CyberArk Privilege Access Security Enterprise Password Vault

nShield® HSM Integration Guide

29 Jul 2022

Contents

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. Requirements

The CyberArk PAS EPV installation requires two Windows Server virtual machines (VMs), one for the Vault, and one for the components. You can download the product binaries from https://support.cyberark.com/SFE/files.aspx.

Component	Minimum Requirement
Memory	4 GB
Processor	1 CPU
Processor Cores	2
Hard Disk	60 GB
CD or DVD	Optional
Network Adapter	1 (to communicate with the HSM and between the two CyberArk PAS server VMs)
USB Controller	Optional (if nShield Remote Administration is used)
Display	Standard configuration

System components required for installation:

On the Vault Server	On the Components Server
Windows Server 2016 or Windows Server 2019	Windows Server 2016 or Windows Server 2019
Cannot be part of a domain	Active Directory (optional)[1]
Windows Firewall must be active	Windows Firewall must be active (optional)
Static IP	Static IP
Disable IPv6	Disable IPv6

On the Vault Server	On the Components Server
.NET Framework 4.8	.NET Framework 4.8
Microsoft Visual C++ Redistributable for Visual Studio 2015-2019	ASP .NET 4.6
	IIS 10

nShield components required for installation:

On the Vault Server	On the Components Server
nShield Security World software	None

CyberArk components required for installation:

On the Vault Server	On the Components Server
CyberArk PAS PrivateArk Vault Server v12.6	CyberArk Central Policy Manager (CPM) v12.6
CyberArk PAS PrivateArk Client v12.6	CyberArk Password Vault Web Access (PVWA) v12.6
	CyberArk PrivateArk Client (optional)[2]
	CyberArk Privileged Session Manager (optional)[3]

[1] If you want this to be a domain to serve CyberArk clients.

[2] If you plan to use this server as a CyberArk client as well. Not required if only hosting the PAS web server.

[3] This component requires Microsoft Remote Desktop Services (RDS) Session Host and Windows update KB2999226.

Familiarize yourself with:

- The documentation for the nShield Connect HSM.
- The documentation and set-up process for CyberArk PAS EPV.

The following preparations need to be made before starting to use nShield products:

- For creation of the Security World, determine who within the organization act as custodians of the administrator card set (ACS).

- Obtain enough blank smartcards to create the ACS. 6 cards are delivered with the nShield Connect HSM.
- Define the Security World parameters. For details of the security implications of the choices, see the *nShield Security Manual*.

1.2. Licensing

Copy the `keys` folder provided by CyberArk to the `C:\` directory of the VM for the CyberArk PAS Vault server. This is the location to which the installer points for the keys and `license.xml` file.

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.

1.3. Product configurations

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	12.60.11
12.1	Connect Plus	12.60.10	12.50.8	12.60.11
12.6	Connect XC	12.80.4	12.50.11	12.80.4
12.6	Connect Plus	12.80.4	12.50.8	12.80.4

1.4. Supported nShield functionality

Feature	Support
Key Generation	Yes
1-of-N Operator Card Set	Yes
FIPS 140-2 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

2. Procedures

Configure CyberArk to use the nShield HSM from the Vault VM.

2.1. 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**.
4. Select **OK**.
5. Select **Yes**.

2.2. Install and configure the nShield HSM

This guide does not cover the basic installation and configuration of the nShield HSM or the nShield Security World client software. For instructions, see the *Installation Guide* for your HSM.

The following lines need to be added to `cknfastrc` configuration file of the Security World. The file is 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
```

In this example, `C:\ProgramData\nCipher\nfast-nfkm-tokensfile` is the location for creating the `preload` file. You can change it to another location as required.

2.3. Configure the CyberArk dbparm.ini configuration file

To configure the CyberArk `dbparm.ini` configuration file:

1. Edit the Vault Server file in `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. 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 nShield HSM at the end of the file.
   - For 12.50.xx and earlier nShield Security World clients:

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

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

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

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

2.4. 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**.
6. Select **OK**.
7. Select **Yes**.
8. 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**.

2.5. Configure the CyberArk PAS Vault for OCS key protection

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

If you are using OCS-protected keys:

1. Open a command prompt as administrator.
2. Run the following command:

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

3. Run CAVautManager providing the OCS passphrase as shown:

```
% CAVaultManager SecureSecretFiles /SecretType HSM /Secret "<OCS passphrase>"
...
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 following line appears towards the end:

```
HSMPinCode=<encrypted OCS passphrase>
```

5. Close the `dbparm.ini` file.

2.6. Regenerate the CyberArk PAS Vault key on the HSM

If you are using a FIPS 140-2 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 140-2 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. Either:
   - Generate a new Vault Server key on the HSM.
   - Load an existing Vault Server key to the HSM.
3. Verify the Vault Server key.

2.6.1. Generate a new Vault Server key on the HSM

To 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:

```
% CAVaultManager GenerateKeyonHSM /ServerKey
...
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.

2.6.2. Load an existing Vault Server key to the HSM

To load an existing Vault Server key to the HSM:

An Entrust nShield HSM configured with a FIPS 140-2 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 nShield 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
```

4. Check the new key with the following command:

```
% nfkminfo -l
```

2.6.3. Verify the Vault Server key

Verify in the output there is a PKCS#11 key called `Cyber-Ark Server Key`:

```
Keys protected by cardsets:
 key_pkcs11_uc... '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`.

2.7. 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`.

2.8. 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. 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`.

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

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

     ```
     % ChangeServerKeys C:\keys-master C:\keys\VaultEmergency.pass HSM#1
     ...
     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. [ENTER]
     Verify new server's master key is at C:\keys-master, and press any key.[ENTER]
     ...
     ChangeServerKeys process was successful. DBParm.ini must be updated to point to new keys for Vault to start.
     ```

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

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

   Insert the OCS cards and enter the OCS passphrase when prompted.

4. Verify that the `KeyID` (`HSM#1`) matches the output of Regenerate the CyberArk PAS Vault key on the HSM. If not, change it in the command to match it.

The following files in `C:\keys` change during this process:

- `backup.key`
- `replicationuser.pass`
- `server.pvk`
- `vaultemergency.pass`
- `vaultuser.pass`

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

To 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 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 Vault key on the HSM, change `HSM#1` to `HSM`.

   This step may have already been completed if the `ChangeServerKeys` command ran successfully.

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

2.10. 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. Once the Vault has started, you can end the paused `preload` session and close the command prompt if one was used.
6. 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.
7. 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
```

3. Rotate and migrate CyberArk Vault Server keys

To rotate and migrate CyberArk 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:

    ```
    % ChangeServerKeys C:\keys-master C:\keys\VaultEmergency.pass HSM#2
    ```

    - 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 `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. Once the Vault has started, you can end the paused `preload` session and close the command prompt if one was used.
13. 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
    ```