July 2016

Crossmatch
DigitalPersona
Altus AD
and
Altus LDS
v**2.0.3**
Update Notes

Contents

General Upgrade and Deployment Information

DigitalPersona Altus **AD** 2.0.3 has the ability to upgrade from the following releases

- DigitalPersona Altus AD 2.0.0
- DigitalPersona Altus AD 1.2.0
- DigitalPersona Altus AD 1.1.0
- DigitalPersona Altus AD 1.0.0
- DigitalPersona Pro Enterprise 5.5.1
- DigitalPersona Pro Enterprise 5.5.0

DigitalPersona Altus **LDS** 2.0.3 has the ability to upgrade from the following releases

- DigitalPersona Altus LDS 2.0.0
- DigitalPersona Altus LDS 1.2.0
- DigitalPersona Altus LDS 1.1.0
- DigitalPersona Altus LDS 1.0.0
- There is *no* upgrade path from Pro 5.x to Altus LDS

Migration Options

For Pro 5.5.x to Altus 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 Enterprise 5.x to Altus AD 2.0.3 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 DigitalPersona Altus AD Administration Guide provides migration instructions on page 15. Another resource is the DigitalPersona Altus AD Migration Guide. The requirements for Altus are basically the same as for Pro. The Altus AD 2.0.3 server is backwards compatible with, and will support the Altus AD 1.x and Pro 5.5.x clients. In going to Altus, end users will experience a difference in UI etc., so it is advisable to test in a lab, or 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 M&S.

Upgrade version hops

Pro 3.5.1 ▶ Pro 4.4.3 ▶ Pro 5.5.1 ▶ Altus AD 2.0.3

Updating from version Pro 5.0.0 through Pro 5.4.1

Upgrading from these versions of Pro requires that you first complete an upgrade to Pro 5.5.1, and then migrate to DigitalPersona Altus AD 2.0.3. (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.)

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 DigitalPersona Altus AD 2.0.3.

Flavors of Altus, “AD” and “LDS”:

Altus **AD**

Crossmatch DigitalPersona Altus 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 products.

Altus **LDS**

Crossmatch DigitalPersona Altus LDS is similar in many ways to Altus AD. Product distinguishers are:

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

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

Altus **Federal**

Crossmatch DigitalPersona Altus AD Federal supports CAC and is identified by the version number 2.0.2.

Altus **LSMS**

Crossmatch DigitalPersona Altus with a module providing Guardian ten-print scanner support.

Altus **Premium**

Crossmatch DigitalPersona Altus “Base”, plus SSO and Password Manager managed logons and SAML

Altus **Base**

Crossmatch DigitalPersona Altus base product only

Fresh install / deployment of Altus

This document provides information for upgrades and migrations of existing Pro / Altus deployments. For fresh installs of Altus 2.0.3, please refer to the Administrator Guides, available at www.crossmatch.com/Support/Reference-Material/DigitalPersona-Altus-Reference-Material, and the readme.txt files included with the software.

Upgrade Planning

Updating to DigitalPersona Altus 2.0.3 requires preparation, planning, and testing.

- Review the readme.txt file included with each Altus product.
- Review the Administrator Guide and identify any potential changes to the system administration settings.
- 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 and resources that may need.
    - Identify any special requirements applicable to your environment.
    - Determine how to mitigate downtime.

Altus clients 2.0.3 require Altus Server 2.0.3

Altus 2.0.3 clients cannot be deployed with an Altus Server version earlier than the client. You must complete the upgrade of all Pro/Altus Servers prior to upgrading Pro/Altus clients. (Ex. Altus AD 1.2 Server is not compatible with Altus AD 2.0.3 client.) The Altus server is compatible with older clients; please consult the server product readme.txt for specific compatibility information.

Laptops and tablets with built-in fingerprint readers

Altus 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 in order for the Altus client to utilize the reader.

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 DigitalPersona Altus 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 Altus 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.

Upgrading from Altus AD 2.0.0 ► Altus AD 2.0.3

1. Run the .\Server\Altus 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 prep wizard
   c. Re-customize any custom attended enrollment or kiosk membership permissions
2. On each Altus AD server:
   a. Remove Altus AD 2.0.0 Administration Tools
   b. Remove Altus AD 2.0.0 Server
   c. Install Altus AD 2.0.3 Server
   d. Install Altus AD 2.0.3 Administration Tools
3. On each Altus AD client
   a. Upgrade from v2.0.0 to v2.0.3, in place, over top
   b. Reboot client

Upgrading from Altus LDS 2.0.0 ► Altus LDS 2.0.3

1. Run the .\Server\Altus LDS Server\Configuration Wizard\DPADLDSConfig.exe
2. 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.
3. On each Altus LDS server:
   a. Remove Altus LDS Administration Tools v2.0.0 from all Altus LDS servers
   b. Remove Altus LDS Server v2.0.0 from all Altus LDS servers
   c. Install Altus LDS Server v2.0.3 on all Altus LDS servers
   d. Install Altus LDS Administration Tools v2.0.3 on all Altus LDS server
4. On each Altus AD client
   a. Upgrade from v2.0.0 to v2.0.3, in place, over top
   b. Reboot client

Upgrading from Altus AD 1.2.0 ► Altus AD 2.0.3

1. Run the .\Server\Altus AD Server\Schema Extension\DPSchemaExt.exe
2. Run the .\Server\Altus 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 prep wizard
   c. Re-customize any custom attended enrollment or kiosk membership permissions
3. On each Altus AD server:
   a. Remove Altus AD 1.2.0 Administration Tools
   b. Remove Altus AD 1.2.0 Server
   c. Install Altus AD 2.0.3 Server
   d. Install Altus AD 2.0.3 Administration Tools

4. On each Altus AD client
    a. 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 Altus 2.0.3 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 v1.2.0 to v2.0.3, in place, over top
    c. Reboot client

Upgrading from Altus LDS 1.2.0 ► Altus LDS 2.0.3

1. Run the .\Server\Altus LDS Server\Configuration Wizard\DPADLDSConfig.exe
2. 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.
3. On each Altus LDS server:
    e. Remove Altus LDS Administration Tools v1.2.0 from all Altus LDS servers
    f. Remove Altus LDS Server v1.2.0 from all Altus LDS servers
    g. Install Altus LDS Server v2.0.3 on all Altus LDS servers
    h. Install Altus LDS Administration Tools v2.0.3 on all Altus LDS server
4. On each Altus AD client
    c. 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 Altus 2.0.3 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.)
    d. Upgrade from v1.2.0 to v2.0.3, in place, over top
    e. Reboot client

Upgrading from Altus AD 1.1.0 ► Altus AD 2.0.3

1. Run the .\Server\Altus AD Server\Schema Extension\DPSchemaExt.exe
2. Run the .\Server\Altus 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 prep wizard
    c. Re-customize any custom attended enrollment or kiosk membership permissions
3. On each Altus AD server:
    a. Remove Altus AD 1.1.0 Administration Tools
    b. Remove Altus AD 1.1.0 Server
    c. Install Altus AD 2.0.3 Server
    d. Install Altus AD 2.0.3 Administration Tools
4. Upgrade Altus AD clients from v1.1.0 to v2.0.3, in place; and reboot all clients

Upgrading from Altus LDS 1.1.0 ► Altus LDS 2.0.3

1. License change
   a. *Do NOT proceed with upgrade until you have new replacement licenses in hand*
   b. The Altus 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 and/or v1.1.0 licenses
   d. After the configuration run and server changes, add the newer v2.0.3 (or v1.2.0) licenses
2. Run the .\Server\Altus LDS Server\Configuration Wizard\DPADLDSConfig.exe
3. 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.
4. On each Altus LDS server:
   a. Remove Altus LDS Administration Tools v1.1.0
   b. Remove Altus LDS Server v1.1.0
   c. Install Altus LDS Server v2.0.3
   d. Install Altus LDS Administration Tools v2.0.3
5. Upgrade Altus LDS clients from v1.1.0 to v2.0, in place; and reboot all clients

Migrating from Pro 5.5.x ► Altus AD 2.0.3

Please reference the information in the Migration Options section.

To self-migrate:

1. Run the Altus AD 2.0.3 .\Server\Altus AD Server\Schema Extension\DPSchemaExt.exe
2. Run the Altus AD 2.0.3 .\Server\Altus 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 prep wizard
   c. Re-customize any custom attended enrollment or kiosk membership permissions
3. Update and transfer GPO policies from Pro 5.5.x to Altus AD 2.0.3 using one of the two options below:
   a. Using Altus AD Policy Migration Tool:
      i. Detailed in the Migration Guide
      ii. If the Altus Migration Tool (AMT) reports that Altus / Pro polices have not been detected, then use the manual steps, below.
   b. Manually:
      i. In GPMC identify the GPOs serving Pro
      ii. Export GPOs to html reports, or document existing policies
      iii. Create new Altus AD GPOs, set all the desired settings, and link GPOs properly
      iv. After all clients are migrated, then the older "Pro" GPOs can be unlinked and later deleted

v. Alternatively, instead of using Pro and new Altus AD GPOs, the same existing GPO can be used – simply note GPO sections marked as legacy and the policies for new features. During migration, policies can be set for both Pro and Altus AD; after client migration is complete, the old Pro policy settings can be cleared.

4. On each Pro / Altus AD server:
   a. Remove Pro 5.5.1 Administration Tools
   b. Remove Pro 5.5.1 Server
   c. Install Altus AD 2.0.3 Server
   d. Install Altus AD 2.0.3 Administration Tools
5. Upgrade Pro / Altus AD clients, from Pro client 5.5.x, to Altus AD client 2.0.3, in place; and reboot all clients
6. Notes on Password Manager (PM)
   a. For a minority of your users you may notice that Password Manager (PM) seems to works, but doesn't fill-in any credential data. **The vast majority of users experience no degradation or data loss.** The fix for this issue seems to be to perform a PM credential data modification, as the user. This issue was found in updates to Altus v1.2.0 and 2.0.0 and should be fixed in this 2.0.3 version. This updates the protected stored data and makes it usable again! Have the user edit PM credentials. Change a username and then change it back, for example. This will force storage format upgrade on server – then everything should work. You may notice some inconsistencies between template credentials shown within the PM console, and template credentials presented to choose from after authenticating and before fill-in. This is due to a format conversion needing to be done internally within Altus PM. Once the user modifies, the format update will happen, and then all will be in sync and look right. Within the PM console, we show only one of the profiles (the first among multiple profiles) because we have not converted all of them into newer format. If the user edits any of them using PM console, or the PM icon, then we will convert them. After that they will observe all their profiles in their console. After upgrade to Altus, we will start converting user profile data into the newer format. This is done per PM template because we will not know which are available on the machine unless the user happens to modify them (add/edit/delete). Any of these actions will cause all the data to be converted. Initially, user PM data may not appear within Altus console but it is not removed/lost unless the user happens to delete it manually.
   b. All centrally MANAGED logons should continue to work from Pro 5.5.1 to Altus AD 2.0.3. (These are "roaming" templates stored in an accessible network share and managed with the Password Manger Admin Tool, PMAT.)
   c. All INDIVIDUAL logons should continue to work from Pro 5.5.1 to Altus AD 2.0.3. (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 Altus Server(s).
   d. There is a backup and import utility in PM for all Pro and Altus versions. This can be used to back up PM credentials, or copy/move them from one machine and Pro/Altus version to another. This procedure should be tested before use in production.

Migrating from Pro versions 4.4.3 through 5.4.1 ► Altus AD 2.0.3

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 Altus AD 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 Altus.

Migrating from Pro 4.x (earlier than v4.4.3) ► Altus AD 2.0.3

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 Altus administration guides and other documentation?**

www.crossmatch.com/Support/Reference-Material/DigitalPersona-Altus-Reference-Material/

DigitalPersona Altus **AD** 2.0.0 Administrator Guide http://www.crossmatch.com/Support/Reference-Material/Guides/Altus/DigitalPersona-Altus-AD-2_0-Administrator-Guide/

DigitalPersona Altus **LDS** 2.0.0 Administrator Guide
http://www.crossmatch.com/Support/Reference-Material/Guides/Altus/DigitalPersona-Altus-LDS-2_0-Administrator-Guide/

DigitalPersona Altus 2.0.0 Client Guide
http://www.crossmatch.com/Support/Reference-Material/Guides/Altus/DigitalPersona-Altus-2_0-Client-Guide/

DigitalPersona Altus Password Manager Application Guide
http://www.crossmatch.com/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=5009

DigitalPersona Altus AD Migration Guide
http://www.crossmatch.com/Support/Reference-Material/Guides/Altus/Altus-AD-Migration-Guide/

DigitalPersona Pro / Altus update notes
http://www.crossmatch.com/support/reference-material/pro-upgrade-notes/

Q: **Do I need to run the Schema Extension?**

Q: **Do I need to run the Domain Configuration Wizard?**

From	*To*	*Run schema extension?*	*Run domain prep?*
Altus AD 2.0.0	Altus AD 2.0.3	No	No
Altus AD 1.2.0	Altus AD 2.0.3	YES	YES
Altus AD 1.1.0	Altus AD 2.0.3	YES	YES
Altus AD 1.0.0	Altus AD 2.0.3	YES	YES
Pro 5.5.1	Altus AD 2.0.3	YES	YES

Note that **any custom attended enrollment permissions and/or custom kiosk memberships configured will be overwritten to their defaults by the domain prep run**. The domain prep will reset the ‘register / delete fingerprints’ permission back to the defaults. For example, after running the domain prep, 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.

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

No. Licenses are stored in AD for Altus AD and in the AD LDS database for Altus 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; Altus data in AD/AD LDS is untouched. Stored in AD/AD LDS is Altus’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 Altus Upgrade Notes?** (If you’re reading a print-out, or to send a link.)

Download or view the Altus AD Upgrade Notes PDF from here: http://www.crossmatch.com/support/reference-material/pro-upgrade-notes/

Server Hardware or Software Changes with Altus AD 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 Altus AD in place** and are:

- Refreshing Domain Controller (DC) hardware
- Upgrading DC Operating System (ex. 2008R2 to 2012R2 Server)
- Adding additional DCs and then decommissioning older DCs

What is Stored in Active Directory (AD)?:

- AD Schema modifications made by the Altus AD Schema Extension wizard

- Permission changes made to the AD Domain by the Altus AD Domain Config wizard
- DigitalPersona Pro / Altus AD licenses
- GPO .admx/.adml/.adm files and actual GPO settings for Altus 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 Altus AD server, client and admin tool software be at the most current versions.

Most day to day Altus functionality will be available even without an Altus Server being accessible due to Altus 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 Altus 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.)

How can one test a new Altus AD Server? Stop the Authentication Service on all the Altus Servers not being tested and then try managing fingerprints from an Altus client. If you get the warning message stating that changes made will be stored locally only, then the Altus client is not properly communicating with the Altus 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 Altus Server is working by using the Altus User Query Tool; log to file, and then view the log, looking for an entry detailing a user with newly registered fingerprints.

Gracefully remove Altus AD Server when you decommission a DC running Pro / Altus Server. Note that it is important to gracefully remove Altus AD Server when you decommission a DC running Pro / Altus Server. The graceful removal of Altus AD Server does a few things:

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

Example:

You have a fully functional Altus AD deployment with two DCs, one of which is an older box running Windows Server 2003. 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 prep again

1. Once the Windows 2012R2 server has been promoted to a DC, install DigitalPersona Altus Server
2. Gracefully remove Altus from the old DC by uninstalling Altus 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 Pro / Altus 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

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.

To use AD Users and Computers and GPMC on machines where Altus AD Server is not installed:

1. Install the Microsoft Admin Pack
2. Install the Altus Administrative Tools – specifically choose custom and ensure the ADUC and/or GPMC snap-in extensions is installed.
3. Manually copy .adm files into %systemroot%\inf\<appropriate language specific folders>.
4. Manually copy .admx files into %systemroot%\PolicyDefinitions\<appropriate language specific folders> on Windows 7 and Server 2008 and later machines.
5. Manually copy .adml files into %systemroot%\PolicyDefinitions\<appropriate language specific folders> on Windows 7 and Server 2008 and later machines.

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 Altus AD, some detailed here are not available in Altus LDS, or they may be done by script or other methods as implemented by CM Solutions.

General User license workflow:

- Once Altus AD “user”, or Altus LDS Server “AD user”, license has been activated, Altus 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 Altus 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 Altus 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 Altus AD ‘delete license…’ option in AD Users & Computers (ADUC), the license is returned to the pool for future use.
- The Altus 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 Altus Administration Tools installed, open the Microsoft Group Policy Management Console (GPMC)
2. Navigate to the GPO where you want the licenses to be stored; using the ‘default domain policy’, or an Altus specific policy linked at the domain level, are recommended
3. Edit the GPO
4. Browse to computer configuration / Policies / Software Settings / Altus Server / Licenses
5. You should see any already activated License IDs here
6. Launch the “Add License…” wizard
7. Choose to activate over the Internet (if the Altus Server / DC does not have Internet access to solo.digitalpersona.com then follow guidance in the Administrator Guide on the remote license tool)
8. Browse to the .dplic file (from Crossmatch via email) -OR- enter License ID and password manually
9. 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 Altus Admin Tools License Activation Manager sub-component installed, open the Microsoft Group Policy Management Console (GPMC)
2. Find the GPO where Altus licenses are
3. Edit the GPO
4. Browse to computer configuration / Policies / Software Settings / Pro-Altus Server / Licenses / select License ID / properties
5. 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 Altus 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 Altus 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)

Extended Server Policy Module (ESPM)

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