



CYBERARK PRIVILEGED ACCESS MANAGER

Integration Guide

Applicable Devices:

CryptoHub



THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION PROPRIETARY TO FUTUREX, LP. ANY UNAUTHORIZED USE, DISCLOSURE, OR DUPLICATION OF THIS DOCUMENT OR ANY OF ITS CONTENTS IS EXPRESSLY PROHIBITED.

TABLE OF CONTENTS

[1] DOCUMENT INFORMATION 3

 [1.1] DOCUMENT OVERVIEW 3

 [1.2] APPLICATION DESCRIPTION 3

[2] FUTUREX CERTIFICATION PROCESS 4

[3] PREREQUISITES 5

[4] CRYPTOHUB INSTRUCTIONS 6

 [4.1] DEPLOY THE CYBERARK SERVICE 6

 [4.2] CREATE A NEW ENDPOINT 6

[5] INSTALL FUTUREX PKCS #11 ON THE CYBERARK SERVER 7

[6] CONFIGURE CYBERARK VAULT TO INTEGRATE WITH CRYPTOHUB 8

 [6.1] INITIAL VAULT CONFIGURATIONS 8

 [6.2] LOAD THE SERVER KEY INTO THE CRYPTOHUB 8

APPENDIX A: XCEPTIONAL SUPPORT 10

[1] DOCUMENT INFORMATION

[1.1] DOCUMENT OVERVIEW

The purpose of this document is to provide information regarding the configuration of the Futurex CryptoHub with CyberArk's Privileged Access Manager (PAM) solution using PKCS #11 libraries. For additional questions related to your CryptoHub, see the relevant administrator's guide.

[1.2] APPLICATION DESCRIPTION

CyberArk's Privileged Access Manager (PAM) solution is a full life-cycle solution for managing the most privileged accounts and SSH Keys in the enterprise. It enables organizations to secure, provision, manage, control and monitor all activities associated with all types of privileged identities, such as:

- Administrator on a Windows server
- Root on a UNIX server
- Cisco Enable on a Cisco device
- Embedded passwords found in applications and scripts

The Privileged Access Manager provides a 'Safe Haven' within your enterprise where all your administrative passwords can be securely archived, transferred and shared by authorized users, such as IT staff, on-call administrators, and local administrators in remote locations.

The multiple security layers (including Firewall, VPN, Authentication, Access control, Encryption, and more) that are at the heart of the Privileged Access Manager offer you the most secure solution available for storing and sharing passwords in an enterprise environment.

After the CyberArk Vault has been installed and has started successfully, you can generate a new Server key on the CryptoHub.

The Server Key is the key used to "open" the Vault, much like the key of a physical Vault. The key is required to start the Vault, after which the Server key can be removed until the Server is restarted. When the Vault is stopped, the information stored in the Vault is completely inaccessible without that key.

[2] FUTUREX CERTIFICATION PROCESS

The Futurex Certification Process is a rigorous and standardized approach to testing and certifying integrations between third-party applications and the Futurex CryptoHub. The certification process is designed to ensure that third-party application integrations are fully tested and validated in a lab environment before they are deployed in a production environment. Futurex's Integration Engineering team implements this process so that customers can have confidence that third-party applications will integrate seamlessly with Futurex CryptoHub devices, and that all operations will result in the expected behavior. The certification process involves several steps, including research, testing, troubleshooting, and certification, and is fully documented in an integration guide for each integration. The full process is outlined below:

1. Research the third-party application to gain a general understanding of the solution and the protocol it uses to integrate with CryptoHub (i.e., PKCS #11, Microsoft CNG, JCE, OpenSSL Engine, KMIP).
2. Determine the scope of the third-party application's use of the CryptoHub, including the specific functionalities it utilizes (i.e., data encryption, key protection, entropy, etc.).
3. Install and configure the third-party application in a lab environment, where all testing and validation will take place.
4. Establish a connection between the third-party application and the CryptoHub, which typically involves configuring TLS certificates and creating roles and identities that the third-party application will use to connect and authenticate to the CryptoHub.
5. Initiate a request from the third-party application to the CryptoHub, such as generating keys or certificates, encrypting or decrypting data, or other cryptographic functions.
6. If any errors occur during the testing process, the Integration Engineering team will diagnose the issues and take necessary corrective actions. If necessary, the team will also document the error(s) by creating engineering change requests (ECRs) to ensure all issues are addressed and resolved before certification.
7. After any necessary engineering changes have been made, a new end-to-end test will be performed to ensure that all errors have been resolved and that all operations are successful.
8. Certify the integration by creating a new CryptoHub service for the third-party application that makes deployment as seamless as possible for users.

Overall, following these steps helps ensure that the integration between the third-party application and the CryptoHub is fully tested and validated, and that any errors or issues are resolved before the integration is certified as fully supported.

[3] PREREQUISITES

Supported Hardware:

- CryptoHub, version 7.0.2.1 and above, with the *PKCS11* license enabled

Supported Operating Systems:

- Windows Server 2016 and above

[4] CRYPTOHUB INSTRUCTIONS

This section walks users through the process in CryptoHub to deploy the CyberArk Privileged Access Manager (PAM) service and create a new Endpoint.

[4.1] DEPLOY THE CYBERARK SERVICE

Complete the following steps to deploy the CyberArk PAM service in CryptoHub:

1. Log in to the CryptoHub under dual-control using your administrator identities.
2. Select the **CyberArk Privileged Access Manager (PAM)** service.
3. Select [**Deploy**].
4. Service Setup
 - Service Name: **CyberArk Privileged Access Manager (PAM)**
 - Service Category: **Privileged Access Management**
 - Select [**Next**]
5. Access Control
 - Authorized Resources: **Administrator**
 - Add Additional Resources: *Optional*
 - Select [**Next**]
6. Service Info
 - Authentication Mechanisms: **UserPass - Default**
 - Select [**Deploy**]

[4.2] CREATE A NEW ENDPOINT

1. Navigate to the **Service Management** page for the newly-deployed CyberArk PAM service.
2. Select [**Endpoints**].
3. Select [**Add new**].
4. In the **Add Endpoint** dialog:
 - Name: *Optional*
 - CryptoHub Hostname: **Leave set the auto-populated hostname**
 - Platform: **Windows**
 - Select [**Add Endpoint**]
5. Save the Endpoint zip file your browser prompts you to download.

[5] INSTALL FUTUREX PKCS #11 ON THE CYBERARK SERVER

The Futurex PKCS #11 (FXPKCS11) module is contained inside the Endpoint zip file downloaded in the last section and is preconfigured to connect and authenticate to the CryptoHub. This section explains how to install FXPKCS11 on the CyberArk server.

1. Extract the Endpoint zip. You will see the following files:
 - **PKCS11Manager.exe** -> Program to test the connection to the CryptoHub and perform basic functions through the FXPKCS11 module such as logging in and generating random data.
 - **ca-chain.pem** -> CA certificate bundle
 - **client-cert.pem** -> Client TLS certificate
 - **client.p12** -> Full Client PKI in encrypted PKCS #12 format (contains the CA chain, client certificate, and client private key)
 - **configTest.exe** -> Program to test configuration and connection to the CryptoHub
 - **fxpkcs11.cfg** -> Configuration file for the FXPKCS11 module that is preconfigured to connect and authenticate to the CryptoHub.
 - **fxpkcs11.dll** -> FXPKCS11 module
2. Move all of the above files to **C:\Program Files\Futurex\fxpkcs11**. This requires you to create the **Futurex\fxpkcs11** directories as an administrator user.
3. The Futurex PKCS #11 module expects to find the FXPKCS11 configuration file (**fxpkcs11.cfg**) in the **C:\Program Files\Futurex\fxpkcs11** directory by default. Alternatively, you can set the **FXPKCS11_CFG** environment variable to point to the location of the FXPKCS11 configuration file if you wish to store it in a different location.

Note: The default location for the FXPKCS11 logs is in the **C:\Program Files\Futurex\fxpkcs11** directory. This location can be customized by modifying the **<LOG-FILE>** definition in the FXPKCS11 configuration file (**fxpkcs11.cfg**).

[6] CONFIGURE CYBERARK VAULT TO INTEGRATE WITH CRYPTOHUB

NOTE: Before proceeding with the steps that follow, the CyberArk PAS solution needs to be installed. For instructions on how to install the CyberArk PAS solution, please refer to CyberArk's online documentation at the following url: <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/InstallationOverview.htm>

After the CyberArk Vault has been installed and has started successfully, you can generate a new Server key on the CryptoHub.

The Server Key is the key used to “open” the Vault, much like the key of a physical Vault. The key is required to start the Vault, after which the Server key can be removed until the Server is restarted. When the Vault is stopped, the information stored in the Vault is completely inaccessible without that key.

[6.1] INITIAL VAULT CONFIGURATIONS

1. To use an CryptoHub that is attached to the network, configure the Firewall in order to allow communication to the CryptoHub device. In *DBParm.ini*, configure the `AllowNonStandardFWAddresses` parameter to open the Firewall and allow access to the HSM device, as shown in the following example:

```
AllowNonStandardFWAddresses=[HSM-IP],Yes,1024:inbound/tcp,1024:outbound/tcp
```

NOTE: If utilizing a cloud CryptoHub that is accessible through the internet (rather than a physical CryptoHub connected to the local network), `AllowNonStandardFWAddresses` should **not** be defined in the *DBParm.ini* file.

2. Configure the PKCS#11 provider DLL and specify it in the `PKCS11ProviderPath` parameter in *DBParm.ini*, as shown in the following example:

```
PKCS11ProviderPath=<path to PKCS#11 provider dll>
```

3. Save *DBParm.ini* and close it.

4. Define the PIN/passphrase to be used by the Vault when accessing an CryptoHub device: From a command line, run the following command, specifying your own PIN/passcode that will be used to access the Server key. The PIN/passcode cannot begin with `"/`:

NOTE: The `"hsmpincode"` is the password of the Identity created on the CryptoHub in step 7.6.

```
CAVaultManager SecureSecretFiles /SecretType HSM /Secret <hsmpincode>
```

Open *DBParm.ini* and make sure that the `HSMPinCode` parameter was added with the encrypted value of the PIN/passcode.

5. Restart the PrivateArk Server to apply the new firewall rules.

6. Shutdown the PrivateArk Server.

[6.2] LOAD THE SERVER KEY INTO THE CRYPTOHUB

The following process installs and stores the Server key on the CryptoHub. Once this process is complete, the Server key is stored as non-exportable key on the CryptoHub and will be used by the Vault.

Generate the server key in the CryptoHub

1. Make sure that the Vault Server is not running.
2. Run the **CAVaultManager** command to generate the server key on the CryptoHub:

```
CAVaultManager.exe GenerateKeyOnHSM /ServerKey
```

The above command will generate a new key for the Vault server and store it in the CryptoHub device and will return the key generation keyword. For example: HSM#5

Each time a key generation is created, the keyword allocated is one number higher than the current server key generation specified in DBParm.ini. In order to create additional key generations successfully, users have to manually delete the first generation of the server key; otherwise, an error will be returned. If the ServerKey parameter in the CAVaultManager command specifies a path instead of an HSM keyword, the first key generation will be created, i.e., HSM#1.

3. Re-encrypt the Vault data and metadata with the newly generated keys on the CryptoHub.
 - Run the ChangeServerKeys command to change the encryption keys that will be used for the Vault server.

```
ChangeServerKeys PathToKeys PathToEmergencyFile HSMKeyword
```

For example, the following command will re-encrypt the Vault data and metadata with the encryption keys in 'K:\PrivateArk\Keys', and the 'HSM#1' key will be used as the server key.

```
ChangeServerKeys K:\PrivateArk\Keys K:\PrivateArk\Keys\VaultEmergency.pass HSM#1
```

4. Open DBParm.ini and in the ServerKey parameter specify the value of the key generation version that was generated and specified in the output of the CAVaultManager command above, as shown in the following example.

```
ServerKey=HSM#1
```

5. Start the Vault server and make sure you can log onto the Vault.

APPENDIX A: XCEPTIONAL SUPPORT



In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com



ENGINEERING CAMPUS

864 Old Boerne Road
Bulverde, Texas, USA 78163
Phone: +1 830-980-9782
+1 830-438-8782
E-mail: info@futurex.com

EXCEPTIONAL SUPPORT

24x7x365
Toll-Free: 1-800-251-5112
E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com