ADSS Server v8.3.14 –

Trust Monitor Installation Guide

ASCERTIA LTD

DECEMBER 2025

Document Version- 1.0.0

© Ascertia Limited. All rights reserved.

This document contains commercial-in-confidence material. It must not be disclosed to any third party without the written authority of Ascertia Limited.

CONTENTS

1 INTRODUCTION 4

1.1 SCOPE 4
1.2 INTENDED READERSHIP 4
1.3 CONVENTIONS 4
1.4 TECHNICAL SUPPORT 4

2 SYSTEM REQUIREMENTS 5

2.1 TYPICAL DEPLOYMENT SCENARIO 6
2.2 HSM SUPPORT FOR KEY WRAPPING 7

3 INSTALLATION OVERVIEW 8

3.1 PRE-INSTALLATION CHECKS 8
3.2 DOCUMENTATION 8
3.3 HARDWARE, NETWORK & OPERATING SYSTEM 8
3.4 MEMORY REQUIREMENTS 9
3.5 DATABASE CONFIGURATIONS 9
3.6 SECURE ENVIRONMENT 10
3.7 SEPARATION OF DATA/PARTITIONING 11
3.8 USING DEFAULT/CUSTOM PORTS 11
3.9 HIGH AVAILABILITY (HA) REQUIREMENTS 11
3.10 DISABLE ANTI-VIRUS 11
3.11 ADSS TRUST MONITOR OPERATOR ACCOUNTS & PRIVILEGES 12
3.12 NOTIFICATIONS & ALERTS 13
3.13 HARDWARE SECURITY MODULE 13
3.14 ADSS TRUST MONITOR PROFILES 13
3.15 PKI BASED DEPLOYMENTS 13

4 ADSS TRUST MONITOR INSTALLATION 14

4.1 INSTALLATION PROCESS 14
4.2 LAUNCHING ADSS TRUST MONITOR ADMIN CONSOLE 39
4.3 UNINSTALLING ADSS TRUST MONITOR 40
4.4 ADSS TRUST MONITOR SERVICE INTERFACE URLS 41
4.5 TROUBLESHOOTING 41

5 POST-INSTALLATION NOTES 43

5.1 SECURE DEPLOYMENT OF ADSS TRUST MONITOR 43
5.2 ADSS TRUST MONITOR OPERATORS 43
5.3 HSM CONFIGURATION 43
5.4 LOCAL CA CONFIGURATION 43
5.5 EXTERNAL TRUST SERVICES 44
5.6 NTP CONFIGURATION 44
5.7 DATABASE LOG ARCHIVING FREQUENCY 44
5.8 ALERT CONFIGURATIONS 44
5.9 LICENSING 44
5.10 PREPARE THE BACKUP STRATEGY 44
5.11 TRACE LOG SIZING GUIDE 45
5.12 ADSS TRUST MONITOR CLIENTS 45

APPENDIX A - CONFIGURING ADSS TRUST MONITOR TO USE AN HSM 46

APPENDIX B - USING UTIMACO CRYPTOSERVER SE-SERIES GEN2 CP5 (PCI/LAN) 47

APPENDIX C - USING A THALES SAFENET LUNA SA HSM (PED) 51

APPENDIX D - USING A THALES SAFENET LUNA PCI HSM (PWD) 54

APPENDIX E - USING A NCIPHER NSHIELD CONNECT HSM 56

APPENDIX F - USING A THALES SAFENET PSG HSM 58

TABLES

TABLE 1 - ADSS TRUST MONITOR SYSTEM REQUIREMENTS 6
TABLE 2 - DATABASE CONNECTION PARAMETERS - TYPICAL 24
TABLE 3 - DATABASE CONNECTION PARAMETERS – ADVANCED 26

FIGURES

FIGURE 1 - TYPICAL ADSS TRUST MONITOR DEPLOYMENT SCENARIO 7
FIGURE 2 - WINDOWS SERVICE PANEL ADSS TRUST MONITOR PROCESS OWNER VIEW 9
FIGURE 3 - ADSS TRUST MONITOR ROLE BASED ACCESS CONTROL EXAMPLE 12
FIGURE 4 - WINDOWS EXAMPLE INSTALLER RUN AS ADMINISTRATOR 14
FIGURE 5 - ADSS TRUST MONITOR INSTALLATION WIZARD SUCCESS SCREEN 29
FIGURE 6 - WINDOWS EXAMPLE UNINSTALL RUN AS ADMINISTRATOR 40

1 Introduction

1.1 Scope

This manual describes how to install one or more instances of ADSS Trust Monitor.

1.2 Intended Readership

This manual is intended for ADSS Trust Monitor administrators responsible for installation and initial configuration. It is assumed that the reader has a basic knowledge of digital signatures, certificates and information security.

1.3 Conventions

The following typographical conventions are used in this guide to help locate and identify information:

- Bold text identifies menu names, menu options, items you can click on the screen, file names, folder names, and keyboard keys.
- `Courier New` font identifies code and text that appears on the command line.
- **`Bold Courier New`** identifies commands that you are required to type in.

1.4 Technical Support

If Technical Support is required, Ascertia has a dedicated support team. Ascertia Support can be reached/accessed in the following ways:

Website	https://www.ascertia.com
Email	support@ascertia.com
Knowledge Base	Ascertia Community Portal

In addition to the free support services detailed above, Ascertia provides formal support agreements with all product sales. Please contact sales@ascertia.com for more details.

When sending support queries to Ascertia Support team send ADSS Trust Monitor logs. Use the Ascertia's trace log export utility to collect logs for last two days or from the date the problem arose. It will help the support team to diagnose the issue faster. Follow the instructions on how to run the trace log export utility

2 System Requirements

The following table lists the system requirements for ADSS Trust Monitor:

Components	Requirements
ADSS Trust Monitor	ADSS Trust Monitor is a JEE 17 application supported on these platforms: **Operating System** The following 64-bit operating systems are supported: • Windows Server 2022, 2019 and 2016 • Linux (RedHat v7.4, v7.9, v8.4, v9.0, Ubuntu v22, AlmaLinux v9.3) **Hardware** A modern multi-core CPU such as the Xeon E3-xxxx or E5-xxxx or E55xx or E56-xx or similar are recommended, with 16 GB RAM (min 8GB RAM) and 200 GB disk space. Additional RAM may be required to power signing or LTANS archive services. Roughly 0.5GB to 1GB of disk space is required to keep the trace logs per 100,000 service transactions. **Database** ADSS Trust Monitor saves its configuration and transactional data in a database. The following databases are supported: • Microsoft SQL Server 2022, 2019, 2017, 2016 (Express, Standard, Web or Enterprise Edition) • Azure SQL Database (Database-as-a-service) • Oracle 19c, 21c (Standard Edition, Enterprise Edition) • PostgreSQL v12, v13, v14.3, v15.5 and v16.1 • MySQL v8.0.13, v8.0.36, • Percona-XtraDB-Cluster v8.0.23. About 1GB of database space is required to store the service logs from 100,000 transactions for each service unless these are regularly auto-archived or customised.
Optional Database Server	The database can be run on a separate server if preferred. This is recommended for high performance environments to allow all server resources to be directed to ADSS Trust Monitor services. **Hardware:** A modern multi-core CPU such as the Xeon E3-xxxx or Xeon E5-xxxx or E55xx or E56-xx or similar range are recommended, with 16 GB RAM, typically 5-10GB or more of disk space will be required depending on usage and transactional data / log retention requirements.
Client systems (systems sending service requests to ADSS Trust Monitor)	Any reasonable system. ADSS Client SDK for Java API requires JRE v1.7 or above. ADSS Client SDK for .NET requires Microsoft .NET Framework 4.5 and Microsoft .NET Core 8.0.
Operator Browsers	The following browsers are supported for ADSS Trust Monitor Operators: • Google Chrome 70.x or above

Components	Requirements
	• Mozilla Firefox 60.x or above • Microsoft Edge 35.x or above • Microsoft Internet Explorer (IE) 11.x
Mobile Devices OS	For authorised remote signing, the native apps (iOS and Android) of Go>Sign Mobile will require the following OS versions: • iOS 9.0 or above • Android 6 (Marshmallow) or above
Optional HSMs	If required the following Hardware Security Modules are supported: • Thales SafeNet Luna and ProtectServer HSMs • Entrust nShield Solo or Connect HSMs • Utimaco CP5 SE & CryptoServer SE Gen2 HSMs • Microsoft Azure Key Vault HSM • Amazon AWS Cloud HSM (Supported when ADSS Server deployed on Linux)
Optional DMZ proxy machine	A DMZ proxy server can be configured if required. The following DMZ proxy machines are supported: • Windows Server -Microsoft IIS, Apache or IBM HTTP Server • Linux - Apache or IBM HTTP Server Use a reasonable CPU, 2GB RAM,100 MB disk space

Table 1 - ADSS Trust Monitor System Requirements

2.1 Typical Deployment Scenario

A typical ADSS Trust Monitor installation schematic looks like this:

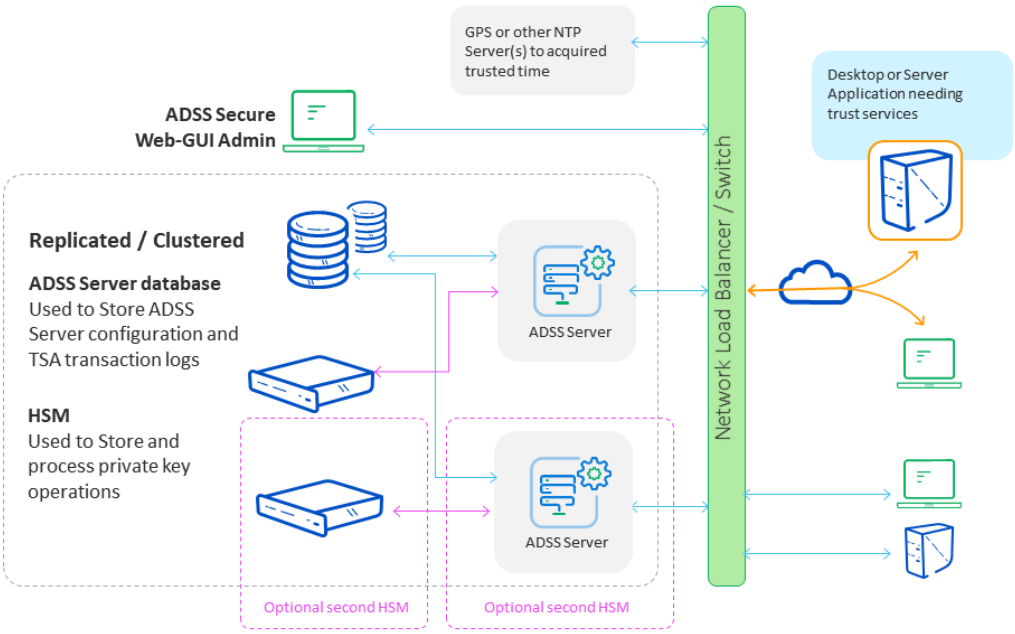


Figure 1 - Typical ADSS Trust Monitor Deployment Scenario

ADSS Trust Monitor and the database it uses can both be installed on the same machine. 12GB RAM is recommended for such a scenario. For high performance environments, it is recommended to install them on separate systems.

The details shown above are the minimum system requirements; these may need to be revised to meet specific usage requirements. For high throughput systems consider using multiple load-balanced ADSS Trust Monitors in a network load-balanced resilient arrangement. Multiple physical CPUs can be added although additional licenses are required for these. Virtualized systems are also supported.

ADSS Trust Monitor can also be installed on the same system as the business application it services.

2.2 HSM Support for Key Wrapping

If you wish to use ADSS Trust Monitor with its HSM based user key generation wrapping and export under a static or dynamic KEK then be careful with the specifications of the HSMs you order or try to reuse.

The best thing to do is to run the ADSS Trust Monitor PKCS#11 Test Utility to check if the HSM supports the mechanisms needed for this and indeed other functions. HSM vendors are known to change the mechanisms that are supported in this area, and some exclude such mechanisms from the allowable list when in FIPS 140-2. If in doubt check with Ascertia support and also check with your HSM vendor that the AES_CBC_ENCRYPT_DATA mechanism is supported for key wrapping and export.

3 Installation Overview

Most of the installation failures or problems are due to a failure to complete all of the steps that are required before commencing the deployment. These pre and post check lists are intended for administrators to use in consultation with system administrators, storage administrators, network administrators, database administrators, and third-party hardware and software vendors to coordinate and plan the tasks for the ADSS Trust Monitor installation. Planning and preparation is essential to ensure that your installation proceeds smoothly.

The following sections guide you through the necessary steps that should follow before proceeding with the actual deployment.

3.1 Pre-Installation Checks

Ascertia recommends the following check list is followed before beginning the actual installation of ADSS Trust Monitor.

3.2 Documentation

Review the documentation thoroughly and ensure all components are in place. At a basic level this means a database and if a production system, Hardware Security Module (HSM). The ADSS Trust Monitor Installation Guides, Database Guides and Quick Guides are all in the /Docs folder of the downloaded zip file. The ADSS Trust Monitor Admin Guide is available in the product's web-admin screen 'help' section and also here:

Welcome (ascertia.com)

Before proceeding with the installation it is advisable to make yourself familiar with the services you intend to use. For example, Signing Service and Verification Service, which depend upon TSA and certificate revocation services.

3.3 Hardware, Network & Operating System

Review the required hardware, network, and operating system and ensure that they are in place before proceeding for ADSS Trust Monitor Installation. For more see the section System Requirements.

3.3.1 Permissions & Service Owners

The following operating system privileges are required for ADSS Trust Monitor installation:

- Windows administrator privilege is required to create Windows Services during the installation. The installation must be performed as a local administrator.
- Linux or Solaris deployments require sufficient privilege to create the necessary service daemons for the Tomcat instances.

For Linux or Solaris systems create the necessary user and group who will own and run ADSS Trust Monitor instances. Note the user does not require any special permissions and an ordinary user account is sufficient. The owner and group can be changed after the initial installation has completed. The instructions to do are detailed here:

https://ascertia.force.com/partners/s/article/How-to-run-ADSS-Server-services-as-a-non-root-user-daemon-on-UNIX-Linux.

Windows deployments will install the services to run under Local System. It is recommended a suitable low level privilege user be assigned ownership of the services. As with Linux and Solaris the user does not require any special permissions. To change the Windows Service owner of the ADSS Trust Monitor modules

you will need to ensure they are stopped first. Use the standard dialogue box of the service to change the owner as shown here for the Console service: -

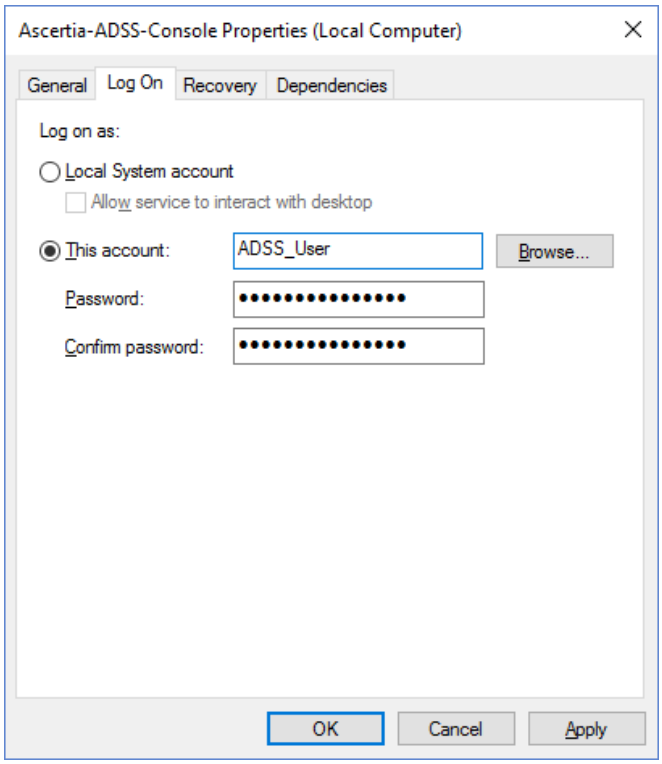


Figure 2 - Windows Service Panel ADSS Trust Monitor Process Owner View

3.3.2 Hostname & IP Address

It is important to ensure the ADSS Trust Monitor host system is correctly configured with regard to hostname, and resolution to IP of such. During the installation ADSS Trust Monitor installer will use the given system hostname as the identifier and subsequently attempt to retrieve the IP address that this name resolves to. Therefore, either a suitable DNS or local hosts file entry must exist to achieve this. Take care when using a combination of long and short host names, i.e. host with and without fully qualified domain attached. Ascertia recommends using the long, fully qualified host name when deploying ADSS Trust Monitor.

3.4 Memory Requirements

Review the memory requirements/disk space for the database as well as Tomcat instances that ADSS Trust Monitor runs on. Note the default values are 1024MB for Core and Console applications and 2048MB for Service instance. For more details on memory requirements see the section System Requirements.

3.5 Database Configurations

Review the database user credentials and connection configuration information. Ensure database connectivity is established. If possible, test the credentials as provided by the database vendor. Follow this FAQ for more details on database formations:

https://ascertia.force.com/partners/s/article/What-are-the-minimum-set-of-database-privileges-required-to-install-ADSS-Server

Note ADSS Trust Monitor uses Hibernate technology for database communication and C3P0 to handle the connection pooling. The default sizes for the connection pools are: -

- ADSS Trust Monitor Console: minimum 20 and maximum 50
- ADSS Trust Monitor Core: minimum 30 and maximum 100
- ADSS Trust Monitor Service: minimum 40 and maximum 1000

3.5.1 Real-Time Certificate Status Checking

If the OCSP Responder service is configured to use real time certificate status database checking, then the table schema required is detailed here:

Step 2 - Validation Policy (ascertia.com)

This table must be created separately by the appropriate SQL Server or Oracle administrator respectively. It is not part of ADSS Trust Monitor installation.

3.5.2 Sizing

ADSS Trust Monitor is a modular based system and disk space is dependent upon the services you have purchased. For a guide as to space required for each service (Signing, Verification, Certification, OCSP, TSA and LTANS) and for logs use the information found here:

https://manuals.ascertia.com/ADSS-Admin-Guide/database.html.

3.5.3 Permissions

Ascertia recommends that two database users are used for ADSS Trust Monitor. First, a user with extended privileges for the deployment and second, a user for normal operations. The permissions required for the installation of ADSS Trust Monitor is detailed here:

https://ascertia.force.com/partners/s/article/What-are-the-minimum-set-of-database-privileges-required-to-install-ADSS-Server.

Operation of ADSS Trust Monitor only requires permissions to add, modify, and delete data.

3.6 Secure Environment

Prior to the deployment of ADSS Trust Monitor it is imperative to ensure the any host is physically and network secure. For example, if deploying ADSS Trust Monitor for use as an issuing CA it is recommended that the CA and HSM modules communicate on a dedicated network link, either virtual or physical.

Ensure that only designated and known individuals have accounts that allow access to the host. This ensures there is an audit trail for system access for example.

ADSS Trust Monitor should be deployed on a dedicated host, either virtual or physical. It is recommended that no other software other than monitoring, is deployed on the same host as ADSS Trust Monitor.

If deploying ADSS Trust Monitor on Windows it is highly recommended that the host is not part of a Windows Domain.

Block all unnecessary ports to ADSS Trust Monitor host. For example, FTP, and Telnet. Once deployed all administration and configuration of ADSS Trust Monitor is done via the admin console, which is accessible via a web browser and uses mutual TLS for authentication.

If deploying ADSS Trust Monitor on Windows:

- Disable NetBIOS.
- Disable the default administrator account, and replace with a non-default named accounts.
- Disable the Guest account, and delete or disable all non-essential accounts.
- Enable event audit system of the local Windows security policy

For Linux/Solaris:

- Root login should only be allowed at the console level and not remotely.
- Ensure administrators authenticate using their own login credentials and then use **su** or equivalent to obtain higher level privileges.

3.7 Separation of Data/Partitioning

It is recommended to separate aspects of ADSS Trust Monitor. For Windows this means deploying ADSS Trust Monitor to a separate partition from the operating system. On Linux and Solaris deployments follow good practice guidelines of deploying the binaries to a different directory structure to that of the log files ADSS Trust Monitor generates during operation.

3.8 Using Default/Custom Ports

Review if it is required to use special custom ports or the default ports for ADSS Trust Monitor Core, Console and Service instances. If using non-default ports note those required. The default ports are:

- 8774 for HTTPS admin console access.
- 8777 for HTTP access to services, i.e. Service instance.
- 8778 for HTTPS (server side TLS) access to services, i.e. Service instance.
- 8779 for HTTPS (mutual TLS) access to services, i.e. Service instance.

Follow this FAQ for changing the default ports of ADSS Trust Monitor Core, Console and Service instances if a change is required after the product has already been deployed:

https://ascertia.force.com/partners/s/article/How-to-change-the-default-ports-for-ADSS-Server-services.

For production systems Ascertia recommends mutual TLS is used on port 8779 where possible and access to server side TLS and clear text HTTP are blocked. For example, access to OCSP Service over HTTP on port 8777 is likely to be required.

3.9 High Availability (HA) Requirements

Identify whether all services should be installed on a single machine or different machines for better performance or high availability. Note it is possible to run the Core and Console services in a high availability set-up but it is not necessary for the Service instance.

The installer allows you to add ADSS Trust Monitor instances to create a high availability environment.

ADSS Trust Monitor High Availability notes and instructions can be found at:

High Availability (ascertia.com)

3.10 Disable Anti-Virus

Disable any anti-virus, malware or equivalent protection software that may interfere with the installation process.

3.11 ADSS Trust Monitor Operator Accounts & Privileges

Record who will have access to ADSS Trust Monitor administration console. These individuals should be given dedicated digital IDs for ongoing accountability and traceability. It is important to disable the default administrator account once individual assigned ones have been put in place.

Determine whether dual authorisation control is required to administer system services. This can be applied to any of the public facing services such as Signing Service and to any of the support modules. For example, CRL Monitor or Key Manager.

3.11.1 Role Based Access & Fine Grain Access Control

ADSS Trust Monitor implements role based access for ADSS Trust Monitor administrator access. The default roles of administrator, security officer and auditor are created during the installation. Please review these once installation is complete to ensure they match your requirements. Any number of roles can be added and configured separately to ensure the greatest flexibility.

Each role has fine grain access control based upon each module. This picture shows some of the choices available for Signing, Verification and Certification Services respectively: -

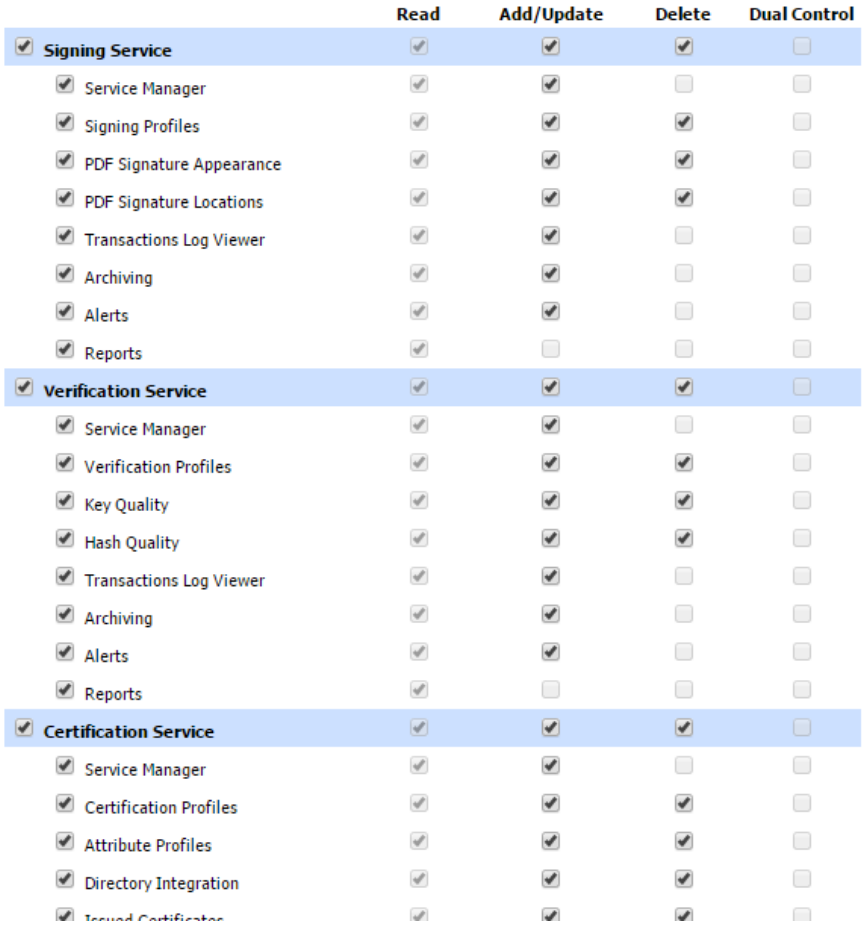


Figure 3 - ADSS Trust Monitor Role Based Access Control Example

3.12 Notifications & Alerts

ADSS Trust Monitor provides notification services via SMTP, SMS and SNMP. Before proceeding with the installation determine which services will be used and which administrators will receive any notifications. Note each ADSS Trust Monitor Service, e.g. Signing allows configuration of notification alerts specific to the service, and which administrators should receive these.

Refer to the service provider for the configuration parameters required to access the respective services. Ascertia recommends that SMTP notification is a minimum for such, and both SMTP and SMS for high value deployments where uptime and security is key.

3.13 Hardware Security Module

For production systems Ascertia recommends the use of a Hardware Security Module. If applicable ensure the HSM and associated client software are in place. In addition, the necessary configuration has been conducted. For example, when using Thales SafeNet Luna SAs that the partition has been created and the passphrase known. In addition, gathered the required individuals if using trusted authentication mode, i.e. PED with PED Keys to protect access.

3.14 ADSS Trust Monitor Profiles

Each ADSS Trust Monitor Service uses a concept of profiles to distinguish configuration sets from one another. For testing the installation procedure allows the creation of sample data that will populate the licensed services with sample profiles. Ascertia recommends this option is not selected for production systems.

The appropriate profiles should be thought about prior to installation. For example, when using Signing Service what profiles are required. That is, what signature format is required, is local hashing being employed, and so forth.

3.15 PKI Based Deployments

Where the Certification Service, RA, OCSP, CRL Monitor, SCVP and associated support modules are used it is important to ensure that applicable CP/CPS and supporting data is in place prior to the installation. The documentation set will affect how the final services within ADSS Trust Monitor are configured. For example, the revocation status checks of certificates within the CPS will state whether OCSP and CRL are acceptable, or if only one is allowed.

4 ADSS Trust Monitor Installation

ADSS Trust Monitor is a Java EE application that has rich functionality. The ADSS Trust Monitor license file contains a list of services/modules licensed for you, so not all services may be available within your ADSS Trust Monitor deployment.

ADSS Trust Monitor is shipped with a customized distribution of Apache Tomcat and Java and Ascertia continues to periodically upgrade these to the latest available versions. Operators and administrators should not attempt upgrade to these separately because it will lead to a system configuration that is not supported by Ascertia. If an upgrade is required, raise it to Ascertia at support@ascertia.com.

ADSS Trust Monitor can be installed in either of these modes:

- GUI based - for Windows/X11 platforms
- Command Line (Non-GUI based) - for remote installation on UNIX platforms

4.1 Installation Process

ADSS Trust Monitor installer must be unzipped to a suitable directory (later referred as **[ADSS-Server-Home]**). ADSS Trust Monitor installation directory path **MUST NOT** contain space characters otherwise the installer will not be launch.

To start the installation, navigate to **[ADSS-Server-Home]/setup** directory. Either using a command line or Windows GUI interface.

Windows

Run the **install.bat** file under administrative privileges, as shown below, (otherwise ADSS Trust Monitor services will not be registered in Windows Services Panel) to launch the installer.

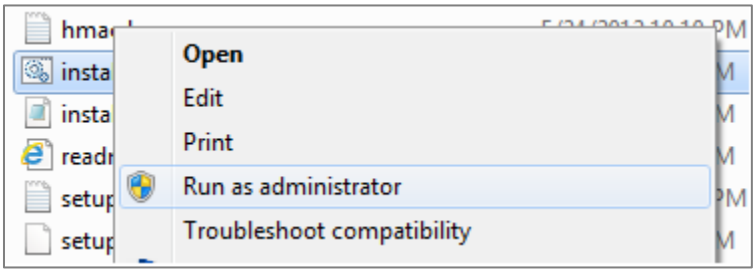


Figure 4 - Windows Example Installer Run as administrator

UNIX

To install ADSS Trust Monitor on UNIX systems the installer must be launched under **root** user privileges (otherwise ADSS Trust Monitor daemons will not be registered in /etc/init.d). After completing the installation, search the Ascertia Community Portal knowledge base for the technical note titled ***'How to run ADSS Server services as a non-root user daemon on UNIX/Linux.'*** This article provides step-by-step guidance on how to update the owner and group settings. Use the following command to mark install.sh file as executable before launching:

```
# sh chmod +x install.sh
```

The following command will kick off the installer in GUI mode:

```
# sh install.sh
```

The following command will run the installer in **Headless Mode (Non-GUI)**:

```
# sh install.sh headless
```

The installation wizard will guide you through the various steps to ensure a complete and correct deployment of ADSS Trust Monitor is achieved. These are detailed next in the upcoming sections. Three services will be registered in Windows Services Panel or /etc/init.d on UNIX.

*When upgrading an earlier version of ADSS Trust Monitor, it is important to start the ADSS Trust Monitor Installation wizard from the new installation directory. This **must be** different from the current installation directory for the previous release.*

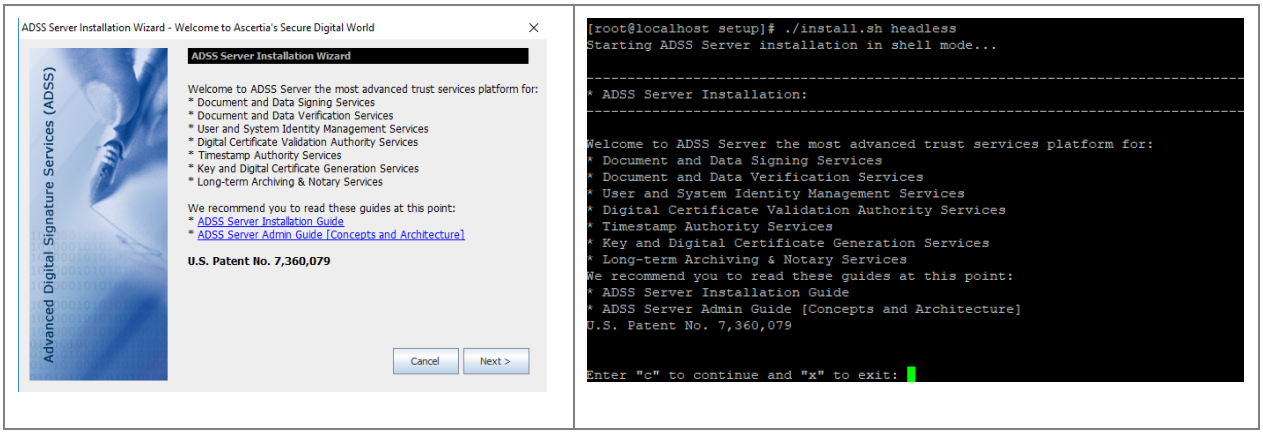
*Note current ADSS Trust Monitor instances **must be** stopped before starting the upgrade process.*

ADSS Trust Monitor is not installed as a single Windows NT service or a Unix daemon. A standard installation of ADSS Trust Monitor is comprised of three components:

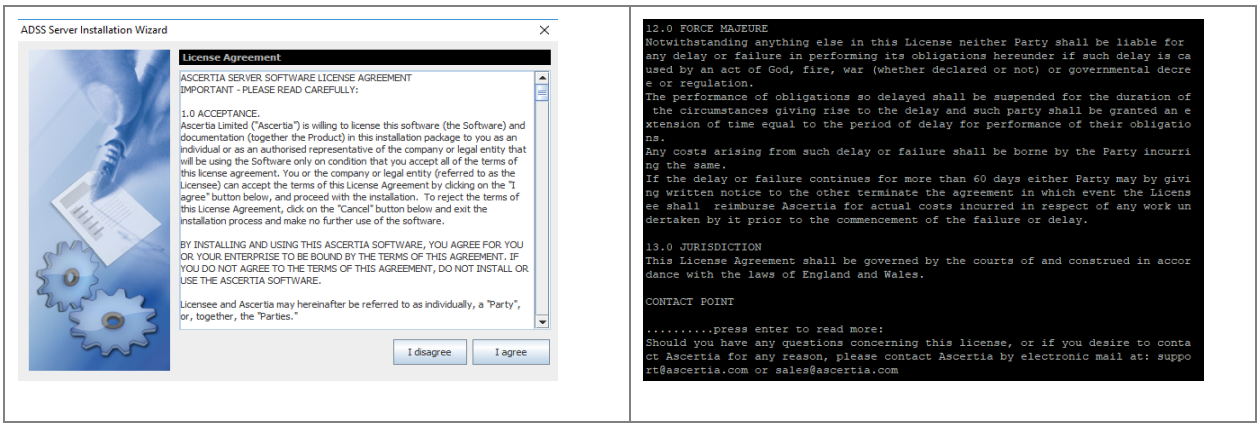
ADSS Core, ADSS Console and ADSS Service.

Each of these components uses a separate JVM. For a standard installation of ADSS Trust Monitor all three components is installed on one machine. For a custom installation, it is possible to install the components on separate machines. It is possible to install multiple ADSS Core, and ADSS Console instances for high availability, together with multiple ADSS Service instances to load-balance the service requests for higher throughput.

Running **install.bat/sh** shows the following screen:

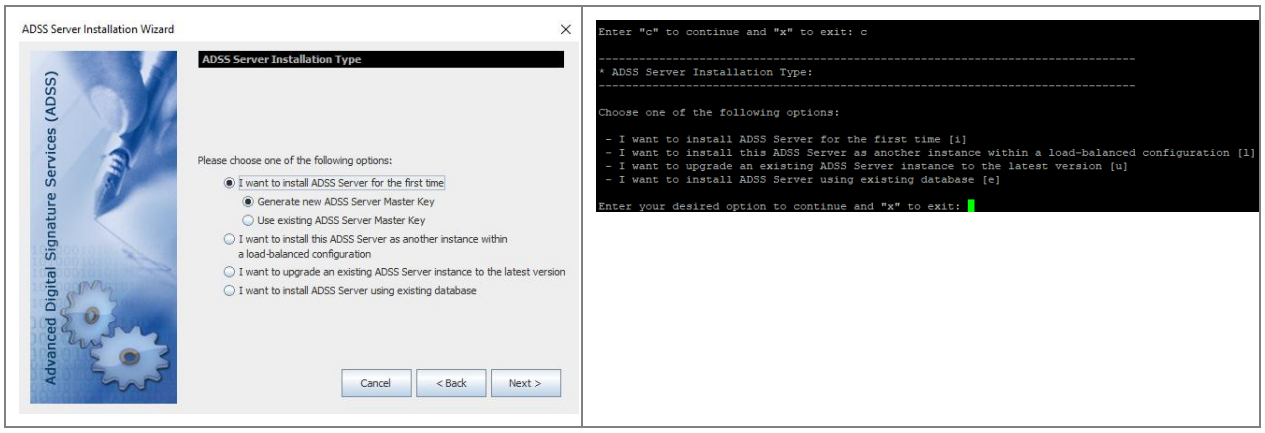


Clicking **Next >** shows the following screen:



If you agree with the displayed terms and conditions, then click "**I agree**" to continue the installation process otherwise click "**I disagree"** to stop the installation process.

Clicking **I agree** shows the following screen:

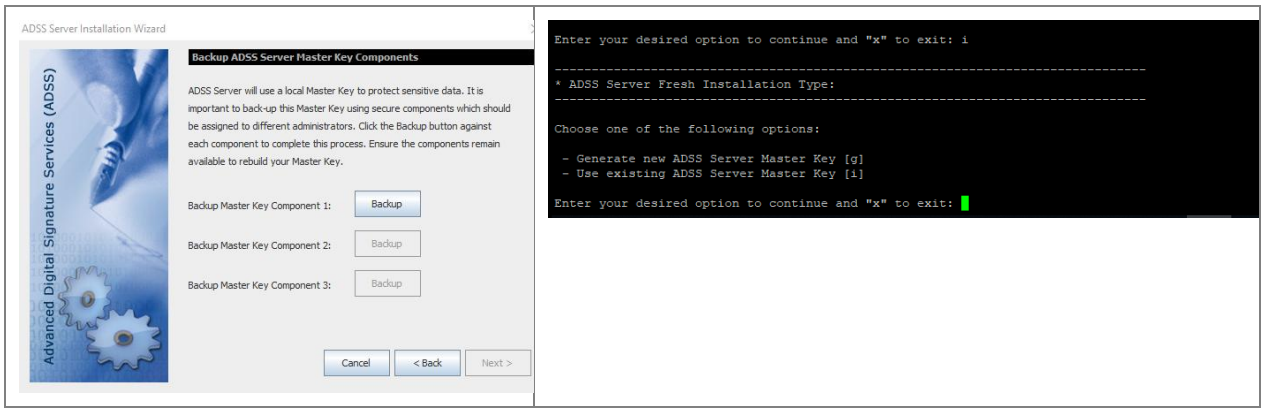


There are various installation options available in ADSS Trust Monitor. These are:

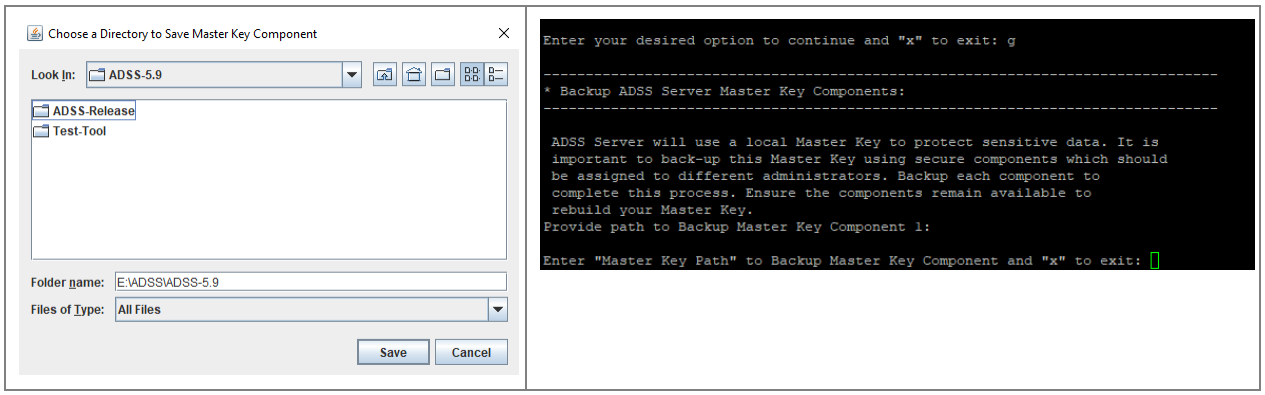
- **I want to install ADSS Trust Monitor for the first time** – Use this option if you want to install the latest ADSS Trust Monitor using a fresh/empty database. Following options are available for this for this type of installation.
  - **Generate new ADSS Trust Monitor Master Key -** This option is recommended when you are installing ADSS Trust Monitor for the first time either for evaluation or production use. This option assumes that a fresh database is already created and proper database access rights are assigned to the database user. Click here for more detail.
  - **Use Existing ADSS Trust Monitor Master Key-** This option is recommended when already installed ADSS Trust Monitor Master Key and configuration to be used for a new replicated ADSS Trust Monitor instance. This option assumes that a fresh database is already created, proper database access rights are assigned to the database user and all the configurations of the existing ADSS Trust Monitor are already exported. Click here for more detail.
- **I want to install this ADSS Trust Monitor as another instance within a load-balanced configuration** – Use this option to add another ADSS Trust Monitor instance to an existing ADSS Trust Monitor installation. You can install all components of ADSS Trust Monitor (Core, Console and/or Service) on multiple machines to better service the incoming requests. This option can also be used to achieve the high availability (fall-back mechanism) if the main instance stops responding. High availability is supported for ADSS Trust Monitor Core and Console instances only. ADSS Trust Monitor Service instance can always be installed in a load-balanced mode where a load-balancer (software or hardware based) manages the incoming requests and if any of the instances fail the load balancer intelligently shifts the load to the other Service instances. Click here for more detail.
- **I want to upgrade an existing ADSS Trust Monitor instance to the latest version** – Use this option if you already have an older ADSS Trust Monitor version installed and want to upgrade it to the latest version. ADSS Trust Monitor provides an automated way to upgrade both the application and the database from the previous versions (v3.0 and above) to the latest version without requiring any manual steps to be performed by administrators. Click here for more detail.
- **I want to install ADSS Trust Monitor using existing database** – Use this option if you want to install the ADSS Trust Monitor using an existing database of **the** These four options are further explained in the following sections:

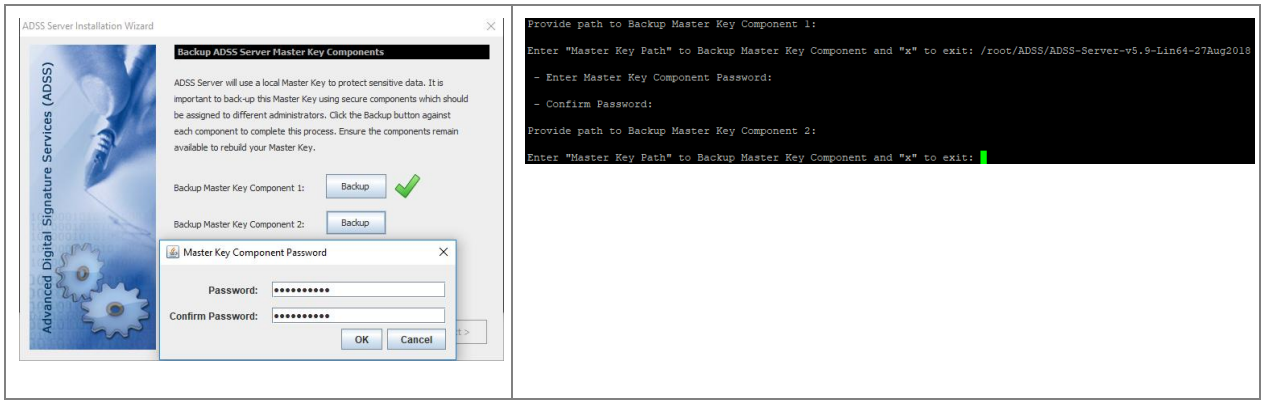
4.1.1 Installing ADSS Trust Monitor for the First Time

Select the option **I want to install ADSS Trust Monitor for the first time** on the ADSS Trust Monitor Installation Type screen:

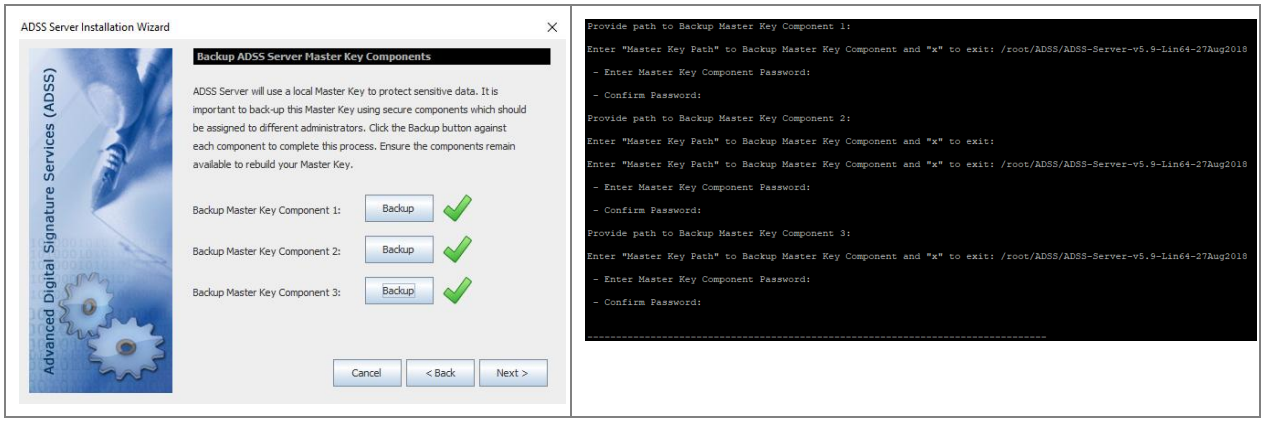


The installer will generate a Master Key to encrypt the data in database and prompt to take a backup of the Master Key in the form of three components. Use the **Backup** button one by one to take the backup of each Master key component, installer will prompt to provide a password for each Master Key component and encrypt it with the provided password before saving on the disk:



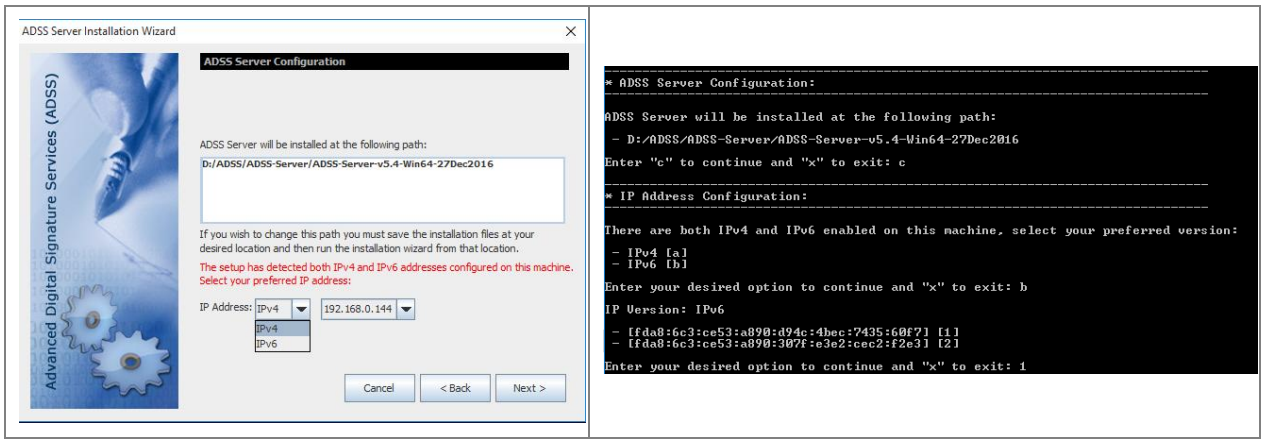


It's recommended to use different password for each Master key component. After completed the Backup the following screen appeared:



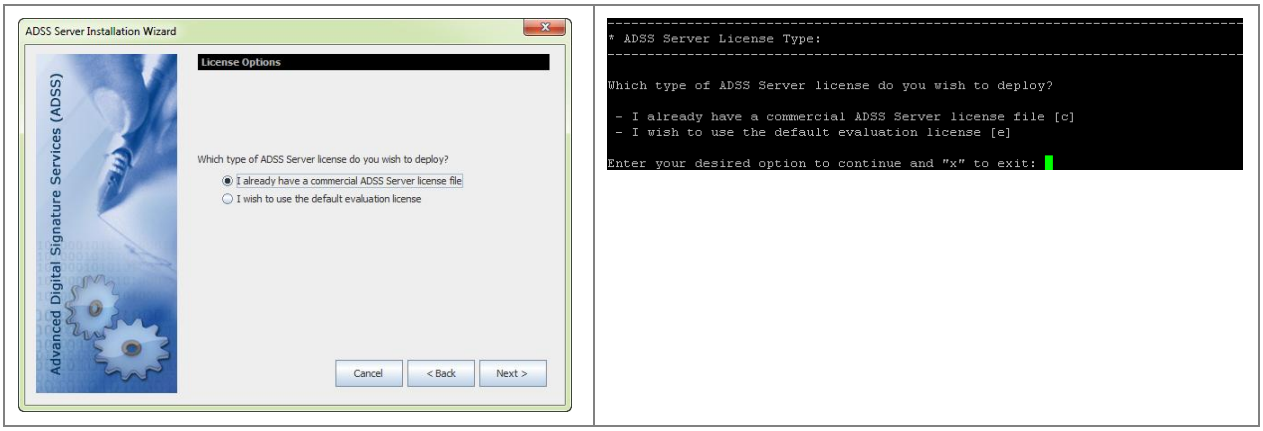
Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Trust Monitor to the next versions and even Ascertia cannot help you to recover these keys.

Once done, click **Next**. This screen shows the path where ADSS Trust Monitor software will be installed and allows to select the IP scheme for the ADSS Trust Monitor installation.



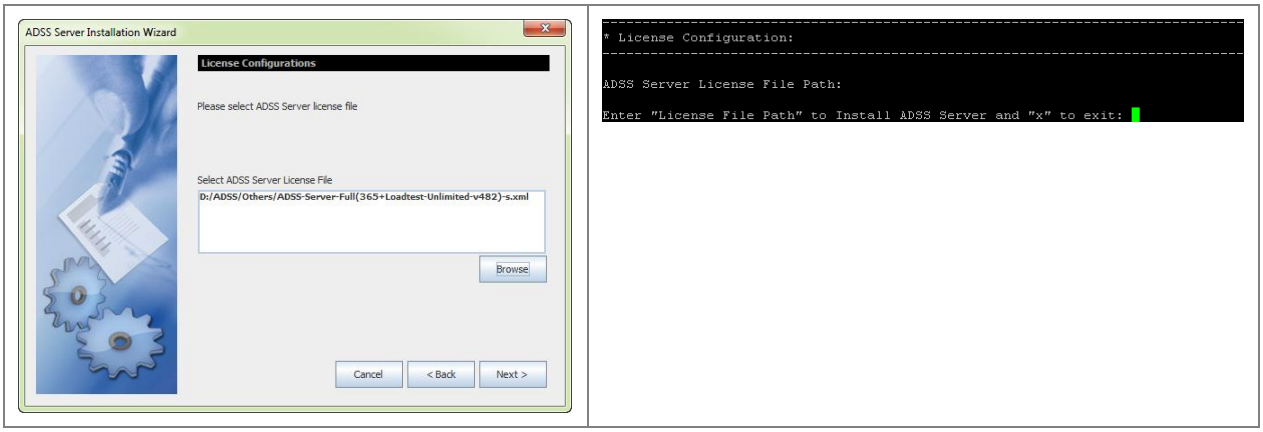
When Deploying ADSS Trust Monitor to Windows Azure, ADSS Trust Monitor installer will only look for the non-public IP address here, it will not look for the public address - it is not important here.

Clicking "**Next**" shows the License Options screen:



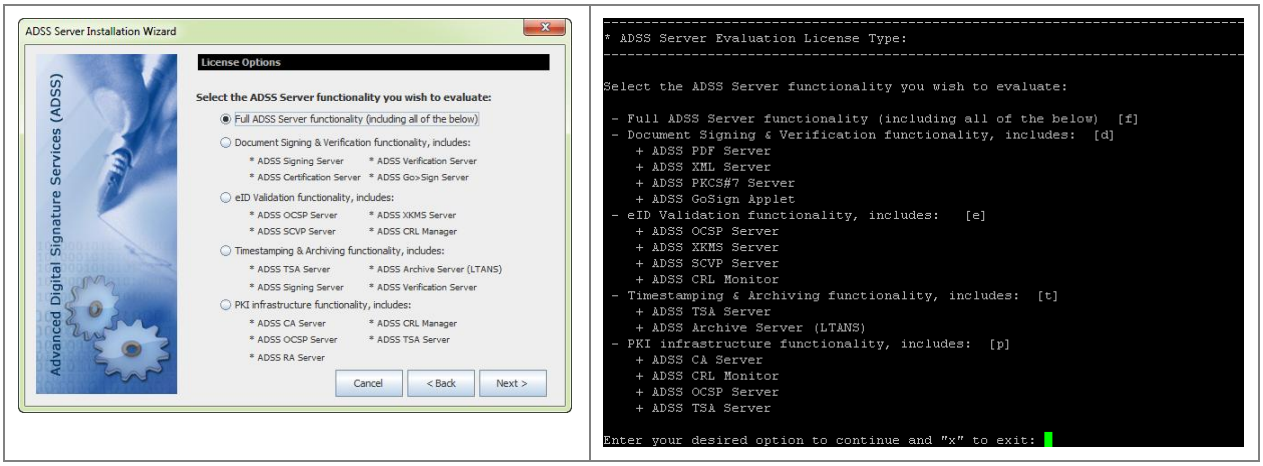
Select one of the license options on this screen: -

- If you wish to evaluate ADSS Trust Monitor, then select option "**I wish to use the default evaluation license**". The evaluation license limit is one month from the date of first installation.
- If you have a commercial ADSS Trust Monitor license, then select the option "**I already have a commercial ADSS Trust Monitor license file**" and you will be prompted to browse it on the next screen:



Use the **Browse** button to choose the commercial license file supplied by your software provider.

If you selected, the option "**I wish to use default evaluation license**" the following screen is shown:



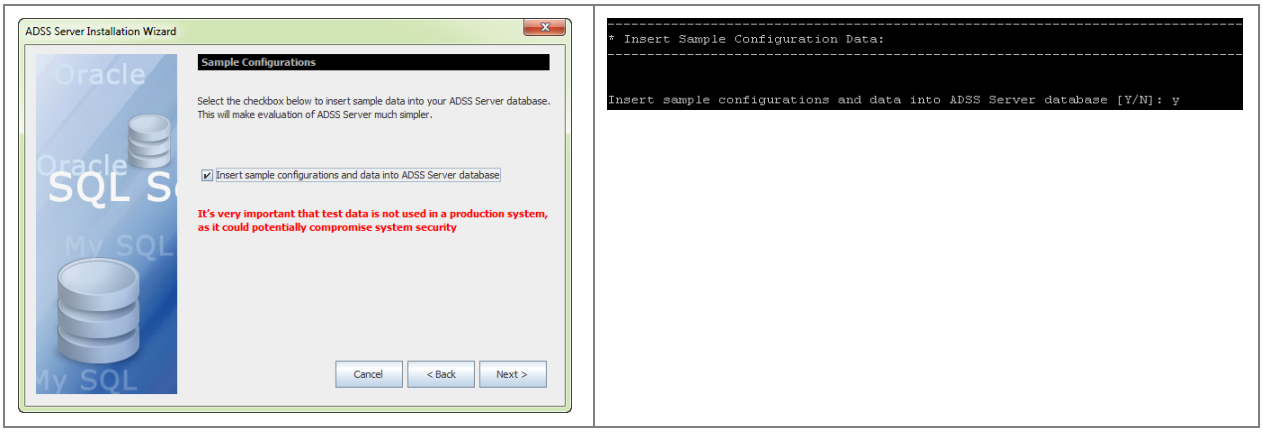
Select one of the options that best suits your business needs. When you select a license option from the list above, service features that are not licensed will not be shown. Custom evaluation licenses can be provided easily by your sales contact. Examples include a license just for PDF Signing, ADSS OCSP Server functionality or long-term archiving.

The default evaluation licenses supplied with ADSS Trust Monitor allows reasonable usage within pre-set time and transaction limits.

An ADSS Trust Monitor can be upgraded to use a full commercial license after evaluation just by overwriting the license file with a replacement.

New licenses take effect on the next full restart of all ADSS Trust Monitor instances.

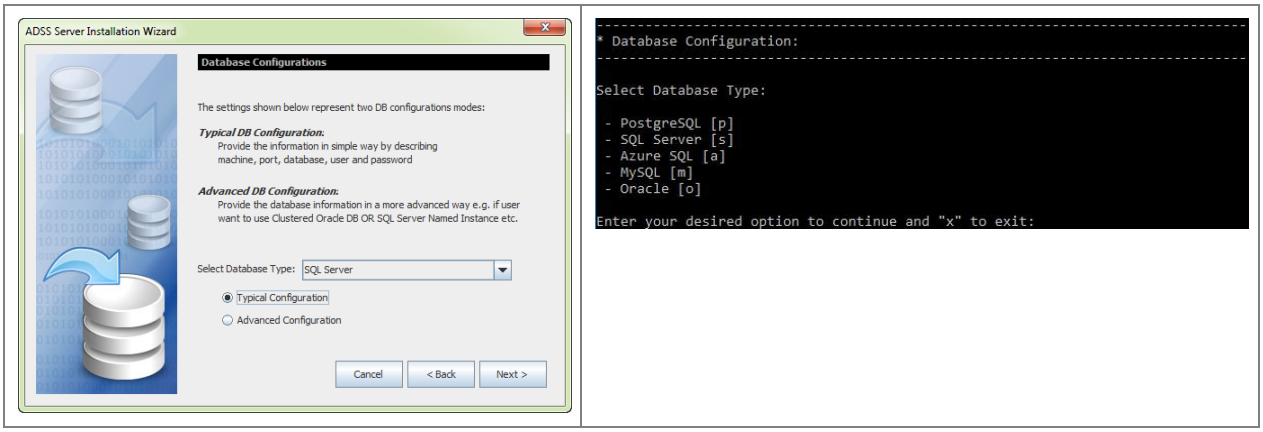
Click "**Next**" to proceed.



Selecting this option will insert the sample data in to the data to allow immediate testing/evaluating of ADSS Trust Monitor.

This option is not recommended if you are installing ADSS Trust Monitor in a production environment.

4.1.1.1 Database Configuration



Use this screen to select database type (e.g. SQL Server) and configuration type (Typical/Advanced)

Typical Configuration allows you to specify the database server name, database name, port etc. The Advanced Configuration also allows configuration of the low-level database driver URL, JARs etc. Unless you are experienced in this area, the typical configuration is recommended.

4.1.1.2 Installing ADSS Trust Monitor with SQL Server Database

The following must be considered when installing ADSS Trust Monitor with SQL Server:

When installing ADSS Trust Monitor with SQL Server, remember to select English as the default database user language, the system will not work if another database language option is selected.

Additionally, the following note must be considered when installing ADSS Trust Monitor with SQL Server 2012:

These configurations should be applied on SQL Server 2012 before installing ADSS Trust Monitor:

- *Open "SQL Server Configuration Manager"*
- *Click "SQL Server Services" on the left pane*
- *Right-click on your SQL Server instance name on the right pane -> Default: SQL Server(MSSQLSERVER)*
- *Click "Properties"*
- *Click "Start-up Parameters"*
- *On the "specify a start-up parameter" textbox type "-T272"*
- *Click "Add"*
- *Confirm the changes*

Source: http://www.big.info/2013/01/how-to-solve-sql-server-2012-identity.html

4.1.1.3 Installing ADSS Trust Monitor with PostgreSQL Database

The following must be considered when installing ADSS Trust Monitor with PostgreSQL:

Make sure you assign the language "plpgsql" after creating the database by executing the following SQL query:

```
create language 'plpgsql'
```

ADSS Trust Monitor establishes a database connection pool on start-up and this connection pool has configurable limits for initial pool size and maximum pool size. For console operations and service requests, ADSS Trust Monitor uses database connections from the established connection pool and acquires more connections as required until the connection pool size reaches the maximum allowed limit. For guidance on configuring database connection limits, refer to the technical note titled 'How to change the default database connection pool size limits in ADSS Server' available in the Ascertia Community Portal knowledge base.

The default connection pool size for a PostgreSQL database is 100 connections and this is generally insufficient for a production deployment of ADSS Trust Monitor. Follow these instructions to increase the maximum connections limit in PostgreSQL:

- *Edit file* `[PostgreSQL Installation Dir.]/data/postgresql.conf`
- *Set the value of the* `max_connections = 1150`
- *Restart PostgreSQL server*
- *Restart ADSS Trust Monitor to have these changes take effect.*

4.1.1.4 Installing ADSS Trust Monitor with MySQL Database

Oracle does not allow free distribution of the required MySQL JDBC connector. You are required to download the latest version from the following link: http://dev.mysql.com/downloads/connector/j/

The following MySQL JDBC driver file has been tested:

- *mysql-connector-java-5.1.36-bin.jar*
- *mysql-connector-java-8.0.13*

If a later version of the file is available, then it should also work. Please contact Ascertia Support to confirm.

1) Rename the downloaded driver file to **mysql-connector-java.jar** and place it in the following locations in ADSS Trust Monitor package:
   - **[ADSS-Server-Home]\core\server\webapps\core\WEB-INF\lib**
   - **[ADSS-Server-Home]\console\server\webapps\console\WEB-INF\lib**
   - **[ADSS-Server-Home]\service\server\webapps\service\WEB-INF\lib**
2) If the downloaded driver is **mysql-connector-java-8.0.13**, refer to the technical note titled ***'How to disable the ECC cipher in Tomcat's Catalina'*** in the Ascertia Community Portal knowledge base for specific instructions on disabling ECC ciphers in Tomcat.
3) Ensure that the proper database privileges are assigned to the ADSS Trust Monitor database user. Create a database and assign the following rights to the user on the database before starting the ADSS Trust Monitor installation:
   - CREATE, DROP, ALTER, DELETE, INDEX, INSERT, SELECT, UPDATE, CREATE TEMPORARY TABLES, ALTER ROUTINE, CREATE ROUTINE, EXECUTE
4) If MySQL database is installed on a UNIX machine, MySQL database server needs to be configured to compare the database table names in case insensitive mode.

   Follow these steps to make this configuration change:
   - Open **"/etc/my.cnf**" in edit mode
   - Under the "**mysqld**" section set the parameter "**lower_case_table_names=1**"

Modify the configuration file before starting the freshly installed MySQL Server v8.0.x otherwise you have to re-install the MySQL Server again.

If ADSS Trust Monitor Installation wizard was already launched before performing the above mentioned steps, then follow these instructions:

1. *Cancel the installation wizard and remove the current ADSS Trust Monitor directory.*
2. *Extract the ADSS Trust Monitor again from the Zip File*
3. *Perform the above mentioned instructions.*
4. *Launch the Installation wizard again so that installer can pick MySQL driver.*

5) Now launch ADSS Trust Monitor Installation wizard to install it with MySQL database.

If MySQL Percona XtraDB Cluster is hosted on Linux, then MySQL database service has to be manually started every time this Linux machine is restarted using following command:

systemctl start mysql@bootstrap.service

MySQL may prevent ADSS Trust Monitor inserting records larger than a particular size. If this problem occurs, then you need to configure MySQL database server to overcome this problem by setting max_allowed_packet parameter. Click here to read how to update the MySQL configuration file.

When using large TEXT or BLOB, the combined size on log files has to be at least 10 times the size of largest such row. e.g. for a 10MB CRL set:

innodb_log_file_size = 100M

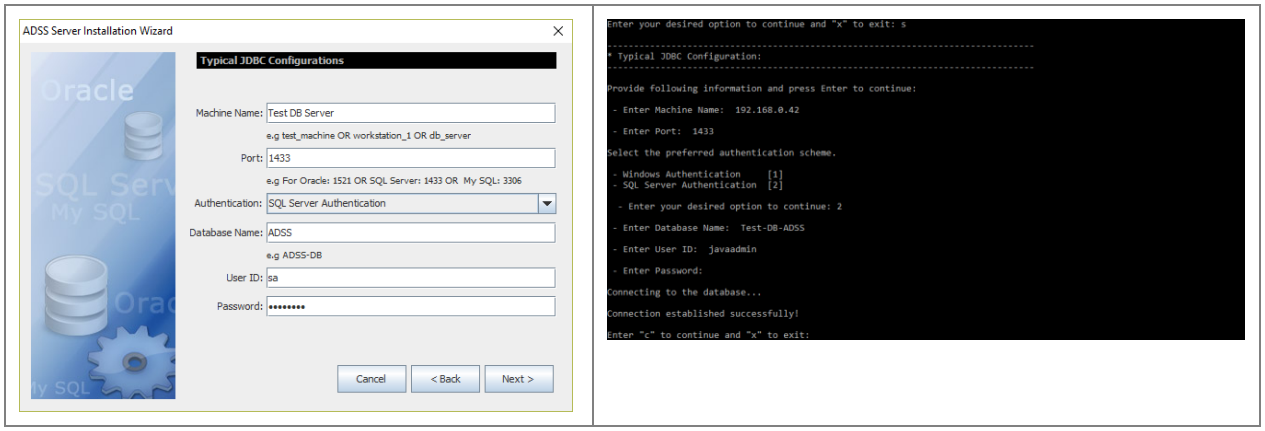
innodb_log_files_in_group = 100

It's worthwhile reading the documentation on how this is changed:

http://dev.mysql.com/doc/refman/5.5/en/innodb-data-log-reconfiguration.html

4.1.1.5 Database Connection Parameters

Getting back to the ADSS Trust Monitor installation, selecting "**Typical Configurations**" on the Database Configurations screen and clicking **Next** shows the following screen:



The configuration items are as follows:

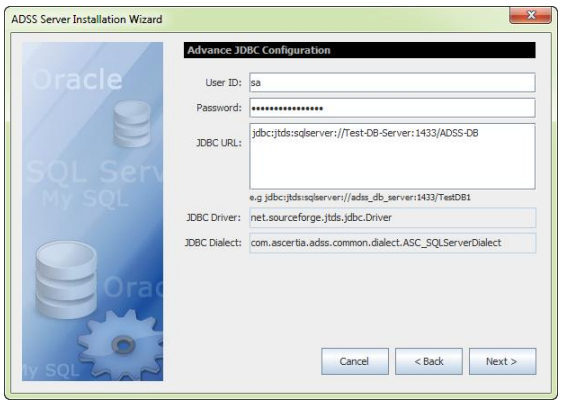
Item	Description
Machine Name	The system name or IP address of the machine where the database server is running, e.g. asc_db_server. If you are installing ADSS Trust Monitor on the same machine as the database, please enter “localhost” as the Machine Name.
Port	The port number of the database, e.g. 1433 for SQL Server.
Authentication Scheme	In case of ADSS Trust Monitor installation with SQL Server as Database, user can be authenticated by two ways i.e.: • SQL Server Authentication • Windows Authentication For SQL Server Authentication, user needs to enter the User Name and Password of SQL Server. Whereas in Windows Authentication, these fields will be disabled and user will be authenticated by the logged-in user Windows/Domain credentials. **Note:** Under typical JDBC configurations only Kerberos authentication is supported. For NTLM based authentication use the advanced JDBC configurations.
Database Name	The name of database for ADSS Trust Monitor. This can be a newly created empty database or an existing database. Make sure the database exists before clicking the Next button.
User ID	The user ID used by ADSS Trust Monitor to connect to the database. Ensure that this user exists and has the appropriate privileges to create and access tables.
Password	The corresponding password for the User ID.

Table 2 - Database Connection Parameters - Typical

Clicking “**Next**” checks the database credentials and connectivity, and moves to the next screen only if successfully validated.

4.1.1.6 Using Advanced Configurations

If you select **Advanced Configurations** in the Database Configurations screen, the following screen is shown:



Advanced Database Configurations are not supported in Headless mode. You must make changes manually in hibernate.cfg.xml after installation.

The configuration items are as follows:

Item	Description
User ID	The user ID used by ADSS Trust Monitor to connect to the database. Ensure that this user exists and has the appropriate privileges to create and access tables.
Password	The corresponding password for the User ID.
JDBC URL	JDBC URL is a database connection string. This is useful for configuring a connection string manually or for database connection pooling, i.e. the connection string provides details of the individual database server name, port, user ID and password running in a database pooled environment. To Install ADSS Trust Monitor with SQL Server using Windows Authentication, leave the User ID and Password fields empty and use the following string: • ***Kerberos Authentication*** *jdbc:jtds:sqlserver://<DATABASE_MACHINE>:1433/<DATABASE_NAME ;integratedSecurity=true* • ***NTLM Authentication*** *jdbc:jtds:sqlserver://<DATABASE_MACHINE>:1433/<DATABASE_NAME ;domain=<DOMAIN_NAME>;useNTLMv2=true* To Install ADSS Trust Monitor using TLS perform the following steps: **1.** Import TLS CA issuer certificate in the ADSS Trust Monitor JDK using certificate import utility. Run utility from <ADSS-Home>/util/bin/import_cert_into_keystore.bat or import_cert_into_keystore.sh. A graphical interface will display to browse intended certificate. **2.** One of the following strings must be used: ***a. PostgresSQL*** *jdbc:postgresql://<Server-Name/IP>:5432/<Database_Name>? ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory* ***b. SQL Server*** *jdbc:jtds:sqlserver://<Server-Name/IP>:1433/<Database_Name>;ssl=require* *If SQL named instance is used then use the following string:*

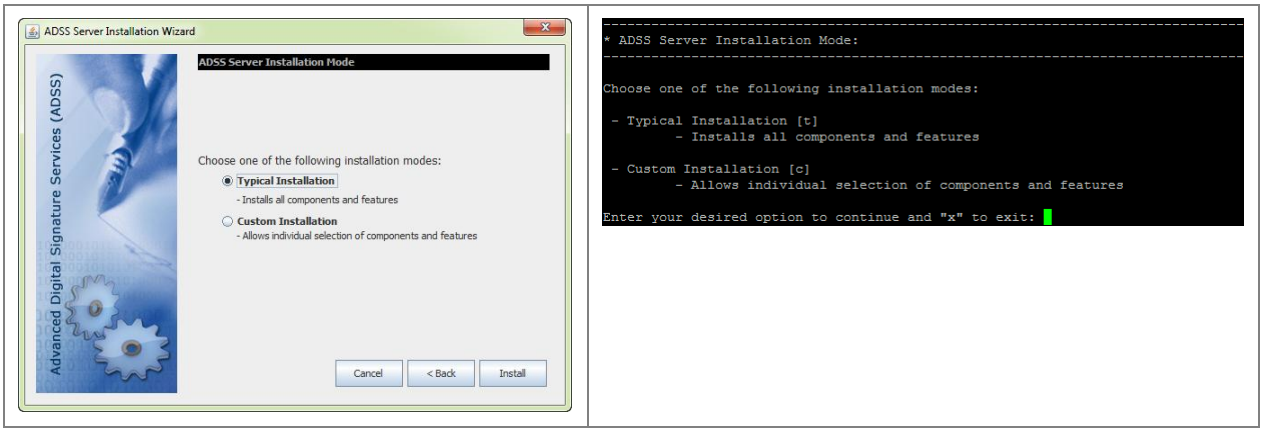
Item	Description
	jdbc:jtds:sqlserver://<Server-Name/IP>/ <Database_Name>;instance=<Instance-Name> ***c. Azure SQL (database as a service)*** *jdbc:sqlserver://<Server-Name/IP>;database=<Database_Name>; ssl=require*
JDBC Driver	The name of the driver used to communicate with the database.
JDBC Dialect	As ADSS Trust Monitor uses Hibernate technology to communicate with the database, it provides the hibernate-package details which is used for communication. Note that Hibernate provides different JDBC dialects for different DBMS. See http://www.hibernate.org/ for more details.

Table 3 - Database Connection Parameters – Advanced

If Windows authentication is used instead of SQL Server authentication, then follow this KB article for the appropriate configurations after the installation:

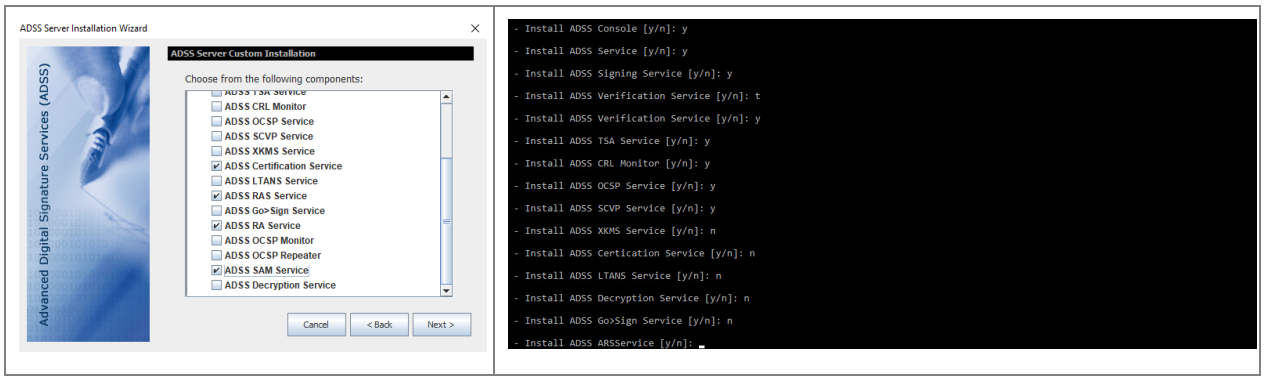
https://ascertia.force.com/partners/s/article/How-to-register-all-the-instances-of-ADSS-Server-SigningHub-Core-under-a-domain-user-account

Clicking "**Next**" on the Typical or Advanced database configuration screen shows the following screen:



Select the installation mode you wish to use:

- **Typical Installation** – Select this option if you want to install all components of ADSS Trust Monitor with default memory parameters, i.e. Core (1024-MB), Console (1024-MB) and Service (2048-MB) on the current system.
- **Custom Installation** – Select this option if you want to install selected ADSS Trust Monitor components and service modules with custom memory parameters. Selecting this option and clicking **Next** shows the following screen:

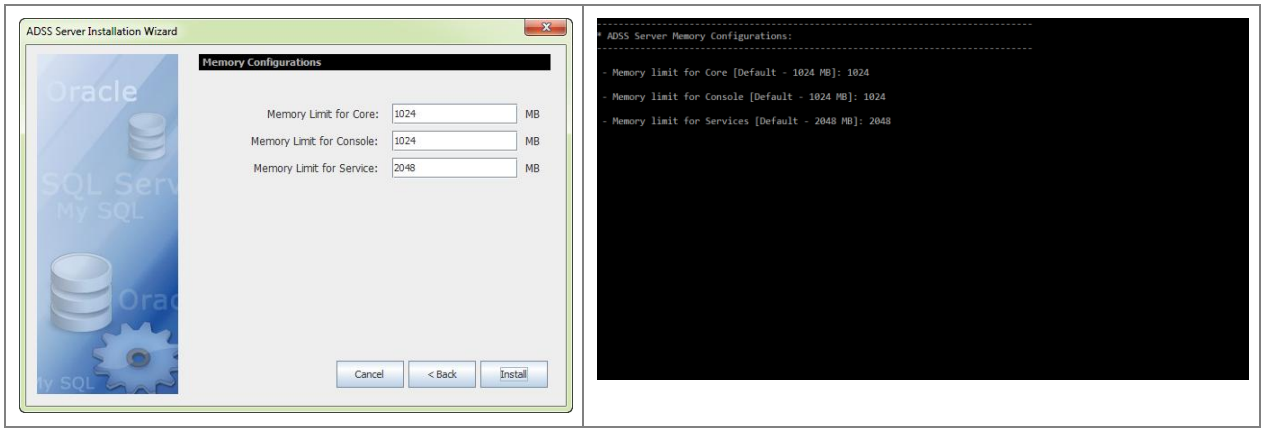


This screen allows you to select ADSS Trust Monitor components to install on this system. During a fresh installation ADSS Core is selected by default and optionally you can choose to install the ADSS Console and ADSS Service components if required.

When selecting ADSS Service components, at least one component must be selected.

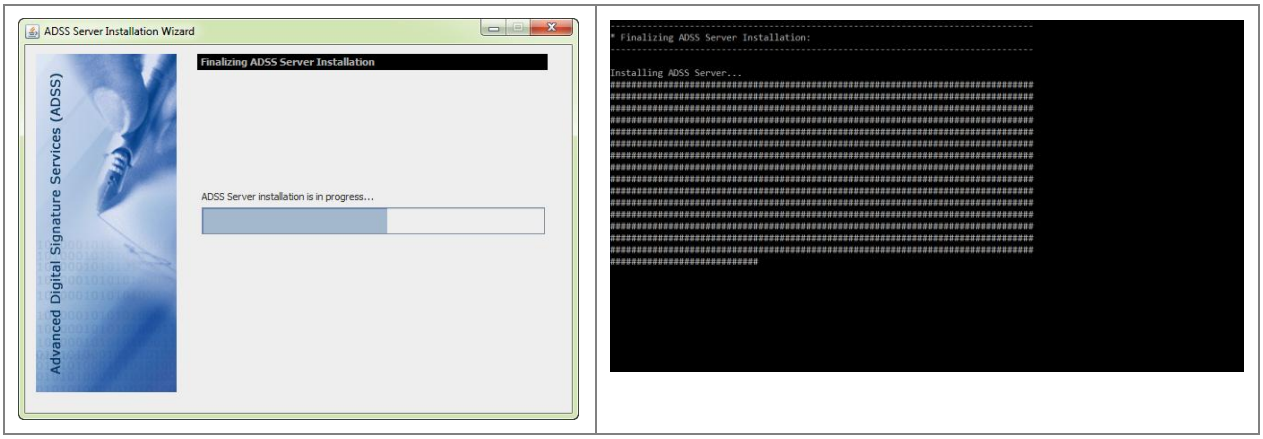
Note the above screenshot shows an installation with a full commercial license for ADSS Trust Monitor. In your case, only those services are shown that are actually licensed to you.

Select the relevant components to install and click **Next** to show the following screen, which allows you to assign the maximum memory limit for each component.

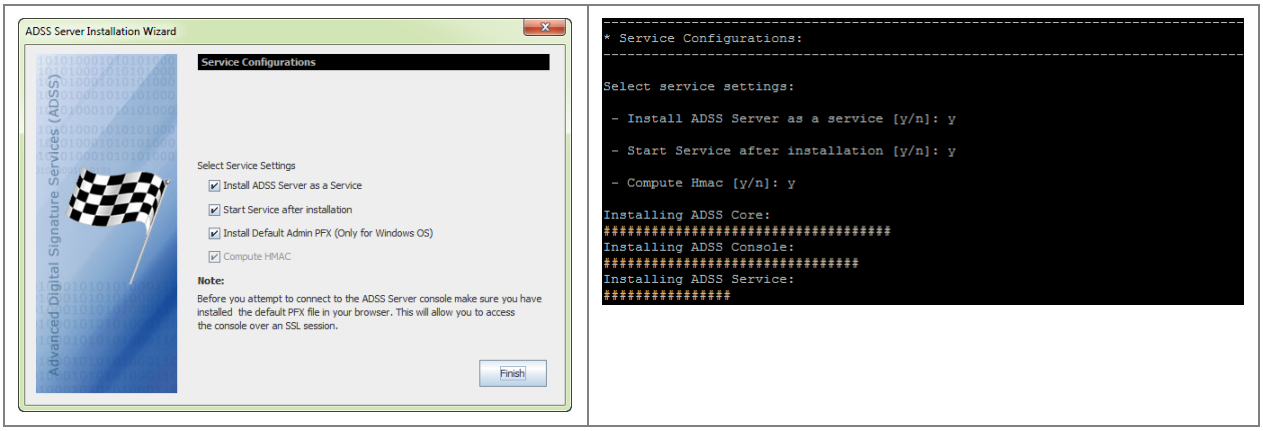


This screen allows you to define the maximum memory limit for each instance of ADSS Trust Monitor. Default maximum memory limit for Core and Console is 1024 MB and for Service instance 2048 MB.

After providing the maximum memory limit clinking on **Install** starts the installation process including execution of database scripts and updating the configuration files.



Once the installation has completed, the following screen is shown:



- **Install ADSS Trust Monitor as a service -** (the default recommended option) In Windows environment, the selected ADSS Trust Monitor components will be registered in Windows Services Panel with the following names:
    - Ascertia-ADSS-Console
    - Ascertia-ADSS-Core
    - Ascertia-ADSS-Service

  On UNIX operating systems, the selected ADSS Trust Monitor components will be registered in **/etc/init.d** with the following names:
    - tomcatd-ADSS-console
    - tomcatd-ADSS-core
    - tomcatd-ADSS-service

- **Start Service after installation -** This option is available only if the previous option is selected. If checked the registered services will be started automatically after installation.

- **Install Default Admin PFX (Only for Windows OS) –** Selecting this option will install the default client authentication certificate in MS CAPI keystore, which allows you to login to the ADSS Trust Monitor Console using Admin operator (this is only required when ADSS Trust Monitor is installed very first time).

*The password of the Default Admin PFX is **password***

It is highly recommended to configure new operator from Access Control module and either inactivate or to change the client authentication certificate for default Admin operator with a certificate certified by your PKI.

It could be a security risk if you continue to use the Admin operator with default certificate in production environment.

This option is disabled on UNIX and **adss_default_admin.pfx** must be imported in Firefox or other web browser, manually from: **[ADSS-Server-Home]/setup/certs/** directory in order to login to the ADSS Trust Monitor Console. Note the web browser does not need to be on the same server as ADSS Trust Monitor. The administration console is accessed over HTTPS.

- **Compute HMAC –** HMAC is a cryptographic checksum computed by ADSS Trust Monitor on every record within the ADSS Trust Monitor database to detect unauthorized changes in the database. It is mandatory to compute HMAC for a fresh installation so the option is checked and greyed out.

Clicking **Finish**, will complete the ADSS Trust Monitor installation wizard and a success message is shown:

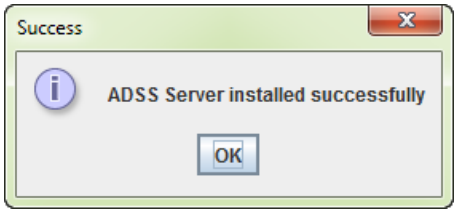
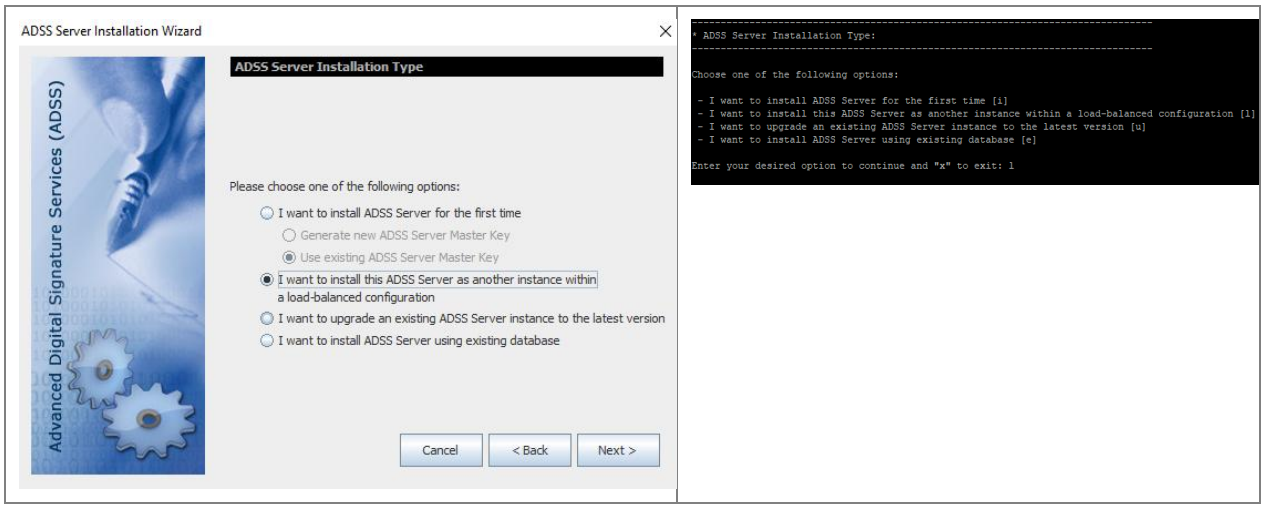


Figure 5 - ADSS Trust Monitor Installation Wizard Success Screen

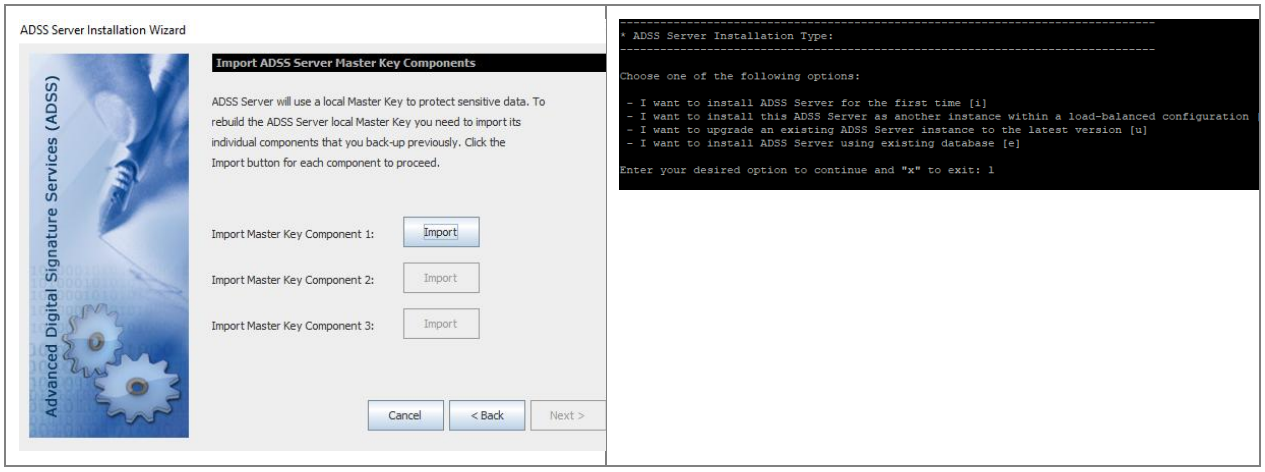
Once the installation is completed, refer to the ADSS Trust Monitor Admin Guide to configure the required services.

4.1.2 Installing ADSS Trust Monitor in a Load-Balanced Configuration

Select the option **I want to install this ADSS Trust Monitor as another instance within a load-balanced configuration** on the ADSS Trust Monitor Installation Type screen:

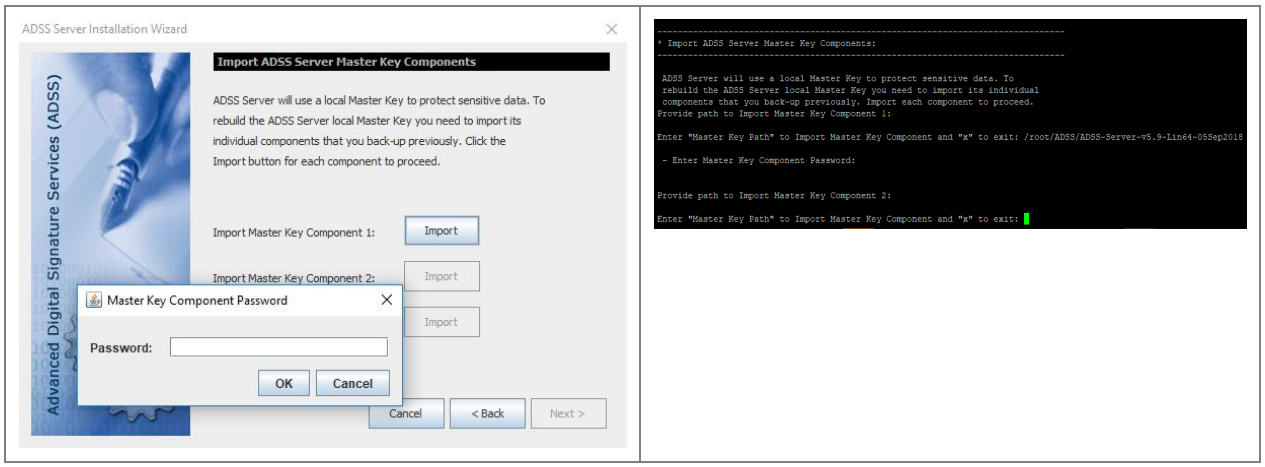


Click Next will show following screen:

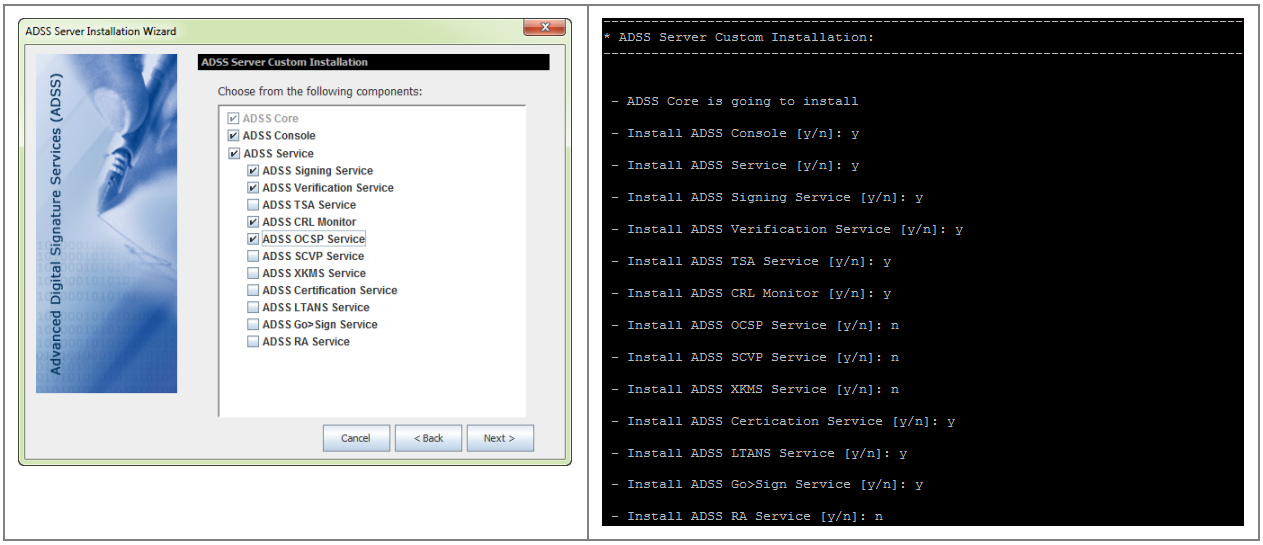


Use the **Import** button one by one to restore the backup of each Master key component (generated during the ADSS Trust Monitor Primary instance installation) so that installer will restore the Master Key, installer will prompt to provide a password for each Master Key component and decrypt it with the provided password.

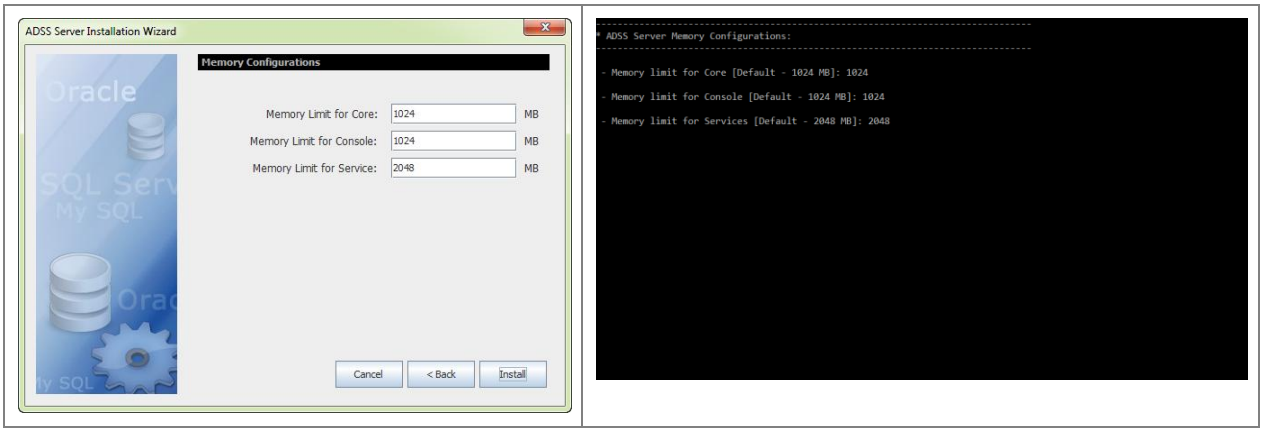
The Master Key backup should be imported in the same sequence and passwords when it was backup during first installation.



Proceed through the Installation wizard as before until ADSS Trust Monitor custom installation screen is shown. When installing ADSS Trust Monitor in a load-balanced configuration the option **Typical ADSS Trust Monitor Installation** is not available.



On this screen, select ADSS Trust Monitor modules you want to use, click "**Next**" button and set the maximum memory limit for the selected instances:



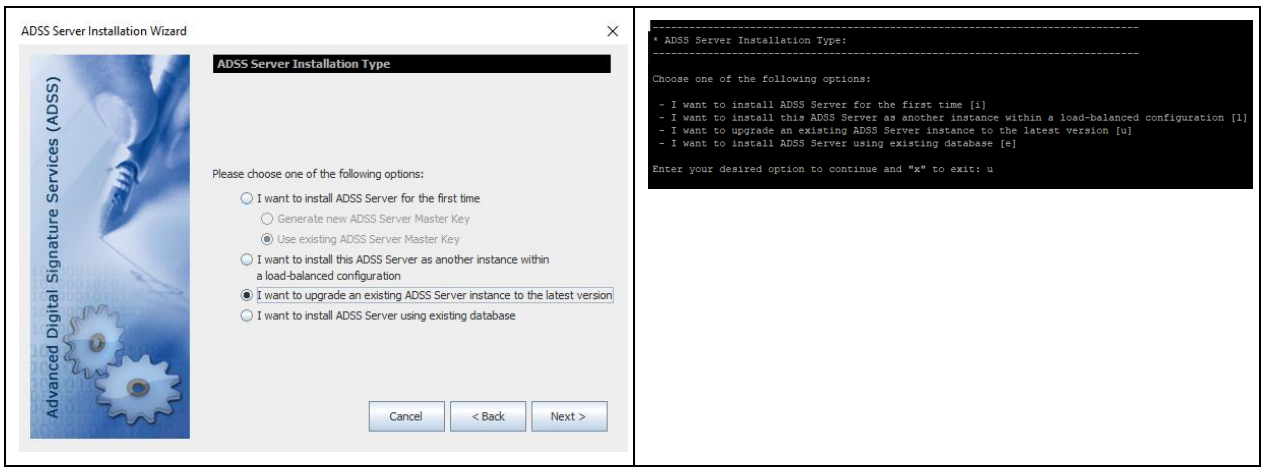
This screen allows you to define the maximum memory limit for each instance of ADSS Trust Monitor. Default maximum memory limit for Core and Console is 1024 MB and for Service instance 2048 MB.

Provide the maximum memory limit and click **Install** and follow rest of the installation wizard to complete the installation.

4.1.3 Upgrading an Existing ADSS Trust Monitor Instance

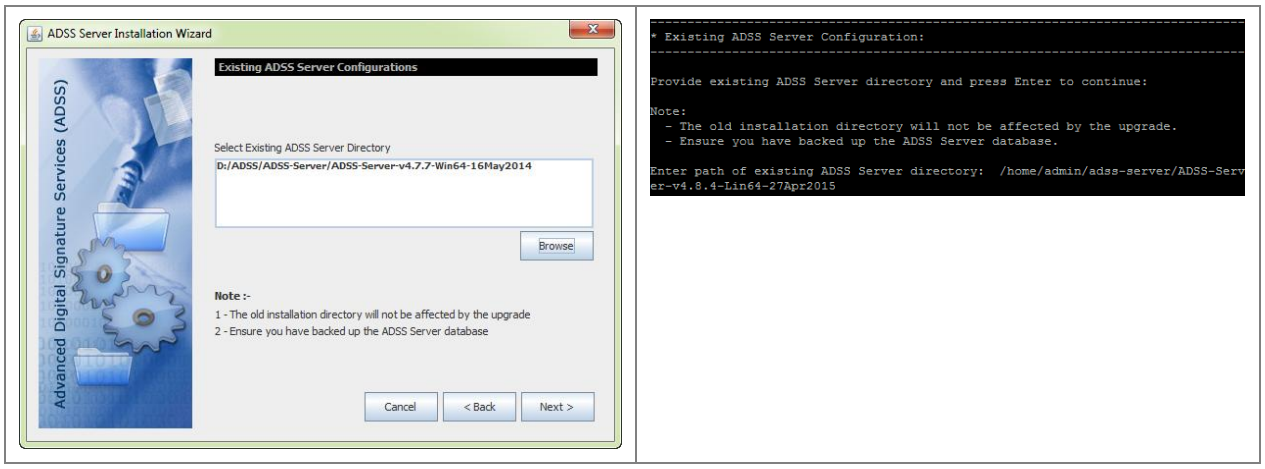
On the current system, download and extract the latest ADSS Trust Monitor software to a new location that is **different** from the current ADSS Trust Monitor installation folder or directory.

Now run the ADSS Trust Monitor installation wizard from the new package, and on the ADSS Trust Monitor Installation Type screen select the option **I want to upgrade an existing ADSS Trust Monitor instance to the latest version**:



Clicking "**Next**" shows the following screen:

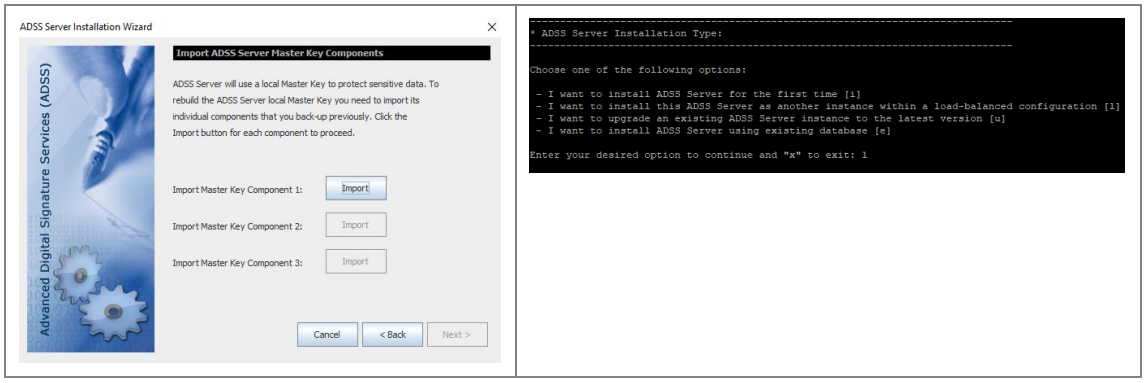
This will show the Existing ADSS Directory path will require in the Wizard as given in below screen:

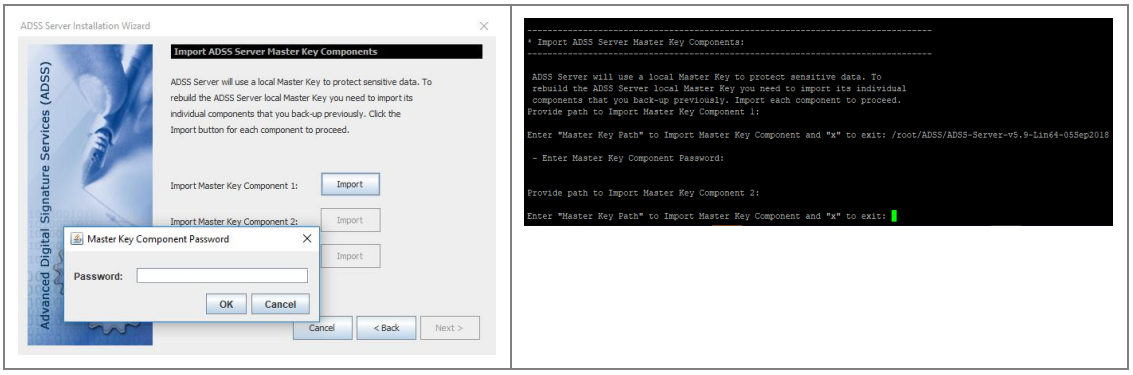


Click **Browse** to select the **existing** ADSS Trust Monitor installation directory and click "**Next**" to proceed:

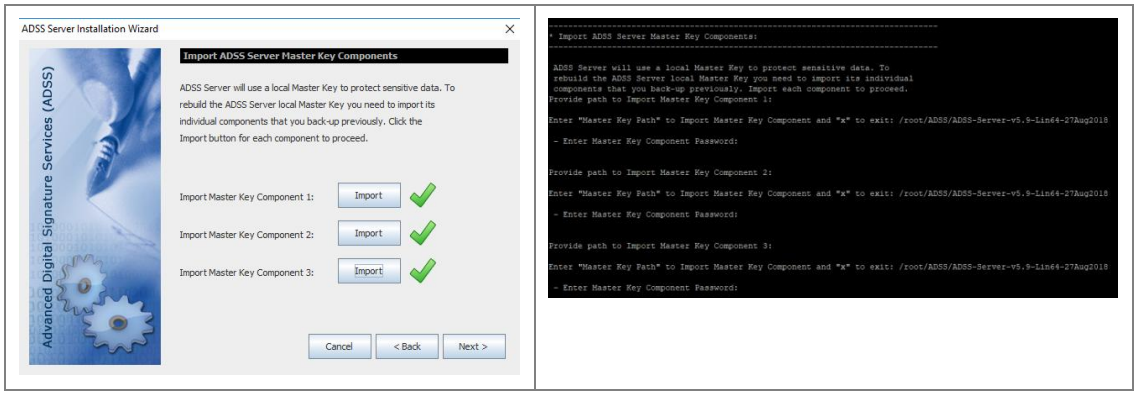
- Upgrading ADSS Trust Monitor from version v5.9 or later doesn't require importing master key components.
- Upgrading ADSS Trust Monitor from version v5.8 or older require importing master key components
    - For upgrading ADSS Trust Monitor Primary Core or Standalone instance, the installer will generate a Master Key to encrypt the data in database and prompt to take a backup of the Master Key in the form of three components at the end of the installation wizard
    - For upgrading ADSS Trust Monitor Secondary Instance, the installer will prompt to **Import** each Master key component (generated during the Primary ADSS Trust Monitor installation) one by one along with password in order to decrypt and import it.

The Master Key backup should be imported in the same sequence and passwords when it was backup during first installation.



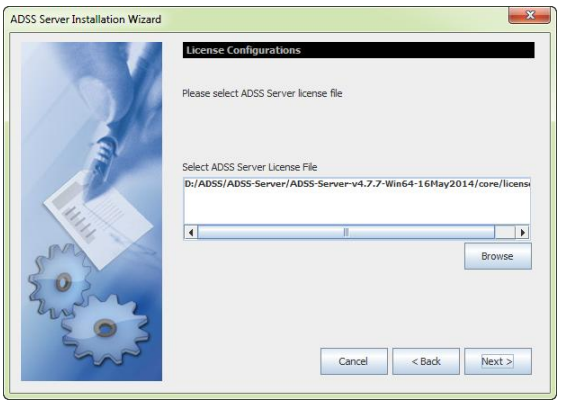


The following screen of Import Backup keys will appear.

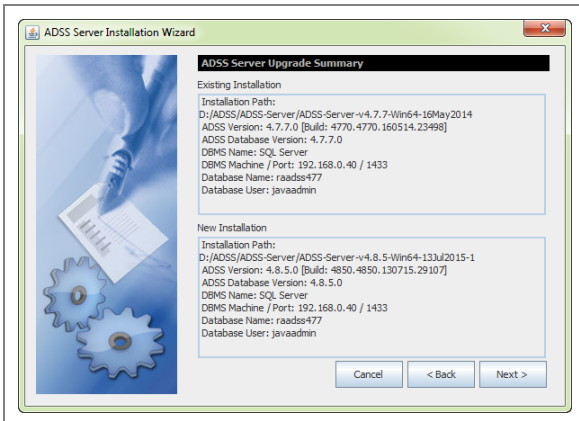


Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Trust Monitor to the next versions or make it load balanced. Even Ascertia cannot help you to recover these keys.

Once done, click **Next.**

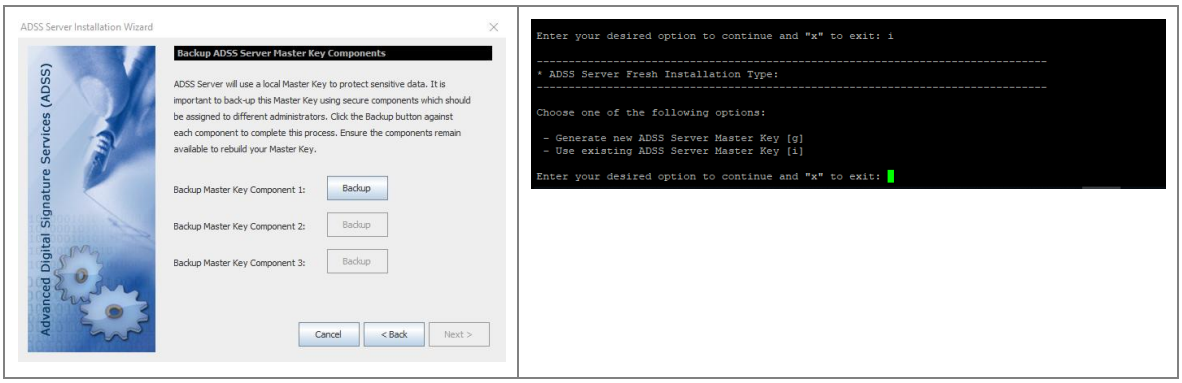


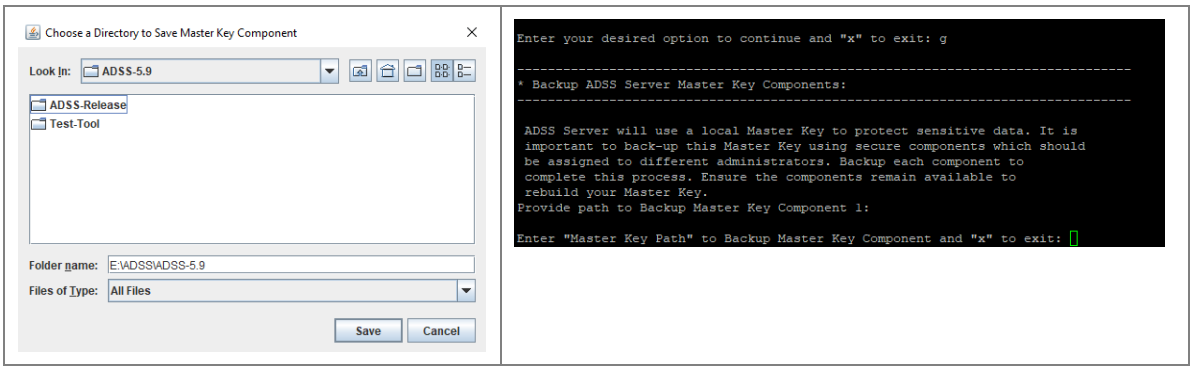
Continue through the installation wizard to reach the screen showing a summary of the old and new installation directories:

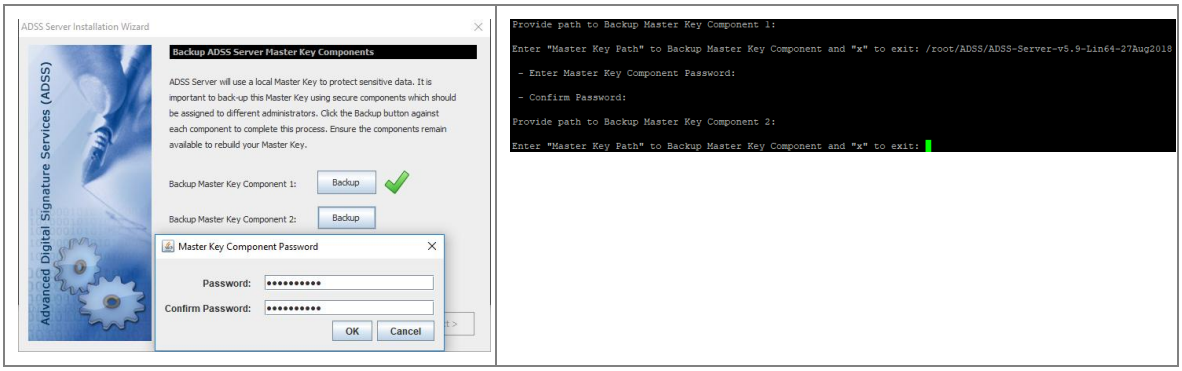


Review the details of both the new and existing installations of ADSS Trust Monitor. If the summary details are correct then click **Next >** to continue the upgrade.

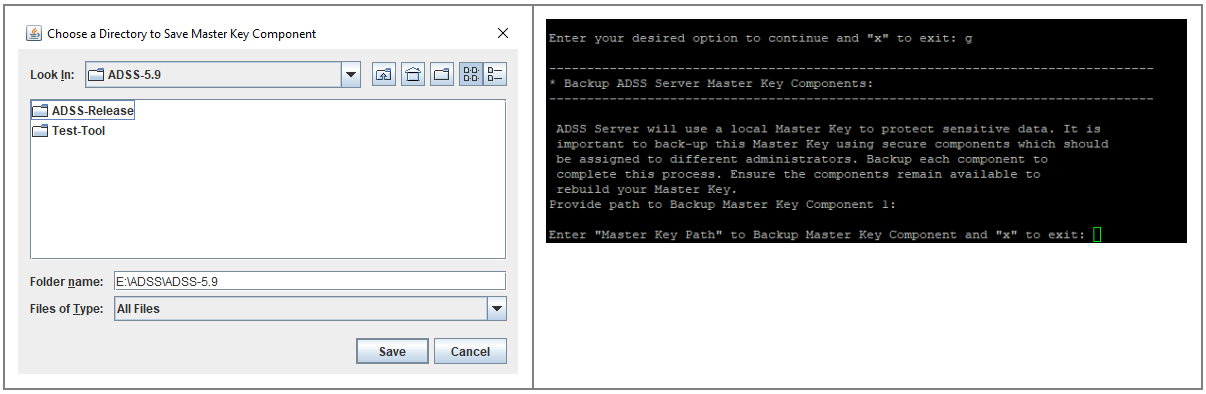
- If it is Primary Core or standalone instance upgrade, then the installer will generate a Master Key to encrypt the data in database and prompt to take a backup of the Master Key in the form of three components. Use the **Backup** button one by one to take the backup of each Master key component, installer will prompt to provide a password for each Master Key component and encrypt it with the provided password before saving on the disk:

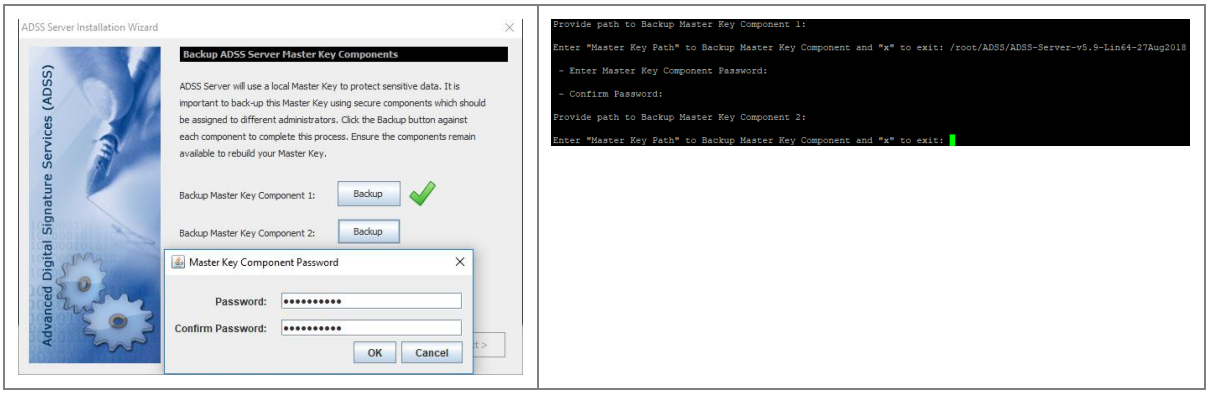






It's recommended to use different password for each Master key component. After completed the Backup the following screen appeared:

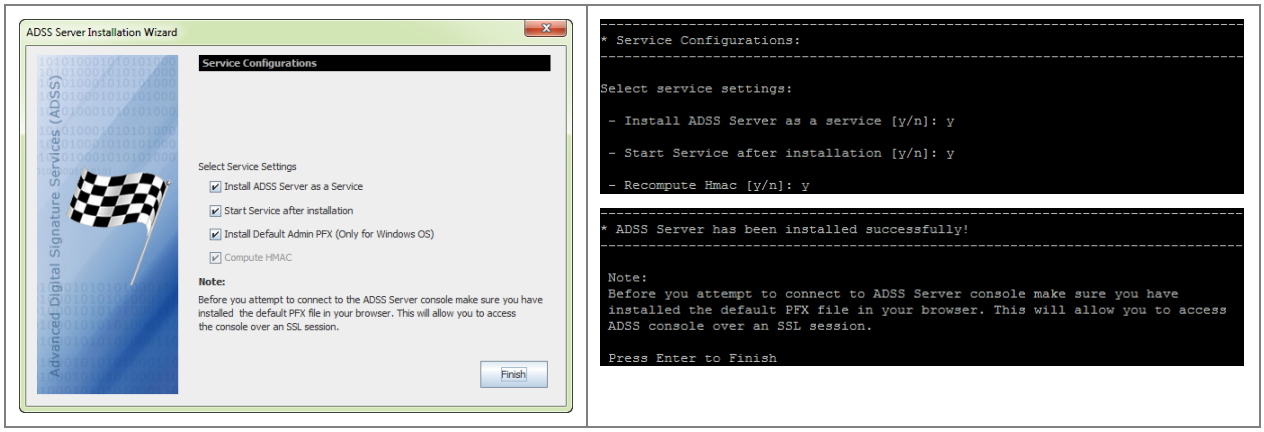




It's recommended to use different password for each Master key component.

Keep the Master key components secure and retain the password. If you lost the keys/password then you cannot upgrade this ADSS Trust Monitor to the next versions and even Ascertia cannot help you to recover these keys.

After the upgrade, it is strongly recommended that the HMAC values are re-computed. On **Finish** screen an option is provided for this:



Compute HMAC – HMAC is shown corrupted for database records for which new columns are added/deleted when upgraded to new version. By checking this option, HMAC will be recomputed on the tables that are alerted to meet new functionality requirements otherwise HMAC values will no longer be valid.

HMAC re-computation can take a substantial period of time depending on the database size (i.e. measured in hours). To minimize this time, it is recommended to complete the installation without re-computing HMAC during the upgrade process to allow ADSS Trust Monitor operations to be started without delay as described next.

The HMAC values on existing records can be recomputed later using a separate utility application. This utility allows ADSS Trust Monitor to continue running at the same time while the utility performs its HMAC re-computation task in background. It also allows HMAC re-computation to take place overnight.

To re-compute HMAC values separately, follow these steps:

1. Login to the ADSS Trust Monitor console.
2. Navigate to Global Settings > System Security page.
3. Generate OTP by clicking the **Generate OTP** button.
4. Open command prompt/ terminal.
5. Navigate to ADSS Trust Monitor installation directory using command:

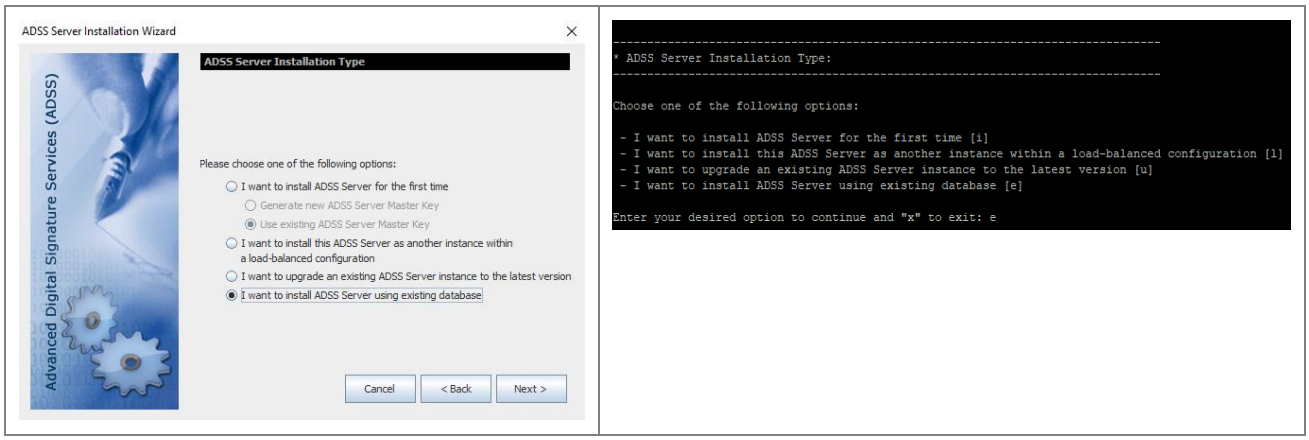
   `cd [ADSS-Server-Home]\setup\`
6. Then type following command to launch HMAC re-compute utility.

   `bin\compute_hmac.bat`
7. Provide OTP that you generated in step 3 to complete the HMAC re-computation process.

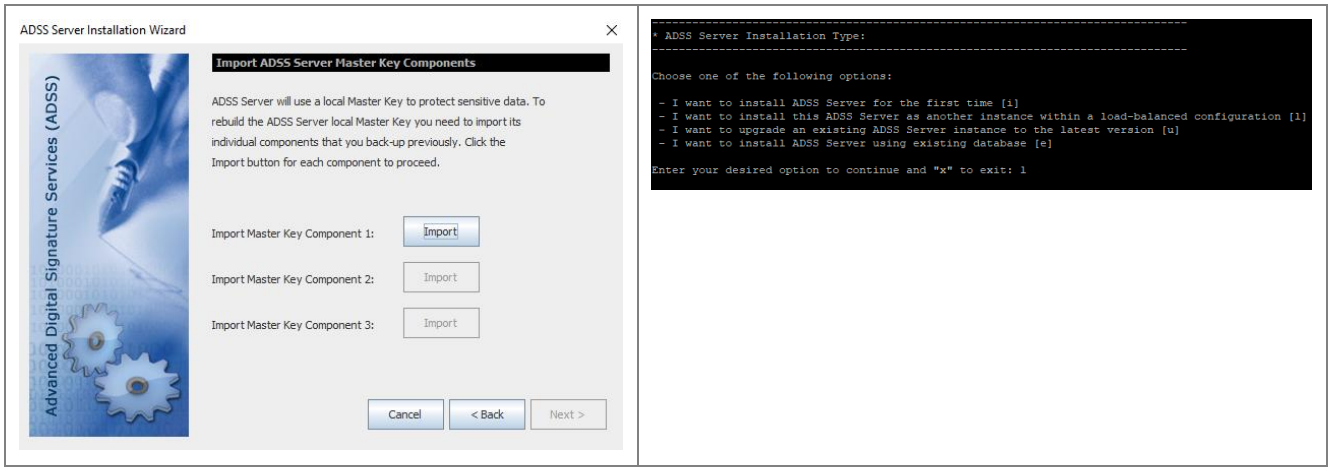
The utility will now re-compute the HMACs for all database records.

4.1.4 Installing ADSS Trust Monitor Using an Existing Database

Select option **I want to install ADSS Trust Monitor using existing database** on ADSS Trust Monitor Installation Type screen:

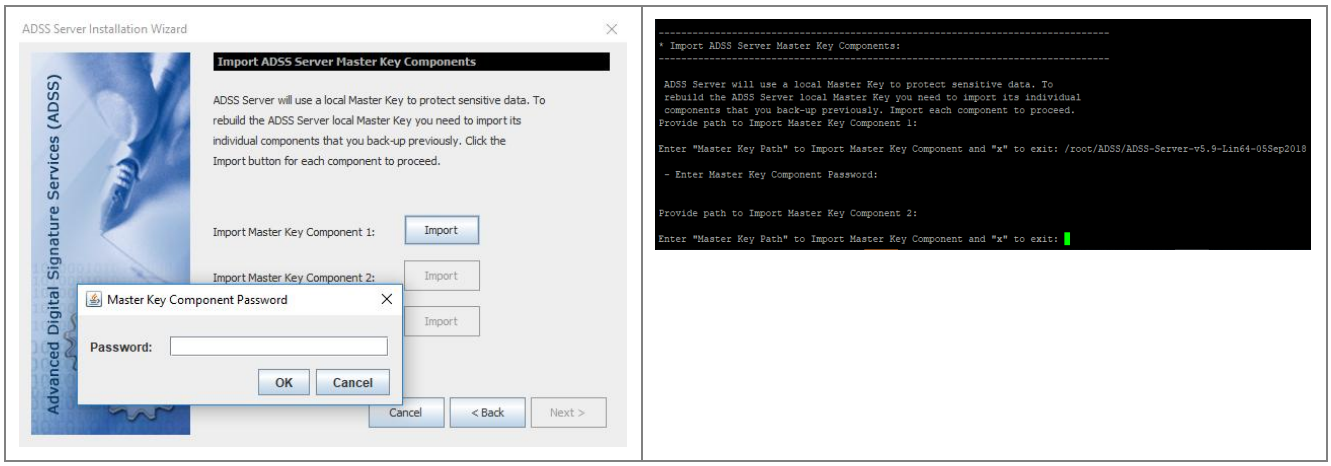


Click Next, then following screen will be shown:

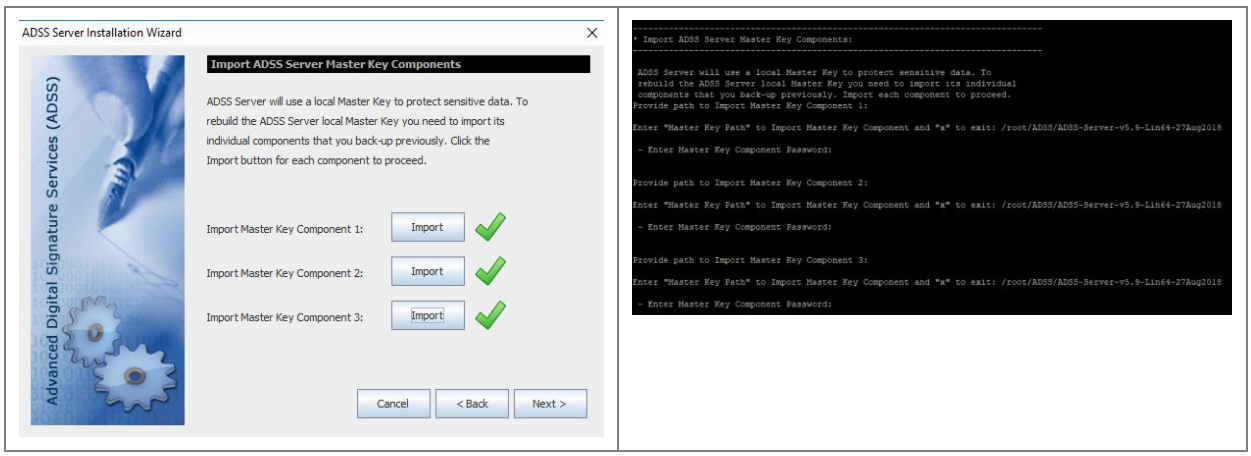


Use the **Import** button one by one to restore the backup of each Master key component (generated during the existing ADSS Trust Monitor installation) so that installer will restore the Master Key, installer will prompt to provide a password for each Master Key component and decrypt it with the provided password.

The Master Key backup should be imported in the same sequence and passwords when it was backup during first installation.



The following screen of Import Backup keys will appear:



Once done, proceed through ADSS Trust Monitor Installation wizard as before. On the **Typical DB Configurations** or **Advanced DB Configurations** screen, provide the details for the existing ADSS Trust Monitor database and continue through the Installation wizard as before.

ADSS Trust Monitor contains a sophisticated Export and Import feature within its Global Settings module. This allows all or selected records to be exported and imported to a new system.

This can be a valuable way of copying ADSS Trust Monitor configuration data from a pre-production system to a production system.

Import & Export MUST only be performed between the same versions of ADSS Trust Monitor.

4.2 Launching ADSS Trust Monitor Admin Console

To access ADSS Trust Monitor Admin Console, open a web browser (where you imported the Administrator PFX above) and type the following URL:

https://{Machine-Name}:8774/adss/console

Where machine-name is one of:

- localhost (in a case when ADSS Trust Monitor is accessed on the local system where it is deployed)
- A local network system name (e.g. adss-server-machine1)
- An IP address
- A URL (e.g. globaltrustfinder.com)

Initially you will be presented with a default TLS client authentication certificate that is pre-configured in ADSS Trust Monitor. It is recommended that you change the default TLS client authentication certificate by creating/importing a new certificate from ADSS Trust Monitor Admin Console after login. Click here for more information. Note you can also use certificates issued by third parties.

Initially you will be presented with a temporary TLS server authentication certificate that is pre-configured in ADSS Trust Monitor. This is the default administrator certificate. You should change it by creating a new certificate using the ADSS Trust Monitor admin console. Refer to the ADSS Trust Monitor Admin Guide for more details. Ascertia recommends creating at least two operators.

A popup dialog may be shown; listing TLS client authentication certificates installed in the browser (including the one installed during ADSS Trust Monitor installation) and asking you to choose appropriate certificate. Choose the certificate with a common name of “ADSS Default Admin” to login the ADSS Trust Monitor Console.

Before launching the admin console, make sure that you have installed/imported adss_default_admin.pfx from [ADSS-Server-Home]/setup/certs/ directory in your web browser.

4.3 Uninstalling ADSS Trust Monitor

To start the uninstallation, navigate to **[ADSS-Server-Home]/setup** directory. Either using a command line or Windows GUI interface.

Windows

To uninstall ADSS Trust Monitor on Windows platform, go to **[ADSS-Server-Home]/setup** directory and run **uninstall.bat** file as administrator. This process will stop and then delete the registered ADSS Trust Monitor components from Windows Service Panel.

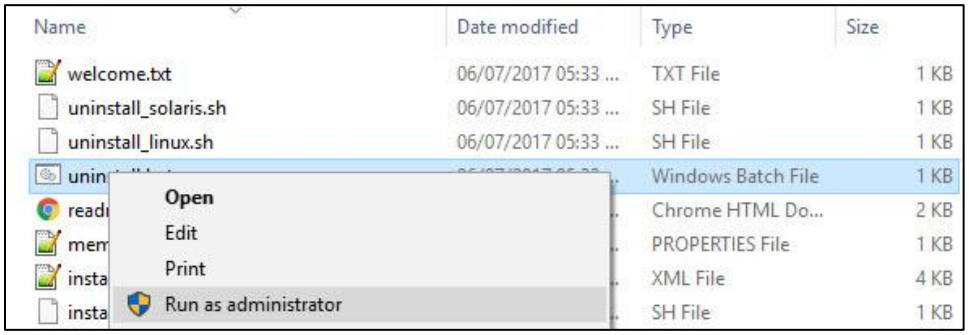


Figure 6 - Windows Example Uninstall Run as administrator

UNIX

To uninstall ADSS Trust Monitor on a UNIX platform, go to **[ADSS-Server-Home]/setup** and run **`sh uninstall_linux.sh or uninstall_solaris.sh`** command accordingly under root user to delete registered ADSS Trust Monitor components from /etc/init.d/.

Use the following command to mark uninstall.sh file as executable before launching:

```
# sh chmod +x uninstall_linux.sh
            Or
# sh chmod +x uninstall_solaris.sh
```

The following command will run the uninstaller:

```
# sh uninstall_linux.sh
          Or
# sh uninstall_solaris.sh
```

On both Windows and UNIX platforms the uninstall procedure will not delete the directory structure and contents of ADSS Trust Monitor, nor remove the database and its contents.

It is very important to securely delete any HSM held keys if the system is uninstalled because of a decommissioning exercise. This is not within the scope of ADSS Trust Monitor and the relevant manufacturer will provide the necessary instructions to achieve this.

4.4 ADSS Trust Monitor Service Interface URLs

Once ADSS Trust Monitor is installed you can use ADSS Trust Monitor service interfaces to process requests from your business applications. Interface URLs are documented in each service's **Interface URLs** page in Admin Guide. Each service has a unique URL and there are also variants for each depending upon which protocol the client wishes to use. For example, OASIS DSS or Ascertia XML based HTTP protocol for signature operations.

4.5 Troubleshooting

If any of the ADSS Trust Monitor Core, Console or Service components fail to start after installation or there is a failure during installation wizard then ensure the following:

- Allow 1150 connections on your database server to allow ADSS Trust Monitor to function at the recommended capacity. Note the connection pooling ensures these are maximum values and will not be created unless capacity demands it.
- The appropriate ADSS Trust Monitor package for Windows/UNIX was chosen to install on the relevant machine.
- There should be no space character anywhere in the ADSS Trust Monitor installation directory path.
- ADSS Trust Monitor should be installed with administrator/root user privileges.
- In case of Windows platform check the following services are found in Windows Services Panel.
    - Ascertia-ADSS-Core
    - Ascertia-ADSS-Console
    - Ascertia-ADSS-Service
- In case of UNIX platform check that following service daemons are found within /etc/init.d/
    - tomcatd-ADSS-core
    - tomcatd-ADSS-console
    - tomcatd-ADSS-service
- If ADSS Trust Monitor does not start automatically after installation, then manually start ADSS Trust Monitor;

  start following services from Windows Services Panel on Windows OS:
    - Ascertia-ADSS-Core
    - Ascertia-ADSS-Console
    - Ascertia-ADSS-Service

  On UNIX, use these commands to start the services:
    - /etc/init.d/tomcatd-ADSS-core restart
    - /etc/init.d/tomcatd-ADSS-console restart
    - /etc/init.d/tomcatd-ADSS-service restart
- If a certificate is not shown, then it is because of one of the following reasons:
    - The browser settings are such that the certificate is automatically selected.
    - There was a problem importing TLS client authentication certificate in to the browser.

Detailed information about known database, service, and console etc. issues can be found here:

http://manuals.ascertia.com/ADSS-Admin-Guide/troubleshooting.html

If Technical Support is required, Ascertia has a dedicated support team providing debugging, integration assistance and general customer support. Ascertia Support can be accessed as described in Chapter 1.

The installation procedure produces a log file called install.log, which is located in **[ADSS-Server-Home]/setup** directory. Any errors during installation will be recorded in this file.

Finally, consult the logs directory as each service produces its own unique log file.

5 Post-Installation Notes

Review this check list after the successful installation of ADSS Trust Monitor.

5.1 Secure Deployment of ADSS Trust Monitor

Make ADSS Trust Monitor deployment secured by following these guide lines:

- Mark the value of property **INVALIDATE_SSL_ON_LOGOUT = TRUE** under Global Settings > Advanced Settings > Console
- Set the lower value of **Console Session Timeout** configured in Global Settings > Miscellaneous
- Configure strong ciphers in the server.xml file for both Console and Service instances. For detailed instructions on updating cipher settings, refer to the technical note titled ***'Changing the SSL/TLS cipher suites used by the ADSS Server for advanced security and improved TLS ranking with SSL Labs'*** in the Ascertia Community Portal knowledge base.

5.2 ADSS Trust Monitor Operators

Each operator should be assigned their own unique certificate as detailed here:

Adding an Operator to ADSS Server (ascertia.com)

Once created their appropriate role and privileges assigned as described above.

Note ADSS Trust Monitor supports third party hardware such as USB Dongles to hold operator credentials. This is encouraged where security is paramount.

If required ADSS Trust Monitor has an Approval Manager module that ensures only Security Officers can approve operations for ADSS Trust Monitor administration.

5.3 HSM Configuration

ADSS Trust Monitor requires HSM partition passphrase if relevant (note the partition/slots will be found automatically by the Crypto Manager of ADSS Trust Monitor and Azure Key Vault does not require a passphrase but does require an Azure Key Vault account). Ensure, if relevant, that the ADSS Trust Monitor host has the correct HSM set-up and configuration, and communication is established between the two entities.

The HSM is configured via the **Key Manager>Crypto Source** menu. Ascertia provide configuration instructions for Thales SafeNet and nCipher nShield in Appendix section at the end of this document.

5.4 Local CA Configuration

When configuring a Local CA ensure:

- The complete certificate information of CA and end entity certificates is entered, and subsequently validated. For example, CDP, and AIA information that will be added to end entity certificates must be accessible by relying parties. Revocation information must be available to external parties that may rely on the information.
- If publishing to LDAP, then suitable user credentials and connection configuration information is required to publish certificates to the directory.

5.5 External Trust Services

If external OCSP, CRLs, and timestamp services are required then make sure that they are available to ADSS Trust Monitor. A test utility is provided for each service when configuring the respective element to ensure connectivity and possibly authentication is successful.

It is important to check that the appropriate CRL monitoring is functioning correctly if relying on third party CAs. Without a functioning CRL (based upon polling) retrieval ADSS Trust Monitor will not be able to successfully validate certificates.

For external CAs the appropriate account information is required. Each respective Managed PKI service provides different account details to allow certificate requests from ADSS Trust Monitor.

5.6 NTP Configuration

If using the TSA service of ADSS Trust Monitor, then Ascertia recommend a suitable time source is configured and the local system clock is not used. ADSS Trust Monitor allows configuration of multiple NTP time sources. The NTP client can maintain a check on the accuracy of the information provided and shut down the service if outside a validity window.

5.7 Database Log Archiving Frequency

Configure the archiving configuration settings for log files. This entails the period of archiving, and associated settings. Note each ADSS Trust Monitor service has the option to configure archiving individually.

Archive settings are dependent upon usage. For high volumes Ascertia recommends an archiving schedule of 30 days maximum. However, this number may well have to be less.

5.8 Alert Configurations

Configure the alert configuration settings required. This means the method (note ADSS Trust Monitor supports email, SMS, and SNMP) and which administrators should receive notifications for which services.

5.9 Licensing

For a production installation, ensure you are using a non-evaluation license of ADSS Trust Monitor.

5.10 Prepare the Backup Strategy

Prepare a disk and database backup procedure to ensure the full service can be restored in the event of failure with the least amount of disruption. ADSS Trust Monitor is not responsible for backing up its own database. The IT team must implement operate the backup using appropriate database vendor or third party tools. ADSS Trust Monitor provides an admin interface option that allows all the configuration settings to be exported as discussed here:

Import/Export Settings (ascertia.com)

Once the system is configured it is recommended that all settings are exported. This is also the recommended way of moving a proven configuration from pre-production to production.

5.11 Trace Log Sizing Guide

ADSS Trust Monitor produces low level information and debug logs on the hard disk. Retention period of these logs can be decided based on your needs. Detailed information about the trace logs and its sizing can be found here:

- Trace Logs (ascertia.com)
- Managing ADSS Server Logs (ascertia.com)

5.12 ADSS Trust Monitor Clients

Once ADSS Trust Monitor is deployed the appropriate clients must be given access to the system and required services. This means configuring their authentication and authorisation details in ADSS Trust Monitor. The Client Manager module allows you to do this. When creating clients Ascertia recommends that the least privilege approach is used and clients configured to allow access to the minimum required services, and in the case of Signing Service, appropriate keys.

Appendix A - Configuring ADSS Trust Monitor to use an HSM

ADSS Trust Monitor will create a connection pool of threads when using PKCS#11 implementation. This applies to HSMs where the underlying PKCS#11 module is configured for use. This does not apply to Azure Key Vault that uses REST architecture API and OAuth 2.0 for access control and authorization.

Follow these steps to configure ADSS Trust Monitor for HSM use:

- Open ADSS Trust Monitor administration console and authenticate.
- Go to **Key Manager > Crypto Source** module from ADSS Trust Monitor Console.
- Complete the form accordingly as described in the following Links:
  - PKCS#11 Standard
  - Utimaco CryptoServer CP5 HSM

An HSM must have its driver installed and configured before using it with ADSS Trust Monitor. The configurations for some of the commonly used HSMs are discussed in the following sections.

After configuring the HSM driver in Key Manager, ADSS Trust Monitor must be restarted using Server Manager > Restart System (All Services + All Configurations) so that the running system is updated.

Appendix B - Using Utimaco CryptoServer Se-Series Gen2 CP5 (PCI/LAN)

This section explains configuring Utimaco CryptoServer Se-Series Gen2 CP5 HSM for use with the ADSS Trust Monitor running on Linux.

B.1 - Steps to configure a PCI based HSM

1) The PCI HSM comes with a manual in a Utimaco provided CD. Ensure you read this document i.e. Documentation\Operating Manuals\ **CryptoServer Se-Series Gen2 CP5 PCIe manual.pdf**. Some of the important points from the document is mentioned in this appendix.
2) The HSM CD doesn't come with a built in driver for Linux rather it has to be compile and installed. See the read me inside the Utimaco provided CD > Software/Linux/Driver. You will a need root user to compile and install.
3) Perform a functional test of the HSM, see Utimaco CryptoServer Se-Series Gen2 CP5 PCIe manual > 6.3.2.2 inside the Utimaco provided CD > Documentation\Operating Manuals
4) Install the Host Software for the CryptoServer CP5 see section 6.4.2
5) Check the Authenticity of the CryptoServer CP5 see 6.5

B.2 - Steps to configure a LAN based HSM

The PCI HSM comes with a manual in a CD, ensure you read this document i.e. Documentation\Operating Manuals\ **CryptoServerCP5_LAN_Operating_Manual.pdf**. Read this document to ensure the LAN HSM is properly installed and running

B.3 - Steps to be done for either PCI or LAN based HSM

Utimaco HSM allows admin accounts and Master Backup Keys to be stored on smart cards. If a smart card is to be then see Utimaco CryptoServer Se-Series Gen2 CP5 PCIe manual > 6.6, 6.8 on how to connect the PIN Pad. Similarly see CryptoServerCP5_LAN_Operating_Manual for LAN based HSM. For simplicity this guide works with existing ADMIN user (this comes as default with the HSM) or with users with password. When using password, ensure you use a strong password and not what is mentioned below.

For PCI based HSM on Linux: *In all of the commands below either use Dev=/dev/cs2.0 OR Dev=/dev/cs2 or depending upon your driver installation*

For LAN based HSM: *In all of the commands below either set the Dev=<PORT>@<HOST> which point to the port and host address where the LAN based HSM is running e.g. Dev=3001@127.0.0.1*

Throughout this documents we have used the device as Dev=/dev/cs2.0 so replace this accordingly.

1) Call GetState to check the status of the HSM:

```
./csadm Dev=/dev/cs2.0 GetState
```

2) Confirm that the HSM state is 'OPERATIONAL'. If this is not then see the CryptoServer Se-Series Gen2 CP5 Administration Manual > 8.5, 8.6 and 8.7. Call ListFirmWare and see the firmwares all loaded by running command:

```
./csadm Dev=/dev/cs2.0 ListFirmWare
```

Ensure these are all loaded - see CryptoServer Se-Series Gen2 CP5 Admin Manual > Appendix A. If firmwares are not loaded, then see CryptoServer Se-Series Gen2 CP5 Administration Manual > 7.8.4 `LoadPkg` on how to load firmware. The admin manual resides in the CD > Documentation\Administration Guides. Note that this command requires authentication with two or more users with the Administrator role and requires minimum permission 4 in the user group 6 (minimum authentication status 04000000). You can use the built in ADMIN user and also create a new user e.g.

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
AddUser=ADMIN3,02000000{CXI_GROUP=SLOT_0000},hmacpwd,pwd99999
```

The ADMIN.Key resides in Software\Linux\x86-64\Administration\key

3) Run the following command to ensure version of modules and versions are correct:

```
./csadm Dev=/dev/cs2.0 GetBootLog
```

```
./csadm Dev=/dev/cs2.0 Version
```

4) To ensure the communication between the machine and the HSM is secure an HSM Authentication Key must be exported and configured inside the machine. For this first export the HSM authentication key and then set in the CS_AUTH_KEYS variable via command shell. This step is important otherwise no command of csadm requiring authentication would run:

```
./csadm Dev=/dev/cs2.0 GetHSMAuthKey <DIR_PATH>/HsmAuthKey.key
```

```
CS_AUTH_KEYS=<DIR_PATH>/HsmAuthKey.key
```

```
export CS_AUTH_KEYS=<DIR_PATH>/HsmAuthKey.key
```

5) Create Master Backup Key (MBK) and import it

   a) Before the HSM can be used a Master Backup Key needs to be created. Ensure that you create one more user (note that one user ADMIN comes as default see CryptoServer Se-Series Gen2 CP5 Administration Manual > 7.5.3 for details). In addition to this existing user one more user is needed as the import command must be authenticated by at least two users with the Administrator role and permission 4 in the user group 6 (minimum authentication status required 04000000). Here we have used another user i.e. ADMIN3 which is authenticated with password.

   b) First create this user (slot 0 is used) e.g.

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
AddUser=ADMIN3,02000000{CXI_GROUP=SLOT_0000},hmacpwd,pWd99999
```

   c) Create the MBK:

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
Key=<DIR_PATH>/mbk1.key#pWd23456,<DIR_PATH>/mbk2.key#pWd12345
MBKGenerateKey=AES,32,2,2,MBK1KEY
```

   d) Import the MBK:

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
LogonPass=ADMIN3,pWd99999
Key=<DIR_PATH>/mbk1.key#pWd23456,<DIR_PATH>/mbk2.key#pWd12345
MBKImportKey=3
```

   e) Confirming import of MBK:

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
MBKListKeys
```

Ideally the MBK keys should be created inside smart cards for added security. See CryptoServer Se-Series Gen2 CP5 Administration Manual > 7.7.2 MBKGenerateKey

6) To confirm that the HSM is now running properly run this command and you should get no errors:

```
./csadm  Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
```

7) To ensure the communication between ADSS Trust Monitor and the HSM place the previously generated HsmAuthKey.key file inside:

<ADSS_SERVER_INSTALLATION_DIR>/conf/hsm/Utimaco

8) Similarly, to ensure that ADSS Trust Monitor could communicate with the HSM over PKCS#11 channel, a PKCS#11 configuration file must be set. This configuration file comes bundled with ADSS Trust Monitor and is present at:

<ADSS_SERVER_INSTALLATION_DIR>/conf/hsm/Utimaco/cs_pkcs11_R2.cfg

9) Ensure that you set the correct device address inside the cs_pkcs11_R2.cfg > CryptoServer section based on whether you are using a PCI or LAN based HSM.

B.4 - Setting up users for ADSS Trust Monitor

1) To ensure ADSS Trust Monitor can create user keys and use them to create signatures, few users need to be created. You can create these users inside any slot e.g. slot 0 (This same slot will be used inside ADSS Trust Monitor configuration as well). These users must be authenticated with a password based authentication:

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
AddUser=SO_0000,00000200{CXI_GROUP=SLOT_0000},hmacpwd,pWd12345
```

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
AddUser=USR_0000,00000022{CXI_GROUP=SLOT_0000},hmacpwd,pWd65997
```

2) The restore key function of Utimaco requires two logins on the slot hence we create another user and assign admin rights to it. This user is also configured inside ADSS Trust Monitor.

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key
AddUser=USR1_0000,00000022{CXI_GROUP=SLOT_0000},hmacpwd,pWd65432
```

3) Run this command to see the list of generated users:

```
./csadm Dev=/dev/cs2.0 ListUser
```

B.5 - Logging

In case of issues connecting with the HSM, you can either review the PKCS#11 log which is created as default in the temp folder with the name: cs_pkcs11_R2.log. You can also change the folder where the PKCS#11 logs are generated by setting the Logpath inside the cs_pkcs11_R2.cfg

Alternatively, you can also get more logs from the HSM. To get the audit log for debugging run this command:

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key GetAuditLog >
./auditlog.txt
```

As the HSM runs, it generates audit logs. CP5 creates 10 audit log files with a storage of maximum 240000 bytes. Note that the HSM does not support Log rotation which means administrator must export these logs at regular intervals to avoid HSM returning error. This could be done with a shell script which runs after some time interval to export the logs. See CryptoServer Se-Series Gen2 CP5 Administration Manual > 8.12.

In case you just need to clear the audit log you can run this command:

```
./csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<DIR_PATH>/ADMIN.key ClearAuditLog
```

Appendix C - Using a Thales SafeNet Luna SA HSM (PED)

This section explains how to configure a Luna SA HSM to use with ADSS Trust Monitor.

C.1 - Configuring the HSM

The following instructions assume that DNS is not being used and fixed IP addresses are. Follow these instructions to configure the Luna SA HSM.

1) Power on the HSM and connect the network cable, PED & console.
2) Open command prompt/ terminal
3) Run the following IP config command for non-DNS systems:

   ```
   net interface -static -device eth0 -ip 192.168.11.82 -netmask
   255.255.0.0 -gateway 192.168.1.1
   ```

   Substitute the right IP address, mask and gateway for your environment.
4) Restart the syslog and network services:

   ```
   service restart syslog
   service restart network
   ```

   Check the new IP address by pinging from the ADSS Trust Monitor system and enable NTP services if available
5) Generate an HSM certificate

   ```
   sysconf regenCert <hsm-ip-address>
   ```
6) Bind the NTLS service

   ```
   ntls bind none -bind <hsm-ip-address>
   ```
7) Initialise the HSM

   ```
   hsm init -label <hsmname>
   ```

   The LUNA PED will be required
8) Set HSM Policies if required (not explored here)
9) Login to the HSM

   ```
   hsm login
   ```

   The LUNA PED will be required
10) Create a Partition (a virtual token) on the HSM (e.g. ADSS)

    ```
    partition -create -name ADSS-Server
    ```

    The LUNA PED will be required & a partition PIN will be produced
11) Its recommended that you change the activation policy of this partition so that a PED based login is not required every time ADSS Trust Monitor starts a session with the HSM

    ```
    partition changePolicy -partition ADSS -policy 22 -value 1
    ```

    The LUNA PED will be required to confirm this
12) Optionally you may also wish to change the auto activation policy so that the HSM can be powered down and up briefly without requiring the PED. Use the same command as before specifying policy number 23.

C.2 - Install HSM Driver

1) Autorun the Thales SafeNet CD and the installer checks for existing Luna SA software and then presents the installation options:
   a) Luna SA Client, the main Luna SA software required by any computer that is to connect with a Luna SA HSM Server
   b) OPTIONAL Luna CSP, CAPI for Luna SA Clients
   c) OPTIONAL Luna JSP, Java Service Provider for Luna SA Clients
2) Select a) to install the Luna SA Client software

C.3 - Configure the Software Client & Register on HSM

Open a command window change directory to the Luna folder. Use the following commands to configure the client & HSM software:

1) Fetch the HSM Certificate

   `ctp admin@TFOCSP:server.pem .` (Note the final dot is important)

2) Register the HSM device on ADSS Trust Monitor host

   `vtl addServer –n <HSM-ip-address> -c server.pem`

3) Create a Client Certificate

   `vtl createCert –n <HSM-ip-address>`

4) Transfer the Client Certificate to the HSM

   `ctp cert\client\<HOST-ip-address>.pem admin@<HSM-ip-address>:`

   You will need to login to the HSM to complete this

5) Register the Client with the HSM on HSM console (logged in):

   `client register –c <HOST-ip-address> -h <HOST-ip-address>`

6) Assign the Client to a Partition and on HSM console (logged in):

   `client assign –client <HOST-ip-address> –partition ADSS-Server`

   Now confirm this operation:

   `client show –client <HOST-ip-address>`

   You will be shown information on this client

On the ADSS Trust Monitor system command prompt in the Luna area key in: **`vtl verify`**

You will be shown a slot number, a serial number and a partition name.

C.4 - Enabling ADSS Trust Monitor to see keys generated using the Thales SafeNet CSP driver

In some cases, keys and certificates may be generated using Thales SafeNet's Windows CSP, e.g. VeriSign certificates must be created this way. ADSS Trust Monitor cannot see such keys because by default the CSP marks the public key as 'private=true', which means "do not share this data". If you wish to allow ADSS Trust Monitor to see such keys within the HSM the setting must be changed.

The recommended way is to use the Thales SafeNet CKDemo application. Follow these steps:

1) Start CKDemo and open a session as a normal user (option 1)
2) Login as the crypto officer (option 3)
3) Find objects (26) and search for the public key of the RSA key pair in question (option 4)
4) Copy the public key (option 21) with the handle from step 3
5) Select add attribute and change CKR_PRIVATE from 01 (true) to 00(false)

Appendix D - Using a Thales SafeNet Luna PCI HSM (PWD)

The use of a Thales SafeNet Luna PCI HSM with password authentication (PWD_AUTH) and not PED based authentication is assumed in the following instructions. Appendix B lists the instructions for PED based HSMs. The Thales SafeNet Software CD has a good HTML based guide – click "START_HERE.html" to activate this. This description acts as a brief summary for Windows users; UNIX users should read the Thales SafeNet documentation for UNIX specific information.

D.1 - Installing HSM Hardware

The HSM should be inserted into a 32-bit or 64-bit PCI slot.

D.2 - Installing HSM Driver

1) Check the information here with the latest information provided by Thales SafeNet because HSM installation information and instructions may have been updated.
2) Install the Thales SafeNet supplied driver located on the CD under Win – run Setup.exe. Work through the installation wizard - it is recommended that you use the default Installation Directory.
3) You are given the option to install Luna CSP software (for use with Microsoft CSP) or Luna JSP software (for Java support) – these are not required.
4) A new folder is created: {drive}:\Program Files\LunaPCI with the cryptoki library, tools and ancillary files and \driver with the hardware driver installation files. The computer will require a restart.
5) Go to the {drive}:\Program Files\LunaPCI\driver directory and double-click "Setup_LunaPCIDriver.bat". A command-prompt window appears briefly and a new \LunaPCIdriver folder is created
6) Since the HSM was installed before the software, you need to tell Windows about the HSM driver – click on "Start > Settings > Control Panel > Add Hardware" dialog, and point to the installed Luna driver located at C:\Program Files\LunaPCIdriver...

D.3 - Configure the HSM Security Officer Account

To perform HSM operations, you must login as the Security Officer (SO). For a new Luna PCI module, the HSM Security Officer password is "default".

In this folder, C:\Program Files\LunaPCI click lunacm.exe to run the client manager.

Now initialise the HSM and assign a name and a security officer password.

```
lunacm:> hsm init -label choose_a_name -password choose_a_complex_password

You are about to initialize the HSM.

The User will be deleted and all data will be erased.

Are you sure you wish to continue?

Type 'proceed' to continue, or 'quit' to quit now -> proceed
```

Make sure to record the username and password and store them securely. Entering incorrect credentials three times will result in the HSM being zeroized, rendering it unusable. The password serves as the new Security Officer password and will be required for the login command.

D.4 - Configure an HSM Partition

Assuming you are still logged into the SO account, at the lunacm:> prompt, type:

```
lunacm:> partition create -password a_partition_password
```

The password should be a minimum of 8 characters.

See the Thales SafeNet documentation if you wish to show and/or set the partition policies or backup and restore the partition.

D.5 - Verifying Installation

1) Open a DOS window and run the Thales SafeNet multitoken2 utility with a test, e.g.

   ```
   Multitoken2 –mode multisignvalue –key 1024 –blob 10 –s 1
   ```

2) This will run signing performance tests on the HSM and present its results on screen.

D.6 - Notes for Solaris Users

1) Log on to the client system as root and open a console or terminal window.
2) Insert the CD (mount it if you do not have automount). Now change directory to the CD (/cdrom or whatever devicename your system uses) and the /solaris directory by typing:

   ```
   cd /cdrom/solaris
   ./install.sh
   ```

3) Follow the prompts (agree to the license agreement, agree to backup any existing Chrystoki.conf file, do not agree to 64-bit support, do not install the JSP.
4) By default, the Client programs are installed in the “/usr/lunapci” directory. You will need to run the LunaCM config manager application. The cryptoki library is found here: /usr/lib/libCryptoki2.

Appendix E - Using a nCipher nShield Connect HSM

This section explains configuring nCipher nShield Connect HSM for use with the ADSS Trust Monitor.

Before configuring the Connect HSM, install the nShield software on the ADSS Trust Monitor machine(s), normally to a subdirectory nfast (on Solaris this will normally be /opt/nfast). Administrator or root privileges are required for the installation

This is a quick guide that should be used in conjunction with the nShield Connect HSM Admin Guide detailed descriptions, which can be found in the nfast/document directory after the software installation.

Using the nShield front panel interface:

2) Network configuration
   a) Enter Connect HSM IP address, subnet mask (menu 1-1-1-1)
   b) Confirm reboot and reboot Connect HSM
   c) Enter default gateway (if required using menu 1-1-1-3)
3) Prepare (RFS) Remote File System on the ADSS Trust Monitor
   a) nfast/bin/anonkneti <HSM IP>. The Connect HSM will respond with an ESN and HASH to be used in the rfs setup command below.
   b) nfast/bin/rfs-setup –force <HSM IP> <HSM ESN> <HSM KNETI HASH>

      e.g. nfast/bin/rfs-setup –force xxx.xxx.xxx.xxx A285-4F5A-7500 2418ec85c86027eb2d5959fef35edc5e1b3b698f
4) Configure Connect HSM to locate the RFS (menu 1-1-3).
   a) Enter remote (ADSS Trust Monitor) IP address
   b) Leave port number as default 9004
5) Allow config file changes on RFS client to be pushed to Connect HSM (menu 1-1-6)
   a) Turn on auto push
   b) Set to RFS IP address
6) Configure log location (menu 1-1-7)
   a) Select Append to store on RFS and Connect HSM or
   b) Select Log to store only on the Connect HSM
7) Set time on Connect HSM (menu 1-1-8)
8) Create a new Security World (menu 3-2-1) and you will be prompted for an ACS (Administrator Card Set). Enter the quorum for the ACS:
   a) Number of cards required to perform an operation
   b) Total number of cards in set
9) Create the Operator Card Set (OCS). This/these provide access to the PKCS#11 key objects used by the ADSS Trust Monitor.
   a) Follow detail in the Admin Guide
   b) If required, choose to create a persistent card set so that the key objects can be accessed in the Connect HSM when the OCS is not present.

      Note: This is a customer defined requirement as there are limitations on the persistence of keys in the Connect HSM e.g. if the HSM is power cycled then the keys from the OCS will be lost.
   c) Provide a pass phrase for the smart card that is being initialised.

Note: This will be used to configure the HSM PIN on the ADSS Trust Monitor

10) Configure the Connect HSM to allow communication from the ADSS Trust Monitor client (menu 1-1-4-1)
    a) New client
    b) Enter remote client IP address
    c) Select client privileged on any port
    d) Unless you are using nTokens select No for nTokens
11) Prepare the ADSS Trust Monitor client to work with the Connect HSM:

    nfast/bin/nethsmenroll -p <HSM IP> <HSM ESN> <HSM KNETI HASH>

12) Enable TCP sockets for Java applications e.g. KeySafe (optional)

    nfast/bin/config-serverstartup -sp

13) Stop and start the "hardserver" nShield Windows Service or UNIX daemon to activate new settings:
    a) For Windows run: **net stop "nfast server"** followed by **net start "nfast server"**
    b) For UNIX run: **nfast/sbin/init.d-nfast stop** followed by **nfast/sbin/init.d-nfast start**
14) Test the configuration using nfast/bin/enquiry which should get a response from the HSM of the form:

```
server:
enquiry reply flags none
enquiry reply level Four
serial number ####-####-####
mode operational
version #.#.#
speed index ###
rec. queue ##..##
...
module #1:
(a)   ...
mode operational
version #.#.#
...
connection status OK
```

Appendix F - Using a Thales SafeNet PSG HSM

The Java Environment installation package is no longer included on the CD's provided. You now need to download the JRE package from the Oracle Java website.

For ProtectServer External HSMs the process is slightly different and a different provider is required

1) For a networked HSM, first install the HSM Access Provider Software "ETnethsm" located on the CD under: "<Operating System>\NET_HSM_Access_Provider". The IP address of the HSM will be prompted for.
2) Install the SafeNetProtectToolkit C runtime "ETcprt.exe" located on the CD under <Operating System>\PTKC_Runtime
3) Install the SafeNetProtect Toolkit SDK "etcpsdk.msi" located on the CD under <Operating System>\ptkc_sdk
4) You will be asked to update the PATH variable – say yes and select HSM and then afterwards check that the PATH system environment variable shows a path to the cryptoki.dll usually located here: C:\Program Files\SafeNet\ProtectToolkit C SDK\bin\hsm
5) Use the supplied gTCAdmin and Key Management Utility (KMU)
6) Use gTCAdmin to initialise the HSM and configure a Security Officer
7) Now create a token slot and access password - this password must be provided to ADSS Trust Monitor later on
8) Use the Start > run programs> SafeNet> PKTC runtime > gCTAdmin to set security officer and user passwords for the HSM
9) Use the Start > run programs> SafeNet> PKTC runtime > KMU to manage slots and keys within the HSM
10) Set the HSM into FIPS mode by issuing the command CTCONF –fF
11) Now verify the HSM is configured:

    Open a DOS window and type "ctkmu l" (L for LIMA) this responds with a listing of all the available slots on HSM.

    "CTCONF -v" is another Thales SafeNet utility that shows the configuration of the HSM.

F.1 - Enabling ADSS Trust Monitor to see keys generated using Thales SafeNet CSP driver

In some cases, keys and certificates may be generated using Thales SafeNet's Windows CSP, e.g. VeriSign certificates must be created this way. ADSS Trust Monitor cannot see such keys because by default the CSP marks the public key as 'private=true', which means "do not share this data". If you wish to allow ADSS Trust Monitor to see such keys within the HSM the setting must be changed.

The recommended way is to use Thales SafeNet's CKDemo application. Follow these steps:

1) Start CKDemo and open a session as a normal user (option 1)
2) Login as the crypto officer (option 3)
3) Find objects (26) and search for the public key of the RSA key pair in question (option 4)
4) Copy the public key (option 21) with the handle from step 3
5) Select add attribute and change CKR_PRIVATE from 01 (true) to 00(false)

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