December 2018

Crossmatch DigitalPersona DP AD v**3.0.2** Upgrade Notes

Crossmatch DigitalPersona DP LDS v**3.0.2** Upgrade Notes

General Upgrade and Deployment Information

Product Naming: Pro to Altus to DPCA to DP

- Originally **DigitalPersona Pro for AD** with releases 1.0.0 through 4.4.3
- Then **DigitalPersona Pro for Enterprise** with releases 5.0.0 through 5.5.1
- Product continues with new name **DigitalPersona Altus**, January 2014, resetting to v1.0.0
- Crossmatch DigitalPersona merger April 2014
- Changed from Crossmatch Altus to **DigitalPersona Composite Authentication** (DPCA) between 2.0.0 and 2.0.3, April 2017
- Changed from DPCA to **DigitalPersona (DP)** between 2.2.0 and 2.3.0, December 2017 (Composite Authentication is now simply a feature, and no longer the product name)

DigitalPersona DP **AD** 3.0 can upgrade from the following releases

- DigitalPersona DP AD 2.3.0
- DigitalPersona Composite Authentication AD 2.2.0
- DigitalPersona Composite Authentication AD 2.1.0
- DigitalPersona Altus AD 2.0.3
- DigitalPersona Altus AD 2.0.0
- DigitalPersona Altus AD 1.2.0
- DigitalPersona Altus AD 1.1.0
- DigitalPersona Pro Enterprise 5.5.1
- DigitalPersona Pro Enterprise 5.5.0

DigitalPersona DP **LDS** 3.0 can upgrade from the following releases

- DigitalPersona DP LDS 2.3.0
- DigitalPersona Composite Authentication LDS 2.2.0
- DigitalPersona Composite Authentication LDS 2.1.0

- DigitalPersona Altus LDS 2.0.3
- DigitalPersona Altus LDS 2.0.0
- DigitalPersona Altus LDS 1.2.0
- DigitalPersona Altus LDS 1.1.0

No upgrade path from Pro 5.x to DPCA LDS / Altus LDS / DP LDS

Migration Options for going from Pro 5.5.x

For DigitalPersona Pro 5.5.x to DigitalPersona (DP) AD migration, customers have two options. Customers can choose to self-migrate or choose to use Professional Services (PS).

Crossmatch Solutions Professional Services

Highly recommended for migration from Pro 4.x or Pro 5.x to current AD product are Crossmatch Solutions Professional Services. The Crossmatch Solutions Team can perform the migration for you as a Professional Service. Contact your sales account manager for additional information.

Self-migration

The DP Administration Guide provides some migration instructions. The requirements for DP are basically the same as was for Pro/Altus/DPCA. DP AD server is backwards compatible with, and will support the DPCA AD 2.x, Altus AD 2.x, Altus AD 1.x, and Pro 5.5.x clients. In going to DP, end users will experience a difference in UI etc., so it is advisable to test in a lab, and upgrade the clients via a pilot group first.

Please note: Tech Support, Crossmatch Customer Care (CMCC), cannot be on standby during self-migration projects. Once the migration is complete however, CMCC will support the migrated deployment under standard Maintenance and Support (M&S).

Updating from version Pro 5.0.0 through Pro 5.4.1 to Pro 5.5.1

Upgrading from these versions of Pro requires that you first complete an upgrade to Pro 5.5.1, and then migrate to DP AD 3.0. (Do NOT upgrade to Pro v5.5.2; this is not a roll-up release of post Pro 5.5.1 patches but rather a special build for a specific customer base.) If staying on Pro 5.5.1 for any amount of time it is highly recommended to deploy patch DP08-02-050, a roll-up of fixes for password resets, recovery access, client/server sync, and more, for Pro 5.5.1.

More information on this topic is here: Migrating from Pro versions 4.4.3 through 5.4.1 ► DP AD 3.0.

Updating from a version Pro 4.x earlier than v4.4.3

Upgrading from releases of DigitalPersona Pro for Active Directory prior to v4.4.3 requires that you first complete an upgrade to DigitalPersona Pro for Active Directory 4.4.3 plus patches, then complete an upgrade to DigitalPersona Pro Enterprise 5.5.1 plus patches, and then migrate to DP AD 3.0. If staying on Pro 4.4.3 for any amount of time, please reference the Supplemental Information for DigitalPersona Pro for Active Directory 4.4.3 Software document.

More information on this topic is here: Migrating from Pro 4.x (earlier than v4.4.3) ► DP AD 3.0.

DigitalPersona (DP) "AD" and "LDS" flavors

DigitalPersona **AD**

DP AD is a direct successor and replacement product for the DigitalPersona Pro for AD 1.x to 4.x, DigitalPersona Pro for Enterprise 5.x, Altus AD 1.x to 2.x, and DPCA AD 2.x products.

DigitalPersona **LDS**

DP LDS is similar in many ways to DP AD.

- DP LDS stores data in a Microsoft AD LDS database instead of Active Directory.
- The DP LDS server need not be run on a Domain Controller.
- Active Directory schema changes are *not* required.
- DP LDS allows for both internal use, like DP AD, and external (customer facing) use, with separate licenses.
- DP LDS is generally deployed customized by the Crossmatch Solutions team Professional Services (PS).

Note that the name of the storage database DP LDS uses is Microsoft Active Directory Lightweight Directory Services; for technical clarity the DigitalPersona LDS product is sometimes referred to as DigitalPersona AD LDS.

DigitalPersona **Federal**

DP Federal supports CAC (DoD Common Access Card). This is a wholly separate product with government pricing.

DigitalPersona **LE**

DP Workstation only, bundled at no additional cost, with LSMS software. The assumption is that as most LSMS instances are on non-domain member hosts isolated from the rest of the customer's network, the DigitalPersona Workstation will function as stand-alone without any additional configuration. DigitalPersona will not use the scanner connected to LSMS, rather a U.are.U 4500 or other reader is still needed. (Note that there is an "Guardian Support" driver folder distributed with the DigitalPersona solution that provides Guardian ten-print scanner support – however that is NOT what DP LE is.)

DigitalPersona **Premium**

DP "Base," plus SSO and Password Manager managed logons and SAML support and more.

DigitalPersona **Logon for Windows**

Only for Windows AD logon and unlock, no Password Manager.

Fresh install / deployment of DigitalPersona

This document provides information for *upgrades* and *migrations* of existing Pro / Altus deployments. For fresh installs of DP 3.0, please refer to the Administrator Guides, available at https://www.crossmatch.com/company/support/documentation, and the readme.txt files included with each DP product and some components.

Upgrade Planning

Updating to DigitalPersona 3.0 requires preparation, planning, and testing.

- Review the readme.txt file included with each DP product.
- Review the Administrator Guide and identify any potential changes to the system administration settings.
- DP client installs may have required prerequisites, like a newer .Net framework for example.
- Check crossmatch.com for applicable server and client and tools patches.
- Incrementally deploy and test your system upgrade, i.e.: servers, then pilot clients, then all clients.
- Prepare a software rollback plan.
- Perform a lab test of the upgrade in an environment that approximates your production environment prior to performing a live/production upgrade:
    - Identify the features and policies you've deployed in your environment.
    - Schedule the timing for your upgrade and estimate how long upgrade will take for your environment.
    - Plan for any resources that may need.
    - Identify any special requirements applicable to your environment.
    - Determine how to mitigate downtime.

DP 3.0 clients require DP Server 3.0

DP 3.0 clients cannot be deployed with an DP Server version earlier than the client version. You must complete the upgrade of all Pro/Altus/DPCA/DP Servers prior to upgrading Pro/Altus/DPCA/DP clients.

Backwards compatibility

The DP server is compatible with older clients. This allows for some ease of migration insofar as all clients don't have to be instantaneously updated. Please consult the server product readme.txt for specific compatibility information. For example, the DP Server 3.0 will support the Altus AD Workstation 2.0.3 and Pro Workstation 5.5.1 clients. Note that Altus 2.0.3 clients and lower are not compatible with the DP STS logon page if using fingerprint or cards.

Laptops and tablets with built-in fingerprint readers

DP supports a broad range of built-in fingerprint readers in notebooks. Some driver software is redistributed by Crossmatch and found in the `.\Client\Drivers` folder in the product package. Any third-party fingerprint applications that use these readers must be disabled or uninstalled for the DP client to utilize the reader. WBF (Windows Biometric Framework) drivers should work out-of-the-box.

Recommended False Accept Rate (FAR) Setting

We recommend setting the False Accept Rate to 'Medium High' (1 in 100,000). The FAR used by all DP Servers and clients must be the same value. The FAR is the mathematical probability of two different fingerprints being falsely matched. For specific instructions on configuring the FAR settings for your deployment, please consult the Administrator's Guide. If the FAR is not explicitly set, defaults will be used.

Maintenance and Support

Please contact maintenancecontracts@crossmatch.com for all information and quotes to renew your Maintenance and Support (M&S) contract. M&S covers new major and minor software releases, bug fixes, and access to technical support.

DigitalPersona Biometric Tokenization engine

Tokenized fingerprints are more secure as they are revocable and unlinkable to specific users. Doing a **default** upgrade from DP 2.2 or earlier, to DP 2.3 or later, does **not** implement fingerprint tokenization. To use tokenization, new deployments of DP 2.3 or higher must explicitly select the new Biometric Tokenization

Engine and deselect the Fingerprint Recognition Engine, on all server and client installs. To upgrade from non-tokenized to tokenized requires: deletion of all fingerprints, modification of all clients and servers from the old engine to the new tokenization engine, and then re-enrollment of fingerprints.

Upgrading from DPCA AD 3.0.0 ► DP AD 3.0.2

1. Check crossmatch.com for applicable server and client and tools patches.
2. On **each DP AD Server**.
   a. Note: If using central store follow steps elsewhere in this document.
   b. Remove Altus AD 3.0.0 Administration Tools.
   c. Remove Altus AD 3.0.0 Server.
   d. Install DP AD 3.0.2 Server.
   e. Install DP AD 3.0.2 Administration Tools.
3. If present, **DP Web Components** upgrade. (Optional for DP AD deployments; skip if not present)
   a. Take screenshots or otherwise document from the config wizard.
   b. Backup `C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPPassiveSTS\web.config` file. This config file can also be found in IIS in the STS site. To propagate any customizations made, after the new software install, file-compare the old custom config with the newly created default config and tweak the new with the needed changes.
   c. Uninstall v3.0.0 and select to keep certificates.
   d. Install 3.0.2 and config to use same certificates and settings as documented in step above.
   e. For more detail reference the Upgrading DP Web Services from DP 2.x ► DP 3.0 (both AD and LDS) steps elsewhere in this document.
4. On each **client**
   a. Upgrade from v3.0.0 to v3.0.2, in place, over top.
   b. Reboot client.
5. See also the attended enrollment upgrade changes steps if using this feature.

Upgrading from DPCA AD 2.x ► DP AD 3.0

1. Check crossmatch.com for applicable server and client and tools patches.
2. Run the `.\Server\DigitalPersona AD Server\DigitalPersona AD Server\Schema Extension\`**`DPSchemaExt.exe`**.
3. Run the `.\Server\DigitalPersona AD Server\DigitalPersona AD Server\Domain Configuration\`**`DPDomainConfig.exe`**.
   a. Document any custom, non-default, attended enrollment permissions and/or custom kiosk memberships configured.
   b. Run the domain configuration wizard.
   c. Re-customize any custom attended enrollment or kiosk membership permissions.
4. **Document all GPOs settings.** Once new DP 3.0 .admx / .adml files are installed the settings based on older administrative templates may be un-editable. Settings from .adm files show in the classic nodes. Settings without administrative template or configured and viewed by DLL show in the extra registry settings nodes. Also settings under the DLL extended GPMC editor section may move or be added with v3.0.
5. On **each DP AD Server**.
   a. Note: If using central store follow steps elsewhere in this document.

b. Remove Altus AD 2.x Administration Tools.
c. Remove Altus AD 2.x Server.
d. Install DP AD 3.0 Server.
e. Install DP AD 3.0 Administration Tools.

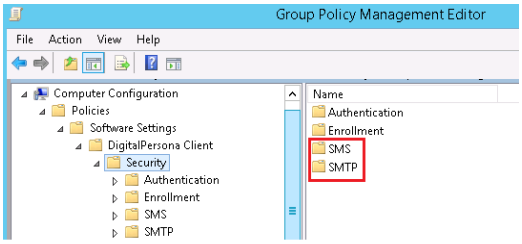
6. **DP Web Components** upgrade. This is optional for DP AD deployments and can be skipped if not present; can be added later also.
   a. Follow the Upgrading DP Web Services from DP 2.x ► DP 3.0 (both AD and LDS) steps elsewhere in this document.
   b. To ensure an upgrade of the DP web server (Web Enrollment and/or Web Admin Console) goes smoothly:
      - If a non-administrative-power user is needed, add the user to the "DPCA SO" group.
      - To demote a "DP_Access" user with domain admin rights from pre-v2.3 delete it prior to installing the v3.0 software. In v2.3 and higher the "DP_Access" user will not be created as domain admin.

7. **Update and transfer GPO policies from DP AD 2.x to DP AD 3.0 using one of these two options.**
   a. Add duplicate settings to same GPO
      i. Note that if there are older settings in use you may not be able to access them to remove them once the new DP .admx files and admin tools DLLs are in place; in this situation use the manually duplicate GPO option just below.
      ii. Instead of using separate GPOs - the same existing GPO can be used.
      iii. Note GPO sections marked as legacy, and policies for new features as you go through.
      iv. Manually go through policies and enable and configure the new DP settings to match the old DP settings.
      v. After client migration is complete, the old policy settings can be cleared; during migration both old and new policies will be in effect with each machine getting the appropriate ones.
   b. Duplicate GPOs; one GPO for 2.x clients, one GPO for 3.x clients
      i. In GPMC identify the GPOs serving DP AD 2.x clients, and rename to note DP v2.x.
      ii. Export GPOs to html reports, or document existing policies, specifically
         1. GPO filtering and security Groups used
         2. Shared managed template folder paths locations
      iii. Create new DP AD 3.x GPOs, set all the desired settings, security filtering if used, and link GPOs properly.
      iv. After all clients are migrated the older DP AD 2.x GPOs can be unlinked and later deleted.
   c. GPO changes
      i. DP AD Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 34 page 251 covers this in detail.
      ii. DP LDS Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 28 page 278 covers this in detail.
      iii. GPO location for SMS OTP has changed. Do not just remove existing/old SMS OTP Nexmo information settings, rather enter the SMS OTP Nexmo information settings again in the new v3.0 GPO location. After upgrade of all DP clients to v3.x remove the v2.x SMS OTP settings.
      iv. Previous and new expanded administrative structures

Previous expanded structure

New expanded structure

v. New expanded software settings



8. Notes on **Password Manager** (PM)
   a. In all Workstation client versions, the DP user console features an **export/backup and import/restore utility. Highly recommended.** This should be used to back up PM credentials, or copy/move them from one machine and Pro/Altus/DPCA/DP version to another. This procedure involves a password protected secret and should be tested before use in production across versions.
   b. Password Manager (PM) v2.0.3 and higher individual logons roam with users, much like managed ones always have. You may want to follow the rangeUpper steps elsewhere in this document to avoid the issue where users can't save logons.
9. On each **client**
   a. Upgrade from v2.x to v3.0, in place, over top.
   b. Reboot client.
10. See also the attended enrollment upgrade changes steps if using this feature.

Upgrading from Altus AD 1.2.0 or 1.1.0 ► DP AD 3.0

1. Check crossmatch.com for applicable server and client and tools patches.

2. Run the `.\Server\DigitalPersona AD Server\DigitalPersona AD Server\Schema Extension\`**`DPSchemaExt.exe`**.
3. Run the `.\Server\DigitalPersona AD Server\DigitalPersona AD Server\Domain Configuration\`**`DPDomainConfig.exe`**.
   a. Document any custom, non-default, attended enrollment permissions and/or custom kiosk memberships configured.
   b. Run the domain configuration wizard.
   c. Re-customize any custom attended enrollment or kiosk membership permissions.
4. **Document all GPOs settings.** Once new DP 3.0 .admx / .adml files are installed the settings based on older administrative templates may be un-editable. Settings from .adm files show in the classic nodes. Settings without administrative template or configured and viewed by DLL show in the extra registry settings nodes. Also settings under the DLL extended GPMC editor section may move or be added with v3.0.
5. On **each Altus AD server**.
   a. Note: If using central store follow steps elsewhere in this document.
   b. Remove Altus AD 1.x.0 Administration Tools.
   c. Remove Altus AD 1.x.0 Server.
   d. Install DP AD 3.0 Server.
   e. Install DP AD 3.0 Administration Tools.
6. **DP Web Components** upgrade. This is optional for DP AD deployments and can be skipped if not present; can be added later also.
   a. Follow the Upgrading DP Web Services from DP 2.x ► DP 3.0 (both AD and LDS) steps elsewhere in this document.
   b. To ensure an upgrade of the DP web server (Web Enrollment and/or Web Admin Console) goes smoothly
      - If a non-administrative-power user is needed, add the user to the "DPCA SO" group.
      - To demote a "DP_Access" user with domain admin rights from pre-v2.3 delete it prior to installing the v3.0 software. In v2.3 and higher the "DP_Access" user will not be created as domain admin.
7. **Update and transfer GPO policies from DP AD 1.x to DP AD 3.0 using one of these two options.**
   a. Add duplicate settings to same GPO
      i. Note that if there are older settings in use you may not be able to access them to remove them once the new DP .admx files and admin tools DLLs are in place; in this situation use the manually duplicate GPO option just below.
      ii. Instead of using separate GPOs - the same existing GPO can be used.
      iii. Note GPO sections marked as legacy, and policies for new features as you go through.
      iv. Manually go through policies and enable and configure the new DP settings to match the old DP settings.
      v. After client migration is complete, the old policy settings can be cleared; during migration both old and new policies will be in effect with each machine getting the appropriate ones.
   b. Duplicate GPOs; one GPO for 1.x clients, one GPO for 3.x clients
      i. In GPMC identify the GPOs serving DP AD 2.x clients, and rename to note DP v1.x.
      ii. Export GPOs to html reports, or document existing policies, specifically
         1. GPO filtering and security Groups used
         2. Shared managed template folder paths locations

iii. Create new DP AD 3.x GPOs, set all the desired settings, security filtering if used, and link GPOs properly.

iv. After all clients are migrated the older DP AD 1.x GPOs can be unlinked and later deleted.

c. <u>GPO changes</u>

i. DP AD Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 34 page 251 covers this in detail.

ii. DP LDS Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 28 page 278 covers this in detail.

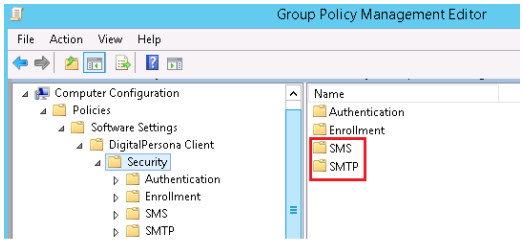
iii. GPO location for SMS OTP has changed. Do not just remove existing/old SMS OTP Nexmo information settings, rather enter the SMS OTP Nexmo information settings again in the new v3.0 GPO location. After upgrade of all DP clients to v3.x remove the v2.x SMS OTP settings.

iv. Previous and new expanded administrative structures

Previous expanded structure

New expanded structure

v. New expanded software settings



8. Notes on **Password Manager** (PM)

a. In all Workstation client versions, the DP user console features an **export/backup and import/restore utility. Highly recommended.** This should be used to back up PM credentials, or copy/move them from one machine and Pro/Altus/DPCA/DP version to another. This procedure involves a password protected secret and should be tested before use in production across versions.

b. Password Manager (PM) v2.0.3 and higher individual logons roam with users, much like managed ones always have. You may want to follow the rangeUpper steps elsewhere in this document to avoid the issue where users can't save logons.

9. On each client.
   a. **If "old" client is v1.2.0 then**: Remove post Altus 1.2.0 patch DP00-04-001 (This roll-up patch was highly recommended for Altus 1.2.0, for general functionality beyond just Chrome, however, the installer does not remove it and so if not removed prior to upgrade it will remain listed on the system but not be removable. If you skipped this step, then simply ignore this artifact left on the machines as it should have no negative impact.)
   b. Upgrade from v1.x.0 to v3.0, in place, over top.
   c. Reboot client.
10. See also the attended enrollment upgrade changes steps if using this feature.

Upgrading from LDS 2.x or 1.2.0 or 1.1.0 ► DP LDS 3.0

1. Check crossmatch.com for applicable server and client and tools patches.
2. **This step relevant only for deployments which started at Altus 1.x.** Note that due to some subtle errors in the early Altus LDS admin guide, the replica AD LDS DB instance may be misnamed. While replicating data, and seeming to appear correctly in the management consoles, it may not actually provide full fail-over functionality. Fail-over should be tested, and if it doesn't work as expected, be re-configured correctly, by full replica DB removal and re-instantiation as per the latest admin guide. Also, if not in place already, recommended is setting the "Computer / Polices / Admin Templates / General Admin / AD LDS instance name" policy explicitly. Note that LDAP Sites and Services is unique and separate from AD Sites and Services.
3. **If "old" server is Altus LDS v1.1.0** then perform the following license change
   a. Do NOT proceed with upgrade until you have new replacement licenses in hand.
   b. The LDS license types (LDS customer-facing and LDS employee-facing) have changed technically; new replacement licenses will need to be obtained from Crossmatch Sales Operations or Customer Care. Existing Altus Employee licenses will need to be deleted manually prior to upgrade. If not removed prior to upgrade these licenses will be displayed as an unknown type and will need to be deleted manually using ADSIEdit.
   c. Prior to the configuration run and server changes, remove the v1.0.0 / v1.1.0 licenses.
   d. After the configuration run and server changes, add the newer v1.2 / v2 /v3 licenses.
4. Run the `.\Server\DigitalPersona LDS Server\DigitalPersona LDS Server\Configuration Wizard\`**`DPADLDSConfig.exe`**. (Note that schema changes mentioned in the LDS product documentation and dialogs is referring to the ADLDS schema and not the Active Directory (AD) schema.)
5. **Document all GPOs settings.** Once new DP 3.0 .admx / .adml files are installed the settings based on older administrative templates may be un-editable. Settings from .adm files show in the classic nodes. Settings without administrative template or configured and viewed by DLL show in the extra registry settings nodes. Also settings under the DLL extended GPMC editor section may move or be added with v3.0.
6. On each **DP LDS server**.
   a. Note: If using central store follow steps elsewhere in this document.
   b. Remove Altus LDS Administration Tools.
   c. Remove Altus LDS Server
   d. Install DP LDS Server v3.0

e. Install DP LDS Administration Tools v3.0

7. **DP Web Components** upgrade.
   a. Follow the Upgrading DP Web Services from DP 2.x ► DP 3.0 (both AD and LDS) steps elsewhere in this document.
   b. To ensure an upgrade of the DP web server (Web Enrollment and/or Web Admin Console) goes smoothly:
      - If a non-administrative-power user is needed, add the user to the "DPCA SO" group, on LDS, additionally add the "DPCA SO" group to the administrators group under role assignments in AZMan.
      - To demote a "DP_Access" user with domain admin rights **from pre-v2.3** delete it prior to installing the v3.0 software. In v2.3 and higher the "DP_Access" user will not be created as domain admin.

8. **Update and transfer GPO policies from DP LDS old to DP LDS 3.0 using one of these two options.**

a. Add duplicate settings to same GPO

i. Note that if there are older settings in use you may not be able to access them to remove them once the new DP .admx files and admin tools DLLs are in place; in this situation use the manually duplicate GPO option just below.
ii. Instead of using separate GPOs - the same existing GPO can be used.
iii. Note GPO sections marked as legacy, and policies for new features as you go through.
iv. Manually go through policies and enable and configure the new DP settings to match the old DP settings.
v. After client migration is complete, the old policy settings can be cleared; during migration both old and new policies will be in effect with each machine getting the appropriate ones.

b. Duplicate GPOs; one GPO for 1.x clients, one GPO for 3.x clients

i. In GPMC identify the GPOs serving DP LDS old clients, and rename to note DP old.
ii. Export GPOs to html reports, or document existing policies, specifically
   1. GPO filtering and security Groups used
   2. Shared managed template folder paths locations
iii. Create new DP LDS 3.x GPOs, set all the desired settings, security filtering if used, and link GPOs properly.
iv. After all clients are migrated the older DP LDS old GPOs can be unlinked and later deleted.

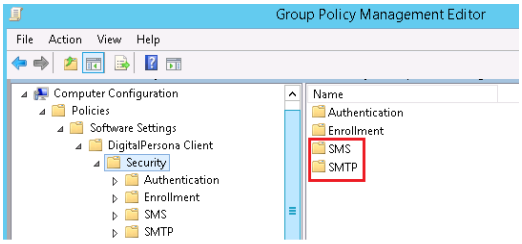
c. GPO changes

i. DP AD Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 34 page 251 covers this in detail.
ii. DP LDS Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 28 page 278 covers this in detail.
iii. GPO location for SMS OTP has changed. Do not just remove existing/old SMS OTP Nexmo information settings, rather enter the SMS OTP Nexmo information settings again in the new v3.0 GPO location. After upgrade of all DP clients to v3.x remove the old SMS OTP settings.
iv. Previous and new expanded administrative structures

Previous expanded structure

New expanded structure

v. New expanded software settings



9. On each **client**
   a. **If "old" client is Altus LDS v1.2.0:** Remove post Altus 1.2.0 patch DP00-04-001 (This roll-up patch was highly recommended for Altus 1.2.0, for general functionality beyond just Chrome, however, the DP LDS Workstation v3.0 installer does not remove it and so if not removed prior to upgrade it will remain listed on the system but not be removable. If you skipped this step, then simply ignore this artifact left on the machines as it should have no negative impact.)
   b. **Upgrade to v3.0**, in place, over top
   c. Reboot client
10. **If "old" server was Altus LDS v1.2.0 or v1.1.0 then note:** After upgrading an administrator may not be able to delete previous "Employee Licenses" using Altus License Manager due to changes in the license format. To resolve the issue, use ADSI (Active Directory Services Interface) editor to delete the record corresponding to the previous license.
11. See also the attended enrollment upgrade changes steps if using this feature.

Upgrading Attended Enrollment to DP v3.0.x

If using attended enrollment (optional), previously an XML config file was needed per machine to configure attended enrollment tiles and workflow, now all this is done through GPOs. With DP version 3.0.x and higher, simply use these central GPO policies instead of individual config files.

1. Computer config / policies / admin templates / DP / general / attended enrollment
    a. Auth of user being enrolled
    b. Security officer auth
    c. Enrolling and omitting
2. Computer config / policies / software settings / DP client / security / enrollment
    a. Enrollment policy

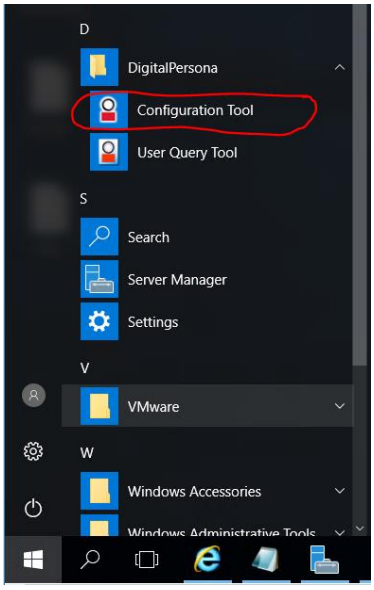
Upgrading DP Web Services from DP 2.x ► DP 3.0 (both AD and LDS)

Web services, and the actual user data, either AD or LDS, are different things, generally on different servers. Web Services upgrade does not touch user data, just IIS and its configuration. Certificates are also untouched by this upgrade.

DP Web Services 2.2 to 2.3 was an in-place, over the top, upgrade. DP Web Services 2.3 to 3.0 upgrade is more of a migration, backing up settings, removing the v2.3, then installing the v3.0, finally, reconfiguring settings.

Upgrade of all DP Web Services should be done at the same time, or as close to the same time as possible, as upgrades of DP Servers. Having different versions of the servers is not supported. With multiple federation servers or other web components services behind a load-balancer, take each webserver offline one at a time and do the upgrade on them.

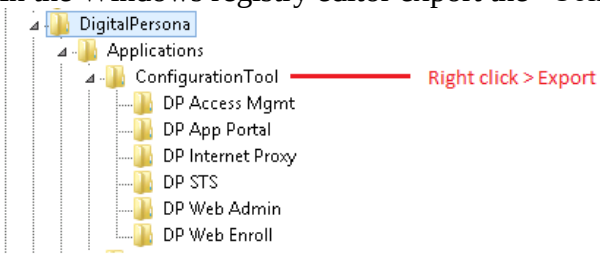
1. **Review / document current settings** prior to the uninstall removing these settings.
    a. Launch DigitalPersona Configuration tool from Start / apps / DP menu.



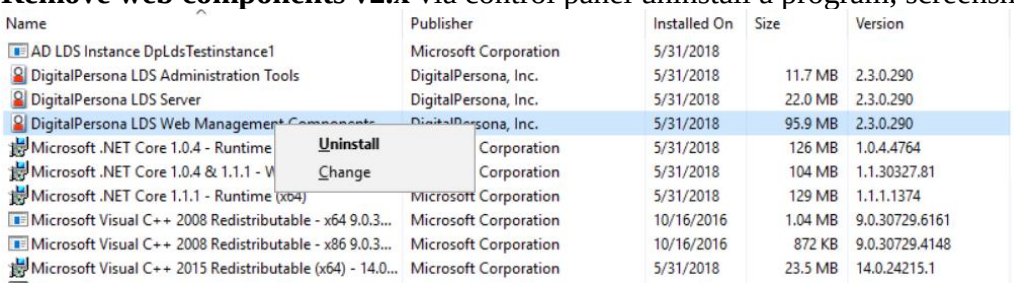
    b. Choose the “Advanced” path and. If warned about resetting config, back up and choose the express path. Screenshot the following from the wizard:
    c. “Publish DP Web Management Components”
    d. “Authentication”
    e. “Step-up Authentication” if shown
    f. “DP Security Token Service” if shown
    g. “Directory access account” and “Authorization Service” screens of the wizard can be ignored.
    h. If you cannot use the wizard to view, then copy off webconfig files from these locations. We can see the setting from these instead of the wizard.
        i. For web policies - C:\Program Files\DigitalPersona\Web Management Components\DP Access Mgmt\DPWebPolicies\web.config
        ii. For STS - C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPPassiveSTS\web.config

iii. For STS - C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPActiveSTS\web.config

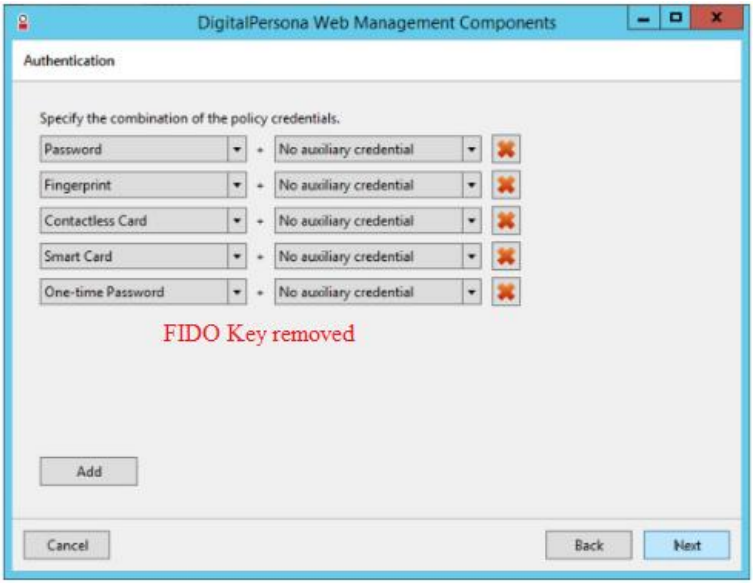
iv. In the Windows registry editor export the “Configuration Tool” folder.



2. **Certificates**
   a. Export with private key your web admin, web enroll, and token signing certificates prior to making any changes. This is to have as a backup.
   b. Keep server certificate that’s in use – step 1. c. above.
   c. Optional certifications cleanup step: Move DP web components related existing certs to 3rd party folder. These certs created by older installs lasted only a year and were generated with each wizard run, whereas the v3.0 and newer code creates longer lasting certs and reuses existing ones. After confirming the v3.x web components installation and configuration created a new cert (when it finds the folder empty, or this is specified in the wizard) the older ones temporarily in the 3rd party folder can be deleted.
3. **Remove web components v2.x** via control panel uninstall a program, screenshot for LDS, similar for AD.



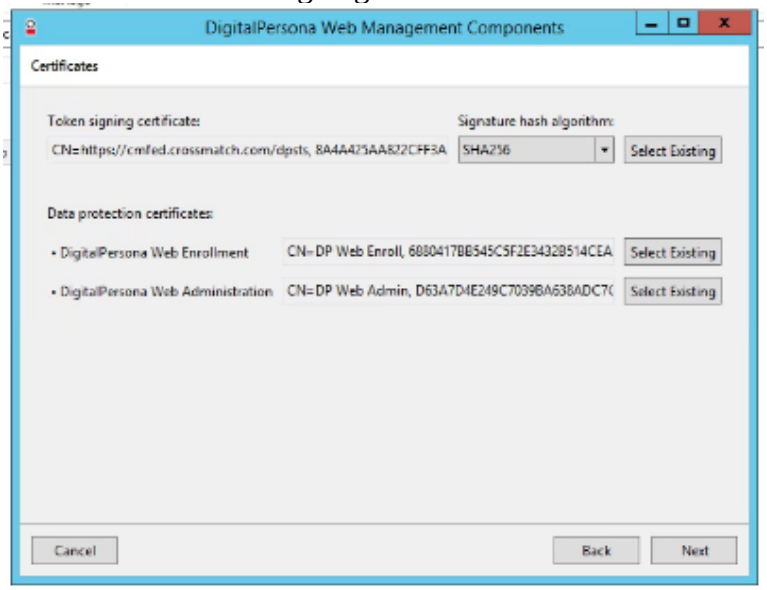
4. Ensure any DP tracing is disabled (unlikely this is on), `HKEY_LOCAL_MACHINE\SOFTWARE\DigitalPersona\Tracing\DoTrace=0`, and trace folder are cleared, `C:\Users\Public\Documents\DigitalPersona\Tracing\`. (If no tracing key then it’s not on.)
5. **Install web components v3.0** from `.\Server\DigitalPersona AD Web Management Components\DigitalPersona AD Web Management Components\`**`Setup.exe`** or `.\Server\DigitalPersona LDS Web Management Components\DigitalPersona LDS Web Management Components\`**`Setup.exe`**, for AD or LDS respectively.
6. **Web components configuration wizard**
   a. Will automatically pops up after a few seconds.
   b. To maintain the same features used and settings from v2.x to v3.0 enter the configurations which were found in step 1.
   c. To implement new features added with version upgraded to, set them up in this wizard. Choose proper base URLs, use existing certificates as appropriate.
   d. If upgrading to v3.0, on the wizard’s authentication screen, where you specify the combination of policy credentials: **remove the FIDO Key** by hitting the red “X” to its right.



Changing the authentication settings from v2.x to v3.0 to include FIDO can change a certificate which might negatively impact your O365 federated authentication. To implement FIDO as an authentication factor for DP web services:

i. Install/configure web components as per these above steps, leaving FIDO out.
ii. Ensure all relevant users enroll FIDO devices.
iii. Once users enrolled, change configuration and enable multi-factor with multiple options including one with FIDO as a secondary factor.

e. In the certificates screen of this wizard reselect the existing corticates, selecting the correct webserver and token signing certificates.



f. On the screen with only the two checkbox items:

i. Leave the IIS add-on console feature checked.
ii. In upgrading to v3.0 **clear the box for IIS replication** as this feature needs some DFS configuration and is not currently fully working.

7. Test by accessing your federated O365 site or launching and authenticating into the DP web console. If load balancing or DNS changes were made to put servers into maintenance, don't forget to revert them.

Migrating from Pro 5.5.x ► DP AD 3.0

Please reference the information in the Migration Options section.

To self-migrate.

1. Check crossmatch.com for applicable server and client and tools **patches** not already detailed in the steps below.
2. Ensure everything is working, to ease potential troubleshooting later.
3. Run the `.\Server\DigitalPersona AD Server\DigitalPersona AD Server\Schema Extension\`**`DPSchemaExt.exe`**.
4. You may want to follow the rangeUpper steps elsewhere in this document to avoid the issue where users can't save logons.
5. Run the `.\Server\DigitalPersona AD Server\DigitalPersona AD Server\Domain Configuration\`**`DPDomainConfig.exe`**.
   a. Document any custom, non-default, attended enrollment permissions and/or custom kiosk memberships configured.
   b. Run the domain configuration wizard.
   c. Re-customize any custom attended enrollment or kiosk membership permissions.
6. **Document all and any GPOs with Pro settings.** Once new DP 3.0 .admx / .adml files are installed the settings based on older administrative templates may be un-editable. Settings from .adm files show in the classic nodes. Settings without administrative template or configured and viewed by DLL show in the extra registry settings nodes.
7. On each Pro / DP AD server
   a. Note: If using central store follow steps, elsewhere in this document.
   b. Note: If upgrading/refreshing DCs (same AD domain) at the same time, you can remove Pro 5.5.1 from the "old" DCs and install DP AD 3.0 onto the "new".
   c. Remove Pro 5.5.1 Administration Tools.
   d. Remove Pro 5.5.1 Server.
   e. Install DP AD 3.0 Server.
   f. Install DP AD 3.0 Administration Tools.
   g. For the DP web server (Web Enrollment and/or Web Admin Console), if a non-administrative-power user is needed, add the user to the "DPCA SO" group.
8. **Update and transfer GPO policies from Pro 5.5.x to DP AD 3.0 using one of the options below.**
   a. <u>Add / duplicate settings</u>
      i. Note that if there are much older Pro settings in use you may not be able to access them to remove them once the new DP .admx files and admin tools DLLs are in place; in this situation use the manually duplicate GPO option just below.
      ii. Instead of using separate existing Pro, and new DP AD, GPOs - the same existing GPO can be used.
      iii. Note GPO sections marked as legacy, and policies for new features as you go through.
      iv. Manually go through policies and enable and configure the DP settings to match the existing Pro settings.
      v. After client migration is complete, the old Pro policy settings can be cleared; during migration both old and new policies will be in effect with each machine getting the appropriate ones.
   b. <u>Manually</u> duplicate GPOs
      i. In GPMC identify the GPOs serving Pro.

ii. Export GPOs to html reports, or document existing policies, specifically
    1. GPO filtering and security Groups used
    2. Shared managed template folder paths locations
iii. Create new DP AD GPOs, set all the desired settings, security filtering if used, and link GPOs properly.
iv. After all clients are migrated, then the older "Pro" GPOs can be unlinked and later deleted.

c. Notes on GPOs
    i. To navigate to all the settings, note that the **Administrative templates** section is expanded with new .admx/.adml files, and the **software settings** section is extended with DLLs.
    ii. The Password Manager path GPO, under the User node, needs to be configured. The Pro 5.x policy is named "Pro", while the different new DP/DPCA/Altus policy has the newer name. Most policies carry over, but do look for a newer setting that replaced it, just in case.
    iii. The newer DP AD GPO policy settings will only be available to view and set after DP Admin Tools are installed.
    iv. Older Pro settings will now be viewed though the filter of newer DP admx files – in order to view with the v5.5.1 admx and snap-in extensions the admin would have to save or build a machine with the v5.5.1 admin tools installed. Alternatively, to cleanup old settings no longer used/needed but which cannot be accessed by the GPMC editor, use the PowerShell `Remove-GPRegistryValue -Name "Default Domain Policy" -Key "[key]" -ValueName "[value]"` command. Note that the `Import-Module -Name grouppolicy` command may likely be needed first, and that the `backup-gpo` command can be used prior to changes being made.

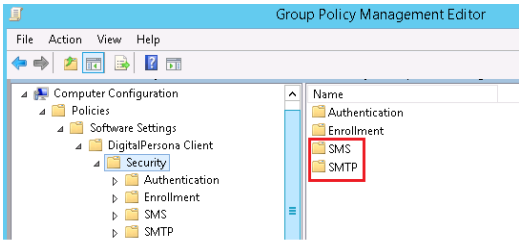
d. Note on GPO policy setting for the kiosk client.
    i. Be sure you know your kiosk shared account passwords prior to migration. If you need to reset them, do so while on the full unchanged v5.5.1 environment.
    ii. Older Pro version policy stored the kiosk shared account password in clear-text, newer DP stores it encrypted. If you have policies with clear-text password content they will not be automatically changed to the newer encrypted format. To get these policies into the newer encrypted format you'll have to recreate the GPO(s).

e. <u>GPO changes</u>
    i. DP AD Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 34 page 251 covers this in detail.
    ii. DP LDS Admin Guide "v2.3 to 3.0 Revised GPO settings" chapter 28 page 278 covers this in detail.
    iii. GPO location for SMS OTP has changed. Do not just remove existing/old SMS OTP Nexmo information settings, rather enter the SMS OTP Nexmo information settings again in the new v3.0 GPO location. After upgrade of all DP clients to v3.x remove the old SMS OTP settings.
    iv. Previous and new expanded administrative structures

Previous expanded structure

New expanded structure

v. New expanded software settings



f. Using the Altus AD Policy Migration Tool for updates to DP AD 2.3.0 plus patches.
   i. As of v3.0.2 release December 2018 this tool is specific to updates to v1.x and v2.x and is not yet compatible with v3.x.
   ii. Detailed in the Migration Guide.
   iii. If the Altus Migration Tool (AMT) reports that DP / Altus / Pro polices have not been detected, then use one of the other options for policy migration.
   iv. Note that this tool may not be part of your DP download, in which case you can request it from your sales account manager or customer care.

9. Notes on **Password Manager** (PM)
   a. In all Workstation client versions, the DP user console features an **export/backup and import/restore utility. Highly recommended.** This should be used to back up PM credentials, or copy/move them from one machine and Pro/Altus/DPCA/DP version to another. This procedure involves a password protected secret and should be tested before use in production across versions.
   b. Password Manager (PM) v2.0.3 and higher individual logons roam with users, much like managed ones always have. You may want to follow the rangeUpper steps elsewhere in this document to avoid the issue where users can't save logons.
   c. PM categories disappear when going from v5.5.1 to v3.x; this is a known issue with no workaround other than manually recreating the categories.

d. All centrally MANAGED logons should continue to work from Pro 5.5.1 to DP AD 3.0. (These are "roaming" templates stored in an accessible network share and managed with the Password Manger Admin Tool, PMAT.)
e. All INDIVIDUAL logons should continue to work from Pro 5.5.1 to DP AD 3.0. (These are templates within each user's Windows profile.) However, to ensure a smooth upgrade of individual PM user logons, during the client upgrade, the workstation should have connectivity to the DP Server(s).

10. **Upgrade clients**
    a. Upgrade/migrate Pro clients from v5.5.x, to DP AD client v3.0, in place / over-top.
    b. Be sure to reboot all clients as part of the install.
    c. **One-way migration -- Password Manager (PM) data secrets saved using DP 3.0 client cannot be opened using Pro 5.5.1**
        i. In going from Pro, to Altus/DPCA/DP, we changed encryption from 3DES to AES (for security improvements), but AES encrypted secrets cannot be read by Pro 5.5.1 clients.
        ii. User PM data stored in AD is migrated from the old to the new format on newer client use.
        iii. During migration any one user should use only one version of the software, Pro 5.5.1 or DP 3.0. He/she must never cross the border. Once a user crosses the border and starts using v3.0, there won't be any way back to v5.5.1 for him/her. This may be an issue with terminal server usage. Pilot groups and waves of client migrations should be selected with care. Once a user uses a 3.0 workstation, they cannot use a 5.5.1 workstation again – if they try to use a 5.5.1 machine after having used a 3.0 machine there are issues.
        iv. Migrate to DPCA 3.0 as soon as possible.

Notes on DP Online client co-installs with DP Workstation

Crossmatch DigitalPersona Online is another product which may be run in parallel with Pro.

Steps for getting Online 5.5.1 and DP 3.0 together.

1. Install DP AD Workstation 3.0.
2. Reboot.
3. If installing any patches decline reboot on workstation install, patch, then reboot once for both.
4. Install DP Online 5.5.1 (decline reboot).
5. Install Patch dp03_01_004.
6. Reboot (for Online client and patch).
7. Repair DP AD Workstation 3.0 (decline reboot, will reboot after registry tweaks).
8. Regedit under Computer\HKEY_Local_Machine\Software\DigitalPersona\Policies (Some keys in steps below may be there from installs above or previous software.)
    a. Add AllowFPRedirect=1 (reg_dword)
    b. Add ForbidFPCompression=1 (reg_dword)
    c. Add TSCompressionType=1 (reg_dword)
9. Under Computer\HKEY_Local_Machine\Software\Policies\DigitalPersona\Altus
    a. Add AllowFPRedirect=1 (reg_dword)
    b. Add ForbidFPCompression=1 (reg_dword)
10. Reboot.

Migrating from Pro versions 4.4.3 through 5.5.1 ► DP AD 3.0

Follow the DigitalPersona Pro Enterprise 5.5.1 Upgrade Notes to get to DigitalPersona Pro 5.5.1. Once on Pro 5.5.1, you can migrate to DP by following the appropriate section of this document. If you plan to stay on Pro 5.5.1 for any period of time, highly recommended is post Pro 5.5.1 Workstation patch DP08-02-050. There are multiple post Pro 5.5.1 patches for third party reader hardware and other issues are available here.

Note: When going from Pro 4.x to Pro 5.x: Though license quantities and the license file extensions may be the same, Pro 4.x and Altus AD / Pro 5.x licenses are programmatically different. A new .dplic file **must be obtained** from M&SOrderDesk@crossmatch.com in going to DP.

In going from Pro 4.4.3 to Pro 5.5.1 you may notice various license count particularities. After a while you may find you seem to be using more licenses on Pro 5.x then you were on Pro 4.x. The Pro 5.x server has a Pro 4.x server module under it which provides backwards compatibility. The 4.x and 5.x licenses are for their specific clients and are managed separately. So, a User accessing a Pro 5.5.1 server(s) from only Pro 4.4.3 client(s) will not affect Pro 5.x license counts or show up in the Pro 5.x User Query Tool results. (If you were to retain a Pro workstation 4.4.3 with the Pro 4.x License Manager Tool, even once you upgraded all your servers to Pro 5.5.1, you would see the 4.x and 5.x licenses separate and more-or-less correct.) Once the User accesses Pro 5.5.1 server(s) from Pro 5.5.1 client(s), then the User will affect Pro 5.x license counts and show up in the Pro 5.x User Query Tool results. There is no clean-up of the Pro 4.x licenses, they are simply abandoned; similarly, once there are no more Pro 4.x clients the Pro 4.x server sub-module and the Pro 4.x DNS SRV RR remain but are no longer used.

Migrating from Pro 4.x (earlier than v4.4.3) ► DP AD 3.0

Follow the DigitalPersona Pro for Active Directory 4.4.3 Upgrade Notes to get to DigitalPersona Pro 4.4.3. Once on Pro 4.4.3, you can upgrade to Pro 5.5.1 by following the appropriate section of this document. There are multiple post Pro 4.4.3 patches available here if you plan to stay on Pro 4.4.3 for any significant amount of time.

Frequently Asked Questions (FAQ)

Q: **Where do I obtain the administration guides and other documentation?**

At https://www.crossmatch.com/company/support/documentation/ you'll find.

- AD Administrator Guide
- LDS Administrator Guide
- Client Guide
- SSO for Office 365 On and Off Premise Deployment Guides
- NetScaler Integration Guide
- Upgrade Notes

Q: **Do I need to run the Schema Extension and/or Domain Configuration Wizard with DP AD?**

From	*To*	*Run schema extension?*	*Run domain configuration?*
DP AD 3.0.0	DP AD 3.0.2	NO	NO
DP AD 2.3.0	DP AD 3.0.x	YES	YES
DPCA AD 2.1 and 2.2	DP AD 3.0.x	YES	YES

Altus AD 1.x and 2.0	DP AD 3.0.x	YES	YES
Pro 5.5.1	DP AD 3.0.x	YES	YES

Versions are numbered Major.Minor.Maintenance. Within a major release the schema is not changed. The domain configuration must be run on even minor updates. Maintenance version changes need neither schema or domain config runs.

Note that **any custom attended enrollment permissions and/or custom kiosk memberships configured will be overwritten to their defaults by the domain configuration run**. The domain configuration will reset the 'register / delete fingerprints' permission back to the defaults. For example, after running the domain configuration, end-users will be able to self-enroll - if you had changed the permissions to prevent self-enrollment, you'll then have to re-configure this again. If you had set up custom attended enrollment group permissions, check to ensure these are still functioning.

Per install of version of DP, you needed to run domain config once per domain, but, aside from resetting some permissions to their defaults, it wouldn't hurt anything if ran more than once outside a single replication cycle. Running the domain config more than once in a domain replication cycle could cause issues, and that's what the warning screen on the domain config details.

Q: I'm **having trouble getting the schema extension to run.** What might I be missing?

Run on the schema master – find which DC this is via the `netdom /query fsmo` command. Ensure the user you are running as is in the schema and enterprise admins groups. Right-click and use the 'run as admin' option.

Q: **Do I need to install administrative templates and/or set GPOs on every Domain Controller (DC) / DP Server?**

No. However, to view Group Policy settings, generally yes, administrative templates need to be present. Administrative templates and GPOs are stored in AD and need only be set once (from any AD Users and Computers or GPMC console) and then they exist in AD and are replicated by AD among all the DCs and to clients.

On Windows 2003 Server .adm files need to be added to GPOs for settings to be available. Windows 2008 Server uses .admx/l files, so this step is no longer needed. If using Microsoft Central Store then .admx/l files need to be manually copied from the default locations to the PolicyDefinitions location. In addition to the Administrative Templates node, DP AD extends the Policies/Software Settings node via a GPMC snap-in extension, which is part of the Administrative Tools install.

Q: **Do I need to add licenses on every DC / DP AD Server?**

No. Licenses are stored in AD for DP AD and in the DP LDS AD LDS database for LDS, and need only be added once; then the licenses are replicated.

Q: **The instructions say to remove Server <older> and then freshly install Server <newer> – will I lose fingerprint or user password data due to these changes?**

No, there should be no user data loss. This is simply the removal of the older version's Authentication Service and then an install of the newer version's Authentication Service; DP data in AD/AD LDS is untouched. Stored in AD/AD LDS is DP's copy of User's domain credentials, OTS/PM secrets from synchronized clients, and OTI/PM secrets from synchronized workstations.

Q: **Where do I obtain these Upgrade Notes?** (If you're reading a print-out, or to send a link.)

Download or view the DP AD Upgrade Notes PDF from here:

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

Server Hardware or Software Changes with DP in Place

Please follow the recommendations detailed below to ensure minimal service interruption, if you are working with an existing production **AD Forest and AD Domain with DP in place** and are refreshing Domain Controller (DC) hardware, upgrading DC Operating System (ex. 2008R2 to 2016 Server), or adding additional DCs and then decommissioning older DCs.

What is Stored in Active Directory (AD)?:

- AD Schema modifications made by the DP AD Schema Extension wizard
- Permission changes made to the AD Domain by the DP AD Domain Config wizard
- DigitalPersona Pro / DP AD licenses
- GPO .admx/.adml/.adm files and actual GPO settings for DP AD
- Users' fingerprint templates
- Users' Password Manager (PM) credentials
- If the Password Manager share is in the AD SYSVOL then this too is stored in AD.

We strongly recommend all DP AD server, client and admin tool software be at the most current versions.

Most day to day DP functionality will be available even without a DP Server being accessible due to DP client caching functionality (by default, caching is enabled) **however:**

- Users will NOT be able to manage fingerprints as this is done through the Server.
- Users will NOT be able to use a fingerprint to access DP clients they've never used a fingerprint to log onto before. (Because their credentials are not in the local cache; credentials are only cached after at least one successful logon.)

If you upgrade or reinstall the server OS and leave DP server in place you will likely have to redo firewall rules for DP. Re-running the DP server will re-apply firewall changes needed. Documenting firewall rules prior to upgrade/re-install is recommended.

How can one test a new DP Server? Stop the Authentication Service on all the DP Servers not being tested and then try managing fingerprints from a DP client. If you get the warning message stating that changes made will be stored locally only, then the DP client is not properly communicating with the DP Server. If you can for example, add a new fingerprint without receiving the warning message, then the Server is accessible and working. You can also see the DP Server is working by using the DP User Query Tool; log to file, and then view the log, looking for an entry detailing a user with newly registered fingerprints.

Gracefully remove DP Server when you decommission a DC running Pro / Altus / DPCA / DP Server. The graceful (programs & features – add remove programs) removal of DP Server does a few things.

- Removes dynamic DNS service records which Pro / DP AD clients use to find the Server
- Removes metadata from AD about the Pro / DP Server (which if left behind can cause some issues)

Example:

You have a fully functional DP AD deployment with two DCs, one of which is an older box running Windows Server 2008R2. You are replacing this DC with new server hardware which will run Windows 2012R2 Server OS.

- All fingerprints, licenses, GPOs. etc. are stored in AD.
- You are already on the current version so there is NO need to run the AD Schema extension or Domain configuration again.

1. Once the Windows 2012R2 server has been promoted to a DC, install DP Server.
2. Gracefully remove DP from the old DC by uninstalling DP Server and then decommissioning the DC as planned.

Administrative Templates

With Pro 5.x and higher some GPO policy settings have been moved from the more traditional Administrative Templates area to a new location – allowing more complex configurations to be created. This GPO location is also where the user licenses are stored. Location is: Computer Configuration, Policies, Software Settings. Remember to look for settings both here and in the Administrative Templates folder.

As a convenience the installation of DP Server automatically.

- Copies .adm files into %systemroot%\inf
- Copies .admx files into %systemroot%\PolicyDefinitions on Server 2008 and later
- Copies .adml files into %systemroot%\PolicyDefinitions\<appropriate language folders> on Server 2008 and later

Password Synchronization tool

If using the optional password synchronization tool, be sure to remove the older version, and install the current version. This must run on all DCs, or none.

Central Store

If using the optional Microsoft central policy definitions store, the admin will have to manually copy .admx/l files to \\FQDN\SYSVOL\FQDN\policies\PolicyDefinitions\ as appropriate. The DP installer is not Central-Store-aware and simply places the files in \\%systemroot%\PolicyDefinitions\.

1. Install the DP Administrative Tools – specifically choose custom and ensure the ADUC and/or GPMC snap-in extensions is installed.
2. Manually copy dp*.admx files from \\%systemroot%\PolicyDefinitions\ into \\FQDN\SYSVOL\FQDN\policies\PolicyDefinitions\
3. Manually copy dp*.adml files from \\%systemroot%\PolicyDefinitions\<appropriate language specific folders>\ into \\FQDN\SYSVOL\FQDN\policies\PolicyDefinitions\<appropriate language specific folders>\

If you have a `\\FQDN\SYSVOL\FQDN\policies\PolicyDefinitions\` folder then you're running Central Store, if you do not have this folder you're not. Microsoft Central Store link.

Licensing

A user license is required for a user to store credential data centrally, allowing "roaming". User licenses can be viewed and managed in multiple ways. In the Group Policy Management Console (GPMC) GPO editor, view the properties of the License ID object. Use the User Query Tool (UQT) to view which users are taking licenses, and for what credentials. All of this licensing section is applicable to DP AD, some detailed here are not available in DP LDS, or they may be done by script or other methods as implemented by Crossmatch Solutions.

General User license workflow:

- Once a DP AD "user", or DP LDS Server "AD user", license has been activated, DP Servers will manage the user license pool.
- When a user registers credentials (fingerprint, smart card, contactless card, proxy card, PIN, Bluetooth device, etc.), and is authenticated by DP Server, that user consumes one user license.
- The use of a Windows / AD password with Single Sign-On (SSO), or with Password Manager managed templates, additionally consumes an DP user license, if not already claimed.
- When a domain user is deleted, its license is returned to the pool for future use.
- When the AD administrator uses the DP AD 'delete license…' option in AD Users & Computers (ADUC), the license is returned to the pool for future use.
- The DP AD Administrative Tools must be in place to access the license node in the GPMC, and the license menus in ADUC.

To activate an additional or new user license:

1. On a computer with the DP Administration Tools installed, open the Microsoft Group Policy Management Console (GPMC).
2. Edit any GPO – the licenses appear in all GPOs.
3. Browse to computer configuration / Policies / Software Settings / DigitalPersona Server / Licenses.
4. You should see any already activated License IDs here.
5. Launch the "Add License…" wizard.
6. Enter License ID and password.
7. At the end you'll see User License total (total of all activated licenses) / number enrolled / number available.

To view the properties of the license itself in AD

1. On a computer with the DP Admin Tools License Activation Manager sub-component installed, open the Microsoft Group Policy Management Console (GPMC).
2. Edit any GPO – the licenses appear in all GPOs.
3. Browse to computer configuration / Policies / Software Settings / {product name} Server / Licenses / select License ID / properties.
4. Here you'll see User License total (total of all activated licenses) / number enrolled / number available.

To view all AD Users taking licenses, having enrolled fingerprints, etc.

1. Launch the User Query Tool (UQT) - part of the DP Administration Tools install.
2. Choose all the relevant checkboxes.
3. View the output from the UQT as a text file and look at the summary at the end; use a spreadsheet application as needed.

To return a user license to the pool

1. Right click on the user account in ADUC (AD Users and Computers) and select ‘delete credentials’ (this step is optional, but avoids some issues if the user does use DP again in the future).
2. Right click on the user accounts in ADUC and select ‘delete license’ (this doesn’t actually delete the license, rather just deletes the link to it).

RangeUpper

To increase the storage space for Password Manager data, make the following change on the AD Domain where your Users are. This is an AD Schema level change done using the ADSI editor.

1. On a computer with the tool installed, running as an account that has rights to modify the Active Directory Schema, launch adsiedit.msc.
2. In the “Connection Settings” dialog chose the radio button to “select a well known naming context”, and choose “Schema”.
3. Expand the Schema and select the “CN=Schema,CN=Configuration,DC=domain_name,DC=com”
4. In the right, details, pane, find and right-click “CN=dp-Password-Manager-Data”, and then click Properties.
5. Find and double-click “rangeUpper”.
6. Clear the value from upper range so it's blank. (Alternately, double, or quadruple, the value here until end-users no longer receive errors on saving changes in Password Manager.)
7. Click OK, and then click OK again.

Alternative to the above, a script to more easily make this change is available here or in the utilities download section of the crossmatch.com website. Check the readme to run the script in the right location with needed permissions.

Extended Server Policy Module (ESPM)

ESPM is add-on module which provides additional user based authentication configuration features. The core product offers machine based control of authentication policies. ESPM extends Pro / Altus / DPCA / DP with additional user based authentication policies. These additional user based policies are a separate purchasable product. ESPM is available for DP AD and LDS. To obtain ESPM contact Crossmatch Sales.

Re-Enrolling Users’ Fingerprints

There are a couple of scenarios where re-registering selected users’ fingerprints is recommended. Re-registering users whose fingerprints have changed over time will decrease false rejects and reduce the need to raise your domain’s FAR (False Accept Rate.) Users whose fingerprints have changed over time include:

- People who work with abrasive materials or solutions and whose fingerprints are damaged or worn down by this work.
- Fingerprints features can change, sometimes significantly for individuals over the age of 60 years.

The User Query Tool can be used to generate a report of all users with fingerprints registered. When logged to file this can then be viewed as a tab delimited spreadsheet. There is a column for “date fingerprint last modified”; this information can help determine which users should re-register their fingerprints.