The DigitalPersona DP AD / LDS Cookbook:

Recipes for cooking up solutions with the DigitalPersona platform

For version 2.3

As of June 2018

Table of Contents

What the DP Cookbook is all about

The DP Cookbook is a series of recipes for cooking up solutions with DP products and components. The recipes are presented in a restaurant style, where the customer choses a meal, consisting perhaps of an appetizer, main dish, a side, and a dessert. We leave the beverage choice to the IT professional doing the cooking and dining.

We have a wonderful trilogy of Admin Guides (DP AD, DP LDS, and DP client) which contain all the information in this cookbook, and more. The admin guides, however, can be too big and reference oriented, whereas, this cookbook is a kind of quick start guide, with pointers to the more verbose and denser admin guide reference material. Please parse through this cookbook to find the dish, or combination of dishes, that meets your security and convenience requirements.

As quality ingredients are crucial for good foods, Crossmatch Inc. provides the DigitalPersona suite of quality software components for the reader to assemble. The DigitalPersona platform, consist of a range of software, hardware, and, integration products. One core piece used in most environment's configurations is the Crossmatch DigitalPersona DP AD Server, DP AD for short. The suite has two main flavors, AD (leveraging Microsoft Active Directory), and LDS (leveraging Microsoft Lightweight Directory Services). AD uses Microsoft Active Directory for storage, LDS uses Microsoft AD LDS for storage; both use AD GPOs for client and server configuration. DP Web Components brings web based user management and enrollment. DP Web Components also serves up DP STS (Secure Token Service), providing web based multifactor federation or Office365 access. DP LDS requires the web console for management, DP AD uses extended Microsoft consoles and the web console can be used as an alternative management interface for some tasks.

Recipes in this cookbook give a higher-level overview of steps needed, and explicitly reference more detailed steps from the following documents, all available here: https://www.crossmatch.com/company/support/documentation/.

- Crossmatch DigitalPersona DP v2.3 – **AD Administrator** Guide
- Crossmatch DigitalPersona DP v2.3 – **LDS Administrator** Guide
- Crossmatch DigitalPersona DP v2.3 – **Client Guide**
    - DP 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
- Crossmatch DigitalPersona DP SSO for Office 365 On Premise – AD Deployment Guide
- Crossmatch DigitalPersona DP SSO for Office 365 On Premise AD – LDS Deployment Guide

All **patches** can be found here: http://downloads.crossmatch.com/

Note that if upgrading an existing setup to v2.3, use the steps in the DigitalPersona DP v2.3 – AD and LDS **Update Notes** instead of the admin guides.

 Hot peppers indicate an extra secure feature-set.

Appetizers / Starters:

Single Server Test / Lab Test Platter!

Windows/AD logon and unlock, Password Manager; DP web console (optional). All on one server machine, with one client. Could be two VMs, or a VM and a physical machine for the client. DP AD flavor.

Recipe	References
1. Build a Windows server, promote it to DC in a new domain in a new forest running AD integrated DNS	
2. Build a client machine with a Windows client OS, point to the new server for DNS, and join to new domain as a member	
3. On the new DC:	
a. Run DP schema extension	DP AD Admin guide / DigitalPersona AD Server Installation chapter / Extending the Active Directory Schema section (page 19 of v2.3)
b. Run DP domain config	DP AD Admin guide / DigitalPersona AD Server Installation chapter / Configuring each domain section (page 20 of v2.3)
c. Increase/clear rangeUpper	DP AD Admin guide / Changing Password Manager Data storage limits chapter (page 222 of v2.3)
d. Install DP AD Server and any server patches config	DP AD Admin guide / DigitalPersona AD Server Installation chapter / Configuring each domain section (page 20 of v2.3)

e. Install DP AD Admin Tools and any tool patches; select them all	DP AD Admin guide / Separate installations chapter / DigitalPersona AD Administration Tools section (page 29 of v2.3)
f. Install DP Web Components and any web component patches (optional) You can run through the **"express" setup** here	DP AD Admin guide / Separate installations chapter / Web Management Components section (page 30 of v2.3)
g. Create a network share for Password Manager templates (usually in sysvol or netlogon for redundant client access)	DP AD Admin guide / Password Manager Admin Tool chapter / Create a shared network folder section (page 166 of v2.3)
4. Configure GPOs, setting at the Domain level:	
a. Licenses `Computer Config / Policies / Software Settings / DP Server / Licenses` – Select 'new' and enter license file and password, or license ID and password, previously obtained from Sales	DP AD Admin guide / License Activation & Management chapter / DigitalPersona AD Server activation section (page 54 of v2.3)
b. Enable Redirect fingerprint data `Computer config / Polices / Admin Templates / DP AD Client / Authentication devices / Fingerprints / Redirect fingerprint data`	DP AD Admin guide / Policies and Settings chapter / Redirect fingerprint data section (page 83 of v2.3)
c. Managed Logons (Password Manager) (User policy) `User Configuration / Policies / Admin Templates / DP AD Client / Managed Apps / Password Manager / Managed Logons` Populate this GPO with domain-name UNC path to network share for Password Manager templates (Unlike almost all the other DP polices, this is a User policy)	DP AD Admin guide / Password Manager Admin Tool chapter / User policy settings section (page 192 of v2.3) DP AD Admin Guide / Policies and Settings chapter / DP Client section (page 96 of v2.3)
5. On the new workstation:	

a. Install DP AD Workstation and any workstation patches	DP AD Client Guide / DigitalPersona Workstation installation chapter (page 13 of v2.3)
b. Install DP AD Admin Tools and any tool patches	DP AD Admin guide / Separate installations chapter / DigitalPersona AD Administration Tools section (page 29 of v2.3)
c. Install DP PMAT (Password Manager Admin Tool) and any PMAT patches	DP AD Admin Guide / Password Manager Admin Tool chapter / Installation & setup section (page 165 of v2.3)
6. Setup PM templates a. Open target screen to train b. Open PMAT and launch new logon screen training wizard and train screen c. Apply changes in PMAT	DP AD Admin Guide / Password Manager Admin Tool chapter / Creating managed logons section (page 167 of v2.3)
7. Test / use the system: a. Logon on the client as a domain user, self-enroll credentials as available (password, fingerprint, PIN, OTP, Cards) – then use newly enrolled factors for logon and unlock b. Navigate to PM trained screens and use PM and enrolled factors to fill-in logon screen credentials	DP AD Client Guide / Client Features chapter / Managing user credential section (page 39 of v2.3)

Entries:

GPOs for all Entries and Specials:

Recipe	References
Domain level:	
Licenses `Computer Config / Policies / Software Settings / DP Server / Licenses` Licenses are needed to actually use the product. Licenses are per user storing credential data.	DP AD Admin Guide / License Activation & Management Chapter / License activation Section (page 54 of v2.3)

Select ‘new’ and enter license file and password, or license ID and password, previously obtained from Sales or Implementations Note that while licenses are relevant to DP AD Server only, they end up homed in AD generally and not in a specific GPO but rather accessible from all GPOs	
Enable Redirect fingerprint data This is needed to RDP from one client to another and use fingerprint and other factors. `Computer config / Polices / Admin Templates / DP AD Client / Authentication devices / Fingerprints / Redirect fingerprint data`	DP AD Admin Guide / Policies and Settings chapter / Authentication Devices section (page 83 of v2.3)
Self-enrollment policy For end-user clarity, limit enrollment to factors intended for use. `Computer config / Polices / Software Settings / DP AD Client / Enrollment / Self-enrollment policy`	DP AD Admin Guide / Policies and Settings chapter / Security/Enrollment section (page 79 of v2.3)
Managed Logons (Password Manager) (User policy) Needs to be enabled and configured for managed logon use with Password Manager. `User Configuration / Policies / Admin Templates / DP AD Client / Managed Apps / Password Manager / Managed Logons` Populate this GPO with domain-name UNC path to network share for Password Manager templates Unlike almost all the other DP polices, this is a User policy	DP AD Admin guide / Password Manager Admin Tool chapter / User policy settings section (page 192 of v2.3) DP AD Admin Guide / Policies and Settings chapter / DP Client section (page 96 of v2.3)
Do not launch getting started (optional) Optionally enable this policy if the popup gets annoying, otherwise it may be very helpful for helping get new users enrolled.	DP AD Admin Guide / Policies and Settings chapter / General Admin section (page 87 of 2.3)

Computer Configuration / Policies / Admin Templates / DP AD Client / General Admin / Do not launch the Getting Started wizard upon logon	
Server level:	
Enable ID server (default setting in newest versions) Needed for identification / authentication with just fingerprint and no username; needed for kiosk client support Computer Configuration / Policies / Admin Templates / DP AD Server / Identification Server Settings / Perform fingerprint identification on server	DP AD Admin Guide / Policies and Settings Chapter / Identification Server settings Section (page 94 of v2.3)
Fingerprint enrollment (optional) Sets min and max number of enrollable fingerprints Computer Configuration / Policies / Admin Templates / DP AD Server / Authentication Devices / Fingerprints / Fingerprint enrollment Note that this policy controls fingerprints stored in central database, the separate client policy controls only local (per machine workgroup style, not domain, storage)	DP AD Admin Guide / Policies and Settings Chapter / Authentication Devices Section (page 92 of v2.3)
Fingerprint verification (optional) Sets FAR, or False Accept Rate; this can be tuned up to reduce false-accepts, down to reduce false-rejects. Computer Configuration / Policies / Admin Templates / DP AD Server / Authentication Devices / Fingerprints / Fingerprint verification	DP AD Admin Guide / Policies and Settings Chapter / Fingerprint verification Section (page 93 of v2.3)
PIN enrollment (optional) Computer Configuration / Policies / Admin Templates / DP	DP AD Admin Guide / Policies and Settings Chapter / PIN enrollment Section (page 93 of v2.3)

AD Server / Authentication Devices / PIN / PIN enrollment	
Account lockout duration, reset, and threshold (optional) Mirrors Microsoft AD account lockout due to bad password entry, but for bad biometrics entries. Set number bad to trigger in amount of time and how long locked. Computer Configuration / Policies / Admin Templates / DP AD Server / Credentials verification lockout / .	DP AD Admin Guide / Policies and Settings Chapter / Credentials verification lockout Section (page 93 of v2.3)
OU level:	
Logon Authentication policy Sets one or more single or multi-factor policies for Windows logon and unlock Computer config / Polices / Software Settings / DP AD Client / Authentication / Logon Authentication policy	DP AD Admin Guide / Policies and Settings Chapter / Logon Authentication policy Section (page 76 of v2.3)
Enhanced Logon Authentication policy For specific conditions, replaces 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 could be required for access instead or two. Computer config / Polices / Software Settings / DP AD Client / Authentication / Enhanced Logon Authentication policy	DP AD Admin Guide / Policies and Settings Chapter / Enhanced Logon Authentication policy Section (page 77 of v2.3)
Session Authentication policy Sets one or more single or multi-factor policies for Password Manager use logon to websites and W32 apps Computer config / Polices / Software Settings / DP AD Client / Authentication / Session Authentication policy	DP AD Admin Guide / Policies and Settings Chapter / Session Authentication policy Section (page 78 of v2.3)
Self-enrollment policy	In cookbook above

If needed more granular than domain level Detailed above in “Domain level”	

Enterprise Business – DP AD flavor

Choose Small, Medium, or Large size.

Windows/AD logon and unlock, Password Manager (PM); DP web console. All DP **AD flavor**.

Recipe	References
1. Assumes existing Microsoft AD environment a. For multi-domain AD forests install server in the domain where the users are b. Many authentication functions are supported in multi-forest environments	
2. Overall configuration is: a. Two or more DCs for DP Server, generally with Admin Tools b. Member server(s) for DP Web Components c. Many DP Workstation clients d. One or more administrative workstations with DP Workstation, DP Admin Tools, and the Password Manager Admin Tool (PMAT)	
3. Onetime setup:	
a. Run DP schema extension	DP AD Admin guide / DigitalPersona AD Server Installation chapter / Extending the Active Directory Schema section (page 19 of v2.3)
b. Run DP domain config	DP AD Admin guide / DigitalPersona AD Server Installation chapter / Configuring each domain section (page 20 of v2.3)
c. Increase/clear rangeUpper	DP AD Admin guide / Changing Password Manager Data storage limits chapter (page 222 of v2.3)
d. Create a network share for Password Manager templates (usually in sysvol or netlogon for redundant client access)	DP AD Admin guide / Password Manager Admin Tool chapter / Create a shared network folder section (page 166 of v2.3)

4. On each DC where DP Server will be running:	
a. Install DP AD Server and any server patches config	DP AD Admin guide / DigitalPersona AD Server Installation chapter / Configuring each domain section (page 20 of v2.3)
b. Install DP AD Admin Tools and any tool patches; select them all	DP AD Admin guide / Separate installations chapter / DigitalPersona AD Administration Tools section (page 29 of v2.3)
5. On the **member server**(s) to be web servers (not the DCs, preferably each role on its own member server): a. Install DP Web Components and any web component patches Be sure to **run through the "advanced" setup** here	DP AD Admin guide / Separate installations chapter / Web Management Components section (page 30 of v2.3)
6. Configure GPOs as detailed in the "GPOs for all Entries and Specials" section in the cookbook above.	In cookbook above
7. On the workstations: a. Install DP AD Workstation and any workstation patches	DP AD Client Guide / DigitalPersona Workstation installation chapter (page 13 of v2.3)
8. On administrative workstations additionally install:	
a. Install DP AD Admin Tools and any tool patches	DP AD Admin guide / Separate installations" chapter / DigitalPersona AD Administration Tools section (page 29 of v2.3)
b. Install DP PMAT (Password Manager Admin Tool) and any PMAT patches	DP AD Admin Guide / Password Manager Admin Tool chapter / Installation & setup section (page 165 of v2.3)
c. If going with a side of "Attended Enrollment", that feature can be installed here as well	See side orders here in the cookbook
9. Setup PM templates on an admin workstation with the target app available a. Open target screen to train b. Open PMAT and launch new logon screen training wizard and train screen c. Apply changes in PMAT	DP AD Admin Guide / Password Manager Admin Tool chapter / Creating managed logons section (page 167 of v2.3)
10. Administer and use the system:	
a. Manage users in ADUC	DP AD Admin Guide / ADUC snap-ins chapter / Users and Computers snap-in section (page 61 of v2.3)

b. Manage clients, servers, and users in GPMC	DP AD Admin Guide / Policies and Settings chapter (page 74 of v2.3)
c. Manage users in web console	DP AD Admin Guide / DigitalPersona Web Administration Console chapter (page 137 of v2.3)
d. Web based self-enrollment	DP AD Admin Guide / DigitalPersona Web Enrollment chapter (page 142 of v2.3)
e. Credential enrollment and management i. Self-enroll credentials as available (password, fingerprint, OTP (PushOTP too if added), cards, PIN) ii. Attended enrollment – see "Attended enrollment" add-on section (password, fingerprint, OTP (PushOTP too if added), cards, PIN	DP AD Client Guide / Client Features chapter / Managing user credential section (page 39 of v2.3) See side orders here in the cookbook for Attended enrollment
f. Logon/unlock machines users with password, fingerprint, OTP (PushOTP too if added), cards, and PIN	DP AD Client Guide / Client Features chapter / Managing user credential section (page 39 of v2.3)
g. Navigate to PM trained screens and use PM and enrolled factors to fill-in logon screen credentials (password, fingerprint, OTP (PushOTP too if added), cards, PIN, and even the optional PM SSO)	DP AD Admin Guide / Password Manager Admin Tool chapter / Creating managed logons section (page 167 of v2.3) DP Client Guide / Password Manager chapter / Managed logons and personal logons section (page 58 of v2.3)

Enterprise Business – DP LDS flavor

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

(1) Unable to extend the AD schema for DP use
(2) When DP Server cannot be installed onto any DCs
(3) When non-AD user accounts are needed

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

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

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

Enrollment in DP LDS matrix:		
	W32 thick client	**Web based**
Self-enrollment	Self-enrollment on DP LDS Workstation is standard.	Web self-enrollment must be explicitly enabled. ["Enabling self-enrollment" section of the "DigitalPersona Web Enrollment" chapter of DP LDS Admin Guide, page 200]
Attended Enrollment	The Attended Enrollment Tool is part of the DP Workstation custom install; do a modify on an installed DP Workstation to add it ["Local installation" section of the "DigitalPersona Attended Enrollment installation" chapter of DP Client Guide, page 31] Tune attended enrollment tiles via an XML file ["Customizing Attended Enrollment" section of the "DigitalPersona Attended Enrollment" chapter of DP Client Guide, page 93] Attended enrollment workflow ["DigitalPersona Attended Enrollment" chapter of DP Client Guide, page 71]	Out of the box with DP LDS web attended enrollment is the expected behavior

Recipe	References
DP LDS Database Server On A Member Server	
1. Add roles and features a. Active Directory Lightweight Directory Services role i. .NET Framework 3.5 Features, including HTTP Activation ii. .NET Framework 4.[56] Features, including HTTP Activation 2. .\Server\DigitalPersona LDS Server\Configuration Wizard\DPADLDSConfig.exe (Active Directory Lightweight Directory Services Setup Wizard) 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 rest e. cntr+a then click for all for Importing LDIF Files f. Shows up in “Programs and Features” listed by unique instance name 3. .\Server\DigitalPersona LDS Server\Setup.exe a. Take defaults b. Shows up in “Programs and Features” as DP LDS Server 4. .\Server\DigitalPersona LDS Administration Tools\setup.exe a. Take defaults b. Shows up in “Programs and Features” as DP LDS Admin Tools 5. GPMC / local computer policy a. Computer config / software settings / DP Server / Licenses b. License shows up and properties including number of remaining license seats can be viewed	
DP LDS Web Server On A Member Server Includes create CA, create cert, export and import cert	
1. Add roles and features a. Web server (IIS) b. ASP .Net 3.5 c. AD Cert Services d. Certification Auth 2. Active Directory Certificate Services config a. CA; Enterprise CA; root CA; new private key; SHA-256; defaults; “configure” 3. Certification Auth MMC a. "Manage" Certificate Templates i. 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 i. Subject / common name / *.domainname ii. Alt name / DNS / *.domainname d. General i. Name of your choice e. Private key i. Key options / make exportable	

f. "Enroll" 5. .\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 6. Tweak web config file for separate boxes for components	

DigitalPersona (LDS) on AWS

A delightful recent entry to the Crossmatch DigitalPersona platform, this is a low cost, cloud based, identity authentication as a service offering. Basically, the same as the "Enterprise Business – DP LDS flavor" recipe above, except all running off-premise, in the cloud.

To deploy, simply add the Crossmatch DigitalPersona from the AWS Marketplace to your AWS setup. You pay Amazon for VM resources and pay Crossmatch for licenses. Your new VM will spin up and setup DP LDS, join it to your Domain, setup optional policies, and start enrolling users for multifactor.

Specials:

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 fulfil, get some quotes from Sales on Professional Services; let the identity exports artfully mix up a custom solution for you.

Sides:

DP has two primary methods of enrollment: attended-enrollment and self-enrollment. There are two ways to do attended enrollment: full client, and web based. DP is either AD or LDS flavored. As such, there are a few variations of enrollment to choose from:

Enrollment method	**DP AD**	**DP LDS**
W32 **Self**-Enrollment	By default, with workstation client (Included in Enterprise Business AD, above)	Optionally enabled, with workstation client (Included in Enterprise Business LDS, above)
Web **Self**-Enrollment	By default, with web components (Included in Enterprise Business AD, above)	Optionally enabled, with web components (Included in Enterprise Business LDS, above)
W32 **Attended**-Enrollment	Optional install with Workstation (Recipe below)	Optional install with Workstation - Needed unless self-enrollment explicitly enabled and used instead (Included in Enterprise Business LDS, above)
Web **Attended**-Enrollment	By default, with web components (Included in Enterprise Business AD, above)	Optional install By default, with web components (Included in Enterprise Business LDS, above)

Attended Enrollment – Full client – AD flavor 

Out of the box with DP 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 DP Attended Enrollment application (custom optional install part of the DP AD Workstation client) either with a runas, 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 admin guide, then re-create the DP 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 DP license on a DP workstation. Attended Enrollment effectively limits and controls DP license use and allocation.

Recipe	References
1. AD groups	DP AD Admin Guide / Attended Enrollment chapter / Setting up

a. Create and nest AD Groups delegating them rights to perform Attended Enrollment b. Secondary to doing the group permission above, runas the Attended Enrollment tool with domain admin rights and/or use a domain admin as the security officer account	Attended Enrollment section (page 70 of v2.3)
2. Install attended enrollment a. The Attended Enrollment Tool is part of the DP Workstation custom install; do a modify on an installed DP Workstation to add it	DP Client Guide / DigitalPersona Attended Enrollment installation" chapter / Local installation section (page 31 of v2.3)
3. 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 Ensure full tag closure on the end of the line after edits. Example:	DP Client Guide / DigitalPersona Attended Enrollment chapter / Customizing Attended Enrollment section (page 93 of v2.3)

Before – tiles for pw, fp, card, PIN, 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>
```

After – tiles for pw, fp:

```
<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>	
4. 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 configured)	DP Client Guide / DigitalPersona Attended Enrollment chapter (page 71 of v2.3)

OTP is One Time Password. Out of the box you get soft-token OTP. Soft Token OTP is done using the DP app on iPhone and Android phones, available on the platforms app store – search for DigitalPersona.

Hardware OTP

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

Import scenario	Documentation reference
DP AD command line - DPOTPMgr.exe	DP AD Admin Guide / Hardware Tokens Management Utility section (page 51 of v2.3)
DP AD web console	DP AD Admin Guide / Manage Hardware OTP Tokens section (Page 141 of v2.3)
DP LDS command line - DPOTPMgr.exe	DP LDS Admin Guide / Hardware Tokens Management Utility section (page 102 of v2.3)
DP LDS web console	DP LDS Admin Guide / Manage Hardware OTP Tokens section (page 179 of v2.3)

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

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	References

Obtain push notification key ID and key for your organization during your implementation, or later, from Sales Account Manager, or Customer Care.	
The DP authenticator app is needed, either on iPhone or Android.	DP Client Guide / Authenticator app and Push Notification" section (Page 48 of v2.3)
The domain level GPOs Push Notification Server API Key and Push Notification Server Tenant ID must be set.	DP AD Admin Guide (Page 85 of v2.3) DP LDS Admin Guide (Page 121 of v2.3)

ConS

ConS is Client on Server. Secure RDP access to your DCs with DP's multifactors. ConS is available in the DP AD flavor only. Be sure to install client only after server, and do not attempt credential management or other features beyond logon and unlock.

Recipe	References
1. Start with the two or more DCs where DP AD Server is already installed, along with any patches, and admin tools and their patches	DP AD Admin guide / DigitalPersona AD Server Installation chapter / Configuring each domain section (page 20 of v2.3) DP AD Admin guide / Separate installations chapter / DigitalPersona AD Administration Tools section (page 29 of v2.3)
2. Install DP AD Workstation and any patches	DP AD Client Guide / DigitalPersona Workstation installation chapter (page 13 of v2.3)
As of March 2018, DP AD Server v2.3 patch dp11_06_230_001 is critical for this configuration	dp11_06_230_001 patch readme.txt

MFA 

There's a lot going on in multifactor authentication. A factor is something you have, know, or are; password, PIN, fingerprint, smart card, (hard) token, phone with soft token app. Contextual factors such as IP address / geographic location, and biometric typing pattern can be factors too. Physical and BIOS security are additional to MFA.

DP offers controls over:

- **Logon policy** - Windows logon and windows un-lock policy
- **Session policy** - W32 and web credential screens within a Windows session policy
- **Enhanced policy** - Step-up, or Enhanced, policies for windows logon/unlock
- Policy for federated app launch and portal access

The logon, session, and enhanced policies are covered in the "GPOs for Entries and Specials" section 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 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 DP User Query Tool (UQT) can be used to report on which Users have and have not enrolled MFA. 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. A self-enrollment policy is available to limit which factors user can enroll if they are self-enrolling. Attended enrollment can be configured to require security officer presence, and to require omitted factors be notated.

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

Kiosk

There are two DP clients, Workstation and Kiosk. The workstation client is more common and generally used. The kiosk client is ideal for shared machines, in a medical exam room or factory floor, for example. Windows logoff and logon between users is eliminated and security is at the application level. Kiosk 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	References
1. Create or designate an OU for the kiosk machines. There can be multiple kiosk OUs, each with their own kiosk policies;	

alternately the DP kiosk GPO settings can be done at the domain level and then will apply to all kiosk machines.	
2. Kiosk Session Authentication Policy (optional) Sets one or more single or multi-factor policies for Windows logon and unlock `Computer config / Polices / Software Settings / DP Client / security / Authentication / Kiosk Session Authentication policy`	DP AD Admin guide / Policies and Settings chapter / DigitalPersona Client (Detail) section (page 79 of v2.3) DP LDS Admin guide / Policies and Settings chapter / Computer Configuration\Software Settings section (page 111 of v2.3)
3. Create or designate a (low privileged) AD User as the kiosk shared account	
4. Kiosk Shared Account Settings Defines the kiosk `Computer config / Polices / Software Settings / DP Client / Kiosk Admin / Kiosk Workstation Shared Account Settings` Note that the domain name needed here is the NetBIOS name	DP AD Admin guide / Policies and Settings chapter / Kiosk Administration section (page 80 of v2.3) DP LDS Admin guide / Policies and Settings chapter / Computer Configuration\Software Settings section (page 114 of v2.3)
5. Prevent users from logging on outside of a Kiosk session (optional) `Computer config / Polices / Software Settings / DP Client / Kiosk Admin / Prevent users from logging on outside of a Kiosk session`	DP AD Admin guide / Policies and Settings chapter / Kiosk Administration section (page 80 of v2.3) DP LDS Admin guide / Policies and Settings chapter / Computer Configuration\Software Settings section (page 114 of v2.3)
6. Allow interactive use of kiosk account (optional) Default behavior is for 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 `Computer config / Polices / Software Settings / DP Client / Kiosk Admin / Logon/Unlock with Shared Account Credentials`	DP AD Admin guide / Policies and Settings chapter / Kiosk Administration section (page 80 of v2.3) DP LDS Admin guide / Policies and Settings chapter / Computer Configuration\Software Settings section (page 114 of v2.3)
7. Auto logon (optional) `Computer config / Polices / Software Settings / DP Client`	DP AD Admin guide / Policies and Settings chapter / Kiosk Administration section (page 79 of v2.3)

/ Kiosk Admin / Allow automatic logon using Shared Kiosk Account	DP LDS Admin guide / Policies and Settings chapter / Computer Configuration\Software Settings section (page 114 of v2.3)
8. Install the kiosk client The kiosk computer needs to be in the kiosk OU with the kiosk GPO linked	DP Client guide / DigitalPersona Kiosk installation chapter / Installation section (page 23 of v2.3)
9. Logon to the kiosk using the 'kiosk user' tile with the kiosk mode checkbox checked	DP Client guide / DigitalPersona Kiosk chapter (page 100 of v2.3)

Default 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 DP 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 a 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. Configure granular control of users able to access the kiosks:

(1) Remove default kiosk membership from domain level
(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 DP Server(s)

VPN Support

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

RADIUS

Support for RADIUS VPN with OTP via the DP NPS Plugin.

Method: Windows Server with the NPS Role is a prerequisite. OTP code or POTP (push) submitted with RADIUS VPN authentication password.

DP set-up: Deploy and configure DP NPS Plugin.

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 creds as per DP configuration, DP fills in VPN creds. Assumes authentication after Windows logon.

DP set-up: Train VPN page in PM.

Site to site or certificate based VPN

This type of VPN works not only with DP, but with most other software platforms. Common use case is laptops in police cars or sanitation trucks running DP AD Workstation client, connecting to headquarters (AD and DNS and DP 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 DP.

DP set-up: Nothing additional on DP side.

SSL VPN

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

DP set-up, one of:

a. Password Manager (PM) supports only publishing username and password.
b. With Radius support OTP Only (6 Digit OTP or Push OTP)
c. With ADFS Plugin support federation authentication using Fingerprint and OTP (email, SMS, Push OTP, OTP)
d. With DP STS, supports all factors i.e. fingerprint, smart card, contactless card, OTP (Email, SMS, Push OTP, OTP) in addition also supports Behavior biometrics.

Desserts:

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 / DP Client / Authentication devices / Fingerprints / Cache user data on local computer` Note that even if this is labeled as for fingerprints, it's actually for all factors.	DP **AD** Admin Guide / Policies and Settings chapter / Computer Configuration\Administrative Templates section (page 84 of v2.3) DP **LDS** Admin Guide / Policies and Settings chapter / Computer Configuration\Administrative Templates section (page 119 of v2.3)

Password recovery questions

You may find your environment is too secure with DP 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 access their account, use password self-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
1. Enable and set these GPOs either at the domain level, at an OU of computers, or as appropriate depending on AD OU and GPO structure which machines need the feature set	
a. `Computer / Polices / Admin Templates / DP AD Client / Security / Settings / Enable Recovery Questions` Here you can select which questions are available, and even make your own	DP **AD** Admin Guide / Policies and Settings chapter / Security/Settings section (page 89 of v2.3) DP **LDS** Admin Guide / Policies and Settings chapter / Security/Settings section (page 125 of v2.3)
b. Optional `Computer / Polices / Software Settings / DP Client / Security / Enrollment / Self`	DP **AD** Admin Guide / Policies and Settings chapter / Security/Enrollment section (page 79 of v2.3)

Enrollment Policy Ensure "self password recovery" is not deselected Note that this policy is likely already set at domain or OU level	DP **LDS** Admin Guide / Policies and Settings chapter / Computer Configuration\Software Settings section (page 115 of v2.3)
c. Optional Computer / Polices / Admin templates / DP Server / Credentials verification lockout / Allow users to unlock AD account using recovery questions	DP **AD** Admin Guide / Policies and Settings chapter / Computer Configuration\Administrative Templates section (page 93 of v2.3) DP **LDS** Admin Guide / Policies and Settings chapter / Computer Configuration\Administrative Templates section (page 127 of v2.3)
2. 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 logged onto and off of Windows successfully	

Report Server

Collates DP data and provided canned and customizable reports for regulatory and audit compliance. Events from clients are consolidated, and reports viewed and managed in a report server web console. Dedicated (or shared) SQL server machine is needed. Events are copied to 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 DP Reports a. Reference DP 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	DP **AD** Admin Guide / DigitalPersona Reports chapter / Install and configure DigitalPersona Reports section (page 110 of v2.3) DP **LDS** Admin Guide / DigitalPersona Reports chapter / Install and configure DigitalPersona Reports section (page 146 of v2.3)