Entrust Certificate Authority

nShield® HSM Integration Guide for Windows Server

2026-10-06

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Product configuration . . . 1
    1.2. Supported nShield hardware and software versions . . . 1
    1.3. Requirements . . . 2
2. Install and configure directory service . . . 3
    2.1. Install directory service . . . 3
    2.2. Configure directory service . . . 3
3. Install and configure the nShield HSM . . . 5
    3.1. Select the protection method . . . 5
    3.2. Install the nShield HSM . . . 5
    3.3. Install the nShield Security World Software and create the Security World . . . 5
    3.4. Create the OCS or Softcard . . . 6
4. Install the Entrust Certificate Authority . . . 9
    4.1. Install the Entrust Certificate Authority PostgreSQL . . . 9
    4.2. Install the Entrust Certificate Authority . . . 11
5. Configure the Entrust Certificate Authority . . . 13
    5.1. Establish a preload session . . . 13
    5.2. Configure the Entrust nShield Edge . . . 16
    5.3. Configure the Entrust Certificate Authority . . . 16
6. Test the integration . . . 34
    6.1. Initialize the Certificate Authority . . . 34
    6.2. Launch the Certificate Authority shell . . . 34
    6.3. Verify the in-memory CA key cache . . . 34
    6.4. Verify the hardware information . . . 35
    6.5. Import the CA key pair from software to hardware . . . 36
    6.6. Export the CA key pair from hardware to software . . . 37
    6.7. Back up nShield Security World files . . . 38
7. Troubleshooting . . . 39
    7.1. (-8973) Could not connect to the Entrust Certificate Authority service. Certificate Authority service may not be running . . . 39
    7.2. Error encountered querying CA hardware . . . 39
    7.3. (-77) Problem reported with crypto hardware . . . 39
    7.4. (-2229) An error occurred. Check the service status and manager logs for details . . . 40
    7.5. HSM logs show errors for algorithms not configured . . . 40
    7.6. No hardware device found . . . 40
    7.7. (-2684) General hardware error . . . 41

7.8. Entrust nShield Edge cluster status "down" or "unknown" . . . 41
7.9. pg_port error . . . 41
8. Additional resources and related products . . . 43
8.1. nShield HSMs . . . 43
8.2. nShield as a Service . . . 43
8.3. Entrust products . . . 43
8.4. nShield product documentation . . . 43

Chapter 1. Introduction

The Entrust Certificate Authority is a Public-Key Infrastructure (PKI) solution. The Entrust nShield Hardware Security Module (HSM) securely stores and manages encryption keys. This document describes how to integrate them to strengthen your PKI's security.

The Entrust nShield HSM is available as an appliance or nShield as a service (nSaaS).

Where procedures differ for post-quantum (PQ) workflows, this guide calls out the PQ-specific steps at the relevant points.

1.1. Product configuration

The integration between the Entrust nShield HSM and Entrust Certificate Authority has been successfully tested in the following configurations:

Product	Version
Entrust Certificate Authority	v11.0.1
Operating System	Windows Server 2025
PostgreSQL Database	15.18.0

1.2. Supported nShield hardware and software versions

The integration was successfully tested with several nShield hardware and software versions.

OCS and Softcard protection were tested in all configurations. Module-protected keys are not supported in Entrust Security Manager v10.0 and later versions.

1.2.1. Post-quantum testing

HSM	Security World Software	Firmware	Netimage	FIPS Level 3
nShield 5c	13.9.6 (STS6)	13.8.6	13.9.6	No
Connect XC	13.9.6 (STS6)	13.8.5	13.9.6	No

1.2.2. Strict FIPS (FIPS Level 3)

HSM	Security World Software	Firmware	Netimage	Note
nShield 5c	13.6.18 (LTS8)	13.4.5 (FIPS 140-3 certified)	13.6.18	Strict FIPS
Connect XC	13.6.18 (LTS8)	12.72.4 (FIPS 140-2 certified)	13.6.18	Strict FIPS

1.3. Requirements

To integrate the Entrust Certificate Authority and the Entrust nShield HSM, you need:

- Access to the Entrust TrustedCare Portal.
- A directory service. See *SIC-Entrust Certificate Authority 10.2.pdf* located in the **Documents** tab at Product Support Center for Authority for supported directories.
- A dedicated server or virtual appliance for the installation.

Familiarize yourself with:

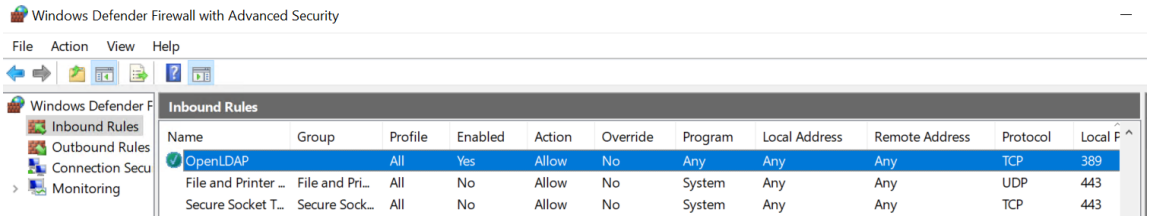
- The Entrust Certificate Authority documentation in the **Documents** tab of Product Support Center for Authority.
- The Entrust nShield Product Documentation.
- Your organizational Certificate Policy, Certificate Practice Statement, and security policy or procedure for PKI and HSM administration:
  - The number and quorum of administrator cards in the Administrator Card Set (ACS) and the policy for managing these cards.
  - The number and quorum of operator cards in the Operator Card Set (OCS) and the policy for managing these cards.
  - The key protection methods: Module, Softcard, or OCS.
  - The level of compliance for the Security World, FIPS 140 Level 3.
  - Key attributes, such as key size, timeout, and any other attributes needed to audit key usage.

Chapter 2. Install and configure directory service

2.1. Install directory service

The Certificate Authority requires a directory service that supports LDAP (Lightweight Directory Access Protocol) or a third-party LDAP-compliant X.500 directory. A remote OpenLDAP directory service with a self-signed certificate was used in this integration. See Product Support Center for Authority for a list of supported directory services.

1. Install the required LDAP client tools on the Certificate Authority server.
2. In the firewall rules on the server hosting the directory service, allow inbound traffic from the Certificate Authority server on port 389.



2.2. Configure directory service

The Certificate Authority directory schema configuration is described in Entrust Certificate Authority.

1. Implement the configuration corresponding to your directory service.

   The following directory service parameters are used in this integration:

   - Top Level DN: `dc=entrustsm,dc=local`
   - CA Directory Location: `ou=CAentry,dc=entrustsm,dc=local`
   - Directory Administrator: `cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local`
   - First Officer: `cn=FirstOfficer,ou=CAentry,dc=entrustsm,dc=local`
2. Test access to the directory service:

```
C:\Users\Administrator>C:\OpenLDAP\ClientTools\ldapsearch -x -H
ldap://<directory_services_server_IP_or_Name> -D "cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -b
"cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -s sub -W
Enter LDAP Password: *******
# extended LDIF
#
# LDAPv3
# base <cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local> with scope subtree
```

```
# filter: (objectclass=*)
# requesting: ALL
#

# EntrustAdmin, CAentry, entrustsm.local
dn: cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: entrustadmin
sn: Administrator
userPassword: **[redacted]**
description: Certificate Authority Directory Administrator
cn: EntrustAdmin

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Chapter 3. Install and configure the nShield HSM

3.1. Select the protection method

OCS or Softcard protection can be used to authorize access to the keys protected by the HSM. Follow your organization's security policy to select an authorization access method.

3.2. Install the nShield HSM

Install the nShield HSM locally, remotely, or remotely via the serial console. Condensed instructions are available in the following Entrust nShield Support articles.

- How To: Locally Set up a new or replacement nShield Connect.
- How To: Remotely Setup a new or replacement nShield Connect.
- How To: Remotely Setup a new or replacement nShield Connect XC Serial Console Model.

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

The complete instruction set is available at nShield v13.6.18 Hardware Install and Setup Guides.

3.3. Install the nShield Security World Software and create the Security World

Install the nShield Security World Software and create the Security World on the same server that will host the Entrust Certificate Authority.

1. Install the Security World software. The complete instruction set is available at nShield Security World Software v13.6.18 Installation Guide.
2. Add the Security World utilities path `C:\Program Files\nCipher\nfast\bin` to the system path.
3. Open firewall port 9004 for the HSM connections.
4. If using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).

5. Configure the server as a client of the HSM.
6. Open a command window and run the following to confirm the HSM is **operational**.

```
# enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number
 mode                 operational
 version              13.6.18
...
Module #1:
  enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        8FE1-B519-C5AA
 mode                 operational
 version              13.4.5
 ...
```

7. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy when creating the Security World. Create extra ACS cards as spares in case one is lost or fails.

ACS cards cannot be duplicated after the Security World is created. You may want to create extras according to your organization's security policy.

8. Confirm the Security World is **Usable**.

```
# nfkminfo
World
 generation  2
 state       0x37270008 Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

3.4. Create the OCS or Softcard

OCS cards are smart cards that are presented to the HSM via the physical smart card reader or the TVD. For more information on OCS use, properties, and k-of-N values, see Operator Card Sets (OCS).

When selecting your protection method, consider:

1. Your organization's security policy.
2. Unattended startup requirements.

The OCS card or Softcard must be presented during the initial configuration of the Entrust Certificate Authority Manager. In production, unattended startup is possible in some scenarios.

3.4.1. Create the OCS

To create the OCS:

1. Ensure file `C:\ProgramData\nCipher\Key Management Data\config\cardlist` contains the serial number of the card(s) to be presented, or the wildcard "*".
2. Open a command window as an administrator.
3. Run the `createocs` utility as described below, entering a passphrase (a password) at the prompt. The passphrase (if any) can be different for each OCS card.

   Create one card for each person with access privilege, plus the spares.

   The `--persist` option enables you to remove the OCS for safe storage. Otherwise, the authentication provided by the OCS is only available while the OCS card is inserted in the Entrust nShield HSM front panel slot, or presented remotely via the TVD. In this example the OCS is presented via the TVD, `slot 2`.

   After an Operator Card Set has been created, the cards cannot be duplicated.

   ```
   # createocs -m1 -s2 -N testOCS -Q 1/1 --persist

   FIPS 140-2 level 3 auth obtained.

   Creating Cardset:
    Module 1: 0 cards of 1 written
    Module 1 slot 0: Admin Card #1
    Module 1 slot 2: empty
    Module 1 slot 3: empty
    Module 1 slot 2: blank cardSteps:

    Module 1 slot 2:- passphrase specified - writing card
   Card writing complete.

   cardset created; hkltu = a165a26f929841fe9ff2acdf4bb6141c1f1a2eed
   ```

4. Verify the OCS was created:

   ```
   # nfkminfo -c
   Cardset list - 1 cardsets:  (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
    Operator logical token hash              k/n timeout  name
    02466cfb08d1115802ebe39920bc562b43b0d43b  1/1  none-PL testOCS
   ```

   The `rocs` utility also shows the newly created OCS:

```
# rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardset
No. Name                    Keys (recov) Sharing
  1 testOCS                 2 (2)        1 of 1; persistent
rocs> quit
```

3.4.2. Create a Softcard

1. Run the following utility, and enter a passphrase at the prompt:

```
# ppmk -n testSC

Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU d9414ed688c6405aab675471d3722f8c70f5d864
```

2. Verify the Softcard was created:

```
# nfkminfo -s
SoftCard summary - 1 softcards:
 Operator logical token hash               name
 d9414ed688c6405aab675471d3722f8c70f5d864  testSC
```

The `rocs` utility also shows the newly created Softcard:

```
# rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cards
No. Name                    Keys (recov) Sharing
  1 testOCS                 2 (2)        1 of 1; persistent
  2 testSC                  0 (0)        (softcard)
rocs> quit
```

Chapter 4. Install the Entrust Certificate Authority

4.1. Install the Entrust Certificate Authority PostgreSQL

Entrust Certificate Authority requires a database to store information about the Certification Authority, X.509 users, and EAC entities. See document *PSIC-Entrust Certificate Authority 10.2.pdf* located in the **Documents** tab of Product Support Center for Authority for supported databases.

This guide uses the PostgreSQL database supplied with Certificate Authority. Install this database on the same server that hosts Entrust Certificate Authority. If you are using your own supplied database, Entrust strongly recommends that you install the database on its own dedicated server.

To install and use Certificate Authority in a cluster, you must use your own supplied database. The Entrust supplied Certificate Authority PostgreSQL Database does not support a clustered environment.

1. Download `EntrustCertificateAuthorityPostgreSQL.15.18.0.49.exe` from the Entrust TrustedCare online support site Certificate Authority.
2. Run the downloaded executable.
3. Run `Install_ECAPG.bat` and select **Finish** when the installer completes.
4. Launch `ent_setup.bat`:

   Open a command window and execute `C:\Program Files\Entrust\easm_postgres15\dbserver\bin\ent_setup.bat`.

5. Enter the following information in the setup window. Then press any key to complete the setup.

Parameter	Value
Database super user **easm_entrust_pg**	Password
Database listen port	Default 5432
PostgreSQL Data directory	Default `C:\eca_pg_data\15`
PostgreSQL Wal directory	Default `c:\eca_pg_wal\15`
Database user **easm_entrust**	Password

Parameter	Value
Database backup user **easm_entbackup**	Password

For example:

```
PS C:\Program Files\Entrust\easm_postgres15\dbserver\bin> .\ent_setup.bat
[ent_setup]
[ent_setup] Logging to 'C:\Users\Administrator\AppData\Roaming\Entrust\postgresql\ent_setup.log'.
[ent_setup]
[ent_setup] ******************************************************
[ent_setup] Starting setup...
[ent_setup] ******************************************************
[ent_setup] Welcome to the Entrust Certificate Authority PostgreSQL Database 15.18 setup.
[ent_setup]    Running as [WINDOWS-SERVER\Administrator]
[ent_setup]
[ent_setup] Checking for a previous version...
[ent_setup]    Registry key [HKLM:\SOFTWARE\Entrust\PostgreSQL\11] does not exist, no installation found.
[ent_setup]
[ent_setup] Checking for current version...
[ent_setup]    Found InstallDir [C:\Program Files\Entrust\easm_postgres15\].
[init]
[init] No upgradeable Entrust Authority Security Manager PostgreSQL Database installation was found.
[init]
[init] Do you wish to initialize Entrust Certificate Authority PostgreSQL Database 15.18 at this time?
(y/n): y
[init] Performing a full initialization for installation at [C:\Program Files\Entrust\easm_postgres15]...
[init]
[init] Checking for 'easm_entrust_pg' OS user...
[init]    User was not found, creating OS user 'easm_entrust_pg'...
[init]
[init]    ***NOTE***: Be sure to adhere to any of your organization's password rules as well.
[init]
[init] The following characters cannot be used when choosing the password:
[init]    < > # \ " / | ' ^ ; &  <space> <tab>
[init] Please choose a password for:    'easm_entrust_pg': ***********
[init] Please confirm the password for: 'easm_entrust_pg': ***********
[init]
[init]    The 'easm_entrust_pg' user has been successfully created.
[init]    Enabling SeServiceLogonRight for easm_entrust_pg...
[init]
[init] A database super user 'easm_entrust_pg' is required.
[init]
[init] The following characters cannot be used when choosing the password:
[init]    < > # \ " / | ' ^ ; &  <space> <tab>
[init] Please choose a password for:    'easm_entrust_pg': ***********
[init] Please confirm the password for: 'easm_entrust_pg': ***********
[init]
[init] Please choose a listen port for the server [5432]:
[init]
[init] Please choose a location for the PostgreSQL Data directory : [c:\eca_pg_data\15]:
[init] Adding full (inheritable) permission for [easm_entrust_pg] to location [c:\eca_pg_data\15]...
[init] Adding full (inheritable) permission for [Administrators] to location [c:\eca_pg_data\15]...
[init] Adding full (inheritable) permission for [WINDOWS-SERVER\Administrator] to location
[c:\eca_pg_data\15]...
[init]
[init] Please choose a location for the PostgreSQL Wal directory : [c:\eca_pg_wal\15]:
[init] Adding full (inheritable) permission for [easm_entrust_pg] to location [c:\eca_pg_wal\15]...
[init] Adding full (inheritable) permission for [Administrators] to location [c:\eca_pg_wal\15]...
[init] Adding full (inheritable) permission for [WINDOWS-SERVER\Administrator] to location
[c:\eca_pg_wal\15]...
[init]
[init] Initializing Database cluster with database super user 'easm_entrust_pg'...
```

```
[init]
[init] Calculating the recommended shared_buffers value...
[init] Installing and updating custom pg_easm_DB.conf...
[init]    Setting archive_command path to C:\Program Files\Entrust\easm_postgres15\bin\pg_archwal.bat
[init]    Setting port = 5432
[init]    Setting shared_buffers = 1073741824 Bytes
[init] Updating postgresql.conf...
[init]    Setting include = pg_easm_DB.conf
[init]    The database cluster is initialized.
[init] Setting EASMPOSTGRESDIR environment variable...
[init] Setting OPENSSL_CONF environment variable...
[init]
[init] Registering PostgreSQL Server as a Windows service...
[init]
[init] Setting PostgreSQL service display name and description...
[init]
[init] Starting the PostgreSQL service...
[init]
[init] Creating database easm_DB...
[init]
[init] A database user 'easm_entrust' is required.
[init]
[init] The following characters cannot be used when choosing the password:
[init]    < > # \ " / | ' ^ ; &  <space> <tab>
[init] Please choose a password for:    'easm_entrust': ***********
[init] Please confirm the password for: 'easm_entrust': ***********
[init] Creating 'easm_entrust' user...
[init]
[init] A database backup role 'easm_entbackup' is required.
[init]
[init] The following characters cannot be used when choosing the password:
[init]    < > # \ " / | ' ^ ; &  <space> <tab>
[init] Please choose a password for:    'easm_entbackup': ***********
[init] Please confirm the password for: 'easm_entbackup': ***********
[init] Creating 'easm_entbackup' database role...
[init]
[init] Creating easm_entrust schema...
[init] Creating extension pgrowlocks...
[init] Creating extension pg_freespacemap...
[init] Creating extension pgstattuple...
[init] Creating extension pg_buffercache...
[init] Creating extension pageinspect...
[init]
[init] Removing full (inheritable) permission for [WINDOWS-SERVER\Administrator] from location
[c:\eca_pg_data\15]...
[init] Removing full (inheritable) permission for [WINDOWS-SERVER\Administrator] from location
[c:\eca_pg_wal\15]...
[init]
[init] Registering PostgreSQL event DLL for [C:\Program Files\Entrust\easm_postgres15]...
[init]
[init] Setting PGPORT environment variable...
[init]
[init] Stopping the PostgreSQL service...
[init]
[init] Starting the PostgreSQL service...
[ent_setup]
[ent_setup] Operation complete!
Press any key to continue . . .
PS C:\Program Files\Entrust\easm_postgres15\dbserver\bin>
```

4.2. Install the Entrust Certificate Authority

1. Download the **Certificate Authority Full and Upgrade Installer 11.0.1 - Windows** from the Entrust TrustedCare online support site Certificate Authority.
2. Double-click the `msi` file downloaded above to begin the installation.

   An installation wizard appears.

3. Once the installation completes, select **Finish** in the **Install Wizard Complete** dialog. The installation path is `C:\Program Files\Entrust`.

Chapter 5. Configure the Entrust Certificate Authority

- Establish a preload session
- Configure the Entrust nShield Edge
- Configure the Entrust Certificate Authority

5.1. Establish a preload session

The OCS or Softcard must be preloaded before you configure the Entrust Security Manager.

1. Create an empty folder called `preload` on the `C:` drive.
2. Edit the environment variables in `cknfastrc`. The file is located at `%NFAST_HOME%\cknfastrc`, by default `C:\Program Files\nCipher\nfast\cknfastrc`. Edit the file to include:

```
# Softcard
CKNFAST_LOADSHARING=1

# Enable Module Protection
CKNFAST_FAKE_ACCELERATOR_LOGIN=1

# Other variables
CKNFAST_NO_UNWRAP=1
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none

# Preload file location
NFAST_NFKM_TOKENSFILE=C:\preload\entrustsmtoken

# PCKS #11 log level and file location
CKNFAST_DEBUG=10
CKNFAST_DEBUGFILE=C:\preload\pkcs11.log
```

   Useful information about environment variables:

   - `NFAST_NFKM_TOKENSFILE=C:\preload\entrustsmtoken` is user-defined and is referenced by the `preload` utility. For example, `%NFAST_HOME%\Bin>preload -c <OCS Name> -f C:\preload\entrustsmtoken pause`.
   - When using a K-of-N Card Set where K>1, set `CKNFAST_LOADSHARING=0`. When using a K-of-N Card Set where K=1, set `CKNFAST_LOADSHARING=1`. This also applies when using Softcard protection.
   - For Enhanced Database Protection (EDP), use `CKNFAST_LOADSHARING=0` after enabling database hardware protection. Restart the system for load sharing to work.

- When using nShield with ePassport CVCA, set `CKNFAST_ASSUME_SINGLE_PROCESS=0`. If ePassport Document Verifier Certificate requests are canceled, this setting ensures that the associated physical key is deleted in the Entrust nShield HSM.

For more information about the environment variables used in `cknfastrc`, see Environment variables

3. Restart the hardserver.

```
C:\Users\Administrator>net stop "nFast Server"
The following services are dependent on the nFast Server service.
Stopping the nFast Server service will also stop these services.

   nShield Audit Log Service
   nFast Remote Administration Service

Do you want to continue this operation? (Y/N) [N]: y
...
The nFast Server service was stopped successfully.

C:\Users\Administrator>net start "nFast Server"
The nFast Server service is starting.
The nFast Server service was started successfully
```

4. Open a command window to run preload exclusively.

Do not close this window throughout the Entrust Certificate Authority configuration. Otherwise you will shut down the session and the configuration will fail. It is OK to minimize the window.

When using a Softcard in FIPS Level 3, you must present an OCS card for FIPS authorization.

5. Preload the OCS by running the utility `preload -c`, or `preload -s` for the Softcard. Present the OCS cards and / or passphrase when prompted.

For example:

```
C:\Users\Administrator>preload -c testOCS -f C:\preload\entrustsmtoken pause
2025-10-23 14:24:12: [1960]: INFO: Preload running with: -c testOCS -f C:\preload\entrustsmtoken pause
2025-10-23 14:24:12: [1960]: INFO: Created a (new) connection to Hardserver
2025-10-23 14:24:12: [1960]: INFO: Modules newly usable: [1].
2025-10-23 14:24:12: [1960]: INFO: Found a change in the system: an update pass is needed.
2025-10-23 14:24:12: [1960]: INFO: Loading cardset: testOCS in modules: [1]

Loading `testOCS':
 Module 1 slot 2: `testOCS' #2
 Module 1 slot 0: Admin Card #11
 Module 1 slot 3: empty
 Module 1 slot 4: empty
 Module 1 slot 5: empty
 Module 1 slot 2:- passphrase supplied - reading card
Card reading complete.
```

```
2025-10-23 14:24:16: [1960]: INFO: Stored Admin key: kfips (003e...) in module #1
2025-10-23 14:24:16: [1960]: INFO: Loading cardset: Cardset: testOCS (edb3...) in module: 1
2025-10-23 14:24:16: [1960]: INFO: Stored Cardset: testOCS (edb3...) in module #1
2025-10-23 14:24:16: [1960]: INFO: Maintaining the cardset testOCS protected key(s)=[].
2025-10-23 14:24:16: [1960]: INFO: Loading complete. Now pausing...
```

If non-persistent cards are used, then the last card in the quorum must remain inserted in the card reader. If persistent cards are used, then the last card in the quorum can be removed from the card reader.

6. Confirm the OCS or Softcard has been preloaded by running the following utility back on the main window. The **Pre-Loaded Objects** will be reported.

```
# preload -f <location of file above> nfkminfo
```

For example:

```
C:\Users\Administrator>preload -f C:\preload\entrustsmtoken nfkminfo
2025-10-23 14:29:08: [316]: INFO: Preload running with: -f C:\preload\entrustsmtoken nfkminfo
2025-10-23 14:29:08: [316]: INFO: Created a (new) connection to Hardserver
2025-10-23 14:29:08: [316]: INFO: Modules newly usable: [1].
2025-10-23 14:29:08: [316]: INFO: Found a change in the system: an update pass is needed.
2025-10-23 14:29:08: [316]: INFO: Maintaining the cardset testOCS protected key(s)=[].
2025-10-23 14:29:08: [316]: INFO: Loading complete. Executing subprocess nfkminfo

 ...

Pre-Loaded Objects (  2):  objecthash   module objectid  generation
 003e04e3c07fb5791f651c992da5527779159f87   1 0x89fa8799 1
 edb3d45a28e5a6b22b033684ce589d9e198272c2   1 0x89fa8782 1
```

Useful information concerning OCS:

- You must present sufficient different OCS cards to fulfill the quorum.
- The tokens file generated by the `preload` utility is valid for one continuous session only. If the session is lost, then the token authorization is lost. You cannot reuse the same token file once the session is lost, even if you use the exact same OCS cards again. To restart re-run preload.
- A session, and token authorization is lost if:
  - There is a temporary power failure.
  - The window running preload is closed.
  - The last card in the quorum is removed if using non-persistent OCS cards.

The tokens file represents a security risk if permissions to access it are not restricted to authorized persons only.

5.2. Configure the Entrust nShield Edge

If you are using an Entrust nShield Edge HSM, continue with this section. Otherwise, proceed to Configure the Entrust Certificate Authority.

The Entrust nShield Edge exhibits slower service startup times compared to the other Entrust nShield HSMs. To ensure optimal performance, increase the Entrust Certificate Authority timeout settings as follows.

1. Navigate to the directory containing the `entMgr.ini` file, by default: `C:\Program Files\Entrust\Certificate Authority\etc\ini`.
2. Edit the `entMgr.ini` file in the **[login]** section and add the following:

```
serviceStartStopWaitSeconds=3600
clusterStartWaitSeconds=1800
clusterStopWaitSeconds=300
```

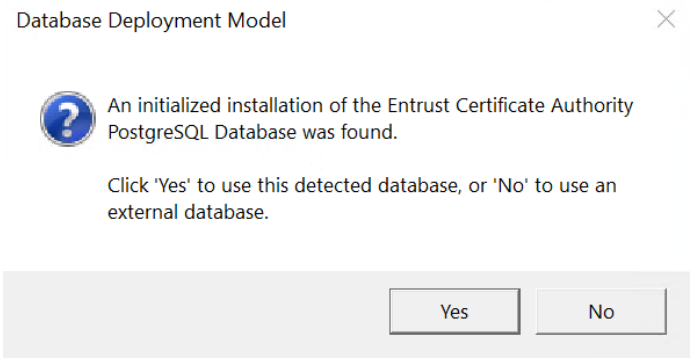
5.3. Configure the Entrust Certificate Authority

This section describes how to configure the Entrust Certificate Authority before it can be used. During configuration, you provide the following:

- Your directory and database connection parameters.
- Your choice of certificate algorithms, lifetimes, and other options.

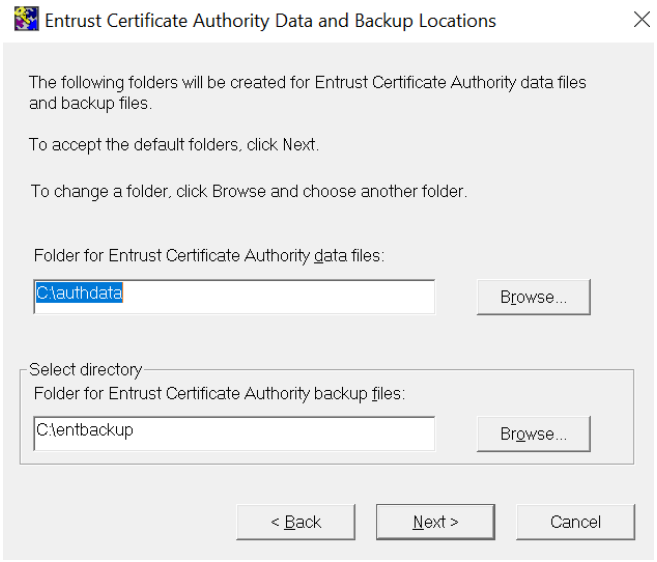
The configuration is stored in `C:\Program Files\Entrust\Certificate Authority\etc\ini\entMgr.ini`. Verify its settings before initializing the CA.

1. Navigate to the Certificate Authority `\bin` directory, by default `C:\Program Files\Entrust\Certificate Authority\bin`.
2. Double-click `entConfig.exe`.
3. In the **Database Deployment Model** window, select according to your setup. We selected **Yes** in this integration to use the Entrust Certificate Authority PostgreSQL database installed locally as described in Install the Entrust Certificate Authority PostgreSQL.



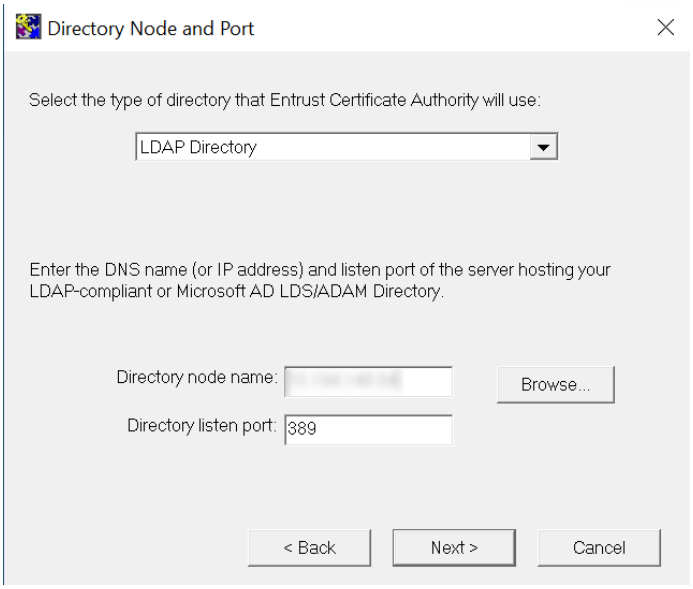
4. In the **Entrust Certificate Authority Configuration** window, select **Next**.
5. In the **Certificate Authority License Information** window, enter the Enterprise licensing information that appears on your Entrust licensing card. Then select **Next**.

6. In the **Certificate Authority Data and Backup Locations** window, enter your location or accept the defaults. Then select **Next**.
   - Data files: `c:\authdata`.
   - Backup files: `c:\entbackup`.

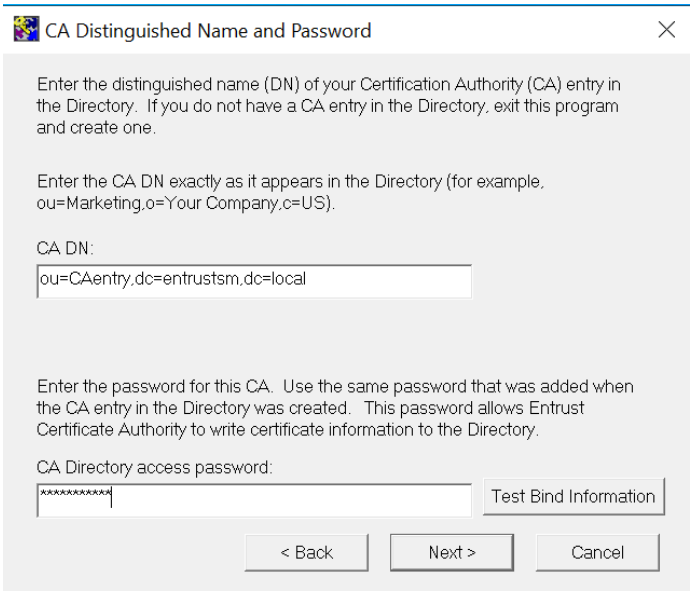


7. In the **Directory Node and Port** window, enter your directory information. We used the directory described in Configure directory service. Then select **Next**.

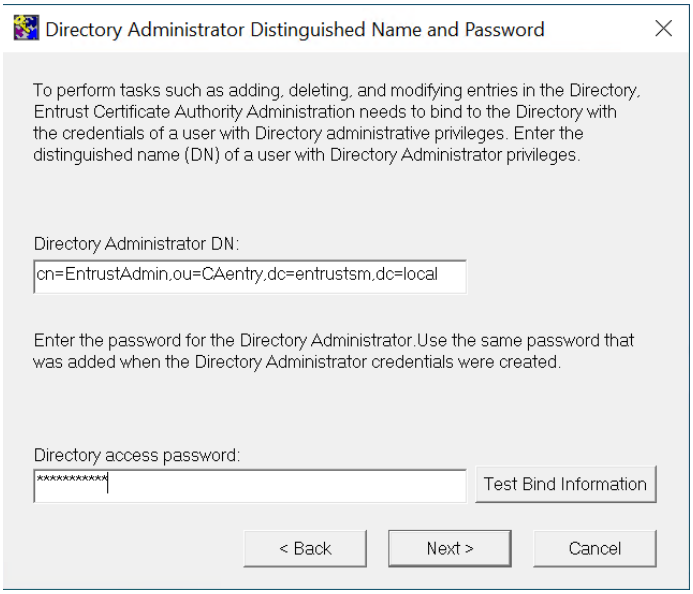
   For example:



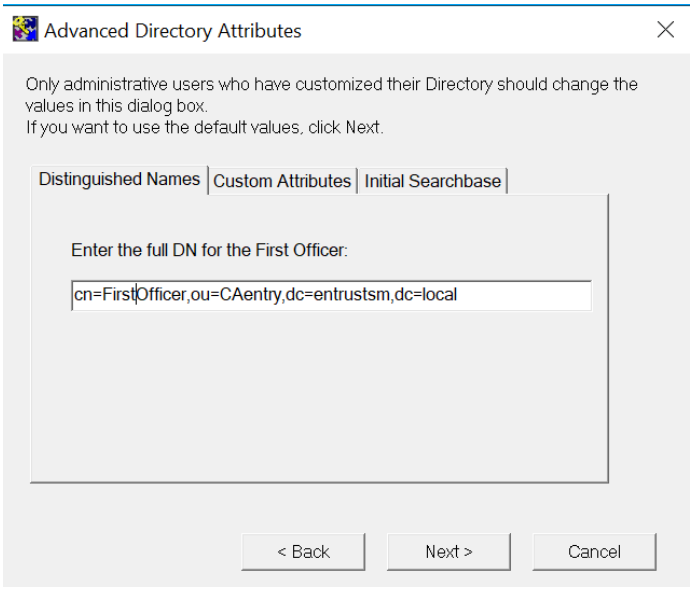
8. In the **CA Distinguished Name and Password** window, enter your **CA DN** and **CA Directory access password**, then select **Test Bind Information**.



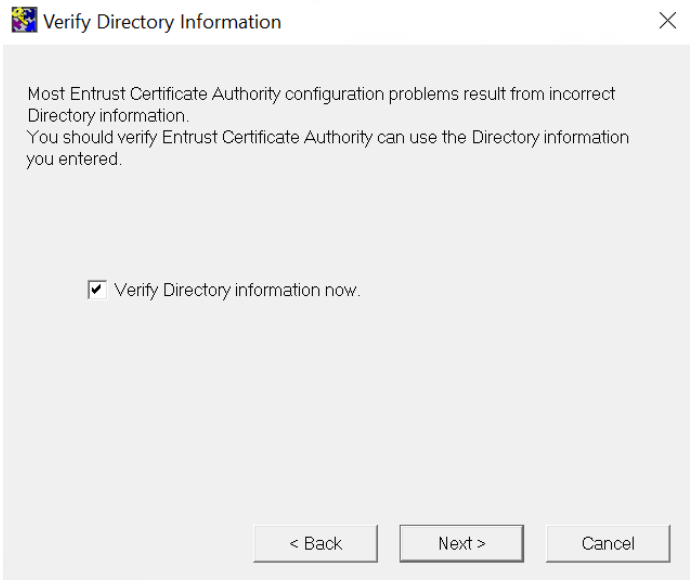
9. If the bind is successful, select **OK**. Otherwise, correct any errors in your directory settings using the **Back** button and retest. Then select **Next**.
10. In the **Directory Administrator Distinguished Name and Password** window, enter your **Directory administrator DN** and **Directory access password**, then select **Test Bind Information**.



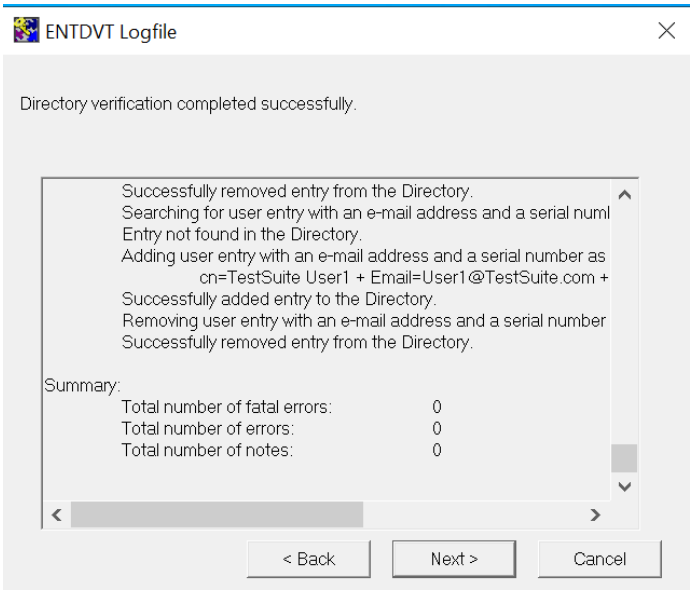
11. If the bind is successful, select **OK**. Otherwise, correct any errors in your directory settings using the **Back** button and retest. Then select **Next**.
12. In the **Advanced Directory Attributes** window, enter the full DN of the first officer. Then select **Next**.



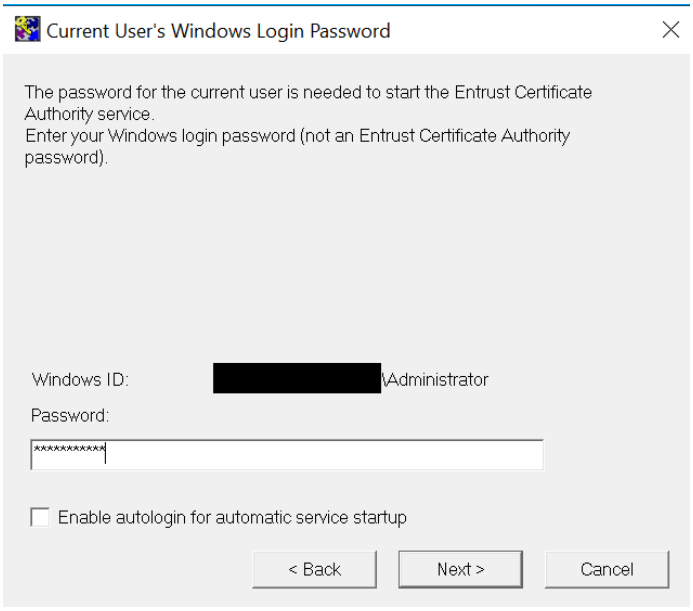
13. In the **Verify Directory Information** window, check **Verify Directory information now**. Then select **Next**.



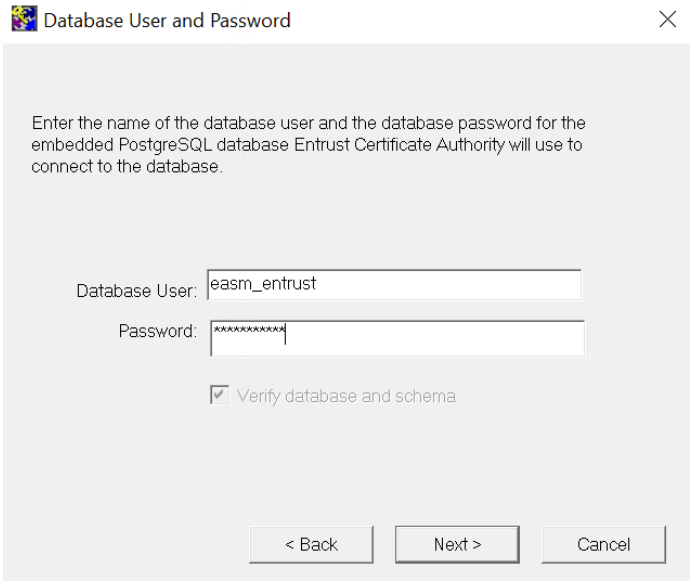
14. In the **ENTDVT Logfile** window, verify there are no fatal errors, errors, or notes in the **Summary** section. Correct any errors in your directory settings using the **Back** button before proceeding. Then select **Next**.



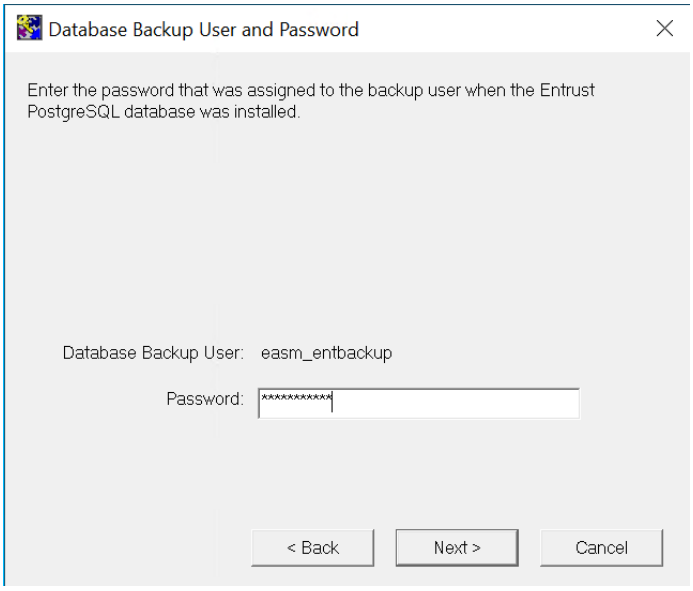
15. In the **Current User's Windows Login Password** window, log in with your Windows credentials. Uncheck **Enable autologin for automatic service startup**. Then select **Next**.



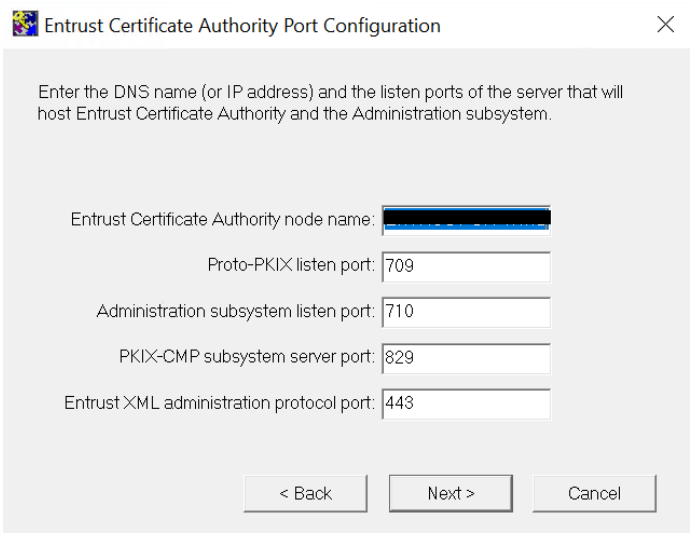
16. In the **Database User and Password** window, enter your database user credentials. Then select **Next**.



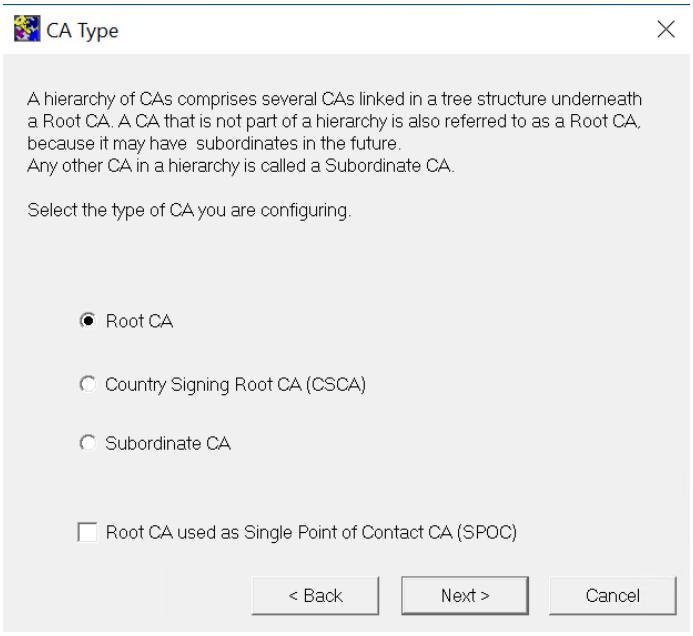
17. In the **Database Backup User and Password** window, enter your database backup user credentials. Then select **Next**.



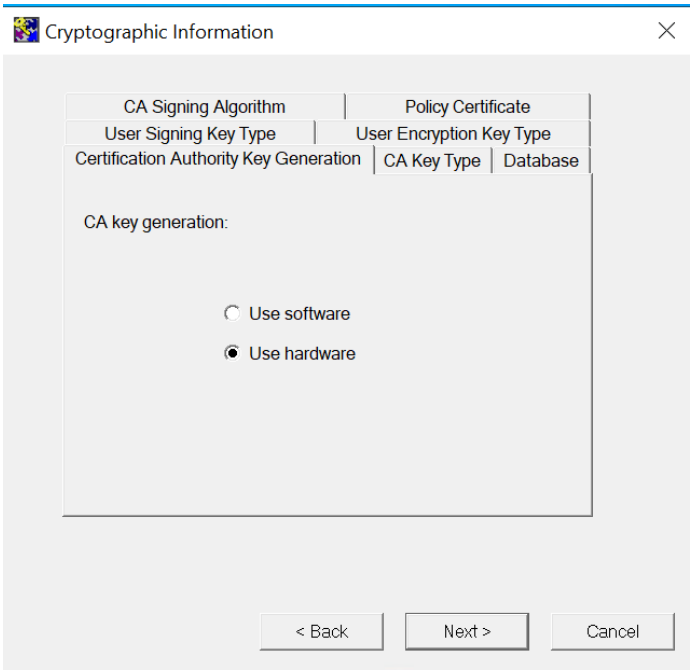
18. In the **Entrust Certificate Authority Port Configuration** window, enter your information, then select **Next**.



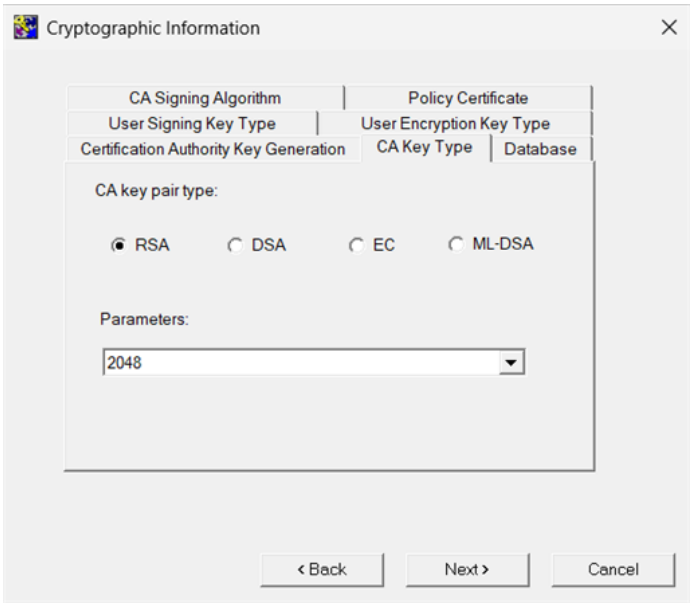
19. In the **CA Type** window, select the **Root CA** radio button. Uncheck **Root CA used as Single Point of Contact CA (SPOC)**, then select **Next**.



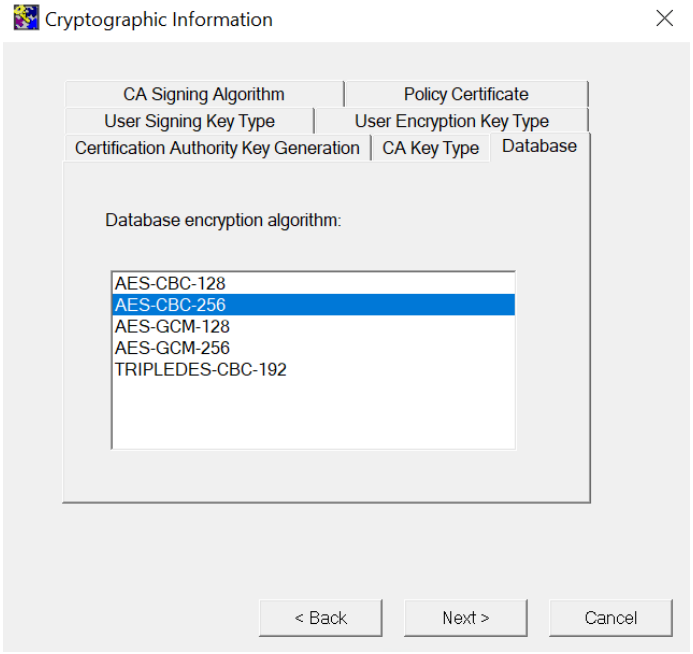
20. In the **Cryptographic Information** window, select in each tab as follows. Select **Next** each time.
21. On the **Certification Authority Key Generation** tab, select **Use hardware**.



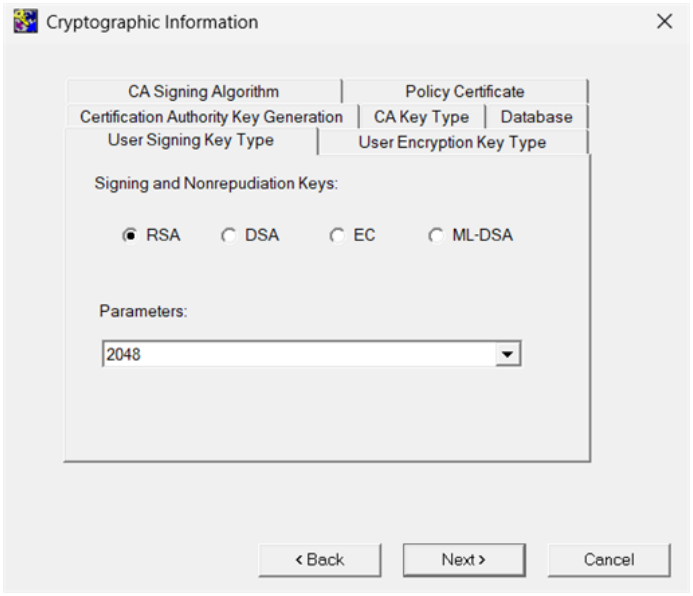
22. On the **CA Key Type** tab, select the key type and length. For a PQ workflow, select the ML-DSA key type and appropriate size, either 44, 65, or 87.



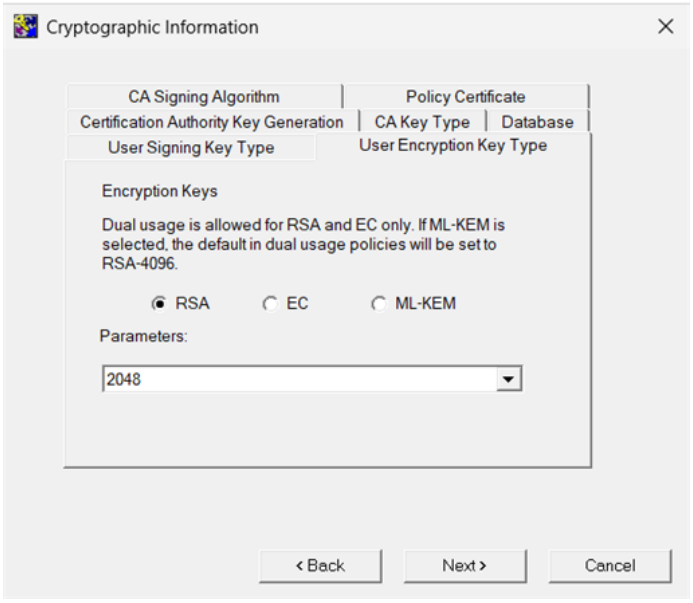
23. On the **Database** tab, select the database encryption algorithm.



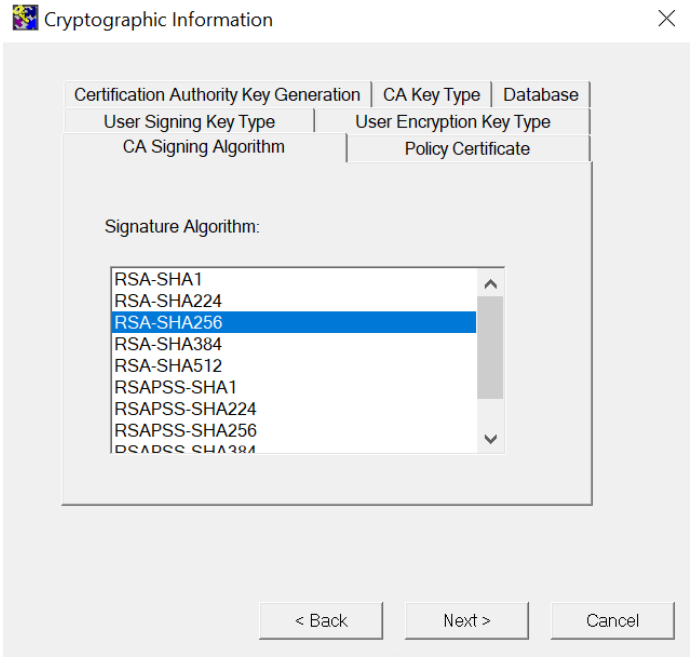
24. On the **User Signing Key Type** tab, select the key type and length. For a PQ workflow, select the ML-DSA key type and appropriate size, either 44, 65, or 87.



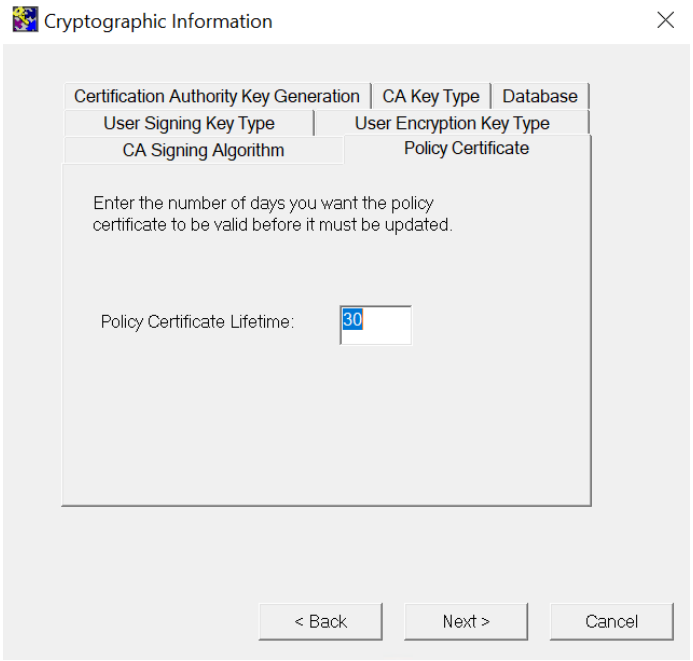
25. On the **User Encryption Key Type** tab, select the key type and length. For a PQ workflow, select the ML-KEM key type and appropriate size, either 512, 768, or 1024.



26. On the **CA Signing Algorithm Type** tab, select the type.

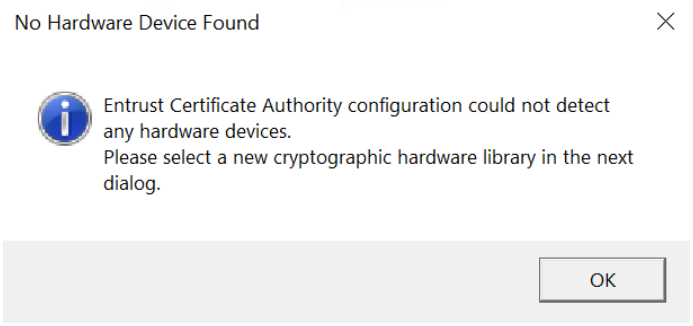


27. On the **Policy Certificate** tab, enter the policy certificate lifetime.

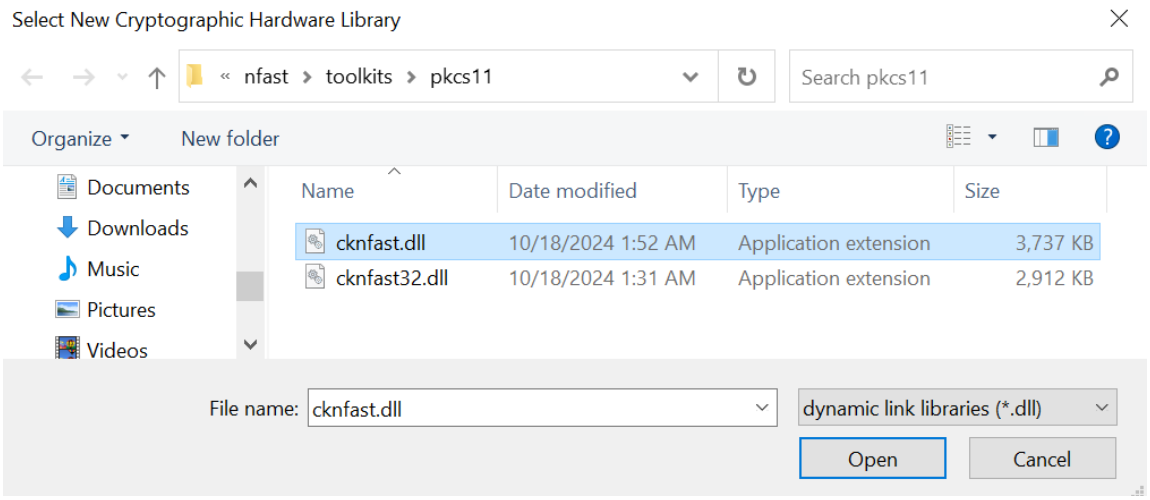


For this integration to work with EC-P and RSAPSS, the ECC activation feature must be enabled for the Entrust nShield HSM. In the `%NFAST_ HOME%\bin` directory, run `FET.exe`.

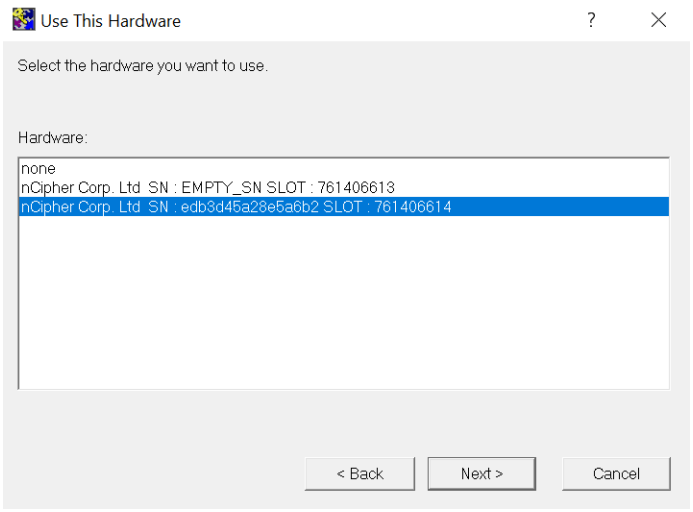
28. If you are using the Entrust nShield Edge, go to the step after next. Otherwise, the **No Hardware Device Found** dialog appears. Select **OK**.



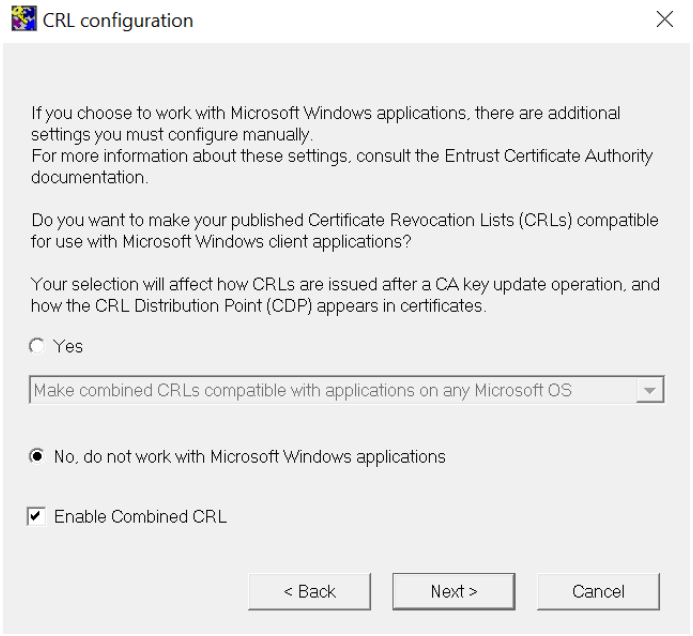
29. In File Explorer, select the nShield PKCS11 library `%NFAST_HOME%\toolkits\pkcs11\cknfast.dll`.
The default location is `C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll`.



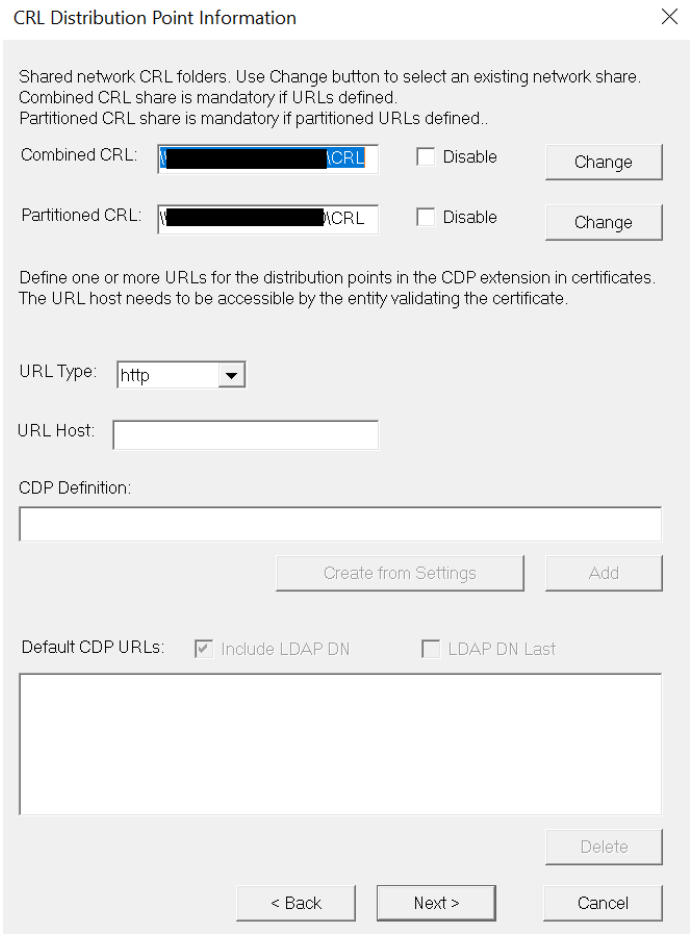
30. In the **Use This Hardware** window, select the Entrust nShield HSM entry with a valid serial number, then select **Next**.



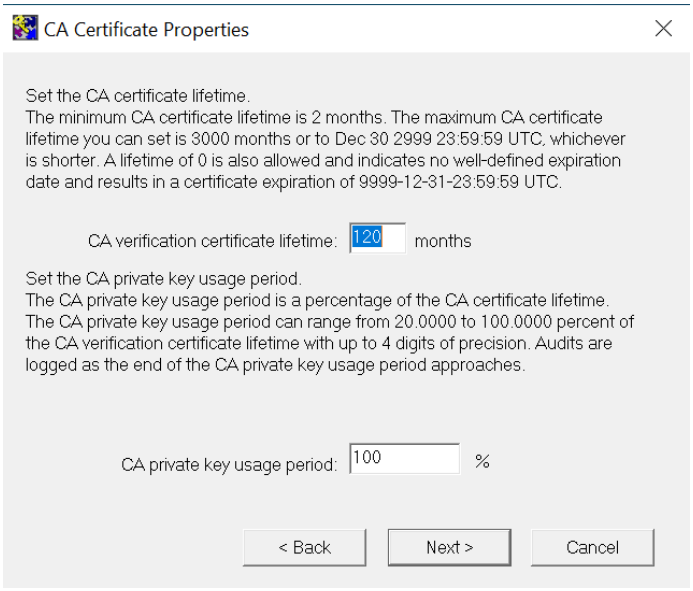
31. In the **CRL Configuration** window, select **No, do not work with Microsoft Windows applications**, then select **Next**.



32. In the **CRL Distribution Point Information** window, select the CRL location, then select **Next**.

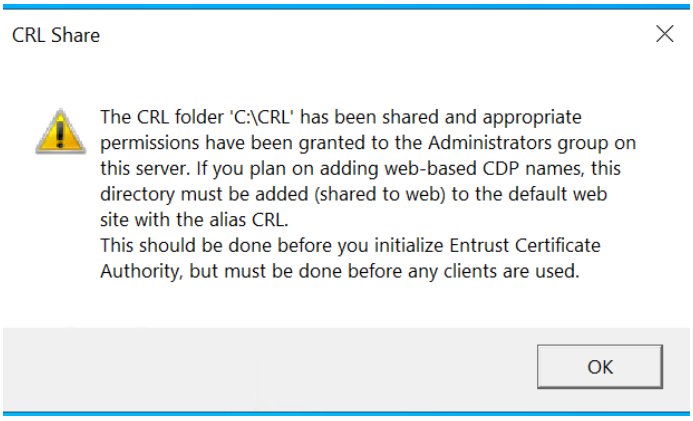


33. In the **CA Certificate Properties** window, enter the CA certificate lifetime and private key usage period, then select **Next**.

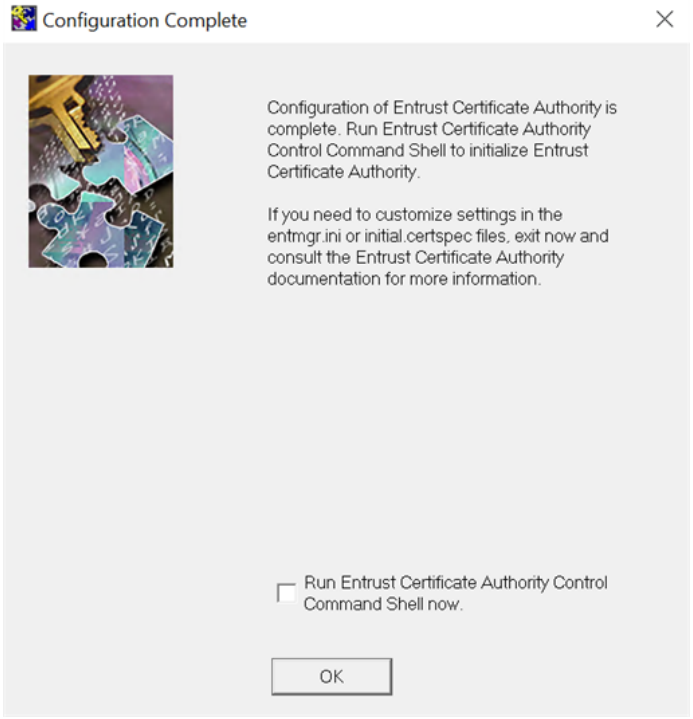


Consult your organization's security policy for recommendations on the CA lifetime.

34. In the **CRL Share Warning** window, select **OK**.



35. In the **Configuration Complete** window, leave **Run Entrust Certificate Authority Control Command Shell now** unchecked, then select **OK**.



Close the configuration utility and any remaining dialogs.

36. Verify the configuration file before initializing the CA:
    - Back up `C:\authdata\manager\entmgr.ini`.
    - In `[Comms]`:
        - Verify the directory server and listener ports.
        - Add `Mgrlisten=709` if it is missing.
    - In `[policy]`:
        - Check that `diradminPW` and `CADsaPw` match the configured directory administrator and CA entry passwords.
    - In `[Authorization]`:
        - Add a Web Server license if required.
        - Check that `WebSerialNumber`, `WebUserLimit`, and `WebKey` are present. If not, add them to the existing section using your license values; keep the Enterprise fields and do not create a second section. You can also add this information later through the Certificate Authority Administration utility.
37. Verify both authenticated directory binds before continuing.
    Run the following commands from `C:\OpenLDAP\ClientTools`, replacing `<directory_server_name>` with the directory server's hostname. Enter each password when prompted:

```
& ".\ldapsearch" -x -h "<directory_server_name>" -D "cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -W
```

```
-b "ou=CAentry,dc=entrustsm,dc=local" -s base "(objectClass=*)"
& ".\ldapsearch" -x -h "<directory_server_name>" -D "ou=CAentry,dc=entrustsm,dc=local" -W -b
"ou=CAentry,dc=entrustsm,dc=local" -s base "(objectClass=*)"
```

Continue only if both commands return `result: 0 Success`. If either command returns a failure, check that the LDAP server is working and was set up correctly.

38. Initialize the CA manually:
    a. Open a new Administrator PowerShell window and set `AUTHDATDIR`:

    ```
    [Environment]::SetEnvironmentVariable('AUTHDATDIR', 'C:\authdata', 'Machine')
    $env:AUTHDATDIR = 'C:\authdata'
    ```

    b. Start the CA shell:

    ```
    Set-Location 'C:\Program Files\Entrust\Certificate Authority\bin'
    .\entsh.exe
    ```

    c. At the `entsh` prompt, run `init`.
39. Enter and confirm the following passwords. Note these for future use.

Parameter	Value
HSM	OCS or softcard passphrase created in Create the OCS or Softcard.
Master1-3	Master user's new passwords
First Officer	First officer's new password

For example:

```
Starting First-Time Initialization...

A Hardware Security Module (HSM) will be used for the CA key:
    nCipher Corp. Ltd  SN : <HSM serial>
    The HSM requires a password.

Enter password for CA hardware security module (HSM):
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 Entrust Certificate Authority Control Command Shell.
Performing database backup...
SUCCESS: Full backup completed successfully.
Press return to exit
```

40. Close the window above.

Chapter 6. Test the integration

6.1. Initialize the Certificate Authority

If you did not initialize the Certificate Authority during configuration:

1. Open an Administrator PowerShell window and set `AUTHDATDIR` for the machine and this session.

```
[Environment]::SetEnvironmentVariable('AUTHDATDIR', 'C:\authdata', 'Machine')
$env:AUTHDATDIR = 'C:\authdata'
```

2. Start the CA shell and run `init`:

```
Set-Location 'C:\Program Files\Entrust\Certificate Authority\bin'
.\entsh.exe
```

```
entsh$ init
```

6.2. Launch the Certificate Authority shell

1. Open a Windows command terminal.
2. Launch the Certificate Authority shell.

```
% cd "C:/Program Files/Entrust/Certificate Authority/bin"
% entsh.exe
```

Run all subsequent test commands in this shell.

6.3. Verify the in-memory CA key cache

1. Launch the Certificate Authority shell.
2. Run the following command.

   The following output is an RSA example. Key type and signing algorithm depend on the configuration, including PQ selections.

```
entsh$ ca key show-cache

Master User Name: Master1
Password:
**** 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:     ou=CAentry,dc=entrustsm,dc=local
serial number:                00B2247A87BD35D3DE1992761309984A1D
current CA certificate:       Y
CA certificate issue date:    Thu Oct 23 20:07:22 2025
CA certificate expire date:   Tue Oct 23 20:37:22 2035
subject key identifier:       43E42F76EEA1B0CD3E0B739743A29832E39F1872
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:              MrFc/z5l+9hIdD0lFGBBLWmskNE=
hardware status: Loaded >> 'nCipher Corp. Ltd  SN : <HSM serial> SLOT : <slot>'.

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

ou=CAentry,dc=entrustsm,dc=local.Master1
```

6.4. Verify the hardware information

1. Launch the Certificate Authority shell.
2. Run the following command.

```
ou=CAentry,dc=entrustsm,dc=local.Master1 $ ca key show-cahw -type all

EAC is not enabled. There is no associated cryptographic hardware for EAC.


**** Hardware Information ****

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

Name:
nCipher Corp. Ltd  SN : <HSM serial> SLOT : <slot>

Has current X.509 CA key: Y
Load Status:              hardware loaded ok
Uses Password:            Y
DB protection HW:         N
In use for X.509 CA keys: Y
In use for EAC keys:      N
ECDSA style:              4 (use raw digest padded to large digest size)
```

```
-----------------------------------------------------

Name:
nCipher Corp. Ltd  SN : EMPTY_SN SLOT : 761406613

Has current X.509 CA key: N
Load Status:              hardware loaded ok
Uses Password:            N
DB protection HW:         N
In use for X.509 CA keys: N
In use for EAC keys:      N
ECDSA style:              4 (use raw digest padded to large digest size)

-----------------------------------------------------
**** End of Hardware Information ****

ou=CAentry,dc=entrustsm,dc=local.Master1
```

6.5. Import the CA key pair from software to hardware

To import the Entrust CA key pair from software to the Entrust nShield HSM:

1. Launch the Certificate Authority shell.
2. Run the following command. When prompted, select the **nCipher** slot as the destination for the new CA key.

   For example:

```
ou=CAentry,dc=entrustsm,dc=local.Master1 $ ca key update

Select the destination for the new CA key.
Choose one of:
1. Software
2. nCipher Corp. Ltd  SN : EMPTY_SN SLOT : 761406613
3. nCipher Corp. Ltd  SN : <HSM serial> SLOT : <slot>
4. Cancel operation
> 3
If the cluster is running it will be stopped and the CA key updated.
Do you wish to continue (y/n) ? [y]
Checking cluster status...

Stopping cluster...

100% complete. Estimated time remaining -:-:- /

CA key and certificate successfully updated.
Recovering CA profile...
Starting cluster...

CA profile successfully recovered.

It is recommended that all revocation lists be re-issued. This can be done later with the 'rl issue'
command. Re-issue
revocation lists now (y/n) ? [y]

Issuing CRLs, please wait ...

1 CRL(s) were issued.
1 ARL(s) were issued.
```

```
1 combined CRL(s) were issued.

Publishing CRLs, please wait ...

ou=CAentry,dc=entrustsm,dc=local.Master1 $
```

3. Confirm that the output includes the **CA profile successfully recovered** message.

6.6. Export the CA key pair from hardware to software

To export the Entrust CA key pair from the Entrust nShield HSM to software:

1. Launch the Certificate Authority shell.
2. Run the following command. When prompted, select **Software** as the destination for the new CA key.

   For example:

```
ou=CAentry,dc=entrustsm,dc=local.Master1 $ ca key update

Select the destination for the new CA key.
Choose one of:
1. Software
2. nCipher Corp. Ltd  SN : EMPTY_SN SLOT : 761406613
3. nCipher Corp. Ltd  SN : <HSM serial> SLOT : <slot>
4. Cancel operation
> 1
If the cluster is running it will be stopped and the CA key updated.
Do you wish to continue (y/n) ? [y]
Checking cluster status...

Stopping cluster...

100% complete. Estimated time remaining -:-:- -

CA key and certificate successfully updated.
Recovering CA profile...
Starting cluster...

CA profile successfully recovered.

It is recommended that all revocation lists be re-issued. This can be done later with the 'rl issue'
command. Re-issue
revocation lists now (y/n) ? [y]

Issuing CRLs, please wait ...

1 CRL(s) were issued.
1 ARL(s) were issued.
1 combined CRL(s) were issued.

Publishing CRLs, please wait ...

ou=CAentry,dc=entrustsm,dc=local.Master1
```

3. Confirm that the output includes the **CA profile successfully recovered** message.

6.7. Back up nShield Security World files

Perform this backup after any new key generation or nShield Security World administration activities.

1. Back up the `C:\ProgramData\nCipher\Key Management Data\local` directory.
2. Store the backup files according to your organization's disaster recovery instructions.

Chapter 7. Troubleshooting

7.1. (-8973) Could not connect to the Entrust Certificate Authority service. Certificate Authority service may not be running

The Entrust Certificate Authority service is not running.

Resolution:

1. Launch the Entrust Certificate Authority shell.
2. Log in with `Master1`.
3. Run `Service Start`.

7.2. Error encountered querying CA hardware

The following error appears during Entrust Certificate Authority configuration.

```
Are you using a hardware device for the CA keys (y/n) ? [n] y

Enter the pathname for the Cryptoki Library.
[/opt/nfast/toolkits/pkcs11/libcknfast.so] >

Error encountered querying CA hardware.
```

Resolution:

- Ensure the preload session is established per Establish a preload session.

7.3. (-77) Problem reported with crypto hardware

The following error appears while initializing the Entrust Certificate Authority.

```
Initialization starting; creating ca keys...
(-77) Problem reported with crypto hardware.
GenerateKeyPairX509
Press return to exit
```

Resolution:

- Verify the following variable is set to **1** in the `%NFAST_HOME%\cknfastrc` file, by default `C:\Program Files\nCipher\nfast\cknfastrc`.

```
CKNFAST_LOADSHARING=1
```

7.4. (-2229) An error occurred. Check the service status and manager logs for details

This indicates a timeout.

Resolution:

1. Launch the Entrust Certificate Authority shell.
2. Run `service status`.
3. If the service is **down**, start it by running `service start`.

If you are using an Entrust nShield Edge, see Configure the Entrust nShield Edge.

7.5. HSM logs show errors for algorithms not configured

The Entrust Certificate Authority performs a FIPS self-test beyond the algorithms and functions explicitly configured, a requirement for FIPS 140 conformance.

Resolution:

- The Entrust Certificate Authority treats these errors as informational only.
- FIPS self-test errors in the HSM log do not stop the Entrust Certificate Authority from starting.

7.6. No hardware device found

During Entrust Certificate Authority configuration, the error message **No Hardware Device Found** appears.

Resolution:

1. Ensure the **nFast** services are running.
2. Ensure the preload session is established per Establish a preload session.
3. In the `C:\authdata\manager\authstartup.ini` file, in the `[Entrust Settings]` section, ensure that the `CryptokiV2LibraryNT` variable is set to the path of the hardware device driver. For example, `CryptokiV2LibraryNT=D:\Program Files\vendor1\device1.dll`.

7.7. (-2684) General hardware error

The Entrust nShield HSM is not available.

Resolution:

1. Ensure the **nFast** services are running.
2. Ensure the preload session is established per Establish a preload session.
3. In the `C:\authdata\manager\authstartup.ini` file, in the `[Entrust Settings]` section, ensure that the `CryptokiV2LibraryNT` variable is set to the path of the hardware device driver. For example, `CryptokiV2LibraryNT=D:\Program Files\vendor1\device1.dll`.

7.8. Entrust nShield Edge cluster status "down" or "unknown"

After initial setup, the Entrust nShield Edge cluster status is "down" or "unknown".

Resolution:

1. Ensure section Configure the Entrust nShield Edge is implemented correctly.
2. In some cases, you may need to start the cluster manually.

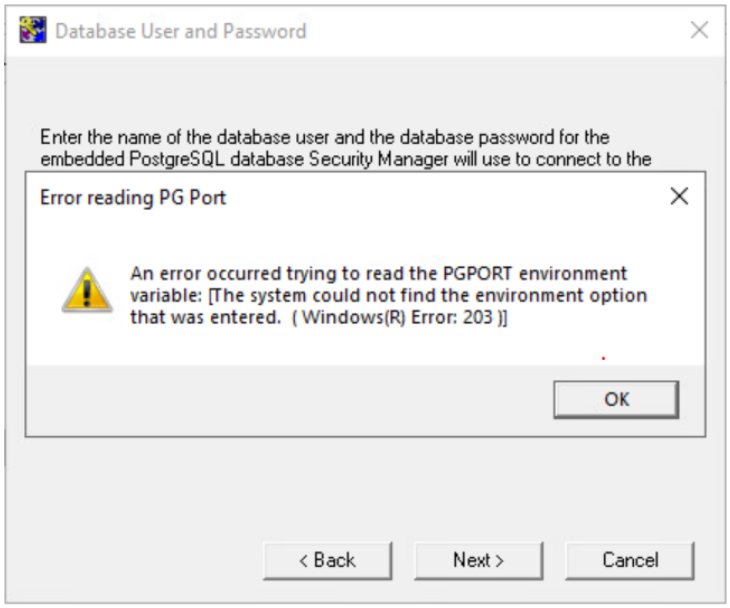
   For example:

```
entsh$ cluster status
ca_wide_entry   disabled
localhost       enabled     quiescent **LOCAL**

entsh$ cluster start
Starting cluster...

entsh$ cluster status
ca_wide_entry   enabled
localhost       enabled     quiescent **LOCAL*
```

For more information regarding the cluster status, refer to the *Cluster Management Guide* in the *Entrust Certificate Authority 10.2 Documentation Suite* located in the **Documents** tab at Product Support Center for Authority.

7.9. pg_port error

The following error message appears:



Resolution:

- Install and configure the PostgreSQL database before configuring the Entrust Certificate Authority.

Chapter 8. Additional resources and related products

8.1. nShield HSMs

8.2. nShield as a Service

8.3. Entrust products

8.4. nShield product documentation