HID DigitalPersona

Client Guide

November 11, 2019

Table of Contents 1

Overview 1

THIS CHAPTER PROVIDES A HIGH-LEVEL OVERVIEW OF THE VARIOUS DIGITALPERSONA CLIENTS AND CLIENT COMPONENTS THAT ARE AVAILABLE AS PART OF THE MOST COMMON DIGITALPERSONA CONFIGURATIONS. THE CHAPTER INCLUDES THE FOLLOWING TOPICS.

Introduction

There are several specialized versions of the major DigitalPersona clients.

- DigitalPersona AD Workstation - Single end-user client that works with the DigitalPersona AD Server (which requires extension of the Active Directory schema).
- DigitalPersona Federal AD Workstation - Single end-user client supporting CAC and PIV smart cards. Works with the DigitalPersona AD Server (which requires extension of the Active Directory schema).
- DigitalPersona LDS Workstation - Single end-user client that works with the DigitalPersona LDS Server (using AD LDS which does not require extension of the Active Directory schema)
- DigitalPersona AD Kiosk - Designed for workstations where multiple users need fast, convenient and secure multi-factor identification and access to shared resources. Works with the DigitalPersona AD Server (which requires extension of the Active Directory schema).
- DigitalPersona LDS Kiosk - Designed for workstations where multiple users need fast, convenient and secure multi-factor identification and access to shared resources. Works with the DigitalPersona LDS Server (using AD LDS which does not require extension of the Active Directory schema).
- DigitalPersona Lite Client - When used in conjunction with the DigitalPersona Web Management Components, enables the use of fingerprint and PKI Smart Card credentials with the DigitalPersona Identity Server, Web Administration Console, Web Enrollment and the DigitalPersona Application Portal (on Windows platforms and supported browsers only).

Each of the above versions have their own unique Windows installer.

DigitalPersona Workstation and Kiosk are included in the DigitalPersona Logon for Windows and DigitalPersona Premium configurations. Specific versions of the clients are required depending on whether you are using DigitalPersona AD or DigitalPersona LDS configurations.

In the following pages, the term *DigitalPersona client* is used when describing features or behavior common to all of the above listed clients (except the Lite Client). References to *DigitalPersona Workstation* or *DigitalPersona Kiosk* or *DigitalPersona Lite Client* will be made in places that are applicable to only those clients. Further distinctions between the AD, AD Federal and LDS versions will be made when text applies to that specific client only.

Instructions for installing the Workstation and Kiosk clients are contained in Section One beginning on page 12. Details on the functions and features of those clients are found in Section Two, beginning on page 45.

Any references to procedures or UI elements, and all images included in this guide, are always to the current version of the product unless another version is specifically referenced. Procedures and images are for the product as installed on Windows 7 unless otherwise noted.

Separate features and components

DigitalPersona Attended Enrollment is an optional feature of both variations of the DigitalPersona Workstation, and is used for supervised enrollment of user credentials. It can be installed by selecting the feature during a Custom installation.

DigitalPersona clients

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

The DigitalPersona solutions support the following clients.

DigitalPersona Workstation

DigitalPersona AD Workstation and DigitalPersona LDS Workstation are the primary full-featured client application for end-users, providing an intuitive means for increasing both security and convenience through a variety of administrator and end-user configurable options including enrollment and use of multiple credentials, and the use of automated logons for enterprise resources, programs and websites.

The client enforces security and authentication policies on managed Windows computers while providing intuitive access to end-user features and functionality. It may be centrally managed by an DigitalPersona AD or LDS Server.

The term DigitalPersona Workstation is generally used to refer to both the DigitalPersona LDS Workstation and DigitalPersona AD Workstation, except where there are actual differences in their features or behavior. For more details, see the chapter *DigitalPersona Workstation* on page 46.

DigitalPersona Kiosk

DigitalPersona LDS Kiosk and DigitalPersona AD Kiosk are client applications managed by an DigitalPersona LDS or DigitalPersona AD Server, that are 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 the Kiosk with their own DigitalPersona credentials, gaining separately controlled access to resources, applications and data.

The term DigitalPersona Kiosk is generally used to refer to both the DigitalPersona LDS Kiosk and DigitalPersona AD Kiosk, except where there are actual differences in their features or behavior.

For a full description of its features, see the chapter *DigitalPersona Kiosk* on page 119.

DigitalPersona Attended Enrollment

Attended Enrollment is a client application feature specifically designed for the *supervised* creation of DigitalPersona users and enrollment of their credentials. It may be selected as a custom feature during the DigitalPersona LDS or

DigitalPersona AD Workstation installation. For a full description of its functionality, see the chapter *DigitalPersona Attended Enrollment* on page *86*.

About 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 when logging on to Windows, accessing network applications and resources, and logging in to VPNs, portals and 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 supports the use of various credentials for authentication, including Windows passwords, fingerprints, PKI Smart Cards, Contactless cards, PIN, Bluetooth devices and One-Time Passwords.

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

By default, initial enrollment of end-user credentials is provided through the DigitalPersona Attended Enrollment component. For further details, see the chapter on Attended Enrollment (page 86).

Administrators may choose to allow users to enroll and manage certain credentials by enabling self-enrollment through the *Self Enrollment Policy* GPO. (See the *Policies and Settings* chapter of your *DigitalPersona Administrator Guide*).

Licensing model

DigitalPersona software features and functionality as described in this Client Guide are included in the core version of the product, unless otherwise indicated.

The basic licensing mechanism is the User license, which permits the enrollment of user credentials by a specified number of DigitalPersona 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.

You should have received from HID Global or from a HID Global authorized reseller all of the license activation keys and/or files that are part of the package you purchased. Contact your HID Global representative, should you have any questions. Some modules or optional components may need to be activated individually.

For information on other licensed versions of the product which may be available, and licensing for specific features, contact your HID Global Account Manager or Reseller - or visit our landing page 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 HID DigitalPersona license activation, see your *HID DigitalPersona Administrator Guide*.

System Requirements

Product/Component	Minimum Requirements

DigitalPersona Workstation
DigitalPersona Kiosk
DigitalPersona Lite Client
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.
	  • 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 reademe.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.****

* 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 logons for 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 the DigitalPersona Kiosk client.

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

For a list of compatible fingerprint readers and scanners, see the readme.txt file included with this software.

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.
- 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: Installations

This section of the DigitalPersona Client Guide includes the following chapters:

Chapter Number and Title	Purpose	Page
2 - DigitalPersona Workstation installation	Requirements and procedure for installing DigitalPersona Workstation.	13
3 - DigitalPersona Kiosk installation	Requirements and procedure for installing DigitalPersona Kiosk.	24
4 - Attended Enrollment installation	Requirements and procedure for installing DigitalPersona Attended Enrollment.	33

DigitalPersona Workstation installation 2

THIS CHAPTER DESCRIBES INSTALLING THE DIGITALPERSONA ALTUS WORKSTATION CLIENT.

Main topics in this chapter	Page

Introduction

Although there are separate installation packages for the DigitalPersona AD Workstation and DigitalPersona LDS Workstation, the actual installations are functionally identical and the term DigitalPersona Workstation is generally used to refer to either one unless a distinction needs to be made due to a difference in functionality or features. Screenshots are taken from the installation of the DigitalPersona LDS Workstation product.

DigitalPersona Workstation will generally be installed remotely using the *Remote installation of DigitalPersona Workstation* procedure defined on page 19. However, in order to show the complete installation steps most clearly, local installation is described first.

DigitalPersona LDS and DigitalPersona AD Servers will be used for authentication and should be installed and configured before installing the DigitalPersona Workstation.

Note that the *DigitalPersona Attended Enrollment* feature is included in the DigitalPersona Workstation client package, but by default is not installed. To install it, you will need to select the feature as part of a custom install according to instructions given in this chapter for local, remote or command line installation. More complete details on installing DigitalPersona Attended Enrollment are available beginning on page 33.

System requirements

Before installing the DigitalPersona Workstation on a computer, make sure it meets the system requirements and prerequisites listed on page 10, and that you have Administrative Rights on the computer.

Deployment considerations

If your environment includes more than one installation of DigitalPersona LDS Server, and if those servers are not part of the same AD LDS configuration set, then your DigitalPersona LDS Workstations should be part of an OU where you can create a GPO defining the specific AD LDS instance name where the DigitalPersona LDS Server is hosted. See the setting *AD LDS instance name* in the *Policies and Settings* chapter of the *DigitalPersona LDS Administrator Guide*.

Upgrading from previous versions

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

Compatibility

This version of DigitalPersona Workstation is compatible with the following DigitalPersona products.

- DigitalPersona Access Management API (Previously Altus Auth SDK)
- DigitalPersona Web Components (Previously Altus Confirm SDK)
- DigitalPersona Server*

It cannot be installed on a computer with any other Altus or DigitalPersona products.

* Client On Server (COS) - Only the AD Workstation is designed to be installed on a domain controller. The LDS Workstation is not designed with this capability, and will not work on a domain controller due to the fact that all domain users will become local users if you run the software on the domain controller.

In the above scenarios, if DigitalPersona Server is installed on the machine, DigitalPersona Workstation *must* be installed after the DigitalPersona Server and it must only be used for authentication. *Do not attempt to enroll or manage user credentials using this configuration, as it may cause unpredictable results.*

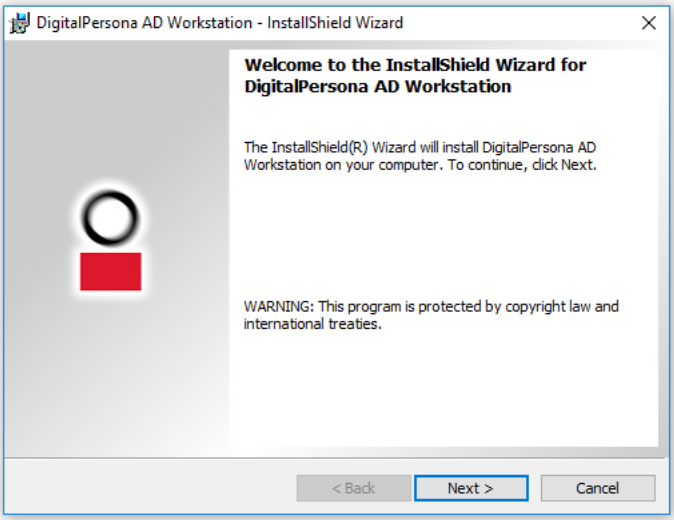
Installation

Local installation

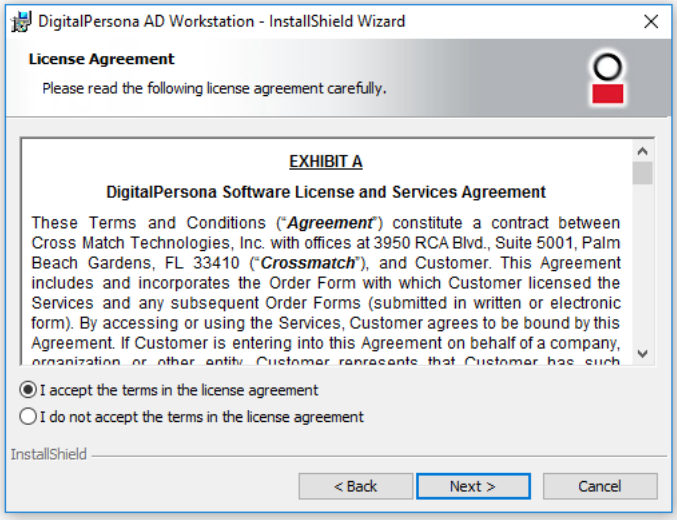
To install DigitalPersona Workstation on a local computer

1. Launch the installer from the DigitalPersona Workstation folder of the product package.
   - Run **Setup.exe** from the DigitalPersona (AD or LDS) Workstation folder of the product package.
   - Or, for silent mode, enter `setup.exe /s /v" /qn"` at the command line.

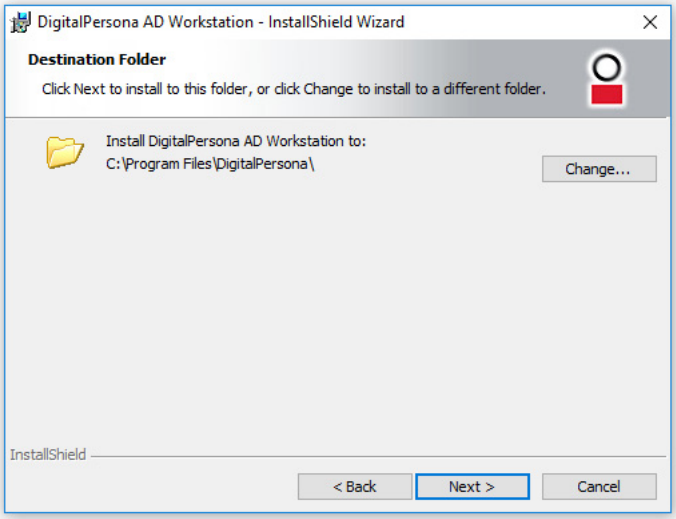
2. When the Welcome page displays, click *Next* to proceed with the installation.



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



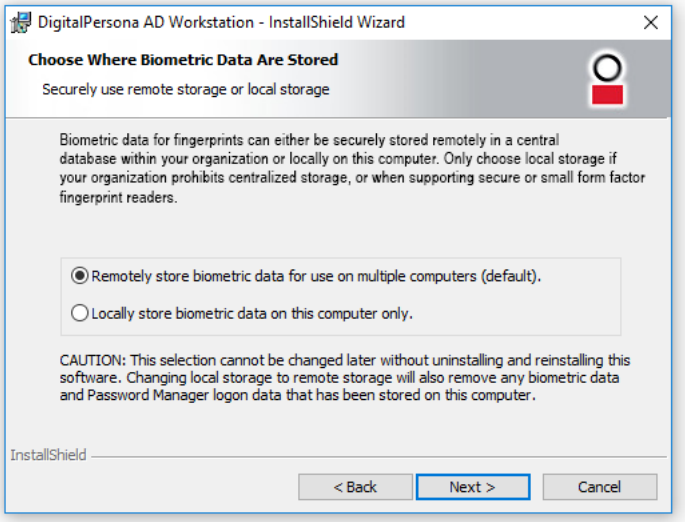
4. On the next page, you can specify the folder that DigitalPersona Workstation will be installed in. If you want to install it to the default location, click *Next*; otherwise, click *Change* to specify a new location and then click *Next* to continue.



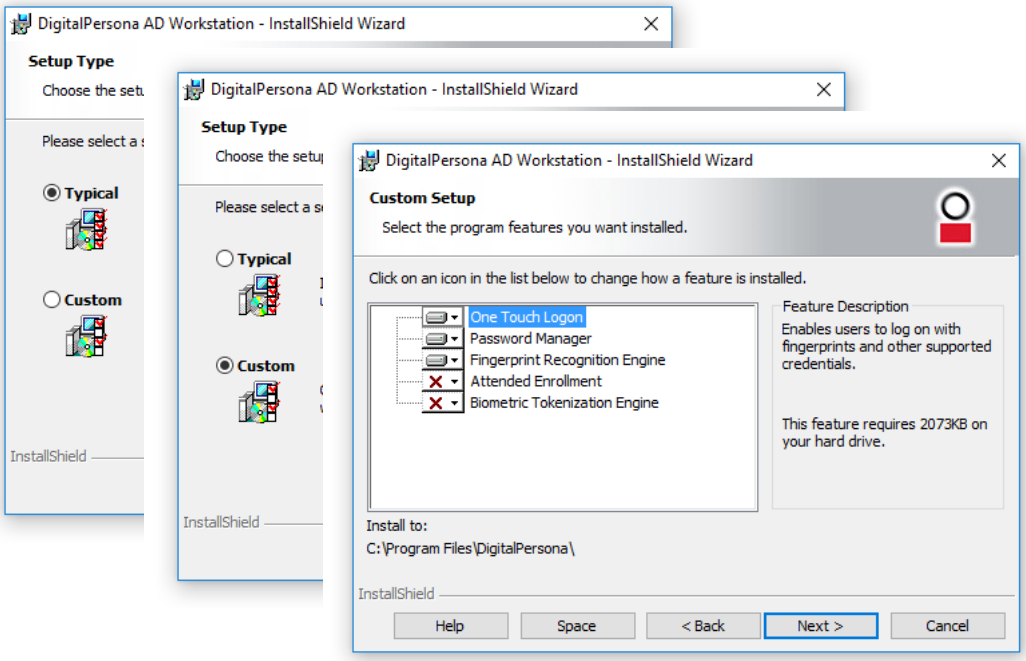
5. On the *Choose Where Biometric Data Are Stored* page, select whether to store biometric data locally or remotely. Storing data remotely allows biometric credentials to roam, i.e. be used on multiple computers.

   Biometric data for fingerprints can either be securely stored remotely in a central database within your organization or locally on this computer. Only choose local storage if your organization prohibits centralized storage of biometric data, or when supporting secure or small form factor fingerprint readers.

   CAUTION: This selection cannot be changed later without uninstalling and reinstalling this software. Changing local storage to remote storage will also remove any biometric data and Password Manager logon data that has been stored on this computer.



6. On the *Setup Type* page, choose from among the following options to indicate the type of installation you want to perform and what program features you want to install.



- **Typical -** Installs the most commonly used features.

  DigitalPersona Logon for Windows: In this product, Password Manager is not part of the Typical Setup Type, but can be selected by choosing the Custom Setup Type.

  DigitalPersona Premium: In this product, Password Manager is included as part of the Typical Setup-type, but can be deselected by choosing the Custom Setup Type.

- **Custom -** Allows selection of which features to install.

  One Touch Logon - Enables users to log on with fingerprints and other approved credentials.

  Password manager - Enables users to configure their fingerprint logons to websites and Windows programs.

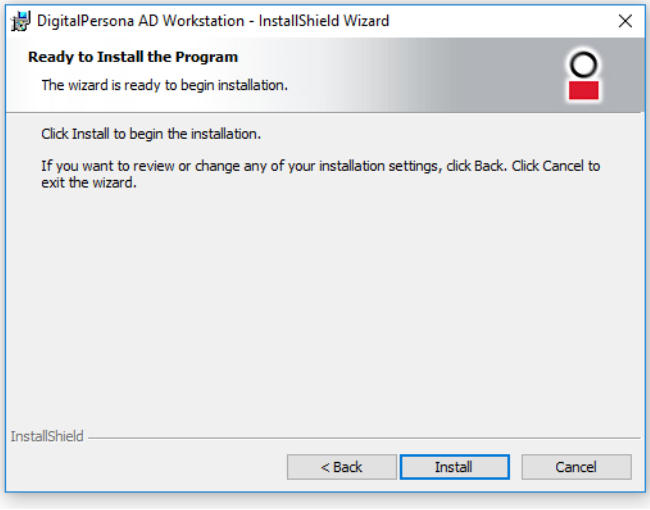
  Fingerprint Recognition Engine - Enables fingerprint matching functionality, i.e. fingerprint enrollment, verification and identification. Note that if you plan on installing the Biometric Tokenization Engine or the optional *DigitalPersona Large Scale ID Wrapper* (available for LDS product only), you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

  Attended Enrollment - Enables designated users to supervise credential enrollment. Note that Attended Enrollment is not installed by default, but must be specifically selected as part of a Custom installation.

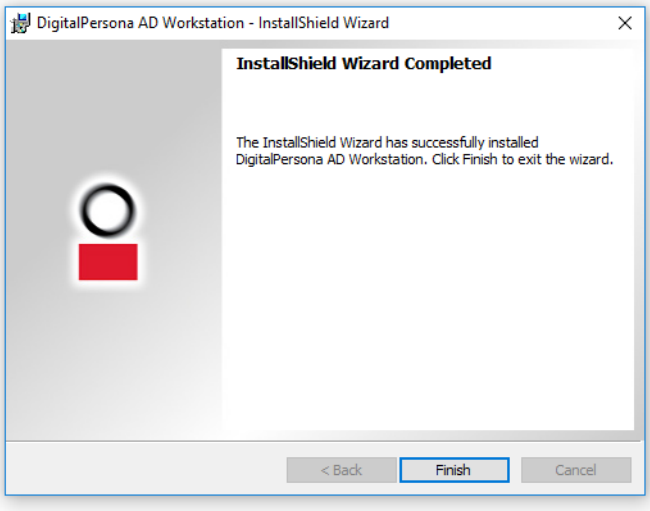
  Biometric Tokenization Engine - Creates a tokenized revocable presentation of a fingerprint. It can be used for enrollment and verification but not for identification. Note that this engine does not support deduplication. Also, switching from the Fingerprint Recognition Engine to the Biometric Tokenization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

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

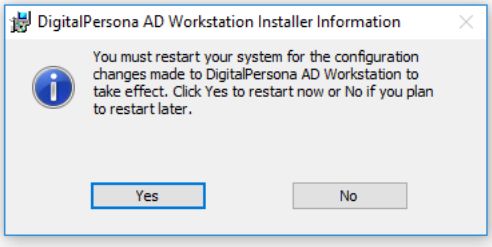
7. Click *Next* and then *Install*, to begin installation.



8. When installation is complete, a final page displays. Click *Finish*.



9. When prompted to do so, click *Yes* to reboot the computer, or *No* if you plan to restart the computer later.



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

For a description of the features and functions of DigitalPersona Altus Workstation, see the chapter beginning on page *46*.

Remote installation of DigitalPersona Workstation

For remote installation of *DigitalPersona Workstation patches*, see *Remote installation of DigitalPersona Workstation patches* on page *20*.

The installer for DigitalPersona Workstation uses Microsoft Windows Installer (MSI) technology, which allows administrators to remotely install or uninstall the software using Active Directory administration tools, or other software deployment tools. This installer is only compatible with program distribution (installation or uninstallation) to computers. It cannot be used for program distribution to users.

Note that, by default, remote installation does not install DigitalPersona Password Manager. To modify the software package to include Password Manager, see step *h* below.

To install DigitalPersona Workstation *remotely* through Active Directory use the following procedure. Some steps will vary depending on the operating system version.

1. For mixed 32- and 64-bit environments, copy the entire contents of the "DigitalPersona Workstation x86|x64" folder to a network share.
2. Create an OU (Organizational Unit) that will be used to distribute the software package.
3. Install any prerequisites (see page 10) on the target computers.
4. Assign the package
    a. Start the Group Policy Management snap-in. To do this, from the Windows Server Manager, *Tools* menu, select *Group Policy Management*.
    b. In the Group Policy Management tree, right-click the OU created in step 2 above and from the context menu, choose *Create a GPO in this domain, and Link it here.* Name the new GPO, then right-click it and choose *Edit*. This will launch the Group Policy Management Editor.
    c. In the Group Policy Management Editor, open *Computer Configuration*, *Policies*, *Software Settings*, *Software installation*.
    d. Right click *Software installation* and select *New*, *Package* from the context menu.
    e. In the *Open* dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\file server\share\file name.msi. *It is important that you do not use the Browse button to access the location. Make sure that you use the UNC path of the shared installer package.*
    f. Click *Open*.
    g. In the *Deploy Software* dialog, click *Assigned*, and then click *OK*. The package is created and listed in the right panel of the Group Policy Management Editor window.
    h. (*Optional)* To add Password Manager to the installation package
        - Right-click the package and select *Properties*.
        - Select the *Modifications* tab.
        - Click the *Add* button.
        - Browse to the DigitalPersona Workstation software source package.

- Select PM.mst.
- Click *OK*.

i. (32-bit installation packages only)

- Right-click the package and select *Properties*.
- On the *Deployment* tab, click *Advanced*.
- Deselect the checkbox *Make this 32-bit X86 application available on Win64 machines*. If this checkbox remains selected, the application will not install.

5. Installation will begin on each client during the first reboot after the computer obtains the deployment policy, i.e. during the next scheduled AD policy refresh or as a result of running GPUPDATE\FORCE on the local computer.

Remote installation of DigitalPersona Workstation patches

This topic addresses the remote installation of client patches through slipstreaming. For standard product installation, see the preceding topic.

The installer for DigitalPersona Workstation uses Microsoft Windows Installer (MSI) technology, which allows administrators to remotely install patches to software using Active Directory administration tools, or other software deployment tools.

For mixed 32- and 64-bit environments, follow these steps twice - patching the administrative installation files for both environments. Note that this installer only works for computer-based policy installation, not user-based.

To install an DigitalPersona Workstation patch remotely through Active Directory, use the following procedure. The following steps assume that an administrative installation package has been created as described in the previous topic. Some steps will vary depending on the operating system version.

1. Update the installation package.

   Open a command prompt session and type the following command to patch the previously created installation package.

   ```
   msiexec.exe /a [path\name of original MSI file]
   ```

   ```
   msiexec.exe /p [path\name of updated MSP file]\ /a [path\name of administrative installation file]
   ```

2. Redeploy the application

   a. Start the Group Policy Management snap-in. To do this, from the Windows Server Manager, *Tools* menu, select *Group Policy Management*.

   b. Right-click the GPO that governs the computers you want to update and select *Edit*. This will launch the Group Policy Management Editor.

   c. In the Group Policy Management Editor, navigate to `Computer Configuration/Policies/Software Settings/Software Installation`.

   d. Right-click the previously deployed DigitalPersona client software package and select *All Tasks\Redeploy application*. Confirm your intent to redeploy the application.

3. Installation will begin on each client during the first reboot after the computer obtains the deployment policy, i.e. during the next scheduled AD policy refresh or as a result of running GPUPDATE\FORCE on the local computer.

Command line Installation

DigitalPersona Workstation 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 can indicate where the software should be installed on the computer and what components should be included or removed.

Parameters	Description
`INSTALLDIR`	(Optional) Specifies the location where the DigitalPersona Workstation software should be installed. If a folder is not specified, the software will be installed in the following directory. `C:\Program Files\DigitalPersona`
`ADDLOCAL`	(Optional) Indicates which DigitalPersona Workstation features to install through one or more of the values listed in the next table.
`REMOVE`	(Optional) Indicates which DigitalPersona software features to uninstall by providing one of the values listed in the next table. In combination with ADDLOCAL=ALL, indicates which features that are *not* to be included in the installation.
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. See page 22 for a list of the available transform files.

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 *default (Typical)* DigitalPersona Workstation software components and features or removes all of the components and features that are currently installed. Note that Typical features do not include Password Manager or Attended Enrollment.

Values	Description
Logon	Installs or removes the Windows Logon feature, *One Touch Logon*.
AttendedEnrollment	Installs the *Attended Enrollment* feature. Cannot be used with *Remove* parameter.
PasswordMgr	Installs the *Password Manager* feature. Cannot be used with *Remove* parameter.
FingerprintEngine	Installs or removes the *DigitalPersona Fingerprint Engine*.
TokenizationEngine	Installs or removes the *DigitalPersona Tokenization Engine*.

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

- If ADDLOCAL or REMOVE are not specified, msiexec will install the default (Typical) DigitalPersona Workstation features. The Typical features do not include Password Manager or Attended Enrollment.
- Individual software features cannot be installed unless the `All` value was used with the `ADDLOCAL` parameter first.
- To install DigitalPersona Workstation software 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=Logon,FingerprintEngine
```

About Transform files

DigitalPersona uses Transform (.mst) files to create an installation package for DigitalPersona components in the supported languages listed below. These files are located in the Bin directory of your product package.

When creating a package for a GPO install, select the **Advanced** option and then add the transform file from the Modifications tab. Ensure that the transform file is included in a folder that is shareable by the Active Directory server computer and all target client computers.

Purpose/Language	Transform file
French	1036.mst
German	1031.mst
Italian	1040.mst
Brazilian Portuguese	1046.mst
Spanish	1034.mst
Chinese Simplified	2052.mst
Chinese Traditional	1028.mst
Japanese	1041.mst
Korean	1042.mst

Uninstalling DigitalPersona Workstation

You can remove DigitalPersona Workstation using the Add or Remove Programs Control Panel or through MSI. In the Control Panel, the Workstation software is listed as *DigitalPersona AD Workstation* or *DigitalPersona LDS Workstation*.

You must have local administrative privileges to modify or uninstall DigitalPersona Workstation.

DigitalPersona Kiosk installation 3

THIS CHAPTER DESCRIBES INSTALLING THE DIGITALPERSONA ALTUS KIOSK CLIENT.

Overview

Although there are separate installation packages for the DigitalPersona LDS and DigitalPersona AD versions of Kiosk, the installations are identical and the term DigitalPersona Kiosk is used to refer to both in this guide. Screenshots are taken from the installation of the DigitalPersona LDS Kiosk product.

DigitalPersona Kiosk will generally be installed remotely using the *Remote Installation of DigitalPersona Kiosk* procedure defined on page *29*. However, in order to show the complete installation steps most clearly, local installation is described first.

DigitalPersona LDS or DigitalPersona AD Servers will be used for user identification and authentication and should be installed and configured before installing the DigitalPersona Kiosk client.

System Requirements

Before installing DigitalPersona Altus Kiosk on a computer, make sure it meets the system requirements and prerequisites listed on page 10.

Upgrading from previous versions

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

https://www.hidglobal.com/documents.

Compatibility

This version of DigitalPersona Kiosk is compatible with the following DigitalPersona products.

- DigitalPersona Access Management API 2.1 or above (Previously Altus Auth SDK)
- DigitalPersona Web Components (Previously Altus Confirm SDK, now included in the above SDK)

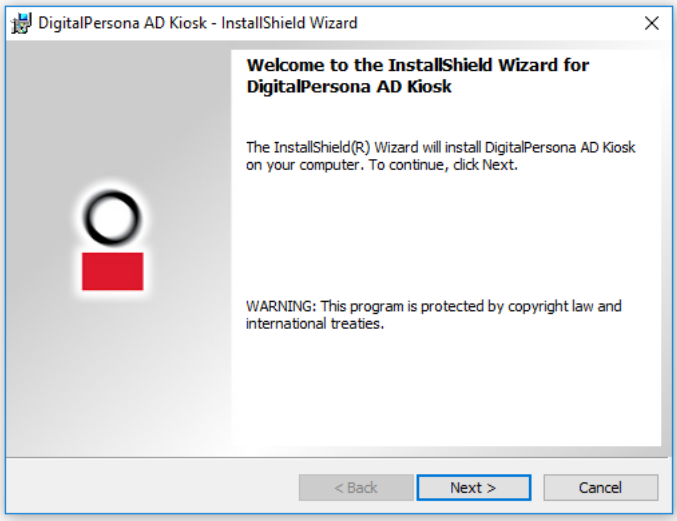
It cannot be installed on a computer with any other DigitalPersona products.

Installation

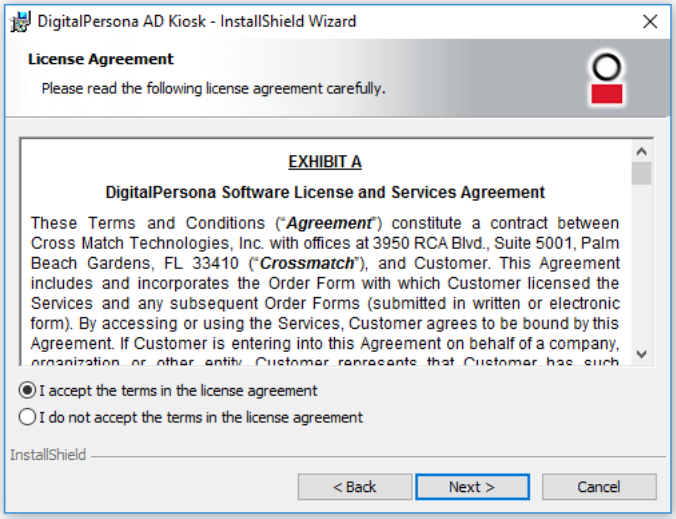
Local installation

To install DigitalPersona Altus Kiosk locally

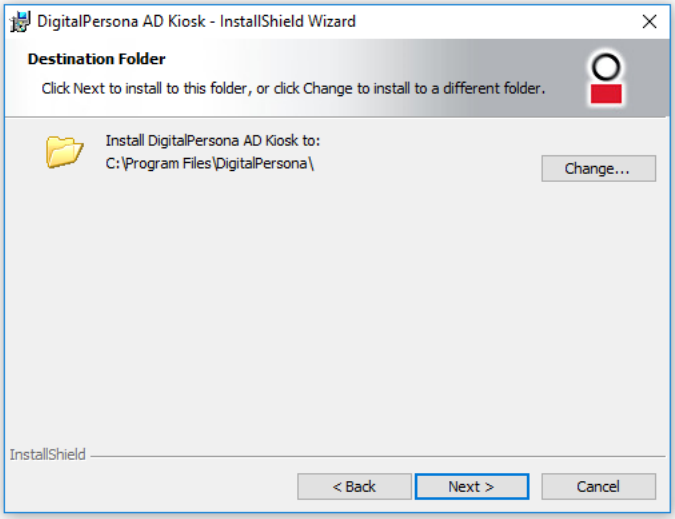
1. Launch the installer from the DigitalPersona LDS|AD Kiosk folder of the product package.
   - Run **Setup.exe** from the DigitalPersona LDS|AD Kiosk folder of the product package.
   - Or, for silent mode, enter `setup.exe /s /v" /qn"` at the command line.
2. When the Welcome page displays, click *Next* to proceed with the installation.



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



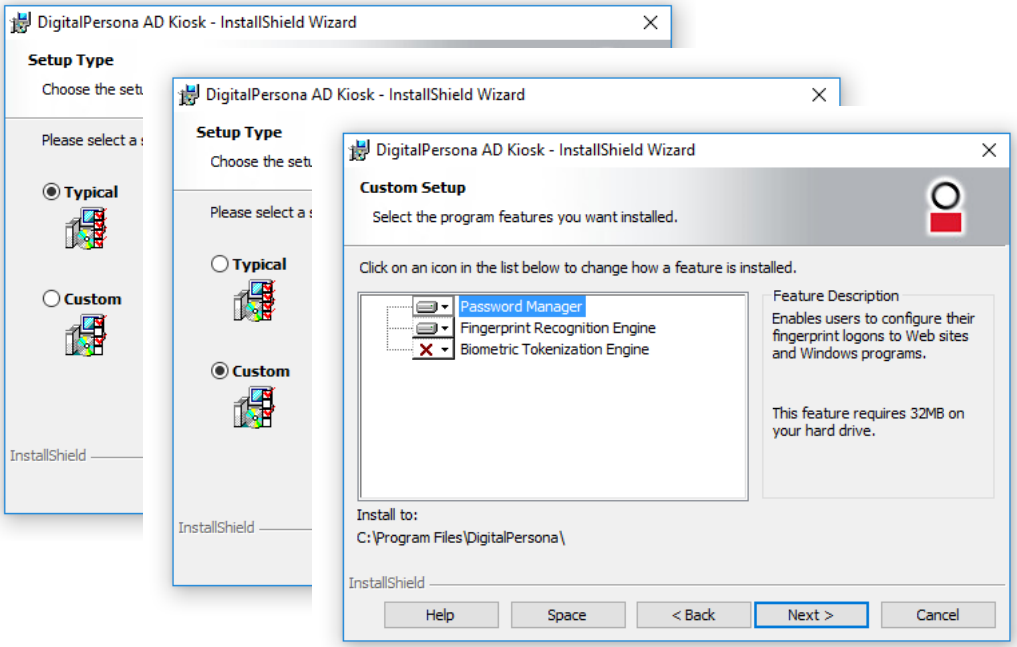
4. On the next page, you can specify the folder that DigitalPersona Kiosk will be installed in. If you want to install to the default location, click *Next*; otherwise, click *Change* to specify a new location and then click *Next* to continue.



5. Choose one of the following options to indicate the type of installation you want to perform.

   - **Typical -** Installs the most commonly used features.
     - *DigitalPersona Logon for Windows:* In this product, Password Manager is not part of the Typical Setup Type, but can be selected by choosing the Custom Setup Type.
     - *DigitalPersona Premium:* In this product, Password Manager is included as part of the Typical Setup-type, but can be deselected by choosing the Custom Setup Type.

- **Custom -** Allows selection of which features to install.



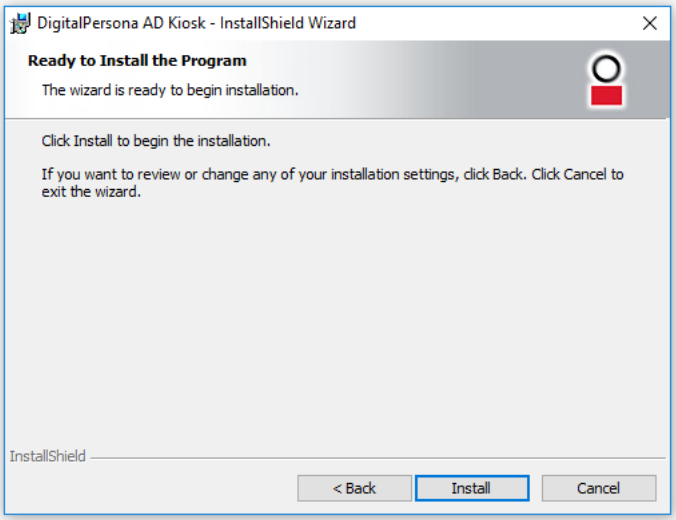
Password manager - Enables users to configure their fingerprint logons to websites and Windows programs.

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* (available for LDS product only), you should deselect the *Fingerprint Recognition Engine* feature. For further details on the wrapper, see the *DigitalPersona Large Scale ID Wrapper: Installation Guide*.

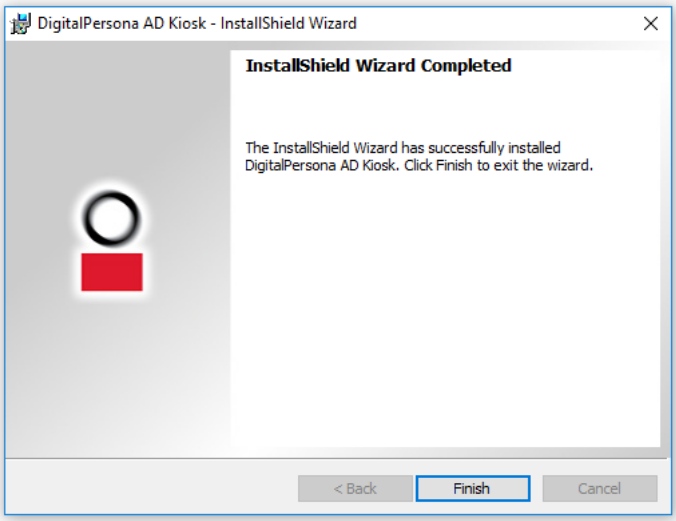
Biometric Tokenization Engine - Creates a tokenized revocable presentation of a fingerprint. It can be used for enrollment and verification but not for identification. Note that this engine does not support deduplication. Also, switching from the Fingerprint Recognition Engine to the Biometric Tokenization 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.

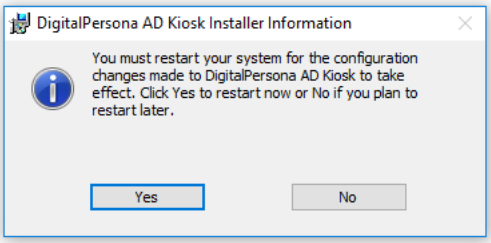
6. Click *Next* and then *Install*, to begin installation.



7. Click *Finish* to close the InstallShield Wizard.



8. When prompted to do so, reboot the computer. Click *Yes* to restart now, or *No* if you plan to restart later.



After the computer restarts, and at every subsequent restart, Pro Kiosk automatically uses the default DNS Server to locate all DigitalPersona Servers for the domain and its site. If more than one DigitalPersona Server is found, Pro

Kiosk will choose the DigitalPersona Server for authentication that offers the most efficient connectivity. For instructions on using Pro Kiosk, see page *119*.

Remote Installation of DigitalPersona Kiosk

For remote installation of *DigitalPersona Kiosk patches*, see *Remote installation of DigitalPersona Kiosk patches* on page *30*.

The installer for Pro Kiosk uses Microsoft Windows Installer (MSI) technology, which allows administrators to remotely install or uninstall the software using Active Directory administration tools, or other software deployment tools.

Note that this installer only works for computer-based policy installation, not user-based installations.

To install DigitalPersona Kiosk *remotely* through Active Directory, use the following procedure. Some steps will vary depending on the operating system version.

For mixed 32- and 64-bit environments, follow these steps twice to create an administrative installation file for each environment.

1. For mixed 32- and 64-bit environments, copy the entire contents of the "DigitalPersona Workstation x86|x64" folder to a network share.
2. (Optional) To install only to a specific OU, create a Group Policy Object (GPO) that will be used to distribute the software package.
3. Assign the package
    a. Start the Group Policy Management snap-in. To do this, from the Windows Server Manager, **Tools** menu, select *Group Policy Management*.
    b. In the Group Policy Management tree, under the appropriate domain, right-click *Default Domain Policy* and choose *Edit* from the context menu. This will launch the Group Policy Management Editor.
    c. In the Group Policy Management Editor, open *Computer Configuration*, *Policies*, *Software Settings*, *Software installation*.
    d. Right click *Software installation* and select *New*, *Package* from the context menu.
    e. In the *Open* dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\file server\share\file name.msi. *It is important that you do not use the Browse button to access the location. Make sure that you use the UNC path of the shared installer package.*
    f. Click *Open*.
    g. Click *Assigned*, and then click *OK*. The package is listed in the right-pane of the Group Policy window.
    h. For 32-bit installation packages only - Right-click the newly created package and select Properties. Then, on the Deployment tab, click Advanced. Deselect the checkbox *Make this 32-bit X86 application available on Win64 machines*. If this checkbox remains selected, the application will not install.
4. Installation will begin on each client during the first reboot after the computer obtains the deployment policy, i.e. during the next scheduled AD policy refresh or as a result of running GPUPDATE\FORCE on the local computer.

Remote installation of DigitalPersona Kiosk patches

This topic addresses the remote installation of client patches through slipstreaming. For standard product installation, see the preceding topic.

The installer for DigitalPersona Kiosk uses Microsoft Windows Installer (MSI) technology, which allows administrators to remotely install patches to software using Active Directory administration tools, or other software deployment tools.

For mixed 32- and 64-bit environments, follow these steps twice - patching the administrative installation files for both environments. Note that this installer only works for computer-based policy installation, not user-based.

To install an DigitalPersona Kiosk patch remotely through Active Directory, use the following procedure. The following steps assume that an administrative install has been created as described in the previous topic. Some steps will vary depending on the operating system version.

1. Update the installation package.

   Open a command prompt session and type the following command to patch the previously created installation package.

   ```
   msiexec.exe /a [path\name of original MSI file]
   ```

   ```
   msiexec.exe /p [path\name of updated MSP file]\ /a [path\name of administrative installation file]
   ```

2. Redeploy the application.

   a. Start the Group Policy Management snap-in. To do this, from the Windows Server Manager, *Tools* menu, select *Group Policy Management*.

   b. Right-click the GPO that governs the computers you want to update and select *Edit*. This will launch the Group Policy Management Editor.

   c. In the Group Policy Management Editor, navigate to `Computer Configuration/Policies/Software Settings/Software Installation`.

   d. Right-click the previously deployed DigitalPersona client software package and select *All Tasks\Redeploy application*. Confirm your intent to redeploy the application.

3. Installation will begin on each client during the first reboot after the computer obtains the deployment policy, i.e. during the next scheduled AD policy refresh or as a result of running GPUPDATE\FORCE on the local computer.

Command line installation

DigitalPersona Kiosk 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

There are one required and one optional 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 path name 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 can indicate where the software should be installed on the computer and what components should be included or removed:.

Parameters	Description
INSTALLDIR	(Optional) Specifies the location where the software should be installed. If a folder is not specified, the software will be installed in the following directory. `C:\Program Files\DigitalPersona`
ADDLOCAL	(Optional) Indicates which DigitalPersona Kiosk features to install through one or more of the values listed in the next table.
REMOVE	(Optional) Indicates which DigitalPersona Kiosk features to uninstall by providing one of the values listed in the next table. In combination with ADDLOCAL=ALL, indicates which features that are *not* to be included in the installation.
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. See page 32 for a list of the available transform files.

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 *default (Typical)* DigitalPersona Kiosk components and features or removes all of the component and features that are currently installed. Note that Typical features do not include Password Manager or Attended Enrollment.
PasswordMgr	Installs the *Password Manager* feature. Cannot be used with *Remove* parameter.
FingerprintEngine	Installs or removes the *DigitalPersona Fingerprint Engine*.
TokenizationEngine	Installs or removes the *DigitalPersona Tokenization Engine*.

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

- If ADDLOCAL or REMOVE are not specified, msiexec will install the default (Typical) DigitalPersona Kiosk features. Note that Typical features do not include Password Manager.
- Individual software features cannot be installed unless the `All` value was used with the `ADDLOCAL` parameter first.
- To install DigitalPersona Kiosk for the first time while omitting one or more of its features, use `ADDLOCAL=ALL`, followed by the `REMOVE` parameter and the name of each feature that you do not want to install, separated by commas.

Example: `msiexec /i setup.msi ADDLOCAL=ALL REMOVE=FingerprintEngine`

About Transform files

DigitalPersona uses Transform (.mst) files to create an installation package for DigitalPersona components in the supported languages listed below, and to add DigitalPersona Password Manager to an installation package. These files are located in the Bin directory of your product package.

When creating a package for a GPO install, select the *Advanced* option and then add the transform file from the Modifications tab. Ensure that the transform file is included in a folder that is shareable by the Active Directory server computer and all target client computers.

Purpose/Language	Transform file
French	1036.mst
German	1031.mst
Italian	1040.mst
Brazilian Portuguese	1046.mst
Spanish	1034.mst
Chinese Simplified	2052.mst
Chinese Traditional	1028.mst
Japanese	1041.mst

Uninstalling DigitalPersona Kiosk

You can remove the DigitalPersona Kiosk software using the Add or Remove Programs Control Panel or through MSI. In the Control Panel, the Kiosk software is listed as *DigitalPersona LDS Kiosk* or *DigitalPersona AD Kiosk*.

You must have local administrative privileges to modify or uninstall DigitalPersona Kiosk.

Attended Enrollment installation 4

THIS CHAPTER DESCRIBES INSTALLING THE DIGITALPERSONA ATTENDED ENROLLMENT CLIENT.

Introduction

This chapter provides instructions for installing DigitalPersona Attended Enrollment, a component of the DigitalPersona Workstation, used to enroll user credentials under supervision of a specified user or group. Note that in both DigitalPersona AD and DigitalPersona LDS, the domain administrator is automatically assigned this permission. In DigitalPersona LDS, members of the Local Administrators Group on a machine where DigitalPersona LDS Server is installed also can enroll users through Attended Enrollment.

To change or add permissions for enrolling other users

DigitalPersona AD - To change (remove, allow or deny) these permissions, see the chapter *Attended Enrollment* in the *DigitalPersona AD Administrator Guide*.

DigitalPersona LDS - To change the tasks assigned to a user (such as the ability to enroll other users), see the chapter *Authorization manager* in the *DigitalPersona LDS Administrator Guide*.

System requirements

Before installing DigitalPersona Attended Enrollment on a computer, make sure it meets the system requirements listed on page 10, and that you have Administrative Rights on the computer.

For a list of compatible fingerprint readers and scanners, see the readme.txt file included with this software.

Compatibility

This version of DigitalPersona Attended Enrollment is compatible with the following DigitalPersona products.

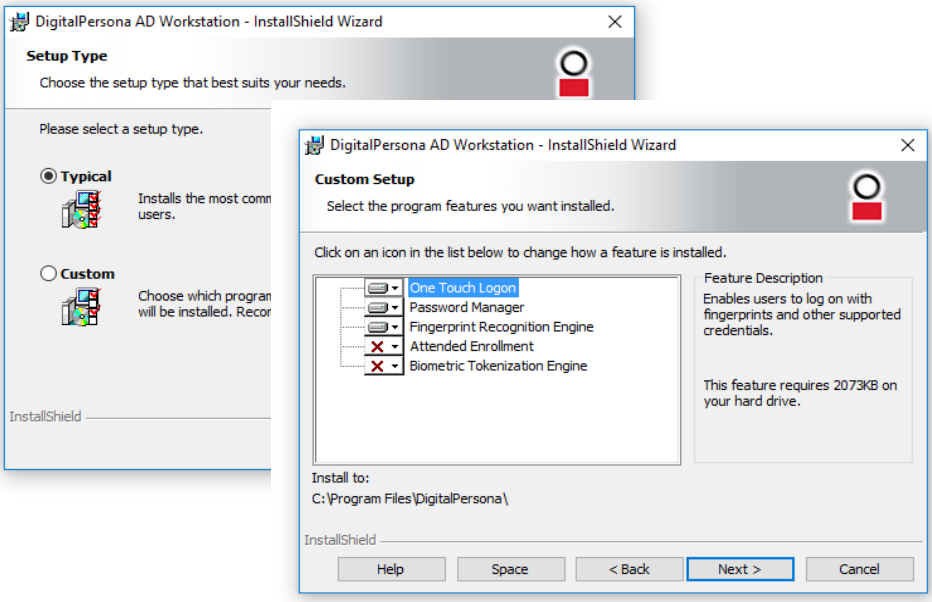
- DigitalPersona LDS or DigitalPersona AD Workstation (Previously Altus LDS/AD Workstation) 1.1 or above
- DigitalPersona Access Management API 2.1 or above (Previously Altus Auth SDK)
- DigitalPersona Web Components (Previously Altus Confirm SDK, now included in the above SDK)

It cannot be installed on a computer with any other DigitalPersona or Altus products.

Local installation

To install DigitalPersona Attended Enrollment on a local computer

1. Launch the installer from the DigitalPersona [AD|LDS] Workstation folder of the product package, by running *Setup.exe*.
   - Or, for silent mode, enter `setup.exe /s /v" /qn"` at the command line.
2. On the *Setup Type* page, select *Custom*.



   (DigitalPersona LDS only) If you plan on installing the optional DigitalPersona Large Scale ID wrapper, you should deselect the Fingerprint Recognition Engine component. For further details, see the *DigitalPersona Altus Large Scale ID wrapper* section of the *Optional installations* chapter in the *DigitalPersona LDS Administrator Guide*.

   Make sure that the same recognition engine that was installed on the client is also installed on the server.
3. Click the *X* next to Attended Enrollment and select *This feature will be installed on local hard drive*.
4. Click *Next* and then *Install*, to begin installation.

For a description of the features and functions of DigitalPersona Attended Enrollment, see the chapter beginning on page 86.

Administrator setup instructions

Because DigitalPersona Attended Enrollment is an optional feature of the DigitalPersona client software, DigitalPersona AD Workstation, Its installation and features are addressed in this Client Guide. However, there is a also a small amount of setup that must be performed in Active Directory by an administrator. Instructions for this setup are contained in the chapter *"DigitalPersona Attended Enrollment"* beginning on page *86*.

Uninstalling DigitalPersona Attended Enrollment

Since DigitalPersona Attended Enrollment is actually a subcomponent of DigitalPersona Workstation, it cannot be uninstalled separately from the Workstation product.

If you must remove DigitalPersona Attended Enrollment from a computer, you will need to uninstall DigitalPersona Workstation first, and then reinstall it without DigitalPersona Attended Enrollment.

Lite Client installation 5

THIS CHAPTER DESCRIBES INSTALLING THE DIGITALPERSONA LITE CLIENT.

Introduction

For a description of DigitalPersona Lite Client features, see page *124*.

System requirements

Before installing the DigitalPersona Lite Client on a computer, make sure it meets the system requirements and prerequisites listed on page 10, and that you have Administrative Rights on the computer.

Deployment considerations

If your environment includes more than one installation of DigitalPersona LDS Server, and if those servers are not part of the same AD LDS configuration set, then your DigitalPersona LDS Lite Clients should be part of an OU where you can create a GPO defining the specific AD LDS instance name where the DigitalPersona LDS Server is hosted. See the setting *AD LDS instance name* in the *Policies and Settings* chapter of the *DigitalPersona LDS Administrator Guide*.

Upgrading from previous versions

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

Compatibility

This version of DigitalPersona Workstation is compatible with the following DigitalPersona products.

- DigitalPersona Access Management API (Previously Altus Auth SDK)
- DigitalPersona Web Components (Previously Altus Confirm SDK)
- DigitalPersona Server*

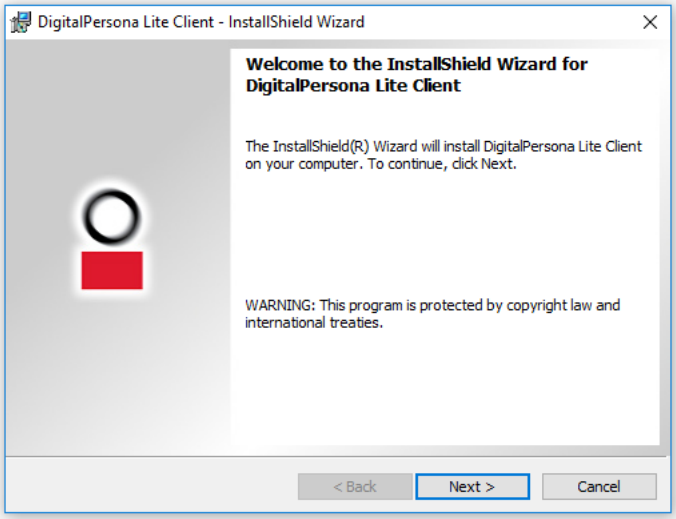
It cannot be installed on a computer with any other Altus or DigitalPersona products.

Installation

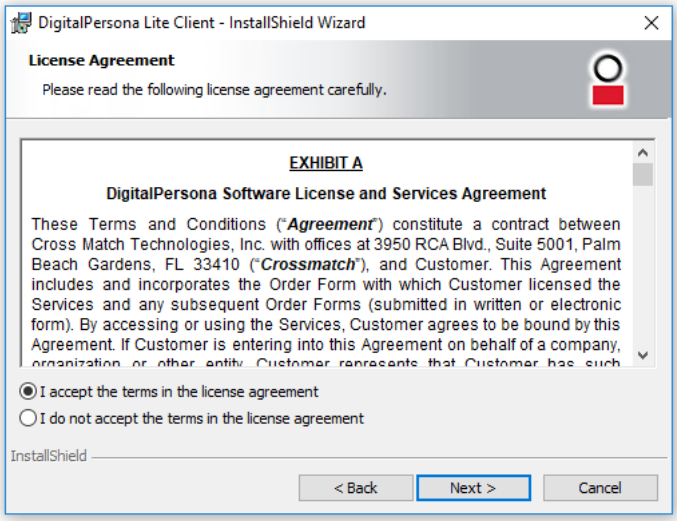
Local installation

To install DigitalPersona Workstation on a local computer

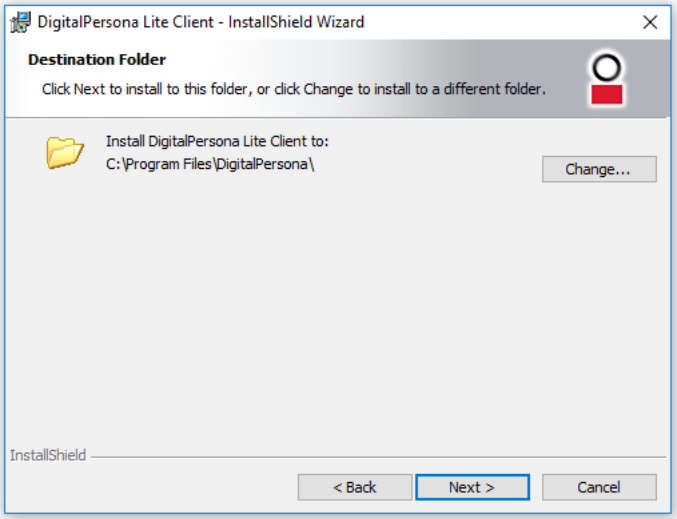
1. Launch the installer from the DigitalPersona Workstation folder of the product package.
   - Run **Setup.exe** from the DigitalPersona Lite Client folder of the product package.
   - Or, for silent mode, enter `setup.exe /s /v" /qn"` at the command line.
2. When the Welcome page displays, click *Next* to proceed with the installation.



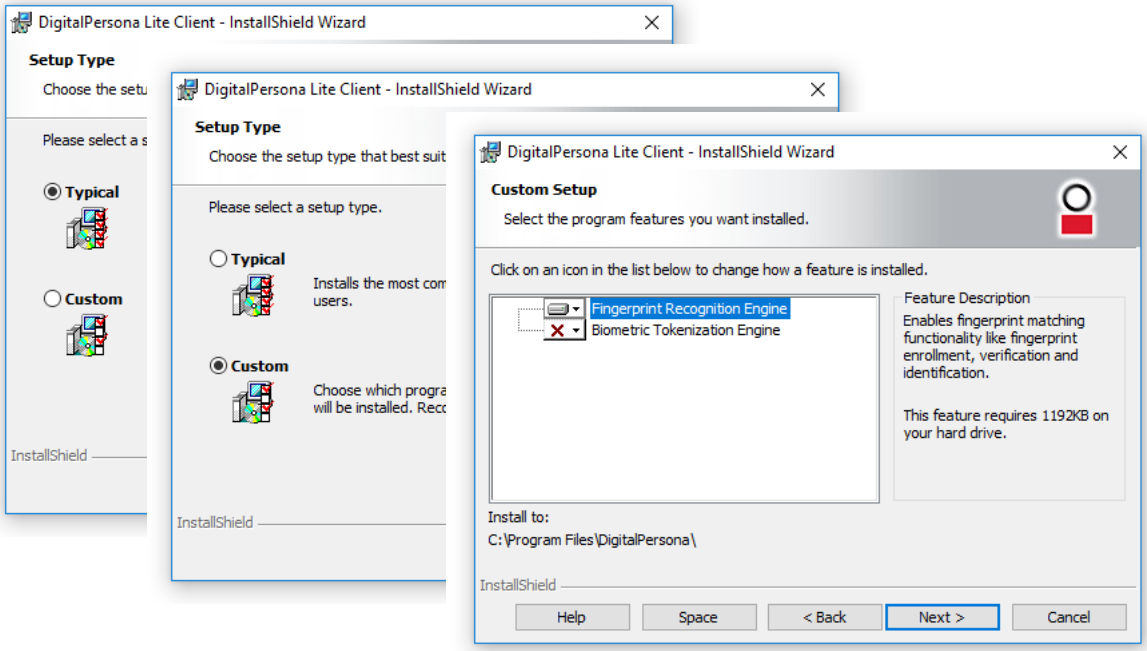
3. Read the License Agreement page. If you agree, select the *I accept the terms in the license agreement* button and click *Next*.



4. On the next page, you can specify the folder that DigitalPersona Workstation will be installed in. If you want to install it to the default location, click *Next*; otherwise, click *Change* to specify a new location and then click *Next* to continue.



5. On the *Setup Type* page, choose from among the following options to indicate the type of installation you want to perform and what program features you want to install.



- **Typical -** Installs the most commonly used features.
- **Custom -** Allows selection of which features to install.

  Fingerprint Recognition Engine

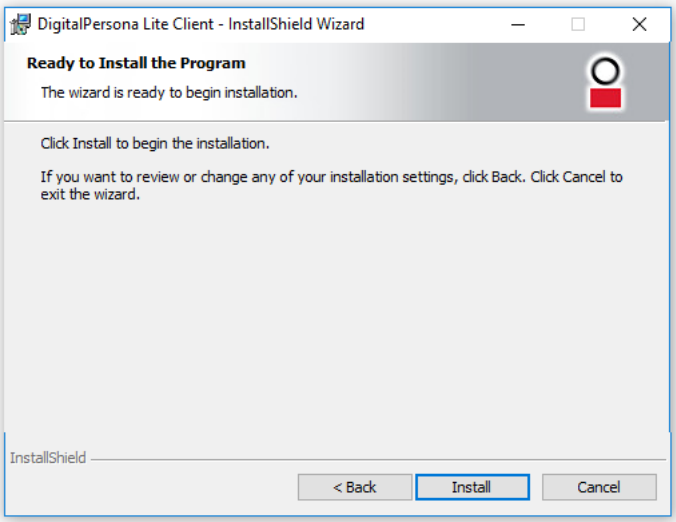
  Enables fingerprint matching functionality, i.e. fingerprint enrollment, verification and identification. Note that if you plan on installing the Biometric Tokenization Engine or the optional *DigitalPersona Large Scale ID Wrapper* (available for LDS product only), you should deselect the *Fingerprint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

  Biometric Tokenization Engine

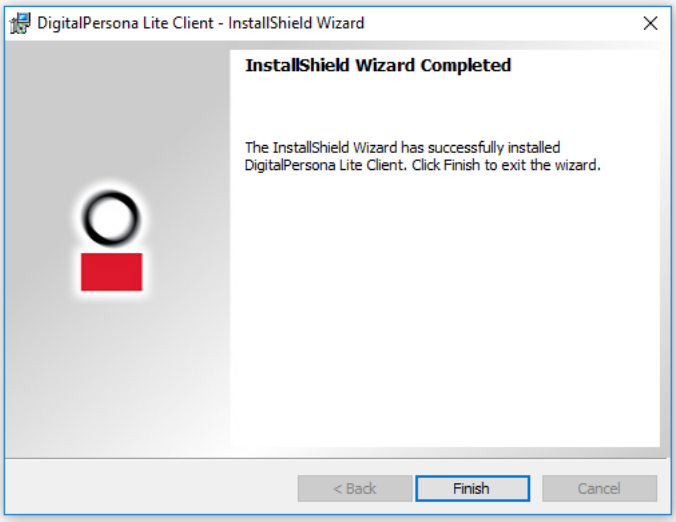
  Creates a tokenized revocable presentation of a fingerprint. It can be used for enrollment and verification but not for identification. Note that this engine does not support deduplication. Also, switching from the Fingerprint Recognition Engine to the Biometric Tokenization Engine will require re-enrollment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

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

6. Click *Next* and then *Install*, to begin installation.



7. When installation is complete, a final page displays. Click *Finish*.



8. When prompted to do so, click *Yes* to reboot the computer, or *No* if you plan to restart the computer later.

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

For a description of the features and functions of the DigitalPersona Lite Client, see the chapter beginning on page *124*.

Remote installation of the DigitalPersona Lite Client

For remote installation of *DigitalPersona Lite Client patches*, see *Remote installation of DigitalPersona Lite Client patches* on page *41*.

The installer for the DigitalPersona Lite Client uses Microsoft Windows Installer (MSI) technology, which allows administrators to remotely install or uninstall the software using Active Directory administration tools, or other software deployment tools. This installer is only compatible with program distribution (installation or uninstallation) to computers. It cannot be used for program distribution to users.

To install the DigitalPersona Lite Client *remotely* through Active Directory use the following procedure. Some steps will vary depending on the operating system version.

1. For mixed 32- and 64-bit environments, copy the entire contents of the "DigitalPersona Lite Client" folder to a network share.
2. (Optional) To install only to a specific OU, create a Group Policy Object (GPO) that will be used to distribute the software package.
3. Install any prerequisites (see page 10) on the target computers.
4. Assign the package
    a. Start the Group Policy Management snap-in. To do this, from the Windows Server Manager, *Tools* menu, select *Group Policy Management*.
    b. In the Group Policy Management tree, under the appropriate domain, right-click **Default Domain Policy** and choose *Edit* from the context menu. This will launch the Group Policy Management Editor.
    c. In the Group Policy Management Editor, open *Computer Configuration*, *Policies*, *Software Settings*, *Software installation*.
    d. Right click *Software installation* and select *New*, *Package* from the context menu.
    e. In the *Open* dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\file server\share\file name.msi. *It is important that you do not use the Browse button to access the location. Make sure that you use the UNC path of the shared installer package.*
    f. Click *Open*.
    g. In the *Deploy Software* dialog, click *Assigned*, and then click *OK*. The package is created and listed in the right panel of the Group Policy Management Editor window.
    h. (32-bit installation packages only)
        - Right-click the package and select *Properties*.
        - On the *Deployment* tab, click *Advanced*.
        - Deselect the checkbox *Make this 32-bit X86 application available on Win64 machines*. If this checkbox remains selected, the application will not install.
5. Installation will begin on each client during the first reboot after the computer obtains the deployment policy, i.e. during the next scheduled AD policy refresh or as a result of running GPUPDATE\FORCE on the local computer.

Remote installation of DigitalPersona Lite Client patches

This topic addresses the remote installation of client patches through slipstreaming. For standard product installation, see the preceding topic.

The installer for the DigitalPersona Lite Client uses Microsoft Windows Installer (MSI) technology, which allows administrators to remotely install patches to software using Active Directory administration tools, or other software deployment tools.

For mixed 32- and 64-bit environments, follow these steps twice - patching the administrative installation files for both environments. Note that this installer only works for computer-based policy installation, not user-based.

To install a DigitalPersona Lite Client patch remotely through Active Directory, use the following procedure. The following steps assume that an administrative installation package has been created as described in the previous topic. Some steps will vary depending on the operating system version.

1. Update the installation package.

   Open a command prompt session and type the following command to patch the previously created installation package.

   ```
   msiexec.exe /a [path\name of original MSI file]
   ```

   ```
   msiexec.exe /p [path\name of updated MSP file]\ /a [path\name of administrative installation file]
   ```

2. Redeploy the application

   a. Start the Group Policy Management snap-in. To do this, from the Windows Server Manager, *Tools* menu, select *Group Policy Management*.

   b. Right-click the GPO that governs the computers you want to update and select *Edit*. This will launch the Group Policy Management Editor.

   c. In the Group Policy Management Editor, navigate to `Computer Configuration/Policies/Software Settings/Software Installation`.

   d. Right-click the previously deployed DigitalPersona client software package and select *All Tasks\Redeploy application*. Confirm your intent to redeploy the application.

3. Installation will begin on each client during the first reboot after the computer obtains the deployment policy, i.e. during the next scheduled AD policy refresh or as a result of running GPUPDATE\FORCE on the local computer.

Command line Installation

The DigitalPersona Lite Client 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

Parameters	Description
`INSTALLDIR`	(Optional) Specifies the location where the DigitalPersona Lite Client should be installed. If a folder is not specified, the software will be installed in the following directory. `C:\Program Files\DigitalPersona`
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. See page 43 for a list of the available transform files.

About Transform files

DigitalPersona uses Transform (.mst) files to create an installation package for DigitalPersona components in the supported languages listed below. These files are located in the Bin directory of your product package.

When creating a package for a GPO install, select the **Advanced** option and then add the transform file from the Modifications tab. Ensure that the transform file is included in a folder that is shareable by the Active Directory server computer and all target client computers.

Purpose/Language	Transform file
French	1036.mst
German	1031.mst
Italian	1040.mst
Brazilian Portuguese	1046.mst
Spanish	1034.mst
Chinese Simplified	2052.mst
Chinese Traditional	1028.mst
Japanese	1041.mst
Korean	1042.mst

Uninstalling the DigitalPersona Lite Client

You can remove the DigitalPersona Lite Client using the Add or Remove Programs Control Panel or through MSI. In the Control Panel, the Workstation software is listed as *DigitalPersona Lite Client*. Requires administrative privileges.

Section Two: Client Features

Section Two of the DigitalPersona Client Guide includes the following chapters:

DigitalPersona Workstation 6

THIS CHAPTER DESCRIBES THE FEATURES OF THE DIGITALPERSONA ALTUS WORKSTATION CLIENT.

Introduction

DigitalPersona Workstation is a robust and fully featured workstation client which allows you to significantly and easily increase the security of computers in your enterprise. Its specific features, options and behavior can be configured though Active Directory GPOs and other tools as explained in the *DigitalPersona LDS* and *DigitalPersona AD Administrator Guides*.

Attended Enrollment, an optional component of DigitalPersona Workstation, allows administrators to assign a specific user or group to supervise the credential enrollment process. (See page *86*.)

DigitalPersona Kiosk, a separate DigitalPersona client with many of the same features, provides users with fast, convenient and secure multi-factor identification and authentication in environments where users share a common Windows account yet need separately controlled access to resources, applications and data. (See page *119*.)

Most of the content in this section is written from the end-user perspective, and is also available through the various DigitalPersona help files.

Note that the availability of some product features described in this chapter may be limited, or behave differently, as determined by GPO policies and other settings described in the *Administration Tools* and *Policies and Settings* chapters in the *DigitalPersona AD* and *DigitalPersona LDS Administrator Guides* and the *DigitalPersona Web Administration Console* chapter in the *DigitalPersona LDS Administrator Guide*.

Multi-factor authentication for Windows Servers and Domain Controllers

It addition to the end-user features described in the following sections, DigitalPersona (AD or LDS) Workstation may be used to provide multi-factor authentication on supported versions of Windows Server (sometimes referred to as Client On Server or COS).

However, only the AD Workstation is designed to be installed on a domain controller. The LDS Workstation is not designed with this capability and will not work on a domain controller due to the fact that all domain users will become local users if you run the software on the domain controller.

In the above scenarios, if DigitalPersona Server is installed on the machine, DigitalPersona Workstation *must* be installed after the DigitalPersona Server and it must only be used for authentication. *Do not attempt to enroll or manage user credentials using this configuration, as it may cause unpredictable results.*

Getting Started

By default, DigitalPersona credentials are enrolled through the DigitalPersona Attended Enrollment component. However, a DigitalPersona administrator may optionally choose to allow Windows users to self-enroll, i.e. enroll their credentials through the DigitalPersona AD Workstation.

The DigitalPersona Console

The DigitalPersona Console is the central location for primary access to DigitalPersona Workstation features and settings.

The image shown above includes DigitalPersona Password Manager and Quick Actions, which are part of the DigitalPersona Console in DigitalPersona Altus Premium version 2.0.3 and DigitalPersona Premium 2.1 or above.

Password Manager (which includes Quick Actions) is an optional feature that may be installed by selecting *Custom* as the *Setup Type* during installation.

The DigitalPersona Console may include the following features.

Credential Manager - Enroll and manage DigitalPersona credentials and their settings.

Password Manager - (Optional) Create and manage Password Manager logons and accounts.

Quick Actions- Configure the DigitalPersona Hot Key sequence, and assign tasks to various credential and key+credential combinations. (Included with DigitalPersona Password Manager.)

Help - Displays online help for the DigitalPersona Console.

Information - Displays information about DigitalPersona Workstation, including the software version, copyright information and the DigitalPersona Server connection status.

User - Displays the Windows account name of the currently logged in user.

Windows authentication

Once your DigitalPersona Workstation client has been installed, logon (authentication) to Windows is controlled by the Logon Authentication Policy and Enhanced Logon Policy, which are set by GPOs in Active Directory. The path to these settings is: *Computer Configuration\Policies\Software Settings\DigitalPersona Client/Security/Authentication.*

For a complete description of these policies, see the *Policies and Settings* chapter, *Logon Authentication Policy*, in the *DigitalPersona Administrator Guides*.

Credentials that may be used to authenticate for Windows logon will be limited to those specified in the policy and supported by required hardware or software present on the workstation. Some credentials, such as PKI Smart Cards, need to be previously formatted and initialized using the manufacturer's middleware. Contactless Cards must be enrolled by the end-user, on their computer, or through the DigitalPersona Attended Enrollment components (see page 86).

The actual process of using your DigitalPersona credentials will vary slightly depending on the type of credential, but will generally follow Microsoft usage with the following exceptions.

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 Windows (and other resources as defined by the administrator).

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.

Card authentication

In order to use a PKI Smart card or Contactless ID card for logging on to Windows, you must click your user tile on the Windows Logon screen before presenting the card. Then you can insert your PKI Smart card for authentication, or use a Contactless ID card in conjunction with another credential as specified by the Logon Authentication Policy in force.

A Contactless Writable card may be presented directly from the Logon screen for immediate logon to Windows.

Locking/Unlocking

To lock a DigitalPersona-managed computer

- Windows 8/10 - From the *Start* screen, click your user name and select *Lock* from the menu.
- Windows 7 - Click *Start*. On the *Shut down* menu, click *Lock*.
- Any Windows OS - Press the Windows Logo key+L.
- When configured by the DigitalPersona administrator, you can lock the computer by removing the card which was used to log on to Windows from the card reader.

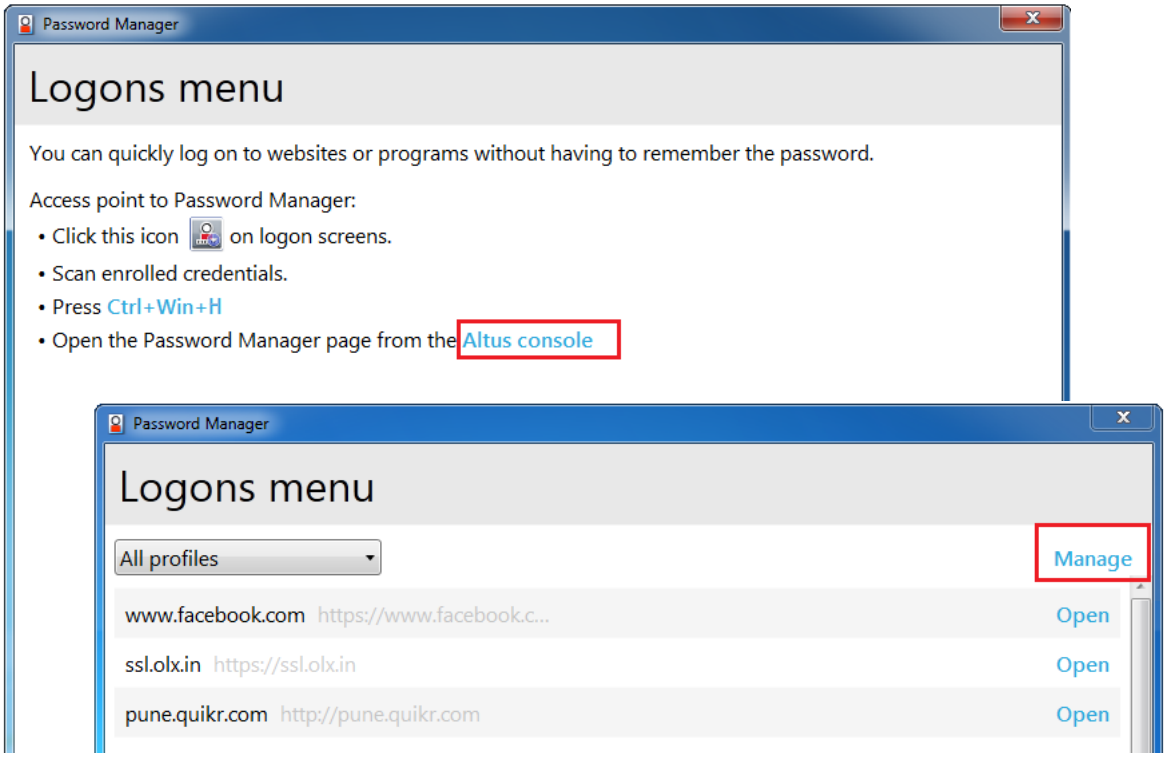
To unlock a DigitalPersona-managed computer

- Use any authorized credential or required combination of credentials to unlock the computer and log on to the workstation.

Opening the DigitalPersona Console

You can open the DigitalPersona Console in any of the following ways:

- Windows 8/10] - From the *Apps* screen, under *DigitalPersona*, select *DigitalPersona Console.*
- Windows 7 - Click *Start*, click *All Programs*, click *DigitalPersona*, and then click *DigitalPersona Console.*
- Double-click the *DigitalPersona Workstation icon* in the notification area, at the far right of the taskbar.
- Right-click the *DigitalPersona icon*, and click *Open DigitalPersona Console.*
- Press the hot key combination *Ctrl+Win Logo Key+H* to open the Logons menu and then click *DigitalPersona Console* (when no logons have been created yet) or *Manage* (after logons have been created.)



Credential Manager 7

THIS CHAPTER DESCRIBES THE CREDENTIAL MANAGER COMPONENT, WHICH IS PART OF THE MOST DIGITALPERSONA CLIENTS.

Introduction

The Credential Manager component is part of the DigitalPersona Workstation, Kiosk and Attended Enrollment clients. It may be used to enroll and manage DigitalPersona credentials and to configure associated settings (depending on configuration by the DigitalPersona Administrator). The Credential Manager component of the Attended Enrollment client is covered separately beginning on page *50*.

Available credentials can vary depending on the security devices built into or connected to the user's computer. The exact credentials required to access a given resource may vary depending on several risk and behavioral factors including user typing pattern, device, browser, location, etc. Each user should enroll as many credentials as possible from those shown on the Credential Manager screen.

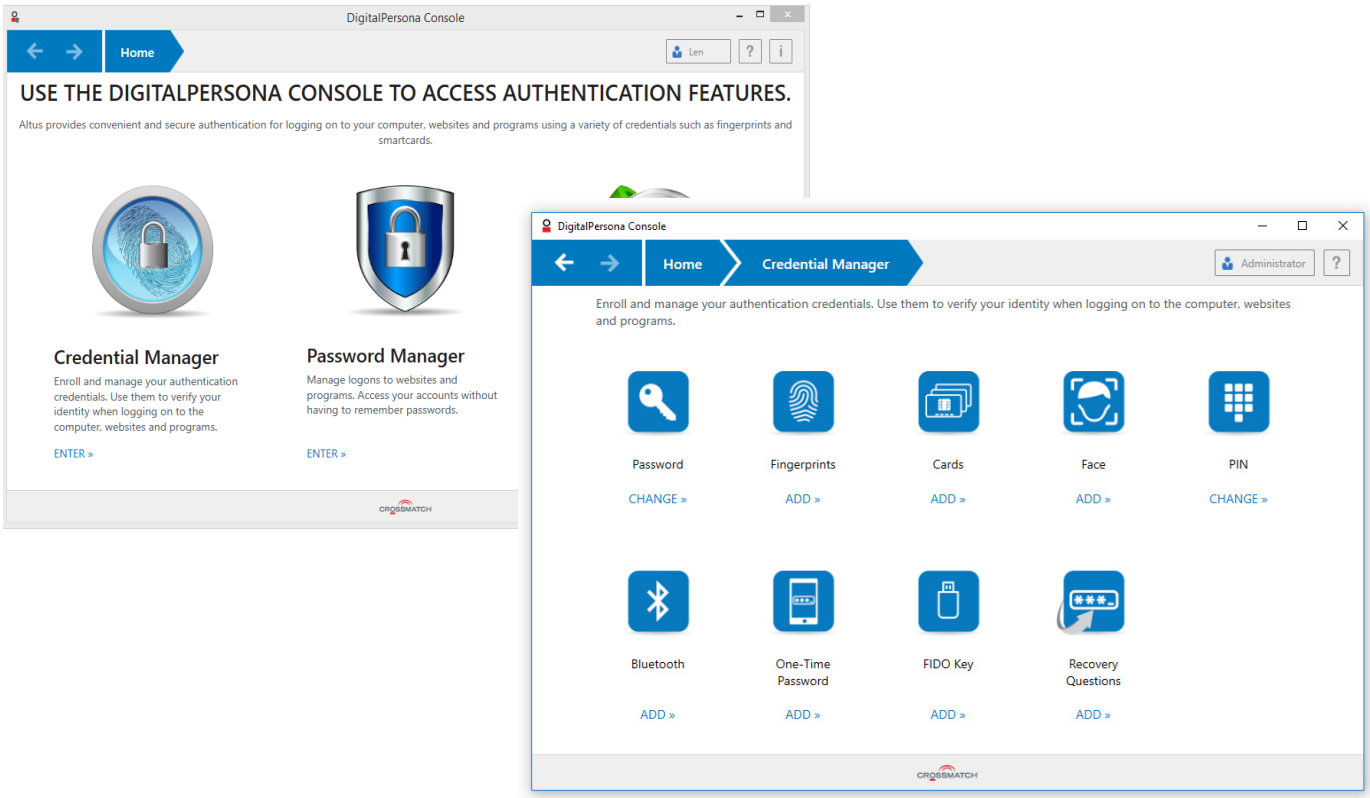
Authorized and supported credentials may be managed from the Credential Manager page unless prohibited by the DigitalPersona Administrator.

- To manage a credential - Click the ADD or CHANGE button on the credential tile and then follow the on-screen instructions.
- To delete a credential - Refer to specific instructions in the help topic for that credential.

Note that managing your credentials (adding, changing or deleting) requires a connection to the DigitalPersona Server. When not connected to a DigitalPersona Server, you cannot manage your credentials, but you can use any cached credentials for authentication. Credentials are cached on a local machine upon first use on that machine. Credentials enrolled through Web Enrollment or the Attended Enrollment component are not cached on a local machine until after their first use.

Your credentials are also used at various times to verify your identity when making changes in the DigitalPersona Console.

Launch the Credential Manager by tapping or clicking the Credential Manager tile from the DigitalPersona Console home page.



By default, this feature is disabled because the Attended Enrollment component is most often used to enroll user credentials. Also, use of the Credential Manager requires a connection to the DigitalPersona Server. If no Server is available, a warning will display, and no tiles will be shown on the Credential Manager page.

If you want to allow end-users to enroll and manage their own DigitalPersona credentials, see the *Policies and Settings* chapter in the *DigitalPersona Administrator Guides*. However, the best practice is to not enable self-enrollment if Attended Enrollment will be used in the environment.

Managing user credentials

The credentials that will be available to a user for verifying their identity may be configured through GPO policies and settings (for managed workstations) by a DigitalPersona Administrator or (if not managed) by the local administrator of the computer.

Some credentials require the presence of built-in or attached hardware. The following steps will help you to enroll or set up your credentials for use with the product's features and applications. Unless otherwise specified through a GPO, any hardware or software credential available will be listed in Credential Manager, and may be managed by the user when self-enrollment has been enabled by the DigitalPersona administrator.

This chapter includes instructions for enrolling and managing supported DigitalPersona credentials.

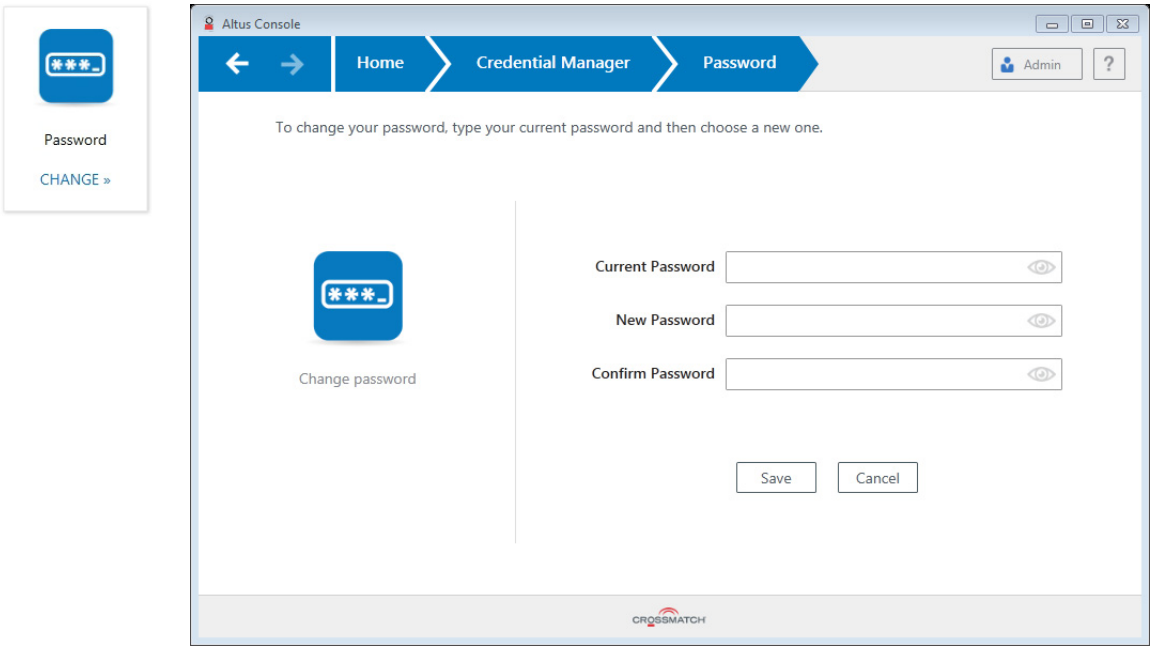
Password credential

DigitalPersona Workstation makes changing your DigitalPersona password simple.

CAUTION: Windows users should be aware that this will change your Windows password.

To change your password, follow these steps.

1. In the DigitalPersona Console, select *Credential Manager*, and then choose *CHANGE* on the *Password* tile.
2. The *Password* page displays.
3. Enter your current password in the *Current password* text box.

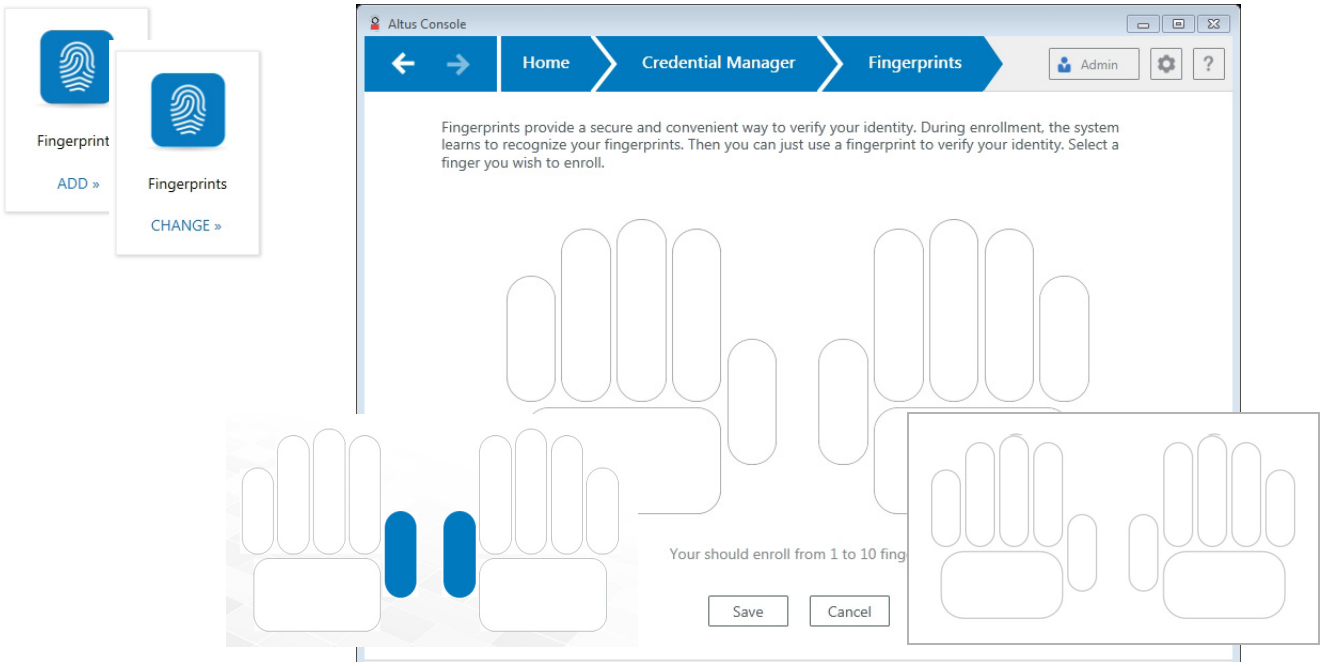


4. Type a new password in the *New password* text box, and then type it again in the *Confirm new password* text box.
5. Click *Save* to immediately change your current password to the new one that you entered.

Fingerprint credential

If there is a fingerprint reader or ten print scanner built into or connected to your computer, you can enroll and manage your fingerprints. Select the Fingerprints tile to display the Fingerprints page, where you can enroll your fingerprints credential.

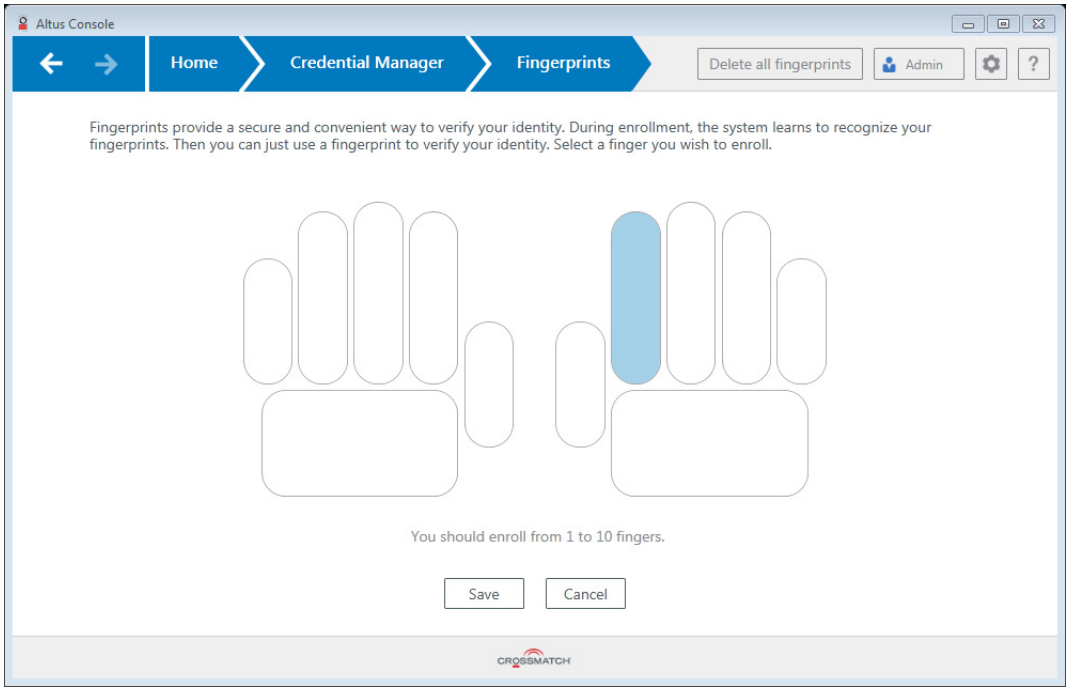
The process of enrolling your fingerprints is slightly different depending on whether you are using a single print fingerprint reader, or a ten-print fingerprint scanner such as one of the HID Guardian products. See the following two sections for descriptions of the steps for each of the hardware devices.



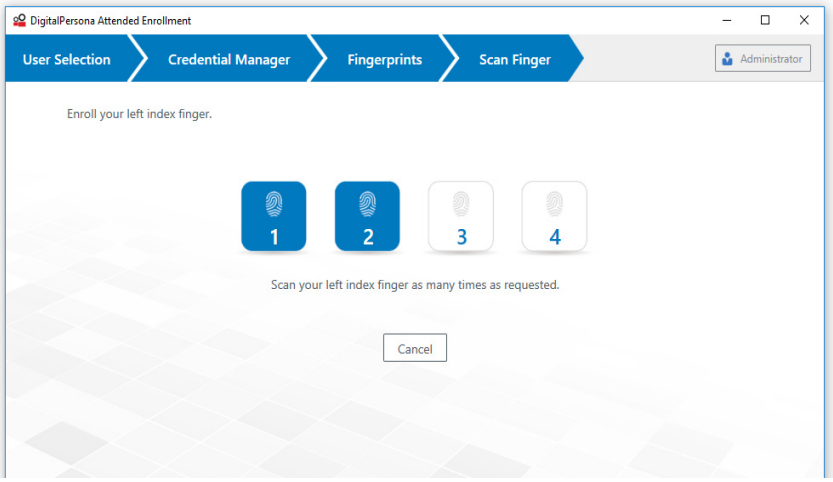
Enrolling fingerprints with a fingerprint reader

To enroll your fingerprints or manage your fingerprints credential

1. In the DigitalPersona Console, select *Credential Manager*, and then choose *ADD* or *CHANGE* on the *Fingerprints* tile to display the Fingerprints page.
   - The *CHANGE* button displays on the Fingerprints tile after the first fingerprint has been enrolled and saved.
   - The *Delete all fingerprints* button displays on the Fingerprints page after at least one fingerprint has been enrolled. Use this button to delete all fingerprints for the logged on user.
2. The Fingerprints page displays an outline of two hands. Fingers that have been previously enrolled are highlighted.
   - To enroll a fingerprint, click the image of any finger not previously enrolled.
   - To delete a single previously enrolled fingerprint, click a highlighted finger on the outline. Then confirm the deletion and click *Save* to return to the Credential Manager page.
   - To delete all fingerprints for this user, click *Delete all fingerprints*. Then confirm the deletion.



3. After selecting a finger to enroll, you are prompted to scan the finger until its fingerprint is successfully enrolled. Index or middle fingers are preferable.



4. When enrollment is complete, the Fingerprints page redisplays with the enrolled finger highlighted.

5. Click *Save*. 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.*

Note that fingerprint enrollment is not complete until you click *Save*. If you leave the computer inactive for a while without clicking *Save*, or close the program, any changes will not be saved.

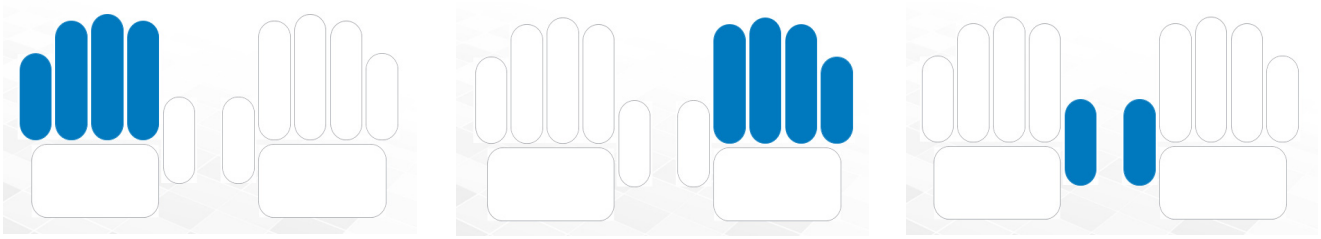
WARNING: Users should never enroll the same finger under multiple Windows accounts. Doing so will cause the finger to be rejected as a valid credential in any Windows account where it has been enrolled.

Enrolling fingerprints with a ten print scanner

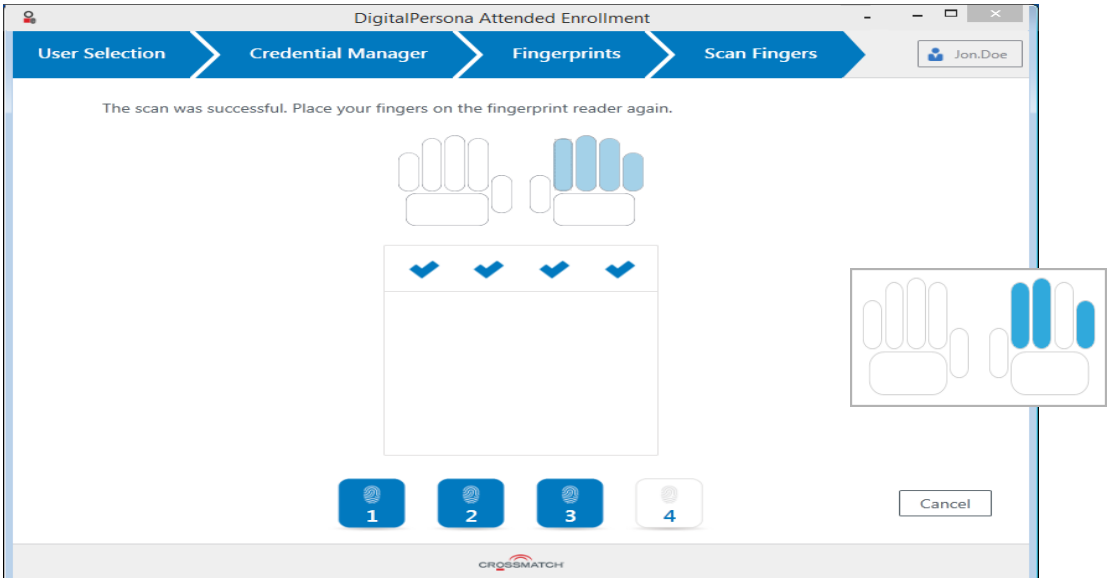
For a list of supported ten print scanners, see the readme.txt file included with this software package. Additional files may need to be installed before use. See the *Optional installations* chapter in the *DigitalPersona Administrator Guides* for further details.

The ten print scanner captures fingerprints in three segments, often described as 4-4-2, that is: four fingers of the left hand, four fingers of the right hand, and the two thumbs together.

1. Click the Fingerprints tile to display the Fingerprints pages.
2. Select which segment to enroll. In the displayed image, choose the left hand, right hand or thumbs.

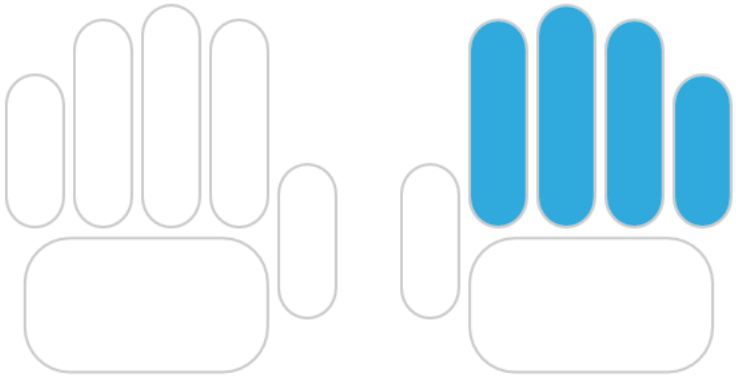


3. Scan the selected fingers or thumbs as many times as requested to enroll them. If the user is missing any fingers, click the associated finger in the image near the top of the page.



4. Each successful enrollment will result in one of the scan numbers turning blue.

5. When enrollment of the segment is complete, the screen shows the fingerprint segment in blue.



6. Select another segment until the fingerprints of both hands and thumbs have been captured.
7. Click *Save*. 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.*

Note that fingerprint enrollment is not complete until you click *Save*. If you leave the computer inactive for a while without clicking *Save*, or close the program, any changes will not be saved.

To delete a partial fingerprint segment

1. Select a previously enrolled segment.
2. Then confirm the deletion.

To delete the entire fingerprint credential

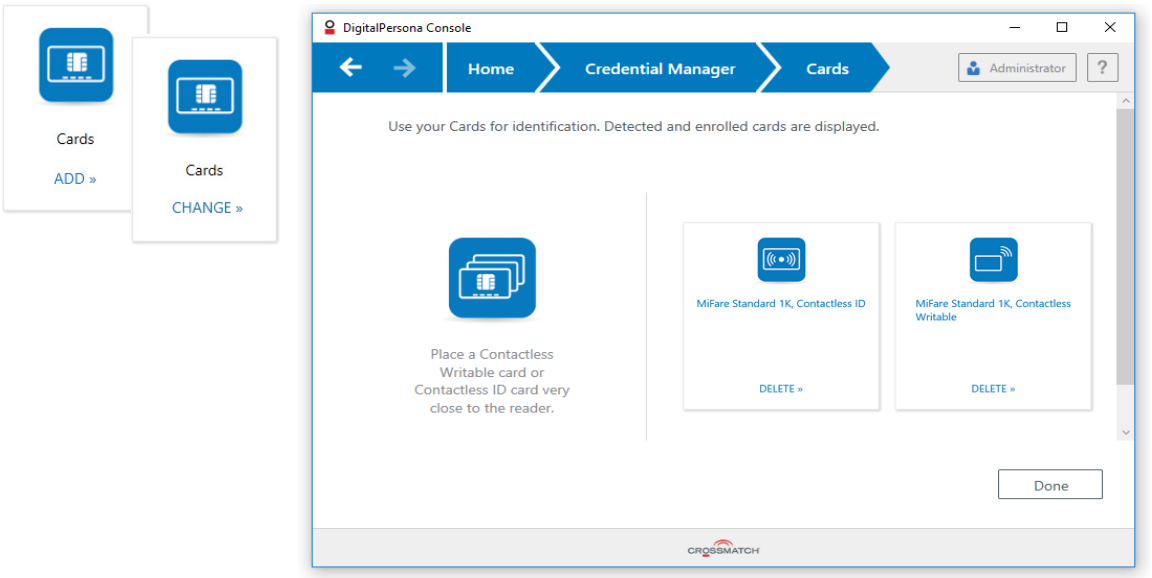
1. Once the credential has been enrolled, a *Delete* button is added to its tile.
2. Click *Delete* on the tile and then *Delete* again to confirm the deletion.

Authentication

To authenticate with the ten-print scanner, use only a single finger or thumb and use only the front half of the scanner screen to scan the fingerprint.

Cards credential

The Cards page provides a means for enrolling a user's Contactless Card credential.



To enroll a Contactless card credential

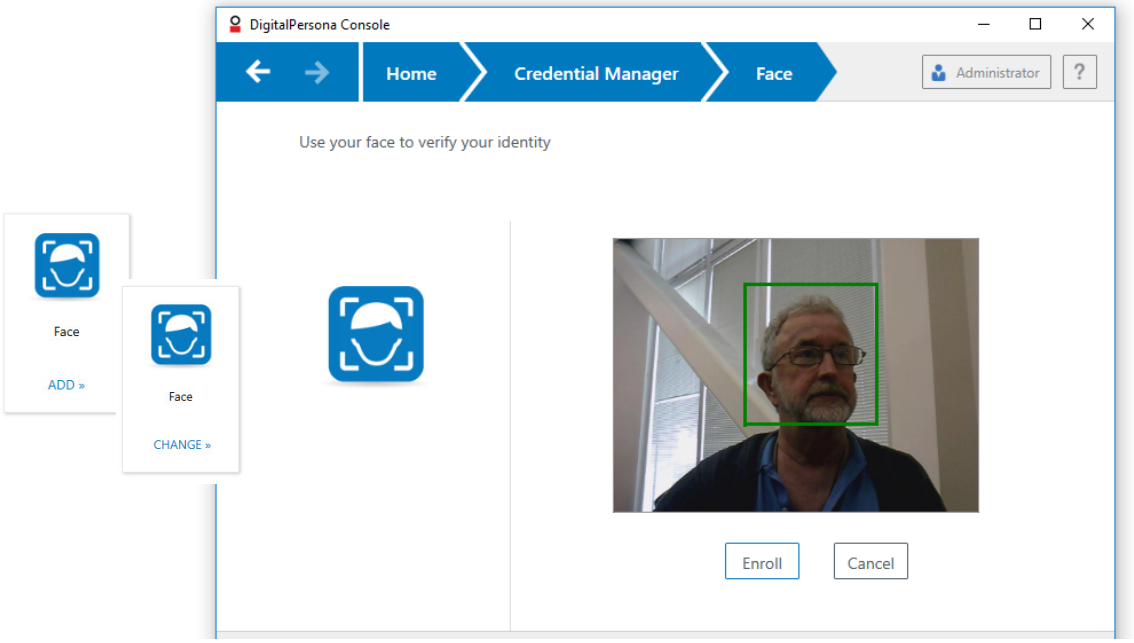
1. On the DigitalPersona Console Home page, click the Cards tile to display the Cards page.
2. Place the Contactless card very close to the reader and click *ENROLL*.
3. The *CHANGE* button displays on the Cards tile after the first card has been enrolled and saved.
4. Click *Done* to return to the Credential Manager page.

To delete a card credential

1. On the DigitalPersona Console Home page, click the Cards tile to display the Cards page.
2. Click *Delete* on the specific card image.
3. Click *Done* to return to the Credential Manager page.

Face credential

The *Face* page enables you to enroll and manage your Face credential.



The Face credential is not supported on 32-bit versions of Windows, and is not enabled by default. To use this credential, the *Enrollment* GPO must be enabled and the Face credential selected.

Your computer must have a built-in or connected camera to enroll a Face credential.

To enroll a Face credential

1. From the DigitalPersona Console, click *Credential Manager*, and then click the *Face* tile to display the *Face* page.
2. If multiple cameras are available, select a camera from the dropdown list.
3. Center your face within the frame and click *Enroll*.
4. A green rectangle will display around your face in the camera image.
5. Once enrollment is complete, the screen will refresh and display the nine separate frames used in enrolling your Face credential.

To change your Face credential

1. Once a Face credential has been enrolled, the word *CHANGE* appears below the credential's tile.
2. Click *CHANGE* to display the *Face* page.
3. Click *Re-Enroll*.

To delete your Face credential

1. Click *CHANGE* to display the *Face* page.
2. In the upper right setion of the page, click *Delete Credential*.

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.

Authentication with your Face credential

To authenticate using your Face credential

1. Do one of the following, depending on where you are authenticating from.
   - At Windows logon, select *Sign-in options* and then select the *Face* tile. If authentication is successful, you will be logged in to Windows.
   - On any *Verify your Identity* screen, select the *Face* tile.

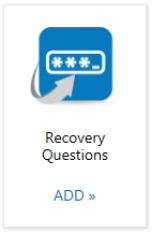
Recovery Questions credential

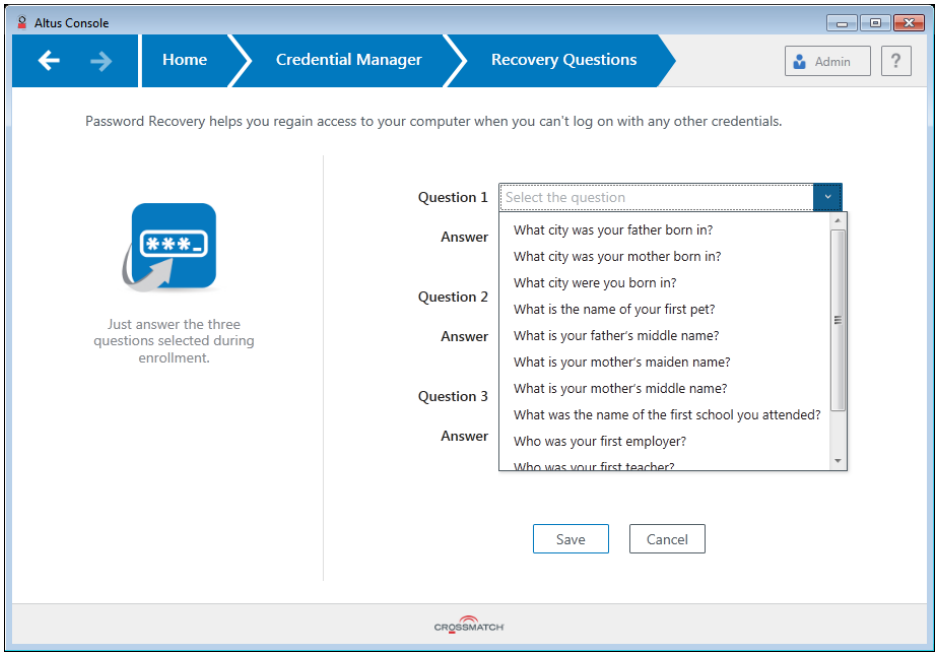
The Recovery Questions credential allows users to regain lost access to their computer when they can't log on with any other credentials. They simply need to answer the three security questions selected during this enrollment process.

This feature is optional and is not available in the DigitalPersona Kiosk products. For DigitalPersona Workstation, it must be explicitly configured by the DigitalPersona Administrator through the *Enable Self Password Recovery* setting. See the *Enable Self Password Recovery* setting in the *Policies and Settings* chapter of the *DigitalPersona Administrator Guides*. On the *Recovery Questions* page, you can enroll or manage your Recovery Questions credential; for example, change your recovery questions or the associated answers. In order to use this recovery credential to gain access to a computer, a user must have previously logged on to the same computer at least once with another valid credential.

To set up Recovery Questions

1. In the DigitalPersona Console, select *Credential Manager*, and then choose *ADD or CHANGE* on the *Recovery Questions* tile.
2. The Recovery Questions page displays.





3. On the *Recovery Questions* page, select three security questions, and then enter an answer for each question. You can also choose to write your own security questions by selecting that option at the bottom of the dropdown menu.

4. After completing the questions and answers, select *Save*.

Administrators can configure the list of security questions displayed or create custom questions through the Enable Self Password Recovery setting. (See the *DigitalPersona Administrator Guide*.)

After your Recovery Questions credential has been enrolled, you can access your computer using them from a link on the Windows Logon screen.

PIN credential

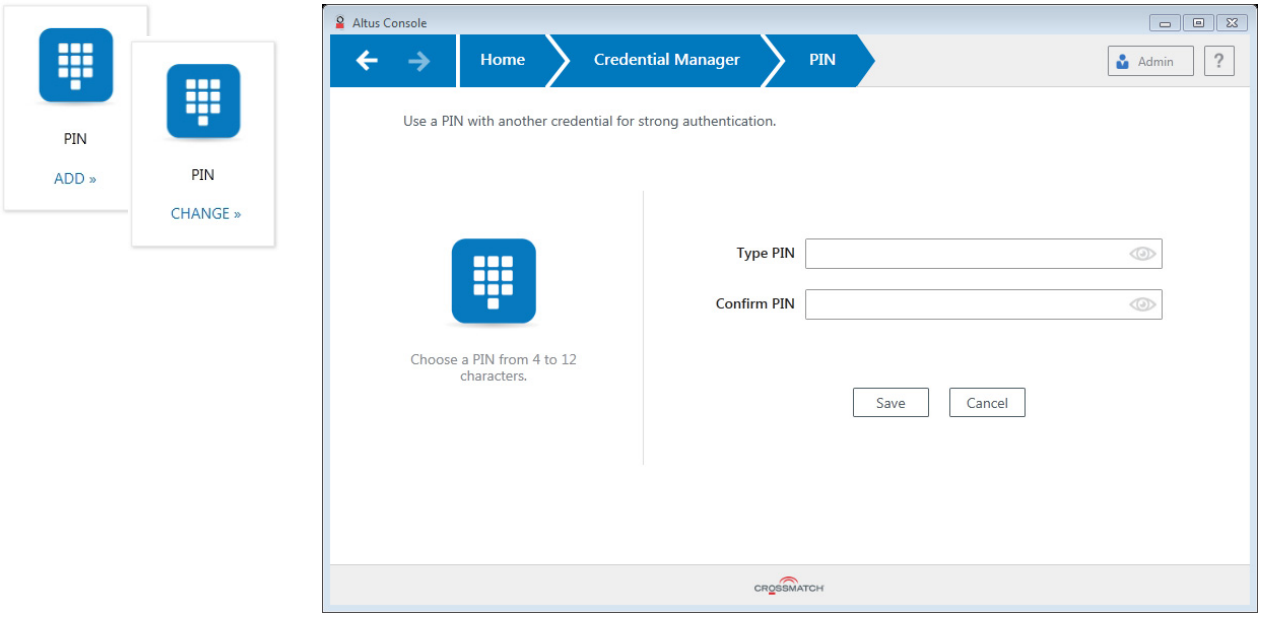
A PIN is a credential composed of user-selected characters. A PIN is often used in combination with another credential to easily enhance its security. This PIN should not be confused with a PKI Smart Card PIN which is used as part of a PKI Smart Card credential.

A PIN may be used as a credential for authentication, when combined with an additional supported credential as defined by the Logon or Session Policy in force.

On the Credential Manager, PIN page, you can create a new PIN or change your existing PIN. The minimum and maximum number of characters allowed is specified on the left side of the page. Once a PIN has been added, the PIN tile label changes from ADD to CHANGE.

To enroll a PIN credential

1. On the DigitalPersona Console Home page, click the PIN tile to display the PIN page.



2. On the PIN page, enter and confirm the characters that you want to use as your PIN.

3. The *CHANGE* button displays on the PIN tile after the PIN has been enrolled and saved.

4. Click *Save* to return to the Credential Manager page.

To delete a PIN credential

1. Choose *Delete Credential* on the PIN page.
2. Confirm the deletion.

Bluetooth credential

Any Bluetooth-enabled device discoverable by this software may be used as a credential for authentication, when combined with an additional supported credential as defined by the Logon or Session Policy in force.

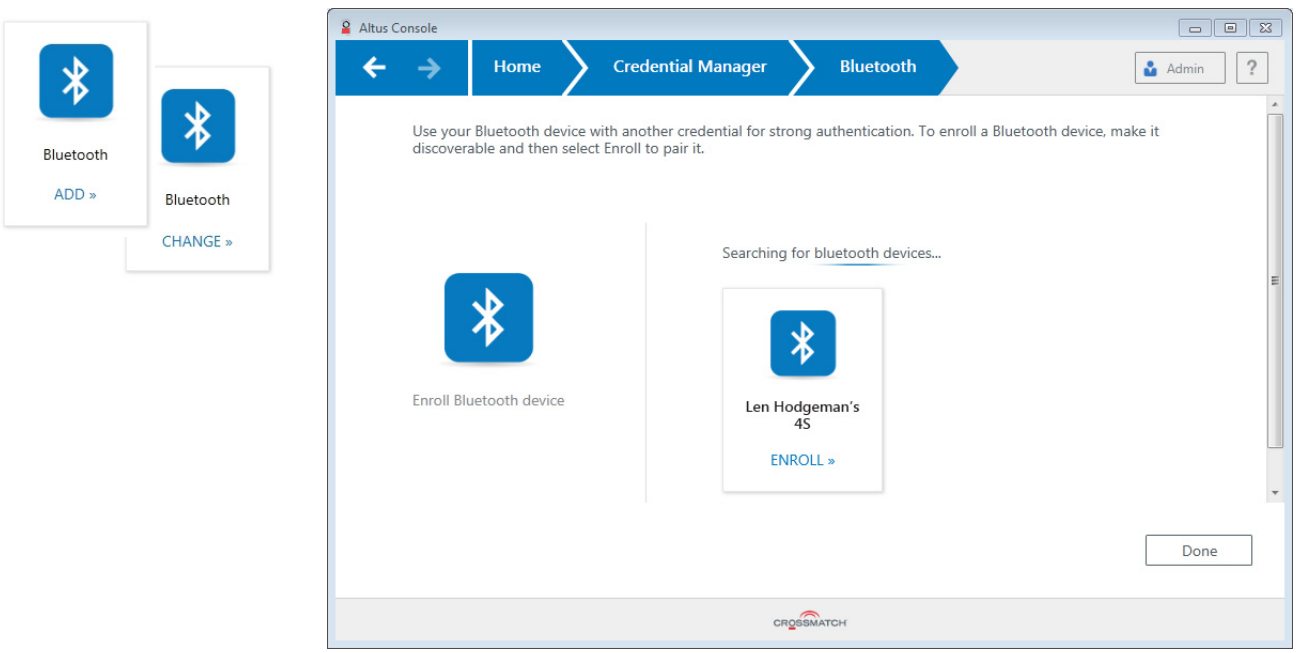
Enrolling a Bluetooth credential *does not* automatically make it available (i.e. roam) on every DigitalPersona client. This is because Bluetooth enrollment pairs the associated device with the machine where it is enrolled initially. To use their Bluetooth credential on a machine other than the one where it was originally enrolled

- The *Cache user data on local computer* GPO setting must be enabled on the DigitalPersona Server, and
- Users will need to pair their device with each Workstation or Kiosk where they expect to use their Bluetooth credential.

All unenrolled and discoverable Bluetooth devices within range are displayed in the bottom portion of the page.

To enroll, pair or manage a Bluetooth credential

1. In the DigitalPersona Console, select *Credential Manager*, and then choose *ADD or CHANGE* on the Bluetooth tile.
2. The Bluetooth Devices page displays.



To enroll a Bluetooth device as a DigitalPersona credential

1. Click *ADD*.
2. On the Bluetooth Devices page, select the desired device and choose *Enroll*. If an expected device is not displayed, ensure that the device is set to be discoverable. If the device has not previously been paired with this computer, you will be asked to pair it, and then the device will be enrolled as a credential. Devices previously paired with the computer will simply be enrolled.

CHANGE - To enroll an additional Bluetooth device, change your current Bluetooth device, or delete a specific Bluetooth device, choose *CHANGE* on the Bluetooth Devices tile. Then on the Bluetooth Devices page, select *Enroll* or *Delete*.

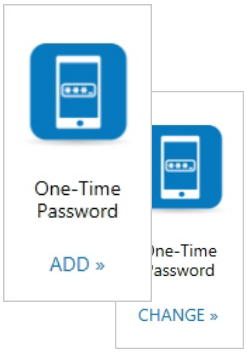
Delete - To delete all enrolled Bluetooth devices, choose *Delete* on the Bluetooth Devices tile. Then confirm the deletion by verifying your identity.

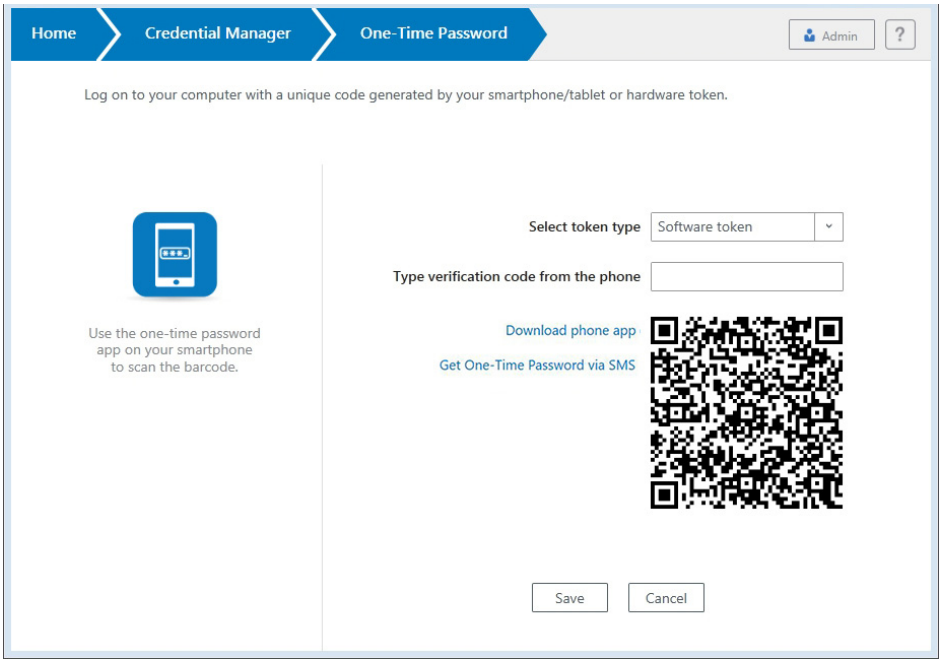
One-Time Password credential

A One-Time Password (OTP) credential uses an automatically generated time-sensitive numeric code for authentication.

The OTP credential can be used for authentication at Windows logon and within a Windows session as defined by the Logon or Session Policy in force, as well as for DigitalPersona Password Manager trained applications, websites or network resources and SAML-compliant portals such as Office 365.

It also can be used for authentication to the DigitalPersona Identity Server, providing access to the DigitalPersona Administration Console, DigitalPersona Web Enrollment and the DigitalPersona Application Portal, as well as for verifying one's identity within Web Enrollment 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 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 that 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 your organization in the CPNS service.
- The associated OTP GPO settings have been enabled and configured by a DigitalPersona administrator as described beginning in the *Policies and Settings* chapter of the DigitalPersona Administrator Guide.
- 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.

WARNING: *If you do not select ACCEPT on the Push Notification page, Push Notification will not be enabled. If you want to enable it in the future, you can do so by navigating to the DigitalPersona App in Settings/Notifications on your iOS device or the equivalent location on your Android device,*

On the Credential Manager, One-Time Password page, you can download an OTP authentication app, and then enroll the OTP credential for use with the authenticator app and OTP Push Notification (if configured).

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 DigitalPersona Console, click *Credential Manager*, and then click the *One-Time Password* tile.
2. On the *One-Time Password* page, select *Software token* as the token type if it is not already selected. (It is the default.)
3. Click the *Download phone app* link to display a dialog where you can download and install the authenticator app for your device.
4. Select your device's app store, and then scan the QR code provided or click the corresponding Download link.

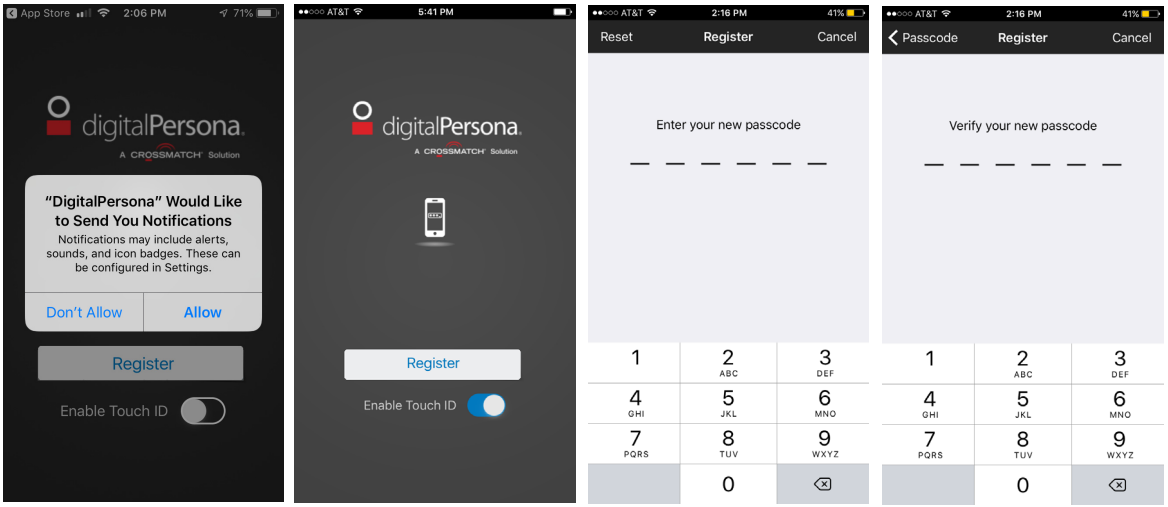
   The *DigitalPersona* app is currently available in the Apple Store and on Google Play. For the Windows and Blackberry mobile platforms, the Microsoft and Google *Authenticator* apps provide nearly identical functionality, although setup and enrollment steps may vary slightly.
5. Scanning the QR code 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.
6. Clicking the Download link 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.

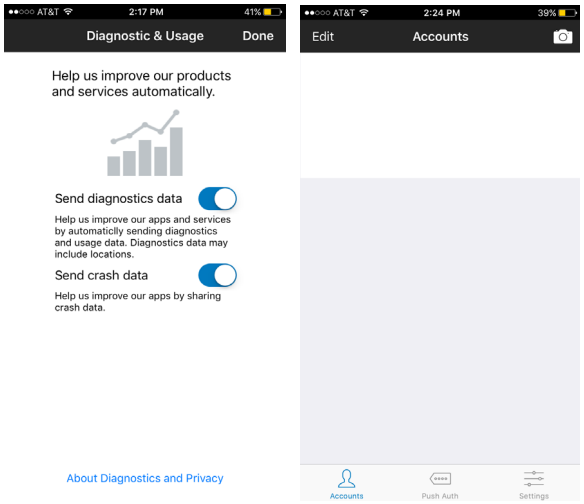
Set up a DigitalPersona account on your device

1. Launch the DigitalPersona mobile app on your device.
2. On iOS - The first time the app is launched, the *Register* screen displays, with a popup dialog requesting you to allow the app to send you notifications. Click *OK* to allow DigitalPersona Mobile to send you notifications. Note that if you do not allow notifications, you will not be able to use the PUSH notification feature for One Touch Passwords.
3. On Android systems - The first time the app is launched, the *Register* screen displays. Notifications are enabled by default for the app, and therefore PUSH OTP will be operational (if the Privacy Policy is accepted as described below).
4. Click *Register*.

5. Enter and verify a six-digit passcode.



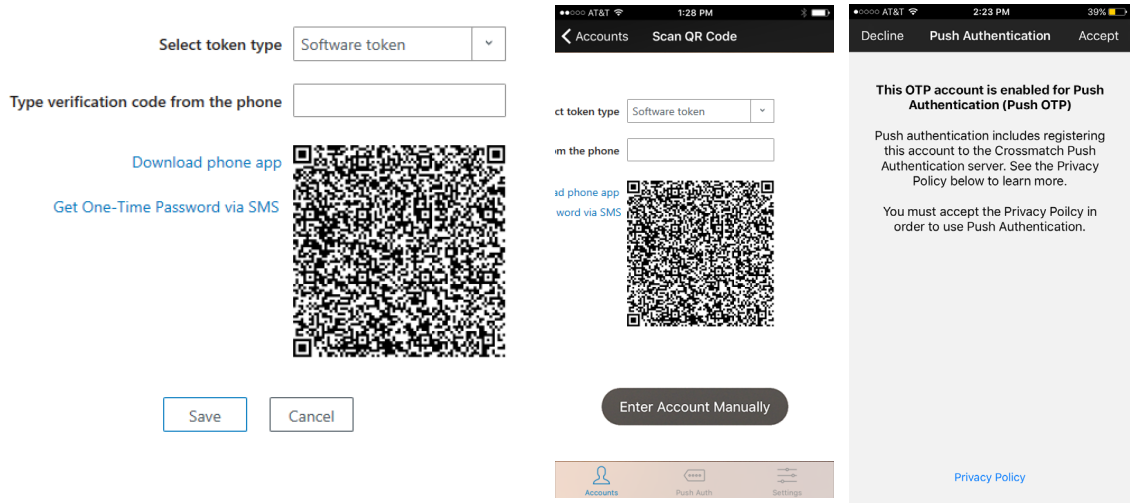
6. On the Diagnostic and Usage page, accept the defaults or tap an option to deselect it.



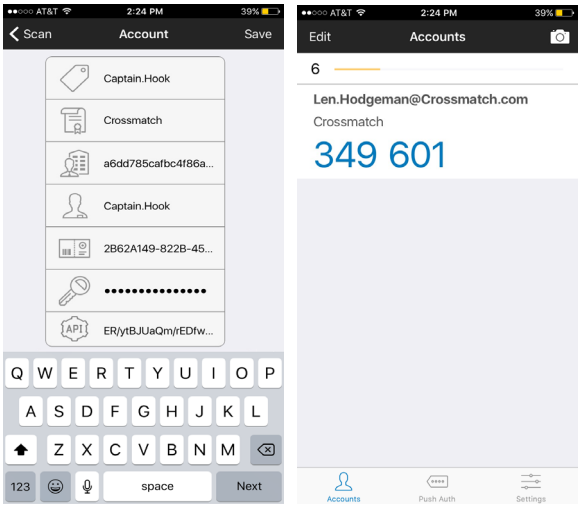
7. On the *Accounts* screen, click the Camera icon. You will be asked for permission to access your device's camera. Tap *OK* if you want to use the camera to scan the QR Code for automatically creating your DigitalPersona Mobile account. If you click *Don't Allow*, you will not be able to create an account or use the Authenticator app.

8. On the *Scan QR Code* screen, scan the QR code that displays on the One-Time Password Page. Do not scan the same QR code again from the dialog that has the app stores on it which was used to download the app.

9. If the Crossmatch Push Authentication Server has been previously setup by your DigitalPersona Administrator, Push Authentication will be automatically enabled for your device once you choose to *Accept* the associated Privacy Policy. If you choose to *Decline* the Privacy Policy, Push Authentication will not be enabled.



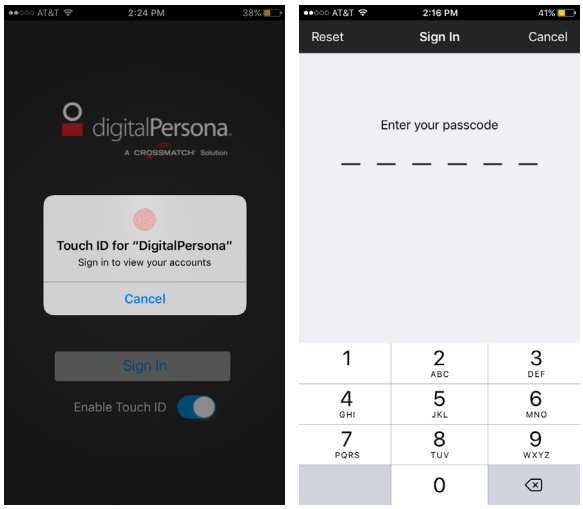
- Once the account information is displayed, tap *Save*. The DigitalPersona Mobile account will be created and the *Accounts* screen displayed with the new account and your first One-Time Password shown.



Manual account creation

This feature is reserved for use by DigitalPersona technicians.

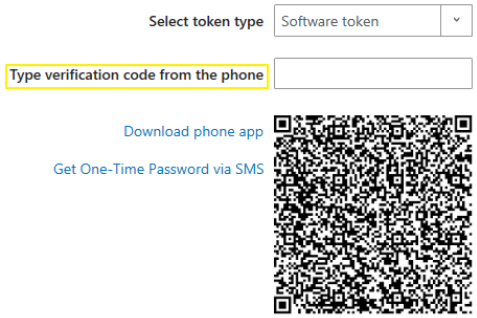
Sign in to the DigitalPersona Mobile app



Once you have registered as described in the previous pages, you can sign in to the app as follows.

1. Launch the DigitalPersona Mobile 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

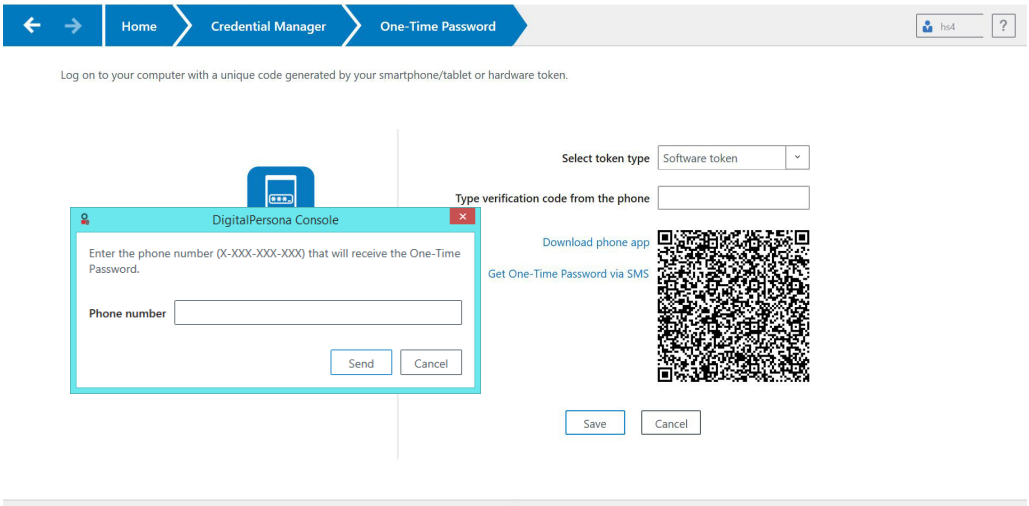


1. On your computer, open the One-Time Password page.
2. On your device, sign in to the DigitalPersona Mobile app.
3. On your computer, enter the six-digit verification code displayed in the app and click *Save*.

OTP for SMS delivery

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.

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.



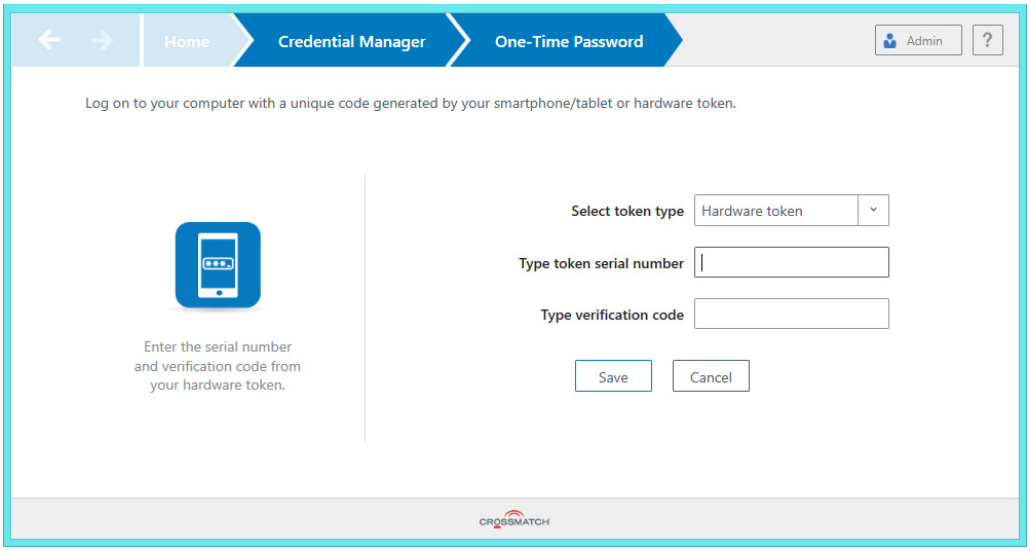
To enroll the OTP via SMS credential

1. On the One-Time Password page, click the *Get One-Time Password via SMS* link.

2. Enter the number for the mobile device that you would like to enroll in order to receive a One-Time Password through SMS delivery.
3. Click *Send*.
4. You will receive an SMS message on your mobile device containing a six-digit verification code.
5. On your computer, enter the verification code into the *Type verification code from the phone* field.
6. The *Credential Manager* page will re-display and the One-Time Password tile will now show the *Change* caption, indicating that a One-Time Password credential has been enrolled.

OTP hardware token

On the Credential Manager, One-Time Password page, you can enroll a hardware token as an 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.



Typical hardware tokens

To enroll an OTP credential using a hardware token

1. From the DigitalPersona Console, click *Credential Manager*, click the *One-Time Password* tile and, from the *Select token type* dropdown list, select *Hardware token*.
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 the *Administration Overview* chapter of the DigitalPersona AD Administrator Guide or in the *Administration Tools* chapter of the DigitalPersona LDS 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.

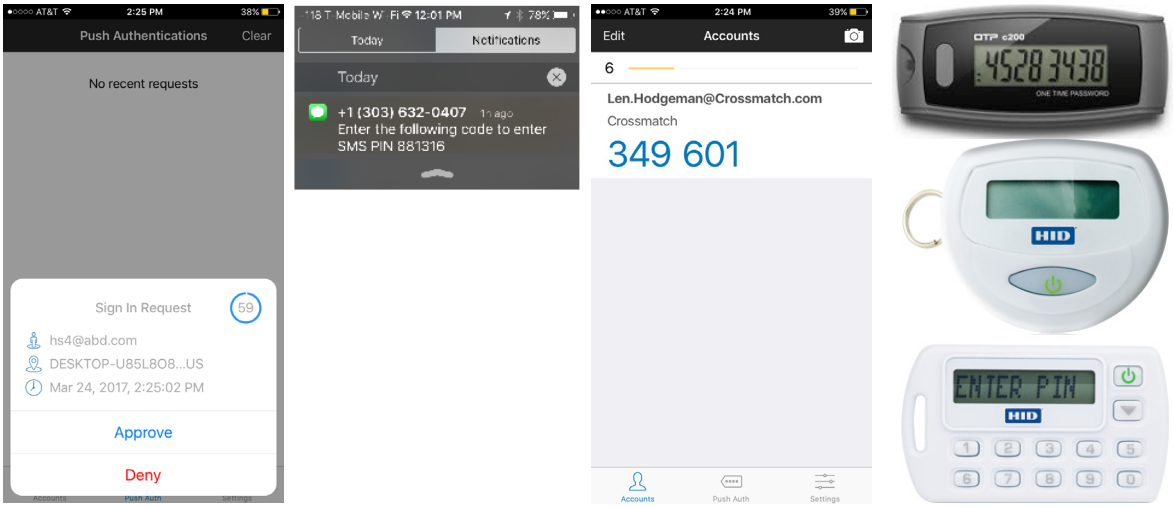
   - At Windows logon, select *Sign-in options* and *then* select the *One-Time Password* (or OTP) tile to display *One-Time Password* options.
   - On any *Verify your Identity* screen, select the *One-Time Password* (or OTP) tile.

One-Time Password tile

2. You can use an OTP credential in any of the following ways.

   - Select *Send push notification* to send a notification to your enrolled mobile device allowing you to Approve or Deny authentication.
   - Select *Send SMS with OTP code* to send an SMS message to your enrolled mobile device with a verification code that you can enter on your computer for authentication.
   - Launch your previously registered authentication app on your mobile device and enter the resulting verification code into the entry field on your computer.

- Activate the display on an enrolled hardware token, and enter the displayed verification code on your computer.



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 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.

To delete your OTP credential

1. On the One-Time Password page, click *Delete Credential*.
2. Confirm that you want to delete the credential.

FIDO Key credential

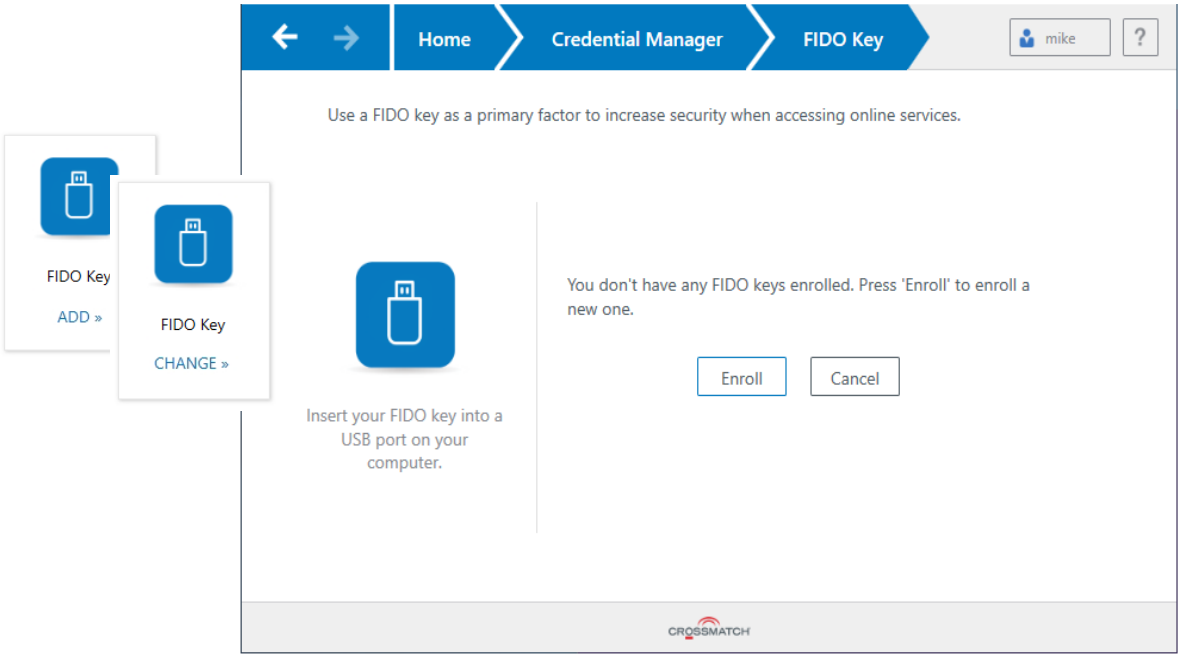
The FIDO Key credential uses a FIDO USB key for authentication. The FIDO Key page is where FIDO keys are enrolled and managed.

IMPORTANT: If FIDO Keys will be used with DigitalPersona Web Components, i.e. Identity Provider, Web Administration Console or Web Enrollment, they should be enrolled through Web Enrollment, and not through the DigitalPersona Workstation User Console. FIDO Keys enrolled through the User Console will not work with DigitalPersona's Web Components.

To enroll or manage a FIDO Key credential

1. In the *Credential Manager*, click *ADD or CHANGE* on the FIDO Key tile.

2. The FIDO Key page displays.



To enroll a FIDO key as a DigitalPersona credential

1. Click *ADD*.
2. On the FIDO Key page, insert a FIDO key into an available USB port and choose *Enroll*.
3. Depending on the type of FIDO key being used, activate it through one of the following actions.
   - Tap the sensor on the device.
   - Press a button on the device.
   - Remove and reinsert the device.

To change the FIDO key being used as a credential

1. Choose *CHANGE* on the FIDO Key tile.
2. On the *FIDO Key* page, select *Re-Enroll*.
3. Tap, press the button on, or re-insert your FIDO key.

Upon successful enrollment, the *Credential Manager* page redisplays.

To delete this credential

1. Choose *CHANGE* on the FIDO Key tile.
2. On the *FIDO Key* page, in the upper right, click *Delete Credential*. In the confirmation dialog, click *Delete*.

Password Manager 8

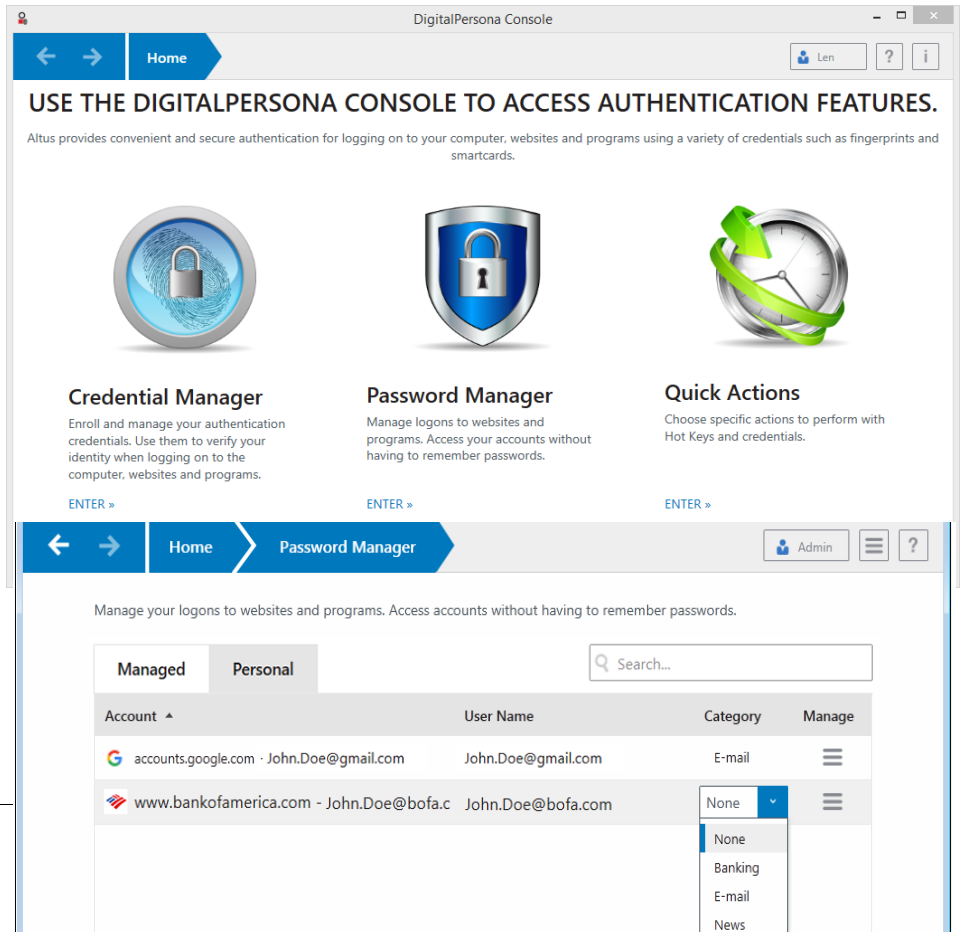
THIS CHAPTER DESCRIBES PASSWORD MANAGER, AN OPTIONAL FEATURE OF THE DIGITALPERSONA WORKSTATION AND KIOSK CLIENTS.

Introduction

Logging on to Windows, websites, and applications is easier and more secure when you use Password Manager. You can use it to create stronger passwords that you don't have to write down or remember, and then log on easily and quickly with DigitalPersona enrolled credentials such as a fingerprint, PKI Smart Cards, Contactless Cards, or your Windows password. Additional auxiliary credentials can also be used in composite authentication.

Password Manager allows you to:

- Managed logons - Add, edit or delete logon account data for managed logons provided by your administrator. This feature may optionally be disabled by the administrator.
- Personal logons - Add, edit, or delete personal logons and logon account data.
- Use personal or managed logons to launch your default browser and log on to any website or program.
- Organize your logons into categories.



Managed logons and personal logons

*Managed logon*s are created, administered and deployed by an administrator using the Password Manager Admin Tool, which is a separate installation from your DigitalPersona product package. For instructions on using the Password Manager Admin Tool, see the *Password Manager Admin Tool* chapter in the *DigitalPersona Administrator Guide*.

In most cases, the first time a managed logon is used, you will be asked for your personal account logon data for a resource. Whether account data is requested, and what type of data is required is determined when the managed logon is created, and also governed by settings described in the *DigitalPersona Administrator Guide*.

If account data is required, it is only entered once. On subsequent use of the logon, account data will be filled in automatically.

Additionally, many options are provided for customizing the use of managed logons for your environment. See the Settings described in the *DigitalPersona Administrator Guide*.

*Personal logon*s are created by an individual for their own use. Account data is entered during the creation of the logon, and filled in automatically during subsequent use of the logon. This chapter primarily addresses the use of personal logons, although much of the information also applies to the use of managed logons.

Note that use of Password Manager logons doesn't require a live connection to the DigitalPersona Server. However, logons can't be created or modified unless your DigitalPersona client can connect to the DigitalPersona Server.

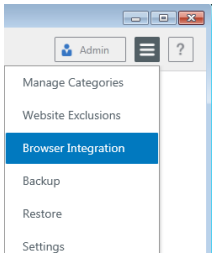
Browser Integration

To use Password Manager with a supported web browser, follow the steps listed below for integrating the browser with Password Manager. Note that Password Manager supports only those browsers listed below.

Internet Explorer

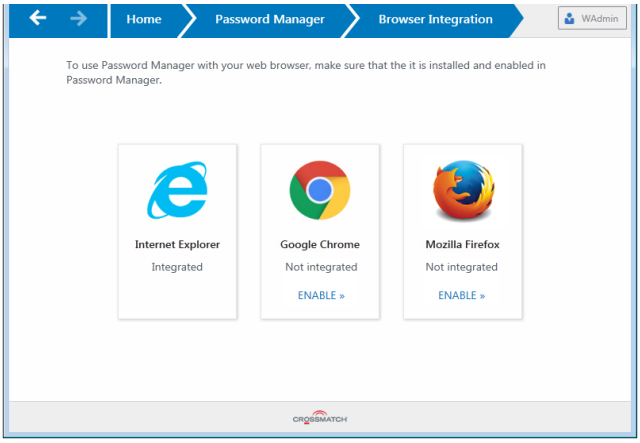
Internet Explorer for the desktop is fully integrated with Password Manager and does not require any further configuration. Password Manager does not support the Internet Explorer Modern UI app.

Google Chrome and Mozilla Firefox



To use Password Manager with the Google Chrome or Mozilla Firefox browsers

1. On the console Home page, choose *Password Manager*.
2. On the Password Manager page, click the Password Manager Menu button.
3. Select *Browser Integration* from the Password Manager Menu.
4. On the Browser Integration page, click *Extension* on one of the browser tiles and follow the onscreen instructions.



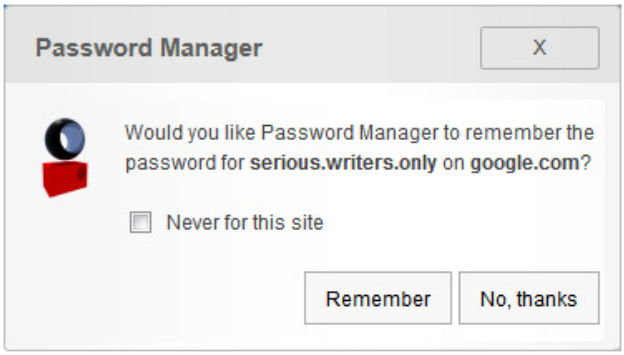
Optionally, you can select *Don't remind* to prevent the DigitalPersona software from occasionally reminding you to install the extension for any of the supported browsers that you have installed.

Adding logons

There are two ways to add a logon for a website or program to Password Manager.

Remember your credentials

Simply log in to a website or program as usual and Password Manager will offer to remember your account information.

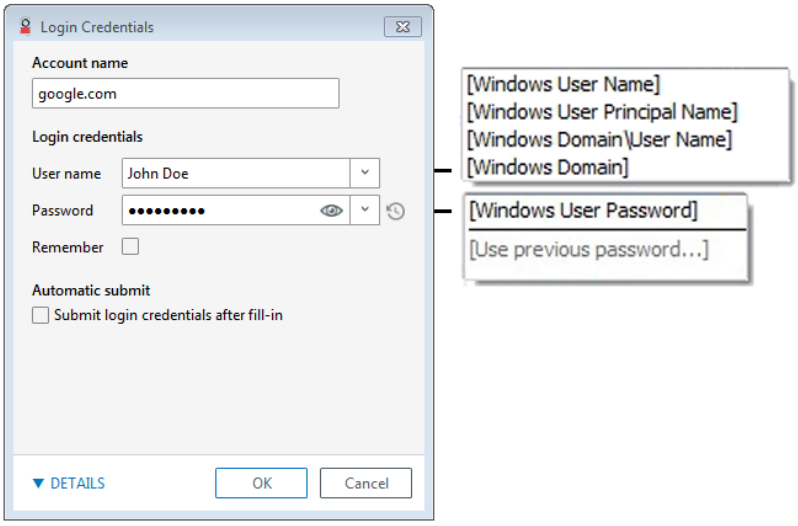


Click *Remember* and your logon information is saved. Next time you can log in with any enrolled credential.

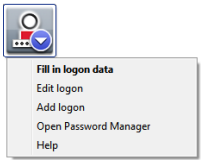
If you do not want to see the Password Manager reminder each time you visit this site, select *Never for this site.*

Login Credentials dialog

Add or edit your personal logons from the Login Credentials dialog,



- *From any logon screen* - With a website or program logon screen displayed in your browser, scan an enrolled fingerprint or present an enrolled card to display the Login Credentials dialog.
- *From a previously trained logon screen* - Click the Password Manager icon and select *Add logon* or *Edit logon*.
- *From Password Manager* - On the Password Manager page, click the *Manage* menu next to any current logon and select *Add Logon* or *Edit Logon* to display the Logon Credentials dialog.



Once the logon information is saved by Password Manager, from then on, your logon information can be automatically filled in and optionally submitted as well.

You can use these logons in several ways.

- Browse to the website or program and have Password Manager fill-in and optionally submit, you credentials.

- Launch the resource from the Password Manager page in the DigitalPersona Console.
- Click a logon from the Logons menu to have Password Manager open the website or program and log you on.

Creating logons

Password Manager logons are created by entering relevant information in the Login Credentials dialog.

To create a logon

1. Display the *Login Credentials* dialog as described on the previous page.
2. Enter your logon data.
   - To populate the User name field with a preformatted Windows credential, click the arrow to the right of the field and select one of the displayed options.

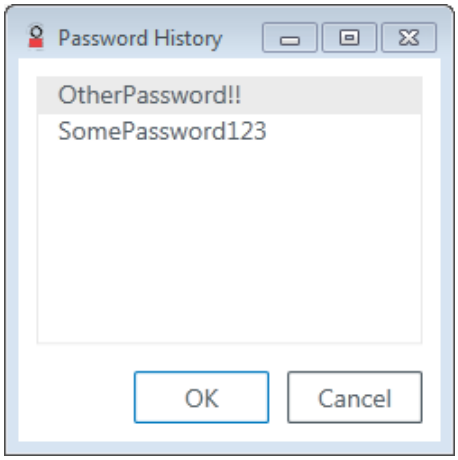
     Windows User Name
     Windows User Principal Name
     Windows Domain\User Name
     Windows Domain

   - To populate the Password field with a preformatted credential, click the arrow to the right of the field and select one of the displayed options. Note the colored line under the Password field. This indicates password strength from red, through yellow to green for optimum strength.

     Windows User Password

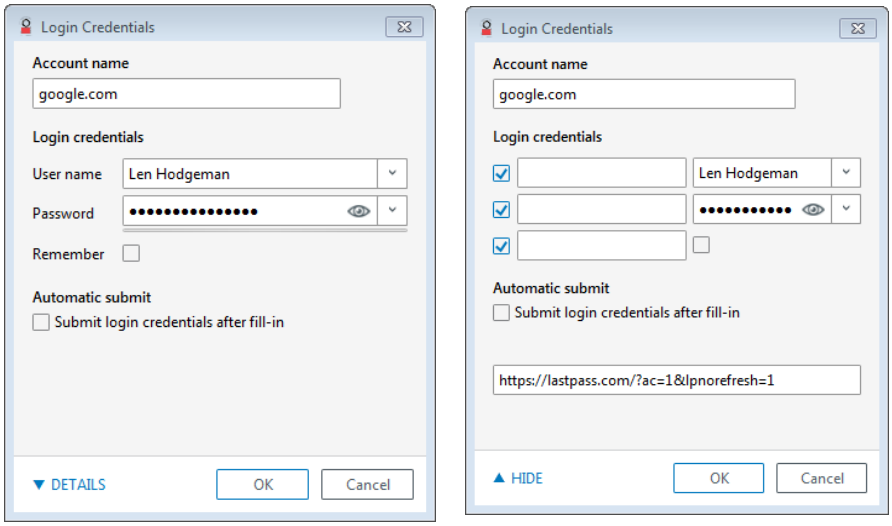
     Use previous password ... -Sometimes, you may modify a password in Password Manager, but this password is rejected by the application. In this case, the software allows you to use a previous password (i.e. a password previously entered for this logon page) instead of the most recent one.

     If you select *Use previous Password*, after authentication you will be prompted to choose a previous password in the *Password History* dialog (shown below). The list includes up to seven previously used passwords.



   - To view the password for this logon, click the *Eye* icon.
   - To have the logon fields filled in, but not submitted, clear the checkbox next to the label *Submit login credentials after fill-in*.

3. If Password Manager does not display the required logon fields, click *DETAILS*. Then select the check box for each field that is required for logon, or you can clear the check box for any fields that are not required for logon.



4. If Password Manager cannot detect all of the required logon fields, a message is displayed asking if you want to continue. Click *Yes* to enter manual mode.

Each time that you access the now "trained" website, program or network resource, the Password Manager icon shown below is displayed on the screen (Internet Explorer) or to the right of the first recognized entry field in Chrome, indicating that you can use any of your enrolled credentials to log on. An administrator can also create managed logons for resources, including Change Password screens (see the *Password Manager Admin Tool* chapter in the *DigitalPersona Administrator Guide*).

Password Manager Icon for Internet Explorer

Password Manager Icon for Internet Explorer indicating a recognized Change Password screen

Password Manager Icon for Chrome

Password Manager Icon for Chrome indicating a recognized Change Password screen

Manual mode

A dialog is displayed with your logon fields filled in. Click the icon for each field and drag it to the appropriate logon field, and then click the button to sign into the website.

Once you use the manual mode of entering the logon data for a site, you must continue to use this method to log on to the same website in the future.

The manual mode of entering logon data is available with Internet Explorer, and is not available when using other web browsers.

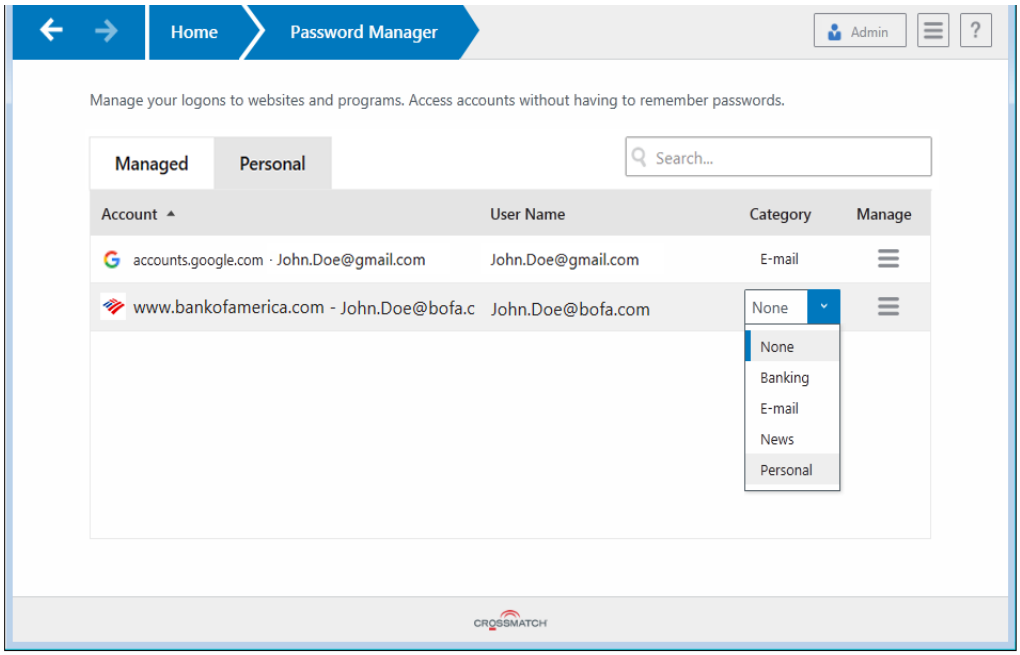
Editing logons

You edit your personal logons through the Login Credentials dialog described above (on page 75).

Organizing logons into categories

Keep your logons in order by assigning them to custom categories.

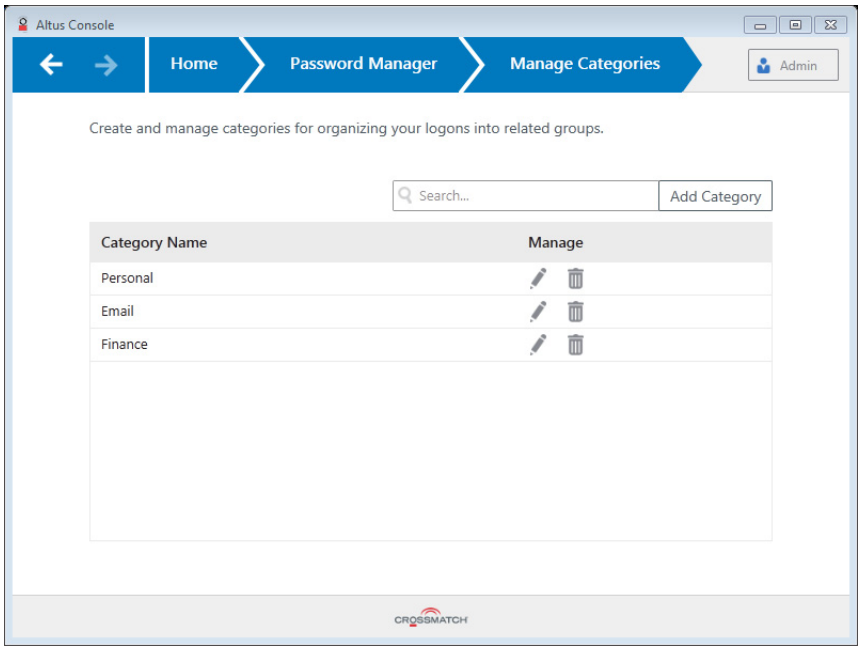
Logons can be added to any previously created category by selecting the category from the Category dropdown menu while a logon is highlighted on the Personal tab. Note that each logon can only belong to a single category.



When creating additional logons for the same web domain,

- If there are two or more accounts belonging to the same web domain, which do not belong to any custom category, then they will be categorized by their domain name (defined as the characters appearing after "http(s)://" and before the domain zone.)
- If an account is already assigned to a custom category, there is no nested category for it based on the domain name.

On the Password Manager page, select *Manage Categories* from the Password Manager *Manage* menu in the upper-right corner. This will display the *Manage Categories* page.



To create a new category

1. Click *Add Category*.
2. Enter a category name in the resulting dialog and click *Save*.

To edit a category name

1. Click *the Edit* icon next to the category.
2. Edit the category name in the resulting dialog and click *Save*.

To remove a category

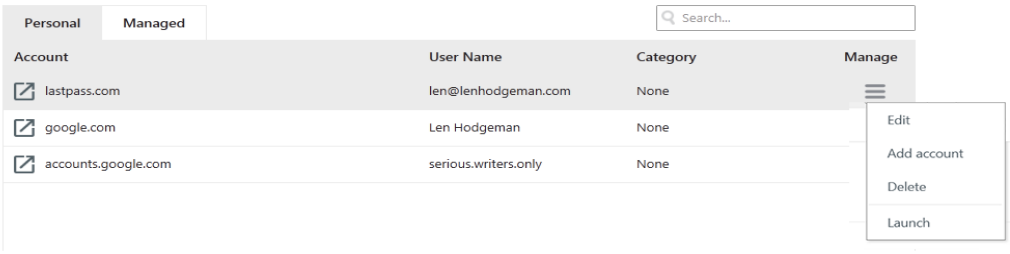
1. Click *the Delete* icon next to the category.
2. Confirm the deletion by clicking *Yes*.

Managing your logons

Password Manager makes it easy to manage your logon information for user names, passwords, and multiple logon accounts, from one central location.

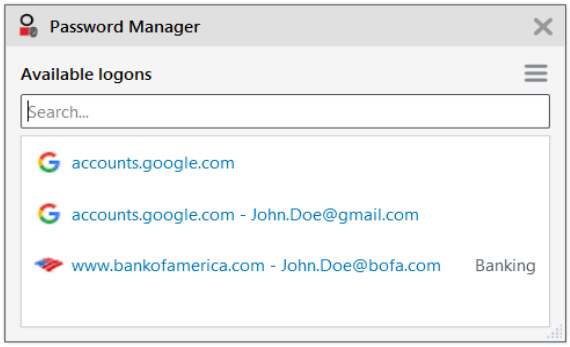
Your logons are listed on the Password Manager page in the DigitalPersona User Console. Each logon includes an entry for the website, program or other resource, and an indented entry for each set of account data created for the resource.

Manage your logons from the Manage logon menu next to each logon.



Using the Logons Menu

Password Manager provides a fast, easy way to launch the websites and programs for which you have created *personal* logons. Double-click a program or website logon from the *Logons Menu* to open the logon screen and automatically fill in your logon data.



Managed logons may also be created by your administrator, and may display on the Logons menu.

When you create a logon, it is automatically added to your Password Manager *Logons Menu*.

To display the Logons Menu, do one of the following:

- Press the Password Manager hot key combination.
  Ctrl+Win+H is the factory setting. You can change the Hot Key combination from the Quick Actions page, accessed by clicking the *Quick Actions* tile in the *Altus Console*.
- Scan your fingerprint (on computers with a built-in or connected fingerprint reader).

Using managed logons

Note to administrators - If you are deploying managed logons to your users, this topic contains information that you will want to make sure is passed on to them. The same information is also included in the end-user help file included with compatible clients.

Logging On

After creating managed logons and deploying them to users, users will be able to launch a logon screen and verify their identity with their specified credentials.

Note: 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.

Logon screens that have a logon created for them display the Password Manager icon on the screen.

Password Manager Icon for Internet Explorer

Password Manager Icon for Chrome

Depending on the attributes defined by the logon administrator, the logon process may vary.

- A user can be automatically logged on, with all fields populated and submitted, simply by verifying their identity.
- The user may need to supply information for required fields the first time they use the logon, but be automatically logged on subsequently.
- If a user has multiple sets of account data, they will be prompted to select the account they wish to log on to in the **Choose Logon Account** dialog box.

Changing passwords

After creating logons and deploying them to users, managed password screens display the Change Password icon on the screen. After verifying their identity, the user is asked to provide an old password, a new password and to confirm the new password.

Depending on the logon attributes, the change password process may vary.

- The user can be allowed to choose a new password with or without constraints on the password content.

A new random password can be automatically generated, in which case the user must log on with alternate credentials.

Website Exclusions

The Website Exclusions list displays websites that are excluded from being managed by Password Manager. There are two ways that a website ends up on this list.

- When Password Manager prompted to remember logon credentials, you selected *Never for this site*.
- You manually added the website's URL to the list.

To access the Website Exclusions list

- From the DigitalPersona Console, click *Password Manager*, select the *Manage* menu and then click *Website Exclusions*.

To add a website to the Website Exclusions list

1. On the Website Exclusions page, select *Exclude Website*.
2. Enter the URL for a website that you want to add to the Website Exclusions list. Click *Save*.

To edit a website on the Website Exclusions list

1. On the Website Exclusions page, click the Edit ( ) icon for the entry that you want to change.

2. Enter your changes and click *Save*.

To delete a website from the Website Exclusions list

- On the Website Exclusions page, click the Delete (✕) icon for the entry that you want to delete and then click Yes to confirm.

To search for websites in the Website Exclusions list

1. Enter the text to search for in the Search field.
2. Click the Search (🔍) icon.

Backing up Password Manager Data

It is recommended that users back up their Password Manager data on a regular basis. How often they back it up depends on how often the data changes. For instance, if a user adds new logons on a daily basis, they should probably back up their data daily.

Note that only their Password Manager data is backed up by this feature, not their enrolled credentials or the DigitalPersona Workstation software.

Backups can also be used to migrate Password Manager data from one computer to another. DigitalPersona Workstation must be installed on any computer that is to receive backed up data before the data can be restored from the backup file.

To back up Password Manager data:

1. Open the DigitalPersona Console.
2. From the console, choose *Password Manager* and then select *Backup* from the *Manage* menu.
3. Enter a name for the backup file. By default, the file will have a .dpb file extension. Click *Browse* to specify a location for the backup file.
4. Enter and confirm a password to protect the file. Then select *Backup*.
5. Verify your identity with any enrolled credential. Then click *OK*.

Restoring Password Manager Data

Password Manager data previously backed up through the Backup feature (as a .dpb file) can be restored to the same computer or another computer where DigitalPersona Workstation is installed.

Note that only a user's Password Manager data is restored by this feature, not their enrolled credentials or the DigitalPersona Workstation software.

To restore Password Manager data

1. Open the Altus Workstation User Console.
2. On the console Home page, choose *Password Manager* and then select *Restore* from the *Manage* menu.
3. Select the previously created backup (.dpb) file. You can enter the path in the field provided or click *Browse* to locate the file.
4. Enter the password used to protect the file.

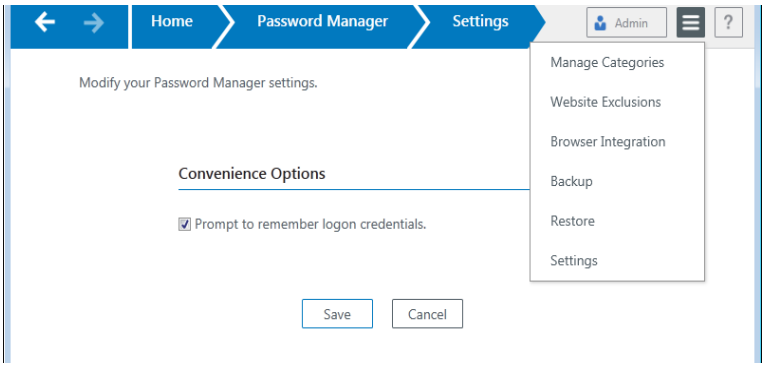
5. Select *Restore*.
6. Verify your identity with any enrolled credential. Then click *OK*.

Settings

On the Password Manager Settings page, you can personalize your experience of Password Manager.

To access the Settings page

1. Click the Password Manager *Manage* menu in the upper right corner of the Password Manager page.



2. Select the *Settings* option.

The Settings page contains the following setting.

Prompt to remember logon credentials - By default, Password Manager prompts you to save your logon credentials, on screens recognized as containing logon fields. Deselecting this setting will stop Password Manager from prompting you to save your logon credentials.

Differences in supported browsers

Internet Explorer

All features described in this guide are supported in those versions of Microsoft Internet Explorer that are listed in the System Requirements.

Chrome and Firefox

When used with supported versions of the Chrome and Firefox browsers, all Password Manager features are available except for Manual Mode and the Lock out Logon Fields property used in creating managed logons. See the *Password Manager Admin Tool* chapter in the *DigitalPersona Administrator Guide*.

When logging in to a website with a managed logon that was created with the *Start Authentication Immediately* property set, after logging out or canceling the authentication dialog and being returned to the login page, the authentication dialog is not redisplayed.

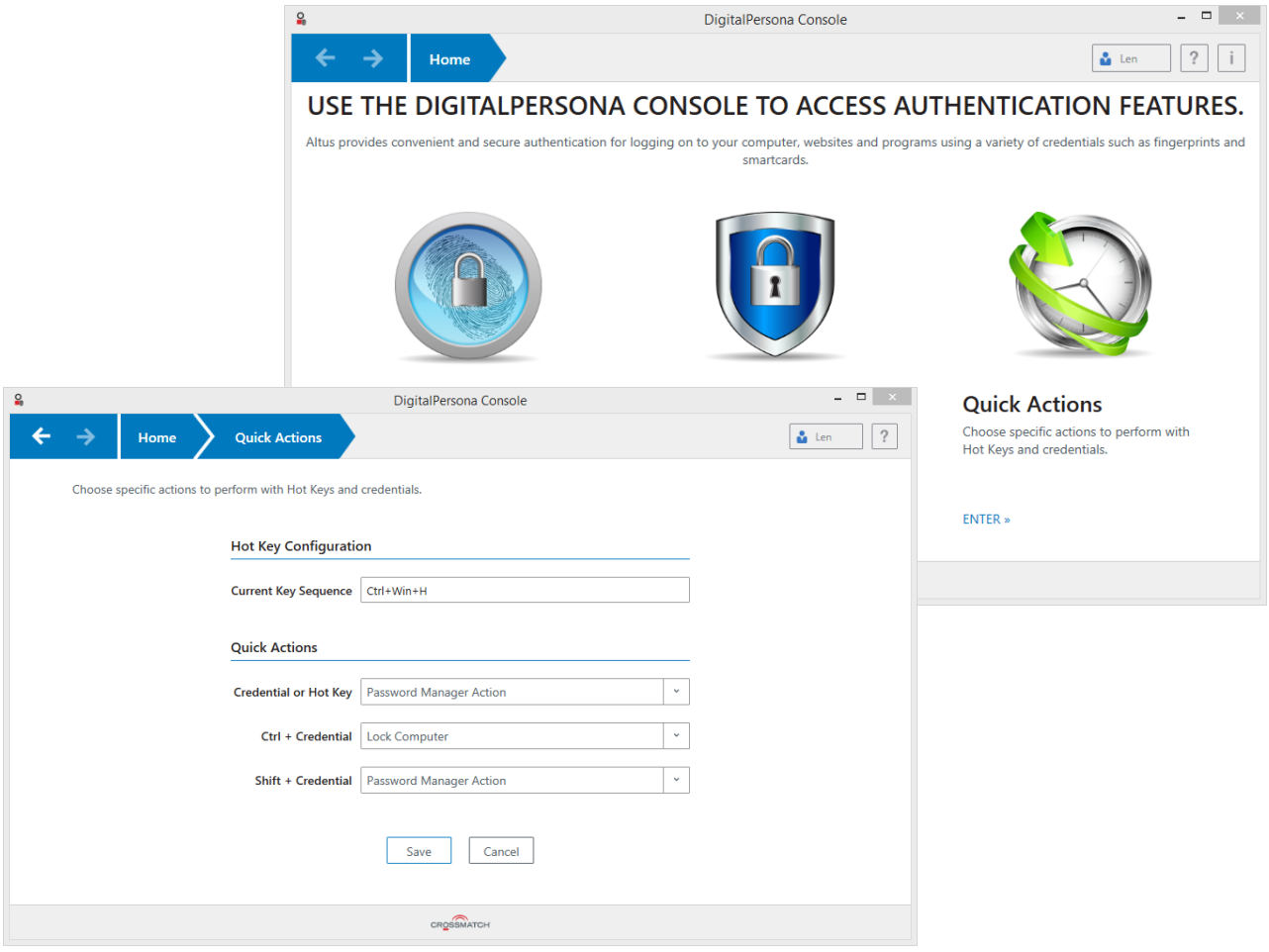
Quick Actions 9

THIS CHAPTER DESCRIBES QUICK ACTIONS, A DIGITALPERSONA CONSOLE FEATURE INCLUDED WITH DIGITALPERSONA PASSWORD MANAGER (AN OPTIONAL COMPONENT OF DIGITALPERSONA PREMIUM).

Introduction

On the Quick Actions page, you can change the DigitalPersona Hot Key sequence and configure Quick Actions, operations performed automatically in response to the use of the DigitalPersona Workstation Hot Key, a credential or a Key+Credential combination.

This feature is available in DigitalPersona LDS Workstation and DigitalPersona AD Workstation. It is not available in DigitalPersona LDS Kiosk or DigitalPersona AD Kiosk.



To manage Quick Actions settings

1. Launch the DigitalPersona Console

2. Tap or click the Quick Actions tile.

Only fingerprint and supported card credentials will initiate a Quick Action. Specific Quick Actions may be disabled by your administrator.

Quick Actions that may be shown are

Password Manager Action - Initiates a specific action depending on context.

When the active window has an associated Password Manager personal logon or managed logon, fills-in account data.

If the window is determined to be a logon screen that does not have an associated personal logon or managed logon, and the *Allow creation of personal logons* setting is enabled or not configured on the DigitalPersona Server, the *Add Logon dialog* displays.

If none of the above cases are true, the *Logons Menu* or *DigitalPersona Console* is shown.

Lock Computer - Locks the computer.

The assignment of the DigitalPersona Workstation Hot Key, and the Quick Actions performed by presenting a credential or Key+Credential combination, may have been configured by your administrator. If so, you will not be able to change them.

DigitalPersona Attended Enrollment 10

THIS CHAPTER DESCRIBES DIGITALPERSONA ATTENDED ENROLLMENT, AN OPTIONALLY INSTALLED COMPONENT OF THE DIGITALPERSONA WORKSTATION CLIENTS.

Introduction

DigitalPersona Attended Enrollment allows the DigitalPersona administrator to delegate a user or group to supervise the credential enrollment process. This feature is not installed as part of the typical (default) installation, but must be selected as part of a Custom installation of DigitalPersona AD or DigitalPersona LDS Workstation. See page 33 for installation details. It is not a feature of the DigitalPersona Kiosk clients.

Supervised (attended) enrollment is the default method of creating DigitalPersona users and enrolling their credentials. However, self-enrollment of user credentials is also an option. See the DigitalPersona LDS or DigitalPersona AD Administrator Guide for details.

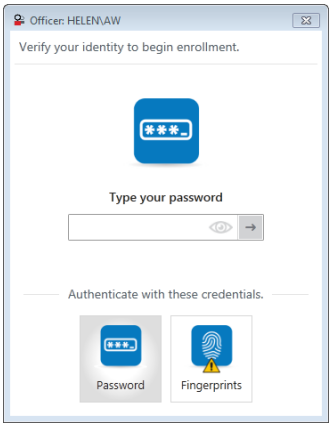
Much of the workflow and behavior of the DigitalPersona Attended Enrollment UI is configurable and is defined in the file *DigitalPersona.Altus.Enrollment.exe.config* file, located in the component's */Bin* folder, by default *C:\Program Files\DigitalPersona\Bin*. See the section *Customizing Attended Enrollment* beginning on page 112.

There are a few small differences in functionality depending on whether Attended Enrollment is installed as part of a DigitalPersona AD or DigitalPersona LDS configuration.

- AD - Only AD users exist. All users of the DigitalPersona software are identified in the user interface as AD users.
- LDS - There are AD users and Non AD users. The term Non AD users signifies those users without records in Active Directory, and AD users are those who have an Active Directory (Windows) account.

Any additional differences between the two configurations will be noted within the content that follows.

Security Officer identification



When launching Attended Enrollment, the first screen requires authentication by a DigitalPersona Security Officer.

The Security Officer submits one of their enrolled credentials. When using a Windows password, they can simply click the arrow to the right of the password field. The User Selection page displays.

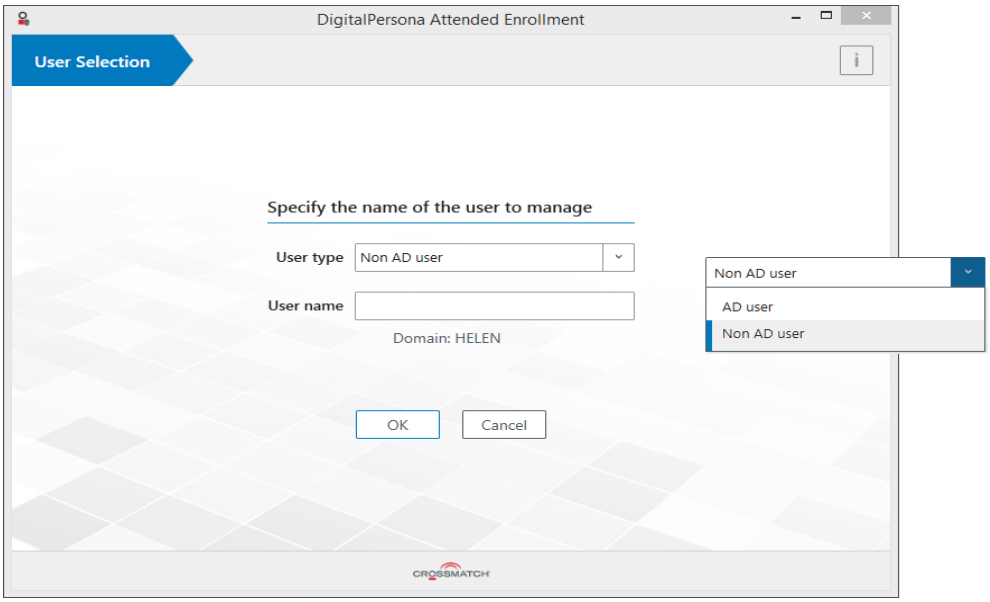
Additionally, by default, the Security Officer will need to authenticate after enrollment of each credential. This feature can be configured through the governing XML file. Also, the user being enrolled will need to authenticate at the end of the enrollment process. The user selection/creation process is slightly different for *Non AD users* and *AD users*, as shown in the following pages.

Non AD User selection/creation (DigitalPersona LDS)

Within a DigitalPersona LDS environment, to select or create a Non AD user:

(For AD user selection, see page 88.)

1. On the *User selection* page, select *Non AD user* from the dropdown list.
2. Enter a valid user name and click *OK*.

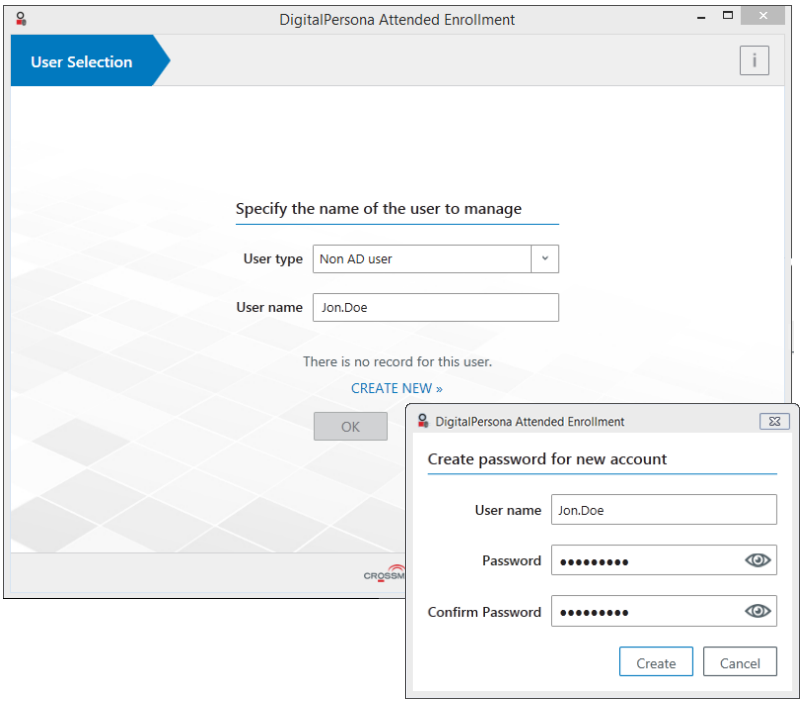


When an entered user name is not found in the DigitalPersona database, you have the option of creating the user at this point (see step 1 below).

If you think you have simply misspelled the name, you can edit the name directly on this page. and click *OK* to search for the user again.

To create a new Non AD user

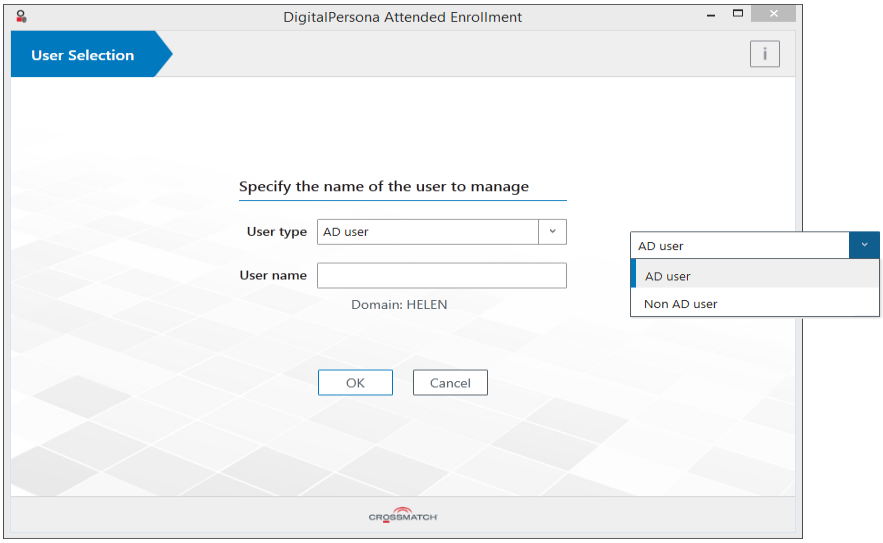
1. On the *User selection* page, select *Non AD* from the dropdown list.
2. Enter a unique user name and click *OK*.
3. If there is no DigitalPersona record for that user name, you can create a new DigitalPersona Non AD user.
4. Click *CREATE NEW>>*.
5. Have the new user enter and confirm a password.
6. Click *Create*.
7. On the *User creation* page, have the new user enter and confirm a DigitalPersona password. Then click *OK*.
8. The *Credential Enrollment* page displays. Credential Enrollment is described beginning on page 89.



AD User selection

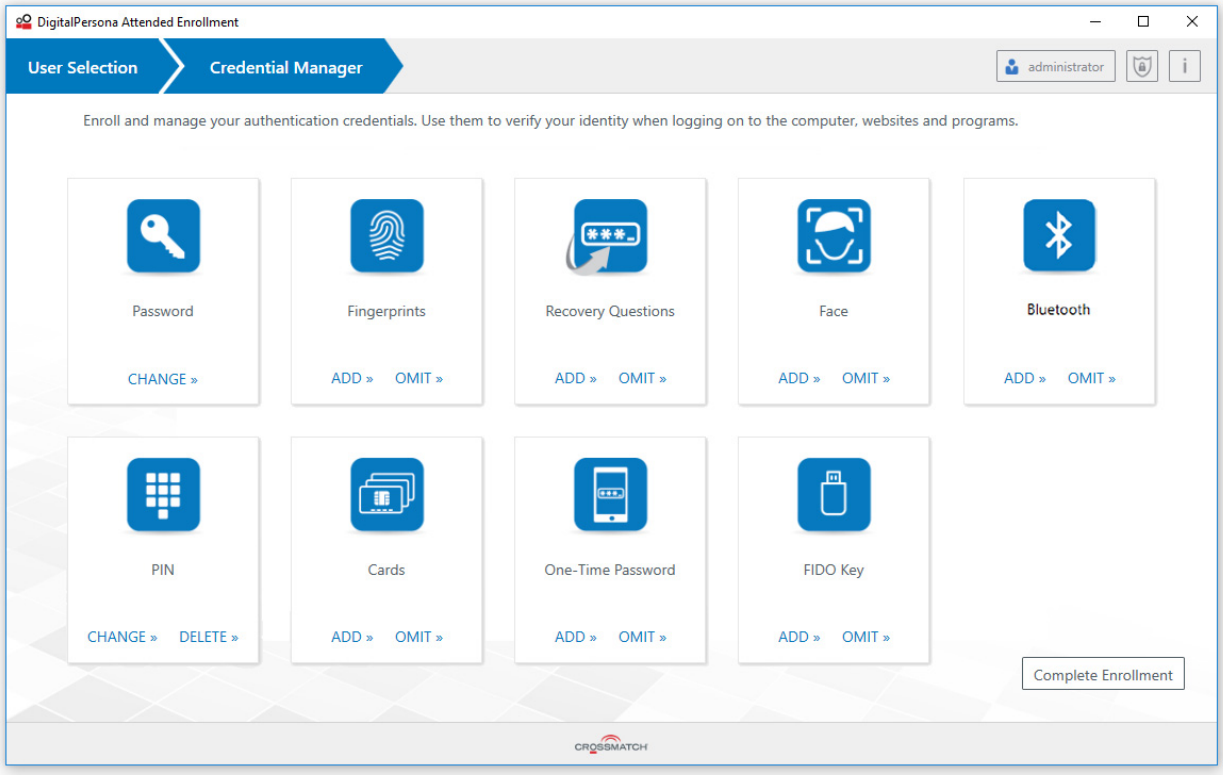
To select an AD user for Attended Enrollment

- (DigitalPersona LDS configuration only) On the *User selection* page, select *AD user* from the dropdown list.
- On the *User selection* page, enter the name of the AD (Windows) user that you want to enroll credentials for, and click *OK*.



Credential enrollment

Once a user is selected, the *Credential enrollment* page displays.



This is the central location within Attended Enrollment where a user's credentials and other identifying information can be enrolled and managed. The Credential Enrollment workflow is the same for both DigitalPersona AD and Non AD users, but the UI and the user experience is different depending on whether a single print fingerprint reader or a ten print scanner is being used for enrollment.

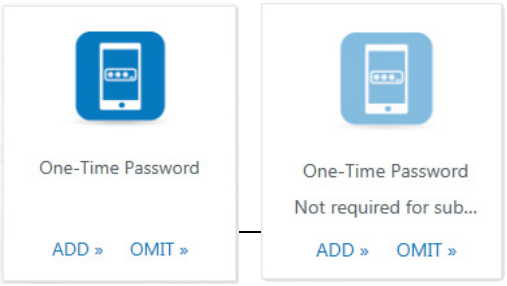
Note that during enrollment, a user's Bluetooth credential will be paired with the machine where attended enrollment is taking place. Supervisors should ensure that the user's device is then unpaired from the attended enrollment machine, since only seven devices can be paired to a single machine per the Bluetooth standard. In practice, usually no more than three or four are recommended. Users will need to pair their Bluetooth device with any computer where they will be using it as a credential

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.

The DigitalPersona administrator can configure which specific tiles appear on the page, and whether or not they must all be enrolled or omitted before enrollment is complete (see Customizing Attended Enrollment on page 112).

By default, in order to complete the initial enrollment for a user, all tiles shown on the page must be visited, and credentials either added (enrolled) or specifically omitted. When information is omitted, the Security Officer must enter a reason for the omission, which is then made part of the user record in the DigitalPersona database. The first portion of the omitted reason will also display on the tile.

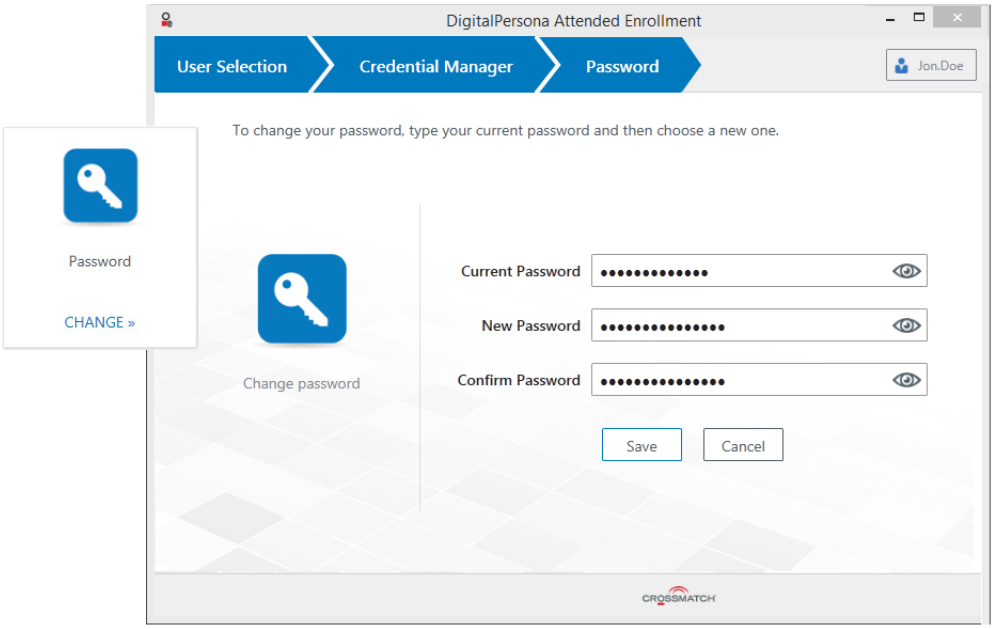
Once a credential has been enrolled, the word ADD will be replaced with CHANGE. When a tile has been marked as omitted, that tile will be dimmed.



Password credential

The Password credential is automatically enrolled for DigitalPersona Non AD users during the initial creation of the user. For AD users, the Password Credential is part of their Active Directory profile.

The Password tile provides a means to change the user's password, by entering their current password, and then entering and confirming a new password.

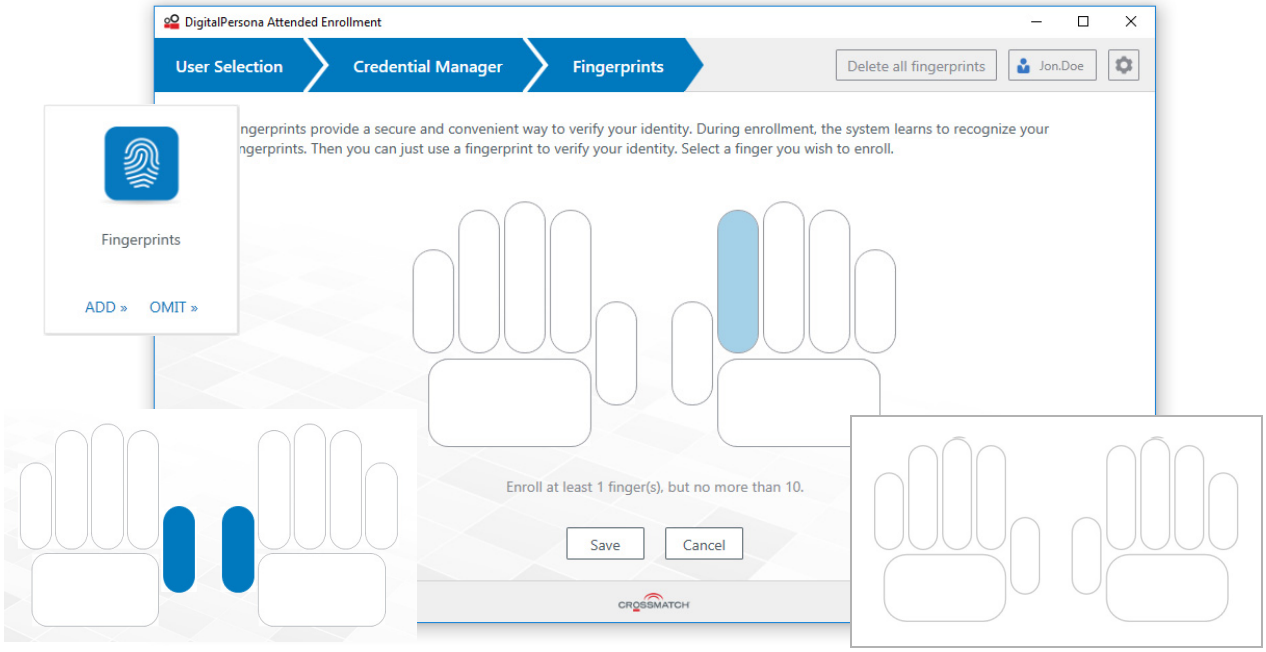


Fingerprints credential

If there is a supported fingerprint reader or ten-print scanner built into or connected to your computer, you can enroll and manage a user's fingerprints. Select the Fingerprints tile to display the Fingerprints page, where you can enroll a user's fingerprints credential.

The process of enrolling a user's fingerprints is slightly different depending on whether you are using a single print fingerprint reader, or a ten-print fingerprint scanner such as one of the HID Guardian products.

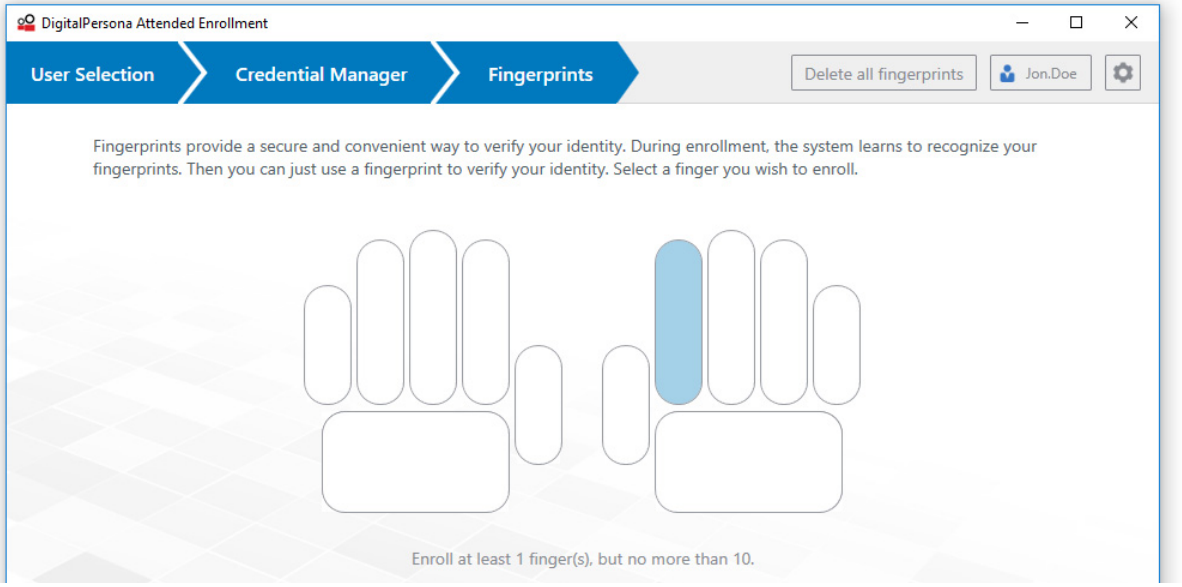
See the following two sections for descriptions of the steps for each of the hardware devices.



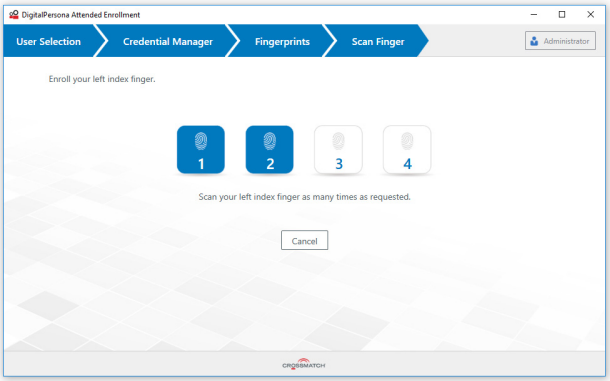
Enrolling fingerprints with a single finger reader

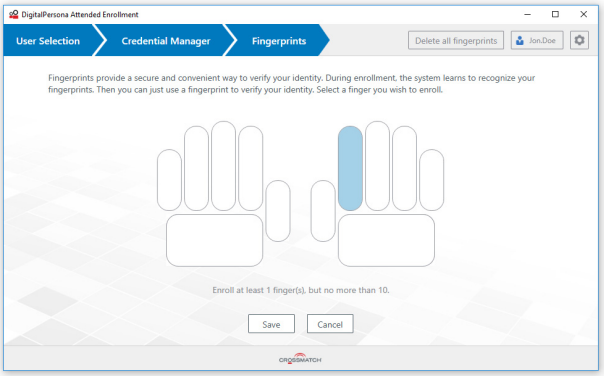
To enroll a fingerprint

1. Click the *Fingerprints* tile to display the *Fingerprints* pages.
2. Click on a finger in the displayed hand image.



3. Scan the selected finger as many times as requested to enroll the fingerprint.



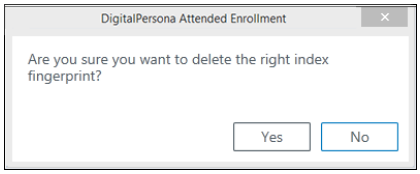


4. When an adequate number of images have been captured, the page will close and the Credential Manager page will redisplay with the newly enrolled finger highlighted.

5. Click *Save*. 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.*

Note that fingerprint enrollment is not complete until you click *Save*. If you leave the computer inactive for a while without clicking *Save*, or close the program, any changes will not be saved.

To delete a fingerprint, click any highlighted finger and confirm the deletion by clicking *Yes*.



To delete the entire fingerprint credential

1. In the upper-right portion of the page, click the *Delete all fingerprints* button.

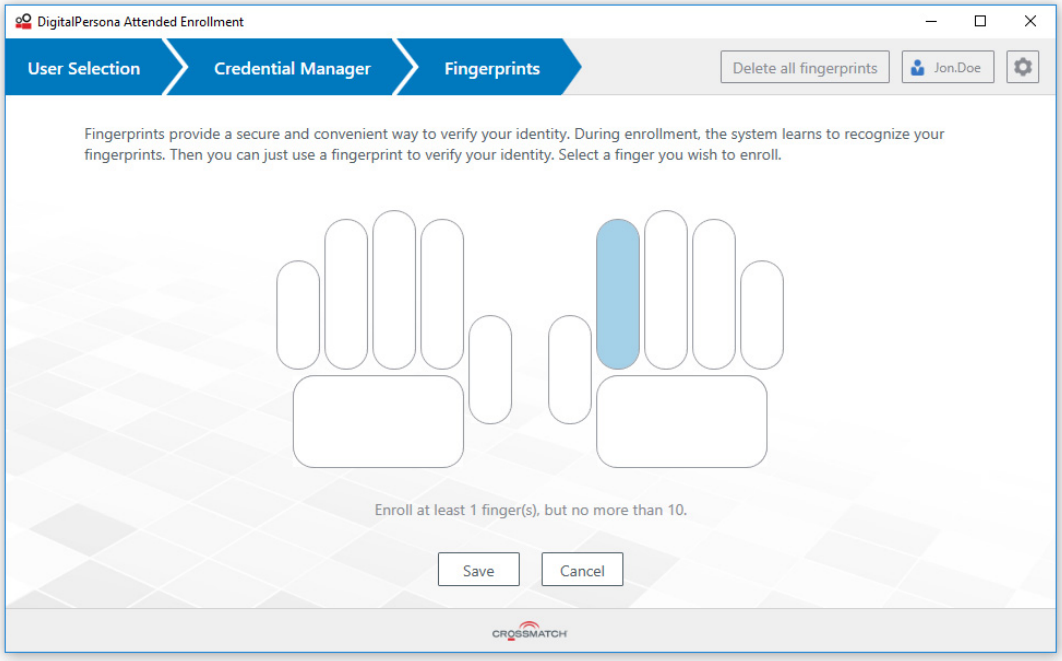
2. In the confirmation dialog, click *Delete* to confirm the deletion.

Enrolling fingerprints with a ten-print scanner

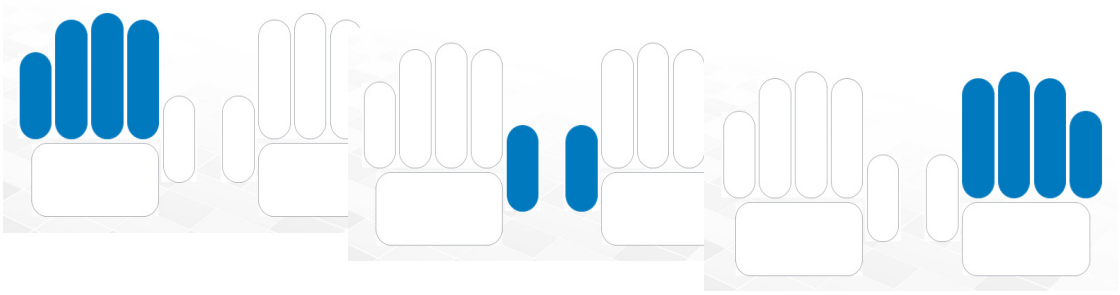
For a list of supported ten-print scanners, see the readme.txt file included with this software package. Additional files may need to be installed before use. See the *Optional installations* chapter of the DigitalPersona AD or DigitalPersona LDS Administrator Guide for further details.

The ten-print scanner captures fingerprints in three segments, often described as 4-4-2; that is four fingers of the left hand, four fingers of the right hand, and the two thumbs together.

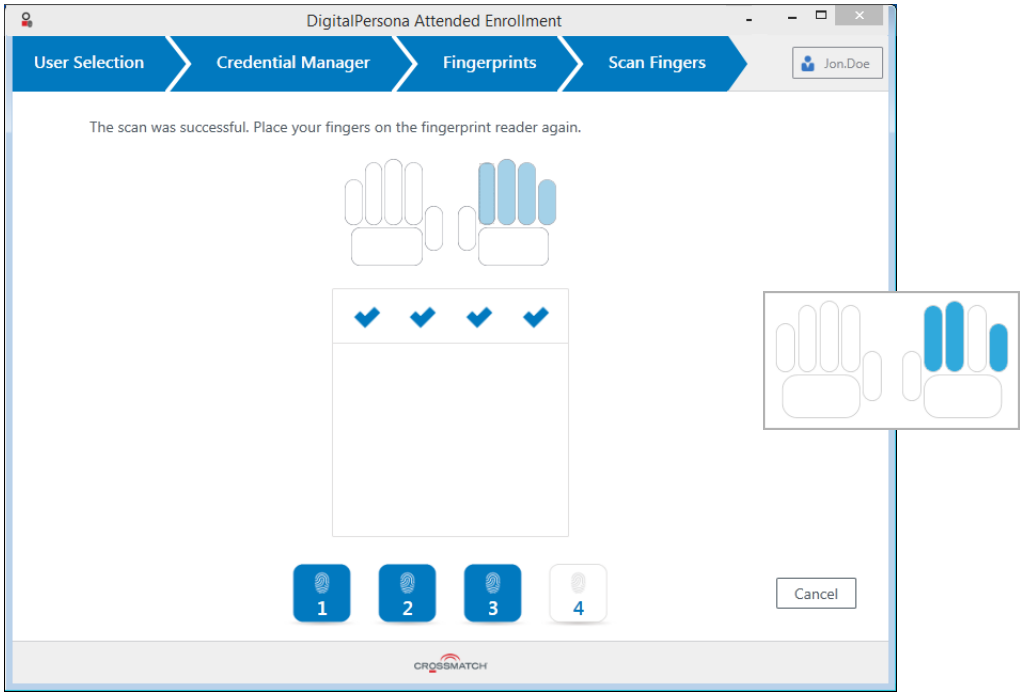
1. Click the *Fingerprints* tile to display the Fingerprints pages.



2. Select which segment to enroll. In the displayed image, choose the left hand, both thumbs or the right hand.

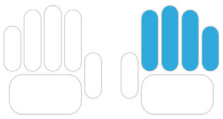


3. On the *Scan Fingers* page, if the user is missing any fingers, click the associated finger to remove it from the scan. Then scan the specified fingers or thumbs as many times as requested to enroll them.



4. Each successful scan will result in one of the scan numbers at the bottom of the window turning blue.

5. When enrollment of the segment is complete, the screen shows the fingerprint segment in a darker blue.



6. Select another segment until the fingerprints of both hands and thumbs have been captured.
7. Click *Save*. 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.*

Note that fingerprint enrollment is not complete until you click *Save*. If you leave the computer inactive for a while without clicking *Save*, or close the program, any changes will not be saved.

To delete a partial fingerprint segment

1. Select a previously enrolled segment.
2. Then confirm the deletion.

To delete the entire fingerprint credential

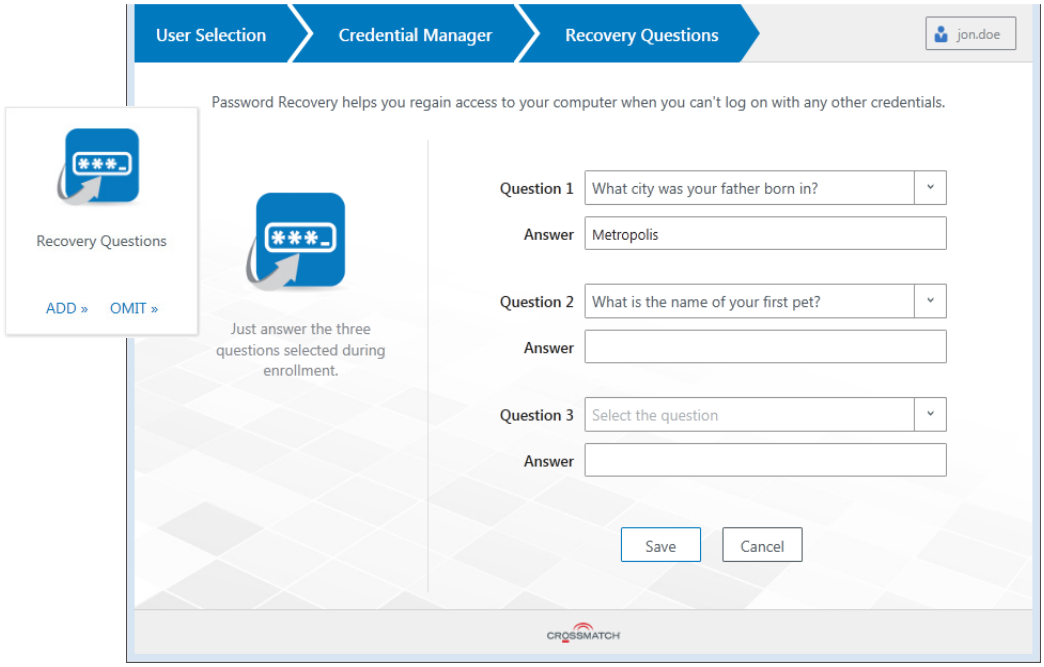
1. In the upper-right portion of the page, click the *Delete all fingerprints* button.
2. In the confirmation dialog, click *Delete* to confirm the deletion.

Authentication with a ten-print scanner

To authenticate with the ten-print scanner, use only a single finger or thumb. Use only the front half of the scanner screen to scan the fingerprint.

Recovery Questions credential

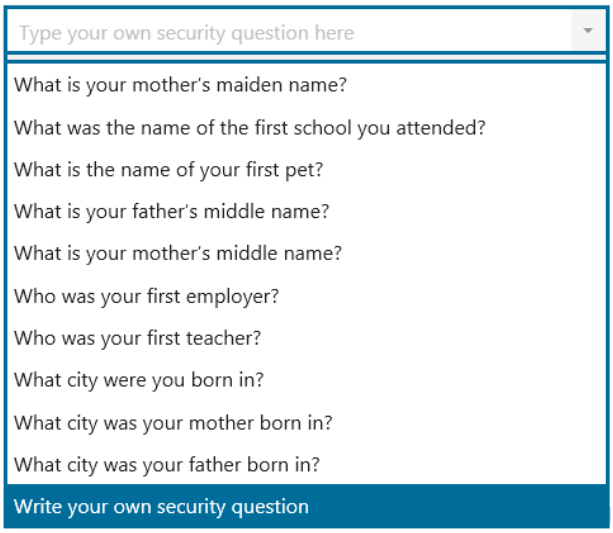
The Recovery Questions credential allows the user to regain access to their Windows account by answering a series a questions that have been previously configured. The Recovery Questions page provides a means to set up a user's Recovery Questions.



To set up a user's Recovery Questions

1. Click the Recovery Questions tile to display the Recovery Questions page.

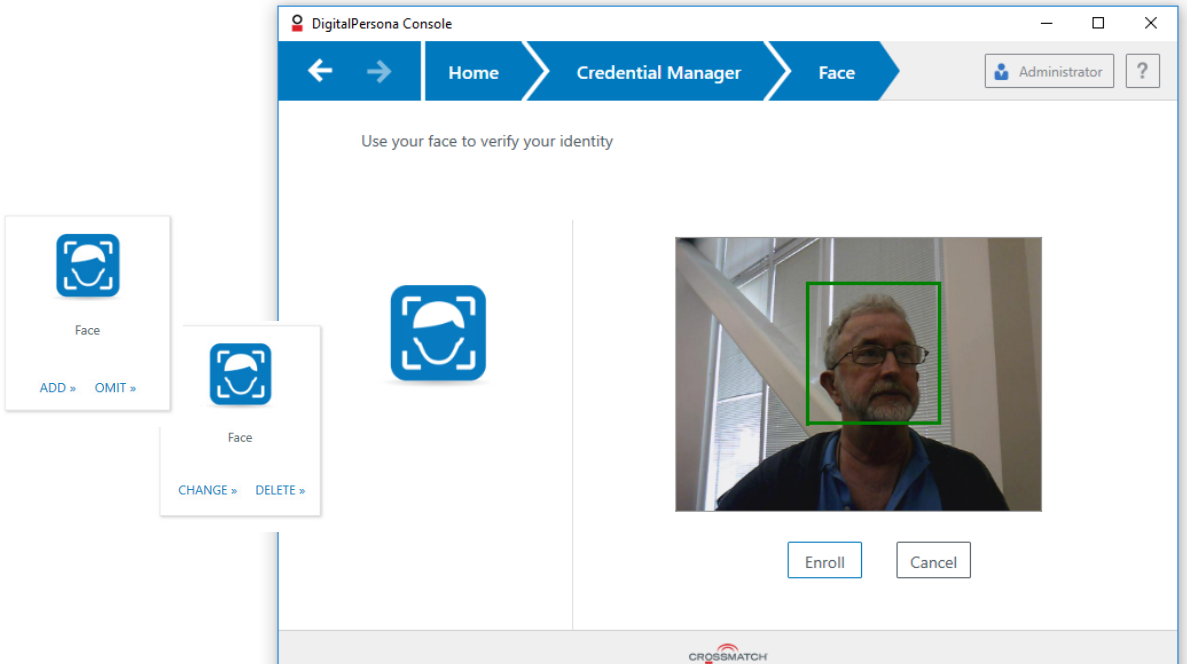
2. The user selects their questions from those available from the dropdown menus, and enters their unique answers. They can also write their own security questions by selecting the last option.



3. Click *Save*.

Face credential

The *Face* page enables you to enroll and manage your Face credential.



Your computer must have a built-in or connected camera to enroll a Face credential.

To enroll a Face credential

1. From the DigitalPersona Console, click *Credential Manager*, and then click the *Face* tile to display the *Face* page.
2. If multiple cameras are available, select a camera from the dropdown list.

3. Center your face within the frame and click *Enroll*.
4. A green rectangle will display around your face in the camera image.
5. Once enrollment is complete, the screen will refresh and display the nine separate frames used in enrolling your Face credential.

To change your Face credential

1. Once a Face credential has been enrolled, the word *CHANGE* appears below the credential's tile.
2. Click *CHANGE* to display the *Face* page.
3. Click *Re-Enroll*.

To delete your Face credential

1. Click *CHANGE* to display the *Face* page.
2. In the upper right setion of the page, click *Delete Credential*.

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.

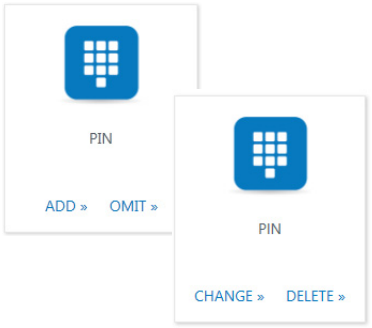
Authentication with your Face credential

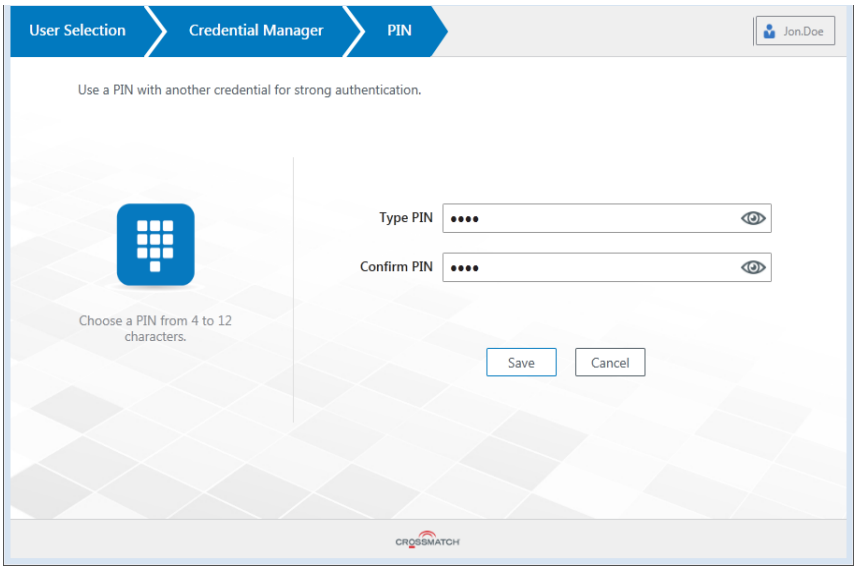
To authenticate using your Face credential

1. Do one of the following, depending on where you are authenticating from.
   - At Windows logon, select *Sign-in options* and then select the *Face* tile. If authentication is successful, you will be logged in to Windows.
   - On any *Verify your Identity* screen, select the *Face* tile.

PIN credential

This tile provides a means for enrolling a user's PIN credential.



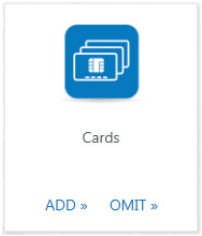


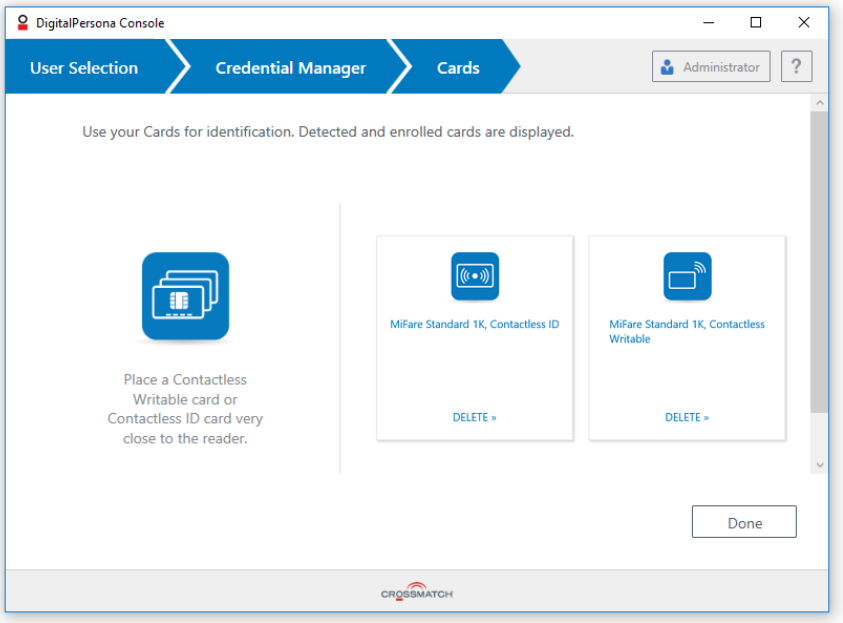
To enroll a PIN credential

1. Click the PIN tile to display the PIN page.
2. Enter and confirm a PIN. The system default requires a PIN between four and twelve alphanumeric characters, however the minimum and maximum PIN length may be specified through a GPO setting by the DigitalPersona administrator.
3. Click *Save*.

Cards credential

This tile provides a means for enrolling a user's Contactless Card credential.





To enroll a card credential

1. On the DigitalPersona Console Home page, click the Cards tile to display the Cards page.
2. Place the Contactless card very close to the reader and click *ENROLL*.
3. The *CHANGE* button displays on the Cards tile after the first card has been enrolled and saved.
4. Click *Done* to return to the Credential Manager page.

To delete a card credential

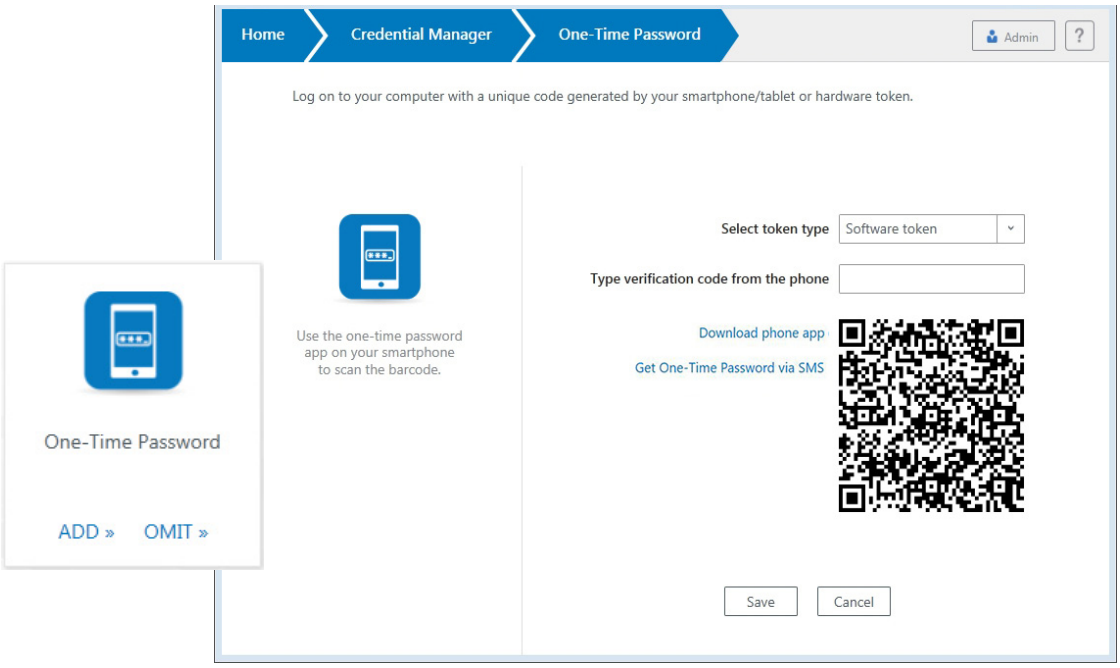
1. On the DigitalPersona Console Home page, click the Cards tile to display the Cards page.
2. Click *Delete* on the specific card image.
3. Click *Done* to return to the Credential Manager page.

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 at Windows logon and within a Windows session as defined by the Logon or Session Policy in force, as well as for DigitalPersona Password Manager trained applications, websites or network resources and SAML-compliant portals such as Office 365.

It also can be used for authentication to the DigitalPersona Identity Server, providing access to the DigitalPersona Administration Console, DigitalPersona Web Enrollment and the DigitalPersona Application Portal, as well as for verifying one's identity within Web Enrollment 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 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 that 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 your organization in the CPNS service.
- The associated OTP GPO settings have been enabled and configured by a DigitalPersona administrator as described beginning in the *Policies and Settings* chapter of the DigitalPersona Administrator Guide.
- Each user must allow notification during the app installation, or enable notifications for the DigitalPersona app in *Settings/Notifications/DigitalPersona* after installation.

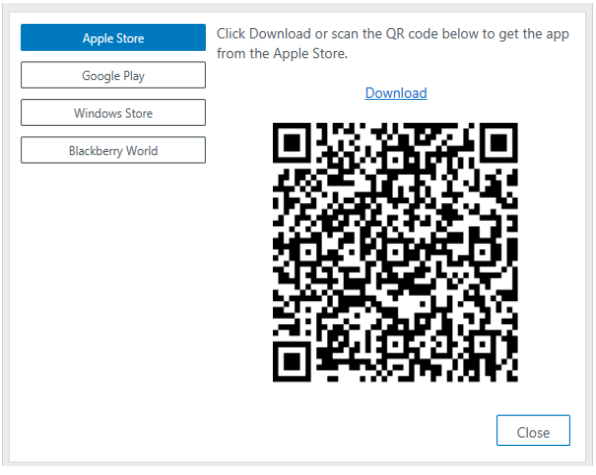
During enrollment, you may choose *not* to use OTP Push Notification by selecting *Decline* on the *Push Authentication* page, in which case, you can still use regular (non-push) OTP.

WARNING: *If you do not select ACCEPT on the Push Notification page, Push Notification will not be enabled. If you want to enable it in the future, you can do so by navigating to the DigitalPersona App in Settings/Notifications on your iOS device or the equivalent location on your Android device,*

On the Credential Manager, One-Time Password page, you can download an OTP authentication app, and then enroll the OTP credential for use with the authenticator app and OTP Push Notification (if configured).

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 DigitalPersona Console, click *Credential Manager*, and then click the *One-Time Password* tile.
2. On the *One-Time Password* page, select *Software token* as the token type if it is not already selected. (It is the default.)
3. Click the *Download phone app* link to display a dialog where you can download and install the authenticator app for your device.
4. 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 and Blackberry mobile platforms, the Microsoft and Google *Authenticator* apps provide nearly identical functionality, although setup and enrollment steps may vary slightly.

5. 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.

6. Clicking the Download link 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

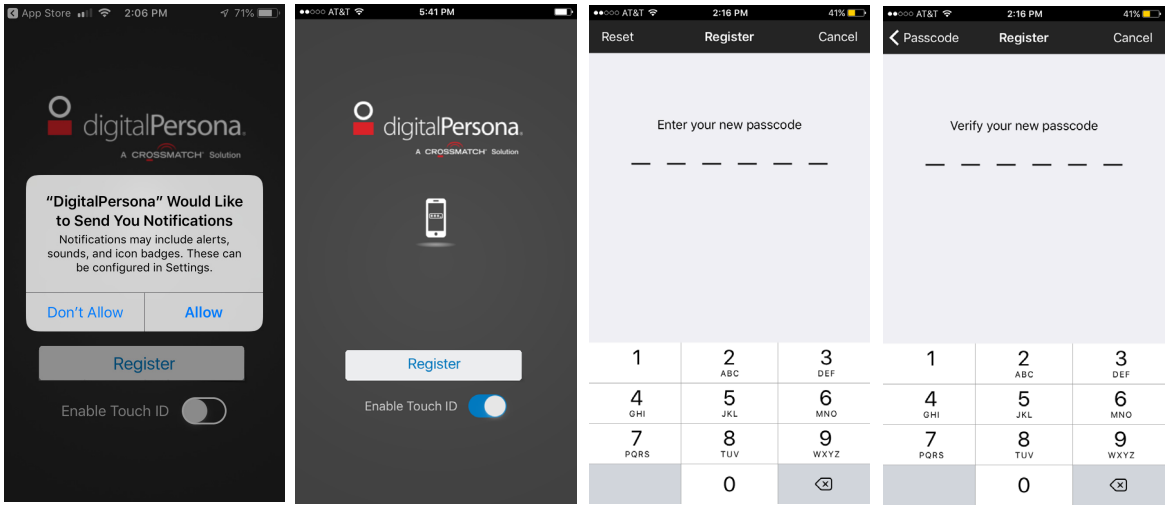
1. Launch the DigitalPersona mobile app on your device.

2. On iOS - The first time the app is launched, the *Register* screen displays, with a popup dialog requesting you to allow the app to send you notifications. Click *OK* to allow DigitalPersona Mobile to send you notifications. Note that if you do not allow notifications, you will not be able to use the PUSH notification feature for One Touch Passwords.

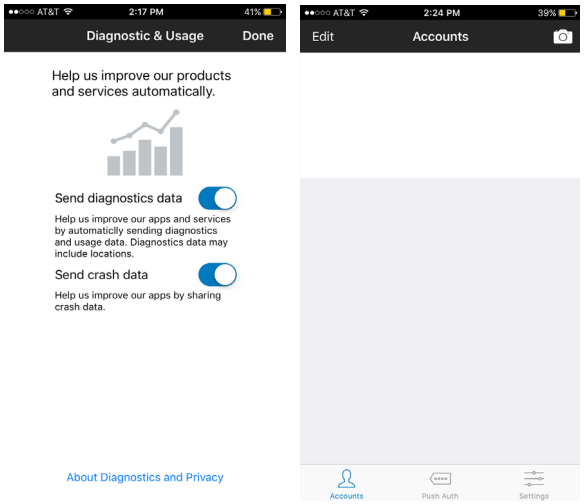
3. On Android systems - The first time the app is launched, the *Register* screen displays. Notifications are enabled by default for the app, and therefore PUSH OTP will be operational (if the Privacy Policy is accepted as described below).

4. Click *Register*.

5. Enter and verify a six-digit passcode.



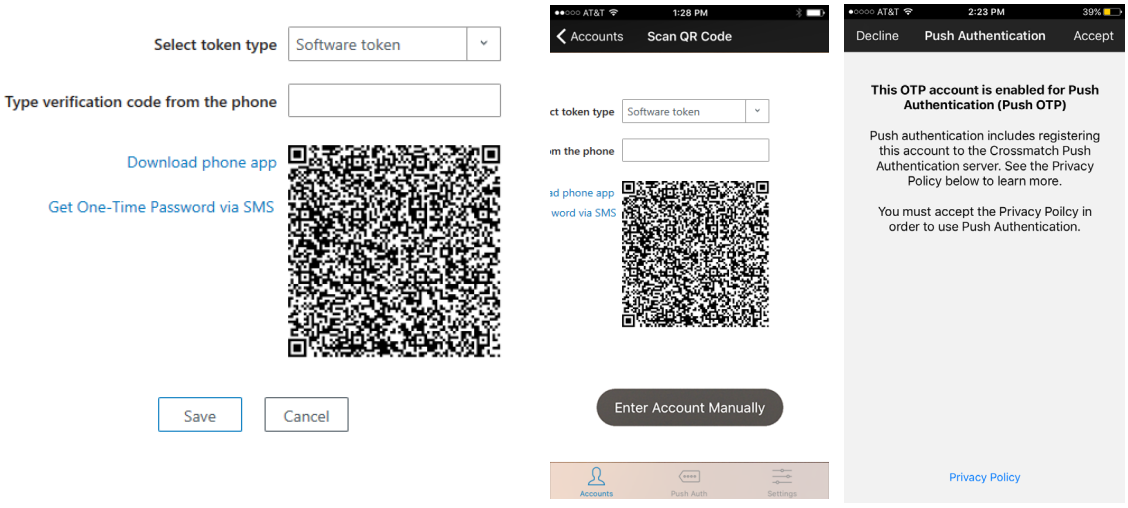
6. On the Diagnostic and Usage page, accept the defaults or tap an option to deselect it.



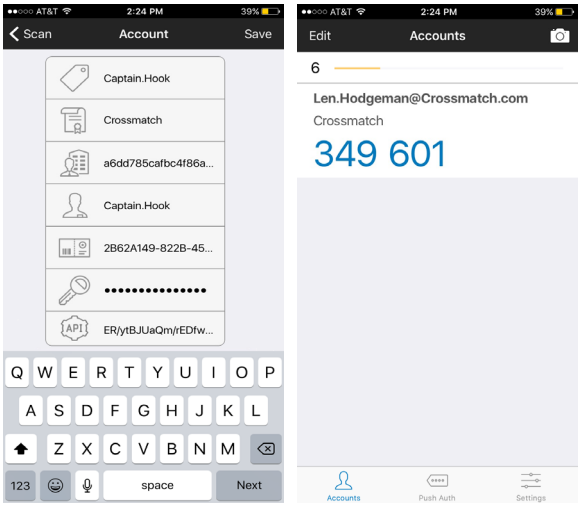
7. On the *Accounts* screen, click the Camera icon. You will be asked for permission to access your device's camera. Tap *OK* if you want to use the camera to scan the QR Code for automatically creating your DigitalPersona Mobile account. If you click *Don't Allow*, you will not be able to create an account or use the Authenticator app.

8. On the *Scan QR Code* screen, scan the QR code that displays on the One-Time Password Page. Do not scan the same QR code again from the dialog that has the app stores on it which was used to download the app.

9. If the Crossmatch Push Authentication Server has been previously setup by your DigitalPersona Administrator, Push Authentication will be automatically enabled for your device once you choose to *Accept* the associated Privacy Policy. If you choose to *Decline* the Privacy Policy, Push Authentication will not be enabled.



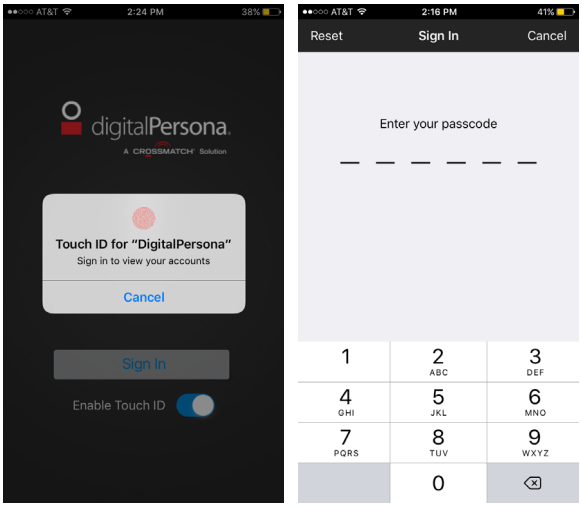
- Once the account information is displayed, tap *Save*. The DigitalPersona Mobile account will be created and the *Accounts* screen displayed with the new account and your first One-Time Password shown.



Manual account creation

This feature is reserved for use by DigitalPersona technicians.

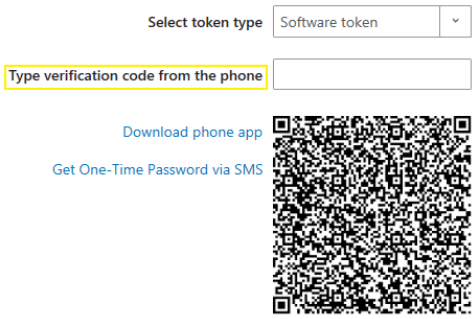
Sign in to the DigitalPersona Mobile app



Once you have registered as described in the previous pages, you can sign in to the app as follows.

1. Launch the DigitalPersona Mobile 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

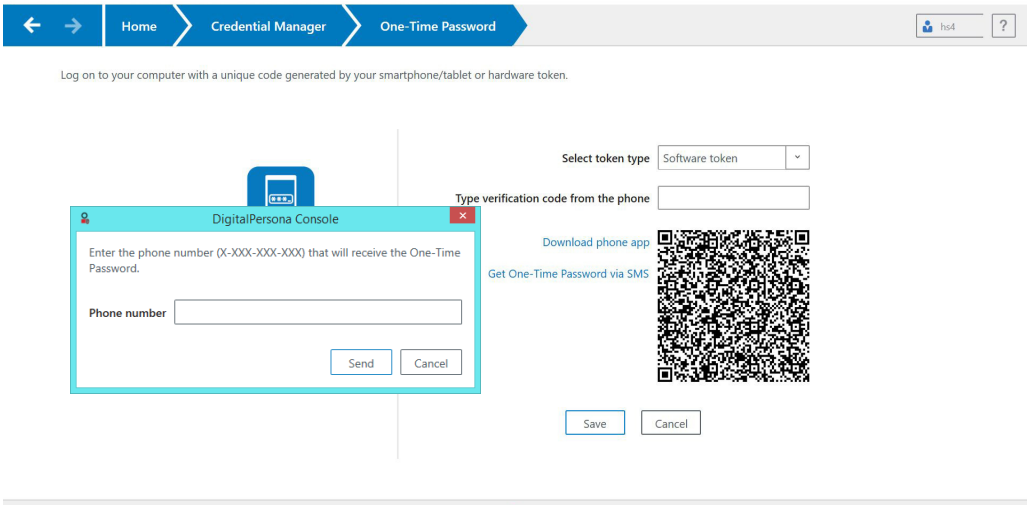


1. On your computer, open the One-Time Password page.
2. On your device, sign in to the DigitalPersona Mobile app.
3. On your computer, enter the six-digit verification code displayed in the app and click *Save*.

OTP for SMS delivery

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.

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.

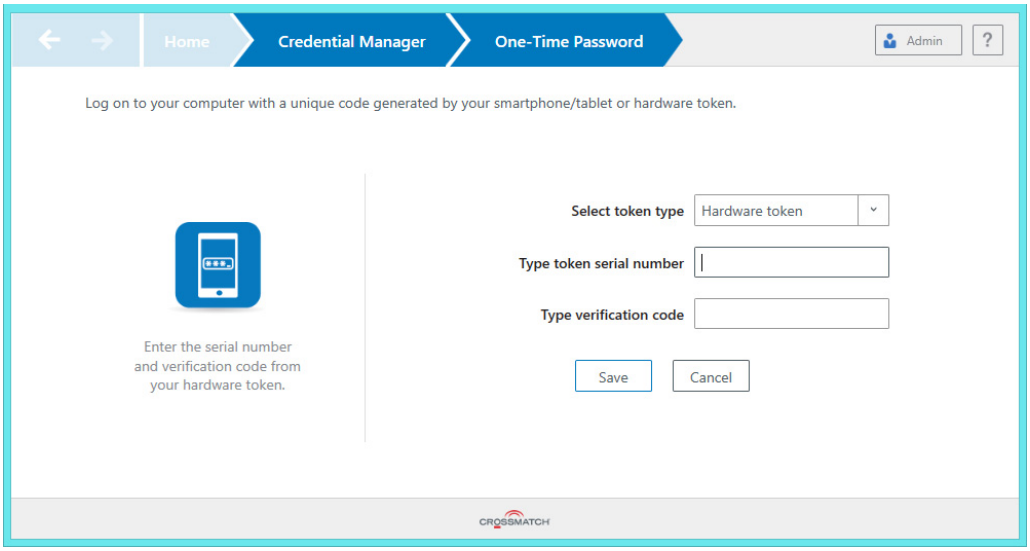


To enroll the OTP via SMS credential

1. On the One-Time Password page, click the *Get One-Time Password via SMS* link.
2. Enter the number for the mobile device that you would like to enroll in order to receive a One-Time Password through SMS delivery.
3. Click *Send*.
4. You will receive an SMS message on your mobile device containing a six-digit verification code.
5. On your computer, enter the verification code into the *Type verification code from the phone* field.
6. The *Credential Manager* page will re-display and the One-Time Password tile will now show the *Change* caption, indicating that a One-Time Password credential has been enrolled.

OTP hardware token

On the Credential Manager, One-Time Password page, you can enroll a hardware token as an 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.



Typical hardware tokens

To enroll an OTP credential using a hardware token

1. From the DigitalPersona Console, click *Credential Manager*, click the *One-Time Password* tile and, from the *Select token type* dropdown list, select *Hardware token*.
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 the *Administration Overview* chapter of the DigitalPersona AD Administrator Guide or in the *Administration Tools* chapter of the DigitalPersona LDS 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

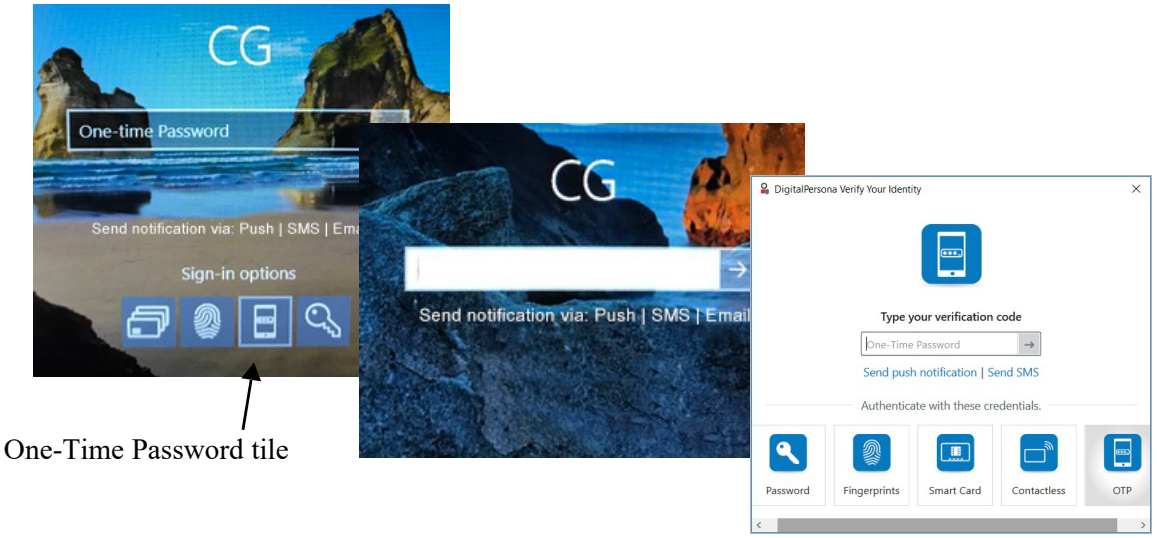
(For AD Users only) If enabled by the administrator through the associated *Allow sending OTP code by email* GPO, the option to have a One-Time Password sent to the user's email address is automatically available (enrolled) upon completing the enrollment of any of the other types of OTP credentials described 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

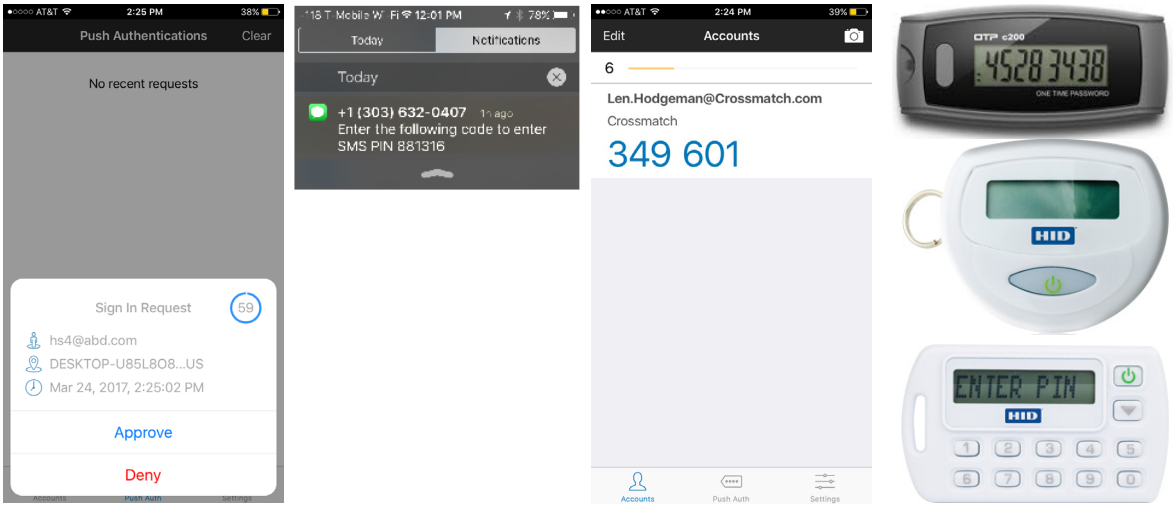
1. Do one of the following, depending on where you are authenticating from.
   - At Windows logon, select *Sign-in options* and *then* select the *One-Time Password* (or OTP) tile to display *One-Time Password* options.
   - On any *Verify your Identity* screen, select the *One-Time Password* (or OTP) tile.



One-Time Password tile

2. You can use an OTP credential in any of the following ways.
   - Select *Send push notification* to send a notification to your enrolled mobile device allowing you to Approve or Deny authentication.
   - Select *Send SMS with OTP code* to send an SMS message to your enrolled mobile device with a verification code that you can enter on your computer for authentication.
   - Launch your previously registered authentication app on your mobile device and enter the resulting verification code into the entry field on your computer.

- Activate the display on an enrolled hardware token, and enter the displayed verification code on your computer.



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 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.

To delete your OTP credential

1. Once the credential has been enrolled, the word *DELETE* will display beneath the OTP tile.
2. On the Credential Manager page, click *DELETE*.
3. Confirm the deletion.

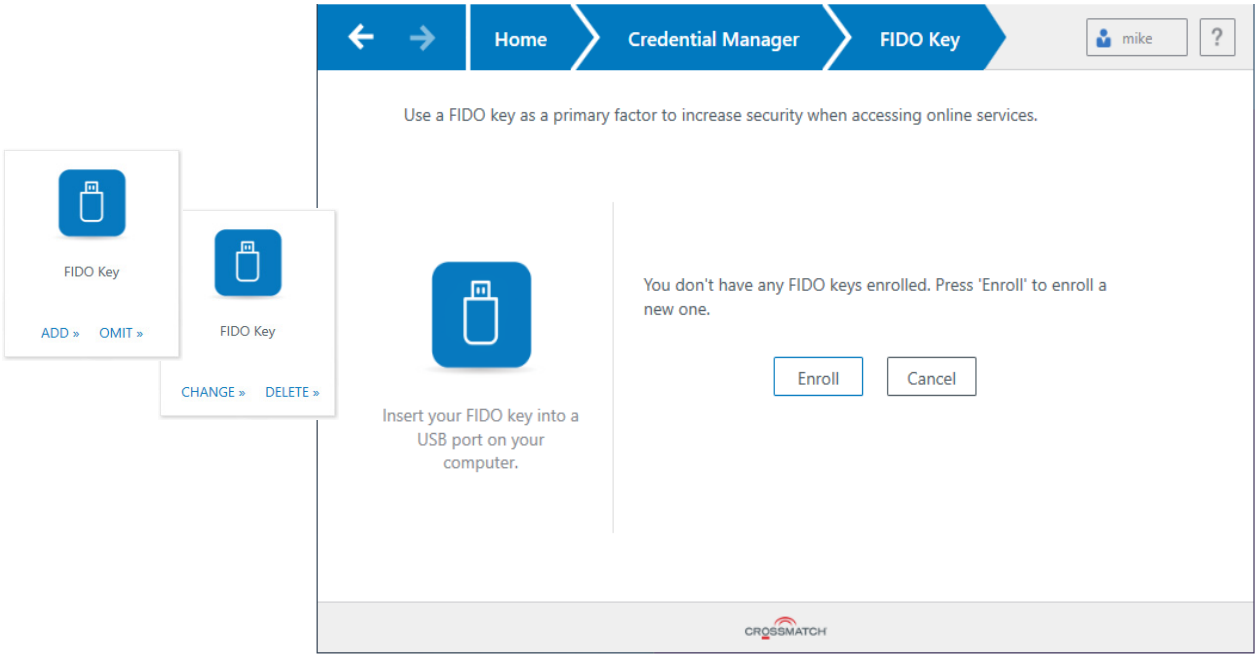
FIDO Key credential

The FIDO Key credential uses a FIDO USB key for authentication. The FIDO Key page is where FIDO keys are enrolled and managed.

IMPORTANT: If FIDO Keys will be used with DigitalPersona Web Components, i.e. Identity Provider, Web Administration Console or Web Enrollment, they should be enrolled through Web Enrollment, and not through the DigitalPersona Workstation User Console. FIDO Keys enrolled through the User Console will not work with DigitalPersona's Web Components.

To enroll or manage a FIDO Key credential

1. In the *Credential Manager*, click *ADD or CHANGE* on the FIDO Key tile.
2. The FIDO Key page displays.



To enroll a FIDO key as a DigitalPersona credential

1. Click *ADD*.
2. On the FIDO Key page, insert a FIDO key into an available USB port and choose *Enroll*.
3. Depending on the type of FIDO key being used, activate it through one of the following actions.
   - Tap the sensor on the device.
   - Press a button on the device.
   - Remove and reinsert the device.

To change the FIDO key being used as a credential

1. Choose *CHANGE* on the FIDO Key tile.
2. On the *FIDO Key* page, select *Re-Enroll*.
3. Tap, press the button on, or re-insert your FIDO key.

Upon successful enrollment, the *Credential Manager* page redisplays.

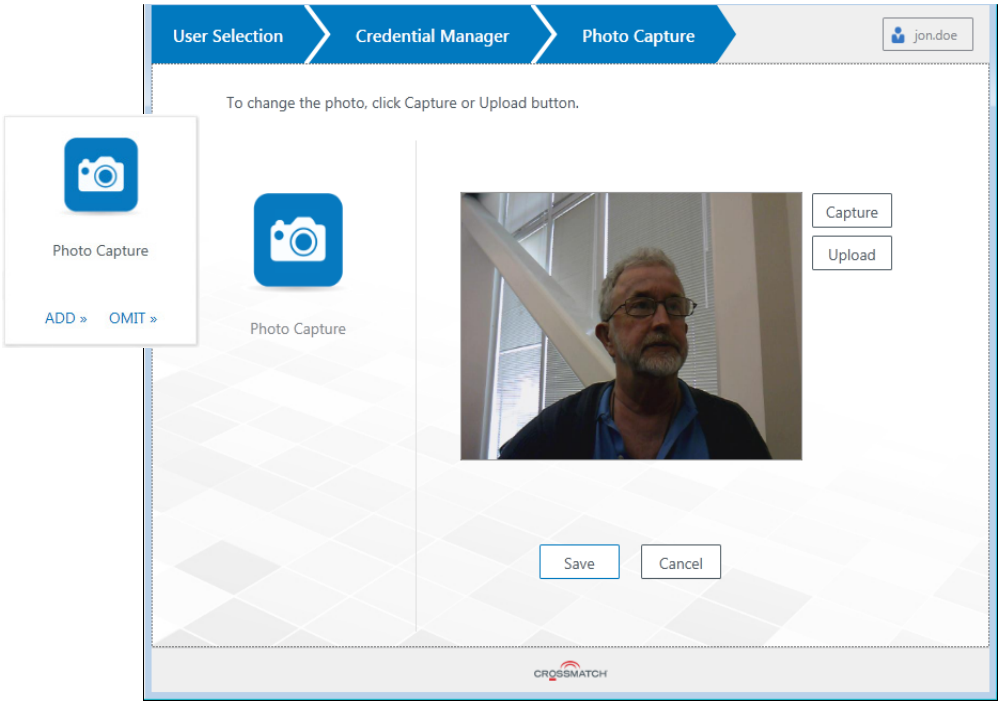
To delete this credential

1. Choose *CHANGE* on the FIDO Key tile.
2. On the *FIDO Key* page, in the upper right, click *Delete Credential*. In the confirmation dialog, click *Delete*.

Photo Capture (DigitalPersona LDS, Non AD user only)

This tile provides a means for taking a photograph of the user. Note that this photograph is for visual identification only and is not a DigitalPersona credential. It cannot be used for verifying your identity when authentication is required for login to Windows, websites or programs.

By default, this page is not available for DigitalPersona AD users and as designed, will not store photos for AD users.



To add a photograph of the user to their account information

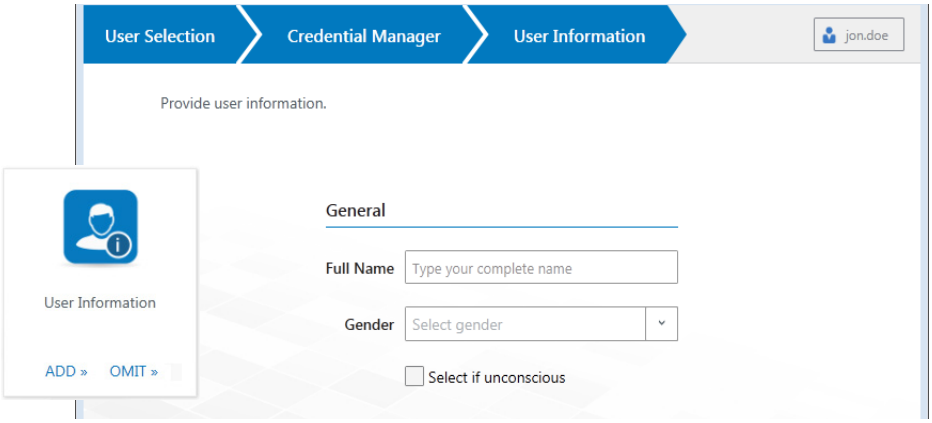
1. Position the user in front of the camera.
2. Click *Capture* to take a photo with a connected camera, or *Upload* to select a photo from your computer or other resource. Then click *Save*.

User Information/Custom page (Non AD User only)

This tile and its associated page provide a means for capturing additional customized information about users (or anything else) during the Attended Enrollment session. By default, this page is not shown, but may be enabled in the *DigitalPersona.Altus.Enrollment.exe.config* file. Note that this option only applies to Non-AD users.

Note that changes made to the *Custom page definition* and any sections of this file other than the *enrollmentConfiguration section* may require updating the DigitalPersona LDS instance schema and could cause the

program to malfunction. We recommend contacting the *HID Global Solutions and Implementation Group* for assistance in creating custom pages.



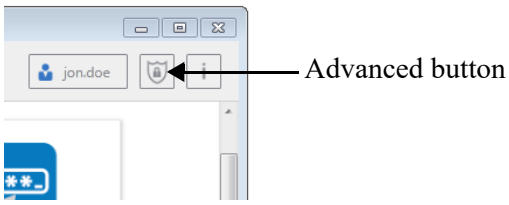
Completing enrollment

By default, all displayed tiles must be either enrolled or omitted, before clicking *Complete enrollment.* This behavior can be changed in the *DigitalPersona.Altus.Enrollment.exe.config* file mentioned above.

Once completed, the program returns to the *User selection* page.

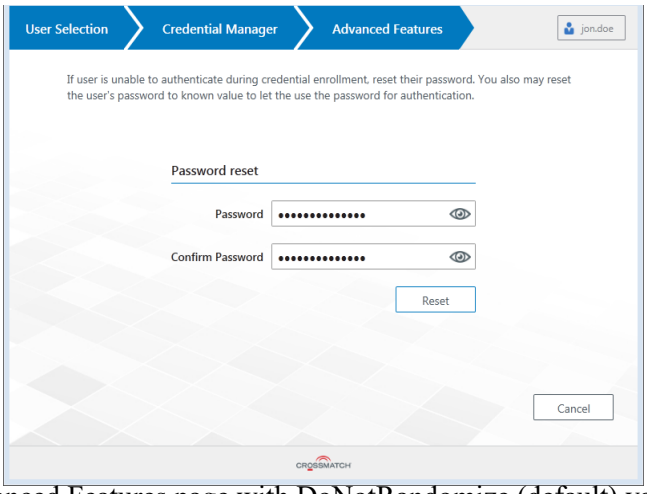
Advanced Features

The DigitalPersona Advanced Features page can be accessed by clicking the *Advanced* button on the *Credential Enrollment* page.

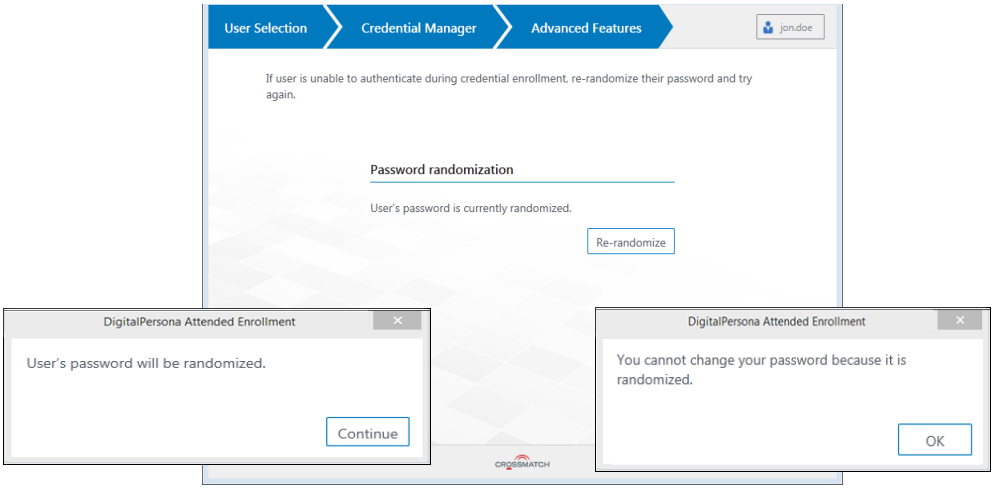


The DigitalPersona Advanced Features page displays.

The behavior of the page will vary depending on the value of the *PasswordRandomization* tag in the file, *DigitalPersona.Altus.Enrollment.exe.config*. The page variations shown below illustrate the changes in the page depending on the value of the tag.

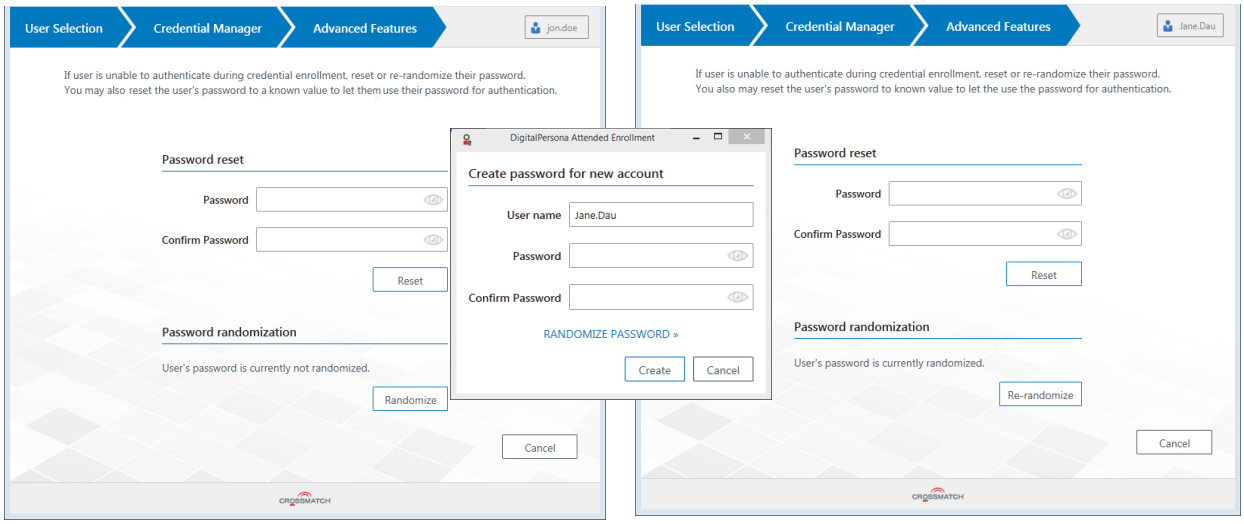


Advanced Features page with DoNotRandomize (default) value s



Advanced Features page with RandomizeAlways value set in

When the value is set to RandomizeAlways, the two additional messages are added to the workflow as shown above. The first message displays when beginning to create or edit a user, and the second message displays when clicking on the Password tile.



Advanced Features page and user creation window with the MayRandomize value set in the configuration file

When the value is set to MayRandomize, the choice to randomize a password is shown when creating a new DigitalPersona Non AD user, and the Advanced Features page provides a means to reset the user's password if not randomized, or re-randomize it if currently randomized.

Customizing Attended Enrollment

Note that this section is included in this guide for backward compatibility with previous versions. Use of the DigitalPersona.Altus.Enrollment.exe.config. for configuring Attended Enrollment is not recommended for versions 3.0.2 and above. For these later versions, the behavior of Attended Enrollment is governed by the following GPOs which are fully described in the Policies and Settings chapter of the DigitalPersona Administrative Guides.

- Policy Enrollment
- Authentication of the user being enrolled
- Security officer authentication
- Require to complete or omit credential

The workflow and UI behavior of Attended Enrollment can be customized significantly through the related configuration file, *DigitalPersona.Altus.Enrollment.exe.config*.

For convenience, all options are explained or briefly illustrated within the file itself. However, this section will provide more detailed explanations of the options.

The *enrollmentConfiguration* section of the file is the only area that should be modified.

Changes to the *Custom page definition* and other sections may cause the program to malfunction, and should only be done by the *HID Global Solutions and Implementation Group*.

passwordRandomization

This tag specifies whether the user's password is randomized during the enrollment process.

<passwordRandomization value="DoNotRandomize" /> <!--DoNotRandomize, RandomizeAlways, MayRandomize-->

The default is *DoNotRandomize*. Additional choices are *RandomizeAlways* and *MayRandomize*.

- DoNotRandomize - Password randomization is not available and the UI offers no option to randomize the user's password.
- RandomizeAlways - Password randomization always occurs, and the UI provides the option (on the Advanced Features page) to reset the user's password.
- MayRandomize - Password randomization is optional and the UI allows the administrator to choose whether to randomize the user's password for each user.

See the previous section, *Advanced Features*, for details on how this affects the Attended Enrollment UI and workflow.

completeAllPages

This tag determines whether or not all displayed credentials must be either enrolled or specifically omitted in order to complete enrollment.

<completeAllPages value="true" /> <!--true, false-->

The default is *true*. Additional choice is *false*.

authenticateOfficer... and authenticateUser

There are several tags defining workflow events that can be specified to require authentication by the DigitalPersona Security Officer or the user being enrolled. Default values are shown in the examples below, but if any of these tags are missing, the default for that tag is *true*.

- <authenticateOfficerOnStarted value="false" />

  Authenticate the Security Officer every time Attended Enrollment is launched.

- *<authenticateOfficerBeforeSave value="true" />*

  Authenticate the Security Officer each time a credential is saved or credential enrollment page is closed.

- *<authenticateOfficerBeforeSkip value="true" />*

  Authenticate the Security Officer at omitting user data, once every time a credential page is closed.

- *<authenticateOfficerBeforeDelete value="true" />*

  Authenticate Security Officer at deleting user data, once every time a credential page is closed or data is deleted.

- *<authenticateOfficerOnCompleted value="true" />*

  Authenticate Security Officer at completing user enrollment.

- *<authenticateUserOnPageEnter value="true" />*

  Authenticate the user once at opening each credential page.

- *<authenticateUserOnCompleted value="true" />*

  Authenticate the user at completing their enrollment.

authenticationPolicyForOfficer

This tag specifies the credentials and credential combinations required for authenticating the DigitalPersona Security Officer.

```
<authenticationPolicyForOfficer>
  <add value="1"/>        <!--Password-->
  <add value="2"/>        <!--Fingerprints-->
  <add value="Pin, Otp"/>  <!--Contactless Card-->
</authenticationPolicyForOfficer>
```

Valid values are:

1 - Password

2 - Fingerprint

4 - Smartcard

8 - RecoveryQuestions

32 - Contactless Card

64 - RecoveryPassword

128 - PIN

256 - Proximity

512 - Bluetooth

2048 - OTP-->

userTypes

This tag specifies the types of users to show in the UI, therefore making them available for Attended Enrollment.

```
<userTypes>
  <add value="AD"/>      <!--DigitalPersona AD (Windows) users-->
  <add value="Altus"/>   <!--DigitalPersona Non AD users-->
</userTypes>
```

The default is to show both types of user. To remove a user type, remove or comment out the associated line.

ExcludedNodes

This tag specifies the GUID for any tiles which should *not* be shown on the Attended Enrollment Credential Manager page, and therefore those associated credentials which will not be able to be enrolled through Attended Enrollment.

```
<excludedNodes>
  <add userType="AD" value="BCC6142F-CE8B-4B48-B605-342842B3DDDB"/> <!--Photo Capture->
  <add userType="AD" value="24FAC572-AE57-45E2-ACCF-4417A44A9F02"/> <!--Custom Page 1-->
</excludedNodes>
```

The above sample shows the default of not showing the tiles and pages for Photo Capture and Custom Page 1 when enrolling credentials for DigitalPersona AD users.

If tiles/pages should be excluded for both user types, use the *add* tag without the UserType parameter, as in the following example.

```
<excludedNodes>
    <add value="BCC6142F-CE8B-4B48-B605-342842B3DDDB"/>   <!--Photo Capture->
    <add value="24FAC572-AE57-45E2-ACCF-4417A44A9F02"/>   <!--Custom Page 1-->
</excludedNodes>
```

Values for the current set of DigitalPersona pages are as follows.

Password = "DE9F54BE-F6B9-4306-BC67-DDD71B27B35B"

Fingerprints = "CBFFA046-6267-4594-AB5C-11A7B5B97035"

Cards = "4FA5D027-18C9-4766-97B9-CE3C5962476F"

PIN = "B07C25CA-FE67-48F1-AC7D-3B204108F52C"

One-Time Password = "9AC39EB1-FCD3-4207-B98A-5B290B2AB8CA"

Recovery Questions = "A6421E1B-6E67-411B-ABBC-45AE4811E6C6"

Photo Capture = "BCC6142F-CE8B-4B48-B605-342842B3DDDB"

Custom page = "3B797E3F-08E8-44A0-ABF2-C136CC4EEA49"

Custom pages and DPLdif utilities

Changes to the *Custom page definition* section of the *DigitalPersona.Altus.Enrollment.exe.config* file may cause the program to malfunction, and should only be done by the *HID Global Solutions and Implementation Group*.

Elements used in the Custom page definition section must already exist in the DigitalPersona LDS database, or be added to the database using the *DPLdifUtilities.Builder.exe* and *DPLdifUtilities.Import.exe* server tools. These are located in your DigitalPersona LDS Server product package, in the *Server Tools* folder.

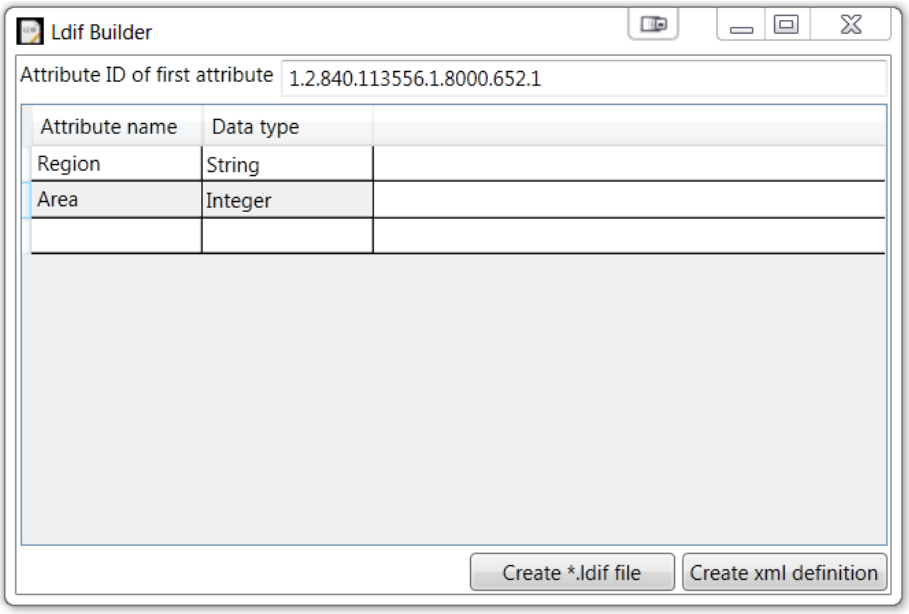
The *DPLdifUtilities.Builder.exe* tool can be run on any modern Windows computer. The *DPLdifUtilities.Import.exe* must be run on the DigitalPersona LDS Server.

The entire default text of the Custom page section is shown below. See the next two sections for instructions on using the server tools mentioned above.

```
<!--Custom page definition-->
<!-- Use the provided DPLdifUtilites.Builder tool to generate pieces of the XML below  -->
<!-- and the corresponding LDIF files for updating the Altus LDS database Schema. -->
<customPages xmlns="http://schemas.crossmatch.com/altus/2.0/custompage">
  <page id="24FAC572-AE57-45E2-ACCF-4417A44A9F02">
    <title>User Information</title>
    <description>Provide user information.</description>
    <fields>
      <group>
        <displayName>General</displayName>
        <fields>
          <text dataType="string" attributeName="givenName">
            <!--Editable string element type-->
            <displayName>Name</displayName>
            <prompt>type your name</prompt>
            <validation>
              <required>Required</required>
              <maxLength value="20">Too long</maxLength>
              <minLength value="2">Too short</minLength>
            </validation>
          </text>
          <dropdown dataType="string" attributeName="description">
            <!--Drop-down list element type-->
            <displayName>Gender</displayName>
            <prompt>select gender</prompt>
            <defaultValue>unknown</defaultValue>
            <isEditable>false</isEditable>
            <items>
              <item>male</item>
              <item>female</item>
              <item>unknown</item>
            </items>
          </dropdown>
          <check dataType="string" attributeName="company">
            <!--Checkbox list element type-->
            <displayName>Check if Crossmatch</displayName>
            <trueValue>Crossmatch, Inc</trueValue>
            <falseValue>DigitalPersona, Inc</falseValue>
          </check>
        </fields>
      </group>
    </fields>
  </page>
</customPages>
```

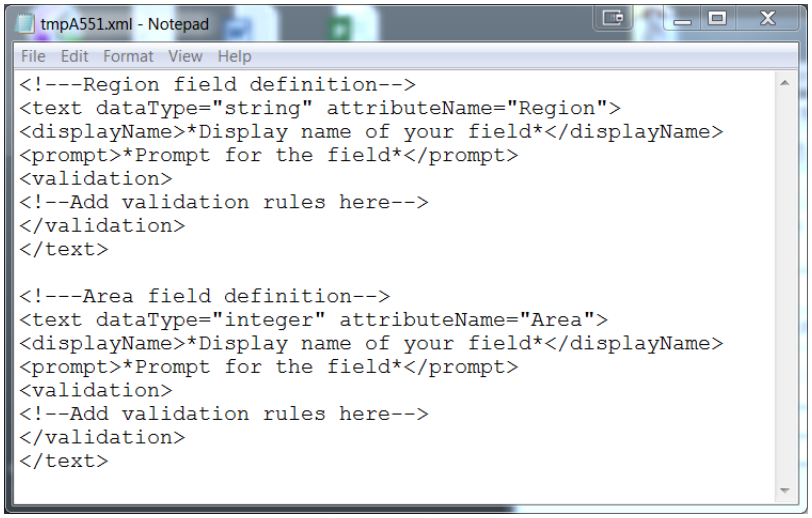
DPLdifUtilities.Builder.exe

The DPLdifUtilities.Builder tool provides a GUI-based way to generate the XML for adding new attributes to Attended Enrollment Custom pages, and for creating the LDAP Data Interchange Format (.ldif) file that can be used to add the attributes to the DigitalPersona LDS database.



To create new attributes

1. Enter a name for the new attribute.
2. Select a data type from the *Data Type* dropdown list.
3. Repeat steps 1 and 2 for each new attribute needed.
4. Click *Create xml definition*.
5. The necessary xml will be generated and opened in your default text reader (e.g. Notepad). Following the above example, it would look like the image below.



6. These generated attributes can be placed in the *DigitalPersona.Altus.Enrollment.exe.config* file, in the Custom page definition section, under the <Fields> node. Save the file, or copy the text directly into the configuration file.
7. The next step is to create the LDIF file that will be used to update the DigitalPersona LDS Server's database. Click the *Create the *.ldif file* button. Save the file to a location where you can copy it to your DigitalPersona LDS Server. You may want to rename it as well.
8. Once the associated LDIF file has been created and imported into the DigitalPersona LDS database (see next section), your new attributes and the fields they represent will be operational on the page.

To add validation rules

1. Add an opening and closing <validation></validation> tag within any <text> tag.
2. Within the validation tag, enter any of the validation rules listed below.

Validation Rules

- Required
- MinLength
- MaxLength
- Number range
- Regex

DPLdifUtilities.Import.exe

To import your new attributes into the DigitalPersona LDS database

1. Copy the entire *Server Tools* folder to the computer where DigitalPersona LDS Server is installed. This will include any .ldif files that you created as well as a required xml file generated by the DPLdifUtilities.Import.exe tool.
2. Ensure that there are no extraneous .ldif files in the folder. The import tool will process any .ldif files found in the directory.
3. Double-click *DPLdifUtilities.Import.exe*. Or, you can drop any .ldif files on top of the executable.

DigitalPersona Kiosk 11

THIS CHAPTER DESCRIBES THE MAIN FEATURES OF THE DIGITALPERSONA KIOSK CLIENT.

Introduction

DigitalPersona Kiosk provides users with fast, convenient and secure multi-factor identification and authentication in environments where users share a common Windows account yet need separately controlled access to resources, applications and data.

Feature overview

DigitalPersona Kiosk provides these features:

Single Sign-On to enterprise applications - Simplifies user logon to enterprise applications, including traditional Windows applications, web applications and Terminals. No changes to those applications are required and setup takes only a few minutes per application.

Multi-factor authentication - Further enhances convenience and security by providing administrators with a choice of credentials (such as fingerprints, PKI Smart Cards and Contactless cards or Windows Passwords, etc.) that can be required in any combination to authenticate users logging on to the PC, to enterprise applications, or for fast user switching between users on the same workstation.

Ability to roam and share user credentials across computers - If your environment requires users to gain access to multiple workstations or kiosks, they do not need to re-enroll their credentials at each computer. DigitalPersona Kiosk can automatically make users' authentication credentials and other data, such as managed logons to enterprise applications, available at each computer within the domain.

Attended or unattended credential enrollment - By default, DigitalPersona Kiosk is configured for centralized enrollment through one or more supervised computers using the DigitalPersona Attended Enrollment component, an optional component of DigitalPersona AD Workstation and DigitalPersona LDS Workstation.

This chapter describes the similarities and differences between DigitalPersona Workstation and DigitalPersona Kiosk functionality from the point of view of the administrator. Most of the basic functionality is common to both DigitalPersona Workstation and DigitalPersona Kiosk. Additional details on user tasks are provided in the DigitalPersona Kiosk Help file.

In the following topics, the term “kiosk” refers to one or more Kiosk Workstations which are tied to a shared Kiosk account.

Comparing DigitalPersona Workstation and Kiosk

This section describes the similarities and differences between DigitalPersona Workstation and DigitalPersona Kiosk.

Both DigitalPersona Kiosk and DigitalPersona Workstation include the following features:

- Multi-factor and alternative authentication credentials
- Password Manager - DigitalPersona Kiosk supports managed logons only. Personal logons created by an individual user in DigitalPersona Workstation are not supported and will not appear on an DigitalPersona Kiosk installation. Managed logons provide similar functionality but are created by an administrator using the Password Manager Admin Tool.
- Both DigitalPersona Workstation and DigitalPersona Kiosk’s default configuration provides centralized enrollment through one or more supervised computers using DigitalPersona Attended Enrollment, an optional component of DigitalPersona Workstation or DigitalPersona AD Workstation.
- If enabled, DigitalPersona Kiosk users can enroll their credentials in the same manner as in DigitalPersona Workstation, i.e. through the User Console. However, the following credentials are not supported in the Kiosk product: Recovery Questions and Bluetooth. Even if a user has enrolled these credentials in DigitalPersona Workstation, they cannot be used in DigitalPersona Kiosk.
- Both clients require DigitalPersona (AD or LDS) Server Version 1.1 or above.

When comparing DigitalPersona Kiosk to DigitalPersona Workstation, DigitalPersona Kiosk *differs* in the following ways:

- A specified Shared Account is always used for Windows logon that is independent of the user account being authenticated. This affects account profile and user preferences.
- By default, all DigitalPersona users are granted Kiosk access. However, in order to logon to DigitalPersona Kiosk, each user must first be created through Attended Enrollment or through Self Enrollment on a DigitalPersona Workstation.
- Any authorized DigitalPersona Kiosk user can unlock a kiosk computer. For example, a user may log on and lock the kiosk computer. Then, a second user can unlock it without performing log off and log on.
- The name of the last user is not shown in Logon or Unlock dialogs regardless of security settings.
- A kiosk user can enroll their own credentials, regardless of which user account was logged on to the kiosk, without logging on to their Windows account. The administrator must have allowed permissions for the user to enroll and delete their fingerprints.
- DigitalPersona Kiosk does not allow use of the Recovery Questions or Bluetooth credentials for accessing the Kiosk account.
- A Face credential may be used for authentication on a Kiosk computer, but cannot be used for identification or when logging onto the kiosk with the Shared Account credentials.

Logging On to Windows

DigitalPersona Kiosk allows users to log on to Windows with any enrolled DigitalPersona credential, such as their DigitalPersona password, their fingerprint or various types of access cards.

All kiosk users share the same Windows session. If the computer becomes locked, any authorized kiosk user will be able to unlock it, view the desktop, and run programs. Users may also have the option to not log into the kiosk session,

but instead to log on to their own Windows account instead of the Shared Account, although this is recommended for administrators only.

Computers where DigitalPersona Kiosk is installed will display an additional Kiosk User tile on the Logon Screen.

The user name for the Windows shared account that DigitalPersona Kiosk uses cannot be used to log on to a kiosk session. All Kiosk users must use their own DigitalPersona credential to log on.

Logging on to Windows without Kiosk

To log on to a computer without using a kiosk session, select *Other User* and enter your Windows user name and password.

When logging in to a computer outside of a kiosk session, the designated Shared Account for the kiosk is not used and therefore DigitalPersona Kiosk features are not available. Specifically, access to the DigitalPersona Console, and the use of Password Manager logons are disabled.

This feature is intended for administrators who might need to access a computer for administrative purposes, and without kiosk features enabled. Non-administrators can be prohibited from logging on to the computer outside of a kiosk session by enabling a setting in the controlling GPO. See *Prevent users from logging on outside of a Kiosk session* in the DigitalPersona LDS or DigitalPersona AD Administrator Guide.

CAUTION: If you lock the computer outside of a kiosk session, other kiosk users will not be able to unlock it, so be sure to log out of a local session on any kiosk workstation.

Automatic logon using the Shared Kiosk Account

Kiosk can be configured to automatically logon to the Shared Kiosk account when Windows starts or restarts. The Windows Logon screen will not be displayed.

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

This option is controlled by the *Allow automatic logon using Shared Kiosk Account* setting described in the DigitalPersona AD or DigitalPersona LDS Administrator Guides.

Changing Your Password

The process of changing your Windows password on a computer with DigitalPersona Kiosk installed is the same as on a computer without DigitalPersona Kiosk installed.

To change your Windows password:

1. Press ***Ctrl+Alt+Delete***.
2. Select *Change a Password*.
3. Enter your Windows user name and your old password.

4. Enter and confirm a new password.

User Account Control

An administrator may use any authorized and enrolled credential instead of their user name and password, to give a standard user permission to perform an activity that is restricted by User Account Control.

When the User Account Control dialog displays, a local administrator with an authorized credential can use their credential to permit the activity.

Using the Password Manager Admin Tool with Kiosk

The Password Manager Admin Tool is an administrative tool that allows an administrator to provide automated logon to password-protected resources, programs and websites.

With DigitalPersona Kiosk, Password Manager includes the following differences when compared to DigitalPersona Workstation implementations:

- Managed logons created with the Password Manager Admin Tool must be deployed to the Shared Account instead of to user accounts.
- Kiosk users do not need to log on to Windows to use managed logons. Their identity is verified each time they log on to the resource. For kiosk users, the Password Manager logon data is never cached locally.

Only managed logons created using the DigitalPersona Password Manager Admin Tool, version 1.0 or higher, are compatible with the current version of DigitalPersona Kiosk.

For additional information on the Password Manager Admin Tool and the creation and use of managed logons, see the DigitalPersona LDS or DigitalPersona AD Administrator Guide.

Logging On to Password-Protected Programs

DigitalPersona Kiosk lets a kiosk user log on to password-protected resources, programs and websites with any enrolled credential. As an administrator, you must enable this feature for specific programs by creating managed logons for them. Password-protected resources with managed logons display a Password Manager icon, shown below, in the upper left corner of the screen (Internet Explorer) or to the right of the first recognized entry field (Firefox and Chrome).

Password Manager Icon for Internet Explorer

Password Manager Icon for Internet Explorer as displayed on Change Password screens

Password Manager Icon for Firefox and Chrome

Password Manager Icon for Firefox and Chrome as displayed on Change Password screens

Administrators can also add a logon for a change password screen to a managed logon.

Users are prompted for their account data the first time they log on to a resource. Then, on subsequent logons, they only need to launch the program, and submit their enrolled credential. DigitalPersona Kiosk automatically enters the user name, domain and password and any other necessary account data in the appropriate logon screen text boxes and, if so configured, submits the account data.

For further information on Password Manager, see the DigitalPersona LDS or DigitalPersona AD Administrator Guide.

Switching Users on DigitalPersona Kiosk Computers

You can log on, unlock or gain access to a password-protected resource on a kiosk computer by using your enrolled credentials. After your work is finished, you can do one of the following:

- *Close the resource and leave the kiosk computer unlocked* - The next user can approach the kiosk computer and provide their credentials to gain access to the password-protected resource.
- *Close the resource and lock the kiosk computer* - The next user can approach the kiosk computer and provide their credentials to unlock the computer. They can then open any password-protected resource with their credentials.
- *Close the resource and log off from the kiosk computer* - The next user can approach the kiosk computer and provide their credentials to log on to the computer. The user is logged into the Shared Account for the kiosk.
- The installation and configuration of DigitalPersona Kiosk is covered in the chapter DigitalPersona Kiosk installation on page *24*.

All other functionality is the same as described in the chapter DigitalPersona Workstation on page *46*.

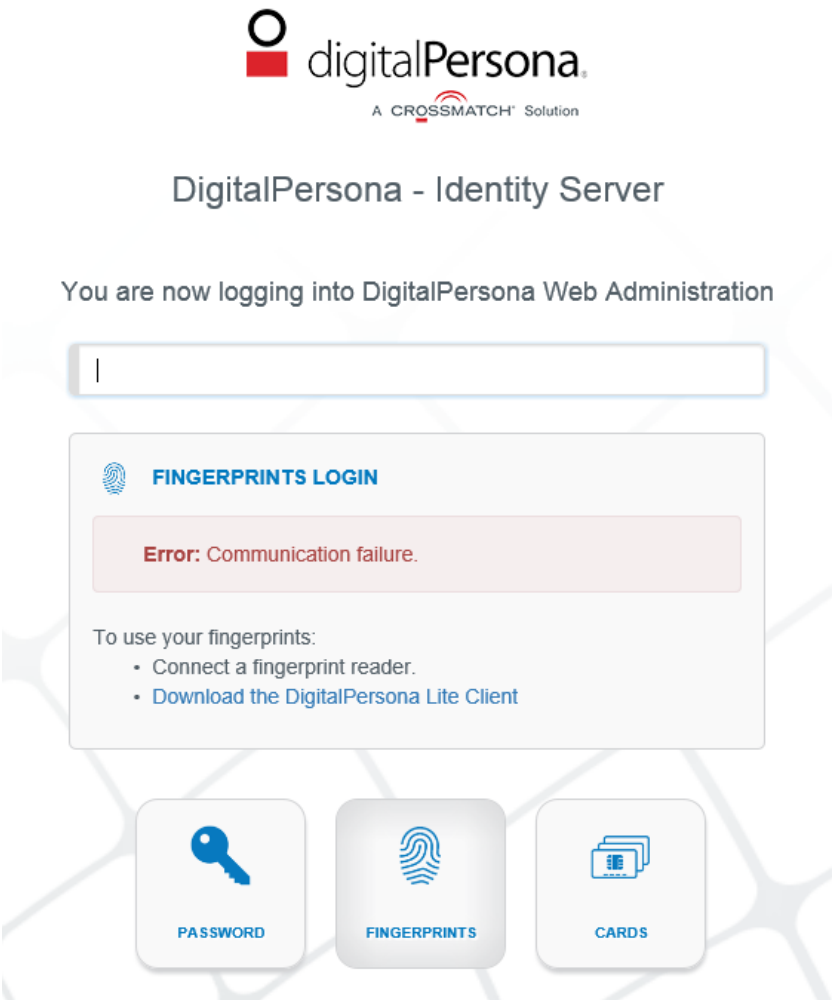
DigitalPersona Lite Client 12

THIS CHAPTER DESCRIBES THE FEATURES OF THE DIGITALPERSONA LITE CLIENT.

The DigitalPersona Lite Client is a lightweight client application adding support for authenticating to the Digitalpersona Identity Server using fingerprint and PKI Smart Card credentials.

It does not have a graphical or command line interface and has no other features in common with the other DigitalPersona clients.

When attempting to authenticate using a fingerprint or PKI Smart card at the DigitalPersona Identity Server, if no DigitalPersona client is installed on the computer, a link will be displayed to enable downloading the DigitalPersona Lite Client.



For system requirements, see page *10*. For installation details, see *Lite Client installation* on page *36*.

Index

