MICROSOFT AD CS

Integration Guide

Applicable Devices:
Vectera Plus

TABLE OF CONTENTS

[1] DOCUMENT INFORMATION

[1.1] DOCUMENT OVERVIEW

The purpose of this document is to provide information regarding the configuration of Futurex HSMs with Microsoft Active Directory Certificate Services' certificate authorities. These directions apply to Windows Server 2012 and above. For additional questions related to your HSM, see the relevant user guide.

[1.2] ABOUT MICROSOFT AD CS

Microsoft Active Directory Certificate Services (AD CS) provide management of certificates through a server that acts as a certificate authority (CA). With Futurex's support of an AD CS, a network-connected Vectera Plus, Excrypt SSP Enterprise v.2 or Excrypt Plus can manage certificate authorities in a scalable manner and allow for secure storage, encryption, and signing via the Futurex CNG library.

[1.3] COPYRIGHT AND TRADEMARK NOTICES

[1.4] TERMS OF USE

[1.5] GUARDIAN INTEGRATION

The Guardian Series 3 introduces mission-critical viability to core cryptographic infrastructure, including:

- Centralize device management
- Eliminates points of failure
- Distribute transaction loads

- Group-specific function blocking
- User-defined grouping systems

Please see applicable guide for configuring HSMs with the Guardian Series 3.

[2] PREREQUISITES

Supported Hardware:

- Vectera Plus, 6.7.x.x and above

Supported Operating Systems:

- Windows 2012 R2 (6.3.9600) and above

Other:

- OpenSSL

[3] INSTALL FUTUREX CNG AND FXCLI USING FXTOOLS

In a Windows environment, the easiest way to install the Futurex CNG module and Futurex Command Line Interface (FXCLI) is through installing **FXTools**. FXTools can be downloaded from the Futurex Portal. Step by step installation instructions are provided below:

NOTE: The Futurex CNG module needs to be installed on the server that will be using the HSM. FXCLI needs to be installed on the workstation that will be used to configure the HSM. Therefore, FXTools needs to be installed on *both* the server that will be using the HSM and the workstation that will be used to configure the HSM.

- Run the FXTools installer as an administrator

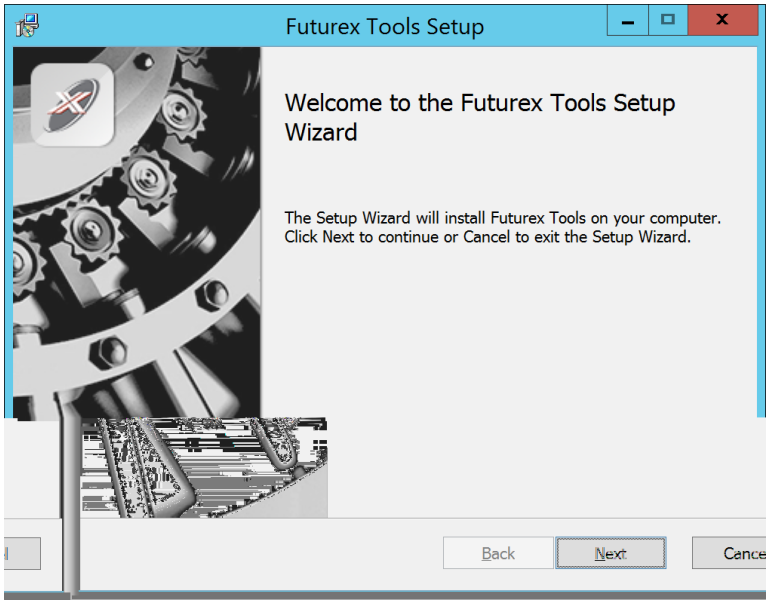


FIGURE: FUTUREX TOOLS SETUP WIZARD

By default, all tools are installed on the system. A user can overwrite and choose not to install certain modules.

- **Futurex Client Tools –** Command Line Interface (CLI) and associated SDK for both Java and C.
- **Futurex CNG Module –** The Microsoft Next Generation Cryptographic Library.
- **Futurex Cryptographic Service Provider (CSP) –** The legacy Microsoft cryptographic library.
- **Futurex EKM Module –** The Microsoft Enterprise Key Management library.
- **Futurex PKCS #11 Module –** The Futurex PKCS #11 library and associated tools.
- **Futurex Secure Access Client –** The client used to connect a Futurex Excrypt Touch to a local laptop, via USB, and a remote Futurex device.

After starting the installation, all noted services are installed. If the Futurex Secure Access Client was selected, the Futurex Excrypt Touch driver will also be installed (Note this sometimes will start minimized or in the background).

After installation is complete, all services are installed in the "*C:\Program Files\Futurex*" directory. The CNG Module, CSP Module, EKM Module, and PKCS #11 Module all require configuration files, located in their

corresponding directory with a *.cfg* extension. In addition, the CNG and CSP Modules are registered in the Windows Registry (*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider*) and are installed in the "*C:\Windows\System32*" directory.

[4] INSTALL EXCRYPT MANAGER

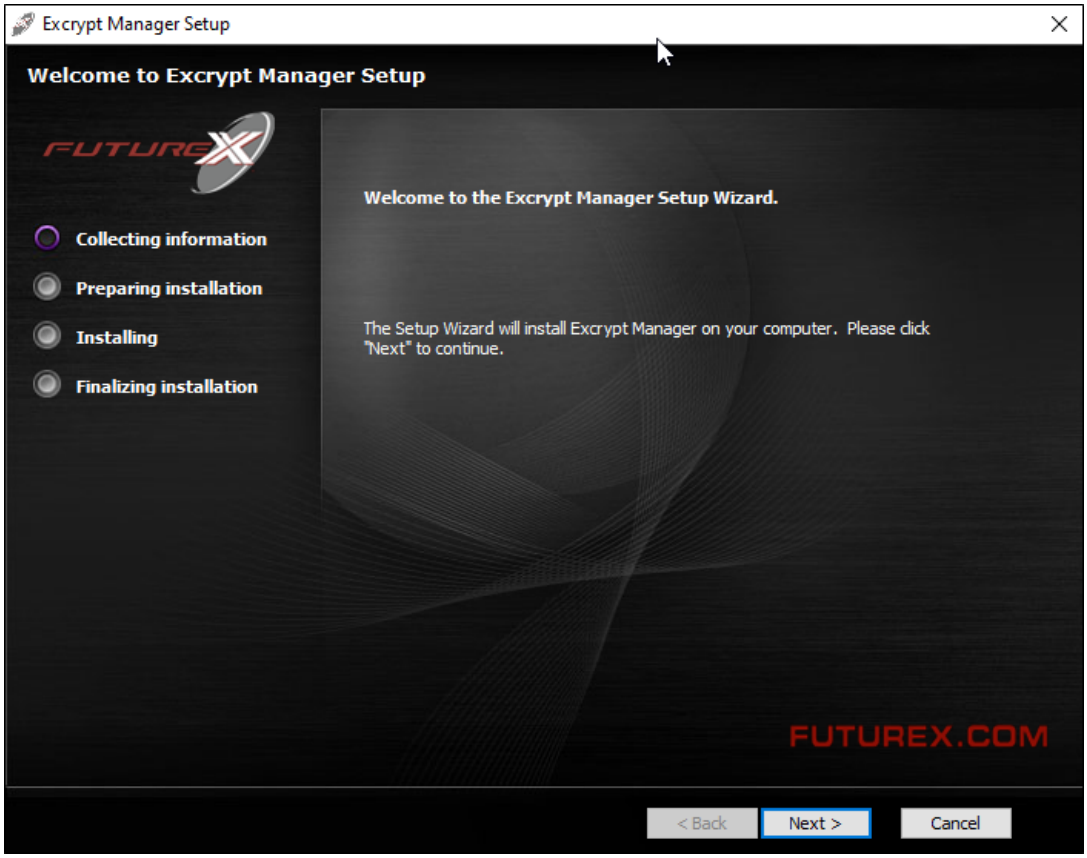
Excrypt Manager is a Windows application that can be used to configure the HSM in subsequent sections. Installing Excrypt Manager is optional because FXCLI, which was installed in the previous section, can be used to perform all of the necessary HSM configurations.

NOTE: Excrypt Manager needs to be installed on the workstation that is being used to configure the HSM.

NOTE: If you plan to use a Virtual HSM for the integration, all configurations will need to be performed using either FXCLI, the Excrypt Touch, or the Guardian Series 3.

NOTE: The Excrypt Manager version must be from the 4.4.x branch or later to be compatible with the HSM firmware, which must be 6.7.x.x or later.

- Run the Excrypt Manager installer as an administrator.



The installation wizard will ask you to specify where you want Excrypt Manager to be installed. The default location is "*C:\Program Files\Futurex\Excrypt Manager*". Once that is done click "Install".

[5] CONFIGURE THE FUTUREX HSM

In order to establish a connection between the CNG library and the Futurex HSM, a few configuration items need to first be performed, which are the following:

NOTE: All of the steps in this section can be completed through either Excrypt Manager or FXCLI (if using a physical HSM rather than a virtual HSM). Optionally, steps 4 through 6 can be completed through the Guardian Series 3, which will be covered in Appendix A.

1. Connect to the HSM via the front USB port (NOTE: If you are using a virtual HSM for the integration you will have to connect to it over the network either via FXCLI, the Excrypt Touch, or the Guardian Series 3)
    a. Connecting via Excrypt Manager
    b. Connecting via FXCLI
2. Validate the correct features are enabled on the HSM
3. Setup the network configuration
4. Load the Futurex FTK
5. Configure a Transaction Processing connection and create a new Application Partition
6. Create a new Identity that has access to the Application Partition created in the previous step
7. Configure TLS Authentication. There are two options for this:
    a. Enabling server-side authentication
    b. Creating client certificates for mutual authentication

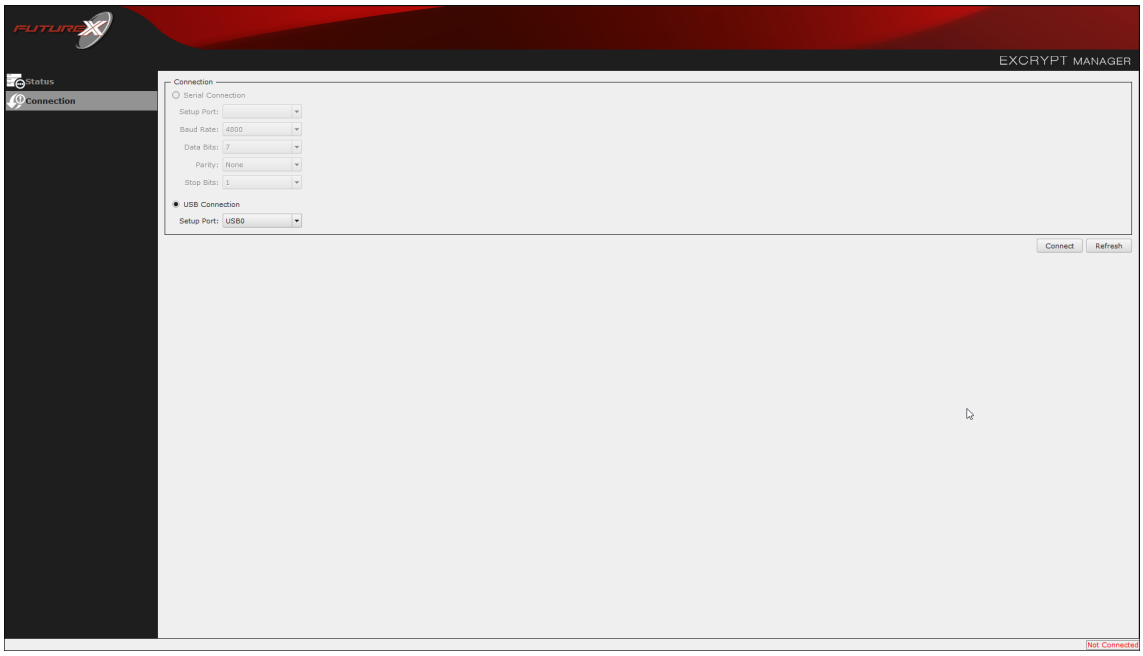
Each of these action items is detailed in the following subsections.

[5.1] CONNECT TO THE HSM VIA THE FRONT USB PORT

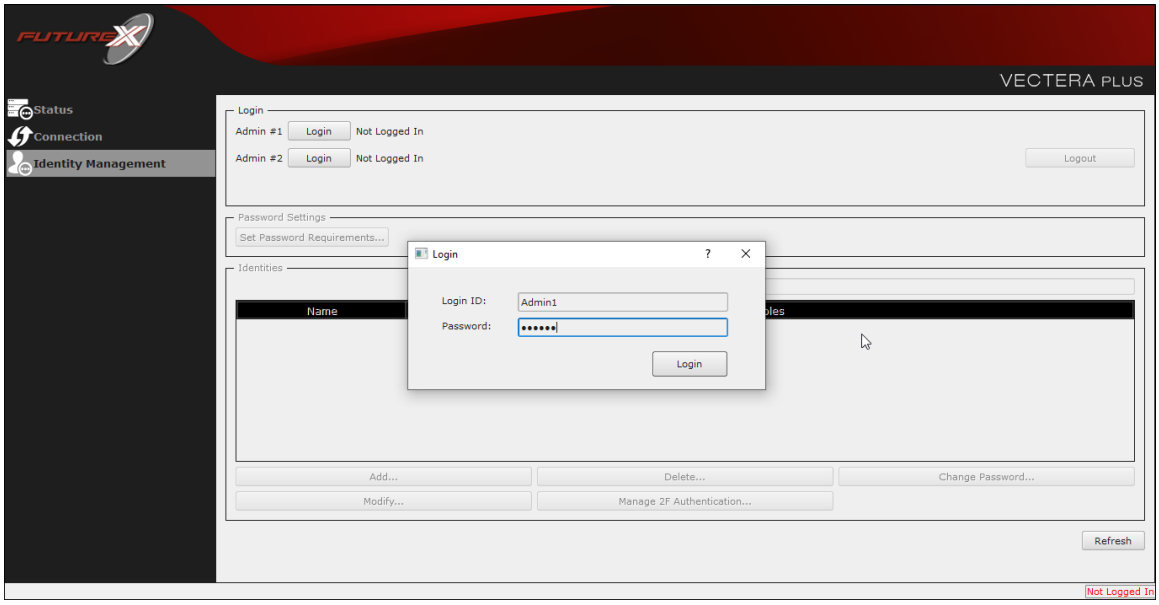
For both Excrypt Manager and FXCLI you need to connect your laptop to the front USB port on the HSM.

Connecting via Excrypt Manager

Open Excrypt Manager, click “Refresh” in the lower right-hand side of the Connection menu. Then select “USB Connection” and click “Connect”.

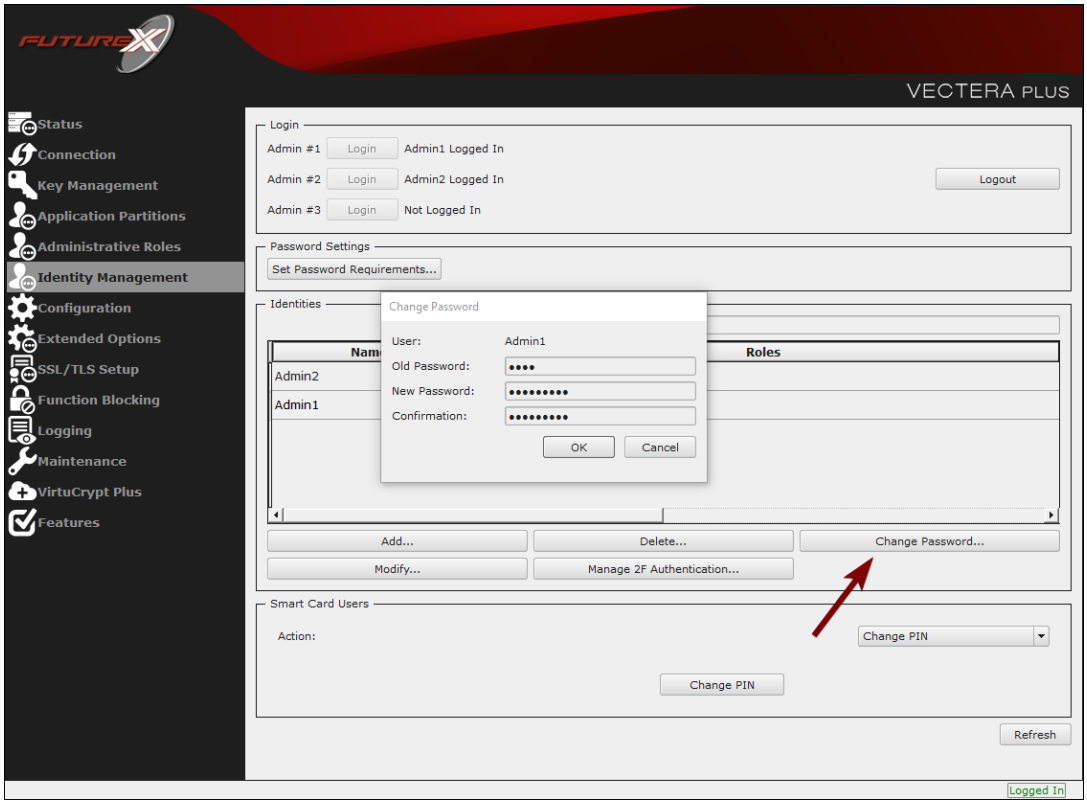


Login with both default Admin identities.



The default Admin passwords (i.e. “safe”) must be changed for both of your default Admin Identities (e.g. “Admin1” and “Admin2”) in order to load the major keys onto the HSM.

To do so via Excrypt Manager navigate to the Identity Management menu, select the first default Admin identity (e.g. “Admin1”), then click the “Change Password…” button. Enter the old password, then enter the new password twice, and click “OK”. Perform the same steps as above for the second default Admin identity (e.g. “Admin2”).



Connecting via FXCLI

Open the FXCLI application and run the following commands:

```
$ connect usb
$ login user
```

NOTE: The "login" command will prompt for the username and password. You will need to run it twice because you must login with both default Admin identities.

The default Admin passwords (i.e. “safe”) must be changed for both of your default Admin Identities (e.g. “Admin1” and “Admin2”) in order to load the major keys onto the HSM.

The following FXCLI commands can be used to change the passwords for each default Admin Identity.

```
$ user change-password -u Admin1
$ user change-password -u Admin2
```

NOTE: The user change-password commands above will prompt you to enter the old and new passwords. It is necessary to run the command twice (as shown above) because the default password must be changed for both default Admin identities.

[5.2] FEATURES REQUIRED IN HSM

In order to establish a connection between the CNG Library and the Futurex HSM, the HSM must be configured with the following features:

- **PKCS #11** -> Enabled
- **Command Primary Mode** -> General Purpose (GP)

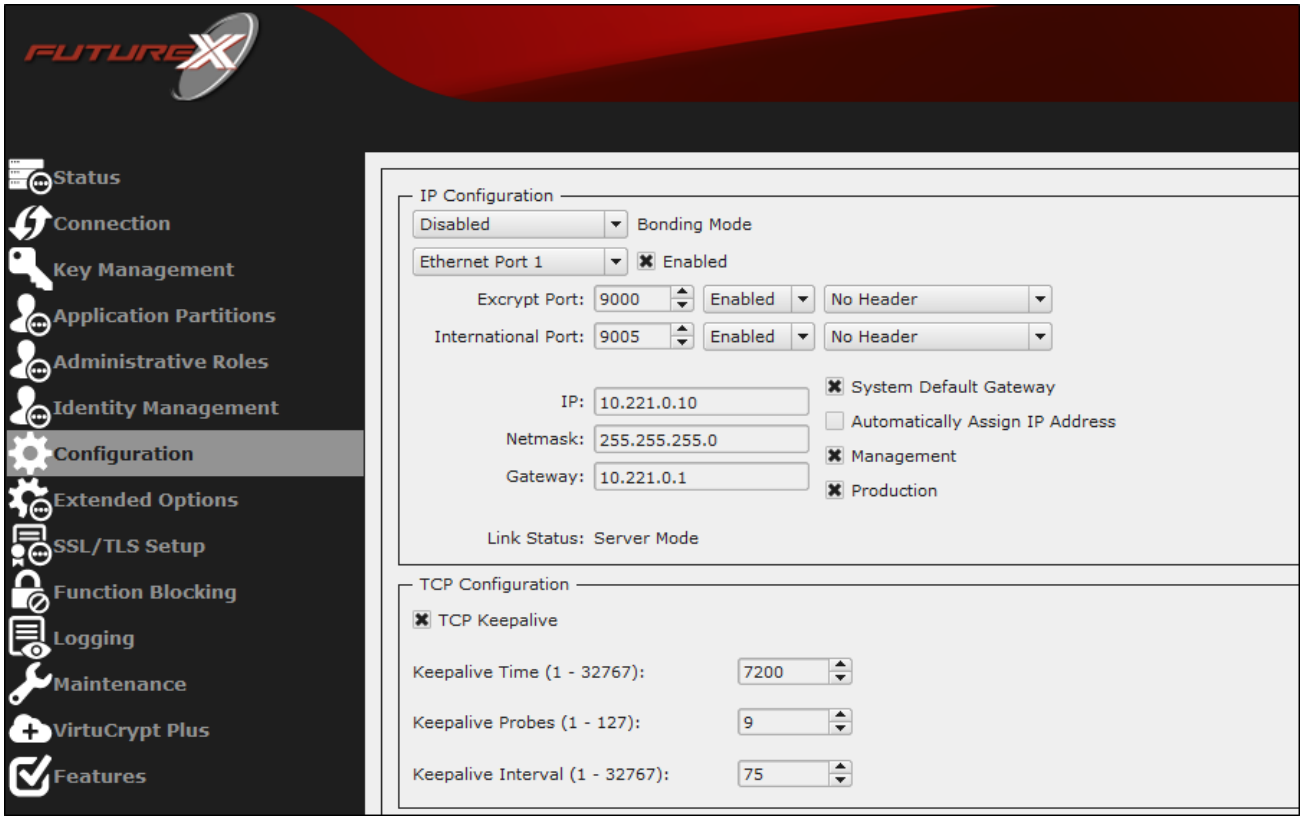
NOTE: For additional information about how to update features on your HSM, please refer to your HSM Administrator's Guide, section **"Download Feature Request File"**.

NOTE: Command Primary Mode = General Purpose, will enable the option to create the FTK major key in the HSM. This key will be required to be able to use the CNG library to communicate with the HSM. For detailed information about how to load major keys in HSMs please refer to your HSM Administrator's Guide.

[5.3] NETWORK CONFIGURATION (HOW TO SET THE IP OF THE HSM)

For this step you will need to be logged in with an identity that has a role with permissions ***Communication:Network Settings****. The default Administrator role and Admin identities can be used.*

Navigate to the *Configuration* page. There you will see the option to modify the IP configuration, as shown below:



Alternatively, the following **FXCLI** command can be used to set the IP for the HSM:

```
$ network interface modify --interface Ethernet1 --ip 10.221.0.10 --netmask 255.255.255.0 --gateway
10.221.0.1
```

NOTE: The following should be considered at this point:

- All of the remaining HSM configurations in this section can be completed using the Guardian Series 3 (please refer to Appendix A for instructions on how to do so), with the exception of the final subsection that covers how to create connection certificates for mutual authentication.
- If you are performing the configuration on the HSM directly now, but plan to add the HSM to a Guardian later, it may be necessary to synchronize the HSM after it is added to a Device Group on the Guardian.
- If configuration through a CLI is required for your use-case, then you should manage the HSMs directly.

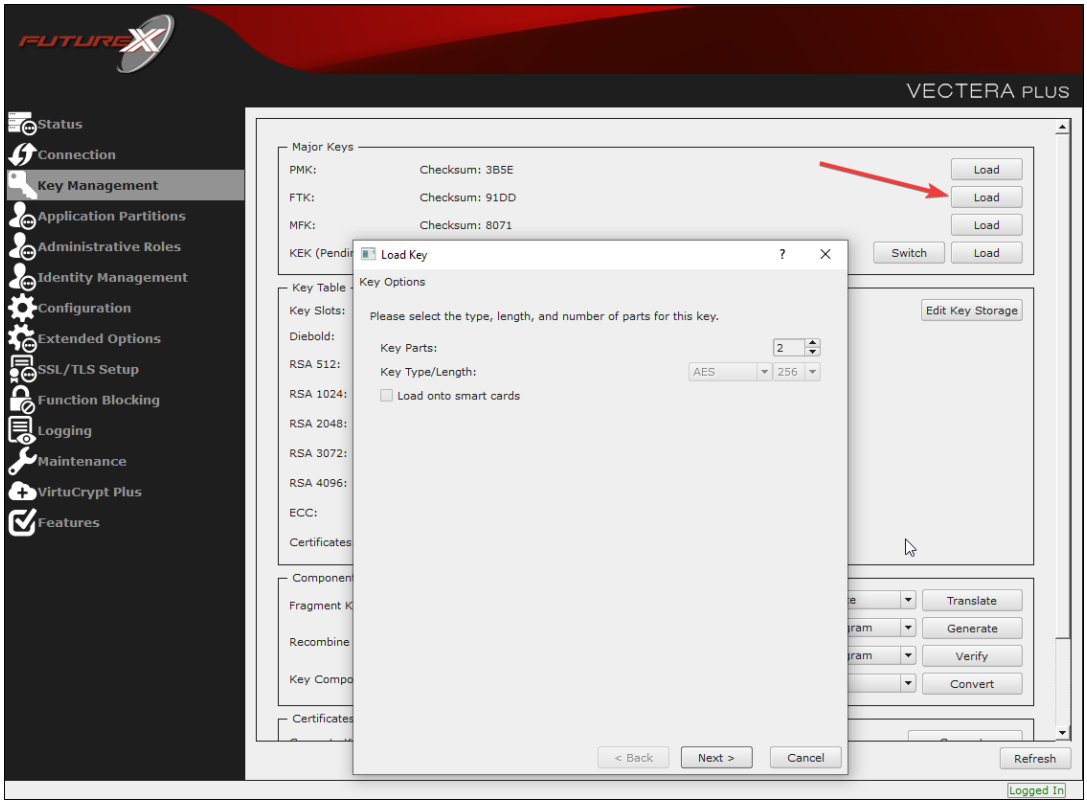
[5.4] LOAD FUTUREX KEY (FTK)

For this step you will need to be logged in with an identity that has a role with permissions ***Major Keys:Load****. The default Administrator role and Admin identities can be used.*

The FTK is used to wrap all keys stored on the HSM used with CNG. If using multiple HSMs in a cluster, the same FTK can be used for syncing HSMs. Before an HSM can be used with CNG, it must have an FTK.

NOTE: This process can also be completed using FXCLI, the Excrypt Touch, or the Guardian Series 3. For more information about how to load the FTK into an HSM using these tools/devices, please see the relevant Administrative Guide.

After logging in, select *Key Management*, then "Load" under FTK. Keys can be loaded as components that are XOR'd together, M-of-N fragments, or generated. If this is the first HSM in a cluster, it is recommended to generate the key and save to smart cards as M-of-N fragments.



Alternatively, the following **FXCLI** commands can be used to load an FTK onto an HSM.

If this is the first HSM you are setting up you will need to generate a random FTK. Optionally, you can also load it onto smart cards simultaneously with the -m and -n flags.

```
$ majorkey random --ftk -m [number_from_2_to_9] -n [number_from_2_to_9]
```

If it's a second HSM that you're setting up in a cluster then you will load the FTK from smart cards with the following command:

```
$ majorkey recombine --key ftk
```

[5.5] CONFIGURE A TRANSACTION PROCESSING CONNECTION AND CREATE AN APPLICATION PARTITION

For this step you will need to be logged in with an identity that has a role with permissions ***Role:Add, Role:Assign All Permissions, Role:Modify, Keys:All Slots****, and* ***Command Settings:Excrypt****. The default Administrator role and Admin identities can be used.*

NOTE: For the purposes of this integration guide you can consider the terms "Application Partition" and "Role" to be synonymous. For more information regarding Application Partitions, Roles, and Identities, please refer to the relevant Administrator's guide.

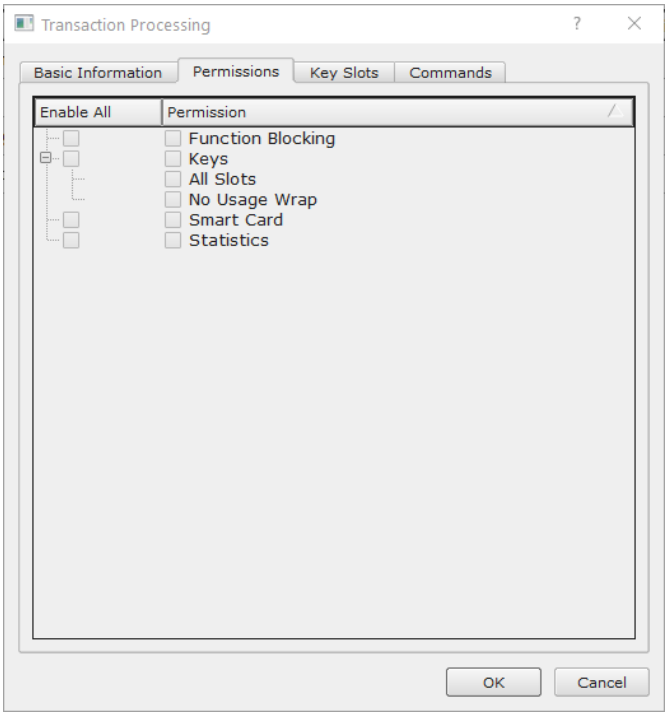
Configure a Transaction Processing Connection

Before an application logs in to the HSM with an authenticated user, it first connects via a “Transaction Processing” connection to the **Transaction Processing** Application Partition. For this reason, it is necessary to take steps to harden this Application Partition. The following three things need to be configured for the Transaction Processing partition:

1. It should not have access to the “All Slots” permissions
2. It should not have access to any key slots
3. Only the CNG communication commands should be enabled

Go to *Application Partitions*, select the Transaction Processing Application Partition, and click Modify.

Navigate to the "Permissions" tab and ensure that the “All Slots” key permission is unchecked. None of the other key permissions should be enabled either.



Under the "Key Slots" tab you need to ensure that there are no key ranges specified. By default, the Transaction Processing Application Partition has access to the entire range of key slots on the HSM.

Lastly, under the “Commands” tab make sure that only the following **CNG Communication commands** are enabled:

- **ECHO**: Communication Test/Retrieve Version
- **PRMD**: Retrieve HSM restrictions
- **RAND**: Generate random data
- **HASH**: Retrieve device serial
- **GPKM**: Retrieve key table information
- **GPKS**: General purpose key settings get/change
- **GPKR**: General purpose key settings get (read-only)

Alternatively, the following **FXCLI** commands can be used to remove all permissions and key ranges that are currently assigned to the **Transaction Processing** role and enable only the CNG Communication commands:

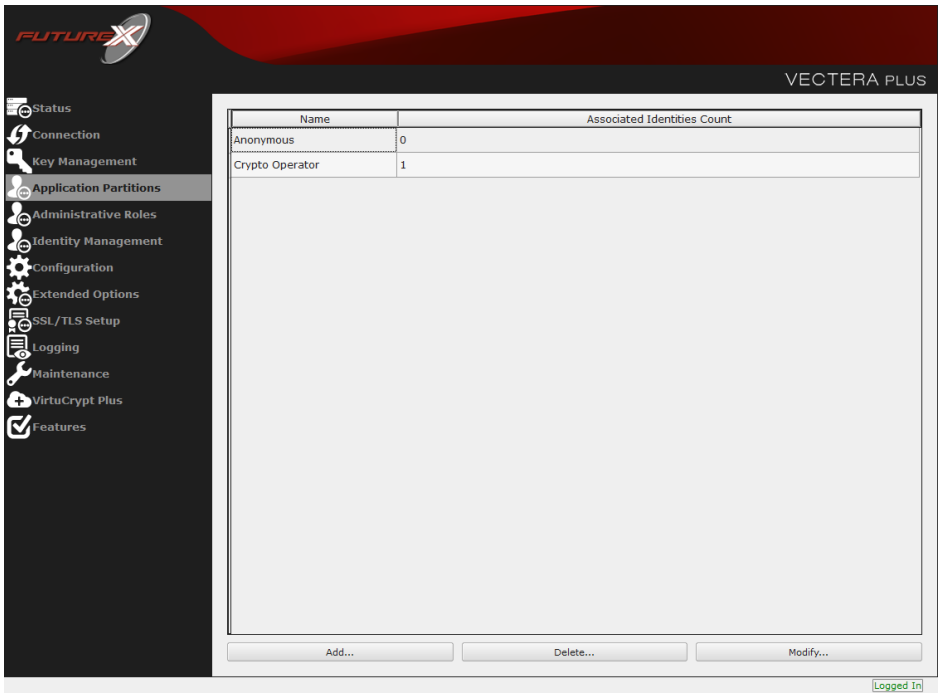
```
$ role modify --name Anonymous --clear-perms --clear-key-ranges
```

```
$ role modify --name Anonymous --add-perm Excrypt:ECHO --add-perm Excrypt:PRMD --add-perm Excrypt:RAND
--add-perm Excrypt:HASH --add-perm Excrypt:GPKM --add-perm Excrypt:GPKS --add-perm Excrypt:GPKR
```

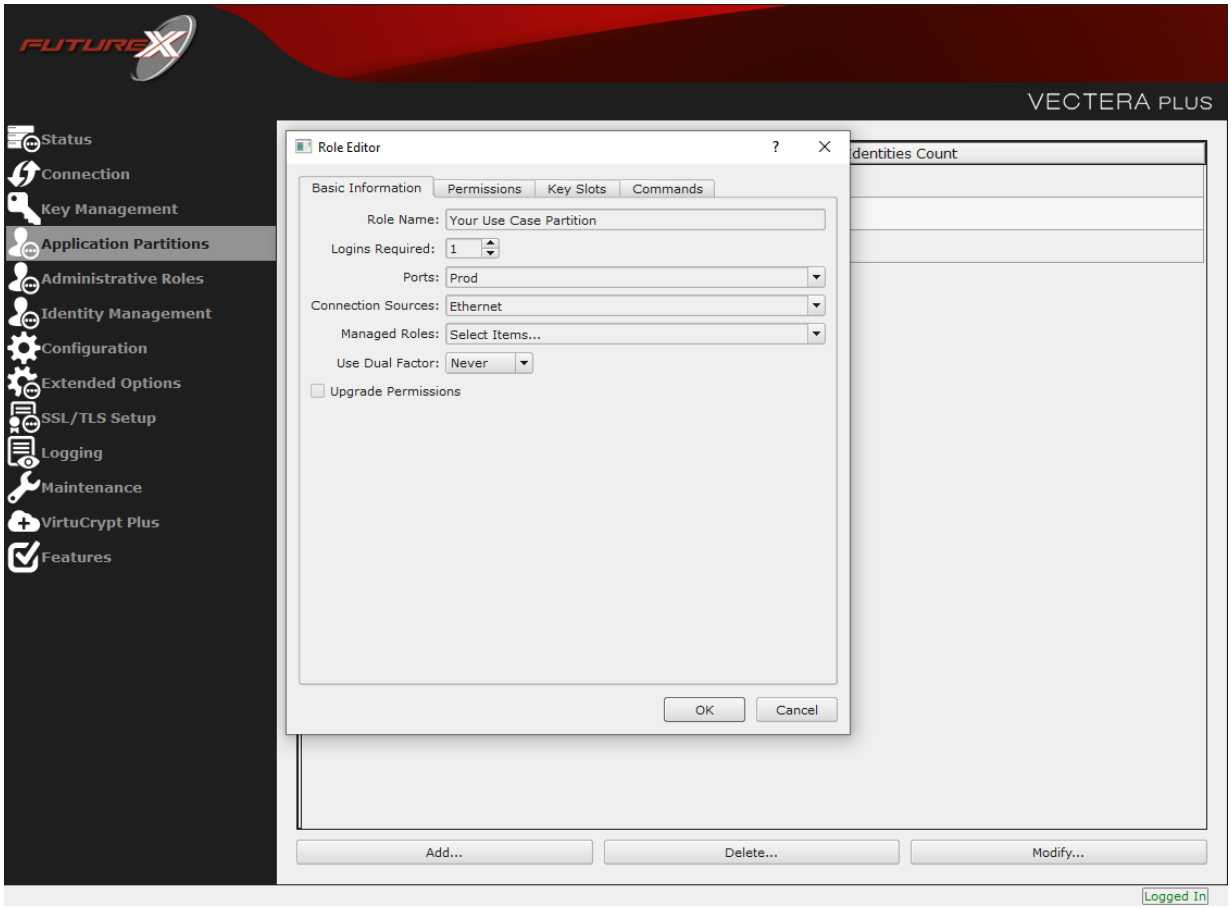
Create an Application Partition

In order for application segregation to occur on the HSM, an Application Partition must be created specifically for your use case. Application partitions are used to segment the permissions and keys on an HSM between applications. The process for configuring a new application partition is outlined in the following steps:

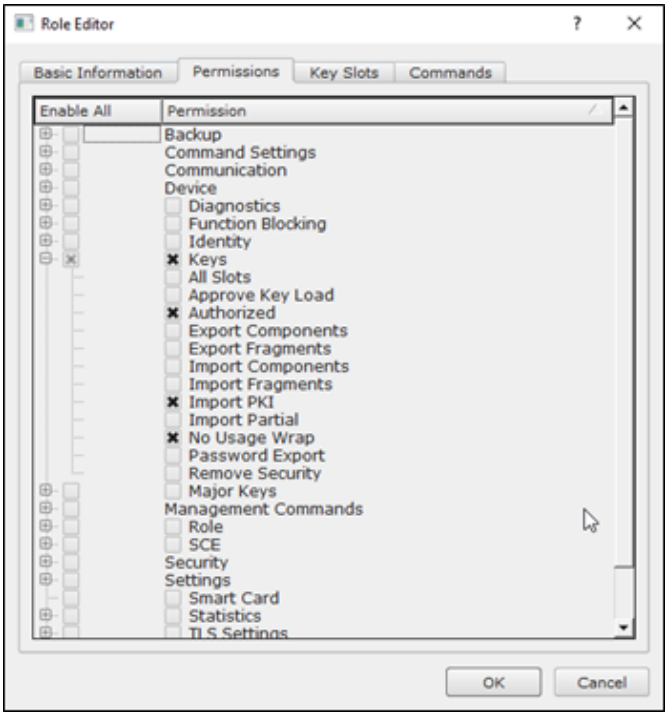
Navigate to the *Application Partitions* page and click the "Add" button at the bottom.



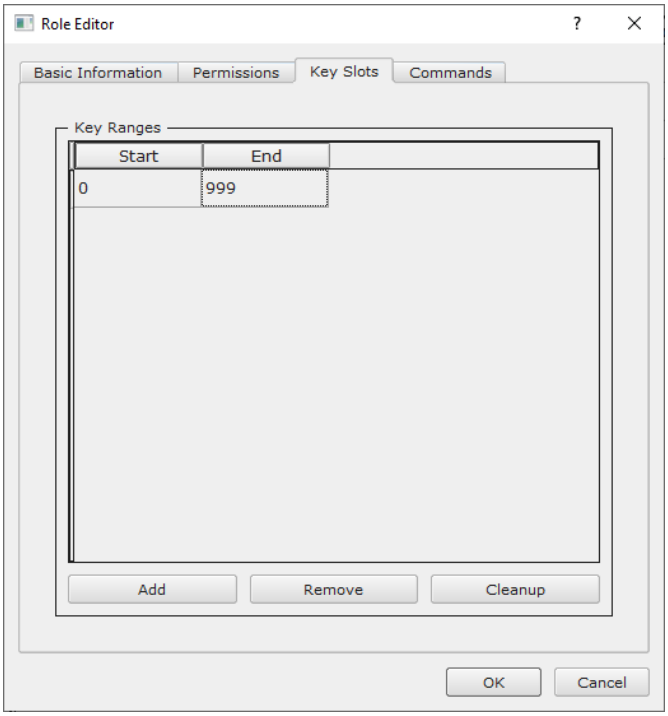
Fill in all of the fields in the *Basic Information* tab exactly how you see below (except for the *Role Name* field). In the *Role Name* field, specify any name that you would like for this new Application Partition. *Logins Required* should be set to "1". *Ports* should be set to "Prod". *Connection Sources* should be configured to "Ethernet". The *Managed Roles* field should be left blank because we'll be specifying the exact Permissions, Key Slots, and Commands that we want this Application Partition/Role to have access to. Lastly, the *Use Dual Factor* field should be set to "Never".



Under the "Permissions" tab, select the key permissions shown in the screenshot below. The **Authorized** permission allows for keys that require login. The **Import PKI** permission allows trusting an external PKI, which is used by some applications to allow for PKI symmetric key wrapping (It is not recommended to enable unless using this use case). The **No Usage Wrap** permission allows for interoperable key wrapping without defining key usage as part of the wrapped key (This is only recommended if exchanging keys with external entities or using the HSM to wrap externally used keys).



Under key Slots, it is recommended that you create a range of 1000 total keys (here we've specified the key range 0-999), which do not overlap with another Application Partition. Within this range, there must be ranges for both symmetric and asymmetric keys. If more keys are required by the application, configure accordingly.



Based on application requirements there are particular functions that need to be enabled on the Application Partition in order to utilize the HSMs functionality. The most often used commands are included below. These can be enabled under the "Commands" tab.

CNG Communication Commands

- ECHO: Communication Test/Retrieve Version
- PRMD: Retrieve HSM restrictions
- RAND: Generate random data
- HASH: Retrieve device serial
- GPKM: Retrieve key table information
- GPKS: General purpose key settings get/change
- GPKR: General purpose key settings get (read-only)

Key Operations Commands

- APFP: Generate PKI Public Key from Private Key
- ASYL: Load asymmetric key into key table
- GECC: Generate an ECC Key Pair
- GPCA: General purpose add certificate to key table
- GPGS: General purpose generate symmetric key
- GPKA: General purpose key add
- GPKD: General purpose key slot delete/clear
- GRSA: Generate RSA Private and Public Key
- LRSA: Load key into RSA Key Table
- RPFP: Get public components from RSA private key

Interoperable Key Wrapping

- GPKU: General purpose key unwrap (unrestricted)
- GPUK: General purpose key unwrap (preserves key usage)
- GPKW: General purpose key wrap (unrestricted)
- GPWK: General purpose key wrap (preserves key usage)

Data Encryption Commands

- ADPK: PKI Decrypt Trusted Public Key
- GHSH: Generate a Hash (Message Digest)
  *Starting in firmware version 7.x, this function is enabled by default and does not need to be specified.
- GPED: General purpose data encrypt and decrypt
- GPGC: General purpose generate cryptogram from key slot
- GPMC: General purpose MAC (Message Authentication Code)
- GPSR: General purpose RSA encrypt/decrypt or sign/verify with recovery
- HMAC: Generate a hash-based message authentication code
- RDPK: Get Clear Public Key from Cryptogram

Signing Commands

- ASYS: Generate a Signature Using a Private Key
- ASYV: Verify a Signature Using a Public Key
- GPSV: General purpose data sign and verify
- RSAS: Generate a Signature Using a Private Key

Alternatively, the following **FXCLI** commands can be used to create the new Application Partition and enable all of the functions that are needed:

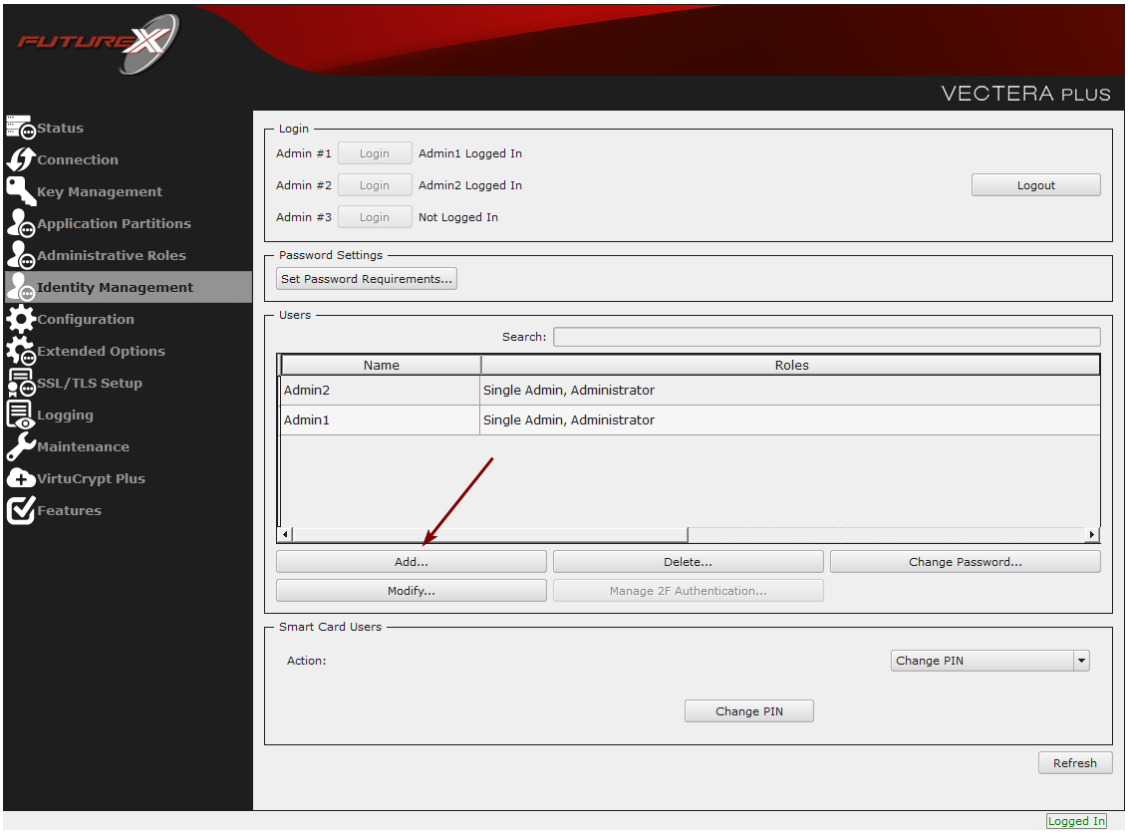
```
$ role add --name Role_Name --application --key-range (0,999) --perm "Keys:Authorized" --perm "Key-
s:Import PKI" --perm "Keys:No Usage Wrap"
```

```
$ role modify --name [role_name] --clear-perms --add-perm Excrypt:ECHO --add-perm Excrypt:PRMD --add-
perm Excrypt:RAND --add-perm Excrypt:HASH --add-perm Excrypt:GPKM --add-perm Excrypt:GPKS --add-perm
Excrypt:GPKR --add-perm Excrypt:APFP --add-perm Excrypt:ASYL --add-perm Excrypt:GECC --add-perm
Excrypt:GPCA --add-perm Excrypt:GPGS --add-perm Excrypt:GPKA --add-perm Excrypt:GPKD --add-perm
Excrypt:GRSA --add-perm Excrypt:LRSA --add-perm Excrypt:RPFP --add-perm Excrypt:GPKU --add-perm
Excrypt:GPUK --add-perm Excrypt:GPKW --add-perm Excrypt:GPWK --add-perm Excrypt:ADPK --add-perm
Excrypt:GHSH --add-perm Excrypt:GPED --add-perm Excrypt:GPGC --add-perm Excrypt:GPMC --add-perm
Excrypt:GPSR --add-perm Excrypt:HMAC --add-perm Excrypt:RDPK --add-perm Excrypt:ASYS --add-perm
Excrypt:ASYV --add-perm Excrypt:GPSV --add-perm Excrypt:RSAS
```

[5.6] CREATE NEW IDENTITY AND ASSOCIATE IT WITH THE NEWLY CREATED APPLICATION PARTITION

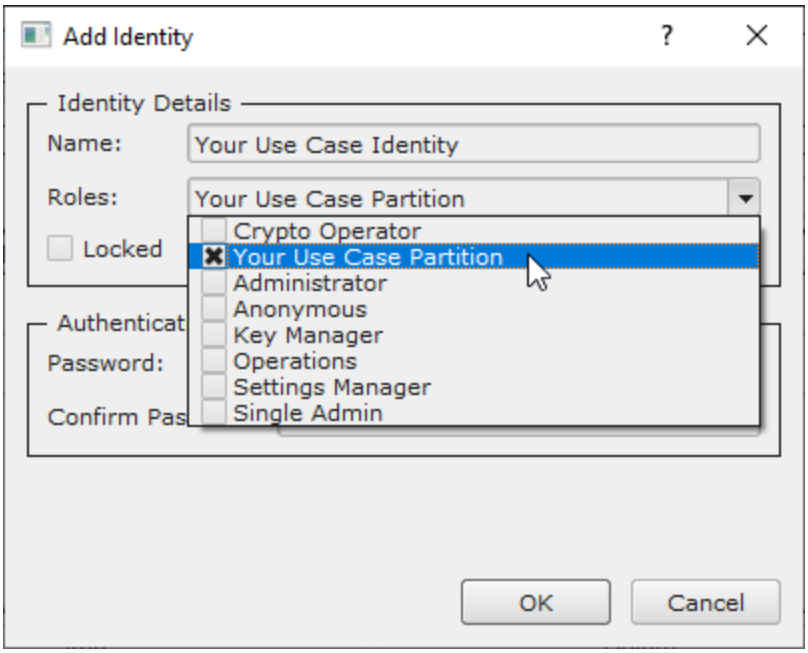
*For this step you will need to be logged in with an identity that has a role with permissions **Identity:Add**. The default Administrator role and Admin identities can be used.*

A new identity must be created, which will need to be associated with the Application Partition created in the previous step. To create this new identity, go to *Identity Management*, and click "Add".



Specify a name for the new identity, and in the Roles dropdown select the name of the Application Partition created in the previous step. This will associate the new Identity with the Application Partition that you

created.



Alternatively, the following **FXCLI** command can be used to create a new Identity and associate it with the role that was created:

```
$ identity add --name Identity_Name --role Role_Name --password [password]
```

This new identity must be set in fxcng.cfg file, in the following section:

```
# Identity that is assigned to the created Application Partition
<CRYPTO-OPR>     [insert name of identity that you created]     </CRYPTO-OPR>

# Password of the Identity above
<CRYPTO-OPR-PASS> [password] </CRYPTO-OPR-PASS>

# Production connection
<PROD-ENABLED>    YES        </PROD-ENABLED>
<PROD-PORT>        9100        </PROD-PORT>
```

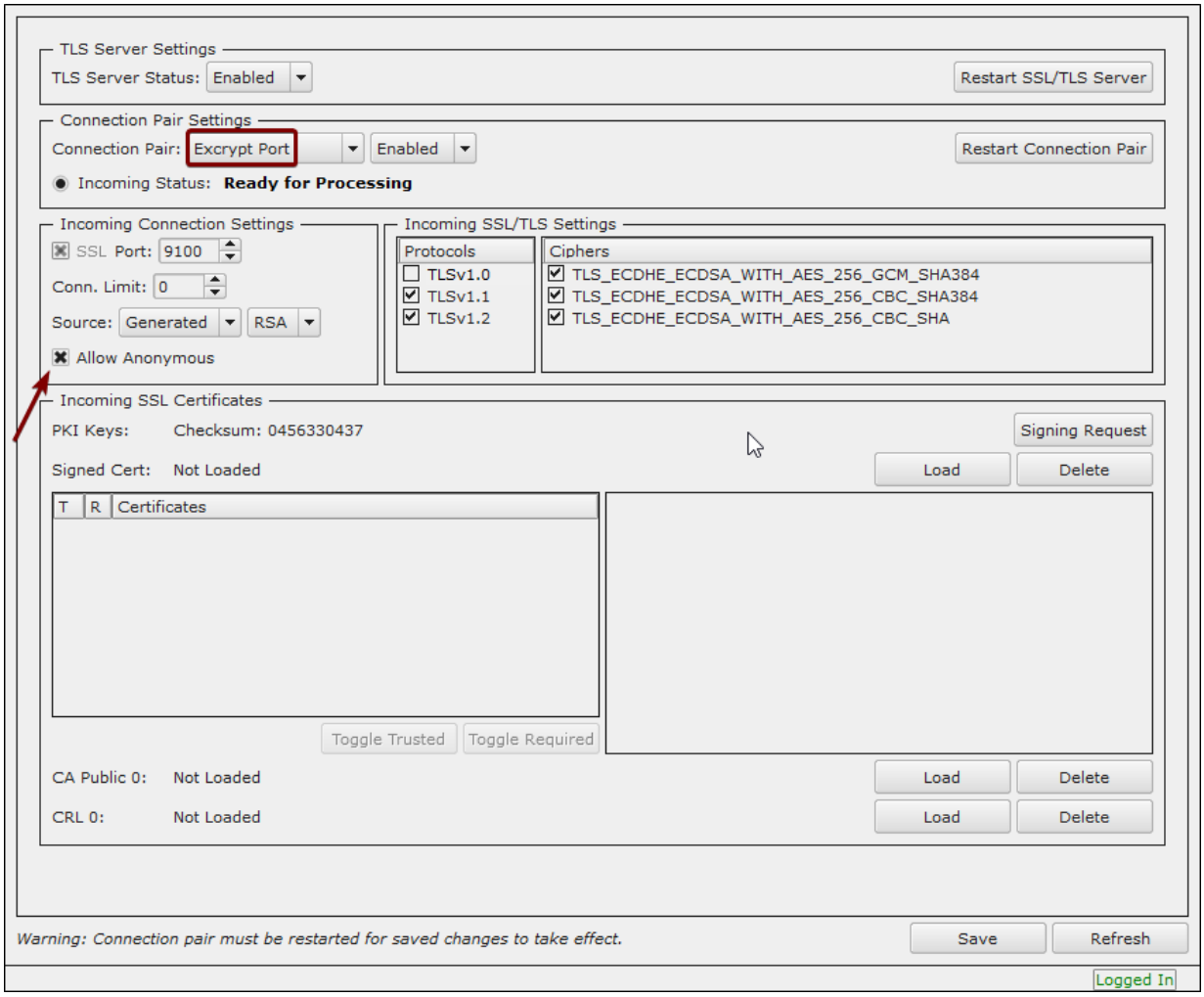
NOTE: Crypto Operator in the fxcng.cfg file must match exactly the name of the identity created in the HSM.

[5.7] CONFIGURE TLS AUTHENTICATION

For this step you will need to be logged in with an identity that has a role with permissions ***Keys:All Slots, Management Commands:Certificates, Management Commands:Keys, Security:TLS Sign****, and* ***TLS Settings:Upload Key****. The default Administrator role and Admin identities can be used.*

Enable Server-Side Authentication (Option 1)

Mutually authenticating to the HSM using client certificates is recommended, but server-side authentication is also supported. To enable server-side authentication go to *SSL/TLS Setup*, then select the Excrypt Port and enable the "Allow Anonymous" setting.



Alternatively, the following **FXCLI** command can be used to enable server-side authentication with the "Allow Anonymous" SSL/TLS setting:

```
$ tls-ports set -p "Excrypt Port" --anon
```

Create Connection Certificates for Mutual Authentication (Option 2)

Mutually authenticating to the HSM using client certificates is recommended, and enforced by default. In the example below, FXCLI is utilized to generate a CA that then signs the HSM server certificate and a client certificate. The client keys and CSR are generated in Windows PowerShell with OpenSSL. For other options for managing certificates required for mutual authentication with the HSM, please review the relevant Administrator's guide.

Find the **FXCLI** program that was installed with FXTools, and run it as an administrator.

Things to note:

- For this example, the computer running FXCLI is connected to the front port of the HSM. Remote management is possible however, using the HSMs Web Portal, or the Excrypt Touch.
- For commands that create an output file, if you do not specify a file path (as is the case here) it will save the file to the directory from which the FXCLI program is executed.
- Using user-generated certificates requires a PMK to be loaded on the HSM.
- If you run **help** by itself it will show a full list of available commands. You can see all of the available options for any given command by running the command name followed by **help**.

```
# Connect your laptop to the HSM via the USB port on the front, then run this command.
$ connect usb
```

```
# Log in with both default Admin identities. This command will prompt for the username and password.
You will need to run this command twice.
$ login user
```

```
# Generate TLS CA and store it in an available key slot on the HSM
$ generate --algo RSA --bits 2048 --usage mak --name TlsCaKeyPair --slot next
```

```
# Create root certificate
$ x509 sign \
    --private-slot TlsCaKeyPair \
    --key-usage DigitalSignature --key-usage KeyCertSign \
    --ca true --pathlen 0 \
    --dn 'O=Futurex\CN=Root' \
    --out TlsCa.pem
```

```
# Generate the server keys for the HSM
$ tls-ports request --pair "Excrypt Port" --file production.csr --pki-algo RSA
```

```
# Sign the server CSR with the newly created TLS CA
$ x509 sign \
    --private-slot TlsCaKeyPair \
    --issuer TlsCa.pem \
    --csr production.csr \
    --eku Server --key-usage DigitalSignature --key-usage KeyAgreement \
    --ca false \
    --dn 'O=Futurex\CN=Production' \
    --out TlsProduction.pem
```

```
# Push the signed server PKI to the production port on the HSM
$ tls-ports set --pair "Excrypt Port" \
    --enable \
    --pki-source Generated \
    --clear-pki \
    --ca TlsCa.pem \
```

```
    --cert TlsProduction.pem \
    --no-anon
```

***NOTE**: The following OpenSSL commands will need to be run from Windows PowerShell, rather than from the FXCLI program.*

```
# Generate the client keys
$ openssl genrsa -out privatekey.pem 2048
```

```
# Generate client CSR
$ openssl req -new -key privatekey.pem -out ClientPki.csr -days 365
```

Using FXCLI, sign the CSR that was just generated using OpenSSL.

```
# Sign the client CSR under the root certificate that was created
$ x509 sign  \
--private-slot TlsCaKeyPair \
 --issuer TlsCa.pem \
 --csr ClientPki.csr \
 --eku Client --key-usage DigitalSignature --key-usage KeyAgreement \
 --dn 'O=Futurex\CN=Client' \
  --out SignedPki.pem
```

Switch back to Windows PowerShell for the remaining commands.

```
## Make PKCS12 file
# Concatenate the signed client cert and private key into one pem file
$ cat SignedPki.pem >> Tree.pem
```

```
$ cat privatekey.pem >> Tree.pem
```

```
# Use OpenSSL to create a PKCS#12 file that can be used to authenticate, as a client, using our CNG
library
$ openssl pkcs12 -export -in Tree.pem -out PKI.p12 -name "ClientPki" -password pass:safest
```

[6] EDIT THE CONFIGURATION FILE

The *fxcng.cfg* file allows the user to set the CNG library to connect to the HSM. To edit, run a text editor as an Administrator and edit the configuration file accordingly. Most notably, the fields shown below must be set (note that the full *fxcng.cfg* file is not included).

NOTE: Our CNG library expects the CNG config file to be in a certain location (*C:\Program Files\Futurex\fxcng\fxcng.cfg*), but that location can be overwritten using an environment variable (FXCNG_CFG).

```
# Connection information
<ADDRESS>             10.0.5.58           </ADDRESS>

# Load balancing
<FX-LOAD-BALANCE>     YES                 </FX-LOAD-BALANCE>

# Log configuration
<LOG-FILE> C:\Program Files\Futurex\fxcng\fxcng.log </LOG-FILE>

# Identity that is assigned to the created Application Partition
<CRYPTO-OPR>          [identity_name]     </CRYPTO-OPR>

# Password of the Identity above
<CRYPTO-OPR-PASS>        [password]         </CRYPTO-OPR-PASS>

# Production connection
<PROD-ENABLED>        YES                 </PROD-ENABLED>
<PROD-PORT>           9100                </PROD-PORT>

# Production SSL information
<PROD-TLS-ANONYMOUS>    NO                </PROD-TLS-ANONYMOUS>
<PROD-TLS-CA>     C:\Program Files\Futurex\fxcng\TlsCa.pem    </PROD-TLS-CA>
<PROD-TLS-CA>     C:\Program Files\Futurex\fxcng\TlsProduction.pem    </PROD-TLS-CA>
<PROD-TLS-KEY>     C:\Program Files\Futurex\fxcng\PKI.p12     </PROD-TLS-KEY>
<PROD-TLS-KEY-PASS>      safest           </PROD-TLS-KEY-PASS>
```

In the **<ADDRESS>** field, the IP of the HSM that the CNG library will connect to is specified.

If a Guardian is being used to manage HSMs in a cluster, the **<FX-LOAD-BALANCE>** field must be defined as "YES". If a Guardian is not being used it should be set to "NO".

In the **<LOG-FILE>** field, set the path to the CNG log file.

In the **<CRYPTO-OPR>** field, the name of identity created in step 6.6 needs to be set.

In the **<CRYPTO-OPR-PASS>** field, the password of the identity specified in the **<CRYPTO-OPR>** field needs to be set to log the application into the HSM automatically. CNG does not support logging in through the API, so having the ability to log in using the FXPKCS11 configuration file allows the application to segment out keys on the HSM by associating the Identity with a specific Application Partition.

The **<PROD-ENABLED>** and **<PROD-PORT>** fields declare that the CNG library will connect to Production port 9100.

The **<PROD-TLS-ANONYMOUS>** field defines whether the CNG library will be authenticating to the server or not.

The **<PROD-TLS-KEY>** field defines the location of the client private key. Supported formats for the TLS private key are PKCS #1 clear private keys, PKCS #8 encrypted private keys, or a PKCS #12 file that contains the client private key and signed client certificate encrypted under the password specified in the **<PROD-TLS-KEY-PASS>** field.

Because a PKCS #12 file is defined in the **<PROD-TLS-KEY>** field in this example, it is not necessary to define the signed client certificate with the **<PROD-TLS-CERT>** tag. It is necessary to define CA cert/s with one or more instances of the **<PROD-TLS-CA>** tag.

For additional details reference the Futurex CNG technical reference found on the Futurex Portal.

Once the *fxcng.cfg* is edited, run the *CNGInstallUtil* file to test the connection against the HSM, and check the *FxCNG-Install-Log.txt* file for errors and information. For more information, see our Administrator's Guide.

[7] VERIFY THAT THE FUTUREX CNG PROVIDER IS INSTALLED

1. In a command prompt, execute:

```
certutil -csptest -csp "Futurex CNG" RSA
```

2. If you see the following text, the module is installed properly:

```
Provider Name: Futurex CNG
      Name:  Provider Module:
      UM(1): fxcng.dll
      0(1): 10001, 1
        0: KEY_STORAGE
...
      Name:  Signature Algorithms:
   RSA
    BCRYPT_ASYMMETRIC_ENCRYPTION_INTERFACE -- 3
    NCRYPT_ASYMMETRIC_ENCRYPTION_OPERATION -- 4
    NCRYPT_SIGNATURE_OPERATION -- 10 (16)

    NCryptCreatePersistedKey(Futurex CNG, RSA)
...
  All Algorithms:
    RSA

CertUtil: -csptest command completed successfully.
```

If you do not see the above text, the module is not installed or configured correctly. Review the logs for additional information. The location of the log file is defined in the configuration file in the previous step.

[8] INSTALL ACTIVE DIRECTORY CERTIFICATE SERVICES

Install AD CS, unless you wish to set up a standalone CA. In order to install AD CS:

1. Click **Start**, **Administrative Tools**, **Server Manager**, and then **Manage**. Click **Add roles and feature**. The *Before You Begin* box will open. Click **Next**.
2. Choose the installation type: Role-based or feature-based installation. Press **Next**.
3. The *Server Selection* page will open. Select the server from the domain (or local machine) on which to install AD CS. Press **Next**.
4. On the *Server Roles* page, check the box next to **Active Directory Certificate Services**. Press **Next**. Press **Add Features**.
5. The *Features* page will open. Press **Next**.
6. The *AD CS* page will open. Press **Next**.
7. In the *Role Services* page, select **Certificate Authority**. Press **Next**.
8. On the *Confirmation* page, press **Install**.
9. Once installation is complete, press **Close**.

[9] CONFIGURE ACTIVE DIRECTORY CERTIFICATE SERVICES

A new installation of AD CS needs to be configured with a Public Key Infrastructure (PKI).

NOTE: If Active Directory is not already installed, please do so before proceeding, unless this is a standalone CA.

1. Click **Start**, **Administrative Tools**, and then **Server Manager**. Select the flag icon to the left of **Manage**.
2. Select **Configure Active Directory Certificate Services** on the destination.
3. The *Credentials* page will open. Ensure your login meets the displayed requirements. Press **Next**.
4. The *Select Role Services* page will open. Select **Certification Authority** to enable the management and issuance of certificates. Click **Next**.
5. The *Specify Setup Type* page will open. The type designates the kind of certificate authority server, and is dependent on your requirements as a business. Select either **Enterprise** or **Standalone**. Enterprise CAs are integrated with Active Directory, while standalone CAs conduct operations offline.
6. The *Specify CA Type* page will open. Click **Root** or **Subordinate**. Select **Root** if you have not yet created a PKI. Select **Subordinate** if you are integrating with an existing PKI. Click **Next**.
7. The *Set Up Private Key* page will open. Select **Use existing private key** or **Create a new private key**.
    - Select **Use existing private key** if you have integrated this CA with the Futurex hardware previously and the private key already exists on the HSM (i.e. this is a reinstallation of the CA server). Then, choose **Select an existing private key on this computer**.
    - If this is a new CA, select **Create a new private key**.
8. If **Create a new private key** was selected:
    - The *Configure Cryptography for CA* window will open. Choose **Futurex CNG** from the drop-down menu.
    - Select a **key character length**: 2048, 3072, or 4096.
    - Select a **hash algorithm** from the drop-down menu: SHA-1, SHA-256, or SHA-512. Checking **Allow administrator interaction when the private key is accessed by the CA** will have no effect.
    - Select **Next**.
9. If **Use existing private key** was selected:
    - The *Existing Key* window will open. **Change** the **Cryptographic provider** to **Futurex CNG**.
    - Clear the **common name** field. Click **Search**. Locate the key you want to use from the search results.
    - Checking **Allow administrator interaction when the private key is accessed by the CA** will have no effect.
    - Select **Next**.
10. The *CA Name* page will open. Configure your PKI names. Click **Next**.
11. If **Root CA** was selected in step 6, the *Set the Certificate Validity Period* page will open. Designate the default validity for the root CA. Click **Next**.
12. If **Subordinate CA** was selected in step 6, The *Certificate Request* page will open.
    - You can choose a **parent CA** instance of AD CS on your domain to issue you a certificate.
    - You may save a **certificate request** to file and have it signed by an external CA.
13. The *Certificate Database* page will open. Click **Next**.
14. The *Confirmation* page will open. Press **Configure**.

15. To confirm that the root CA was installed successfully, enter this command in a command prompt:

```
$ certutil -csptest -csp "Futurex CNG" RSA
```

A successful response to this command should contain:

```
STATE: 4  RUNNING
```

For more information on installing and configuring Active Directory Certificate Services, refer to Microsoft's documentation.

[10] ENFORCING WINDOWS ACCESS CONTROL ON AN HSM LEVEL

NOTE: For this step you will need to be logged in with an Identity that has a role with permissions **Keys:All Slots**. The default Administrator role and Admin identities can be used.

The Futurex CNG allows Windows to associate an Access Control List (ACL) with an HSM key slot. Windows will update this ACL during keypair generation and permission updates. To lock the ACL from changing, perform the following steps:

1. Connect the Excrypt Manager application to the Vectera Plus HSM.
2. Login under dual-control.
3. Choose the **Key Management** page.
4. Choose **Edit Key Storage**.
5. Locate the board slot containing the CNG private key.
    - This information is logged by the CNG provider during keypair generation.
6. Check the **Immutable** security option.
7. Press **Apply Changes**.

[11] VIEW CERTIFICATE STORE

The following command can be used to view the CA's certificate store. The LDAP URI will vary depending on your organization's Active Directory domain (IE: fx.futurex.com) and CA name (IE: fx-FXCA).

```
certutil -viewstore "ldap:///CN=fx-FXCA,CN=Certification Authorities,
CN=Public Key Services,CN=Services,CN=Configuration,DC=fx,
DC=futurex,DC=com?cACertificate?base?objectClass=certificationAuthority"
```

Between tests you may choose to clear the certificate store using a command similar to the following:

```
certutil -delstore "ldap:///CN=fx-FXCA,CN=Certification Authorities,
CN=Public Key Services,CN=Services,CN=Configuration,DC=fx,
DC=futurex,DC=com?cACertificate?base?objectClass=certificationAuthority" fx-FXCA
```

[12] SIGN CERTIFICATE USING THE HSM

The following steps will demonstrate one way to test using the HSM to sign a certificate for the CA server.

1. Open the **Certificate Manager** on the CA server
2. Right-click on **Personal** -> **All Tasks** -> **Request New Certificate…**
3. The *Certificate Enrollment* dialog will open. Press **Next**.
4. The *Certificate Enrollment Policy* page will open. Choose a certificate enrollment service associated with the CA server, e.g. **Active Directory Enrollment Policy** for an Enterprise CA. Press **Next**.
5. The *Request Certificates* page will open. Choose a certificate template. Press **Enroll**.
6. If the HSM is connected you will receive a success message. If the HSM is offline you will receive an error.
7. To locate the certificate we just issued:
    - Open the **Active Directory Certificate Authority** tool from the Server Manager.
    - Expand the node associated with your CA common name.
    - Click **Issued Certificates**.
    - A certificate matching your request should be found on this page.

APPENDIX A: MIGRATING AN EXISTING CA KEY FROM SOFTWARE STORAGE TO THE HSM

This process will involve the following steps:

1. Back up the CA database, CA certificate, and private key on the AD CS server
2. Remove the CA role service from the AD CS server
3. Import the private key into the Vectera Plus HSM
4. Import the CA certificate, re-add the CA role service, and restore the CA database and configuration on the AD CS server

[12.1] BACK UP THE CA DATABASE, CA CERTIFICATE, AND PRIVATE KEY ON THE AD CS SERVER

You must use an account that is a CA administrator. On an enterprise CA, the default configuration for CA administrators includes the local Administrators group, the Enterprise Admins group, and the Domain Admins group. On a standalone CA, the default configuration for CA administrators includes the local Administrators group.

[12.1.1] To back up a CA database and private key by using the Certification Authority snap-in

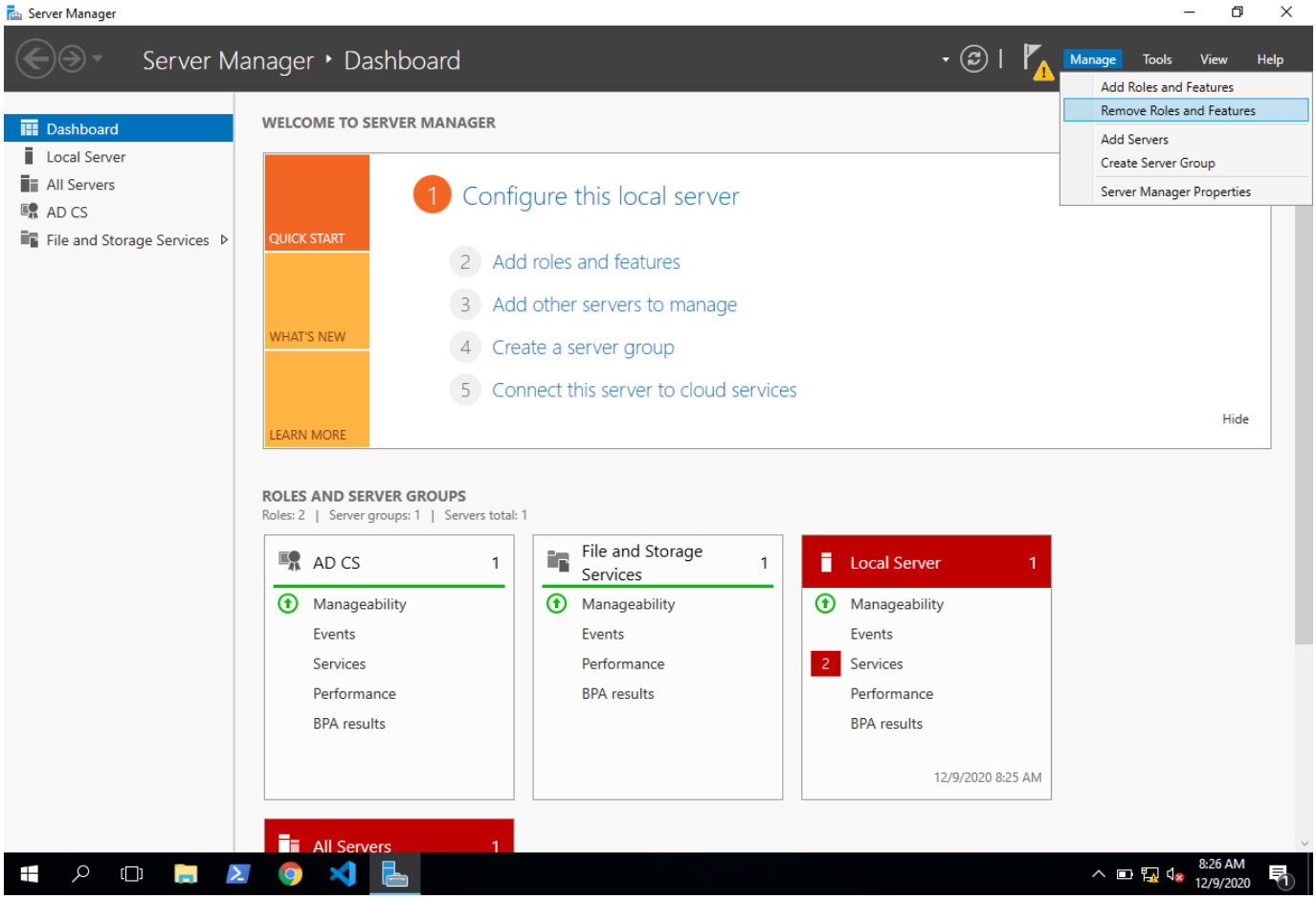
1. Choose a backup location and attach media, if necessary.
2. Log on to the source CA.
3. Open the **Certification Authority** snap-in.
4. Right-click the node with the CA name, point to **All Tasks**, and then click **Back Up CA**.
5. On the **Welcome** page of the CA Backup wizard, click **Next**.
6. On the **Items to Back Up** page, select the **Private key and CA certificate** and **Certificate database and certificate database log** check boxes, specify the backup location, and then click **Next**.
7. On the **Select a Password** page, type a password to protect the CA private key, and click **Next**.
8. On the **Completing the Backup Wizard** page, click **Finish**.
9. After the backup completes, verify the following files in the location you specified:
    - *CAName.p12* containing the CA certificate and private key
    - Database folder containing files *certbkxp.dat*, *edb#####.log*, and *CAName.edb*
10. Open a Command Prompt window, and type **net stop certsvc** to stop the Active Directory Certificate Services service.
    IMPORTANT: The service should be stopped to prevent issuance of additional certificates. If certificates are issued by the source CA after a database backup is completed, repeat the CA database backup procedure to ensure the database backup contains all issued certificates.

11. Copy all backup files to a location that is accessible from the destination server; for example, a network share or removable media.

These steps can also be completed using Powershell or Certutil.exe. Instructions for these methods can be found in the following Microsoft knowledge base article: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn486805(v=ws.11)

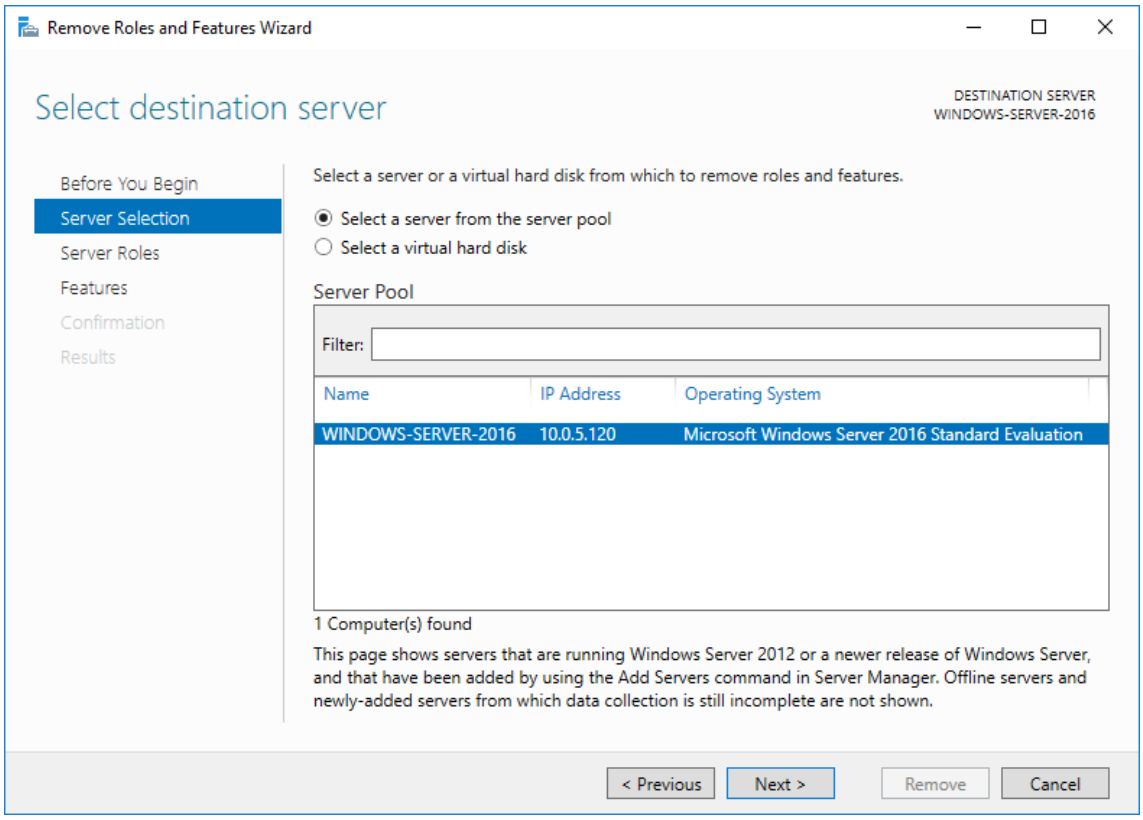
[12.2] REMOVE THE CA ROLE SERVICE FROM THE AD CS SERVER

In Server Manager, click the **Manage** button in the top menu, then select **Remove Roles and Features**, as shown below:

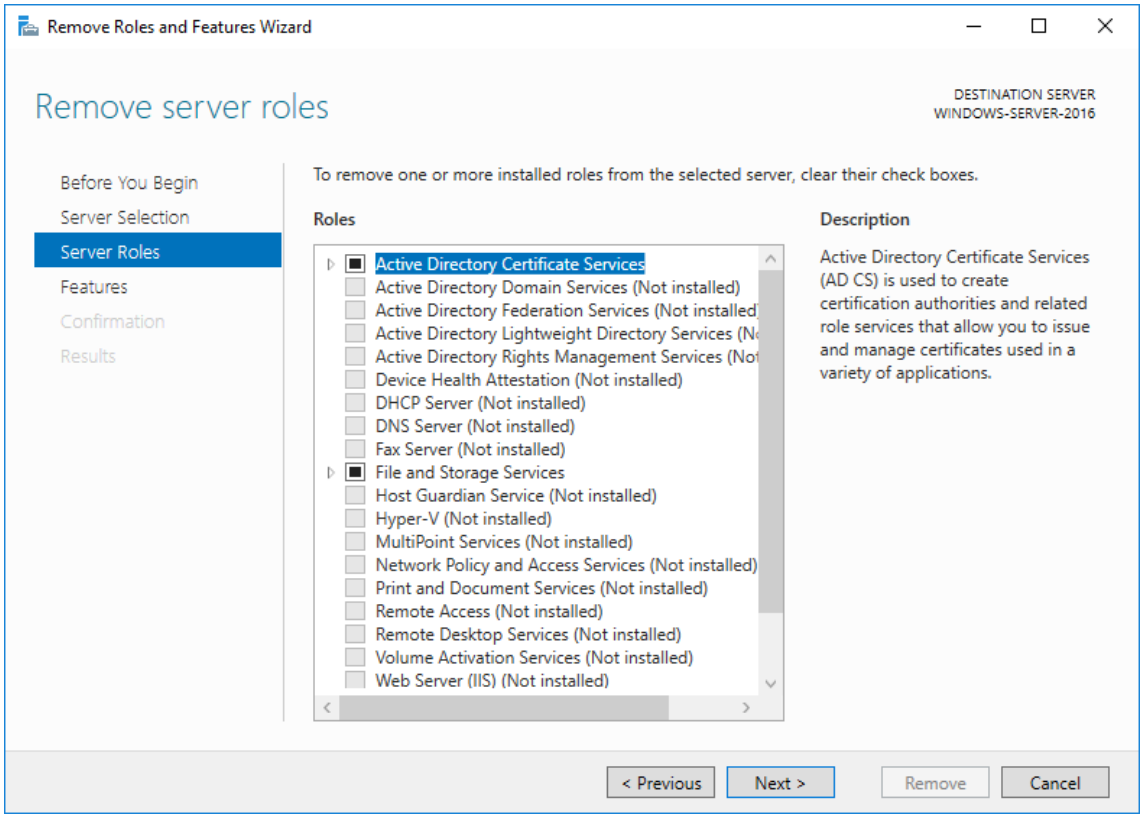


This will open the *Remove Roles and Features Wizard*. In the first *Before you begin* dialog, click **Next >**.

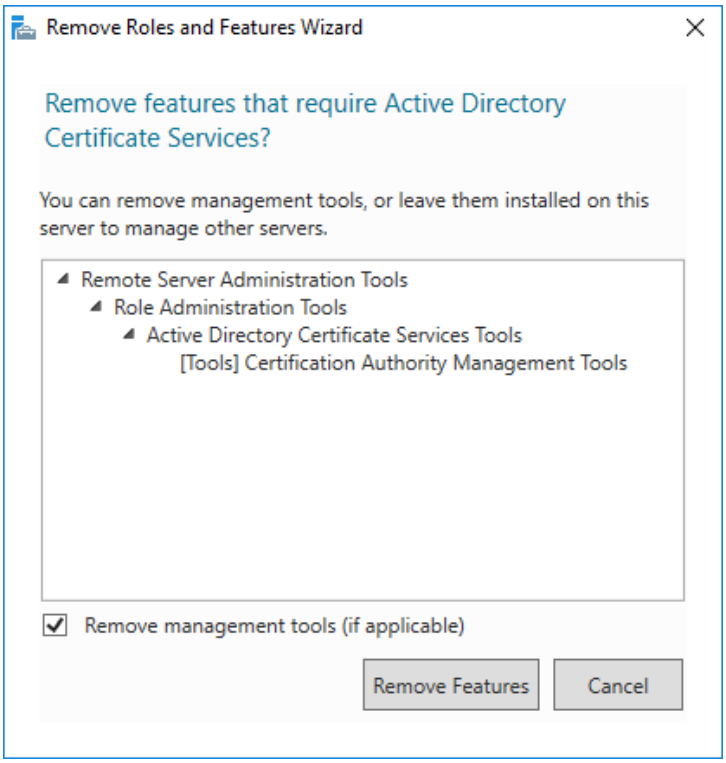
In the *Select destination server* dialog, leave the default option selected, and click **Next >**.



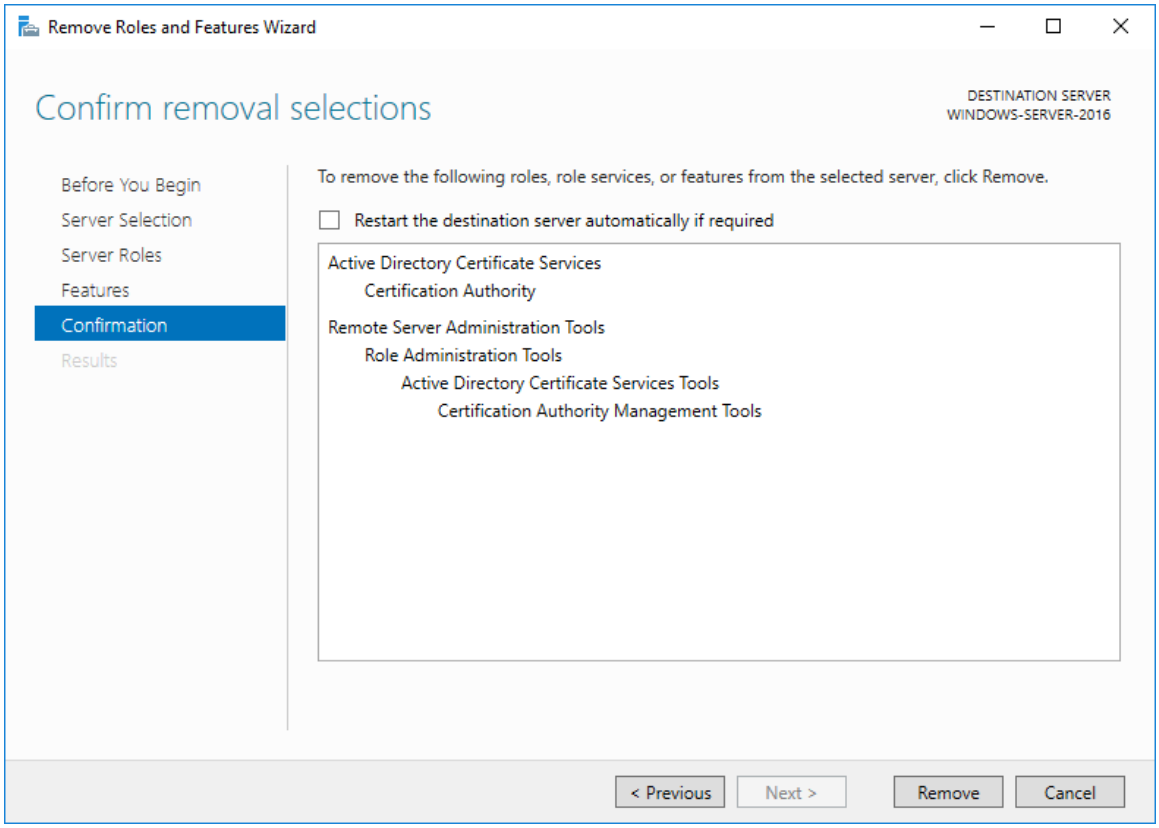
In the *Remove server roles* dialog, select the **Active Directory Certificate Services** role.



The following dialog will pop up. Click **Remove Features**.



Click **Next >** until you reach the *Confirmation* page, then click **Remove**.



Once the feature removal completes, close the window and restart the server to finish removing features.

[12.3] IMPORT THE PRIVATE KEY INTO THE VECTERA PLUS HSM

In this section, the HSM CLI application will be used to import the private key that was backed up from AD CS.

First, run the following command to connect to the HSM via USB (**NOTE:** The computer that is running HSM CLI must be directly connected to front USB port of the HSM.)

```
$ connect usb
```

Then, login with the default Admin identities.

```
$ login user
```

NOTE: The **login user** command will prompt for the username and password. You will need to run it twice because you must login with both default Admin identities.

Now, run the following command to import the private key of the CA into an available key slot on the HSM.

```
$ pkcs12 import -f C:\Futurex\WINDOWS-SERVER--CA.p12 -p safest -s 10 --label WINDOWS-SERVER--CA --win-system-dacl
```

If the import was successful, when you run the `keytable reload` command you will see the private key in the slot that was designated.

```
$ keytable reload
result:
    status: success
    statusCode: 0
slots:
    -
        slot: 10
        type: "key"
        name: "WINDOWS_SERVER__CA"
        kcv: "266B"
        algorithm: RSA
        bits: 2048
        usage: Sign,Verify
        startValidity: "1971-01-01 00:00:00"
        endValidity: "2999-01-01 00:00:00"
        exportable: true
        clearExportable: false
        passwordExportable: false
        requiresAuth: false
        modifiable: true
        externalData:
"0100000003000001257494E444F57532D5345525645522D2D434100001020000001257494E444F57532D5345525645522D2D434100001200000010087C59F43B051DEF062AAD4AA8128913D3344D4AF197B28C709242504E9323B65A6609251EB2061674E2B55F3B1CCD85C573D76EAD3F6EDFECA3AAD729EC25EEC5AE078E38E0E803E92C86C06C5C11914CD5FCF12DE26465534CCD911D9568D12093EF4CA311B4D2795CA92BD23F43898DC382A65B131597F7C946DDEAD3DEF0A792B85321A074D8E31B11A20700A531B1746F1A8F7239EC17EE4FD1F8C8209B142E7C8BA51C2724B286CEDA0141D0021154CD43FAEF77BBC3390A88172B9ADD6D54BED3E1E3855AB9AB822F1B900D430C22542DAB2FA96AE8A03268D717F6F98F6817320CF87E3C63BE5AB374C1606377DB481C1C327E46BF6E553E6FB3E3F8B000001210000000400080000000001220000000301000100000163000000010080000DA7E0000004801000494000000000000000000000000000140000000200340002000000000318000000001001020000000000052000000020020000000314000000001001010000000000512000000"
```

[12.4] IMPORT THE CA CERTIFICATE, RE-ADD THE CA ROLE SERVICE, AND RESTORE THE CA DATABASE AND CONFIGURATION ON THE AD CS SERVER

[12.4.1] Importing the CA certificate

1. Start the Certificates snap-in for the local computer account.
2. In the console tree, double-click **Certificates (Local Computer)**, and click **Personal**.
3. On the Action menu, click **All Tasks**, and then click **Import** to open the Certificate Import Wizard. Click **Next**.
4. Locate the *<CAName>*.p12 file created by the CA certificate and private key backup, and click **Open**.
5. Type the password, and click **OK**.
6. Click **Place all certificates in the following store**.
7. Verify **Personal** is displayed in **Certificate store**. If it is not, click **Browse**, click **Personal**, click **OK**.

NOTE: The imported CA certificate file was in PKCS #12 format; therefore, it contained both the certificate and the private key. The private key should not exist in AD CS, however, because it is stored on the HSM. We'll delete both the private key's association with the CA certificate and the private key itself in the steps that follow.

8. In the console tree, double-click **Personal Certificates**, and click the imported CA certificate.
9. On the **Action** menu, click **Open**. Click the **Details** tab, copy the serial number to the Clipboard, and then click **OK**.
10. Open a Command Prompt window, type **`certutil -store My "{Serialnumber}"`** and then press **ENTER**.
11. From the output of the previous command, copy the value that is in the **Unique container name** field to the clipboard.
12. Run the following command to delete the private key's association with the CA certificate:
    ```
    certutil -delkey -csp ksp "{Key Container}"
    ```
13. Run the following command to delete the private key:
    ```
    certutil -delkey -csp ksp "{Key Name}"
    ```

    NOTE: The `Key Name` value is the same as the certificate's name, as it shows in the Certificates snap-in menu.

An important final step is associating the private key now stored on the HSM with the CA certificate stored in AD CS.

14. Run the following command to repair the association between the imported CA certificate and the private key stored in the HSM:
    ```
    certutil -repairstore -csp "Futurex CNG" My "2545a152bd9befa84b967ee57d3b6faf"
    ```

[12.4.2] Re-adding the CA role service by using Server Manager

1. In the console tree, click **Roles**.
2. On the **Action** menu, click **Add Roles**.
3. If the **Before you Begin** page appears, click **Next**.
4. On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box, and click **Next**.
5. On the **Introduction to AD CS** page, click **Next**.
6. On the **Role Services** page, click the **Certification Authority** check box, and click **Next**.
7. On the **Specify Setup Type** page, specify either **Enterprise** or **Standalone**, to match the source CA, and click **Next**.
8. On the **Specify CA Type** page, specify either **Root CA** or **Subordinate CA**, to match the source CA, and click **Next**.
9. On the **Set Up Private Key** page, select **Use existing private key** and **Select a certificate and use its associated private key**.
10. In the Certificates list, click the imported CA certificate, and then click Next.
11. On the CA Database page, specify the locations for the CA database and log files.
12. On the Confirmation page, review the messages, and then click Configure.

[12.4.3] Restoring the CA database and configuration

The procedures in this section should be completed only after the CA role service has been re-installed.

[12.4.3.1] To restore the CA database by using the Certification Authority snap-in

1. Start the Certification Authority snap-in.
2. Right-click the node with the CA name, point to **All Tasks**, and then click **Restore CA**.
3. On the **Welcome** page, click **Next**.
4. On the **Items to Restore** page, select **Certificate database and certificate database log**.
5. Click **Browse**. Navigate to the parent folder that holds the **Database** folder (the folder that contains the CA database files created during the CA database backup).
   WARNING: Do not select the **Database** folder. Select its parent folder.
6. Click **Next** and then click **Finish**.
7. Click **Yes** to start the CA service (certsvc).

APPENDIX B: 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 will help do 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 cannot be found 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

XCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com