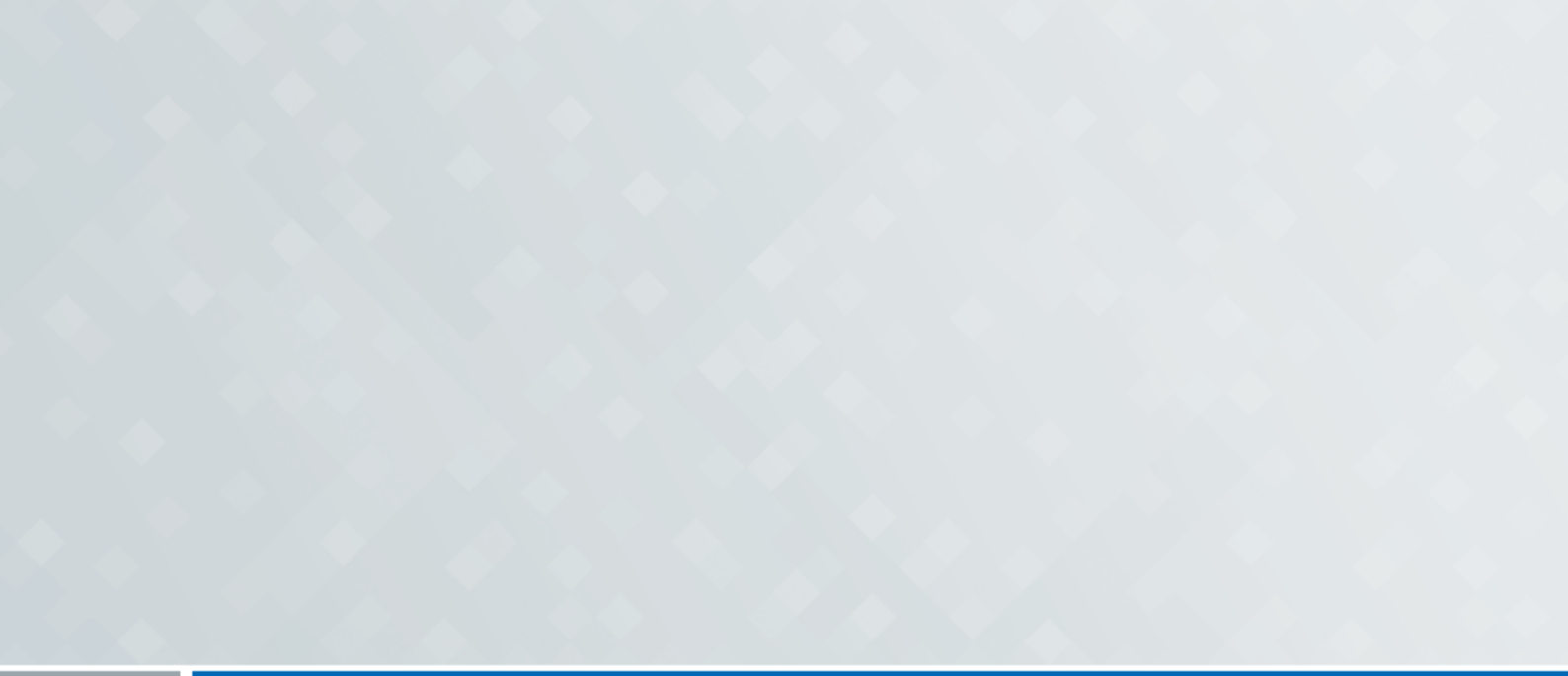




Entrust

Authority Security Manager (PKI)

10.0

Integration Guide

CryptoServer HSM

SecurityServer 4.31.1 and 4.45.5



Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-07-28
Status	PUBLISHED
Document No.	IG-2026-0085
All rights reserved	No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems. Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1	Introduction	4
1.1	About this Guide	4
1.2	Target Audience for this Guide	4
1.3	Document Conventions	4
1.4	Abbreviations	5
2	Overview	8
3	Prerequisites and Requirements	9
3.1	Software Requirements	9
3.2	Hardware Requirements	9
4	Installing the Security Manager	11
4.1	Preparing to install the Security Manager	11
4.2	Installing Security Manager PostgreSQL Database on Windows	11
4.3	Installing the Security Manager on Windows	16
5	Configuring PKCS#11	18
5.1	Introduction and Prerequisites	18
5.2	Installing PKCS#11 on the Workstation	18
5.3	Generating an MBK	19
5.4	Importing the MBK	20
5.5	Initializing PKCS#11 on the HSM	20
6	Configuring the Security Manager on Windows	23
7	Backup and Restore	48
7.1	Backing up and Restoring Key Database	48
7.2	Backing up and Restoring a Key Database with P11CAT	49
8	FIPS Requirements	50
9	Further Information	51
10	References	52
11	Contact and Support Information	53

1 Introduction

Thank you for purchasing our CryptoServer security system. We hope you are satisfied with our product. This paper provides an integration guide explaining how to integrate an Utimaco CryptoServer Hardware Security Module (HSM) with Entrust Authority Security Manager.

Please do not hesitate to contact us if you have any suggestions or comments.

1.1 About this Guide

This guide describes how to enable HSM integration with Entrust Authority Security Manager, including the Security Manager installation.

1.2 Target Audience for this Guide

This guide is intended for Security Manager administrators and HSM administrators.

1.3 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select Details and click on Properties button
Monospaced	Code that is given for explanation or as an example, file paths	<code>certreq.exe -new request.inf IISCertRequest.csr</code>
<i>Italic</i>	References and important terms	Operating system listed in Software Requirements

Table 1: Document conventions

We use special icons to highlight the most important notes and information.



Here you will find important safety information that should be followed.



Here you will find additional notes or supplementary information.



This message marks the result expected after the successful execution of an instruction.

1.4 Abbreviations

We use the following abbreviations in this guide:

Abbreviation	Meaning
HSM	Hardware Security Module
PKI	Public Key Infrastructure
TSP	Time-Stamp Protocol
LDAP	Lightweight Directory Access Protocol
CA	Certification Authority
CRL	Certificate Revocation List
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
PKCS	Public Key Cryptography Standards

Abbreviation	Meaning
NTFS	New Technology File System
DV	Document Verifier
CVCA	Country Verifying Certification Authority
CA DN	Certification Authority Distinguished Name
DN	Distinguished Name
RDN	Relative Distinguished Name
AD LDS	Active Directory Lightweight Directory Services
NIC	Network Interface Card
ASH	Administration Service Handler
XML	Extensible Markup Language
XAP	XML Administration Protocol
SSL	Secure Sockets Layer
CSCA	Country Signing Root Certificate Authority
CDP URL	CRL Distribution Point URL

Abbreviation	Meaning
AIA	Authority Information Access

Table 2: List of abbreviations

2 Overview

Entrust Authority Security Manager is a public key infrastructure (PKI) platform, which will help organizations easily manage their security infrastructure. This certification authority (CA) system allows organizations to easily manage digital keys and certificates that secure user and device identities.

If the security of the generated keys and certificates needs to be enhanced, the Entrust Authority Security Manager can be configured to use a Hardware Security Module (HSM). When the HSM module is enabled with Entrust Authority Security Manager, this strengthens the protection of keys and certificates.

CryptoServer is a hardware security module developed by Utimaco IS GmbH, i.e. it is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage, as well as store, cryptographic keys and data. It can be used as a universal, independent security component in heterogeneous computer systems.

3 Prerequisites and Requirements

Ensure that the system environment you will be using meets the following hardware and software requirements.

3.1 Software Requirements

Software	Software Requirements
Operating System	Windows Server® 2016, Standard or Datacenter Edition or later Note: Evaluation versions of Windows Server are not supported by Entrust Security Manager
Entrust Authority™	Security Manager 10.0
Java	Recommended Version 8
Database	PostgreSQL

Table 3: List of software requirements

3.2 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.31.1 CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.45.5

Hardware	Hardware Requirements
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.31.1 CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.45.5

Table 4: List of hardware requirements

4 Installing the Security Manager

4.1 Preparing to install the Security Manager

The section describes the steps and information needed for the new installation of a Security Manager. The overall installation process includes the following steps.

1. If needed, download the Security Manager documentation, especially the *Security manager Operations Guide* and *Security Manager Administration User Guide*.
2. Prepare for installation of a new Security Manager, which includes collecting the installation and configuration data required.
3. Make sure to disable any anti-virus software during the installation process.
4. Install one of the supported LDAP-compliant directories for storing Certification Authority (CA) certificates, certificate revocation lists (CRLs) and user information. The recommendation is that you create a directory before proceeding to the installation of the Security Manager.
5. Optionally, install the hardware security modules (HSMs). The Security Manager (requires 64-bit HSM drivers) supports storing of the keys on the PKCS#11 version 2 HSMs.
6. Install the PostgreSQL as the Security Manager database provided by Entrust, which stores information about the Certification Authority, the X.509 users and the EAC entities.
7. Install the Security Manager software. Note that before the installation, people with administrative roles (e.g.: Site Planner, Directory Administrator, Database Administrator, Master User and First Officer) should be selected. For more information about the Security Manager roles, see the Security Manager Administration User Guide.
8. Configure the Security Manager.
9. Optionally, customize the Security Manager files, in which you can configure some of the important settings.
10. Initialize the Security Manager. This step is mandatory before using the PKI system.

4.2 Installing Security Manager PostgreSQL Database on Windows

This section explains how to install an Entrust Authority Security Manager PostgreSQL Database on the supported operating systems. The Security Manager PostgreSQL Database is an Entrust-

supplied database of the Security Manager. It stores information about the Security Manager infrastructure, X.509 users and EAC entities.

To improve the security, reliability and performance, it is recommended that the Security Manager PostgreSQL Database is installed on a server that is separated from the server hosting your directory.



The drive file system, where the database will be installed, should be configured as an NTFS file system. Also, do not use remote software to install the database.



Example dialog boxes and file paths may differ from software version to software version.

When installing the Security Manager PostgreSQL Database, make sure to record all usernames and passwords that are used to install it (they will be needed, when installing the Security Manager software).

To install the Security Manager PostgreSQL Database on Microsoft Windows, follow the steps below.

1. Disable any anti-virus software to prevent any conflicts during the installation process.
2. Log in to Entrust TrustedCare with the credentials supplied by the Entrust sales representative.
3. Browse to the Security Manager 10.0 software downloads page. **PKI -> Authority -> Security Manager.**
4. Download the Security Manager PostgreSQL Database installer ZIP package: PostgreSQL 11.7 (64-bit) Full and Upgrade Installer - Windows.
5. Extract the installer ZIP package to a temporary location.
6. Navigate to the extracted folder.
7. Run the installer: `SM_PostgreSQL_11_7_Win_setup.exe`.
8. Log in to the Windows server that will host the Security Manager PostgreSQL Database and Security Manager.
 - If you are using Microsoft Active Directory Domain Services (AD DS), log in with a domain administrator account (the account must be a member of the Domain Admins group in the

Active Directory - the Entrust Configuration Wizard for the Microsoft Active Directory account) can be used.

- If you are using other directories, log in with a user account that is a member of the local administrator's group.

9. Close any open applications.

10. Run the installer to begin the Security Manager PostgreSQL Database installation.

11. The installer checks the operating system for the required software.

- a. A list of the required software that is not found will be displayed.
- b. Click on **Install** to install the required software.

12. The InstallShield Wizard appears. Click on **Next** to continue.

13. The **License Agreement** page appears.

- a. Read the license agreement carefully.
- b. If you accept all the terms of the license agreement, click on **Yes** to continue.

14. The **Choose Destination Location** page appears.

- a. Use the default installation folder or change it by clicking on the **Browse** button (do not select a mapped network drive).
- b. Click on **Next** to continue.

15. The **Select Drive for Database** page appears.

- a. Select the drive where you want to store the PostgreSQL data (requires at least 1.5 GB of free space).
- b. Click on **Next** to continue.

16. The **Database Write-ahead Log Drive** page appears.

- a. Select the drive, where the PostgreSQL Write Ahead Log (WAL) files will be stored (requires at least 1 GB of free space).
- b. Click on **Next** to continue.

17. The **Possible Data Security Issue** dialog box appears in case you choose to store the PostgreSQL WAL files and PostgreSQL data on the same drive. Click on **Yes** if you want to go back and change the information or click on **No** to proceed.

18. The **PostgreSQL Windows (R) Account Password** page appears. The installer will create a Windows user account for PostgreSQL called "easm_entrust_pg" that will own the Security Manager PostgreSQL database and database processes. See the figure below.



Figure 1 : PostgreSQL Windows (R) Account Password page

- a. Enter a strong password.



A strong password should contain at least 8 characters, at least one uppercase character, one lowercase character, one number and one non-alphanumeric character.

- b. Click on **Next** to continue.

19. Repeat the above process for users in the PostgreSQL called "easm_entrust" and "easm_entbackup".
20. The **Password for Database User** page appears. The installer will create a user in the PostgreSQL called "easm_entrust" that will own the Security Manager schema and data in the database.

- a. Enter a strong password.
 - b. Click on **Next** to continue.
21. The **Password for Database Backup User** page appears. The installer will create a user in the PostgreSQL called easm_entbackup that is required to back up and restore the Security Manager data.
 - a. Enter a strong password.
 - b. Click **Next** to continue
22. The **PostgreSQL Database Port** page appears. By default, the PostgreSQL uses port 5432 (otherwise use one between 1000 and 65535).
 - Click on **Next** to continue.
23. The **Check Setup Information** page appears. See the figure below.
 - a. Review the PostgreSQL install settings and go back if anything needs to be changed.
 - b. Record the locations of the PostgreSQL data directory and PostgreSQL WAL files directory (by default `C:\easm_entrust_pg_data_11` and `C:\easm_entrust_pg_wal_11`). If anti-virus software is installed, these directories ought to be excluded from the antivirus scans.
 - c. Click on **Next** to install PostgreSQL.



Find the log file `postgres-11.7-install.log` in `C:\Users\<user>\AppData\Local\Temp` to investigate any errors that might encountered during installation.

24. The **Setup Status** page with progress bar appears. After PostgreSQL is installed, the InstallShield Wizard Complete page appears.

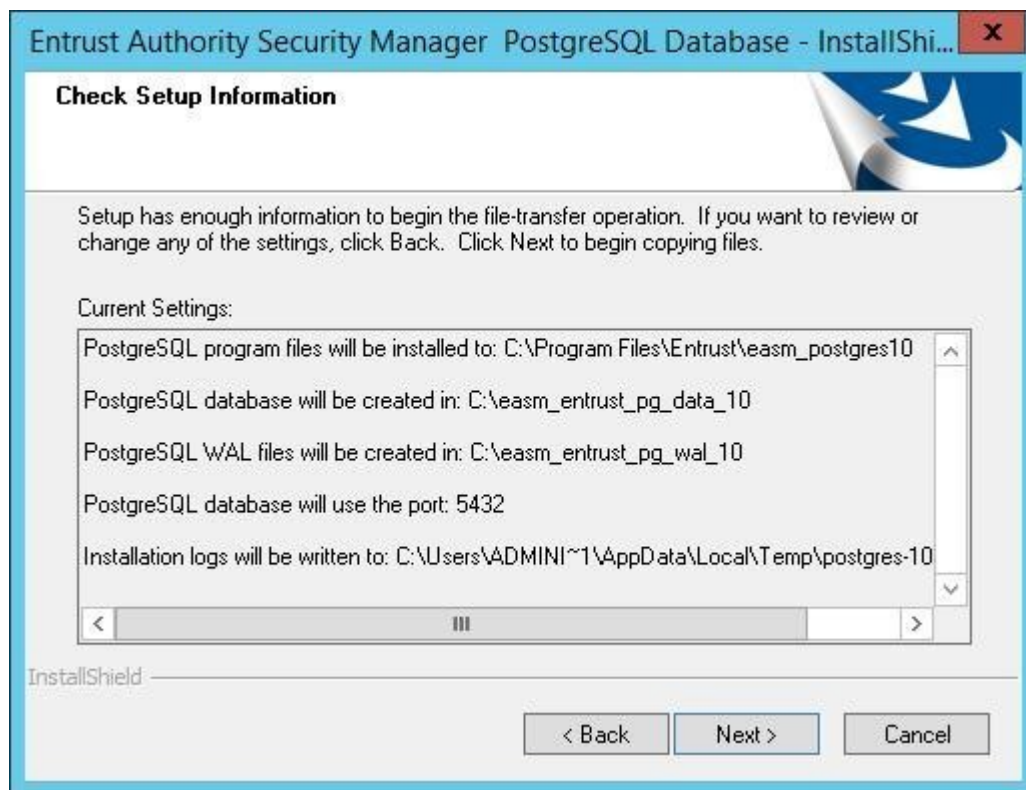


Figure 2 : The Check Setup Information page

25. Click Finish.

4.3 Installing the Security Manager on Windows

The section describes steps for installing the Security Manager on the Windows operating system. Successful installation needs a drive with a file system that is configured as NTFS (New Technology File System). To avoid errors and security issues also avoid using remote software, such as Telnet.

Steps to install Security Manager on Windows are as follows.

1. Log in to Entrust TrustedCare with the credentials supplied by the Entrust sales representative.
2. Go to the Security Manager 10.0 software downloads page.
3. Download the Security manager installer `SM_10_Win_Setup.exe`.
4. Log in to the Windows server hosting the PostgreSQL with the same user account that was used to install PostgreSQL.

5. Close any open applications.
6. Run the installer. This will open the InstallShield Wizard.
7. Click on **Next** to continue. This will open the **License Agreement** page.
8. Read the Security Manager license agreement carefully. Click on **Yes** if you accept all the terms of the license agreement. Otherwise, click on **No**. Clicking on **Yes** will open the **Choose Destination Location** window.
9. By default, the Security Manager is installed in the following folder: `C:\Program Files\Entrust\Security Manager\10.0.0`. Click on **Browse** to change the folder. The pathname supports only ASCII characters.
10. Click on **Next** to install the Security Manager, which will open the **Setup Status** page. If the Security Manager was installed successfully, the **InstallShield Wizard Complete** page will appear.



Before using the **Security Manager**, you can install a patch for unconfigured and uninitialized **Security Manager**. Do not run the **Security Manager Configuration** if you want to patch it. Otherwise, take a note that you should configure the **Security Manager**, before you can use it. In case you are using Microsoft Windows Server 2016 or later, deselect the **Run Security Manager Configuration** option, because you need to run it as an administrator to prevent file copy operation errors. If you selected **Run Security Manager Configuration**, the **Entrust Authority Security Manager** wizard appears.

11. Click on **Finish**. The Security Manager was successfully installed.

For more information on this topic, please, refer to [SMII], [SMOI], and [SMDI].

5 Configuring PKCS#11

5.1 Introduction and Prerequisites

Before the PKCS#11 interface and library can be used, some manual actions must be performed. Follow the steps below to configure the PKCS#11 library and initialize a PKCS#11 slot. For further information about the PKCS#11 setup, please refer to [CSPKCSDBG].



Please ensure you have selected the correct Utimaco SecurityServer PKCS#11 Provider.

Versions of SecurityServer prior to 4.40: PKCS#11 R2

Versions of SecurityServer from 4.40: PKCS#11 R3

For the most part, the use/config and structures are the same, however the file names differ with either R2 or R3.

5.2 Installing PKCS#11 on the Workstation

The installation file for the PKCS#11 is located on the Product CD. The installer creates an environment variable called `CS_PKCS11_R2_CFG` or `CS_PKCS11_R3_CFG`, depending on target version. It will contain the path to Utimaco's PKCS#11 configuration file. This file must be created or copied into place and edited.

We must set the `CS_PKCS11_R<vers>_CFG` environment variable to point to this location. To be able to access the HSM via PKCS#11, the configuration file needs to be modified.

1. Set the path to the logfile and set the desired log level.

```
[Global] # For unix: #Logpath = /tmp # For windows:  
Logpath = C:/ProgramData/Utimaco/PKCS11_R<vers>  
# LogLevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE) Logging = 4
```

2. Set the IP address of the HSM.

```
[CryptoServer]
# Device specifier (here: CryptoServer is CSLAN with IP address 10.10.20.200)
Device = 288@10.10.20.200
```

3. Optionally, make additional modifications to the configuration file, such as setting up an external store as described in [CSPKCSM]. We suggest modifying the PKCS#11 config file to **KeepAlive** flag active.

```
[Global]

# Prevents expiring session after inactivity of 15 minutes

KeepAlive = true
```

5.3 Generating an MBK

One of the steps of the HSM initialization is generating a new MBK, which can be used for creating backups, for using an external storage and for synchronizing HSM clusters. The MBK for a cluster is an AES256 key.

It is required to generate an MBK for the HSM to become operational. All cryptographic operations and many other non-crypto operations are blocked, when the HSM contains no active MBK.

To generate an MBK:

1. Open the Crypto Administration Tool.
2. Achieve the permission level of at least **02000000**.
3. Click **Manage MBK** to access the **Remote Master Backup Key Management** window and select the **Generate** tab.
4. Type the name of the MBK in the **MBK Name** section.
5. Select the backup mode of the MBK shares as either **XOR** or **m out of n**.

- If m out of n was selected it is necessary to select the number of m (shares) and n (shares) by using the drop-down menus, set by default as 2 and 3.
6. In case this MBK also needs to be imported at the same time into the HSM, select the Automatic MBK Import option.
 7. Click **Generate**.
 8. Select whether the MBK shares should be saved on smartcards or as keyfiles by selecting either the Smartcard Token or the Keyfile Token option.
- If you chose to export the MBK shares on smartcards, follow the instructions on the smart card reader to export all of the m parts.

5.4 Importing the MBK

In case the MBK was not imported, when it was generated, or if you want to upload it to another HSM to create a cluster, you need to import it from the keyfiles or smartcards that carry its parts. The MBK was divided into multiple parts by using Shamir's Secret Sharing or XOR and can be restored by using the m out of n or XOR principle.

1. Make sure that at least m out of n smart cards/keyfiles are available.
2. Open the CryptoServer Administration Tool.
3. Achieve the permission level of at least **02000000**.
4. Click **Manage MBK** to access the **Remote Master Backup Key Management** window and select the **Import** tab.
5. Select the type of MBK that will be imported and the value m .
6. Click **Import**.
7. Select whether to save the MBK parts on smartcards or as keyfiles by selecting either Smartcard Token or Keyfile Token option.
8. Follow the instructions to import all the m parts.

5.5 Initializing PKCS#11 on the HSM

In addition to PKCS#11, the PKCS#11 graphical interface tool (P11CAT) and the PKCS#11 command line interface (p11tool2) are installed as well. This chapter shows how to use the

P11CAT to initialize the PKCS#11 Slot 0. There are 10 active PKCS#11 slots by default. The number of PKCS#11 slots can be modified in the PKCS#11 configuration file.

1. Make sure that the PKCS#11 configuration file contains the IP address of your HSM and that the HSM is running.
2. Open the P11CAT tool on your workstation. When opening the tool for the first time, the slots should be as shown in the figure below.

Slot List			
Slot ID	Token Init.	PIN Init.	Login Status
0000 0000			
0000 0001			
0000 0002			
0000 0003			
0000 0004			
0000 0005			
0000 0006			
0000 0007			
0000 0008			
0000 0009			

Figure 3 : PKCS#11 slots before initialization

3. Select the row **0000 0000** under the **Slot ID** on the top left-hand side in the **Slot List**.
4. Click on **Login/Logout**.
5. Click on **Login Generic**.
6. Login as a user with permission mask at least **20000000** (User Manager permission).
7. Click on **Slot Management**.
8. Create a Security Officer (SO) for Slot 0. Click on **Init Token**. Write the **Token Label**. Set the **SO PIN**. Confirm the **SO PIN**. Click on **Init Token**. Observe the changed **Token Init** status for the Slot 0.
9. Logout the ADMIN user. Click on **Login/Logout**. Click on **Logout All**.
10. Login as the SO. Click on **Login/Logout**. Click on **Login SO**. Enter the SO PIN. Click on **Login**.
11. Click on **Slot Management**.
12. Create the User for Slot 0. Select **Init PIN**. Enter the **Normal User PIN**. Confirm the **Normal User PIN**. Click on **Init PIN**. Observe the changed **PIN Init** status for the Slot 0.

13. Logout the SO. Click on **Login/Logout**. Click on **Logout All**.

The Slot 0 is now initialized. An application or a user can now connect to the PKCS#11 Slot 0 and create or store objects on the slot. Find further information on creating or deleting objects and users in [CSPKCSM] and [LPKCSHD].

6 Configuring the Security Manager on Windows

Before initialization of the Security Manager, it needs to be configured. Configuration provides data that allows the Security manager to connect with a directory and the Security Manager database. Certificate algorithms, lifetimes and other options for the Certification Authority (CA) can also be selected.



Configuring the Security Manager is available only once, so be careful during the following steps. Try not to make a mistake! While some of the settings can be changed by editing the `entmgr.ini` file it may be necessary to completely uninstall and then reinstall Security Manager.

The configuration data can be entered directly into the Security Manager wizard or specific files (`entconfig.ini` or `entrustdirectorysetup.ini`) can be changed.

To configure Security Manager on Windows, follow the next steps.

1. Log in to Windows (use the same user account that was used for installing the Security Manager).
2. Run the Security Manager configuration as an administrator.

On Windows Server 2016 go to **Start > Entrust Authority (TM) Security Manager**, then right-click on the **Security Manager Configuration** and select **Run as administrator** (this can prevent file copy operation errors).

- a. On the Windows Server 2012 R2, click on **Start** then click the down arrow to access the **Apps**. Right-click on the **Security Manager Configuration** and select **Run as administrator**. When listed by name or category, the **Security Manager Configuration** is listed under **Entrust**.
 - b. The **Entrust Authority (TM) Security Manager Configuration** dialog box appears.
3. Click **Next** to bring up the **Security Manager License Information** page.

Security Manager License Information

Enter the information that appears on your Security Manager license card. Proceed to the other pages if you purchased other licenses. Note that you can enter Web information later using Security Manager Administration.

CVCA for Foreign DVs | DV for Inspection Systems | CVCA for Domestic DVs

Enterprise | Web

Enterprise license information is required for Security Manager.

Serial number:

Enterprise user limit:

Enterprise licensing code:

Next > Cancel

Figure 4 : The Security Manager License Information page

4. Enter the Security Manager license information.

- Under the **Enterprise** tab, enter your **Enterprise license information**. These fields are mandatory.
- Enter the information under the **Web** tab if you purchased a Web license (you can configure it also by changing `entmgr.ini` file).
- To configure the Security manager as a CVCA, enter the license information into tabs **CVCA for Foreign DVs** and **CVCA for Domestic DVs** (for managing domestic or foreign Document Verifiers). Configuration changes are also available by configuring the `entmgr.ini` file.
- Enter your Document Verifier license information under the DV for Inspection Systems to configure the Security Manager as a Document Verifier (or change the `entmgr.ini` file).

5. Click on **Next** to continue. **Security Manager Data and Backup Locations** page will appear.



Figure 5 : The Security Manager Data and Backup Locations page

6. Choose where the Security Manager data and backup files should be stored.
 - a. In the Folder for Security Manager data files field, enter the path for the Security Manager data files (by default it is `C:\authdata`). The drive should use an NTFS file system.
 - b. In the Folder for Security Manager backup files field, enter the path for the Security Manager backup files (by default it is `C:\entbackup`). The drive should use an NTFS file system.
 - c. Click **Next** to continue to **The Directory Node and Port** page.
 - d. If you are using Microsoft Active Directory, proceed to Step 7. If you are using Active Directory Lightweight Directory Services (AD LDS), proceed to Step 8. If you are using an LDAP directory, proceed to Step 9.
7. To configure the Security Manager for Active Directory:
 - a. Select Microsoft Active Directory, see the figure below.

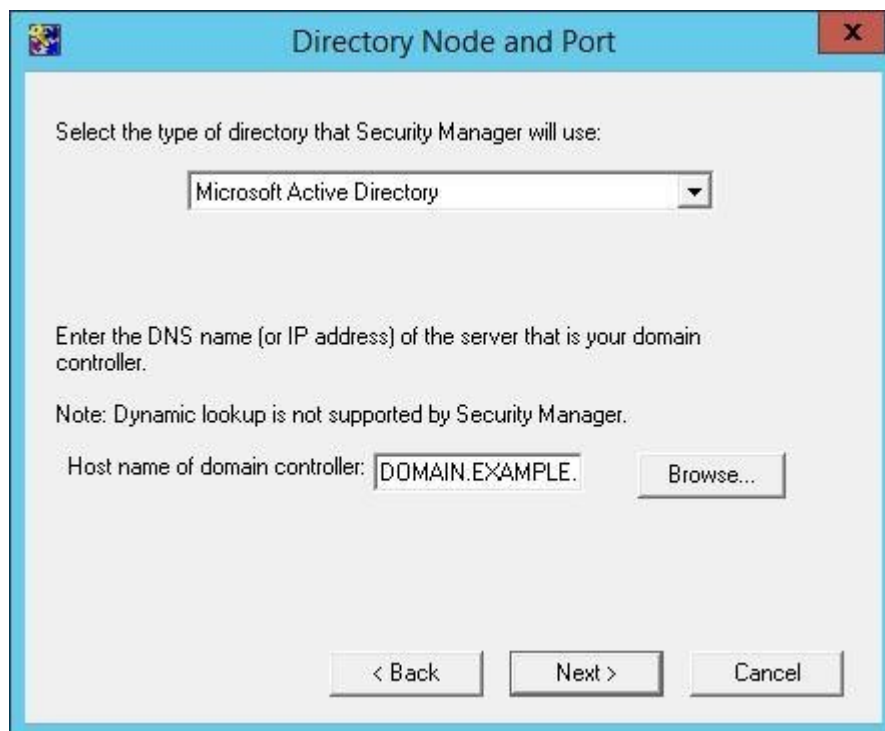


Figure 6 : Choosing Microsoft Active Directory as the type of directory

- b. In the Host name of domain controller field, enter the DNS node name or IP address of the server hosting Microsoft Active Directory.
- c. Click Next to continue, which opens the **CA Name** page.
- d. If a CA entry was created in the Active Directory by using the Entrust Configuration Wizard for Microsoft Active Directory, enter the common name of the CA entry in the CA common name field. By default, the Security Manager configuration program uses the name of the currently logged-in user to determine the relative distinguished name (RDN) value of the CA entry in the AIA container. For example:
`cn=CA,cn=AIA,cn=Public Key Services,cn=Services,cn=Configuratio
n,dc=Company One,dc=com`
- If the CA entry was created manually outside of the AIA container, select **Edit CA DN** and then enter the distinguished name of the CA entry you created.
- e. Click on **Next** to continue. Confirm the distinguished name of the CA if the CA DN is correct.
- f. Click on **Yes**, if the DN of the CA entry is correct. Otherwise, click on **No**.
- g. Proceed to Step 10.

8. To configure the Security Manager for Active Directory Lightweight Directory Services (AD LDS), follow the steps.
 - a. In the drop-down list, select Microsoft AD LDS.
 - b. In the Directory node name field, enter the DNS node name or an IP address of the server hosting the AD LDS.
 - c. In the Directory listen to port field, enter the port that AD LDS listens to for requests.
 - d. Click **Next**, which will open the **CA Distinguished Name and Password** page. See the figure below.

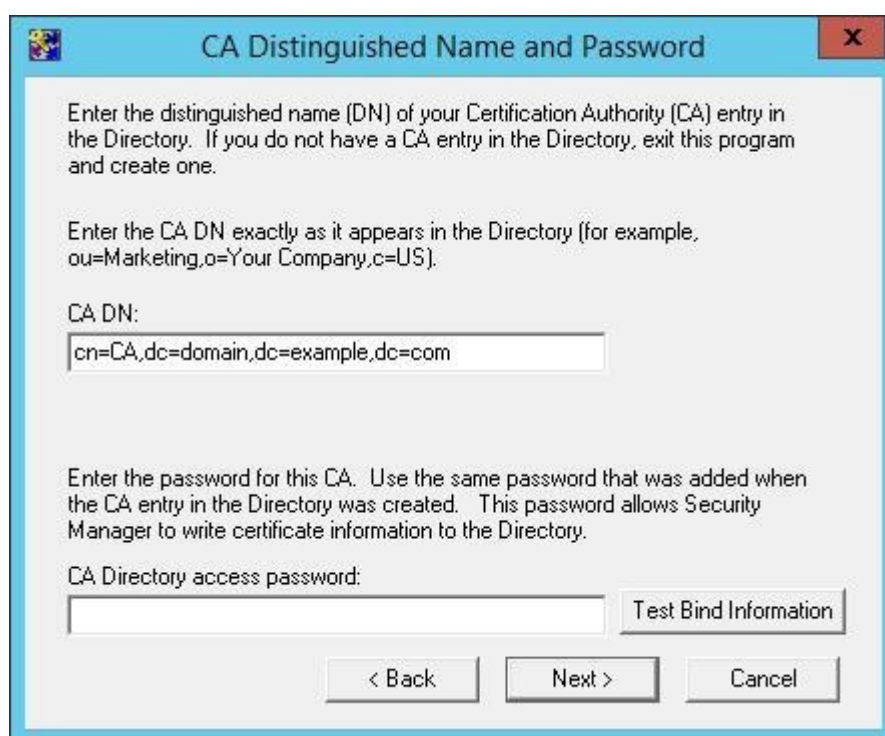


Figure 7 : The CA Distinguished Name and Password page

- e. In the CA DN field, enter the distinguished name (DN) of the CA entry.
- f. In the CA Directory access password field, enter the password for the CA entry.
- Click **Test Bind Information** to determine if the CA DN and password are correct. The configuration tool attempts to connect to the CA with the information provided. Correct the information if necessary.
- g. Click on **Next** to continue. The **Directory Administrator Distinguished Name and Password** page will appear, see Figure 8.

- h. In the Directory Administrator DN field, enter the distinguished name (DN) of a user with directory administration privileges. This entry will be used to connect to the directory to add, modify and delete directory entries.
- i. In the Directory access password field, enter the password of the Directory Administrator.
- j. Click on **Test Bind Information** to determine if the Directory Administrator DN and password are correct. The configuration tool attempts to connect to the Directory Administrator with the information provided. Correct the information in the fields if necessary.
- k. Click on **Next** to continue.
- l. Proceed to Step 10.

Directory Administrator Distinguished Name and Pass...

To perform tasks such as adding, deleting, and modifying entries in the Directory, Security Manager Administration needs to bind to the Directory with the credentials of a user with Directory administrative privileges. Enter the distinguished name (DN) of a user with Directory Administrator privileges.

Directory Administrator DN:

Enter the password for the Directory Administrator. Use the same password that was added when the Directory Administrator credentials were created.

Directory access password:

Figure 8 : The Directory Administrator Distinguished Name and Password page

- 9. To configure the Security Manager for an LDAP directory, follow the steps below.
 - a. Select the LDAP Directory.
 - b. In the Directory node name field enter the DNS node name or IP address of the server hosting the LDAP directory.

- c. In the Directory listen to port field, enter the port that the LDAP directory listens to for requests.
 - d. Click on **Next**, which will open the **CA Distinguished Name and Password** page, see the figure above.
 - e. In the CA DN field, enter the distinguished name (DN) of the CA entry.
 - f. In the CA Directory access password field, enter the password for the CA entry.
 - g. Click on **Test Bind Information** to determine if the CA DN and password are correct. The configuration tool attempts to connect to the CA entry by using the information provided. Correct the information in the fields if necessary.
 - h. Click on **Next** to continue. The **Directory Administrator Distinguished Name and Password** page will appear, see the figure below.
 - i. In the Directory Administrator DN field, enter the distinguished name (DN) of a user with directory administration privileges. The Security Manager Administration uses this entry to connect to the directory to add, modify and delete directory entries.
 - j. In the Directory access password field, enter the password of the Directory Administrator.
 - k. Click on **Test Bind Information** to determine if the Directory Administrator DN and password are correct. The configuration tool attempts to connect to the Directory Administrator entry by using the information provided. Correct the information in the fields if necessary.
 - l. Click on **Next** to continue.
10. The **Advanced Directory Attributes** page appears, see the figure below.

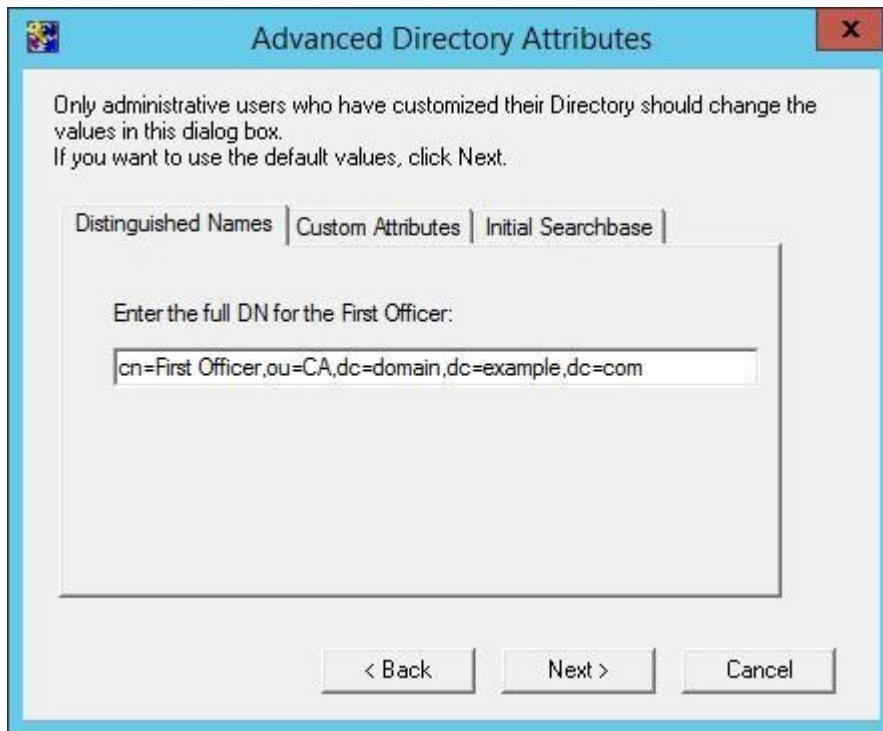


Figure 9 : The Advanced Directory Attributes page

- a. Click on the **Distinguished Names** tab.
- b. In the **Enter the full DN for the First Officer** field, enter the distinguished name of the First Officer (by default: "cn=First Officer", followed by the distinguished name of the CA).
- c. Click on the **Custom Attributes** tab.
- d. In the text field, enter the attribute your directory uses for email addresses (the "mail" attribute in most cases).
- e. Select Include email addresses in `subjectAltName` values of user certificates to include the email addresses in the `subjectAltName` extension of user certificates.
- f. To include the Microsoft userPrincipalName attribute value in the subjectAltName extension of user certificates, select Include the Microsoft(R) `userPrincipalName` in `subjectAltName` values of user certificates.
- g. Click on the **Initial Search** base tab.
- h. Enter the distinguished name of the initial search based on user entries.
- i. Click on **Next**.

11. The **Verify Directory Information** page appears, see the figure below.



Figure 10 : The Verify Directory Information

- a. To run the Entrust Directory Verification Tool and verify your directory information, select **Verify Directory information now**.
- b. Click on **Next**.
- c. If you chose to verify your directory information, the Entrust Directory Verification Tool runs, and you will be prompted with the **ENTDVT Logfile** page.

12. This page displays the results of directory verification, as well as configuration information. This information is saved in the `entdvtetails.log` file. By default, this file is located in: `C:\Program Files\Entrust\Security Manager\10.0.0\Tools\dvt\`.

- a. At the end of the log file, you will see notes, errors and fatal errors.

- b. If the tool encountered any problems, scroll through the log file to determine which tests failed and the exact nature of the problem. Resolve if necessary (go back or run the configuration again).
 - c. Click on **Next** if there were no problems.
- 13. The **Current User's Windows Login Password** page appears.
 - a. In the **Password** field enter the password for the Windows account (Windows ID).
 - b. If you want to enable autologin, select Enable autologin for automatic service startup which manually starts the Security manager service without requiring the Master User to manually start it. This may cause a security risk.
 - c. Click **Next** to continue.
- 14. By selecting the ODBC, the Data Source page appears.
 - a. Select **EASM_Entrust_PostgreSQL**.
 - b. Click on **Next** to continue.
- 15. The Database User and Password page appears.
 - a. In the **Password** field enter the password for the database user that was chosen, when the PostgreSQL database was installed.
 - b. Click **Next** to continue.
- 16. The **Database Backup User and Password** page appears.
 - a. In the **Password** field enter the password for the database backup user that was chosen, when the PostgreSQL database was installed.
 - b. Click **Next** to continue.
- 17. The **Security Manager Port Configuration** page appears.



The host network interface card (NIC) must be enabled before configuring the ports.

- a. In the **Security Manager** node name field enter the DNS hostname or IP address of the server hosting the Security Manager.
- b. In the Proto-PKIX listen to port field enter the port to use for the Entrust Proto-PKIX subsystem. The default port is 709.

- c. In the Administration subsystem listen to port field enter the port to use for the Administration Service Handler (ASH) subsystem. The default port is 710.
- d. In the PKIX-CMP subsystem server port field enter the port to use for the PKIX-CMP subsystem. The default port is 829.
- e. In the Entrust XML administration protocol port field enter the port to use for the XML Administration Protocol (XAP) subsystem. The default port is 443 (do not use this port if you are planning to use SSL) or 1443.
- f. Click **Next** to continue.

18. The **CA Type** page appears.

- a. Select the type of the CA to configure (Root CA, Country Signing Root CA (CSCA) or Subordinate CA).
- b. Click **Next** to continue, which will bring up the **Cryptographic Information** page, see the figure below.

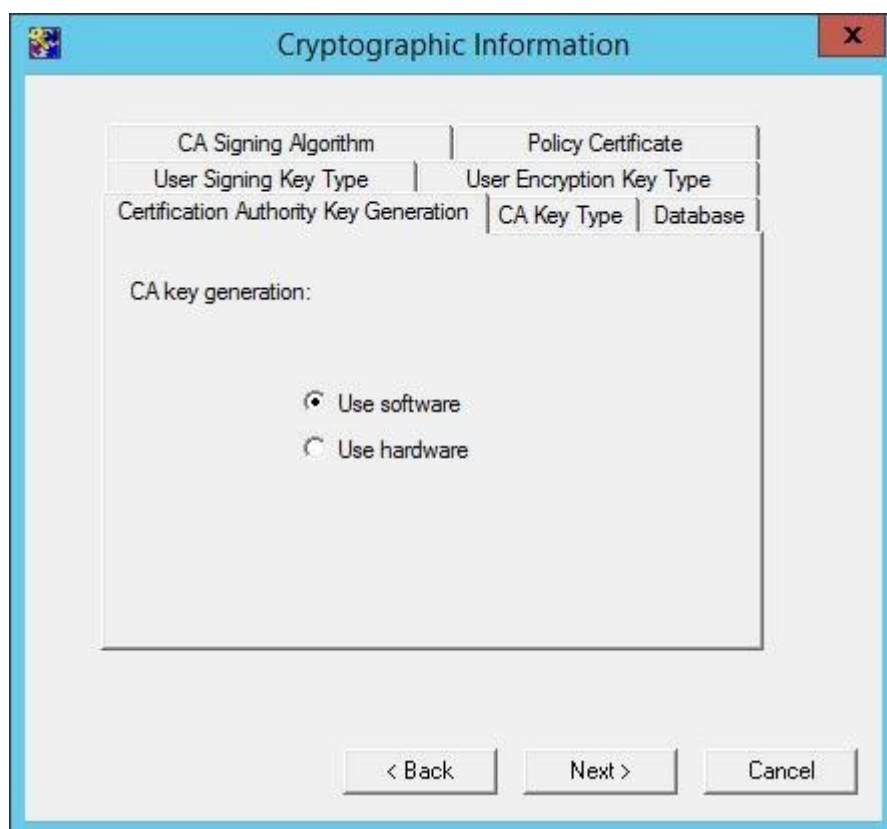


Figure 11 : The Cryptographic Information page

19. Click the **Certification Authority Key Generation** tab. Select between storing the CA keys on software or hardware.
20. Click the **CA Key Type** tab.
 - a. Select the key pair type (RSA, DSA or EC) to use as the CA keys. Note that not all Security Manager client applications support all the available algorithms.
 - b. In the Parameters drop-down list, select the key size (RSA or DSA) or the domain parameters (EC) for the CA key type.
21. Click the **Database** tab. Select the encryption algorithm that you want to use to encrypt and protect data in the Security Manager database for software-based database protection.
22. Click the **User Signing Key Type** tab.
 - a. Select the key pair type (RSA, DSA or EC). This will be used for user signing and nonrepudiation keys.
 - b. Select the key size (RSA or DSA) or the domain parameters (EC) for the user signing and non-repudiation keys.
23. Click the **User Encryption Key Type** tab.
 - a. Under **Encryption and Dual Usage Keys** select the key pair type (RSA or EC) that users will use for encryption operations.
 - b. Select the key size (RSA or DSA) or the domain parameters (EC) for the user encryption and dual usage keys.
24. Click the **CA Signing Algorithm** tab. Select the algorithm that the Security Manager will use to sign certificates and revocation lists. The algorithm selected depends on the key type that was selected for the CA.
25. Click the **Policy Certificate** tab. Enter the number of days until policy certificates should be valid, before they need to be updated (30 days is by default).
26. Click the **Next** button.
27. If the CA keys should be stored on a device, then:
 - a. In case that no hardware devices are detected, the **No Hardware Device Found** dialog box appears. Click **OK**. The **Select New Cryptographic Hardware Library** dialog box will appear. Then select the correct cryptographic hardware library for the hardware device.
 - b. The **Use This Hardware** dialog box appears. Select the hardware slot that will store the CA keys, see the figure below.

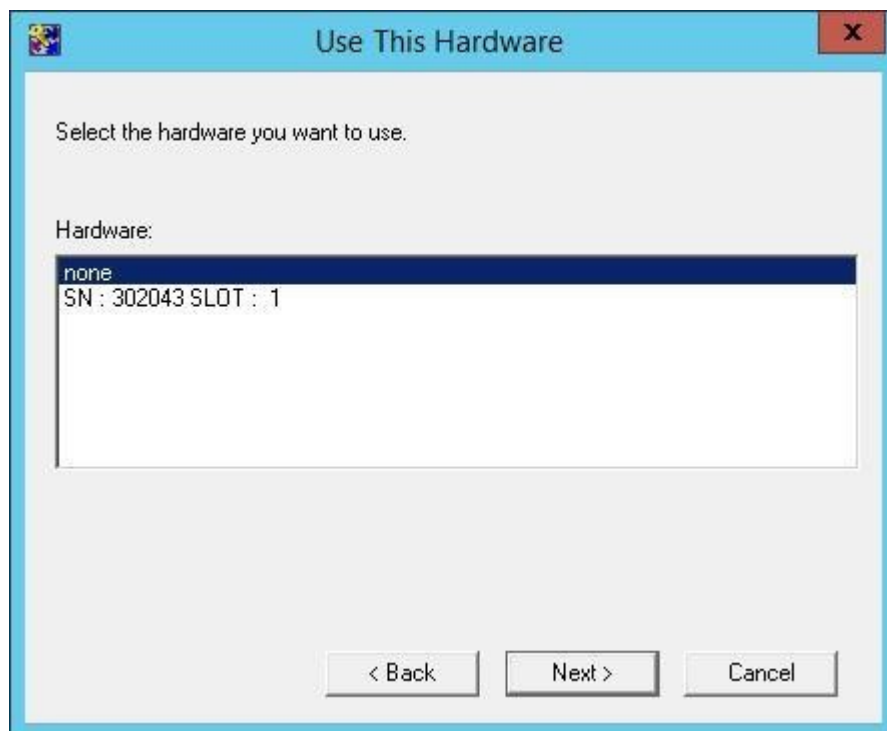


Figure 12 : Use This Hardware dialog box

c. Click the **Next** button.

28. If a root CA or a subordinate CA is being configured, the CRL configuration page appears. If you plan to support Microsoft client applications that use the Microsoft Cryptographic API (such as native Microsoft Outlook clients), it needs to be configured. When configuring a subordinate CA, ensure that the root CA is configured for the same level of Microsoft compatibility.

a. To begin, click on **Yes** then select one of the following options from the drop-down list:

- To configure CRLs to work with applications on any Microsoft operating system, select Make combined CRLs compatible with applications on any Microsoft OS. When this option is selected, the Security Manager will issue combined CRLs.
- To configure CRLs to work with applications on Microsoft Windows XP/2003 or later operating systems, select Make partitioned CRLs compatible with applications on Windows XP/2003 or later. When this option is selected, the Security Manager will issue partitioned CRLs.

b. If you do not want the Security Manager to work with Microsoft client applications, click **No**, do not work with Microsoft Windows applications.

c. To enable the combined CRL, select **Enable Combined CRL**.

d. Click **Next** to continue.

29. For a root CA or a subordinate CA, the CRL Distribution Point Information page will appear in case that you selected to work with Microsoft client applications (in that case specify at least one CDP URL). CDP URLs in the Default CDP URLs list are global default CDP URLs. See the figure below.

The screenshot shows the 'CRL Distribution Point Information' dialog box. It has a title bar with a close button (X). The main area contains instructions: 'Shared network CRL folders. Use Change button to select an existing network share. Combined CRL share is mandatory. Partitioned CRL share is mandatory if partitioned URLs defined.' Below this are two sections: 'Combined CRL:' and 'Partitioned CRL:'. Each has a text input field (both containing '\\WIN2012\CRL'), a 'Disable' checkbox (unchecked), and a 'Change' button. Further down, instructions state: 'Define one or more URLs for the distribution points in the CDP extension in certificates. The URL host needs to be accessible by the entity validating the certificate.' This is followed by a 'URL Type:' dropdown menu (set to 'http') and a 'URL Host:' text input field. Below these is a 'CDP Definition:' section with a large empty text area, a 'Create from Settings' button, and an 'Add' button. At the bottom, there's a 'Default CDP URLs:' section with two checkboxes: 'Include LDAP DN' (checked) and 'LDAP DN Last' (unchecked). Below this is another large empty text area and a 'Delete' button. At the very bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 13 : The CRL Distribution Point Information page

a. For Combined CRL:

- In the text field, enter the path to the folder, where the Security Manager will write combined CRLs. To work with Microsoft client applications, the Security Manager should write combined CRLs to a shared folder on the network. The folder must be named CRL. The account used by the Security manager services should have direct writing privileges for that location.
- To disable or prevent the Security Manager from writing combined CRLs to files, select **Disable** (this option is disabled if you chose to configure CRLs to work with applications on any Microsoft OS).

b. For Partitioned CRL:

- In the text field, enter the path to the folder, where the Security Manager will write partitioned CRLs. To work with Microsoft client applications on modern Windows installations, the Security Manager should write partitioned CRLs to a shared folder on the network. The folder should be named CRL. The account used by the Security manager services should have direct writing privileges for that location.

c. Enter a CDP URL into the CDP Definition field or create a CDP URL from settings as follows:

- Select a CDP URL type (HTTP, LDAP, file, FTP).
- In the URL Host field, enter the host name or the IP address of the Web server, FTP server or the File server that will host the CRL files. Click **Create from Settings**. The CDP Definition field is filled with a CDP URL based on the CDP type and host information provided.

d. To add the CDP URL specified in the CDP Definition field to the Default CDP URLs list, click **Add**.

e. To remove a CDP URL from the Default CDP URLs list, select the CDP URL that needs to be removed and click **Delete**.

f. For Default CDP URLs (the global default CDP definitions), you can configure how the LDAP DN is handled in the list of CDPs. The LDAP DN refers to the DN of the CRL in the Security Manager directory.

g. Click **Next** to continue.

h. If you chose to work with Microsoft client applications, but did not specify any CDP URLs, the following warning appears: To go back, click **Cancel**. To continue, click **OK** (if you do not want to add CDP URL).

30. If you are configuring a CSCA, the CRL Distribution Point Information page appears, see the figure below. The CDP URLs in the Default CDP URLs list are global default CDP URLs. CDP URLs in the CSCA CDP URLs list are CDP URLs that will apply to the following CSCA-specific certificate types: CSCA root certificates, CSCA link certificates, Master List Signer certificates and Document Signer certificates.

CRL Distribution Point Information

Shared network CRL folders. Use Change button to select an existing network share.
Combined CRL share is mandatory.
Partitioned CRL share is mandatory if partitioned URLs defined..

Combined CRL: ☐ Disable

Partitioned CRL: ☐ Disable

Define one or more URLs for the distribution points in the CDP extension in certificates.
The URL host needs to be accessible by the entity validating the certificate.

URL Type:

URL Host: ☒ CSCA ☐ Default ☐ All

CDP Definition:

Default CDP URLs: ☒ Include LDAP DN ☐ LDAP DN Last

CSCA CDP URLs:

Figure 14 : The CRL Distribution Point Information page

a. For Combined CRL:

- In the text field enter the path to the folder where the Security Manager will write combined CRLs. To work with Microsoft client applications, the Security Manager should write combined CRLs to a shared folder on the network. The folder must be named CRL.

b. For Partitioned CRL:

- In the text field, enter the path to the folder where the Security Manager will write partitioned CRLs. To work with Microsoft client applications on Windows XP/2003 or later operating systems, the Security Manager should write partitioned CRLs to a shared folder on the network. The folder should be named CRL.

c. Enter a CDP URL into the CDP Definition field or create a CDP URL from settings as follows:

- From the URL Type drop-down list select a CDP URL type (HTTP, LDAP, file, FTP or https).
- To add a CDP URL to the Default CDP URLs list, the URL Type should be HTTP, LDAP or https. In case that a CDP URL is added to the CSCA CDP URLs list.
- Click **Create** from Settings. The CDP Definition field is filled with a CDP URL based on the CDP type and host information provided.

d. To add the CDP URL specified in the CDP Definition field to the Default CDP URLs or CSCA CDP URLs list select, which list will contain the CDP URL.

- To add the CDP URL to the Default CDP URLs list, select CSCA.
- To add the CDP URL to the CSCA CDP URLs list, select Default.
- To add the CDP URL to both lists, select All.

e. To remove a CDP URL from the Default CDP URLs list, select the CDP URL that should be removed and click **Delete**.

f. To remove a CDP URL from the CSCA CDP URLs list, select the CDP URL that should be removed and click **Delete**.

g. You can configure how LDAP DN is handled in the list of CDPs for the default CDP URLs. The LDAP DN refers to the DN of the CRL in the Security Manager directory.

h. Click on **Next** to continue.

i. In case that no CDP URLs were specified for a CSCA the following warning appears: "To go back, click on **Cancel**. To continue, click on **OK**."

31. If you are configuring a CSCA, the Issuer Alternative Name page appears, see the figure below. CSCA certificates, Master List Signer certificates and Document Signer certificates issued by the CSCA should include an issuer alt name extension (should provide contact information associated with your CSCA and a directory string made of ICAO-assigned country codes). The Security Manager will DER-encode the data and include it in the CSCA root certificates, Master List Signer certificates and Document Signer certificates, issued by the CSCA.

Issuer Alternative Name

Configure the mandatory IssuerAltName\SubjectAltName for a CSCA. It must include contact information with one or more of rfc822Name, dNSName and uniformResourceIdentifier. It also must include a directoryName with ICAO-assigned country codes using the 'l' or 'st' attribute. Examples are 'l=CAN', 'st=HKG'.

If it is not defined now it must be defined in the entmgr.ini configuration file before first time initialization.

Name Type:

Syntax: E-mail address

Name Value:

Add

Name	Value
------	-------

< ||| >

Delete

< Back Next > Cancel

Figure 15 : The Issuer Alternative Name page

- a. To add value to the IssuerAltName extension, select the type of information to add and enter a value in the Name-Value field. Click **OK**.

- b. To remove a value from the IssuerAltName extension, select the name of the value that should be removed from the list, and click **Delete**.
- c. Click on **Next** to continue.
- d. If no IssuerAltName values were specified, the following warning appears (see the figure below):

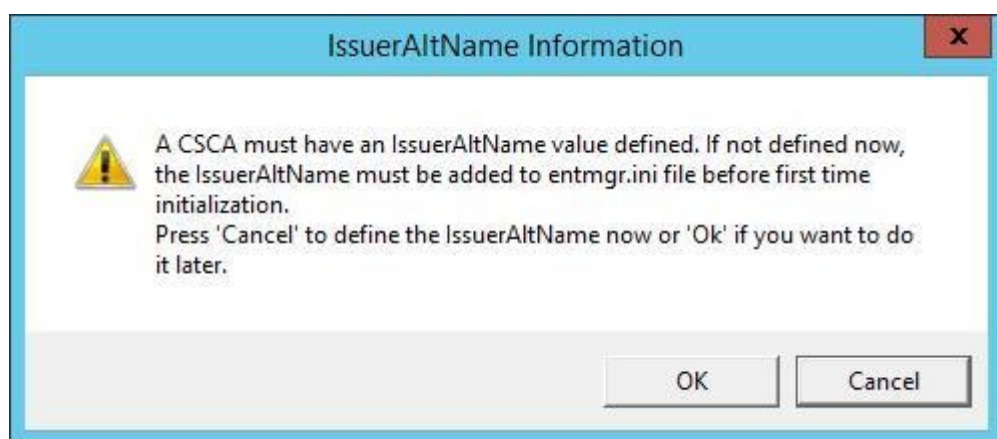
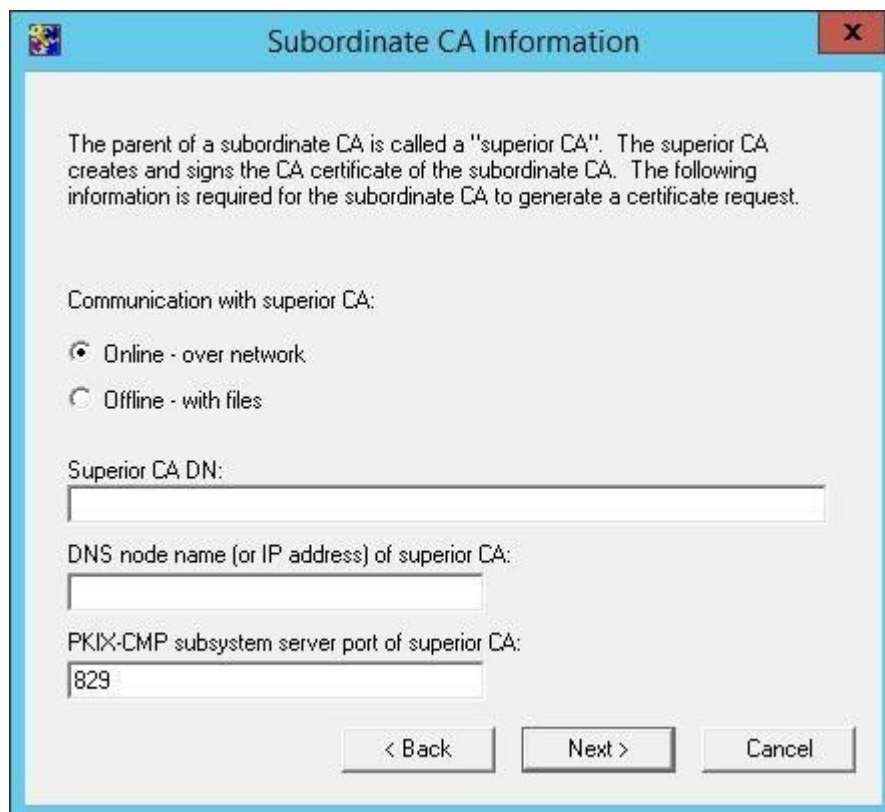


Figure 16 : The IssuerAltName information warning

- 32. The **Enable long expiry dates** dialog box appears.
 - a. To allow the CA to issue certificates with expiry dates beyond the end of the year 2037, select **Yes**.
 - b. Click on **Next** to continue.
- 33. If a subordinate CA is being configured, the Subordinate CA Information page appears, see the figure below.



Subordinate CA Information

The parent of a subordinate CA is called a "superior CA". The superior CA creates and signs the CA certificate of the subordinate CA. The following information is required for the subordinate CA to generate a certificate request.

Communication with superior CA:

☒ Online - over network
☐ Offline - with files

Superior CA DN:

DNS node name (or IP address) of superior CA:

PKIX-CMP subsystem server port of superior CA:

< Back Next > Cancel

Figure 17 : The Subordinate CA information

- a. Under the Communication with superior CA, select the method that the subordinate CA will use to request and obtain its initial subordinate CA certificate with its superior CA.
 - b. If the subordinate CA will communicate online with its superior CA:
 - In the Superior CA DN field, enter the distinguished name of the superior CA. For example, ou=Superior CA,dc=company,dc=com.
 - In the DNS node name (or IP address) of superior CA field, enter the DNS hostname or IP address of the server hosting the superior CA.
 - In the PKIX-CMP subsystem server port of superior CA field, enter the port that the superior CA uses for PKIX-CMP requests.
 - c. Click on **Next**.
34. If a subordinate CA is being configured and the subordinate CA will communicate with the superior CA online, the Superior CA Signing Algorithm page appears.

- a. Select the signature algorithm that the superior CA will use to sign the subordinate CA verification certificate and then click on **Next**.
 - b. Proceed to Step 40.
35. If a root CA or CSCA is being configured, the CA Certificate Properties page appears.
- a. In the CA verification certificate lifetime field, enter the lifetime (in months) of the CA's verification certificate.
 - b. The CA private key usage period is a percentage of the CA verification certificate lifetime. For example, 33 % of 180 months is 60 months (5 years). When the private key reaches near the end of its lifetime, the Security Manager starts writing messages to the audit logs, informing you that the CA is nearing expiry.
 - c. Click on **Next** to continue.
36. If the CVCA license information was entered, the Configuration Information for CVCA page appears, see the figure below.

Configuration Information for CVCA

The following information is required to initialize your CVCA. All the fields require data.

Country: Country Code:

☐ User Defined Country Code

Mnemonic Label (1-9 Characters):

Terminal Authentication Algorithm:

Key Type:

Holder Access Rights: ☐ Iris ☒ Fingerprint

Certificate Lifetime (25 year maximum):

Term

☒ Years: ☐ Weeks: Lifetime:

☐ Months: ☐ Days:

Certificate Expiry Warning Threshold (days):

Sequence Number Algorithm:

Type

☒ Numeric ☐ Alphanumeric

☐ Use the Country Code in the Sequence Algorithm

< Back Next > Cancel

Figure 18 : The Configuration information for CVCA page

- In the Country drop-down list, select your country.
- In the Mnemonic Label field, enter a unique label for the CVCA.
- In the Terminal Authentication Algorithm drop-down list, select a terminal authentication algorithm.
- In the Key Type drop-down list, select a key type.
- The holder access rights can be allowed, if necessary.
- Under the Certificate Lifetime, enter the lifetime of CVCA certificates.
- In the Certificate Expiry Warning Threshold (days) field, enter the number of days before a CVCA certificate expires, until the Security Manager starts warning you of the impending expiry. A value of 0 suppresses the warnings.

- h. Under the Sequence Number Algorithm.
 - Click on **Numeric** to use a numeric sequence number algorithm.
 - Click on **Alphanumeric** to use an alphanumeric sequence number algorithm.
 - i. To include the country code in the sequence number algorithm, select Use the Country Code in the Sequence Number Algorithm.
 - j. Click on **Next** to continue.
37. If the DV license information was entered, the Configuration Information for DV page appears.
- a. In the Country drop-down list, select your country.
 - b. In the Mnemonic Label field, enter a unique label for the DV.
 - c. Click on **Next** to continue.
38. If the folders that were specified for the combined or partitioned CRLs exist, a **Remove Duplicate Share** dialog box appears. This dialog box warns you that if you continue, the wizard will delete the current shared folder and create a new shared folder.
39. When the configuration wizard creates a shared CRL folder, the **CRL Share** dialog box appears. The CRL folder was created and granted the appropriate permissions to the Administrators' group on the server.
- a. For domain users to access the CRL file in the folder, read permission for the CRL folder has to be granted to the Domain Users group. If a Web-based CDP is used, the CRL folder must be added (shared to the Web) to the default Web site with the alias CRL.
 - b. Click on **OK**.
40. The Configuration Complete page appears. See the figure below.



Figure 19 : The Configuration Complete page

41. To initialize the Security Manager immediately, select Run Security Manager Control Command Shell now. If you want to do that later and customize some of the Security Manager files, then click don't select that option.
42. Clicking on **OK** will close the Security Manager configuration wizard.
43. If you chose to initialize Security Manager later, the **Configuration Incomplete** dialog box appears. Click on **OK** to close it.



After configuring the Security Manager either securely destroy the copies of the collected configuration data and the entconfig.ini file, or lock them in a safe place, because they contain sensitive information.



It is not possible to configure the Security Manager again. If you made a mistake, you can change some of the settings by editing the entmgr.ini file, or by uninstalling or reinstalling the Security Manager and then configuring it again.

More information about this topic can be found in [SMII], [SMOI] and [SMDI].

7 Backup and Restore

The Utimaco HSM enables different ways of making backups of either the entire database of keys or just groups of keys. All the backups are encrypted by using the Master Backup Key (MBK), generated by the system administrator, when setting up the HSM. More information about the MBK can be found in [CSADMIN].

7.1 Backing up and Restoring Key Database

All the keys inside the HSM are stored in a CXI database and it is possible to back up the entire database at once. In the same way, the user database can be backed up as well. In FIPS mode this feature is not supported.

1. Open the Crypto Administration Tool.
2. Make sure that the HSM is connected and in the operational mode.
3. Click on **Login/Logoff** to open the **Login/Logoff User** window.
4. Login the appropriate users to achieve the permission level of at least **22000000**.
5. Click on **Backup/Restore** to open the CryptoServer Database **Backup/Restore Wizard** window.
 - a. In the **Command** section select either:
 - Back up databases from source CryptoServer to backup directory.
 - Restore databases from backup directory to target CryptoServer.
 - Copy databases from source CryptoServer to target CryptoServer.

In the **Settings** section:

- Select the appropriate Source CryptoServer.
- If available, select the appropriate Target CryptoServer.
- In the Backup directory section type the appropriate backup directory path (set to **C:\Program Files\Utimaco\CryptoServer\Administration** as default) or click ... to browse for the appropriate directory.

6. Select the databases to backup or restore.

7. Click **Execute**.
8. A confirmation window appears.



For a FIPS backup, please use the P11CAT or the P11tool2 tools.

7.2 Backing up and Restoring a Key Database with P11CAT

It is possible to backup separate PKCS#11 slots by using either the P11CAT or the p11tool2. In this guide we use the P11CAT for the backup procedure. Please refer to [CSP11TOOL2] for the backup procedure with the p11tool2.

1. Open the PKCS#11 CryptoServer Administration (P11CAT).
2. Log in to the slot you wish to backup as the Cryptographic User (achieve the permission level of at least 00000002).
3. Click on **Backup/Restore**.
4. Click on **Backup/Restore Keys**.
5. Select one of the 4 options. Click the one that corresponds to your case. The possibilities are to perform either:
 - Backup Internal Keys.
 - Backup External Keys.
 - Restore Key Backup to Internal Key Store.
 - Restore Key Backup to External Key Store.
6. A pop-up window opens.
 - a. Select the directory where the key database will be backed up and type the name of the key database in the section File name.
 - b. If you chose to restore a key backup to an internal or an external key store, select the directory where your backup is located.
 - c. To confirm your choice, click on **Save**.
7. In the **Status** window a log of the performed action is displayed.

8 FIPS Requirements

All the steps are identical for the HSM in FIPS 140-2 approved mode. The only difference is that the backup of the entire key database is not possible. In this case the P11CAT or the p11tool2 are used for backing up the keys.



Note that although the integration does not require extra steps, the HSM running in FIPS mode will accept ONLY FIPS compliant parameters. Be careful to select FIPS compliant algorithms, key lengths and elliptic curves when generating new keys. For more information about the FIPS compliant algorithms please refer to the CryptoServer User and Administration Guides.

9 Further Information

This document forms a part of the information and support, which is provided by the Utimaco IS GmbH company. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website:

<https://utimaco.com>.

10 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSPKCSDG]	CryptoServer - PKCS#11 R2 Developer Guide	2012-0007
[CSPKCSDG]	CryptoServer - PKCS#11 R3 Developer Guide	2022-0001
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[LPKCSHD]	Learning PKCS#11 in Half a Day	2015-0008
[SMII]	SecurityManager Installation Guide	
[SMOI]	SecurityManager Operations Guide	
[SMDI]	SecurityManager Database Configuration Guide	
[CSP11TOOL2]	CryptoServer PKCS#11 p11tool2 Reference Manual	2012-0004

Table 5: List of references

11 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

<https://support.hsm.utimaco.com/support/rma/new>

Other Support Queries

- Mail (preferred contact method)
support@utimaco.com
Attach the diagnostic information to your email.
- Web portal
<https://support.hsm.utimaco.com/support/cases/new/>
The diagnostic information will be requested in our response if necessary.
- By phone
AMERICAS +1-844-UTIMACO (+1 844-884-6226)
EMEA +49 800-627-3081
APAC +81 800-919-1301
The diagnostic information will be requested in our response if necessary.