Entrust KeyControl

nShield® HSM Integration Guide

14 Jan 2022

Contents

1. Introduction

This guide describes the procedure to integrate Entrust KeyControl and Entrust nShield HSM for establishing a hardware root of trust for all encryption keys. It also describes how the KeyControl Admin Key is protected in the HSM.

The combined solution facilitates regulatory compliance with a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust.

1.1. Product configuration

Product	Version
KeyControl	5.5 Multi Tenant
nShield HSM hardware	Connect XC
nShield firmware	12.50.11 - Image 12.80.4

2. Installing the Entrust KeyControl Server

The Entrust KeyControl server is a software solution deployed from an OVA or ISO image. Entrust recommends that you read the Entrust KeyControl Installation Overview to fully understand the KeyControl server deployment.

To configure a KeyControl cluster (active-active configuration is recommended), Entrust recommends the use of the OVA installation method, as described in the Entrust KeyControl OVA Installation instructions.

The KeyControl OVA must be deployed from the VCenter server. Do *not* deploy from an ESXi host.

After the KeyControl server is deployed, configure the first KeyControl node as described in the Entrust Configuring the First KeyControl Node installation guide.

After completing this procedure, add the second node as described in the Entrust Adding a New KeyControl Node to an Existing Cluster (OVA Installation) to create the recommended active-active cluster.

> ℹ Although an active-active cluster is not a requirement, and a single KeyControl node can be deployed to perform the functions of KMIP, Entrust strongly recommends deploying the solution with a minimum of four nodes in an active-active cluster solution.

Your KeyControl license determines how many KeyControl nodes you can have in a cluster. For full information about the KeyControl licensing, see the Entrust Managing the KeyControl License admin page.

2.1. Configure the KeyControl Server

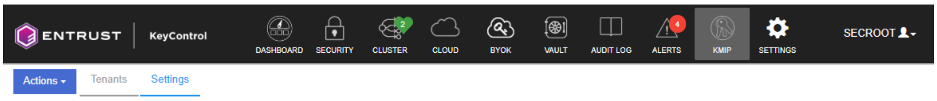
After the Entrust KeyControl server is deployed and the initial installation is complete, you can configure the network settings, e-mail server preferences, and certificate configuration. For these procedures, see the KeyControl System Configuration admin guide.

2.2. Configure the KeyControl Server as a KMIP server

To use external key management, applications require an external key management server such as the Entrust KeyControl server. The KeyControl server is the KMIP server and the application is the KMIP client.

To configure the KeyControl server as a KMIP server, see the Configuring a KeyControl KMIP Server section of the admin guide.

1. Log into the KeyControl web user interface using an account with Security Admin privileges.
2. In the top menu bar, select the **KMIP** icon and then select the **Settings** tab.



3. In the **Settings** tab:
   a. For **State**, select **ENABLED**.
   b. For **Host Name**, enter the hostname or IP address.
   c. For **Port**, enter the port number. The default is 5696.
   d. For **Auto-Reconnect**, select **OFF**.
   e. For **Verify**, select **Yes**.
   f. For **Certificate Type**, select **Default**.
   g. For **Non-Blocking I/O**, select **No**.
   h. For **Timeout**, select **Infinite**.
   i. For **Log Level**, select **CREATE-MODIFY**.
   j. For **Restrict TLS**, select **DISABLED**.
   k. For **SSL/TLS Ciphers**, accept the defaults.
4. Select **Apply**.

2.3. Set up an Active Directory Server

With KeyControl 5.5 Multi Tenancy, you must have an Active Directory Server. This will be used when creating the tenants in KeyControl. To create a tenant, you must have access to the Active Directory server and the user information that will be used to manage the tenant instance.

> KeyControl requires that the user record in the AD server has a **userPrincipalName** property. This field should use the following format: `uid@domain`, for example: `kcuser1@keycontrolad.com`.

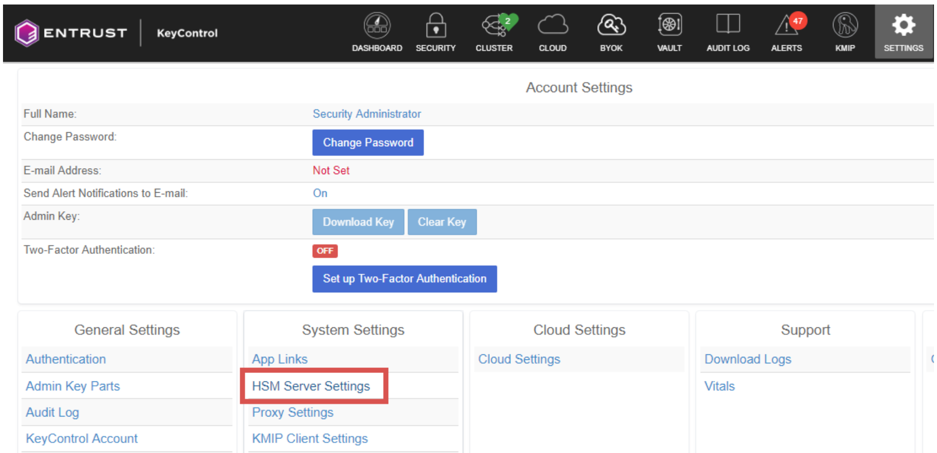
3. Procedures

3.1. Prerequisites

- Entrust KeyControl has been deployed and configured.
- The nShield HSM has been deployed and configured.
- An Active Directory server has been deployed and configured.
- You have rights to add new clients to the HSM configuration.

3.2. Initialize the HSM on KeyControl

1. Log into the KeyControl web user interface using an account with Security Admin privileges.
2. In the top menu bar, select **Settings**, and then select **System Settings** > **HSM Server Settings**.

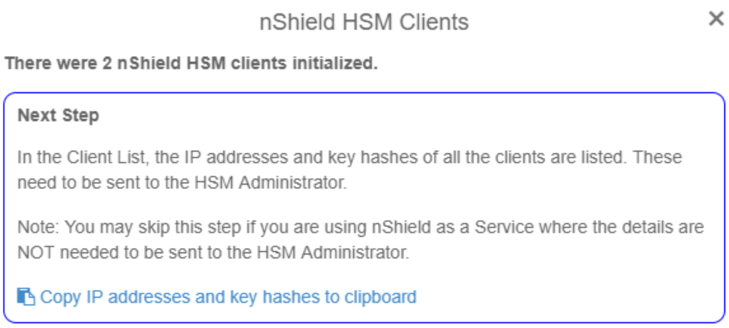


Account Settings

Full Name:	Security Administrator
Change Password:	Change Password
E-mail Address:	Not Set
Send Alert Notifications to E-mail:	On
Admin Key:	Download Key Clear Key
Two-Factor Authentication:	OFF Set up Two-Factor Authentication

General Settings	System Settings	Cloud Settings	Support
Authentication	App Links	Cloud Settings	Download Logs
Admin Key Parts	HSM Server Settings		Vitals
Audit Log	Proxy Settings		
KeyControl Account	KMIP Client Settings		

3. Select **Actions** > **HSM Type** > **Entrust nShield HSM**.
4. In **nShield HSM Clients**, select **Copy IP address and key hashes to clipboard**.


nShield HSM Clients ×

There were 2 nShield HSM clients initialized.

Next Step

In the Client List, the IP addresses and key hashes of all the clients are listed. These need to be sent to the HSM Administrator.

Note: You may skip this step if you are using nShield as a Service where the details are NOT needed to be sent to the HSM Administrator.

Copy IP addresses and key hashes to clipboard

5. Paste the contents of the clipboard into a file.

   Your HSM administrator will need the IP address and hash pairs to add the

KeyControl nodes as an HSM clients.

The following is an example data file for a 2-node KeyControl cluster:

```
172.16.124.100 32a28a759b2055cf3d2956eb295da931c205ae9c
172.16.124.101 56eb295da931c205ae9c32a28a759b2055cf3d29
```

3.3. Add one or more KeyControl nodes to the HSM

Send the IP address and hash pair for each KeyControl node in the cluster to the HSM administrator.

The HSM administrator adds each KeyControl node as a client to the HSM and sends back the following information:

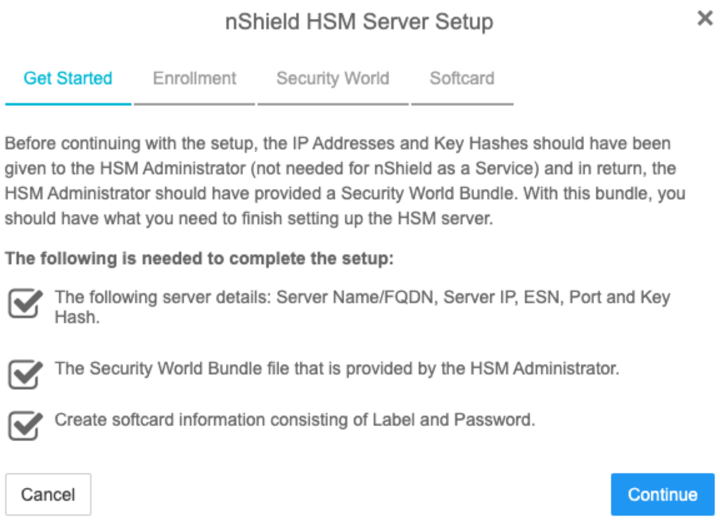
- A zipped file that contains the nShield Security World and HSM module files.
- The FQDN of the HSM.
- The IP address of the HSM.
- The Electronic Serial Number (ESN) and the key hash of the HSM. This can be obtained by running the following command on the nShield RFS server:

```
[anonkneti <hsm-ip-address>]
```

- The network port number that the HSM uses.

3.4. Set up the nShield HSM Server

1. In the **Get Started** step of the **nShield HSM Server Setup** dialog, select **Continue**.



Before continuing with the setup, the IP Addresses and Key Hashes should have been given to the HSM Administrator (not needed for nShield as a Service) and in return, the HSM Administrator should have provided a Security World Bundle. With this bundle, you should have what you need to finish setting up the HSM server.

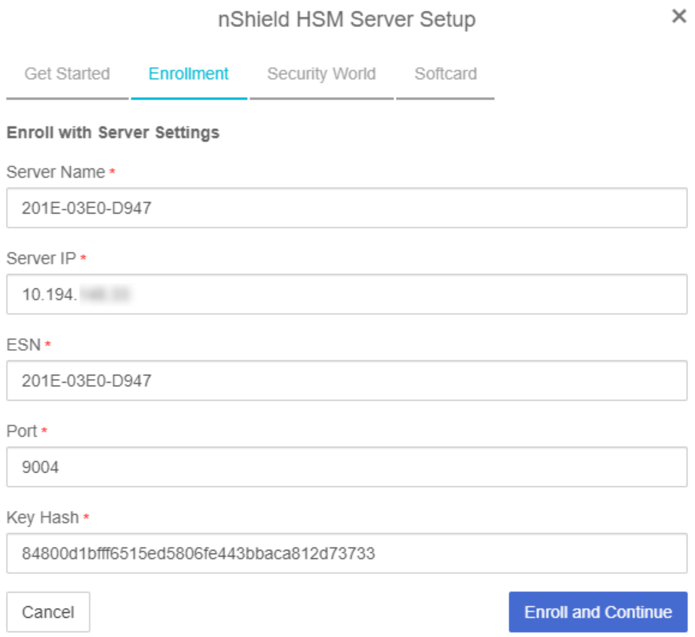
The following is needed to complete the setup:

☑ The following server details: Server Name/FQDN, Server IP, ESN, Port and Key Hash.

☑ The Security World Bundle file that is provided by the HSM Administrator.

☑ Create softcard information consisting of Label and Password.

2. In the **Enrollment** step of the dialog:
    a. For **Server Name**, enter the server FQDN of the HSM.
    b. For **Server IP**, enter the IP address of the HSM.
    c. For **ESN**, enter the ESN of the HSM.
    d. For **Port**, enter the required port. The default is 9004.
    e. For **Key Hash**, enter the key hash of the HSM.
    f. Select **Enroll and Continue**.



Enroll with Server Settings

Server Name *: 201E-03E0-D947

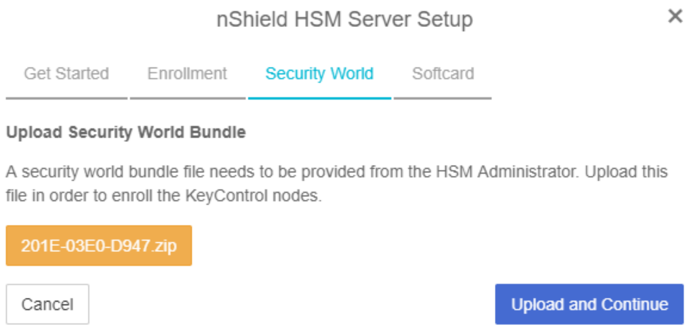
Server IP *: 10.194.[redacted]

ESN *: 201E-03E0-D947

Port *: 9004

Key Hash *: 84800d1bfff6515ed5806fe443bbaca812d73733

3. In the **Security World** step of the dialog:
    a. Select **Load File**.
    b. Browse to the zipped file that you received from the HSM administrator in Add one or more KeyControl nodes to the HSM.
    c. Select **Upload and Continue**.

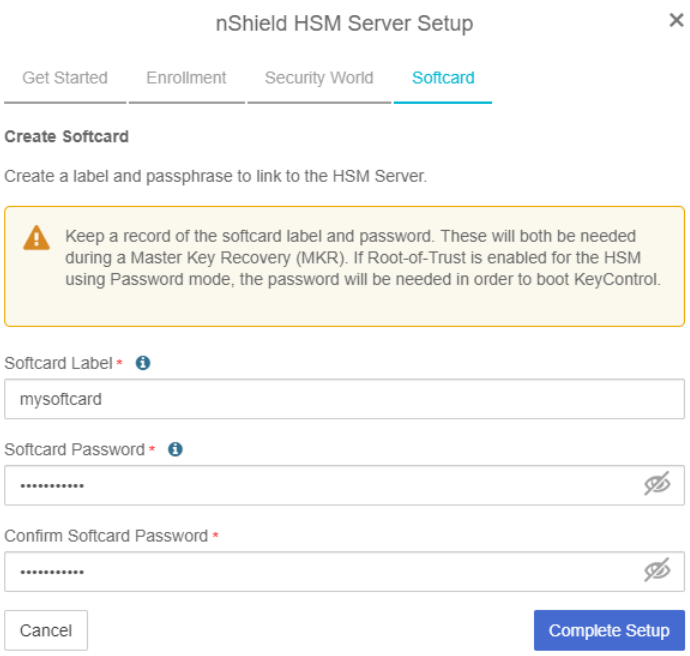


Upload Security World Bundle

A security world bundle file needs to be provided from the HSM Administrator. Upload this file in order to enroll the KeyControl nodes.

4. In the **Softcard** step of the dialog:
    a. For **Softcard Label**, enter a unique name. This value is user-defined.
    b. For **Softcard Password**, enter a password. This value is user-defined.

c. For **Confirm Softcard Password**, re-enter the password. For example:



Create Softcard

Create a label and passphrase to link to the HSM Server.

Keep a record of the softcard label and password. These will both be needed during a Master Key Recovery (MKR). If Root-of-Trust is enabled for the HSM using Password mode, the password will be needed in order to boot KeyControl.

Softcard Label * : mysoftcard

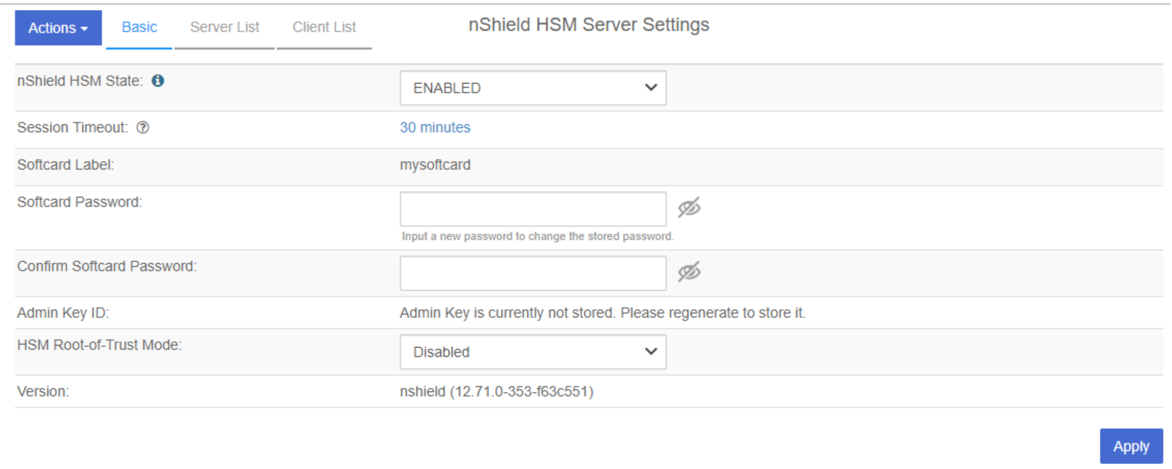
Softcard Password * : •••••••••••

Confirm Softcard Password * : •••••••••••

d. Keep a record of the Softcard label and password. These will be needed during a Master Key Recovery (MKR). If Root-of-Trust is enabled for the HSM using Password mode, the password is also needed to boot KeyControl.

e. Select **Complete Setup**.

The nShield Connect HSM is now configured to work with Entrust KeyControl. For example:



nShield HSM State:	ENABLED
Session Timeout:	30 minutes
Softcard Label:	mysoftcard
Softcard Password:	Input a new password to change the stored password.
Confirm Softcard Password:	
Admin Key ID:	Admin Key is currently not stored. Please regenerate to store it.
HSM Root-of-Trust Mode:	Disabled
Version:	nshield (12.71.0-353-f63c551)

3.5. Create a KMIP tenant

With KeyControl 5.5 Multi Tenancy, you must create a tenant before setting up any KMIP services. Before creating the tenant, you will need information about the Active Directory server and the AD user that will be used for setting up the tenant.

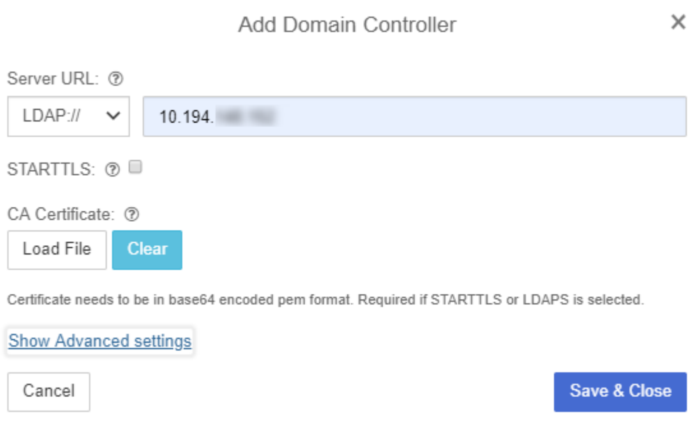
1. Log into the KeyControl web user interface using an account with Security Admin privileges.
2. In the top menu bar, select **KMIP**, and then select the **Tenants** tab.
3. Select **Actions** > **Create a KMIP tenant**.

   The **Create a KMIP Tenant** dialog appears.

4. In the **About** tab, enter the **Name** of the tenant and a **Description**.

   > The tenant name cannot be changed after the tenant is created.

5. Select **Next**.
6. In the **Admin** tab, for **Active Directory**, select **Other Active Directory**.
7. In the **Active Directory Domain**, select the **+** icon to add the AD server:
   a. In the **KMIP Active Directory Domain** dialog, enter the **Domain Name**.
   b. For **Domain Controllers**, select the **+** icon.
   c. In the **Add Domain Controller** dialog, for **Server URL**, select the required protocol (for example, **LDAP**), and then enter the IP/FQDN of the AD server.
   d. Accept the defaults for remaining properties. For example:



Add Domain Controller

Server URL: LDAP:// 10.194.[redacted]

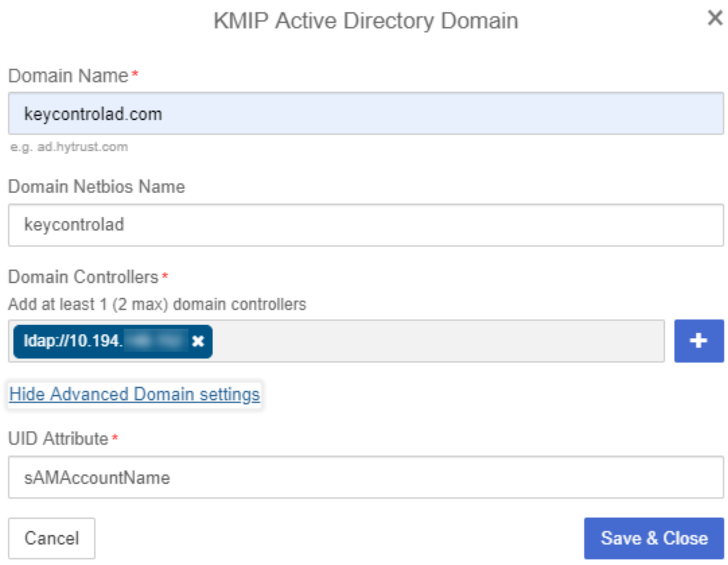
STARTTLS: □

CA Certificate:

Certificate needs to be in base64 encoded pem format. Required if STARTTLS or LDAPS is selected.

   e. Select **Save and Close**.
8. Select **Show Advanced Domain settings**.

   The **KMIP Active Directory Domain** dialog appears. This shows the **UID attribute** will be used. The default is **sAMAccountName**. For example:



Domain Name*

keycontrolad.com

e.g. ad.hytrust.com

Domain Netbios Name

keycontrolad

Domain Controllers*

Add at least 1 (2 max) domain controllers

ldap://10.194.[redacted] ✖

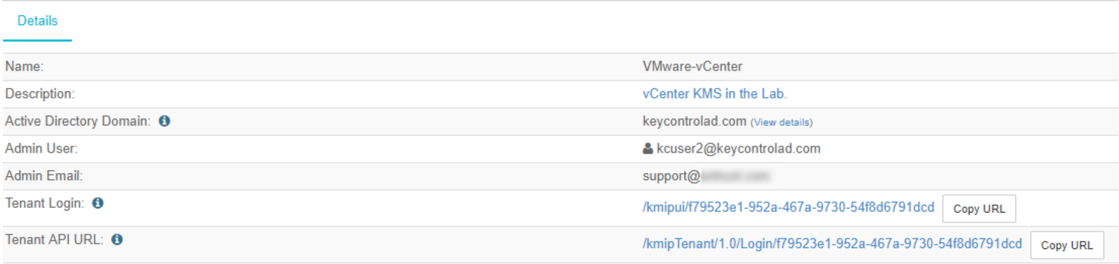
UID Attribute*

sAMAccountName

9. Select **Save and Close**.
10. Enter the AD User id in the **Name (UPN)** field and the **Email address** that should be used for communications with the tenant.

> The **Name (UPN)** field requires that the user record in the AD server has a **userPrincipalName** property. This field should use the following format: `uid@domain`, for example: `kcuser1@keycontrolad.com`.

11. Select **Create**. This will create the tenant in KeyControl. Once it is created, it will be listed under the **Tenants** tab.
12. Select the newly created tenant. When you select it the information about the tenant is displayed. For example:



Name:	VMware-vCenter
Description:	vCenter KMS in the Lab.
Active Directory Domain: ℹ	keycontrolad.com (View details)
Admin User:	kcuser2@keycontrolad.com
Admin Email:	support@[redacted]
Tenant Login: ℹ	/kmipui/f79523e1-952a-467a-9730-54f8d6791dcd Copy URL
Tenant API URL: ℹ	/kmipTenant/1.0/Login/f79523e1-952a-467a-9730-54f8d6791dcd Copy URL

13. Test the tenant by selecting the **Tenant Login** URL, and attempt to log in with the user you provided during the tenant configuration. If successful, the tenant is ready to create the certificate bundle for the client application.

> The **Tenant Login** URL is used later, to Enable KMIP key wrapping and Establish trust between the KeyControl Server and the Client Application.

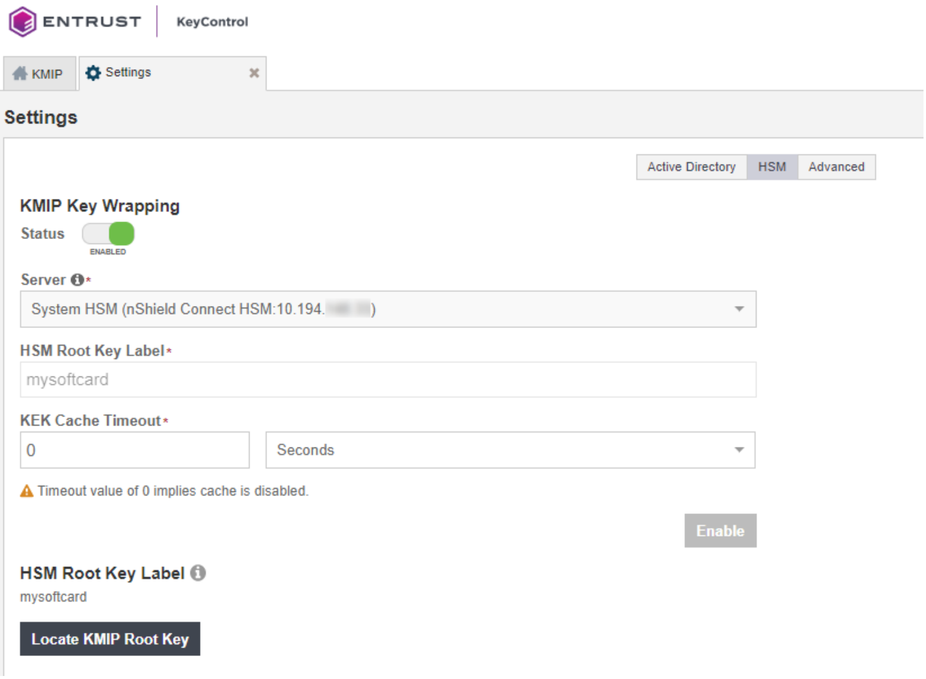
3.6. Enable KMIP key wrapping

With Multi Tenancy, KMIP key wrapping is set at the tenant level. Each tenant will be configured according to its requirements.

1. Log into the KeyControl web user interface using the **Tenant Login** URL.

> The **Tenant Login** URL was displayed at the end of the Create a KMIP tenant procedure, and is different from the standard KeyControl web user interface URL.

2. In the top menu bar, select the **Settings** icon.
3. Select the **Settings** tab, and then the **HSM** tab. For example:



Settings

KMIP Key Wrapping

Status: ENABLED

Server*: System HSM (nShield Connect HSM:10.194.[redacted])

HSM Root Key Label*: mysoftcard

KEK Cache Timeout*: 0 Seconds

Timeout value of 0 implies cache is disabled.

HSM Root Key Label

mysoftcard

4. For **KMIP Key Wrapping**, enable the **Status**.
5. For **Server**, select **System HSM (nShield Connect HSM)**.
6. In the **HSM Root Key Label** field, enter a unique name for the **HSM Root Key**.
7. For **KEK Cache Timeout**, enter how long you want KeyControl to cache the HSM-derived Key Encryption Keys (KEKs). The maximum length is 24 hours.
8. Select **Enable**.

Once you apply the changes, a re-key of the KMIP objects takes place. You can check the audit logs for this action record.

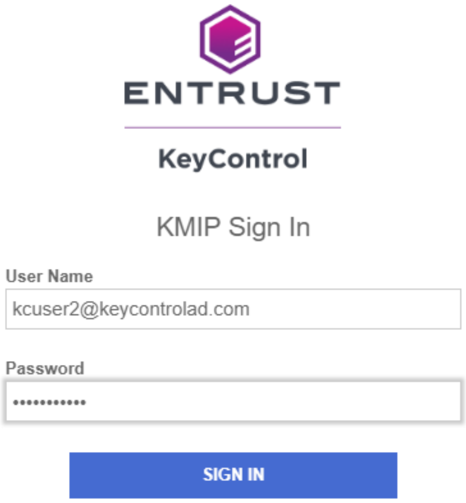
3.7. Establish trust between the KeyControl Server and the Client Application

Certificates are required to facilitate all KMIP communications between the KeyControl Server and the Client Application.

1. Log into the KeyControl web user interface using the **Tenant Login** URL.

   > The **Tenant Login** URL was displayed at the end of the Create a KMIP tenant procedure, and is different from the standard KeyControl web user interface URL.

   For example:



ENTRUST

KeyControl

KMIP Sign In

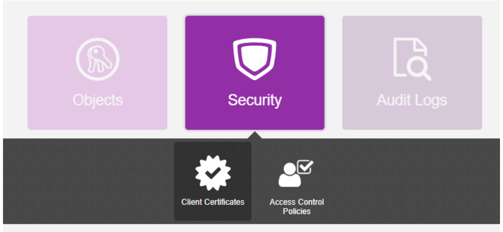
User Name

kcuser2@keycontrolad.com

Password

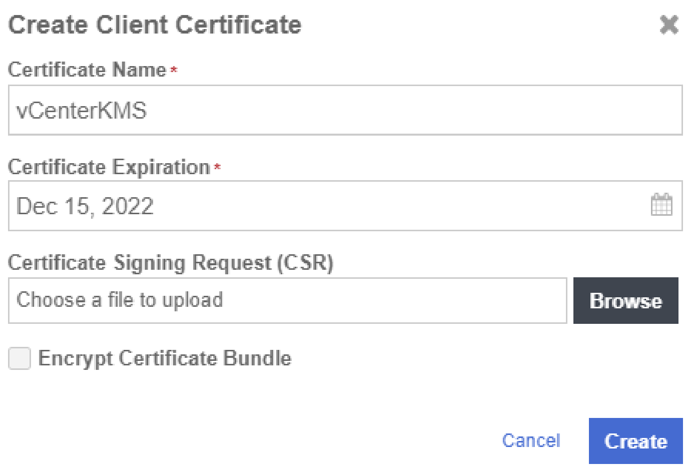
•••••••••••

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



   The **Manage Client Certificate** tab appears.

3. Select the **+** icon on the right to create a new certificate.
4. In the **Create Client Certificate** dialog:
   a. For **Certificate Name**, enter a name.
   b. For **Certificate Expiration**, set the date on which you want the certificate to expire.
   c. Accept the defaults for remaining properties. For example:



Create Client Certificate

Certificate Name*: vCenterKMS

Certificate Expiration*: Dec 15, 2022

Certificate Signing Request (CSR): Choose a file to upload

□ Encrypt Certificate Bundle

d. Select **Create**.

5. Select the new certificate once it is created, and select **Download**.

   A zip file downloads, which contains:

   - A `<cert_name>.pem` file that includes both the client certificate and private key.

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

     The private key section of the `<cert_name>.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`.

   These files will be used at the Client Application to establish trust between KeyControl and the Client Application.

For more information on how to create a certificate bundle, refer to Establishing a Trusted Connection with a KeyControl-Generated CSR.