CyberArk Privilege Access Security Enterprise Password Vault

nShield® HSM Integration Guide

2024-10-21

Table of Contents

Chapter 1. Introduction

CyberArk Privilege Access Security Enterprise Password Vault (CyberArk PAS EPV) manages privileged credentials and access rights. This integration guide provides the steps to integrate CyberArk PAS EPV 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	v14.2.1
Central Policy Manager (CPM)	v14.2
Password Vault Web Access (PVWA)	v14.2.1
Windows Server	2022

1.2. Supported nShield hardware and software versions

Entrust has successfully tested nShield HSM integration with CyberArk PAS in the following configurations:

CyberArk PAS	nShield Hardware	nShield (Connect) Image	nShield HSM Firmware	Security World Software
12.1	Connect XC	12.60.10	12.50.11 (FIPS 140-2 certified)	12.60.11
12.1	Connect Plus	12.60.10	12.50.8 (FIPS 140-2 certified)	12.60.11

CyberArk PAS	nShield Hardware	nShield (Connect) Image	nShield HSM Firmware	Security World Software
12.6	Connect XC	12.80.4	12.50.11 (FIPS 140-2 certified)	12.80.4
12.6	Connect Plus	12.80.4	12.50.8 (FIPS 140-2 certified)	12.80.4
12.6	Connect XC	12.80.5	12.72.1 (FIPS 140-2 certified)	12.80.4
12.6	Connect Plus	12.80.5	12.72.0 (FIPS 140-2 certified)	12.80.4
12.6	nShield Edge [1]	N/A	12.50.8 (FIPS 140-2 certified)	12.71.0
12.6	nShield 5c	13.2.2	13.2.2	13.2.2
13.2	Connect XC	12.80.5	12.72.1 (FIPS 140-2 certified)	13.4.4
13.2	nShield Edge	N/A	12.72.0 (FIPS 140-2 certified)	13.4.4
13.2	nShield 5c	13.3.2	13.2.2	13.4.4
14.2	nShield 5c	13.6.1	13.2.4 (FIPS 140-3 certified)	13.6.3

[1] This nShield Edge test case tested by CyberArk.

1.3. Supported nShield functionality

Feature	Support
Key Generation	Yes
1-of-N Operator Card Set	Yes
FIPS 140 Level 3 mode support	Yes

Feature	Support
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

To integrate the Entrust nShield HSM and the CyberArk PAS EPV, you require:

- Two dedicated Windows servers for the installation of CyberArk PAS EPV.
- Access to the CyberArk Market Place at https://cyberark.my.site.com/mplace/s/#software.
- Access to Entrust TrustedCare Portal https://trustedcare.Entrust.com/.

Familiarize yourself with:

- The documentation and set-up process for CyberArk PAS EPV.
- The Entrust nShield HSM: *Installation Guide* and *User Guide*.
- Your organizational Security Policy or Procedure in place:
  - 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 keys protection method: Module, or OCS.
  - The level of compliance for the Security World, FIPS 140 Level 3.
  - Key attributes such as key size, time-out, or needed for auditing key usage.

Chapter 2. CyberArk PAS EPV deployment

The CyberArk PAS EPV installation requires two Windows Server virtual machines (VMs):

- Vault server
- Components server.

2.1. Software

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

Windows and other pre-requisite software installed:

Vault Server VM	Components Server VM
Windows Server 2022	Windows Server 2022
.NET Framework 4.8 or higher	.NET Framework 4.8 or higher
	ASP.NET 4.6 or higher
	IIS 7.5 or higher
	IIS Management Console
	IIS 6 Metabase Compatibility

Application software installed:

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

2.2. Domain

The following table shows the domain for the Vault server and Component server VMs.

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

2.3. Licensing

The `keys-master` folder should be kept on removable media, for example a CD.

The CyberArk Digital Vault Security Standard states the following about the `keys-master` folder: The Recovery Private Key (Master CD) should be stored in a physical safe. The `recprv.key` file in this folder is considered extremely sensitive. It is normally never stored on the server. Rather, it is kept on removable media and stored in a safe until needed for the `ChangeServerKeys.exe` command in Rewrap the CyberArk PAS Vault key from the software to HSM.

Chapter 3. Install and configure the Entrust nShield HSM

3.1. Install the HSM

Install the nShield Connect 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.

The complete instruction set is available at nShield v13.6.3 HSM User Guide.

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

Perform these steps in the CyberArk PAS EPV Vault server.

1. Install the Security World software by executing file `setup.msi`. The complete instruction set is available at nShield Security World Software v13.6.3 Installation Guide.
2. Add the Security World utilities path `C:\Program Files\nCipher\nfast\bin` to the Windows system path.
3. Open firewall port 9004 for the Entrust nShield HSM connections.
4. If using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).
5. Configure the CyberArk PAS EPV Vault server as a client Entrust nShield HSM.
6. Open a command window and run the following to confirm the HSM is `operational`.

```
C:\Users\Administrator>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number
 mode                 operational
 version              13.6.3
...
Module #1:
```

```
enquiry reply flags  none
enquiry reply level  Six
serial number        7852-268D-3BF9
mode                 operational
version              13.2.4
...
```

7. Create your Security World if one does not already exist or copy an existing one. Follow your organization's security policy for this. Create extra ACS cards as spares in case of a card failure or a lost card.

   ACS cards cannot be duplicated after the Security World is created.

8. Confirm the Security World is `usable`.

```
C:\ProgramData\nCipher\Key Management Data>nfkminfo
World
 generation  2
 state       0x3737000c Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

3.3. 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 the *User Guide* for your HSM.
- Module protection has no passphrase.

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

1. Edit the `cknfastrc` configuration file based on the selected protection method. This file is located in the *%NFAST_HOME%* directory, which is typically `C:\Program Files\nCipher\nfast`.

   If you get a permissions error trying to edit the file, right select **cknfastrc > Properties > Security > Edit Users** and check **Allow for Full Control**. After editing the file, you can remove full control. Ensure that the **Read** and **Read & execute** options are selected.

- If you are using module-protected keys:

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

- If you are using OCS-protected keys and K=1:

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

- If you are using 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 `cardlist` configuration file. This file is located in the `C:\ProgramData\nCipher\Key Management Data\config` directory.

Chapter 4. Integrate the Entrust nShield HSM with CyberArk PAS EPV

4.1. Stop the Vault Server

To stop the Vault Server:

1. Open the PrivateArk Server application.
2. Select the red stoplight button.
3. Select **Normal shutdown**. Then select **OK**.
4. Select **Yes**.

4.2. Configure the CyberArk dbparm.ini file

1. In the Vault server, edit the file `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini`.

   To comment out items in the `dbparm.ini` file, use an asterisk (*) at the beginning of the line.

2. If you are using an nShield Connect XC or nShield 5c, add the following `AllowNonStandardFWAddresses` directives to the end of the `[main]` section. This tells the Vault server to create firewall rules for this IP/port combination.

   ```
   AllowNonStandardFWAddresses=[HSM.IP.ADD.RESS],Yes,9004:outbound/tcp
   AllowNonStandardFWAddresses=[HSM.IP.ADD.RESS],Yes,9005:outbound/tcp
   ```

3. Repeat the previous step for each HSM that needs to communicate with the Vault server.
4. Add the location of the PKCS#11 provider for the Entrust nShield HSM at the end of the file.
   - For 12.50.xx and earlier Entrust nShield Security World clients:

     ```
     [HSM]
     PKCS11ProviderPath="C:\Program Files (x86)\nCipher\nfast\toolkits\pkcs11\cknfast-64.dll"
     ```

   - For 12.60.xx and later Entrust nShield Security World clients:

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

5. Save and close the `dbparm.ini` file.

4.3. Start and stop the Vault Server

Start then stop the Vault server to process the new firewall rules from the `AllowNonStandardFWAddresses` directives just added to the `dbparm.ini` file:

1. Open the PrivateArk Server application.
2. Select the green stoplight button.
3. When the server starts, you should the following output indicating the new firewall rules were processed:

```
Firewall contains external rules.
Firewall is open for client communication
Firewall is open for non standard address.
Firewall is open for non standard address.
Firewall is open for non standard address.
Firewall is open for non standard address.
```

4. Select the red stoplight button after the server comes up.
5. Select **Normal shutdown**. Then select **OK**.
6. Select **Yes**.
7. Validate that the HSM communication works:
   a. Run the `enquiry` and `nfkminfo` commands in a command prompt.
   b. Verify that the module is operational and the world state is **Usable** and **Initialized**.

4.4. Configure the CyberArk PAS EPV Vault for OCS key protection

If you are using module-protected keys, skip this section and continue with Regenerate the CyberArk PAS EPV Vault key on the HSM.

If you are using OCS-protected keys:

1. In the Vault server, open a command window as administrator.
2. Make the required directory current:

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

3. Run `CAVaultManager` providing the OCS passphrase:

```
C:\Program Files (x86)\PrivateArk\Server>CAVaultManager SecureSecretFiles /SecretType HSM /Secret "<OCS
passphrase>"
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 adds it to `dbparm.ini`. If you want to validate the passphrase against the OCS card to make sure have it correct, use `cardpp -m1 --check` and enter the passphrase when prompted.

4. Open the `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` file and verify that the line `HSMPinCode=<encrypted OCS passphrase>` appears towards the end.

   For example:

```
...
[HSM]
PKCS11ProviderPath="C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll"
HSMPinCode=A4FEFBD484E3FBB8B14BAC7051F923ACFA73458B22E6DBB082ADFBE46C93626F5E97A11144872DD8BA823321759F41CB
```

5. Close the `dbparm.ini` file.

Chapter 5. Test the integration between the Entrust nShield HSM and CyberArk PAS EPV

5.1. Regenerate the CyberArk PAS EPV Vault key on the HSM

If you are using a FIPS 140 Level 3 Security World, ensure that a recognized OCS card is inserted into an available slot of the HSM to provide FIPS authorization before running the following commands. An ACS cannot be used for FIPS authorization for this application. If you are using module protection for your Vault key in a FIPS 140 Level 3 world, you still need to create and use an OCS for FIPS authorization, but not key protection. If loadsharing across multiple HSMs is enabled while using module protection, insert an OCS into slot 0 of each HSM sharing the Security World. The K/N quorum must be 1/N.

1. Open a command prompt as administrator.
2. Got to either:
    - Generate a new Vault Server key on the HSM.
    - Load an existing Vault Server key to the HSM.

5.1.1. Generate a new Vault Server key on the HSM

1. Make the required directory current:

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

2. If you are generating a new key using module protection, or OCS K-of-N with K=1:

```
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).
ITADM114I Successfully connected to Database, Database id 0.
CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#1).
```

3. If you are generating a new key using OCS K-of-N with K>1, use `preload` to launch `CAVaultManager`. Enter the OCS passphrase when prompted. For example:

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

2021-07-20 07:54:32: [2432]: INFO: Preload running with: -m1 -f <preload FilePath> --cardset-name=<OCS
Cardset-Name> CAVaultManager.exe GenerateKeyOnHSM /ServerKey
...
2021-07-20 07:55:17: [2432]: INFO: Loading complete. Executing subprocess CAVaultManager.exe
GenerateKeyOnHSM /ServerKey
...
CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#1).
```

Note down the `KeyID` that is at the end of the command output. It is required for modifying the `ServerKey` directive in `dbparam.ini` and later steps.

5.1.2. 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 using keys created and protected by the nShield HSM. The use of an HSM assures customers that keys created by the Entrust nShield HSM are protected from issuance.

1. If you are using module protection or OCS K-of-N with K=1:

   ```
   % CAVaultManager LoadServerKeyToHSM /WrapKey
   ...
   CAVLT143I Server Key was successfully uploaded to HSM device
   ```

2. If you are loading an existing software key using OCS K-of-N with K>1, use `preload` to launch `CAVaultManager`:

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

3. Open the `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` file and change the `ServerKey` line now.

   Change from:

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

   Change to:

   ```
   ServerKey=HSM
   ```

5.1.3. Verify the Vault Server key

Verify the new generated or loaded key with the following command, a PKCS #11 key called `Cyber-Ark Server 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
```

Using the **nfkminfo** utility.

```
C:\Users\Administrator>nfkminfo -l

Keys protected by cardsets:
 key_pkcs11_ucedb3d45a28e5a6b22b033684ce589d9e198272c2-1438e9e578e8f89d5eb5a20163459586801a3cb0 `Cyber-Ark Server
Key'
```

- If you used OCS, the key should be listed under `Keys protected by cardsets`.
- If you used module protection, the key should be listed under `Keys with module protection`.

5.2. Modify dbparm.ini to point to the recovery private key

In the `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` file, modify the `RecoveryPrvKey` line in the `[main]` section to point to the master private key so that the PAS key can be rewrapped from the software key to the HSM key.

- Change from:

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

- Change to:

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

If you are keeping your Recovery Private Key on removable media as recommended, set the `RecoveryPrvKey` attribute to the appropriate location rather than using `C:\keys-master\RecPrv.key`.

5.3. Rewrap the CyberArk PAS Vault key from the software to HSM

If you are using OCS protected keys, ensure that a card from the relevant OCS is available to the HSM.

1. Back up the content of the `keys` folder (default location: `C:\keys`) to another location.
2. Open a command prompt as administrator.
3. Make the required directory current:

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

4. Rewrap the Vault secrets.

   If you are keeping your Recovery Private Key on removable media as recommended, use the appropriate path instead of `C:\keys-master`.

   The `KeyID` (`HSM#1`) in the following command should match the output of Regenerate the CyberArk PAS EPV Vault key on the HSM. If not, change it in the command to match it.

   If you loaded an existing key to the HSM using `CAVaultManager LoadServerKeyToHSM /WrapKey` in Regenerate the CyberArk PAS EPV Vault key on the HSM, change `HSM#1` to `HSM`.

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

     ```
     C:\Program Files (x86)\PrivateArk\Server>ChangeServerKeys C:\keys-master C:\keys\VaultEmergency.pass
     HSM#1
     17/09/2024 15:33:26 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).
     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-master\RecPrv.key, and press any key.
     Verify new server's master key is at C:\keys-master, and press any key.

     17/09/2024 15:34:10 CHSRVK043I Signing entropy file C:\PrivateArk\Safes\entropy.rnd with new keys.
     ...
     17/09/2024 15:34:14 CHSRVK054I ChangeServerKeys process was successful. DBParm.ini must be updated to
     point to new keys for Vault to start.
     17/09/2024 15:34:14 CHSRVK042I ChangeServerKeys process ended.
     ```

   - If you are using OCS keys and K-of-N with K>1, you must use the `preload` command. Insert the OCS cards and enter the OCS passphrase when

prompted.

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

5. Verify the following files in `C:\keys` changed during this process:
   - `Backup.key`
   - `ReplicationUser.pass`
   - `Server.pvk`
   - `VaultemErgency.pass`
   - `VaultUser.pass`

5.4. Modify dbparm.ini to use the new HSM key

1. Edit the `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` file.
2. Modify the `ServerKey` line in the `[main]` section to point to the new HSM key.

   `HSM#1` is the `KeyID` taken from the output of the `CAVaultManager GenerateKeyonHSM /ServerKey` command executed in Regenerate the CyberArk PAS EPV Vault key on the HSM:
   - Change from:

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

   - Change to:

     ```
     ServerKey=HSM#1
     ```

   If the server key was loaded to the HSM using `CAVaultManager LoadServerKeyToHSM /WrapKey` in Regenerate the CyberArk PAS EPV Vault key on the HSM, change `HSM#1` to `HSM`.

3. Save and close the `dbparm.ini` file.

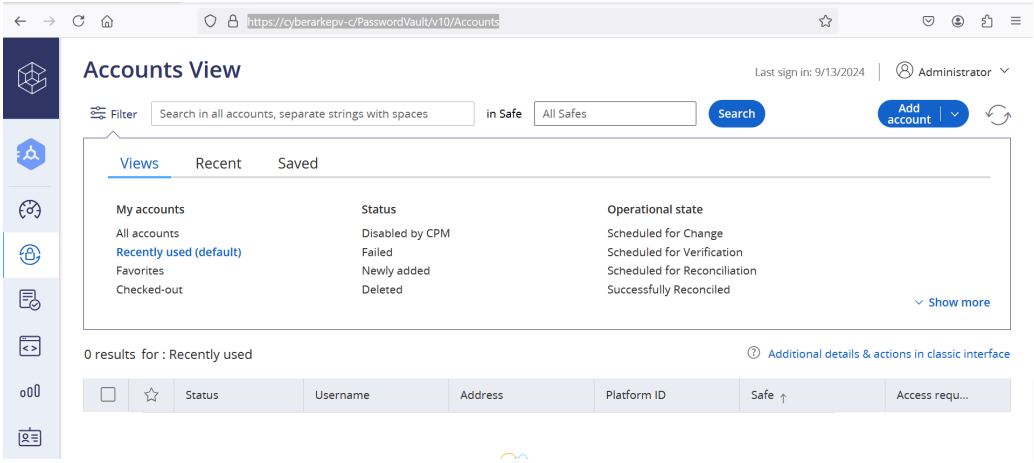
5.5. Start the Vault Server

If you are using OCS-protected keys, ensure that a card from the relevant OCS is available to the HSM.

1. If you are using OCS key protection with K>1 for K-of-N, you have to use the `preload` command every time the Vault Server is started. Otherwise, skip this step.
    a. Open a command prompt as administrator.
    b. Run the following `preload` command:

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

    c. Insert the OCS cards and enter the OCS passphrase when prompted.
2. Open the PrivateArk Server application.
3. Start the PrivateArk Server by selecting the green stoplight button.
4. Ensure the server starts with no errors in the output.
5. Verify you can log in to the Vault web access using CyberArk authentication:
    a. From the Components server, browse to the Password Vault Web Access URL defined during installation of the PAS Password Vault Web Access Component.
    b. Log in using the credentials specified during installation.



6. Open the Windows Event Viewer on the Vault server to show that a client connection was made to the HSM to access the key:
    a. Start Windows Event Viewer and navigate to **Windows Logs > Application**.
    b. The following is an example of the Windows Event Viewer **Windows Logs > Application** Event Log:

```
2021-07-16 09:30:44 t1124: Hardserver [FP]: Notice: CreateClient (v1) pid: 2660, process name:
C:\Program Files (x86)\PrivateArk\Server\dbmain.exe
```

5.6. Rotate and migrate CyberArk Vault Server keys

1. Stop the Vault Server:
   a. Open the PrivateArk Server application.
   b. Select the red stoplight button.
   c. Select **Normal shutdown**.
   d. Select **OK**.
   e. Select **Yes**.
2. Back up the original HSM keys from the `C:\ProgramData\nCipher\Key Management Data\local` and the CyberArk `C:\keys` directories.
3. Create another HSM key.

   If the existing key is `HSM#1`, the new one should be `HSM#2`.

   - If you are generating a new HSM key using module protection, or OCS K-of-N with K=1:

     ```
     % CAVaultManager GenerateKeyonHSM /ServerKey
     ...
     CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#2)
     ```

   - If you are generating a new HSM key using OCS K-of-N with K>1, use `preload` to launch CAVaultManager. Insert the OCS cards and enter the passphrase when prompted.

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

4. Rotate the server keys to the new HSM key:
   - For a module-protected key, or for an OCS with K=1, rewrap the Vault secrets with the following:

     ```
     % C:\Program Files (x86)\PrivateArk\Server>ChangeServerKeys C:\keys-master
     C:\keys\VaultEmergency.pass HSM#2
     07/10/2024 10:27:06 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).
     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-master\RecPrv.key, and press any key.
     Verify new server's master key is at C:\keys-master, and press any key.

     07/10/2024 10:27:39 CHSRVK043I Signing entropy file C:\PrivateArk\Safes\entropy.rnd with new keys.
     07/10/2024 10:27:39 CHSRVK034I Encrypting server private key.
     07/10/2024 10:27:39 CHSRVK058I Encrypting Backup key.
     ```

```
07/10/2024 10:27:39 CHSRVK057I Encrypting Database access passwords.
...
07/10/2024 10:27:44 CHSRVK054I ChangeServerKeys process was successful. DBParm.ini must be updated to
point to new keys for Vault to start.
07/10/2024 10:27:44 CHSRVK042I ChangeServerKeys process ended.
```

- If you are using OCS keys and K-of-N k>1, you have to use the `preload` command. Insert the OCS cards and enter the passphrase when prompted.

```
% preload -m <module number> -f "<preload FilePath>" --cardset-name=<OCS Cardset-Name>
ChangeServerKeys C:\keys-master C:\keys\VaultEmergency.pass HSM#2
```

5. Update `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini` to point to the new key.
   - Change from:

```
ServerKey=HSM#1
```

   - Change to:

```
ServerKey=HSM#2
```

If a key was loaded to the HSM using `CAVaultManager LoadServerKeyToHSM /WrapKey`, then change `HSM` to `HSM#2`, and not `HSM#1` to `HSM#2`.

6. Save and close the `dbparm.ini` file.
7. Confirm that your original HSM key has been backed up.
8. Remove the original HSM key from `C:\ProgramData\nCipher\Key Management Data\local` to ensure that the Vault starts with the new key.
9. If you are using OCS key protection with K>1 for K-of-N:
   a. Open a command prompt as administrator.
   b. Run the following command:

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

   c. Insert the OCS cards and enter the passphrase when prompted.
10. Start the Vault server by selecting the green stoplight button in the PrivateArk Server application.

11. Verify the Vault server starts with no errors in the console output.
12. Optionally, open Windows Event Viewer. Verify in **Windows Logs > Application** the following line is present, indicating the new Vault server key was retrieved from the HSM to start the server:

```
Hardserver [FP]: Notice: CreateClient (v1) pid: 3788, process name: C:\Program Files
(x86)\PrivateArk\Server\dbmain.exe
```

Chapter 6. Additional resources and related products

6.1. nShield Connect

6.2. nShield as a Service

6.3. Entrust digital security solutions

6.4. nShield product documentation