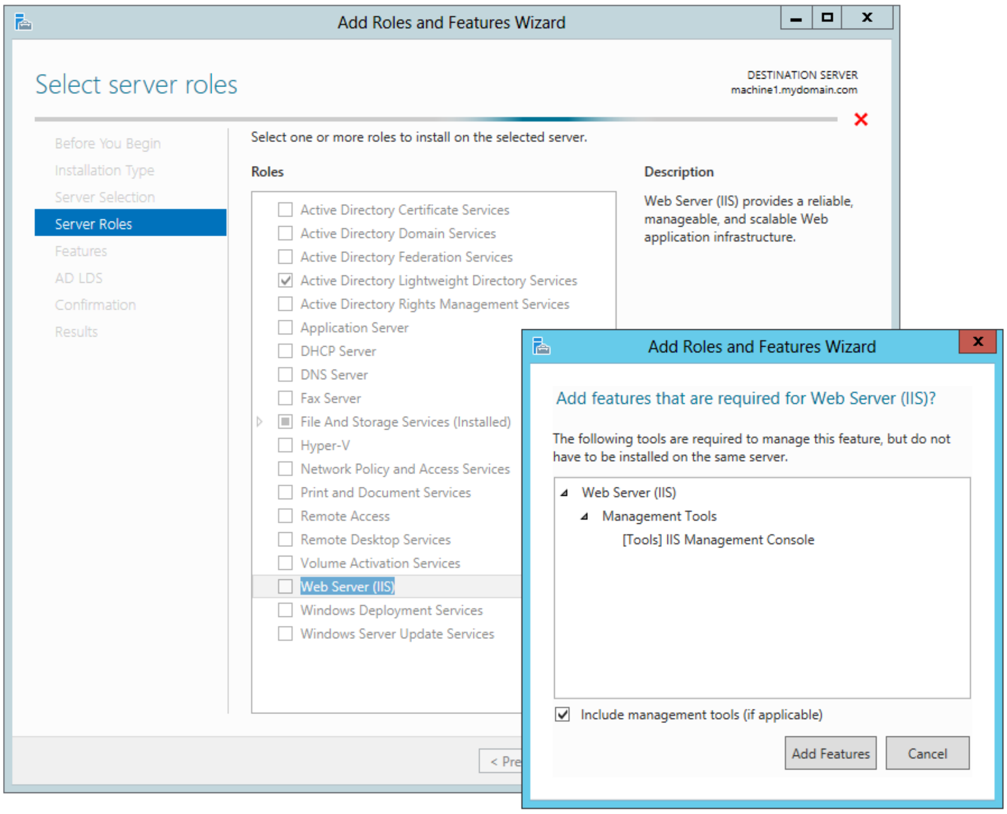
Add features that are required for Active Directory Lightweight Directory Services?

You cannot install Active Directory Lightweight Directory Services unless the following role services or features are also installed.

- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - [Tools] AD LDS Snap-Ins and Command-Line Tools

☑ Include management tools (if applicable)

If you are planning to also install the Web Administration Console, make sure to select Web Server (IIS) and any required management features. Then click *Next*.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
machine1.mydomain.com

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☑ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File And Storage Services (Installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Add Roles and Features Wizard

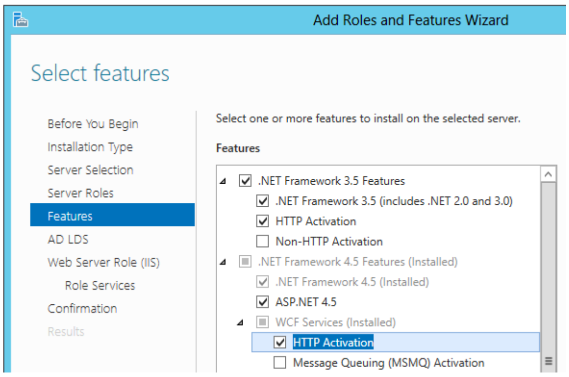
Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

Web Server (IIS)
    Management Tools
        [Tools] IIS Management Console

☑ Include management tools (if applicable)

7. On the Select features page, in addition to the features selected by default, ensure that those features listed below are selected. Click Add Features as requested.
   - .NET Framework 4.5 Features, including HTTP Activation
8. Then click *Next*.
9. The following page simply explains how to create an AD LDS instance, by using the AD LDS Setup Wizard, and how to remove the AD LDS role through the Windows Control Panel. Click *Next*.



Add Roles and Features Wizard

Select features

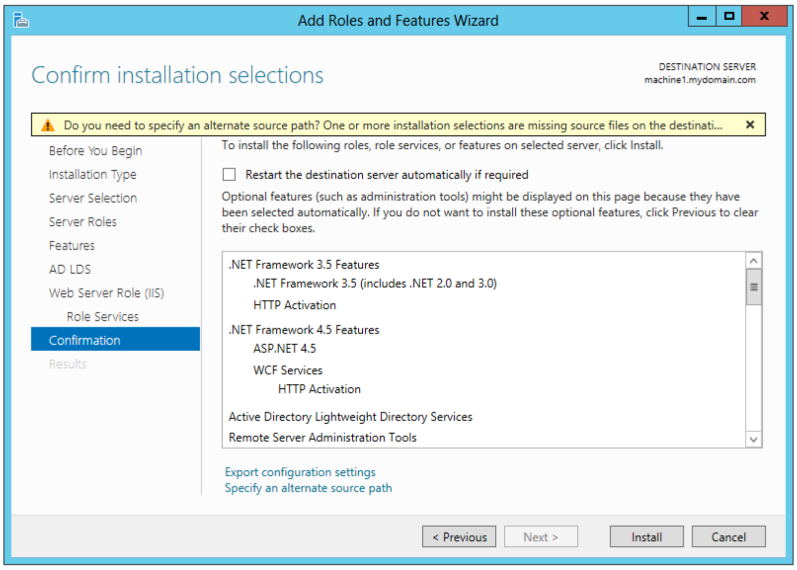
Select one or more features to install on the selected server.

Features

- ☑ .NET Framework 3.5 Features
  - ☑ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - ☑ HTTP Activation
  - ☐ Non-HTTP Activation
- ▣ .NET Framework 4.5 Features (Installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5
  - ▣ WCF Services (Installed)
    - ☑ HTTP Activation
    - ☐ Message Queuing (MSMQ) Activation

10. If installing the Web Server Role (IIS)
    - Click Next on the Web Server Role (IIS) page, which explains IIS features.

11. The *Confirm installation Selections* page displays.



Confirm installation selections

DESTINATION SERVER
machine1.mydomain.com

⚠ Do you need to specify an alternate source path? One or more installation selections are missing source files on the destinati... ✕

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

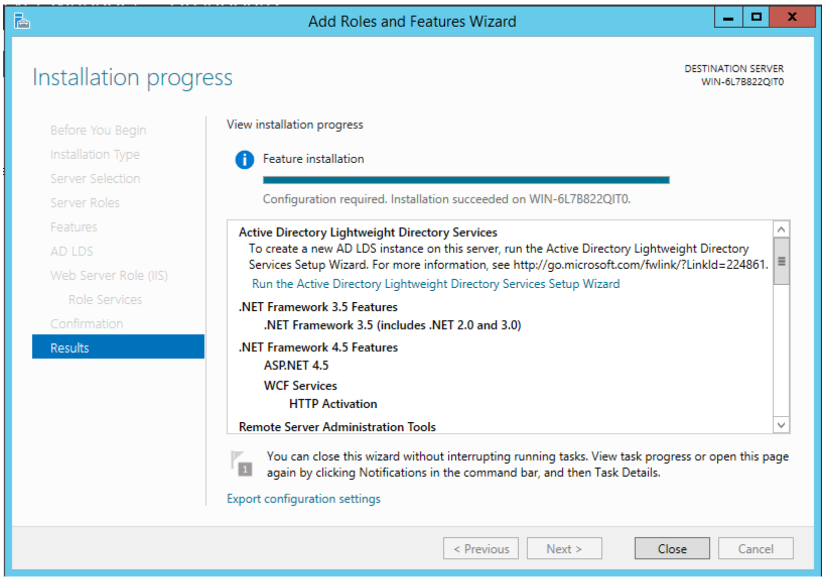
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)
    HTTP Activation
.NET Framework 4.5 Features
    ASP.NET 4.5
    WCF Services
        HTTP Activation
Active Directory Lightweight Directory Services
Remote Server Administration Tools

Export configuration settings
Specify an alternate source path

12. Click *Install*.

13. The *Installation Progress* page displays a bar indicating the approximate progress of the installation process. Note that you can close the wizard (by clicking the Close (X) button) without interrupting the installation, and open it again to view progress by clicking *Notifications* and then *Task Details* in the Server Manager Dashboard Command Bar.



Installation progress

DESTINATION SERVER
WIN-6L7B822QIT0

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-6L7B822QIT0.

Active Directory Lightweight Directory Services
  To create a new AD LDS instance on this server, run the Active Directory Lightweight Directory Services Setup Wizard. For more information, see http://go.microsoft.com/fwlink/?LinkId=224861.
  Run the Active Directory Lightweight Directory Services Setup Wizard
.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.5 Features
    ASP.NET 4.5
    WCF Services
        HTTP Activation
Remote Server Administration Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

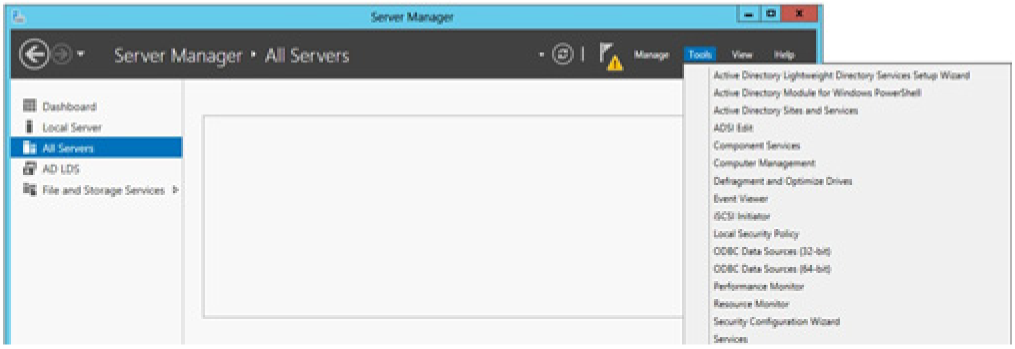
14. Upon completion of the installation, you can choose to run the Active Directory Lightweight Directory Services Setup Wizard from the link provided, or close the wizard and follow the instructions in the next section to run the wizard. An automatic refresh will also be performed upon closing the Add Roles and Features Wizard.

Set up a unique instance of AD LDS

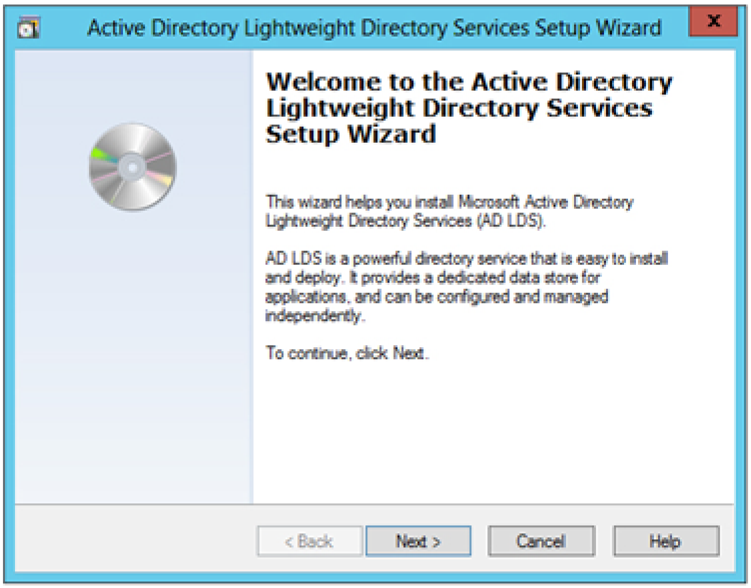
Once the LDS *feature* has been installed, you will use the Active Directory Lightweight Directory Services Setup Wizard to install and set up a unique *instance* of AD LDS to be used as a data store for DigitalPersona LDS. Note that the computer must be a member of a domain before beginning this wizard or LDS will be run a system service account and the instance will not be able to replicate data with AD LDS instances on other computers.

To set up LDS

1. In the Server Manager Dashboard Command Bar, select *Tools*. Then select *Active Directory Lightweight Directory Services Setup Wizard*.


Server Manager
Server Manager • All Servers
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD LDS
File and Storage Services
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Event Viewer
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services

2. The Active Directory Lightweight Directory Services Setup Wizard displays. Click *Next*.


Active Directory Lightweight Directory Services Setup Wizard
< Back
Next >
Cancel
Help

Welcome to the Active Directory Lightweight Directory Services Setup Wizard

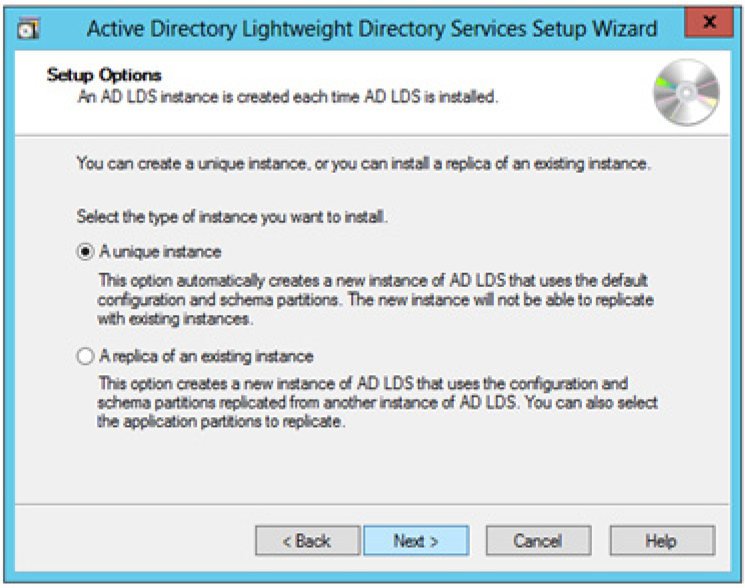
This wizard helps you install Microsoft Active Directory Lightweight Directory Services (AD LDS).

AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.

To continue, click Next.

3. On the *Setup options* page, select whether to create a unique instance of AD LDS or to create a replica of an existing instance. Then click *Next*.

   Select *A unique instance* unless you want to replicate a previously created instance for load balancing or failover. Click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

Setup Options

An AD LDS instance is created each time AD LDS is installed.

You can create a unique instance, or you can install a replica of an existing instance.

Select the type of instance you want to install.

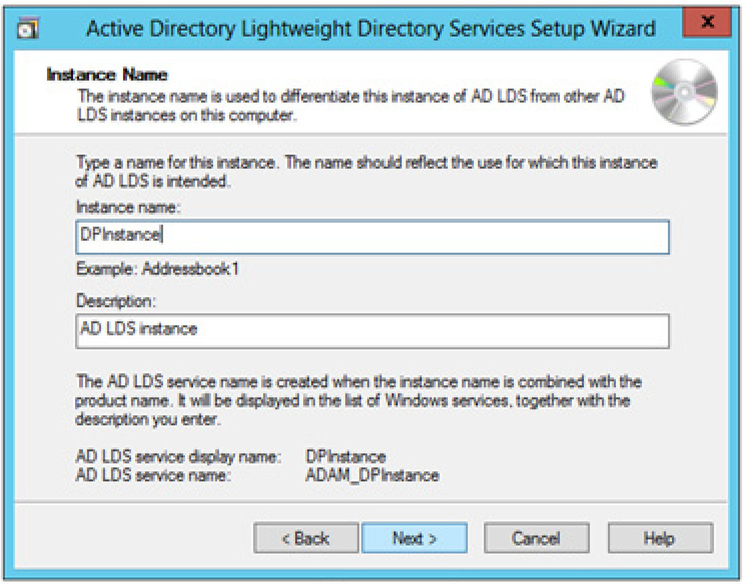
● A unique instance

This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.

○ A replica of an existing instance

This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.

4. On the *Instance name* page, enter a unique name that will be used to differentiate this instance of AD LDS from other AD LDS instances that may exist on this computer. Click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

Instance Name

The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.

Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.

Instance name: DPInstance

Example: Addressbook1

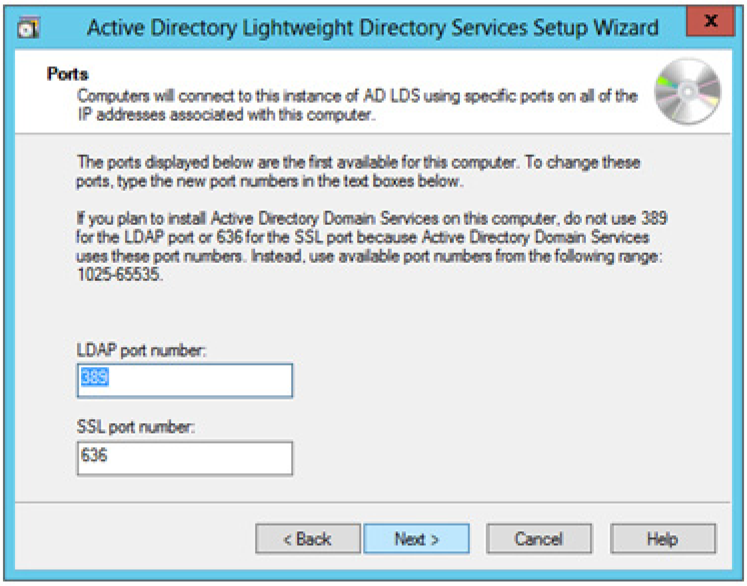
Description: AD LDS instance

The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.

AD LDS service display name: DPInstance
AD LDS service name: ADAM_DPInstance

Set up a unique instance of AD LDS

5. On the *Ports* page, in most cases, use the default ports provided. On a domain controller, these will generally be 50000 and 50001. Otherwise, the default ports will usually be 389 and 636. Click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

Ports

Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.

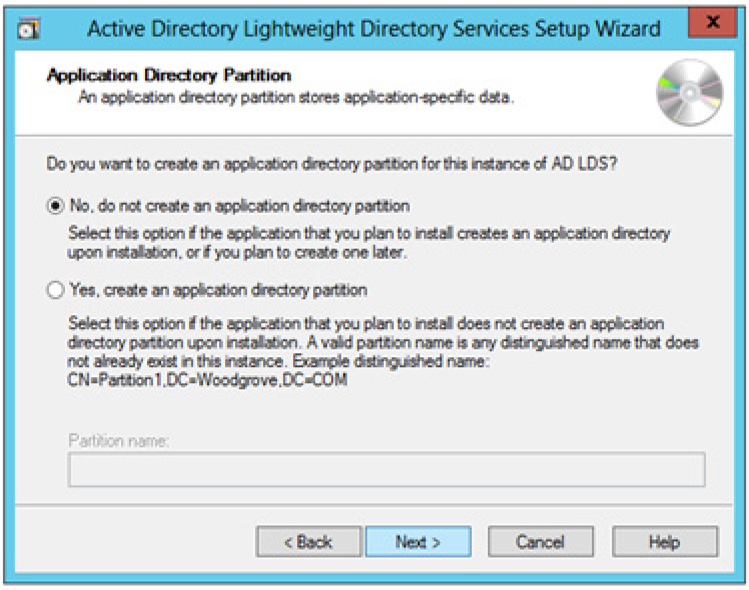
The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number: 389

SSL port number: 636

6. On the *Application Directory Partitions* page, you should accept the default to *not* create an application directory partition. Click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

Application Directory Partition

An application directory partition stores application-specific data.

Do you want to create an application directory partition for this instance of AD LDS?

● No, do not create an application directory partition

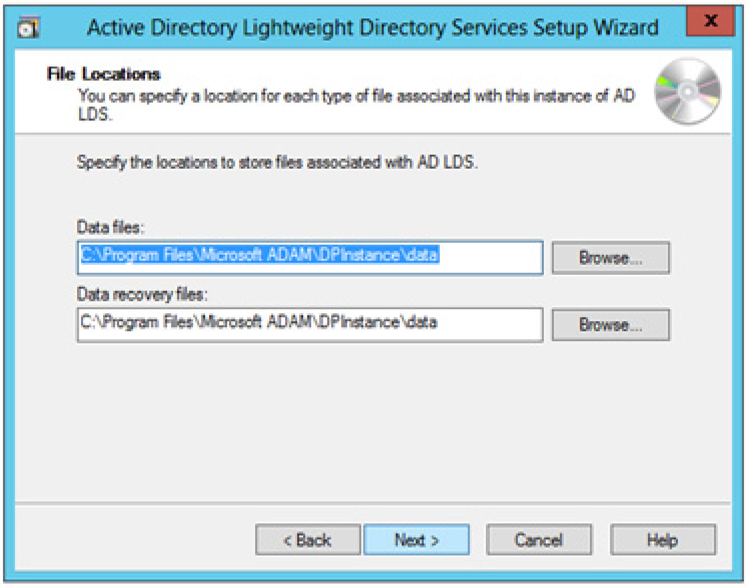
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.

○ Yes, create an application directory partition

Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM

Partition name:

7. On the *File location* page, accept the default. Click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

File Locations

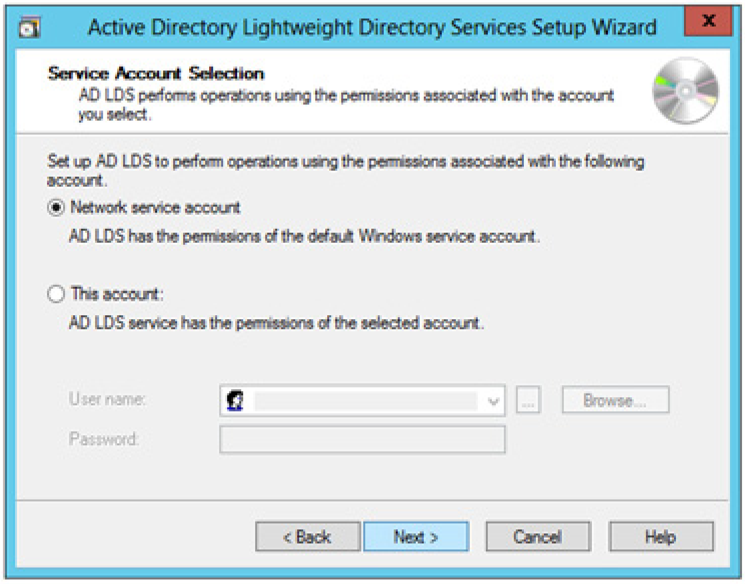
You can specify a location for each type of file associated with this instance of AD LDS.

Specify the locations to store files associated with AD LDS.

Data files:
C:\Program Files\Microsoft ADAM\DPInstance\data

Data recovery files:
C:\Program Files\Microsoft ADAM\DPInstance\data

8. On the *Service account selection* page, accept the default to use the network service account to perform operations. Click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

Service Account Selection

AD LDS performs operations using the permissions associated with the account you select.

Set up AD LDS to perform operations using the permissions associated with the following account.

● Network service account

AD LDS has the permissions of the default Windows service account.

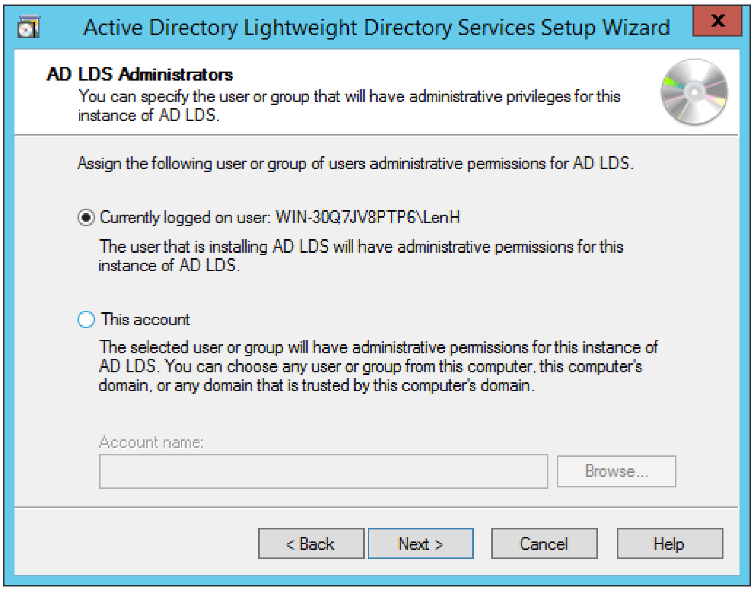
○ This account:

AD LDS service has the permissions of the selected account.

User name:

Password:

9. On the *AD LDS Administrators* page, specify the user or group that will have administrative privileges for this instance of AD LDS. In most cases, accept the default that the currently logged on user, i.e. the one performing this installation, will have administrative permissions. Click *Next*.


Active Directory Lightweight Directory Services Setup Wizard
X

AD LDS Administrators

You can specify the user or group that will have administrative privileges for this instance of AD LDS.

Assign the following user or group of users administrative permissions for AD LDS.

● Currently logged on user: WIN-30Q7JV8PTP6\LenH

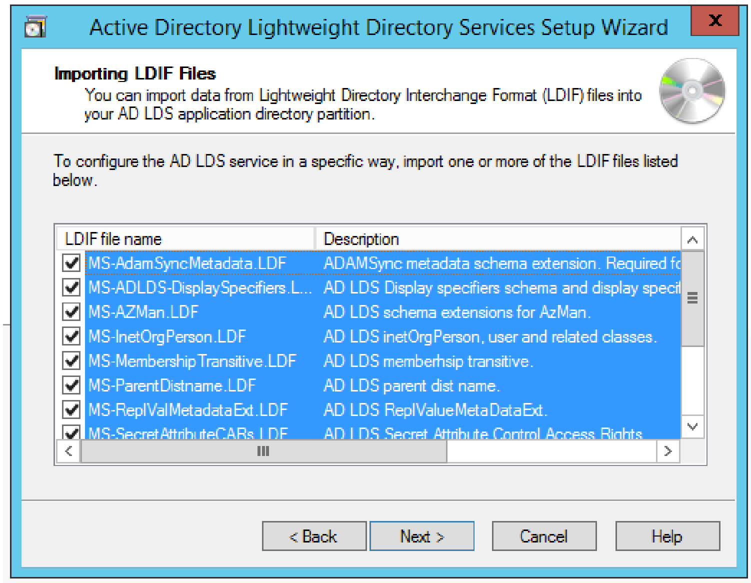
The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.

○ This account

The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.

Account name:

10. On the *Importing LDIF Files* page, select all of the listed options by pressing Ctrl+A and then clicking any selection box. Then click *Next*.


Active Directory Lightweight Directory Services Setup Wizard
X

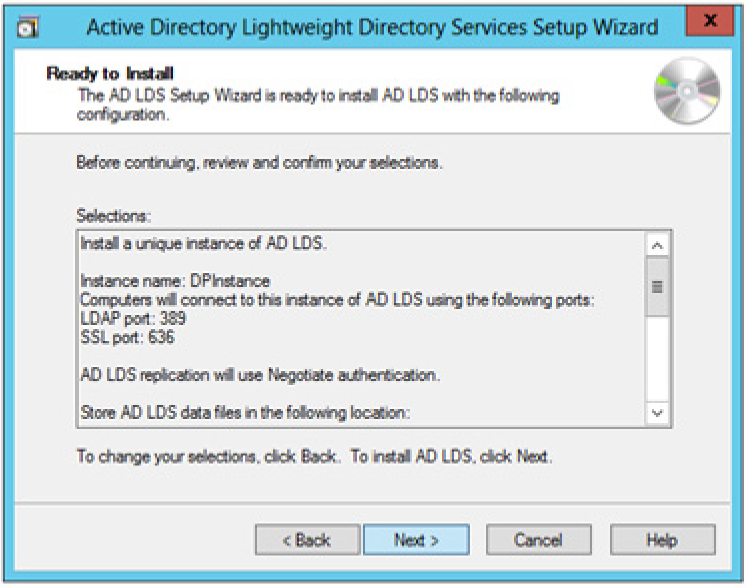
Importing LDIF Files

You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.

To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.

LDIF file name	Description
☑ MS-AdamSyncMetadata.LDF	ADAMSync metadata schema extension. Required fo
☑ MS-ADLDS-DisplaySpecifiers.L...	AD LDS Display specifiers schema and display specif
☑ MS-AZMan.LDF	AD LDS schema extensions for AzMan.
☑ MS-InetOrgPerson.LDF	AD LDS inetOrgPerson, user and related classes.
☑ MS-MembershipTransitive.LDF	AD LDS memberhsip transitive.
☑ MS-ParentDistname.LDF	AD LDS parent dist name.
☑ MS-ReplValMetadataExt.LDF	AD LDS ReplValueMetaDataExt.
☑ MS-SecretAttributeCARs.LDF	AD LDS Secret Attribute Control Access Rights

11. On the *Ready to install* page, review and confirm your selections. Click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

Ready to Install

The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.

Before continuing, review and confirm your selections.

Selections:

Install a unique instance of AD LDS.

Instance name: DPInstance
Computers will connect to this instance of AD LDS using the following ports:
LDAP port: 389
SSL port: 636

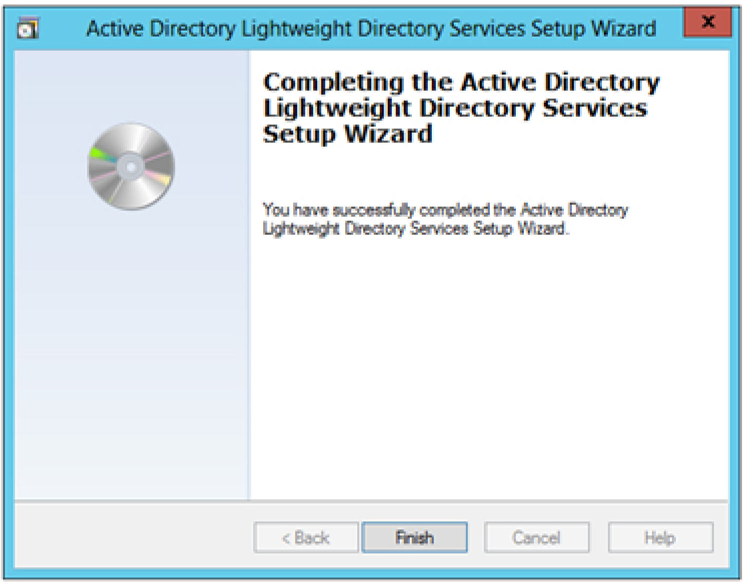
AD LDS replication will use Negotiate authentication.

Store AD LDS data files in the following location:

To change your selections, click Back. To install AD LDS, click Next.

12. The *Installing AD LDS* page indicates the progress as the unique instance of AD LDS is installed.

13. When the installation is completed, the final page of the wizard displays. Click *Finish* to close the setup wizard,



Active Directory Lightweight Directory Services Setup Wizard

Completing the Active Directory Lightweight Directory Services Setup Wizard

You have successfully completed the Active Directory Lightweight Directory Services Setup Wizard.

and *Close* to close the Add Roles and Features Wizard, if it has not already been closed.

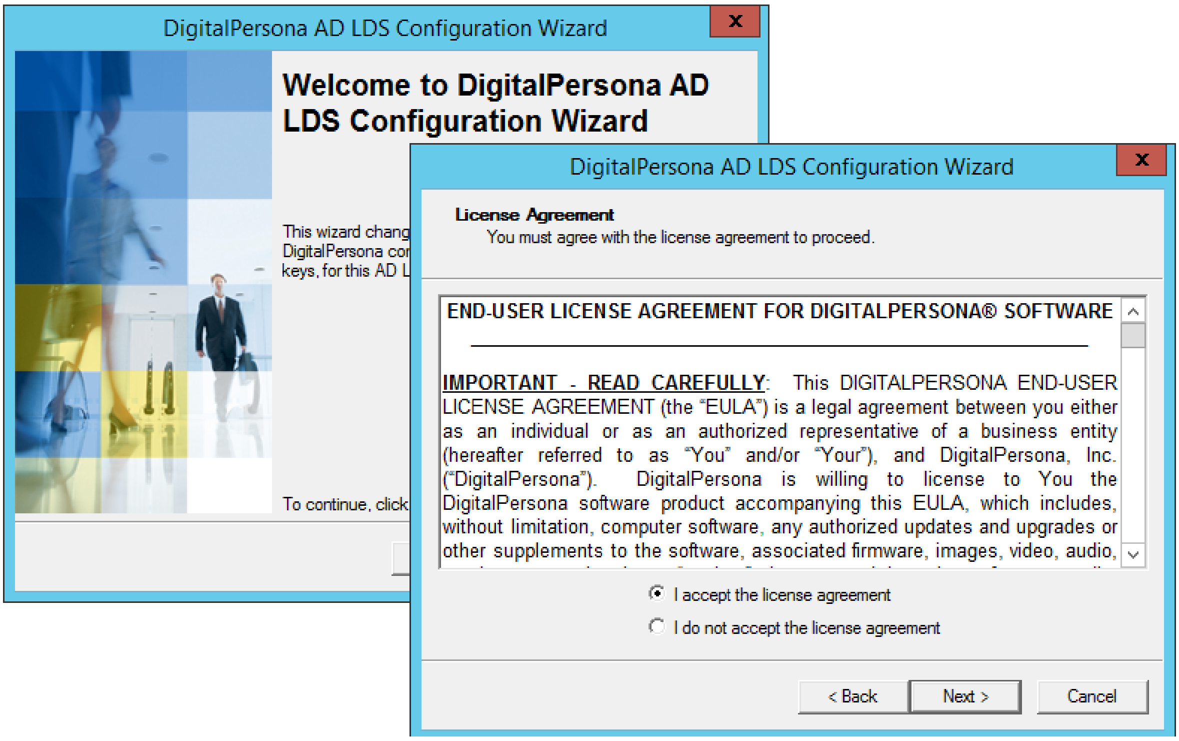
Configure the AD LDS service

Configure the Active Directory Lightweight Directory Service by running the DigitalPersona AD LDS Configuration Wizard. The wizard extends the instance's default AD LDS schema for use by DigitalPersona and creates necessary DigitalPersona configuration data including cryptographic keys. The wizard must be run by the user (or member of the group) that was defined as the AD LDS Administrator during the AD LDS installation (see step 9 on page 33).

To configure the DigitalPersona AD LDS Server instance

Set up a unique instance of AD LDS

1. Launch the *DigitalPersona AD LDS Configuration Wizard* by running *DPADLDSConfig.exe*, located in the product package at: *..\Server\DigitalPersona|LDS Server\Configuration Wizard*.
2. The wizard's *Welcome* page displays. Click *Next*.



DigitalPersona AD LDS Configuration Wizard

Welcome to DigitalPersona AD LDS Configuration Wizard

This wizard chang
DigitalPersona cor
keys, for this AD L

To continue, click

DigitalPersona AD LDS Configuration Wizard

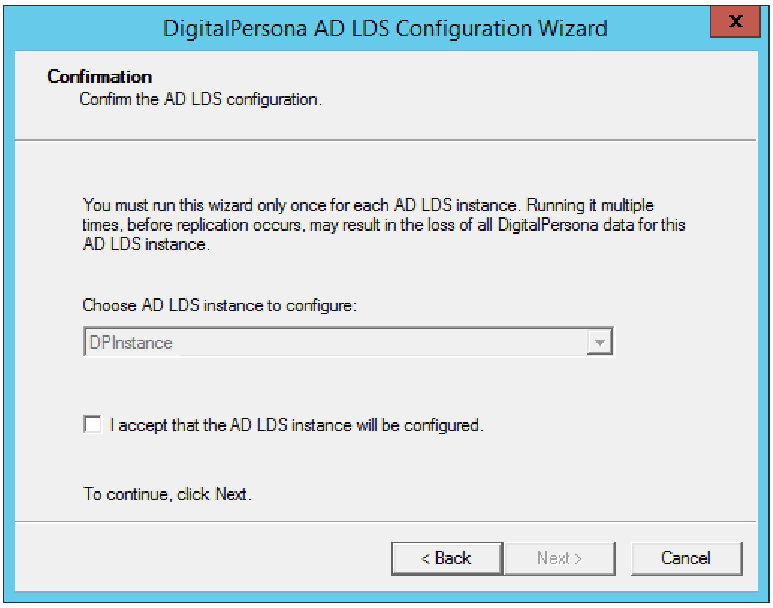
License Agreement
You must agree with the license agreement to proceed.

END-USER LICENSE AGREEMENT FOR DIGITALPERSONA® SOFTWARE

IMPORTANT - READ CAREFULLY: This DIGITALPERSONA END-USER LICENSE AGREEMENT (the "EULA") is a legal agreement between you either as an individual or as an authorized representative of a business entity (hereafter referred to as "You" and/or "Your"), and DigitalPersona, Inc. ("DigitalPersona"). DigitalPersona is willing to license to You the DigitalPersona software product accompanying this EULA, which includes, without limitation, computer software, any authorized updates and upgrades or other supplements to the software, associated firmware, images, video, audio,

● I accept the license agreement
○ I do not accept the license agreement

3. On the *License Agreement* page, select *I accept the license agreement*. Click *Next*.



DigitalPersona AD LDS Configuration Wizard

Confirmation
Confirm the AD LDS configuration.

You must run this wizard only once for each AD LDS instance. Running it multiple times, before replication occurs, may result in the loss of all DigitalPersona data for this AD LDS instance.

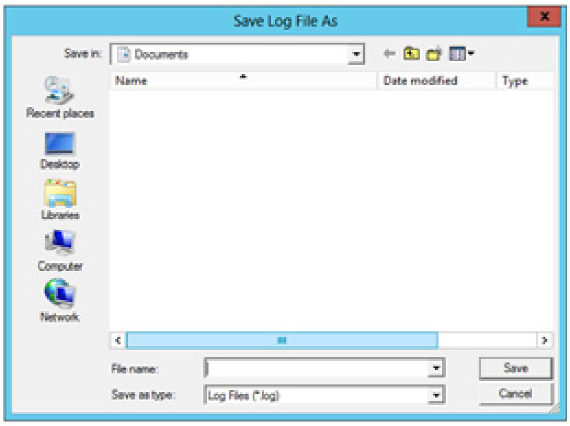
Choose AD LDS instance to configure:
DPInstance

□ I accept that the AD LDS instance will be configured.

To continue, click Next.

4. On the *Confirmation* page, confirm that the correct AD LDS instance appears in the *Choose AD LDS instance to configure* field and check the *I accept that this AD LDS instance will be configured* checkbox. If there is only one AD LDS instance on the computer, the instance will be automatically selected, and grayed out, since there is no other instance available for selection.

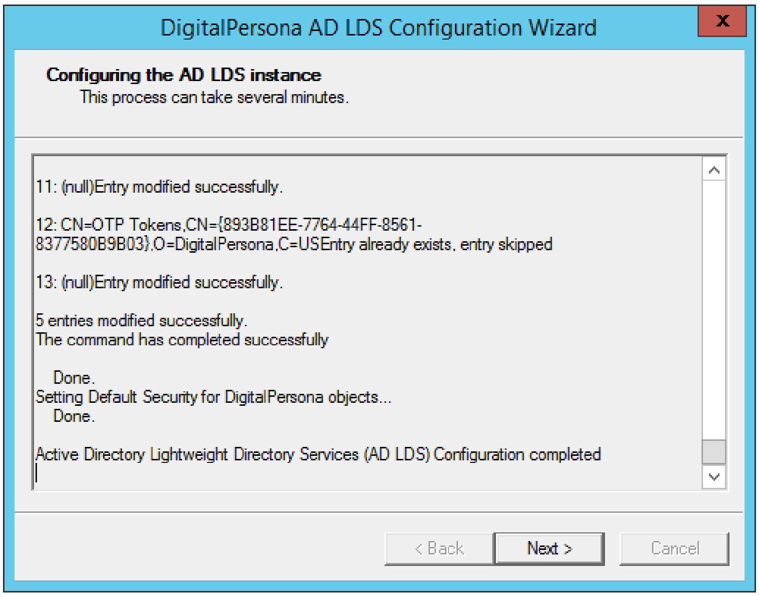
5. In the *Save Log File As* window, select a location where you want DigitalPersona LDS log files saved to, and enter a name for the file.



Save in: Documents

Save as type: Log Files (*.log)

6. The *Configuring the AD LDS instance* page displays relevant information as the configuration progresses, as well as any errors that occur during the process.

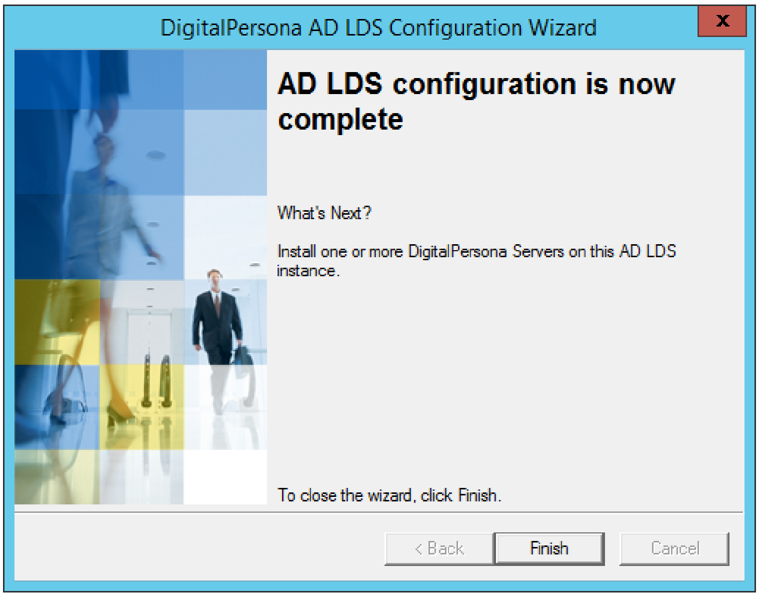


Configuring the AD LDS instance

This process can take several minutes.

```
11: (null)Entry modified successfully.

12: CN=OTP Tokens,CN={893B81EE-7764-44FF-8561-
8377580B9B03},O=DigitalPersona,C=USEntry already exists, entry skipped

13: (null)Entry modified successfully.

5 entries modified successfully.
The command has completed successfully

   Done.
Setting Default Security for DigitalPersona objects...
   Done.

Active Directory Lightweight Directory Services (AD LDS) Configuration completed
```

7. The final page will indicate a successful installation or provide help in troubleshooting any issues that may arise.



AD LDS configuration is now complete

What's Next?

Install one or more DigitalPersona Servers on this AD LDS instance.

To close the wizard, click Finish.

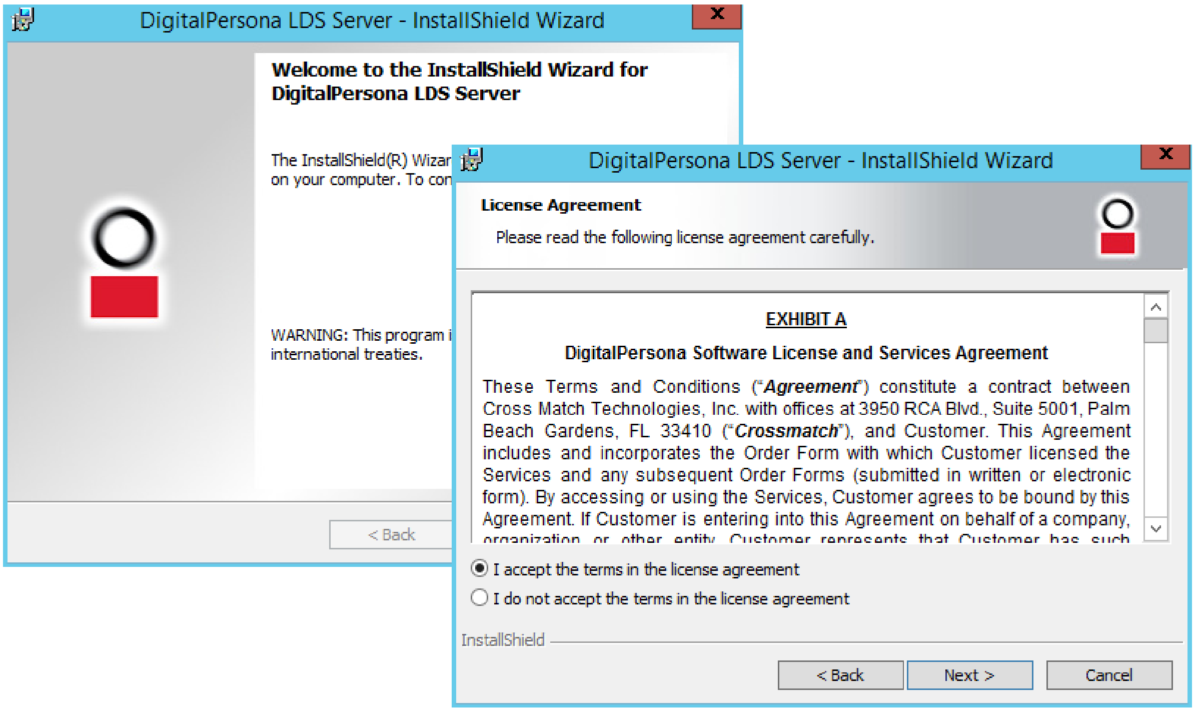
Install DigitalPersona LDS Server

Before installing DigitalPersona Server, ensure that the computer meets the minimum requirements listed on page 19, and that the Windows AD LDS feature has been added to the Windows Server and properly configured.

To install the DigitalPersona LDS Server

1. Launch the *DigitalPersona LDS Server - InstallShield Wizard* by running *Setup.exe*, located in the *..\Server\ DigitalPersona LDS Server* folder in the product package.
2. The wizard's *Welcome* page displays. Click *Next*.

Read the *License Agreement* page. If you agree with the stated terms, select *I accept the license agreement*. and click *Next*.



DigitalPersona LDS Server - InstallShield Wizard

Welcome to the InstallShield Wizard for DigitalPersona LDS Server

The InstallShield(R) Wizar
on your computer. To con

WARNING: This program i
international treaties.

< Back

DigitalPersona LDS Server - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

EXHIBIT A

DigitalPersona Software License and Services Agreement

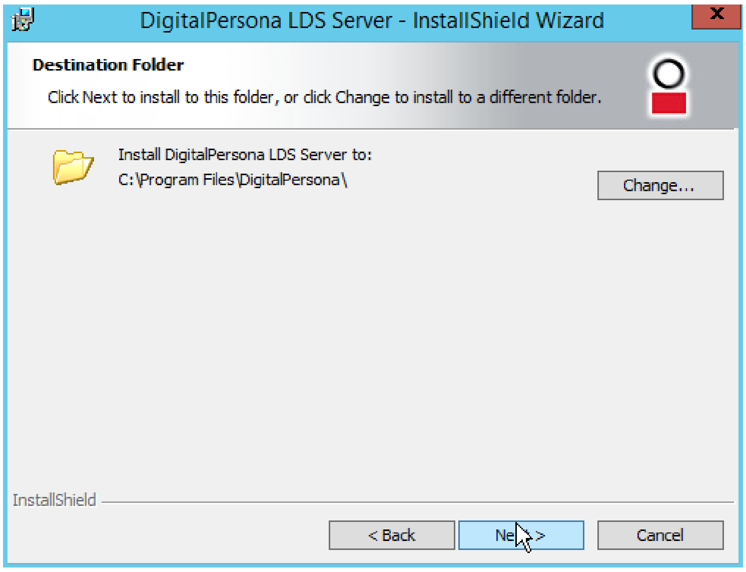
These Terms and Conditions ("*Agreement*") constitute a contract between Cross Match Technologies, Inc. with offices at 3950 RCA Blvd., Suite 5001, Palm Beach Gardens, FL 33410 ("*Crossmatch*"), and Customer. This Agreement includes and incorporates the Order Form with which Customer licensed the Services and any subsequent Order Forms (submitted in written or electronic form). By accessing or using the Services, Customer agrees to be bound by this Agreement. If Customer is entering into this Agreement on behalf of a company, organization or other entity, Customer represents that Customer has such

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

InstallShield

3. On the *Destination Folder* page, accept the default install destination folder, or click *Change* to install to a different folder. Click *Next*.



DigitalPersona LDS Server - InstallShield Wizard

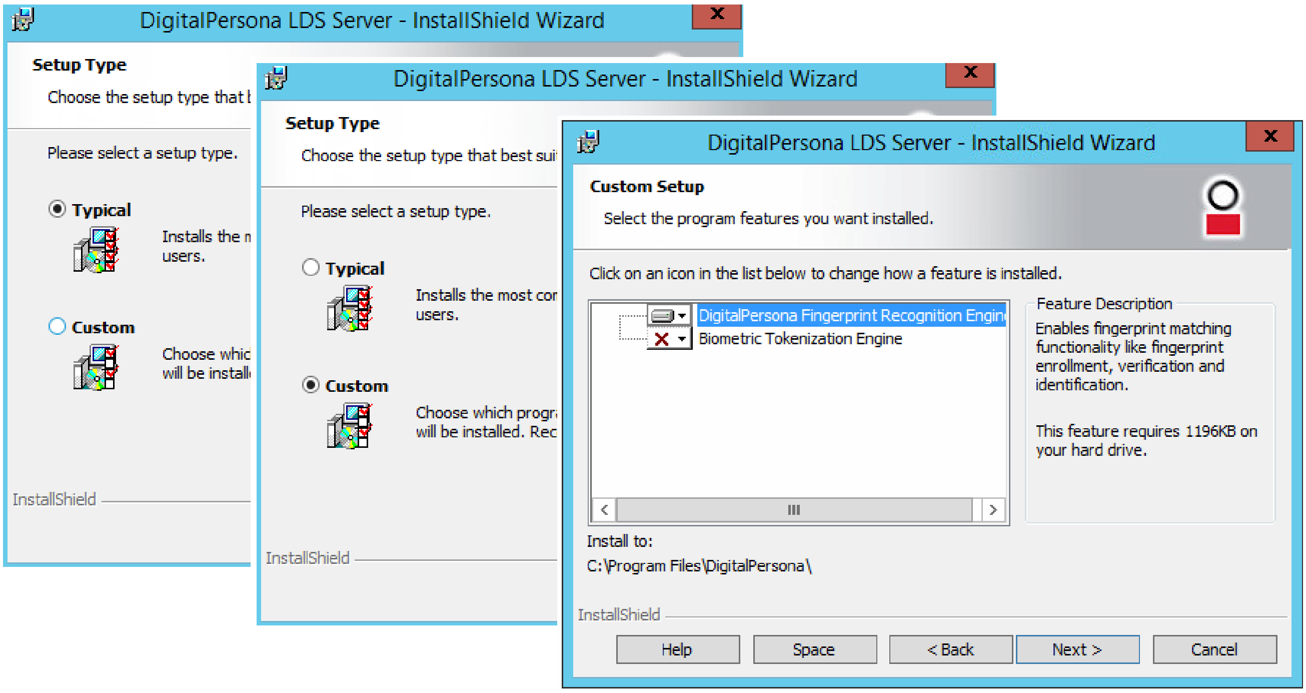
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install DigitalPersona LDS Server to:
C:\Program Files\DigitalPersona\

InstallShield

4. On the *Setup type* page, choose one the following options to indicate the type of installation you want to perform.



DigitalPersona LDS Server - InstallShield Wizard

Setup Type

Choose the setup type that b

Please select a setup type.

● **Typical**

Installs the m
users.

○ **Custom**

Choose whic
will be install

InstallShield

DigitalPersona LDS Server - InstallShield Wizard

Setup Type

Choose the setup type that best sui

Please select a setup type.

○ **Typical**

Installs the most cor
users.

● **Custom**

Choose which progr
will be installed. Rec

InstallShield

DigitalPersona LDS Server - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

DigitalPersona Fingerprint Recognition Engin
Biometric Tokenization Engine

Feature Description

Enables fingerprint matching functionality like fingerprint enrollment, verification and identification.

This feature requires 1196KB on your hard drive.

Install to:

C:\Program Files\DigitalPersona\

InstallShield

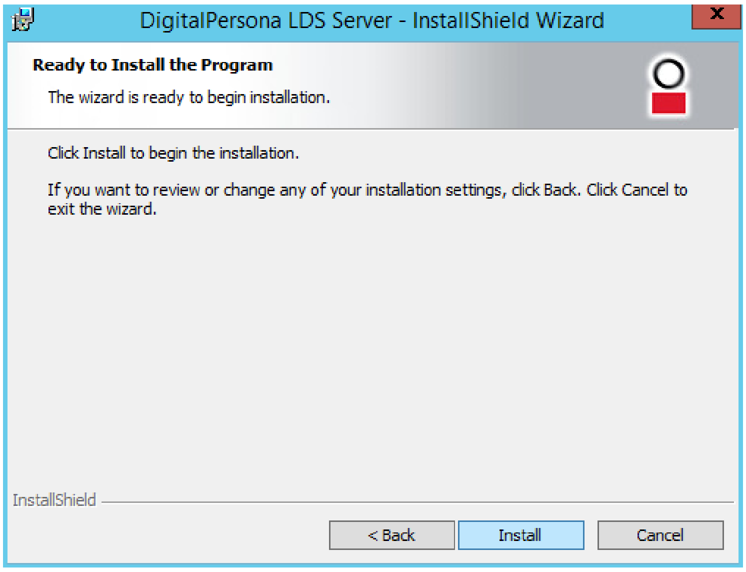
- **Typical -** Installs the LDS Server and the DigitalPersona Fingerprint Recognition Engine.
- **Custom -** Allows selection of which features to install.

  Fingerprint Recognition Engine - 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 - 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.

5. On the *Ready to install* page, click *Install*.



DigitalPersona LDS Server - InstallShield Wizard

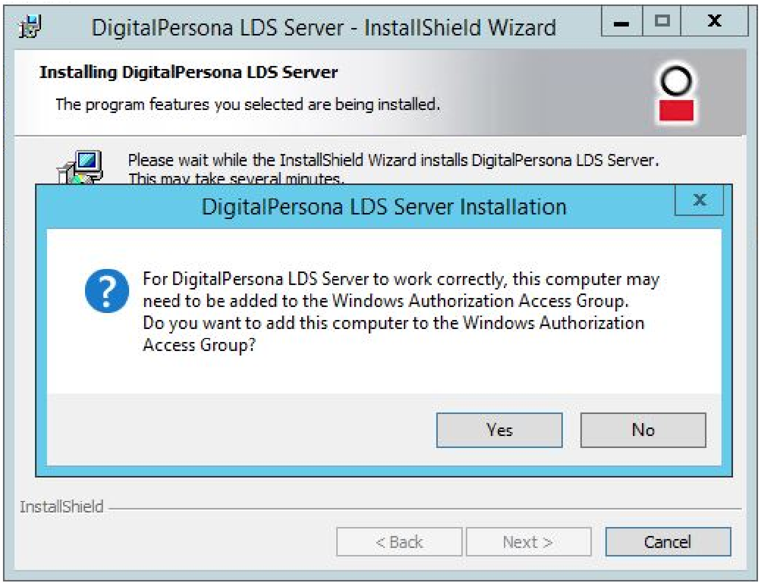
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

6. The *Installing DigitalPersona LDS Server* page displays the progress of the installation.



DigitalPersona LDS Server - InstallShield Wizard

Installing DigitalPersona LDS Server

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs DigitalPersona LDS Server. This may take several minutes.

DigitalPersona LDS Server Installation

For DigitalPersona LDS Server to work correctly, this computer may need to be added to the Windows Authorization Access Group. Do you want to add this computer to the Windows Authorization Access Group?

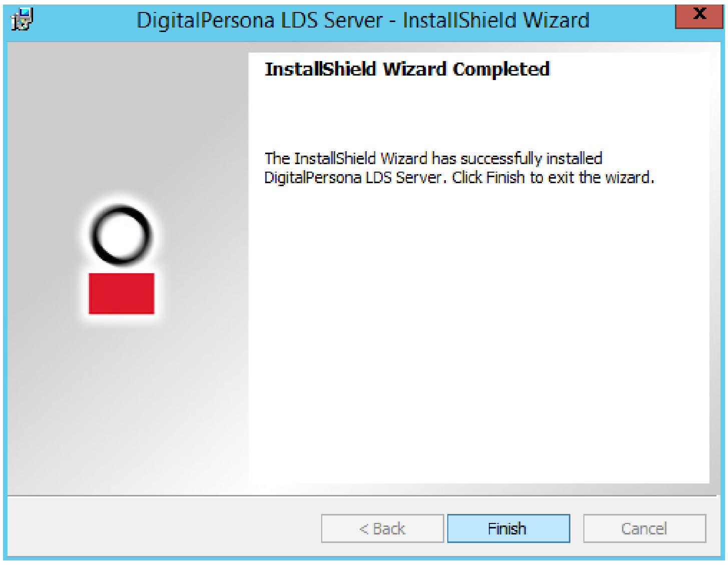
Windows Authorization Access Group - In order for DigitalPersona Server to provide access control, it requires access to authorization information on user account objects.

By default, members of the "Pre-Windows 2000 Compatible Access" group have access to this data. If the “Permissions compatible with pre-Windows 2000 servers" option was selected during the DCPromo process when the domain was created, “Everyone" would have been added to the "Pre-Windows 2000 Compatible Access" group and DigitalPersona Server would be able to access the necessary user authorization information in Active Directory.

However, if this option was not selected, DigitalPersona Server would not have access to the user authorization information and as result, user enrollment will fail with an "Access Denied" error.

Therefore, the machine account where DigitalPersona Server is running must be added to the Windows Authorization Access Group.

7. Upon completion of the wizard, the *InstallShield Wizard Completed* page displays. Click *Finish* to close the wizard.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DigitalPersona LDS Server. Click Finish to exit the wizard.

DigitalPersona LDS Administration Tools

The DigitalPersona LDS Administration Tools are part of a separate installation package included in the DigitalPersona product package. It includes the *User Query Snap-in* (used to query user data) and the *GPMC/GPOE Extensions* (used to manage DigitalPersona policies and settings), and can also be used to manage DigitalPersona LDS Licenses.

Note that Domain Admin permissions are required to manage DigitalPersona licenses, unless you add the Manage Licenses permission to additional users in the Microsoft Authorization Manager (AzMan). See page 148 for details.

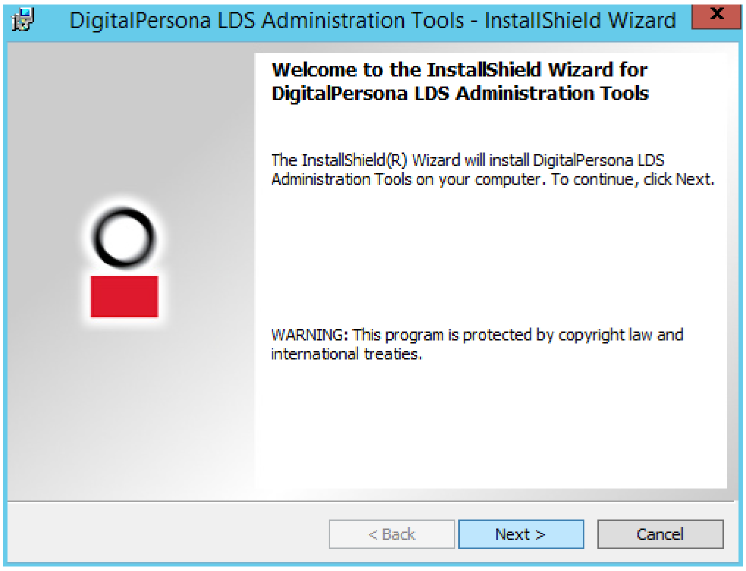
If you will be managing your DigitalPersona LDS Server directly from the computer it is installed on, you will want to install the DigitalPersona Administration Tools on that computer. However, you can also manage the DigitalPersona LDS Server from another domain joined computer in which case you would install the Administration Tools on that computer. (See page 92 and following for full descriptions of the tools.) It must be installed on a machine that also has either the DigitalPersona LDS Server, or DigitalPersona LDS Workstation.

The tools may be installed on a single workstation for centralized administration of DigitalPersona; 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.

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

Installation

1. Locate and launch the *setup.exe* located in the ..*\Server\DigitalPersona LDS Administration Tools* folder of the product package. The *DigitalPersona LDS Administration Tools Wizard* displays.



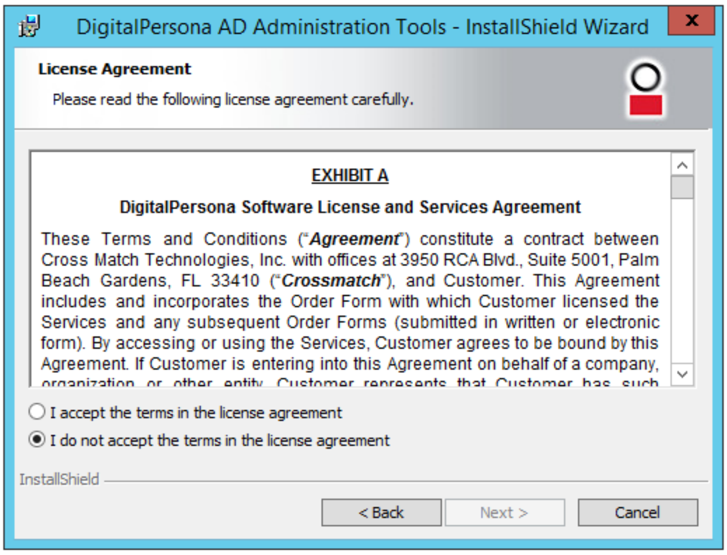
DigitalPersona LDS Administration Tools - InstallShield Wizard

Welcome to the InstallShield Wizard for DigitalPersona LDS Administration Tools

The InstallShield(R) Wizard will install DigitalPersona LDS Administration Tools on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. On the *Welcome* page, click *Next*.



DigitalPersona AD Administration Tools - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

EXHIBIT A

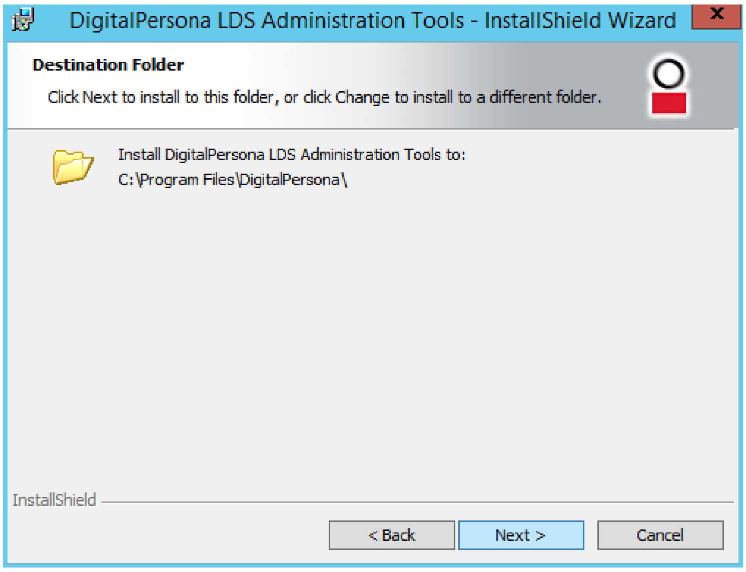
DigitalPersona Software License and Services Agreement

These Terms and Conditions ("***Agreement***") constitute a contract between Cross Match Technologies, Inc. with offices at 3950 RCA Blvd., Suite 5001, Palm Beach Gardens, FL 33410 ("***Crossmatch***"), and Customer. This Agreement includes and incorporates the Order Form with which Customer licensed the Services and any subsequent Order Forms (submitted in written or electronic form). By accessing or using the Services, Customer agrees to be bound by this Agreement. If Customer is entering into this Agreement on behalf of a company, organization or other entity, Customer represents that Customer has such

○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

3. On the *License Agreement* page, accept the agreement and click *Next.*



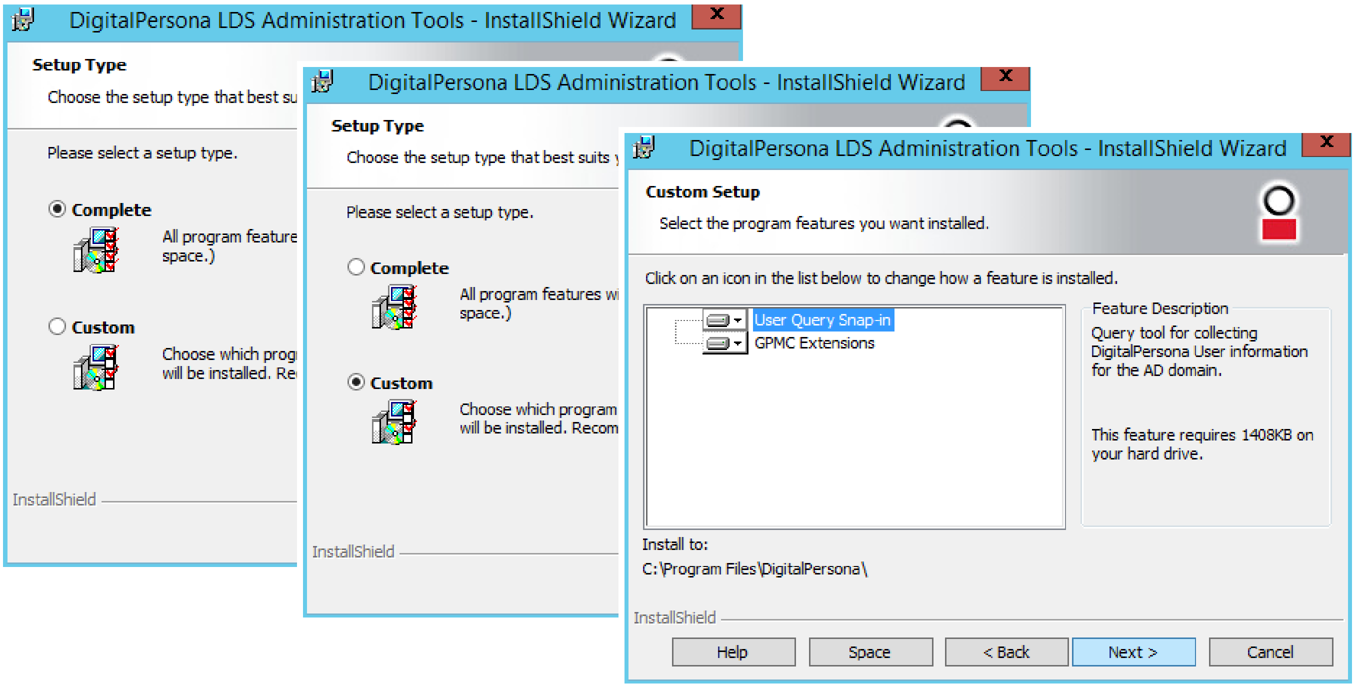
DigitalPersona LDS Administration Tools - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install DigitalPersona LDS Administration Tools to:
C:\Program Files\DigitalPersona\

4. 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 remove this button in order to ensure that associated products are installed to the same directory.



DigitalPersona LDS Administration Tools - InstallShield Wizard

Setup Type

Choose the setup type that best su

Please select a setup type.

● **Complete**
All program feature
space.)

○ **Custom**
Choose which prog
will be installed. Re

DigitalPersona LDS Administration Tools - InstallShield Wizard

Setup Type

Choose the setup type that best suits y

Please select a setup type.

○ **Complete**
All program features wi
space.)

● **Custom**
Choose which program
will be installed. Recom

DigitalPersona LDS Administration Tools - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

User Query Snap-in
GPMC Extensions

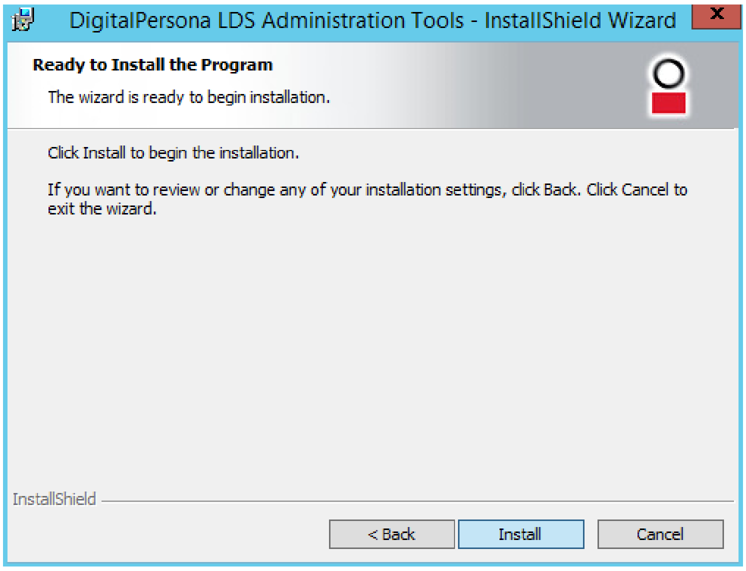
Feature Description
Query tool for collecting DigitalPersona User information for the AD domain.

This feature requires 1408KB on your hard drive.

Install to:
C:\Program Files\DigitalPersona\

5. On the *Setup Type* page, select a *Complete* installation or choose *Custom* to control which features are installed and where they are installed.

- *Complete* - Installs all available features: the *User Query Snap-in* for collecting DigitalPersona LDS user information for the AD domain, and the *GPMC Extensions,* used to link product policies and settings to Active Directory containers.
- *Custom* - By default, installs all features, but allows deselecting any feature.



DigitalPersona LDS Administration Tools - InstallShield Wizard

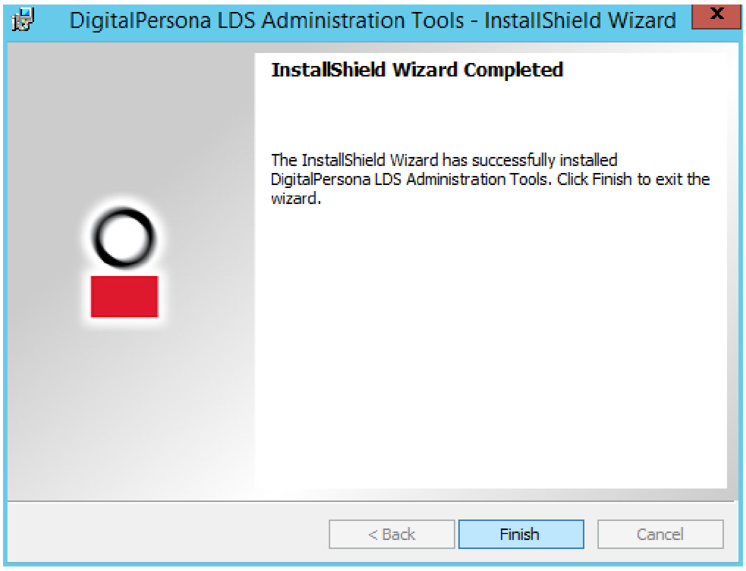
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

6. On the *Ready to Install the Program* page, click *Install*.



DigitalPersona LDS Administration Tools - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DigitalPersona LDS Administration Tools. Click Finish to exit the wizard.

7. On the *Installshield Wizard completed* page, click *Finish*.

User Query Snap-in

The User Query Snap-in feature is installed by default as part of the DigitalPersona Administration Tools. Use of the User Query Snap-in requires a licensed copy of DigitalPersona LDS Workstation, and the logged on user must have domain administrator privileges.

For a description of the features available through this snap-in, and additional implementations of it, see page 92.

GPMC Extensions

The GPMC Extensions feature is installed by default as part of the DigitalPersona Administration Tools.

DigitalPersona 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.

For a complete description of the features available through this component, see *GPMC Extensions* on page *100*. The policies and settings are described in the chapter, *Policies and Settings* on page *118*.

Activate the DigitalPersona Server License

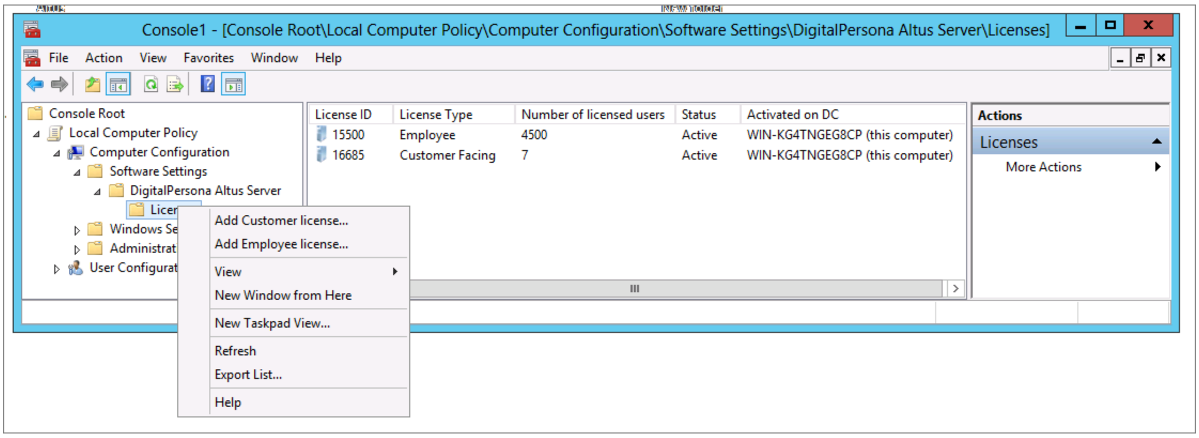
In most cases, you will activate your DigitalPersona Servers over the internet through Active Directory and the DigitalPersona Activation wizard. For additional license activation options, see the chapter *License Activation & Management* on page *76*. The following procedure assumes that license activation is performed on the DigitalPersona LDS Server machine. This is not required, but the DigitalPersona LDS Administration Tools must be installed on the computer being used to activate the license.

To activate a DigitalPersona User license

1. From the computer where the DigitalPersona Server to be licensed is installed, open the Local Group Policy Editor (gpedit.msc).

2. Navigate to: Computer Configuration, Software Settings, DigitalPersona Server, Licenses.

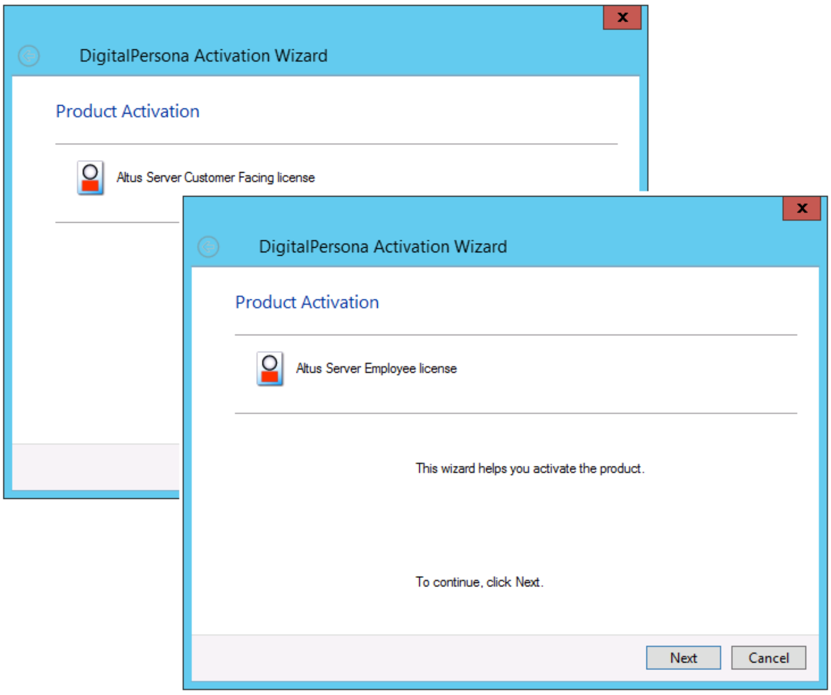
3. Right-click on *Licenses* and select *Add Customer license* or *Add Employee license*.



Console1 - [Console Root\Local Computer Policy\Computer Configuration\Software Settings\DigitalPersona Altus Server\Licenses]

License ID	License Type	Number of licensed users	Status	Activated on DC
15500	Employee	4500	Active	WIN-KG4TNGEG8CP (this computer)
16685	Customer Facing	7	Active	WIN-KG4TNGEG8CP (this computer)

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



DigitalPersona Activation Wizard

Product Activation

Altus Server Customer Facing license

DigitalPersona Activation Wizard

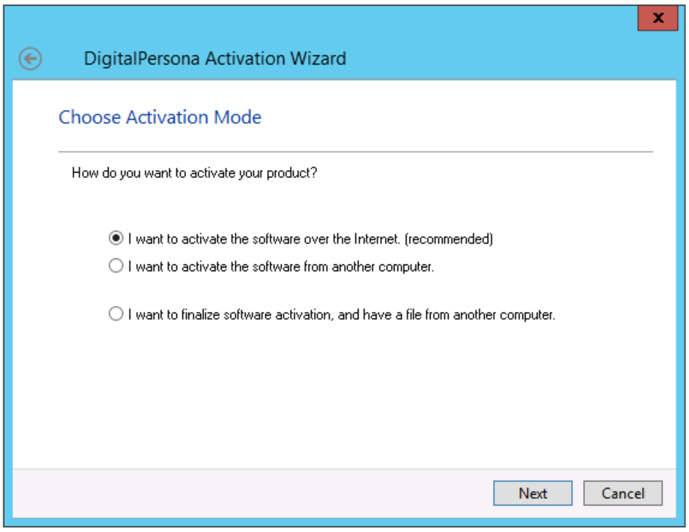
Product Activation

Altus Server Employee license

This wizard helps you activate the product.

To continue, click Next.

5. Select the option to *I want to activate the software over the Internet.*



DigitalPersona Activation Wizard

Choose Activation Mode

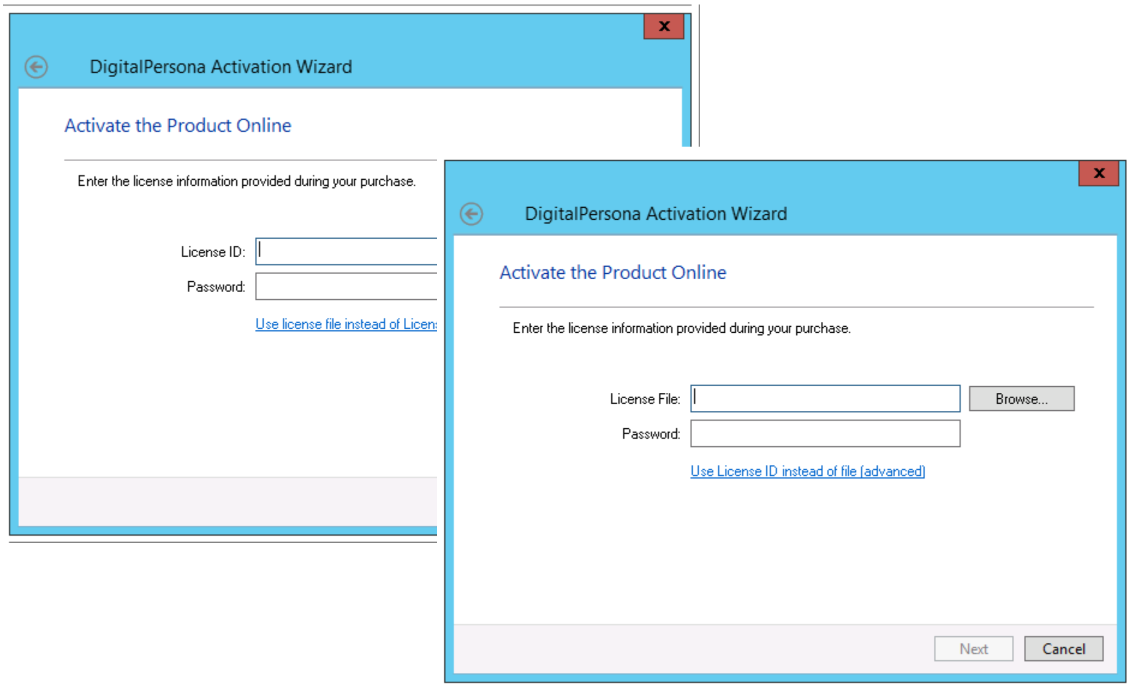
How do you want to activate your product?

● I want to activate the software over the Internet. (recommended)

○ I want to activate the software from another computer.

○ I want to finalize software activation, and have a file from another computer.

6. On the next page, enter the License ID and password provided with your product purchase. Or, if you have been given a License Activation (.dplic) file, click the *Use license file instead of License ID link* to display a page where you can activate the product with the License Activation file.



DigitalPersona Activation Wizard

Activate the Product Online

Enter the license information provided during your purchase.

License ID:

Password:

Use license file instead of Licen

DigitalPersona Activation Wizard

Activate the Product Online

Enter the license information provided during your purchase.

License File:

Password:

Click **Next**. Upon successful activation, a confirmation dialog will display.

Define the authorization store name

The administration and management of role-based permissions, tasks and operations for DigitalPersona LDS is accomplished through the DigitalPersona Authorization Store and the Microsoft Authorization Manager.

For ease of use, the Authorization Manager Snap-in may be added to a new or existing Microsoft Management Console on any computer that is a member of the same domain as the DigitalPersona LDS Server. The Authorization Manager can also be run directly from the command line by entering *azman.mmc*. A shortcut to the MMC placed on the Start screen or Windows taskbar provides immediate and convenient access to the Authorization Manager and Authorization Store.

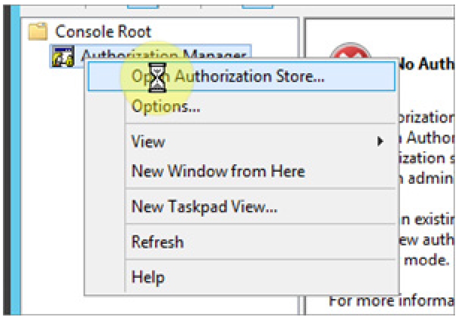
Installation and administration of the Microsoft Authorization Manager Snap-in must be performed by a member of the computer's local Administrators group.

For details on the DigitalPersona LDS-specific features and configuration provided by the DigitalPersona Authorization Store, see the chapter *“Authorization Manager (AzMan)”* starting on page 146.

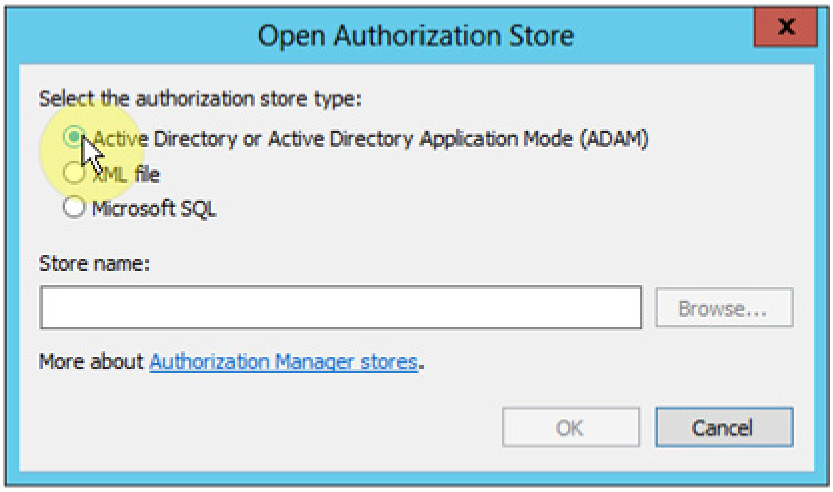
To enter the Authorization Store name for DigitalPersona LDS

Define the authorization store name

1. Launch the Microsoft Authorization Manager by typing *azman.msc* on the start screen.



2. In the Microsoft Authorization Manager, select *Open Authorization Store*.
3. Select *Active Directory or Active Directory Application Mode (ADAM)*.


Open Authorization Store
Select the authorization store type:
● Active Directory or Active Directory Application Mode (ADAM)
○ XML file
○ Microsoft SQL
Store name:
Browse...
More about Authorization Manager stores.
OK
Cancel

4. Enter the authorization store name and click *OK*.

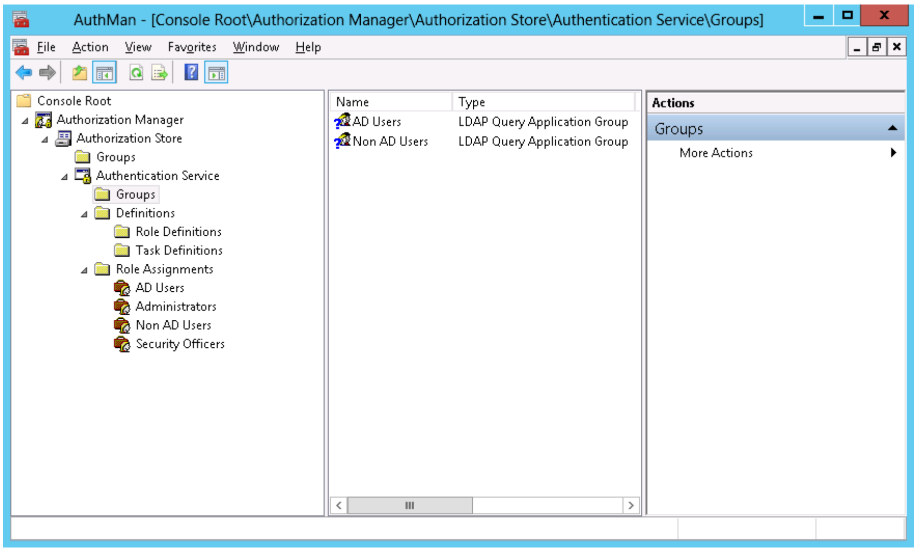
   Since the syntax of the store name is rather complex, the necessary string defining the store name is provided in a file for you so that you can copy and paste it into the *Store name* field. The file name and location (based on a default installation) is:

   Program Files\DigitalPersona\Bin\AzMan.txt

   The authorization store name will be a string similar to the following -

```
MSLDAP://127.0.0.1:50000/CN=Authorization Store,CN={893B81EE-7764-44FF-8561-
8377580B9B03},O=DigitalPersona,C=US
```

5. Once the authorization store has been set up, the Authorization Manager will be populated with the roles, tasks and operations defined for DigitalPersona LDS.



Name	Type
AD Users	LDAP Query Application Group
Non AD Users	LDAP Query Application Group

Although the system does not ask you to reboot the computer, doing so is recommended.

For details on the DigitalPersona LDS authorization store, its objects and attributes and how they are used, see the chapter “Authorization Manager (AzMan)” starting on page 146.

Configure additional servers (Recommended)

HID Global recommends the use of additional DigitalPersona LDS Servers to make use of the solution’s built-in load balancing and failover capabilities.

However, each DigitalPersona LDS Server and its associated AD LDS database must reside on a separate machine. Multiple DigitalPersona LDS Servers cannot coexist on the same machine, and an associated database must be on the same machine as the DigitalPersona LDS Server.

To configure an additional DigitalPersona LDS Server for load balancing and failover, follow the steps provided below. This will result in multiple AD LDS instances that are automatically synchronized and load balanced.

It is recommended to have the first AD LDS instance and DigitalPersona LDS Server completely set up following the instructions in the first part of this chapter before creating any additional instances. This is because any additional AD LDS instances require information from the original instance for configuration when joining the configuration set.

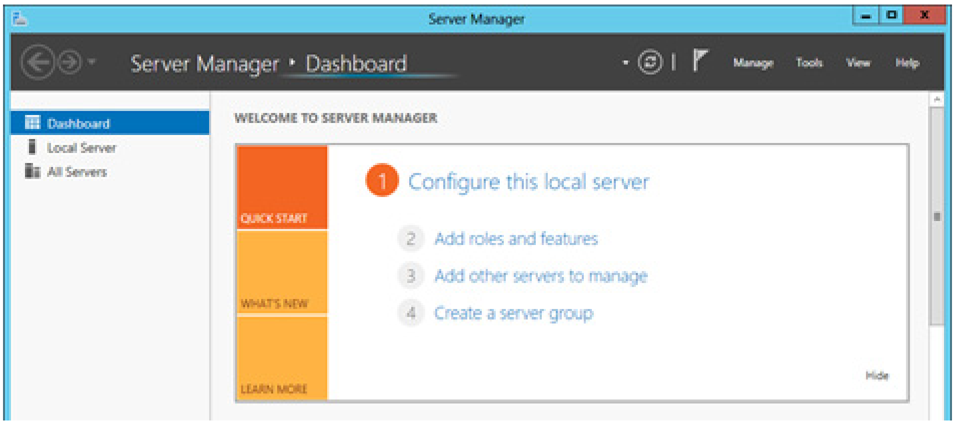
For scenarios where separate DigitalPersona LDS Servers are desired that are *not* synchronized and will not load balance or failover, simply follow the instructions for installation and setup provided in the first part of this chapter.

Add Server roles and features

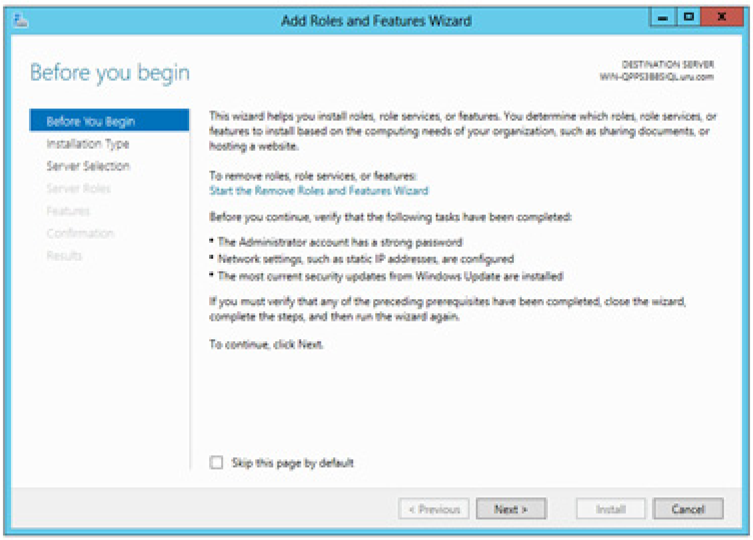
Before installing DigitalPersona LDS Server, there are a few roles and features that need to be added to the default installation of Windows Server.

To add the required roles and features required by the DigitalPersona LDS Server

1. In Windows Server, open the Server Manager and select *Dashboard*.



2. Under *Configure this local server*, click *Add roles and features*.



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

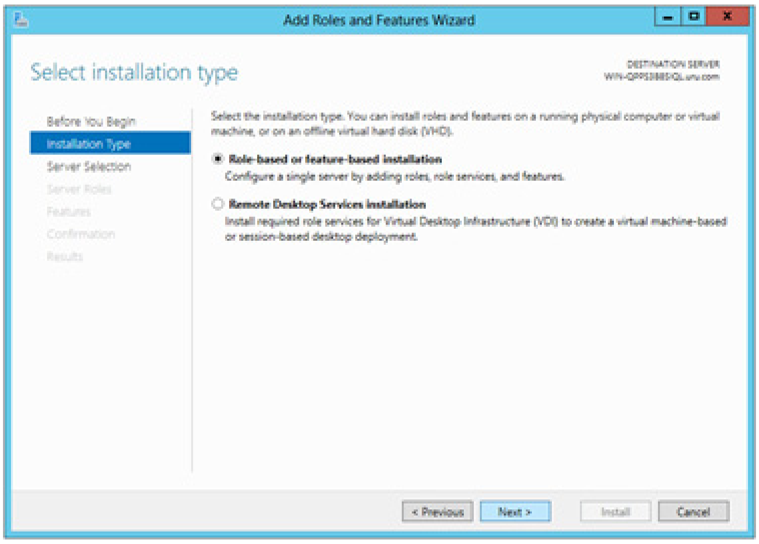
To continue, click Next.

□ Skip this page by default

3. On the *Before you begin* page of the Add Roles and Features Wizard, verify that you have completed the prerequisite tasks before continuing. Then click *Next*.

Configure additional servers (Recommended)

4. On the *Select installation type* page, select *Role-based or feature-based installation*. Then click *Next*.



Select installation type

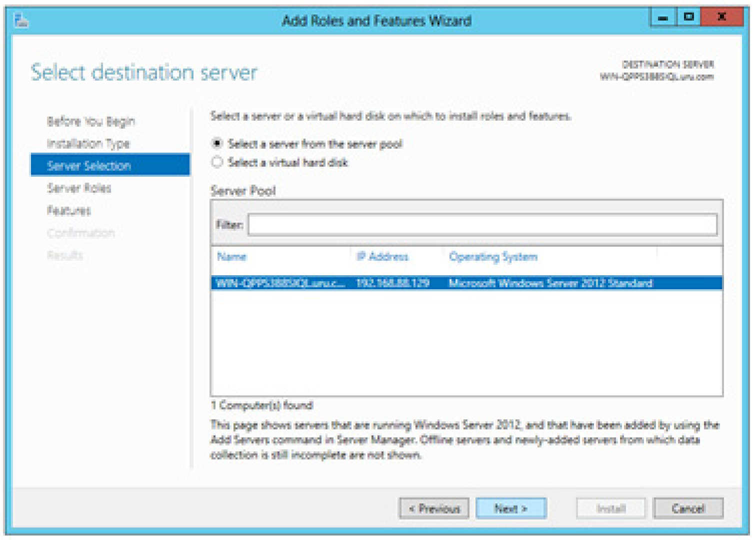
DESTINATION SERVER
WIN-QPPS388SIQL.uru.com

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

5. On the *Select destination server* page, choose *Select a server from the server pool*. Then click *Next*.



Select destination server

DESTINATION SERVER
WIN-QPPS388SIQL.uru.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

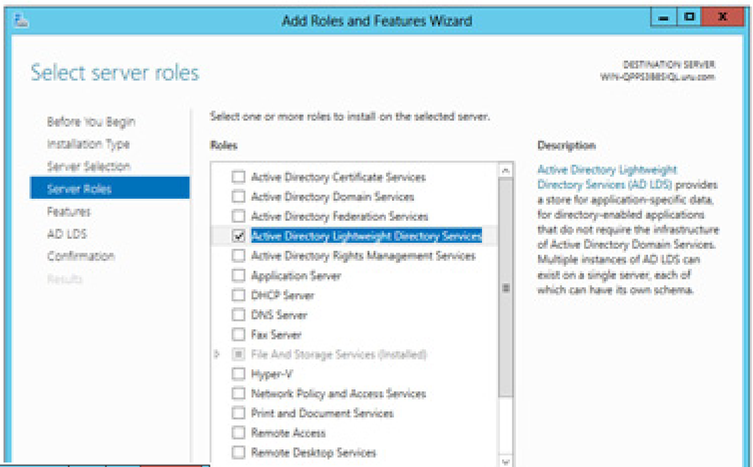
Name	IP Address	Operating System
WIN-QPPS388SIQL.uru.c...	192.168.88.129	Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Configure additional servers (Recommended)

6. On the *Select server roles* page, in addition to the roles selected by default, ensure that the *Active Directory Lightweight Directory Services role* is included and then click *Next*.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-QPPS388SIQL.unu.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD LDS
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☑ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▨ File And Storage Services (Installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

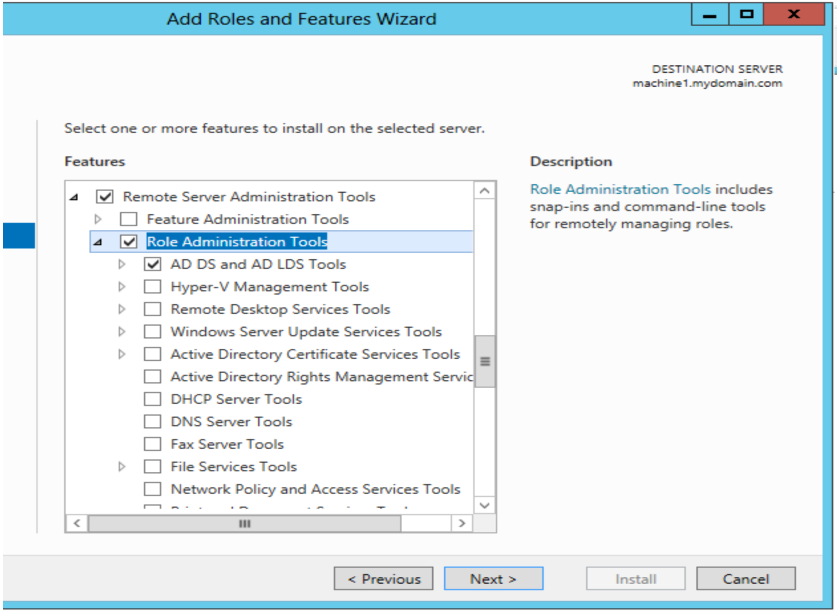
Description

Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.

7. On the *Select features* page, in addition to the features selected by default, ensure that the following features are selected and then click *Next*.

   Group Policy Management

   AD DS and AD LDS Tools



Add Roles and Features Wizard

DESTINATION SERVER
machine1.mydomain.com

Select one or more features to install on the selected server.

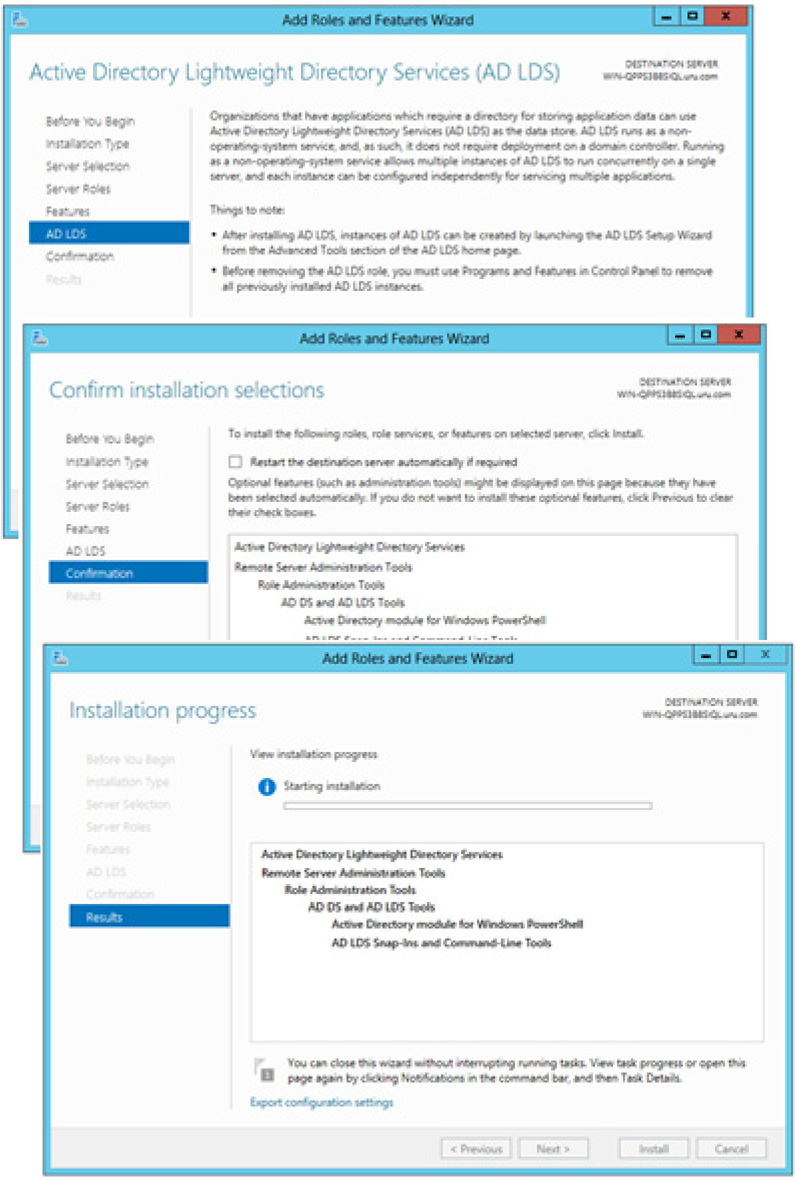
Features

- ☑ Remote Server Administration Tools
  - ☐ Feature Administration Tools
  - ☑ Role Administration Tools
    - ☑ AD DS and AD LDS Tools
    - ☐ Hyper-V Management Tools
    - ☐ Remote Desktop Services Tools
    - ☐ Windows Server Update Services Tools
    - ☐ Active Directory Certificate Services Tools
    - ☐ Active Directory Rights Management Servic
    - ☐ DHCP Server Tools
    - ☐ DNS Server Tools
    - ☐ Fax Server Tools
    - ☐ File Services Tools
    - ☐ Network Policy and Access Services Tools

Description

Role Administration Tools includes snap-ins and command-line tools for remotely managing roles.

8. The following page simply explains how to create an AD LDS instance, by using the AD LDS Setup Wizard, and how to remove the AD LDS role through the Windows Control Panel. Click *Next*.
9. On the *Confirm installation selections* page, click *Install*.
10. The *Installation progress* page displays a bar indicating the approximate progress of the installation process. Note that you can close the wizard (by clicking the Close (X) button) without interrupting the installation, and open it again to view progress by clicking *Notifications* and then *Task Details* in the Server Manager Dashboard Command Bar.



Organizations that have applications which require a directory for storing application data can use Active Directory Lightweight Directory Services (AD LDS) as the data store. AD LDS runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service allows multiple instances of AD LDS to run concurrently on a single server, and each instance can be configured independently for servicing multiple applications.

Things to note:

- After installing AD LDS, instances of AD LDS can be created by launching the AD LDS Setup Wizard from the Advanced Tools section of the AD LDS home page.
- Before removing the AD LDS role, you must use Programs and Features in Control Panel to remove all previously installed AD LDS instances.

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Lightweight Directory Services
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell

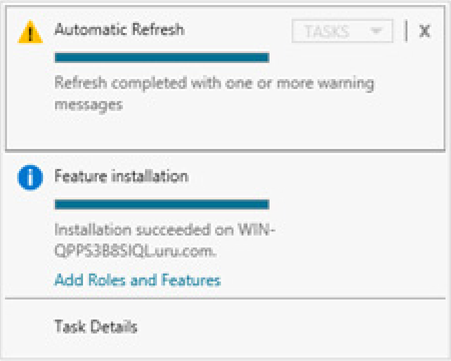
View installation progress

Starting installation

Active Directory Lightweight Directory Services
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD LDS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

11. Upon completion of the installation, the wizard will close and the following information will display. An automatic refresh will also be performed.



Automatic Refresh

Refresh completed with one or more warning messages

Feature installation

Installation succeeded on WIN-QPPS3B8SIQL.uru.com.

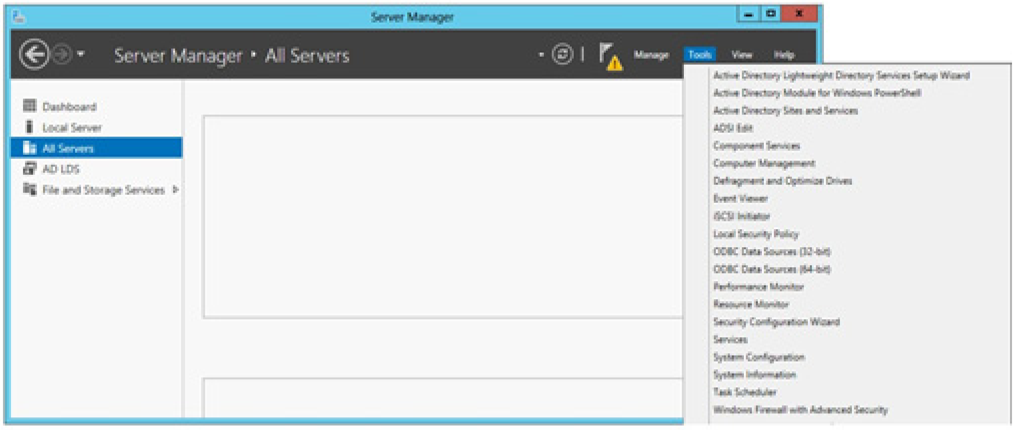
Set up a replica of an existing AD LDS instance

Once the LDS *feature* has been installed, you will use the Active Directory Lightweight Directory Services Setup Wizard to install a new AD LDS instance on this machine that is a replica of the existing *instance* created during the installation of your first DigitalPersona LDS Server.

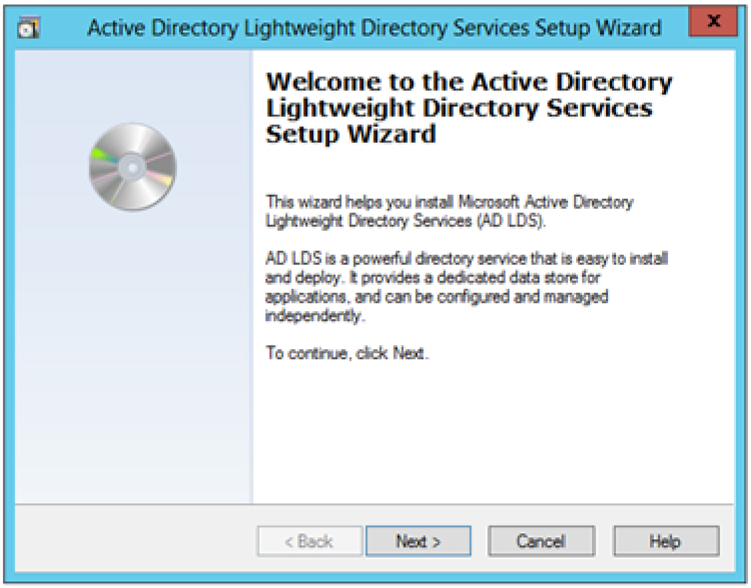
To set up an AD LDS replica

Configure additional servers (Recommended)

1. In the Server Manager Dashboard Command Bar, select *Tools*. Then select *Active Directory Lightweight Directory Services Setup Wizard*.


Server Manager
Server Manager • All Servers
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD LDS
File and Storage Services
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Event Viewer
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security

2. The Active Directory Lightweight Directory Services Setup Wizard displays. Click *Next*.


Active Directory Lightweight Directory Services Setup Wizard
< Back
Next >
Cancel
Help

Welcome to the Active Directory Lightweight Directory Services Setup Wizard

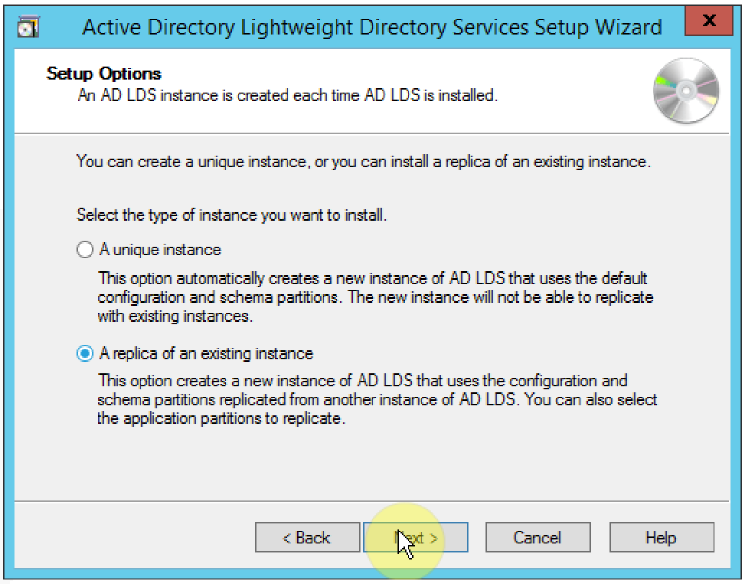
This wizard helps you install Microsoft Active Directory Lightweight Directory Services (AD LDS).

AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.

To continue, click Next.

Configure additional servers (Recommended)

3. On the *Setup options* page, select *A replica of an existing instance*. Then click *Next*. This will create a new AD LDS instance on this machine that uses the configuration and schema pattern from the instance associated with your previously installed DigitalPersona LDS Server.



Active Directory Lightweight Directory Services Setup Wizard

Setup Options

An AD LDS instance is created each time AD LDS is installed.

You can create a unique instance, or you can install a replica of an existing instance.

Select the type of instance you want to install.

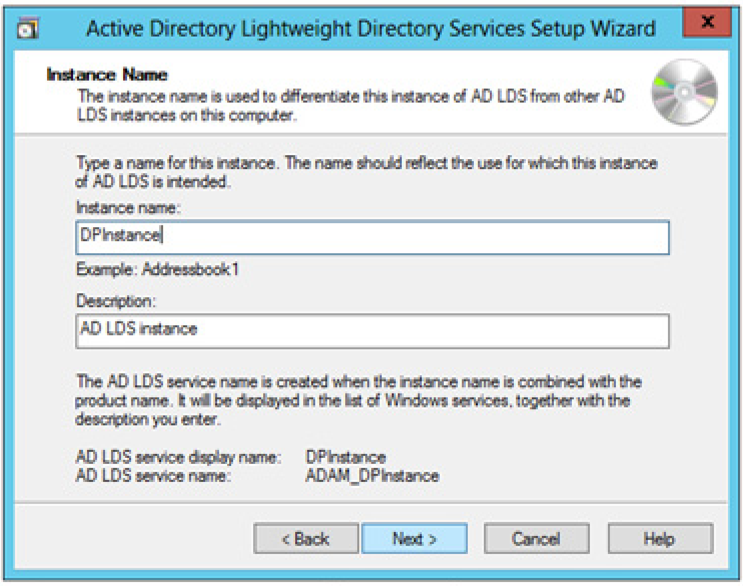
○ A unique instance

This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.

● A replica of an existing instance

This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.

4. Enter the name for the instance you are creating. This must be the same name as the original instance that you are replicating. Optionally, enter a description.



Active Directory Lightweight Directory Services Setup Wizard

Instance Name

The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.

Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.

Instance name: DPInstance

Example: Addressbook1

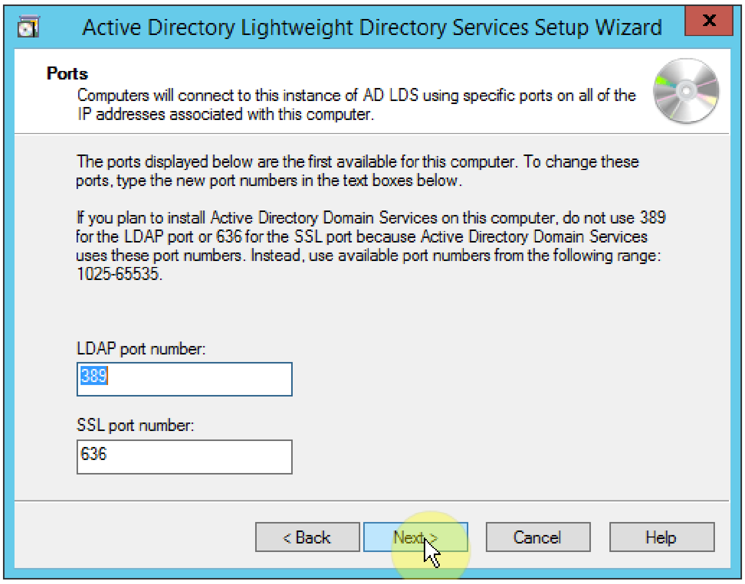
Description: AD LDS instance

The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.

AD LDS service display name: DPInstance

AD LDS service name: ADAM_DPInstance

5. Enter the LDAP and SSL port numbers for this instance. The default port numbers for this computer are shown. In most cases, the default port numbers should be accepted.



Active Directory Lightweight Directory Services Setup Wizard

Ports

Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.

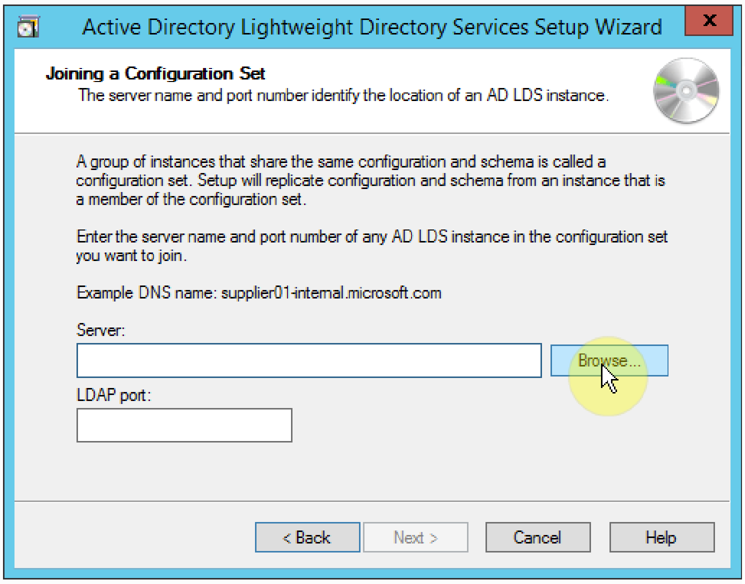
The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number: 389

SSL port number: 636

6. Enter the Server Name and LDAP port for the Configuration Set that you want to join.



Active Directory Lightweight Directory Services Setup Wizard

Joining a Configuration Set

The server name and port number identify the location of an AD LDS instance.

A group of instances that share the same configuration and schema is called a configuration set. Setup will replicate configuration and schema from an instance that is a member of the configuration set.

Enter the server name and port number of any AD LDS instance in the configuration set you want to join.

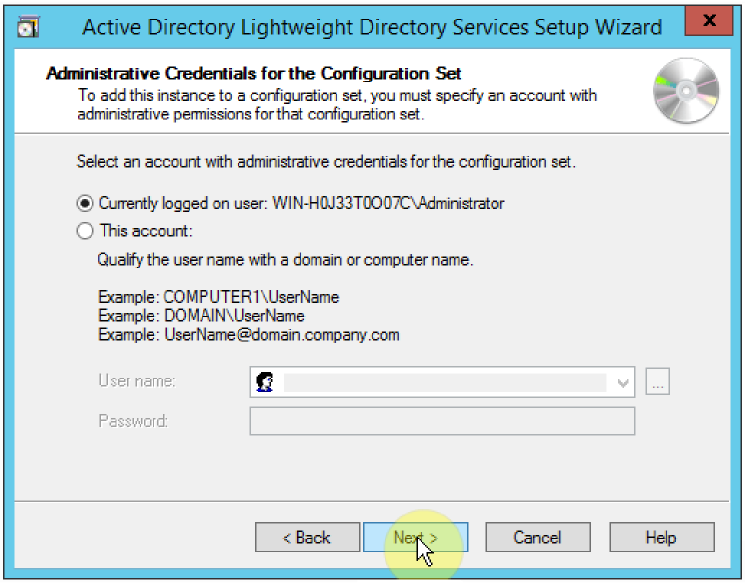
Example DNS name: supplier01-internal.microsoft.com

Server:

LDAP port:

7. If you do not have the exact Server Name and port, click *Select* to search for and select the server. You will be asked for your network credentials. Enter the LDAP port that was used in the installation of the original DigitalPersona LDS instance. Once the Configuration Set information has been entered, click *Next* to continue.

8. Select an account with administrative credentials for the configuration set.



Active Directory Lightweight Directory Services Setup Wizard

Administrative Credentials for the Configuration Set

To add this instance to a configuration set, you must specify an account with administrative permissions for that configuration set.

Select an account with administrative credentials for the configuration set.

● Currently logged on user: WIN-H0J33T0O07C\Administrator

○ This account:

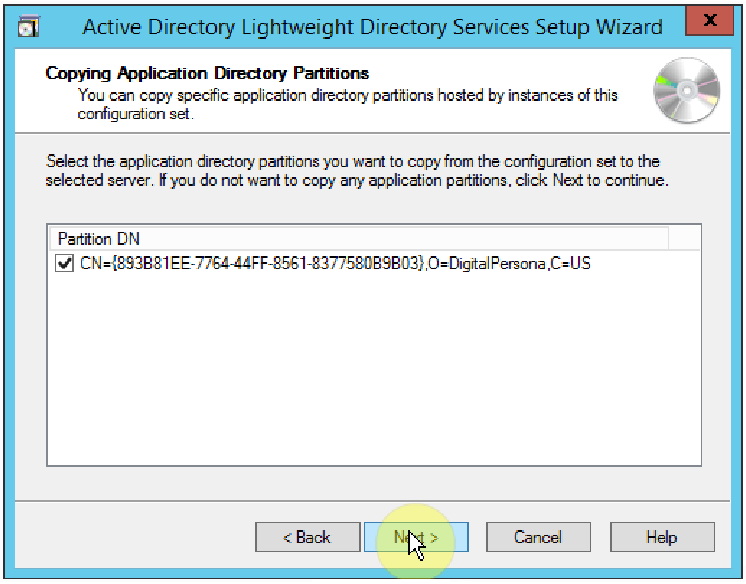
Qualify the user name with a domain or computer name.

Example: COMPUTER1\UserName
Example: DOMAIN\UserName
Example: UserName@domain.company.com

User name:

Password:

9. Select the Application Directory Partitions to copy from the Configuration Set to the selected server.



Active Directory Lightweight Directory Services Setup Wizard

Copying Application Directory Partitions

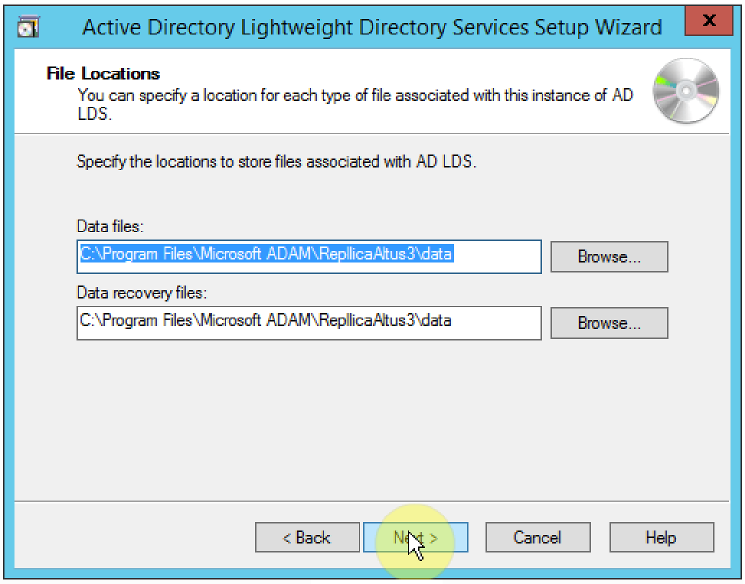
You can copy specific application directory partitions hosted by instances of this configuration set.

Select the application directory partitions you want to copy from the configuration set to the selected server. If you do not want to copy any application partitions, click Next to continue.

Partition DN
☑ CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US

If no Application Directory Partition is shown, this may indicate that the DigitalPersona AD LDS Configuration Wizard was not run on the initial AD LDS instance. Close this wizard, return to the original instance and run the configuration wizard there before continuing.

10. Specify a location for each type of file associated with this instance of AD LDS.



Active Directory Lightweight Directory Services Setup Wizard

File Locations

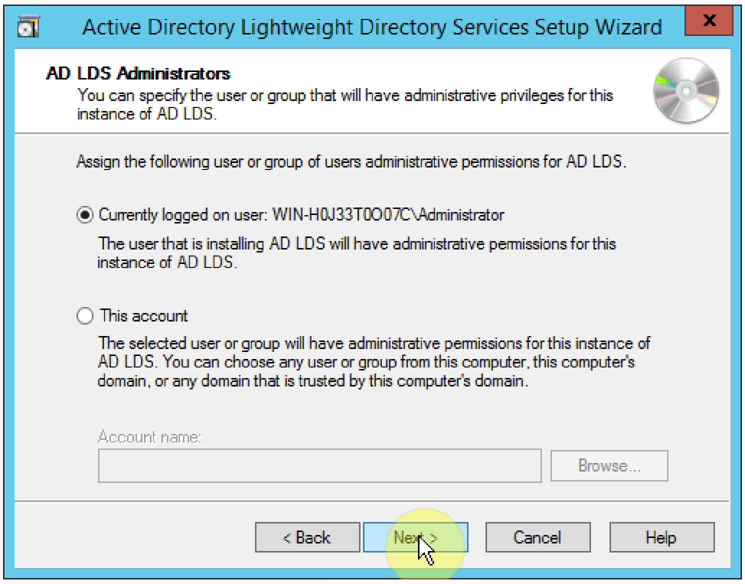
You can specify a location for each type of file associated with this instance of AD LDS.

Specify the locations to store files associated with AD LDS.

Data files: C:\Program Files\Microsoft ADAM\ReplicaAltus3\data

Data recovery files: C:\Program Files\Microsoft ADAM\ReplicaAltus3\data

11. Specify the user or group that will have administrative privileges for this AD LDS instance.



Active Directory Lightweight Directory Services Setup Wizard

AD LDS Administrators

You can specify the user or group that will have administrative privileges for this instance of AD LDS.

Assign the following user or group of users administrative permissions for AD LDS.

● Currently logged on user: WIN-H0J33T0O07C\Administrator

The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.

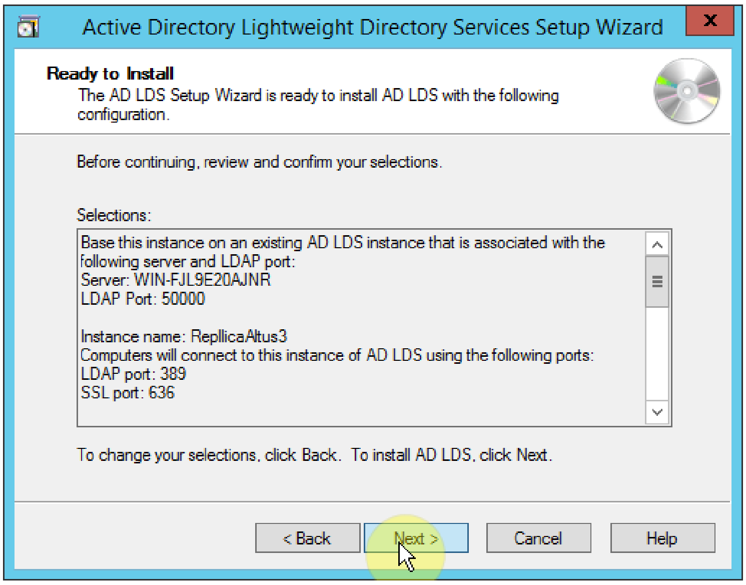
○ This account

The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.

Account name:

Configure additional servers (Recommended)

12. At the Ready to Install page, click *Next*.



Active Directory Lightweight Directory Services Setup Wizard

Ready to Install

The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.

Before continuing, review and confirm your selections.

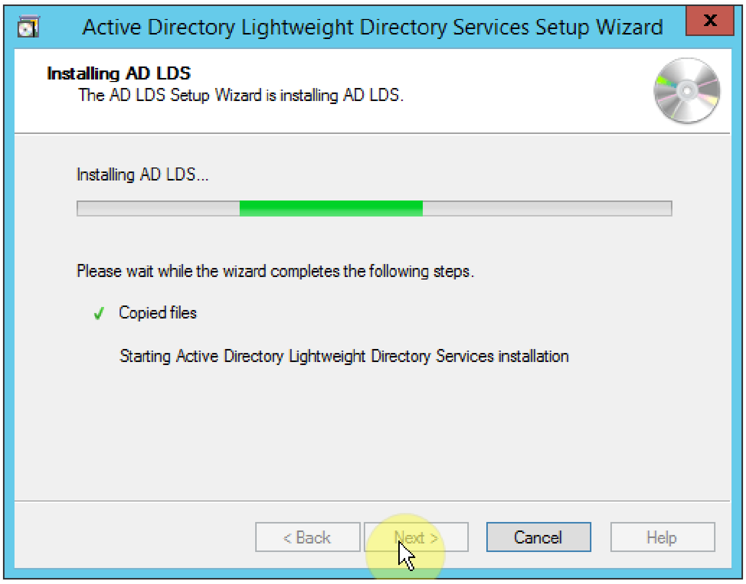
Selections:

Base this instance on an existing AD LDS instance that is associated with the following server and LDAP port:
Server: WIN-FJL9E20AJNR
LDAP Port: 50000

Instance name: ReplicaAltus3
Computers will connect to this instance of AD LDS using the following ports:
LDAP port: 389
SSL port: 636

To change your selections, click Back. To install AD LDS, click Next.

13. During the installation, a progress bar is shown along with details about the installation process.



Active Directory Lightweight Directory Services Setup Wizard

Installing AD LDS

The AD LDS Setup Wizard is installing AD LDS.

Installing AD LDS...

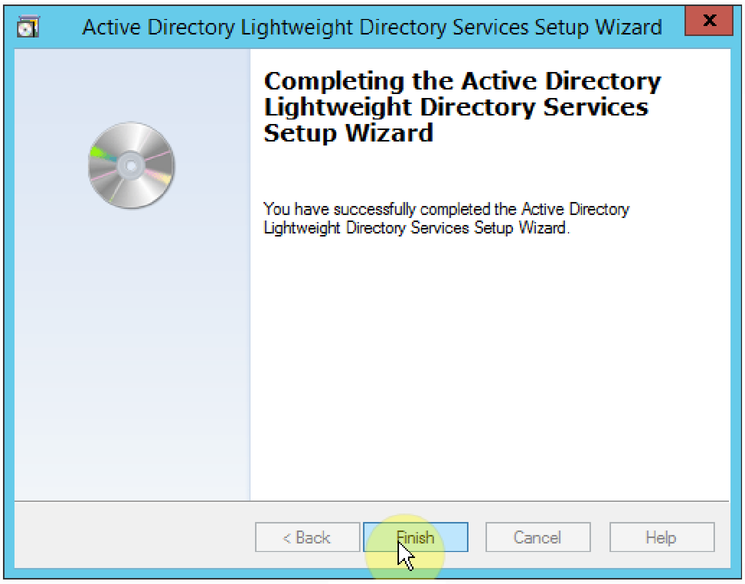
Please wait while the wizard completes the following steps.

✓ Copied files

Starting Active Directory Lightweight Directory Services installation

< Back
Next >
Cancel
Help

14. When the AD LDS Setup Wizard has finished the installation, a final dialog displays. Click *Finish*.

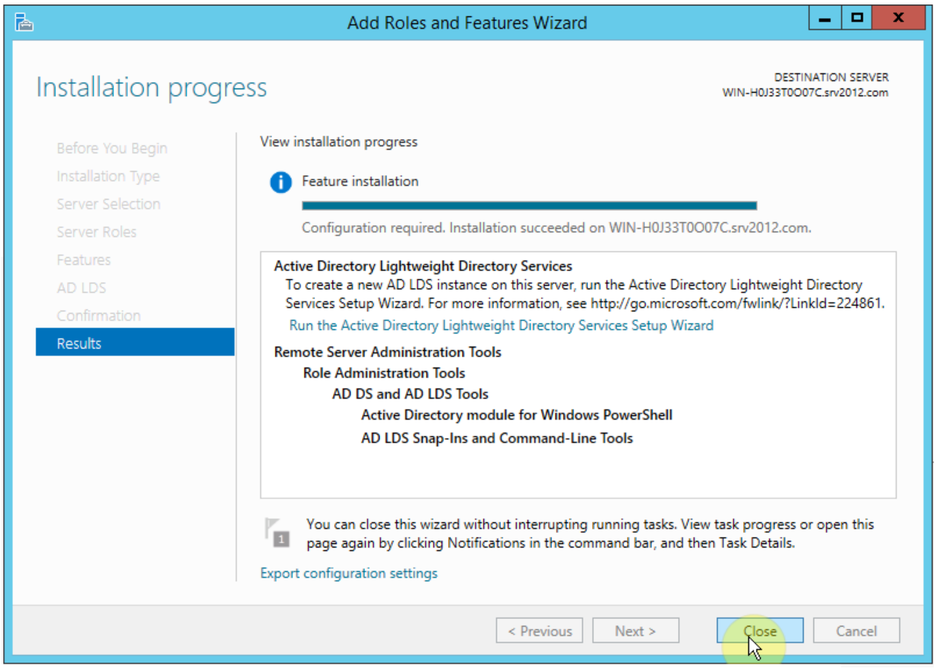


Active Directory Lightweight Directory Services Setup Wizard

Completing the Active Directory Lightweight Directory Services Setup Wizard

You have successfully completed the Active Directory Lightweight Directory Services Setup Wizard.

15. Closing the above dialog leaves the Add Roles and Features Wizard page on the screen. Additional tasks will be running, but you can close this page without interrupting them. You can open the page again by clicking *Notifications* in the command bar and then *Task Details*.



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-H0J33T0O07C.srv2012.com

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-H0J33T0O07C.srv2012.com.

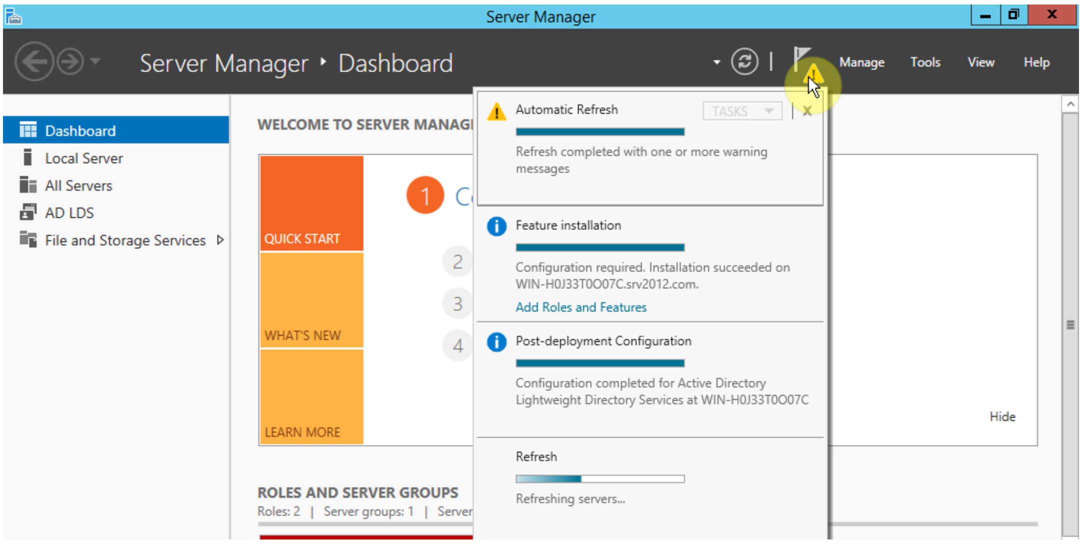
Active Directory Lightweight Directory Services
To create a new AD LDS instance on this server, run the Active Directory Lightweight Directory Services Setup Wizard. For more information, see http://go.microsoft.com/fwlink/?LinkId=224861.
Run the Active Directory Lightweight Directory Services Setup Wizard

Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD LDS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

16. Finally, closing the Add Roles and Features page will leave the Server Manager Dashboard on the screen. There will be an error flag in the upper right of the page until the AD LDS replica setup has completed post deployment configuration. To cause the page to refresh, click the Refresh button to the left of the warning flag.



Automatic Refresh

Refresh completed with one or more warning messages

Feature installation

Configuration required. Installation succeeded on WIN-H0J33T0O07C.srv2012.com.

Add Roles and Features

Post-deployment Configuration

Configuration completed for Active Directory Lightweight Directory Services at WIN-H0J33T0O07C

Refresh

Refreshing servers...

Configuration of the AD LDS Service

DO NOT run the DigitalPersona AD LDS Configuration Wizard when setting up your replica. Configuration and schema information for the replica is automatically set to match the joined unique instance associated with your previous DigitalPersona LDS Server.

Configuring replication frequency and availability

By default, replication of data from one instance to another within a configuration set is set to occur every 180 minutes (3 hours). This time interval is configurable. Additionally specified blocks of time may be designated as available or unavailable for replication in order to limit scheduled replication intervals to certain times of the day (such as after normal business hours).

For instructions on configuring replication frequency and availability, see the following article on Microsoft’s TechNet site: *https://technet.microsoft.com/en-us/library/cc731862(v=ws.11).aspx*

Install DigitalPersona Server

Before installing DigitalPersona Server, ensure that the computer meets the minimum requirements listed on page 19, and that the Windows AD LDS feature has been added to the Windows Server machine and properly configured. Note that installations of DigitalPersona LDS Server using a replica of the AD LDS instance tied to a properly licensed of DigitalPersona LDS Server do not require an additional license, as the license information is automatically applied as part of the replication process.

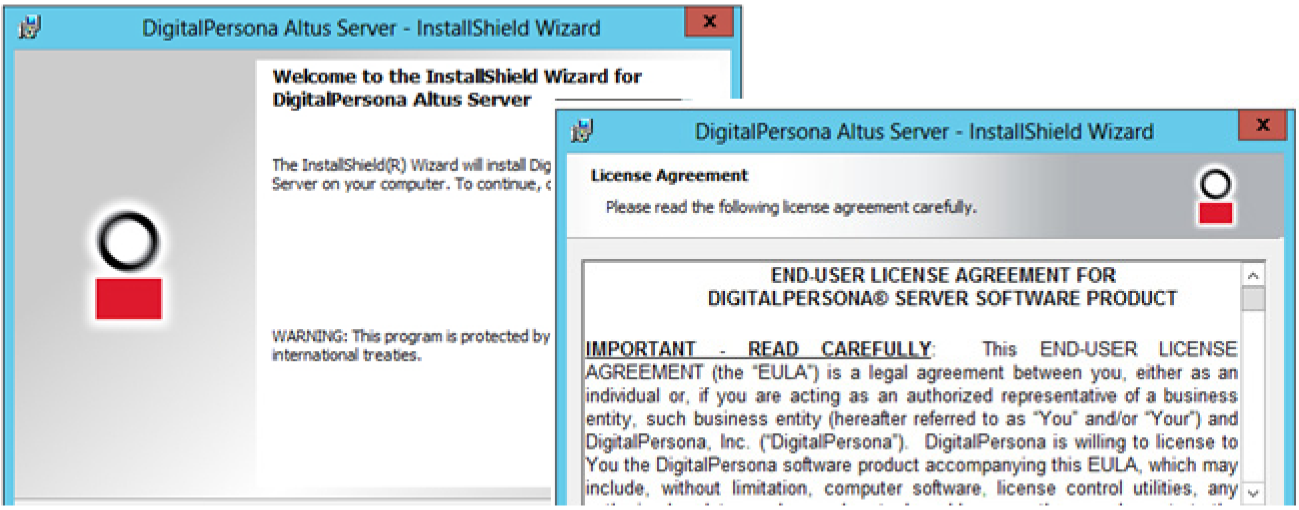
To install the DigitalPersona LDS Server

1. Launch the *DigitalPersona LDS Server - InstallShield Wizard* by running *Setup.exe*, located in the *Server/ DigitalPersona LDS Server* folder in your product package. (Or see page 65 for Command Line installation.)

2. The wizard's *Welcome* page displays. Click *Next*.

Configure additional servers (Recommended)

3. Read the *License Agreement* page. If you agree with the stated terms, select *I accept the license agreement*. and click *Next*.



DigitalPersona Altus Server - InstallShield Wizard

Welcome to the InstallShield Wizard for DigitalPersona Altus Server

The InstallShield(R) Wizard will install Dig Server on your computer. To continue, c

WARNING: This program is protected by international treaties.

DigitalPersona Altus Server - InstallShield Wizard

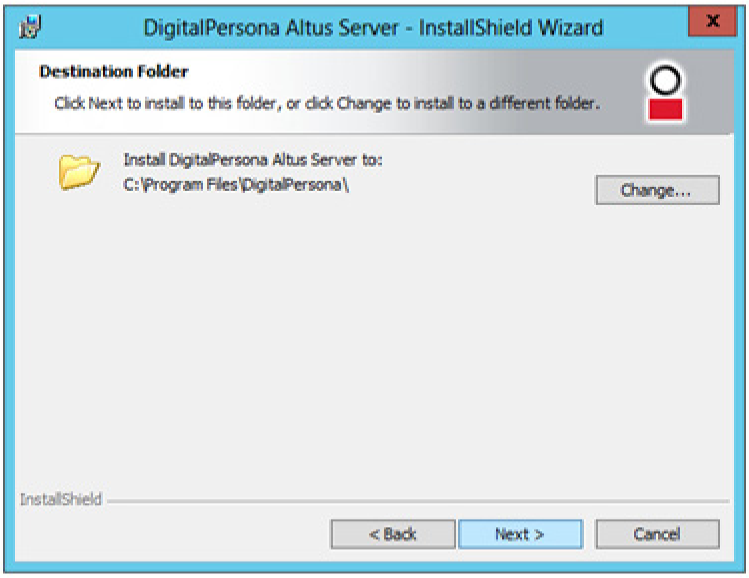
License Agreement

Please read the following license agreement carefully.

END-USER LICENSE AGREEMENT FOR DIGITALPERSONA® SERVER SOFTWARE PRODUCT

IMPORTANT - READ CAREFULLY: This END-USER LICENSE AGREEMENT (the "EULA") is a legal agreement between you, either as an individual or, if you are acting as an authorized representative of a business entity, such business entity (hereafter referred to as "You" and/or "Your") and DigitalPersona, Inc. ("DigitalPersona"). DigitalPersona is willing to license to You the DigitalPersona software product accompanying this EULA, which may include, without limitation, computer software, license control utilities, any

4. On the *Destination Folder* page, accept the default install destination folder, or click *Change* to install to a different folder. Click *Next*.

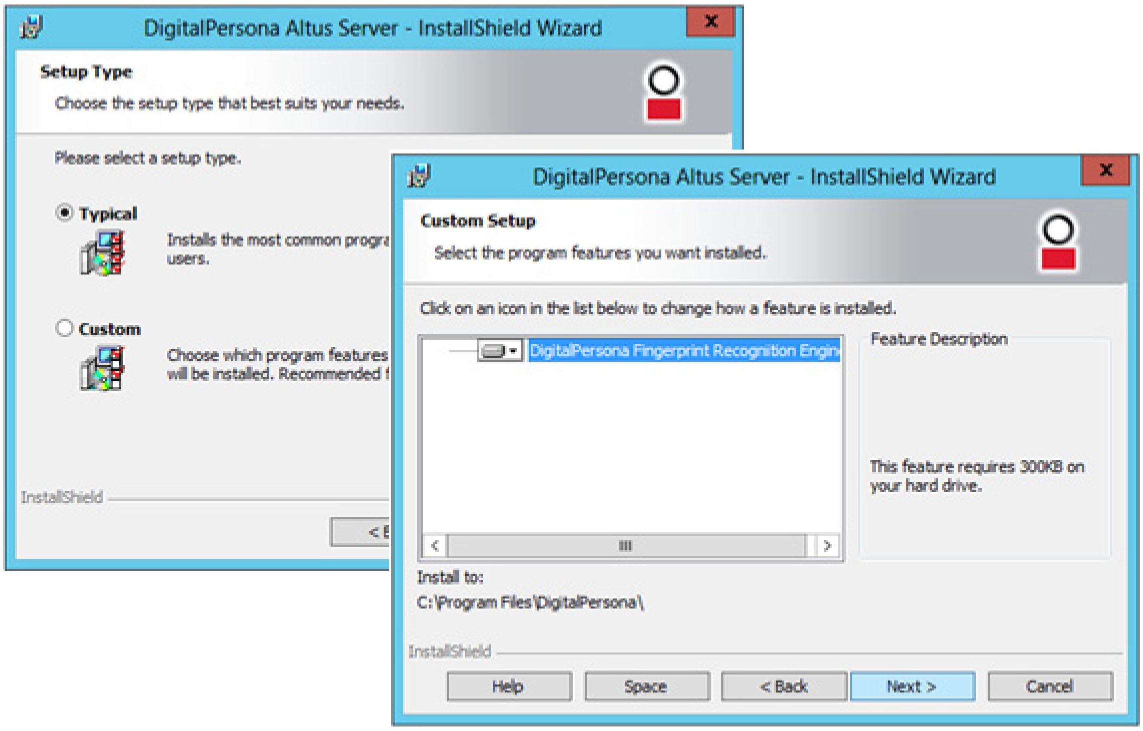


Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install DigitalPersona Altus Server to:
C:\Program Files\DigitalPersona\

5. On the *Setup type* page, choose the type of install you want to perform, *Typical* or *Custom*. Then click *Next*.



DigitalPersona Altus Server - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Typical**

Installs the most common progra
users.

○ **Custom**

Choose which program features
will be installed. Recommended f

InstallShield

DigitalPersona Altus Server - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

DigitalPersona Fingerprint Recognition Engin

Feature Description

This feature requires 300KB on your hard drive.

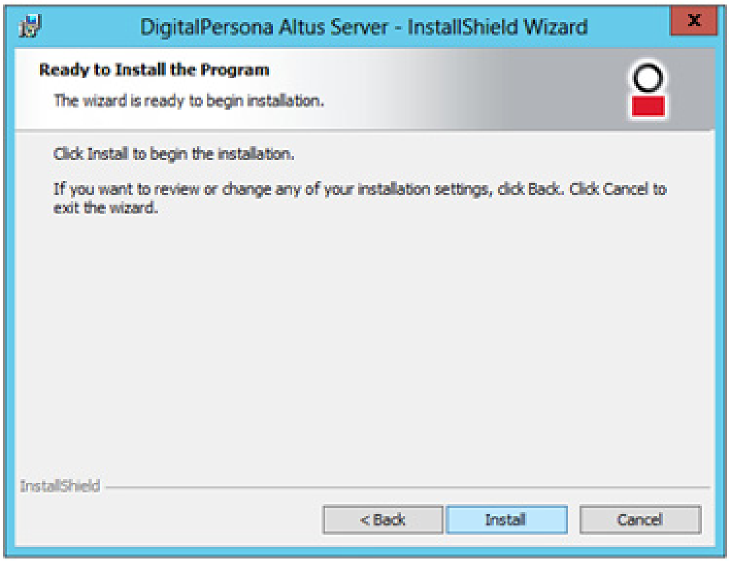
Install to:
C:\Program Files\DigitalPersona\

InstallShield

6. The Custom setup allows removing the DigitalPersona Fingerprint Recognition Engine from the installation in progress. This option allows the administrator to separately install a different fingerprint recognition engine.

   WARNING: The fingerprint recognition engine installed on the server and on the DigitalPersona client must be the same.

7. On the *Ready to Install the Program* page, click *Install*.



DigitalPersona Altus Server - InstallShield Wizard

Ready to Install the Program

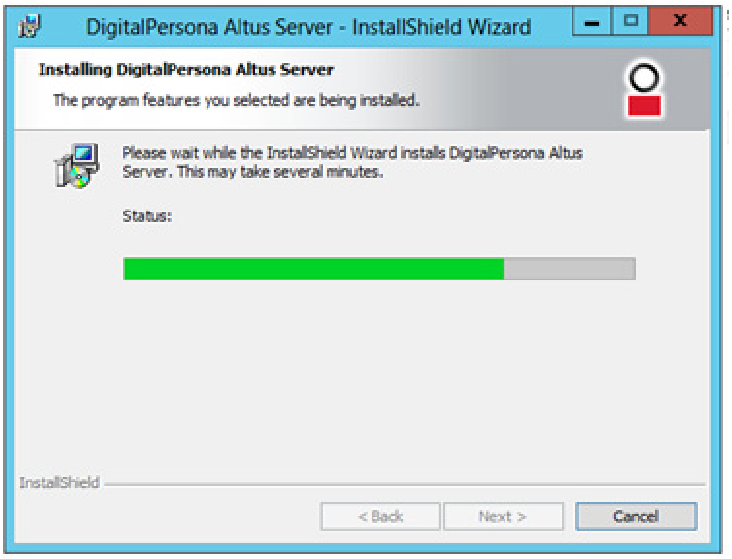
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShield

8. The *Installing DigitalPersona LDS Server* page displays the progress of the installation.



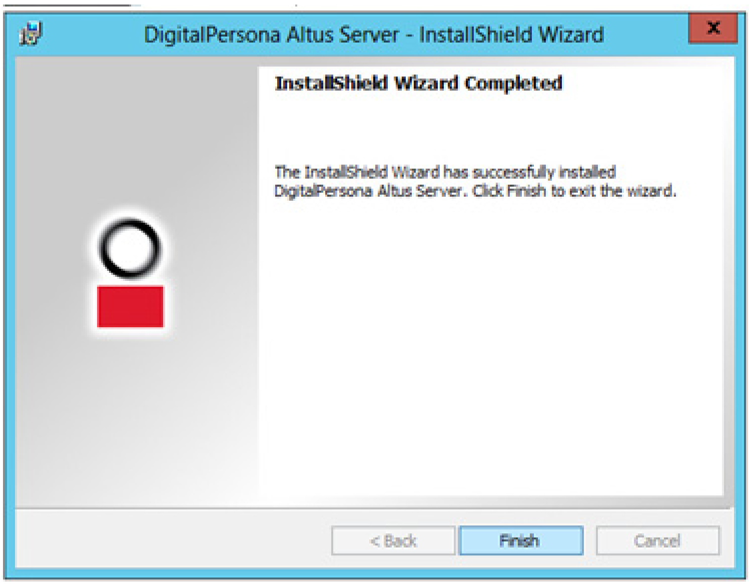
Installing DigitalPersona Altus Server

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs DigitalPersona Altus Server. This may take several minutes.

Status:

9. Upon completion of the wizard, the *InstallShield Wizard Completed* page displays. Click *Finish* to close the wizard.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DigitalPersona Altus Server. Click Finish to exit the wizard.

Do not activate a DigitalPersona Server License

When installing a DigitalPersona LDS Server using a replicated AD LDS instance, you do not need to separately license the additional DigitalPersona LDS Server. Licensing information from the original unique AD LDS instance is replicated for any additional DigitalPersona LDS Servers in the same configuration set.

Optionally open the DigitalPersona Authorization Store

In most cases, when configuring additional DigitalPersona LDS Servers for load balancing and failover, you would not need to use the Microsoft Authorization Manager or connect it to the DigitalPersona Authorization Store on the additional servers.

However, the Authorization Manager Snap-in may be added to any new or existing Microsoft Management Console on any computer that is a member of the same domain as the installed DigitalPersona LDS Servers. The Authorization Manager can also be run directly from the command line by entering *azman.mmc*. A shortcut to the MMC placed on the Start screen or Taskbar provides immediate and convenient access to the Authorization Manager and Authorization Store.

Installation and administration of the Microsoft Authorization Manager Snap-in must be performed by a member of the computer's local Administrators group.

For instructions on opening the DigitalPersona Authorization Store, see *Define the authorization store name* on page 47.

For details on the DigitalPersona LDS-specific features and configuration provided by the DigitalPersona Authorization Store, see the chapter *"Authorization Manager (AzMan)"* starting on page 146.

Command line Installation

DigitalPersona LDS Server can also be installed or uninstalled using MSI at the command line.

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

```
msiexec /i setup.msi INSTALLDIR=[directory] ADDLOCAL=[software] REMOVE=[software]
TRANSFORMS=[Name of transform file]/qn
```

Command line Options

Options	Description
/i	(Required) Indicates that MSI will be used to install the DigitalPersona software. It must be followed by the full pathname to the setup.msi file.
/qn	(Optional) Hides the user interface when installing the software on the computer, allowing a "silent install." If used, it is placed at the end of the command line.

Parameters

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

Parameters	Description
INSTALLDIR	(Optional) Specifies the location where the DigitalPersona software should be installed. If a folder is not specified, defaults to: `C:\Program Files\DigitalPersona`
ADDLOCAL	(Optional) Indicates which DigitalPersona features to install by providing one of the values listed below.
REMOVE	(Optional) Indicates which DigitalPersona software features to uninstall by providing one of the values listed below.

Parameters	Description
TRANSFORMS	(Optional) Use the TRANSFORMS parameter to specify a UI language other than U.S. English. Separate multiple transforms with a semicolon. Do not use semicolons within the name of your transform, as the Windows Installer service will interpret those incorrectly.

ADDLOCAL and REMOVE Values

The table below lists the values that may be provided with the `ADDLOCAL` and `REMOVE` parameters and provides a description of each value:

Values	Description
ALL	Installs all DigitalPersona software components and features or removes all of the components and features that are currently installed.
FingerprintEngine	Installs or removes the DigitalPersona Fingerprint Engine.
STS	Installs or removes the DigitalPersona Secure Token Service.
WebAdminConsole	Installs or removes the DigitalPersona Web Administrative Console.
TokenizationEngine	Installs or removes the Biometric Tokenization Engine.

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

- If ADDLOCAL or REMOVE are not specified, msiexec will install all DigitalPersona Workstation features.
- Individual software features cannot be installed unless the `All` value was used with the `ADDLOCAL` parameter first.
- To install DigitalPersona LDS Server for the first time while omitting one or more software features, use `ADDLOCAL=ALL`, followed by the `REMOVE` parameter with each software component you do not want to install separated by a comma. For example;

```
msiexec /i setup.msi ADDLOCAL=ALL REMOVE=STS,WebAdminConsole
```

Published information

The DigitalPersona Server publishes its service using the following properties:

- Service Class Name, DPAltusSvr.
- Service Class GUID, set to {708A50AA-F647-49E8-820A-F3D6BAF02330}.

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

Configuration for use with DigitalPersona LDS Kiosk (Optional)

If your environment will include installations of DigitalPersona LDS Kiosk, you will need to specifically configure the DigitalPersona LDS Server for use with the DigitalPersona LDS Kiosk component.

After completing the procedures described in the preceding pages, follow these instructions for setting up and configuring the DigitalPersona LDS Server and environment for use with DigitalPersona LDS Kiosk.

1. **Optionally, create an OU for each kiosk and assign computers to the kiosk OU.** See *Creating the OU for the Kiosk* below. By default, all computers in the AD domain are treated as a single kiosk. You may want to set up multiple, separate kiosks by using OUs.
2. **Create a Shared Account in Active Directory** and specify the account information either by GPO or on individual kiosk computers. See the topics *Kiosk Shared Account Settings* and *Adding Shared Account Settings Using GPO* below.
3. **Install DigitalPersona LDS Kiosk on computers.** See the *DigitalPersona Kiosk Installation* chapter in the DigitalPersona Client Guide.
4. **Enroll user credentials.** By default, DigitalPersona users are not allowed to enroll their own credentials, as user creation and credential enrollment are handled centrally through the DigitalPersona Attended Enrollment component. For more information, refer to the chapter *DigitalPersona Attended Enrollment* in the DigitalPersona Client Guide.

Configure Kiosk GPO settings

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 the topic *Adding Shared Account Settings Using GPO* below.

Creating the OU for the Kiosk

When you install DigitalPersona LDS Server and DigitalPersona LDS 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 LDS 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 LDS 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 LDS Kiosk to authenticate multiple users while using only one logon session for the Shared Account.

Adding Shared Account Settings Using GPO

The DigitalPersona Kiosk Shared Account setting is provided as part of the GPMC Extensions component of the DigitalPersona Administration Tools, a separate installation available in your DigitalPersona LDS product package.

This setting is located at Computer Configuration/Policies/Software Settings/DigitalPersona Client/Kiosk Administration.

You can use the Group Policy Management Editor to modify these 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.

Password Manager Admin Tool settings

If you plan on using managed logons with DigitalPersona LDS 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 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 the chapter *Policies and Settings* on page *118*. For additional information on managed logons, see the chapter *Password Manager Admin Tool* on page *182*.

Uninstalling DigitalPersona LDS Server

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

When you uninstall the Server software, the published information (described in the topic *Published information* on page 66) is removed.

Separate installations 3

THIS CHAPTER DESCRIBES DIGITALPERSONA COMPONENTS THAT ARE *NOT* AUTOMATICALLY INSTALLED AS PART OF EITHER THE DIGITALPERSONA SERVER OR CLIENT INSTALLATIONS.

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

Components included in the product package

DigitalPersona LDS Administration Tools

The DigitalPersona LDS Administration Tools are part of a separate installation package included in the DigitalPersona product package.

Installation of the LDS Administration Tools is necessary for licensing the DigitalPersona Server. The package also includes the optional User Query Snap-in (used to query user data) and the GPMC/GPOE Extensions (used to manage DigitalPersona policies and settings. Additional information on these tools is provided in a separate chapter, *Administration Tools*, beginning on page *92.* For installation details, see page *41*.

Separate product packages

The following components and modules are separately installed and may required additional licenses depending on the product package purchased.

Web Management Components

The Web Management Components module contains a collection of components that together enable management of a DigitalPersona solution through a web based interface. For installation instructions and complette details, see *Section Three: Web Management* beginning on page *216*.

Password Manager Admin Tool

The Password Manager Admin Tool is used by DigitalPersona 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 182.

DigitalPersona LDS Extended Server Policy Module (ESPM)

The DigitalPersona LDS ESPM adds additional per-user authentication policy settings to the DigitalPersona LDS Administration Console. For a description of these settings, see page 109.

To install the DigitalPersona LDS Extended Server Policy Module

1. Copy the package received from HID Global, your channel partner or reseller to the computer where the DigitalPersona LDS Server is installed.
2. Launch *setup.exe*, and follow the onscreen instructions.

Licensing is included with 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 HID Global 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 HID Global 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:[adminstrator 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/PIC 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.

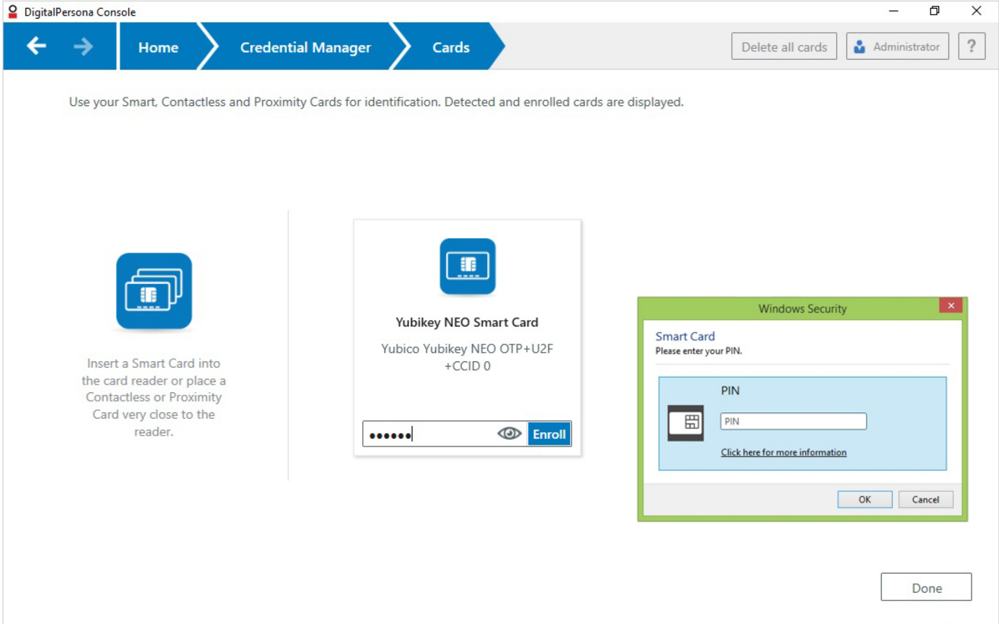
The Minidriver is available through Microsoft Windows Update, or can be downloaded directly from the Yubico website at https://www.yubico.com/support/knowledgebase/categories/downloads/. For additional details about the driver, see the following YubiKey document: https://www.yubico.com/wp-content/uploads/2017/10/YubiKey_Smart_Card_Minidriver_User_Guide_10_2017_R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


DigitalPersona Console
Home
Credential Manager
Cards
Delete all cards
Administrator
?
Use your Smart, Contactless and Proximity Cards for identification. Detected and enrolled cards are displayed.
Insert a Smart Card into the card reader or place a Contactless or Proximity Card very close to the reader.
Yubikey NEO Smart Card
Yubico Yubikey NEO OTP+U2F +CCID 0
••••••
Enroll
Windows Security
Smart Card
Please enter your PIN.
PIN
PIN
Click here for more information
OK
Cancel
Done

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 LDS Administrator Guide includes the following chapters.

Administration overview 5

THIS CHAPTER DESCRIBES THE FEATURES, TOOLS AND UTILITIES PROVIDED BY DIGITALPERSONA LDS TO ASSIST THE ADMINISTRATOR IN MANAGING VARIOUS ASPECTS OF THE PRODUCT, AS WELL AS CUSTOMIZING AND EXPANDING THE FUNCTIONALITY OF THE PRODUCT.

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 LDS Server or DigitalPersona LDS Workstation. Others are available as separate modules, which may be obtained from your HID Global Account Manager or product Reseller.

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

About GPO settings

Many of the settings that govern the features and behavior of the DigitalPersona LDS solution are controlled through Active Directory GPO settings (see *Policies and Settings* on page *118*). Additional settings and behaviors may be configured though Microsoft's ADSI Editor and through custom VBScript scripts.

We strongly recommend managing all DigitalPersona policies through a separate GPO 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 for at the local computer.

For this reason – especially if the needs specific to your environment require you to provide end users with local administrative privileges – HID Global 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.

License Activation & Management 6

THIS CHAPTER DESCRIBES THE FEATURES IN DIGITALPERSONA LDS THAT ARE USED FOR ACTIVATING THE ALTS LDS SERVER.

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 paramaters and flags, as well as a short description of the activation procecss, 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

The following Licensed product options are available for the HID DigitalPersona LDS solution.

DigitalPersona Premium Employee License - Permits the enrollment of user credentials, and subsequent use by a specified number of users. These users may be AD users or Non AD users.

DigitalPersona Customer Facing License - Permits the enrollment of user credentials and subsequent use by a specified number of Non AD users only.

Face authentication - Permits enrollment and use of the Face credential by licensed users.

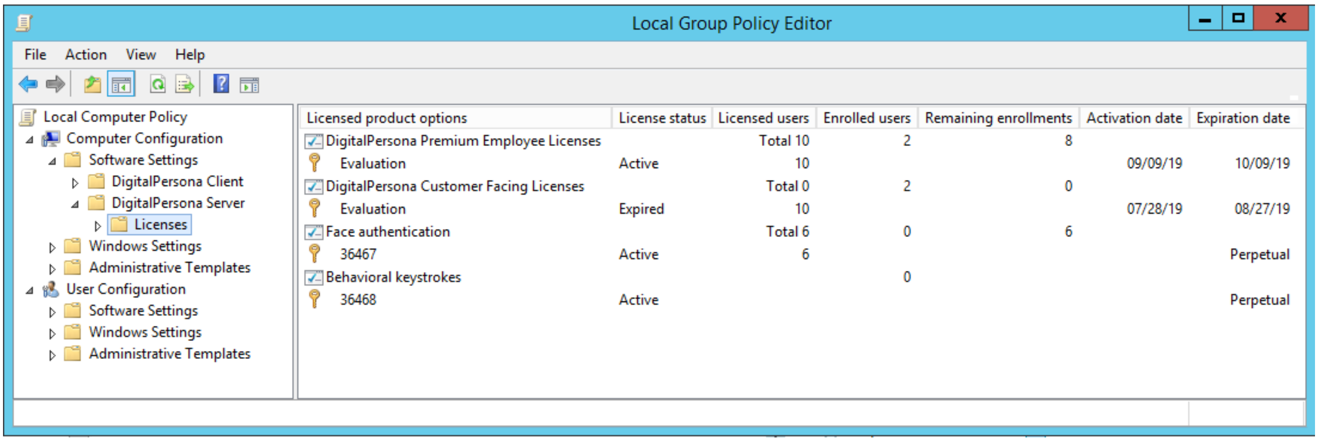
*Behavioral keystroke*s - Permits enrollment and use of the Behavioral keystrokes feature for licensed users.

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.



Licensed product options	License status	Licensed users	Enrolled users	Remaining enrollments	Activation date	Expiration date
☑ DigitalPersona Premium Employee Licenses		Total 10	2	8		
Evaluation	Active	10			09/09/19	10/09/19
☑ DigitalPersona Customer Facing Licenses		Total 0	2	0		
Evaluation	Expired	10			07/28/19	08/27/19
☑ Face authentication		Total 6	0	6		
36467	Active	6				Perpetual
☑ Behavioral keystrokes			0			
36468	Active					Perpetual

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.

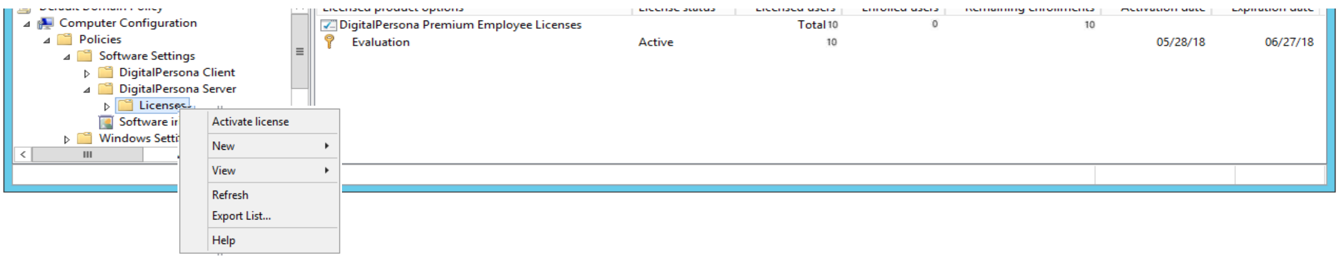
If you need to activate a license for a DigitalPersona Server that is not connected to the internet, see the topic *License activation from another computer* below.

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

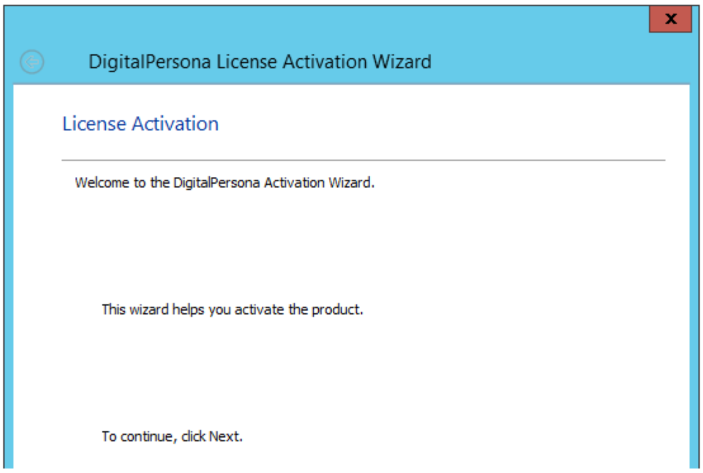
1. In the Group Policy Management Editor, navigate to: *Computer Configuration, Software Settings, DigitalPersona Server, Licenses*.

2. Right-click on *Licenses* and select *Activate license*.



Licensed product options	License status	Licensed users	Enrolled users	Remaining enrollments	Activation date	Expiration date
DigitalPersona Premium Employee Licenses		Total 10	0	10		
Evaluation	Active	10			05/28/18	06/27/18

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



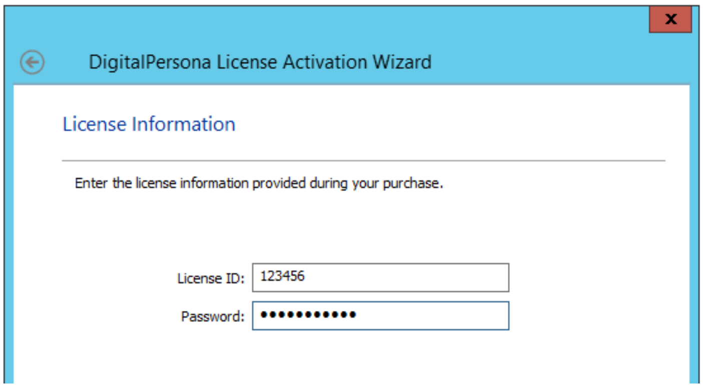
License Activation

Welcome to the DigitalPersona Activation Wizard.

This wizard helps you activate the product.

To continue, click Next.

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



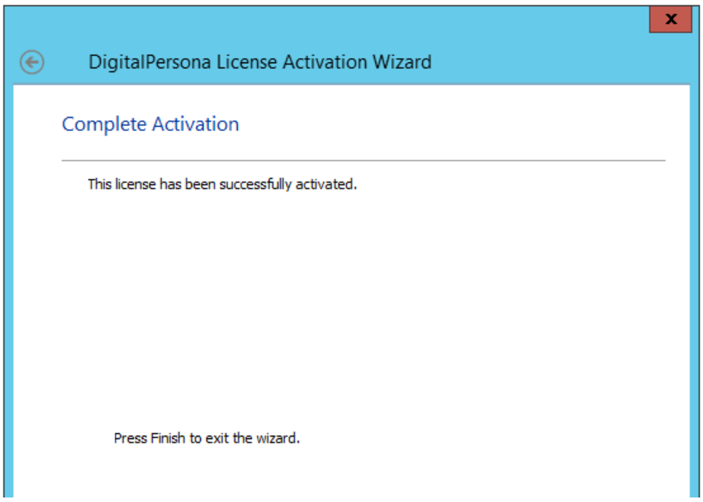
License Information

Enter the license information provided during your purchase.

License ID: 123456

Password: ●●●●●●●●●●●

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



Complete Activation

This license has been successfully activated.

Press Finish to exit the wizard.

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.*

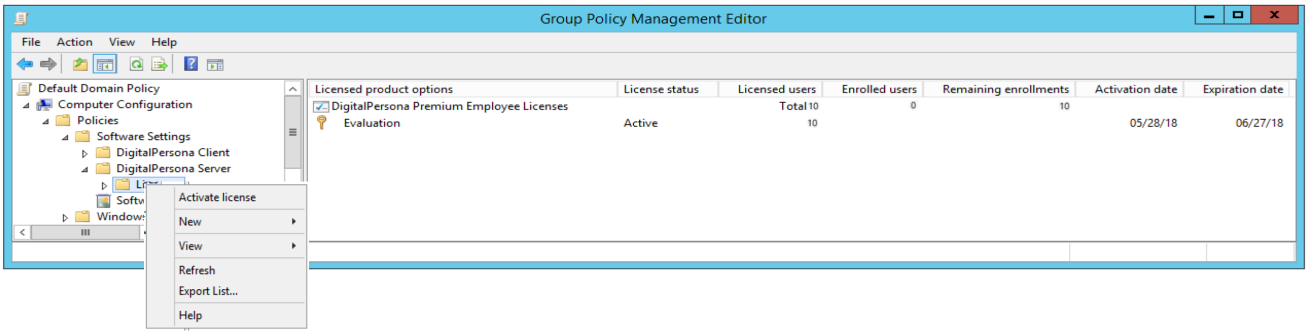
To remotely activate your DigitalPersona license

On your DigitalPersona Server,

1. In the Group Policy Management Editor; navigate to *Computer Configuration, Policies, Software Settings, DigitalPersona Server, Licenses*.

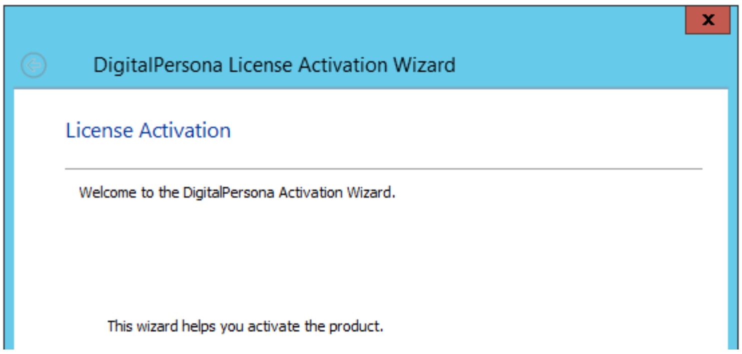
License activation from another computer

2. Right-click on *Licenses* and select *Activate license*.



Licensed product options	License status	Licensed users	Enrolled users	Remaining enrollments	Activation date	Expiration date
DigitalPersona Premium Employee Licenses		Total 10	0	10		
Evaluation	Active	10			05/28/18	06/27/18

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

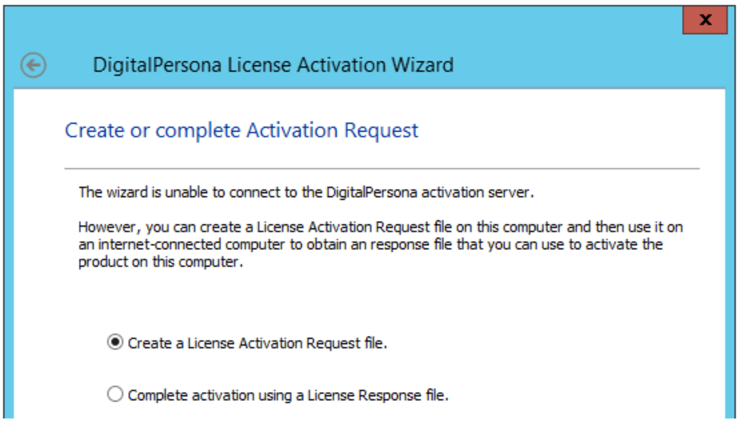


License Activation

Welcome to the DigitalPersona Activation Wizard.

This wizard helps you activate the product.

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



Create or complete Activation Request

The wizard is unable to connect to the DigitalPersona activation server.

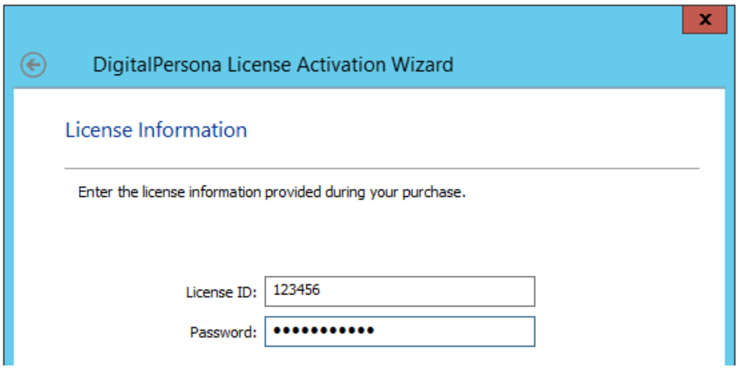
However, you can create a License Activation Request file on this computer and then use it on an internet-connected computer to obtain an response file that you can use to activate the product on this computer.

● Create a License Activation Request file.

○ Complete activation using a License Response file.

License activation from another computer

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



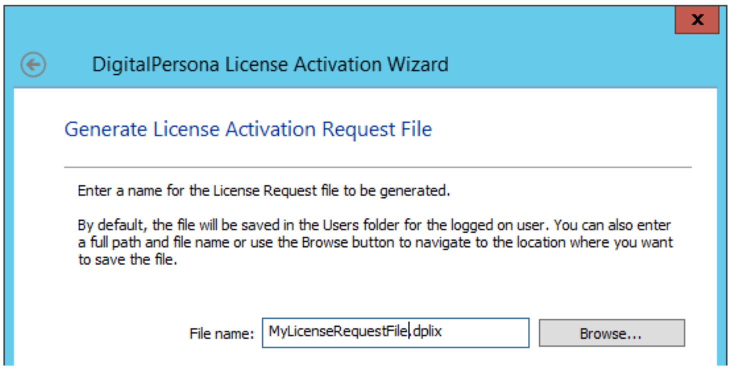
License Information

Enter the license information provided during your purchase.

License ID: 123456

Password: ●●●●●●●●●●●

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



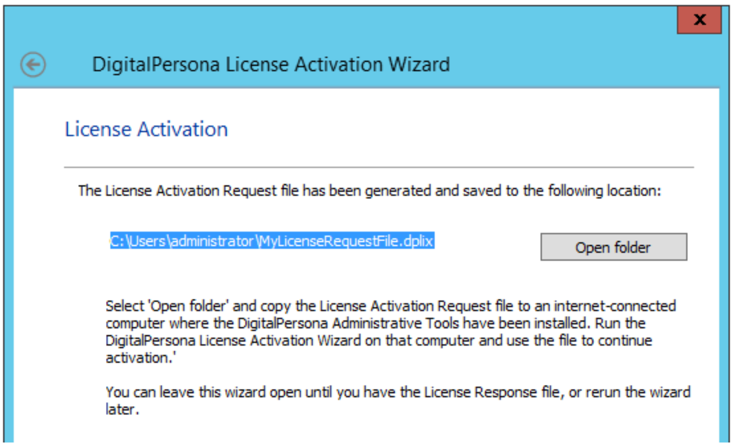
Generate License Activation Request File

Enter a name for the License Request file to be generated.

By default, the file will be saved in the Users folder for 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.

File name: MyLicenseRequestFile.dplix

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.



License Activation

The License Activation Request file has been generated and saved to the following location:

C:\Users\administrator\MyLicenseRequestFile.dplix

Select 'Open folder' and copy the License Activation Request file to an internet-connected computer where the DigitalPersona Administrative Tools have been installed. Run the DigitalPersona License Activation Wizard on that computer and use the file to continue activation.'

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

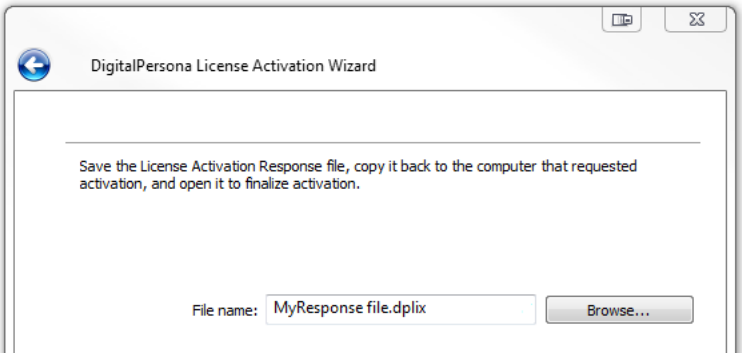
7. Copy the resulting *License Activation Request (.dplix) file* to a shared directory or device that can be accessed from a computer with an internet connection and the DigitalPersona Administrative Tools installed.

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

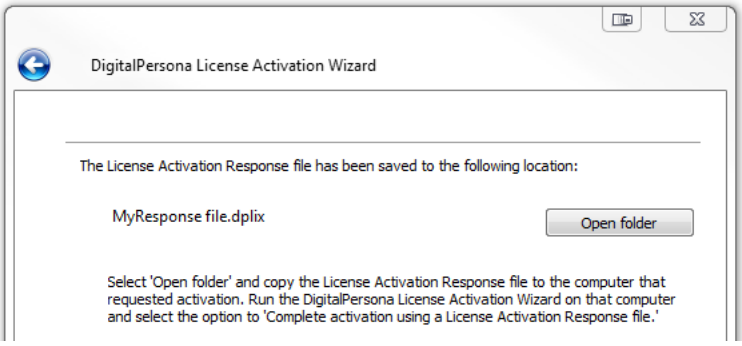


DigitalPersona License Activation Wizard

Save the License Activation Response file, copy it back to the computer that requested activation, and open it to finalize activation.

File name: MyResponse file.dplix

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.



DigitalPersona License Activation Wizard

The License Activation Response file has been saved to the following location:

MyResponse file.dplix

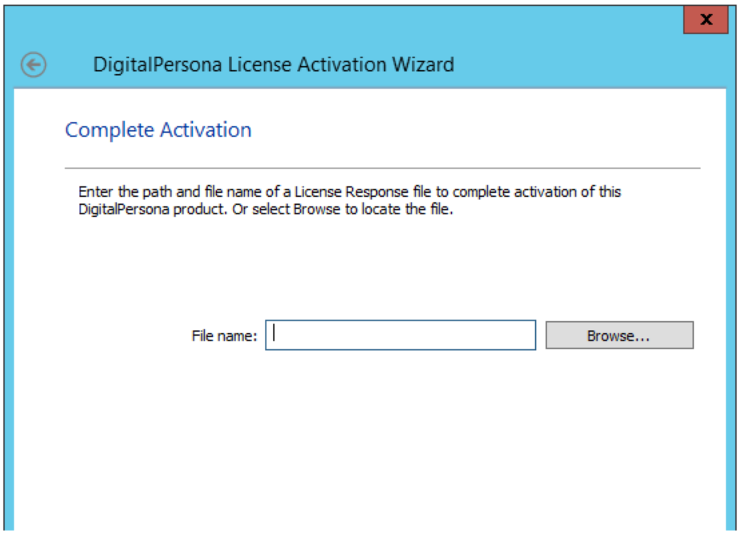
Select 'Open folder' and copy the License Activation Response file to the computer that requested activation. Run the DigitalPersona License Activation Wizard on that computer and select the option to 'Complete activation using a License Activation Response file.'

12. Click *Next* and then click *Finish* to close the wizard.
13. Copy the response file back to the DigitalPersona Server machine.

On the DigitalPersona Server

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

15. 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.



Complete Activation

Enter the path and file name of a License Response file to complete activation of this DigitalPersona product. Or select Browse to locate the file.

File name:

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

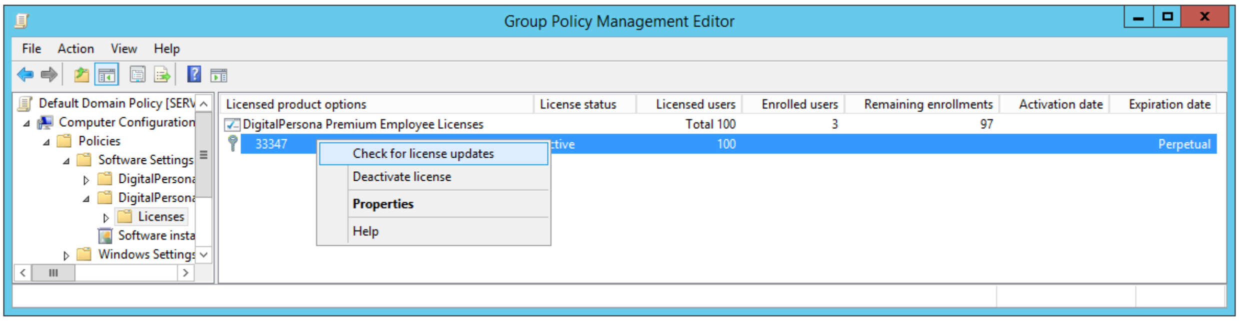
17. Upon successful activation, the final page of the wizard displays. Click *Finish* to close the wizard.

Checking for license updates

To check for updates to your licenses

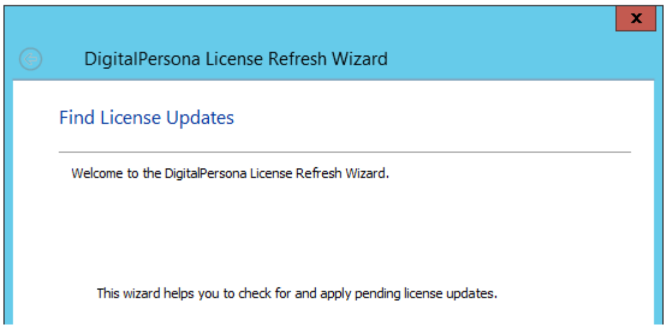
1. In the Group Policy Management Editor; navigate to *Computer Configuration, Policies, Software Settings, DigitalPersona Server, Licenses*.

2. Right-click on a license and select *Check for license updates*.



Licensed product options	License status	Licensed users	Enrolled users	Remaining enrollments	Activation date	Expiration date
DigitalPersona Premium Employee Licenses		Total 100	3	97		
33347	ctive	100				Perpetual

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

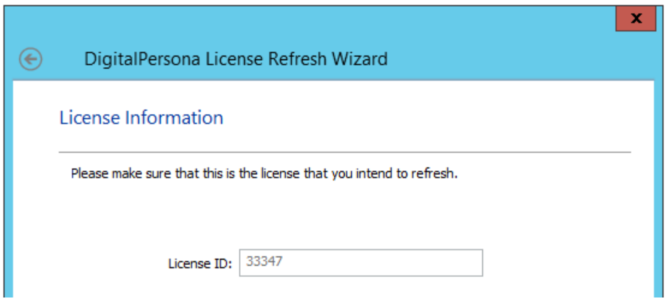


Find License Updates

Welcome to the DigitalPersona License Refresh Wizard.

This wizard helps you to check for and apply pending license updates.

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

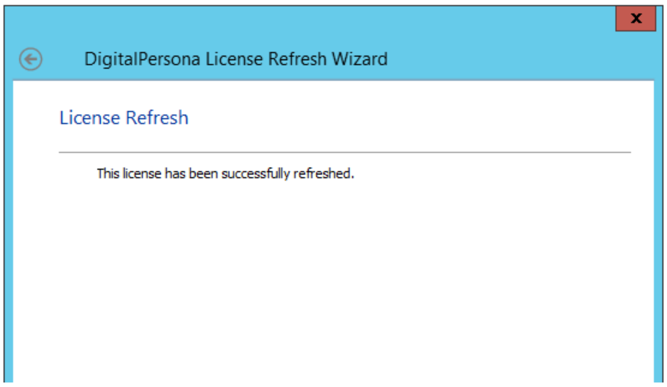


License Information

Please make sure that this is the license that you intend to refresh.

License ID: 33347

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

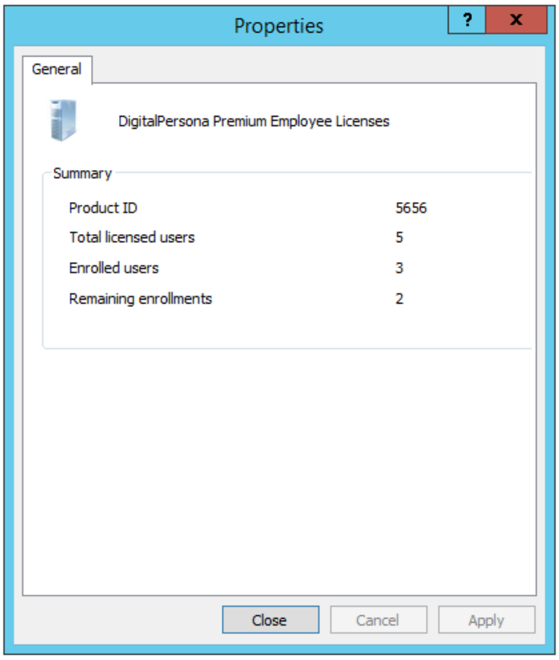


License Refresh

This license has been successfully refreshed.

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*.

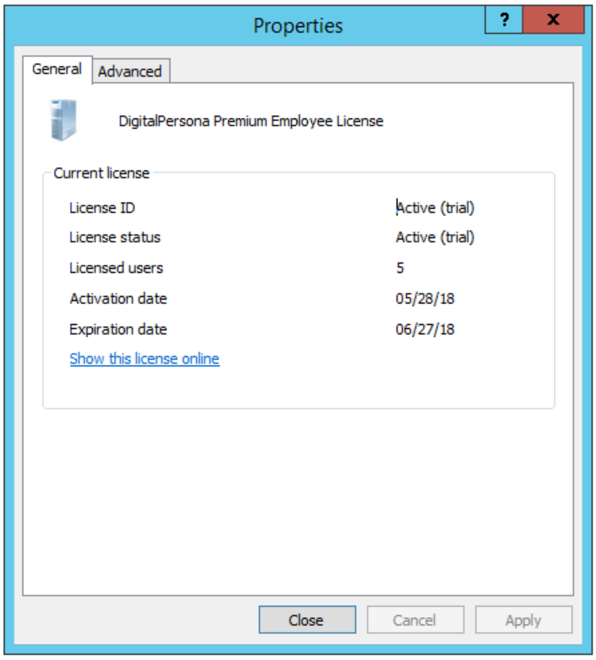


DigitalPersona Premium Employee Licenses

Summary

Product ID	5656
Total licensed users	5
Enrolled users	3
Remaining enrollments	2

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



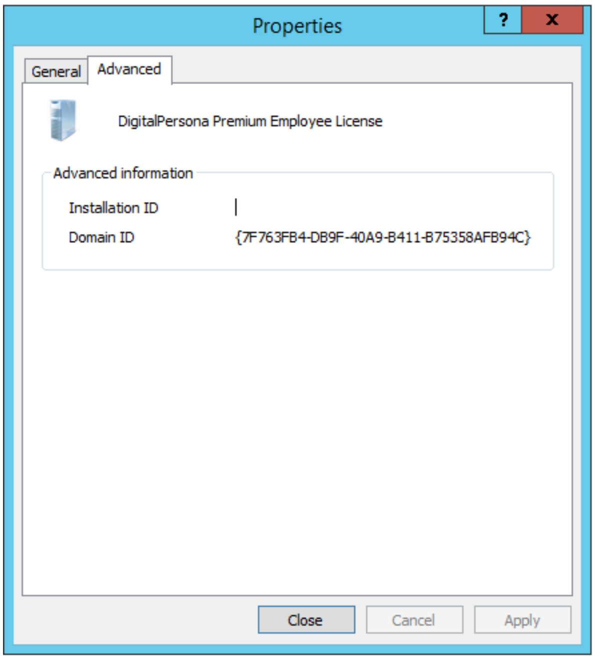
DigitalPersona Premium Employee License

Current license

License ID	Active (trial)
License status	Active (trial)
Licensed users	5
Activation date	05/28/18
Expiration date	06/27/18

Show this license online

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



DigitalPersona Premium Employee License

Advanced information

Installation ID

Domain ID {7F763FB4-DB9F-40A9-B411-B75358AFB94C}

License deactivation

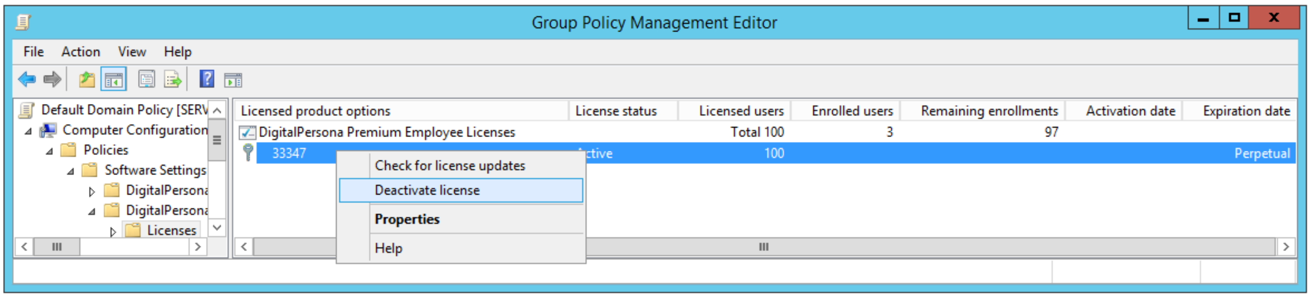
Your DigitalPersona license may be deactivated through the *DigitalPersona Deactivation Wizard*, launched through the Active Directory Group Policy Management Editor on the computer where the DigitalPersona Server is installed.

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

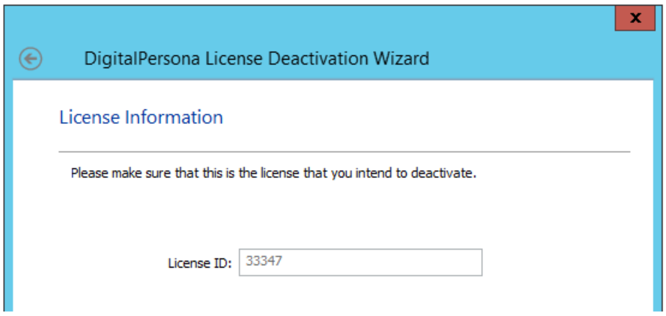
1. In MMC, navigate to: *Computer Configuration, Software Settings, DigitalPersona Server, Licenses*.
2. Right-click on *Licenses* and select *Deactivate license*.



Licensed product options	License status	Licensed users	Enrolled users	Remaining enrollments	Activation date	Expiration date
DigitalPersona Premium Employee Licenses		Total 100	3	97		
33347	ctive	100				Perpetual

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

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

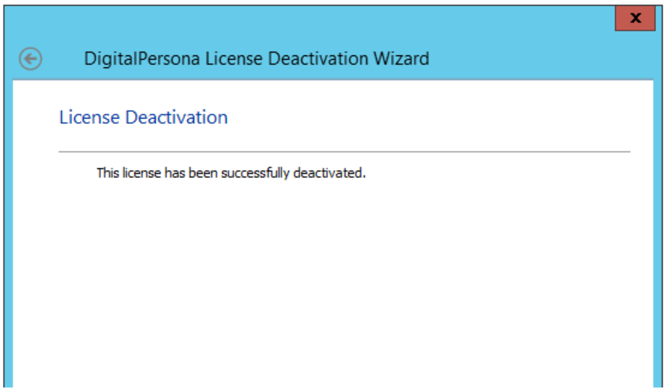


License Information

Please make sure that this is the license that you intend to deactivate.

License ID: 33347

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



License Deactivation

This license has been successfully deactivated.

License deactivation from another computer

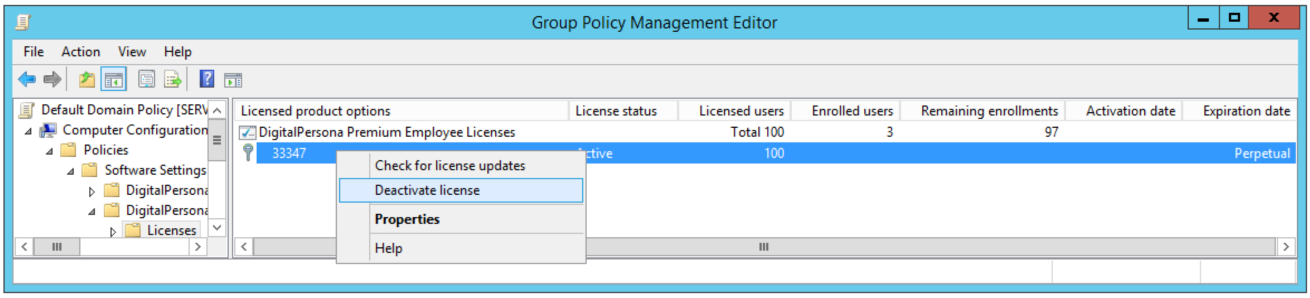
If your DigitalPersona Server does not have access to the internet, you can deactivate it remotely through the use of any computer that has internet access. *Installation of the Group Management Console and the DigitalPersona Administration Tools are required on the machine.*

To remotely deactivate your DigitalPersona license

On your DigitalPersona Server,

1. In the Group Policy Management Editor, navigate to *Computer Configuration, Policies, Software Settings, DigitalPersona Server, Licenses*.

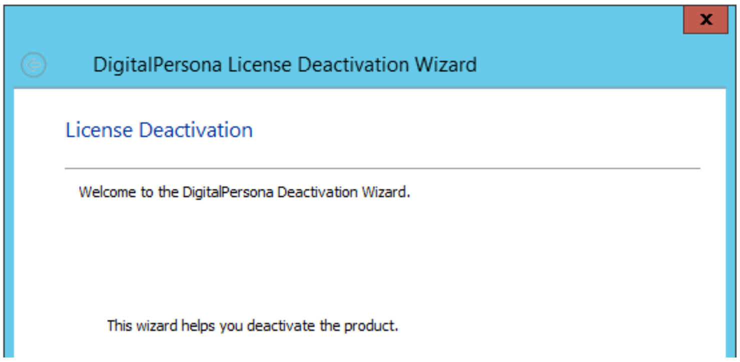
2. Right-click on *Licenses* and select *Deactivate license*.



Licensed product options	License status	Licensed users	Enrolled users	Remaining enrollments	Activation date	Expiration date
☑ DigitalPersona Premium Employee Licenses		Total 100	3	97		
33347	ctive	100				Perpetual

License deactivation from another computer

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



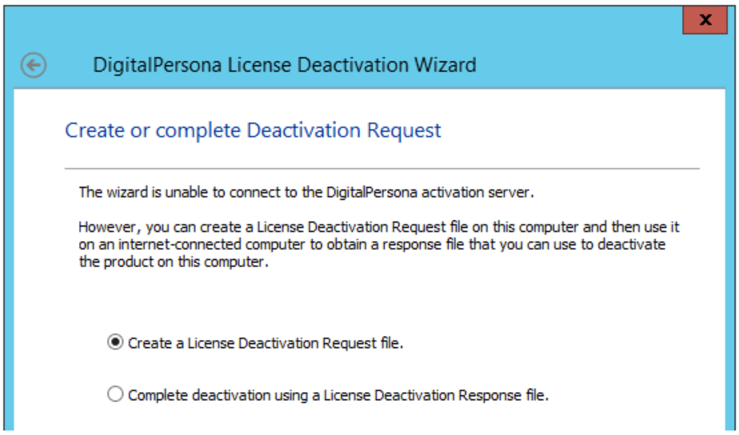
DigitalPersona License Deactivation Wizard

License Deactivation

Welcome to the DigitalPersona Deactivation Wizard.

This wizard helps you deactivate the product.

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



DigitalPersona License Deactivation Wizard

Create or complete Deactivation Request

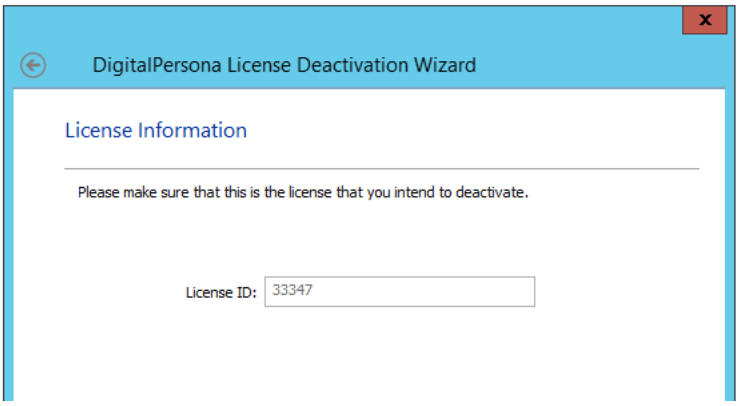
The wizard is unable to connect to the DigitalPersona activation server.

However, you can create a License Deactivation Request file on this computer and then use it on an internet-connected computer to obtain a response file that you can use to deactivate the product on this computer.

● Create a License Deactivation Request file.

○ Complete deactivation using a License Deactivation Response file.

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



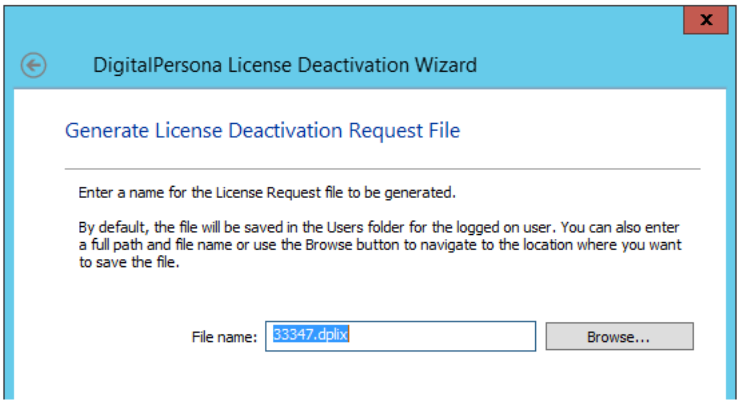
DigitalPersona License Deactivation Wizard

License Information

Please make sure that this is the license that you intend to deactivate.

License ID: 33347

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



DigitalPersona License Deactivation Wizard

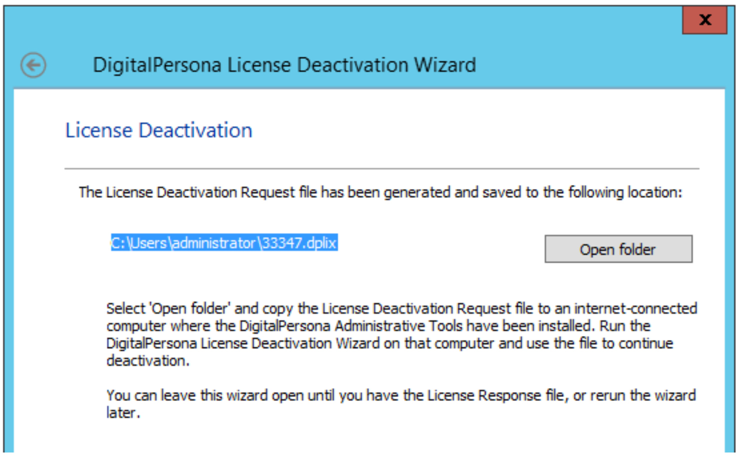
Generate License Deactivation Request File

Enter a name for the License Request file to be generated.

By default, the file will be saved in the Users folder for 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.

File name: 33347.dplix

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.



DigitalPersona License Deactivation Wizard

License Deactivation

The License Deactivation Request file has been generated and saved to the following location:

C:\Users\administrator\33347.dplix

Select 'Open folder' and copy the License Deactivation Request file to an internet-connected computer where the DigitalPersona Administrative Tools have been installed. Run the DigitalPersona License Deactivation Wizard on that computer and use the file to continue deactivation.

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

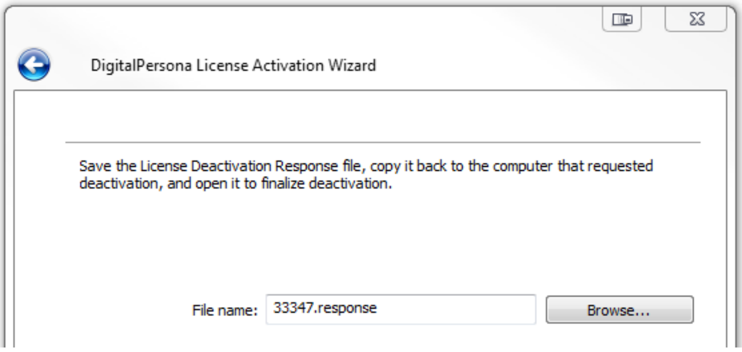
7. Copy the resulting *License Deactivation Request (.dplix) file* to a shared directory or device that can be accessed from a computer with an internet connection and the DigitalPersona Administrative Tools installed.

   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*.

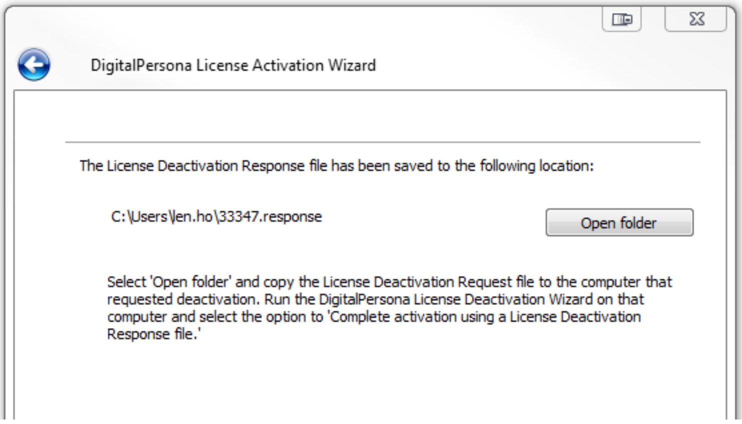


DigitalPersona License Activation Wizard

Save the License Deactivation Response file, copy it back to the computer that requested deactivation, and open it to finalize deactivation.

File name: 33347.response

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.



DigitalPersona License Activation Wizard

The License Deactivation Response file has been saved to the following location:

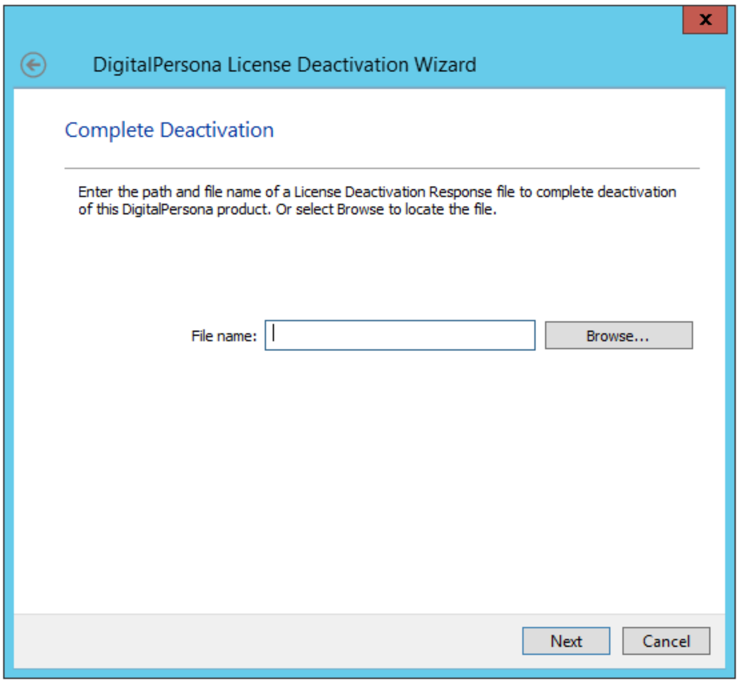
C:\Users\jen.ho\33347.response

Select 'Open folder' and copy the License Deactivation Request file to the computer that requested deactivation. Run the DigitalPersona License Deactivation Wizard on that computer and select the option to 'Complete activation using a License Deactivation Response 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. The click *Next*.



Complete Deactivation

Enter the path and file name of a License Deactivation Response file to complete deactivation of this DigitalPersona product. Or select Browse to locate the file.

File name:

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.

Administration Tools 7

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

Overview

The DigitalPersona LDS Administration Tools includes the following components, which are installed by default through the installation wizard.

- The DigitalPersona *GPMC/GPOE Extensions* and the *User Query Tool* ADUC snap-ins may be deselected during installation by choosing a Custom install.
- The *Hardware Token Management Utility* is not shown in the Custom installation dialog and cannot be deselected.

Additional DigitalPersona LDS administrative functions are implemented through the use of VBScript. These scripts are automatically copied to your computer during installation of the DigitalPersona LDS Administration Tools. Finally, the ADSI Edit tool can be used to directly configure certain attributes in the DigitalPersona database.

User Query Snap-in

The DigitalPersona User Query Snap-in is a component within the DigitalPersona Administration Tools. These tools are a separate installation and are located in the DigitalPersona LDS Administration Tools folder of your product package. This tool provides a means for the administrator to query the DigitalPersona user database for information about DigitalPersona 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 93)
- Interactive dialog-based application (page 96)
- Command line utility (page 98)

The User Query Tool can only be successfully run on the computer where DigitalPersona LDS Server is installed. Once installed, the Interactive dialog-based application can be run from the Start menu by selecting 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, such as:

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

The DigitalPersona 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
   {
   [propget, id(1), helpstring("Returns number of licenses installed.")]
      HRESULT NumberOfLicensesInstalled([out, retval] LONG* pVal);
   [propget, 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

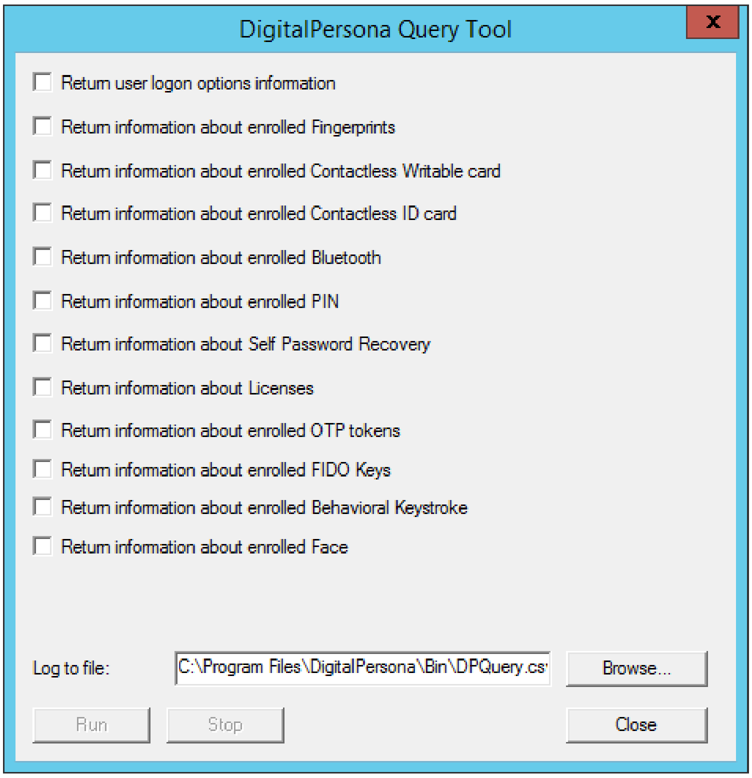
This is a sample of a VB script that returns the date and time of the first and last fingerprint enrollments for a user.

```
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. On the Start menu, point to ***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.



□ Return user logon options information

□ Return information about enrolled Fingerprints

□ Return information about enrolled Contactless Writable card

□ Return information about enrolled Contactless ID card

□ Return information about enrolled Bluetooth

□ Return information about enrolled PIN

□ Return information about Self Password Recovery

□ Return information about Licenses

□ Return information about enrolled OTP tokens

□ Return information about enrolled FIDO Keys

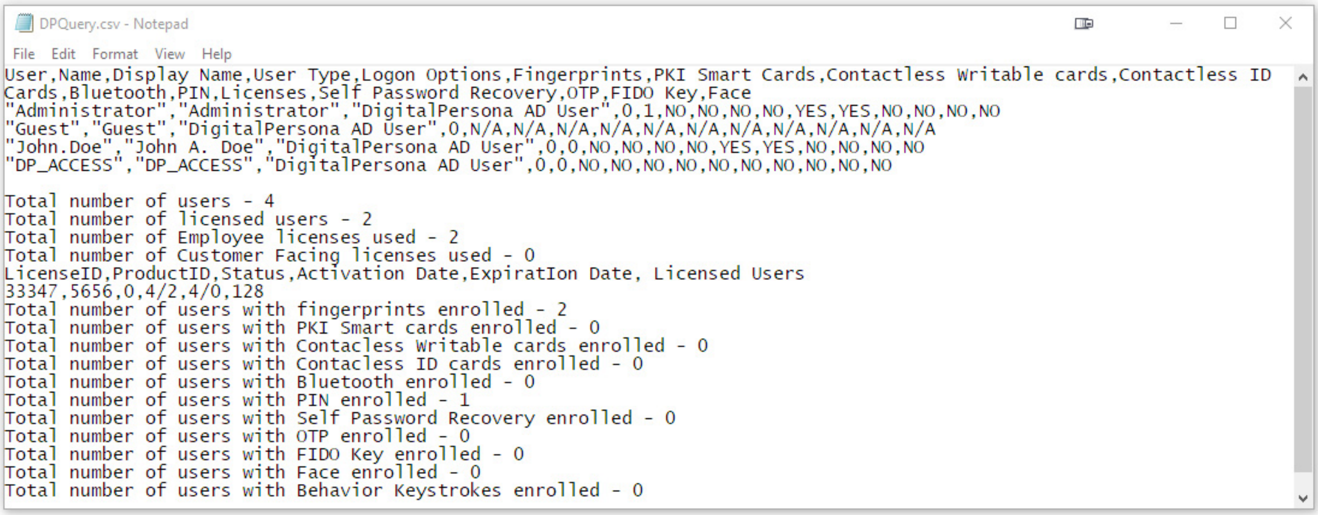
□ Return information about enrolled Behavioral Keystroke

□ Return information about enrolled Face

Log to file: C:\Program Files\DigitalPersona\Bin\DPQuery.cs

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 following table.



```
User,Name,Display Name,User Type,Logon Options,Fingerprints,PKI Smart Cards,Contactless Writable cards,Contactless ID
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,N/A,N/A,N/A,N/A,N/A,N/A
"John.Doe","John A. Doe","DigitalPersona AD User",0,0,NO,NO,NO,NO,YES,YES,NO,NO,NO,NO
"DP_ACCESS","DP_ACCESS","DigitalPersona AD User",0,0,NO,NO,NO,NO,NO,NO,NO,NO,NO,NO

Total number of users - 4
Total number of licensed users - 2
Total number of Employee licenses used - 2
Total number of Customer Facing licenses used - 0
LicenseID,ProductID,Status,Activation Date,ExpiratIon Date, Licensed Users
33347,5656,0,4/2,4/0,128
Total number of users with fingerprints enrolled - 2
Total number of users with PKI Smart cards enrolled - 0
Total number of users with Contacless Writable cards enrolled - 0
Total number of users with Contacless ID cards enrolled - 0
Total number of users with Bluetooth enrolled - 0
Total number of users with PIN enrolled - 1
Total number of users with Self Password Recovery enrolled - 0
Total number of users with OTP enrolled - 0
Total number of users with FIDO Key enrolled - 0
Total number of users with Face enrolled - 0
Total number of users with Behavior Keystrokes 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 Standard.
Logon Options	0 - No log on 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.
Contactless Writable cards	Yes or No. Indicates whether this credential has been enrolled by the specified user.
Contactless ID 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.

Column	Description
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 Contactless Writable cards enrolled

Total number of users with Contactless ID 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 *[Installation path\Bin]DPQuery.exe* using the following syntax and parameters. (The default location is C:\Program Files\DigitalPersona\Bin.

Syntax

```
DPQuery.exe [-noui] [-dn=”BaseDN”] [-out=”FileName”] [-ac] [-fp] [-cw] [-ci] [-bt]
[-pin] [-lic] [-rec]
```

Parameters

Parameter	Description
-noui	Run utility silently with no graphical interface, writing results to the DPQuery.csv file 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 96 displays.
-dn= “BaseDN”	Sets the Distinguished Name of the search base for the query. If this parameter is not present, the query runs against all users. • *Non AD users* - To query DigitalPersona Non AD users only, copy and modify the string found in the AzMan.txt file created during the DigitalPersona LDS installation. The AzMan.txt file is located in the [Installation path]Bin folder, where the default location would be “C:\Program Files\DigitalPersona\Bin.” The AzMan text string will be similar to the following: MSLDAP://127.0.0.1:50000/CN=Authorization Store,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US Remove the *MS* from the front of the string and replace the words *Authorization Store* with *AltusUsers*. • AD users - To query DigitalPersona AD users only, copy and modify the AzMan.txt string as follows. Remove the *MS* from the front of the string and replace the words *Authorization Store* with *AltusAD Users*. • Other user groups - To query other user groups that may have been created, copy and modify the AzMan.txt string as follows. Remove the *MS* from the front of the string and replace the words *Authorization Store* with the name of the group. To determine the exact name of any additional groups, you can use ADSI Edit to connect to the AD LDS instance.
-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.
-cw	Add information about Contactless Writable cards enrolled for each user in a query.
-ci	Add information about Contactless ID 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.
-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.

Parameter	Description
-face	Add information about Face credentials enrolled for each user in a query.

Examples

Show the User Interface (interactive dialog) for selecting query parameters.

DPQuery.exe

Do not use the UI, but report license information for all users

```
DPQuery.exe -noui -lic
```

Report license information and fingerprints enrolled for Non AD users only.

```
DPQuery.exe -noui -dn="LDAP://127.0.0.1:50000/CN= Altus Users,CN={893B81EE-7764-44FF-
8561-8377580B9B03},O=DigitalPersona,C=US" -lic -fp
```

Report information about Bluetooth credentials enrolled for AD users only.

DPQuery.exe -noui -dn="LDAP://127.0.0.1:50000/CN= Altus AD Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US" -bt

GPMC Extensions

DigitalPersona Server and its associated 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 chapters, *GPMC/GPOE Extensions* beginning on page *111* and *Policies and Settings* beginning on page *118*.

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.

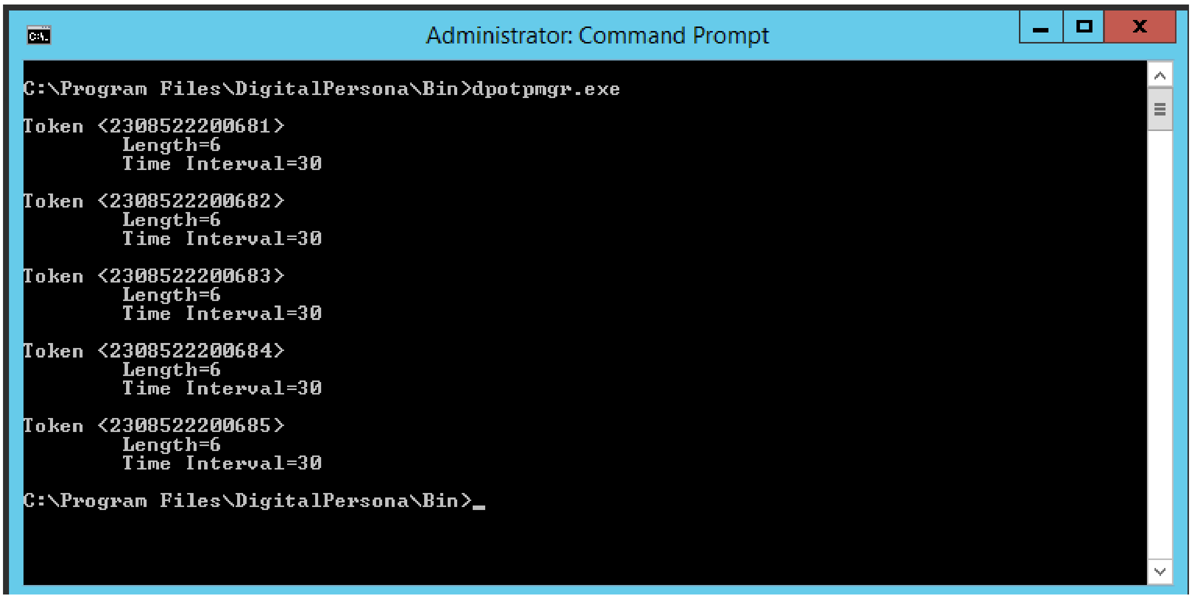
Examples

```
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.



```
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.

DigitalPersona LDS Administration Scripts

Some of the DigitalPersona LDS administrative functions are implemented through the use of VBScript. These scripts are automatically copied to your computer during installation of the DigitalPersona LDS Administration Tools.

By default, they will be located in the following directory on the target computer.

Program Files\DigitalPersona\Altus Administration Tools\Scripts

If a previous DigitalPersona product has been installed on the computer, scripts will be copied to

[Install Directory]DigitalPersona\Altus Administration Tools\Scripts

The available scripts are:

- CountUtilizedLicenses
- CreateUserList
- DeleteCredentials*
- DeleteUserList
- FP+Pwd (Fingerprint plus Password)*
- RandomizePassword*
- UnlockAccount*

* Scripts designated by asterisks in the above list use text files (.csv) to input parameters to the scripts. These text files have the same name as the script with “UserList” added to the script name and a .csv extension. They require previous installation of the Microsoft Access Database Engine 2010 Redistributable in order to process the scripts. It is available for free download from the following web page.

http://www.microsoft.com/en-us/download/details.aspx?id=13255

CSV files

Each CSV file has a heading on the first line, “name.” This should not be changed. The names of users to be processed by the script are then listed, one to each line.

The user name listed must be the exact user names as shown in the DigitalPersona LDS database. These can be viewed and verified through the Microsoft ADSI Edit tool (see page 105).

Running the scripts

- Run a script by double-clicking on it, or from a command prompt, for example:
  cscript CountUtilizedLicenses.vbs
- You can also choose to output any script results to a text file, for example:
  cscript CountUtilizedLicenses.vbs >> results.txt

The purpose and use of each script is explained in the following text.

CountUtilizedLicenses

This script counts the number of utilized DigitalPersona LDS licenses, i.e. every user from either Active Directory or AD LDS consumes one license.

Requires Microsoft Access Database Engine 2010 Redistributable.

Instructions

- In the CountUtilizedLicenses file, under the Constants section,

  Verify the server name and port specified for the constant C_Server. If you are unsure of the correct information, you can find it in the file AzMan.txt, located (based on default installation) at

  Program Files\DigitalPersona\Bin\AzMan.txt

CreateUserList

This script creates a list of users specified in the CreateUserList.csv file.

DeleteCredentials

This script deletes credentials for those users specified in the DeleteCredentials.csv file.

Requires Microsoft Access Database Engine 2010 Redistributable.

Instructions

1. In the DeleteCredentials.vbs file, under the Constants section,

   - Verify the server name and port specified for the constant, C_Server. If you are unsure of the correct information, you can find it in the file AzMan.txt, located (based on default installation) at

     Program Files\DigitalPersona\Bin\AzMan.txt

   - Find the GUID for the credential that you want to delete and copy it to the DeleteToken parameter “guidCredential.”

2. Under the Setup section,

   - Verify the location of the associated DeleteCredentialsUserList.csv file and revise the *strCSVFolder* string as necessary.

3. In the associated *text file*, DeleteCredentials.cvs, list the user names whose specified credentials are to be deleted.

Note that only one credential may be specified and deleted at a time. To delete an additional credential for the same list of users, simply change the “guid credential” parameter and run the script again.

DeleteUserList

This script creates a list of users specified in the CreateUserList.csv file.

FP+Pwd

This script sets the “User must user Windows Password and Fingerprint to logon” flag for all users specified in the associated .csv file.

Requires Microsoft Access Database Engine 2010 Redistributable.

Instructions

1. In the Fp+Pwd.vbs file, under the Setup section, edit the following variables.

   - strSearchAttribute - Enter the Active Directory attribute that is to be used to match rows in the CSV file to Active Directory user accounts. You should make sure to use unique attributes, e.g. sAMAccountName (Pre Windows 2000 Login) or userPrincipalName.

     Other attributes can be used but are not guaranteed to be unique. If multiple user accounts are found, an error is returned and no update is performed.

   - strCSVFolder - Enter (or leave as default) the folder where the associated .csv file is located.
   - strCSVFile - Enter (or leave as default) the name of the associated .csv file.

2. Run this script from a command prompt in cscript mode, e.g. cscript Fp+Pwd.vbs or cscript Fp+Pwd.vbs >> results.txt to output the results to a text file.

RandomizePassword

This script sets the Randomize user’s Windows password and “User must change password at next logon” flags for all users specified in the associated .csv file.

To force the specified users to change their passwords on their next logon the *Password never expires* flag should not be set.

Requires Microsoft Access Database Engine 2010 Redistributable.

Instructions

1. In the DeleteCredentials.vbs file, under the Constants section,

   - Verify the server name and port specified for the constant, C_Server. If you are unsure of the correct information, you can find it in the file AzMan.txt, located (based on default installation) at

     Program Files\DigitalPersona\Bin\AzMan.txt

2. Under the Setup section,

- Verify the location of the associated RandomizePasswordUserList.csv file and revise the *strCSVFolder* string as necessary.

3. In the associated *text file*, RandomizePassword.cvs, list the user names whose passwords are to be randomized.

UnlockAccount

This script removes the lock preventing the use of a fingerprint credential or DigitalPersona password for authentication, for any users specified in the associated .csv file.

Requires Microsoft Access Database Engine 2010 Redistributable.

Instructions

1. In the DeleteCredentials.vbs file, under the Constants section,

   - Verify the server name and port specified for the constant, C_Server. If you are unsure of the correct information, you can find it in the file AzMan.txt, located (based on default installation) at

     Program Files\DigitalPersona\Bin\AzMan.txt

2. Under the Setup section,

   - Verify the location of the associated UnlockAccountUserList.csv file and revise the *strCSVFolder* string as necessary.

3. In the associated *text file*, UnlockAccountUserList.cvs, list the user names whose accounts are to be unlocked.

XML Configuration

Some of the DigitalPersona LDS components can be extensively customized through the use of XML files included with the components. These components are:

- DigitalPersona Console
- DigitalPersona Attended Enrollment

For full descriptions of these features, their syntax and parameters, see the following files.

- DPClientConsole.exe.xml
- DPAttendedEnrollment.exe.xml

The files will be located in the Bin subdirectory within the folder where the DigitalPersona LDS component was installed. By default, this is C:\Program Files (x86)\DigitalPersona\Bin.

Examples of the type of customization available through these files are:

- Password Randomization
- Authentication Rules & Policies
- User Sources
- Pages shown
- Custom page elements

ADSI Edit tool

Further administrative tasks may be accomplished by viewing and directly editing DigitalPersona LDAP database user attributes with the Active Directory Service Interfaces Editor (ADSI Edit).

ADSI Edit tool

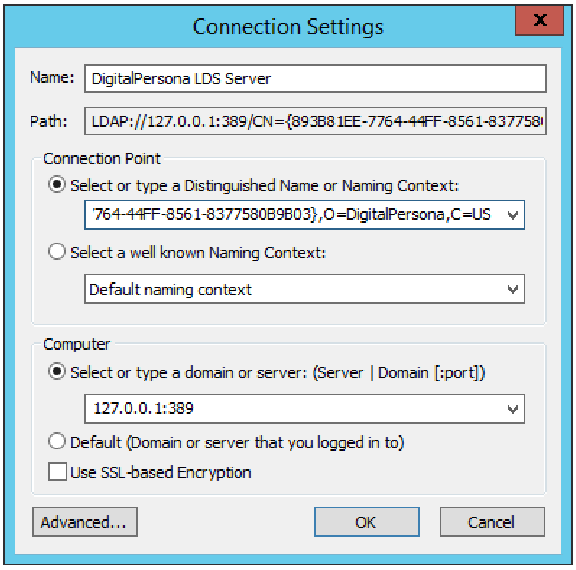
ADSI Edit (Adsiedit.msc) is an MMC snap-in. You can add the snap-in to any .msc file through the Add/Remove Snap-in menu option in MMC, or launch it by entering adsiedit.msc file in the command window.

You can run ADSI Edit from a client computer or server. The computer does not have to be a member of a domain. However, to see domain objects using Adsiedit.msc, you must have the snap-in to view the Active Directory domain that you connect to.

By default, members of the Domain Users group have this snap-in. To modify objects using ADSIEdit, you must have at least the Edit permission on the Active Directory objects that you want to change. By default, members of the Domain Admins group have this permission.

To access the DigitalPersona LDS database from the ADSI Edit tool

1. Launch ADSI Edit (as described above).
2. In the ADSI Edit window, right-click ADSI Edit and select *Connect to* ... to open the Connection Settings dialog.



Connection Settings

Name: DigitalPersona LDS Server

Path: LDAP://127.0.0.1:389/CN={893B81EE-7764-44FF-8561-837758

Connection Point

● Select or type a Distinguished Name or Naming Context:

764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US

○ Select a well known Naming Context:

Default naming context

Computer

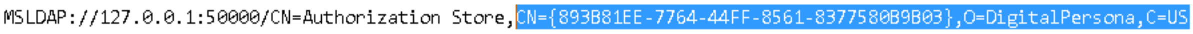
● Select or type a domain or server: (Server | Domain [:port])

127.0.0.1:389

○ Default (Domain or server that you logged in to)

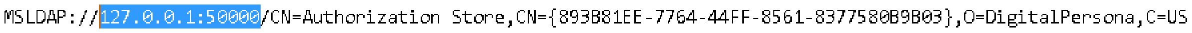
□ Use SSL-based Encryption

3. In the Connection Settings dialog, enter the Distinguished Name for the LDAP object that you want to connect to.You can copy the Distinguished Name from the Azman.txt file created during the installation of DigitalPersona LDS Server. This will be the part of the file content highlighted in the illustration below.



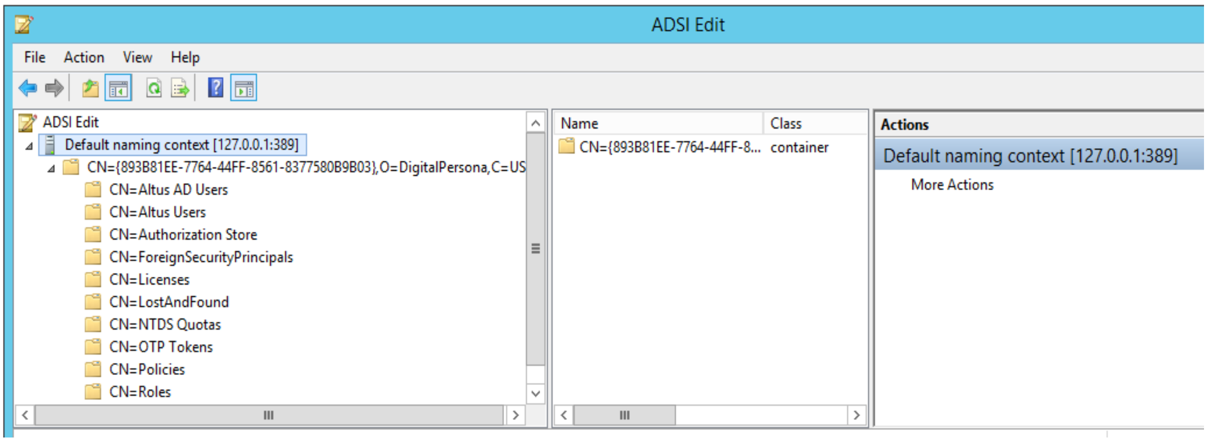
```
MSLDAP://127.0.0.1:50000/CN=Authorization Store,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US
```

4. Also enter the IP Address and port of the computer where your DigitalPersona LDS Server is installed. This too can be found in the Azman.txt file, as follows. Then click *OK*.



```
MSLDAP://127.0.0.1:50000/CN=Authorization Store,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US
```

5. Once connected to the DigitalPersona AD LDS database, ADSI Edit should appear populated similar to the illustration below.



The DigitalPersona LDS attributes are as follows.

- dpAccountName - (Altus User) Name of the DigitalPersona account, i.e. DigitalPersona user name.
- dpLockoutTime - 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.
- dpOmitReasons - A multivalued attribute containing any reasons entered by a Security Officer for omitting credentials during the enrollment process.
- dpUserAccountControl - Specifies the flags to control fingerprint credentials behavior for the user.
- dpUserCredentialsData - Stores fingerprint registration templates for the user.
- dpUserPayload - Stores the user’s unified key data.
- dpUserPublicKey - Stores the user’s public key.
- dpUserRecoveryKey - The user’s recovery key.

To create a user-based logon policy through ADSI Edit

1. Connect to the DigitalPersona database (see steps 1-5 above if not already connected).

2. Right-click on a specific user and select *Properties*.

3. Select *dpUserAccountControl* and click *Edit*.

4. The displayed value should be one of the following numbers.

0 - No log on 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.

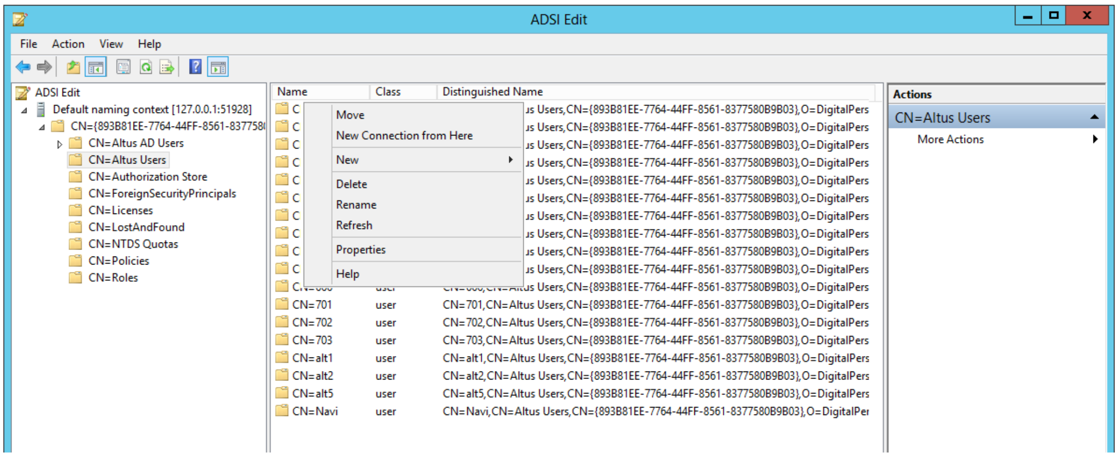
8 - Account is locked out from use of fingerprints credentials. Note that this is *not* used to lock the account, but only to indicate that if this value is displayed that the account has been programmatically locked for some reason. To unlock the account, change the value to one of the other provided values.

To delete DigitalPersona Non AD users through ADSI Edit

1. Connect to the DigitalPersona database (see steps 1-5 above).

2. Select the *Altus Users* object.

3. Click on any users you want to delete and select *Delete* from the context menu.



Name	Class	Distinguished Name
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
C		us Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
CN=701	user	CN=701,CN=Altus Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
CN=702	user	CN=702,CN=Altus Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
CN=703	user	CN=703,CN=Altus Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
CN=alt1	user	CN=alt1,CN=Altus Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
CN=alt2	user	CN=alt2,CN=Altus Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
CN=alt5	user	CN=alt5,CN=Altus Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPers
CN=Navi	user	CN=Navi,CN=Altus Users,CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPer

Extended Server Policy Module 8

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

The DigitalPersona LDS Extended Server Policy Module (ESPM) is a separately purchased and installed server module that adds additional per user policies configurable through the *Set policy* dialog from within the DigitalPersona Web Administration Console.

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 Set Policy dialog.

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.

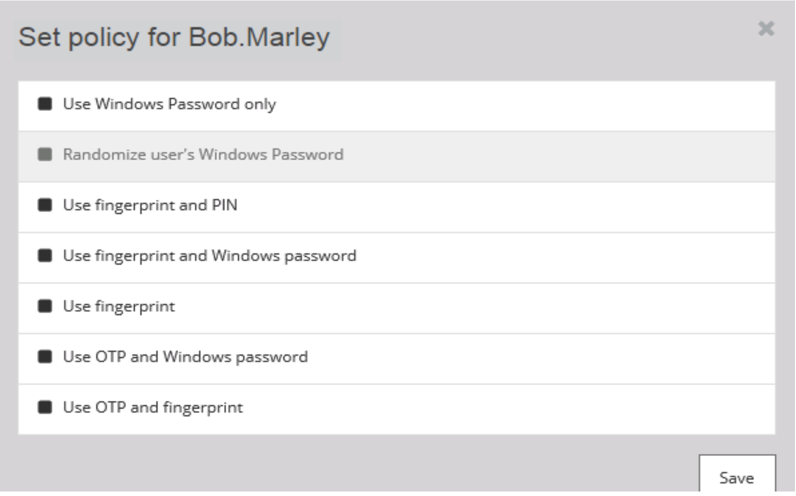
- Use fingerprint and Windows Password

  The user must verify their identity with their fingerprint credential in addition to Windows authentication (a PKI 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.



Set policy for Bob.Marley

- ■ Use Windows Password only
- ■ Randomize user's Windows Password
- ■ Use fingerprint and PIN
- ■ Use fingerprint and Windows password
- ■ Use fingerprint
- ■ Use OTP and Windows password
- ■ Use OTP and fingerprint

GPMC/GPOE Extensions 9

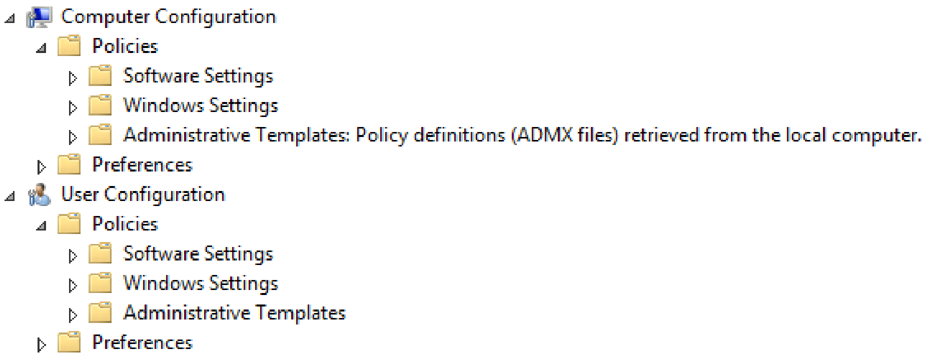
THIS CHAPTER DESCRIBES DIGITALPERSONA EXTENSIONS TO THE MICROSOFT GROUP POLICY MANAGEMENT CONSOLE AND GROUP POLICY MANAGEMENT EDITOR.

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 extesnions from the viewpoint of the GPO Editor, since that is where they can be enabled and configured or dsisabled.

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



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.
  - Preferences
- User Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - Preferences

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 Software Settings snapins are installed automatically as part of the DigitalPersona LDS Server installation, but the Administrative Templates are only installed as part of the DigitalPersona LDS 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 client Administrative Templates locally, see the topic *Installing the Client Administrative Templates Locally* on page *116*.

Additional extensions or templates may be provided as new components are released, and will be specified in the readme 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

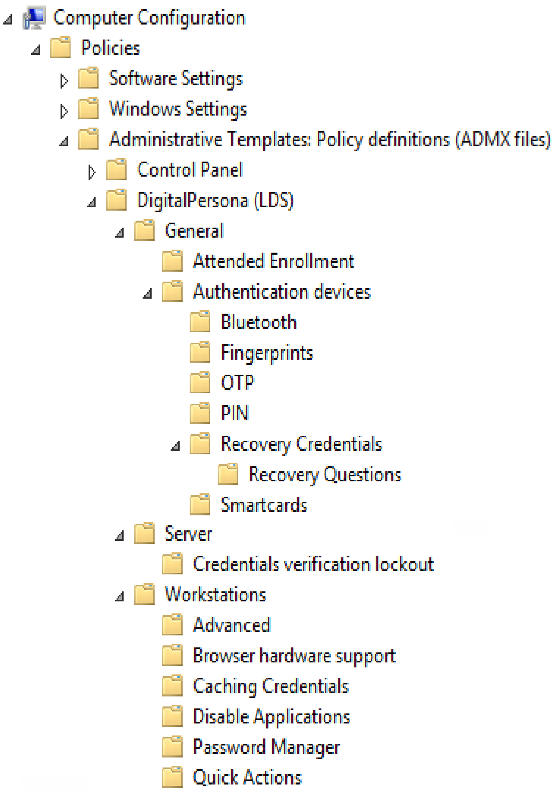
Security		
	Authentication	Logon Authentication Policy
		Enhanced Logon Authentication Policy
		Session Authentication Policy
		Kiosk Session Authentication Policy
	Enrollment	Enrollment Policy
	SMS	SMS Configuration
	SMTP	SMTP Configuration
Kiosk Administration		
		Allow automatic logon using Shared 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

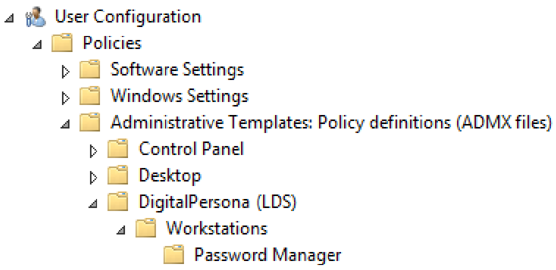
Node	Setting
Licenses	None (Used for license management)

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 LDS Administrative Tools.



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX files)
      - Control Panel
      - DigitalPersona (LDS)
        - General
          - Attended Enrollment
          - Authentication devices
            - Bluetooth
            - Fingerprints
            - OTP
            - PIN
            - Recovery Credentials
              - Recovery Questions
            - Smartcards
        - Server
          - Credentials verification lockout
        - Workstations
          - Advanced
          - Browser hardware support
          - Caching Credentials
          - Disable Applications
          - Password Manager
          - Quick Actions



- User Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX files)
      - Control Panel
      - Desktop
      - DigitalPersona (LDS)
        - Workstations
          - Password Manager

Note that if installing individual Administrative Templates, a corresponding .adml (language) file needs to be located in the language subfolder where they template is stored.

Administrative Template	Description or Setting
DPCA_LDS_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_LDS_General.admx	Creates these settings under the following node: Computer Configuration/Policies/Administrative Templates/ DigitalPersona (AD)/General
	Attended Enrollment Security officer authentication Require to complete or omit credential Authentication devices

Administrative Template	Description or Setting
	Bluetooth
	Fingerprints
	OTP
	PIN
	Recovery Credentials
	Enable Recovery Questions
	Cards
	Lock the computer upon card removal
	Event logging
	Level of detail in event logs
DPCA_LDS_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
	Add user-level credentials to Other User sign-in options
	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

Administrative Template	Description or Setting
	Quick Actions
	Credential
	Ctrl+Credential
	Shift+Credential
DPCA_LDS_PasswordManager.admx	Creates these settings under the following node: Computer Configuration/Policies/Administrative Templates/DigitalPersona (AD)/Workstations/Password Manager
	Authenticate other user for password manager operations
	Display password complexity popup
	Note that when installed by itself, it does not appear under a DigitalPersona node or mention DigitalPersona.
	Creates these settings under the following node: User Configuration/Policies/Administrative Templates/DigitalPersona (AD)/Workstations/Password Manager
	Allow creation of personal logons
	Managed logons
DPCA_LDS_Servers.admx	Creates these settings under the following node: User Configuration/Policies/Administrative Templates/DigitalPersona (AD)/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

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 the Client 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*.

Policies and Settings 10

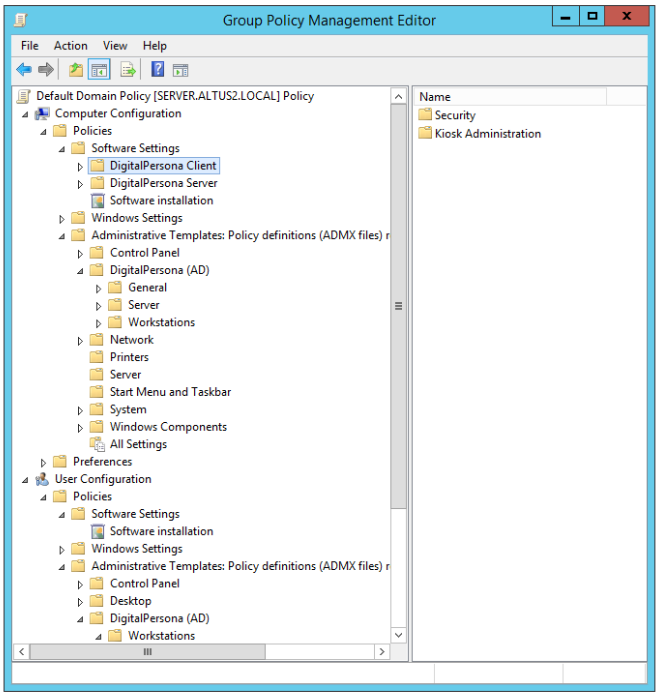
This chapter describes the policies and settings available through Active Directory to manage the behavior of the DigitalPersona Server and clients.

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 GPMC extensions and the User Query Tool. They are available as separate components installed through the DigitalPersona Administration Tools, which is included in your product package. See page 100 for a description of the GPMC Extensions and page 92 for information about the User Query Tool.

Note that the structure shown here 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 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 Workstation settings from the Microsoft Management Console (MMC), after installing the GPMC Extensions component of the DigitalPersona 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, 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 GPOs without concern for disrupting DigitalPersona 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 Administration Tools, the following nodes are created under the Computer Configuration\Software Settings node.

DigitalPersona Client (Summary)

These client settings can be found at the following location:

Computer Configuration/Software Settings/DigitalPersona Client.

These settings are used to configure and govern DigitalPersona LDS clients.

Category	Subcategory	Setting	Page
Security			
	Authentication	Logon Authentication Policy	120
		Enhanced Logon Authentication Policy	121
		Session Authentication Policy	123
		Kiosk Session Authentication Policy	123
	Enrollment	Enrollment Policy	124
	SMS	SMS Configuration	124
	SMTP	SMTP Configuration	124
Kiosk Administration			
		Allow automatic logon using Shared Kiosk Account	125
		Logon/Unlock with Shared Account Credentials	125
		Prevent users from logging on outside of a Kiosk session	125

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.

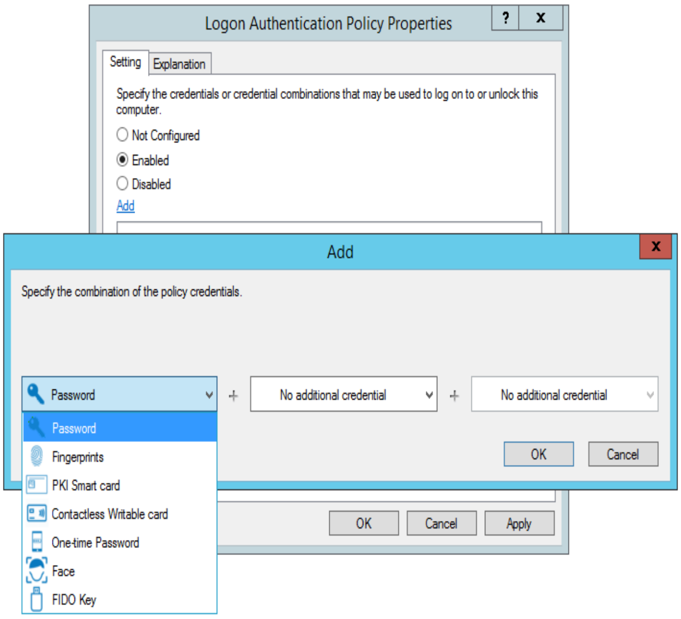
Primary and Secondary credentials

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
- PKI Smart Cards
- Contactless Writable Cards
- One-Time Passwords
- 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:

- Contactless ID Cards
- PIN
- Bluetooth devices



Logon Authentication Policy Properties

Setting | Explanation

Specify the credentials or credential combinations that may be used to log on to or unlock this computer.

○ Not Configured
● Enabled
○ Disabled

Add

Add

Specify the combination of the policy credentials.

Password + No additional credential + No additional credential

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.
- Select the Credentials and/or credential combinations that can be used for authentication during Windows logon. Then click *OK*.
- 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 in the upper-right corner of the item.
- Click *Apply*.

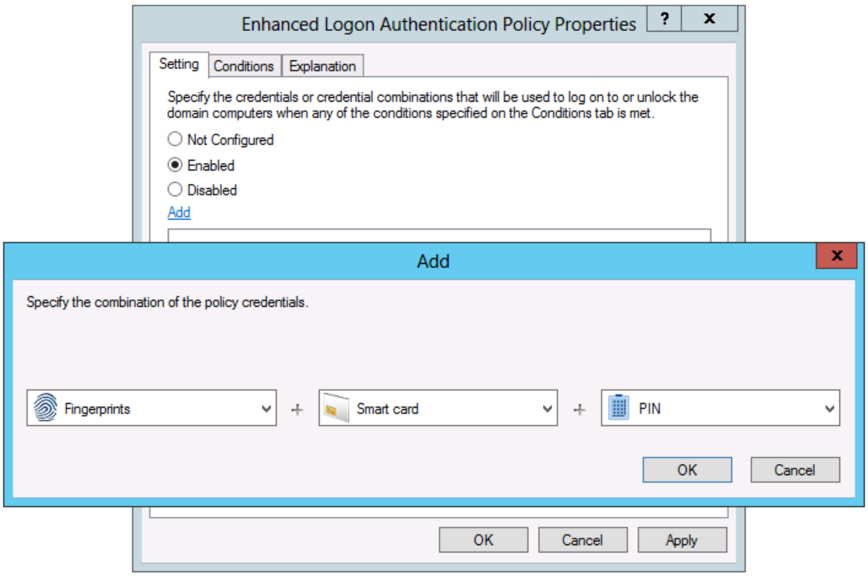
Enhanced Logon Authentication Policy

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.



Enhanced Logon Authentication Policy Properties

Specify the credentials or credential combinations that will be used to log on to or unlock the domain computers when any of the conditions specified on the Conditions tab is met.

○ Not Configured
● Enabled
○ Disabled

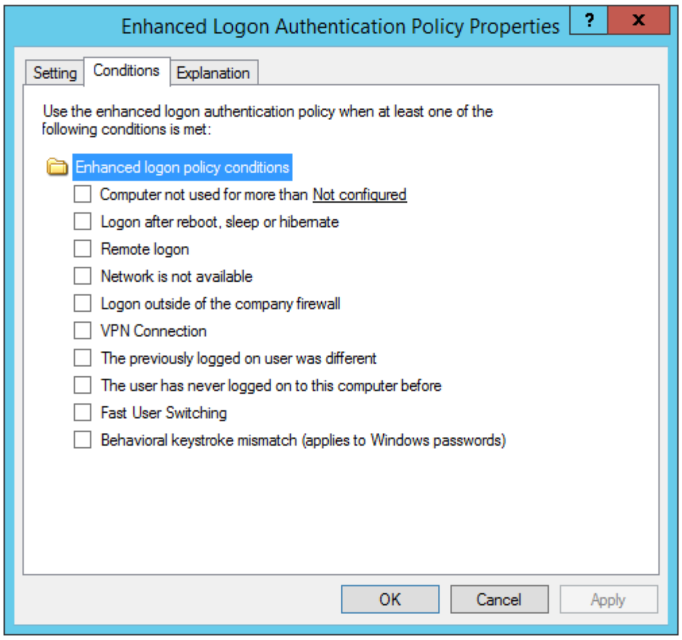
Add

Specify the combination of the policy credentials.

Fingerprints + Smart card + PIN

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.



Use the enhanced logon authentication policy when at least one of the following conditions is met:

Enhanced logon policy conditions
- □ Computer not used for more than Not configured
- □ Logon after reboot, sleep or hibernate
- □ Remote logon
- □ Network is not available
- □ Logon outside of the company firewall
- □ VPN Connection
- □ The previously logged on user was different
- □ The user has never logged on to this computer before
- □ Fast User Switching
- □ Behavioral keystroke mismatch (applies to Windows passwords)

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 121* 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 121* 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 *27*.

- 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 licenses, see the *License Activation and Management* chapter.

Computer Configuration\Policies\Administrative Templates

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

DigitalPersona (AD|LDS) \ General (Summary)

These settings are used to configure and govern DigitalPersona clients.

Category	Subcategory	Setting name	Page
Attended Enrollment			127
		Authentication of the user being enrolled	127
		Security Officer authentication	127
		Require to complete or omit credential	127
Authentication Devices			128
	Bluetooth	Lock computer when your phone is out of range	128
		Silent authentication	128
	Face	Use Infrared Cameras for Face Recognition	111
		Face Verification	112
	Fingerprints	Redirect fingerprint data	112
		Fingerprint enrollment	129
		Fingerprint verification	129

Category	Subcategory	Setting name	Page
	OTP	Allow sending OTP through email	130
		Time-Based OTP Validation Window	130
		Push Notification Server API Key	130
		Push Notification Server Tenant ID	130
		Custom SMS or Mail Message	130
	PIN	PIN enrollment	131
	Recovery Credentials	Recovery Questions	131
	Cards	Lock the computer upon card removal	132
		Allow the use of Contactless ID cards as a single (Primary) credential	132
Event logging		Level of detail in event logs	132
Proxy Server configuration			133

DigitalPersona\General (Detail)

Attended Enrollment

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 credntial

  - 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

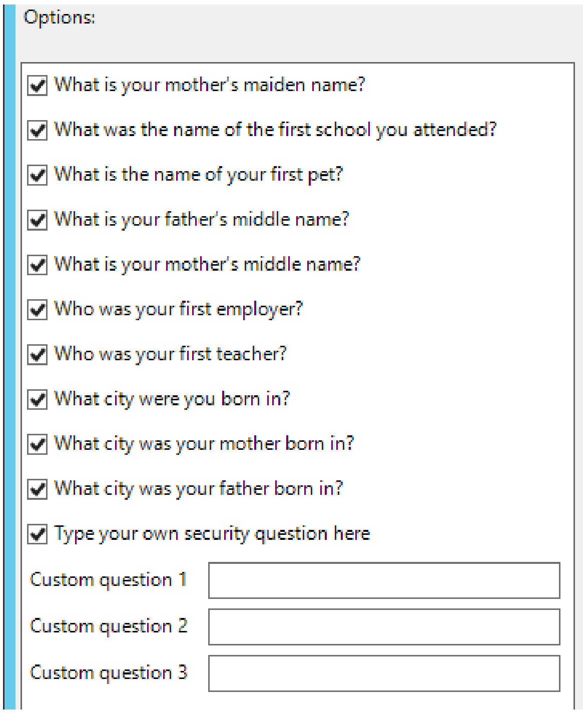
Recovery Questions

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.



Options:

☑ What is your mother's maiden name?
☑ What was the name of the first school you attended?
☑ What is the name of your first pet?
☑ What is your father's middle name?
☑ What is your mother's middle name?
☑ Who was your first employer?
☑ Who was your first teacher?
☑ What city were you born in?
☑ What city was your mother born in?
☑ What city was your father born in?
☑ Type your own security question here

Custom question 1
Custom question 2
Custom question 3

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.

Cards

Lock the computer upon card removal

Configure whether or not the computer locks upon removing a card from an attached card reader.

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

Allow the use of Contactless ID cards as a single (Primary) credential

Configure whether or not Contactless ID cards can be used as single (Primary) credential for login to computers and authentication when enrolling other credentials.

- If enabled, Contactless ID cards can be used as a Primary credential.
- If disabled or not configured, Contactless ID cards cannot be used as a Primary credential. They can only be used in combination with another Primary credential.

WARNING: Use of a Contactless ID card as a primary credential is generally not recommended and may increase your security risk.

In addition to enabling this GPO, you must perform the following steps to complete the process.

1. Run *gpupdate /force*
2. Close and reopen the GPO Editor.
3. Add the Contactless ID Card as a permitted credential in the *Logon Policy* GPO (for Windows Logon).
4. Add the Contactless ID Card as a permitted credential in the *Session Authentication Policy* GPO (For session authentication, i.e. when enrolling and managing credentials).
5. Run *gpupdate /force.*

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.

Proxy Server configuration

Specifies the name and port of a Proxy Server. When specified, all HTTP/HTTPS requests from DigitalPersona software are sent through this Proxy Server as an intermediary.

- If enabled, and a Proxy Server is specified, all queries are sent through the designated Proxy Server.
- If disabled or not configured, all queries are sent to the original URL.

DigitalPersona Server (Summary)

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

Category	Setting name	Page
Credentials verification lockout		
	Allow users to unlock their Windows account using DigitalPersona Recovery Questions	133
	Account lockout duration	133
	Reset account lockout counter after	134
	Account lockout threshold	134

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 Workstations (Summary)

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

Category	Setting name	Page
Advanced		
	AD LDS instance name	135
	Do not launch the Getting Started wizard upon logon	135
	Add user-level credentials to Other User sign-in options	135
	Identification Server domain	136
	Compatibility with Microsoft fingerprint support	135
	Allow DigitalPersona client to use DigitalPersona Server	136
	Show Taskbar icon	136
	Allow VPN-less access	136
Browser hardware support		136
Caching Credentials		
	Cache user data on local computer	136
	Maximum size of identification list	137
Disable Applications		
	Prevent Password Manager from running	137
Password Manager		

Category	Setting name	Page
	Display password complexity popup	137
Quick Actions		137

DigitalPersona Workstations (Detail)

Advanced

AD LDS instance name

Specifies the name of the AD LDS instance where a DigitalPersona Server is hosted.

- If enabled and an instance name is entered, queries are sent to the specified instance.
- If disabled or not configured, queries are sent to any AD LDS instance found in the environment.

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.

Add user-level credentials to Other User sign-in options

- If enabled, all user-level policy credentials (including ESPM if installed) and not already part of the Logon Authentication Policy will be added to sign-on options for Other User on the Windows Logon screen.
- If disabled or not configured, only the credentials (sign-in options) defined by the Logon Authentication policy will be shown for Other User and user-level policy credentials will not be shown as options for Other User on the Windows Logon screen.
- Note: If a user-level policy contains credentials (singly or as part of a credential combination) which are not specified in the computer-level Logon Authentication Policy, those credentials and any credentials associated with them in a credential combination, will not be displayed as sign-in options from the Other user tile. This could result in a valid user be unable to log on to Windows.

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.

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 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.mydomain1.com;www.mydomain2.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.

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

Authenticate other user for Password Manager operations

- If enabled, a user other than the logged in user may authenticate for Password Manager operations using a credential supporting user identification (such as their fingerprint), subject to session policy.
- If disabled or not configured, only the currently logged in user may authenticate for Password Manager operations.

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.

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	Setting name	Page
Password Manager		
	Allow creation of personal logons	138
	Managed logons	138

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.

Password Randomization 11

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

Introduction

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 LDS 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 complete details on Attended Enrollment

Password Randomization Options

The Password Randomization setting is specified in the *DigitalPersona.Altus.Enrollment.exe.config* file described above.

You can specify one of the following three values.

- DoNotRandomize
- RandomizeAlways
- MayRandomize

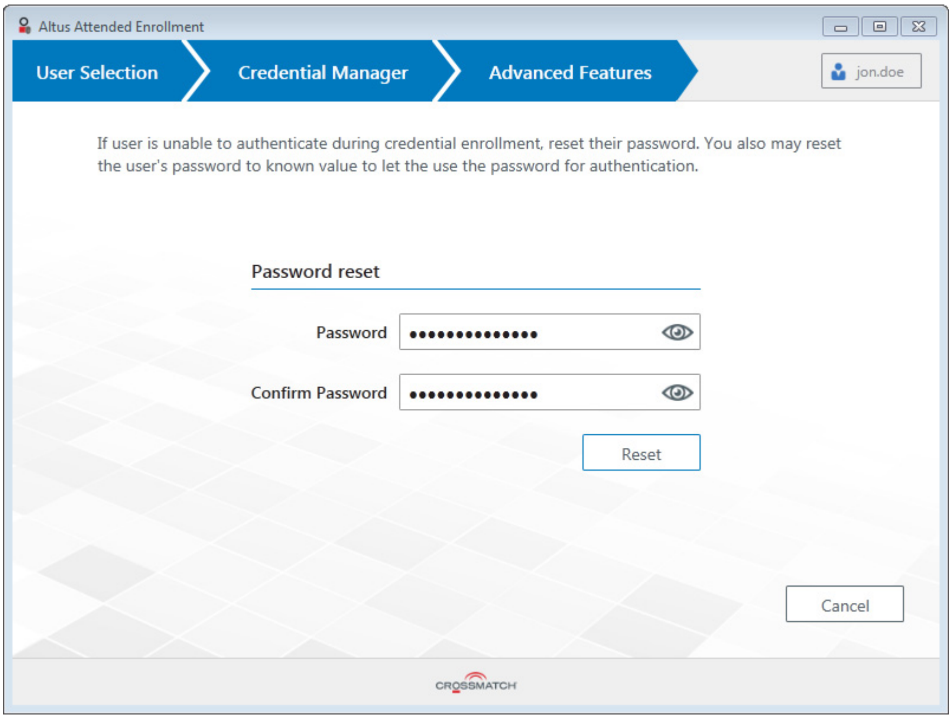
DoNotRandomize - (Default) Passwords are not randomized, and the UI elements for password randomization are not displayed. Passwords cannot be randomized during enrollment or from the DigitalPersona Advanced Features page as shown on the following page. Behavior of password entry during enrollment is described in the *DigitalPersona Web Administration Console* chapter beginning on page *243* and in the *Credential Manager* chapter of the *DigitalPersona Client Guide*.

RandomizeAlways - Passwords are randomized automatically. Some UI elements relating to password randomization are displayed. However, the UI does not allow the entry or creation of passwords during enrollment and does not allow changing a randomized password to a non-randomized password or re-randomizing a password. See *RandomizeAlways UI* on page *140*.

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 *142*.

DoNotRandomize

When DoNotRandomize is specified in the XML 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.



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

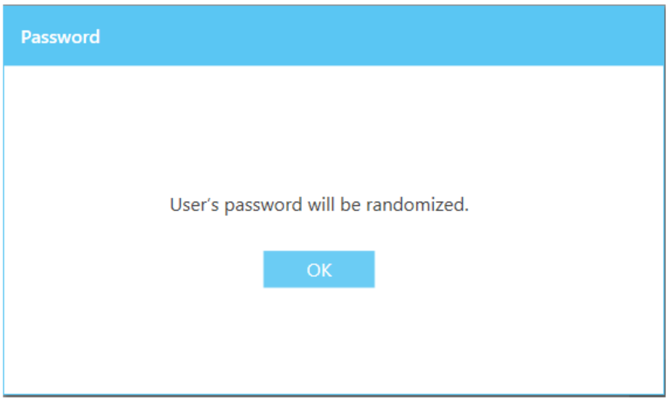
Password reset

Password ••••••••••••••

Confirm Password ••••••••••••••

RandomizeAlways UI

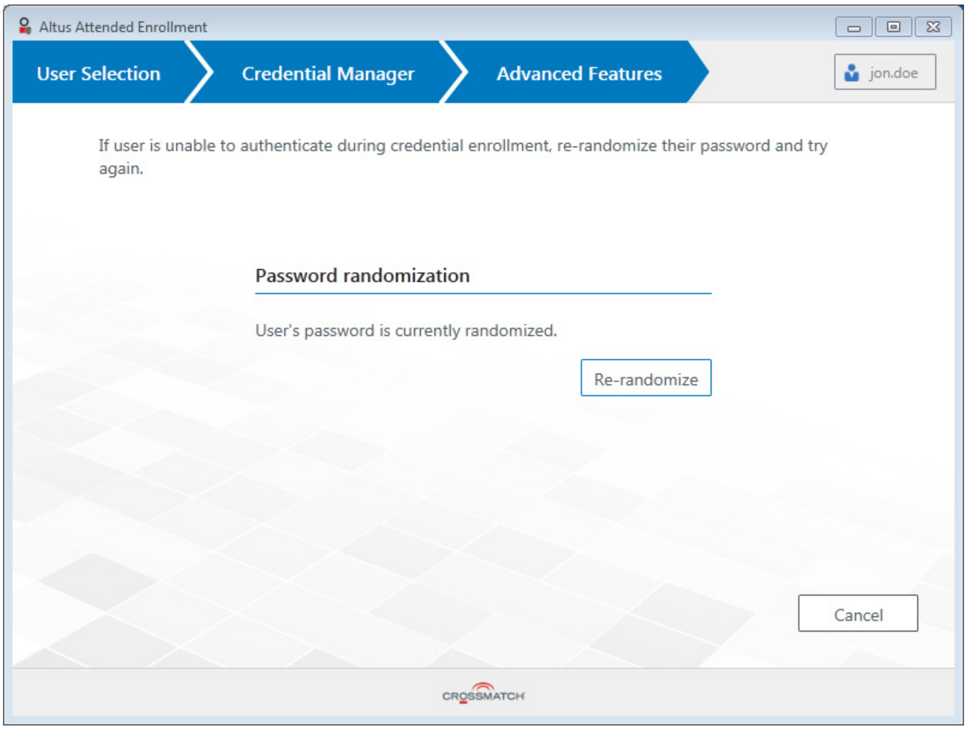
When *RandomizeAlways* is specified, instead of asking the user to enter a password during the creation of a DigitalPersona LDS User, the DigitalPersona client instead displays a message that the user's password will be randomized.



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 change 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 which was previously (and is currently) randomized. During the credential enrollment process a message displays that the "User's password will be randomized," and once enrolled, the user will not be able to change their password.



If user is unable to authenticate during credential enrollment, re-randomize their password and try again.

Password randomization

User's password is currently randomized.

To re-randomize a user’s password

- Click *Re-randomize*.

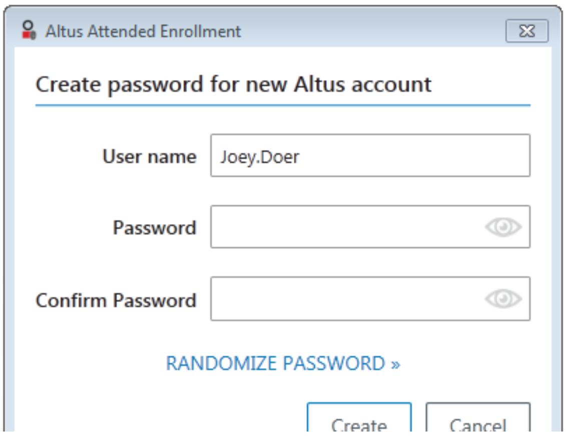
Note that this operation is an administrative function and therefore does not require the user’s authentication.

MayRandomize UI

The UI behavior is slightly different depending on whether you are creating a new DigitalPersona LDS Non AD user or enrolling a current AD user.

Creating a DigitalPersona LDS (Non AD) account

When *MayRandomize* is specified, a *RANDOMIZE PASSWORD* link for optionally generating a random password displays below the password fields during the creation of a Non AD user. Clicking this link changes it to read *REVERT,* which when clicked on, will cancel the impending password randomization and redisplay the dialog with Password fields and the original link.

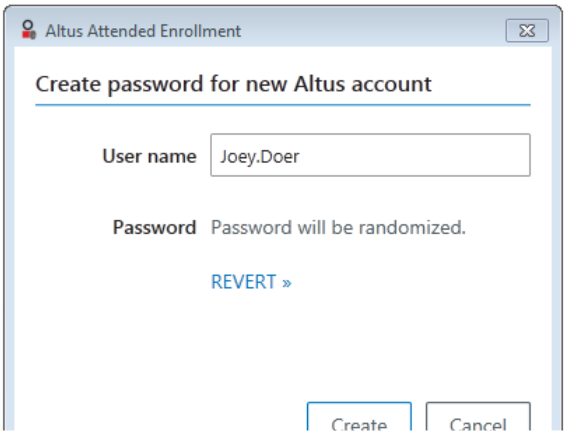


Create password for new Altus account

User name: Joey.Doer

Password:

Confirm Password:



Create password for new Altus account

User name: Joey.Doer

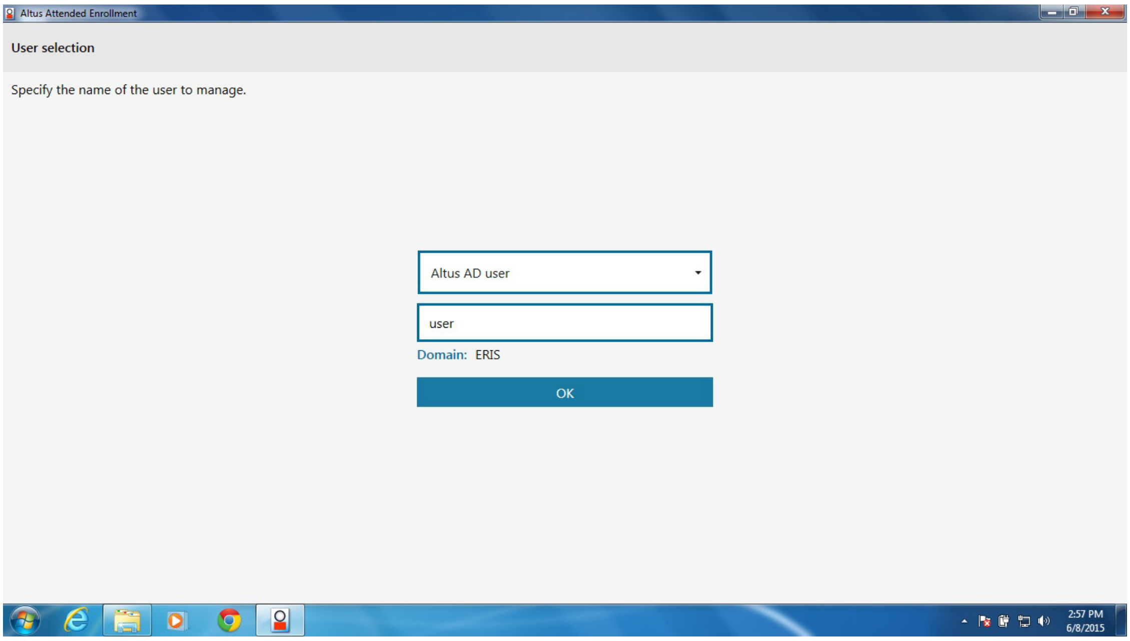
Password: Password will be randomized.

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

Clicking *RANDOMIZE PASSWORD* will generate a random password for this user and disable the ability to change the user's password from the *Password* tile.

AD user

There is no *Generate random password* link on the User selection page for AD users.



User selection

Specify the name of the user to manage.

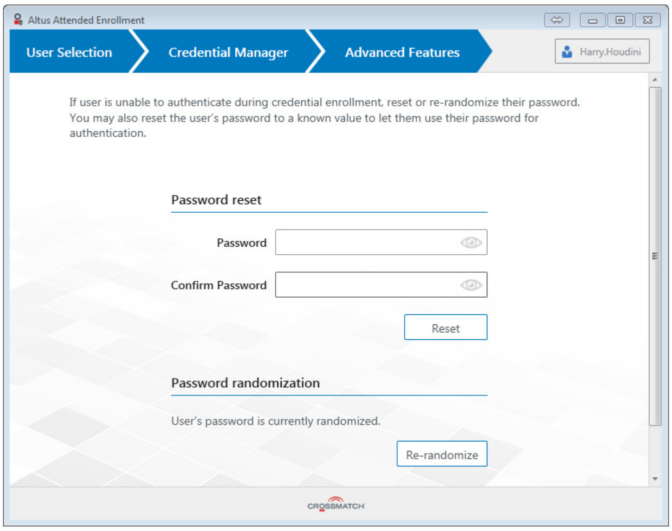
Altus AD user

user

Domain: ERIS

Also in this mode (MayRandomize), the DigitalPersona Advanced Features page displays UI elements allowing the administrator to reset, randomize or re-randomize the user's password. These operations do not require further authentication by the user.

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



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.

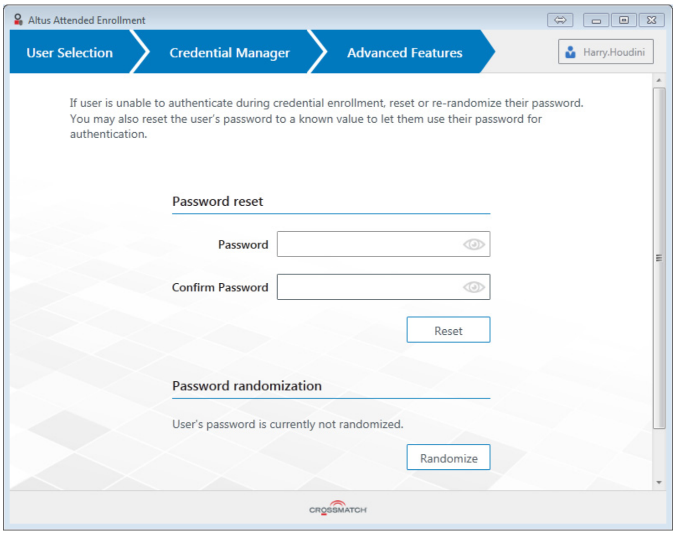
Password reset

Password

Confirm Password

Password randomization

User's password is currently randomized.



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

Password

Confirm Password

Password randomization

User's password is currently not 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 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.

Single Sign-On 12

THIS CHAPTER DESCRIBES SINGLE SIGN-ON (SSO), A FEATURE OF DIGITALPERSONA COMPOSITE AUTHENTICATION 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, providing 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 (through the Password Manager Admin Tool),

- 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 an 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 182.

Authorization Manager (AzMan) 13

THIS CHAPTER DESCRIBES THE ADMINISTRATION AND MANAGEMENT OF DIGITALPERSONA LDS ROLE-BASED PERMISSIONS, TASKS AND OPERATIONS MANAGED THROUGH THE DIGITALPERSONA AUTHORIZATION STORE AND THE WINDOWS AUTHORIZATION MANAGER (AZMAN).

For instructions on opening the DigitalPersona Authorization Store, see page 64.

Overview

The Microsoft Authorization Manager (AzMan) creates and manages an Authorization Store, which serves as a repository for DigitalPersona LDS authorization policies and defines a namespace for DigitalPersona LDS roles, tasks, and operations.

Installation and administration of the Microsoft Authorization Manager Tool should be by a member of the computer's Local Administrators group.

Although the group names, roles and tasks defined by DigitalPersona LDS can be customized, the operations that make up a task cannot be modified. You can change which operations may be performed as part of a given task, but removing a critical operation from a task may result in the failure of the task.

Those roles, tasks and operations defined by default during installation are described below.

Definition of terms

Operations - A set of permissions that are associated with system-level or API-level security procedures such as WriteAttributes or ReadAttributes. Operations are building blocks for tasks.

Tasks - A collection of operations and sometimes other tasks. Well-designed tasks represent recognizable work items (for example, "submit purchase order" or "submit expense").

Groups - There are two types of AzMan groups used by DigitalPersona LDS: Windows Groups and AzMan Groups.

- Windows Groups: are standard Windows Groups of any scope like Local, Global or Universal Groups supported by Windows OS and Active Directory itself.
- AzMan Groups: The only AzMan group used by DigitalPersona LDS is the LDAP Query Group. In AzMan, you can use LDAP queries to find objects in the DigitalPersona AD LDS or Active Directory databases. You can use an LDAP query to specify an LDAP query group by typing the desired LDAP query in the space provided on the Query tab of the Properties dialog box of the application group.

LDAP Query Groups

The following two LDAP Query Groups are predefined by DigitalPersona LDS.

Group name	LDAP Query	Group description
DigitalPersona AD Users	"(&(objectCategory=userProxy)(objectClass=userProxy))"	All user accounts in DigitalPersona AD LDS database which also exist in the Active Directory database. Active Directory users are automatically added to this group upon enrollment.
Altus Users	"(&(objectCategory=person)(objectClass=user)(dpAccountName=*))"	All user accounts in DigitalPersona AD LDS database which do not exist in the Active Directory database. Users are automatically added to this group upon enrollment if they are not in Active Directory.

To add an additional application group

- Right click the *Group* node and selected *New Application Group*.

Definitions

The Definition node contains two types of definitions, Role Definitions and Task Definitions.

Role Definitions

Each AzMan Role has the following properties.

- Role Name
- List of Users and Groups belonging to the Role
- List of AzMan Tasks assigned to this Role

The following DigitalPersona LDS AzMan roles are predefined.

Role name	Group	Default tasks	Role description
DigitalPersona AD Users	Altus AD Users (AzMan Group)	Manage Self	All Active Directory users have this Role assigned. It allows reading and writing public LDAP attributes from/to the DigitalPersona AD LDS database.
Altus Users	Altus Users (AzMan Group)	Manage Self	All DigitalPersona LDS users who do not exist in the Active Directory database have this Role assigned. It allows reading and writing public LDAP attributes from/to the DigitalPersona AD LDS database.

Role name	Group	Default tasks	Role description
Security Officers	Administrators (Windows Local Group)	Query Users Enroll Users	By default only Windows users which belong to the Local Administrators group on a machine where DigitalPersona LDS Server is installed have this Role assigned. It allows enrolling credentials for any type of user in the DigitalPersona AD LDS database. Domain Administrators are assigned this role automatically during setup.
Administrators	Administrators (Windows Local Group)	Query Users Manage Users Enroll Users Manage Licenses Manage Policies	By default only Windows users which belong to the Local Administrators group on a machine where DigitalPersona LDS Server is installed have this Role assigned. Local administrators are assigned this role automatically during setup. It allows practically any operation on DigitalPersona LDS users.

Tasks Definitions

The following authorization tasks are predefined.

Enroll Customers

User can enroll other customers (non Active Directory users). Default operations included are: Create User, Enroll Customer, Modify User Info and Set User Account Control.

Enroll Employees

User can enroll other employees (Active Directory users). Default operations included are: Create User, Enroll Employee, Modify User Info and Set User Account Control.

Enroll Self

User can enroll their own credentials. Default operations included are: Self Create User and Self Enroll Credentials.

Enroll Users

User can enroll other DigitalPersona users. Default operations included are: Create User, Enroll Credentials and Modify User Info and Set User Account Control.

Manage Licenses

User can activate DigitalPersona LDS licenses and import OTP hardware seed files. Default operations included are: Activate Licenses.

Manage Policies

User can create and manage DigitalPersona LDS policies. Default operations included are: Assign Policies, Create Policies and Delete Policies.

Manage Self

User can manage their own DigitalPersona account. Default operations included are: Get Own Info and Modify Own Info.

Manage Users

User can manage other DigitalPersona users and their accounts. Default operations included are: Create User, Delete User, Enroll Credentials, Modify User Info, Recover User, Set User Account Control and Unlock User Account.

Query Self

User can query the DigitalPersona LDS database for their own information. Default operations included are: Get Own Info.

Query Users

User can query the DigitalPersona LDS database for user information. Default operations included are: Get User Info.

Authorization Operations

The following authorization operations are predefined.

Activate License - Activates a product license.

Assign Policies - Assigns a policy to a DigitalPersona LDS group.

Create Policies - Create DigitalPersona LDS policy.

Create User - Create DigitalPersona LDS Non AD user record.

Delete Policies - Delete DigitalPersona LDS policies.

Delete User - Delete DigitalPersona LDS Non AD user.

Enroll Credentials - Enroll DigitalPersona LDS Non AD user credentials.

Enroll Customer Credentials - Enroll customer (DigitalPersona LDS Non AD user) credentials.

Enroll Employee Credentials - Enroll employee (AD user) credentials.

Get Own Info - Query DigitalPersona LDS database for own user information (attributes).

Get User Info - Query DigitalPersona LDS database for user information (attributes).

Modify Own Info - Change user’s own DigitalPersona LDS user information.

Modify User Info - Change DigitalPersona LDS user information.

Recover User - Perform user recovery. (This feature is not implemented in the current version. The operation is reserved for future use.)

Self Create User - Create DigitalPersona LDS record. Must be a Windows AD user.

Self Enroll Credentials - Enroll own user credentials without needing Security Officer role.

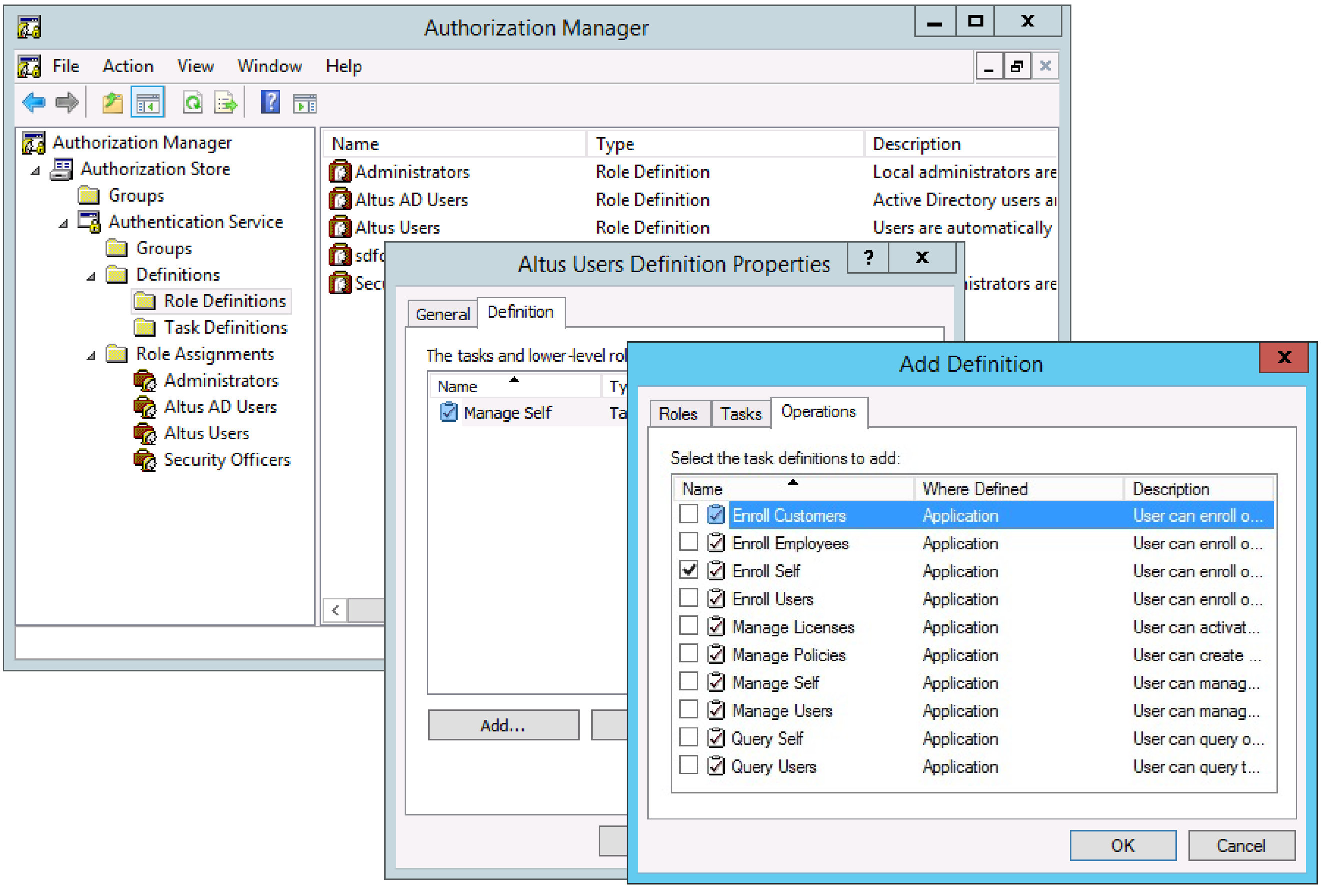
Set User Account Control - Set User Account control bits.

Unlock User Account - Remove lock from user account.

Enabling self-enrollment

You can enable DigitalPersona (AD/Employee and LDS/Customer) users to enroll and manage their own DigitalPersona LDS credentials by Adding the *Enroll Self* task to the predefined DigitalPersona AD Users or Altus Users role or to another role that you create.

WARNING: If you are using DigitalPersona Attended Enrollment to enroll users, self-enrollment should not be enabled for the same group of users.



Name	Type	Description
Administrators	Role Definition	Local administrators are
Altus AD Users	Role Definition	Active Directory users a
Altus Users	Role Definition	Users are automatically
sdfc		
Secu		istrators are

The tasks and lower-level rol

Name	Ty
Manage Self	Ta

Select the task definitions to add:

	Name	Where Defined	Description
□	Enroll Customers	Application	User can enroll o...
□	Enroll Employees	Application	User can enroll o...
☑	Enroll Self	Application	User can enroll o...
□	Enroll Users	Application	User can enroll o...
□	Manage Licenses	Application	User can activat...
□	Manage Policies	Application	User can create ...
□	Manage Self	Application	User can manag...
□	Manage Users	Application	User can manag...
□	Query Self	Application	User can query o...
□	Query Users	Application	User can query t...

Recovery 14

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

DigitalPersona LDS 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.

User recovery

Installation of DigitalPersona LDS 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 *Recover User*, which launches the *Recover access* wizard.
3		The administrator transmits the displayed Recovery account name and password to the user. This will enable them to authenticate at the pre-boot level. Upon use, this password is automatically changed.
4	The user enters the provided information, gaining access to the computer at the pre-boot level.	
5	At the Windows logon screen, the user clicks their user tile. On their user tile screen, they click the *One time access* link.	
6	The user transmits the displayed Security Key to the administrator.	

Step	User or DigitalPersona software	Administrator
7		The administrator clicks *Next*, enters the Security Code and clicks *Next* again.
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 *OK*, gaining access to their Windows account.	

Computer recovery

Installation of DigitalPersona LDS also adds the *Recover Computer* command to Active Directory's computer object context menu. This command can be used to easily recover access to a computer where an AD User has been locked out during pre-boot authentication.

To recover a computer from a pre-boot lockout

Step	User or DigitalPersona software	Administrator
1	The AD User contacts your helpdesk for assistance in recovering from a pre-boot lockout.	
2		The administrator locates their computer in Active Directory, right-clicks on the computer and selects the *Recover Computer* command.
3		The administrator transmits the displayed Recovery Account name and password to the user.
4	The user can enter the Recovery Account name and password to authenticate at the pre-boot level.	
5	Upon use, this password is automatically changed.	

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.

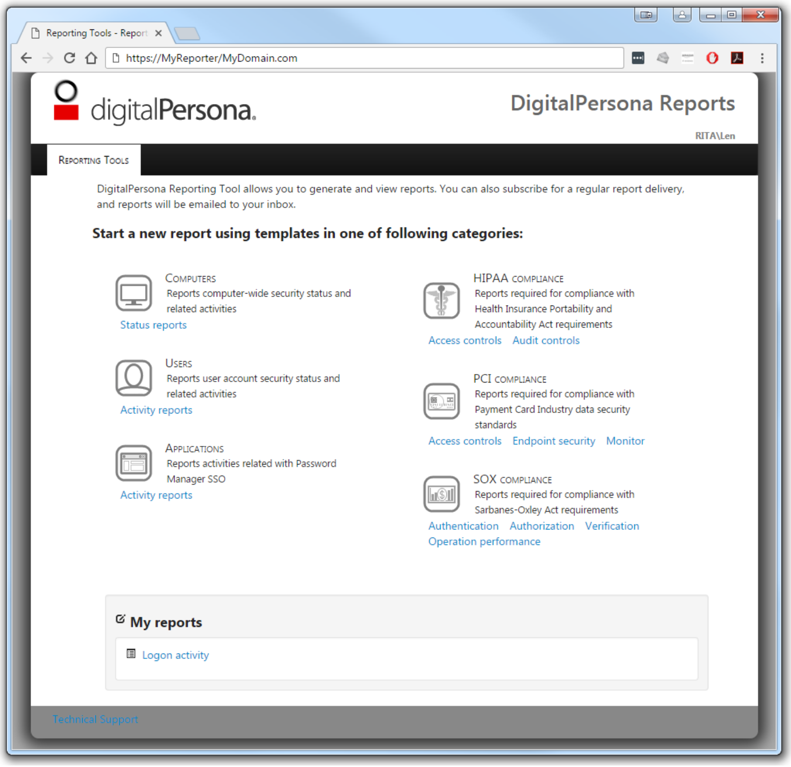
3. Click the DigitalPersona tab.
4. Clear the *Account is locked out for fingerprint authentication* checkbox.This checkbox is for unlocking accounts and cannot be used by an administrator to lock an account. If the account is unlocked, the checkbox is disabled.
5. Click OK to close the dialog box and 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 REPORTS COMPONENT TO THE DIGITALPERSONA SOLUTION. COMPLIANCE.

DigitalPersona Reports 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.



DigitalPersona Reporting Tool allows you to generate and view reports. You can also subscribe for a regular report delivery, and reports will be emailed to your inbox.

Start a new report using templates in one of following categories:

Computers
Reports computer-wide security status and related activities
Status reports

Users
Reports user account security status and related activities
Activity reports

Applications
Reports activities related with Password Manager SSO
Activity reports

HIPAA compliance
Reports required for compliance with Health Insurance Portability and Accountability Act requirements
Access controls   Audit controls

PCI compliance
Reports required for compliance with Payment Card Industry data security standards
Access controls   Endpoint security   Monitor

SOX compliance
Reports required for compliance with Sarbanes-Oxley Act requirements
Authentication   Authorization   Verification
Operation performance

My reports
Logon activity

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 *165*).

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.

Component name	Description
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

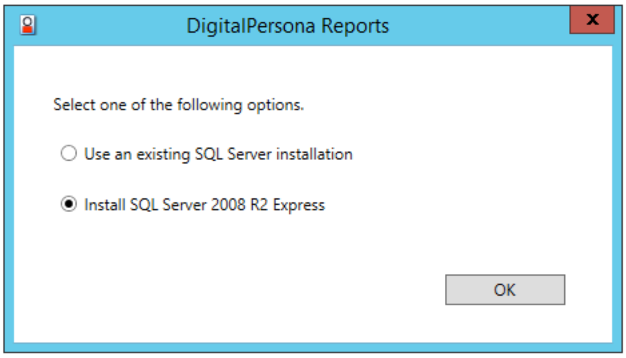
Installation

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.



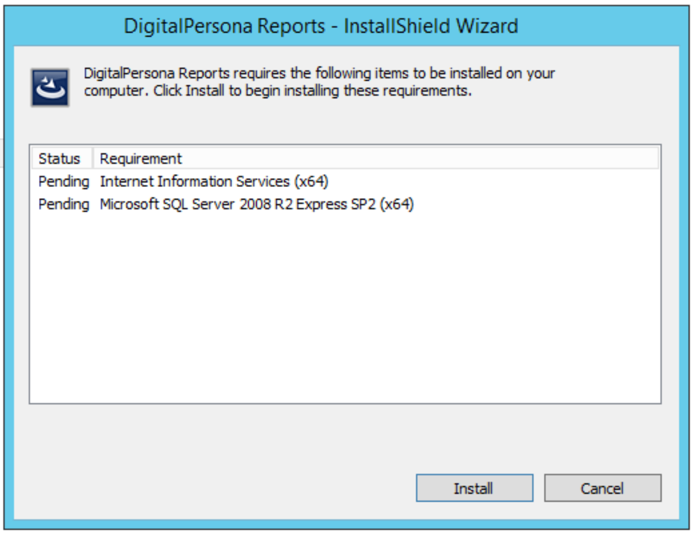
DigitalPersona Reports

Select one of the following options.

○ Use an existing SQL Server installation

● Install SQL Server 2008 R2 Express

   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*.



DigitalPersona Reports - InstallShield Wizard

DigitalPersona Reports requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	Internet Information Services (x64)
Pending	Microsoft SQL Server 2008 R2 Express SP2 (x64)

   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.

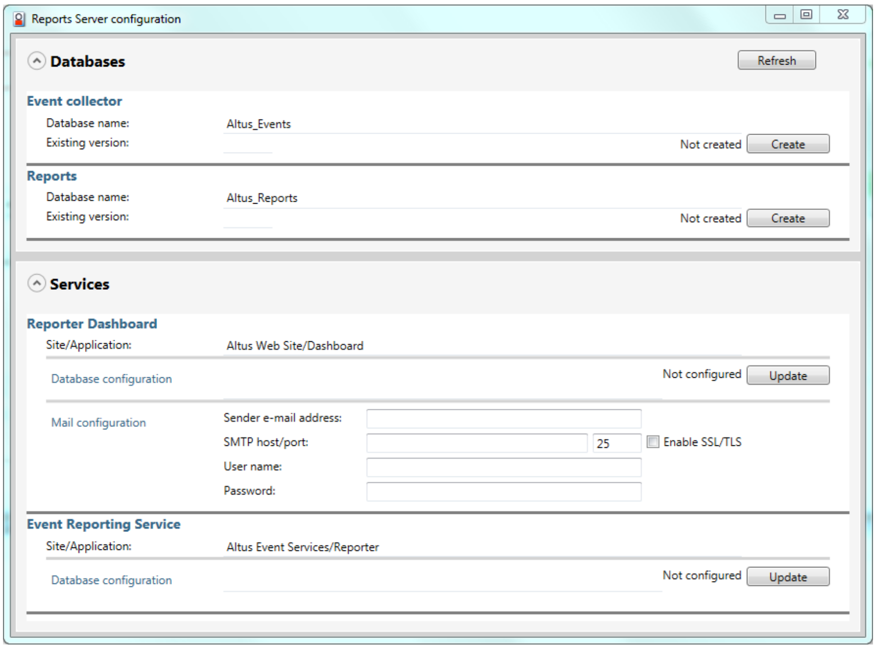
   e. The DigitalPersona Reports software will then install.

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.



Reports Server configuration

Databases — Refresh

Event collector
Database name: Altus_Events
Existing version: — Not created — Create

Reports
Database name: Altus_Reports
Existing version: — Not created — Create

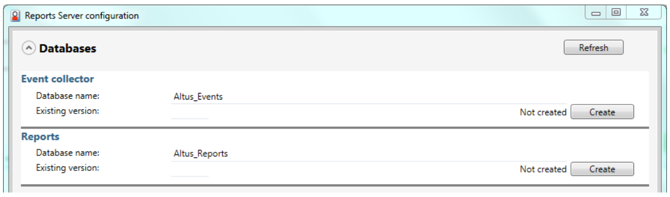
Services

Reporter Dashboard
Site/Application: Altus Web Site/Dashboard
Database configuration — Not configured — Update
Mail configuration
Sender e-mail address:
SMTP host/port: 25 □ Enable SSL/TLS
User name:
Password:

Event Reporting Service
Site/Application: Altus Event Services/Reporter
Database configuration — Not configured — Update

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)



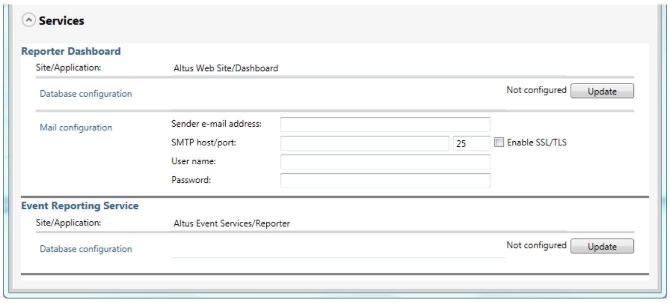
Reports Server configuration

Databases — Refresh

Event collector
Database name: Altus_Events
Existing version: — Not created — Create

Reports
Database name: Altus_Reports
Existing version: — Not created — Create

- Configure web services to use those databases



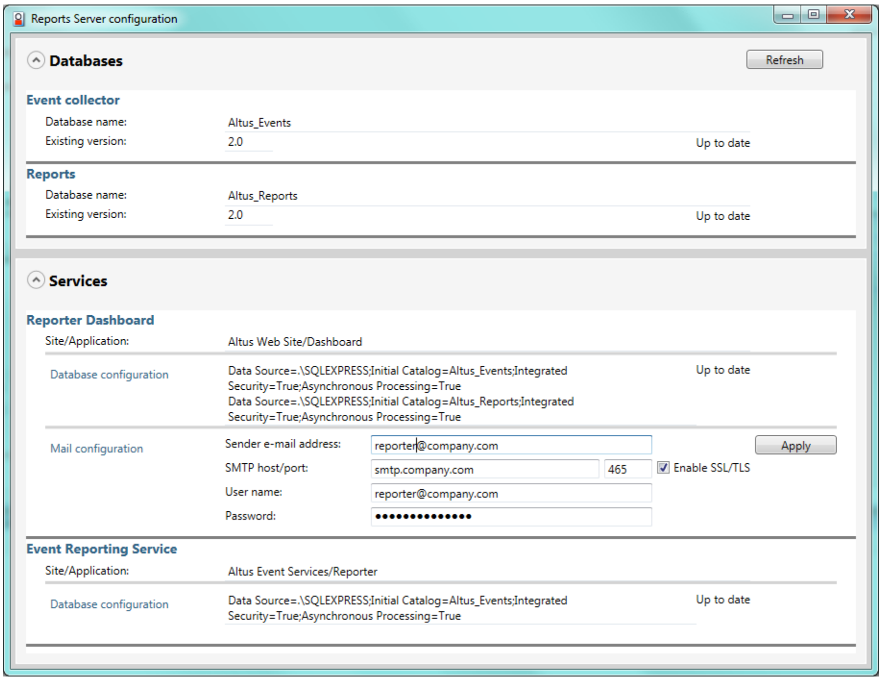
Services

Reporter Dashboard
Site/Application: Altus Web Site/Dashboard
Database configuration — Not configured — Update
Mail configuration
Sender e-mail address:
SMTP host/port: 25 □ Enable SSL/TLS
User name:
Password:

Event Reporting Service
Site/Application: Altus Event Services/Reporter
Database configuration — Not configured — Update

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

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



Databases

Event collector

Database name: Altus_Events

Existing version: 2.0 Up to date

Reports

Database name: Altus_Reports

Existing version: 2.0 Up to date

Services

Reporter Dashboard

Site/Application: Altus Web Site/Dashboard

Database configuration: Data Source=.\SQLEXPRESS;Initial Catalog=Altus_Events;Integrated Security=True;Asynchronous Processing=True Data Source=.\SQLEXPRESS;Initial Catalog=Altus_Reports;Integrated Security=True;Asynchronous Processing=True Up to date

Mail configuration:

Sender e-mail address: reporter@company.com

SMTP host/port: smtp.company.com 465 ☑ Enable SSL/TLS

User name: reporter@company.com

Password: ••••••••••••••

Event Reporting Service

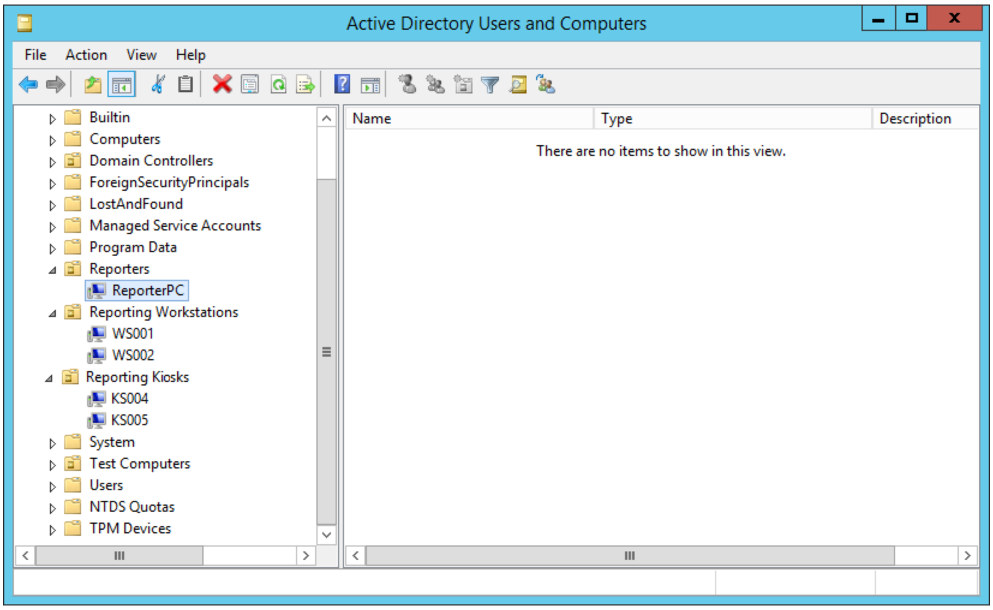
Site/Application: Altus Event Services/Reporter

Database configuration: Data Source=.\SQLEXPRESS;Initial Catalog=Altus_Events;Integrated Security=True;Asynchronous Processing=True Up to date

Configure Active Directory GPO settings

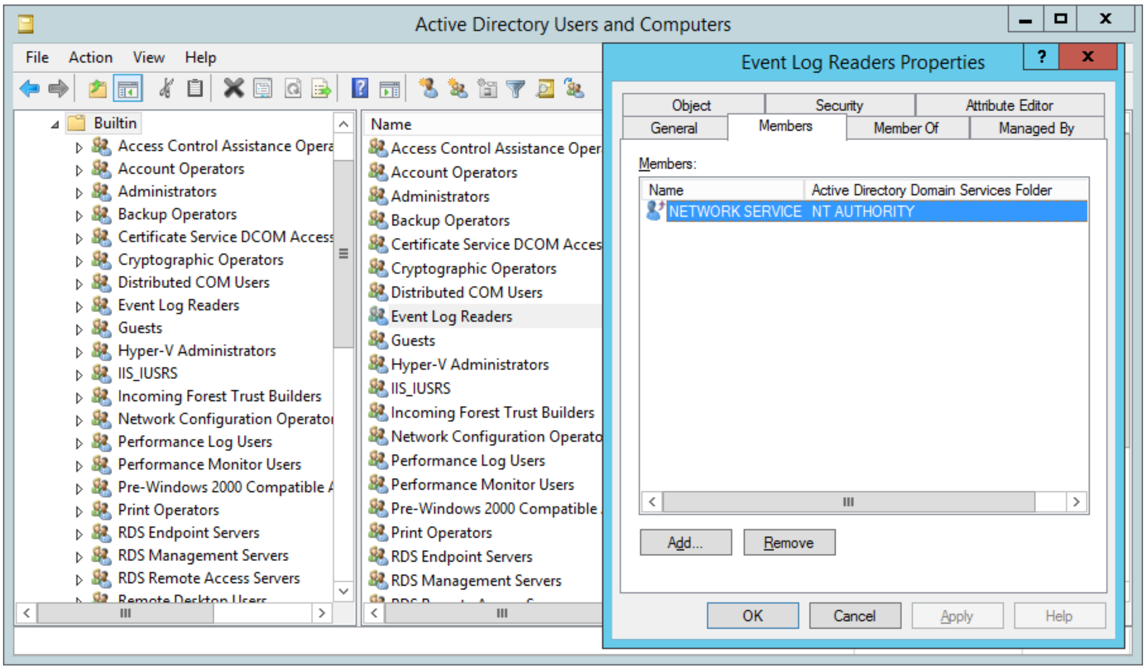
In Active Directory Users and Computers

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



There are no items to show in this view.

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.



Name	Active Directory Domain Services Folder
NETWORK SERVICE	NT AUTHORITY

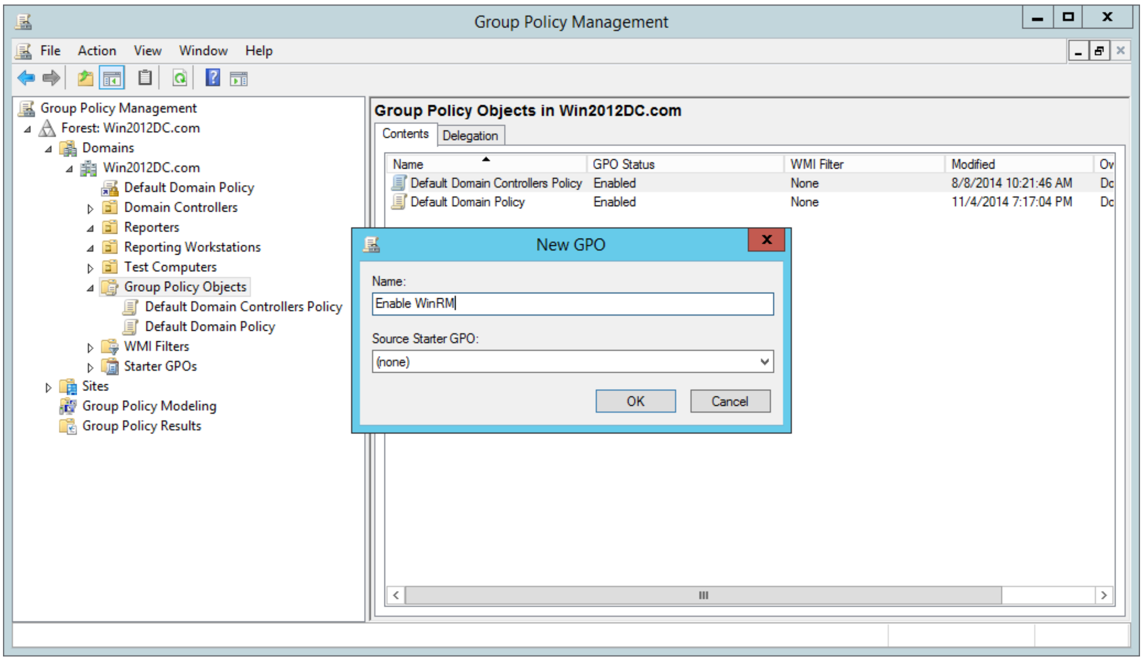
- In ADUC, navigate to *<yourdomain>\Builtin\Event Log Readers*.
- Right-click on *Event Log Readers* and select *Properties* from the shortcut menu. Then select the *Members* tab.
- Select *NETWORK SERVICE* and click *Add*.

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

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

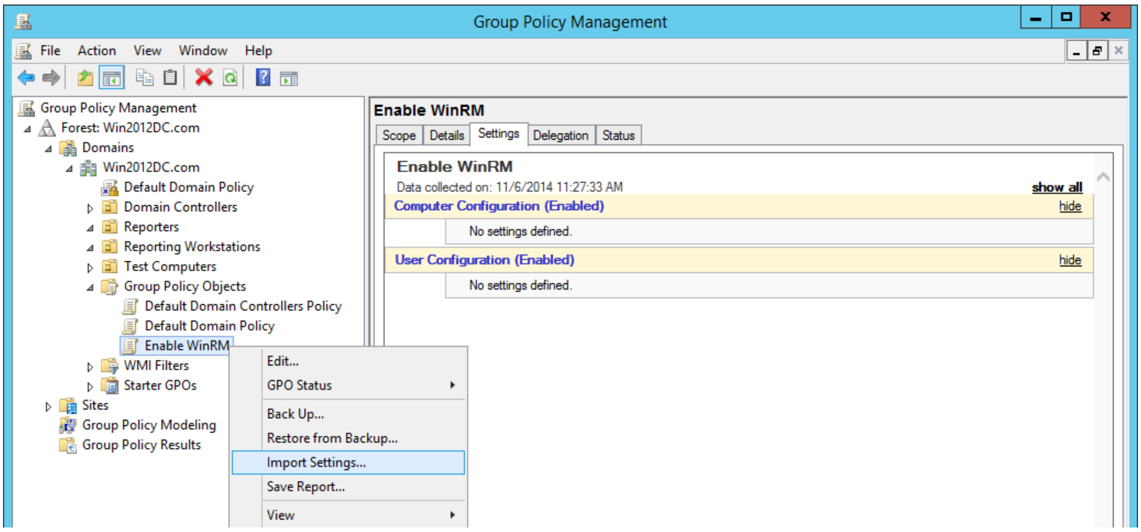


Name	GPO Status	WMI Filter	Modified	Ov
Default Domain Controllers Policy	Enabled	None	8/8/2014 10:21:46 AM	Dc
Default Domain Policy	Enabled	None	11/4/2014 7:17:04 PM	Dc

Name: Enable WinRM

Source Starter GPO: (none)

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



Enable WinRM

Data collected on: 11/6/2014 11:27:33 AM

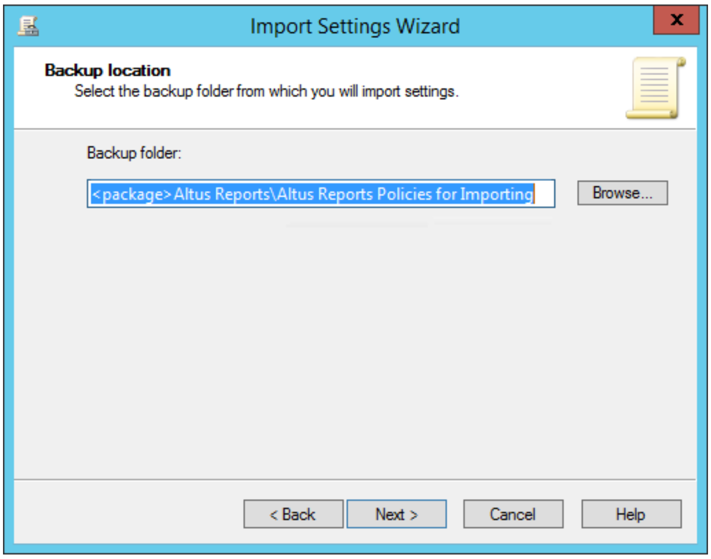
Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

No settings defined.

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



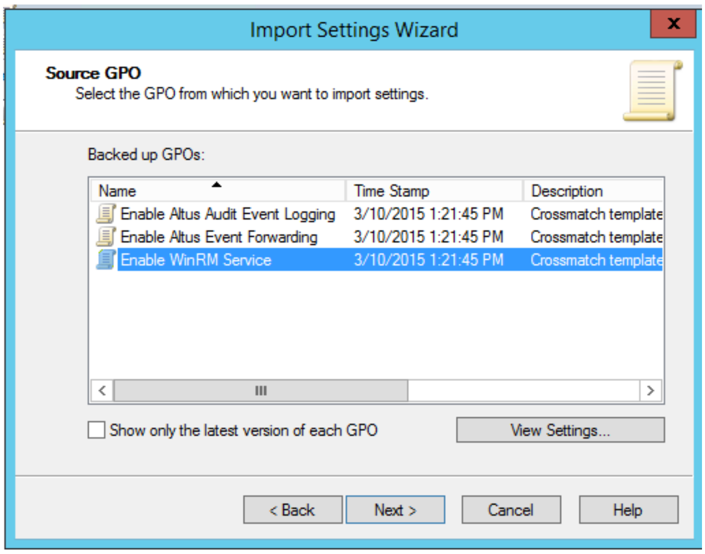
Import Settings Wizard

Backup location

Select the backup folder from which you will import settings.

Backup folder: <package>Altus Reports\Altus Reports Policies for Importing

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



Import Settings Wizard

Source GPO

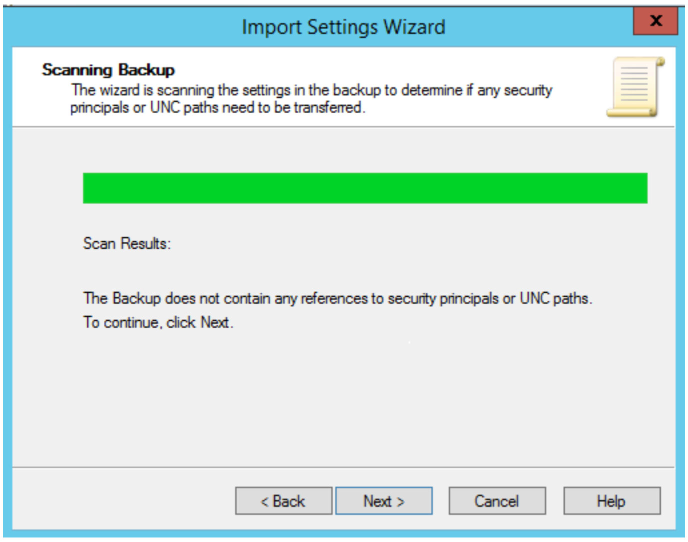
Select the GPO from which you want to import settings.

Backed up GPOs:

Name	Time Stamp	Description
Enable Altus Audit Event Logging	3/10/2015 1:21:45 PM	Crossmatch template
Enable Altus Event Forwarding	3/10/2015 1:21:45 PM	Crossmatch template
Enable WinRM Service	3/10/2015 1:21:45 PM	Crossmatch template

□ Show only the latest version of each GPO

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



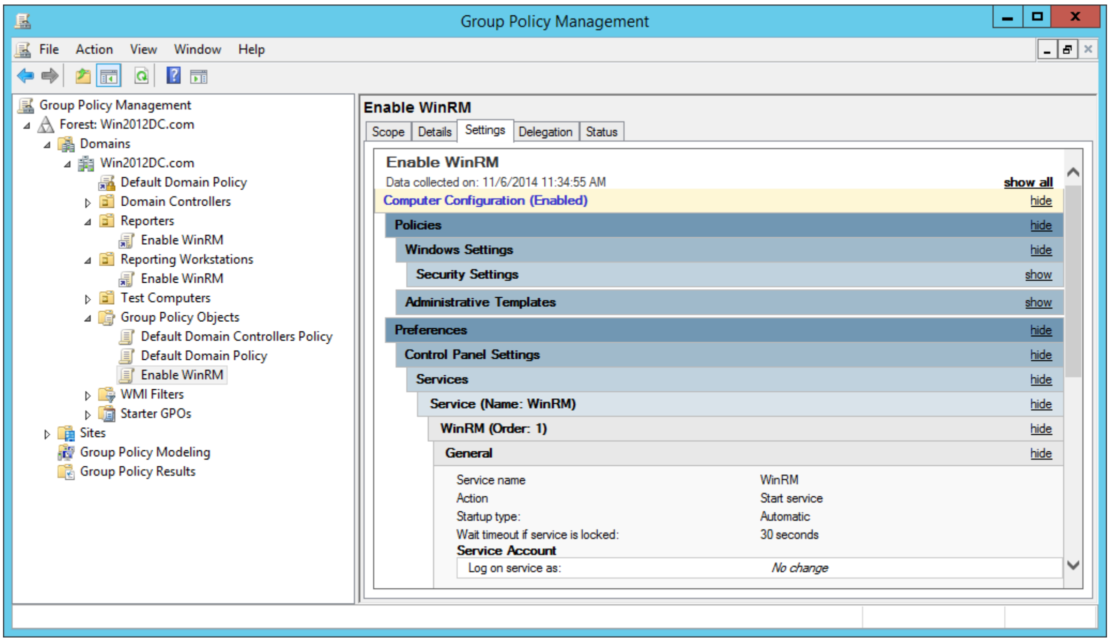
Scanning Backup

The wizard is scanning the settings in the backup to determine if any security principals or UNC paths need to be transferred.

Scan Results:

The Backup does not contain any references to security principals or UNC paths.
To continue, click Next.

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



Enable WinRM

Data collected on: 11/6/2014 11:34:55 AM — show all

Computer Configuration (Enabled) — hide

Policies — hide

Windows Settings — hide

Security Settings — show

Administrative Templates — show

Preferences — hide

Control Panel Settings — hide

Services — hide

Service (Name: WinRM) — hide

WinRM (Order: 1) — hide

General — hide

Service name	WinRM
Action	Start service
Startup type:	Automatic
Wait timeout if service is locked:	30 seconds

Service Account

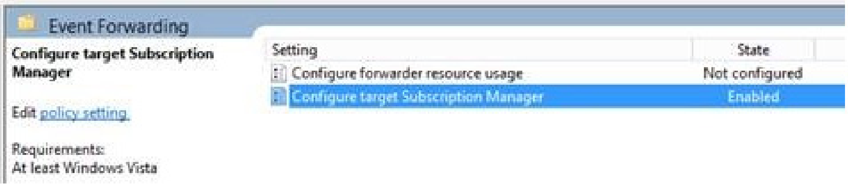
Log on service as:	*No change*

2. Repeat steps *a* through *l* for each DigitalPersona GPO listed at the beginning of step 1.

3. Configure the *target Subscription Manager* URI.

a. Navigate to *Computer Configuration, Policies, Administrative Templates, Windows Components, Event Forwarding.*

b. Right-click on the *Enable DigitalPersona Event Forwarding* GPO created above, and then double-click on the *Configure target Subscription Manager* setting.



Event Forwarding

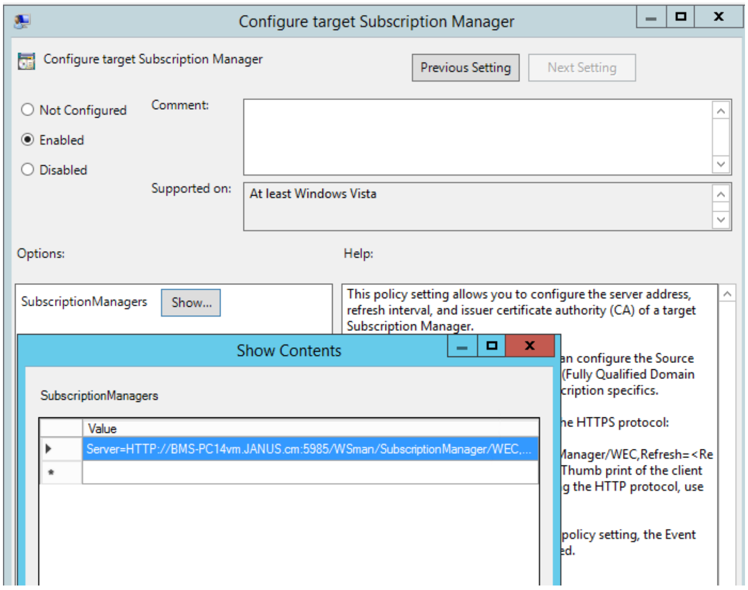
Configure target Subscription Manager

Edit policy setting.

Requirements:
At least Windows Vista

Setting	State
Configure forwarder resource usage	Not configured
Configure target Subscription Manager	Enabled

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.



Configure target Subscription Manager
Configure target Subscription Manager
Previous Setting
Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SubscriptionManagers Show...

Help:

This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.

an configure the Source (Fully Qualified Domain cription specifics.

he HTTPS protocol:

Manager/WEC,Refresh=<Re Thumb print of the client g the HTTP protocol, use

policy setting, the Event ed.

SubscriptionManagers

	Value
▸	Server=HTTP://BMS-PC14vm.JANUS.cm:5985/WSman/SubscriptionManager/WEC,...
*	

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.

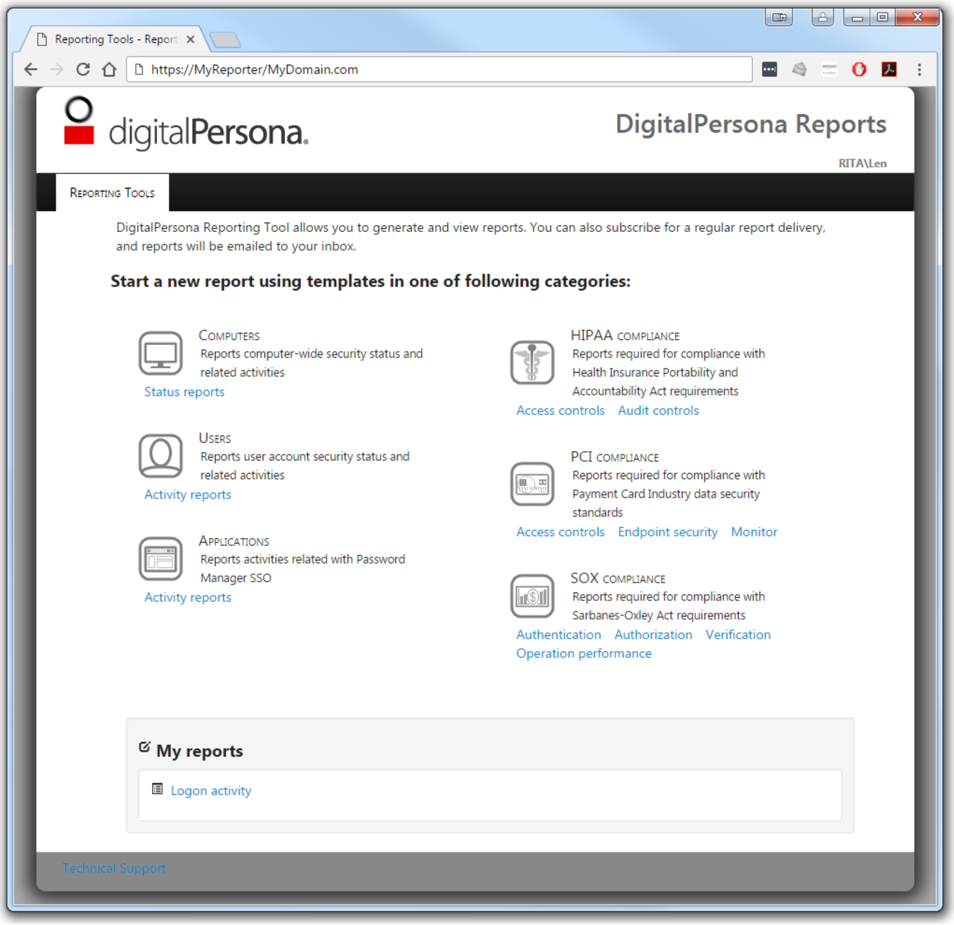
The *Event Forwarding* service is running and events are appearing in the *Forwarded Events* event log.
See the *Troubleshooting steps* topic at the end of this chapter (page 170) if you experience problems with the Event forwarding setup.

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.



DigitalPersona Reports

RITA\Len

DigitalPersona Reporting Tool allows you to generate and view reports. You can also subscribe for a regular report delivery, and reports will be emailed to your inbox.

Start a new report using templates in one of following categories:

Computers
Reports computer-wide security status and related activities
Status reports

Users
Reports user account security status and related activities
Activity reports

Applications
Reports activities related with Password Manager SSO
Activity reports

HIPAA compliance
Reports required for compliance with Health Insurance Portability and Accountability Act requirements
Access controls Audit controls

PCI compliance
Reports required for compliance with Payment Card Industry data security standards
Access controls Endpoint security Monitor

SOX compliance
Reports required for compliance with Sarbanes-Oxley Act requirements
Authentication Authorization Verification Operation performance

My reports

Logon activity

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.

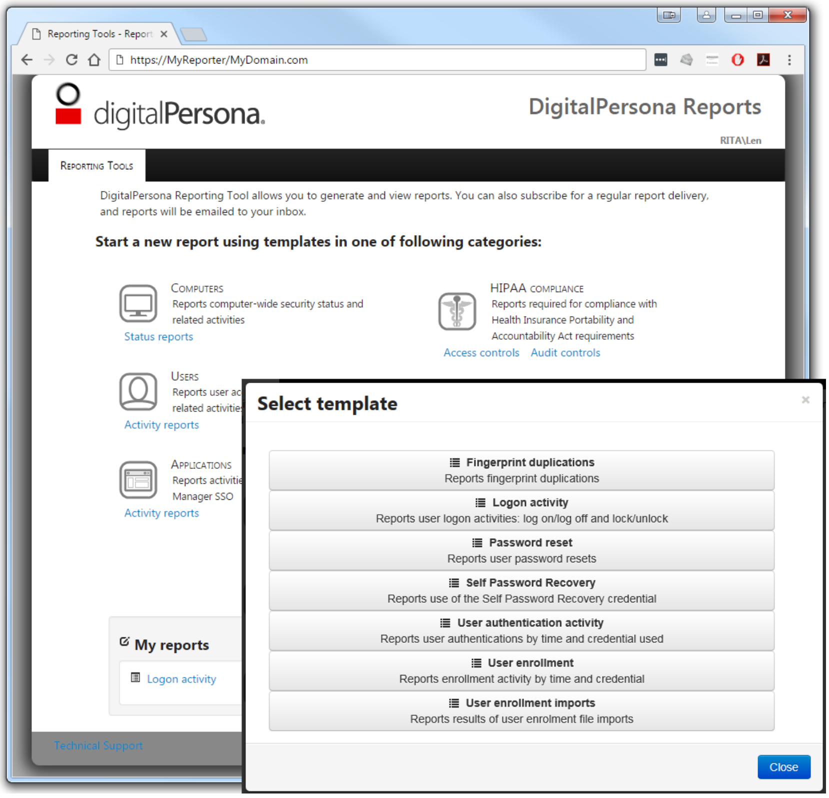
Note that when creating or editing reports, you must click the **Save** or **Run Now** buttons to save any new or modified information.

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.



DigitalPersona Reporting Tool allows you to generate and view reports. You can also subscribe for a regular report delivery, and reports will be emailed to your inbox.

Start a new report using templates in one of following categories:

Computers
Reports computer-wide security status and related activities
Status reports

HIPAA compliance
Reports required for compliance with Health Insurance Portability and Accountability Act requirements
Access controls Audit controls

Users
Reports user ac… related activitie…
Activity reports

Applications
Reports activiti… Manager SSO
Activity reports

My reports
Logon activity

Technical Support

Select template

Fingerprint duplications
Reports fingerprint duplications

Logon activity
Reports user logon activities: log on/log off and lock/unlock

Password reset
Reports user password resets

Self Password Recovery
Reports use of the Self Password Recovery credential

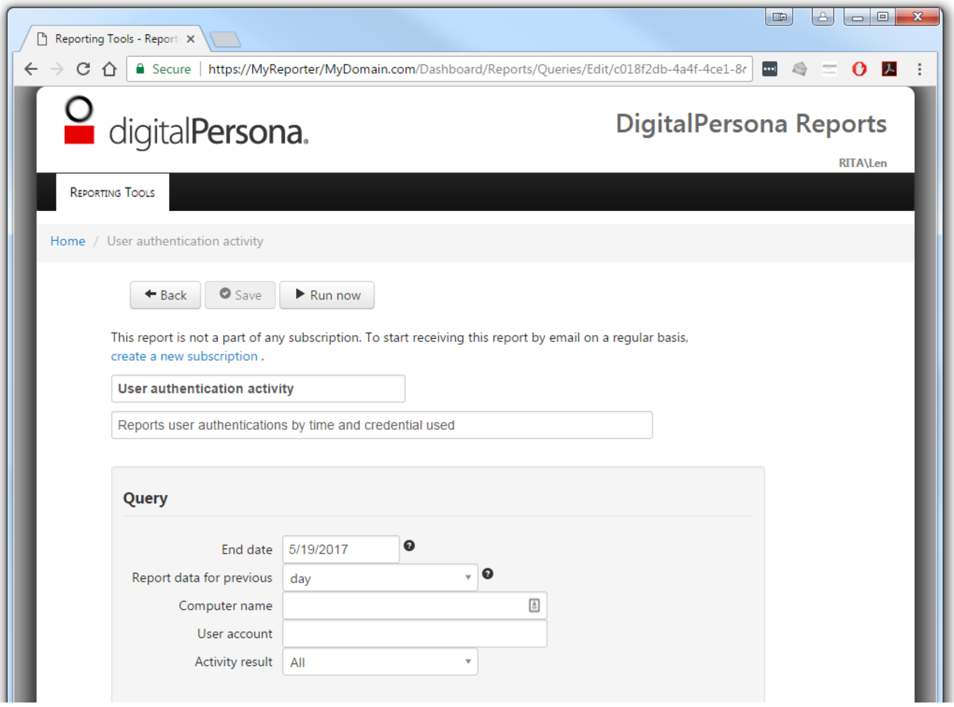
User authentication activity
Reports user authentications by time and credential used

User enrollment
Reports enrollment activity by time and credential

User enrollment imports
Reports results of user enrolment file imports

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.


Reporting Tools - Report
Secure https://MyReporter/MyDomain.com/Dashboard/Reports/Queries/Edit/c018f2db-4a4f-4ce1-8r
digitalPersona.
DigitalPersona Reports
RITA\Len
Reporting Tools
Home / User authentication activity
Back
Save
Run now

This report is not a part of any subscription. To start receiving this report by email on a regular basis, create a new subscription .

User authentication activity

Reports user authentications by time and credential used

Query

End date	5/19/2017
Report data for previous	day
Computer name	
User account	
Activity result	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.*

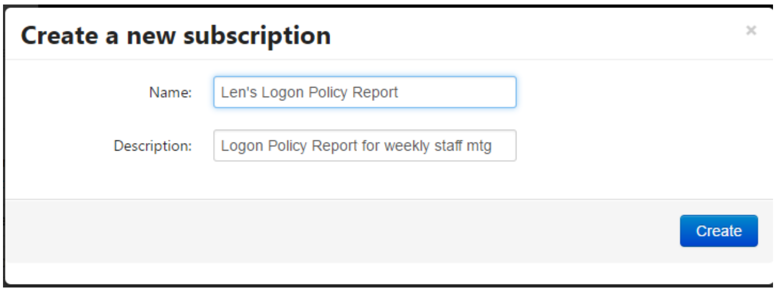
Note that data entered in the fields on this form is *not* automatically saved as you move from field to field. If you close a tab or browser window before Saving or Running a report your data will be lost.

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 169).

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*.

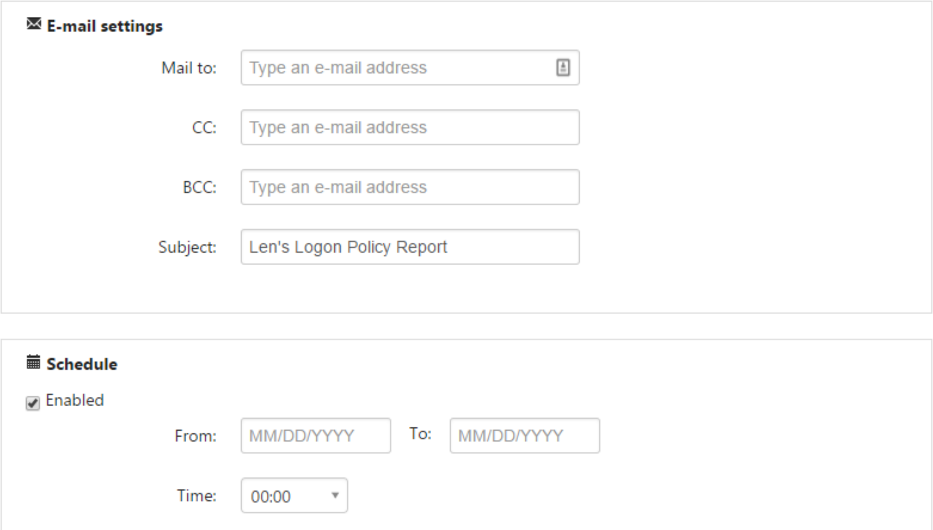


Create a new subscription

Name: Len's Logon Policy Report

Description: Logon Policy Report for weekly staff mtg

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

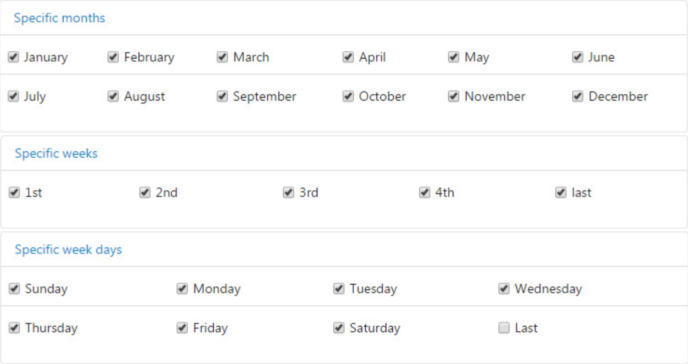
4. Enter a subject for the email that recipients will receive when they get the report.

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

☑ January ☑ February ☑ March ☑ April ☑ May ☑ June

☑ July ☑ August ☑ September ☑ October ☑ November ☑ December

Specific weeks

☑ 1st ☑ 2nd ☑ 3rd ☑ 4th ☑ last

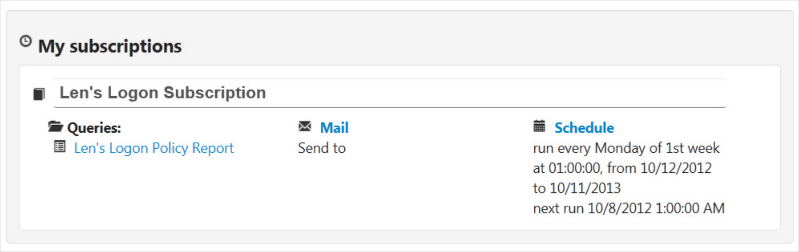
Specific week days

☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday

☑ Thursday ☑ Friday ☑ Saturday □ 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*.



My subscriptions

Len's Logon Subscription

Queries:
Len's Logon Policy Report

Mail
Send to

Schedule
run every Monday of 1st week
at 01:00:00, from 10/12/2012
to 10/11/2013
next run 10/8/2012 1:00:00 AM

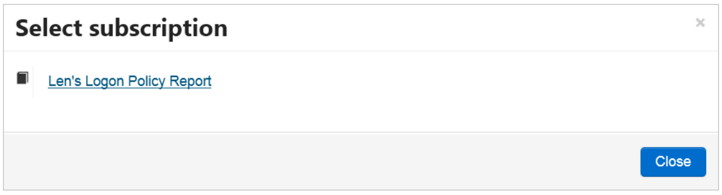
Adding a report to an existing subscription

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*.

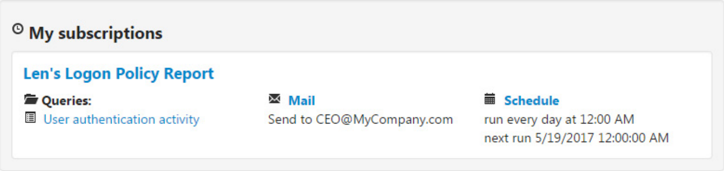
3. Select the subscription that you want to add the report to.



Select subscription

Len's Logon Policy Report

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



My subscriptions

Len's Logon Policy Report

Queries:
User authentication activity

Mail
Send to CEO@MyCompany.com

Schedule
run every day at 12:00 AM
next run 5/19/2017 12:00:00 AM

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?

DigitalPersona Events 16

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

Overview

DigitalPersona LDS 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	172
User Management	512	173
Secret Management	768	174
Service Management	1024	175
Password Manager	1536	176
Credential Authentication	2048	176
DNS Registration	2304	177
Deployment	4096	177
OTP Management	4358	178
Windows Logon	4864	178
Authentication Domain Management	5632	178
Behavior Training	6144	179
Identity Provider	6656	179

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 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 *132*).

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

These events may be generated during credentials management.

		Level	
Event	ID	Srvr	Clnt
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 beginning on page *314*.

*** 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

The user's fingerprints are enumerated 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 finger	9

User Management

Task Category: 512

These events may be generated during user management, and during import and export of user enrollment data to a file.

		Level	
Event	ID	Srvr	Clnt
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 User to the database	532	E	-
User deleted from the database	533	A	-
Cannot delete User from the database	534	E	-
User account was unlocked using Password Reset	535	A	E

		Level	
Event	ID	Srvr	Clnt
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
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

These events may be generated during Secret management.

		Level	
Event	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

		Level	
Event	ID	Srvr	Clnt
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

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

		Level	
Event	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.

		Level (Workstation)	
Event	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
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

These events may be generated during the authentication of credentials.

		Level	
Event	ID	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

These events may be generated during DNS registration.

		Level	
Event	ID	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

These events may be generated during license management operations.

		Level	
Event	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

These events may be generated during OTP management.

		Level	
Event	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

These events may be generated during Logon operations.

		Level	
Event	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 event*s. See the setting *Level of detail in event logs* on page *132*. Status events provide information about the state of various policies on client computers.

		Level	
Event	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.

Behavior Training

Task Category: 6144
The following events may be generated during Behavior Training operations.

Event	ID	Level*
User Behavior training is complete	6145	A
User’s primary credential has been changed. Behavior credential is reset back to training mode.	6146	A
Behavior credential is in training mode	6147	A
Level: E = Error, A - Audit, Dt = Details		

Identity Provider

Task Category: 6656
The following events may be generated during Identity Provider operations.

Event	ID	Level*
Pre-login success	6657	A
Local credential verification success	6658	A
External login success	6659	A

Event	ID	Level*
Resource owner password flow login success	6660	A
Refresh token refresh success	6661	A
Endpoint success	6662	A
Authorization code redeem success	6663	A
Pre-login failure	6689	A
Local credential verification failure	6690	A
External login failure	6691	A
Resource owner password flow login failure	6692	A
Refresh token refresh failure	6693	A
Endpoint failure	6694	A
Authorization code redeem failure	6695	A
External login error	6721	E
Unhandled exception	6722	E
Signing certificate has no private key, or key is not accessible	6723	E
Make sure the account running your application has access to the private key		
Signing certificate key length is less than 2048 bits	6724	E
Partial login complete	6753	Dt
A user was logged out	6754	A
Content Security Policy (CSP) report	6755	Dt
Client permissions revoked	6756	Dt
Access token issued	6757	Dt
Identity token issued	6758	Dt
Authorization code issued	6759	DtD
Refresh token issued	6760	Dt
No signing certificate configured	6761	E
The signing certificate will expire in the next 30 days	6762	A
Signing certificate validation success	6763	Dt
WS-Federation sign-in response issued	6764	A
Authentication policy has been satisfied	6765	A

Event	ID	Level*
Level: E = Error, A - Audit, Dt = Details		

* All events are written on the machine where WMC is installed, which may be on the same machine as the DigitalPersona Server or on a separate machine.

Password Manager Admin Tool 17

THIS CHAPTER DESCRIBES THE PASSWORD MANAGER ADMIN TOOL, AN OPTIONAL COMPONENT PROVIDED WITH DIGITALPERSONA PREMIUM THAT AN ADMINISTRATOR CAN USE TO CREATE MANAGED LOGONS TO WEBSITES, PROGRAMS AND NETWORK RESOURCES.

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 passwords, fingerprints and access cards) 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 HID Global 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.

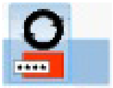
After managed logons are deployed, they are made available to managed computers after their next restart, or after a specified time interval as configured by the administrator.

- 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.

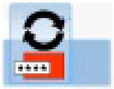
Each time that a user accesses the “trained” website, program or network resource, the Password Manager icon shown below is displayed in the upper left corner of the screen (Internet Explorer) or to the right of the first recognized entry field (Chrome), indicating that they can use any of their enrolled 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.

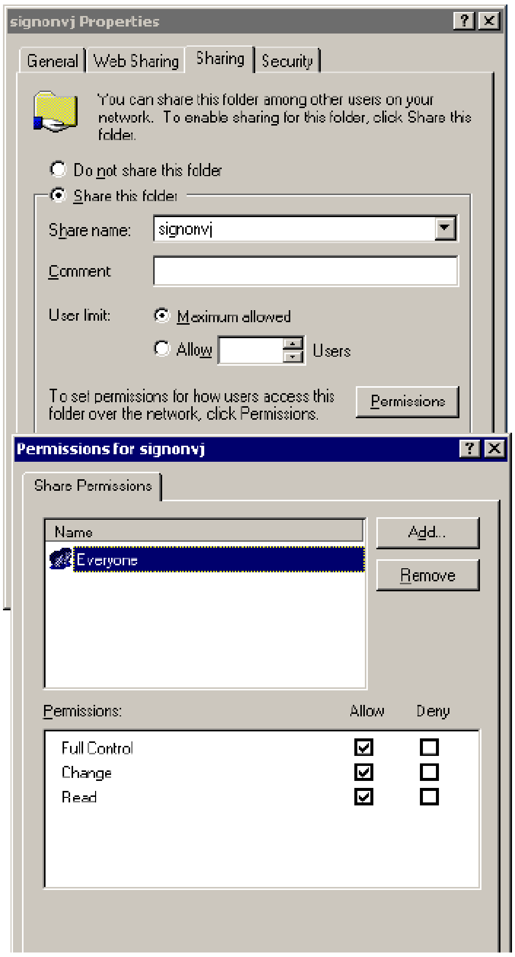
The folder should be created on a shared network drive accessible to the DigitalPersona server in order to make the logons available for deployment. However, the folder may be created on a local drive for initial testing and later copied to a shared drive. Folders are created and managed from the Logons 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.



signonvj Properties

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: signonvj

Comment:

User limit: ● Maximum allowed ○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

Permissions for signonvj

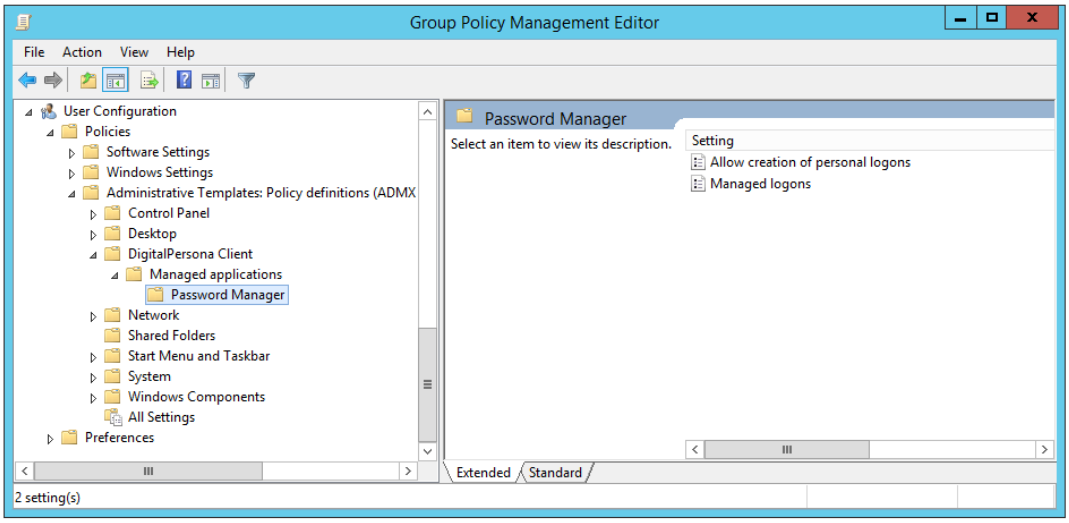
Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

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 the 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.



Password Manager

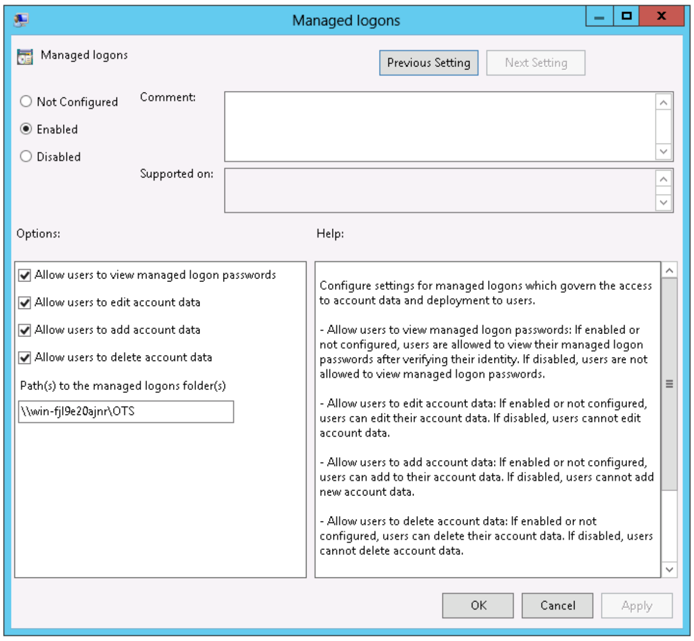
Select an item to view its description.

Setting
Allow creation of personal logons
Managed logons

2 setting(s)

4. Double click on *Managed logons* (in the right pane).

5. Click on *Enabled* to enable this policy. The default setting is "Not Configured."



○ Not Configured
● Enabled
○ Disabled

☑ Allow users to view managed logon passwords
☑ Allow users to edit account data
☑ Allow users to add account data
☑ Allow users to delete account data

Path(s) to the managed logons folder(s): \\win-fjl9e20ajnr\OTS

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

- Allow users to view managed logon passwords: If enabled or not configured, users are allowed to view their managed logon passwords after verifying their identity. If disabled, users are not allowed to view managed logon passwords.

- Allow users to edit account data: If enabled or not configured, users can edit their account data. If disabled, users cannot edit account data.

- Allow users to add account data: If enabled or not configured, users can add to their account data. If disabled, users cannot add new account data.

- Allow users to delete account data: If enabled or not configured, users can delete their account data. If disabled, users cannot delete account data.

6. Specify the path to the shared folder that you created in the previous section. To specify multiple folders, you can use the pipe (|) character.

7. 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.

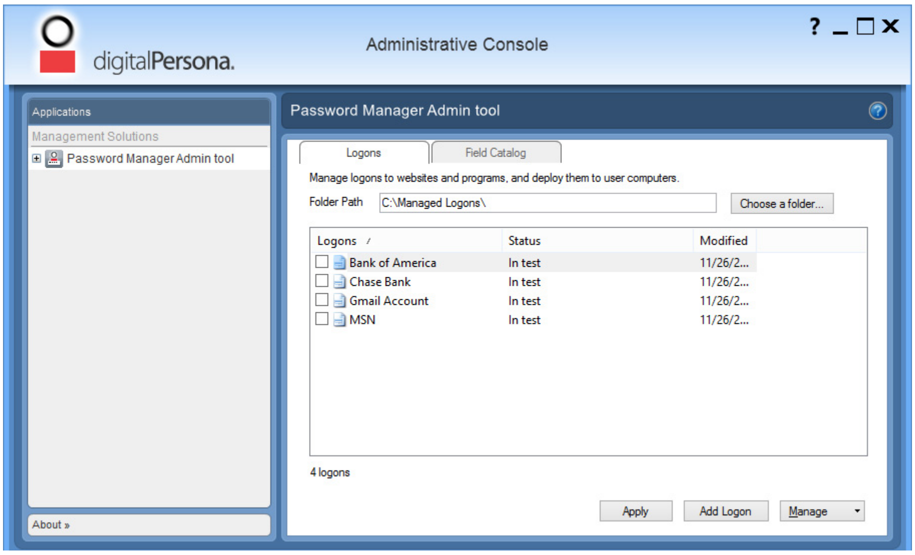
The Password Manager Admin Tool includes intuitive wizards that will guide you through the few steps necessary to automatically create a managed logon and an optional change password screen for most websites and programs. For more complex screens, there is also a manual mode that provides more sophisticated 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.



Manage logons to websites and programs, and deploy them to user computers.

Folder Path C:\Managed Logons\

Logons	Status	Modified
□ Bank of America	In test	11/26/2...
□ Chase Bank	In test	11/26/2...
□ Gmail Account	In test	11/26/2...
□ MSN	In test	11/26/2...

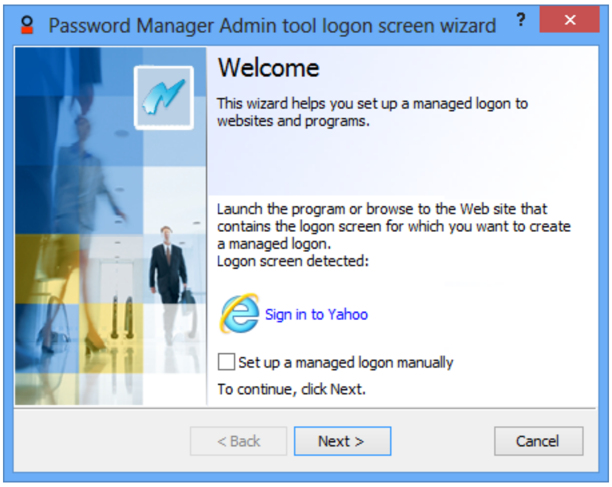
4 logons

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*.



Password Manager Admin tool logon screen wizard

Welcome

This wizard helps you set up a managed logon to websites and programs.

Launch the program or browse to the Web site that contains the logon screen for which you want to create a managed logon.
Logon screen detected:

Sign in to Yahoo

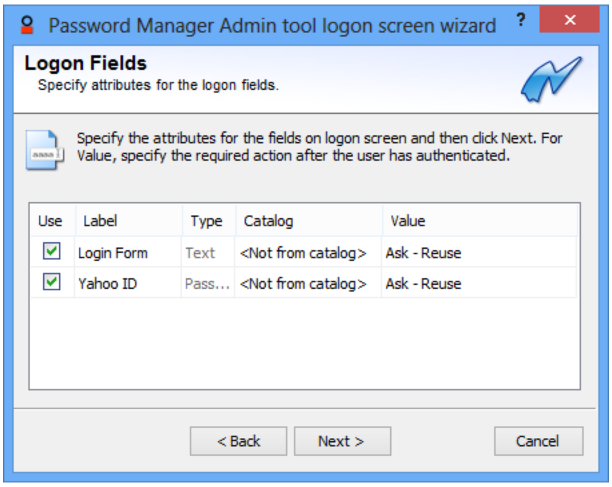
□ Set up a managed logon manually

To continue, 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 194*.

7. 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 - 189) and values (see page - 190) and then click *Next*.



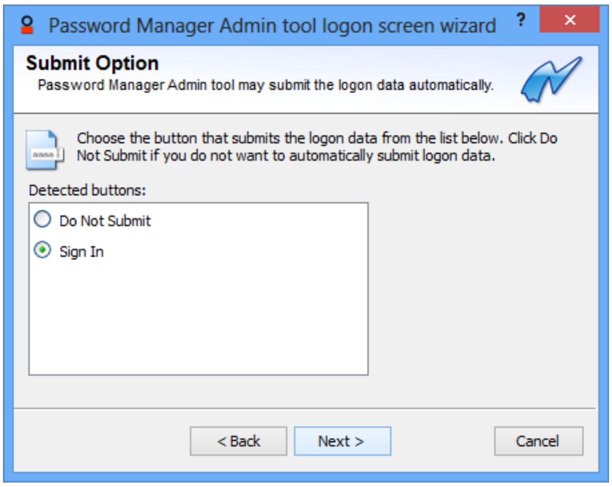
Logon Fields

Specify attributes for the logon fields.

Specify the attributes for the fields on logon screen and then click Next. For Value, specify the required action after the user has authenticated.

Use	Label	Type	Catalog	Value
☑	Login Form	Text	<Not from catalog>	Ask - Reuse
☑	Yahoo ID	Pass...	<Not from catalog>	Ask - Reuse

8. On the *Submit Option* page, choose the button that submits the logon data.



Submit Option

Password Manager Admin tool may submit the logon data automatically.

Choose the button that submits the logon data from the list below. Click Do Not Submit if you do not want to automatically submit logon data.

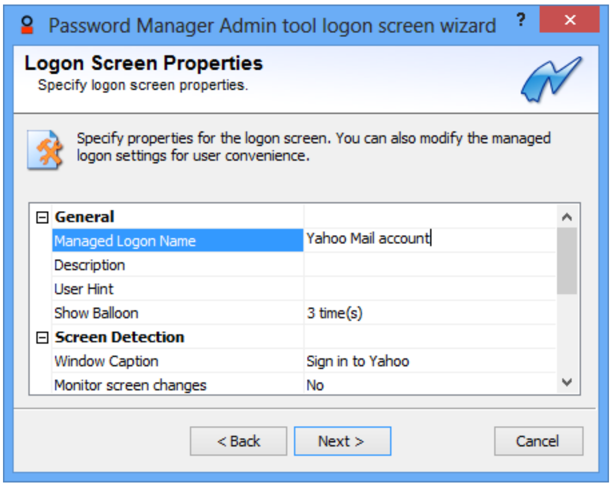
Detected buttons:

○ Do Not Submit

● Sign In

- 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.

9. Click *Next* to display the *Logon Screen Properties* page, where you can view and modify the various properties (see page - 191) for detailed descriptions of the Logon Screen properties.



Logon Screen Properties

Specify logon screen properties.

Specify properties for the logon screen. You can also modify the managed logon settings for user convenience.

⊟ **General**	
Managed Logon Name	Yahoo Mail account
Description	
User Hint	
Show Balloon	3 time(s)
⊟ **Screen Detection**	
Window Caption	Sign in to Yahoo
Monitor screen changes	No

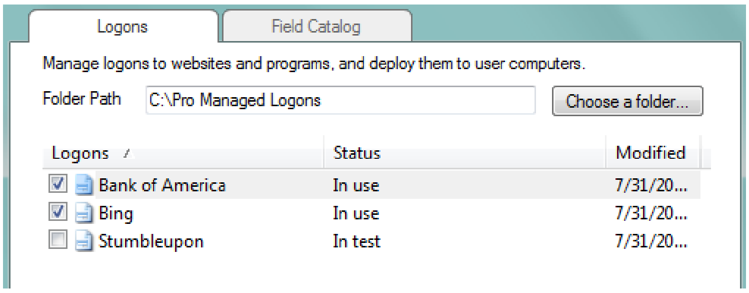
10. Click *Next*, and then click *Finish* to create the logon and close the wizard.

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 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.



Manage logons to websites and programs, and deploy them to user computers.

Folder Path: C:\Pro Managed Logons

Logons	Status	Modified
☑ Bank of America	In use	7/31/20...
☑ Bing	In use	7/31/20...
☐ Stumbleupon	In test	7/31/20...

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:

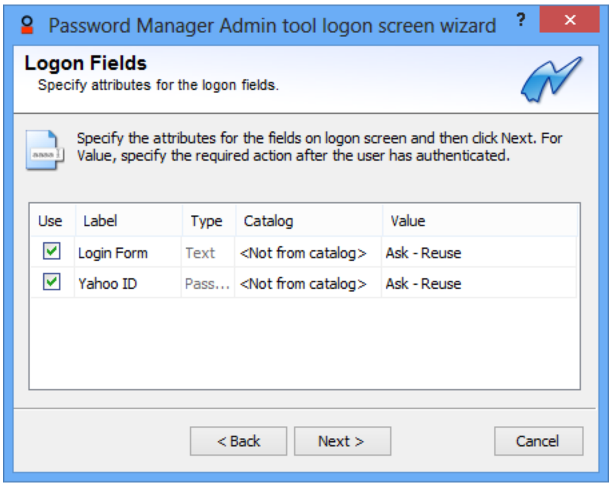
Logons created by the administrator (also called *managed* logons) take precedence over any personal logons created for the same screen by the application. The personal logon will no longer be able to be used to log on, but can be opened from the *Personal tab* by right-clicking the logon and selecting *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 *194*.

Logon Fields attributes

Logon Fields attributes are used in the Logon Screen Wizard during the creation of managed logons and Change Password screens.



Logon Fields

Specify attributes for the logon fields.

Specify the attributes for the fields on logon screen and then click Next. For Value, specify the required action after the user has authenticated.

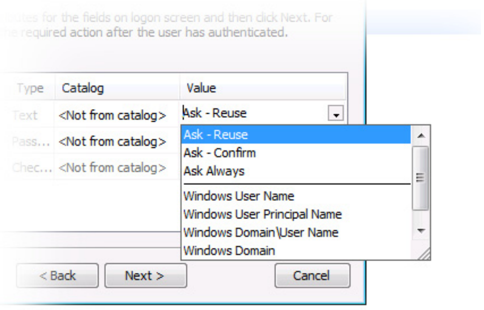
Use	Label	Type	Catalog	Value
☑	Login Form	Text	<Not from catalog>	Ask - Reuse
☑	Yahoo ID	Pass...	<Not from catalog>	Ask - Reuse

Column headings specify the attributes for each field on a Logon Screen or Change Password screen.

Field	Description
Use	Check the *Use* 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. *Password* hides the password on the logon screen so it cannot be viewed. *Text* displays readable text.
Catalog	For added convenience, you can create specifications for frequently used fields using the Field Catalog 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 211.
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.



utes for the fields on logon screen and then click Next. For
e required action after the user has authenticated.

Type	Catalog	Value
Text	<Not from catalog>	Ask - Reuse
Pass...	<Not from catalog>	
Chec...	<Not from catalog>	

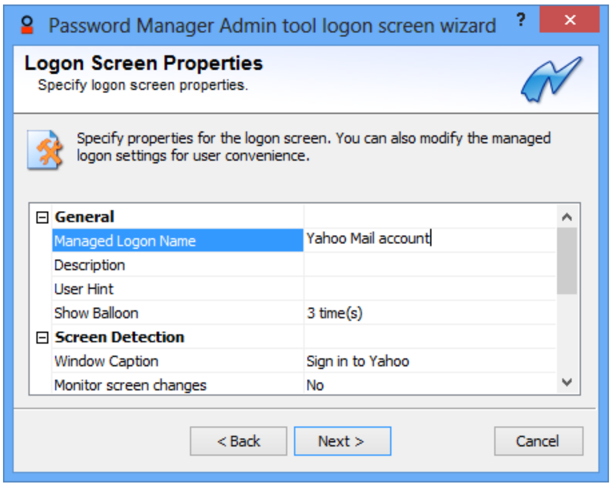
A Value dropdown menu provides a list of options for specifying values to be supplied by the user or automatically by Password Manager. The available options vary depending on the type of field selected.

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.

Option	Description
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.
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.


Password Manager Admin tool logon screen wizard
Logon Screen Properties
Specify logon screen properties.
< Back
Next >
Cancel

Specify properties for the logon screen. You can also modify the managed logon settings for user convenience.

⊟ General	
Managed Logon Name	Yahoo Mail account
Description	
User Hint	
Show Balloon	3 time(s)
⊟ Screen Detection	
Window Caption	Sign in to Yahoo
Monitor screen changes	No

Category	Property	Description
General	Managed Logon Name	The name of the logon.

Category	Property	Description
	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 *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	Title of the screen as detected by the wizard; used to match the managed logon to the specified screen. 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. For example: *Some Application Login Some Company*Login My Bank Login*

Category	Property	Description
	Monitor screen changes	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. 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. Use of this setting is resource intensive, and it is disabled by default.
	URL	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: *Do Not Match* - This is the default. URL matching will not be performed. *String Match* - Matches the exact string displayed. *Wildcard Match* - Matches a displayed string utilizing an asterisk (*) to represent the portion of the URL that may change. *Regular Expression* - Matches a displayed string constructed as a regular expression (See *Regular Expression syntax* on page *207*). *Case Sensitive* - Ignore case when matching. *Restore Defaults* - Return to the default URL settings.

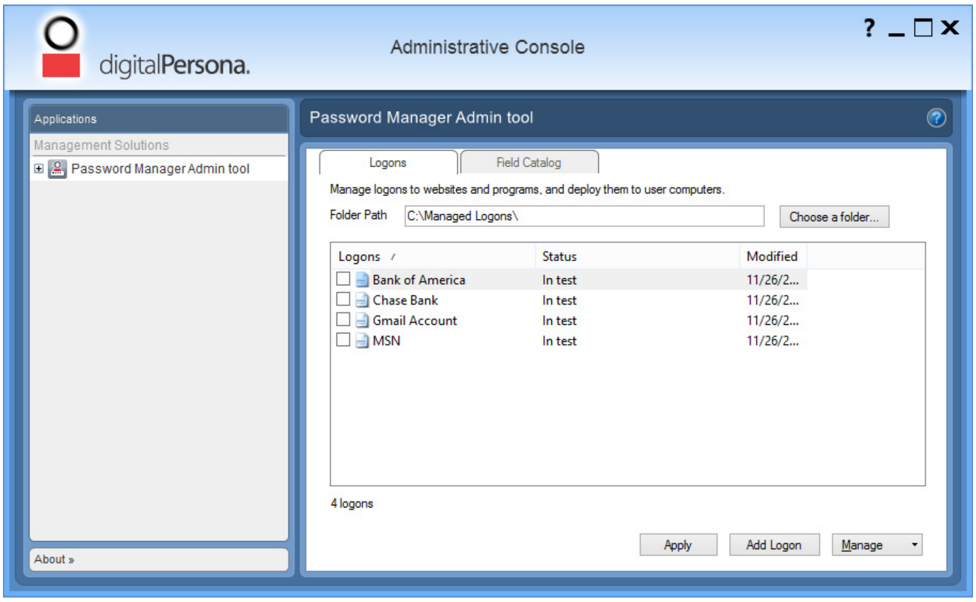
Category	Property	Description
	Extended Match	Displayed only when creating a logon for a program, not a website. Click the button next to the *Extended Match* field and select any labels that should be used for matching when recognizing the screen. Click the checkbox next to the labels to use. After making selections and clicking *OK*, 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.
Authentication	Start Authentication Immediately	If set to *Yes*, the user is prompted for their credential immediately after the logon screen displays. The default setting is *No*.
	Lock out logon fields	If set to *Yes*, the user is prevented from typing data in the logon fields. The default setting is *No*.
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:

1. From within the Administrative Console, launch the Password Manager Admin Tool.



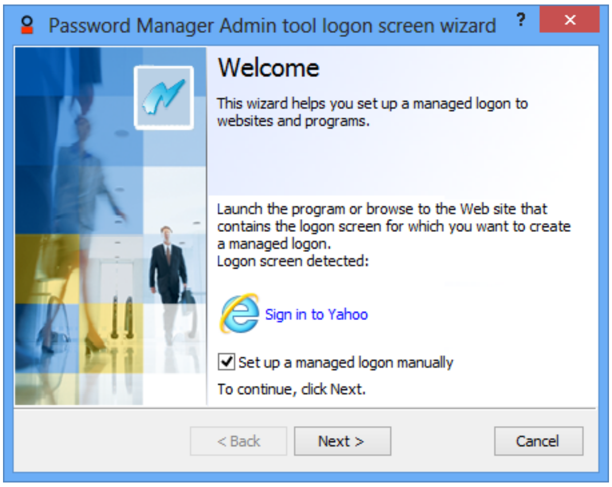
Manage logons to websites and programs, and deploy them to user computers.

Folder Path C:\Managed Logons\

Logons	Status	Modified
□ Bank of America	In test	11/26/2...
□ Chase Bank	In test	11/26/2...
□ Gmail Account	In test	11/26/2...
□ MSN	In test	11/26/2...

4 logons

2. 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*.
3. Click *Add Logon*. The Password Manager Admin Tool Logon wizard starts.
4. Launch the logon screen for the password-protected website or program.
5. On the first page of the wizard, confirm that the logon screen has been detected and verify the title of the logon screen.
6. Select *Set up a managed logon manually* and then click *Next*.



This wizard helps you set up a managed logon to websites and programs.

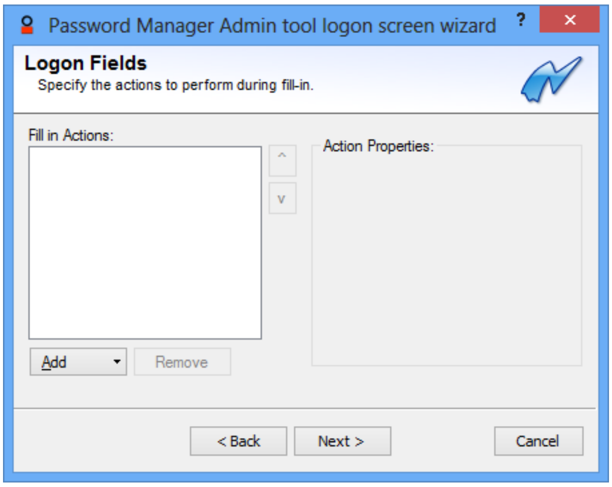
Launch the program or browse to the Web site that contains the logon screen for which you want to create a managed logon.
Logon screen detected:

Sign in to Yahoo

☑ Set up a managed logon manually

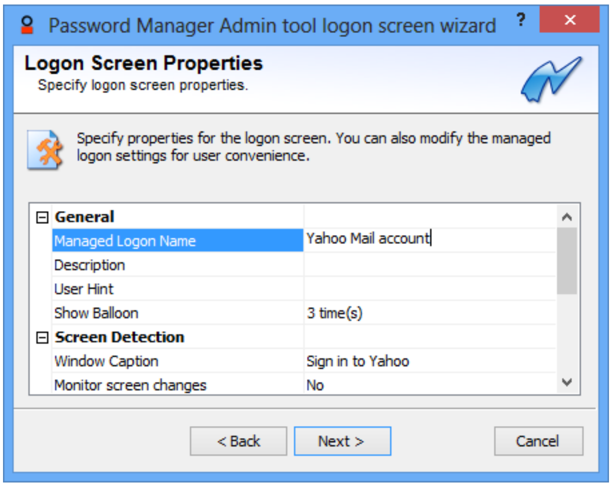
To continue, click Next.

7. On the *Logon Fields* page, click *Add* and select an action (see page 197) from the dropdown menu.


Password Manager Admin tool logon screen wizard
Logon Fields
Specify the actions to perform during fill-in.
Fill in Actions:
Action Properties:
Add
Remove
< Back
Next >
Cancel

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 - 191) for the logon screen.


Password Manager Admin tool logon screen wizard
Logon Screen Properties
Specify logon screen properties.
< Back
Next >
Cancel

Specify properties for the logon screen. You can also modify the managed logon settings for user convenience.

General	
Managed Logon Name	Yahoo Mail account
Description	
User Hint	
Show Balloon	3 time(s)
Screen Detection	
Window Caption	Sign in to Yahoo
Monitor screen changes	No

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.

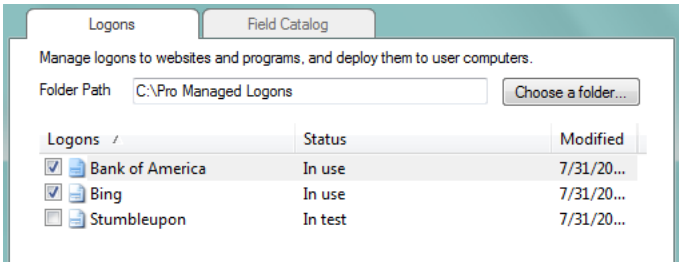
You do not have to click Apply after creating *each* logon or making every change, but you do need to click Apply before any new logons or changes to logons will be saved to the server.

See Also: Creating managed logons on page 186.

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.



Manage logons to websites and programs, and deploy them to user computers.

Folder Path C:\Pro Managed Logons

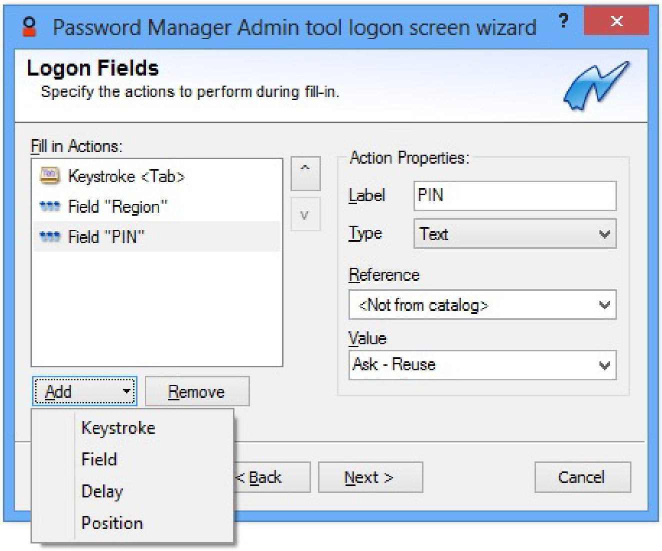
	Logons	Status	Modified
☑	Bank of America	In use	7/31/20...
☑	Bing	In use	7/31/20...
□	Stumbleupon	In test	7/31/20...

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 automacially 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.



Logon Fields

Specify the actions to perform during fill-in.

Fill in Actions:

- Keystroke <Tab>
- Field "Region"
- Field "PIN"

Action Properties:

Label: PIN

Type: Text

Reference: <Not from catalog>

Value: Ask - Reuse

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	Label - Type a label name for the corresponding field on the logon screen. The labels are displayed when users are prompted to type a value for a logon field. Type - Select the type of field, either **text** or **password**. Choosing password hides the password on the logon screen; choosing text displays readable text. Reference - Optionally, select a field previously defined on the Field Catalog tab. 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.
Delay	Specify how many seconds to wait before the next action in the list is performed.
Position	Specify a location where the system will perform a mouse click. Position is measured from the top left corner of the client window area. Client X - Type a number of pixels for the X axis position for the action. Client Y - Type a number of pixels for the Y axis position for the action. ⌖ 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.

Creating an extended authentication policy

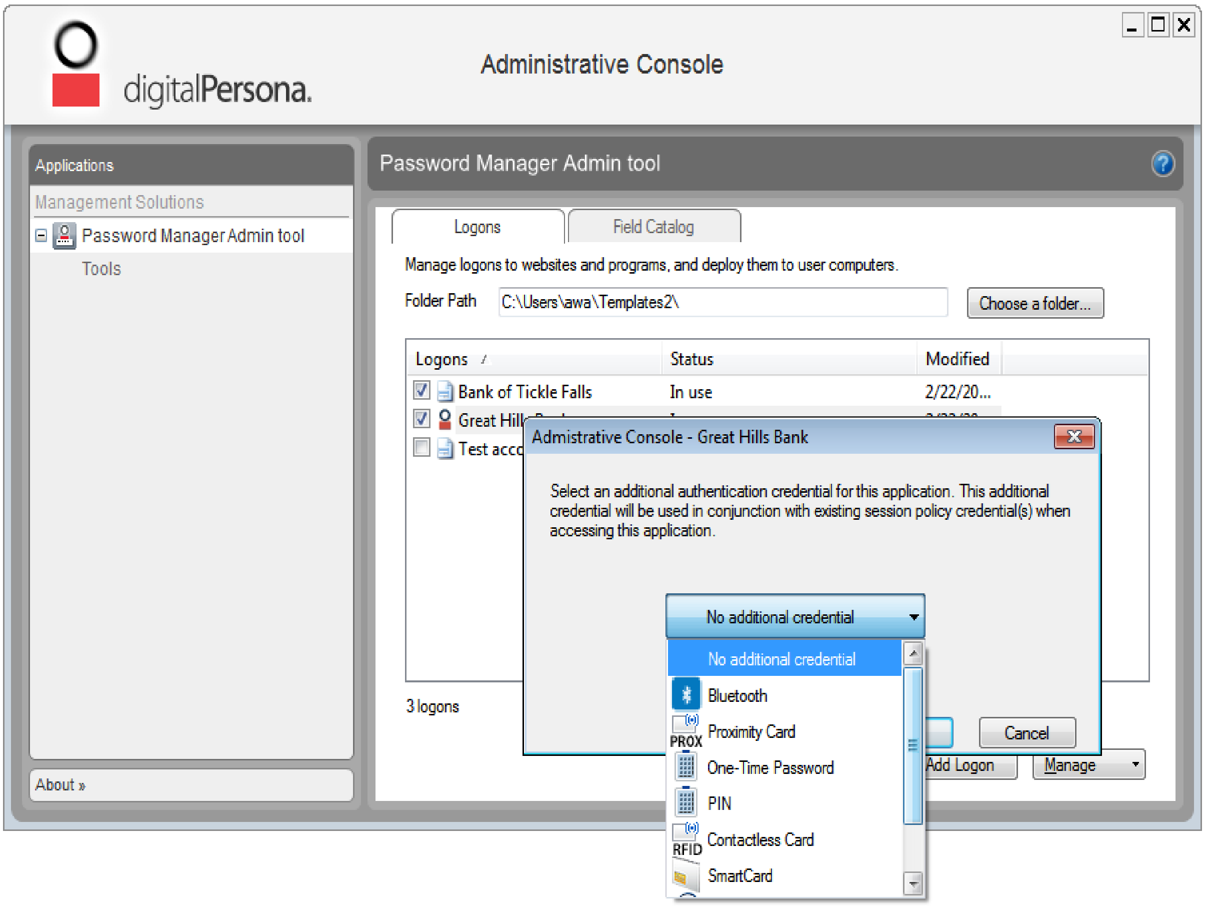
The authentication credentials required for users to access resources (websites, programs, etc.) through managed logons is defined by the DigitalPersona Session Authentication Policy.

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.



Manage logons to websites and programs, and deploy them to user computers.

Folder Path C:\Users\awa\Templates2\

Logons	Status	Modified
☑ Bank of Tickle Falls	In use	2/22/20...
☑ Great Hill		
□ Test acc		

3 logons

Admistrative Console - Great Hills Bank

Select an additional authentication credential for this application. This additional credential will be used in conjunction with existing session policy credential(s) when accessing this application.

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.

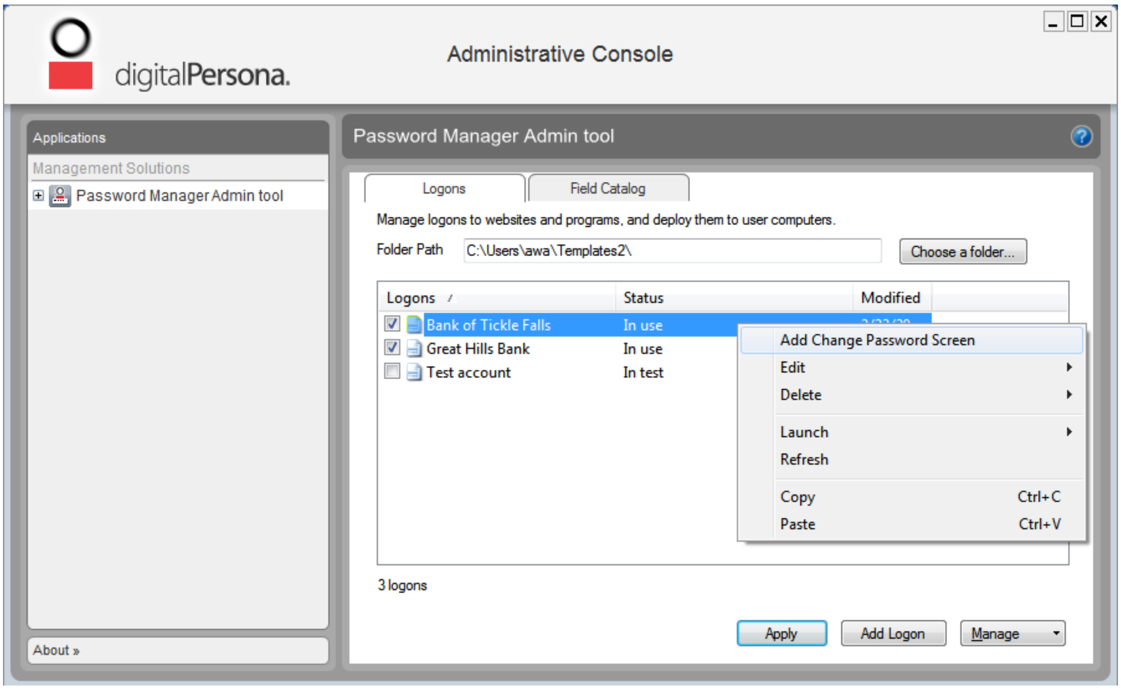
Setting Up a Change Password screen

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.



Manage logons to websites and programs, and deploy them to user computers.

Folder Path C:\Users\awa\Templates2\

Logons	Status	Modified
☑ Bank of Tickle Falls	In use	
☑ Great Hills Bank	In use	
□ Test account	In test	

3 logons

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.

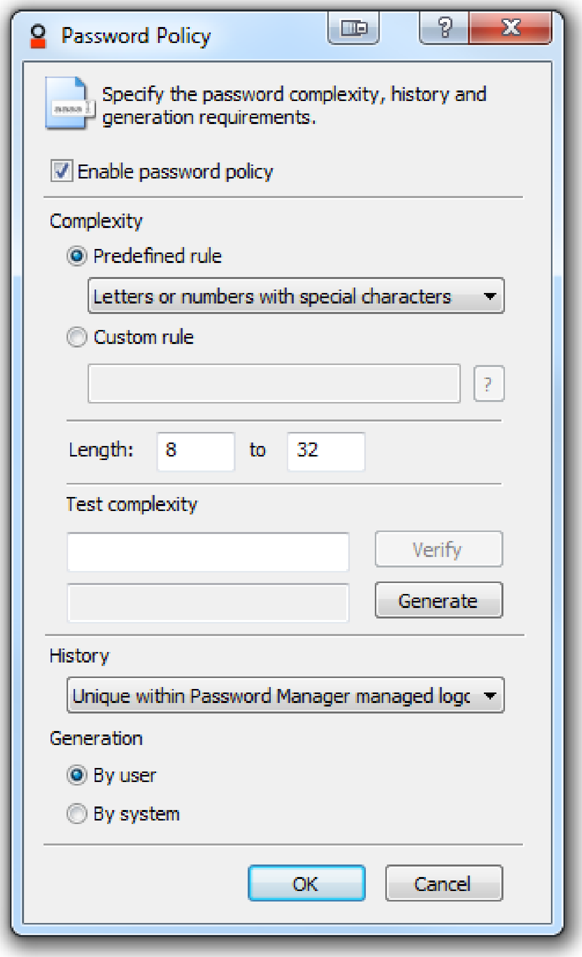
    You do not need to click Apply after creating making every change, but you do need to click Apply to save any changes that you have made.

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 194.

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.



Password Policy

Specify the password complexity, history and generation requirements.

☑ Enable password policy

Complexity

● Predefined rule

Letters or numbers with special characters

○ Custom rule

Length: 8 to 32

Test complexity

History

Unique within Password Manager managed logc

Generation

● By user

○ By system

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	
Predefined rule	The password must conform to the predefined rule selected from the dropdown menu. These include: Letters and numbers - allows any combination of letters and/or numbers. Numbers only - allows numbers only. Letters only - allows letters only. 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. Letters or numbers with at least one number - passwords may contain either letters or numbers with at least one number.

Option	Description
Custom rule	Enter a pattern for verifying or generating a password using the following notation: A = UPPERCASE LETTERS, i.e. A through Z a = lowercase letters, i.e. a through z d = digits, i.e. 0 through 9 s = special characters, i.e. !"#$%&'()*+,-./:;??@[\]^_`{|}~ ( ) = Use the enclosed indicators in random order. 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. [ ] = Define a custom character set i.e. [abcdef] would limit the user to only those letters in the specified position. 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. {n,m} Define a range of acceptable occurrences of the previously indicated character set. 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. 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. 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. ~ = Prevent two identical consecutive characters For example: This symbol would prevent passwords such as ab**CC**d or fkiq&**33**. & = Prevent a character being in the same position as in the most recent password For example: This symbol would prevent using the password abc**3**def if the most recent previous password was dar**3**feg.
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	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. *Verify* - Enter a password in the text field to the left of the Verify button and it will be verified against the defined complexity rule. *Click* 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.
History	From this dropdown menu, you can select additional password constraints relating to the history of the password. *None* - No other constraints are applied to the password contents. *Different than the Windows password* - The new password must be different than the current Windows password. *Unique within Password Manager managed logons* - The new password must be different from any other password associated with this managed logon for a specified user account. *Different than the current password* - The new password must be different than the current password for this website or program Note that the History constraints are not applied when verifying or generating passwords within this dialog, but only on an actual Change Password screen.
Generation	*By User* - 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. *By System* - Password Manager generates the password automatically. An alternate credential must be used to log on.

Setting up a Change Password Screen manually

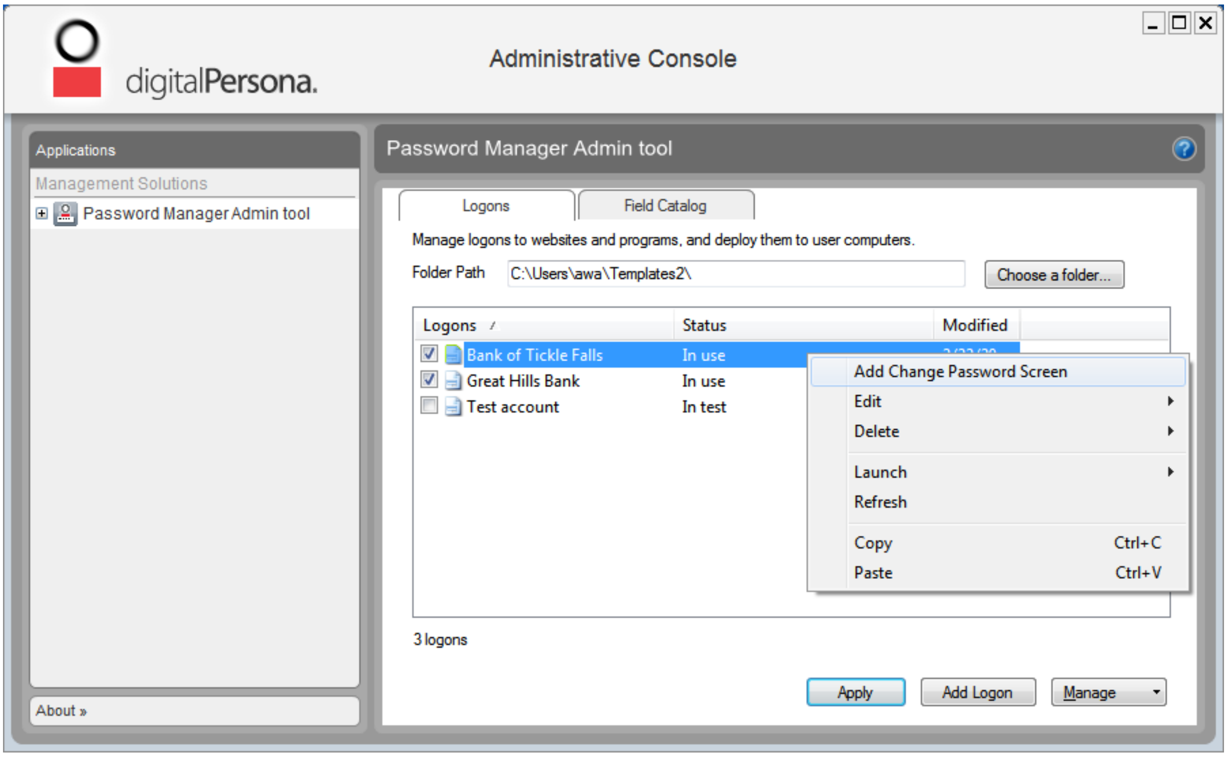
If the Password Manager Admin Tool does not detect fields automatically in Change Password screens, you can manually specify the fields and actions required. Creating a Change Password screen manually allows you to include additional controls such as adding keystrokes, forcing delays between actions, 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*.



Manage logons to websites and programs, and deploy them to user computers.

Folder Path C:\Users\awa\Templates2\

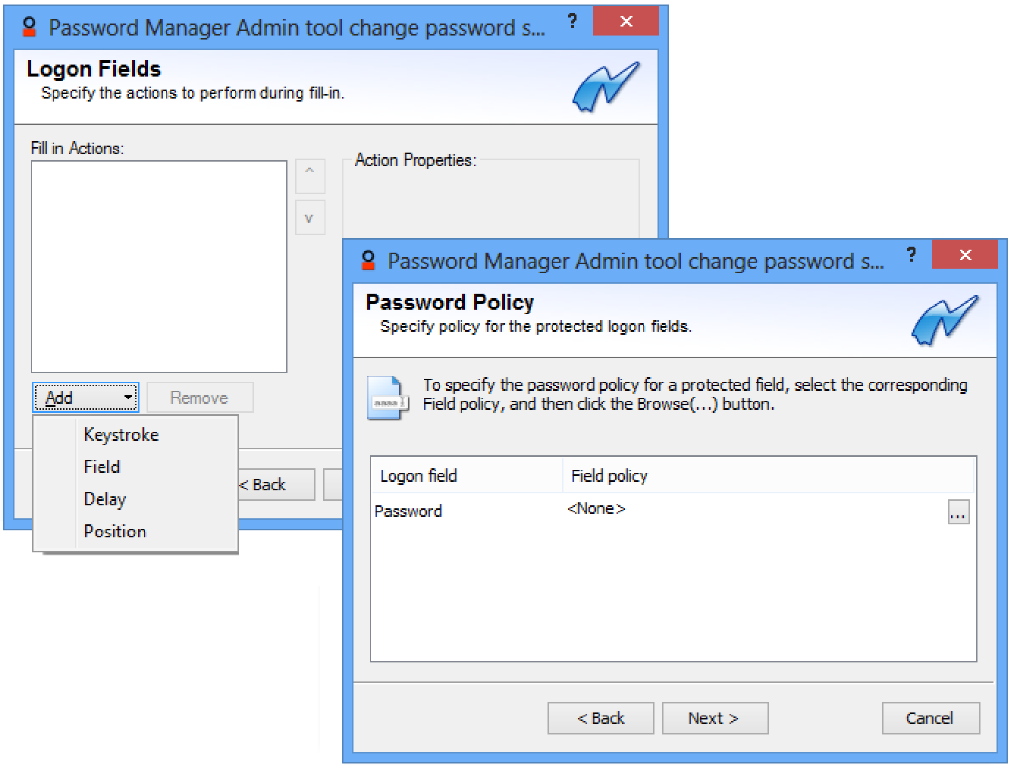
	Logons	Status	Modified
☑	Bank of Tickle Falls	In use	
☑	Great Hills Bank	In use	
□	Test account	In test	

3 logons

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.



Password Manager Admin tool change password s...

Logon Fields

Specify the actions to perform during fill-in.

Password Manager Admin tool change password s...

Password Policy

Specify policy for the protected logon fields.

To specify the password policy for a protected field, select the corresponding Field policy, and then click the Browse(...) button.

Logon field	Field policy
Password	<None>

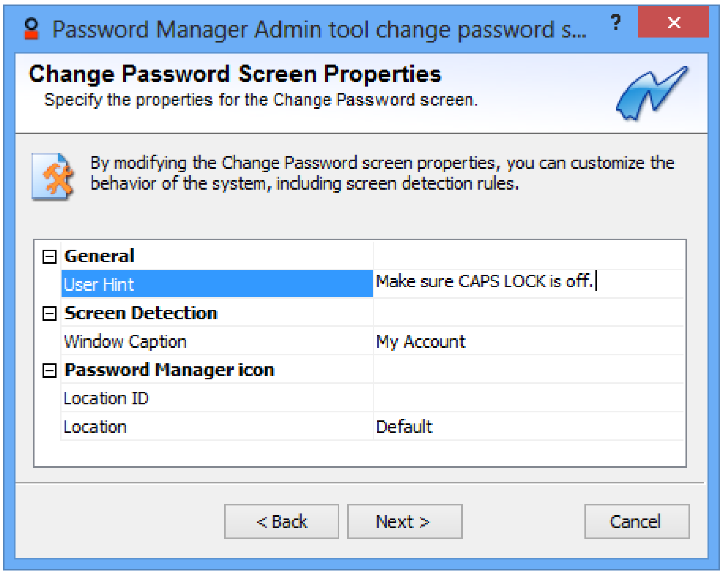
For example, you might study a Change Password screen and discover that it takes nine presses of the tab key to get to the first input field (Change Password).

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.



Password Manager Admin tool change password s...

Change Password Screen Properties

Specify the properties for the Change Password screen.

By modifying the Change Password screen properties, you can customize the behavior of the system, including screen detection rules.

⊟ **General**	
User Hint	Make sure CAPS LOCK is off.
⊟ **Screen Detection**	
Window Caption	My Account
⊟ **Password Manager icon**	
Location ID	
Location	Default

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

Regular Expression syntax

MC	Description
[ ]	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]. 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'.
[^]	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*	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 "abcac". 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 "*".
{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".
+	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: ab aaaaaaaab But will not match: b

MC	Description
|	The | operator will match either of its arguments, so for example: abc|def will match either "abc" or "def". Parenthesis can be used to group alternations, for example: ab(d|ef) will match either of "abd" or "abef".
?	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 196*).

The following logon management features are described in this section.

Feature	Page
Editing logons	209
Deleting logons	210
Deploying logons	210
The Field Catalog	211
Finding logons	212
Finding duplicate logons	213
Finding logons with enhanced authentication policies	213

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	189
Values	190
Logon properties	191
Logon Fields actions	197
Password policies	201

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:

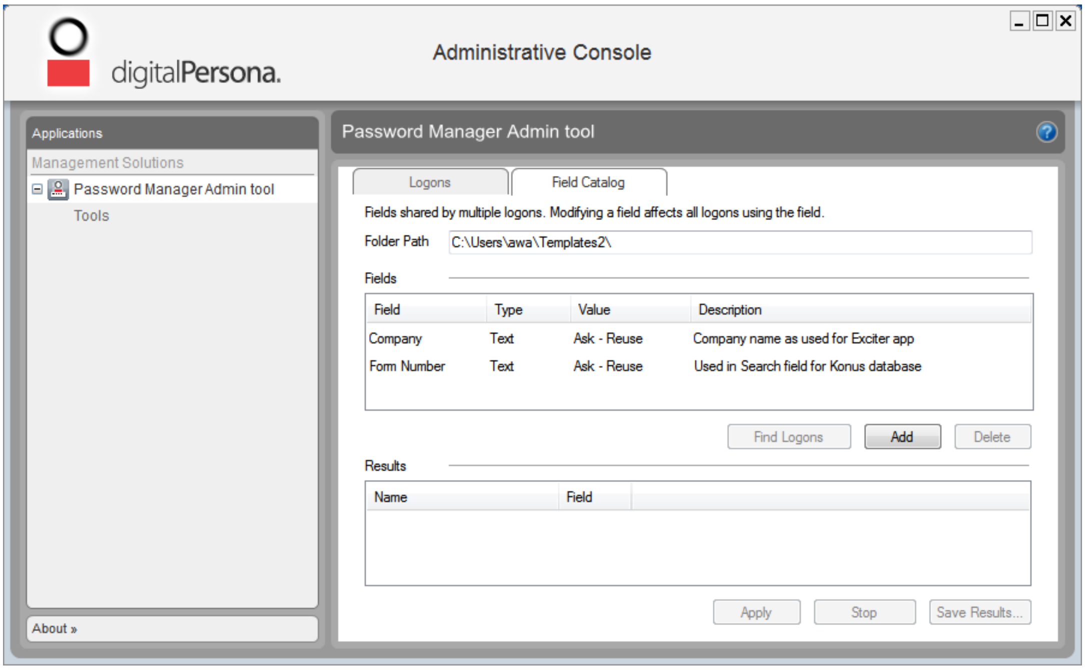
1. Check the boxes next to logons to change their status from *In Test* to *In Use*. Only logons with an *In Use* status will be visible to users.

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.



Fields shared by multiple logons. Modifying a field affects all logons using the field.

Folder Path C:\Users\awa\Templates2\

Field	Type	Value	Description
Company	Text	Ask - Reuse	Company name as used for Exciter app
Form Number	Text	Ask - Reuse	Used in Search field for Konus database

Name	Field

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 190) 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 194).
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 196.

Finding fields in logons

You can search for managed logons that contain fields selected from the Field Catalog.

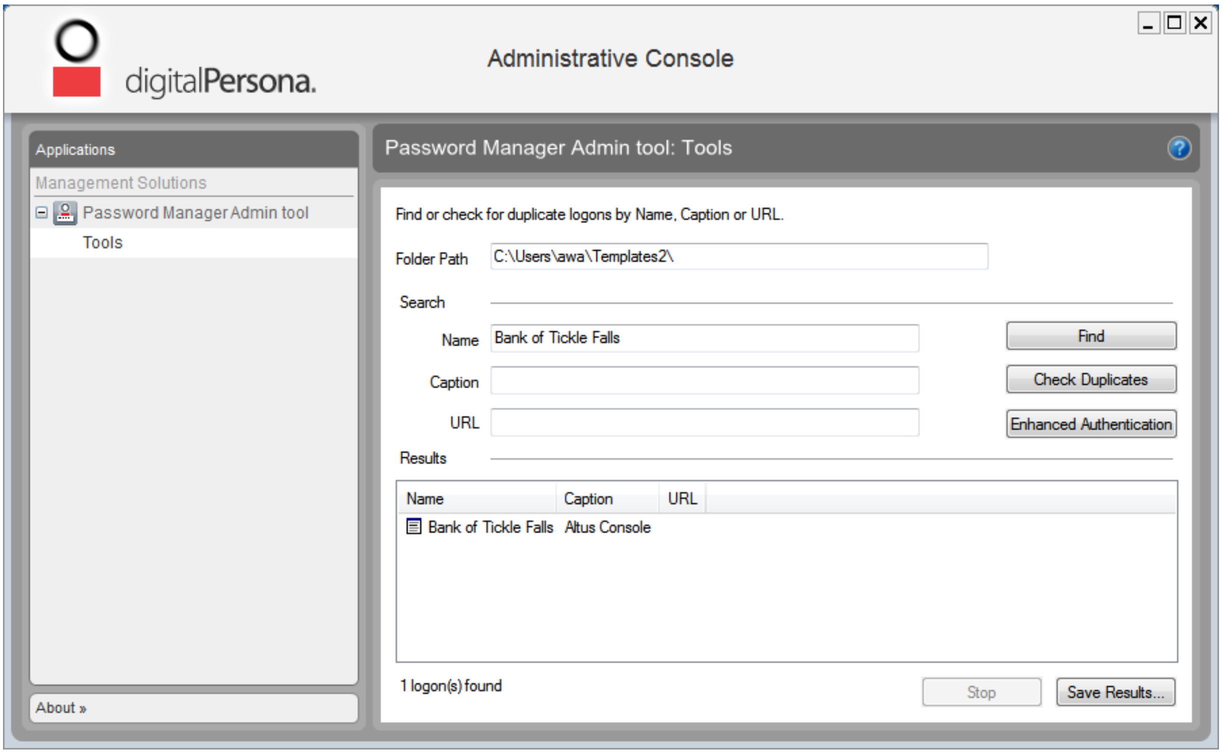
To search for logons that contain selected fields:

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.



Find or check for duplicate logons by Name, Caption or URL.

Folder Path: C:\Users\awa\Templates2\

Search

Name: Bank of Tickle Falls

Caption:

URL:

Results

Name	Caption	URL
Bank of Tickle Falls	Altus Console	

1 logon(s) found

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 authenticaiton 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.

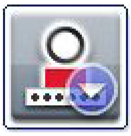
These settings can be configured in the Group Policy Management Editor under the node User Configuration\Policies\Administrative Templates\DigitalPersona Client\Managed Applications\Password Manager. More detailed explanations are provided on the Explain tab for each of the settings and in the *Policies and Settings* chapter of the DigitalPersona Administrator Guides.

Logging On

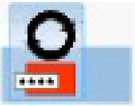
After creating managed logons and deploying them, users will then be able to launch a logon screen and verify their identity with their specified credentials.

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.



Internet Explorer



Chrome

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.

Changing passwords

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 LDS Administrator Guide includes the following chapters:

Web Management Components Installation 19

THIS CHAPTER DESCRIBES HOW TO INSTALL, CONFIGURE AND UNINSTALL THE WEB MANAGEMENT COMPONENTS.

The Web Management Components module contains a collection of components that together enable management of a DigitalPersona solution 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 LDS Server and the DigitalPersona LDS 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 and any pre-requisites, see the table beginning on page *19*.

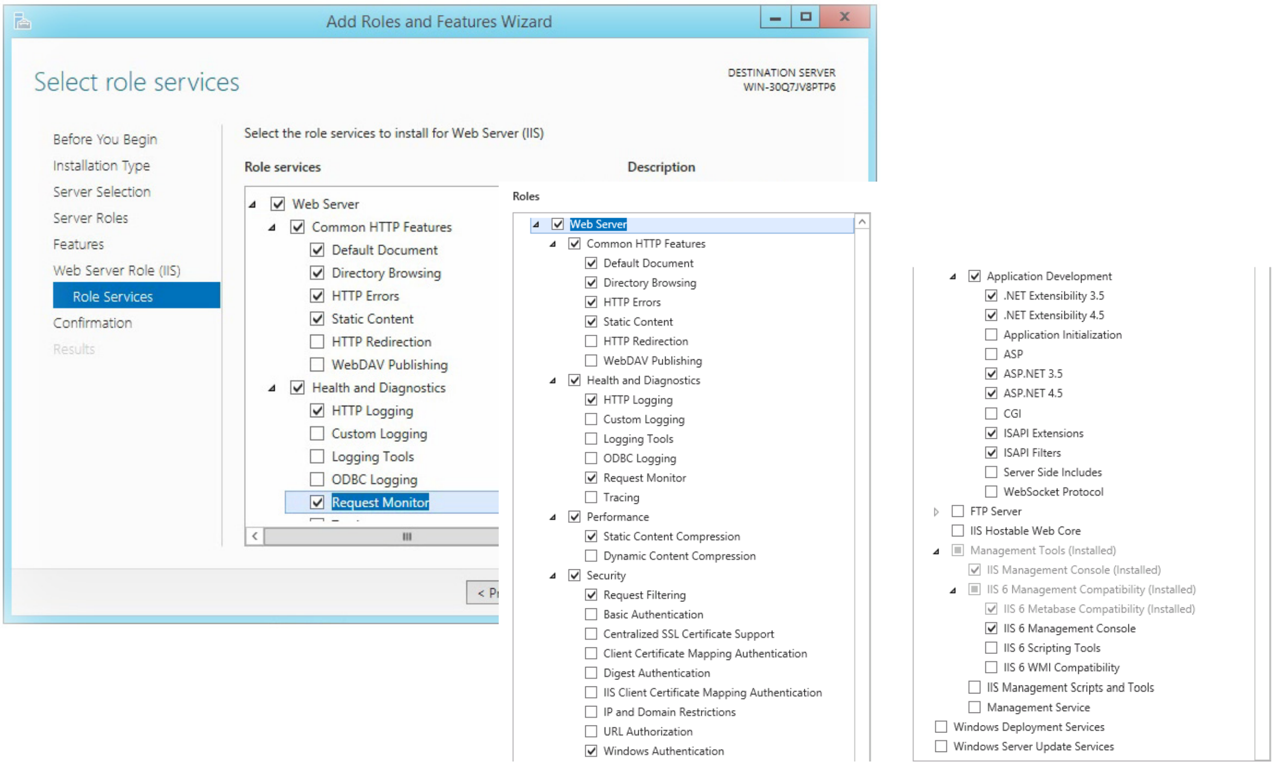
Installation wizard

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



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN-30Q7JV8PTP6

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services

Description

☑ Web Server
- ☑ Common HTTP Features
  - ☑ Default Document
  - ☑ Directory Browsing
  - ☑ HTTP Errors
  - ☑ Static Content
  - ☐ HTTP Redirection
  - ☐ WebDAV Publishing
- ☑ Health and Diagnostics
  - ☑ HTTP Logging
  - ☐ Custom Logging
  - ☐ Logging Tools
  - ☐ ODBC Logging
  - ☑ Request Monitor

< Pr

Roles

☑ Web Server
- ☑ Common HTTP Features
  - ☑ Default Document
  - ☑ Directory Browsing
  - ☑ HTTP Errors
  - ☑ Static Content
  - ☐ HTTP Redirection
  - ☐ WebDAV Publishing
- ☑ Health and Diagnostics
  - ☑ HTTP Logging
  - ☐ Custom Logging
  - ☐ Logging Tools
  - ☐ ODBC Logging
  - ☑ Request Monitor
  - ☐ Tracing
- ☑ Performance
  - ☑ Static Content Compression
  - ☐ Dynamic Content Compression
- ☑ Security
  - ☑ Request Filtering
  - ☐ Basic Authentication
  - ☐ Centralized SSL Certificate Support
  - ☐ Client Certificate Mapping Authentication
  - ☐ Digest Authentication
  - ☐ IIS Client Certificate Mapping Authentication
  - ☐ IP and Domain Restrictions
  - ☐ URL Authorization
  - ☑ Windows Authentication

- ☑ Application Development
  - ☑ .NET Extensibility 3.5
  - ☑ .NET Extensibility 4.5
  - ☐ Application Initialization
  - ☐ ASP
  - ☑ ASP.NET 3.5
  - ☑ ASP.NET 4.5
  - ☐ CGI
  - ☑ ISAPI Extensions
  - ☑ ISAPI Filters
  - ☐ Server Side Includes
  - ☐ WebSocket Protocol

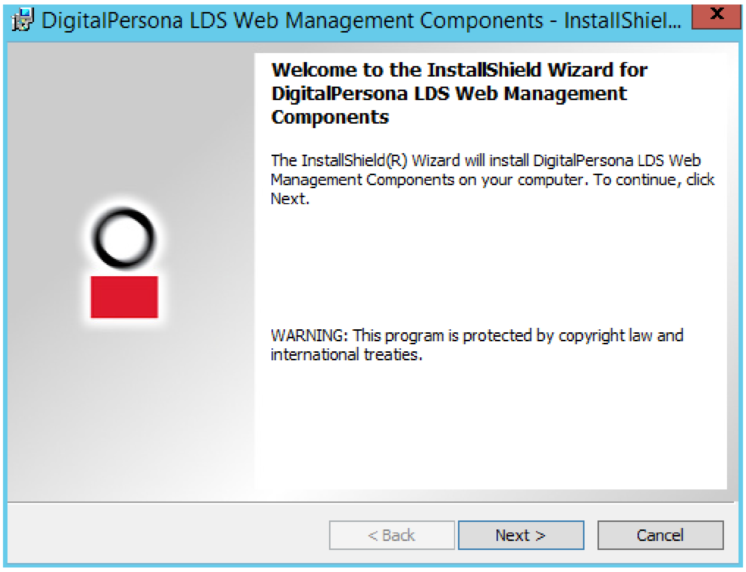
☐ FTP Server
☐ IIS Hostable Web Core
▣ Management Tools (Installed)
- ☑ IIS Management Console (Installed)
- ▣ IIS 6 Management Compatibility (Installed)
  - ☑ IIS 6 Metabase Compatibility (Installed)
  - ☑ IIS 6 Management Console
  - ☐ IIS 6 Scripting Tools
  - ☐ IIS 6 WMI Compatibility
- ☐ IIS Management Scripts and Tools
- ☐ Management Service

☐ Windows Deployment Services
☐ Windows Server Update Services

Installation steps

1. Locate and launch the *setup.exe* located in the *DPCA 2.2.0 SSO for Office 365\DigitalPersona LDS Web Management Components* folder within the product package. The *DigitalPersona LDS Web Management*

Components Wizard displays. If Windows Web Server (IIS) has not been previously added to the machine, it will be added as part of this process, and a reboot may be required in order to continue.

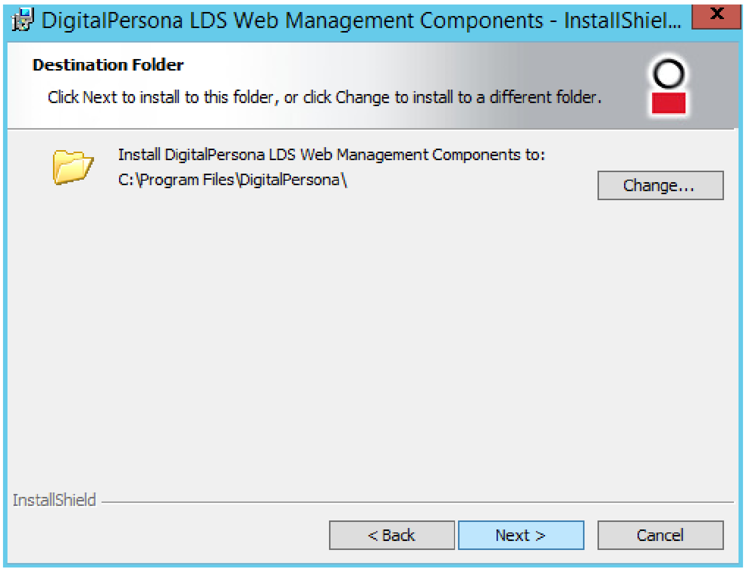

DigitalPersona LDS Web Management Components - InstallShiel...

Welcome to the InstallShield Wizard for DigitalPersona LDS Web Management Components

The InstallShield(R) Wizard will install DigitalPersona LDS Web Management Components on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. On the *Welcome* page, click *Next*. Then on the *License Agreement* page, accept the agreement and click *Next.*


DigitalPersona LDS Web Management Components - InstallShiel...

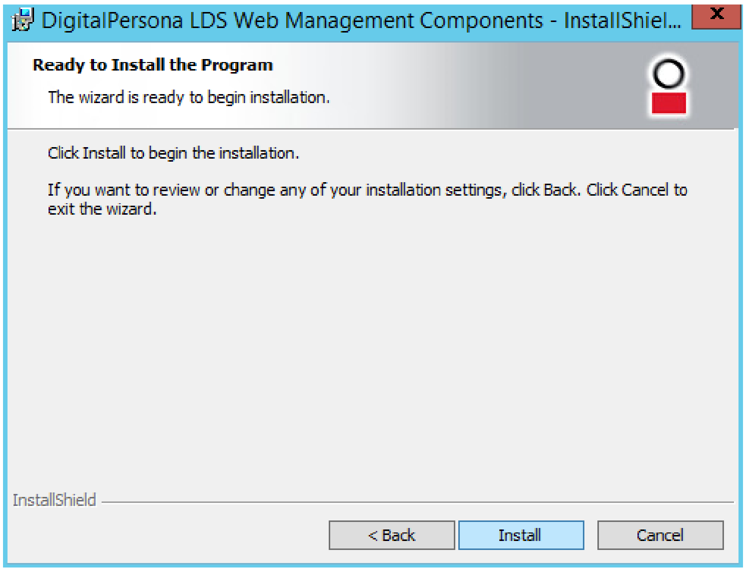
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install DigitalPersona LDS Web Management Components to:
C:\Program Files\DigitalPersona\

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.



DigitalPersona LDS Web Management Components - InstallShiel...

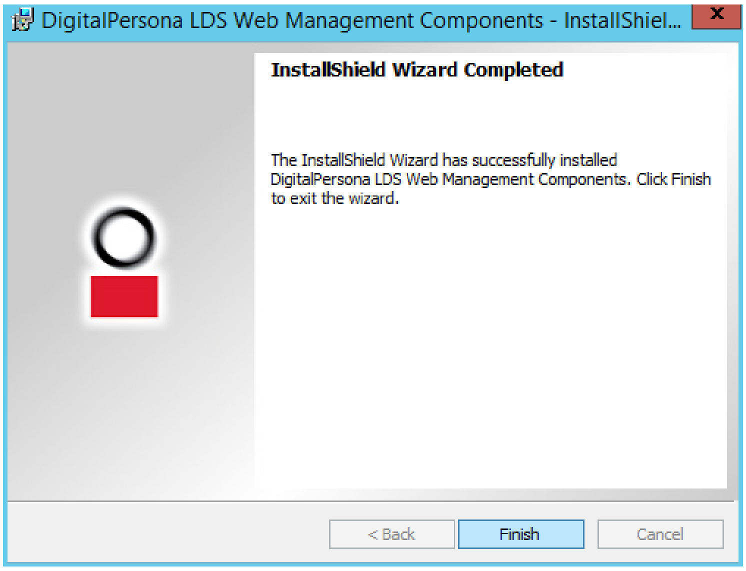
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

4. On the *Ready to Install the Program* page, click *Install*.



DigitalPersona LDS Web Management Components - InstallShiel...

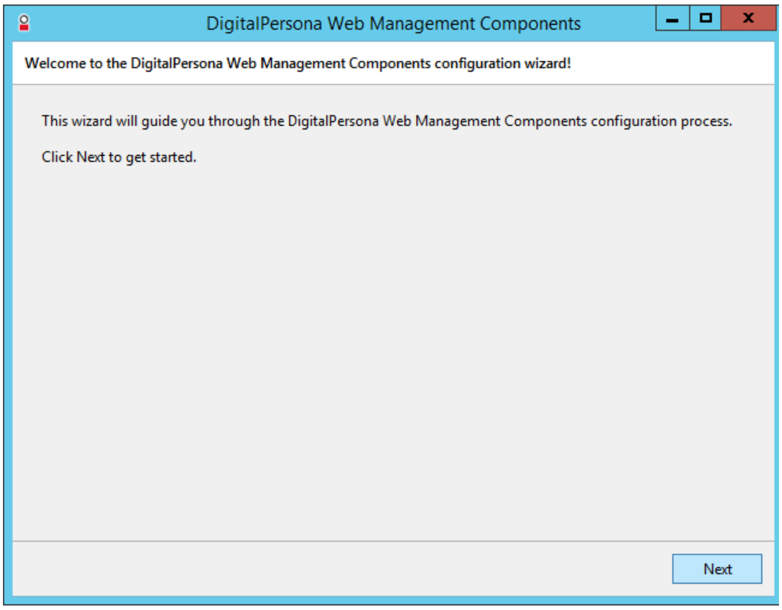
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DigitalPersona LDS Web Management Components. Click Finish to exit the wizard.

5. On the *InstallShield Wizard completed* page, click *Finish*.

Configuration wizard

Immediately following the completion of the installation wizard, a second wizard displays to guide you through the configuration process.



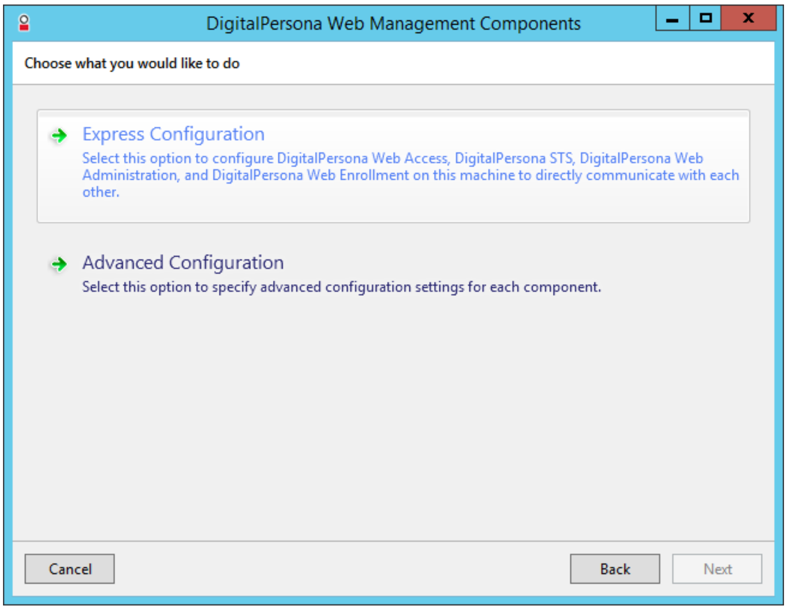
DigitalPersona Web Management Components

Welcome to the DigitalPersona Web Management Components configuration wizard!

This wizard will guide you through the DigitalPersona Web Management Components configuration process.

Click Next to get started.

1. Click *Next* to begin the configuration process.



DigitalPersona Web Management Components

Choose what you would like to do

Express Configuration
Select this option to configure DigitalPersona Web Access, DigitalPersona STS, DigitalPersona Web Administration, and DigitalPersona Web Enrollment on this machine to directly communicate with each other.

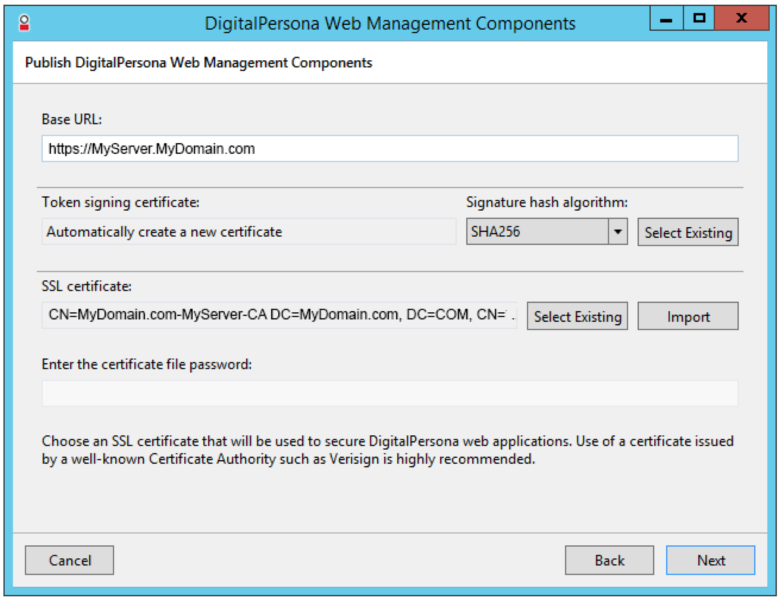
Advanced Configuration
Select this option to specify advanced configuration settings for each component.

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, either on a single machine or with each component on a separate machine.

Express Configuration

3. For *Express Configuration*, continue with the following steps. For Advanced Configuration, skip to the topic *Advanced Configuration*. on page *226.*



DigitalPersona Web Management Components

Publish DigitalPersona Web Management Components

Base URL:

https://MyServer.MyDomain.com

Token signing certificate: Automatically create a new certificate

Signature hash algorithm: SHA256

SSL certificate: CN=MyDomain.com-MyServer-CA DC=MyDomain.com, DC=COM, CN=

Enter the certificate file password:

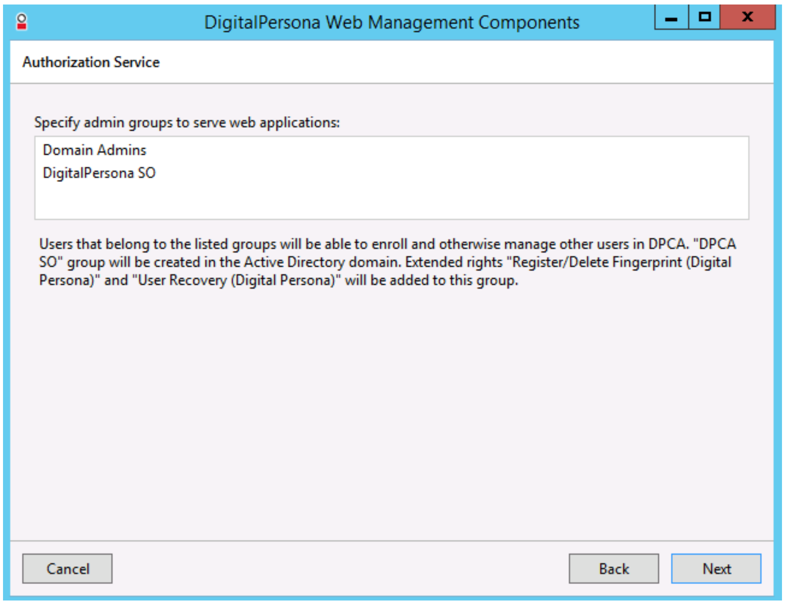
Choose an SSL certificate that will be used to secure DigitalPersona web applications. Use of a certificate issued by a well-known Certificate Authority such as Verisign is highly recommended.

4. Confirm that the Base URL is correct.

5. You can have the wizard create a token signing certificate automatically and choose the hash algorithm used to create it, or choose *Select Existing* to use a certificate of your own for token signing..

6. 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.

7. If the certificate is password protected, enter the password for the certificate. Do not select *Skip this page* unless you are using these components with the *DigitalPersona SSO for Office 365* package for Microsoft Azure. Click *Next*.



Authorization Service

Specify admin groups to serve web applications:

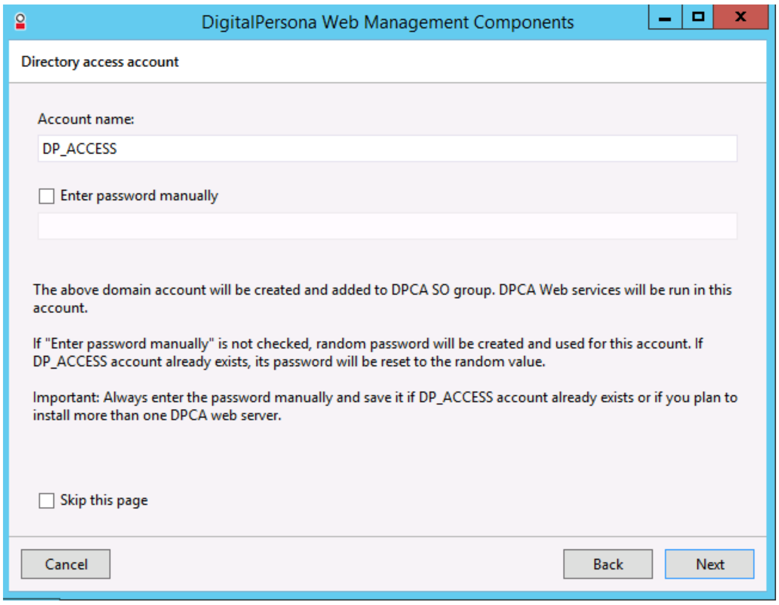
Domain Admins
DigitalPersona SO

Users that belong to the listed groups will be able to enroll and otherwise manage other users in DPCA. "DPCA SO" group will be created in the Active Directory domain. Extended rights "Register/Delete Fingerprint (Digital Persona)" and "User Recovery (Digital Persona)" will be added to this group.

8. The *Authorization Service* page specifies the groups who have administrative access to DigitalPersona web applications. By default these two groups are the Domain Admins and DigitalPersona Security Officers (DPCA SO). Users who need administrative access to DigitalPersona web applications should be added to one of these groups.

   Whichever group you decide to use for administraive access, it also needs to be added to the Administrators or Security Officers group in the Microsoft Authorization Manager.

9. Click *Next*.



Directory access account

Account name:

DP_ACCESS

□ Enter password manually

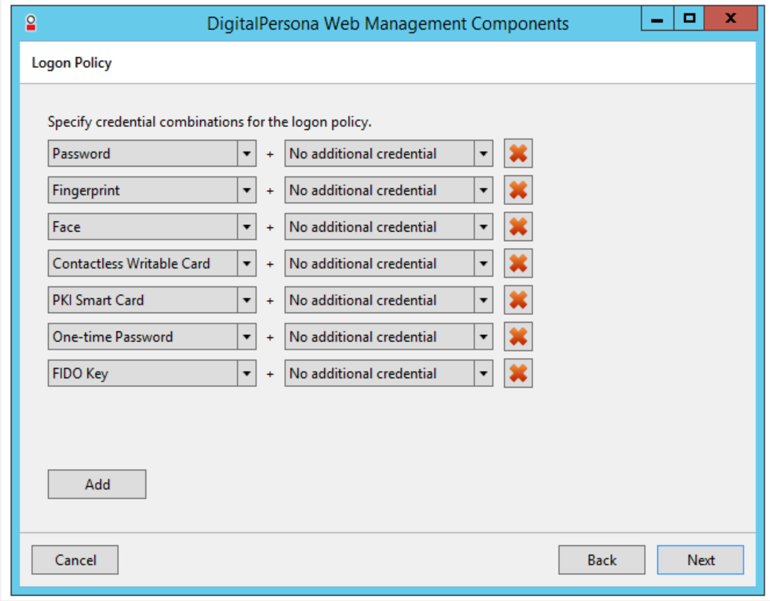
The above domain account will be created and added to DPCA SO group. DPCA Web services will be run in this account.

If "Enter password manually" is not checked, random password will be created and used for this account. If DP_ACCESS account already exists, its password will be reset to the random value.

Important: Always enter the password manually and save it if DP_ACCESS account already exists or if you plan to install more than one DPCA web server.

□ Skip this page

10. On the *Directory Access account* page, accept the default and click *Next*. If desired, select *Enter password manually* to create a password for the account. Click *Next.*



DigitalPersona Web Management Components

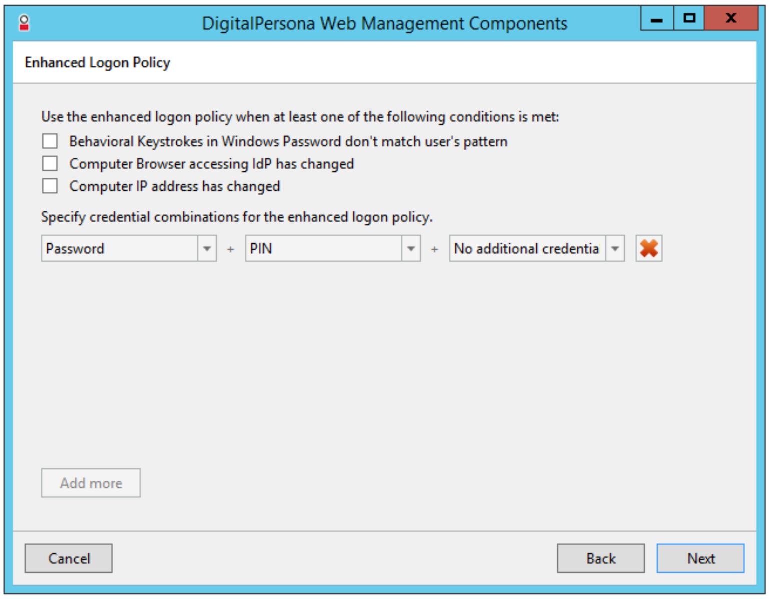
Logon Policy

Specify credential combinations for the logon policy.

Password + No additional credential ☒
Fingerprint + No additional credential ☒
Face + No additional credential ☒
Contactless Writable Card + No additional credential ☒
PKI Smart Card + No additional credential ☒
One-time Password + No additional credential ☒
FIDO Key + No additional credential ☒

11. On the *Authentication* page, specify each credential or credential combination that may be used to authenticate a user’s identity in DigitalPersona web applications. 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.

12. Click *Next* to continue.



DigitalPersona Web Management Components

Enhanced Logon Policy

Use the enhanced logon policy when at least one of the following conditions is met:

□ Behavioral Keystrokes in Windows Password don't match user's pattern
□ Computer Browser accessing IdP has changed
□ Computer IP address has changed

Specify credential combinations for the enhanced logon policy.

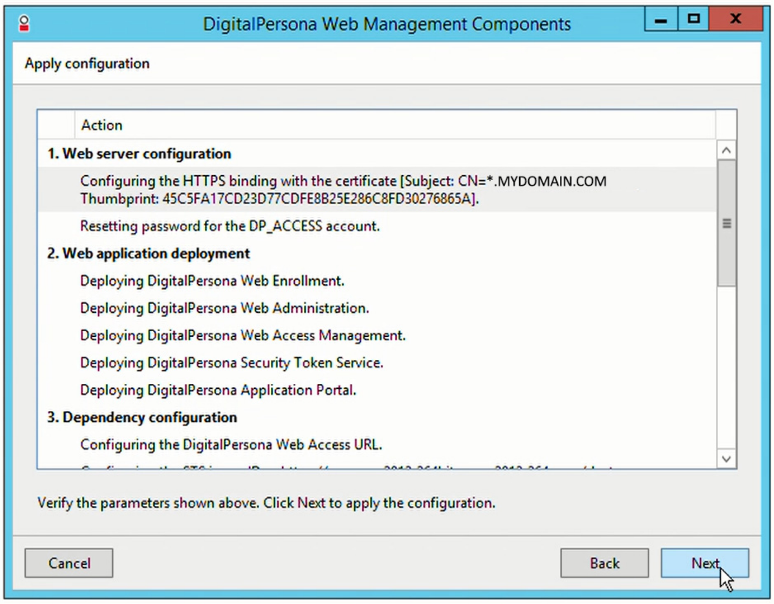
Password + PIN + No additional credentia ☒

13. The *Enhanced Logon Policy* page enables additional (step-up) authentication for the DigitalPersona Identity Server when any of the selected conditions occur.

- Select the desired conditions for step-up authentication.

- Specify up to three credentials that will be required for authentication when the selected conditions occur.
- To add additional credential combinations, click *Add more*.

Click *Next*. For more about step-up authentication, see the topic *Step-Up authentication* on page *233*.



Apply configuration

Action

1. Web server configuration

Configuring the HTTPS binding with the certificate [Subject: CN=*.MYDOMAIN.COM Thumbprint: 45C5FA17CD23D77CDFE8B25E286C8FD30276865A].

Resetting password for the DP_ACCESS account.

2. Web application deployment

Deploying DigitalPersona Web Enrollment.

Deploying DigitalPersona Web Administration.

Deploying DigitalPersona Web Access Management.

Deploying DigitalPersona Security Token Service.

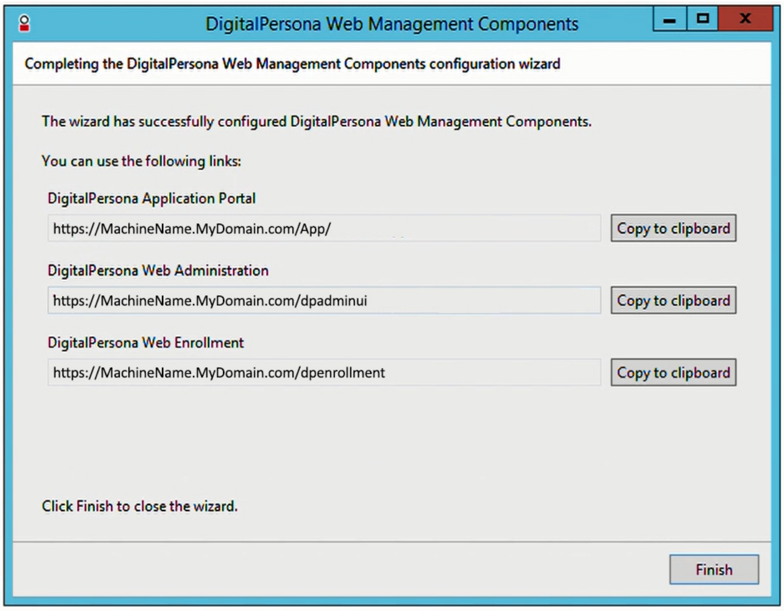
Deploying DigitalPersona Application Portal.

3. Dependency configuration

Configuring the DigitalPersona Web Access URL.

Verify the parameters shown above. Click Next to apply the configuration.

14. On the *Apply configuration* page, verify the actions that will be performed during configuration, and any parameters shown and then click *Next.*



Completing the DigitalPersona Web Management Components configuration wizard

The wizard has successfully configured DigitalPersona Web Management Components.

You can use the following links:

DigitalPersona Application Portal

https://MachineName.MyDomain.com/App/

DigitalPersona Web Administration

https://MachineName.MyDomain.com/dpadminui

DigitalPersona Web Enrollment

https://MachineName.MyDomain.com/dpenrollment

Click Finish to close the wizard.

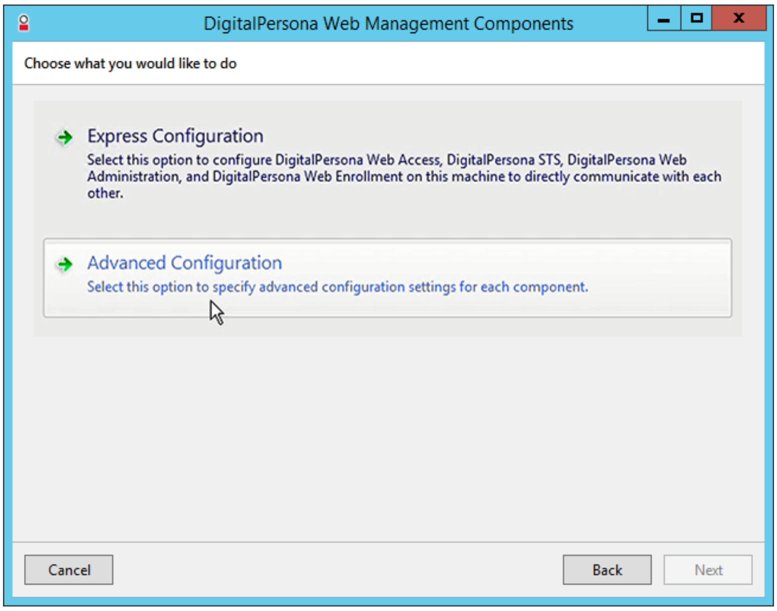
15. On the final page, the URLs to the three resulting web applications are shown. Click the button next to a URL to copy it to the clipboard so that you can open it in a supported browser. You may also want to create shortcuts to these pages for distribution to users. After testing the URLs and your ability to log in to the web applications, click *Finish* to close the wizard.

16. 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 installation wizard where *Advanced Configuration* is selected.

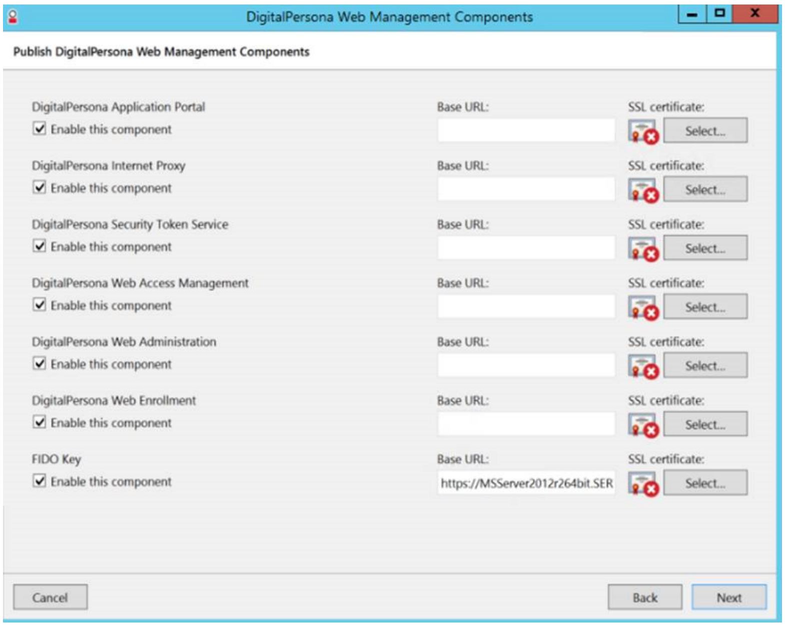


Choose what you would like to do

Express Configuration
Select this option to configure DigitalPersona Web Access, DigitalPersona STS, DigitalPersona Web Administration, and DigitalPersona Web Enrollment on this machine to directly communicate with each other.

Advanced Configuration
Select this option to specify advanced configuration settings for each component.

1. Create DNS records for each component.
2. After selecting *Advanced Configuration*, click *Next*.



Publish DigitalPersona Web Management Components

DigitalPersona Application Portal
☑ Enable this component
Base URL:
SSL certificate: Select...

DigitalPersona Internet Proxy
☑ Enable this component
Base URL:
SSL certificate: Select...

DigitalPersona Security Token Service
☑ Enable this component
Base URL:
SSL certificate: Select...

DigitalPersona Web Access Management
☑ Enable this component
Base URL:
SSL certificate: Select...

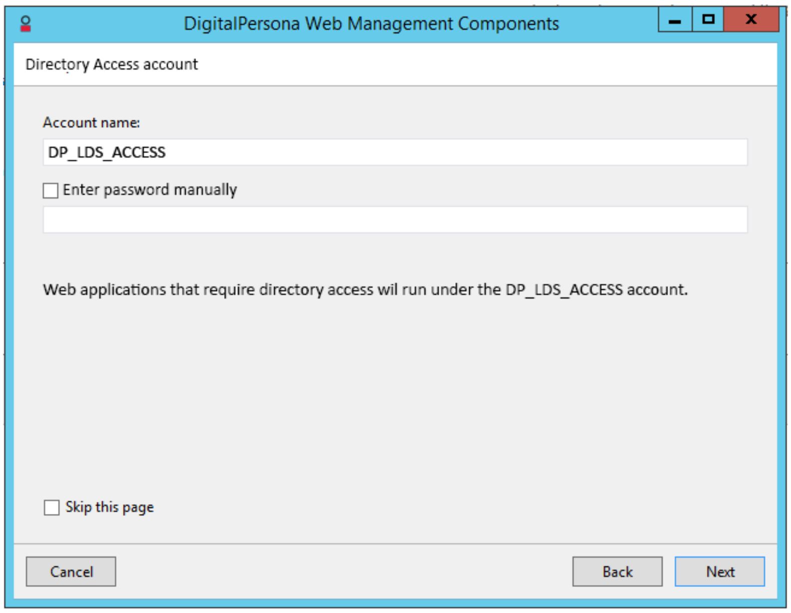
DigitalPersona Web Administration
☑ Enable this component
Base URL:
SSL certificate: Select...

DigitalPersona Web Enrollment
☑ Enable this component
Base URL:
SSL certificate: Select...

FIDO Key
☑ Enable this component
Base URL: https://MSServer2012r264bit.SER
SSL certificate: Select...

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*.



DigitalPersona Web Management Components

Directory Access account

Account name:

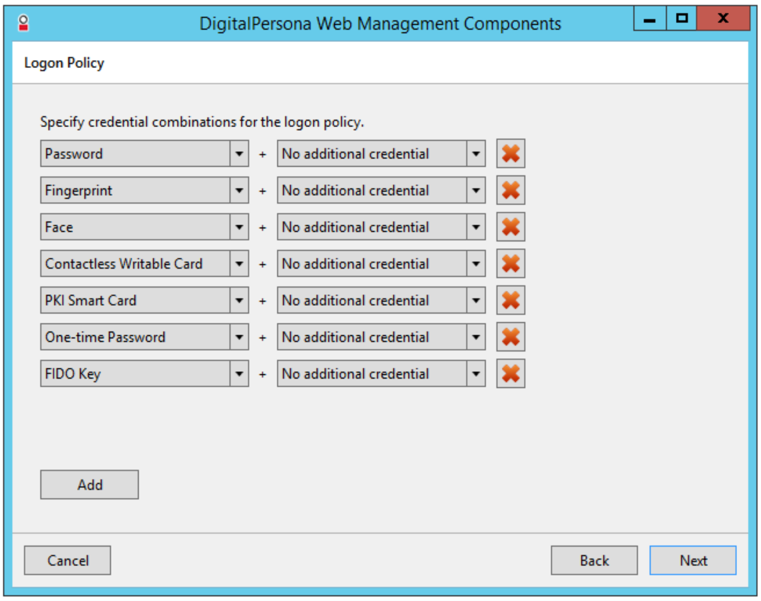
DP_LDS_ACCESS

□ Enter password manually

Web applications that require directory access wil run under the DP_LDS_ACCESS account.

□ Skip this page

6. On the *Directory Access account* page, accept the default and click *Next*.



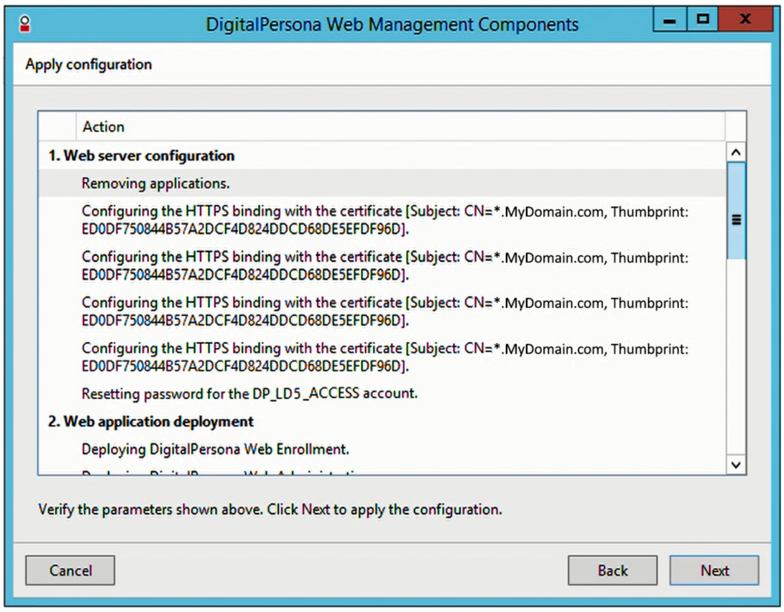
DigitalPersona Web Management Components

Logon Policy

Specify credential combinations for the logon policy.

Password	+	No additional credential	✖
Fingerprint	+	No additional credential	✖
Face	+	No additional credential	✖
Contactless Writable Card	+	No additional credential	✖
PKI Smart Card	+	No additional credential	✖
One-time Password	+	No additional credential	✖
FIDO Key	+	No additional credential	✖

7. On the *Authentication* page, specify each credential or credential combination that may be used to authenticate a user’s identity in DigitalPersona web applications. 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.



Apply configuration

Action

1. Web server configuration

Removing applications.

Configuring the HTTPS binding with the certificate [Subject: CN=*.MyDomain.com, Thumbprint: ED0DF750844B57A2DCF4D824DDCD68DE5EFDF96D].

Configuring the HTTPS binding with the certificate [Subject: CN=*.MyDomain.com, Thumbprint: ED0DF750844B57A2DCF4D824DDCD68DE5EFDF96D].

Configuring the HTTPS binding with the certificate [Subject: CN=*.MyDomain.com, Thumbprint: ED0DF750844B57A2DCF4D824DDCD68DE5EFDF96D].

Configuring the HTTPS binding with the certificate [Subject: CN=*.MyDomain.com, Thumbprint: ED0DF750844B57A2DCF4D824DDCD68DE5EFDF96D].

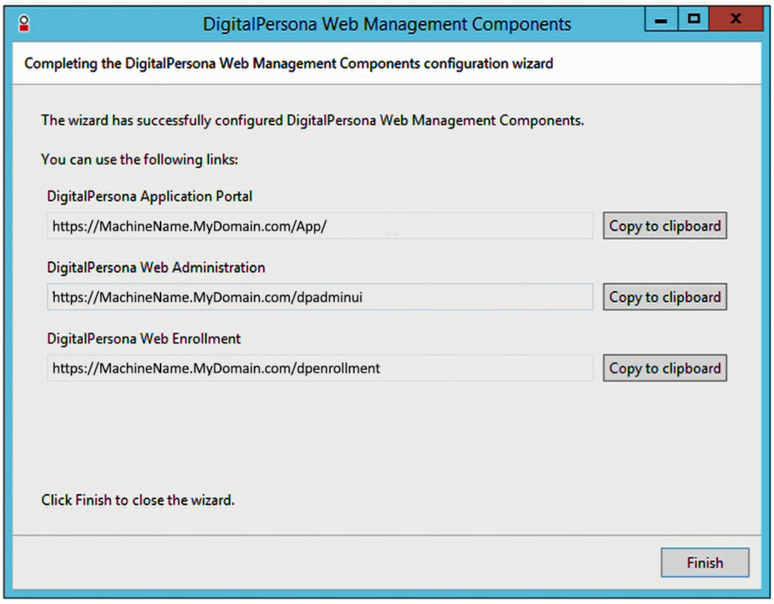
Resetting password for the DP_LD5_ACCESS account.

2. Web application deployment

Deploying DigitalPersona Web Enrollment.

Verify the parameters shown above. Click Next to apply the configuration.

8. On the *Apply configuration* page, verify the actions that will be performed during configuration, and any parameters shown and then click *Next.*



Completing the DigitalPersona Web Management Components configuration wizard

The wizard has successfully configured DigitalPersona Web Management Components.

You can use the following links:

DigitalPersona Application Portal

https://MachineName.MyDomain.com/App/

DigitalPersona Web Administration

https://MachineName.MyDomain.com/dpadminui

DigitalPersona Web Enrollment

https://MachineName.MyDomain.com/dpenrollment

Click Finish to close the wizard.

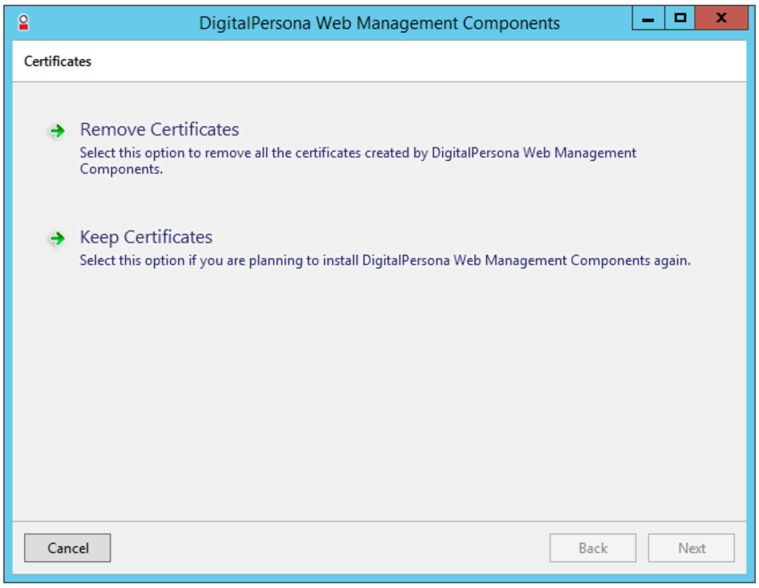
9. On the final page, the URLs to the three resulting web applications are shown. (Although there are five components, there are only three web applications.) Click the button next to a URL to copy it to the clipboard so that you can open it in a supported browser. You may also want to create shortcuts 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.

10. 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.


DigitalPersona Web Management Components

Certificates

Remove Certificates
Select this option to remove all the certificates created by DigitalPersona Web Management Components.

Keep Certificates
Select this option if you are planning to install DigitalPersona Web Management Components again.

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.

‘Internal Server Error’ on the Web Administration Console

Follow the steps below to resolve a possible *Internal Server Error* after authenticating with the DigitalPersona Identity Server for access to the Web Administration Console.

1. On the machine where the Web Administration component is installed, use Regedit to locate the LDS Port. Navigate to *SOFTWARE\DigitalPersona\LDAP*. Under the *ADAM Port,* note the decimal value.

2. Open the *web.config* file, located here:

   C:\Program Files\DigitalPersona\Web Management Components\DP Web Admin\DPAdminAPI\web.config

3. Make the following three changes in the file.

   - Change the value of *ActiveDirectoryContext* from 127.0.0.1 to the domain controller Hostname (DNS name) or IP Address. *Do not change the port # in this section.*
   - Locate the node that contains “name = *AltusContext”* and uncomment the *param name* and *value* elements, replacing the *value* string with the following:

- LDAP://serverHost:port/CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US.
- where port is the port number from step 1 above.
- For example:

```
<register type="IDirectoryContext" name="AltusContext" mapTo="DirectoryContext">
      <constructor>
             <param name="nameOrConnectionString">
             <value value="LDAP://127.0.0.1:50000/CN={893B81EE-7764-44FF-8561-8377580B9B03},
O=DigitalPersona,C=US"/>
             </param>
      </constructor>
 </register>
```

- Locate the node that contains “name = *ActiveDirectoryDal”* and uncomment the *param name* and *value* elements, replacing the *value* string with the following:

  LDAP://serverHost:port/CN={893B81EE-7764-44FF-8561-8377580B9B03},O=DigitalPersona,C=US.

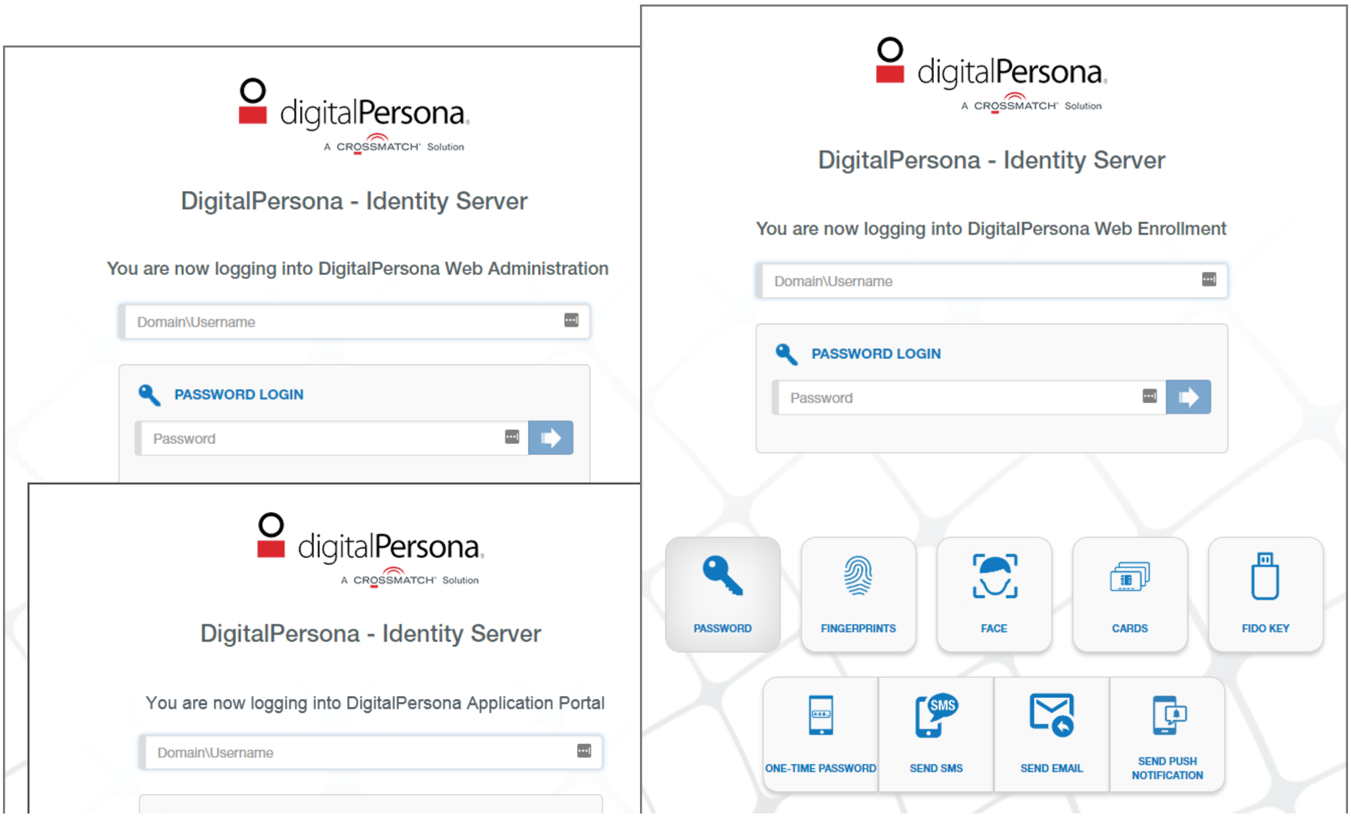
  where port is the port number from step 1 above.
- For example:

```
<register type="IUserManagerFactory"
mapTo="DigitalPersona.Altus.Administration.Manager.Interop.AltusUserManagerFactory,
DigitalPersona.Altus.Administration.Manager.Interop">
<constructor>
        <param name="connectionString">
         <value value="LDAP://127.0.0.1:50000/CN={893B81EE-7764-44FF-8561-
8377580B9B03},O=DigitalPersona,C=US"/>
       </param>
      </constructor>
    </register>
```

DigitalPersona Identity Server 20

THIS CHAPTER DESCRIBES THE DIGITALPERSONA IDENTITY SERVER AND ITS FEATURES.

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.



DigitalPersona - Identity Server

You are now logging into DigitalPersona Web Administration

DigitalPersona - Identity Server

You are now logging into DigitalPersona Web Enrollment

DigitalPersona - Identity Server

You are now logging into DigitalPersona Application Portal

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.

Step-Up authentication

If Step-up Authentication has been enabled, additional credentials may be specified by the administrator to be required for authentication depending on various risk factors including:

- Behavioral biometrics - analysis of a user’s keystroke and mouse movement while entering data into text fields presented by the Identity Server.
- IP Address - Access from a new IP Address.
- Originating device - User Agent String of the web browser being used for access.

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	PKI Smart card*, Contactless Writable card and Contactless ID card
Certificates*	Y	Y	Y	Y	N	N	N	See topic *Using a Certificate credential* below.
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	

Credential	IE	Edge	Chrome	Firefox	Safari	iOS	Android	Comments
Face	N	Y	Y	Y	Y	Y*	Y**	On an iOS device, the Face credential is supported on iOS11+ with the Safari browser. On an Android device, the Face credential is supported on Android 7.0+ with either the Chrome or Firefox browser.
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.

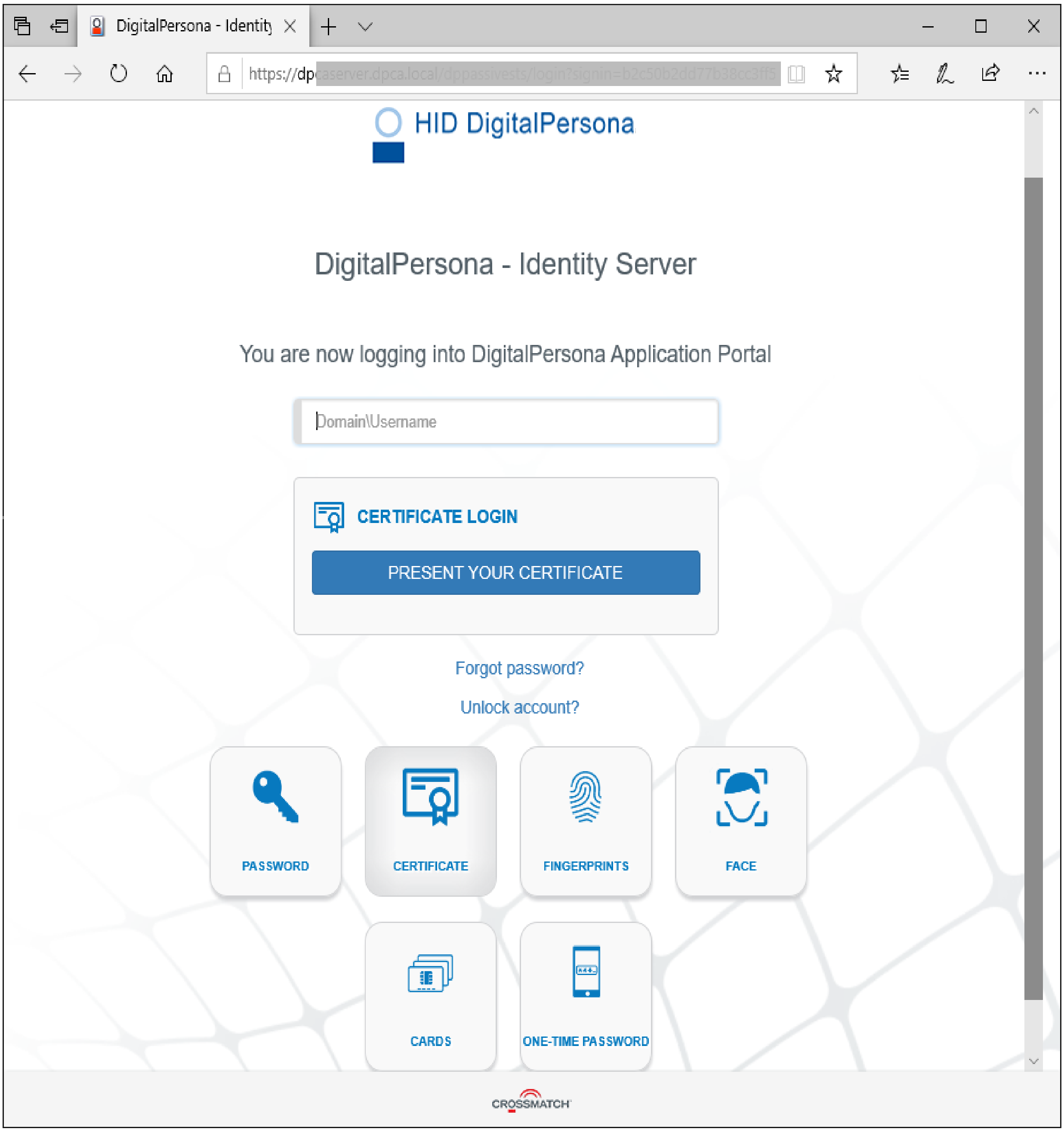
* If a certificate-based PKI Smart Card has been enrolled for a user, they will not see a tile labeled PKI Smart Card, but will see a tile labeled Certificates. See below for more details.

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.

Using a Certificate credential

If a Certificate credential is specified as part of the enforced Logon Policy, a Certificate tile will be displayed on the Identity Provider Logon page. Upon clicking the tile, the user is asked to present their certificate as shown in the following image.



https://dpcaserver.dpca.local/dppassivests/login?signin=b2c50b2dd77b38cc3ff5

DigitalPersona - Identity Server

You are now logging into DigitalPersona Application Portal

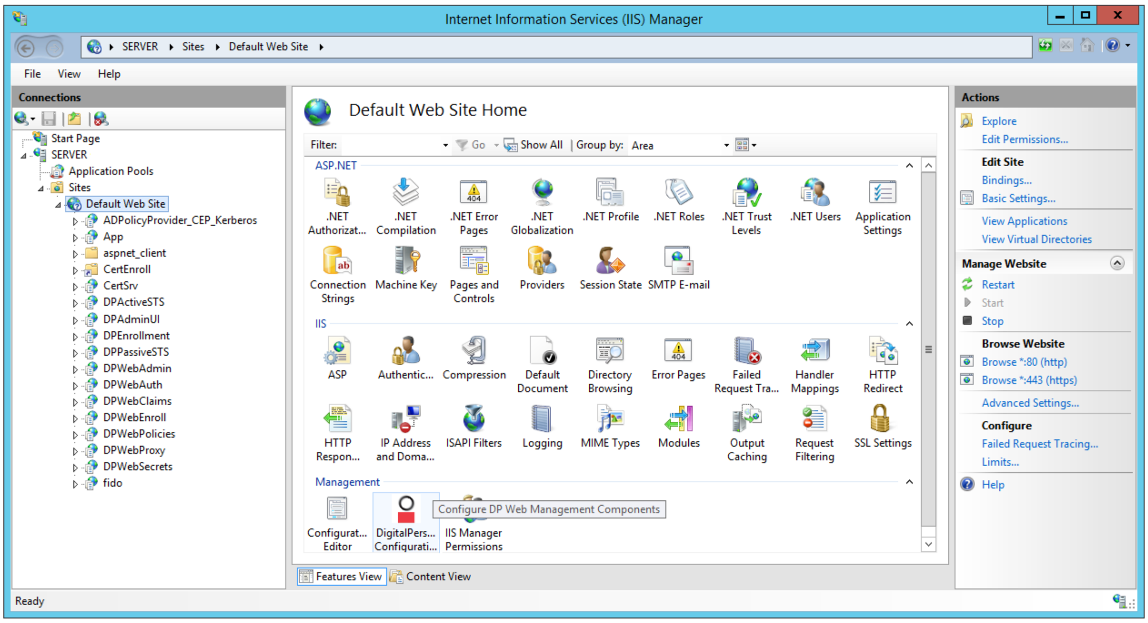
Domain\Username

- If multiple Windows Security certificates exist on the device, the user will need to select the appropriate certificate. The selection process will differ slightly for various web browsers. Note that Firefox requires that *ActiveClient v7.1 or above* middleware be installed on the device in order to use certificate login to the Identity Server.
- If the certificate is located on a PKI Smart Card, the user will also be asked to enter their Smart card PIN.
- The authentication will be effective for the browser session and no longer effective once the browser closes.

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*.



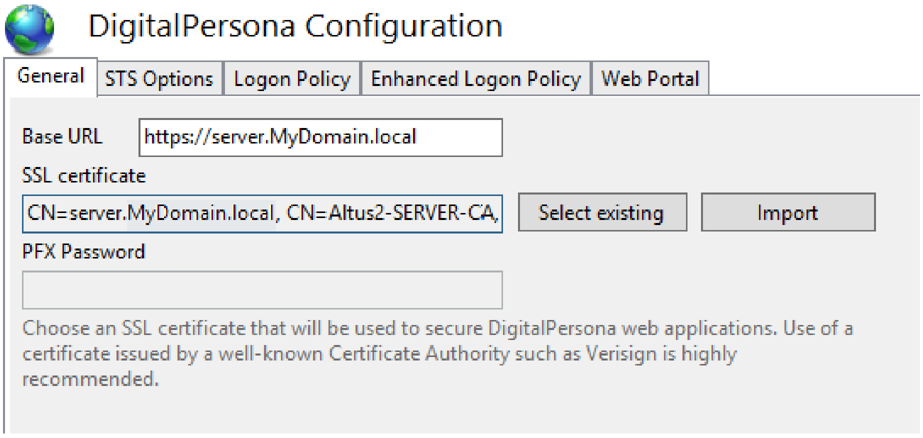
Installation

The DigitalPersona Configuration IIS plugin is installed by default as part of the DigitalPersona 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 SSL certificate 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.



DigitalPersona Configuration

Base URL: https://server.MyDomain.local

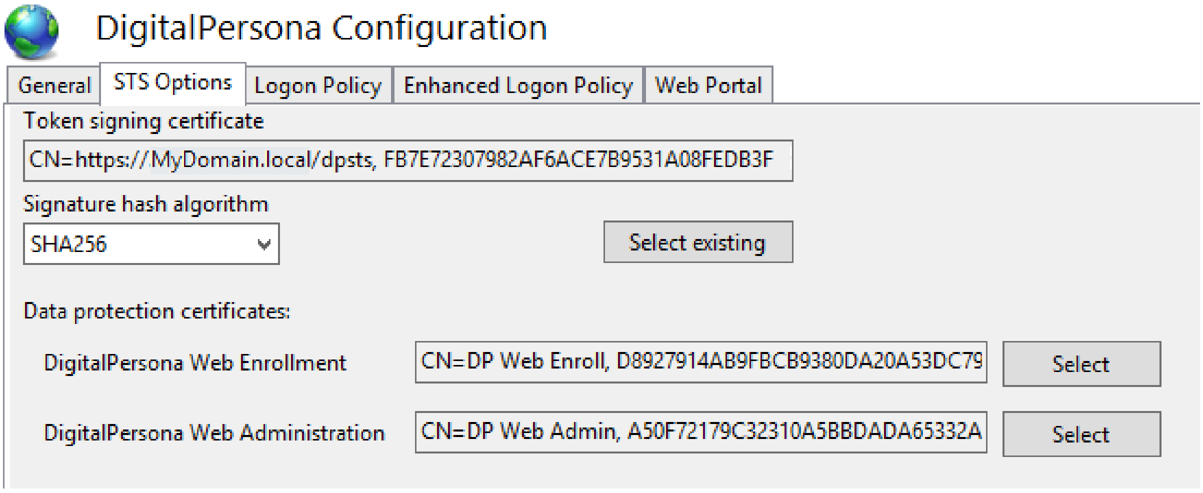
SSL certificate: CN=server.MyDomain.local, CN=Altus2-SERVER-CA,

PFX Password

Choose an SSL certificate that will be used to secure DigitalPersona web applications. Use of a certificate issued by a well-known Certificate Authority such as Verisign is highly recommended.

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.



DigitalPersona Configuration

Token signing certificate: CN=https://MyDomain.local/dpsts, FB7E72307982AF6ACE7B9531A08FEDB3F

Signature hash algorithm: SHA256

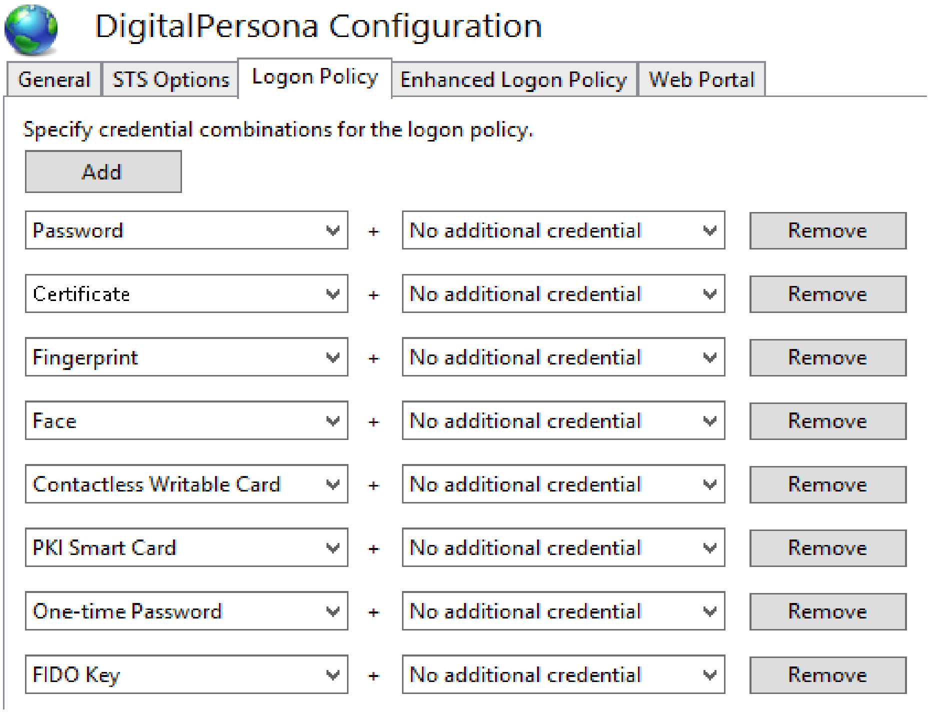
Data protection certificates:

DigitalPersona Web Enrollment: CN=DP Web Enroll, D8927914AB9FBCB9380DA20A53DC79

DigitalPersona Web Administration: CN=DP Web Admin, A50F72179C32310A5BBDADA65332A

Logon Policy tab

On the Logon 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 *Remove* to delete a line.



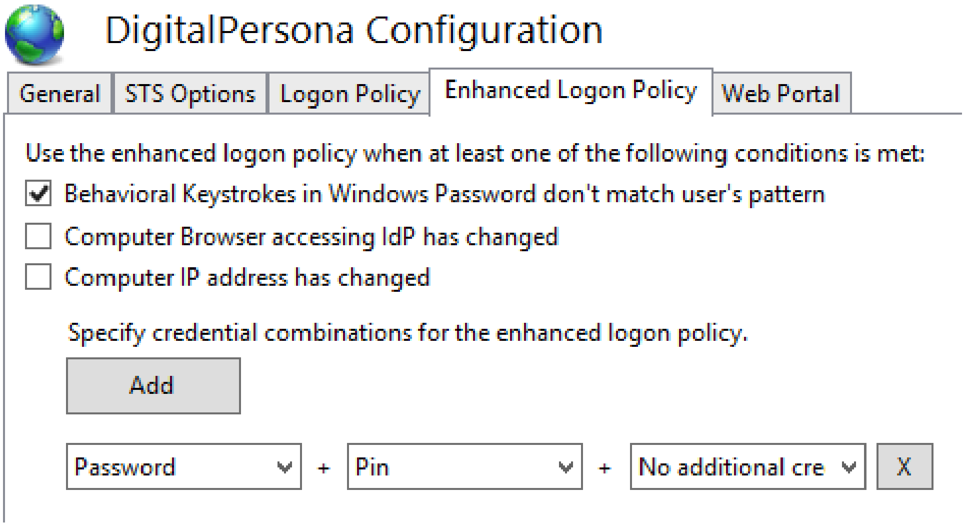
DigitalPersona Configuration

Specify credential combinations for the logon policy.

Password	+	No additional credential	Remove
Certificate	+	No additional credential	Remove
Fingerprint	+	No additional credential	Remove
Face	+	No additional credential	Remove
Contactless Writable Card	+	No additional credential	Remove
PKI Smart Card	+	No additional credential	Remove
One-time Password	+	No additional credential	Remove
FIDO Key	+	No additional credential	Remove

Enhanced Logon Policy tab

On the Enhanced Logon Policy tab, you can specify an enhanced logon (step-up) policy for the DigitalPersona Identity Server that is enforced when any of the selected conditions occur.



DigitalPersona Configuration

Use the enhanced logon policy when at least one of the following conditions is met:

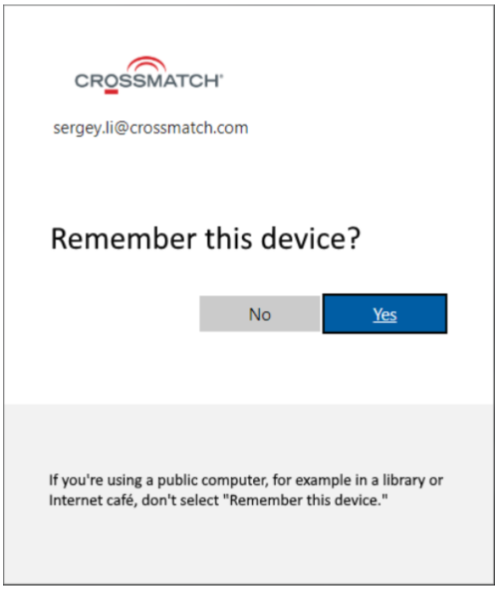
☑ Behavioral Keystrokes in Windows Password don't match user's pattern
□ Computer Browser accessing IdP has changed
□ Computer IP address has changed

Specify credential combinations for the enhanced logon policy.

Password + Pin + No additional cre X

- Select the desired conditions for step-up authentication.
  - *Behavioral Keystrokes in Windows Password don't match user's pattern* - analyzes keyboard use and enforces step-up authentication when a user's keystroke pattern deviates from historical data. Applies only to the Password field, so a Password credential must be a permitted authentication credential.

- *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.



sergey.li@crossmatch.com

Remember this device?

If you're using a public computer, for example in a library or Internet café, don't select "Remember this device."

- *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 in *not* within the trusted range, the sytem 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\DPPassiveSTS\web.config.

  The information is added to the <AltusConfirm> node in the following format.

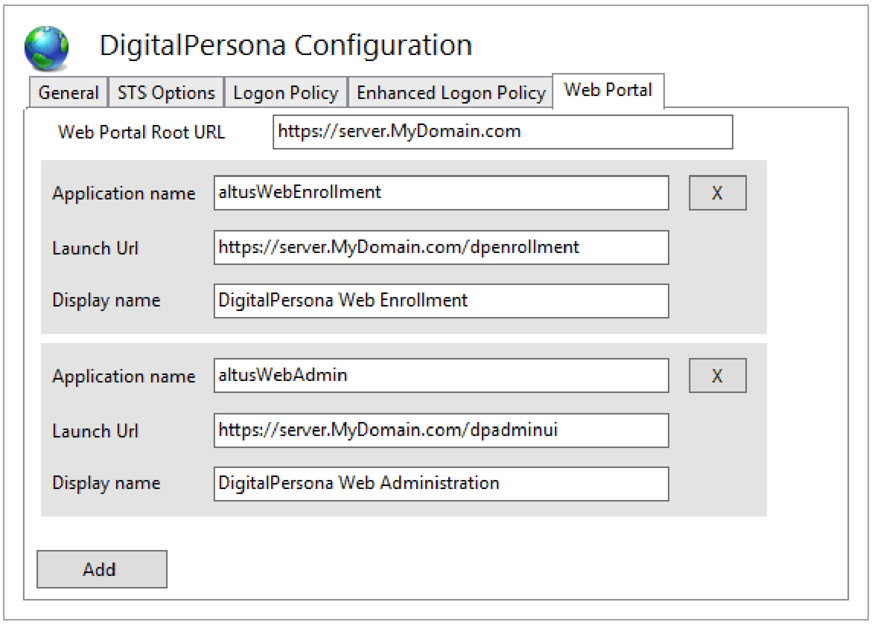
  ```
  <TrustedIPs>
      <add StartAddress=”192.168.56.102” EndAddress=”192.168.56.199” />
  <TrustedIPs>
  ```

  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.



DigitalPersona Configuration

Web Portal Root URL: https://server.MyDomain.com

Application name: altusWebEnrollment
Launch Url: https://server.MyDomain.com/dpenrollment
Display name: DigitalPersona Web Enrollment

Application name: altusWebAdmin
Launch Url: https://server.MyDomain.com/dpadminui
Display name: DigitalPersona Web Administration

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

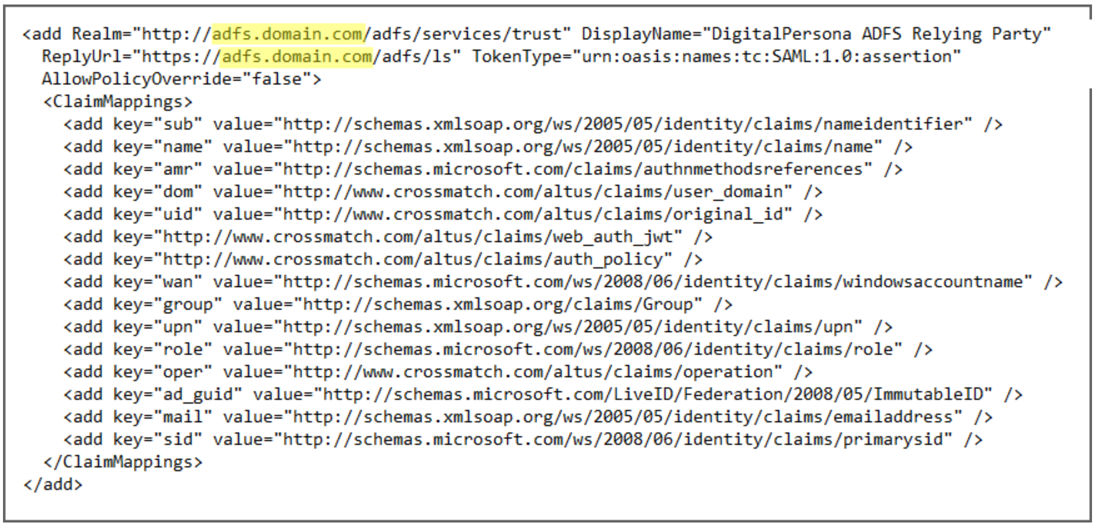
In order to add DigitalPersona Identity Server (STS) features to ADFS, you need to establish a Claim provider trust. This is accomplished through the following procedure.

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/authnmethodsreferences" />
    <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/primarysid" />
  </ClaimMappings>
</add>
```

3. Replace *adfs.domain.com* within the first and second lines with the machine name and domain where AD FS is installed.

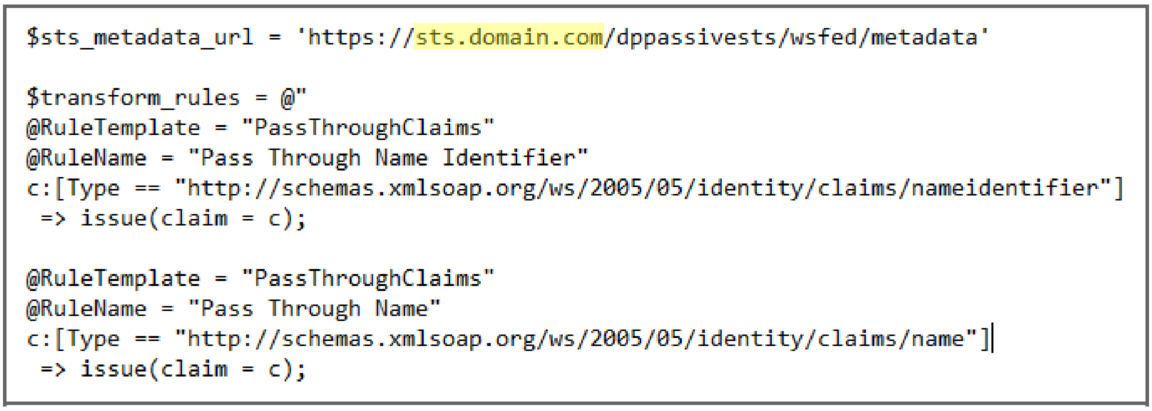
4. Save the file.

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.

DigitalPersona Web Administration Console 21

THIS CHAPTER DESCRIBES THE FEATURES OF THE DIGITALPERSONA WEB ADMINISTRATION CONSOLE.

Overview

The DigitalPersona Web Administration Console provides a convenient web-based way to administer DigitalPersona *AD Users* and *Non AD Users*. From the console, the domain administrator or Security Officer can manage DigitalPersona users and the most common user policies. Additional user settings and policies for AD Users can be configured in Active Directory. There are slight differences in functionality for AD Users, as defined below.

- AD Users are displayed and user policies can be managed, but their credentials cannot be enrolled until an account is first created for the user in the DigitalPersona LDS database. This is accomplished by selecting the *Create New* button in the *Details* panel and entry of their Windows password.
- Once at least one credential (other than the user's Password) has been enrolled, the *Create New* button is replaced by a *Manage Credentials* button, which launches the *DigitalPersona Web Enrollment* component (See the *Web Enrollment* chapter in this Administrator Guide.
- When AD Users are removed (by clicking the **X** to the right of their name), they will still be displayed when *All Users* is selected, but their credentials will be deleted and their user license will be returned to the license pool. A *Removed Users* option on the dropdown menu also allows displaying only removed AD Users.

The DigitalPersona Web Administration Console can be accessed through any of the web browsers listed in the system requirements on page 19 as long as it has JavaScript enabled.

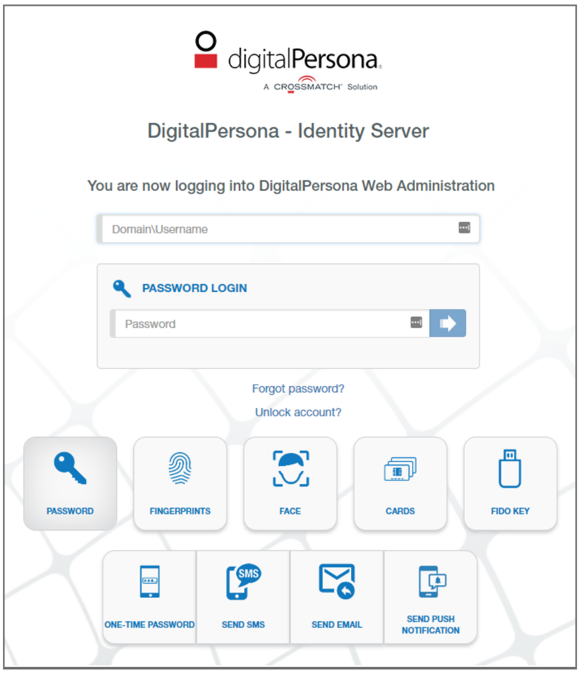
When accessing the console remotely, only credentials (such as Passwords and OTP) that do not require attached hardware (fingerprint and card readers, for example) can be used to log on to the console, unless a DigitalPersona client (such as DigitalPersona Workstation, Kiosk or Lite Client) is also installed on the machine.

Logging in

In order to log in to the DigitalPersona Web Administration Console, you must be a DigitalPersona AD user. You must also be listed in the Microsoft Authorization Manager (AzMan) as a member of the built-in DigitalPersona *Administrators* group, or assigned to a role that contains at least the *Query Users* and *Manage Users* permissions (see page 148 and following).

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.



DigitalPersona - Identity Server

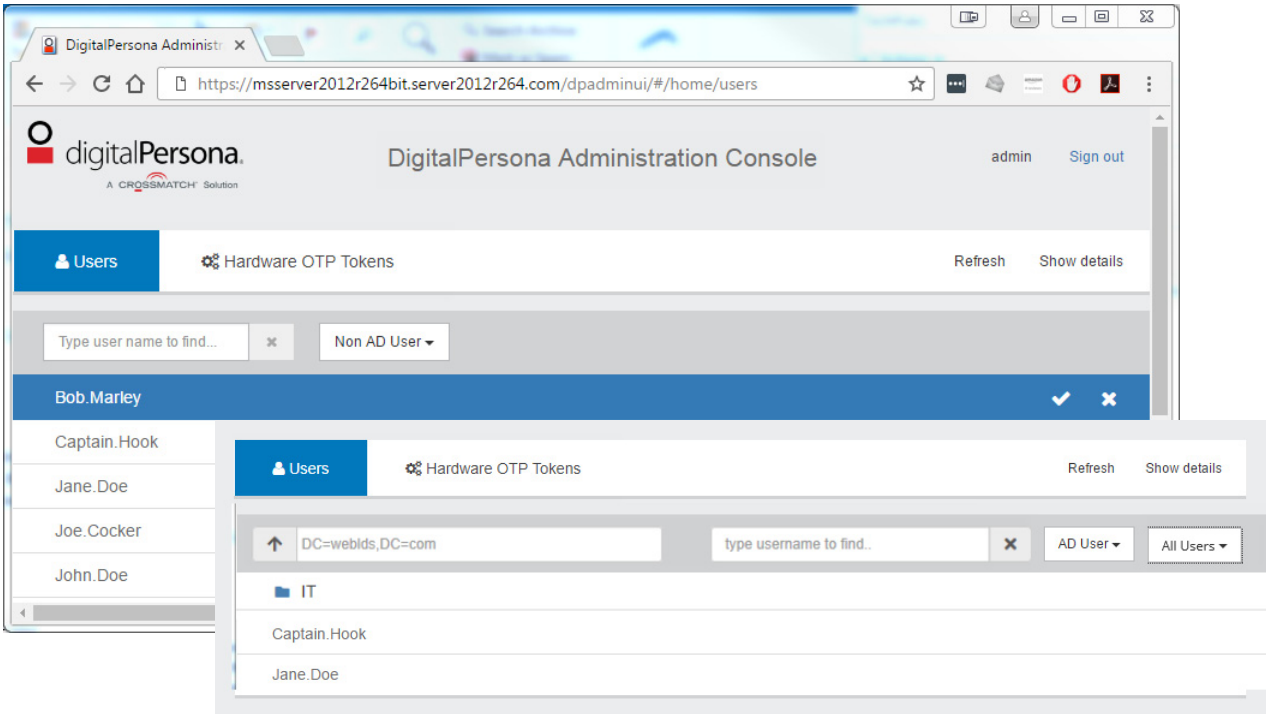
You are now logging into DigitalPersona Web Administration

Domain\Username

Password

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 *232* for details.

Administration Console features



The following sections describe the features available through the DigitalPersona Administration Console.

Features summary

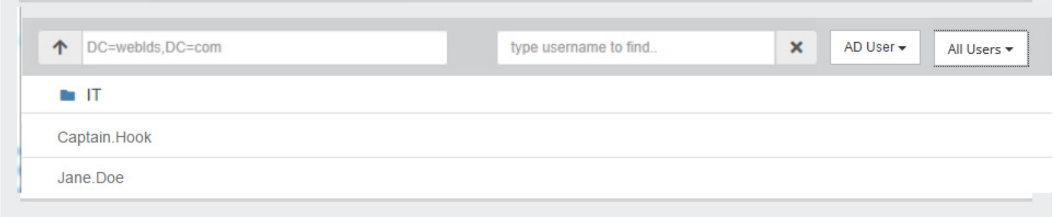
Through the console, the administrator can perform the following activities. Further details are provided in the sections that follow.

- Search for and filter *AD Users* or *Non AD* Users.
- Use the dropdown menu to choose between displaying only AD Users or Non AD Users.
- With AD Users selected, choose to display *Enrolled Users* and *Locked Users*.
- List the enrolled credentials for a user
- Remove specific user credentials
- Recover a user’s Windows password
- Unlock a user account
- Manage (enroll or unenroll) a user’s credentials
- Set user policies
- Remove a user

Additionally, the types of credentials displayed, and the policies setting which credentials or credential combinations are required for authentication or log in to the DigitalPersona Web Administration Console (through the DigitalPersona Identity Provider) may be specified through a *web.config.XML file.* See *Configuring the DigitalPersona Identity Server* in the preceding chapter for details.

Search for and filter users

Use the Search field and Users drop down menu to search for and filter enrolled users by their status, i.e. all Enrolled Users or only users whose accounts have been locked (Locked Users). When displaying AD Users, if Organization Units exist in Active Directory, you can click on an OU to display users within that Organizational Unit or the Up arrow to view a parent OU.

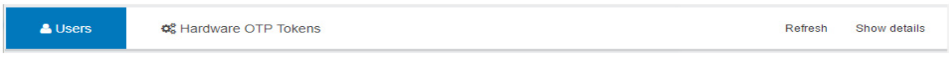


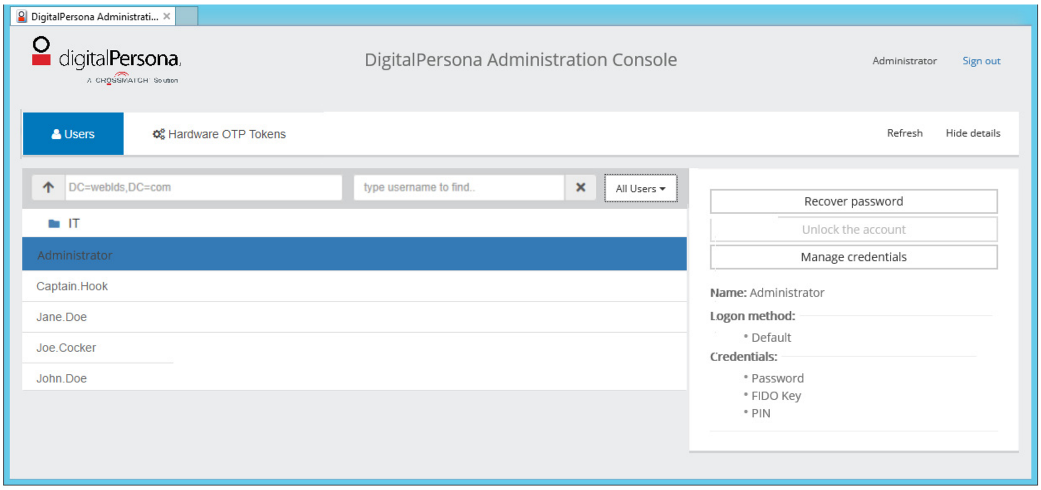
Note that users are listed by their Windows Display Name and therefore cannot be searched by their SAM account name.

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 users and click *Show details*.





Name: Administrator

Logon method:

- Default

Credentials:

- Password
- FIDO Key
- PIN

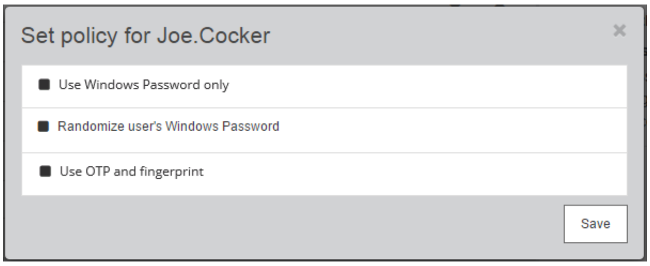
Note that if the user is in Active Directory but has not been added to the DigitalPersona LDS database, the *Manage Credentials* button is replaced by a *Create New* button .

Set policy

This feature is disabled when a Non AD User is selected.

To set the credentials required for an AD user to authenticate

1. Select a user.
2. Click *Show details*.
3. In the *Details* panel, click *Set policy.*
4. In the *Authentication policy* window, you can set the user policies as shown in the illustration to the right. Then click *Save*. With the installation of the optional Extended Server Policy Module (ESPM), additional settings are available. See the Extended Server Policy Module chapter on page 109.



Set policy for Joe.Cocker

■ Use Windows Password only

■ Randomize user's Windows Password

■ Use OTP and fingerprint

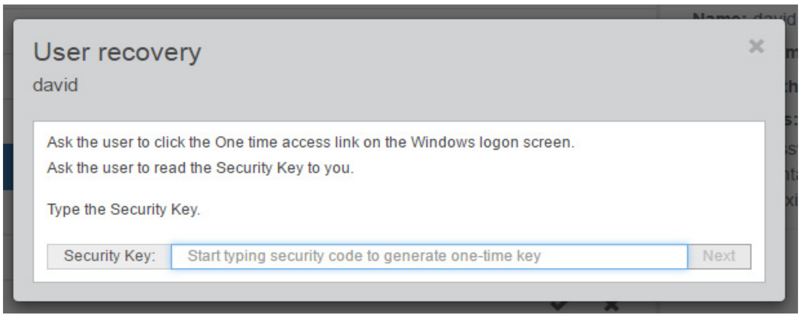
Recover password (user recovery)

This feature is disabled when a Non AD User is selected.

The DigitalPersona Web Administration Console provides assisted access to an AD 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. 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.
2. The user will read the *Security Key* displayed on the screen.
3. A DigitalPersona administrator or designated person types the Security Key into the User recovery window and clicks *Next*.



User recovery

david

Ask the user to click the One time access link on the Windows logon screen.

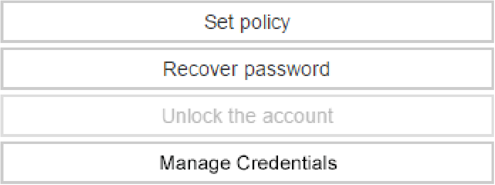
Ask the user to read the Security Key to you.

Type the Security Key.

Security Key: Start typing security code to generate one-time key

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. This button is not active (is greyed out) unless the account is locked.



Once the account is locked, the button becomes active, and pressing it will unlock the specified user's account.

Delete/unenroll a user

To delete a user and unenroll the credentials of a DigitalPersona user

1. Select a user.
2. Click the **X** next to the user name.
3. Confirm the deletion by clicking *OK*. Their name will be removed from the list and the associated license returned to the license pool.
   - If the user is a *Non AD User*, they will be removed from the LDS database and their credentials deleted.
   - For *AD Users,* although their credentials will be deleted, their Active Directory account cannot be removed through the DigitalPersona Web Administration Console, but must be deleted through Active Directory.

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.

Note that the *Manage Credentials* button is replaced by a *Create New* button *if* the user is in Active Directory but has not been added to the DigitalPersona LDS database. Clicking either button will launch the Web Enrollment component where you can enroll, modify and delete a user's credentials.

Remove (unenroll) specific user credentials

To remove one or more of a user's enrolled credentials

1. Select a user.
2. If user details are not shown, click *Show details*.
3. Under *Credentials*, click the **X** next to the credential that you want to unenroll.
4. Confirm the removal by clicking *OK*.

Manage Hardware OTP Tokens

In order to use hardware-based OTP tokens in the environment, the administrator must import seed files provided by the hardware vendor to the DigitalPersona Server. The administrator, or the AzMan group the administrator belongs to, must have the *Manage Licenses* task assigned to it.

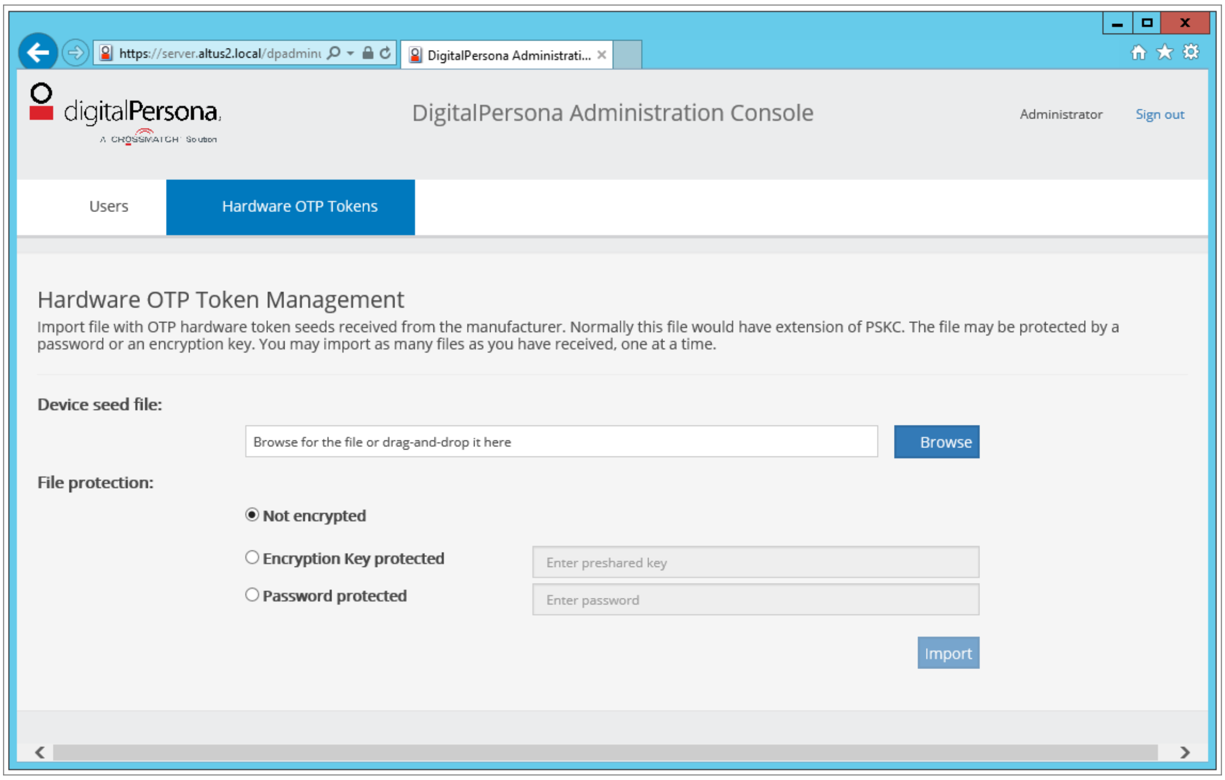
To import OTP hardware token seed files

1. Select the *Hardware OTP Tokens* tab (see image below).

2. Drag-and-drop the seed file into the *Device seed file* text box, or click *Browse* to navigate to the file. 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*.



https://server.altus2.local/dpadmin
DigitalPersona Administrati...
digitalPersona
A CROSSMATCH Solution
DigitalPersona Administration Console
Administrator
Sign out
Users
Hardware OTP Tokens

Hardware OTP Token Management

Import file with OTP hardware token seeds received from the manufacturer. Normally this file would have extension of PSKC. The file may be protected by a password or an encryption key. You may import as many files as you have received, one at a time.

Device seed file: Browse for the file or drag-and-drop it here [Browse]

File protection:

● Not encrypted

○ Encryption Key protected — Enter preshared key

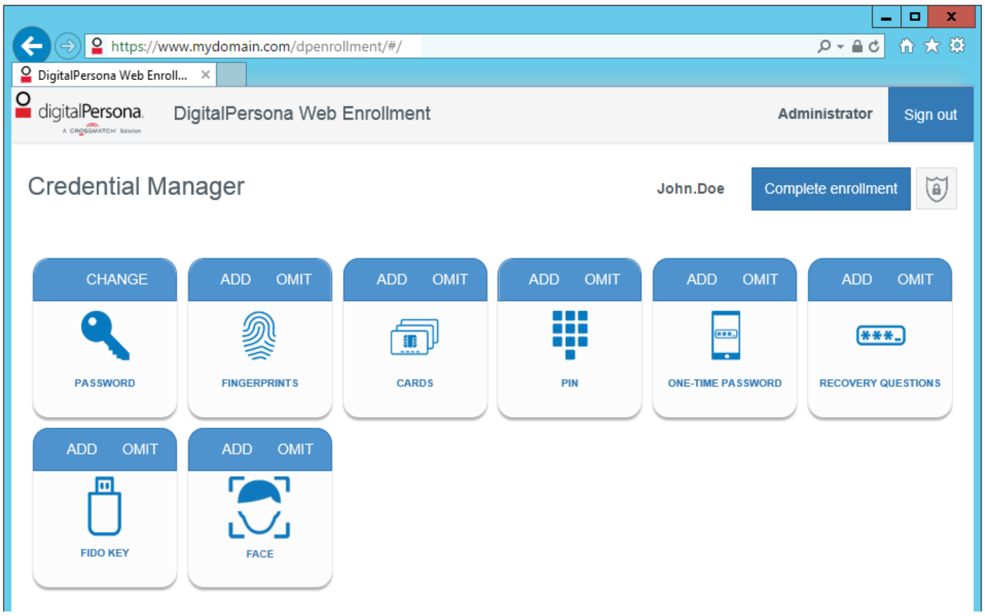
○ Password protected — Enter password

DigitalPersona Web Enrollment 22

THIS CHAPTER DESCRIBES DIGITALPERSONA WEB ENROLLMENT A WEB BASED APPLICATION FOR ENROLLING AND MANGING DIGITALPERSONA COMPOSITE AUTHENTICATION CREDENTIALS.

Overview

DigitalPersona Web Enrollment is a web based application that provides both attended (supervised) enrollment and management, and 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 *19* 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 *69.*

By default, DigitalPersona Web Enrollment is configured for attended enrollment only, i.e. Administrators, Security Officers, or other delegated users with the *Query Users* and *Manage Users* permissions, must supervise the enrollment and management of user credentials. Additionally, any Windows user that belongs to the Local Administrators group on a machine where DigitalPersona LDS Server is installed is automatically assigned the role of Security Officer and can enroll other users and assist them in managing their DigitalPersona credentials.

Domain administrators also have this role assigned to them automatically during setup. Other specified users or groups may be assigned this role through the Windows Authorization Manager. See the *Authorization Manager (AzMan)* chapter beginning on page *146*.

However, allowing users to enroll and mange their own credentials is also available and is easily accomplished. See the topic *Enabling self enrollment* beginning on page *274*.

Note that when self enrolling, the *Omit* option shown on the credential icons in the image below is not displayed, and all required credentials must be enrolled in order to complete enrollment. Also, the *Omit* option is not shown unless the *Require enrolling or omitting each credential GPO* is enabled.

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.

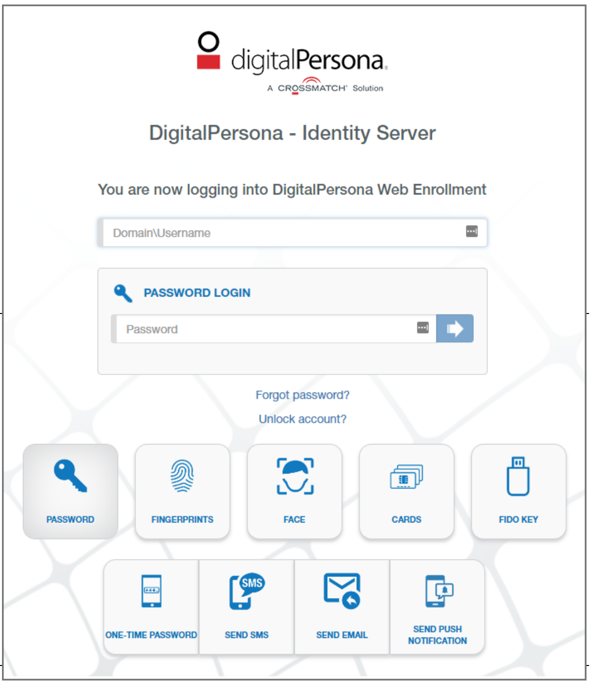
Use of the One-Time Password (OTP) Push Notification or SMS features with the One-Time Password credential requires the administrator to create an account on the Crossmatch Push Notification Server (see page 204) and then enable and configure the OTP GPO in Active Directory (see page 3).

For instructions on deploying the application, see the topic *Web Management Components Installation* beginning on page *217*.

DigitalPersona Identity Server

The DigitalPersona Identity Server (provided through STS or the Secure Token Service) is the authentication gateway for the Web Enrollment application.

In order to use Web Enrollment, administrators, Security Officers and other users first need to log in to the Identity Server.



DigitalPersona - Identity Server

You are now logging into DigitalPersona Web Enrollment

User categories

There are two categories of DigitalPersona users: AD Users and Non AD Users.

- AD Users are those DigitalPersona users with an Active Directory (Windows) account.
- Non AD users are those DigitalPersona users whose records are stored in the DigitalPersona LDS database.

Attended enrollment

Attended enrollment is the default means of enrolling users through the Web Enrollment application. The basic workflow of attended enrollment is as follows.

- A Security Officer navigates to the Web Enrollment application URL.
- On the DigitalPersona Identity Server, they enter their DigitalPersona authentication credential.
- On the first page of the Web Enrollment application, they select whether the user to be managed is an *AD User* or a *Non AD User* from the dropdown menu.
- The person supervising the enrollment enters the username for the account to be managed. If a username is not found, the administrator can choose to
    - Search for the username again
    - Enroll a new *Non AD* user
    - Enroll a new *AD User*, but only if the user already exists in Active Directory.
- Once a user is selected or created, the supervising user clicks *Manage user.*
- On the *Credential Manager* page, they select a credential to enroll or manage,.
- The user enters their password.
- The supervising user enrolls, omits or modifies the user’s DigitalPersona credentials and then clicks *Complete Enrollment.* When omitting credentials, a reason for the omission must be entered. The option to omit credentials is only available when the *Require enrolling or omitting each credential GPO* is enabled.
- The *Credential Manager* page closes and the user selection page redisplays.

Self enrollment

Self enrollment allows Digitalpersona users to enroll and manage their own credentials. To enable self enrollment, see the section *Enabling self enrollment* on page *274.*

With self enrollment enabled, the basic process is as follows. For additional details, see the following sections.

- A DigitalPersona user navigates to the Web Enrollment URL.
- On the DigitalPersona Identity Server, they enter their DigitalPersona authentication credentials.*
    - Supervising users - Select *Self Enrollment* to display the *Credential Manager* page.
    - Other users (with *Self Enroll* permission) - The *Credential Manager* page displays.
- The user selects a credential to enroll or modify.
- When they are through managing their credentials, they click *Complete Enrollment.*

* See the following sections for login scenarios and detailed login instructions.

Login scenarios (attended and self enrollment)

There is a slight variation in the UI behavior and workflow for administrators and non-administrative users, and for initial and subsequent logins. The following is a summary of the steps for different scenarios. More detailed instructions are provided in the following sections.

Login scenarios	Description
Administrator initial login	The first time that a DigitalPersona Administrator or Security Officer logs in to DigitalPersona Web Enrollment, you will • Navigate to the Web Enrollment URL. • Log in to the Identity Server with your domain\username or username@domain.com and password. • The Username field in Web Enrollment is automatically filled in. Enter your password. • Click *Enroll new.* • The *Credential Manager* page displays, where you can enroll additional DigitalPersona credentials.

Login scenarios (attended and self enrollment)

Login scenarios	Description
Administrator subsequent login	After their initial login, DigitalPersona Administrators and Security Officers will • Navigate to the Web Enrollment URL. • Log in to the Identity Server with your domain\username or username@domain.com and password. • (Option 1) Select *Self Enroll.* • (Option 2) Enroll other user's credentials. • Select *AD User* or *Non AD User* from the dropdown menu. • Specify the username for the person whose credentials you want to enroll or manage. • For previously enrolled users, click *Manage user* and have them enter their password. • To enroll a new user, click *Enroll new* and have them enter and confirm a password. • The *Credential Manager* page displays, where crentials can be enrolled and managed.
AD User initial login (Self-enrollment must be enabled)	The first time that a DigitalPersona AD User logs in, they will • Navigate to the Web Enrollment URL. • Log in to the Identity Server with their domain\username or username@domain.com and password. • The Username field in Web Enrollment is automatically filled in. Enter user password. • Click *Enroll new* to log in. • The *Credential Manager* page displays, where they can enroll additional DigitalPersona credentials.
AD User subsequent login (Self-enrollment must be enabled)	After their initial login, DigitalPersona AD Users will • Navigate to the Web Enrollment URL. • Log in to the Identity Server with their domain\username or username@domain.com and password. • The *Credential Manager* page displays, where they can manage their DigitalPersona credentials.
Non AD User login (Self-enrollment must be enabled)	Each time that a Non AD User logs in, they will • Navigate to the Web Enrollment URL. • Log in to the Identity Server with their username (only) and password. Note that the format *domain\username* or *Username@domain.com* is not valid. • The *Credential Manager* page displays, where they can enroll additional DigitalPersona credentials.

Selecting or creating a user (Attended enrollment)

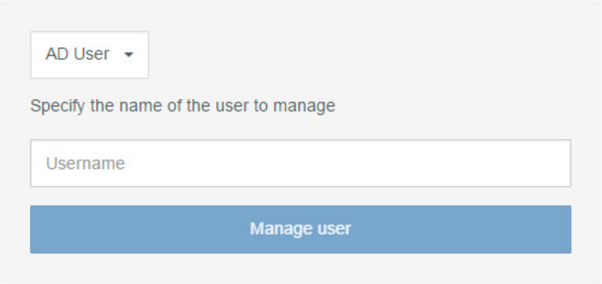
A Security Officer can select a user for web credential enrollment or modification either from within the DigitalPersona Web Administration Console or directly from the DigitalPersona Web Enrollment component.

Selecting a user

(Selection of a user from within the DigitalPersona Administration Console is covered in the previous chapter.)

To select a user for credential enrollment or modification

1. Within DigitalPersona Web Enrollment, select whether the user is an *AD User* (default) or *Non AD User.*
2. 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.



3. Click *Manage user.*

   If the user has an account in the LDS database, the *Verify Your Identity* dialog display, where the user must enter their password. Upon authentication, the *Credential Manager* page displays.

   If the user name is *not* in the DigitalPersona LDS database, you then have the option to

   - Search for the username again
   - Enroll a new *Non AD* user
   - Enroll a new *AD User*, but only if the user already exists in Active Directory.

Creating a user

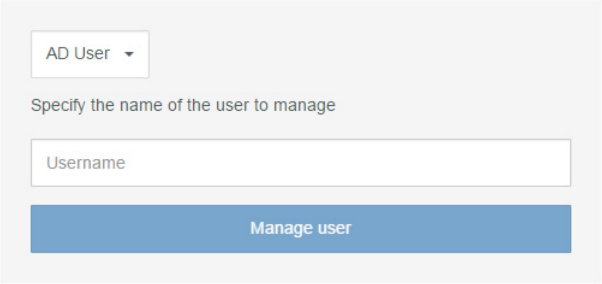
A new DigitalPersona user can be created from within the DigitalPersona Administration Console or in Web Enrollment. Creating a user from within the DigitalPersona Administration Console is covered in the previous chapter.

Creating a new AD User

A new DigitalPersona *AD User* can only be created if the user name already exists in Active Directory, in which case the password entered must be their Windows password. Note that this creates a DigitalPersona user of the type *AD User*, but cannot be used to create a new *Windows user account* in Active Directory.

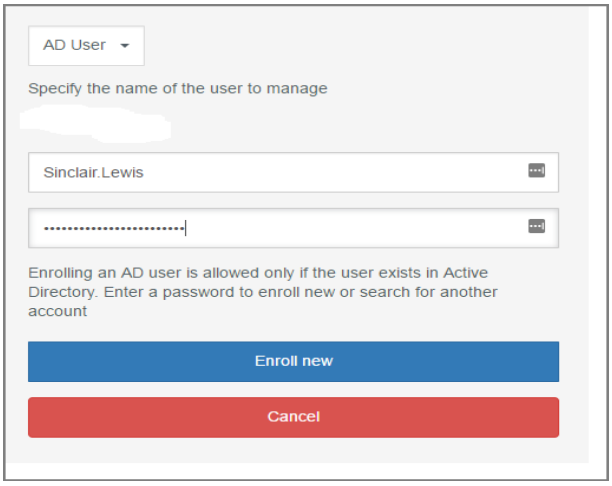
1. Within DigitalPersona Web Enrollment, select *AD User.*

2. 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.



3. Click *Manage user.*

4. A message indicates that the account does not exist. Have the user enter their password. This will enable the *Enroll new* button.



Sinclair.Lewis

••••••••••••••••••••••••••

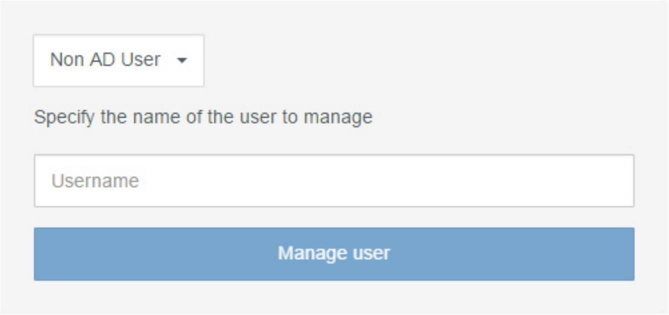
Enrolling an AD user is allowed only if the user exists in Active Directory. Enter a password to enroll new or search for another account

5. Click *Enroll new* to create a new record in the DigitalPersona LDS database and display the *Credential Manager* page.

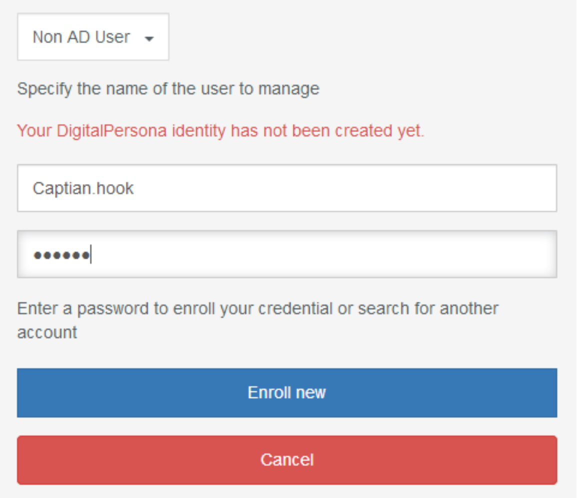
Creating a new Non AD User

1. Within DigitalPersona Web Enrollment, select *Non AD User.*

2. Enter a unique user name for the user. As soon as the first character of the name is entered, the *Manage user* button is enabled.



3. Click *Manage user.*
4. A message indicates that the DigitalPersona Identity does not exist. Have the user choose and enter a password. This will enable the *Enroll new* button.



Non AD User

Specify the name of the user to manage

Your DigitalPersona identity has not been created yet.

Captian.hook

••••••

Enter a password to enroll your credential or search for another account

5. Click *Enroll new* to create a new record in the DigitalPersona LDS database and display the *Credential Manager* page.

Logging in to Web Enrollment (self enrollment)

To enable self enrollment, see the section *Enabling self enrollment* on page *274.*

If self enrollment has been enabled, DigitalPersona users can enroll and manage their own credentials.

To enroll or manage one's own credentials, a user will perform the following steps.

1. Navigate to the Web Enrollment URL.
2. On the DigitalPersona Identity Server, enter their DigitalPersona authentication credentials. See the section Login scenarios (attended and self enrollment) on page 253 for further details.
3. The *Credential Manager* page displays.
4. Select a credential to enroll or modify.
5. When through managing their credentials, click *Complete Enrollment.*

Managing user credentials

Once a user has a record in the DigitalPersona LDS database, regardless of whether they are an AD User or Non AD User, and whether or not enrollment is being supervised or users are self-enrolling and managing their credentials, the process of enrolling and managing credentials is the same with the following exception.

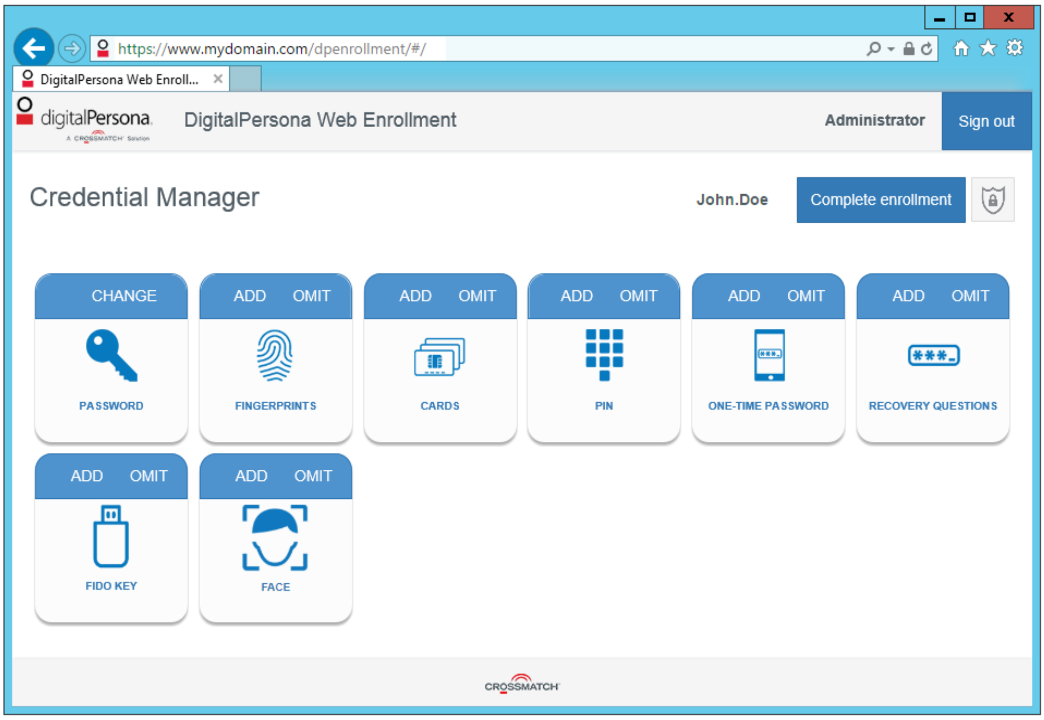
In Attended Enrollment, credentials icons have an *Omit* option that allows supervising users to omit enrolling an otherwise required credential. This option is not present during self enrollment.

The administrator should note though, that Web Enrollment is different from DigitalPersona Attended Enrollment, an optional feature of the DigitalPersona Workstation Client, in the following ways.

- Bluetooth credentials cannot be enrolled.
- Password Randomization, un-randomization and re-randomization of passwords are not available.
- There are no Photo or Custom pages.

Credential enrollment

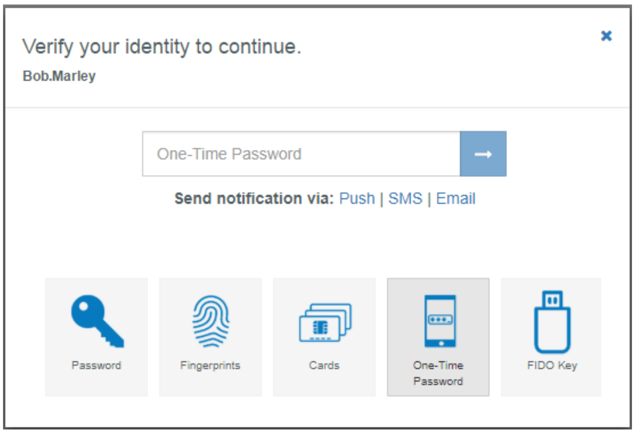
Once a user is either selected by a supervising user or logged in (if self enrollment has been enabled), the *Credential Manager* page displays.



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.



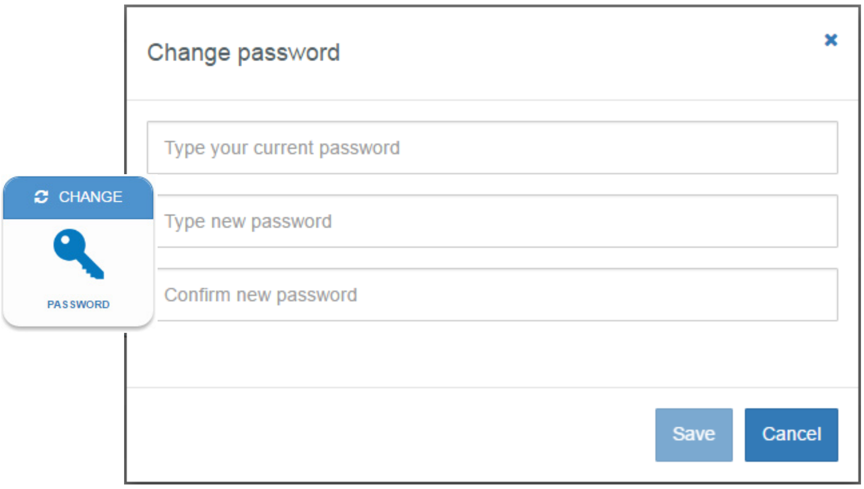
Verify your identity to continue.

Bob.Marley

Password credential

The Password credential is automatically enrolled for DigitalPersona Non AD users during the initial creation of the user through the Web Administration Console. For AD users, the Password Credential (Windows password) is part of their Active Directory profile.

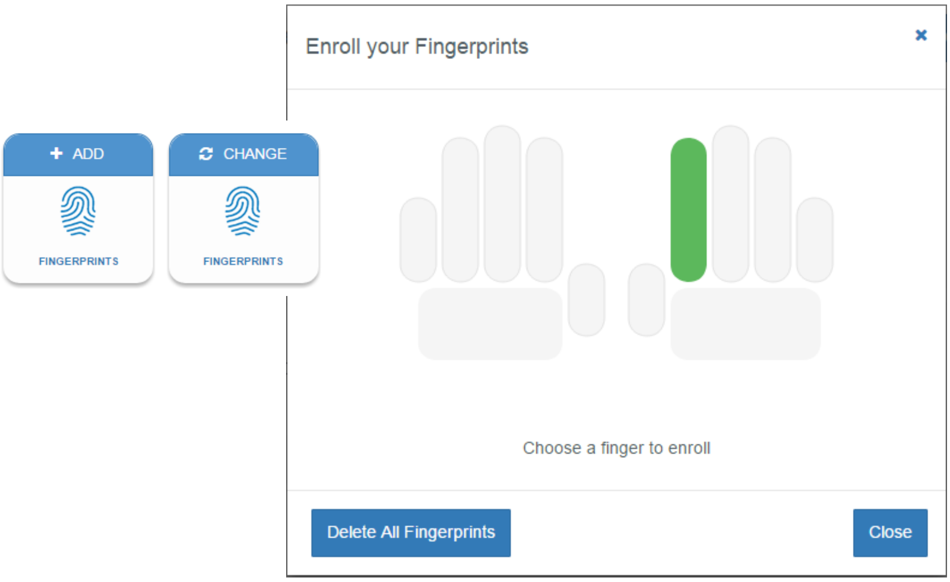
The *Password* tile launches the *Change password* window, where a user can change their password by entering their current password, and then creating and confirming a new password.



Change password

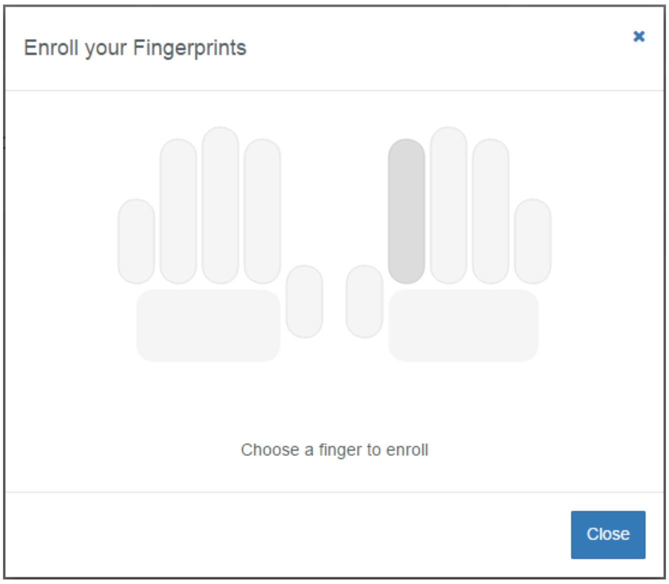
Fingerprints credential

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.

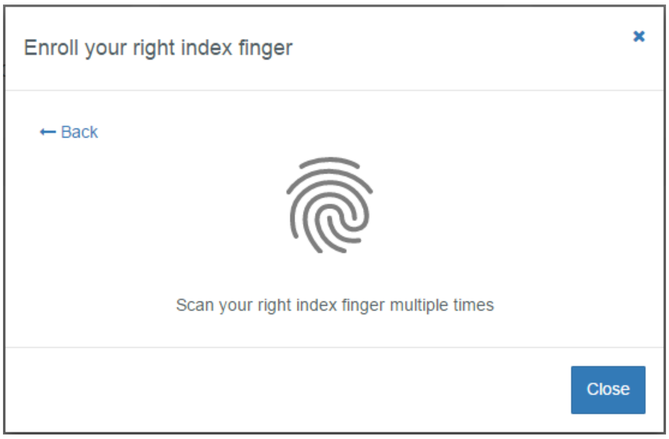


To enroll a fingerprint

1. Click the *Fingerprints* tile to display the *Enroll your Fingerprints* window.
2. Select a finger in the displayed hand image.



3. 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.



Enroll your right index finger

Scan your right index finger multiple times

4. When an adequate number of images have been captured, this window will close automatically and the *Enroll your Fingerprints* window will redisplay. Note that verification by both the Security Officer and the user may be required before the fingerprint credential is saved.

5. Click *Close* to return to the Credential Manager page.

WARNING: 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

1. Click any highlighted finger.

2. Confirm the deletion by clicking *Yes* in the message box that displays.

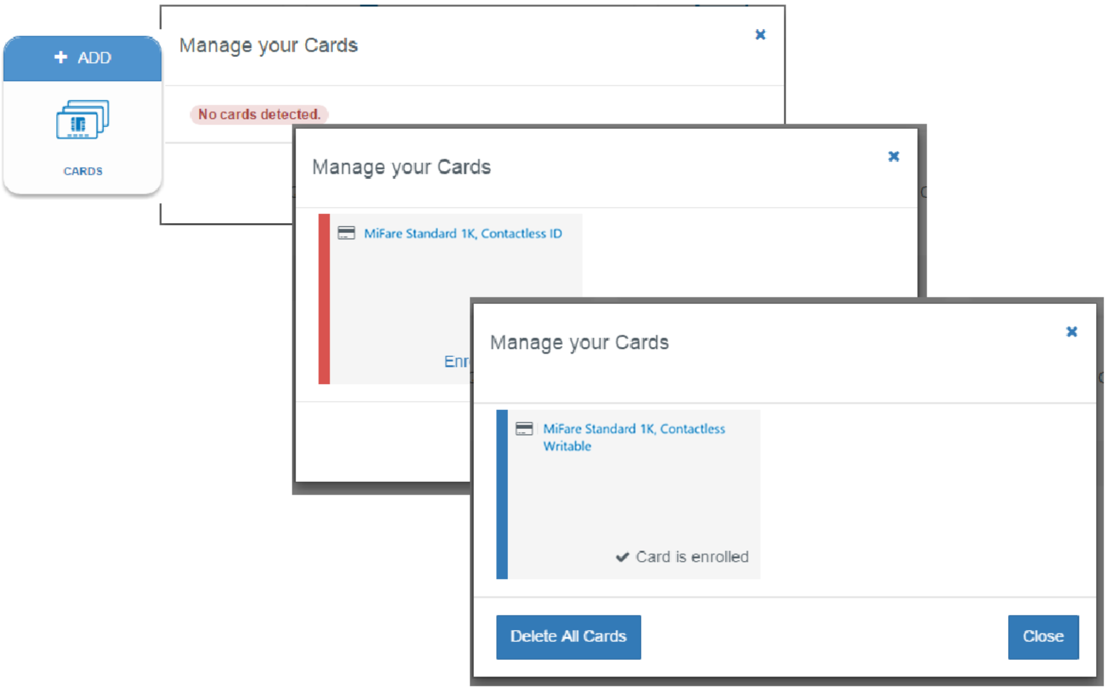
To delete the entire fingerprint credential

1. Once the credential has been enrolled, a *Delete All Fingerprints* button is added to the *Enroll your fingerprints* window.

2. Click *Delete All Fingerprints* and then click *Yes* in the message box that displays to confirm the deletion.

Cards credential

This tile provides a means for enrolling a user's Contactless Writable or Contactless ID Card credential.



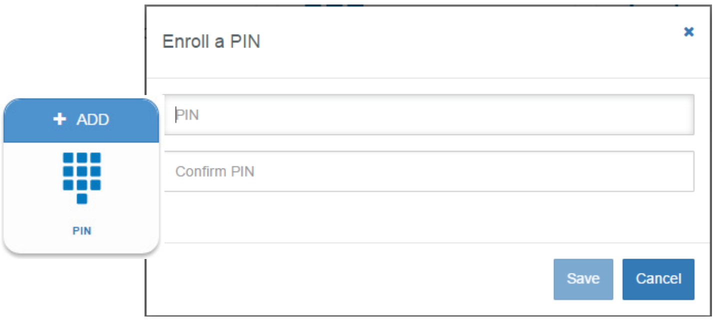
To enroll a Contactless Card credential

1. Click *Add* or *Change* on the *Cards* tile to display the *Manage your Cards* window.
2. Place your Contactless 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 by automating the entry of required account information, but is not required as 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 features 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 - (For AD Users only) 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.

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 (when using the DigitalPersona app only), after the following steps have been taken:

- The implementation team has created a tenant record for you in the CPNS service.
- The associated OTP GPO settings have been enabled and configured by a DigitalPersona administrator as described beginning on page 130.

- Each user must allow notification during the app installation, or enable notifications for the DigitalPersona app in *Settings/Notifications/DigitalPersona* after installation.

During enrollment, you may choose *not* to use OTP Push Notification by selecting *Decline* on the *Push Authentication* page, in which case, you can still use regular (non-push) OTP.

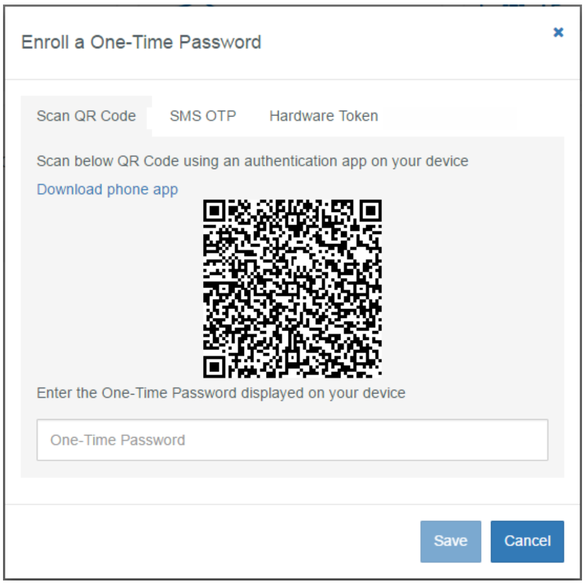
From a link in the One-Time Password window, you can download an OTP authentication app from various platform-centric app stores, and then enroll the OTP credential for use with the authenticator app (and OTP Push Notification, if configured and in the DigitalPersona app only) by scanning the QR Code 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 authentication app.
- Setup a DigitalPersona account on your device.
- Sign in to the DigitalPersona app
- Enroll the credential in the DigitalPersona Console

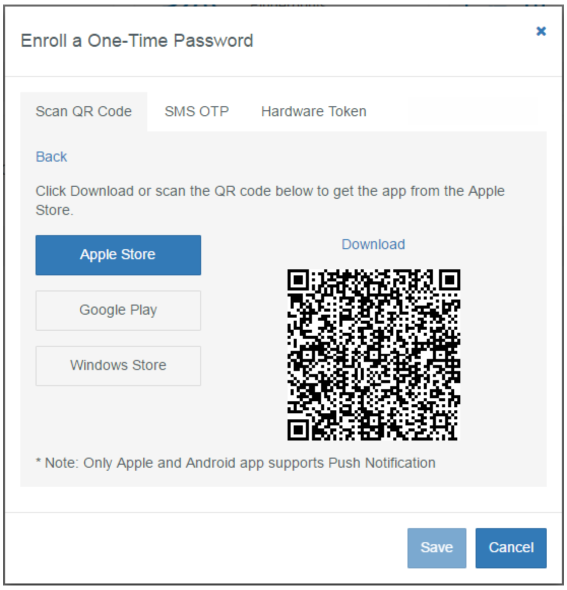
Download an authenticator app

1. 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.



Scan below QR Code using an authentication app on your device

Enter the One-Time Password displayed on your device



Click Download or scan the QR code below to get the app from the Apple Store.

* Note: Only Apple and Android app supports Push Notification

2. 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.

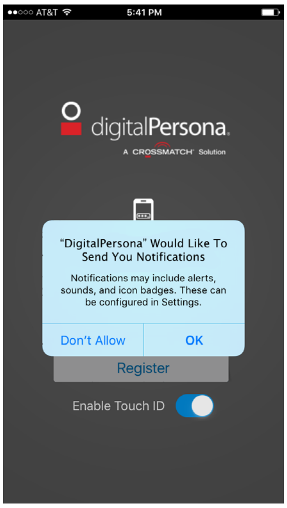
3. Scanning the QR code with a QR Code scanner app on your device is the simplest procedure. It will automatically open your device's default web browser and display the product page for the selected authentication app so that you can download and install the app.

4. 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.

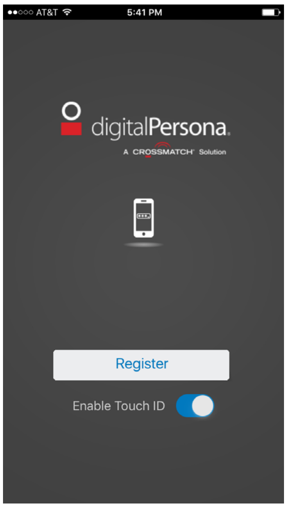
Set up a DigitalPersona account on your device

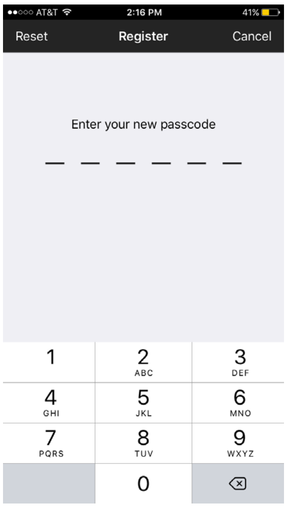
1. Launch the authentication app on your device. The first time the app is launched, the *Register* screen displays. Click *OK* to allow the DigitalPersona app to send you notifications. Then click *Register*.
2. Enter and verify a six-digit passcode.



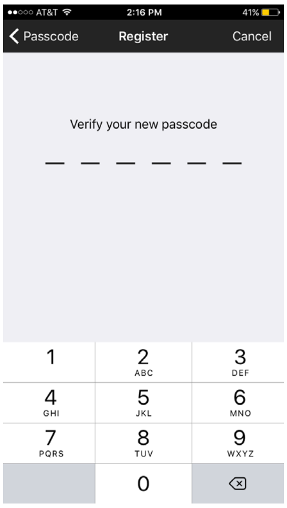
"DigitalPersona" Would Like To Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.



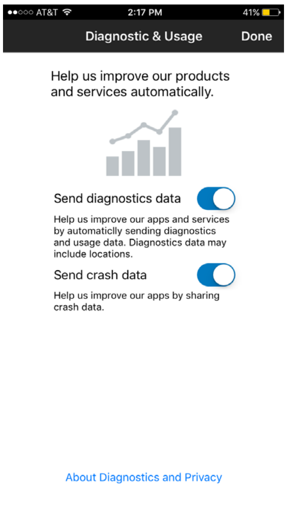


Enter your new passcode



Verify your new passcode

3. On the Diagnostic and Usage page, accept the defaults or tap an option to deselect it.



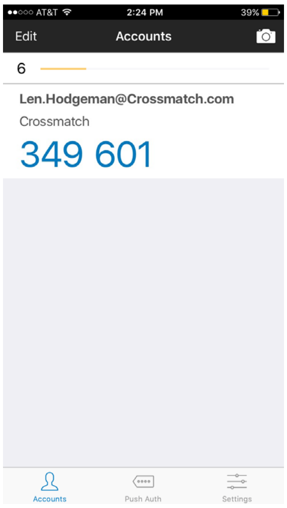
Help us improve our products and services automatically.

Send diagnostics data

Help us improve our apps and services by automaticlly sending diagnostics and usage data. Diagnostics data may include locations.

Send crash data

Help us improve our apps by sharing crash data.



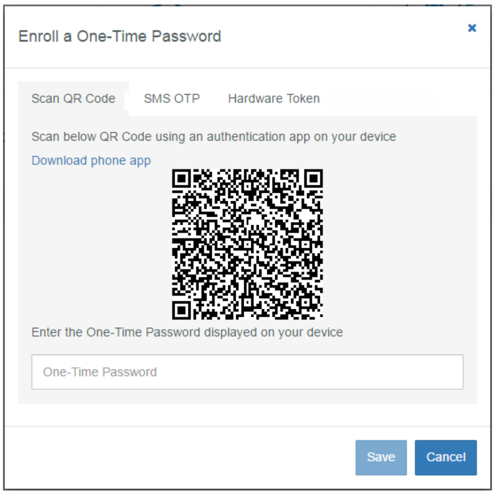
Len.Hodgeman@Crossmatch.com

Crossmatch

349 601

4. 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.
5. 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*.
6. 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.



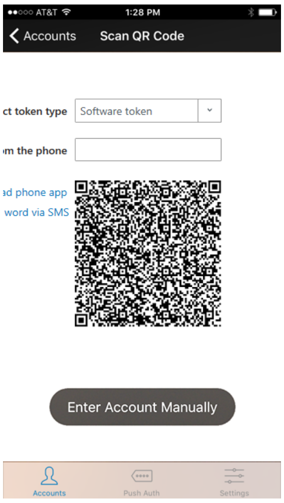
Enroll a One-Time Password

Scan below QR Code using an authentication app on your device

Download phone app

Enter the One-Time Password displayed on your device

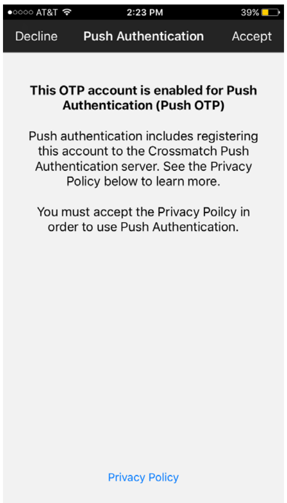
One-Time Password



ct token type Software token

ım the phone

ıd phone app
word via SMS

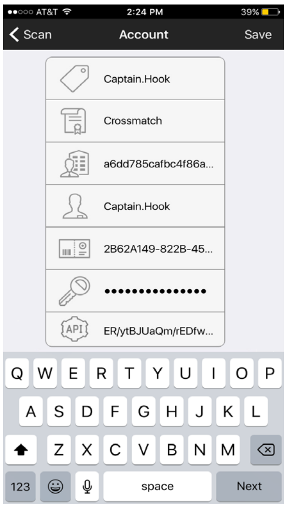


This OTP account is enabled for Push Authentication (Push OTP)

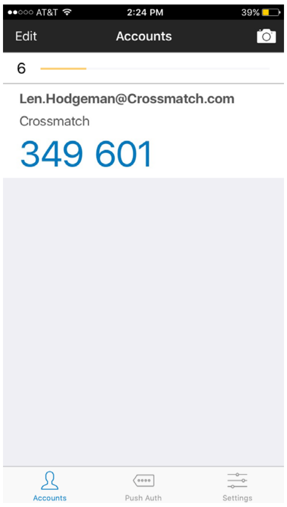
Push authentication includes registering this account to the Crossmatch Push Authentication server. See the Privacy Policy below to learn more.

You must accept the Privacy Policy in order to use Push Authentication.

- 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.



Captain.Hook
Crossmatch
a6dd785cafbc4f86a...
Captain.Hook
2B62A149-822B-45...
•••••••••••••••
ER/ytBJUaQm/rEDfw...



6

Len.Hodgeman@Crossmatch.com

Crossmatch

349 601

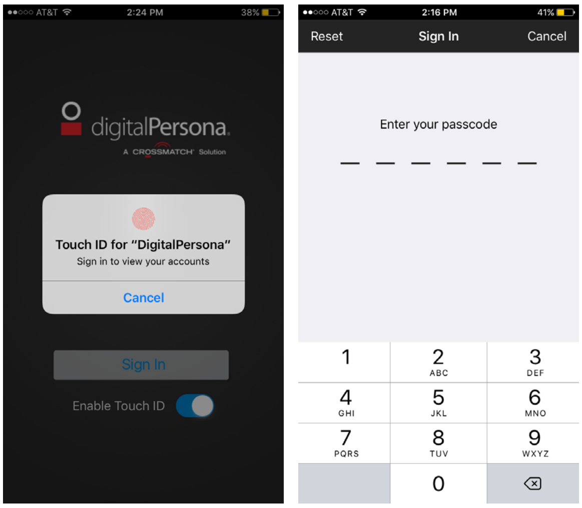
Manual account creation

Manual account creation is not available at this time.

Sign in to the DigitalPersona Mobile app

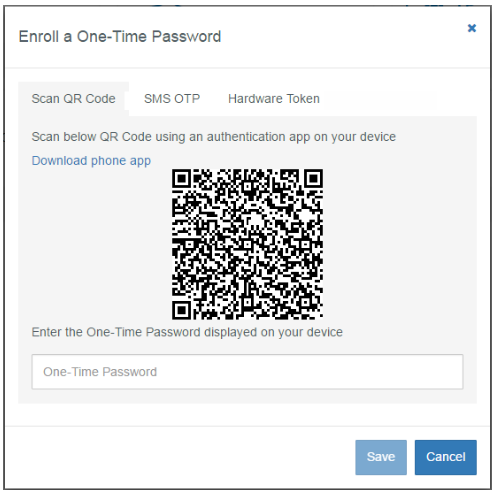
Once you have registered as described in the previous pages, you can sign in to the app as follows.

1. Launch the DigitalPersona app.
2. Sign In.
   - Fingerprint enabled devices - You can enable fingerprint authentication to the DigitalPersona Mobile app by selecting *Enable Touch ID* 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*.


Enroll a One-Time Password

Scan QR Code | SMS OTP | Hardware Token

Scan below QR Code using an authentication app on your device

Download phone app

Enter the One-Time Password displayed on your device

One-Time Password

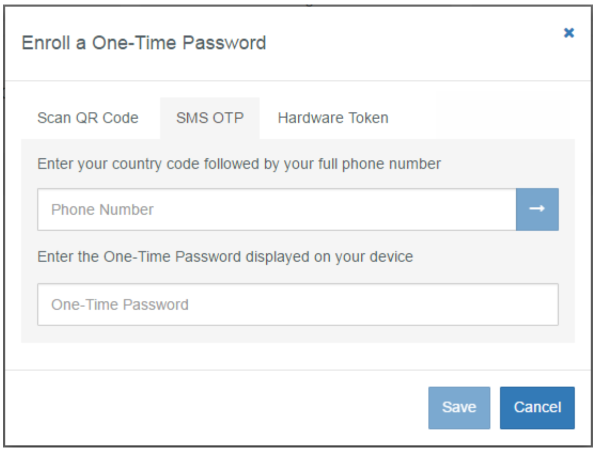
Save | Cancel

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 an 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 in the *Policies and Settings* chapter of the DigitalPersona Administrator Guide.


Enroll a One-Time Password

Scan QR Code | SMS OTP | Hardware Token

Enter your country code followed by your full phone number

Phone Number →

Enter the One-Time Password displayed on your device

One-Time Password

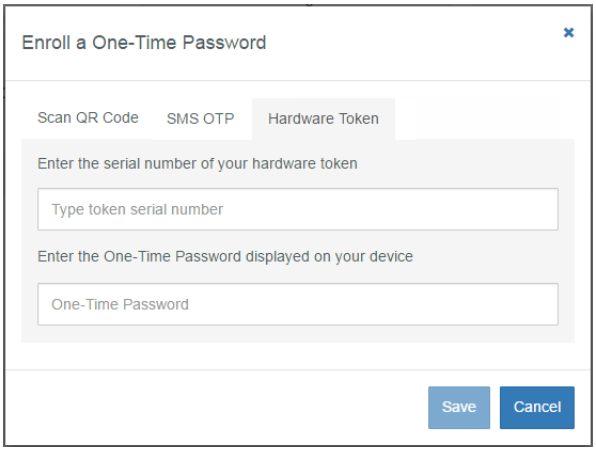
Save | Cancel

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.

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.



Enroll a One-Time Password

Enter the serial number of your hardware token

Type token serial number

Enter the One-Time Password displayed on your device

One-Time Password

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 file 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

(For AD Users only) If enabled by the administrator through the associated *Allow sending OTP code by email* GPO, 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.

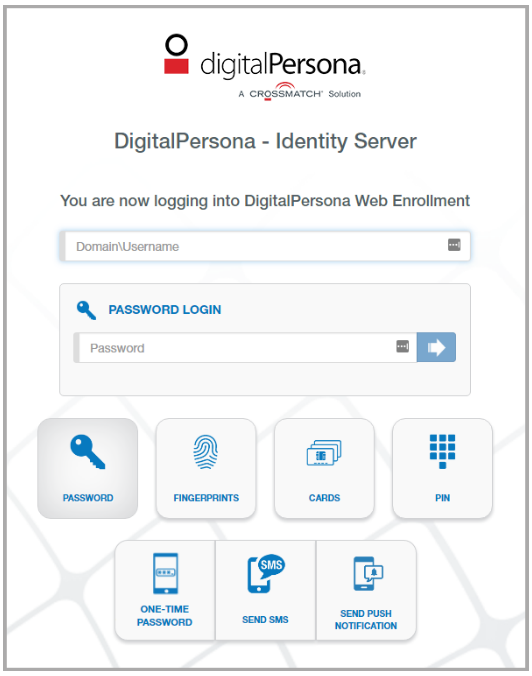
NOTE: In order to authenticate using OTP via SMS or OTP via email,the user's workstation must be able to connect to the DP Server, either within the network, through a VPN or using the VPN-less (web proxy) feature which is enabled through the *Allow VPN-less access* GPO.

Authentication with a One-Time Password

To authenticate with your One-Time Password

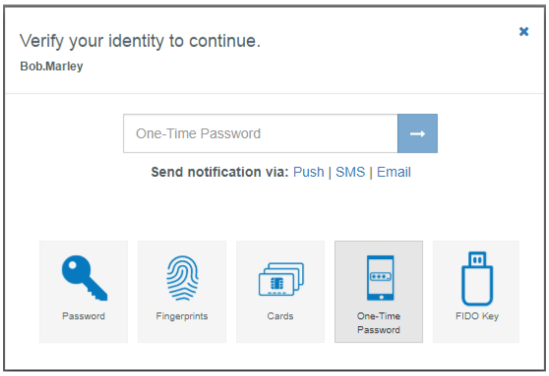
1. Do one of the following, depending on where you are authenticating from.

   - 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.



DigitalPersona - Identity Server

You are now logging into DigitalPersona Web Enrollment



Verify your identity to continue.

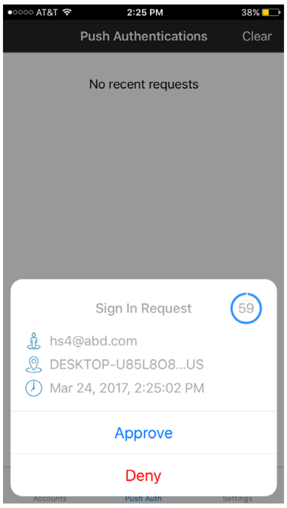
Bob.Marley

Send notification via: Push | SMS | Email

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.



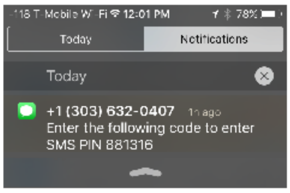
No recent requests

Sign In Request 59

hs4@abd.com

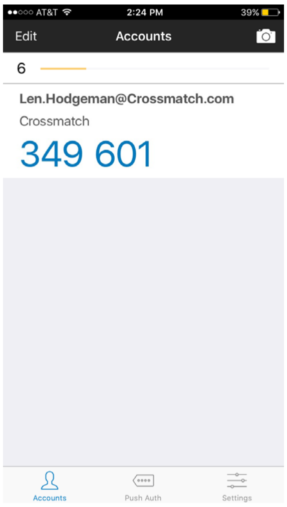
DESKTOP-U85L8O8...US

Mar 24, 2017, 2:25:02 PM



+1 (303) 632-0407 1m ago

Enter the following code to enter SMS PIN 881316



6

Len.Hodgeman@Crossmatch.com

Crossmatch

349 601

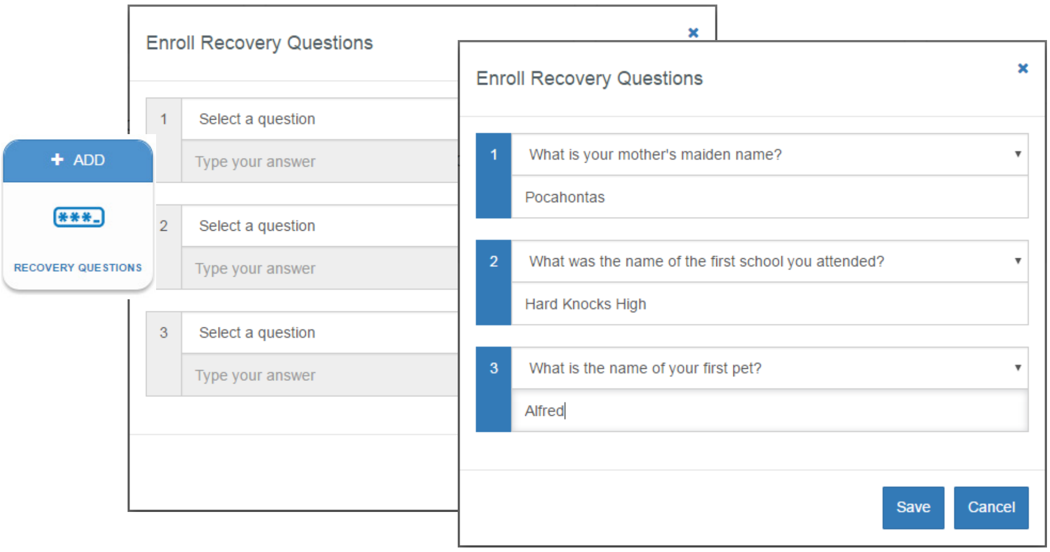
3. In most cases, enter your One-Time Password into the One-Time Password field on your workstation screen and select the arrow button. When using push notification, you do not need to enter the code on your computer, as tapping *Approve* or *Deny* on your mobile device automatically authenticates to 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

(AD Users only) The Recovery Questions credential allows a DigitalPersona *AD User* to regain access to their Windows account by answering a series a questions that have been previously configured.



Enroll Recovery Questions

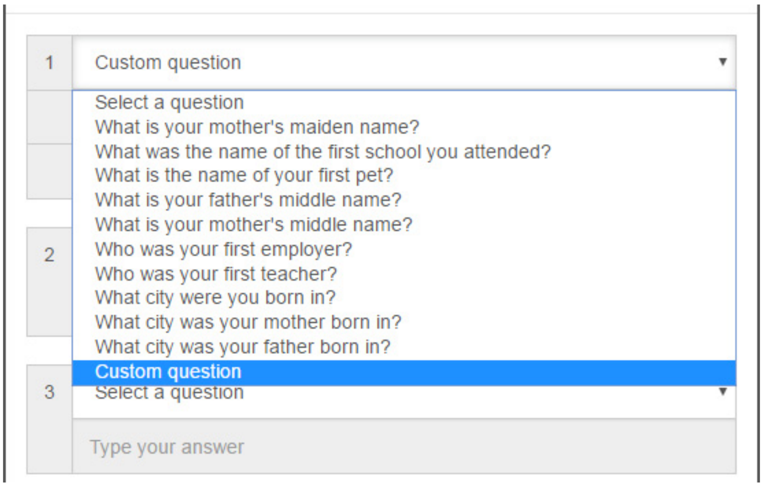
1 What is your mother's maiden name?
Pocahontas

2 What was the name of the first school you attended?
Hard Knocks High

3 What is the name of your first pet?
Alfred

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.


1
Custom question
Select a question
What is your mother's maiden name?
What was the name of the first school you attended?
What is the name of your first pet?
What is your father's middle name?
What is your mother's middle name?
Who was your first employer?
Who was your first teacher?
What city were you born in?
What city was your mother born in?
What city was your father born in?
Custom question
2
3
Select a question
Type your answer

FIDO key credential

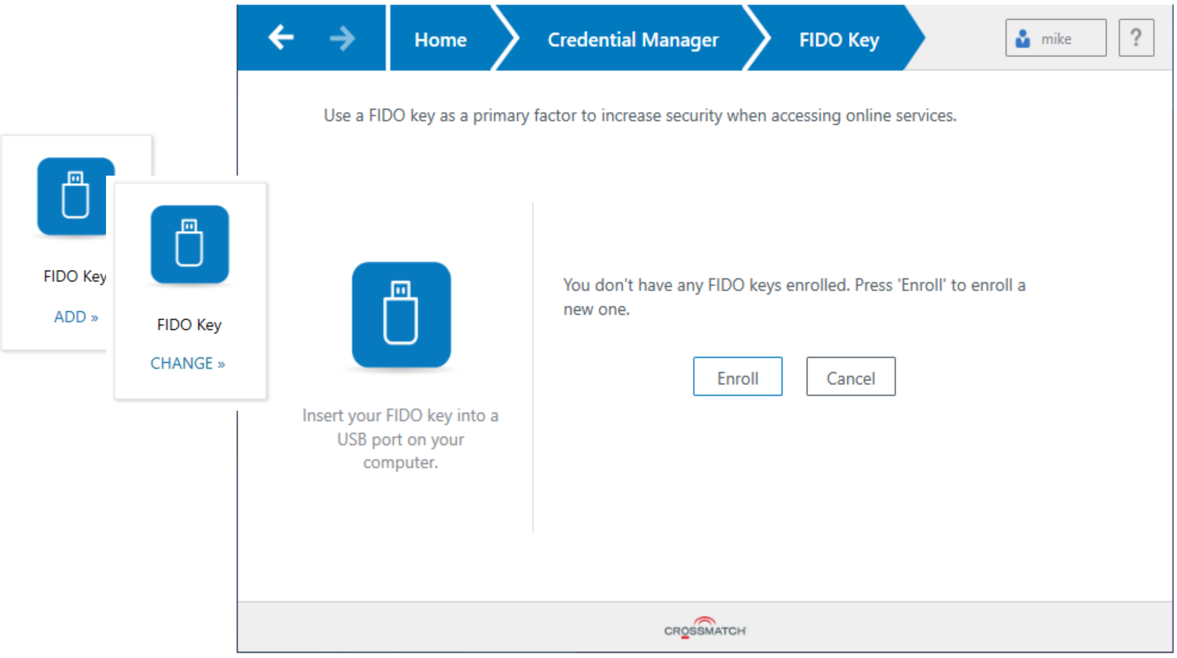
The FIDO Key credential uses a FIDO USB key for authentication. The FIDO Key page is where FIDO keys are entrolled and managed.

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.



Use a FIDO key as a primary factor to increase security when accessing online services.

Insert your FIDO key into a USB port on your computer.

You don't have any FIDO keys enrolled. Press 'Enroll' to enroll a new one.

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.

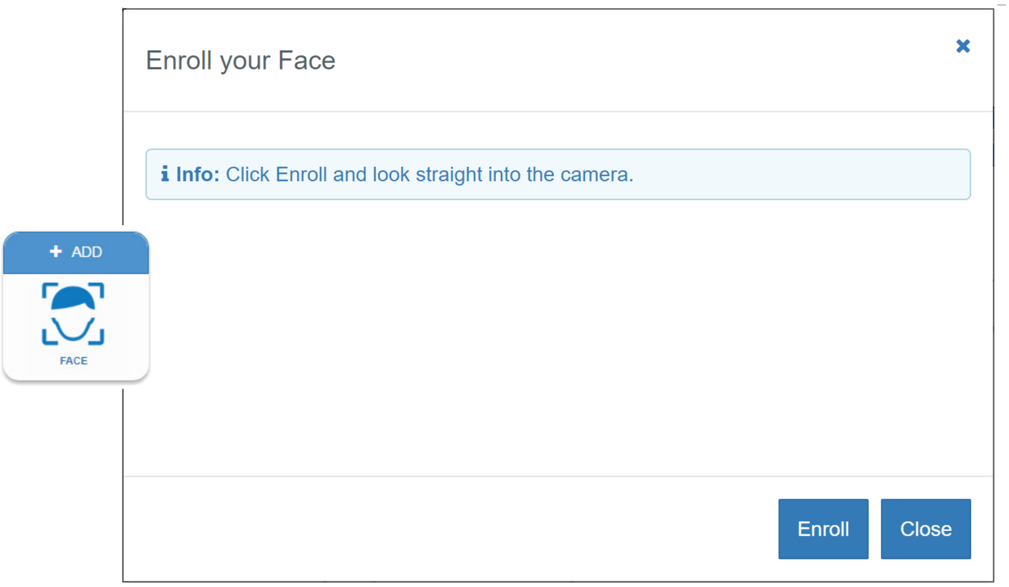
To delete this credential

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:

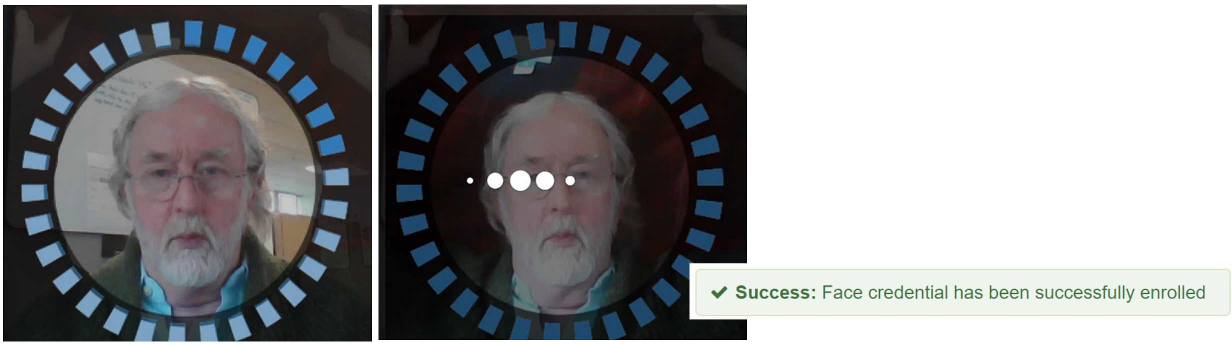
- A separate Face credential license must be purchased and installed on the same machine as the DigitalPersona Server.
- The Enrollment GPO must be enabled and the Face credential selected.
- Your computer must have a built-in or connected camera to enroll a Face credential.


Enroll your Face

Info: Click Enroll and look straight into the camera.

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 willbe 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.


✔ **Success:** Face credential has been successfully enrolled

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 messages 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 messages 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.

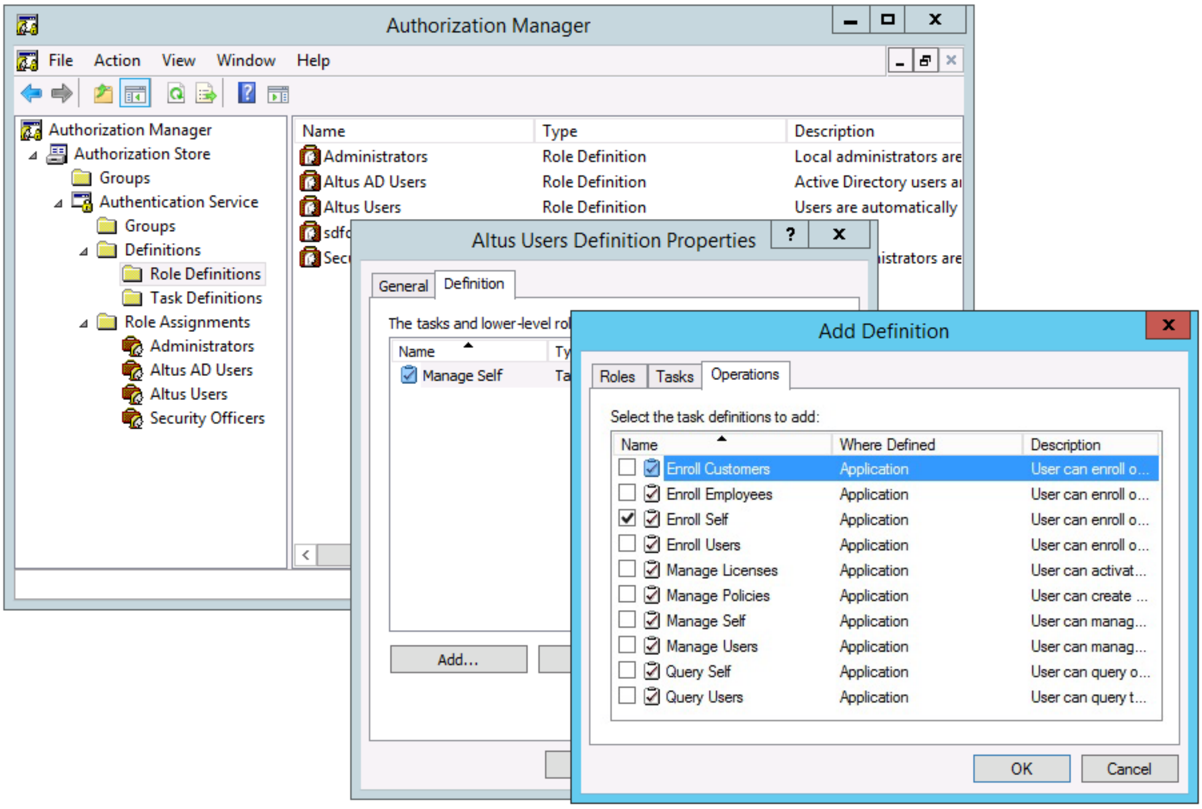
Enabling self enrollment

The Windows Authorization Manager is where you set up your *AD Users* and *Non AD Users* to enroll and manage their own DigitalPersona credentials.

To enable DigitalPersona users to enroll and manage their own DigitalPersona credentials

1. Launch Windows Authorization Manager. (If you are not on the LDS Server machine, see instructions for installing and setting up the Windows Authorization Manager on page *47*.
2. Add the *Enroll Self* task to the predefined DigitalPersona *AD Users* and *Non AD* roles or to another separate role that you create. Note that the term *Altus Users* has been deprecated and replaced with the term *Non AD User*, and

the term *Altus AD Users* with *AD Users* in this documentation, except where the legacy UI specifically still uses the term as is this case in the Authorization Manager.



Name	Type	Description
Administrators	Role Definition	Local administrators are
Altus AD Users	Role Definition	Active Directory users a
Altus Users	Role Definition	Users are automatically
sdfc		
Sec		istrators are

The tasks and lower-level rol

Name	Ty
☑ Manage Self	Ta

Select the task definitions to add:

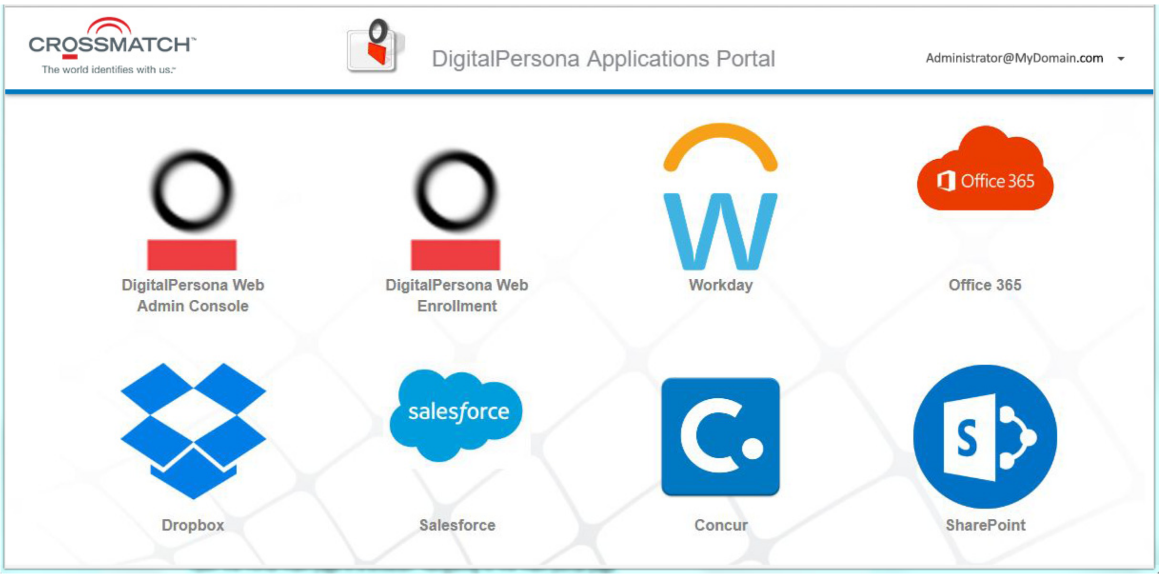
Name	Where Defined	Description
□ Enroll Customers	Application	User can enroll o...
□ Enroll Employees	Application	User can enroll o...
☑ Enroll Self	Application	User can enroll o...
□ Enroll Users	Application	User can enroll o...
□ Manage Licenses	Application	User can activat...
□ Manage Policies	Application	User can create ...
□ Manage Self	Application	User can manag...
□ Manage Users	Application	User can manag...
□ Query Self	Application	User can query o...
□ Query Users	Application	User can query t...

DigitalPersona Application Portal 23

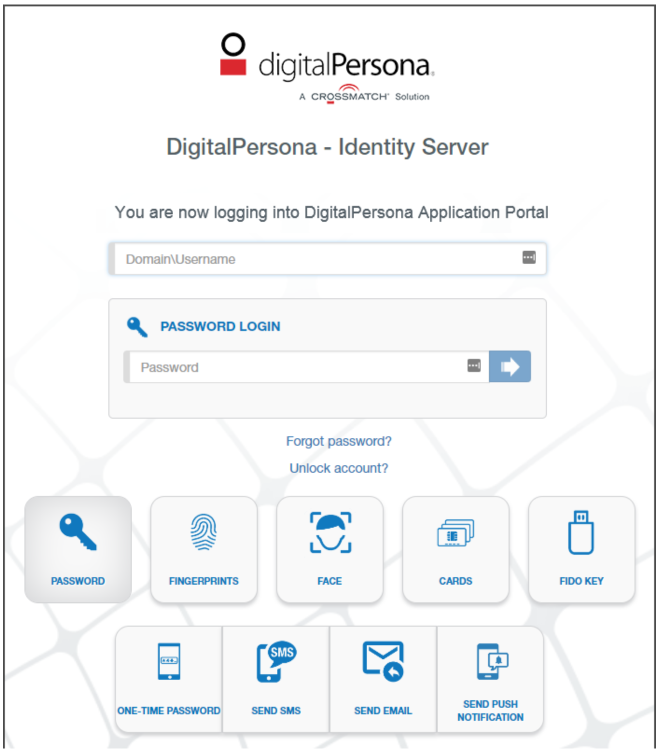
THIS CHAPTER DESCRIBES DIGITALPERSONA APPLICATIONS PORTAL AND ITS CONFIGURATION

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.


CROSSMATCH
The world identifies with us.
DigitalPersona Applications Portal
Administrator@MyDomain.com
DigitalPersona Web Admin Console
DigitalPersona Web Enrollment
Workday
Office 365
Office 365
Dropbox
salesforce
Salesforce
Concur
SharePoint

Sign on to the Application Portal is provided through the DigitalPersona Identity Server, further described on page 231.



DigitalPersona - Identity Server

You are now logging into DigitalPersona Application Portal

Domain\Username

PASSWORD LOGIN

Password

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 applications. You should now be able to access the DigitalPersona Web Administration Console and the DigitalPersona Web Enrollment applications without needing to authenticate again.

Section Four: Appendices

Section Four of the DigitalPersona LDS Administrator Guide includes the following chapters:

Troubleshooting 25

THIS CHAPTER ADDRESSES COMMON QUESTIONS OR ISSUES RELATING TO DIGITALPERSONA, AND HOW TO TROUBLESHOOT AND RESOLVE THE QUESTIONS OR ISSUES.

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.

Resolving configuration error during DigitalPersona LDS install

Issue

Running the DigitalPersona LDS Configuration Wizard (DPADLDSConfig.exe) results in the following error:

Loading entries: Add error on entry starting on line 11: Operations Error

The server side error is:

0x20d6 No superior reference has been configured for the directory service. The directory service is therefore unable to issue referrals to objects outside this forest.

The extended server error is:

000020D6: SvcErr: DSID-0310081B, problem 5012 (DIR_ERROR), data 0

Resolution

This is an occasional issue whose exact cause has not yet been determined. The following procedure is effective in resolving the issue.

- Copy the following folder to the desktop on the server machine.

..\DigitalPersona LDS Server\Configuration Wizard

- Right-click on the DigitalPersona LDS Configuration Wizard (DPADLDSConfig.exe) from the folder you just created on the desktop and select *Run as administrator*.

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 (formerly U.are.U)	Comment
HID DigitalPersona 4500	Drivers for this fingerprint reader are automatically installed as part of the DigitalPersona Workstation or Kiosk installation. The driver can be reinstalled from this directory: *C:\Windows\DPDrv*.
HID DigitalPersona 5xxx	Support for the 5xxx series of HID DigitalPersona external fingerprint readers is technically not from a driver, but rather a code library enabling DigitalPersona support for the this series of fingerprint readers. It is not installed automatically. The library can be found in the *\Drivers\UareU 5100_5160_5200_5300* folder within the DigitalPersona product package. After installation, the reader will be listed in the Device Manager as *PC camera* with Microsoft shown as the provider.
Other non-DigitalPersona	Drivers are provided (but not automatically installed) for the following non-DigitalPersona fingerprint readers. Egistec, Eikon, MINI, and Validity FDG-100, VFS201, VFS451, VFS471, VFS491, VFS495. The drivers can be found in the *\Drivers* 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 the client is unable to contact the DigitalPersona LDS 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

Follow these steps to troubleshoot unavailable server or domain issues.

1. Ensure that you have a network connection. If not, connect your computer to the network.

2. Check whether or not DCOM is enabled. If not, enable DCOM on your computer.

   - Run DCOMCNFG.EXE.
   - Open the *Computers* folder and right click the computer where you wish to enable DCOM. Select *Properties* then *Default Properties* (third tab on the second row).
   - Select *Enable Distributed COM on this computer*. Then click *OK*.

3. Ping your DPCA Server. If ping fails, troubleshoot and resolve the network problem.

4. Temporarily disable the firewall on both the DigitalPersona client and Server. Check whether this solves the connection issue. If it does, configure the firewall, referring to the previous topic *How to configure ports used by DigitalPersona for firewall* on page 280.

5. Check that the Active Directory Global Catalog (GC) is accessible from your computer. If not resolve the issue. using DCDIAG (Domain Controller Diagnosis) to ensure that the GC is up and available.

6. Open ADUC and check that the computer object where DPCA Server is installed has a child SCP object for our service. If not, re-install the DPCA Server.

7. Check that the SCP object has serviceBindingInformation set. If not, restart the DPCA Server computer.

8. If the above steps do not resolve the issue, call DigitalPersona customer support.

How to resolve missing Password Manager Data

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

1. Copy 'dpPasswordManagerData_rangeUppe.ps1' to a local directory.

2. 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.mydomain.com/AppID or https://www.mydomain.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

FIDO Token AppIDs

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 auntehentication.

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 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.

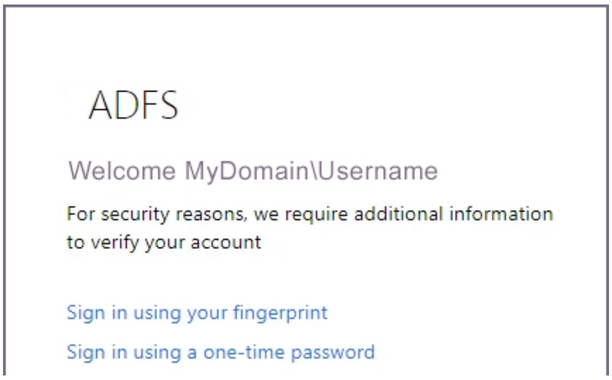
5. Modify the desktop FIDO authentication token to get the Fido AppID from the WebGetSettings interface and use it in enrollment and authentication.

DigitalPersona ADFS Extension 26

THIS CHAPTER DESCRIBES DIGITALPERSONA APPLICATIONS PORTAL AND ITS CONFIGURATION

Overview

The DigitalPersona ADFS Extension adds fingerprint and OTP authentication methods (DigitalPersona credentials) to an ADFS environment.



ADFS

Welcome MyDomain\Username

For security reasons, we require additional information to verify your account

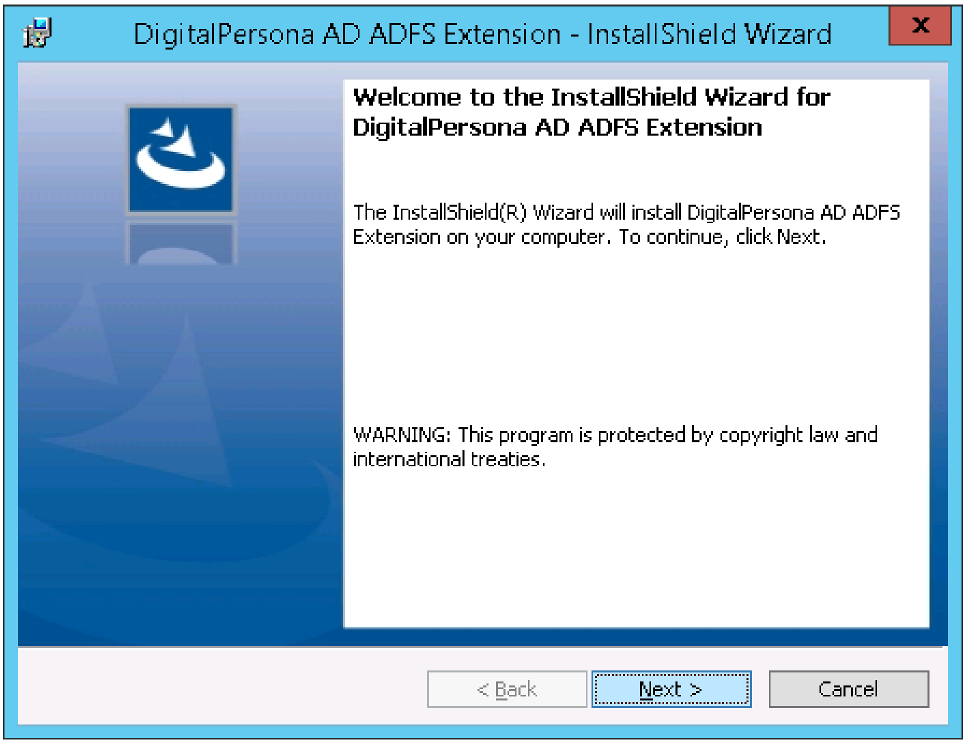
Sign in using your fingerprint

Sign in using a one-time password

Installation

To install the DigitalPersona ADFS Extension

1. Launch the installation wizard by running the *DigitalPersona ADFS Extension.exe* file. Click *Next*.



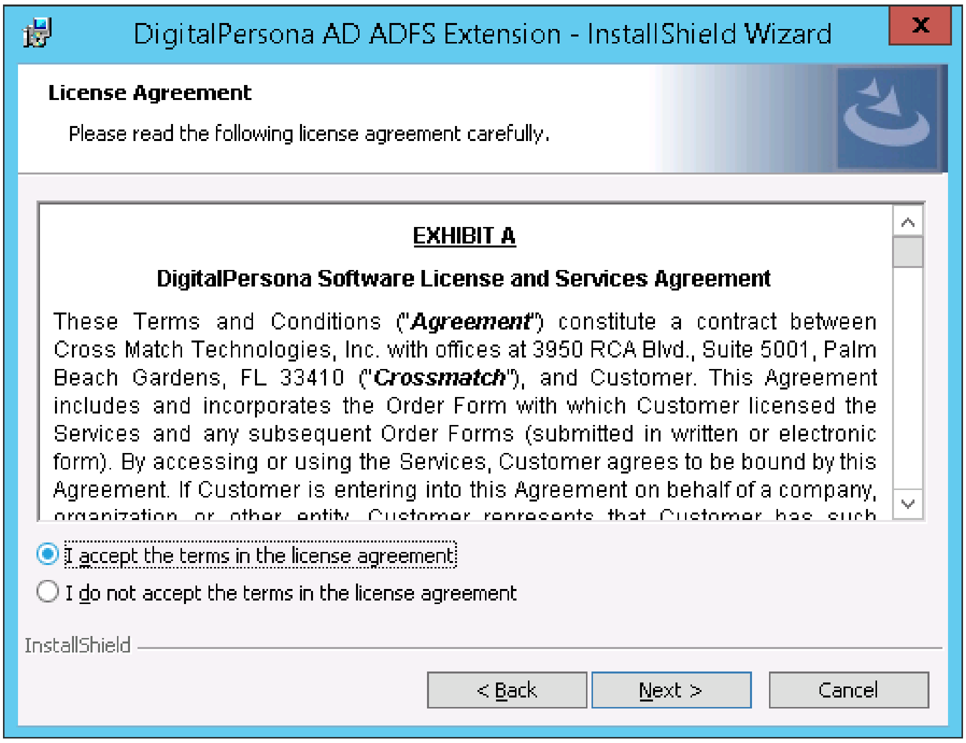
DigitalPersona AD ADFS Extension - InstallShield Wizard

Welcome to the InstallShield Wizard for DigitalPersona AD ADFS Extension

The InstallShield(R) Wizard will install DigitalPersona AD ADFS Extension on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. Accept the license agreement. Click *Next*.



DigitalPersona AD ADFS Extension - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

EXHIBIT A

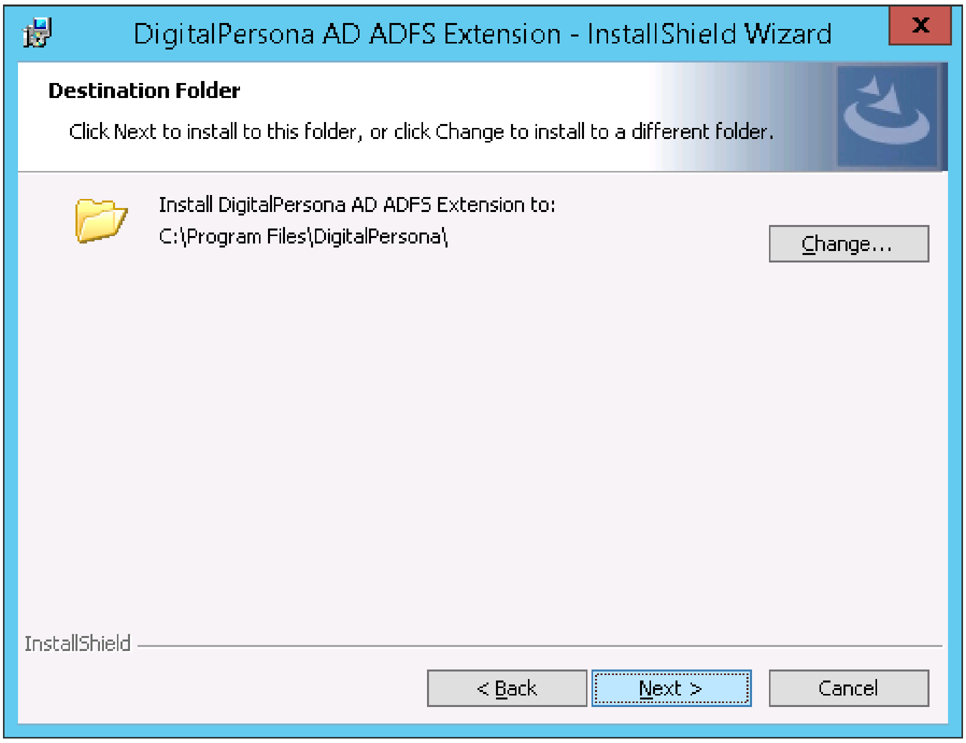
DigitalPersona Software License and Services Agreement

These Terms and Conditions ("***Agreement***") constitute a contract between Cross Match Technologies, Inc. with offices at 3950 RCA Blvd., Suite 5001, Palm Beach Gardens, FL 33410 ("***Crossmatch***"), and Customer. This Agreement includes and incorporates the Order Form with which Customer licensed the Services and any subsequent Order Forms (submitted in written or electronic form). By accessing or using the Services, Customer agrees to be bound by this Agreement. If Customer is entering into this Agreement on behalf of a company, organization or other entity, Customer represents that Customer has such

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. Accept the default destination folder, or click *Change* to install to a different folder. Then click *Next*.



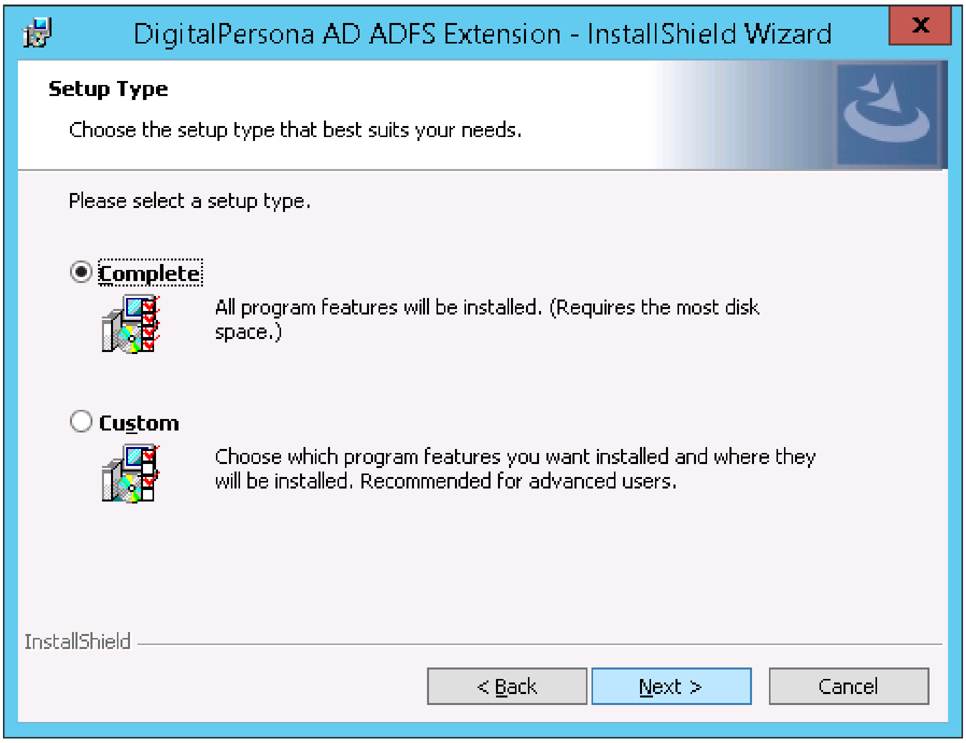
DigitalPersona AD ADFS Extension - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install DigitalPersona AD ADFS Extension to:
C:\Program Files\DigitalPersona\

4. Accept the default *Setup Type* of *Complete,* and click *Next.*



Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

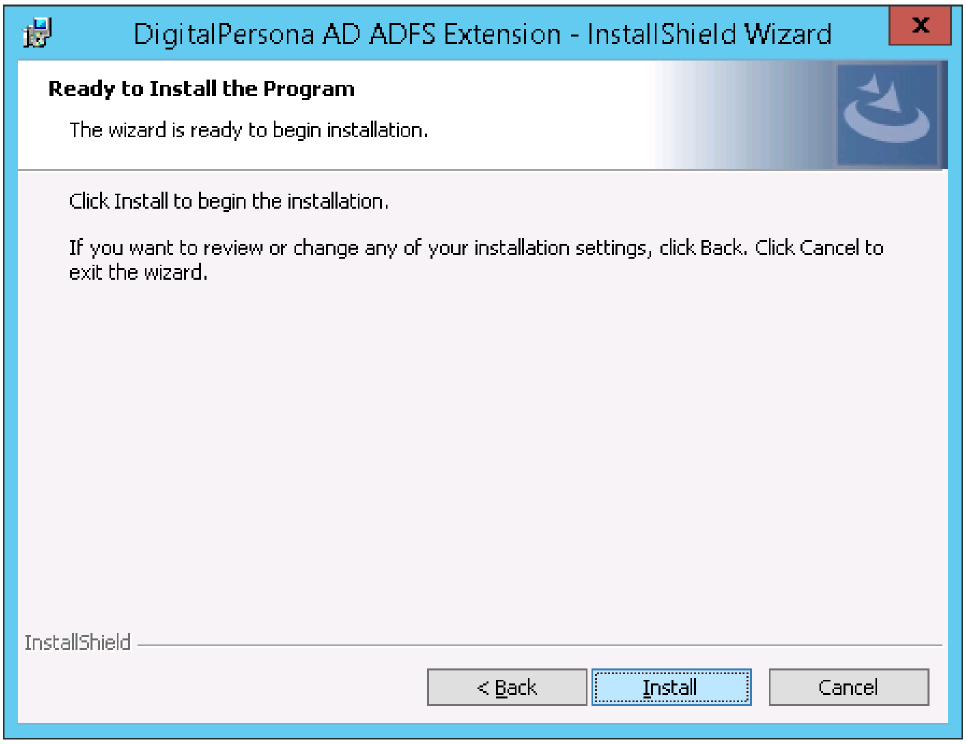
● Complete

All program features will be installed. (Requires the most disk space.)

○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

5. On the *Ready to Install the Program* page, click *Install* to begin the installation.



DigitalPersona AD ADFS Extension - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

6. When installation is completed, on the final page of the wizard, click *Finish*.

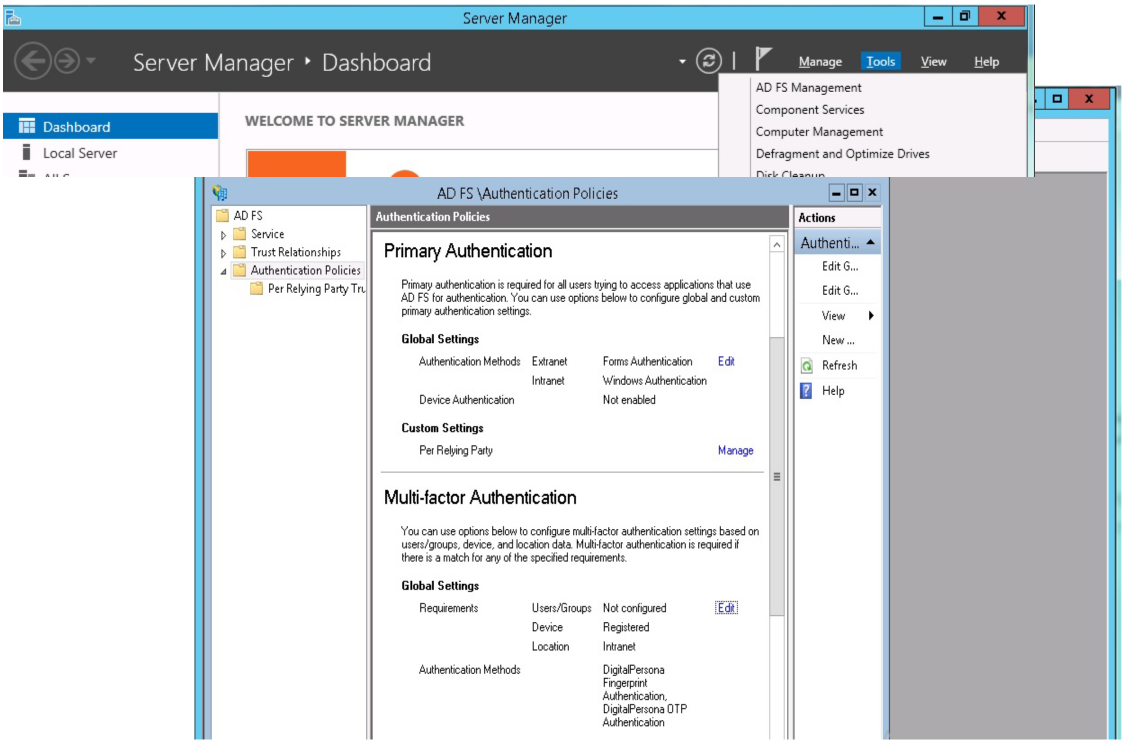
Selecting and deselecting DigitalPersona credentials

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*.



Authentication Policies

Primary Authentication

Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure global and custom primary authentication settings.

Global Settings

Authentication Methods	Extranet	Forms Authentication	Edit
	Intranet	Windows Authentication	
Device Authentication		Not enabled	

Custom Settings

Per Relying Party — Manage

Multi-factor Authentication

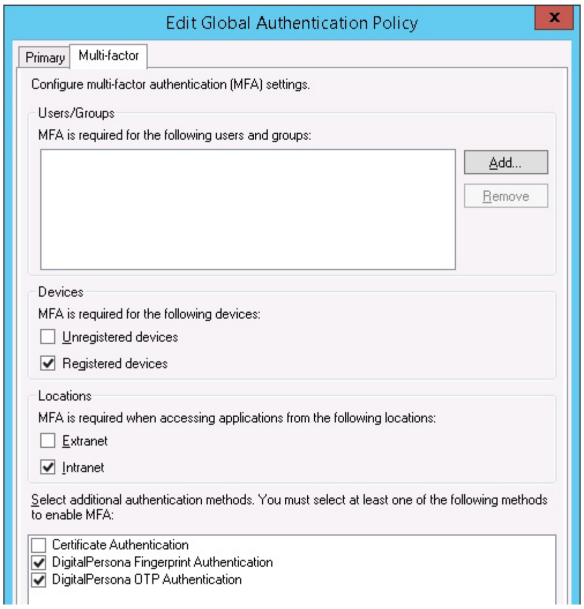
You can use options below to configure multi-factor authentication settings based on users/groups, device, and location data. Multi-factor authentication is required if there is a match for any of the specified requirements.

Global Settings

Requirements	Users/Groups	Not configured	Edit
	Device	Registered	
	Location	Intranet	
Authentication Methods		DigitalPersona Fingerprint Authentication, DigitalPersona OTP Authentication	

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.



Configure multi-factor authentication (MFA) settings.

Users/Groups

MFA is required for the following users and groups:

Devices

MFA is required for the following devices:

☐ Unregistered devices
☑ Registered devices

Locations

MFA is required when accessing applications from the following locations:

☐ Extranet
☑ Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

☐ Certificate Authentication
☑ DigitalPersona Fingerprint Authentication
☑ DigitalPersona OTP Authentication

DigitalPersona NPS Plugin 27

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.

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.

Also, the DigitalPersona NPS Plugin can only be used to open a VPN channel for DigitalPersona AD users, not for Non AD users.

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 *267* 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.

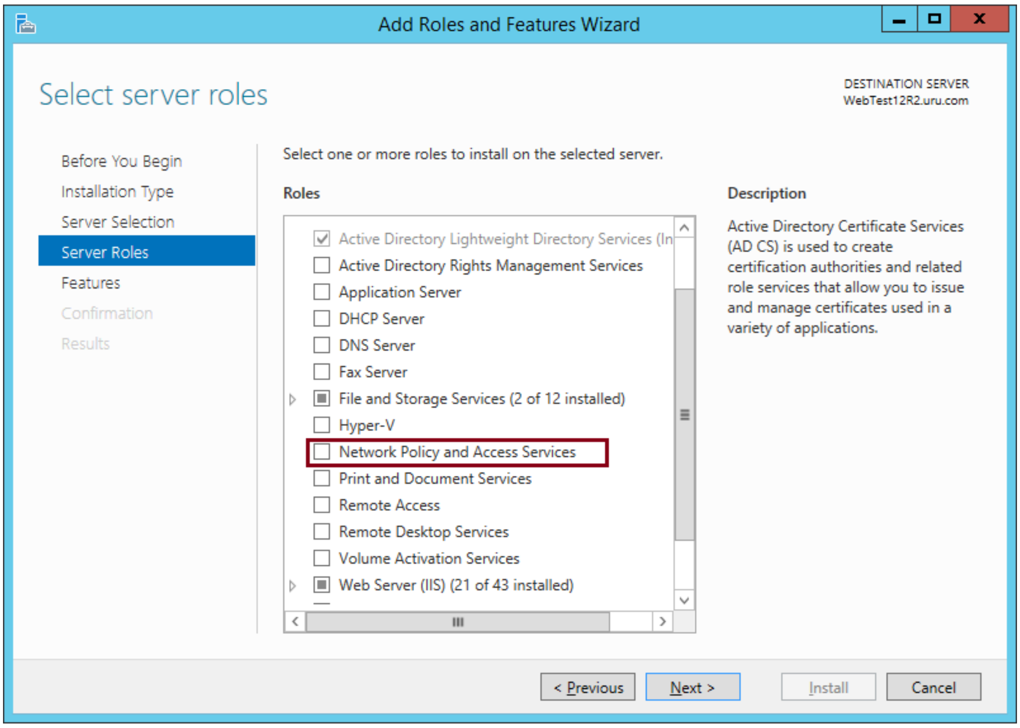
NPS is a server role of Windows Server 2012 R2 and later that performs authentication, authorization, and accounting for wireless, authenticating switch, and remote access dial-up and virtual private network (VPN) connections.

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*.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WebTest12R2.uru.com

Select one or more roles to install on the selected server.

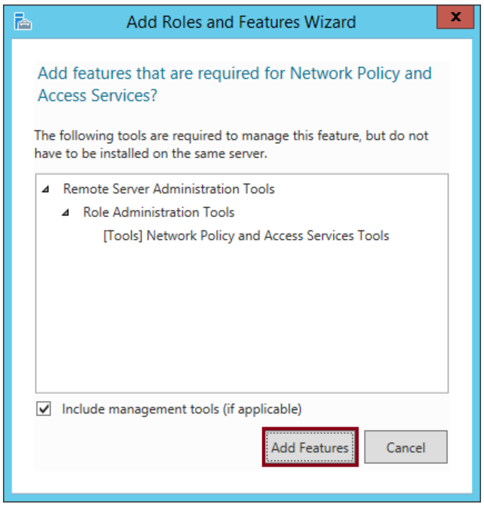
Roles

- ☑ Active Directory Lightweight Directory Services (In
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▨ File and Storage Services (2 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ▨ Web Server (IIS) (21 of 43 installed)

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

5. On the *Add Features* dialog, click *Add Features*.



Add Roles and Features Wizard

Add features that are required for Network Policy and Access Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] Network Policy and Access Services Tools

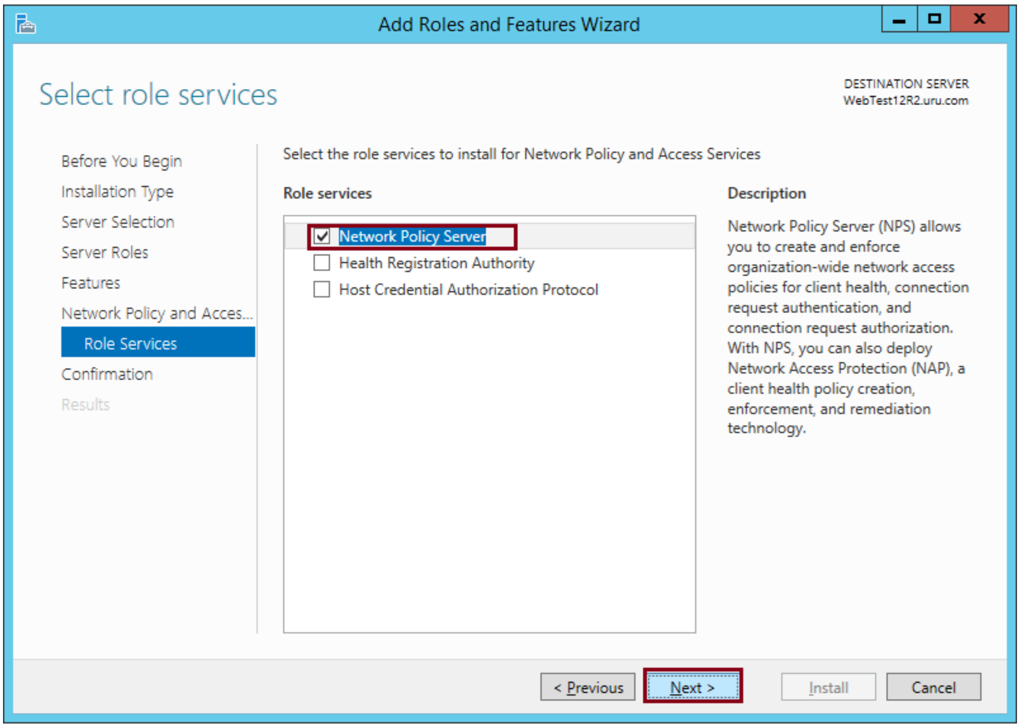
☑ Include management tools (if applicable)

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*.



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WebTest12R2.uru.com

Select the role services to install for Network Policy and Access Services

Role services

☑ Network Policy Server
□ Health Registration Authority
□ Host Credential Authorization Protocol

Description

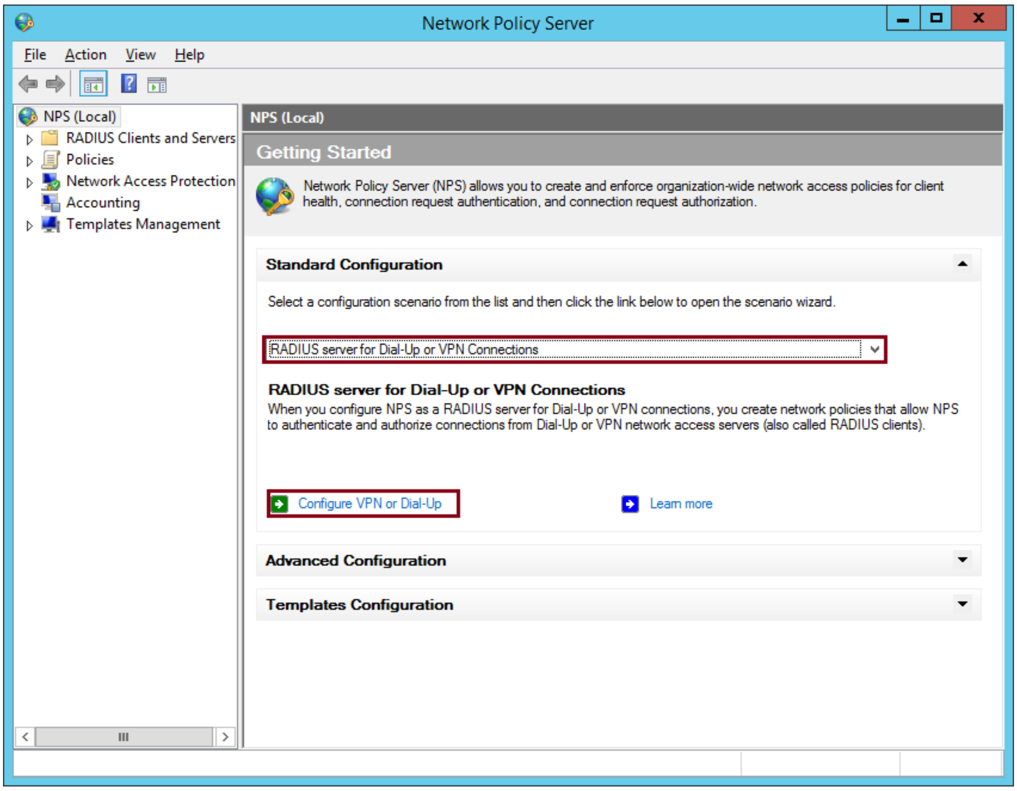
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

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*.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

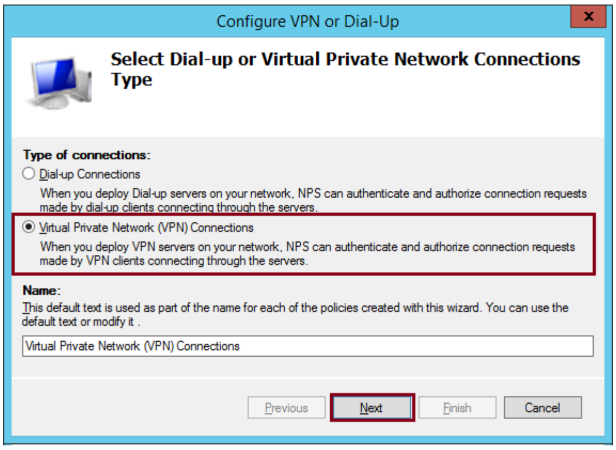
Select a configuration scenario from the list and then click the link below to open the scenario wizard.

RADIUS server for Dial-Up or VPN Connections

RADIUS server for Dial-Up or VPN Connections

When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).

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*.



Select Dial-up or Virtual Private Network Connections Type

Type of connections:

○ Dial-up Connections

When you deploy Dial-up servers on your network, NPS can authenticate and authorize connection requests made by dial-up clients connecting through the servers.

● Virtual Private Network (VPN) Connections

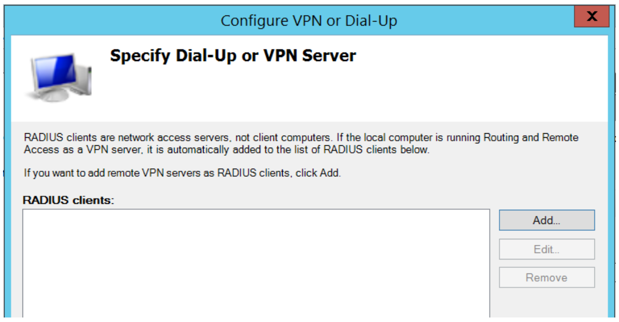
When you deploy VPN servers on your network, NPS can authenticate and authorize connection requests made by VPN clients connecting through the servers.

Name:

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .

Virtual Private Network (VPN) Connections

15. On the *Specify Dial-Up or VPN Server* page, click *Add*.



Specify Dial-Up or VPN Server

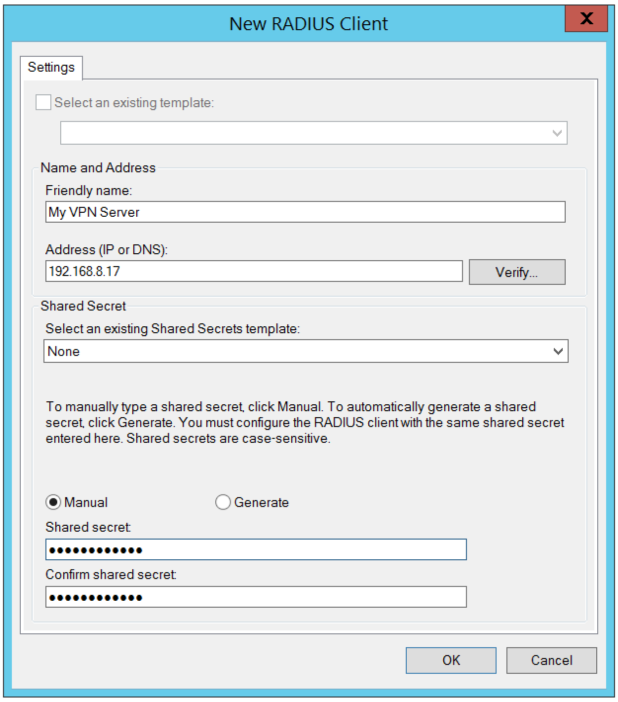
RADIUS clients are network access servers, not client computers. If the local computer is running Routing and Remote Access as a VPN server, it is automatically added to the list of RADIUS clients below.

If you want to add remote VPN servers as RADIUS clients, click Add.

RADIUS clients:

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.



□ Select an existing template:

Name and Address

Friendly name: My VPN Server

Address (IP or DNS): 192.168.8.17

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

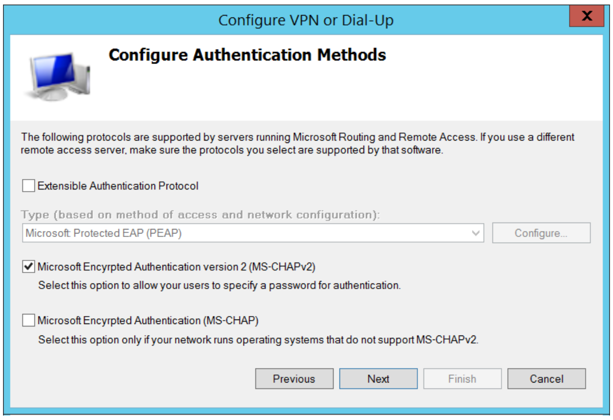
● Manual ○ Generate

Shared secret: ••••••••••••

Confirm shared secret: ••••••••••••

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*.



Configure Authentication Methods

The following protocols are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the protocols you select are supported by that software.

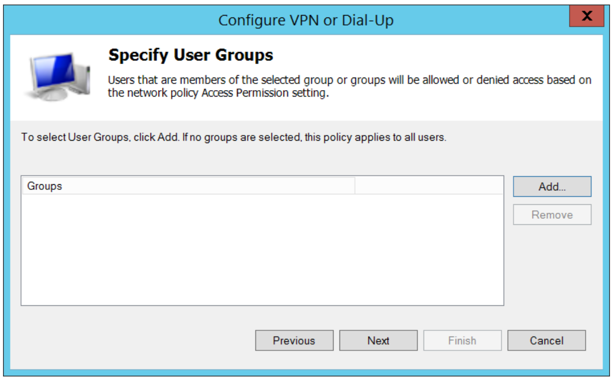
☐ Extensible Authentication Protocol

Type (based on method of access and network configuration):
Microsoft: Protected EAP (PEAP)

☑ Microsoft Encrypted Authentication version 2 (MS-CHAPv2)
Select this option to allow your users to specify a password for authentication.

☐ Microsoft Encrypted Authentication (MS-CHAP)
Select this option only if your network runs operating systems that do not support MS-CHAPv2.

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*.



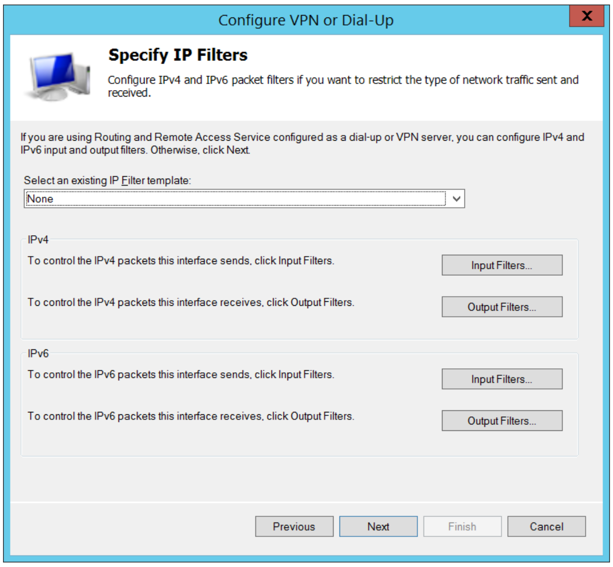
Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

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*.



Configure VPN or Dial-Up

Specify IP Filters

Configure IPv4 and IPv6 packet filters if you want to restrict the type of network traffic sent and received.

If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure IPv4 and IPv6 input and output filters. Otherwise, click Next.

Select an existing IP Filter template: None

IPv4

To control the IPv4 packets this interface sends, click Input Filters.

To control the IPv4 packets this interface receives, click Output Filters.

IPv6

To control the IPv6 packets this interface sends, click Input Filters.

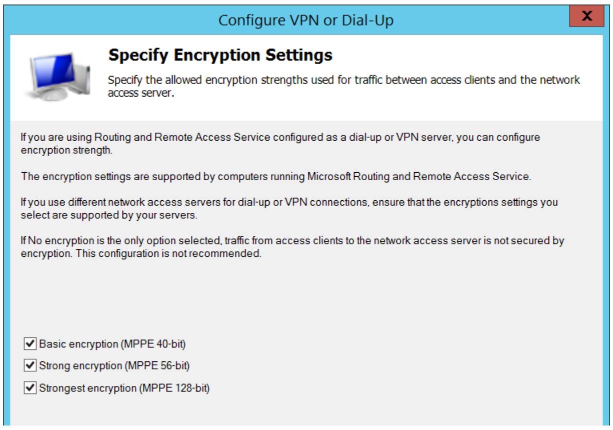
To control the IPv6 packets this interface receives, click Output Filters.

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.



Configure VPN or Dial-Up

Specify Encryption Settings

Specify the allowed encryption strengths used for traffic between access clients and the network access server.

If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure encryption strength.

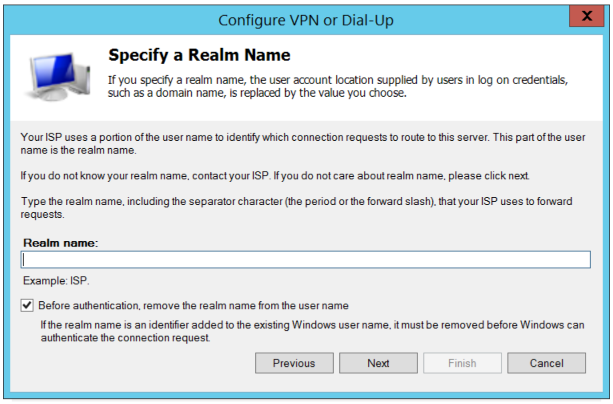
The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

If you use different network access servers for dial-up or VPN connections, ensure that the encryptions settings you select are supported by your servers.

If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

☑ Basic encryption (MPPE 40-bit)
☑ Strong encryption (MPPE 56-bit)
☑ Strongest encryption (MPPE 128-bit)

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*.



Configure VPN or Dial-Up

Specify a Realm Name

If you specify a realm name, the user account location supplied by users in log on credentials, such as a domain name, is replaced by the value you choose.

Your ISP uses a portion of the user name to identify which connection requests to route to this server. This part of the user name is the realm name.

If you do not know your realm name, contact your ISP. If you do not care about realm name, please click next.

Type the realm name, including the separator character (the period or the forward slash), that your ISP uses to forward requests.

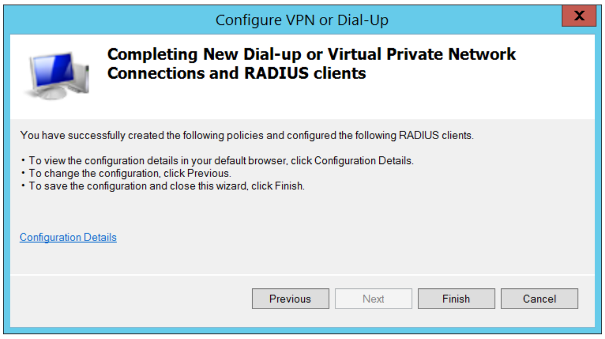
Realm name:

Example: ISP.

☑ Before authentication, remove the realm name from the user name

If the realm name is an identifier added to the existing Windows user name, it must be removed before Windows can authenticate the connection request.

24. On the *Completing* ... page, click *Finish*.



Configure VPN or Dial-Up

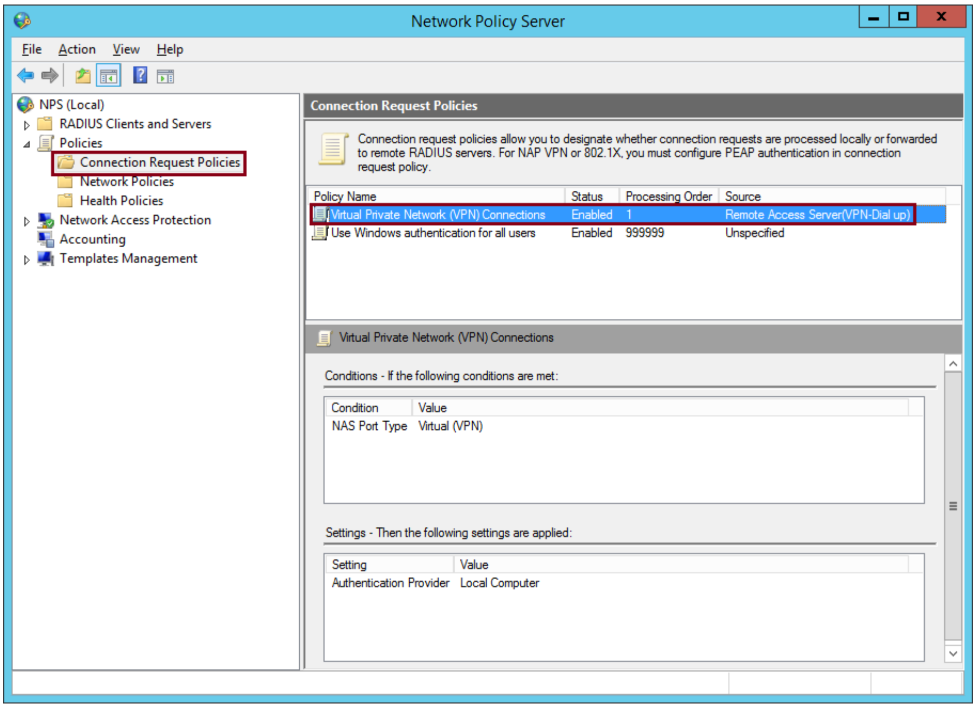
Completing New Dial-up or Virtual Private Network Connections and RADIUS clients

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

Configuration Details

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.



Connection Request Policies

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
Virtual Private Network (VPN) Connections	Enabled	1	Remote Access Server(VPN-Dial up)
Use Windows authentication for all users	Enabled	999999	Unspecified

Virtual Private Network (VPN) Connections

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Virtual (VPN)

Settings - Then the following settings are applied:

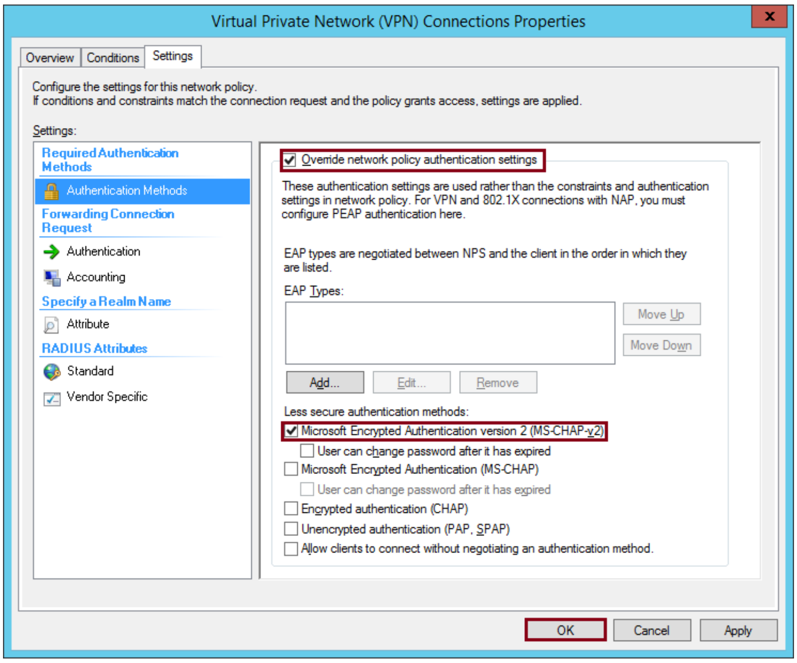
Setting	Value
Authentication Provider	Local Computer

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)



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

☑ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  □ User can change password after it has expired
□ Microsoft Encrypted Authentication (MS-CHAP)
  □ User can change password after it has expired
□ Encrypted authentication (CHAP)
□ Unencrypted authentication (PAP, SPAP)
□ Allow clients to connect without negotiating an authentication method.

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 298).

2. The *Shared secret* must be the same as that specified in step 18 on page 298.

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*.

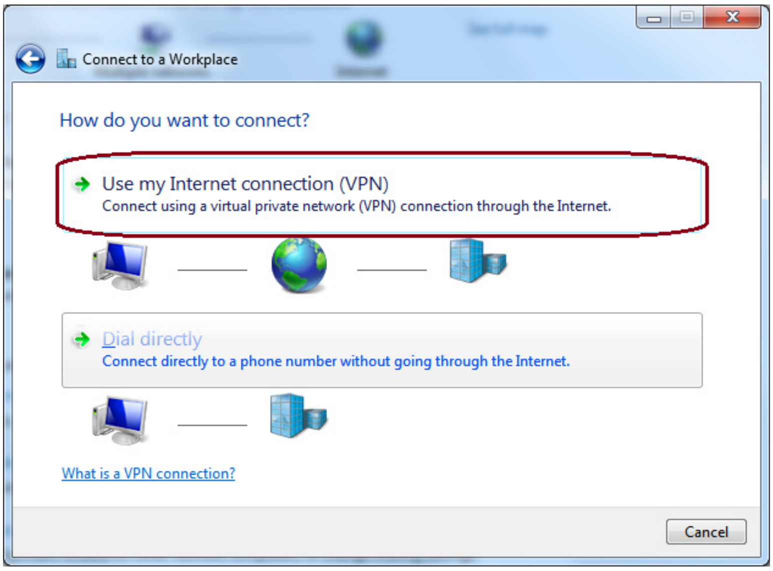
4. Follow the onscreen instructions.

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)*.



Connect to a Workplace

How do you want to connect?

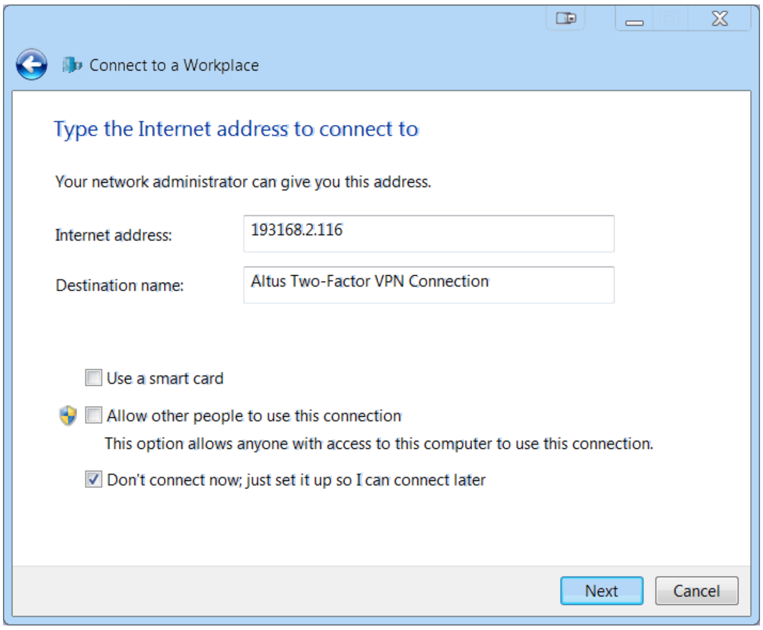
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

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*.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 193168.2.116

Destination name: Altus Two-Factor VPN Connection

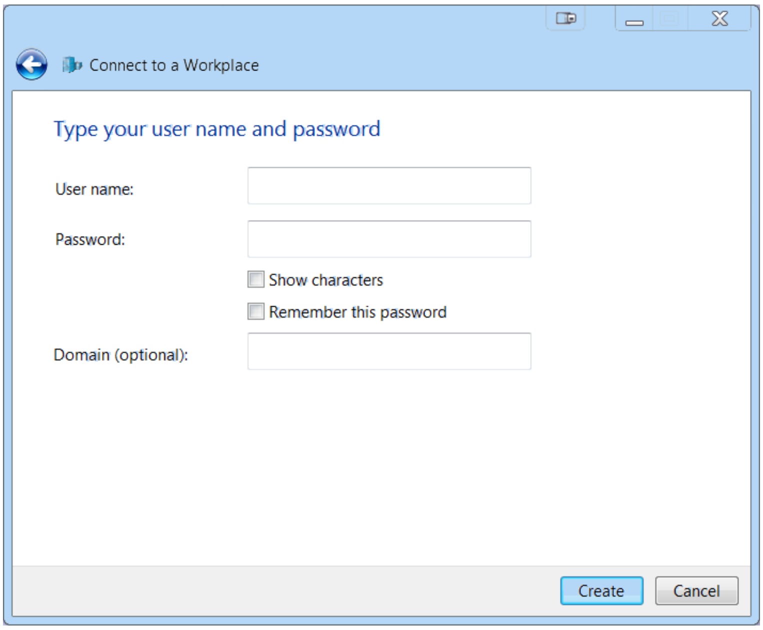
☐ Use a smart card

☐ Allow other people to use this connection

This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

6. On the following page, do not fill in any fields, simply click *Create*.



Connect to a Workplace

Type your user name and password

User name:

Password:

☐ Show characters

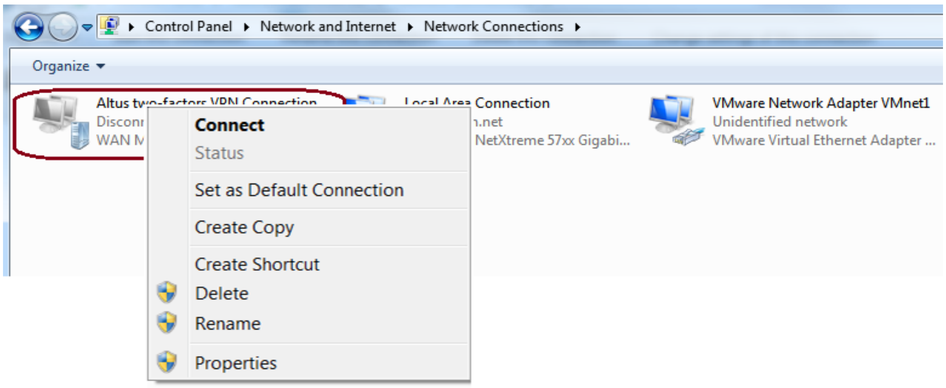
☐ Remember this password

Domain (optional):

7. Once the VPN connection has been created, it needs to be configured.

Configuring the VPN connection

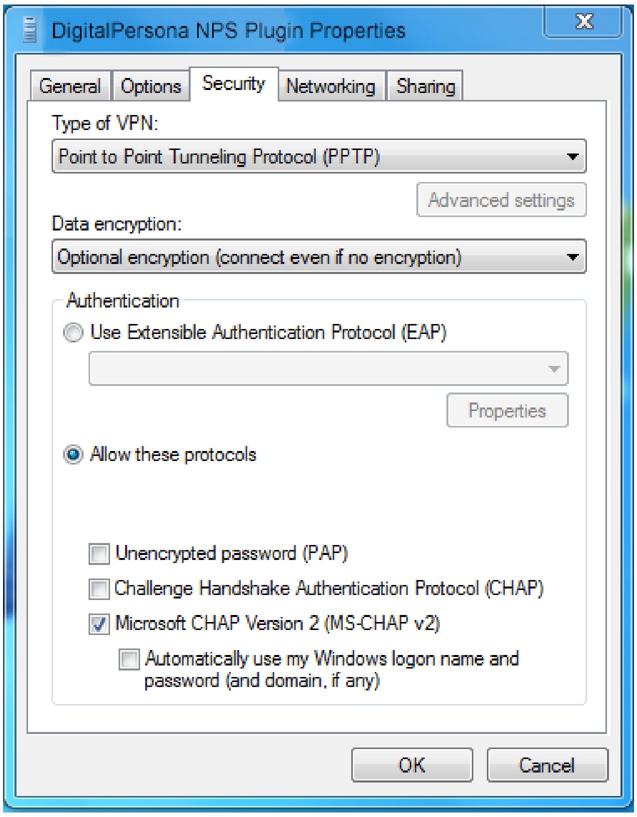
1. In the Control Panel, select *Network Connections*. Right-click the connection and select *Properties*.


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Organize ▾
Altus two-factors VPN Connection
Disconn
WAN M
Local Area Connection
.net
NetXtreme 57xx Gigabi...
VMware Network Adapter VMnet1
Unidentified network
VMware Virtual Ethernet Adapter ...
Connect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
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.



Type of VPN: Point to Point Tunneling Protocol (PPTP)

Data encryption: Optional encryption (connect even if no encryption)

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

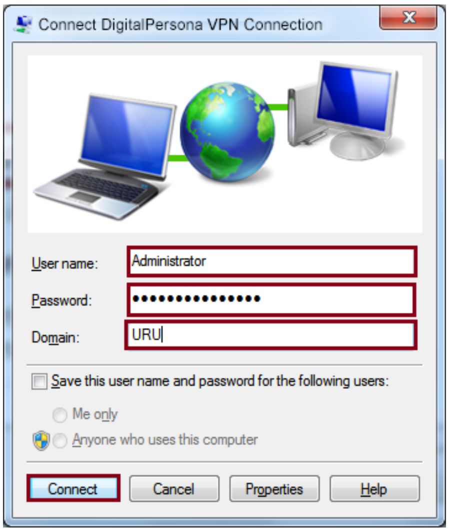
☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

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*.



Connect DigitalPersona VPN Connection

User name: Administrator

Password: •••••••••••••••

Domain: URU

☐ Save this user name and password for the following users:

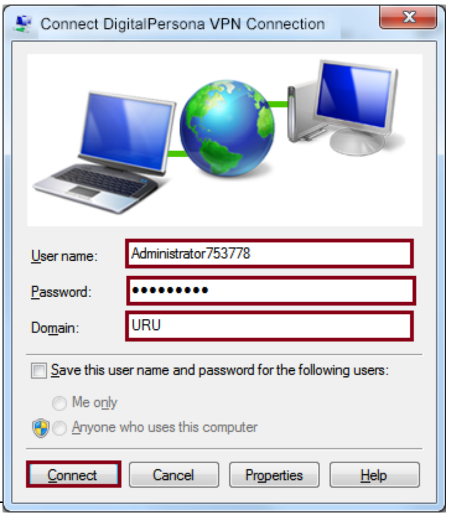
○ Me only

○ Anyone who uses this computer

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*.



Connect DigitalPersona VPN Connection

User name: Administrator753778

Password: ••••••••••

Domain: URU

☐ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

Using OTP Push Notification (v3.1+)

OTP Push notification, in version 3.1 and above, is implemented to automatically recognize a One-Time Password (OTP) appended to your VPN password when delimited by a comma. For example, MyP@ssw0rd,34875.

When a password is submitted without an appended OTP, the DigitalPersona Server will initiate push notification automatically, sending a notification to your enrolled device requesting authorization.

This feature may be referred to as “Auto-Push OTP”.

Using OTP Push Notification with PAP (v3.0.2-)

In order to use OTP Push Notification over PAP with DigitalPersona products prior to v3.1, you would follow these 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 - 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 (v3.0.2-)

In order to use OTP Push Notification over MS-CHAPv2 with DigitalPersona products prior to v3.1, you would follow these 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 - 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

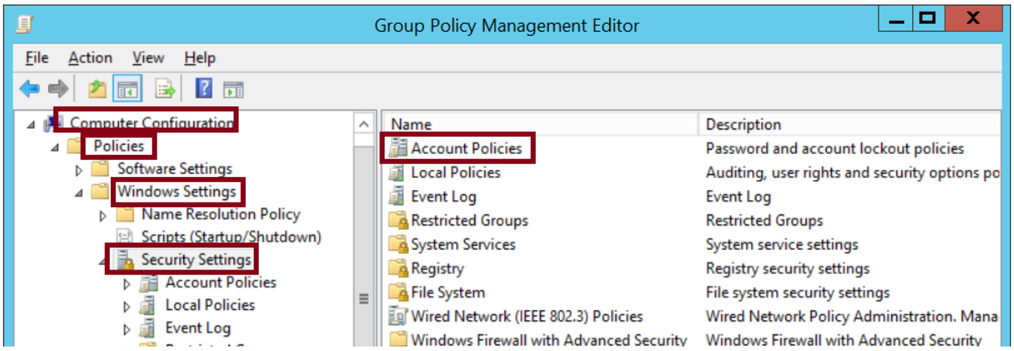
To use the CHAP protocol with the DigitalPersona NPS Plugin, the *Store password using reversible encryption* Password Policy must be enabled.

See the following for further details.

Configuration required when using CHAP

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773343(v=ws.10
To allow reversible encryption complete the following steps.

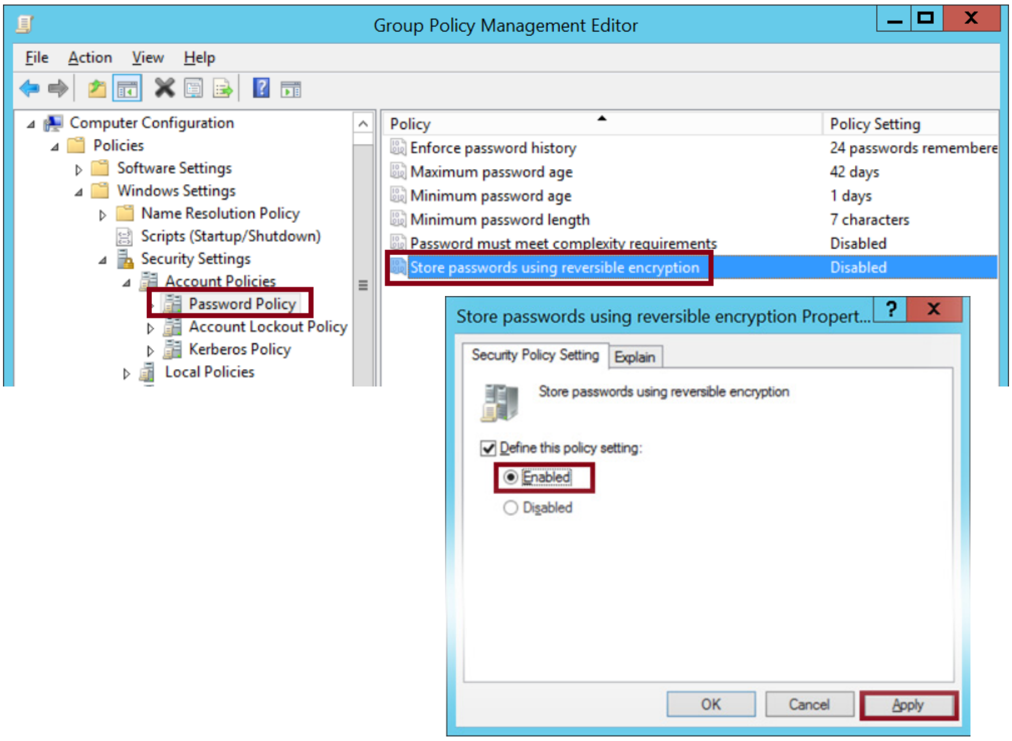
1. Open the Group Policy Management Editor.
2. Open the Default Domain Policy for editing.
3. Navigate to Computer Configuration|Policies|Windows Settings|Security Settings|Account Policies.



Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options po
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File system security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Mana
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security

4. Open *Password Policy* and double-click *Store password using reversible encryption*.

5. Enable the policy and click *Apply*.



Policy	Policy Setting
Enforce password history	24 passwords remembere
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Store passwords using reversible encryption Propert...

Security Policy Setting | Explain

Store passwords using reversible encryption

☑ Define this policy setting:

● Enabled

○ Disabled

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.

- User name - (AD Users only) 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 and Non AD Users are not supported.
- Password: - Enter your Windows password.

6. Then click *OK*.

Citrix Support 28

THIS CHAPTER PROVIDES INFORMATION ABOUT DIGITALPERSONA’S SUPPORT FOR DEPLOYMENT IN THE CITRIX ENVIRONMENT.

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.

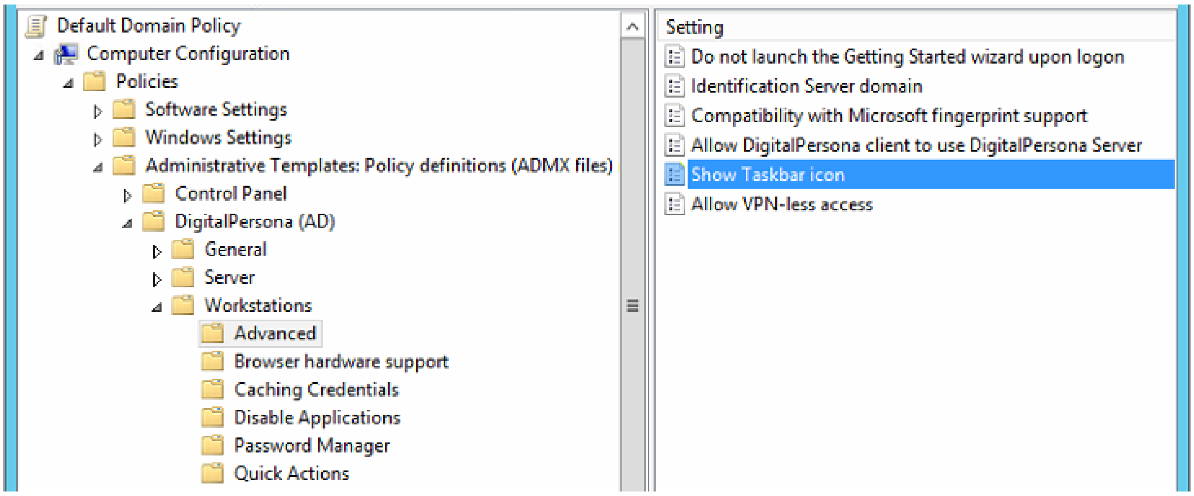
XenDesktop limitation

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 >Polices > 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.

Resolving missing DigitalPersona system tray icon

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*.

Fingerprint Adjudication and Deduplication 29

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.

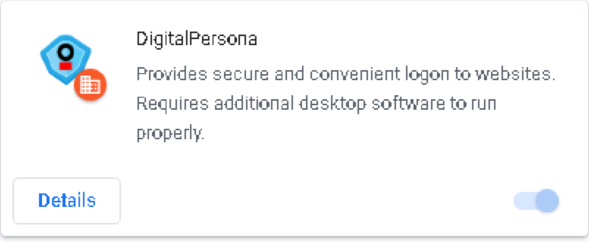
Finger	#
Left pinky finger	0
Left ring finger	1
Left middle finger	2
Left index finger	3
Left thumb	4
Right thumb	5
Right index finger	6
Right middle finger	7
Right ring finger	8
Right pinky finger	9

Chrome install via GPO 30

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.



DigitalPersona

Provides secure and convenient logon to websites. Requires additional desktop software to run properly.

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.

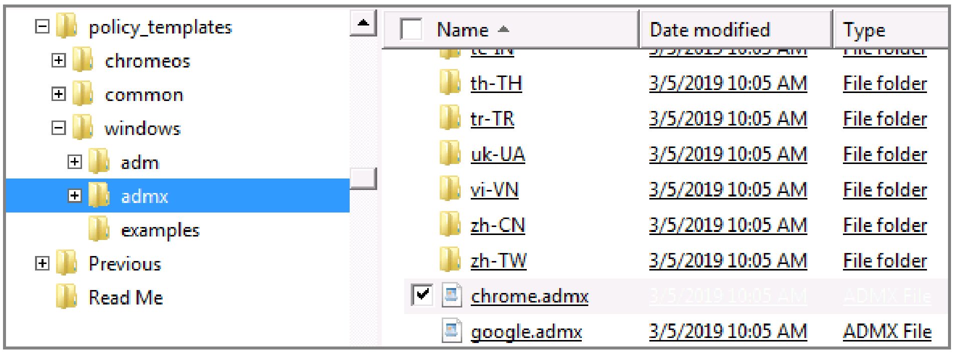
Installation

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).



policy_templates
chromeos
common
windows
adm
admx
examples
Previous
Read Me

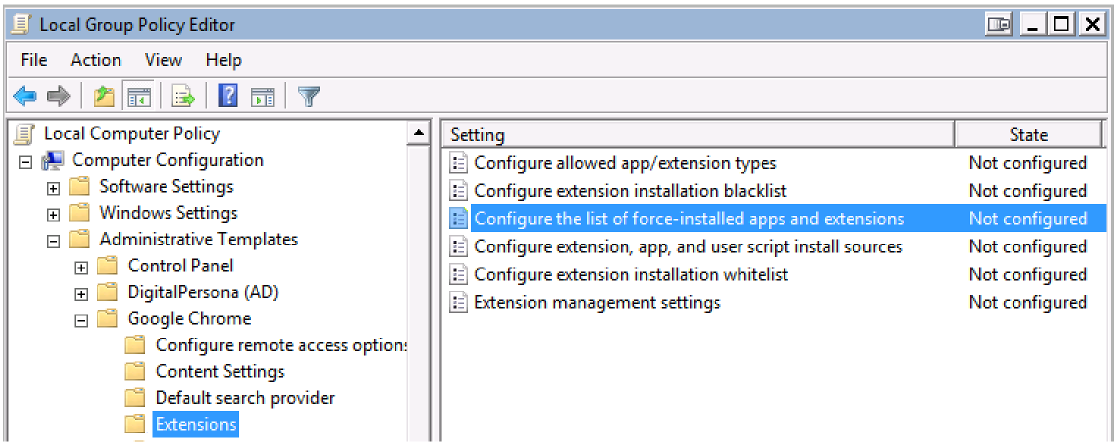
Name	Date modified	Type
th-TH	3/5/2019 10:05 AM	File folder
tr-TR	3/5/2019 10:05 AM	File folder
uk-UA	3/5/2019 10:05 AM	File folder
vi-VN	3/5/2019 10:05 AM	File folder
zh-CN	3/5/2019 10:05 AM	File folder
zh-TW	3/5/2019 10:05 AM	File folder
☑ chrome.admx	3/5/2019 10:05 AM	ADMX File
google.admx	3/5/2019 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.

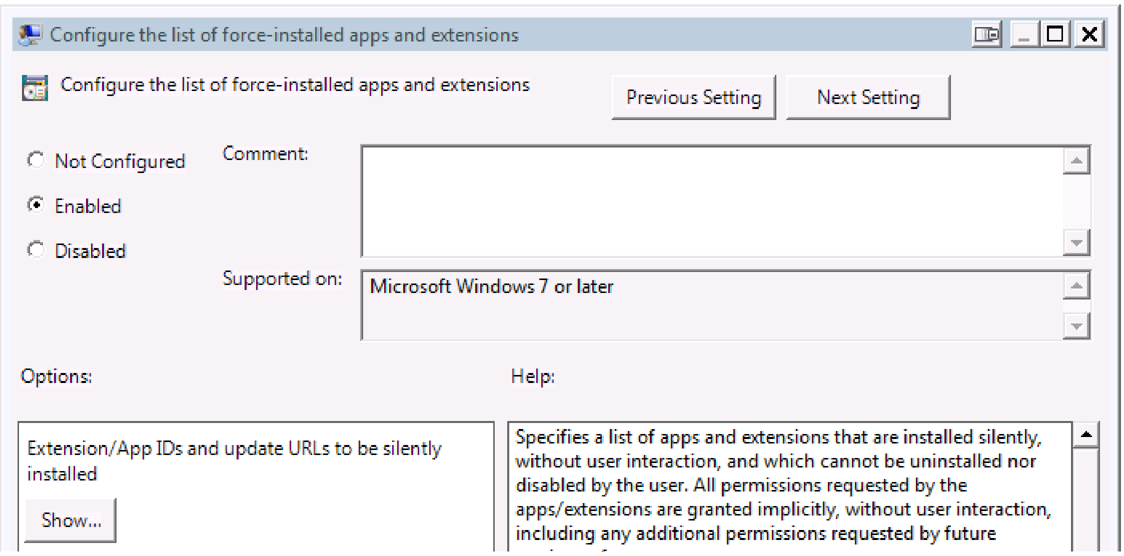
   To launch the Local Group Policy Editor, click on the *Start* button, type *Run* and press *Enter* to open the *Run window*. The type *gpedit.msc* and click *OK* to open the Local Computer Policy Editor.

6. Navigate to the following folder: *Local Computer Policy\Computer Configuration\Administrative Templates\Google Chrome\Extensions*.



Setting	State
Configure allowed app/extension types	Not configured
Configure extension installation blacklist	Not configured
Configure the list of force-installed apps and extensions	Not configured
Configure extension, app, and user script install sources	Not configured
Configure extension installation whitelist	Not configured
Extension management settings	Not configured

7. Double-click *Configure the list of force-installed apps and extensions* to open a dialog of the same name.


Configure the list of force-installed apps and extensions
Configure the list of force-installed apps and extensions
Previous Setting
Next Setting
Show...

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Microsoft Windows 7 or later

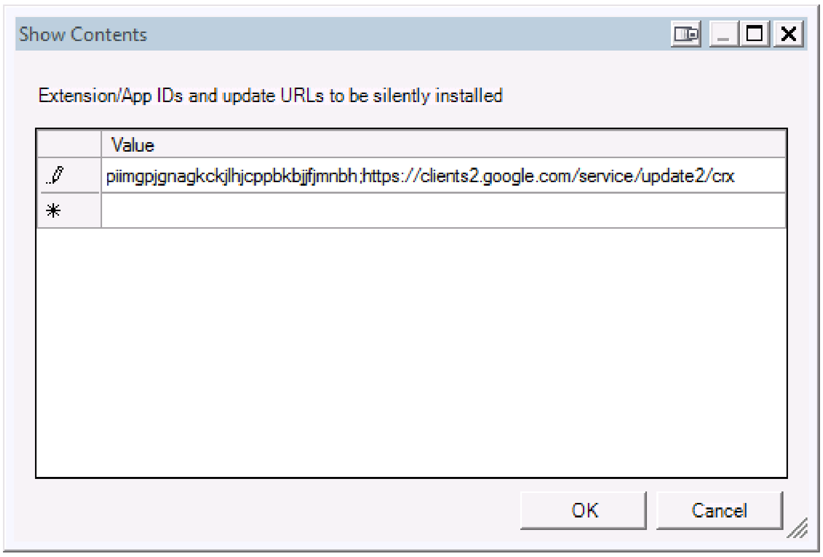
Options:

Extension/App IDs and update URLs to be silently installed

Help:

Specifies a list of apps and extensions that are installed silently, without user interaction, and which cannot be uninstalled nor disabled by the user. All permissions requested by the apps/extensions are granted implicitly, without user interaction, including any additional permissions requested by future

8. Select the *Enabled* radio button and then click *Show...*. to display the *Show Contents* dialog.



Extension/App IDs and update URLs to be silently installed

	Value
	piimgpjgnagkckjlhjcppbkbjjfjmnbh;https://clients2.google.com/service/update2/crx
*	

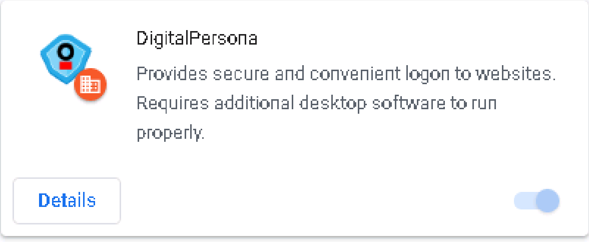
9. Copy and paste the following string into the text field and then click *OK*.

   piimgpjgnagkckjlhjcppbkbjjfjmnbh;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.


DigitalPersona

Provides secure and convenient logon to websites. Requires additional desktop software to run properly.

Support for secure and small sensors 31

THIS CHAPTER DESCRIBES DIGITALPERSONA 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

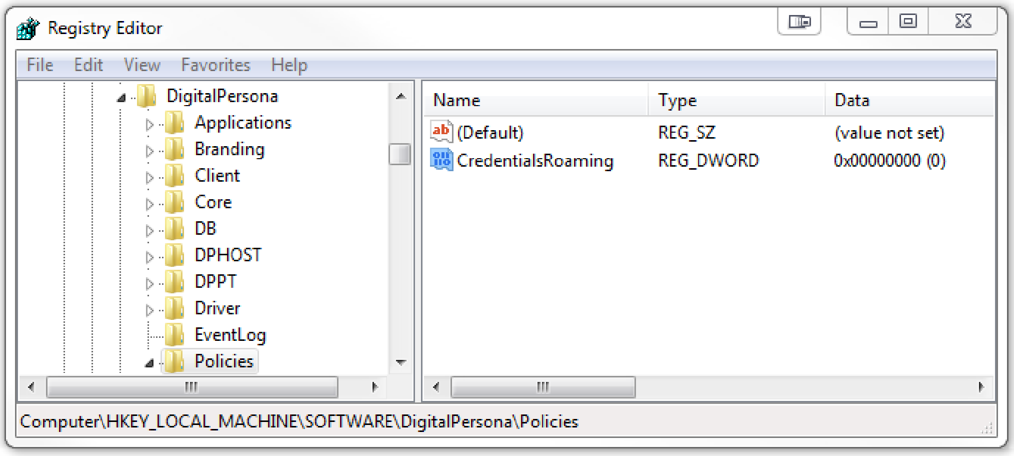
Complete the following steps to override the default *CredentialsRoaming* policy setting (which actually only affects roaming of fingerprints) in order to support the use of Microsoft's WBF driver for fingerprint matching and storage on the computer.

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
CredentialsRoaming	REG_DWORD	0x00000000 (0)

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.

v2.3 to 3.0 Revised GPO settings 32

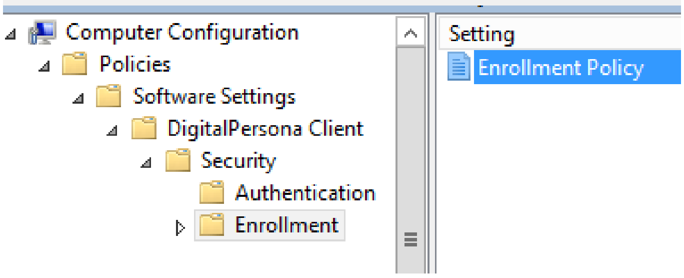
Version 3.0 of the DigitalPersona solution includes a significant reorganization of the containers and policy settings governing the software (compared to version 2.3), as well as several new, revised and renamed containers and policy settings, described below as they appear in the Windows Group Policy Editor. For complete descriptions of each setting, refer to the *Policies and Settings* chapter beginning on page *118*.

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

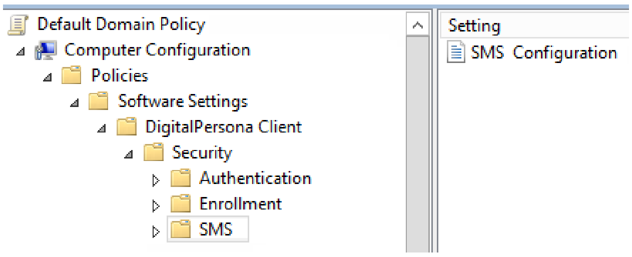
The *Security* GPO includes two new settings.

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 Client/Authentication Devices\OTP* GPO.

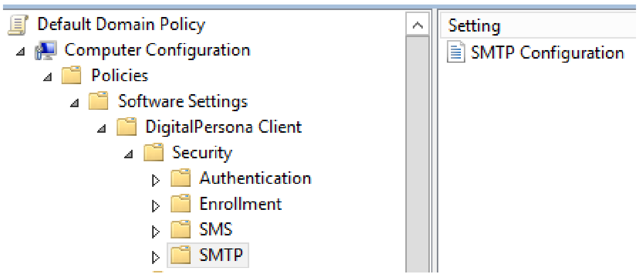
These values are

- 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.



- Default Domain Policy
  - Computer Configuration
    - Policies
      - Software Settings
        - DigitalPersona Client
          - Security
            - Authentication
            - Enrollment
            - SMS
            - SMTP

Setting

SMTP Configuration

These values are

- SMTP Server
- Port
- Email Address
- Email Password

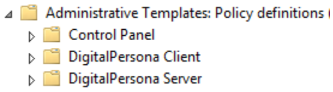
Additionally, a field is provided for entering an *Incoming Email Address* and a *Test Settings* button, which can be used to confirm that the designated SMTP Server is working.

Computer Configuration/Policies/Administrative Templates

New Administrative Templates structure

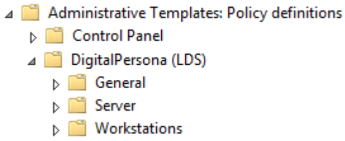
Within the Computer Configuration/Policies/Administrative Templates container, the structure has been changed significantly, both at the topmost DigitalPersona level (as shown below) and at suceeding levels as shown in the images that follow.

Previous high-level structure



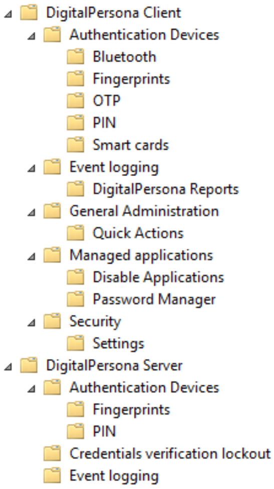
- Administrative Templates: Policy definitions (
  - Control Panel
  - DigitalPersona Client
  - DigitalPersona Server

New high-level structure



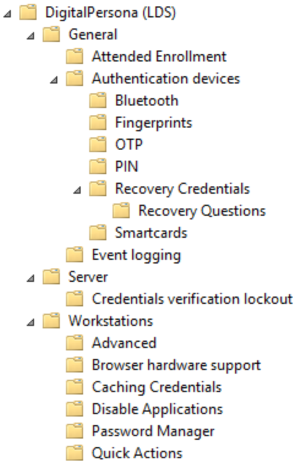
- Administrative Templates: Policy definitions
  - Control Panel
  - DigitalPersona (LDS)
    - General
    - Server
    - Workstations

Previous expanded strcture



- DigitalPersona 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 Server
  - Authentication Devices
    - Fingerprints
    - PIN
  - Credentials verification lockout
  - Event logging

New expanded structure



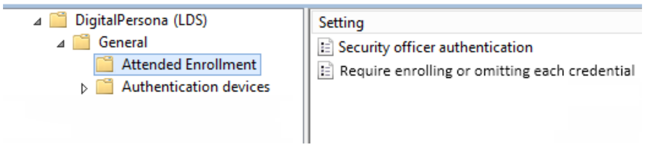
- DigitalPersona (LDS)
  - General
    - Attended Enrollment
    - Authentication devices
      - Bluetooth
      - Fingerprints
      - OTP
      - PIN
      - Recovery Credentials
        - Recovery Questions
      - Smartcards
    - Event logging
  - Server
    - Credentials verification lockout
  - Workstations
    - Advanced
    - Browser hardware support
    - Caching Credentials
    - Disable Applications
    - Password Manager
    - Quick Actions

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.

- Security Officer authentication
- Require enrolling or omitting each credential



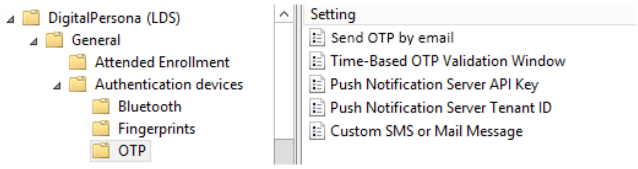
- DigitalPersona (LDS)
  - General
    - Attended Enrollment
    - Authentication devices

Setting

- Security officer authentication
- Require enrolling or omitting each credential

Send OTP by email

This setting is new, supporting the ability in this version for an AD User to choose to have their One-Time Password sent to them by email.



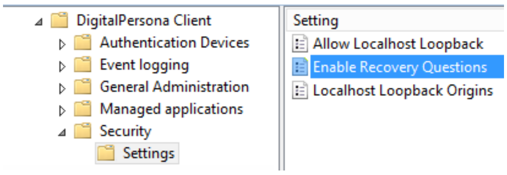
- DigitalPersona (LDS)
  - General
    - Attended Enrollment
    - Authentication devices
      - Bluetooth
      - Fingerprints
      - OTP

Setting

- Send OTP by email
- Time-Based OTP Validation Window
- Push Notification Server API Key
- Push Notification Server Tenant ID
- Custom SMS or Mail Message

Recovery Credentials

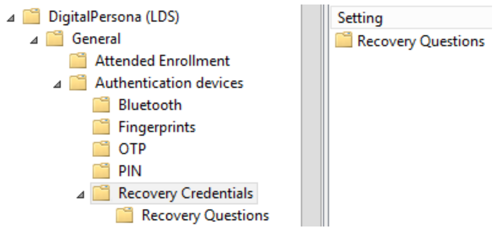
This GPO is new, and includes a new GPO, *Recovery Questions* and within that, the *Enable Recovery Questions* setting, moved from the previous *DigitalPersona Client/ Security/Settings*.



- DigitalPersona Client
  - Authentication Devices
  - Event logging
  - General Administration
  - Managed applications
  - Security
    - Settings

Setting

- Allow Localhost Loopback
- Enable Recovery Questions
- Localhost Loopback Origins



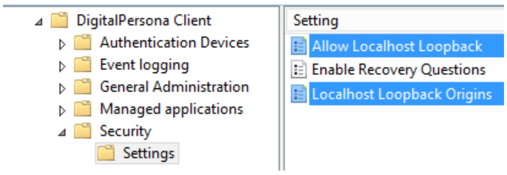
- DigitalPersona (LDS)
  - General
    - Attended Enrollment
    - Authentication devices
      - Bluetooth
      - Fingerprints
      - OTP
      - PIN
      - Recovery Credentials
        - Recovery Questions

Setting

- Recovery Questions

Browser hardware support

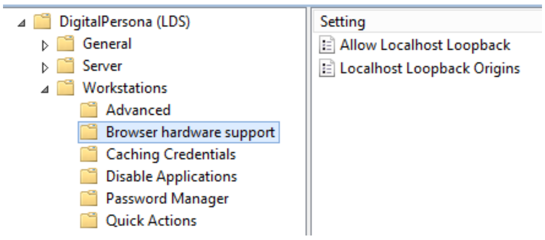
This GPO is new, and includes two settings previously located in the *DigitalPersona Client/Security/Settings* containers, *Allow Localhost Loopback* and *Localhost Loopback Origins.*



- DigitalPersona Client
  - Authentication Devices
  - Event logging
  - General Administration
  - Managed applications
  - Security
    - Settings

Setting

- Allow Localhost Loopback
- Enable Recovery Questions
- Localhost Loopback Origins



- DigitalPersona (LDS)
  - General
  - Server
  - Workstations
    - Advanced
    - Browser hardware support
    - Caching Credentials
    - Disable Applications
    - Password Manager
    - Quick Actions

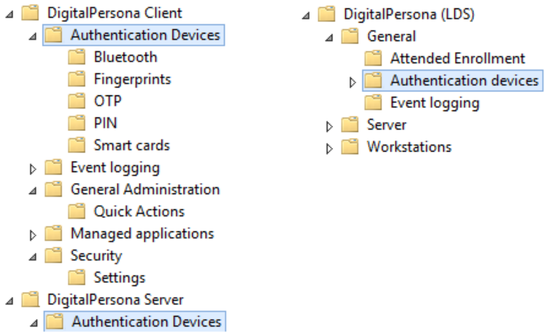
Setting

- Allow Localhost Loopback
- 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, located in the *DigitalPersona/General* container, which includes the previous settings for both Server and Client.

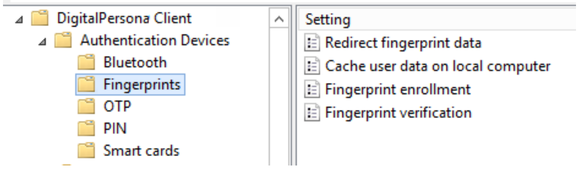


- DigitalPersona Client
  - Authentication Devices
    - Bluetooth
    - Fingerprints
    - OTP
    - PIN
    - Smart cards
  - Event logging
  - General Administration
    - Quick Actions
  - Managed applications
  - Security
    - Settings
- DigitalPersona Server
  - Authentication Devices

- DigitalPersona (LDS)
  - General
    - Attended Enrollment
    - Authentication devices
    - Event logging
  - Server
  - Workstations

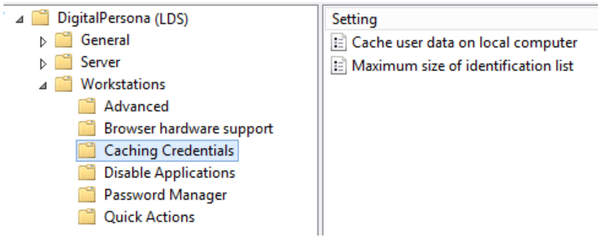
Cache user data on local computer

This setting was previously located within the *DigitalPersona Client/Authentication Devices/Fingerprint* GPO, and has been relocated to the *DigitalPersona/Workstations/Caching Credentials* GPO.



- DigitalPersona Client
  - Authentication Devices
    - Bluetooth
    - Fingerprints
    - OTP
    - PIN
    - Smart cards

Setting
- Redirect fingerprint data
- Cache user data on local computer
- Fingerprint enrollment
- Fingerprint verification

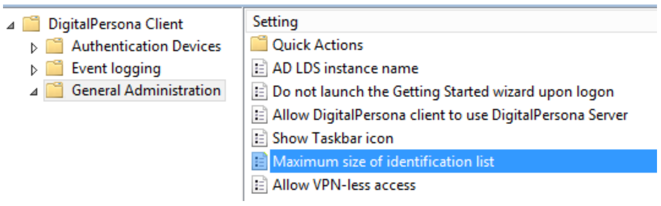


- DigitalPersona (LDS)
  - General
  - Server
  - Workstations
    - Advanced
    - Browser hardware support
    - Caching Credentials
    - Disable Applications
    - Password Manager
    - Quick Actions

Setting
- Cache user data on local computer
- Maximum size of identification list

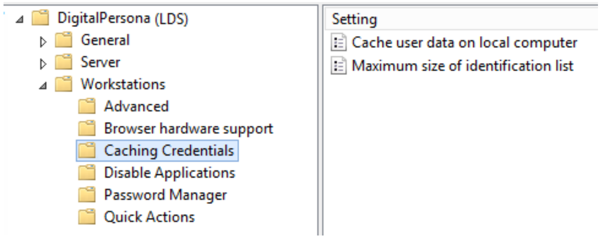
Maximum size of identification list

This setting was previously located within the *DigitalPersona Client/General Administration* GPO, and has been relocated to the *DigitalPersona/Workstations/Caching Credentials* GPO.



- DigitalPersona Client
  - Authentication Devices
  - Event logging
  - General Administration

Setting
- Quick Actions
- AD LDS instance name
- Do not launch the Getting Started wizard upon logon
- Allow DigitalPersona client to use DigitalPersona Server
- Show Taskbar icon
- Maximum size of identification list
- Allow VPN-less access

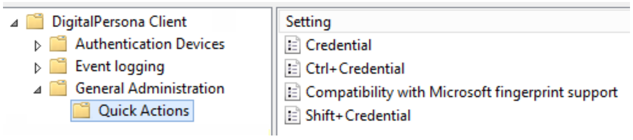


- DigitalPersona (LDS)
  - General
  - Server
  - Workstations
    - Advanced
    - Browser hardware support
    - Caching Credentials
    - Disable Applications
    - Password Manager
    - Quick Actions

Setting
- Cache user data on local computer
- Maximum size of identification list

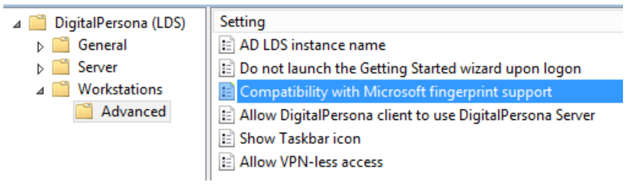
Compatability with Microsoft fingerprint support

This setting was previously located within the *DigitalPersona Client/General Administration/Quick Actions* GPO, and has been relocated to the *DigitalPersona/Workstations/Advanced* GPO.



- DigitalPersona Client
  - Authentication Devices
  - Event logging
  - General Administration
    - Quick Actions

Setting
- Credential
- Ctrl+Credential
- Compatibility with Microsoft fingerprint support
- Shift+Credential

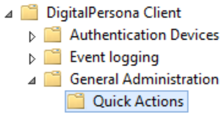


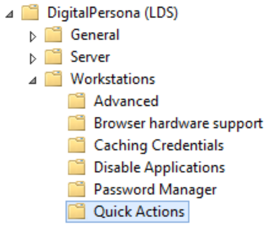
- DigitalPersona (LDS)
  - General
  - Server
  - Workstations
    - Advanced

Setting
- AD LDS instance name
- Do not launch the Getting Started wizard upon logon
- Compatibility with Microsoft fingerprint support
- Allow DigitalPersona client to use DigitalPersona Server
- Show Taskbar icon
- Allow VPN-less access

Quick Actions

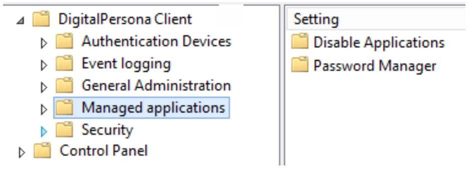
This GPO was previously located within the *DigitalPersona Client/General Administration* container, and has been relocated to the *DigitalPersona/Workstations* GPO.

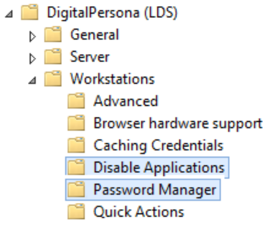




Managed Applications

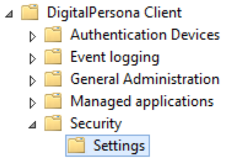
This GPO, previously located within the *DigitalPersona Client* container, has been deleted. The *Disable Applications* and *Password Manager* GPOs have been relocated to the *DigitalPersona/Workstations* container.

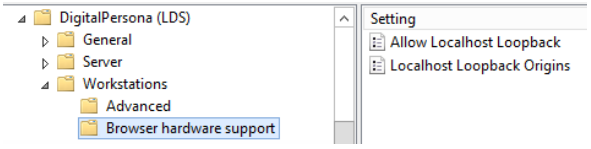




Localhost settings

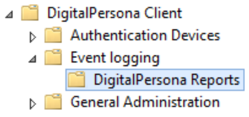
Two settings, *Allow Localhost Loopback* and *Localhost Loopback Origins,* previously in the *DigitalPersona Client/Security/Settings* GPO, have been relocated to the *DigitalPersona/Workstations/Advanced/Browser hardware support* GPO.

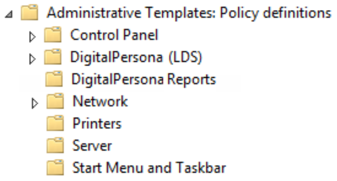




DigitalPersona Reports

This container, and the *Event Logging* container above is, previously in the *DigitalPersona Client* container, has been removed as it is no longer being used. The funcionality has been replaced by the process of importing the DigitalPersona Reports GPOs described in the *DigitalPersona Reports* chapter beginning on page *154.*





DigitalPersona LDS Server publishing and locator 33

DPCA LDS Server publishing

When an instance of DPCA LDS is installed, the service installer creates service connection point objects (SCP) in Active Directory. The SCP object is created as a child object of the computer object in AD where the DigitalPersona LDS Server is installed.

The following attributes are set for this SCP object:

***keywords* -** keywords is a multi-valued attribute which is replicated in the Global Catalog (GC) and indexed there so it can be searched later in GC by the service locator. The following keywords are set:

- DPCA LDS Service Class Name;
- LDS Instance Name;
- Site where DPCA LDS Server computer is located;

serviceClassName - DPCA LDS Service Class Name.

serviceDnsName - The DNS name of the computer where the DigitalPersona LDS Server is located.

When the DPCA LDS Service starts, it also adds the following attribute to the SCP object:

serviceBindingInformation: - The information required for the DPCA LDS Client to connect to the DPCA LDS Server.

When the DPCA LDS Service stops, it removes the ***serviceBindingInformation*** data so that clients can no longer connect to it.

When DigitalPersona LDS gets uninstalled, it deletes the SCP object that was created during installation.

Locator

The DPCA LDS Server Locator on the DPCA LDS Client performs the following steps to connect to DPCA LDS Server.

1. Connects to the Global Catalog (GC).
2. Runs a search query in the GC for CSP objects with ***keywords*** set to
   - DPCA LDS Service Class Name
   - LDS Instance DPCA LDS Client belongs to
   - site where DPCA LDS Client resides in;
3. If the query above returns 0 servers, the DPCA LDS Server Locator runs a search query in GC for CSP objects with ***keywords*** set to
   - DPCA LDS Service Class Name
   - LDS Instance DPCA LDS Client belongs to

4. The DPCA LDS Server Locator randomly chooses one of the servers returned by the query in steps #2 or #3 and then queries serviceBindingInformation.
5. The DPCA LDS Server Locator connects to the DPCA LDS Server using the binding information provided.

Block AD password policy inheritance 34

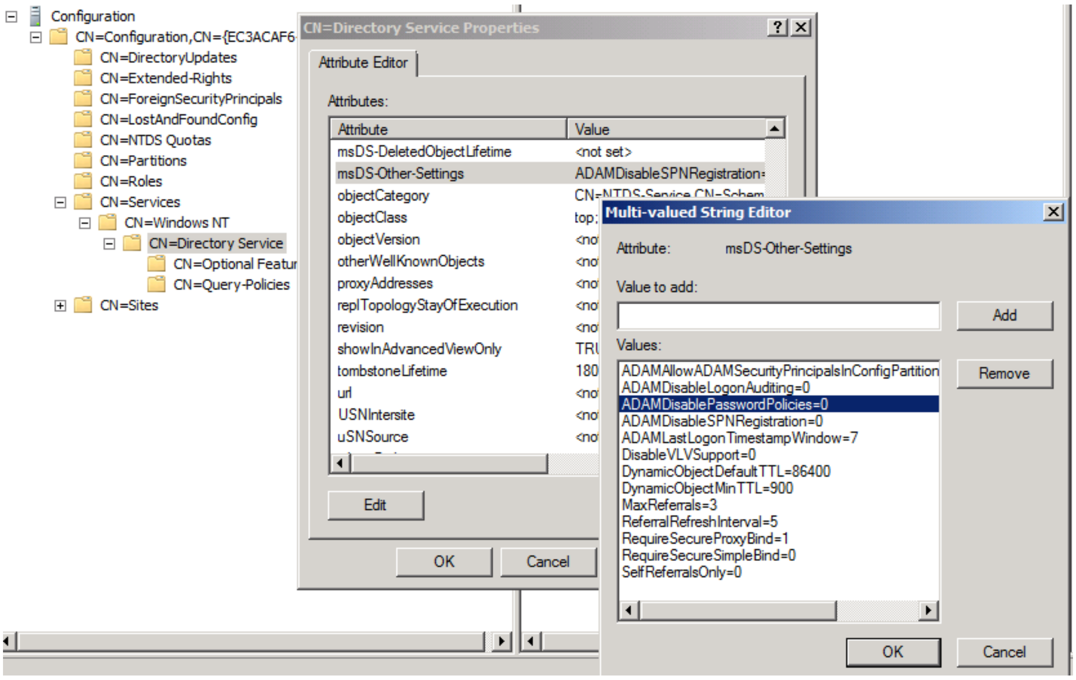
THIS CHAPTER DESCRIBES HOW TO BLOCK AD PASSWORD POLICY INHERITANCE.

By default, password policies for both AD Users and Non AD Users are governed by any existing AD password policies.

However, there may be business reasons where this is undesirable for certain scenarios. You can disable this inheritance (for Non AD Users only) in one of the following ways. Note however, that this will result in no password policy being enforced for Non AD Users, which means that even setting a blank password will be possible.

ADSI Edit

1. Using Microsoft's ADSI Edit tool (AdsiEdit.msc)
   a. Connect to the DigitalPersona LDS instance.
   b. Expand the Configuration container and drill down to the CN=Directory Service node.
   c. Display its Properties dialog box and locate the *msDS-Other-Settings* attribute.
   d. Click the Edit button.
   e. In the Multi-valued String Editor dialog box, locate the *ADAMDisablePasswordPolicies* entry.
   f. Set its value to 0.
2. In the String Editor, set the value of *ADAMDisablePasswordPolicies* to 1.



Attribute	Value
msDS-DeletedObjectLifetime	<not set>
msDS-Other-Settings	ADAMDisableSPNRegistration=
objectCategory	CN=NTDS-Service,CN=Schem
objectClass	top;
objectVersion	<no
otherWellKnownObjects	<no
proxyAddresses	<no
replTopologyStayOfExecution	<no
revision	<no
showInAdvancedViewOnly	TRU
tombstoneLifetime	180
url	<no
USNIntersite	<no
uSNSource	<no

Attribute: msDS-Other-Settings

```
ADAMAllowADAMSecurityPrincipalsInConfigPartition
ADAMDisableLogonAuditing=0
ADAMDisablePasswordPolicies=0
ADAMDisableSPNRegistration=0
ADAMLastLogonTimestampWindow=7
DisableVLVSupport=0
DynamicObjectDefaultTTL=86400
DynamicObjectMinTTL=900
MaxReferrals=3
ReferralRefreshInterval=5
RequireSecureProxyBind=1
RequireSecureSimpleBind=0
SelfReferralsOnly=0
```

DSMGMT

You can use the DSMGMT command line tool from an elevated Run command window or Powershell to

Syntax

dsmgmt “Configurable Settings” Connections “connect to server localhost:389” q “Set ADAMDisablePasswordPolicies to 1” “Commit changes” q q

Index