HID DigitalPersona Cookbook

Real-World solutions using the DigitalPersona platform

January 2020

hidglobal.com

Copyright

Trademarks

Revision history

Date	Description	Revision
January 2020	Initial release.	O.A

Contacts

For additional offices around the world, see **www.hidglobal.com/contact/corporate-offices**

Americas and Corporate

611 Center Ridge Drive
Austin, TX 78753
USA
Phone: +1 866 607 7339
Fax: +1 949 732 2120

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong
Phone: +852 3160 9833
Fax: +852 3160 4809

Europe, Middle East and Africa (EMEA)

Haverhill Business Park Phoenix Road
Haverhill, Suffolk CB9 7AE
England
Phone: +44 (0) 1440 711 822
Fax: +44 (0) 1440 714 840

Brazil

Condomínio Business Center
Av. Ermano Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP
Brazil
Phone: +55 11 5514-7100

HID Global Technical Support: www.hidglobal.com/support

Contents

Chapter 1

1 Introduction to the Cookbook

1.1 Overview

The HID DigitalPersona Solutions Cookbook is a series of recipes for cooking up solutions using the ingredients provided as part of the DigitalPersona solutions, products and components.

The recipes are presented in a format based on traditional restaurant offerings, allowing you to create the perfect meal, consisting of perhaps an appetizer, an entrée (main course), a selection of side dishes, and an optional dessert. (We leave the beverage choices to the IT professional doing the preparation and cooking.)

Just as quality ingredients are critical to creating great meals, the DigitalPersona suite of quality software components presents you with the tools that can be assemble into a tasty spread that meets each enterprise's needs.

The DigitalPersona solution, consists of a range of software, hardware and integration components.

One core component used in most environment's configurations is the Crossmatch DigitalPersona Server. It comes in two flavors, the DigitalPersona AD Server (leveraging Microsoft Active Directory), and the DigitalPersona LDS Server (leveraging Microsoft Lightweight Directory Services).

While both servers use Active Directory Group Policy Objects (GPOs) for server and client configuration, the AD Server uses Microsoft Active Directory for storage and the LDS Server uses Microsoft AD LDS for storage.

The workstation, or kiosk, client is run on endpoints, enabling MFA windows logon and unlock. Password Manager is a part of our complete meal, enabling MFA for websites and applications in the windows session.

Another core component is the DigitalPersona Web Components module, which provides a Web Administrator Console for web-based user management and a DigitalPersona Web Enrollment site for credential enrollment. It also includes the DigitalPersona Identity Server and STS (Secure Token Service), for implementing web-based multifactor federation or Office365 access.

Extended Microsoft consoles (ADUC and GPMC) are the primary means of management for the AD solution. The Web Administrator Console is the main management tool for the DigitalPersona LDS solution. It can be used for some management tasks when using the AD solution too.

The DigitalPersona solution also includes a well-stocked pantry; consisting of a documentation set including the following -

- AD Administrator Guide
- LDS Administrator Guide
- Client Guide
- SSO for Office 365 On Premise AD - LDS Solution Deployment Guide
- SSO for Office 365 On Premise - AD Solution Deployment Guide
- NetScaler RADIUS Authentication - Integration Guide

- Card Support Guide
- Token Support Guide
- VDI Support Guide

The Administrator Guides, however, at over 300 pages each, can be rather daunting to some administrators. They are comprehensive and quite detailed, whereas this cookbook attempts to be a kind of quick start guide, with pointers to the more verbose and exhaustive reference material in the Administrator Guides.

You will also find ingredients from the DigitalPersona Client Guide, which covers the clients for both the AD and LDS flavors of the DigitalPersona solution. Topics in the Client Guide include:

- DigitalPersona Workstation, Kiosk, and w32 attended enrollment, client installs, by interactive setup.exe and .msi push
- Client features including: credential provider, credential management, password manger, attended enrollment, and kiosk functionality
- OTP enrollment and use
- Browser integration

So, take a look through this cookbook to find the dish, or combination of dishes, that will help you to create a complete meal that meets your security and convenience requirements.

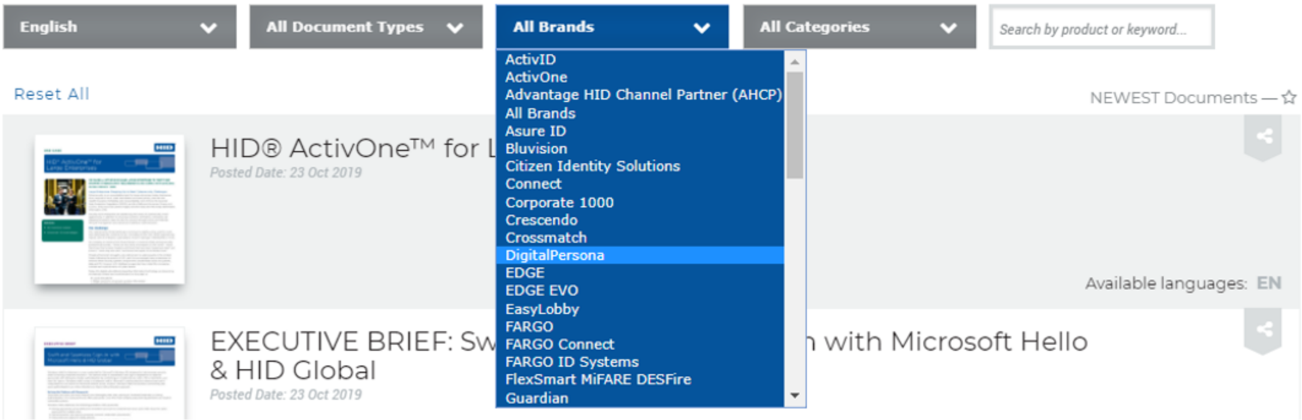
🌶️ Hot peppers indicate an extra secure feature-set.

Note that the features and workflows described in this document are based on the 3.2.0 version of the DigitalPersona solution. Most of the content will apply to earlier versions as well. Content specific to version 3.2.0, 3.1.0, or 2.x will be labeled as such.

All chapter references are to the HID DigitalPersona Administrator Guides unless otherwise specified.

1.2 Resources

- Documentation: All of the above-mentioned documentation is available by selecting DigitalPersona from the All Brands dropdown menu at the following location: https://www.hidglobal.com/documents



- Patches: All patches can be found here: http://downloads.crossmatch.com.
- Upgrade Notes are found here: https://www.hidglobal.com/documents. If upgrading an existing setup, use the installation & configuration instructions from the current Upgrade Notes document instead of those in the Administrator Guide.

Chapter 2

2 Appetizers/Starters

2.1 Single Server Test/Lab Test Platter - DigitalPersona AD flavor

Provides Windows/AD logon and unlock, Password Manager and (optionally the DigitalPersona Web Administration Console), all on one server machine, with one client.

This could be by using VMs, or a VM for the Server and a physical machine for the client.

Recipe	References
1. Build a Windows server, promote it to DC in a new domain in a new forest and running AD integrated DNS.	**Note**: All below references are to the HID DigitalPersona AD Administrator Guide unless otherwise noted. All topics specified below can be located through the Index at the back of the book.
2. Build a client machine with a supported Windows client OS, point it to the new server for DNS, and join it to the new domain as a member.	
3. On the new DC:	
a. Run the DigitalPersona Schema Extension.	Chapter: DigitalPersona AD Server Installation Topic: Extending the Active Directory Schema
b. Run the DigitalPersona AD Active Directory Domain Configuration Wizard.	Chapter: DigitalPersona AD Server Installation Topic: Configuring each domain
c. Increase/Clear rangeUpper	Chapter: Troubleshooting Topic: Changing Password Manager Data storage limits
d. Install DigitalPersona AD Server and any server patches	Chapter: DigitalPersona AD Server Installation Topic: Installing DigitalPersona AD Server **Note**: Patches are found here: http://downloads.crossmatch.com/
e. Install the DigitalPersona AD Administration Tools selecting the *Complete* Setup Type.	Chapter: Separate installations Topic: DigitalPersona AD Administration Tools
f. (Optionally) Install the DigitalPersona Web Components and any associated patches. In the DigitalPersona Web Management Components configuration wizard, you can select *Express Configuration*.	Chapter: Web Management Components installation Topic: All topics except Advanced Configuration **Note**: Patches are found here: http://downloads.crossmatch.com/
g. Create a network share for storing Password Manager managed logons (usually in sysvol or netlogon for redundant client access).	Chapter: Password Manager Admin Tool Topic: Setting up the Password Manager Admin Tool
4. Configure GPO settings at the domain level:	

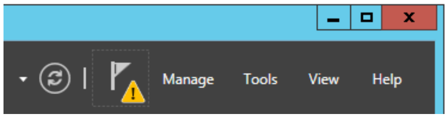
Recipe	References
a. Licenses GPO In the GP Management Editor, go to: `Computer Config / Policies / Software Settings / DigitalPersona Server / Licenses.` Right-click Licenses and select Activate to launch the DigitalPersona License Activation Wizard.	Chapter: License Activation & Management Topic: License activation **Note**: A 30-day 10-user trial license is included. For new licenses, a license file and password, or license ID and password will be provided with your purchase.
b. Redirect fingerprint data GPO In the GP Management Editor, go to: `Computer config / Polices / Administrative Templates / DigitalPersona AD Client / Authentication devices / Fingerprints / Redirect fingerprint data`	Chapter: Policies and Settings Topic: Redirect fingerprint data **Note**: For versions 3.2 and above, this GPO is enabled by default.
c. Managed Logons GPO (User policy) In the GP Management Editor, go to: `User Configuration / Policies / Administrative Templates / DigitalPersona AD Client / Managed Apps / Password Manager / Managed Logons` Configure user options (optional) and specify domain-name UNC path to the network share defined in item 3g above where Password Manager managed logons will be stored.	Chapter: Policies and Settings Topic: Managed Logons **Note**: This is a *User* policy.
5. On the new workstation:	
a. Install DigitalPersona AD Workstation and any associated patches. Note: Patches can be found here. http://downloads.crossmatch.com	*HID DigitalPersona Client Guide* Chapter: DigitalPersona Workstation installation
b. Install DigitalPersona AD Administration Tools and any associated patches. Note: Patches can be found here. http://downloads.crossmatch.com	*HID DigitalPersona AD Administrator Guide* Chapter: Separate Installations Topic: DigitalPersona AD Administration Tools

Recipe	References
c. Install DigitalPersona Password Manager Admin Tool (PMAT) and any associated patches. Note: Patches can be found here. http://downloads.crossmatch.com	Chapter: Password Manager Admin Tool Topic: Installation & setup
6. Set up Password Manager managed logons. a. Specify the path to the shared folder where managed logons will be stored. b. Click *Add Logon*. c. Follow instructions in the Password Manager Admin Tool Logon Screen wizard.	Chapter: Password Manager Admin Tool Topic: Creating managed logons
7. Test / use the system: a. Log on to the DigitalPersona client machine as a domain user. b. Enroll available credentials (i.e. password, fingerprint, PIN, OTP, Cards). c. Use credentials to logon and unlock your client machine. d. Navigate to a trained logon page and use your DigitalPersona credentials to fill-in logon screen fields.	HID DigitalPersona Client Guide Chapter: Password Manager Topics: Introduction Browser Integration Using managed logons

2.2 DigitalPersona LDS flavor

Note that LDS is used instead of AD only when: schema can't be extended, no software can be installed onto DCs, or when user who are not AD users are needed. One more machine is needed to test LDS than is needed for AD testing.

Recipe	References
1. Build two Windows servers, promote one to DC in a new domain in a new forest and running AD integrated DNS, join the other to this domain as a member.	NOTE: All below references are to the HID DigitalPersona LDS Administrator Guide unless otherwise noted. All topics specified below can be located through the Index at the back of the book.
2. Build a client machine with a supported Windows client OS, point it to the new server for DNS, and join it to the new domain as a member.	
On the new Server (not the DC)	
3. Add roles and features ▪ Active Directory Lightweight Directory Services role ▪ .NET Framework 3.5 Features, including HTTP Activation ▪ .NET Framework 4.[56] Features, including HTTP Activation	Chapter: DigitalPersona LDS Server Installation & Setup Topic: Add server roles and features

Recipe	References
4. Run the Active Directory Lightweight Directory Services Setup Wizard. [Product package]\Server\DigitalPersona LDS Server\Configuration Wizard\DigitalPersonaADLDSConfig.exe a. Choose a unique instance b. Provide a unique name c. LDAP 398 and SSL 636 (or 50000 and 50001 if on a DC) d. Defaults for remainder of settings e. CNTRL+A, then click for all for Importing LDIF Files. f. Shows up in *Programs and Features* listed by its unique instance name.	**Note**: Alternatively, you can run the Active Directory Lightweight Directory Services Setup Wizard by clicking the yellow flag warning in the upper right of the Server Manager Console. 
5. Install DigitalPersona Web Management Components. [Product package]\Server\DigitalPersona LDS Web Management Components\setup.exe a. Base URL and wildcard web cert made above for each site wanted b. Use same cert for signing STS c. Set MFA for website content access d. Set step-up and behavioral biometrics e. You can change these values later through the DigitalPersona IIS Plug-in. f. Tweak web config file for separate boxes for components.	Chapter: Web Management Components Installation
On the Domain Controller	
6. Install the DigitalPersona LDS Server. [Product package]\Server\DigitalPersona LDS Server\Setup.exe a. Accept defaults. b. Shows up in *Programs and Features* as DigitalPersona LDS Server.	Chapter: DigitalPersona LDS Server Installation & Setup Topic: Add server roles and features
7. Install the LDS Administration Tools. [Product package]\Server\DigitalPersona LDS Administration Tools\setup.exe a. Take defaults b. Shows up in “Programs and Features” as DigitalPersona LDS Admin Tools	Chapter: DigitalPersona LDS Server Installation & Setup Topic: Install DigitalPersona LDS Server
8. GPMC / local computer policy `Computer config / software settings / DigitalPersona Server / Licenses` License shows up and properties including number of remaining license seats can be viewed.	Chapter: DigitalPersona LDS Server Installation & Setup Topic: License activation

Recipe	References
9. Add roles and features a. Web server (IIS) b. ASP .Net 3.5 c. AD Cert Services d. Certification Authority	
10. Active Directory Certificate Services config CA; Enterprise CA; root CA; new private key; SHA-256; defaults; “configure”	
11. Certification Auth MMC "Manage" Certificate Templates. Web Server; Properties; Security; auth users allow enroll	
12. Certificates MMC a. Personal / certs / all tasks / request new cert b. Next / next / web server / hyperlink c. Subject tab ▪ Subject / common name / *.domainname ▪ Alt name / DNS / *.domainname d. General - Name of your choice e. Private key - Key options / make exportable f. "Enroll"	
13. Configure GPO settings at the domain level (on the Domain Controller):	
a. Licenses GPO In the GP Management Editor, go to: Computer Config / Policies / Software Settings / DigitalPersona Server / Licenses. Right-click *Licenses* and select *Activate* to launch the DigitalPersona License Activation Wizard.	Chapter: DigitalPersona LDS Server Installation & Setup Topic: License activation
b. Redirect fingerprint data GPO In the GP Management Editor, go to: `Computer config / Polices / Administrative Templates / DigitalPersona AD Client / Authentication devices / Fingerprints / Redirect fingerprint data`	Chapter: Policies and settings Topic: Redirect fingerprint data

Recipe	References
c. Managed Logons GPO (User policy) In the GP Management Editor, go to: `User Configuration / Policies / Administrative Templates / DigitalPersona AD Client / Managed Apps / Password Manager / Managed Logons` Configure user options (optional) and specify domain-name UNC path to the network share defined in item 3g above where Password Manager managed logons will be stored.	Chapter: Policies and settings Topic: Managed logons
14. On a new workstation:	
a. Install DigitalPersona LDS Workstation and any associated patches. Note: Patches can be found here. http://downloads.crossmatch.com/	*HID DigitalPersona Client Guide* Chapter: Policies and settings Topic: Managed logons
b. Install DigitalPersona LDS Administration Tools and any associated patches. Note: Patches can be found here. http://downloads.crossmatch.com/	*HID DigitalPersona LDS Administrator Guide* Chapter: Separate installations Topic: DigitalPersona LDS Administration Tools
c. Install DigitalPersona Password Manager Admin Tool (PMAT) and any associated patches. Note: Patches can be found here. http://downloads.crossmatch.com/	Chapter: Separate installations Topic: Password Manager Admin Tool
15. Setup Password Manager managed logons. a. Specify the path to the shared folder where managed logons will be stored. b. Click Add Logon. c. Follow instructions in the Password Manager Admin Tool Logon Screen wizard.	Chapter: Password Manager Admin Tool
16. Test / use the system: a. Log on to the DigitalPersona client machine as a domain user. b. Enroll available credentials (i.e. password, Fingerprints, PIN, OTP, Cards). c. Use credentials to logon and unlock your client machine. d. Navigate to a trained logon page and use your DigitalPersona credentials to fill-in logon screen fields.	

Chapter 3

3 Entrées

3.1 GPOs for all Entrées and Specials

Recipe	References
1. Licenses GPO `Computer Config / Policies / Software Settings / DigitalPersona Server / Licenses` a. Right-click on Licenses and select Activate license. b. Follow instructions in the DigitalPersona Activation Wizard. Licenses are needed to use the product beyond the 30-day trial period. A license is consumed for each user whose credential data is being stored.	Chapter: License Activation & Management Topic: License activation **Note**: Licenses are homed in Active Directory, and not in a specific GPO but rather are accessible from all GPOs.
2. Redirect fingerprint data GPO `Computer config / Polices / Admin Templates / DigitalPersona AD Client / Authentication devices / Fingerprints / Redirect fingerprint data` This is needed to RDP from one client to another and to use fingerprint and other factors.	Chapter: Policies and Settings Topic: Authentication Devices
3. Enrollment Policy GPO `Computer config / Polices / Software Settings / DigitalPersona AD Client / Enrollment / Enrollment policy` For ease of use, we recommend enabling, and limiting credentials displayed to just those that will be used. **Note**: Available in version 3.0 and above.	Chapter: Policies and Settings Topic: Enrollment policy **Note**: Previous versions used a *Self-enrollment policy* for defining credentials permitted in the User Console, and XML files for credentials permitted in Attended Enrollment and Web Enrollment (version 3.1 +).
4. Managed Logons GPO (User policy) `User Configuration / Policies / Admin Templates / DigitalPersona AD Client / Managed Apps / Password Manager / Managed Logons` Enable and configure for managed logon use with Password Manager. Populate this GPO with the domain-name UNC path to the network share where Password Manager managed logons will be stored.	Chapter: Password Manager Admin Tool Topic: User policy settings Chapter: Policies and Settings Topic: Managed Logons **Note**: Unlike almost all the other DigitalPersona polices, this is a User policy.

Recipe	References
5. Do not launch the Getting Started wizard upon logon GPO (Optional) `Computer Configuration / Policies / Admin Templates / DigitalPersona AD Client / General Admin / Do not launch the Getting Started wizard upon logon` Enable this policy if the frequent display of the popup becomes annoying. Otherwise it may be very helpful in encouraging new users enrolled.	Chapter: Policies and Settings Topic: Do not launch the Getting Started wizard upon logon
Server level	
6. Perform fingerprint identification on server GPO `Computer Configuration / Policies / Admin Templates / DigitalPersona AD Server / Identification Server Settings / Perform fingerprint identification on server` Enable for identification / authentication with just fingerprint and no user name; needed for Kiosk client support.	Chapter: Policies and Settings Topic: Identification Server settings **Note**: This is enabled by default in versions 5.5.1 and above.
7. Fingerprint enrollment GPO (optional) `Computer Configuration / Policies / Admin Templates / DigitalPersona AD Server / Authentication Devices / Fingerprints / Fingerprint enrollment` Sets minimum and maximum number of fingerprints that can be enrolled by a user.	Chapter: Policies and Settings Topic: Fingerprint enrollment **Note**: This policy controls fingerprints stored in the central database. A separate client policy controls only local storage (per machine workgroup style, not domain).
8. Fingerprint verification GPO (Optional) `Computer Configuration / Policies / Admin Templates / DigitalPersona AD Server / Authentication Devices / Fingerprints / Fingerprint verification` Sets the False Accept Rate (FAR), which can be increased to reduce false-accepts or decreased to reduce false-rejects.	Chapter: Policies and Settings Topic: Fingerprint verification
9. PIN enrollment GPO (Optional) `Computer Configuration / Policies / Admin Templates / DigitalPersona AD Server / Authentication Devices / PIN / PIN enrollment`	Chapter: Policies and Settings Topic: PIN enrollment
10. Account lockout duration GPO Reset account lockout counter after GPO Account lockout threshold GPO (Optional) `Computer Configuration / Policies / Admin Templates / DigitalPersona AD Server / Credentials verification lockout` Mirrors Microsoft AD account lockout due to invalid password entry, but for invalid biometrics entries. Set the number of minutes a user is locked out before automatically unlocked, the minutes before lockout counter is reset and the number of attempts that triggers a lockout.	Chapter: Policies and Settings Topic: Credentials verification lockout
OU level	

Recipe	References
11. Logon Authentication policy GPO `Computer config / Polices / Software Settings / DigitalPersona AD Client / Authentication / Logon Authentication policy` Sets one or more single or multi-factor policies for Windows logon and unlock.	Chapter: Policies and Settings Topic: Logon Authentication policy
12. Enhanced Logon Authentication policy GPO `Computer config / Polices / Software Settings / DigitalPersona AD Client / Authentication / Enhanced Logon Authentication policy` Under specified conditions, replaces the Logon Authentication policy with one or more single or multi-factor policies for Windows logon and unlock. For example, if a computer hasn't been used in some time, three factors might be required for access instead of two.	Chapter: Policies and Settings Topic: Enhanced Logon Authentication policy
13. Session Authentication policy GPO `Computer config / Polices / Software Settings / DigitalPersona AD Client / Authentication / Session Authentication policy` Sets one or more single or multi-factor policies for Password Manager use logon to websites and W32 apps.	Chapter: Policies and Settings Topic: Session Authentication policy

3.2 Enterprise Business - DigitalPersona AD flavor

Choose a Small, Medium, or Large portion.

Includes Windows/AD logon and lock/unlock, Password Manager (PM) and the DigitalPersona Web Administration Console. All DigitalPersona AD flavor.

Recipe	References
1. Assumes existing Microsoft AD environment For multi-domain AD forests, install the DigitalPersona AD Server in the domain where the users are.	**Note**: Many authentication functions are supported in multi-forest environments.
2. Overall configuration is: a. Two or more DCs for the DigitalPersona Servers, generally with DigitalPersona Administration Tools installed. b. Member server(s) for DigitalPersona Web Components c. Multiple DigitalPersona Workstation clients d. One or more administrative workstations with DigitalPersona Workstation, DigitalPersona Administration Tools, and the Password Manager Admin Tool (PMAT)	
3. Onetime setup	

Recipe	References
a. Run DigitalPersona schema extension.	Chapter: DigitalPersona AD Server Installation Topic: Extending the Active Directory Schema
b. Run the DigitalPersona AD Active Directory Domain Configuration Wizard.	Chapter: DigitalPersona AD Server Installation Topic: Configuring each domain
c. Increase/clear rangeUpper.	Chapter: Troubleshooting Topic: Changing Password Manager Data storage limits
d. Create a network share for Password Manager templates (usually in sysvol or netlogon for redundant client access).	Chapter: Password Manager Admin Tool Topic: Create a shared network folder
4. On each DC where the DigitalPersona Server will be running -	
a. Install DigitalPersona AD Server and any available patches. Note: Patches can be found here. http://downloads.crossmatch.com/	Chapter: DigitalPersona AD Server Installation Topic: Configuring each domain
b. Install the DigitalPersona Admin Tools and any tool patches; with all custom options selected. Note: Patches can be found here. http://downloads.crossmatch.com/	Chapter: Separate installations Topic: DigitalPersona AD Administration Tools
5. On the **member server(s)** to be web servers (not the DCs, preferably each role on its own member server): Install the DigitalPersona Web Components using the *Advanced Configuration* option, and any associated patches.	Chapter: Web Management Components Installation **Note**: Patches can be found here. http://downloads.crossmatch.com/
6. Configure GPOs as detailed in Chapter 3.1 GPOs for all Entrées and Specials section above.	
7. On each workstation: Install DigitalPersona AD Workstation and any associated patches.	*HID DigitalPersona AD Client Guide* Chapter: DigitalPersona Workstation installation **Note**: Patches can be found here. http://downloads.crossmatch.com/
8. On administrative workstations, additionally, you can:	
a. Install DigitalPersona AD Admin Tools and any associated patches. **Note**: Patches can be found here. http://downloads.crossmatch.com/	*HID DigitalPersona AD Administrator Guide* Chapter: Separate installations Topic: DigitalPersona AD Administration Tools
b. Install DigitalPersona Password Manager Admin Tool and any associated patches. **Note**: Patches can be found here. http://downloads.crossmatch.com/	Chapter: Password Manager Admin Tool Topic: Installation & setup
c. If going with a side of *Attended Enrollment*, that feature can be installed here as well.	See additional details in Chapter 5 Side Orders.

Recipe	References
9. Set up Password Manager managed logons on an admin workstation with the target app available. a. Open the logon screen that you want to train. b. Open the Password Manager Admin Tool. c. Specify the path to the shared folder where managed logons will be stored. d. Click Add Logon. e. Follow instructions in the Password Manager Admin Tool Logon Screen wizard.	Chapter: Password Manager Admin Tool Topic: Creating managed logons
10. Administer and use the system:	
a. Manage users in ADUC.	Chapter: ADUC Snap-ins Topic: Users and Computers snap-in
b. Manage clients, servers, and users in GPMC.	Chapter: Policies and Settings
c. Manage users in the DigitalPersona Web Admin Console.	Chapter: DigitalPersona Web Administration Console
d. Web based self-enrollment.	Chapter: DigitalPersona Web Enrollment
e. Credential enrollment and management ▪ Self-enroll credentials as available (password, Fingerprints, OTP (PushOTP too if added), cards, PIN) ▪ Attended enrollment – see “Attended enrollment” add-on section (password, Fingerprints, OTP (Push OTP too if added), cards, PIN	DigitalPersona AD Client Guide Chapter: Client Features Topic: Managing user credentials **Note**: See additional details in Chapter 5 Side Orders.
f. Logon/unlock machines users with password, Fingerprints, OTP (PushOTP too if added), cards, and PIN.	
g. Navigate to PM trained screens and use PM and enrolled factors to fill-in logon screen credentials (password, Fingerprints, OTP (Push OTP too if added), cards, PIN, and even the optional PM SSO).	Chapter: Password Manager Topic: Managed logons and personal logons

3.3 Enterprise Business – DigitalPersona LDS flavor

There are a few deployment use-cases where the LDS flavor of DigitalPersona must be used instead of the AD flavor:

- If unable to extend the AD schema for DigitalPersona use.
- When DigitalPersona Server cannot be installed onto any DCs.
- When non-AD user accounts are needed.

Note that DigitalPersona AD leverages Microsoft management consoles (ADUC and GPMC) for administration, whereas DigitalPersona LDS does not. LDS management is by script and web console. Also, even with DigitalPersona LDS, most configuration is done via GPOs.

Separate member servers should be used for each of DigitalPersona authentication server, AD LDS server, and DigitalPersona web server. (Separate web servers in DigitalPersona AD from DCs too.)

In future versions of the DigitalPersona LDS product more and more controls will be moved from GPOs to native DigitalPersona LDS storage (i.e.: Microsoft AD LDS).

DigitalPersona LDS Enrollment Options Matrix		
	W32 thick client	Web-based
Self-enrollment	Self-enrollment on DigitalPersona LDS *Workstation* is standard.	**Note**: Web-based self-enrollment must be explicitly enabled. *HID DigitalPersona LDS Administrator Guide* Chapter: DigitalPersona Web Enrollment Topic: Enabling self-enrollment
Attended Enrollment	The Attended Enrollment component is an optional part of the DigitalPersona LDS Workstation Custom install. Or you can select *Modify* on an already installed DigitalPersona Workstation to add it. *DigitalPersona Client Guide* Chapter: DigitalPersona Attended Enrollment installation Topic: Local installation **Note:** Tune attended enrollment tiles and workflow via associated GPOs (v3.0.2+) or XML files (versions prior to 3.0.2). Chapter: DigitalPersona Attended Enrollment Topic: Customizing Attended Enrollment	**Note**: Web-based attended enrollment through the Web Enrollment component is the default enrollment method. *HID DigitalPersona LDS Administrator Guide* Chapter: DigitalPersona Web Enrollment

3.3.1 DigitalPersona LDS Database Server on a member server

Recipe	References
1. Add roles and features ▪ Active Directory Lightweight Directory Services role ▪ .NET Framework 3.5 Features, including HTTP Activation ▪ .NET Framework 4.[56] Features, including HTTP Activation	Chapter: License Activation & Management Topic: License activation **Note**: While licenses are only relevant to the DigitalPersona Server, they end up homed in Active Directory itself, and not in a specific GPO but rather accessible from all GPOs.
2. Run the Active Directory Lightweight Directory Services Setup Wizard. [Product package]\Server\DigitalPersona LDS Server\Configuration Wizard\DigitalPersonaADLDSConfig.exe a. Choose a unique instance b. Provide a unique name c. LDAP 398 and SSL 636 (or 50000 and 50001 if on a DC) d. Defaults for remainder of settings e. CNTRL+A, then click for all for Importing LDIF Files. f. Shows up in *Programs and Features* listed by its unique instance name.	Chapter DigitalPersona LDS Server Installation & Setup Topic: Set up a unique instance of AD LDS
3. Install the DigitalPersona LDS Server. [Product package]\Server\DigitalPersona LDS Server\Setup.exe a. Accept defaults. b. Shows up in *Programs and Features* as DigitalPersona LDS Server.	Chapter DigitalPersona LDS Server Installation & Setup Topic: Install DigitalPersona LDS Server
4. Install the LDS Administration Tools. `[Product package]\Server\DigitalPersona LDS Administration Tools\setup.exe` a. Accept defaults b. Shows up in “Programs and Features” as DigitalPersona LDS Admin Tools	Chapter Separate installations Topic: DigitalPersona LDS Administration Tools
5. GPMC / local computer policy `Computer config / software settings / DigitalPersona Server / Licenses` a. License shows up. b. Properties including number of remaining license seats can be viewed.	Chapter: Policies and settings Topic: Licenses

3.3.2 DigitalPersona LDS Web Server on a member server

Includes

- Creating a Certificate Authority
- Creating a certificate
- Exporting and then importing a certificate.

Recipe	References
1. Add roles and features ▪ Web server (IIS) ▪ ASP .Net 3.5 ▪ AD Cert Services ▪ Certification Authority	Chapter: License Activation & Management Topic: License activation **Note**: While licenses are only relevant to the DigitalPersona Server, they end up homed in Active Directory itself, and not in a specific GPO but rather accessible from all GPOs.
2. Active Directory Certificate Services config CA; Enterprise CA; root CA; new private key; SHA-256; defaults; "configure"	
3. Certification Auth MMC "Manage" Certificate Templates. Web Server; Properties; Security; auth users allow enroll	
4. Certificates MMC a. Personal / certs / all tasks / request new cert b. Next / next / web server / hyperlink c. Subject tab Subject / common name / *.domainname Alt name / DNS / *.domainname d. General Name of your choice e. Private key Key options / make exportable f. "Enroll"	
5. Install DigitalPersona Web Management Components. `[Product package]\Server\DigitalPersona LDS Web Management Components\setup.exe` a. Base URL and wildcard web cert made above for each site wanted. b. Use same cert for signing STS c. Set MFA for website content access d. Set step-up and behavioral biometrics e. You can change these values later through the DigitalPersona IIS Plug-in.	Chapter: Web management Topic: Web Management Components Installation

3.3.3 DigitalPersona LDS on Amazon Web Services

A delightful slice of the Crossmatch DigitalPersona platform, this is a low cost, cloud based, identity authentication as a service offering (IAaaS). Basically, the same as the "Enterprise Business - DigitalPersona LDS flavor" recipe above, except all running off-premise, in the cloud.

To deploy, simply

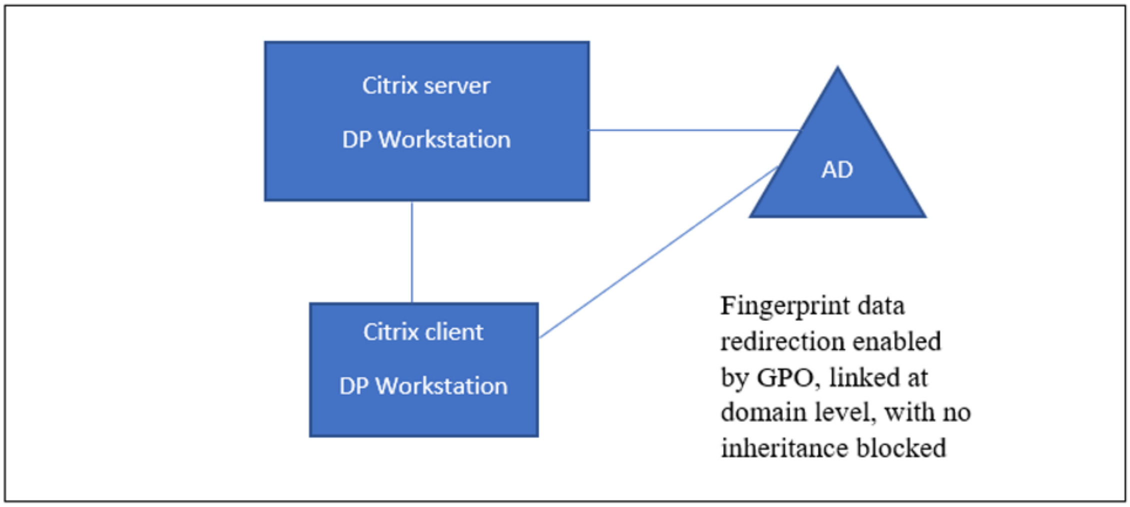
Recipe
1. Add the (Crossmatch) DigitalPersona Amazon Machine Image from the AWS Marketplace to your AWS setup. You pay Amazon for VM resources and pay HID Global for the required product and feature licenses.
2. Your new VM will spin up and set up DigitalPersona LDS.
3. Then join it to your domain, set up optional policies, and start enrolling users for multifactor authentication.

Chapter 4

4 Specials

4.1 Citrix

Recipe	References
1. Install a DigitalPersona client on the Citrix server(s) and on the client computers. **Note**: XenApp 7.5, XenDesktop 7.5, and Citrix Receiver 3.4.0 are supported.	*HID DigitalPersona Client Guide* DigitalPersona Workstation Installation Chapter: Citrix Support
2. Ensure that the fingerprint data redirection GPO is enabled. `Computer config / Polices / Admin Templates / DigitalPersona AD Client / Authentication devices / Fingerprints / Redirect fingerprint data` This is needed to RDP from one client to another and to use fingerprint and other factors.	*HID DigitalPersona Administrator Guide* Chapter: Policies and Settings Topic: Authentication Devices
3. Use Microsoft RDP or Citrix ICA as your VDI transfer protocol.	
4. If the Citrix client is installed after, or updates, on the DigitalPersona Workstation client, then a repair or re-install will re-register the needed DigitalPersona Citrix ICA DLLs.	



Fingerprint data redirection enabled by GPO, linked at domain level, with no inheritance blocked

4.1.1 Additional configuration

Recipe	References
1. 1.Remove duplicate tray icon (if present). Disable the Show taskbar icon setting at: `Computer Configuration >Polices > AdministrativeTemplates: Policy definitions > DigitalPersona Client > General Administration`	Chapter: Citrix Support Topic: Resolving duplicate DigitalPersona system tray icons
2. Enable DigitalPersona tray icon (if missing). Set following registry key to 0x20. `HKEY_LOCAL_MACHINE/System/CurrentControlSet /Control/Citrix/wfshell/TWI/SeamlessFlags`	Chapter: Citrix Support Topic: Resolving missing DigitalPersona system tray icon
3. If the load on the Citrix is too high and causing issues, remove the DigitalPersonaAgent by running `DigitalPersonaAgent.exe /unregserver`	

4.2 OTP authentication for RADIUS VPN

Enhance an existing VPN solution by adding OTP to your existing password credential or replacing your password with OTP. DigitalPersona provides support for RADIUS VPN with OTP via the DigitalPersona NPS Plugin. Windows Server with the NPS Role is a prerequisite.

The OTP code itself is entered with the VPN credentials, or if using Push OTP the word "push" may need to be entered as part of the credentials - see the Syntax column in the table below.

VPN authentication protocol	OTP setup	Syntax for VPN authentication by *username* and *password* fields	Notes
			▪ OTP is the actual six-digit code. ▪ push is the word "push". ▪ The commas are entered.
MS CHAP v2	Push OTP	un: username,push pw: password	3x factors: UN, PW, OTP; requires Credential enrollment
	OTP	un: username,OTP pw: password	3x factors: UN, PW, OTP

VPN authentication protocol	**OTP setup**	**Syntax for VPN authentication by *username* and *password* fields**	**Notes**
PAP Use PAP with SSTP or maybe L2TP, but not with PPTP	"autopush"	un: username pw: password	Available by default in DigitalPersona v3.1 and higher, tries push, then non-push automatically. 2x factors: UN, OTP; requires Credential enrollment.
	Push OTP w/ VPNAllowOTPOnly=1	un: username pw: push	2x factors: UN, OTP; may be okay to use with less secure VPN auth protocols as password is not transmitted; requires Credential enrollment.
	OTP w/ VPNAllowOTPOnly=1	un: username pw: OTP	
	Push OTP	un: username pw: password,push	3x factors: UN, PW, OTP; requires Credential enrollment.
	OTP	un: username pw: password,OTP	3x factors: UN, PW, OTP

Recipe	References
1. Have, or setup, a VPN Server. 2. Have and configure, or setup, a Network Policy Server (NPS). If setting up, add the "Network Policy and Access Services” role. 3. On the Getting Started page, select RADIUS server for Dial-Up or VPN Connections from the dropdown menu and then click Configure VPN or Dial-Up. 4. Add a new RADIUS client, which is the VPN server. 5. Use a shared secret and MSCHAP2 to secure the NPS / VPN server communication. 6. Specify MPPE encryption settings. 7. In the NPS console, under Policies, select Connection Request Policies. Then, in the main panel, double-click Virtual Private Network (VPN) Connections to display its Properties page, then click the Settings tab and, select Authentication Methods. 8. Select override network policy authentication settings. 9. Select either MSCHAP2 or PAP as appropriate for your environment and security needs; see the table above.	Chapter: DigitalPersona NPS Plugin Topic: Installing Network Policy Server (NPS)
10. Configure your VPN Server to use the NPS RADIUS server.	Chapter: DigitalPersona NPS Plugin Topic: Configuring your VPN Server to use the NPS RADIUS server
11. Install the DigitalPersona NPS Plugin by running its .exe on the same server as the NPS server and restart the machine.	Chapter: DigitalPersona NPS Plugin Topic: Deploying the DigitalPersona NPS Plugin
12. See the white cells in the previous table. To authenticate to your VPN connection through OTP (One-Time Password) only, on the NPS server, create and set to "1" - `HKLM\SW\DigitalPersona\Policies\Default\TOTP\VPNAllowOTPOnly`	
13. Test a VPN Client, see previous table for syntax.	

Notes:

- The NPS plug-in is all or nothing for the whole server, aside from typing or not typing “push” all users will have to use the same protocols and configuration.
- NT Rad Ping, PAP Radius Test client: https://www.novell.com/coolsolutions/tools/14377.html
- NPS Best Practices: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-best-practices
- NPS Role History https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831683(v=ws.11)

4.3 Secret sauce

None of the other recipes in this cookbook a good fit for your needs? When your requirement goes beyond what a recipe can fulfill, get some quotes from your Sales representative on our Professional Services; let the identity exports artfully mix up a custom solution for you.

Chapter 5

5 Side Orders

5.1 Credential enrollment

DigitalPersona provides two primary methods of credential enrollment: attended-enrollment and self-enrollment. There are two ways to do attended enrollment: through the DigitalPersona Workstation client, or through DigitalPersona Web Enrollment. The following table shows the availability and default status of the different types of enrollment.

Enrollment method	DigitalPersona AD	DigitalPersona LDS
W32 Self-enrollment	By default, with Workstation client (included in DigitalPersona AD).	Optionally enabled, with Workstation client (included in DigitalPersona LDS).
Web Self-enrollment	HID DigitalPersona Administrator Guide Chapter: Policies and Settings Topic: Authentication Devices	Optionally enabled, with Web Management Components (included in DigitalPersona LDS above).
W32 Attended Enrollment	Optional feature in Custom install of DigitalPersona Workstation (see Recipe below).	Optional feature in Custom install of DigitalPersona Workstation. Needed unless self-enrollment is explicitly enabled and used instead (included in DigitalPersona LDS).
Web Attended enrollment	By default, with Web Management Components (included in DigitalPersona AD).	Optional install. Installed by default with Web Management Components (included in DigitalPersona LDS).

5.1.1 Attended Enrollment: Full client, AD flavor 🌶

Out of the box with DigitalPersona AD, end users can self-enroll and manage all their own credentials. Generally, this is sufficient and preferred. For added control and security, the full Win32 client Attended Enrollment application can be used

Security officers, or enrollers, are people with an AD User who is a member of the Attended Enrollers group. An enroller launches the DigitalPersona Attended Enrollment application (custom optional install part of the DigitalPersona AD Workstation client) either with a Run As, or logged on as the enroller. The end user enrolls just as they would self enroll, except the security officer is watching them, and then also authenticates/validates the enrollment when it's done.

It's possible to set up a hybrid where users in specific OUs can self enroll. Setup attended enrollment as per the Administrator Guide, then re-create the DigitalPersona allowed user self register/delete permission, but at a sub-OU of Users level instead of at the domain level.

Anyone can register their fingerprints and use a DigitalPersona license on a DigitalPersona workstation. Attended Enrollment effectively limits and controls DigitalPersona license use and allocation.

Recipe	References
1. Create AD groups a. Create and nest AD Groups granting them allow rights to Register/Delete Fingerprint (DigitalPersona) against Descendant User objects. b. Secondary to doing the group permission above, Run As the Attended Enrollment component with domain admin rights and/or use a domain admin as the security officer account.	Chapter: Attended Enrollment Topic: Setting up Attended Enrollment
2. Install Attended Enrollment The Attended Enrollment component is part of the DigitalPersona Workstation custom install; do a Modify on an installed DigitalPersona Workstation to add it.	*HID DigitalPersona Client Guide* Chapter: DigitalPersona Attended Enrollment installation Topic: Local installation
3. DigitalPersona version 3.0.0 and above: Configure the Enrollment Policy GPO.	*HID DigitalPersona Administrator Guide* Chapter: Policies and Settings Topic: Enrollment Policy
4. For DigitalPersona versions prior to 3.0.0: Configure attended enrollment instance a. An admin authentication at the end of the wizard, or admin overrides on omits, may be needed - these requirements can be tuned per workstation via a self-documented XML file b. Once optimized, this config file can be copied and re-used. c. Ensure full tag closure on the end of the line after any edits.	*HID DigitalPersona Client Guide* Chapter: DigitalPersona Attended Enrollment Topic: Customizing Attended Enrollment

Recipe	References
Example (before changes): Shows tiles for Fingerprints, Cards, PIN and OTP. <excludedNodes> <!-- <add value="DE9F54BE-F6B9-4306-BC67-DDD71B27B35B" /> --> <!--Password--> <!-- <add value="CBFFA046-6267-4594-AB5C-11A7B5B97035" /> --> <!--Fingerprints--> <!-- <add value="4FA5D027-18C9-4766-97B9-CE3C5962476F" /> --> <!--Cards--> <!-- <add value="B07C25CA-FE67-48F1-AC7D-3B204108F52C" /> --> <!--PIN--> <!-- <add value="9AC39EB1-FCD3-4207-B98A-5B290B2AB8CA" /> --> <!--OTP--> <add userType="Altus" value="A6421E1B-6E67-411B-ABBC-45AE4811E6C6" /> <!--Recovery Questions--> <add userType="AD" value="BCC6142F-CE8B-4B48-B605-342842B3DDDB" /> <!--Photo--> <add userType="AD" value="24FAC572-AE57-45E2-ACCF-4417A44A9F02" /> <!--Custom Page 1--> </excludedNodes>	
Example (before changes): Shows tiles for Password and Fingerprints only. <excludedNodes> <!-- <add value="DE9F54BE-F6B9-4306-BC67-DDD71B27B35B" /> --> <!--Password--> <!-- <add value="CBFFA046-6267-4594-AB5C-11A7B5B97035" /> --> <!--Fingerprints--> <add value="4FA5D027-18C9-4766-97B9-CE3C5962476F" /> <!--Cards--> <add value="B07C25CA-FE67-48F1-AC7D-3B204108F52C" /> <!--PIN--> <add value="9AC39EB1-FCD3-4207-B98A-5B290B2AB8CA" /> <!--OTP--> <add value="A6421E1B-6E67-411B-ABBC-45AE4811E6C6" /> <!--Recovery Questions--> <add userType="AD" value="BCC6142F-CE8B-4B48-B605-342842B3DDDB" /> <!--Photo--> <add userType="AD" value="24FAC572-AE57-45E2-ACCF-4417A44A9F02" /> <!--Custom Page 1--> </excludedNodes>	
5. Attended enrollment workflow a. Open the tool with rights. b. End-user authenticates. c. End-user enrolls. d. Admin user authenticates to authorize finalization of enrollment (if so configured).	

5.1.2 Software OTP

OTP is One Time Password. Out of the box you get support for soft-token OTPs. Soft Token OTP is done using the DigitalPersona app on iPhone and Android phones, available on the respective platform's app store - search for DigitalPersona.

5.1.3 Hardware OTP

Some Onetime Password (OTP) hardware tokens can be used as authentication factors in DigitalPersona. A Hardware Token OTP is configured first by importing a seed file obtained with purchase of the hard tokens; for a token to be enrolled by a user it must already be imported and in a pool of available tokens.

Import scenario	**Reference**
From the command line, run - `C:\Program Files\DigitalPersona\Bin\DPOTPMgr.exe /i /f`	Chapter: Administration Tools Topic: Hardware Tokens Management Utility
From the DigitalPersona Web Administration Console - use the Hardware OTP Tokens tab to import the seed files.	Chapter: DigitalPersona Web Administration Console Topic: Manage Hardware OTP Tokens

Make sure to choose known supported tokens, such as the Vasco Go 6, Feitian OTP c200, or Fortinet FTK-200.

5.1.4 Push Soft OTP 🌶️

Add push notification to the out of the box Soft Token OTP feature, making it even quicker and easier. Instead of having to enter the code from the token into the authentication dialog, the user just okays the push on their phone!

Recipe	**Reference**
1. Obtain Crossmatch Push Notification Server (CPNS) push notification key ID and key for your organization during your implementation, or later, from your Sales Account Manager or Customer Care.	
2. The DigitalPersona authenticator app is needed, either on an iOS or Android device.	*HID DigitalPersona Client Guide* Chapter: Credential Manager Topic: Authenticator app and Push Notification
3. The domain level GPOs Push Notification Server API Key and Push Notification Server Tenant ID must be set.	*HID DigitalPersona Administrator Guide* Chapter: Policies and Settings Topics: Push Notification Server API Key Push Notification Server Tenant ID

5.2 Terminal Server

Reserved for future use.

5.3 Client on Server (ConS)

The DigitalPersona Client on Server feature enables an administrator to secure access to your DCs with DigitalPersona's multifactor authentication. Be sure to install the client only after server, and do not attempt credential management or other features beyond logon and unlock. *ConS is available in the DigitalPersona AD flavor only.*

Recipe	**Reference**
1. Start with the two or more DCs where DigitalPersona AD Server is already installed, along with any patches, and admin tools and their patches	Chapter: DigitalPersona AD Server Installation Topic: Configuring each domain Chapter: Separate installations Topic: DigitalPersona AD Administration Tools
2. Install DigitalPersona AD Workstation and any patches.	*HID DigitalPersona Client Guide* Chapter: DigitalPersona Workstation installation
3. As of March 2018, DigitalPersona AD Server v2.3 patch DigitalPersona11_06_230_001 is critical for this configuration.	DigitalPersona11_06_230_001 patch readme.txt

5.4 Beyond MFA 🌶

DigitalPersona closes the gaps in today's user authentication solutions. In addition to the traditional set of authentication factors - what you have, are and know (such as password, PIN, Fingerprints, PKI Smart Cards, (hard) token, phone with soft token app) - it offers authentication for the contextual risk factors of time, velocity, location and behavior (for example, IP address / geographic location, and biometric typing pattern. These factors cover what you do, where you are, and when you act. Choose the right level of protection for every application, every user and every system.

Physical and BIOS security are additional to MFA.

DigitalPersona offers controls over:

- Logon policy - Windows logon and windows un-lock policy
- Enhanced policy - Step-up, or Enhanced, policies for windows logon/unlock
- Session policy - W32 and websites within a Windows session
- Federation IDP (STS) policy, for application launch, portal access, and web administration.
- Backup accesses: Password recovery, and account access

The logon, session, and enhanced policies are covered in Section 3.1 GPOs for all Entrées and Specials under the OU level heading. The enhanced policy overrides and adds to or extends the logon policy in certain pre-defined situations. The logon, session, and enhanced, policies all work by arranging rows and columns of factors; each row is a set of one or more factors (columns) which all must be used. Users essentially pick on a row to use.

These policies should almost always be set at sub-OU level and not broader, so as to prevent locking yourself, or everyone, out of the domain. Child OUs can be made under production OUs were Computer accounts are, MFA policies linked to these OUs, Computers moved into them, and testing done, before wider adaption.

The DigitalPersona User Query Tool (UQT) reports on which Users have and have not enrolled which factors and features.

MFA can present a catch-22. With self-enrollment, policies should allow password alone initially, then after most user have enrolled, MFA can be enforced. With attended enrollment, MFA can be enforced initially, and users who can't get in can go through the attended enrollment process. An enrollment policy limits which factors user can enroll if they are self-enrolling. Attended enrollment can be configured to require security officer presence, and to require that any omitted factors be notated.

Two features override MFA for emergencies and special exceptions: Password recovery, and account access.

Password recovery allows the user to forget or loss their password, then use three pre-enrolled recovery question answer pairs to either reset their password, or just skip password and get it (can be disabled by GPO). With a password and something else MFA in place, the password recovery would just help get past the password, the something else is still needed.

Account access involves interaction with a domain admin type and allows bypass of MFA.

Note on client behavior with MFA enforced: We have two option how user can authenticate own credentials: 1) local cache or 2) remote DigitalPersonaCA Server. You lost the ability to use option #1 because you wiped out local cache when you uninstall beta version. So you only can use option #2. To use option #2 you would need connection with DigitalPersonaCA Serve located in our CM environment. Which mean you need both 1) internet access and 2) VPN connection to our internal network (you may use Direct Access instead of VPN). You still can use Windows Password but to use any other credential you need wait until you get connected to our internal network. It will be just fine if we allow just password to logon but recently we deploy MFA policy and you would be require to provide something else.

See PM SSO (Password Manager Single Sign-On) section also.

5.5 Password Manager change screen templates

Reserved for future use.

5.6 Password Manager Single Sign-On (SSO)

Password Manager is a feature of the DigitalPersona client. Managed Logons can be used to provide simple SSO to applications, resources and websites.

Recipe	Reference
1. Set the Session Authentication Policy GPO to disabled. `Computer Configuration >Polices > Software Settings > DigitalPersona Client > Authentication > Session Authentication Policy`	Chapter: Policies and Settings Topic: Session Authentication Policy
2. Create managed logons for each resource that you want to use with SSO. a. Launch the Password Manager Admin Tool. b. Click Add Logon to launch the Password Manager Admin Tool Logon Screen wizard. c. Launch the website, application or resource that you want to use with SSO. d. Follow instructions in the wizard. e. On the Logon Screen Properties page, scroll down to the Authentication section and set Start Authentication Immediately to Yes.	*HID DigitalPersona Administrator Guide* Chapter: Password Manager Admin Tool Topic: Creating managed logons

5.7 Kiosk

There are two DigitalPersona clients, Workstation and Kiosk. The workstation client is more common and generally used. The kiosk client is ideal for shared machines, such as in a medical exam room or on the factory floor, for example. Windows logoff and logon between users is eliminated and security is enforced at the application level.

The Kiosk client program logs onto Windows as a shared account, users authenticate as authorized users to logon and unlock Windows. Within Windows Password Manager is used to authenticate with the user's credentials into websites and applications. While only the fingerprint of the logged-on user can be used within the Workstation windows session, any authorized fingerprint may be used within the Kiosk windows session.

Recipe	Reference
1. Create or designate an OU for the kiosk machines. There can be multiple kiosk OUs, each with their own kiosk policies; alternately the DigitalPersona kiosk GPO settings can be done at the domain level and then will apply to all kiosk machines.	
2. Kiosk Session Authentication Policy GPO (Optional) `Computer configuration / Polices / Software Settings / DigitalPersona Client / Security / Authentication / Kiosk Session Authentication policy` Sets one or more single or multi-factor policies for Windows logon and unlock.	Chapter: Policies and Settings Topic: Kiosk Session Authentication Policy
3. Create or designate a (low privileged) AD User as the kiosk shared account	Chapter: DigitalPersona AD Server Installation Topic: Setting up DigitalPersona AD Server for use with DigitalPersona AD Kiosk
4. Kiosk Shared Account Settings GPO Defines the account used for the Kiosk. `Computer config / Polices / Software Settings / DigitalPersona Client / Kiosk Admin / Kiosk Workstation Shared Account Settings` Note that the domain name needed here is the NetBIOS name.	Chapter: Policies and Settings Topic: Kiosk Administration
5. Prevent users from logging on outside of a Kiosk session GPO (Optional) `Computer config / Polices / Software Settings / DigitalPersona Client / Kiosk Admin / Prevent users from logging on outside of a Kiosk session`	Chapter: Policies and Settings Topic: Kiosk Administration

Recipe	Reference
6. Allow interactive use of kiosk account GPO (Optional) `Computer config / Polices / Software Settings / DigitalPersona Client / Kiosk Admin / Logon/Unlock with Shared Account Credentials` Default behavior is for the user to authenticate as themselves (and logon with kiosk shared account). This policy allows the user to provide the kiosk shared account credentials for access to the kiosk.	Chapter: Policies and Settings Topic: Kiosk Administration
7. Auto logon (Optional) `Computer config / Polices / Software Settings / DigitalPersona Client / Kiosk Admin / Allow automatic logon using Shared Kiosk Account` Set this GPO to allow automatic logon using the Shared Kiosk account.	Chapter: Policies and Settings Topic: Kiosk Administration
8. Install the kiosk client The kiosk computer needs to be in the kiosk OU that has the Kiosk GPO linked to it.	*HID DigitalPersona Client Guide* Chapter: DigitalPersona Kiosk installation
9. Logon to the kiosk using the Kiosk user tile, with the kiosk mode checkbox checked.	*HID DigitalPersona Client Guide* Chapter: DigitalPersona Kiosk

5.7.1 Restricting Kiosk access

The default Kiosk behavior is that any authorized user can access a kiosk machine.

If all that is needed for access to the kiosk is an AD username and password, then a user with no license can walk up to a kiosk, logon with AD username and password, take a DigitalPersona license from the license pool, and access the machine.

If you require fingerprint, for example, to access the kiosks, then the user would have to enroll their finger(s) before being able to try to use the kiosk. To limit / control who and how credentials are enrolled, attended enrollment must be used and self-enrollment disabled.

To control which users can use kiosks we have an AD privilege called "kiosk membership". By default, this is set to 'allowed' for users at the domain level and inherits down to OUs and then Users. To configure granular control of users able to access the DigitalPersona Kiosks, follow the recipe below.

Recipe	Reference
1. Remove default kiosk membership from the domain level.	Chapter: Identification List
2. Assign kiosk membership at one or more OUs, where it will inherit down to child OUs and Users.	
3. Enable the Restrict identification to a specific list of users GPO against the DigitalPersona Server(s).	

5.8 ESPM

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

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

Recipe	Reference
1. Install the DigitalPersona AD or LDS Administration Tools.	Chapter: Separate Installations
2. Specify custom user policies for log on to Windows.	Chapter: Extended Server Policy Module

5.9 Thin Clients

Reserved for future use.

5.10 VPN Support

There are various types of VPNs and ways DigitalPersona interacts with them. A Site to site or certificate-based VPN could be transparent to DigitalPersona. RADIUS could be enhanced with second, perhaps push, factor. Thick VPN client, assuming authentication after Windows logon, could be DigitalPersona Password Manager enabled. SSL VPNs can be made to authenticate via DigitalPersona factors. Using DigitalPersona STS's proxy feature enables DigitalPersona client / server traffic over a limited VPN-like connection.

5.10.1 RADIUS

OTP authentication for RADIUS VPN is detailed in the Specials section.

5.10.2 Thick client VPN client

Method: User has cached credentials to enter Windows/AD credentials. Launches 32 or 64 bit VPN client. VPN client is Password Manager (PM) trained, so user is prompted for MFA credentials as per DigitalPersona configuration, DigitalPersona fills in VPN credentials. Assumes authentication after Windows logon.

DigitalPersona set-up: Train VPN page in Password Manager.

5.10.3 Site to site or certificate-based VPN

This type of VPN works not only with DigitalPersona, but with most other software platforms. Common use cases are laptops in police cars or sanitation trucks running DigitalPersona AD Workstation client, connecting to headquarters (AD and DNS and DigitalPersona server) as though they were hard-wired to the network.

Method: This Type of VPN is established from Corporate Firewall to External Firewalls. It is transparent to DigitalPersona.

DigitalPersona set-up: Nothing additional on DigitalPersona side.

5.10.4 SSL VPN

Method: User accesses SSL VPN webpage, authenticates with an option below.

DigitalPersona set-up, one of:

- Password Manager (PM) supports only publishing username and password.
- With Radius support OTP Only (6 Digit OTP or Push OTP)
- With ADFS Plugin support federation authentication using Fingerprint and OTP (email, SMS, Push OTP, OTP)
- With DigitalPersona STS, supports all factors i.e. Fingerprints, PKI Smart Cards, Contactless Writable Cards, OTP (Email, SMS, Push OTP, OTP) in addition also supports Behavior biometrics.

Chapter 6

6 Desserts

6.1 No local cache 🌶️

Extra Secure configuration as this forces server authentication only. With no local cache setup, authentication requires network and server; there are significantly less vectors for offline attacks. With added security comes a loss of convenience and redundancy.

Recipe	References
1. Against the domain, or OU(s) of Computers, set to DISABLED: `Computer / Polices / Admin Templates / DigitalPersona Client / Authentication devices / Fingerprints / Cache user data on local computer`	Chapter: Policies and Settings Topic: Computer Configuration \ Administrative Templates **Note**: Even though this setting is under Fingerprints, it actually applies to all credentials.

6.2 Password Recovery Questions

You may find your environment is too secure with DigitalPersona deployed. Users are having trouble getting in if they forgot a password or are missing a factor or reader that day. To provide a sort of backdoor to allow users to regain access to their account, use Recovery Questions, instead of a call to the help desk.

This optional feature is potentially less secure than just using strong multi-factors.

Recipe	References
Enable and set the following GPOs either at the domain level, at an OU of computers, or as appropriate depending on the AD OU and GPO structure which machines need the feature set.	**Note**: Before being able to use this feature on a given Windows instance, users have to not only have enrolled self password recovery answers, but must have successfully logged on and off Windows at least once.
`Computer / Polices / Administrative Templates / DigitalPersona Client / Security / Settings / Enable Recovery Questions` Here you can select which questions are available, and even create your own questions.	Chapter: Policies and Settings Topic: Enable Recovery Questions

Recipe	References
`Computer / Polices / Software Settings / DigitalPersona Client / Security / Enrollment / Enrollment Policy` (Optional) Ensure "Self Password Recovery" is selected.	Chapter: Policies and Settings Topic: Enrollment Policy **Note**: This policy is likely already set at domain or OU level.
`Computer / Polices / Admin templates / DigitalPersona Server / Credentials verification lockout / Allow users to unlock their Windows account using DigitalPersona Recovery Questions` (Optional) Configure whether or not users are allowed to unlock their Windows account using DigitalPersona Recovery Questions.	Chapter: Policies and Settings Topic: Allow users to unlock their Windows account using DigitalPersona Recovery Questions
`Computer Configuration/Policies / Administrative Templates / DigitalPersona AD / General / Authentication devices / Recovery Credentials / Self Password Reset / Allow users to reset their Windows passwords` (Optional) Configure whether users are allowed to reset their Windows password using DigitalPersona Recovery Questions or the Forgot Password link on the Identity Provider (STS) page.	Chapter: Policies and Settings Topic: Allow users to reset their Windows passwords

6.3 Report Server

Collates DigitalPersona data and provides both canned and customizable reports for regulatory and audit compliance. Events from DigitalPersona Servers, Web Components and Clients are consolidated, and reports viewed and managed in the DigitalPersona Reports web console. A Dedicated (or shared) SQL server machine is needed. Events are copied to a central server, which creates some network load.

Recipe	References
1. A database (DB) machine is needed, basically any member server with enough resources to pull data from clients and to run SQL. Note that VMs are generally not recommended for SQL.	
2. Install DigitalPersona Reports a. Reference DigitalPersona Reports readme.txt b. May install SQL Express and IIS for you, with some reboots as needed. c. GPOs are configured as a part of these steps via manual and import tasks. d. FQDN for your environment needs to be set in the Subscription Manager setting.	Chapter: DigitalPersona Reports Topic: Install and configure DigitalPersona Reports

This page is intentionally left blank.

hidglobal.com