Entrust KeyControl

nShield® HSM Integration Guide

16 Dec 2022

Contents

1. Introduction

This guide describes:

- The procedure to install and configure KeyControl as a KMIP server.
- The optional procedure to integrate Entrust KeyControl and Entrust nShield HSM for establishing a hardware root of trust for all encryption keys. This also describes how the KeyControl Admin Key is protected in the HSM.

If both procedures are performed, 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	10.0
nShield HSM hardware	Connect XC
nShield firmware	12.50.11 (FIPS certified), Image 12.80.4
nShield firmware	12.72.1 (FIPS certified), Image 12.80.5

2. Install and configure the Entrust KeyControl server

2.1. Install the 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 online documentation 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 online documentation.

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 (OVA Install) online documentation.

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

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 online documentation.

2.2. 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.

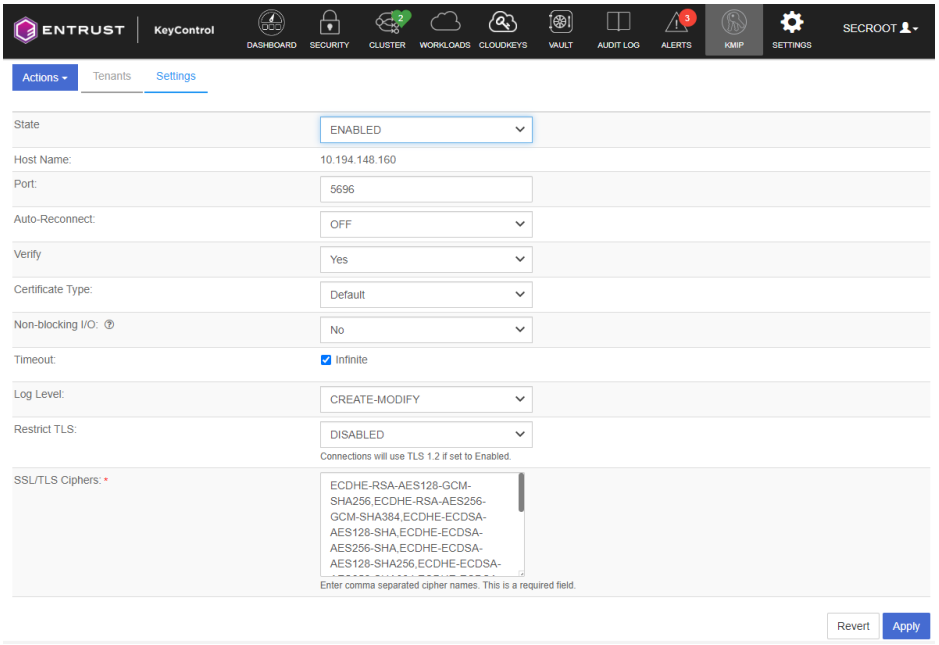
2.3. Configure the KeyControl Server as a KMIP server

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 Entrust Configuring a KeyControl KMIP Server section of the admin guide online documentation.

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 **Port**, accept the default **5696**.
    c. For **Auto-Reconnect**, select **OFF**.
    d. For **Verify**, select **Yes**.
    e. For **Certificate Type**, select **Default**.
    f. For **Non-Blocking I/O**, select **No**.
    g. For **Timeout**, select **Infinite**.
    h. For **Log Level**, select **CREATE-MODIFY**.
    i. For **Restrict TLS**, select **DISABLED**.
    j. For **SSL/TLS Ciphers**, accept the defaults.
4. Select **Apply**.

2.4. Create a KMIP tenant

For multi tenancy, you must create a tenant before setting up any KMIP services.

To create a KMIP 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**.

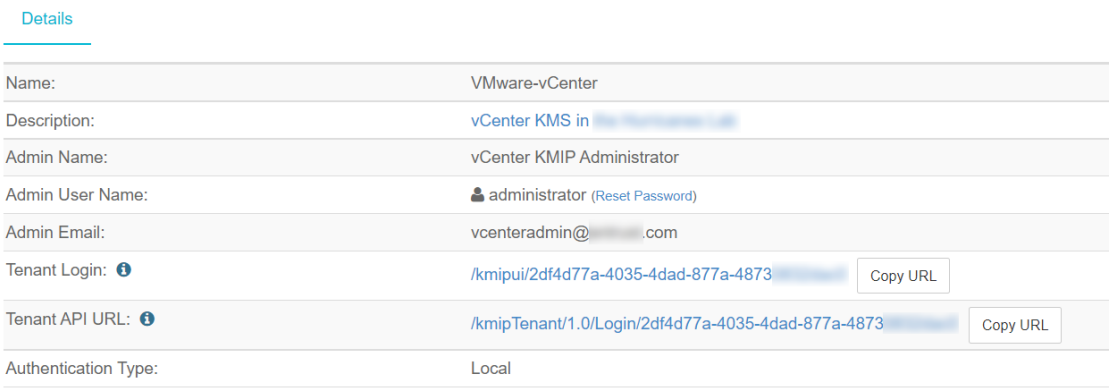
   

   The tenant name cannot be changed after the tenant is created.

5. Select **Next**.
6. In the **Authentication** tab, for **Authentication Type**, select **Local User Authentication**.

   If you want to use **Managed Authentication**, this will require an Active Directory server. For the purpose of this guide, **Local User Authentication** is used. Refer to the KeyControl Online documentation for more information on how to use **Managed Authentication**. Refer to the Entrust KMIP Tenant Authentication online documentation.

7. Select **Next**.
8. In the **Admin** tab, enter the Administrator information:
   a. For **User Name**, enter the Administrator user name.
   b. For **Full Name**, enter the Administrator full name.
   c. For **Email**, enter the Administrator email.
   d. For **Password**, set the Administrator password.
   e. For **Password Expiration**, set the date when you want the password to expire.
9. Select **Create**. This will create the tenant in KeyControl. Once it is created, it will be listed under the **Tenants** tab.
10. Select the newly created tenant. Information about the tenant is displayed. For example:



11. Test the tenant by selecting the **Tenant Login** URL, and attempt to log in as 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 to Establish trust between the KeyControl Server and the Client Application.

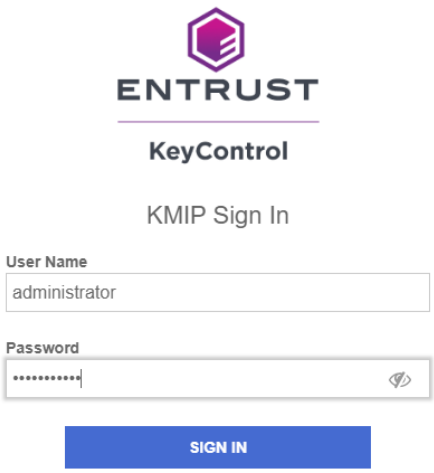
2.5. Establish trust between the KeyControl Server and the Client Application

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.

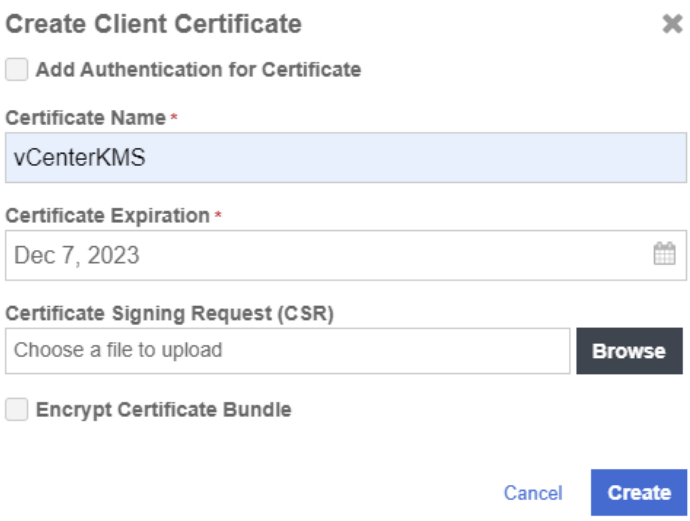
For example:



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:



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 the Entrust Establishing a Trusted Connection with a KeyControl-Generated CSR online documentation.

3. Integrate Entrust Key Control server and Entrust nShield HSM

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

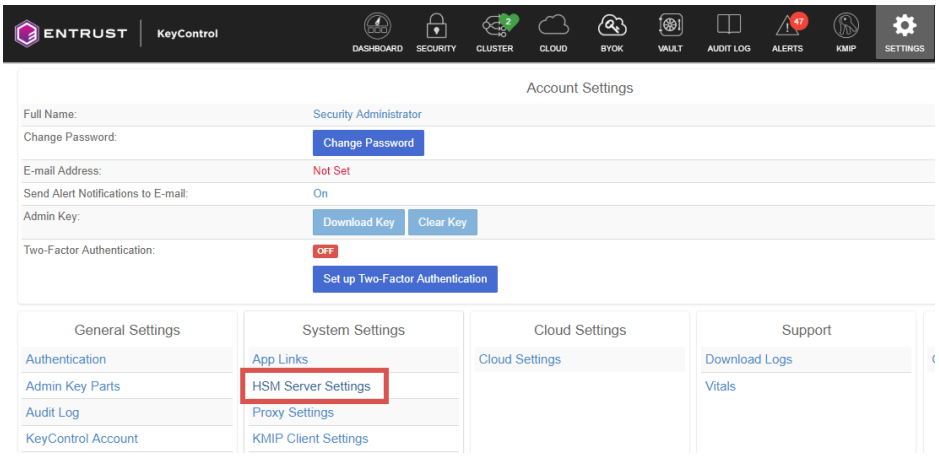
The combined solution facilitates regulatory compliance with a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust.

3.1. Prerequisites

- Entrust KeyControl has been deployed and configured. For details, see [Installation].
- The Entrust nShield HSM has been deployed and configured. For details, see the *Installation Guide* for your HSM.
- 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**.



3. Select **Actions** > **HSM Type** > **Entrust nShield HSM**.
4. In the **nShield HSM Clients** dialog, select **Copy IP address 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
```

6. Save the file.

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:

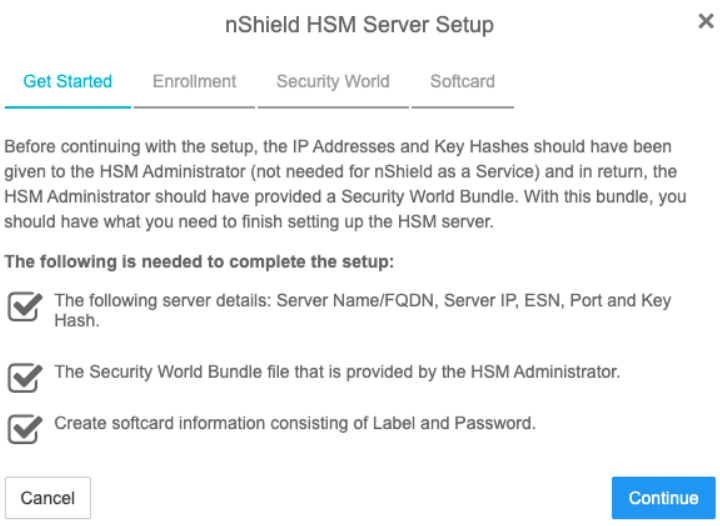
- A zipped file that contains the nShield Security World and HSM module files.
- The FQDN of the HSM.
- The IP address of the HSM.
- The Electronic Serial Number (ESN) and the key hash of the HSM. This can be obtained by running the following command on the nShield RFS server:

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

- The network port number that the HSM uses.

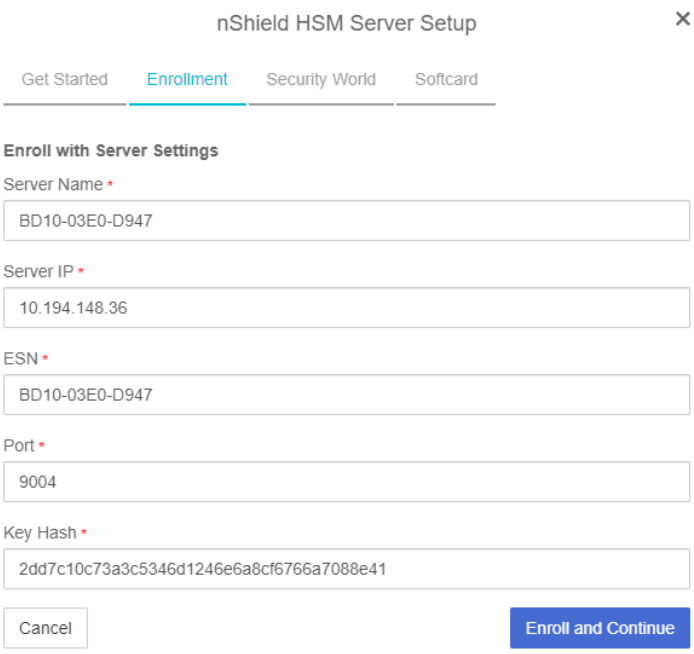
3.4. Set up the nShield HSM Server

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

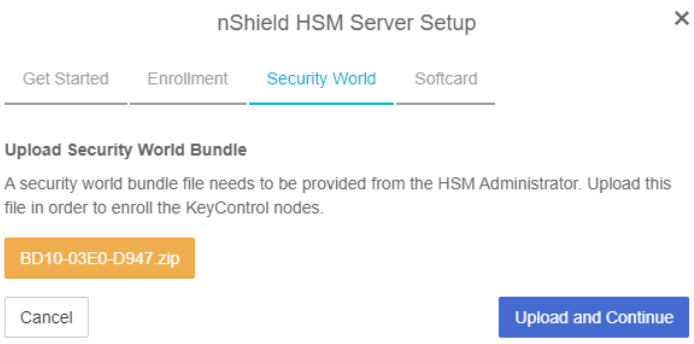


2. In the **Enrollment** step of the dialog:

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**.

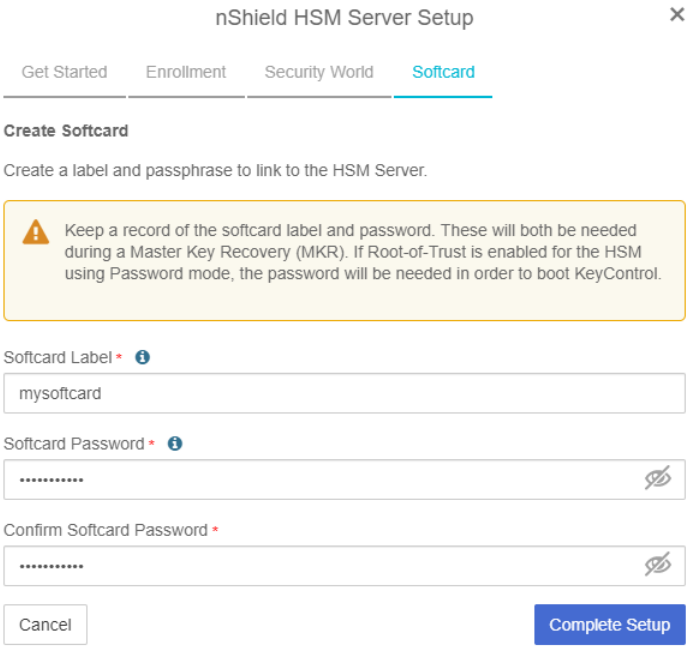


3. In the **Security World** step of the dialog:
   a. Select **Load File**.
   b. Browse to the zipped file that you received from the HSM administrator in Add one or more KeyControl nodes to the HSM.
   c. Select **Upload and Continue**.



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.

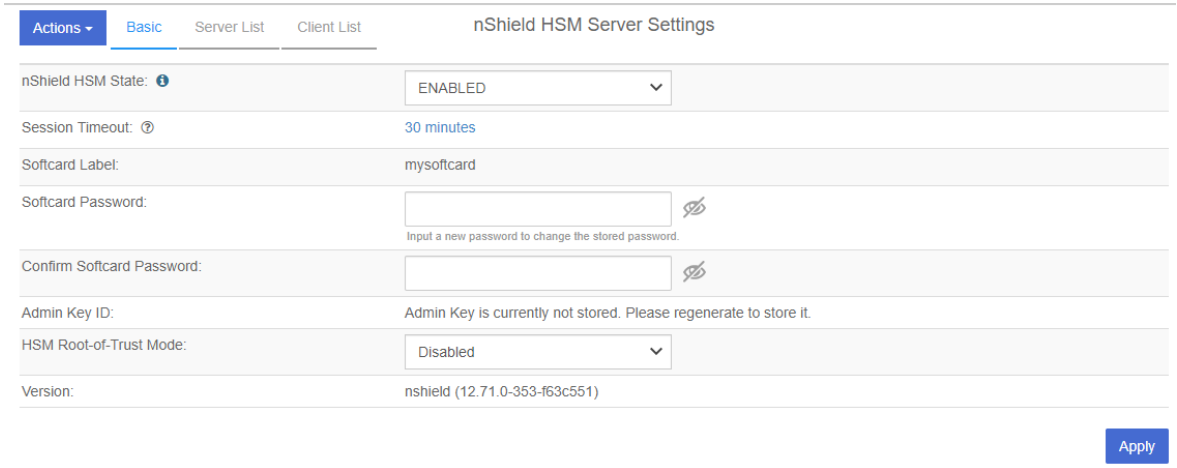
c. For **Confirm Softcard Password**, re-enter the password. For example:



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:



With Multi Tenancy, KMIP key wrapping is set at the tenant level. Each tenant will set up according to their requirements. Refer to Enable KMIP key wrapping for details.

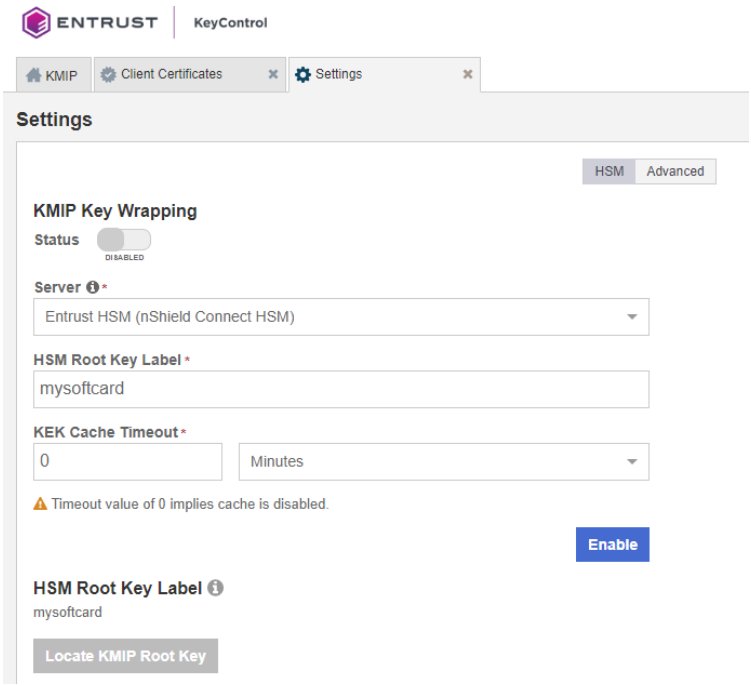
3.5. Enable KMIP key wrapping

For 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:



4. For **KMIP Key Wrapping**, enable the **Status**. If this is the first time doing this, you will not be able to set **Status** to **Enabled**. This will happen when you select the **Enable** action at the bottom of the dialog.
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.