

This document provides information about how to complete the upgrade from an older version of ADSS Server to the latest version v7.0.2. 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**

| <b>Upgrading from ADSS Server v6.8 or below</b> |   |
|---|---|
| Databases                                       | <p><b><u>MySQL Database</u></b></p> <p>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.</p> <p>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 <a href="#">here</a>.</p>   |
| SAM Service                                     | <p>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 <b>SignHash API</b> where a new <b>hashAlgo</b> parameter will be sent to ADSS SAM Service.</p> <p><b>Note:</b> A new hashAlgo parameter will only be sent in case where '<b>Compute final hash at signing time</b>' checkbox is unchecked in SAM Profile, else, SAM Service will identify the requested hash bytes as SHA2 hashing algorithm.</p>  |
| iText   | <p>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.</p>  |
| TLS Handshake                                   | <p>While upgrading from ADSS v6.8 to an above version, If the user tries to send a request to ADSS Server over TLS connection using an old client application with JDK-8, then TLS handshake can be failed and client application may not establish a TLS connection with the ADSS Server.</p> <p>In order to tackle this issue, follow the below knowledge based article:<br/> <a href="https://ascertia.force.com/partners/s/article/TLS-Handshake-not-working-with-older-client-applications-after-ADSS-Server-upgraded-to-v6-9">https://ascertia.force.com/partners/s/article/TLS-Handshake-not-working-with-older-client-applications-after-ADSS-Server-upgraded-to-v6-9</a></p> |
| <b>Upgrading from ADSS Server v6.6 or below</b> |   |
| Azure Key Vault                                 | <p>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.</p>  |

| Upgrading from ADSS Server v6.5 or below   |   |
|--|---|
| Databases                                  | <p><b><u>Oracle Configurations</u></b></p> <p>During upgradation from ADSS Server 6.5.0.x, following parameters must be set at instance and schema level before installing ADSS with Oracle:</p> <pre>NLS_TIMESTAMP_FORMAT='MM/DD/YYYY HH24:MI:SS' NLS_COMP='LINGUISTIC' NLS_COMP='BINARY_CI'</pre> <p>These parameters can be set separately at both Instance and Schema levels. Follow below mentioned points to set these parameters at both levels:</p> <ol style="list-style-type: none"> <li>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: <pre>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;</pre> <p>Instance restart is required after successful execution of above-mentioned queries.</p> </li> <li>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: <pre>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;</pre> </li> </ol> |
| Upgrading from ADSS Server v5.0 or below   |   |
| Client Manager                             | The operator must update the Client Manager → Advance Settings when DEK/KEK are already configured.   |
| Upgrading from ADSS Server v4.8.5 or below |   |
| Setup                                      | <p>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.</p> <p><b>Note:</b> 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.</p>   |
| System Integrity                           | HMAC should be recomputed for some critical fixes, <a href="#">details</a> .  |
| Access Control                             | Operator Role access rights need updating to make new features visible, <a href="#">details</a> .   |
| Key Manager                                | Crypto profile in Key Manager need updating because HSM vendor name configuration is moved in <a href="#">Crypto Profile</a> from the <a href="#">GlobalSettings &gt;&gt; Advanced Settings &gt;&gt; general</a> .  |

|   |   |
|---|---|
| Database  | <p>Support for old database versions has been removed now the minimum supported versions are:</p> <ul style="list-style-type: none"> <li>• Microsoft SQL Server 2012 (Express, Standard, Web or Enterprise Edition)</li> <li>• Oracle 11g</li> <li>• PostgreSQL v9.3.25</li> <li>• MySQL v5.5.62</li> </ul> <p>Ensure that the database server version must match the minimum criteria as mentioned above.</p>  |
| <b>Upgrading from ADSS Server v4.8.3 or below</b> |   |
| Setup   | <p>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.</p> <p><b>Note:</b> 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.</p> |
| Access Control                                    | Operator Role access rights need updating to make new features visible, details.  |
| <b>Upgrading from ADSS Server v4.8.2 or below</b> |   |
| Setup   | <p>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.</p> <p><b>Note:</b> 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.</p> |
| 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.  |
| <b>Upgrading from ADSS Server v4.7.7 or below</b> |   |
| Setup   | <p>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.</p> <p><b>Note:</b> 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.</p> |
| Access Control                                    | Operator Role access rights need updating to make new features visible, <a href="#">details</a> .   |
| Manage CAs  | If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, <a href="#">details</a> .   |

| Upgrading from ADSS Server v4.7.6 or below |   |
|--|---|
| Setup                                      | <p>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.</p> <p><b>Note:</b> 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.</p> |
| Access Control                             | Operator Role access rights need updating to make new features visible, <a href="#">details</a> .   |
| Manage CAs                                 | If an external CA is configured in Manage CAs module then register its certificate in the Trust Manager module, <a href="#">details</a> .   |
| Upgrading from ADSS Server v4.7.5 or below |   |
| Setup                                      | <p>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.</p> <p><b>Note:</b> 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.</p> |
| Access Control                             | Operator Role access rights need updating to make new features visible, <a href="#">details</a> .   |
| 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, <a href="#">details</a> .   |
| Upgrading from ADSS Server v4.7.1 or below |   |
| Setup                                      | <p>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.</p> <p><b>Note:</b> 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.</p> |
| Access Control                             | Operator Role access rights need updating to make new features visible, <a href="#">details</a> .   |
| 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, <a href="#">details</a> .   |

| Upgrading from ADSS Server v4.5.2 or below |   |
|--|---|
| Setup                                      | <p>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.</p> <p><b>Note:</b> 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.</p> |
| Access Control                             | Operator Role access rights need updating to make new features visible, <a href="#">details</a> .   |
| 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, <a href="#">details</a> .   |
| Upgrading from ADSS Server v4.3 or below   |   |
| Setup                                      | <p>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.</p> <p><b>Note:</b> 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.</p> |
| Access Control                             | Operator Role access rights need updating to make new features visible, <a href="#">details</a> .   |
| License                                    | ADSS LTANS Service – license update for signing and verification services, <a href="#">details</a> .  |
| Verification Profiles                      | Verification service profiles need updating, <a href="#">details</a> .  |
| 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, <a href="#">details</a> .   |
| Upgrading from ADSS Server v4.2 or below   |   |
| Multiple changes                           | Speak to Ascertia support   |

## **Section 2 – Detailed information regarding each change**

| <b>Area to Review<br/>(From section 1)</b> | <b>Detailed Upgrade Information</b>   |
|--|---|
| Access Control                             | <p>Access rights need updating to see new features</p> <p>After the upgrade process completes, the ADSS Server Administrator should login, go to the Access Control &gt; Manage Role &gt; 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.</p>   |
| Signing Service                            | <p>User key management within an HSM changed at v4.7.6</p> <p>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.</p> <p>Users will be asked to set a password for their signing keys when the first signing operation is performed after the upgrade.</p>  |
| Manage CAs                                 | <p>Trusted authorities for External CAs must be configured in Trust Manager and then for each external CA from v4.8.2</p> <p>When an external CA is configured:</p> <ol style="list-style-type: none"> <li>1. Register its CA certificate in Trust Manager</li> <li>2. Edit the External CA and select the TA registered in step 1</li> <li>3. Specify the Validity Period of the certificate</li> <li>4. When an external offline CA is configured then additionally set the CA Type to “Offline External CA”</li> <li>5. Update the settings and restart the services from Server Manager</li> </ol>  |
| Import Logs                                | <p>Archived logs are zipped from v4.7.6</p> <p>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.</p> <p>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.</p> <p>Follow these steps to create an OCSP zip archive file:</p> <ol style="list-style-type: none"> <li>1. Select the details file</li> <li>2. Select the main file</li> <li>3. Zip both these files</li> <li>4. Import the zipped file in the OCSP Service</li> </ol> <p>If this order is not followed then the archive import will fail for the OCSP Service.</p> |
| Verification, XKMS and SCVP Profiles       | <p>Verification, XKMS or SCVP service profiles need updating</p> <p>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.</p>   |
| License                                    | <p>ADSS LTANS Service – license update for signing and verification services</p> <p>When signing or verify signed documents within the ADSS LTANS Service ADSS Server Signing and Verification Modules need to be licensed.</p>   |

| <b>Area to Review<br/>(From section 1)</b> | <b>Detailed Upgrade Information</b>   |
|--|---|
| System Integrity                           | From v4.8.5<br>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 <a href="#">click here</a> for instructions to retain your password in the upgraded ADSS Server   |

\*\*\* End of document \*\*\*