



Unbound Key Control

Integration Guide

Version 2.0.1907

July 2019

Table of Contents

1. CyberArk Enterprise Password Vault	ii
--	-----------

1. CyberArk Enterprise Password Vault

UKC can be used to provide enhanced key protection to the CyberArk Enterprise Password Vault.

More information about the Password Vault can be found [here](#).

Use the following steps to prepare UKC for integration with the CyberArk vault:

1. Install the UKC cluster including an Auxiliary server.
2. Create a partition for the CyberArk vault server.
3. Change the user's password.

Note

A blank password is not allowed by CyberArk.

4. Install and configure the UKC client (Windows server).

For more information on UKC, see the [UKC Users Guide](#).

The following configuration is needed on the CyberArk server:

Note

You must update the *hosts* file so that the Unbound Entry Point server name can be used instead of the IP address.

1. Add these lines to the *dbparam.ini* file:

```
AllowNonStandardFWAddresses=[{HSM IP Address}],Yes,{port}:inbound/tcp,
{port}:outbound/tcp
```

```
PKCS11ProviderPath={Path to ekmpkcs11.dll}
```

2. Stop the vault that is using the PrivateArk server.
3. Run the following command line:

```
CAVaultManager SecureSecretFiles /SecretType HSM /Secret {the password of the
user's partition}
```

4. Reopen the *dbparam.ini* file and verify that a new parameter was added called *HSMPinCode*.
5. To generate a new key for the server, stop the CyberArk service and run the following command. It creates a new AES key on the assigned partition and returns the key generation keyword, such as *HSM#1*.

```
CAVaultManger GenerateKeyOnHSM /ServerKey
```

6. A new AES key should be created with the following description "Cyber-Ark Server Key". Check that it exists by running the following command:

```
ucl list
```

7. Run the following command, replacing `<HSMkeyword>` with the keyword generated in step 5.

```
ChangeServerKeys PathToKeys PathToEmergencyFile <HSMkeyword>
```

8. Open the `dbparam.ini` file and change the `ServerKey` entry. Use the keyword from the previous step.

```
ServerKey=<HSMkeyword>
```

9. Start the vault using the PrivateArk server to verify that the server is using the new keys.