NetApp ONTAP and Entrust KeyControl

Integration Guide

2024-04-29

Table of Contents

Chapter 1. Introduction

This document describes the integration of the NetApp ONTAP data management software with the Entrust KeyControl key management solution using the open standard KMIP protocol. KeyControl serves as a key manager for encryption keys by using various protocols, including KMIP.

1.1. Product configuration

Entrust has successfully tested the integration of KeyControl with NetApp ONTAP in the following configurations:

Product	Version
NetApp ONTAP	9.8P3, 9.9.1, 9.10.1, 9.12.1, 9.14.1
Entrust KeyControl	5.3, 5.4, 5.5.1, 10.0, 10.1, 10.1.1, 10.2

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- NetApp ONTAP 9 Online Documentation.
- Entrust KeyControl Online Documentation Set.

Chapter 2. Deploy Entrust KeyControl

The following steps summarize the deployment of the Entrust KeyControl:

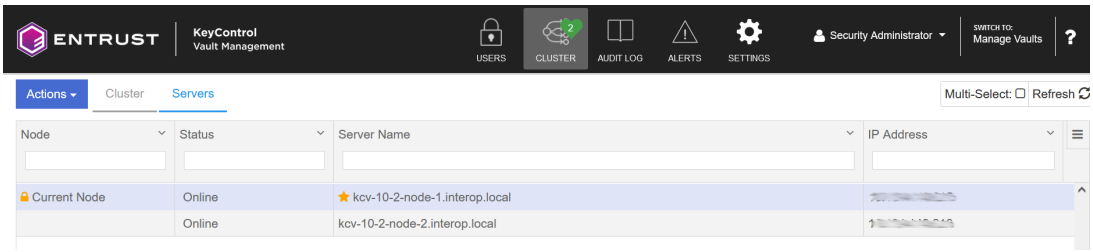
1. Deploy a Entrust KeyControl cluster
2. Create a KMIP Vault in Entrust KeyControl
3. Create the Entrust KeyControl client certificate bundle

2.1. Deploy a Entrust KeyControl cluster

For the purpose of this integration, a two-node cluster was deployed.

1. Download the Entrust KeyControl software from Entrust TrustedCare. This software is available both as an OVA or ISO image. The OVA installation method in VMware is used in this deployment.
2. Install Entrust KeyControl as described in Entrust KeyControl OVA Installation.
3. Configure the first Entrust KeyControl node as described in Configuring the First Entrust KeyControl Node (OVA Install).
4. Add second Entrust KeyControl node to cluster as described in Adding a New Entrust KeyControl Node to an Existing Cluster (OVA Install).

Both nodes need access to an NTP server. Sign in to the console to change the default NTP server if required.



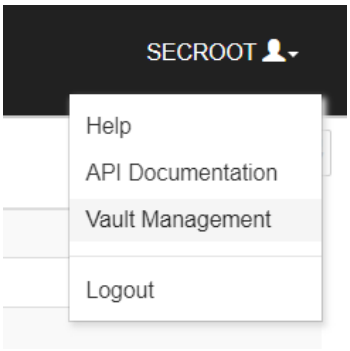
5. Install the Entrust KeyControl license as described in Managing the Entrust KeyControl License.
6. Add a record in your DNS server for the Entrust KeyControl cluster. Associate all KeyControl Cluster node IPs to the one record.
7. Install a signed certificate from your local root CA. See Appendix A - Install a signed certificate from your local root CA in the Entrust KeyControl cluster

2.2. Create a KMIP Vault in Entrust KeyControl

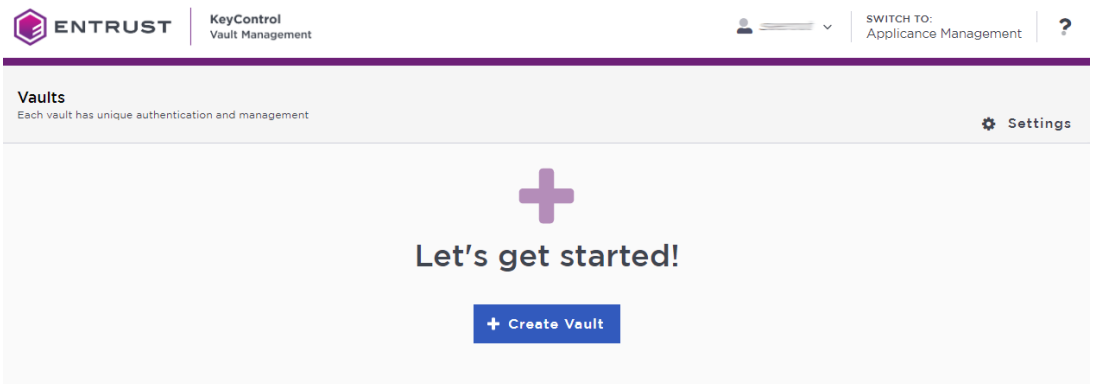
The Entrust KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a KMIP Vault in the Entrust KeyControl Vault Server.

Refer to the Creating a Vault section of the admin guide for more details.

1. Sign in to the Entrust KeyControl Vault Server web user interface:
   a. Use your browser to access the IP address of the server.
   b. Sign in using the **secroot** credentials.
2. From the user's dropdown menu, select **Vault Management**.



3. In the Entrust KeyControl Vault Management interface, select **Create Vault**.



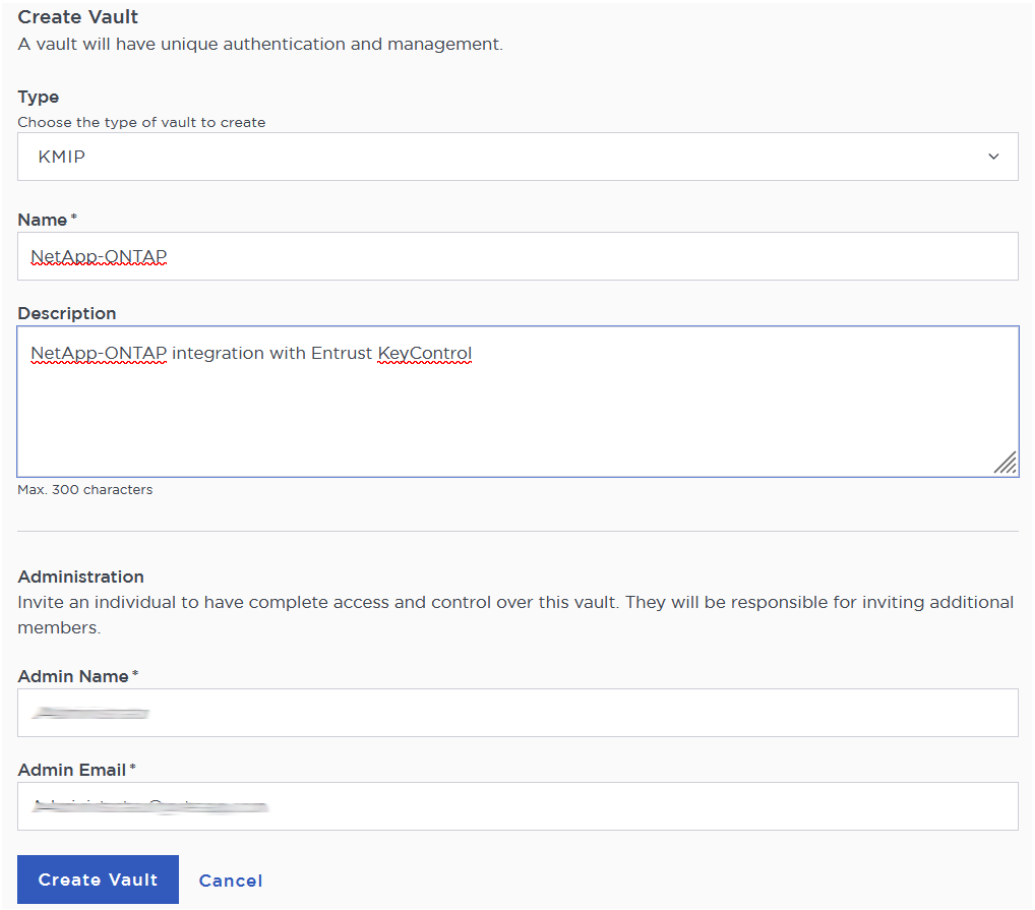
   Entrust KeyControl Vault supports the following types of vaults:

   - **Cloud Key Management** - Vault for cloud keys such as BYOK and HYOK.
   - **KMIP** - Vault for KMIP Objects.
   - **PASM** - Vault for objects such as passwords, files, SSH keys, and so on.
   - **Database** - Vault for database keys.
   - **Tokenization** - Vault for tokenization policies.
   - **VM Encryption** - Vault for encrypting VMs.

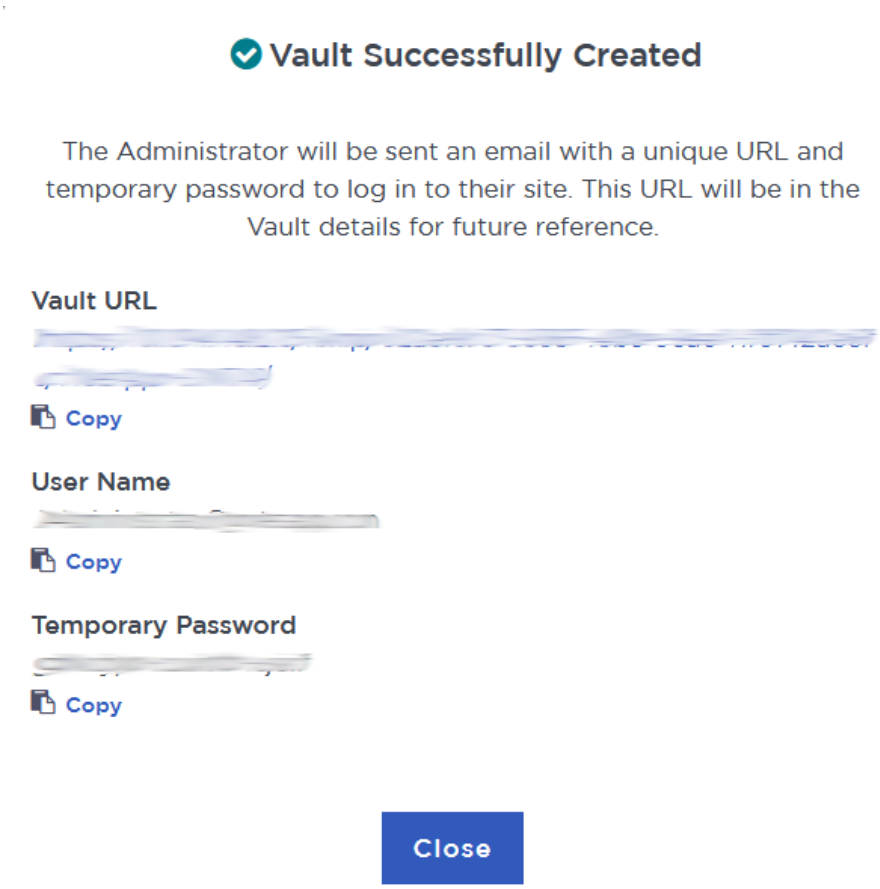
4. In the **Create Vault** page, create a **KMIP** Vault:

Field	Value
Type	**KMIP**
Name	Vault name
Description	Vault description
Admin Name	Vault administrator username
Admin Email	Vault administrator email

For example:

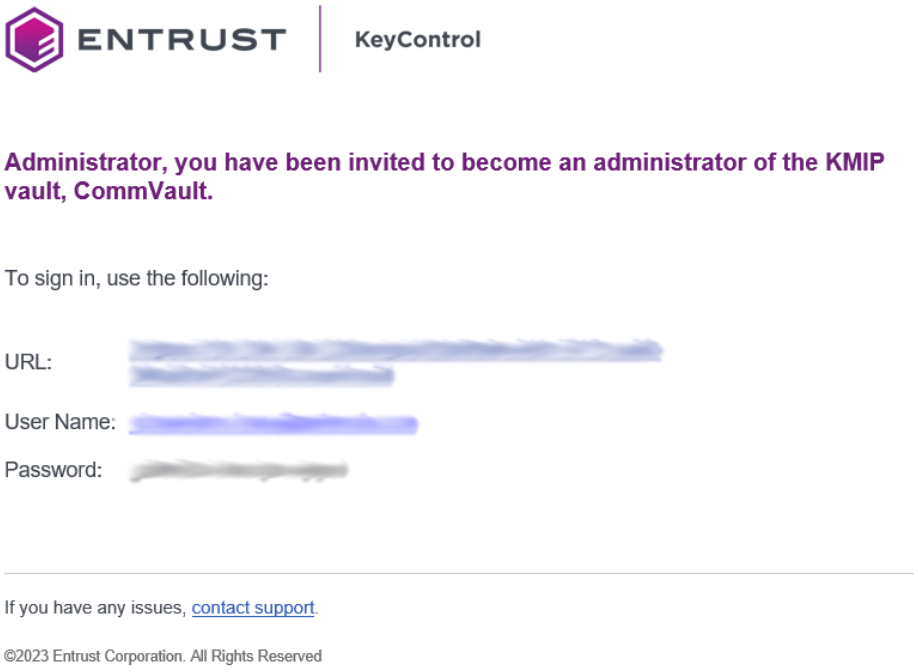


5. Select **Create Vault**. Then select **Close**.



The new vault's URL and sign-in credentials will be emailed to the administrator's email address entered above. In closed gap environments where email is not available, the URL and sign-in credentials are displayed at this time.

Example email:



ENTRUST | KeyControl

Administrator, you have been invited to become an administrator of the KMIP vault, CommVault.

To sign in, use the following:

URL:

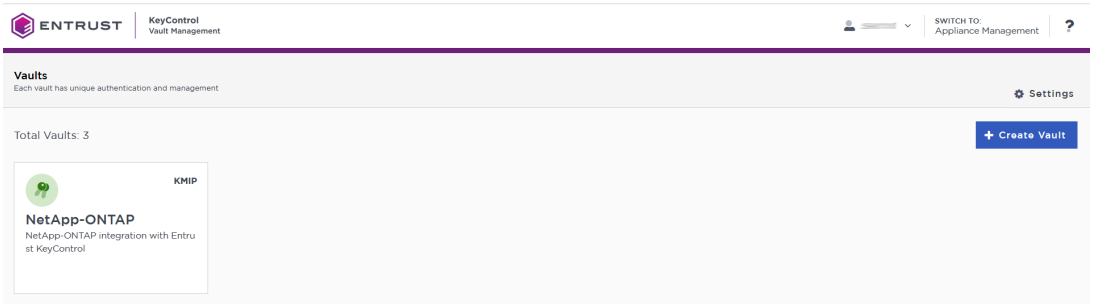
User Name:

Password:

If you have any issues, contact support.

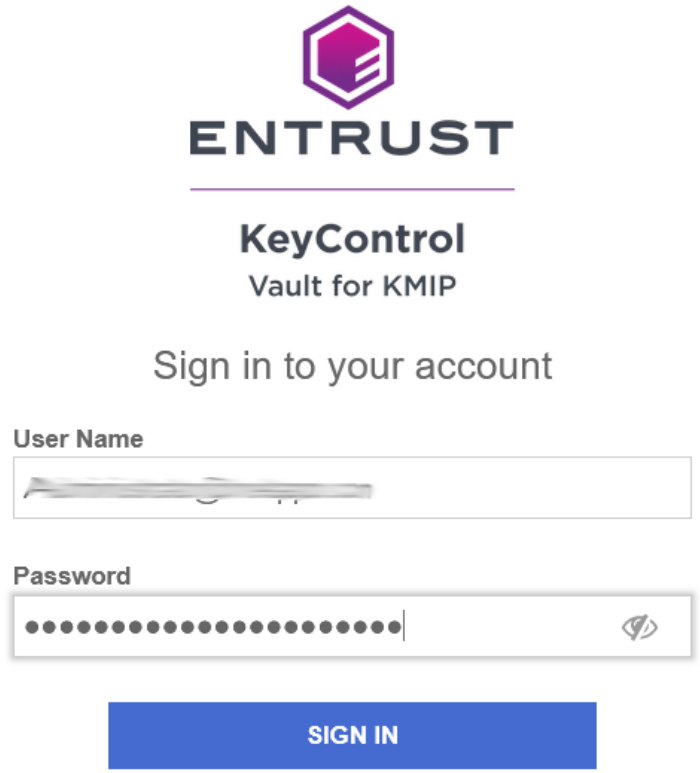
6. Bookmark the URL.
7. The newly created Vault is added to the **Vault Management** dashboard.

   For example:



8. Sign in to the URL provided above with the temporary password. Change the initial password when prompted. Sign in again to verify.

   For example:



9. Notice the new vault.

   For example:

2.3. Create the Entrust KeyControl client certificate bundle

Certificates are required to facilitate the KMIP communications from the Entrust KeyControl KMIP Vault and NetApp ONTAP application and conversely. The built-in capabilities in Entrust KeyControl are used to create and publish the certificate.

1. Login to the KMIP Vault with the URL and credentials from Create a KMIP

Vault in Entrust KeyControl.

2. Select **Security**, then **Client Certificates**.

3. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate. The **Create Client Certificate** dialog box appears.
4. In the **Create Client Certificate** dialog box:

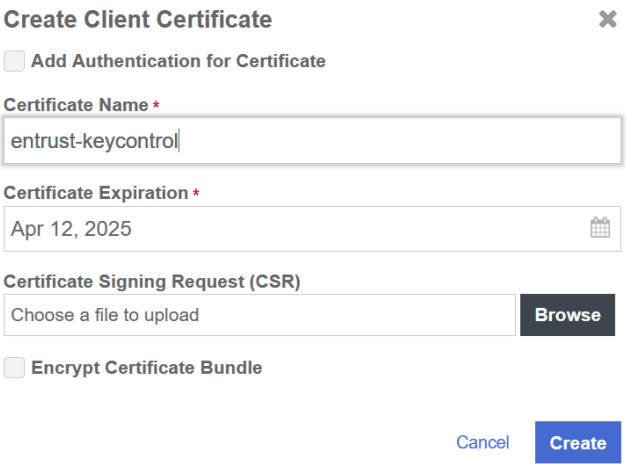
   a. Enter the username.

   b. Enter the expiration date.

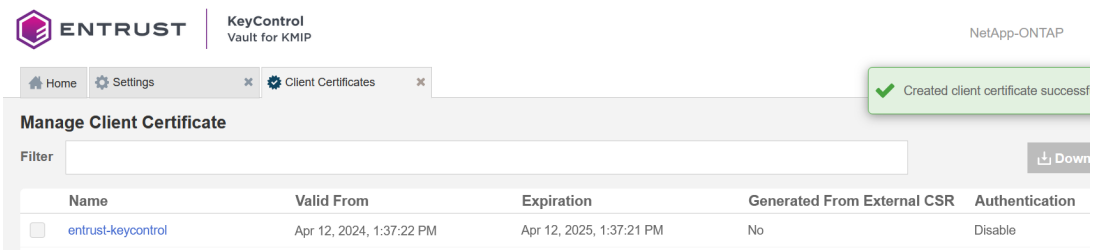
   c. Leave **Certificate Signing Request (CSR)** field as default.

   d. Select **Create**.

   For example:



   The new certificates are added to the **Manage Client Certificate** pane.

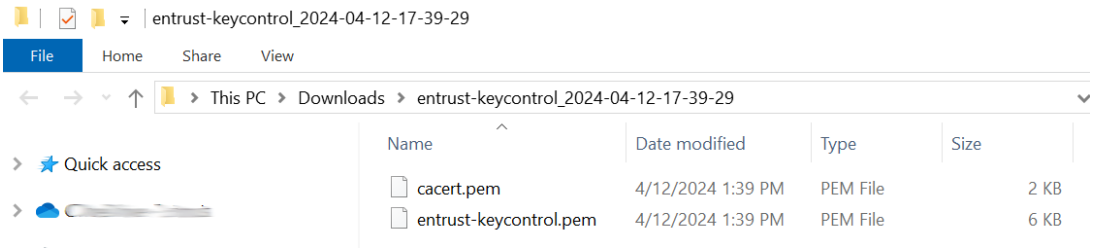


5. Select the certificate and select the **Download** icon to download the certificate.
6. Unzip the downloaded file. It contains the following:
    - A `certname.pem` file that includes both the client certificate and private key. In this example, this file is called `entrust-keycontrol.pem`.

      The client certificate section of the `certname.pem` file includes the lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" and all text between them.

      The private key section of the `certname.pem` file includes the lines "-----BEGIN PRIVATE KEY-----" and "-----END PRIVATE KEY-----" and all text in between them.

    - A `cacert.pem` file which is the root certificate for the KMS cluster. It is always named `cacert.pem`.



Chapter 3. Deploy NetApp Simulate ONTAP

This integration testing was performed using Simulate ONTAP configured as a single node. Simulate ONTAP 9.x is a virtual simulator for ONTAP® software. The virtual simulator was deployed as a virtual machine in VMware.

1. Download the simulator ova file from Simulate ONTAP Download
2. Deploy the virtual machine. For the purpose on this integration, the **STORAGE SYSTEM NAME** is set to **mycluster**.
3. Add a record in your DNS server for the **Cluster Management**.
4. Configure the NTP server per NetApp documentation.
5. Install the root CA certificate from your root CA.

   For example:

```
mycluster::> security certificate install -vserver mycluster -type server-ca -subtype kmip-cert

...

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:
CA: interop-CONTROLLER-CA-4
serial: 3DAC5A62645AD5AB4E569666B3E4DA66

The certificate's generated name for reference: interop-CONTROLLER-CA-4
```

   Note the certificate's generated name above, e.g. **interop-CONTROLLER-CA-4**. It will be needed in section Setup Entrust KeyControl as the external KMIP server.

Chapter 4. Integrate Entrust KeyControl with NetApp ONTAP

The following steps summarize the integration of Entrust KeyControl with NetApp ONTAP.

- Install the Entrust KeyControl client bundle into NetApp ONTAP
- Setup Entrust KeyControl as the external KMIP server

4.1. Install the Entrust KeyControl client bundle into NetApp ONTAP

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.

```
>ssh admin@xxx.xxx.xxx.xxx
Password:

Last login time: 4/11/2024 19:44:22
mycluster::>
```

2. Run the following command. Paste the certificate section from the `entrust-keycontrol.pem` file from section Create the Entrust KeyControl client certificate bundle when prompted. Paste the private key section when prompted.

```
mycluster::> security certificate install -vserver mycluster -type client -subtype kmip-cert

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIEbzCCA1egAwIBAgIFANedlIcwDQYJKoZIhvcNAQELBQAwVzELMAkGA1UEBhMC
VVMxFTATBgNVBAoTDEh5VHJ1c3QgSW5jLjExMC8GA1UEAxMoSHlUcnVzdCBLZXlD
b250cm9sIENlcnRpZmljYXRlIEF1dGhvcml0eTAeFw0yNDA0MTIxNzM3MjFaFw0y
NTA0MTIxNzM3MjFaMEExCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxIeVRydXN0IElu
Yy4xGzAZBgNVBAMTEmVudHJ1c3Qta2V5Y29udHJvbDCCAiIwDQYJKoZIhvcNAQEB
BQADggIPADCCAgoCggIBAM4hA5shy2Hg/hGohHbPKXnFoMOmb8pg1fdOQJkbYgeE
XXdsI7flIYazFM0zW4EzBMtvt334hYFWzVLcnYLSLqveA2Z0cfnTuTQxjooUccKU
O/cXUJEo4DLgm38GQYo6lqQ6I53ULDLc+Ru13qvgzEBBZH1QogWOawp2r/RtxMOO
8IuukNht24pCrR8TKebVqws1ZFxqBCC1FDdxJwj3ICzCcN5f0b9ilZ6bfQWJaZNH
IJuAwzEFGm+hnXyKa6rru1HuYLe+I55StcmpDTMsrGgG7wdWccz6aDCov6fb8+7s
FpWnhLfcl71B59fFZ0vivCBZc52gBNjqiZ1LOBeImFeFxG9wWGw0KTuaSsqXs1a2
bksH04d41ypZwTKESD6pVm2OG4ZJcOx31dlarZ5bYHfA/omy7nor6X5aZeneVz3X
jcJ1Zq1cNfsoDKBdVZMN+9vK45NJwBMKVv3kX9kRj4K1Om11K23ft3EAz9dHVn8m
Rvkese3EWiVSPdJ+dmCowPAExgziFLkP4Fu81QKg8j8MMMkflV6kM3GRHDD2SR3Z
RMBVXlYKZ3dRtBI8tBRqygUBvEjof7U3ipz3Ud7yfiLTcbndV/Grx1+L3SlyR23n
gmVT8lNN9xyMPL+aynLEOIdf+4rZtJpr2v/dVgeQ2TZKwfTWGK32q3cjbc8XxeVZ
AgMBAAGjWDBWMAkGA1UdEwQCMAAwHQYDVR0OBBYEFLIzJE8cOJBHq9c4KXv4GrNS
eg1tMB8GA1UdIwQYMBaAFHeHQXWETJvG04kYPw0AdMOwEPnfMAkGA1UdEQQCMAAw
DQYJKoZIhvcNAQELBQADggEBAE93rfmybwGfMd1pIQuoz00t/zY9qgaGfAQKKMr7
WSwJanuQTOH2R8yBpNWl+M7dEggB9ooiRxzSkqV8Xp9e52aonkg3pKgkEJCpuQVc
cY1M/CY+G1FD+V/TrUkxM3jI8NohdynWrQBa9XHxiwkHYFB+PBvpz+RYKnaI9G2o
AHh+maljHIY3xnrvfRNN6XKZXqX+TCbw/TC77Eki+vYsh/0NmCpPX78MdARdB3Pg
```

```
D3TO9gFlwJCaMgljsaUxpNI14jHi3nW3oY2x2OZfOtrj9+nzH617h5X5NPyib2SX
CLg8cOSNe6pNUusdeH4Z3JvxVWBWGwBbxevIyt49G2BpQic=
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQDOIQObIcth4P4R
qIR2zyl5xaDDpm/KYNX3TkCZG2IHhF13bCO35SGGsxTNM1uBMwTLb7d9+IWBVs1S
3J2C0i6r3gNmdHH507k0MY6KFHHClDv3F1CRKOAy4Jt/BkGKOpakOiOd1Cwy3Pkb
td6r4MxAQWR9UKIFjmsKdq/0bcTDjvCLrpDYbduKQq0fEynm1asLNWRcagQgtRQ3
cScI9yAswnDeX9G/YpWem30FiWmTRyCbgMMxBRpvoZ18imuq67tR7mC3viOeUrXJ
qQ0zLKxoBu8HVnHM+mgwqL+n2/Pu7BaVp4S33Je9QefXxWdL4rwgWXOdoATY6omd
SzgXiJhXhcRvcFhsNCk7mkrKl7NWtm5LB9OHeNcqWcEyhEg+qVZtjhuGSXDsd9XZ
Wq2eW2B3wP6Jsu56K+l+WmXp3lc9143CdWatXDX7KAygXVWTDfvbyuOTScATClb9
5F/ZEY+CtTptdStt37dxAM/XR1Z/Jkb5HrHtxFolUj3SfnZgqMDwBMYM4hS5D+Bb
vNUCoPI/DDDJH5VepDNxkRww9kkd2UTAVV5WCmd3UbQSPLQUasoFAbxI6H+1N4qc
91He8n4i03G53Vfxq8dfi90pckdt54JlU/JTTfccjDy/mspyxDiHX/uK2bSaa9r/
3VYHkNk2SsH01hit9qt3I23PF8XlWQIDAQABAoICACCxB7tg3rrFTkZKrceSD4fq
mhatnOlB9m1kkcY2m5OJoLFCC2AtDOYqHNB2prqU9tu0+isWcUYUGDheGPUYlKJZ
cbycFz+CHstyWKL5nxk3HVOQ9QwwqW4oRUEeIuLja+Tb+64aanAer7t/WrNz0bEX
LfLaCPhMoBlmvX1Ms3o4f1oH85z/v2PsMzzMc0bS+G+spiAqCEGPtoccgQ5g809l
/zSlicSKxCQFkQyBwKbFDxzajRqHLqwpu6p24aCYBnt2DQzXMRr5Dy/OifNl0Gon
P12wjhfuVvvwp4Td05A/DU3q5Zerer1faH/GJR3Z9fBDf5yuNlaYy/6QYXMKDO77
rYxG/+a8woYx5tpnc+lLiCkLu9f44LtIka07XGSSrrz5mK0hVllpAt9yoN6J/lz6
mLii/v7XGZSG/Y9cBANy8efQeA7ogK6x0v7/NV1OF8/W11FtpwQ1C+SAXB7gXf/m
qa/OIbZtf7igANcYm7EQgC1BQxeFA09vVwmy3X+3XdwGyqwA+LL7DodVvNYhVeLh
3Kxepf/qSpn8Zr9S+6VyoJ4lwOfs3HXa6u3GT0NN2vWOIaDSnQGdMh2nh4vFDcXN
YwWjs68xhQXdXWJyoYYw2uS/kc7Rag/iJ8SBNN+zluXWDAJfakBEj0qVxEICL0lg
YRSeYDG8zFEAhoUuFe8BAoIBAQDwVYAGdywul0+7WJO4jMxpXA0khtlJabJ2zoqj
z98ze1lbX5nh0SZ7kDN2mSHSOF1P+vG8WqCYWiPD/JWuQSgiYQnpwEsseyiLL687
RODMLHInB0r1GJA+XNVevMSJH4ffklNYjRFJfpafJbrRXDqKdukNfPg9g8m8eGuw
wR/lHYa/OIoCwEhvhBXVSEy5FbNzid1mWSfaMQ+1xN7yPKuiCti7pVlam8W6xKT7
IfKj8rZMQCfkj+Y8W1OYGHrP5TmtluTmedSch294rPKmp7fmK7Y2OtFtgl3bhKFI
zTnK6YKtDdV1lJ89NKiyh8Pm37OQ3FmVZ6kymeJSqxRzbTVxAoIBAQDbkLplsD5h
QnFaUInEcb2X9Wkwd35vcn0gDgx84Jth356CfkhF2FqRIFj12tMQGseDvWsLuAKb
Yb/AegTkGEPwQJpXJI05pBWw9+ptxIdqOXgnzB5vvGZ4oNAxrx5GNiSXDvGTcZI/
3feAHq47fNAbHf8vZOsUyCj61tzt8XuO8QJnCCWiLo+RM2DXu7UDyoLVmLp7KNdd
7AMCFws8rDt7ZjgIFiTjT7DRF09GqxEM4ZFhBoYW20MH5nXpOAd2vkcB4BPNHMxk
gxfd6IvqNuqazbQ6RgEugpqgkh+Tt1nE4dMrkW+ORoJ6LMo16uOyN+Iy3b/qOLmS
agGoVKRcpZppAoIBAQDC5tO4apTuA8+pQyApHiX3m6sc4C7+ljUgnEdaqY19Fp9U
tqb4tsDanArgNzdyYDtsTToVYfmzFAbFPeW1NynxF3kOk99i503t8nHNQwJ7EeBR
PlzPf2ga6vYuqi9IdMWfze7BdUV7sKk9zz894emnuN8vDRXT7TiBG7dZ1ISlLdjE
4nkp2f3kUd3S5ZsyziKFpFxkUBE9pWP0KQAUupcGBn3VTzazgHhOCoMxFkrMIl0s
YSr49KnmcLnOMqwGRQMNf72KG2sMtdj0qGzwMju08eYG/JQylvK+v0R84dHoeI59
AScG/8xTuozEm82HQgtBgzEzNKnGW31rRUqEgSBBAoIBAA1G7C6YAL2q4eXfNuV9
J0TYHztCDpA4sR5OGy01+89oUVJ8xmwK0Dc0aIy9ZcP0ipoJyz5TKz0wJQNDnaYZ
XYparbqVSEDzDii8ZR2sI7Alt4FYk4KYNu4Wc2B9wWvnfEDyM2OCG6DnED9cG5cX
ThJFtxerl5eTHv9EHOn6j0kug8GtOXFcNWxHWhTRkfmftleqO6SU7KkOS4RF1nUd
yR8GKF88z5A7UmriaPXSBF7uCPeACH27VotUwU6QB8uDaBHR9gCSPD3bu4a8uDE6
juc7hyl68DlaxnTtQSGSlcgVC8r3qXJGCz/OE5A9GvW88V24ERHdykLzTBRcwe+k
R/kCggEBAIBWtqHNRYbeKPn96HB7O6TSbOH8eP4oLrhUpVb+BjwREG+AwJPniyY7
bOz7VlIDwUKHH8DhKzw8QLq+Xz7mTaFlmaV4DrV32UeM2buKrG9EIPGpx08C/okI
AZq+OvLqovMO1HyBedbSy6Tkni66wb27/NJJBzPDYsZVkgv3Klp5rSSHmCI2z0vS
wnBz+9T8b1XO9cVEKKoiHW3nGmtxb4gUJMn2LzJQcJrNZLji4qqVDA4OecKh+nRq
xjNHGtEs8NXdjDDLqK75zldB/aj2uaJkGdbow08K2AAmYB52A/v6e4fPfpYWJ0Hg
jbRmQvfbnH4ZSxPkISFXplaFY27gYYI=
-----END PRIVATE KEY-----


Enter certificates of certification authorities (CA) which form the certificate chain of the client
certificate. This
starts with the issuing CA certificate of the client certificate and can range up to the root CA
certificate.

Do you want to continue entering root and/or intermediate certificates {y|n}: n
```

```
You should keep a copy of the private key and the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:
CA: HyTrust KeyControl Certificate Authority
serial: D79D9487

The certificate's generated name for reference: entrust-keycontrol_D79D9487
```

3. Note the certificate's generated name above, e.g. **entrust-keycontrol_D79D9487**. It will be needed in section Setup Entrust KeyControl as the external KMIP server.

4.2. Setup Entrust KeyControl as the external KMIP server

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Enable the external KMIP server. The argument of **-client-cert** is the certificate's generated name from section Install the Entrust KeyControl client bundle into NetApp ONTAP. The argument of **-server-ca-certs** is the certificate's generated name from section Deploy NetApp Simulate ONTAP.

Notice the IP of both nodes in the Entrust KeyControl cluster.

```
mycluster::> security key-manager external enable -key-servers 10.194.148.215:5696,10.194.148.216:5696
-client-cert entrust-keycontrol_D79D9487 -server-ca-certs interop-CONTROLLER-CA-4
```

3. Verify the external key-management is configured.

```
mycluster::> security key-manager external show-status

Node  Vserver  Primary Key Server                                Status
----  -------  ------------------------------------------------  ------------
mycluster-01
      mycluster
               10.194.148.215:5696                               available
               10.194.148.216:5696                               available
2 entries were displayed.
```

Chapter 5. Test integration

This test procedure requires test scripts available from NetApp. The output files resulting from executing the test scripts need to be sent back to NetApp for verification.

1. Load the test scripts into NetApp ONTAP
2. Execute the kmip_before_reboot_test.sh test script
3. Execute the kmip_post_reboot_test.sh test script
4. Enable FIPS mode
5. Execute the before and post test scripts a second time
6. Verify FIPS mode is unchanged after reboot

5.1. Load the test scripts into NetApp ONTAP

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter system shell. Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

4. scp the test script files from a server of your choice into the Systemshell of the NetApp ONTAP node. Provide the password when prompted.

```
mycluster-01% scp root@10.194.148.52:/root/Downloads/kmip_before_reboot_test.sh kmip_before_reboot_test.sh
root@10.194.148.52's password:
kmip_before_reboot_test.sh                                                    100% 7346   731.0KB/s
00:00
```

```
SSH terminating : scp.c : main : 690,errs = 0.

mycluster-01% scp root@10.194.148.52:/root/Downloads/kmip_post_reboot_test.sh kmip_post_reboot_test.sh
root@10.194.148.52's password:
kmip_post_reboot_test.sh                                                    100% 6047     3.6MB/s
00:00
SSH terminating : scp.c : main : 690,errs = 0.
```

5. Verify the test scripts files are in the current directory.

```
mycluster-01% ls
kmip_before_reboot_test.sh      kmip_post_reboot_test.sh
```

5.2. Execute the kmip_before_reboot_test.sh test script

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter Systemshell. Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

4. Execute the `kmip_before_reboot_test.sh` test script and redirect the output to file `before_reboot_output_1.txt`. KeyControl presents itself as a single entity even though it may be composed of multiple nodes (two in this test case). Therefore, select **no** in the **Please enter whether this is a clustered key-server config (yes or no):** question below.

```
mycluster-01% bash kmip_before_reboot_test.sh > before_reboot_output_1.txt
Please enter key server name: KeyControl
Please enter key server version: 10.2
```

```
Please enter whether this is a clustered key-server config (yes or no): no
Sleeping for 10 seconds before checking if aggregate was created...
Sleeping for 10 seconds before checking if vserver was created...
```

5. Exit Systemshell.

```
mycluster-01% exit
```

6. Reboot the node. Wait 10 minutes before logging back into the cluster.

```
mycluster::*> reboot -node mycluster-01
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: y


Connection to xxx.xxx.xxx.xxx closed.
```

5.3. Execute the kmip_post_reboot_test.sh test script

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter Systemshell. Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

4. Execute the `kmip_post_reboot_test.sh` test script and redirect the output to file `post_reboot_output_1.txt`.

```
mycluster-01% bash kmip_post_reboot_test.sh > post_reboot_output_1.txt
Please enter key server name: KeyControl
Please enter key server version: 10.2
```

```
Please enter whether this is a clustered key-server config (yes or no): no
```

5. Exit Systemshell.

```
mycluster-01% exit
```

5.4. Enable FIPS mode

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enable FIPS mode.

```
mycluster::*> security config modify -interface SSL -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components
to fail.
         MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible. An
SNMP users
         or SNMP traphosts that are non-compliant to FIPS will be deleted automatically. An SNMPv1 user,
SNMPv2c user
         or SNMPv3 user (with none or MD5 as authentication protocol or none or DES as encryption protocol
or both) is
         non-compliant to FIPS. An SNMPv1 traphost or SNMPv3 traphost (configured with an SNMPv3 user non-
compliant to
         FIPS) is non-compliant to FIPS.
Do you want to continue? {y|n}: y
```

4. Reboot all nodes in the cluster. Wait 10 minutes before logging back into the cluster.

```
mycluster::*> reboot -node *
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: Y
1 entry was acted on.


Connection to 10.194.148.113 closed.
```

5. Log back into the NetApp ONTAP Cluster Management.

6. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

7. Verify FIPS mode is enabled.

```
mycluster::*> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- --------- ------------------------------------------------------------
true       TLSv1.3,  TLS_RSA_WITH_AES_128_CCM, TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CCM,

 ...

                     TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA,
                     TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA,
                     TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA,
                     TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384
```

5.5. Execute the before and post test scripts a second time

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter Systemshell. Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.
```

```
mycluster-01%
```

4. Execute the `kmip_before_reboot_test.sh` test script and redirect the output to file `before_reboot_output_2.txt`.

```
mycluster-01% bash kmip_before_reboot_test.sh > before_reboot_output_2.txt
Please enter key server name: KeyControl
Please enter key server version: 10.2
Please enter whether this is a clustered key-server config (yes or no): no
Sleeping for 10 seconds before checking if aggregate was created...
Sleeping for 10 seconds before checking if vserver was created...
```

5. Exit Systemshell.

```
mycluster-01% exit
```

6. Reboot the node. Wait 10 minutes before logging back into the cluster.

```
mycluster::*> reboot -node mycluster-01
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: y


Connection to xxx.xxx.xxx.xxx closed.
```

7. Log back into the NetApp ONTAP Cluster Management.
8. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

9. Enter Systemshell. Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

10. Execute the `kmip_post_reboot_test.sh` test script and redirect the output to file

p`ost_reboot_output_2.txt`.

```
mycluster-01% bash kmip_post_reboot_test.sh > post_reboot_output_2.txt
Please enter key server name: KeyControl
Please enter key server version: 10.2
Please enter whether this is a clustered key-server config (yes or no): no
```

11. scp the test script output files to a server of your choice. Provide the password when prompted.

```
mycluster-01% scp before_reboot_output_1.txt
root@xxx.xxx.xxx.xxx:/root/Downloads/before_reboot_output_1.txt
root@10.194.148.52's password:
before_reboot_output_1.txt                                                    100%   11KB 856.1KB/s
00:00
SSH terminating : scp.c : main : 690,errs = 0.

mycluster-01% scp before_reboot_output_2.txt
root@xxx.xxx.xxx.xxx:/root/Downloads/before_reboot_output_2.txt
root@10.194.148.52's password:
before_reboot_output_2.txt                                                    100%   11KB  10.8MB/s
00:00
SSH terminating : scp.c : main : 690,errs = 0.

mycluster-01% scp post_reboot_output_1.txt root@xxx.xxx.xxx.xxx:/root/Downloads/post_reboot_output_1.txt
root@10.194.148.52's password:
post_reboot_output_1.txt                                                      100%   10KB 585.4KB/s
00:00
SSH terminating : scp.c : main : 690,errs = 0.

mycluster-01% scp post_reboot_output_2.txt root@xxx.xxx.xxx.xxx:/root/Downloads/post_reboot_output_2.txt
root@10.194.148.52's password:
post_reboot_output_2.txt                                                      100%   10KB   9.6MB/s
00:00
SSH terminating : scp.c : main : 690,errs = 0.
```

12. Send these output files to NetApp for verification.

5.6. Verify FIPS mode is unchanged after reboot

1. Exit Systemshell.

```
mycluster-01% exit
```

2. Disable FIPS mode.

```
mycluster::*> security config modify -interface SSL -is-fips-enabled false
```

3. Reboot all nodes in the cluster.

```
mycluster::*> reboot -node *
```

```
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: Y
1 entry was acted on.


Connection to 10.194.148.113 closed.
```

4. Log back into the NetApp ONTAP Cluster Management.
5. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

6. Verify FIPS mode is disabled on the cluster.

```
mycluster::*> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- --------- ------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM, TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CCM,

 ...

                     TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA,
                     TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA,
                     TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384,
                     TLS_CHACHA20_POLY1305_SHA256
```

Chapter 6. Integrating with an HSM

For guidance on integrating the Entrust KeyControl with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the Entrust KeyControl nShield HSM Integration Guide available at Entrust documentation library.

Chapter 7. Appendix A - Install a signed certificate from your local root CA in the Entrust KeyControl cluster

Any CA can be use for this integration. For the purpose of this integration, a Microsoft Windows CA configured as a local root CA was utilized.

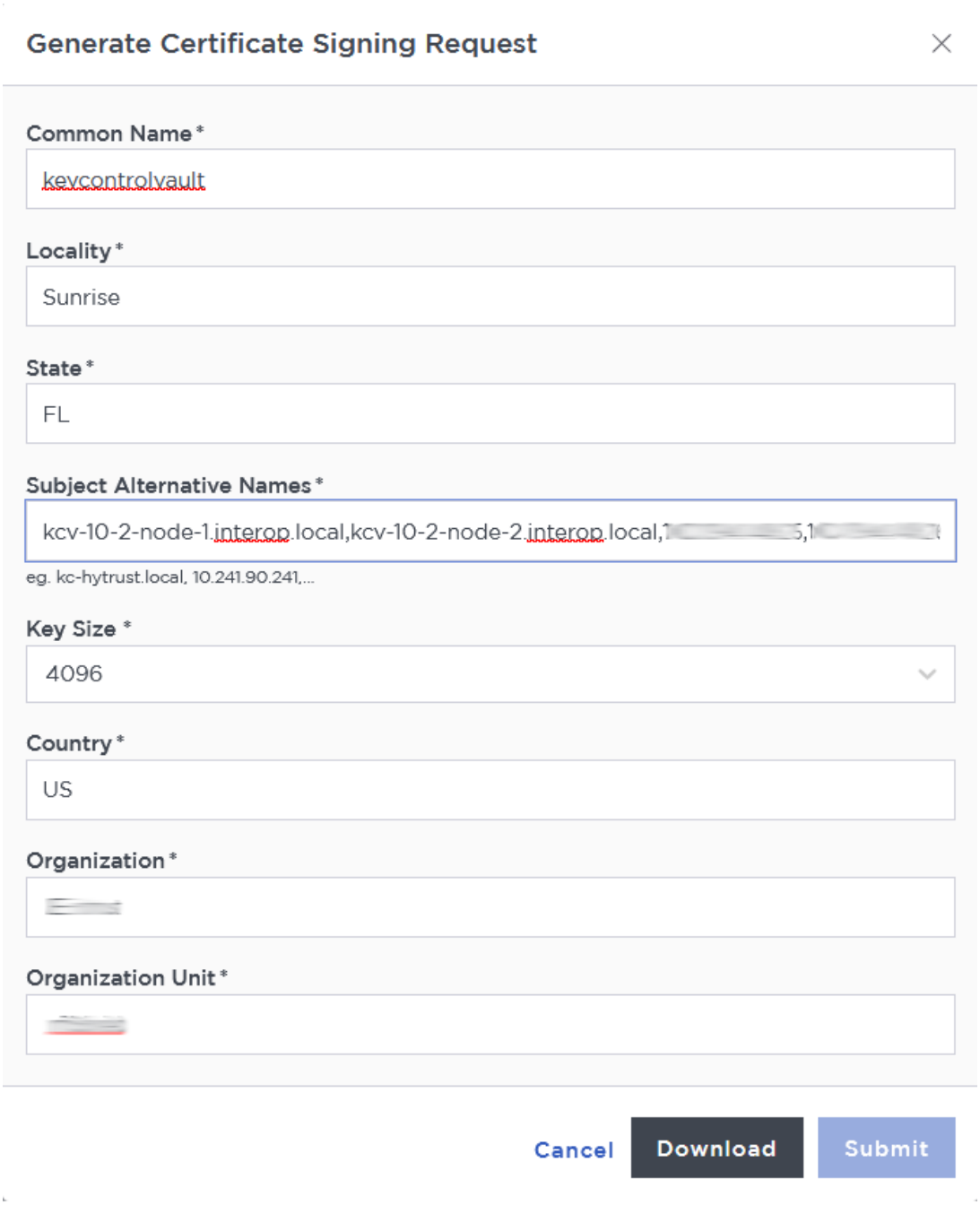
1. Create a CSR
2. Sign the certificate
3. Install certificate

7.1. Create a CSR

1. Log into the Entrust KeyControl server web GUI.
2. In the **Vault Management** dashboard, select the **Settings** icon on the top right.
3. Select the **Action** icon pull-down menu. Then select **Generate CSR**.
4. Enter your information.

Include the FQDN and / or IP of all the Entrust KeyControl nodes in the **Subject Alternative Names**.

For example:

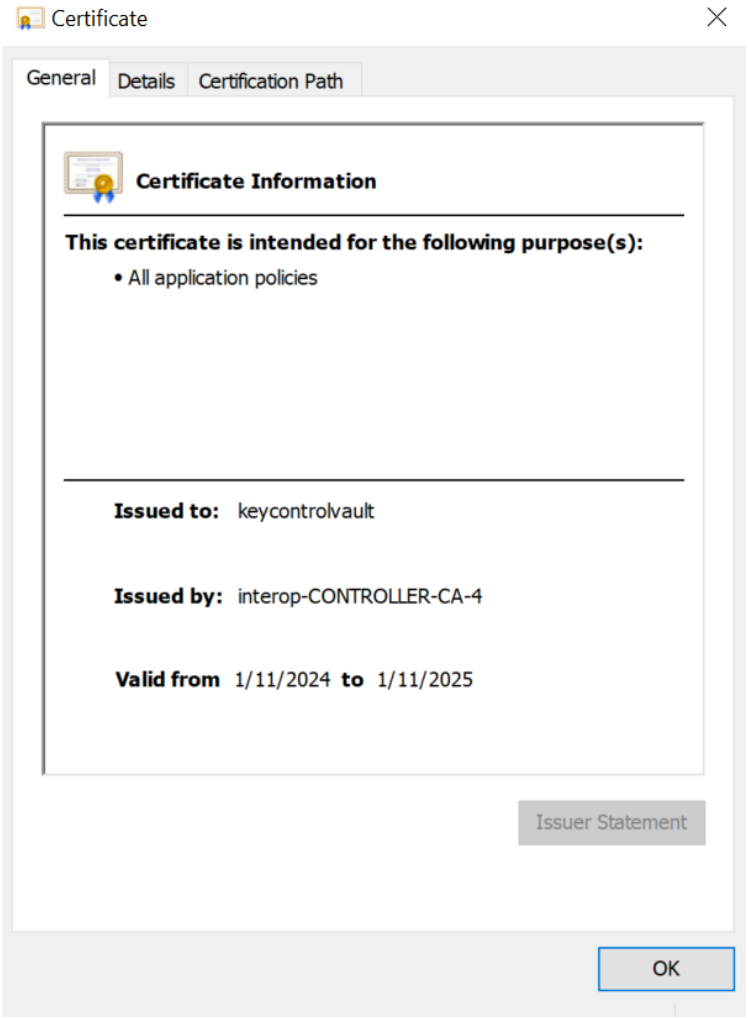


7.2. Sign the certificate

1. Log into your local root CA with Administrator privileges.
2. Copy the CSR created above to a local folder.
3. Launch the **certsvr** application.
4. Right-click on the **<certification authority name>** in the left pane and select **All Tasks** / **Submit new request...**.
5. Select the copied CSR.

6. Select **<certification authority name>** / **Pending Request** in the left pane.
7. Right-click on the request in the right pane and select **All Tasks** / **Issue**.
8. Select **<certification authority name>** / **Issued Certificates** in the left pane.
9. Select the certificate.

   For example:



10. Select the **Details** tab / **Copy to File...**. Follow the instructions, selecting **Base-64 encoded X.509** in **Export File Format**. Example name `keycontrolvault`.
11. Export the local root CA certificate in pem format.

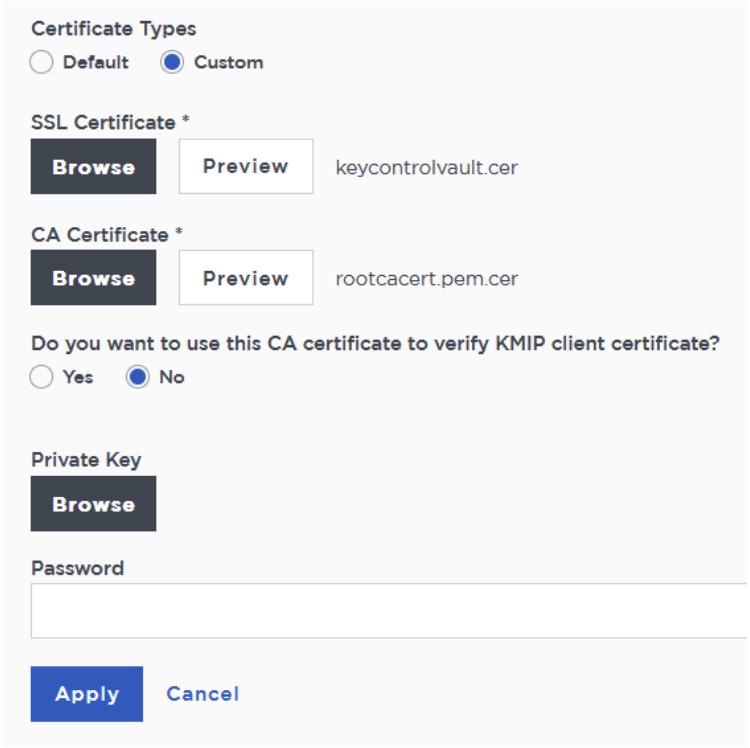
```
C:\Users\Administrator>certutil -ca.cert C:\Users\Administrator\Downloads\rootcacert.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDlzCCAn+gAwIBAgIQPaxaYmRa1atOVpZms+TaZjANBgkqhkiG9w0BAQsFADBS
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdpbnRlcm9w
MSAwHgYDVQQDExdpbnRlcm9wLUNPTlRST0xMRVItQ0EtNDAeFw0yNDAxMTEyMTEx
MzZaFw0zNDAxMTEyMTIxMzZaMFIxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEXMBUG
CgmSJomT8ixkARkWB2ludGVyb3AxIDAeBgNVBAMTF2ludGVyb3AtQ09OVFJPTExF
Ui1DQS00MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2rthVuA/D9c3
```

```
pRcg1OKXayMBSTEurG0H6icp09re683suJoGDxBBV1Qp0+I6v2PwkkDD46lYlhCn
ycr/+UenUS0As30NM9FbWejVdYBH2JHhHZDi2A9HyprWVFb+tLktX1VXbwTXP3QO
+WPIEBtXRXTyP0ivkuMVRuyEd+qwTzvldjUGd0j5pRMb2cmI/sFRKN9CjDBNxDDX
z/wKB+Kaf9n6oh7RrWXIh5+v/N3gI4EG8z2fL0l0TmPzWdTafg9edvSnOviKVrmT
qzGmxlT6DQt8xGRecDiJMH3+9R3XvRLhflcpANdqMAZnNipDCx4re4+DBH7S8mSh
Vr1nK2xybQIDAQABo2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUYzwTn023Ko23BcNb3u5i
zpQLc5QwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQELBQADggEBACmiaN0t
tBkyzkxpWy5xA+ePDyCBFLuQ6W1BByI6TCPOLp6CFsmYg9NB4c61+Y5lpIQhDJFf
AODT1LZRTq6b5h8vl1GdNzim2wPrtjviNvmQ0Q5R/2tJzR9D3SB6Hv+bU5lRP7j/
giWpEx5ImmmfG7BJ4DxWxpA2sooC02iP2TOw5GJcI+varjKNCsyYSiyYhigOpnh/
3ZlpMv2IGB/YykLfCPL2SOtYq0LcAnniiXmxx9iylgZwi3xQPx35JLn8b2Mrg0qI
iMaAoCzJXU09aZcMv+ZCQ27PaowRmxx+WSdYt8ZORP+cHC+xemLyamnyxzXp07qE
MsNUdQy+Lo5h5XI=
-----END CERTIFICATE-----

CertUtil: -ca.cert command completed successfully.

C:\Users\Administrator>certutil -encode C:\Users\Administrator\Downloads\rootcacert.cer
C:\Users\Administrator\Downloads\rootcacert.pem.cer
Input Length = 923
Output Length = 1328
CertUtil: -encode command completed successfully.
```

12. Copy the `keycontrolvault` certificate and the `rootcacert.pem.cer` to a location accessible by the Entrust KeyControl server.

7.3. Install certificate

1. Log into the Entrust KeyControl server web GUI.
2. In the **Vault Management** dashboard, select the **Settings** icon on the top right.
3. Select **Custom** radio button in **Certificate Types**.
4. Browse and select the certificate as shown.



5. The other defaults settings are appropriate for most applications. Make any changes necessary.
6. Select **Apply**.

Chapter 8. Additional resources and related products

8.1. nShield Connect

8.2. nShield as a Service

8.3. KeyControl

8.4. Entrust products

8.5. nShield product documentation