Trusted Cyber Technologies

THALES

Entrust Authority Security Manager and Luna HSM

Integration Guide

007-500033-001

REV E

03 NOVEMBER 2021

ENTRUST
TECHNOLOGY ALLIANCE
PROGRAM

Preface

Scope

This technical integration guide provides an overview of how to integrate Entrust Authority Security Manager (EASM) with the Thales TCT Luna Hardware Security Module (HSM) in an X.509 Public Key Infrastructure (PKI) configuration.

Technical Support Information

If a problem occurs during installing, registering, or operating this product, please review the documentation. For assistance in resolving the issue, contact the supplier or Thales Trusted Cyber Technologies (Thales TCT) Support. Thales TCT Customer Support operates 24 hours a day, 7 days a week. The level of access for this service is governed by the support plan arrangements made between Thales TCT and the organization. Please consult the support plan for further information about entitlements, including the hours when telephone support is available.

Contact method	Contact information	
Address	Thales Trusted Cyber Technologies 3465 Box Hill Corporate Center Drive Suite D Abingdon, MD 21009 USA	
Phone	United States	(866) 307-7233
Web	http://www.thalestct.com/support/	
Support and Downloads	http://www.thalestct.com/support/ Provides access to the Thales Trusted Cyber Technologies Knowledge Base and quick downloads for various products.	

Please refer to: www.thalestct.com/document-disclaimer for information regarding use and limitations associated with this document.

Table of Contents

1 Introduction

Overview

This document covers the necessary information to install, configure and integrate the Entrust Authority Security Manager with the Luna HSM. Integrating the Luna HSM with Security Manager provides enhanced hardware-based security validated to FIPS Level 2 or 3, depending on the Luna HSM configuration.

The Entrust Authority Security Manager serves as the X.509 Certification Authority in an Entrust infrastructure. Although it can operate in "software" mode, it can optionally use hardware devices where cryptographic operations and key storage are performed. By managing the full lifecycles of certificate-based digital identities, Entrust Authority Security Manager enables encryption, digital signature and authentication capabilities to be applied consistently and transparently across a broad range of applications and platforms.

Third-Party Application Versions Tested

- Entrust Authority Security Manager
- Entrust Authority Security Manager PostgreSQL
- Microsoft AD LDS

Integration Matrix

The table below enumerates all the versions of products tested in this integration.

Platforms Tested	Entrust Authority Security Manager	Microsoft AD LDS	Luna HSM Software	Luna HSM Firmware	Luna Client
Windows Server 2019	10.0.1.4	88	5.4.10-4	6.21.6	7.11.2-85
Windows Server 2019	10.0.1.4	88	7.11.0-25	7.11.1	7.11.2-85

Note: As of 01 November 2021, the Luna Network HSM v 7.11 seen above has been validated by Entrust for EASM v.10. Test results for the earlier version of the HSM were not submitted for validation, but integration testing by Thales TCT was successful.

Prerequisites

In order to integrate Entrust Authority Security Manager with Luna HSM, the following prerequisites must be met:

- The Luna HSM is installed and operational
- The Luna Client is installed on the server
- The Network Trust Link (NTL) is established between the Luna Client and the Luna HSM. If assistance is needed to establish the NTL on a 7.11.1 client or newer, please see the following guide available in the support portal, which describes a quick and easy way of establishing the link:

  How To: LunaCM ClientConfig Deploy

  For older client versions, please refer to the following guide:

  Guide: Configuring a Network Trust Link between a Luna Client and a Luna HSM

The following third party software also must be installed:

- Entrust Authority PostgreSQL Database
- Entrust Authority Security Manager
- Directory Server (AD LDS is used in this guide)

Integration Synopsis

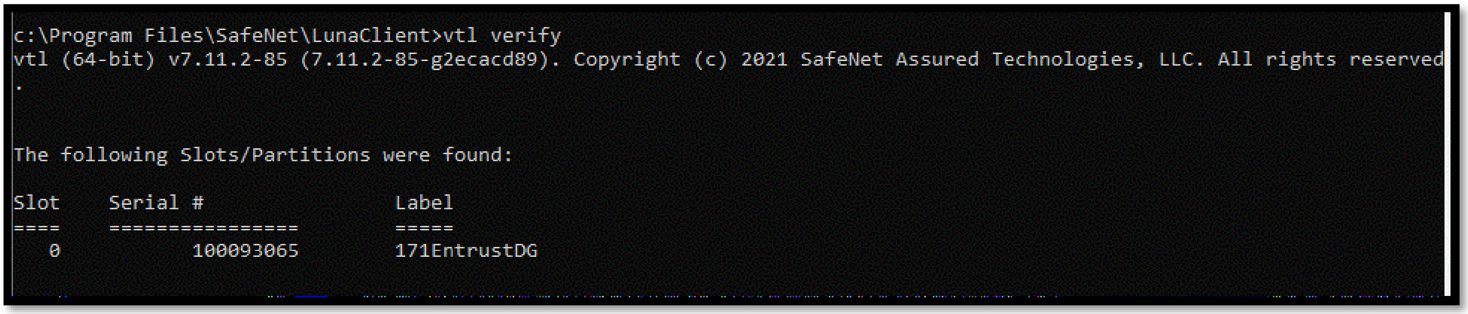
- Establish (or verify) the connection between the Luna Client and Luna HSM
- Configure Entrust Authority Security Manager to use the HSM
- Initialize Security Manager

2 Establish Network Trust Link between a Luna Client and a Luna HSM

The Luna Client installed on the server enables communication between Security Manager and the HSM via a secure connection called a Network Trust Link.   The first step in the integration is to establish this Network Trust Link if it has not already been done during Luna Client installation.

Use the following command to determine or verify that the connection has been established and a partition exists on the HSM that the client can access. If no slot and partition are found, use the document listed in the Prerequisites section to establish the Network Trust Link. The slot will be needed for a later step in the document, as will the partition password.

```
c:\Program Files\SafeNet\LunaClient>vtl verify
```



```
c:\Program Files\SafeNet\LunaClient>vtl verify
vtl (64-bit) v7.11.2-85 (7.11.2-85-g2ecacd89). Copyright (c) 2021 SafeNet Assured Technologies, LLC. All rights reserved
.


The following Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
   0           100093065        171EntrustDG
```

3 Integrate Entrust Authority Security Manager with Luna HSM

Rather than entering configuration data directly into the Security Manager configuration wizard, it is recommended to pre-populate directory-related fields, Security Manager-related fields, or both by entering data in the **`entconfig.ini`** file (Windows only).

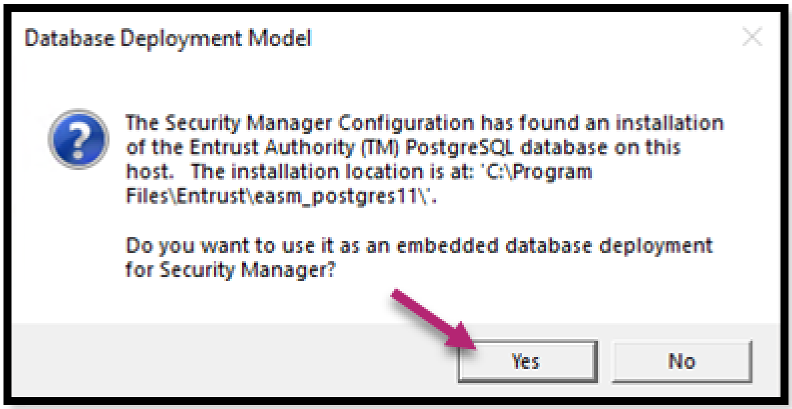
The **`entconfig.ini`** file is located in the following directory:

```
C:\Program Files\Entrust\Security Manager\etc\ini
```

1. Run the **Entrust Authority Security Manager Configuration Utility**. Navigate to the Security Manager **`\bin`** directory and double click **`entConfig.exe.`**

```
C:\Program Files\Entrust\Security Manager\bin\entConfig.exe
```

2. The **Database Deployment Model** will pop up. Click **Yes**.

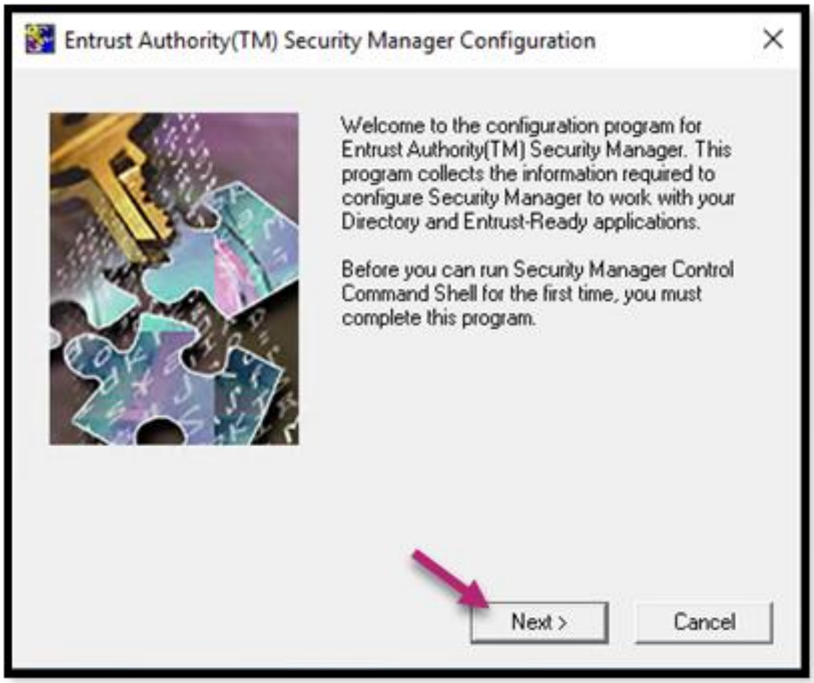


Database Deployment Model

The Security Manager Configuration has found an installation of the Entrust Authority (TM) PostgreSQL database on this host. The installation location is at: 'C:\Program Files\Entrust\easm_postgres11\'.

Do you want to use it as an embedded database deployment for Security Manager?

3. The **Entrust Security Manager Configuration** dialog box will launch. Click **Next**.



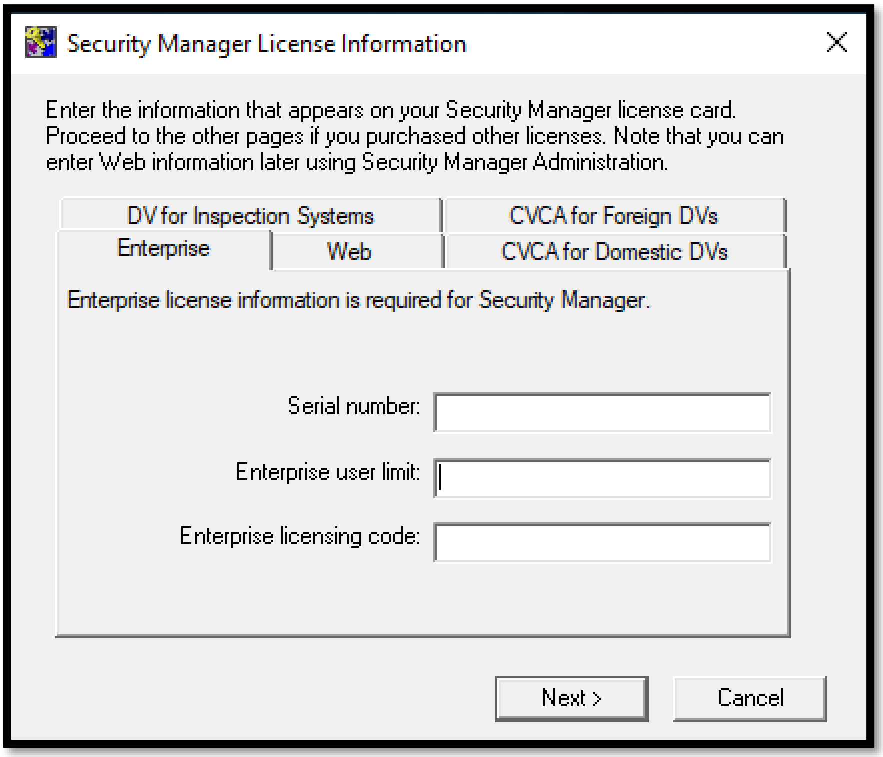
Entrust Authority(TM) Security Manager Configuration

Welcome to the configuration program for Entrust Authority(TM) Security Manager. This program collects the information required to configure Security Manager to work with your Directory and Entrust-Ready applications.

Before you can run Security Manager Control Command Shell for the first time, you must complete this program.

4. The Entrust Configuration wizard will launch. Click **Next**.

5. On the **Security Manager License Information** dialog, enter the license information from the Security Manager license card. Click **Next**. If the `entConfig.exe` file has been edited previously, as recommended, this information will be populated.



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.

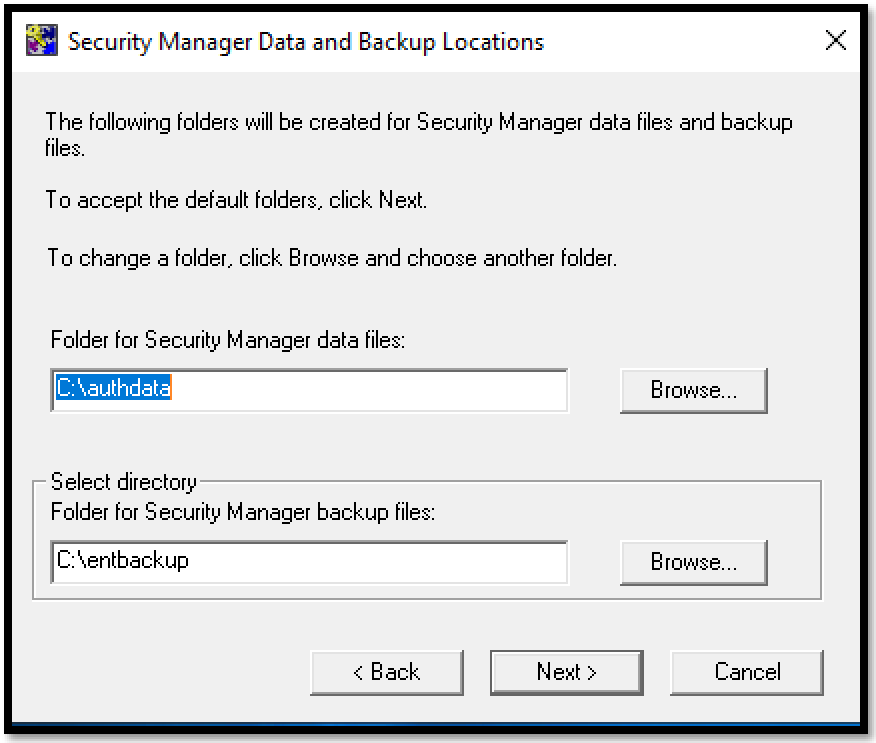
Enterprise license information is required for Security Manager.

Serial number:

Enterprise user limit:

Enterprise licensing code:

6. On the **Security Manager data and backup locations** dialog, update the directories or accept the defaults. Click **Next**.



Security Manager Data and Backup Locations

The following folders will be created for Security Manager data files and backup files.

To accept the default folders, click Next.

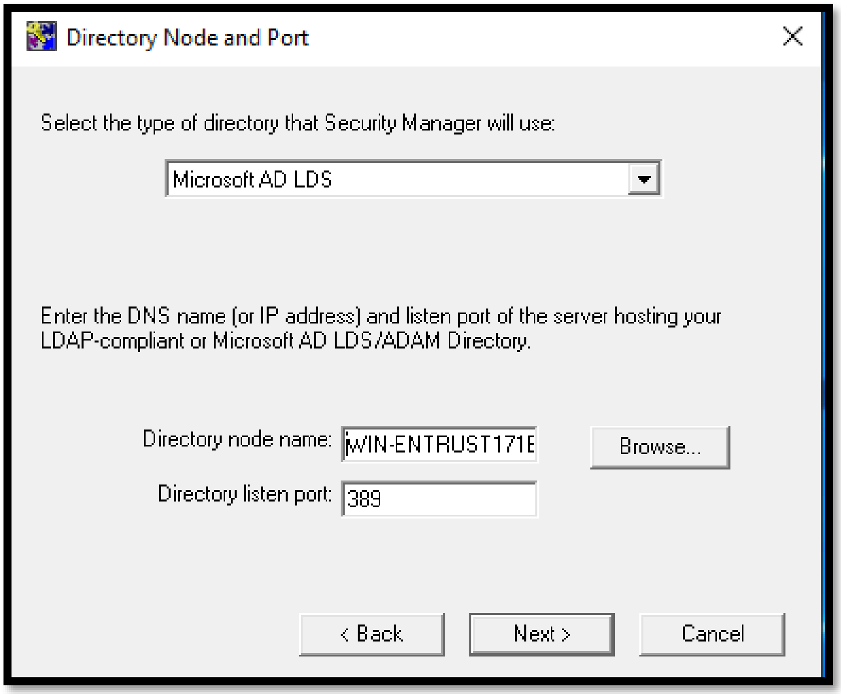
To change a folder, click Browse and choose another folder.

Folder for Security Manager data files: C:\authdata

Select directory

Folder for Security Manager backup files: C:\entbackup

7. On the **Directory Node and Port** dialog window, select the type of directory being used and node name and listening details or accept the defaults. Click **Next**.



Directory Node and Port

Select the type of directory that Security Manager will use:

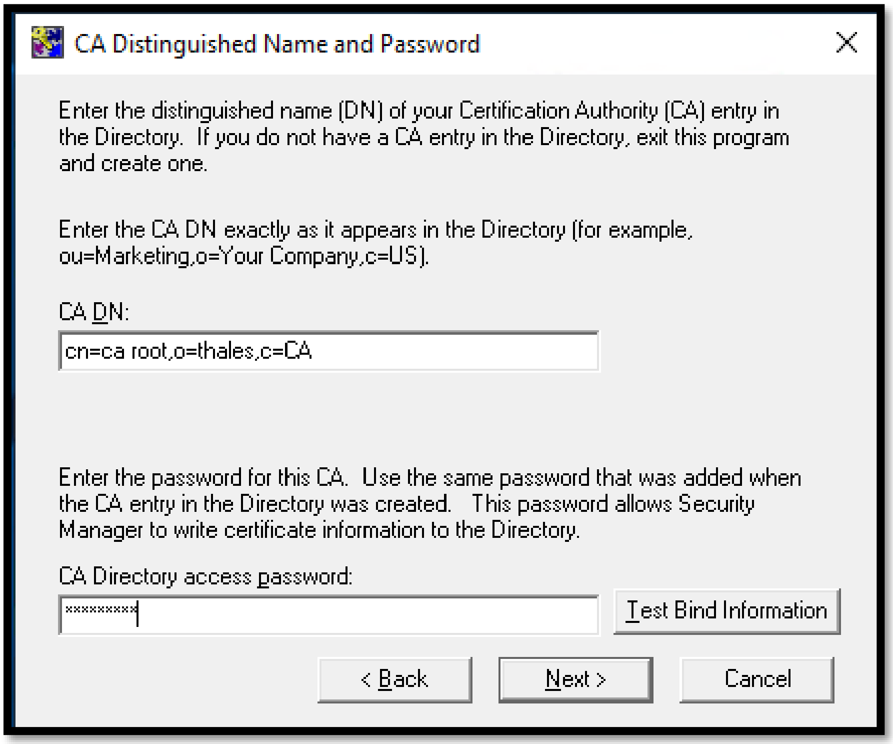
Microsoft AD LDS

Enter the DNS name (or IP address) and listen port of the server hosting your LDAP-compliant or Microsoft AD LDS/ADAM Directory.

Directory node name: WIN-ENTRUST171E

Directory listen port: 389

8. The **CA Distinguished Name and Password** dialog will display; the CA DN will already be populated. Enter the password that was established when the Directory was created. Click **Test Bind Information**.



CA Distinguished Name and Password

Enter the distinguished name (DN) of your Certification Authority (CA) entry in the Directory. If you do not have a CA entry in the Directory, exit this program and create one.

Enter the CA DN exactly as it appears in the Directory (for example, ou=Marketing,o=Your Company,c=US).

CA DN:

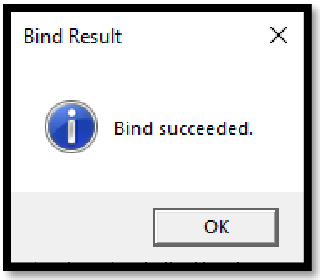
cn=ca root,o=thales,c=CA

Enter the password for this CA. Use the same password that was added when the CA entry in the Directory was created.   This password allows Security Manager to write certificate information to the Directory.

CA Directory access password:

****

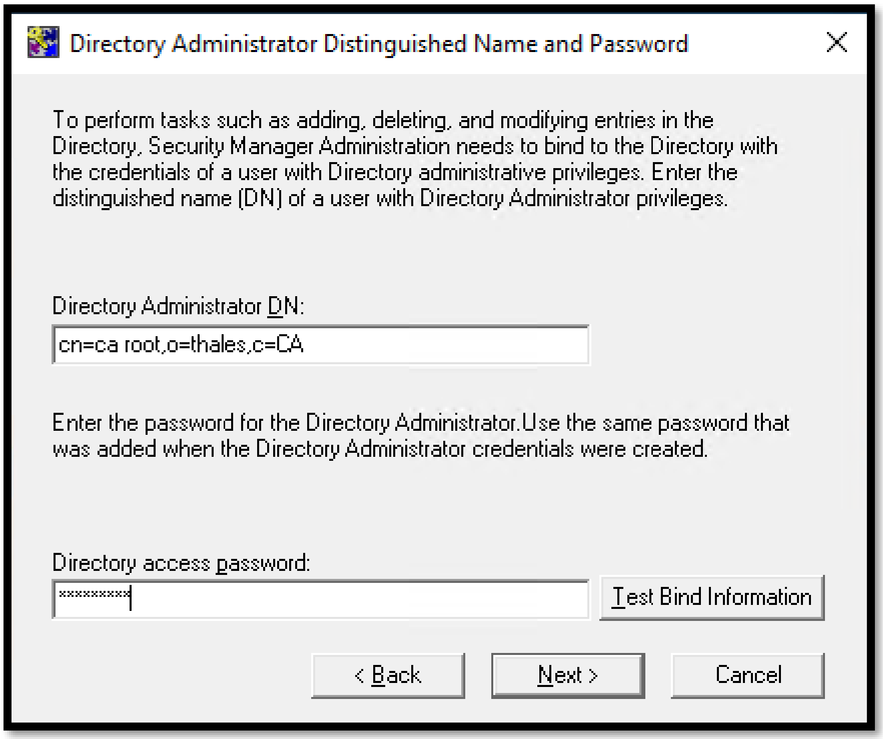
9. A **Bind Result** dialog will display indicating that the bind was successful. Click **OK**.



Bind Result

Bind succeeded.

10. The **Directory Administrator Distinguished Name and Password** dialog will display. The **Directory Administrator DN** will already be populated. Enter the password that was established when the Directory Administrator credentials were created. Click **Test Bind Information**.



Directory Administrator Distinguished Name and Password

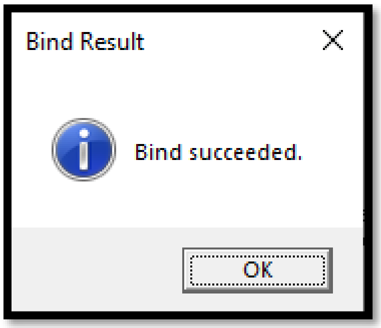
To perform tasks such as adding, deleting, and modifying entries in the Directory, Security Manager Administration needs to bind to the Directory with the credentials of a user with Directory administrative privileges. Enter the distinguished name (DN) of a user with Directory Administrator privileges.

Directory Administrator DN: cn=ca root,o=thales,c=CA

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

Directory access password: **********

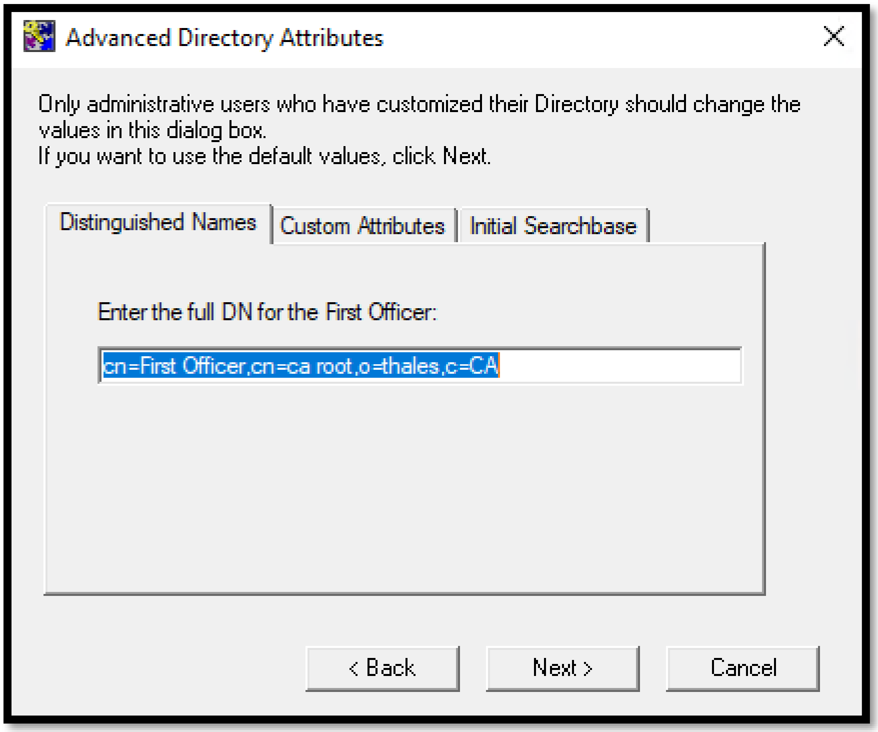
11. A **Bind Result** dialog will display indicating that the bind was successful. Click **OK**.



Bind Result

Bind succeeded.

12. The **Advanced Directory Attributes** dialog will display. Accept the defaults. Click **Next**.



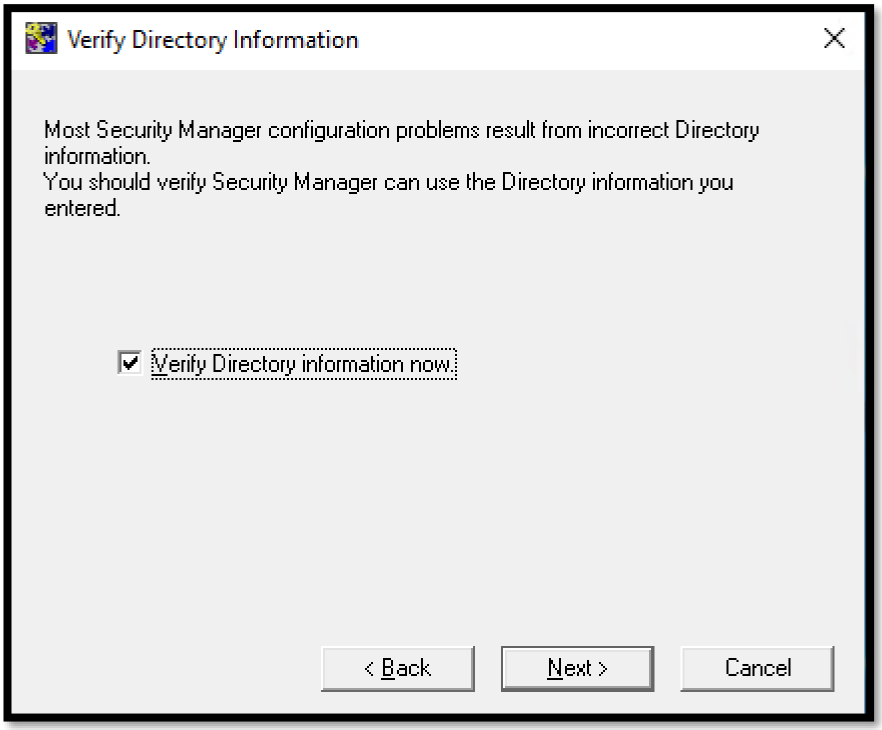
Advanced Directory Attributes

Only administrative users who have customized their Directory should change the values in this dialog box.
If you want to use the default values, click Next.

Enter the full DN for the First Officer:

cn=First Officer,cn=ca root,o=thales,c=CA

13. The **Verify Directory Information** dialog will display. Accept the default to verify the directory. Click **Next**.

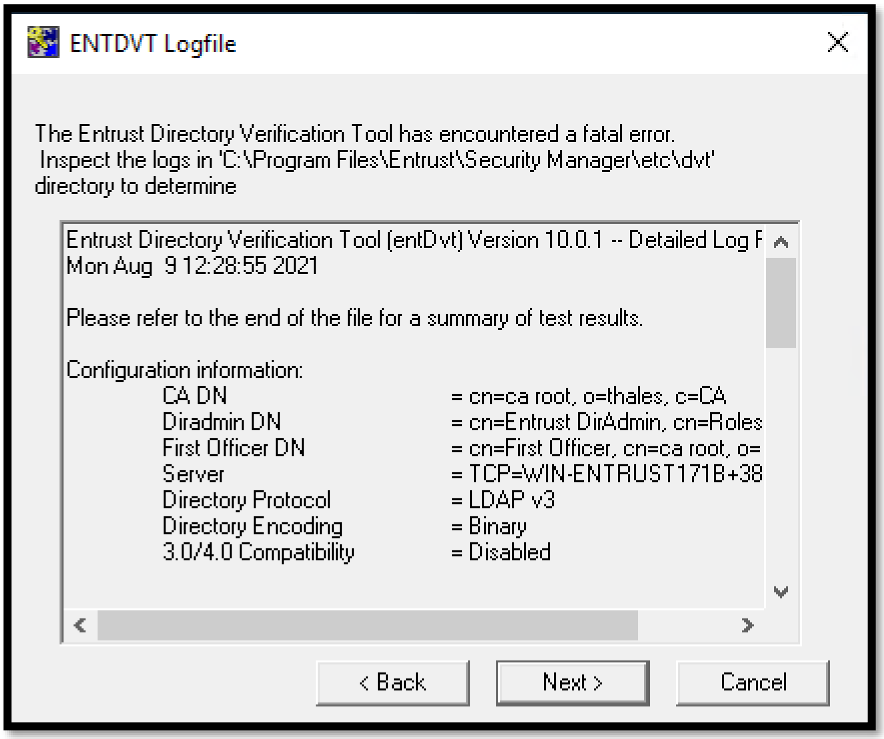


Verify Directory Information

Most Security Manager configuration problems result from incorrect Directory information.
You should verify Security Manager can use the Directory information you entered.

☑ Verify Directory information now.

14. The **ENTDVT Logfile** dialog will display with the results of the directory test. Scroll to the end of the results. No fatal errors, errors or notes should be recorded. If there are errors, these will need to be resolved after reviewing the details of the log. When there are no errors, click **Next**.

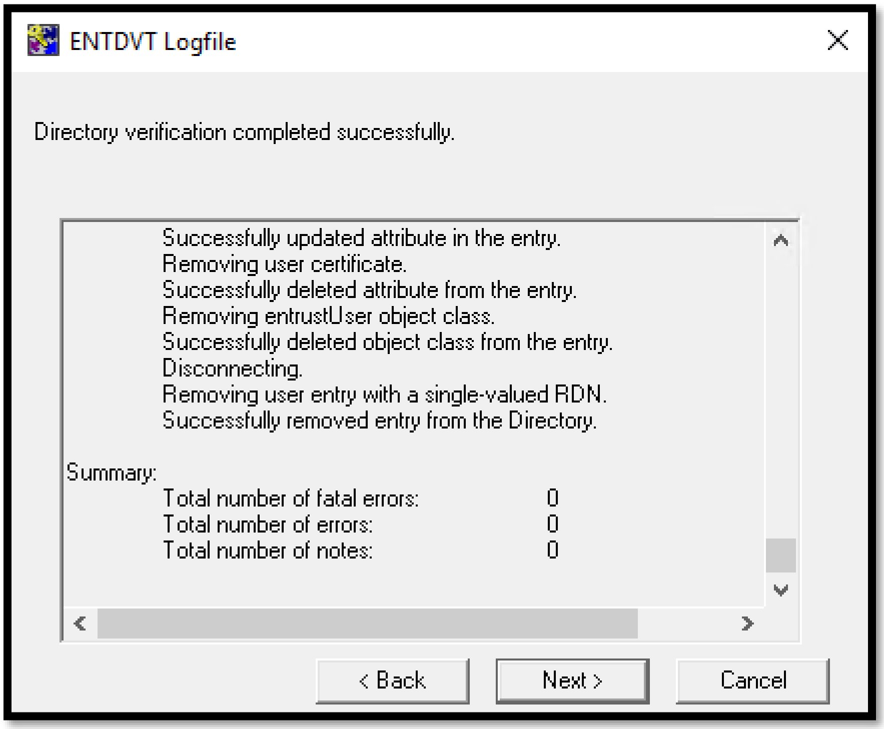


The Entrust Directory Verification Tool has encountered a fatal error.
 Inspect the logs in 'C:\Program Files\Entrust\Security Manager\etc\dvt' directory to determine

```
Entrust Directory Verification Tool (entDvt) Version 10.0.1 -- Detailed Log F
Mon Aug  9 12:28:55 2021

Please refer to the end of the file for a summary of test results.

Configuration information:
            CA DN                              = cn=ca root, o=thales, c=CA
            Diradmin DN                        = cn=Entrust DirAdmin, cn=Roles
            First Officer DN                   = cn=First Officer, cn=ca root, o=
            Server                             = TCP=WIN-ENTRUST171B+38
            Directory Protocol                 = LDAP v3
            Directory Encoding                 = Binary
            3.0/4.0 Compatibility              = Disabled
```

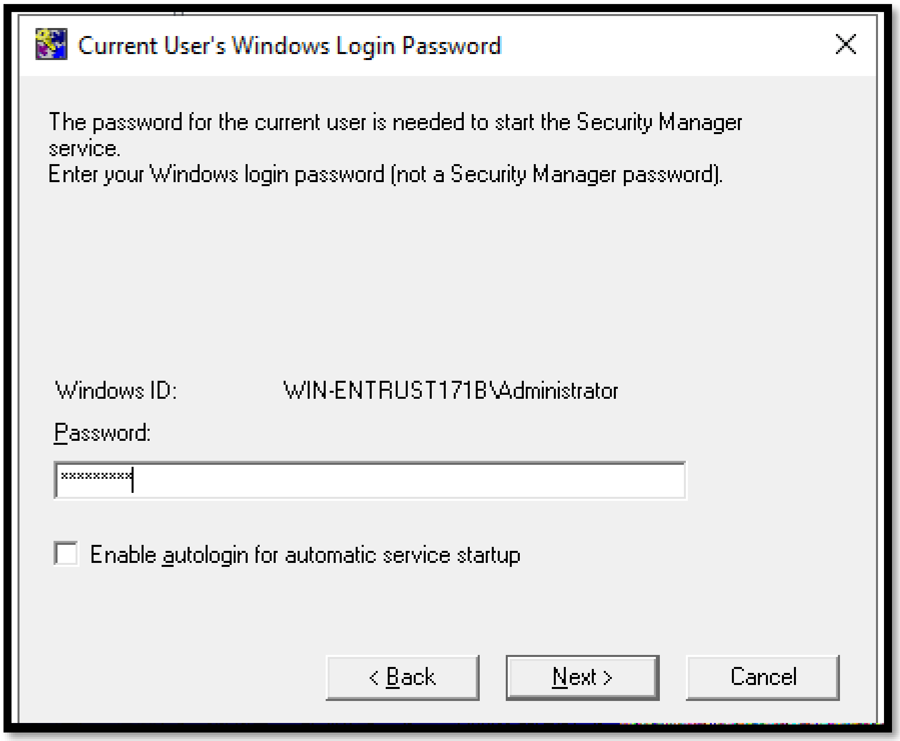


Directory verification completed successfully.

```
            Successfully updated attribute in the entry.
            Removing user certificate.
            Successfully deleted attribute from the entry.
            Removing entrustUser object class.
            Successfully deleted object class from the entry.
            Disconnecting.
            Removing user entry with a single-valued RDN.
            Successfully removed entry from the Directory.

Summary:
            Total number of fatal errors:          0
            Total number of errors:                0
            Total number of notes:                 0
```

15. The **Current User's Windows Login Password** dialog will display. Enter the current Windows user's password. Click **Next**.



Current User's Windows Login Password

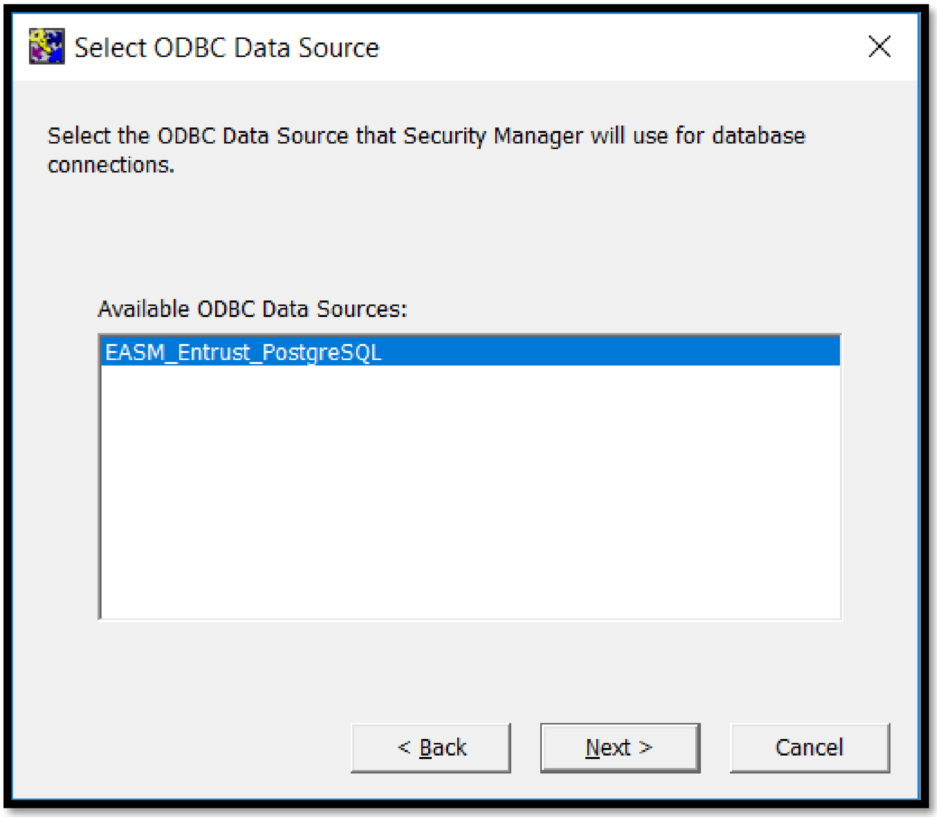
The password for the current user is needed to start the Security Manager service.
Enter your Windows login password (not a Security Manager password).

Windows ID: WIN-ENTRUST171B\Administrator

Password: *********

□ Enable autologin for automatic service startup

16. The **Select ODBC Data Source** dialog will display. Click **Next**.



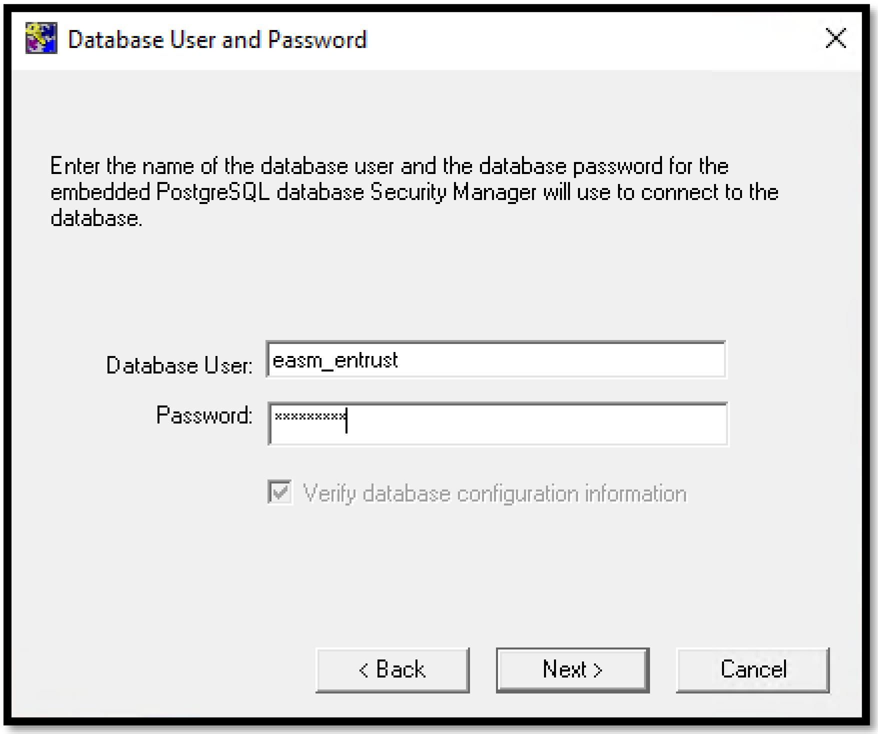
Select ODBC Data Source

Select the ODBC Data Source that Security Manager will use for database connections.

Available ODBC Data Sources:

EASM_Entrust_PostgreSQL

17. The **Database User and Password** dialog will display. Enter the password that was created for the easm_entrust PostgreSQL user during the Entrust Postgres installation. Click **Next**.



Database User and Password

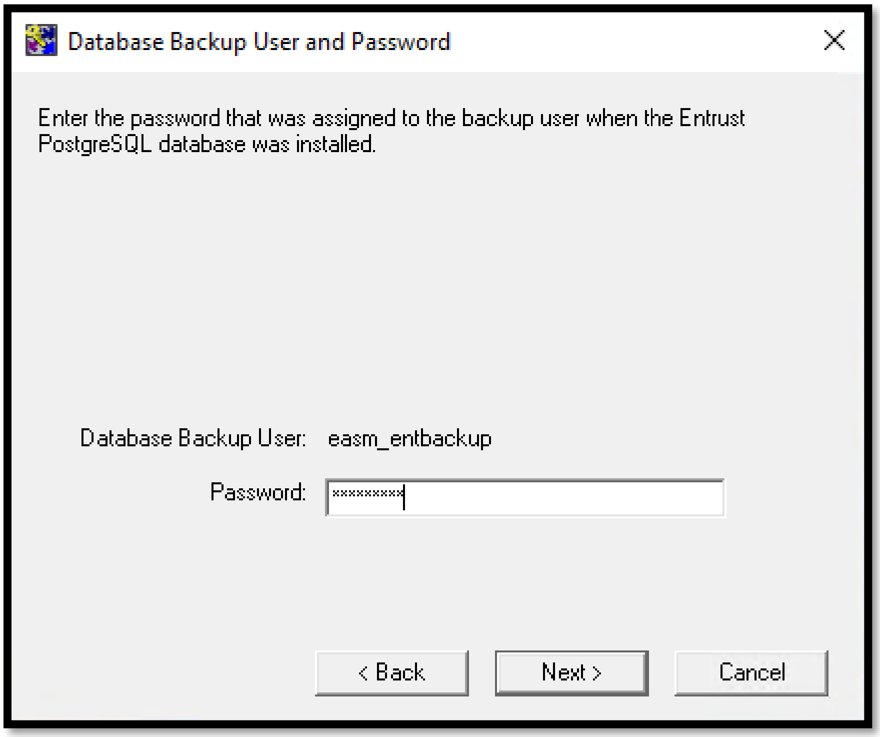
Enter the name of the database user and the database password for the embedded PostgreSQL database Security Manager will use to connect to the database.

Database User: easm_entrust

Password: *********

☑ Verify database configuration information

18. The **Database Backup User and Password** dialog will display. Enter the password that was created for the easm_entbackup PostgreSQL user from the Entrust Postgres installation. Click **Next**.



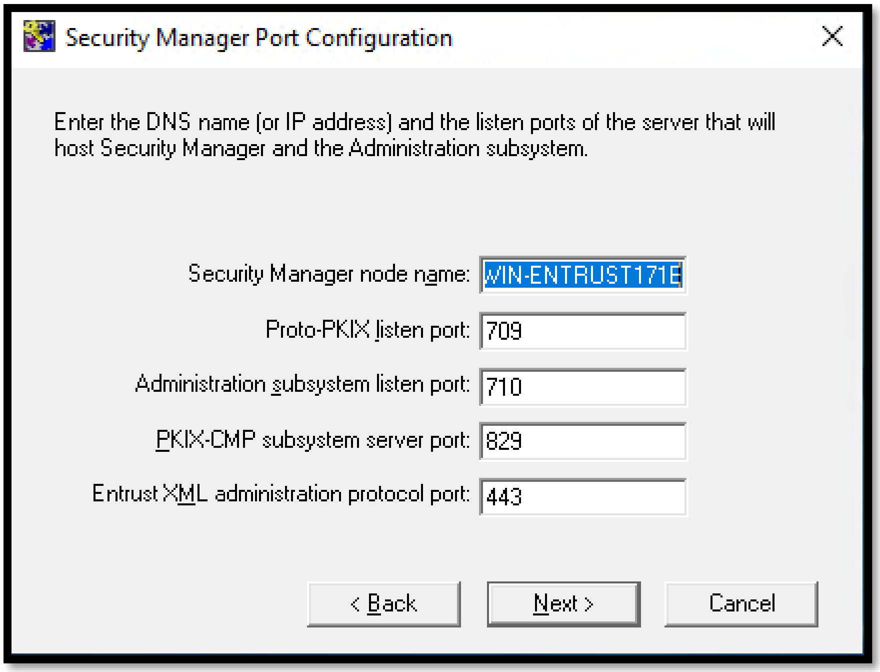
Database Backup User and Password

Enter the password that was assigned to the backup user when the Entrust PostgreSQL database was installed.

Database Backup User: easm_entbackup

Password: *********

19. Set the desired **Security Manager Port Configuration** values and click **Next**.



Security Manager Port Configuration

Enter the DNS name (or IP address) and the listen ports of the server that will host Security Manager and the Administration subsystem.

Security Manager node name: WIN-ENTRUST171E

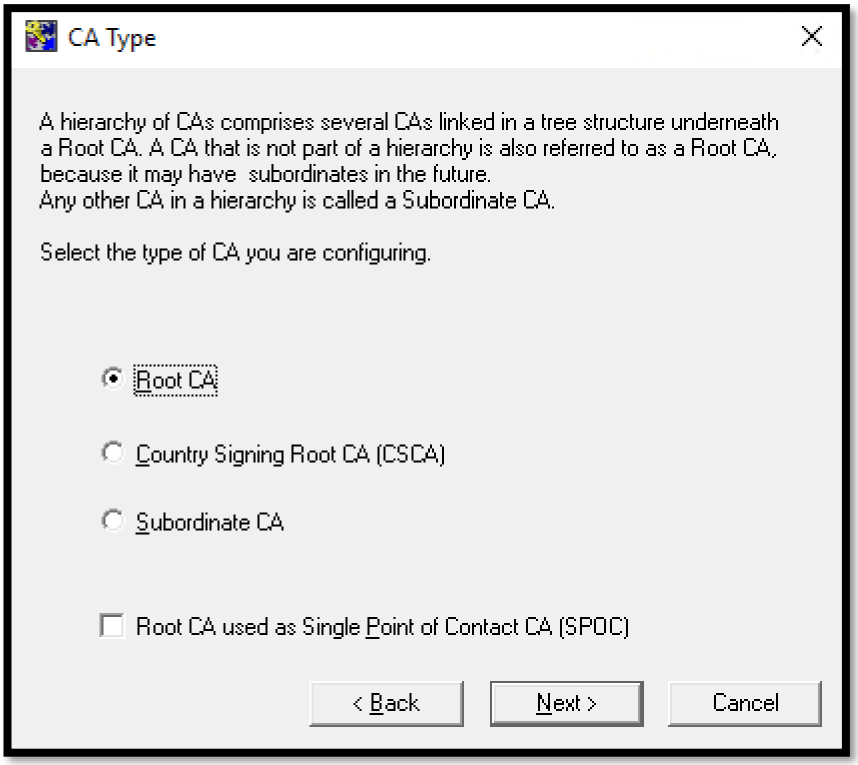
Proto-PKIX listen port: 709

Administration subsystem listen port: 710

PKIX-CMP subsystem server port: 829

Entrust XML administration protocol port: 443

20. Set the **CA Type** value and click **Next**.



CA Type

A hierarchy of CAs comprises several CAs linked in a tree structure underneath a Root CA. A CA that is not part of a hierarchy is also referred to as a Root CA, because it may have subordinates in the future.
Any other CA in a hierarchy is called a Subordinate CA.

Select the type of CA you are configuring.

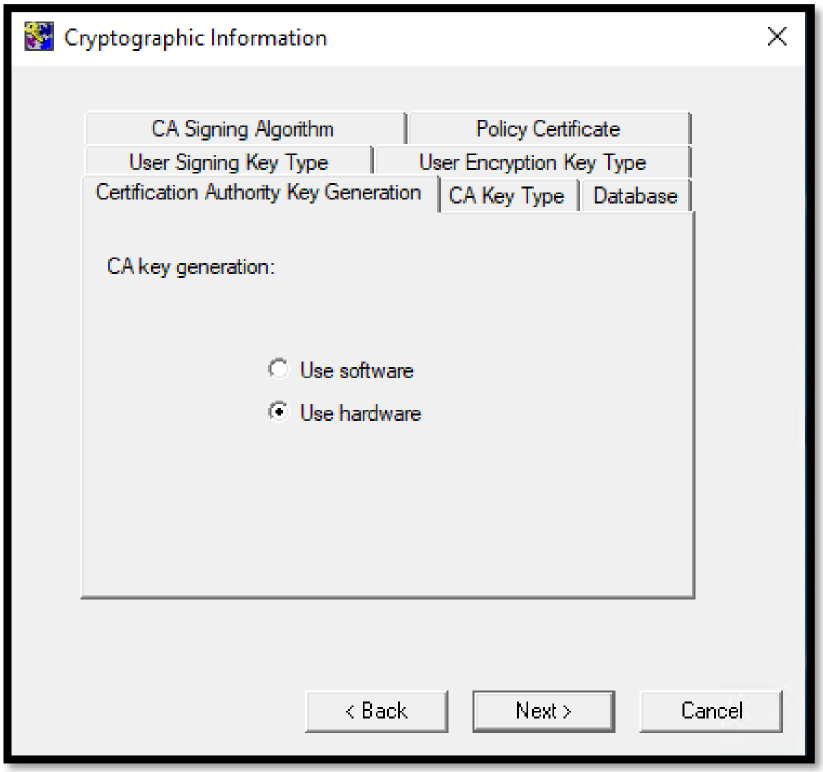
● Root CA

○ Country Signing Root CA (CSCA)

○ Subordinate CA

☐ Root CA used as Single Point of Contact CA (SPOC)

21. The **Cryptographic Information** dialog will display with the **Certification Authority Key Generation** tab selected. Select **Use hardware**, and click **Next**.

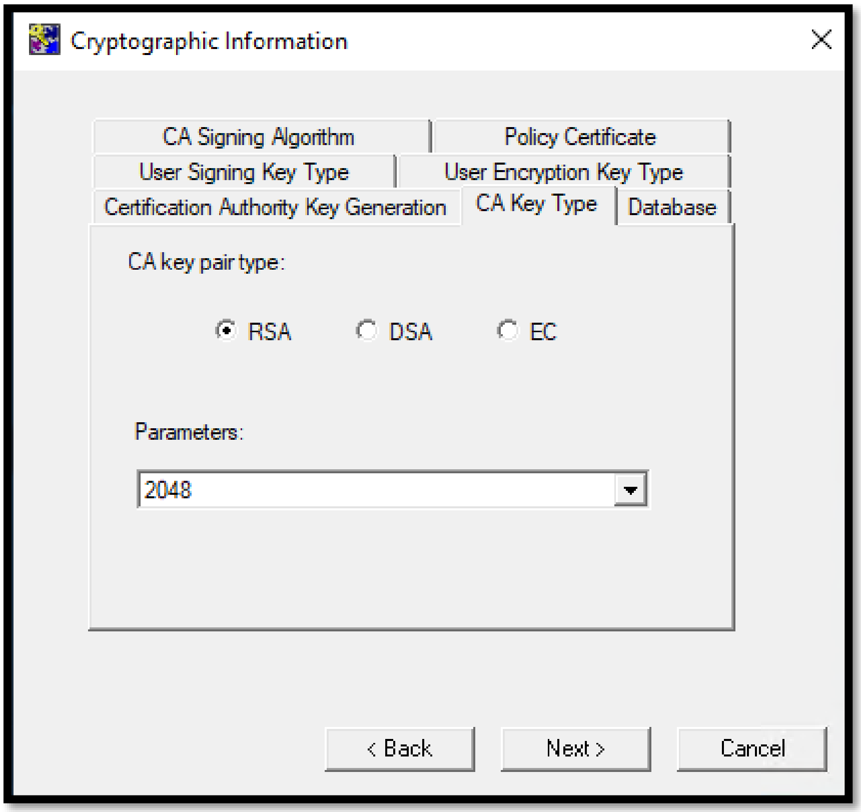


CA key generation:

○ Use software

● Use hardware

22. The **CA Key Type tab** defines the CA key pair type and parameters. Select the desired CA key pair type and parameter. Click **Next**.



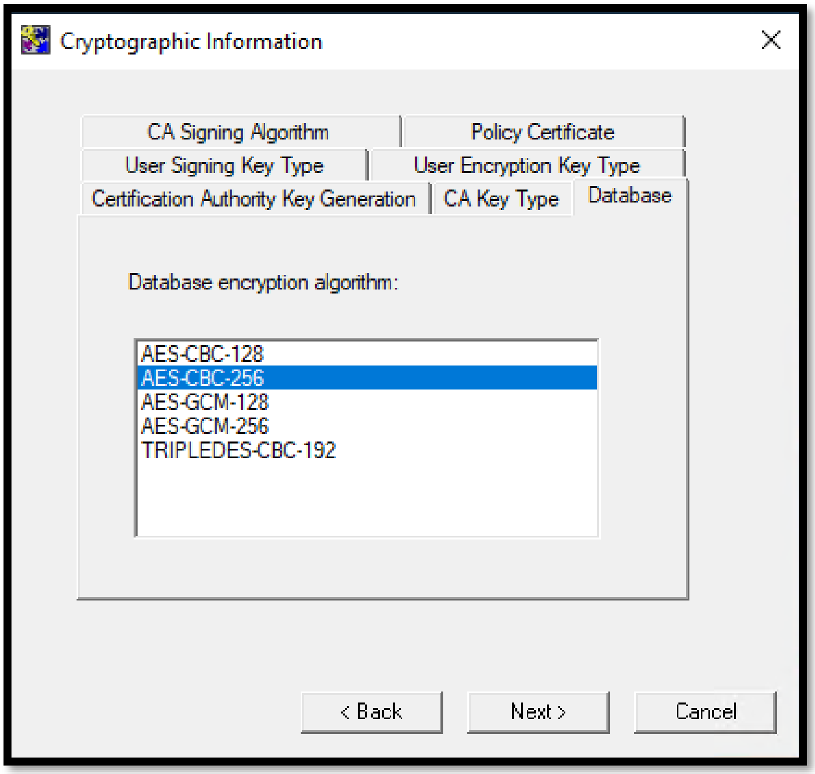
CA key pair type:

● RSA ○ DSA ○ EC

Parameters:

2048

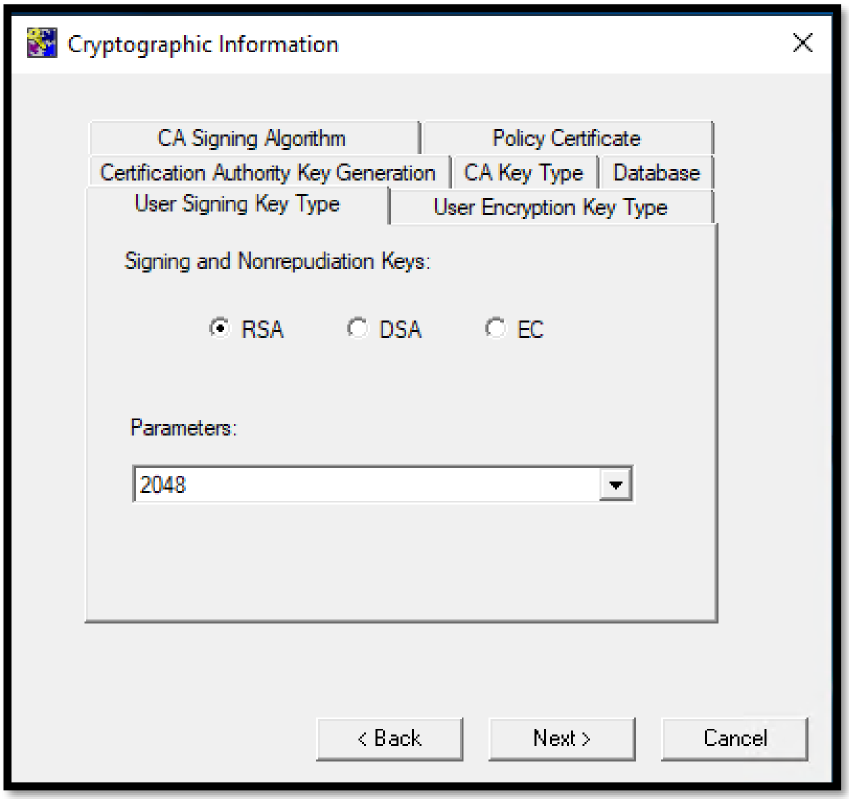
23. On the **Database** tab, select the desired database encryption algorithm. Click **Next**.



Database encryption algorithm:

AES-CBC-128
AES-CBC-256
AES-GCM-128
AES-GCM-256
TRIPLEDES-CBC-192

24. The **User Signing Key Type** tab defines the key pair type and parameters for user signing keys. Select the desired type and parameter. Click **Next.**



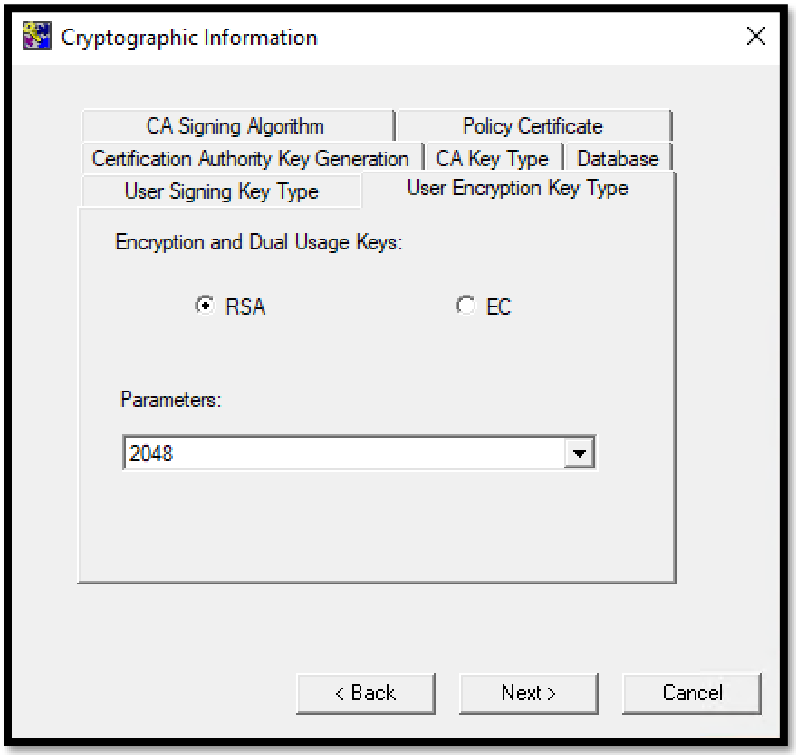
Signing and Nonrepudiation Keys:

● RSA ○ DSA ○ EC

Parameters:

2048

25. The **User Encryption Key Type** tab defines the key pair type and parameters for user encryption keys. Select the desired type and parameter. Click **Next.**



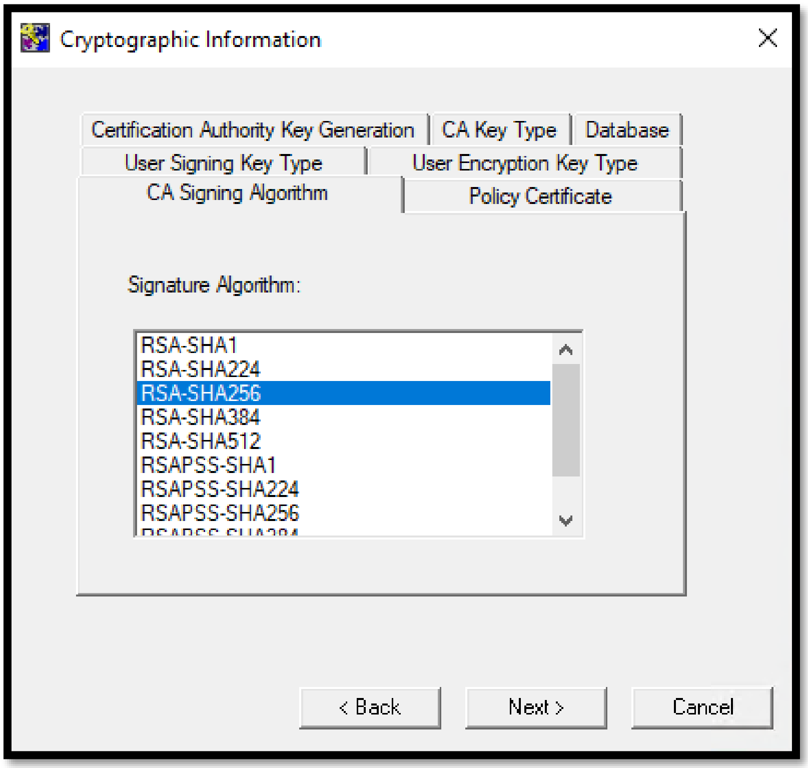
Encryption and Dual Usage Keys:

● RSA ○ EC

Parameters:

2048

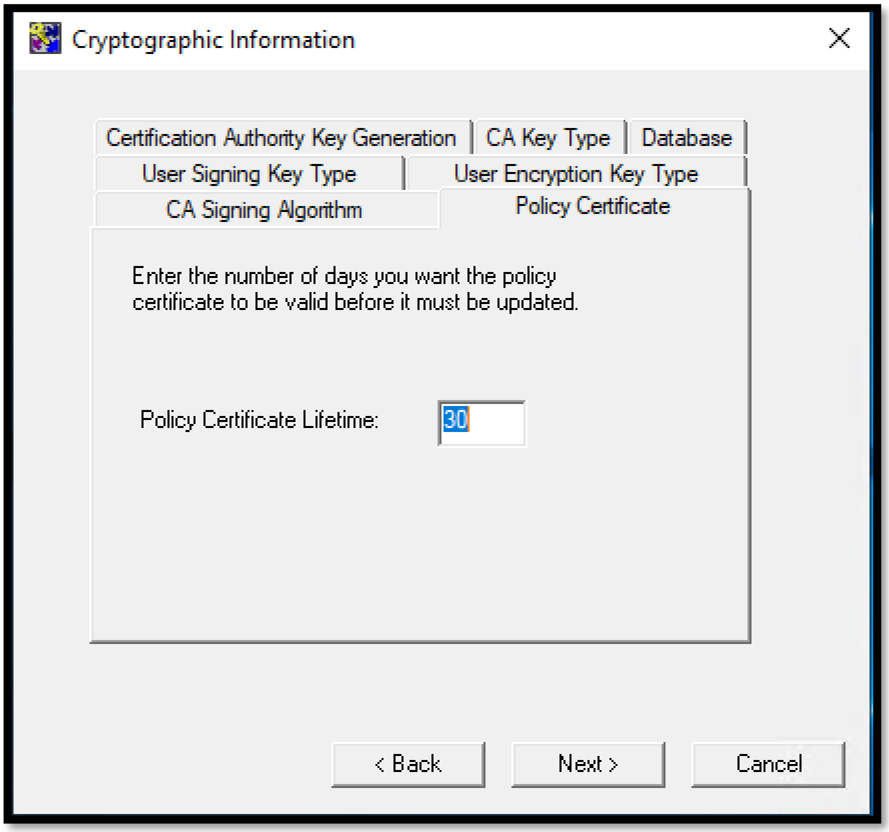
26. On the **CA Signing Algorithm** tab, select the CA Signature Algorithm. Click **Next**.



Signature Algorithm:

RSA-SHA1
RSA-SHA224
RSA-SHA256
RSA-SHA384
RSA-SHA512
RSAPSS-SHA1
RSAPSS-SHA224
RSAPSS-SHA256

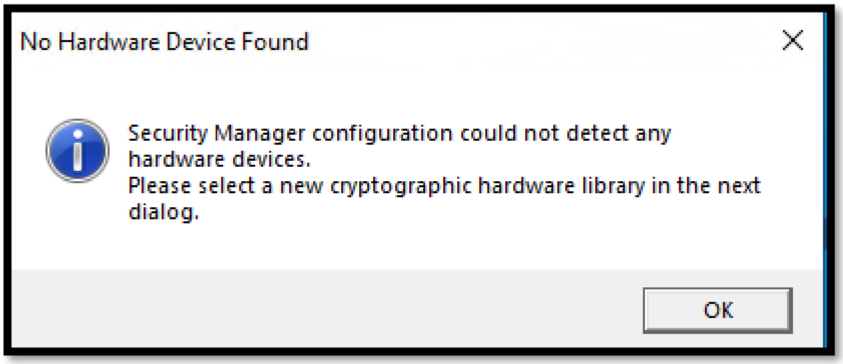
27. On the **Policy Certificate** tab, which defines the lifetime of the Entrust policy certificate, enter the **Policy Certificate Lifetime** value. Click **Next**.



Enter the number of days you want the policy certificate to be valid before it must be updated.

Policy Certificate Lifetime: 30

28. A **No Hardware Device Found** dialog box will display. Click **OK** to proceed with providing Security Manager with the location of the necessary library file.

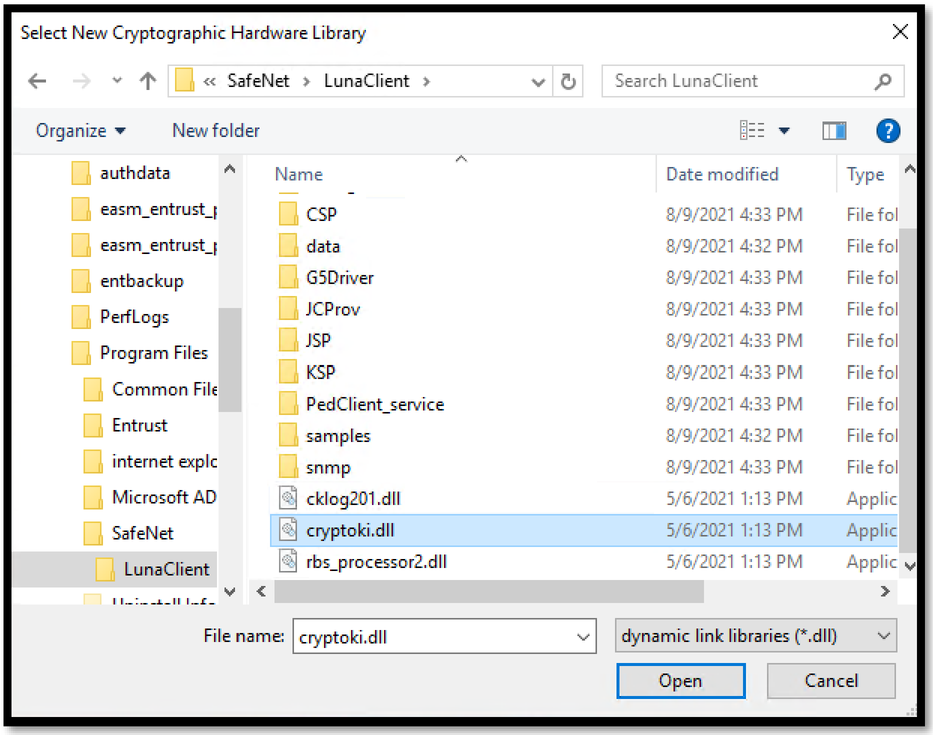


Security Manager configuration could not detect any hardware devices.
Please select a new cryptographic hardware library in the next dialog.

29. In the resulting **Select New Cryptographic Hardware Library** dialog box, navigate to the location of the **cryptoki.dll** library file that Security Manager will use to communicate with the Luna HSM and click **Open**.

    Unless a custom installation path was specified when installing the Luna client, **cryptoki.dll** can be found at the following location:

    ```
    C:\Program Files\SafeNet\LunaClient\cryptoki.dll
    ```

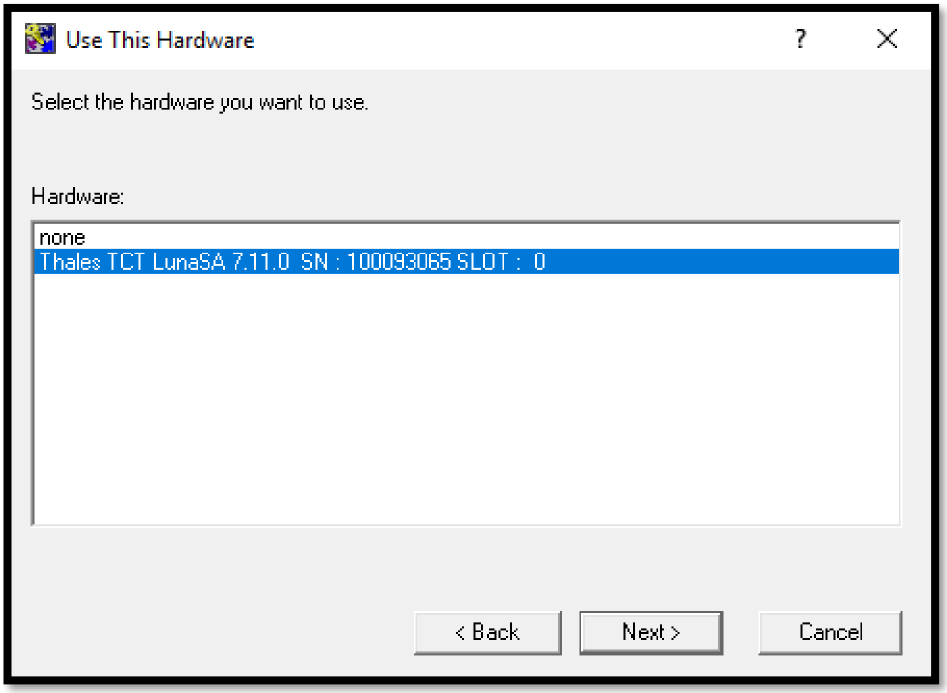


Name	Date modified	Type
CSP	8/9/2021 4:33 PM	File fol
data	8/9/2021 4:32 PM	File fol
G5Driver	8/9/2021 4:33 PM	File fol
JCProv	8/9/2021 4:33 PM	File fol
JSP	8/9/2021 4:33 PM	File fol
KSP	8/9/2021 4:33 PM	File fol
PedClient_service	8/9/2021 4:33 PM	File fol
samples	8/9/2021 4:32 PM	File fol
snmp	8/9/2021 4:33 PM	File fol
cklog201.dll	5/6/2021 1:13 PM	Applic
cryptoki.dll	5/6/2021 1:13 PM	Applic
rbs_processor2.dll	5/6/2021 1:13 PM	Applic

File name: cryptoki.dll

dynamic link libraries (*.dll)

30. On the **Use This Hardware** dialog, the available HSM slot(s) will be listed. Select the desired HSM slot and click **Next**.

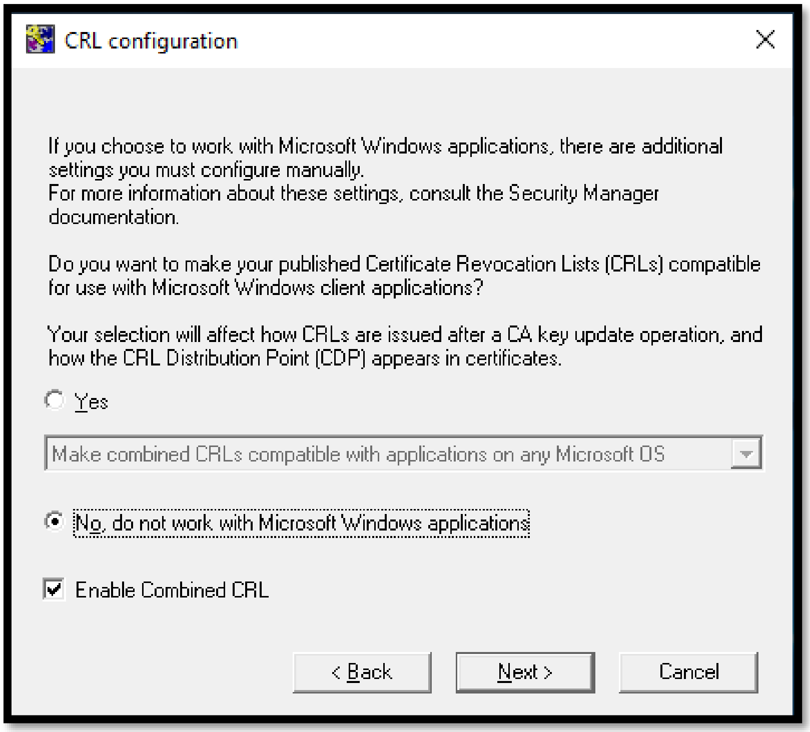


Select the hardware you want to use.

Hardware:

none
Thales TCT LunaSA 7.11.0 SN : 100093065 SLOT : 0

31. On the **CRL Configuration** dialog, select **No, do not work with Microsoft Windows applications**. Click **Next**.



CRL configuration

If you choose to work with Microsoft Windows applications, there are additional settings you must configure manually.
For more information about these settings, consult the Security Manager documentation.

Do you want to make your published Certificate Revocation Lists (CRLs) compatible for use with Microsoft Windows client applications?

Your selection will affect how CRLs are issued after a CA key update operation, and how the CRL Distribution Point (CDP) appears in certificates.

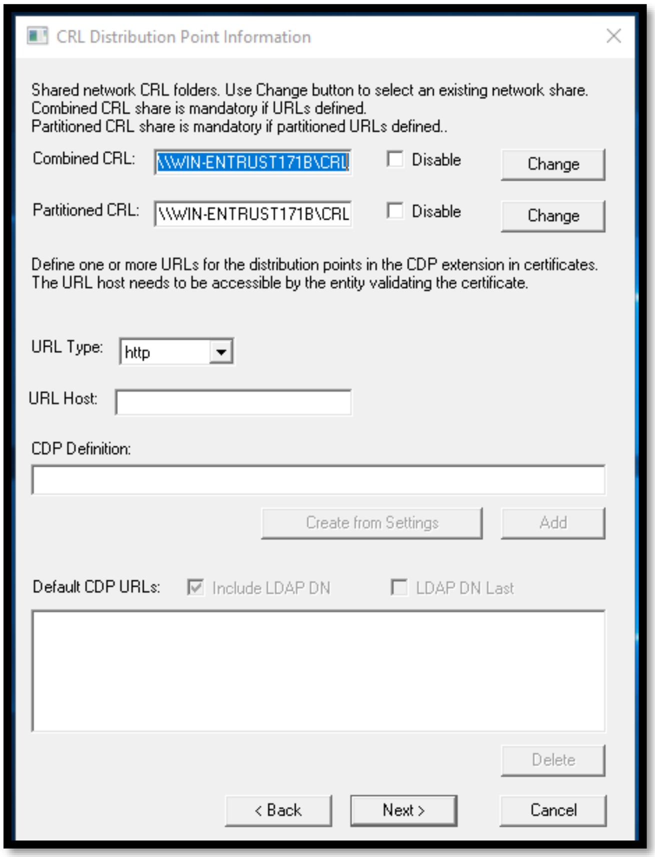
○ Yes

Make combined CRLs compatible with applications on any Microsoft OS

● No, do not work with Microsoft Windows applications

☑ Enable Combined CRL

32. The **CRL Distribution Point Information** dialog will display. Click **Next**.



CRL Distribution Point Information

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

Combined CRL: \\WIN-ENTRUST171B\CRL □ Disable

Partitioned CRL: \\WIN-ENTRUST171B\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.

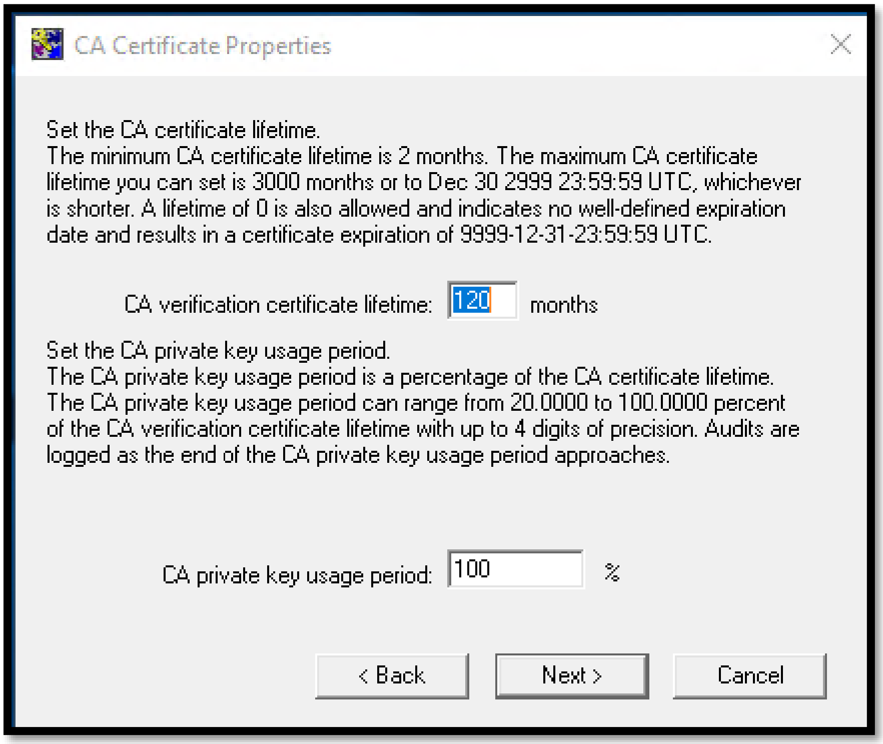
URL Type: http

URL Host:

CDP Definition:

Default CDP URLs: ☑ Include LDAP DN □ LDAP DN Last

33. Set the desired **CA Certificate Properties** values. Click **Next**



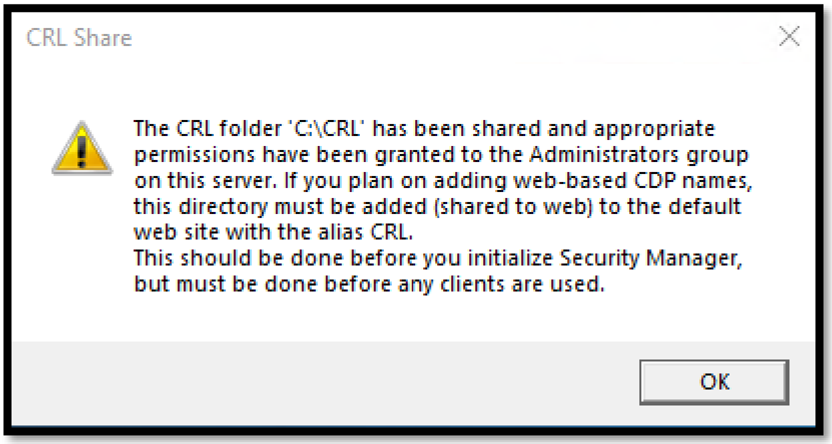
Set the CA certificate lifetime.
The minimum CA certificate lifetime is 2 months. The maximum CA certificate lifetime you can set is 3000 months or to Dec 30 2999 23:59:59 UTC, whichever is shorter. A lifetime of 0 is also allowed and indicates no well-defined expiration date and results in a certificate expiration of 9999-12-31-23:59:59 UTC.

CA verification certificate lifetime: 120 months

Set the CA private key usage period.
The CA private key usage period is a percentage of the CA certificate lifetime. The CA private key usage period can range from 20.0000 to 100.0000 percent of the CA verification certificate lifetime with up to 4 digits of precision. Audits are logged as the end of the CA private key usage period approaches.

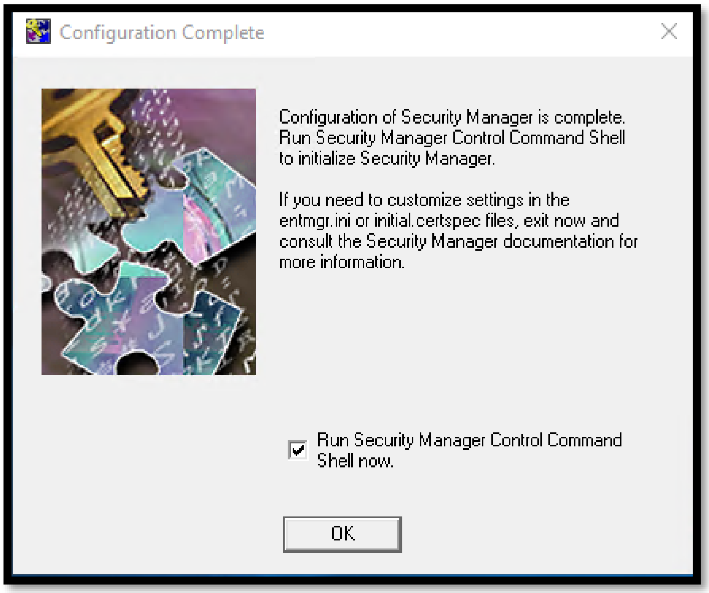
CA private key usage period: 100 %

34. A **CRL Share** warning dialog will display indicating a share for C:\CRL has been created. Click **OK**.



The CRL folder 'C:\CRL' has been shared and appropriate permissions have been granted to the Administrators group on this server. If you plan on adding web-based CDP names, this directory must be added (shared to web) to the default web site with the alias CRL.
This should be done before you initialize Security Manager, but must be done before any clients are used.

35. The **Configuration Complete** dialog box will be displayed. Check the **Run Security Manager Control Shell now** option. Click **OK** to complete the configuration process.

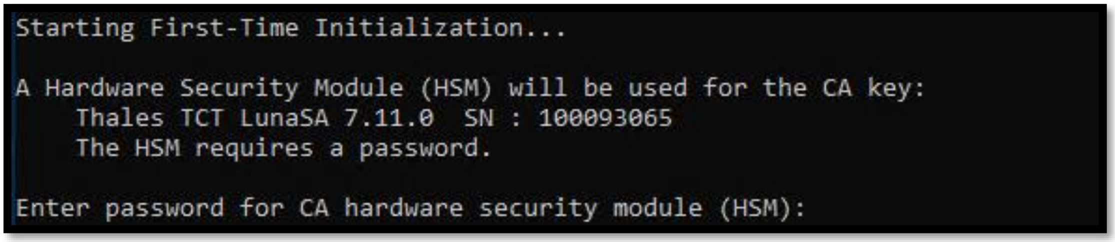


Configuration of Security Manager is complete. Run Security Manager Control Command Shell to initialize Security Manager.

If you need to customize settings in the entmgr.ini or initial.certspec files, exit now and consult the Security Manager documentation for more information.

☑ Run Security Manager Control Command Shell now.

36. The Security Manager Control Command Shell will launch and begin the CA initialization process. Entrust Authority Security Manager detects the hardware, and requests the hardware password in order to generate the CA keys on the Luna HSM. Enter the HSM partition password.

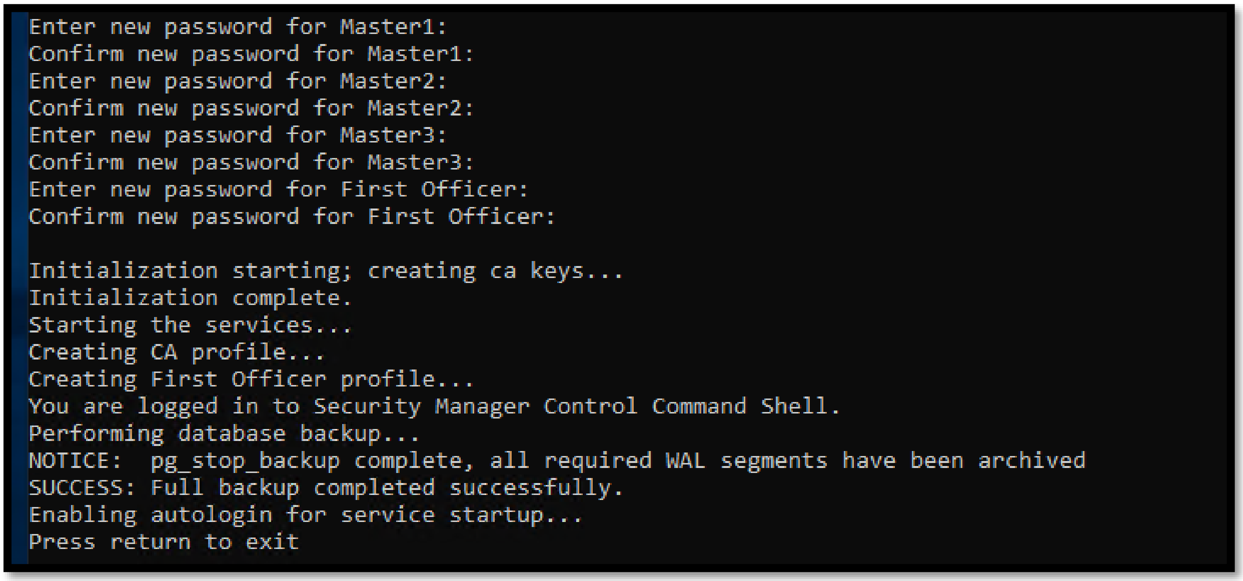


```
Starting First-Time Initialization...

A Hardware Security Module (HSM) will be used for the CA key:
    Thales TCT LunaSA 7.11.0  SN : 100093065
    The HSM requires a password.

Enter password for CA hardware security module (HSM):
```

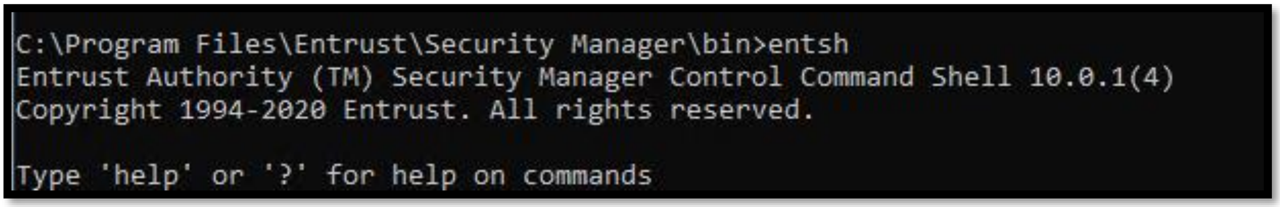
37. Create and confirm the passwords for the necessary Entrust Security Manager Accounts. When complete, press return to exit the initialization script.



```
Enter new password for Master1:
Confirm new password for Master1:
Enter new password for Master2:
Confirm new password for Master2:
Enter new password for Master3:
Confirm new password for Master3:
Enter new password for First Officer:
Confirm new password for First Officer:

Initialization starting; creating ca keys...
Initialization complete.
Starting the services...
Creating CA profile...
Creating First Officer profile...
You are logged in to Security Manager Control Command Shell.
Performing database backup...
NOTICE:  pg_stop_backup complete, all required WAL segments have been archived
SUCCESS: Full backup completed successfully.
Enabling autologin for service startup...
Press return to exit
```

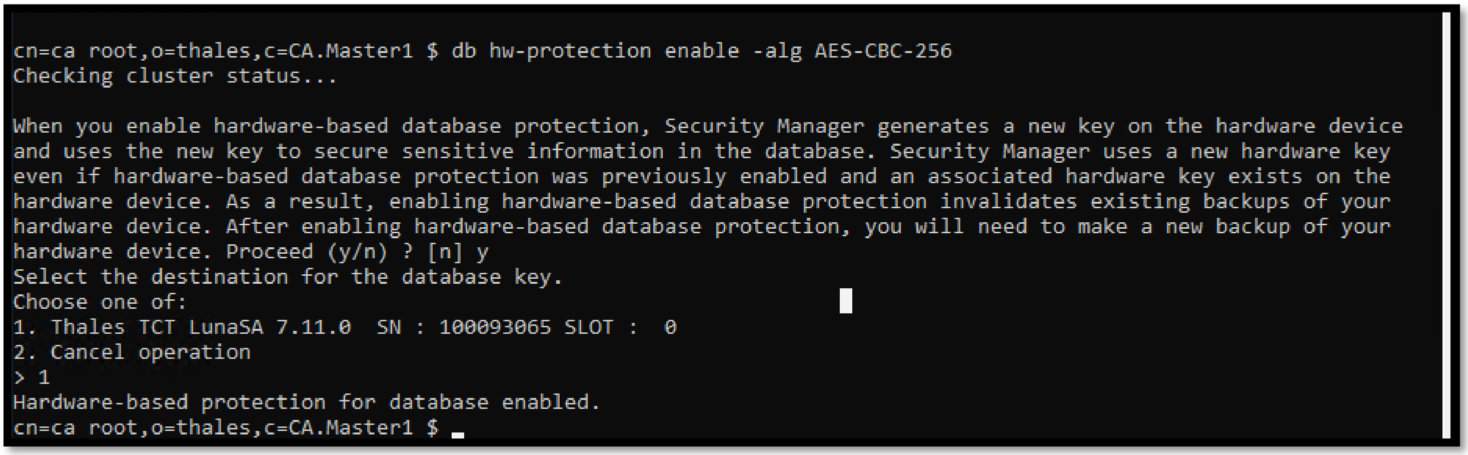
38. To re-open the Security Manager Control Command Shell, **run entsh.exe**, found in the C:\Program Files\Entrust\Security Manager\bin directory.. Log in to continue configuring or using Security Manager.



```
C:\Program Files\Entrust\Security Manager\bin>entsh
Entrust Authority (TM) Security Manager Control Command Shell 10.0.1(4)
Copyright 1994-2020 Entrust. All rights reserved.

Type 'help' or '?' for help on commands
```

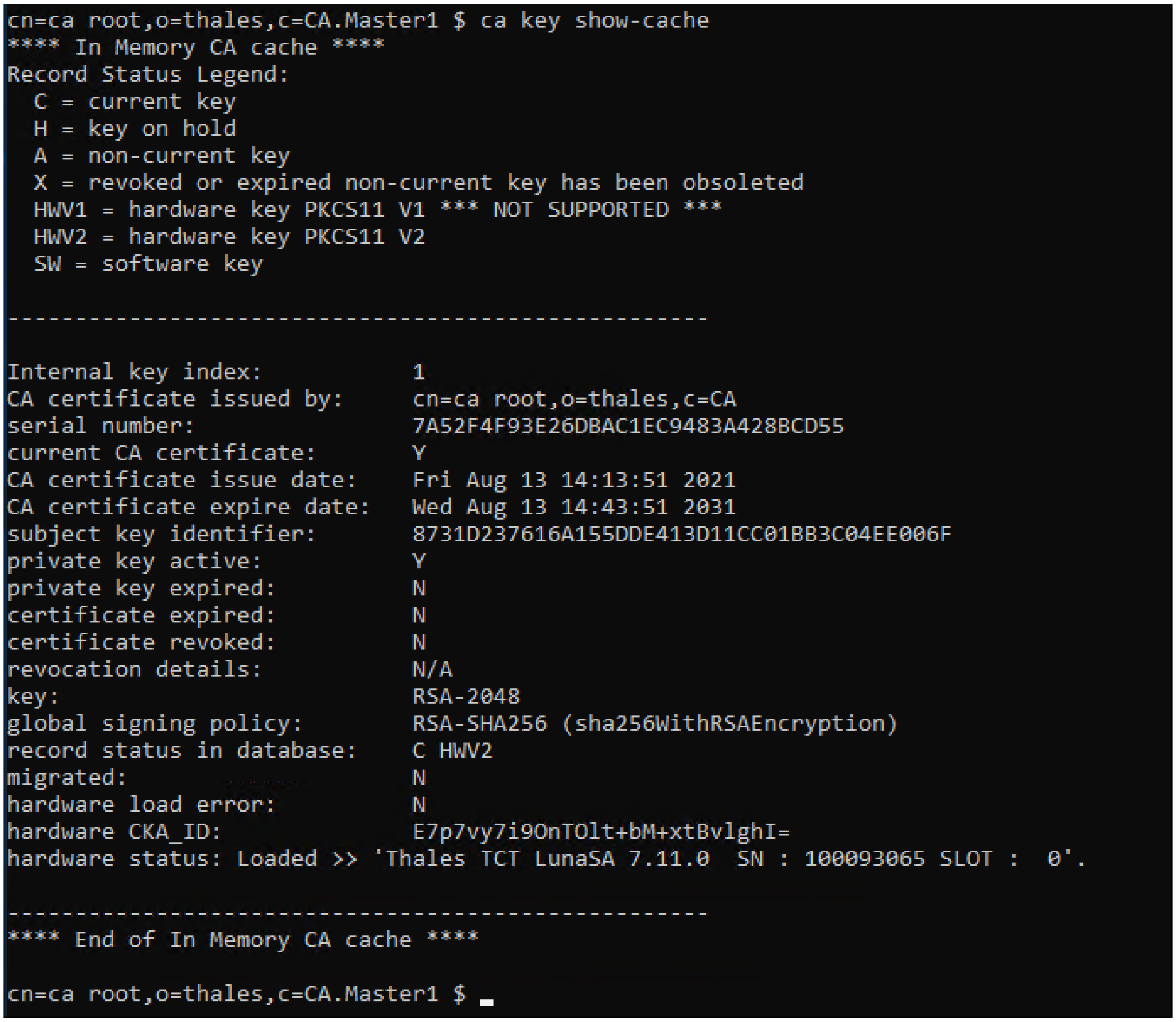
39. To use the HSM for hardware protection of sensitive information in the database, issue the command **`db hw-protection enable -alg <algorithm>.`** After enabling hardware protection, the HSM password is required when logging in to the Control Command Shell.



```
cn=ca root,o=thales,c=CA.Master1 $ db hw-protection enable -alg AES-CBC-256
Checking cluster status...

When you enable hardware-based database protection, Security Manager generates a new key on the hardware device
and uses the new key to secure sensitive information in the database. Security Manager uses a new hardware key
even if hardware-based database protection was previously enabled and an associated hardware key exists on the
hardware device. As a result, enabling hardware-based database protection invalidates existing backups of your
hardware device. After enabling hardware-based database protection, you will need to make a new backup of your
hardware device. Proceed (y/n) ? [n] y
Select the destination for the database key.
Choose one of:
1. Thales TCT LunaSA 7.11.0  SN : 100093065 SLOT :  0
2. Cancel operation
> 1
Hardware-based protection for database enabled.
cn=ca root,o=thales,c=CA.Master1 $ _
```

40. Keys may be confirmed on the Luna HSM either through the Security Manager Control Command Shell or through the Luna HSM utilities directly.



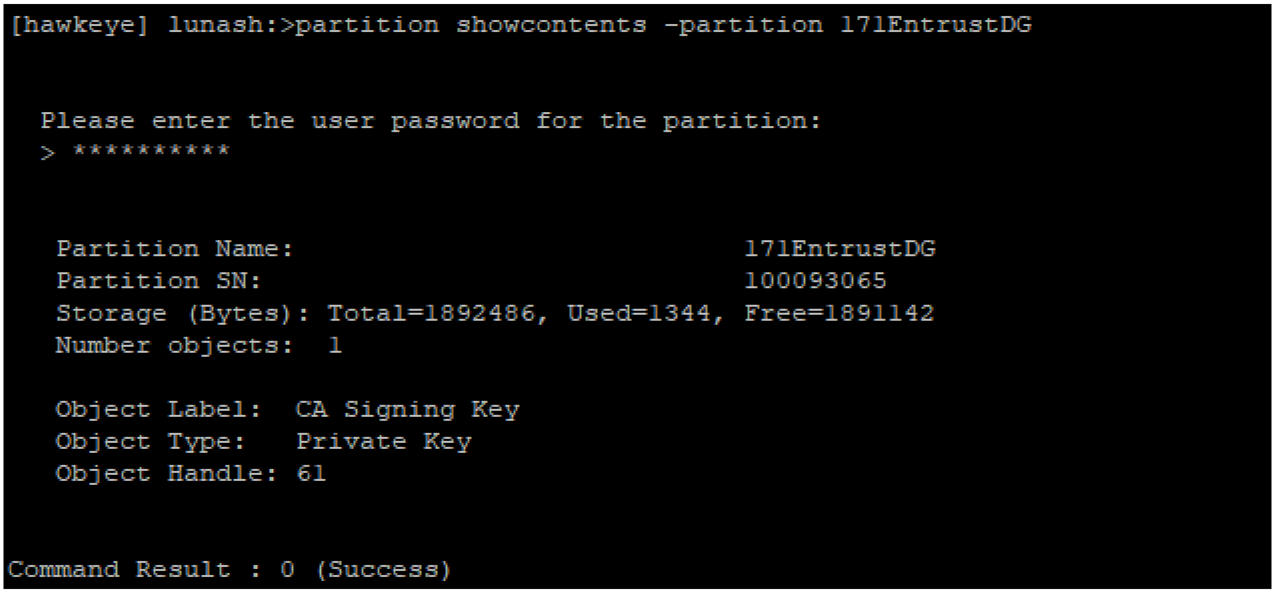
```
cn=ca root,o=thales,c=CA.Master1 $ ca key show-cache
**** In Memory CA cache ****
Record Status Legend:
  C = current key
  H = key on hold
  A = non-current key
  X = revoked or expired non-current key has been obsoleted
  HWV1 = hardware key PKCS11 V1 *** NOT SUPPORTED ***
  HWV2 = hardware key PKCS11 V2
  SW = software key

----------------------------------------------------

Internal key index:           1
CA certificate issued by:     cn=ca root,o=thales,c=CA
serial number:                7A52F4F93E26DBAC1EC9483A428BCD55
current CA certificate:       Y
CA certificate issue date:    Fri Aug 13 14:13:51 2021
CA certificate expire date:   Wed Aug 13 14:43:51 2031
subject key identifier:       8731D237616A155DDE413D11CC01BB3C04EE006F
private key active:           Y
private key expired:          N
certificate expired:          N
certificate revoked:          N
revocation details:           N/A
key:                          RSA-2048
global signing policy:        RSA-SHA256 (sha256WithRSAEncryption)
record status in database:    C HWV2
migrated:                     N
hardware load error:          N
hardware CKA_ID:              E7p7vy7i9OnTOlt+bM+xtBvlghI=
hardware status: Loaded >> 'Thales TCT LunaSA 7.11.0  SN : 100093065 SLOT :  0'.

----------------------------------------------------
**** End of In Memory CA cache ****

cn=ca root,o=thales,c=CA.Master1 $ _
```



```
[hawkeye] lunash:>partition showcontents -partition 171EntrustDG


  Please enter the user password for the partition:
  > **********


   Partition Name:                           171EntrustDG
   Partition SN:                             100093065
   Storage (Bytes): Total=1892486, Used=1344, Free=1891142
   Number objects:  1

   Object Label:  CA Signing Key
   Object Type:   Private Key
   Object Handle: 61


Command Result : 0 (Success)
```