Palo Alto Idira Identity Security Platform

nShield® HSM Integration Guide

2026-09-23

Table of Contents

Chapter 1. Introduction

Palo Alto Idira Identity Security Platform (ISP) provides next-generation identity security by managing privileged credentials and access rights. This integration guide provides the steps to integrate the Palo Alto Idira Privileged Access Manager (PAM) - Self-Hosted solution with an Entrust nShield Hardware Security Modules (HSM). The integration uses the PKCS #11 cryptographic API.

1.1. Product configuration

Entrust tested the integration with the following versions:

Product	Version
Vault Server	v15.2.2.84
Central Policy Manager (CPM)	v15.2.1
Password Vault Web Access (PVWA)	v15.2.2
Windows Server	2025

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

HSM	Security World Software	Firmware	Netimage
Connect XC	13.6.18	12.72.4 (FIPS 140-2 certified)	13.6.18
nShield 5c	13.6.18	13.4.5 (FIPS 140-3 certified)	13.6.18
nShield Edge	13.6.15	12.72.2	N/A

1.3. Supported nShield functionality

Feature	Support
Key Generation	Yes

Feature	Support
1-of-N Operator Card Set	Yes
FIPS 140 Level 3 mode support	Yes
Key Management	Yes
K-of-N Operator Card Set	Yes
Common Criteria mode support	N/A
Key Import	Yes
Softcards	No
Load Sharing	Yes
Key Recovery	N/A
Module-only keys	Yes
Failover	Yes

1.4. Requirements

You must have:

- Access to the Entrust TrustedCare Portal. To request an account, contact nshield.support@entrust.com.
- Access to the Idira Privileged Access Manager - Self-Hosted software.

You should also familiarize yourself with:

- The Idira Privileged Access Manager - Self-Hosted documentation.
- The nShield Security World documentation.
- Your organization's certificate policy, certificate practice statement (CPS), and any security policies or procedures governing the administration of the PKI and HSM environment.
- The number of Administrator Cards in the Administrator Card Set (ACS), the quorum required for administrative operations, and the policies governing the management of these cards.
- The Security World compliance level. For more information, see FIPS 140 Level 3 compliance.

- Key attributes and requirements, such as key size, timeout settings, audit requirements, and key usage policies.
- Whether the Security World should be instantiated as recoverable or non-recoverable.

Chapter 2. Idira ISP deployment

The Idira ISP environment used for this integration is deployed across two Windows servers:

- Vault Server
- Components Server

2.1. Software

The following tables show the various software installed in the Vault Server and Component Server.

Windows and other prerequisite software installed:

	Vault Server	Components Server
Windows Server 2025	✓	✓
.NET Framework 4.8	✓	✓
ASP.NET 4.8	✓	✓
IIS 10.0		✓
IIS Management Console		✓

Application software installed:

	Vault Server	Components Server
Vault Server	✓	
Entrust nShield Security World software	✓	
Central Policy Manager (CPM)		✓
Password Vault Web Access (PVWA)		✓

2.2. Domain

The following table shows the domain for the Vault Server and Component Server.

	Vault Server	Components Server
Domain	WORKGROUP (not joined)	<domain-name> (joined)

Chapter 3. Install and configure the Entrust nShield HSM

- Install the nShield Security World Software
- Install the Entrust nShield HSM
- Enroll the Entrust nShield HSM
- Create a security world
- Select the protection method

3.1. Install the nShield Security World Software

1. Sign in to the Vault Server using an account with administrator privileges.
2. Install the Security World software.
   For detailed instructions, see the nShield Security World documentation.
3. Add the Security World utilities path to the system path.
   This path is typically `C:\Program Files\nCipher\nfast\bin`.
4. Run the `enquiry` utility to confirm that the Security World is in `operational` mode.

```
C:\Users\Administrator>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number
 mode                 operational
 version              13.6.18
```

5. Open firewall port 9004 for the Entrust nShield HSM connections.
6. If using Remote Administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).

3.2. Install the Entrust nShield HSM

Install the nShield Connect HSM. Condensed instructions are available in the Entrust TrustedCare Portal.

- How To: Locally Set up a new or replacement nShield Connect.
- How To: Set up new or replacement nShield 5s.
- How To: Remotely Setup a new or replacement nShield Connect.
- How To: Remotely Setup a new or replacement nShield Connect XC Serial Console

Model.

For detailed instructions see the Hardware install and setup guides.

3.3. Enroll the Entrust nShield HSM

1. Inform the HSM about the Vault Server.

   For instructions see Configuring the nShield HSM to use the client.

   If you are using a high-availability setup, repeat the client configuration for each HSM.

2. Enroll the Vault Server as a client of the HSM.

   For instructions see Configuring client computers to use the nShield HSM.

   If you are using a high-availability setup, repeat the enrollment for each HSM.

3. Run the `enquiry` utility to confirm that the HSM is in `operational` mode.

```
C:\Users\Administrator>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        6A74-1261-7843 810B-03E0-D947
 mode                 operational
 version              13.6.18
...
Module #1:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        6A74-1261-7843
 mode                 operational
 version              13.4.5
 ...
Module #2:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        810B-03E0-D947
 mode                 operational
 version              12.72.4
```

3.4. Create a security world

1. Create a new Security World, if one does not already exist, or copy an existing one.

   Follow your organization's security policy for this. For more information see Create a new Security World.

   

   ACS cards cannot be duplicated after the Security World is created. You may want to create extras in case of a card failure or a

> lost card.

2. Confirm the Security World is in a `Usable` state with the `nfkminfo` utility.

```
C:\Users\Administrator>nfkminfo
World
 generation  2
 state       0x3737000c Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
Module #2
 generation 2
 state      0x2 Usable
```

3.5. Select the protection method

OCS or Module protection can be used to authorize access to the keys protected by the HSM.

- Operator Cards Set (OCS) are smartcards that are presented to the physical smartcard reader of an HSM. For more information on OCS use, properties, and k-of-N values, see Operator Card Sets (OCS).
- Module protection has no passphrase.

Follow your organization's security policy to select an authorization access method.

1. Edit the `C:\Program Files\nCipher\nfast\cknfastrc` file containing the nShield PKCS #11 library environment variables per the selection above.
    - For module-protected keys:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
CKNFAST_LOADSHARING=1
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

    - For OCS-protected keys with K=1:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
CKNFAST_LOADSHARING=1
```

    - For OCS-protected keys and K>1:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
CKNFAST_LOADSHARING=1
NFAST_NFKM_TOKENSFILE=C:\ProgramData\nCipher\nfast-nfkm-tokensfile
```

2. If using OCS protection, edit the `C:\ProgramData\nCipher\Key Management Data\config\cardlist` configuration file.
   Instructions are in the file itself.

Chapter 4. Integrate the Entrust nShield HSM with the Idira ISP

4.1. Update dbparm.ini per the HSM

1. Sign in to the Vault Server using an account with administrator privileges.
2. Stop the Vault Server by selecting the **Stop Server** icon in the **Server Central Administration** window.
3. In the **Shutdown Server** pop-up window, select **Normal shutdown**.
4. Open `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` in a text editor.
5. Add the following directive pair for each HSM to the end of the `[MAIN]` section. This tells the Vault Server to create firewall rules for this IP/port combination.

   ```
   AllowNonStandardFWAddresses=[HSM_IP_ADDRESS],Yes,9004:outbound/tcp
   AllowNonStandardFWAddresses=[HSM_IP_ADDRESS],Yes,9005:outbound/tcp
   ```

   For example:

   ```
   ...
   TerminateOnDBErrorCodes=2003
   MinSupportedClientVersion=11.5.0.0
   MaxConcurrentUsersByClientID=6000(APPProv),10(Synchrnzr),1(CCP),1(DAP)
   AllowNonStandardFWAddresses=[xxx.xxx.xxx.xxx],Yes,9004:outbound/tcp
   AllowNonStandardFWAddresses=[xxx.xxx.xxx.xxx],Yes,9005:outbound/tcp
   AllowNonStandardFWAddresses=[xxx.xxx.xxx.xxx],Yes,9004:outbound/tcp
   AllowNonStandardFWAddresses=[xxx.xxx.xxx.xxx],Yes,9005:outbound/tcp
   [BACKUP]
   BackupKey=C:\keys\Backup.key
   [CRYPTO]
   ...
   ```

6. Append the path of the PKCS #11 provider library for the Entrust nShield HSM.

```
[HSM]
PKCS11ProviderPath="C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll"
```

7. Save and close the file.

4.2. Configure the Vault Server for OCS key protection

If you are using module-protected keys, skip this section and proceed to Generate the Vault Server key on the HSM.

1. Open a command prompt with administrator privileges and navigate to the following directory:

   ```
   cd "C:\Program Files (x86)\PrivateArk\Server"
   ```

2. Run `CAVaultManager` as follows, providing the OCS passphrase.

   ```
   .\CAVaultManager SecureSecretFiles /SecretType HSM /Secret "<OCS passphrase>"
   ```

   For example:

   ```
   C:\Program Files (x86)\PrivateArk\Server>.\CAVaultManager SecureSecretFiles /SecretType HSM /Secret
   "xxxxxxxx"
   ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
   ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-
   512 (Protocol Integrity), SHA2-512 (Files Integrity).
   CAVLT146I HSM secret was secured successfully.
   ```

   This command does not validate the passphrase against the OCS card. It only encrypts the passphrase and stores it in `dbparm.ini`.

   To validate the passphrase against the OCS card, run the nShield utility `cardpp -m1 --check` and enter the passphrase when prompted.

3. Use the `type` command to display the `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` file contents. Verify that the line `HSMPinCode=<encrypted OCS passphrase>` appears towards the end.

   For example:

   ```
   >type "C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini"
   ...
   [HSM]
   PKCS11ProviderPath="C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll"
   HSMPinCode=0F0C6B6D5CC378F95A3256068F690451DF279C3924F3BFC20AD6CCA7CF7FC30498DC3EA7D72E31AD02463E492DCA8655
   ```

4.3. Generate the Vault Server key on the HSM

If you are using a FIPS 140 Level 3 Security World, ensure that an OCS card is inserted into an available HSM slot to provide FIPS authorization before executing the following commands. An ACS cannot be used for FIPS authorization with this application.

If you are using module protection for the Vault Server key in a FIPS 140 Level 3 Security World, you must still create and use an OCS for FIPS authorization, even though it will not be used for key protection.

If load sharing is enabled across multiple HSMs while using module protection, insert an OCS card into each HSM participating in the Security World. The OCS quorum must be configured as 1/N.

1. Open a command prompt with administrator privileges and navigate to the following directory:

```
cd "C:\Program Files (x86)\PrivateArk\Server"
```

2. Depending on your needs, follow the steps in the relevant section:
   - Generate a new Vault Server key on the HSM (recommended)
   - Load an existing Vault Server key to the HSM

An Entrust nShield HSM configured with a FIPS 140 Level 3 Security World does not permit the import of existing keys. For enhanced security, Entrust recommends generating and protecting keys within the nShield HSM. Using an Entrust nShield HSM provides assurance that keys generated by the HSM remain protected from disclosure.

4.3.1. Generate a new Vault Server key on the HSM

- To generate a new key using module protection or an OCS with a 1-of-N quorum (K=1), run the `CAVaultManager` command:

```
C:\Program Files (x86)\PrivateArk\Server> .\CAVaultManager GenerateKeyonHSM /ServerKey
ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-
512 (Protocol Integrity), SHA2-512 (Files Integrity).
ITAFW052I Firewall is open for non standard address.
ITAFW052I Firewall is open for non standard address.
...
ITAFW052I Firewall is open for non standard address.
ITAFW052I Firewall is open for non standard address.
ITADM114I Successfully connected to Database, Database id 0.
CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#1).
```

- To generate a new key using an OCS with a K-of-N quorum where K > 1, start the `preload` utility before running the `CAVaultManager` command:

```
> preload -m <module number> -f "<preload FilePath>" --cardset-name=<OCS Cardset-Name> CAVaultManager
GenerateKeyonHSM /ServerKey
```

Example:

```
> preload -m 1 -f "C:\ProgramData\nCipher\nfast-nfkm-tokensfile" --cardset-name=testOCS CAVaultManager
GenerateKeyonHSM /ServerKey

2025-09-12 09:50:54: [4292]: INFO: Preload running with: -m 1 -f C:\ProgramData\nCipher\nfast-nfkm-
tokensfile --cardset-name=testOCS2 CAVaultManager GenerateKeyonHSM /ServerKey
2025-09-12 09:50:55: [4292]: INFO: Created a (new) connection to Hardserver
2025-09-12 09:50:55: [4292]: INFO: Modules newly usable: [1].
2025-09-12 09:50:55: [4292]: INFO: Found a change in the system: an update pass is needed.
2025-09-12 09:50:55: [4292]: INFO: Loading cardset: testOCS2 in modules: [1]

Loading `testOCS2':
 Module 1 slot 2: `testOCS2' #1
 Module 1 slot 0: empty
 Module 1 slot 3: empty
 Module 1 slot 4: empty
 Module 1 slot 5: empty
 Module 1 slot 2:- passphrase supplied - reading card
 Module 1 slot 2: `testOCS2' #1: already read
 Module 1 slot 2: empty
 Module 1 slot 2: `testOCS2' #2
 Module 1 slot 2:- passphrase supplied - reading card
Card reading complete.

2025-09-12 09:51:32: [4292]: INFO: Stored Admin key: kfips (003e...) in module #1
2025-09-12 09:51:32: [4292]: INFO: Loading cardset: Cardset: testOCS2 (f0b9...) in module: 1
2025-09-12 09:51:32: [4292]: INFO: Stored Cardset: testOCS2 (f0b9...) in module #1
2025-09-12 09:51:32: [4292]: INFO: Maintaining the cardset testOCS2 protected key(s)=[].
2025-09-12 09:51:32: [4292]: INFO: Loading complete. Executing subprocess CAVaultManager GenerateKeyonHSM
/ServerKey
ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-
512 (Protocol Integrity), SHA2-512 (Files Integrity).
ITADM114I Successfully connected to Database, Database id 0.
CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#1).
```

Note the Key ID, `KeyID=HSM#1`, at the end of the command output.

After you have generated a new key, verify it according to the procedure in Verify the Vault Server key.

4.3.2. Load an existing Vault Server key to the HSM

If you must use an existing Vault Server key:

1. Open `C:\Program Files\nCipher\nfast\cknfastrc` in a text editor and append the following line, then save and close the file.

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=wrapping_crypt
```

2. Load the software key:

   - To load an existing software key using module protection or an OCS with a 1-of-N quorum (K=1), run the `CAVaultManager` command:

     ```
     > .\CAVaultManager LoadServerKeyToHSM /WrapKey
     ```

     Example:

     ```
     C:\Program Files (x86)\PrivateArk\Server> .\CAVaultManager LoadServerKeyToHSM /WrapKey

     ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
     ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit),
     SHA2-512 (Protocol Integrity), SHA2-512 (Files Integrity).
     ITADM114I Successfully connected to Database, Database id 0.
     CAVLT143I Server Key was successfully uploaded to HSM device
     ```

   - To load an existing software key using an OCS with a K-of-N quorum where K > 1, start the `preload` utility before running the `CAVaultManager` command:

     ```
     > preload -m <module number> -f "<preload FilePath>" --cardset-name=<OCS Cardset-Name> CAVaultManager
     LoadServerKeyToHSM /WrapKey
     ```

3. Open `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` in a text editor and update `ServerKey` to reference the new uploaded key, then save and close the file.

   From:

   ```
   ServerKey=C:\keys\Server.key
   ```

   To:

   ```
   ServerKey=HSM
   ```

4.4. Verify the Vault Server key

Verify the newly generated or loaded key by running one of the following utilities. Note that the key is a PKCS #11 key named `CyberArk Server Key`.

- To verify the key using the **rocs** utility:

  ```
  C:\Program Files (x86)\PrivateArk\Server>rocs
  ```

```
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list keys
  No. Name                    App        Protected by
    1 Cyber-Ark Server Key    pkcs11     testOCS
rocs> exit
```

- To verify the key using the **nfkminfo** utility:

```
C:\Program Files (x86)\PrivateArk\Server>nfkminfo -l

Keys protected by cardsets:
 key_pkcs11_ucedb3d45a28e5a6b22b033684ce589d9e198272c2-92c66522d74cce447056ca72f3a048927e31c778 `Cyber-Ark
Server Key'
```

  - When using OCS protection, the key is listed under **Keys protected by cardsets:**.
  - When using module protection, the key is listed under **Keys with module protection:**.

4.5. Update dbparm.ini to reference the recovery private key

Idira IPS recommends storing the recovery private key on removable media. The path to the removable media is defined by the `RecoveryPrvKey` parameter in the `[MAIN]` section of `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini`.

For the purposes of this integration, the recovery private key is stored locally in the default installation directory `C:\keys\`.

Open `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` in a text editor and update `RecoveryPrvKey` as follows. Then save and close the file.

From:

```
RecoveryPrvKey=D:\RecPrv.key
```

To:

```
RecoveryPrvKey=C:\keys\RecPrv.key
```

4.6. Wrap the Vault Server keys with the HSM key

1. Back up the Vault Server keys.
   The default location, `C:\keys`, is used in this example. If you back up the keys to a

different location, use that path instead in the commands in this procedure.

2. Open a command prompt with administrator privileges and navigate to the following directory:

```
cd "C:\Program Files (x86)\PrivateArk\Server"
```

3. If using OCS protected keys, present the OCS card to the HSM and enter the OCS passphrase when prompted.
4. Run one of the following commands as required.
   The HSM key is `HSM#1`, as generated in the examples in Generate a new Vault Server key on the HSM.

   - For a module-protected key, or for OCS protected keys with K=1:

     ```
     > .\ChangeServerKeys C:\keys C:\keys\VaultEmergency.pass HSM#1
     ```

     Example:

     ```
     C:\Program Files (x86)\PrivateArk\Server>.\ChangeServerKeys C:\keys C:\keys\VaultEmergency.pass HSM#1
     17/09/2026 15:31:48 CHSRVK041I ChangeServerKeys process started.
     ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
     ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit),
     SHA2-512 (Protocol Integrity), SHA2-512 (Files Integrity).
     ITAFW051W Error open firewall for non standard address. Code: 4, -1.
     ITADM114I Successfully connected to Database, Database id 0.
     ITAQS031I Object cache is loaded.
     HSM generation 1 was chosen, are you sure you want to change server keys to HSM (y/n)?
     y
     Verify that the current master key is at C:\keys\RecPrv.key, and press any key.
     Verify new server's master key is at C:\keys, and press any key.

     17/09/2026 15:32:44 CHSRVK043I Signing entropy file C:\PrivateArk\Safes\entropy.rnd with new keys.
     17/09/2026 15:32:44 CHSRVK034I Encrypting server private key.
     ...
     17/09/2026 15:32:51 CHSRVK020I Keys of Safe AccountsFeedDiscoveryLogs changed successfully.
     17/09/2026 15:32:51 CHSRVK054I ChangeServerKeys process was successful. DBParm.ini must be updated to
     point to new keys for Vault Server to start.

     Do you want to update DBParm.ini with the new  keys location? Enter "NO" to quit or "YES" for update:
     YES
     17/09/2026 15:33:00 CHSRVK087I DBParm.ini file was successfully updated.
     17/09/2026 15:33:00 CHSRVK042I ChangeServerKeys process ended.
     ```

   - For OCS protected keys with K>1, start the `preload` utility first:

     ```
     > preload -m <module number> -f "<preload FilePath>" --cardset-name=<OCS Cardset-Name>
     ChangeServerKeys C:\keys C:\keys\VaultEmergency.pass HSM#1
     ```

5. Verify that the following files in `C:\keys\` were updated during this process:

- Backup.key
- ReplicationUser.pass
- Server.pvk
- VaultEmergency.pass
- VaultUser.pass

4.7. Update dbparm.ini to use the new HSM key

After the Vault Server keys have been wrapped with the HSM key HSM#1, update C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini to reference the new key:

1. Open C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini in a text editor.
2. Update ServerKey to reference the new HSM#1 key, then save and close the file.

```
ServerKey=HSM#1
```

If an existing Vault Server key was loaded into the HSM as described in Load an existing Vault Server key to the HSM, rather than generating a new HSM key as described in Generate a new Vault Server key on the HSM, set ServerKey=HSM instead of HSM#1.

4.8. Start the Vault Server

1. If using OCS protection, present the OCS card to an available HSM slot. For OCS protected keys with K>1, start the preload utility.

```
> preload -m <module number> -f "<preload FilePath>" --cardset-name=<OCS Cardset-Name> pause
```

2. Open the PrivateArk Server application and start the server.
3. Verify the server starts successfully with no reported errors.
4. Open Windows Event Viewer and verify that a client connection to the HSM was established to access the key.

   For example, under applications:

```
2026-09-17 16:50:28 t7524: Hardserver [FP]: Notice: CreateClient (v1) pid: 7952, process name: C:\Program
Files (x86)\PrivateArk\Server\dbmain.exe
```

5. On the Components Server, open a web browser and navigate to the Password Vault

Web Access (PVWA) URL and verify that you can successfully sign in.

Chapter 5. Test the integration between the Entrust nShield HSM and Idira ISP

This test consists of rotating the Vault Server keys.

1. Stop the Vault Server.
2. Back up the original HSM key blob files from `C:\ProgramData\nCipher\Key Management Data\local` and the Vault Server key files from `C:\keys\`.
3. Open a command prompt with administrator privileges and navigate to the following directory:

```
cd "C:\Program Files (x86)\PrivateArk\Server"
```

4. Generate a new Vault Server key on the HSM key following the instructions in Generate a new Vault Server key on the HSM.
   If the existing key is `HSM#1`, the new key will be `HSM#2`.

   For example:

```
C:\Program Files (x86)\PrivateArk\Server>.\CAVaultManager GenerateKeyonHSM /ServerKey
ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-
512 (Protocol Integrity), SHA2-512 (Files Integrity).
ITAFW052I Firewall is open for non standard address.
ITAFW052I Firewall is open for non standard address.
...
ITAFW052I Firewall is open for non standard address.
ITAFW052I Firewall is open for non standard address.
ITADM114I Successfully connected to Database, Database id 0.
CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#2).
```

5. Verify that the following key blob files correspond to the existing and newly generated key.

```
C:\Program Files (x86)\PrivateArk\Server>dir "C:\ProgramData\nCipher\Key Management Data\local" | findstr
key_pkcs11
09/16/2026  05:19 PM             7,248 key_pkcs11_ucedb3d45a28e5a6b22b033684ce589d9e198272c2-
92c66522d74cce447056ca72f3a048927e31c778
09/18/2026  09:09 AM             7,448 key_pkcs11_ucedb3d45a28e5a6b22b033684ce589d9e198272c2-
d4884f839e3754cc11c8ce34bb27a1355182a408
```

6. Wrap the Vault Server keys with the new HSM key following the instructions in Wrap the Vault Server keys with the HSM key.

   For example

```
C:\Program Files (x86)\PrivateArk\Server>.\ChangeServerKeys C:\keys C:\keys\VaultEmergency.pass HSM#2
```

```
18/09/2026 09:22:34 CHSRVK041I ChangeServerKeys process started.
ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-
512 (Protocol Integrity), SHA2-512 (Files Integrity).
ITAFW051W Error open firewall for non standard address. Code: 4, -1.
ITADM114I Successfully connected to Database, Database id 0.
ITAQS031I Object cache is loaded.
HSM generation 2 was chosen, are you sure you want to change server keys to HSM (y/n)?
y
Verify that the current master key is at C:\keys\recprv.key, and press any key.
Verify new server's master key is at C:\keys, and press any key.

18/09/2026 09:22:56 CHSRVK043I Signing entropy file C:\PrivateArk\Safes\entropy.rnd with new keys.
18/09/2026 09:22:56 CHSRVK034I Encrypting server private key.
...
18/09/2026 09:22:59 CHSRVK020I Keys of Safe AccountsFeedDiscoveryLogs changed successfully.
18/09/2026 09:22:59 CHSRVK054I ChangeServerKeys process was successful. DBParm.ini must be updated to point
to new keys for Vault to start.

Do you want to update DBParm.ini with the new  keys location? Enter "NO" to quit or "YES" for update:
YES
18/09/2026 09:23:09 CHSRVK087I DBParm.ini file was successfully updated.
18/09/2026 09:23:09 CHSRVK042I ChangeServerKeys process ended.
```

7. Update `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` to reference the new `HSM#2` key following the instructions in Update dbparm.ini to use the new HSM key.

```
ServerKey=HSM#2
```

8. **IMPORTANT:** Verify that a backup of the original HSM key blob files and the Vault Server key files exists before proceeding.
9. Remove the original HSM key blob file from `C:\ProgramData\nCipher\Key Management Data\local` so only the new key blob file remains.

```
C:\Program Files (x86)\PrivateArk\Server>dir "C:\ProgramData\nCipher\Key Management Data\local" | findstr
key_pkcs11
09/18/2026  09:09 AM             7,448 key_pkcs11_ucedb3d45a28e5a6b22b033684ce589d9e198272c2-
d4884f839e3754cc11c8ce34bb27a1355182a408
```

10. Start the Vault Server as described in Start the Vault Server.

Chapter 6. Additional resources and related products

6.1. nShield HSMs

6.2. nShield as a Service

6.3. Entrust products

6.4. nShield product documentation