ADSS Server - Upgrade Notes

This document provides information about how to complete the upgrade from an older version of ADSS Server to the latest version v8.3.14. An upgrade from any prior version can be applied in one jump.

Before upgrading to next version of ADSS Server, kindly make sure that all the services (Core, Console, Service) have been manually stopped in both Linux and Windows.

The next table summarises the points to take special note of. A later table explains these points in detail.

Section 1 – Summary of the upgrade changes that operations staff need to be aware of

Upgrading from ADSS Server v8.3.6 or below	
Unity Console	When upgrading to ADSS Server Unity Console v8.3.7, if the application is already open in the browser before applying the regular release or any patch, users should log out and log back in after the update.
Upgrading from ADSS Server v8.3.5 or below	
RSA Vulnerability Detection	When upgrading to ADSS Server v8.3.6, it is essential to enable the RSA_VULNERABILITY_DETECTION property to ensure compliance with latest CA/B Forum Guidelines. This setting helps prevent RSA-related vulnerabilities, such as the ROCA Infineon RSA key vulnerability (CVE-2017-15361) and the Close Primes Vulnerability (CVE-2022-26320).
Mobile API Authentication	The List Registered Device API will now work with User Access Token due to user privacy concerns, rendering the existing Go>Sign Mobile Application incompatible. For backward compatibility, it will work in restricted mode with client access token. Therefore, after upgrading to ADSS Server v8.3.6, we must set the value of the MOBILE_API_AUTHENTICATION property to TRUE in the Unity Service > Advanced Settings of the ADSS Server Console to address this issue.
Upgrading from ADSS Server v8.3.4 or below	
Firebase Push Notifications	Apps using the deprecated FCM legacy APIs for HTTP and XMPP should migrate to the HTTP v1 API at the earliest opportunity. Sending messages (including upstream messages) with those APIs was deprecated on June 20, 2023, and shutdown begins July 22, 2024. With Firebase Push Notifications migrating from legacy FCM APIs to HTTP v1, users need to make the following changes after upgrading to the ADSS Server version 8.3.5: 1. Update the server address i.e. https://fcm.googleapis.com/v1/projects/[PROJECT_ID]/messages:send 2. Upload the service account file instead of the secret key. Users can download the service account JSON file and the updated server address from the Google FCM Portal. https://firebase.google.com/
Upgrading from ADSS Server v8.3.3 or below	

Mobile API Authentication	The List Registered Device API will now work with User Access Token due to user privacy concerns, rendering the existing Go>Sign Mobile Application incompatible. For backward compatibility, it will work in restricted mode with client access token. Therefore, after upgrading to ADSS Server v8.3.4, we must set the value of the MOBILE_API_AUTHENTICATION property to TRUE in the Global Settings > Advanced Settings > RAS Service of the ADSS Server Console to address this issue.
Upgrading from ADSS Server v8.1 or below	
iText	While upgrading from ADSS Server v8.1 or below, it must be noted that Ascertia ADSS Client SDK (Java) no longer uses iText 7 to generate PDF signature in local hash. Instead, ADSS Client SDK has now adopted for Apache PdfBox (Java) for this purpose. However, ADSS Client SDK (.NET) will keep using iText 7 for PDF signatures in local hashing. For more details, refer to **[ADSS-Client-SDK-Installation-Directory]/docs/ADSS-Client-SDK-Upgrade-Notes**.
TSA Service	While upgrading to ADSS Server 8.2, in order to use the SHA3 Algorithm with TSA Service, the operator must update the value of the **SUPPORTED_HASH_ALGORITHM** parameter in Global Settings > Advance Settings > TSA Service by adding **',SHA3-224,SHA3-256,SHA3-384,SHA3-512,2.16.840.1.101.3.4.2.7,2.16.840.1.101.3.4.2.8,2.16.840.1.101.3.4.2.9,2.16.840.1.101.3.4.2.10'** and then save the parameter with the updated value. Once done, the operator must restart the NT Services for changes to occur.
Upgrading from ADSS Server v8.0 or below	
XAdES Signatures	While upgrading from ADSS Server v8.0 or below, the operator need to update their respective Signing, Verification and Go>Sign profiles and select their required XAdES signature type (XAdES Legacy Signatures ETSI TS 101 903, XAdES Baseline Signatures (ETSI EN 319 132-1) or XAdES Extended Signatures ETSI EN 319 132-2).
Upgrading from ADSS Server v7.1 or below	
Server Configuration	After upgrading to ADSS Server v8.0, the operator needs to perform the following tasks: • In order to make sure that the inter-service communication is performed over a secure HTTPS channel, update the value of property **SERVICE_MANAGER_PORT** to either '8778' or any other port that you have configured for TLS Server communication. This property can be found under Global Settings → Advance Settings → General on ADSS Server Console. • The operator must make sure that the ADSS TLS Server Certificate must contain either DNS Name or IP Address in SAN extension for all ADSS Server instances. Otherwise, we need to create a new TLS Server Certificate with the required DNS Name or IP Address.
Upgrading from ADSS Server v7.0.2 or below	
OCSP Service	After upgrading to ADSS Server v7.1, OCSP Service will only add nonce in response, if the value of nonce is greater than **15** octets, or, less than **32** octets. This limitation is in accordance with RFC 8954.
Upgrading from ADSS Server v6.8 or below	

Databases	**MySQL Database** MySQL v5.5.x are no longer supported in ADSS Server v6.8 or below, hence, it is recommended to update the MySQL version to 8.x. If you still want to use MySQL version 5.5.x then some defined configuration steps are required to be performed on your MySQL database. Details of these steps is given here.
SAM Service	In order to use SHA3 Hashing Algorithms while upgrading to ADSS Server 6.9.0.x, a client has to directly integrate its business application with ADSS SAM Service and update the **SignHash API** where a new **hashAlgo** parameter will be sent to ADSS SAM Service. **Note:** A new hashAlgo parameter will only be sent in case where **'Compute final hash at signing time'** checkbox is unchecked in SAM Profile, else, SAM Service will identify the requested hash bytes as SHA2 hashing algorithm.
iText	Ascertia ADSS Client SDK (v6.9) for Java and .Net are no longer ship with embedded iText libraries. Customers must source iText 7 directly from the iText team. Customers can use itextsharp.dll / iText.jar together with the ADSS SDK within their custom applications.
Upgrading from ADSS Server v6.6 or below	
Azure Key Vault	To keep the Azure Key Vault client secret secure, the operator must update the Crypto Source Azure Key Vault profile by visiting the Edit screen.

<table>
<tr><th colspan="2">Upgrading from ADSS Server v6.5 or below</th></tr>
<tr><td>Databases</td><td>

Oracle Configurations

During upgradation from ADSS Server 6.5.0.x, following parameters must be set at instance and schema level before installing ADSS with Oracle:

```
NLS_TIMESTAMP_FORMAT='MM/DD/YYYY HH24:MI:SS'
NLS_COMP='LINGUISTIC'
NLS_COMP='BINARY_CI'
```

These parameters can be set separately at both Instance and Schema levels. Follow below mentioned points to set these parameters at both levels:

1) To change parameters at instance level some queries need to be executed. An example of how these queries need to be executed is mentioned below:

```
alter system set NLS_TIMESTAMP_FORMAT='MM/DD/YYYY
HH24:MI:SS' scope = file;
alter system set NLS_COMP='LINGUISTIC' scope=spfile;
alter system set NLS_COMP='BINARY_CI' scope=spfile;
```

Instance restart is required after successful exaction of above-mentioned queries.

2) To change parameters at schema level, a logon trigger for our schema needs to be created. Below is an example of how to create a logon trigger:

```
CREATE OR REPLACE TRIGGER
sys.schema_nls_session_settings AFTER LOGON ON SCOTT.SCHEMA
BEGIN
execute immediate 'alter session set
NLS_COMP=''LINGUISTIC''';
execute immediate 'alter session set
NLS_SORT=''BINARY_CI''';
END;
```

</td></tr>
<tr><th colspan="2">Upgrading from ADSS Server v5.0 or below</th></tr>
<tr><td>Client Manager</td><td>The operator must update the Client Manager → Advance Settings when DEK/KEK are already configured.</td></tr>
<tr><th colspan="2">Upgrading from ADSS Server v4.8.5 or below</th></tr>
<tr><td>Setup</td><td>The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password.
Note: Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.</td></tr>
<tr><td>System Integrity</td><td>HMAC should be recomputed for some critical fixes, details.</td></tr>
<tr><td>Access Control</td><td>Operator Role access rights need updating to make new features visible, details.</td></tr>
<tr><td>Key Manager</td><td>Crypto profile in Key Manager need updating because HSM vendor name configuration is moved in Crypto Profile from the GlobalSettings >> Advanced Settings >> general.</td></tr>
</table>

Database	Support for old database versions has been removed now the minimum supported versions are: • Microsoft SQL Server 2012 (Express, Standard, Web or Enterprise Edition) • Oracle 11g • PostgreSQL v9.3.25 • MySQL v5.5.62 Ensure that the database server version must match the minimum criteria as mentioned above.
Upgrading from ADSS Server v4.8.3 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
Upgrading from ADSS Server v4.8.2 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
Manage CAs	If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, details.
Upgrading from ADSS Server v4.7.7 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
Manage CAs	If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, details.

Upgrading from ADSS Server v4.7.6 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
Manage CAs	If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, details.
Upgrading from ADSS Server v4.7.5 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
Signing Service	User key management changed when using an HSM from v4.7.6 onwards
Import Logs	Archived logs are zipped from v4.7.6 onwards
Manage CAs	If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, details.
Upgrading from ADSS Server v4.7.1 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
Signing Service	User key management changed when using an HSM from v4.7.6 onwards
Import Logs	Archived logs are zipped from v4.7.6 onwards
Manage CAs	If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, details.

Upgrading from ADSS Server v4.5.2 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
Verification Profiles	Verification service profiles need updating
Signing Service	User key management changed when using an HSM from v4.7.6 onwards
Import Logs	Archived logs are zipped from v4.7.6 onwards
Manage CAs	If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, details.
Upgrading from ADSS Server v4.3 or below	
Setup	The ADSS Server installer will generate a Master Key to encrypt the data in database and prompt operator to take a backup of the Master Key in the form of three components encrypted with operator provided password. **Note:** Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Server to the next versions or can make a load balance installation for this ADSS Server. Even Ascertia cannot help you to recover these keys.
Access Control	Operator Role access rights need updating to make new features visible, details.
License	ADSS LTANS Service – license update for signing and verification services, details.
Verification Profiles	Verification service profiles need updating, details.
Signing Service	User key management changed when using an HSM from v4.7.6 onwards
Import Logs	Archived logs are zipped from v4.7.6 onwards
Manage CAs	If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, details.
Upgrading from ADSS Server v4.2 or below	
Multiple changes	Speak to Ascertia support

Section 2 – Detailed information regarding each change

Area to Review (From section 1)	Detailed Upgrade Information
Access Control	Access rights need updating to see new features After the upgrade process completes, the ADSS Server Administrator should login, go to the Access Control > Manage Role > Update screen and allow themselves (or any other appropriate operators) access rights to be able to see and control the features within the new modules/ sub-modules.
Signing Service	User key management within an HSM changed at v4.7.6 From ADSS Server v4.7.6 onwards, any user keys held centrally within an HSM must be protected by a user-defined password. After upgrading an ADSS Server release older than v4.7.6, to the latest version, the signing keys in the HSM must be updated with a password. Users will be asked to set a password for their signing keys when the first signing operation is performed after the upgrade.
Manage CAs	Trusted authorities for External CAs must be configured in Trust Manager and then for each external CA from v4.8.2 When an external CA is configured: 1. Register its CA certificate in Trust Manager 2. Edit the External CA and select the TA registered in step 1 3. Specify the Validity Period of the certificate 4. When an external offline CA is configured then additionally set the CA Type to “Offline External CA” 5. Update the settings and restart the services from Server Manager
Import Logs	Archived logs are zipped from v4.7.6 Archived files used to be created in CSV format until ADSS Server v4.7.5. From v4.7.6 onwards log files are zipped before archiving, to save the disk space. To import archived files created by a version of ADSS Server prior to v4.7.6 deployment the log files need to be zipped before import, otherwise ADSS Server will not recognise. Note that for OCSP Service, the main and detail files must both be available in the zip file before importing. Follow these steps to create an OCSP zip archive file: 1. Select the details file 2. Select the main file 3. Zip both these files 4. Import the zipped file in the OCSP Service If this order is not followed then the archive import will fail for the OCSP Service.
Verification, XKMS and SCVP Profiles	Verification, XKMS or SCVP service profiles need updating Trust building for the TSA and OCSP responder certificates, is now defined within the profile trust anchor. If any of the Verification, XKMS or SCVP services are used, then the trust anchor list within the service profile must be updated to include the TSA and OCSP responder certificates OR better still their issuer CAs in the list of trusted certification authorities.
License	ADSS LTANS Service – license update for signing and verification services When signing or verify signed documents within the ADSS LTANS Service ADSS Server Signing and Verification Modules need to be licensed.

Area to Review (From section 1)	Detailed Upgrade Information
System Integrity	From v4.8.5 Recompute HMAC for all the records by executing the [ADSS-Server-Installation-Dir]/setup/bin/compute_hmac.bat utility because there are critical fixes in this area. Follow the instructions on page 35 of Installation Guide to recompute HMAC.
Keystore Password	If you had changed the ADSS Server keystore password in your old installation of ADSS Server then click here for instructions to retain your password in the upgraded ADSS Server

*** End of document ***