Entrust KeyControl

nShield® HSM Integration Guide

06 Jan 2023

Contents

1. Introduction

This guide describes:

- The procedure to install and configure KeyControl as a KMIP server.
- The procedure to integrate Entrust KeyControl and Entrust nShield HSM for establishing a hardware root of trust for all encryption keys.
- The procedure to protect the KeyControl Admin Key in the HSM.

When all of these procedures are performed, the combined solution facilitates regulatory compliance with a FIPS 140 Level 3 and Common Criteria EAL4+ root of trust.

> Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

1.1. Product configuration

Entrust has successfully tested nShield HSM integration with KeyControl in the following configurations:

Product	Version
KeyControl	10.0
nShield HSM hardware	Connect XC

1.1.1. Supported features

Entrust has successfully tested nShield HSM integration with the following features:

Feature	Support
Softcards	Yes
Module-only key	Not Supported
OCS cards	For FIPS Authorization Only
nSaaS	Not tested

1.1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.1.2.1. Connect XC

Tested configurations:

Security World Software	Firmware	Image	FIPS 140 Level 3
12.80.4	12.50.11 (FIPS Certified)	12.80.4	No
12.80.4	12.72.1 (FIPS Certified)	12.80.5	Yes

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.

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

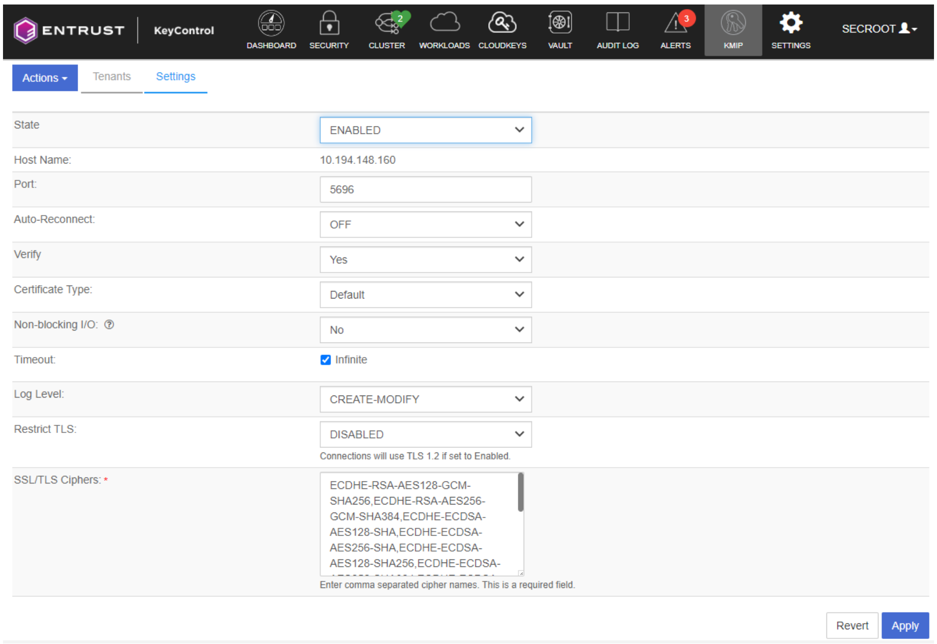
After the Entrust KeyControl server is deployed and the initial installation is complete, you can configure the network settings, e-mail server preferences, and certificate configuration. For these procedures, see the KeyControl System Configuration admin guide.

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.



State	ENABLED
Host Name:	10.194.148.160
Port:	5696
Auto-Reconnect:	OFF
Verify	Yes
Certificate Type:	Default
Non-blocking I/O:	No
Timeout:	☑ Infinite
Log Level:	CREATE-MODIFY
Restrict TLS:	DISABLED Connections will use TLS 1.2 if set to Enabled.
SSL/TLS Ciphers: *	ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES128-SHA,ECDHE-ECDSA-AES256-SHA,ECDHE-ECDSA-AES128-SHA256,ECDHE-ECDSA- Enter comma separated cipher names. This is a required field.

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.

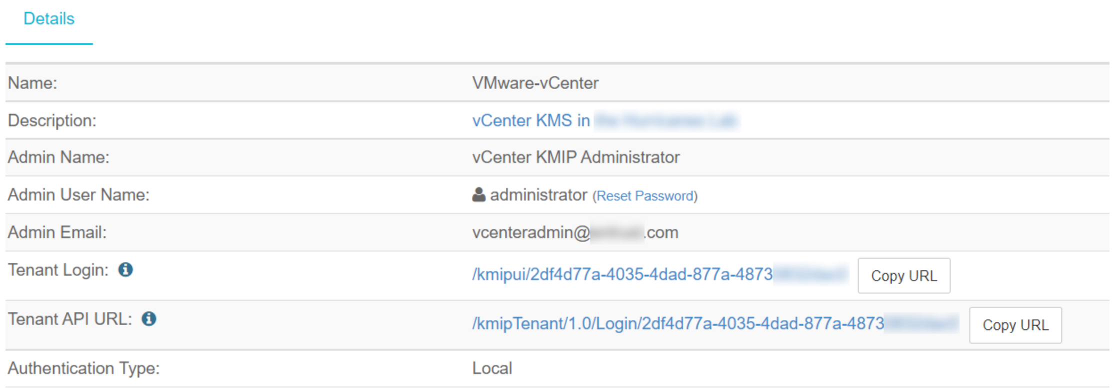
4. In the **About** tab, enter the **Name** of the tenant and a **Description**.

   > 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 external IDP or 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:



Name:	VMware-vCenter
Description:	vCenter KMS in [redacted]
Admin Name:	vCenter KMIP Administrator
Admin User Name:	administrator (Reset Password)
Admin Email:	vcenteradmin@[redacted].com
Tenant Login: ℹ	/kmipui/2df4d77a-4035-4dad-877a-4873[redacted] Copy URL
Tenant API URL: ℹ	/kmipTenant/1.0/Login/2df4d77a-4035-4dad-877a-4873[redacted] Copy URL
Authentication Type:	Local

11. Test the tenant. To do this, select the **Tenant Login** URL and attempt to log in as the user specified 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.

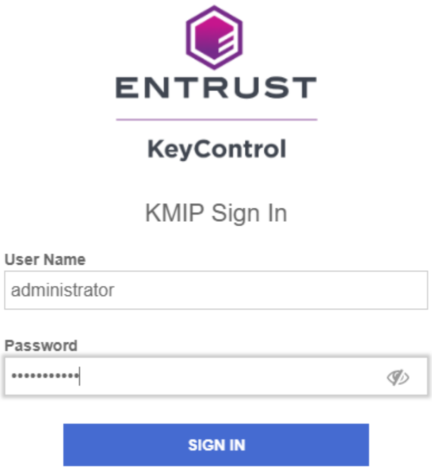
2.5. Establish trust between the KeyControl Server and the Client Application

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:



ENTRUST

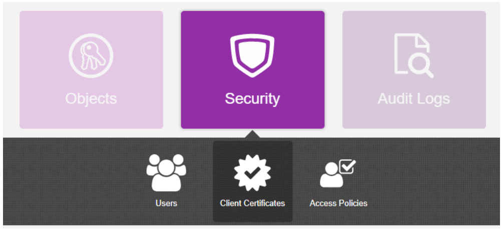
KeyControl

KMIP Sign In

User Name: administrator

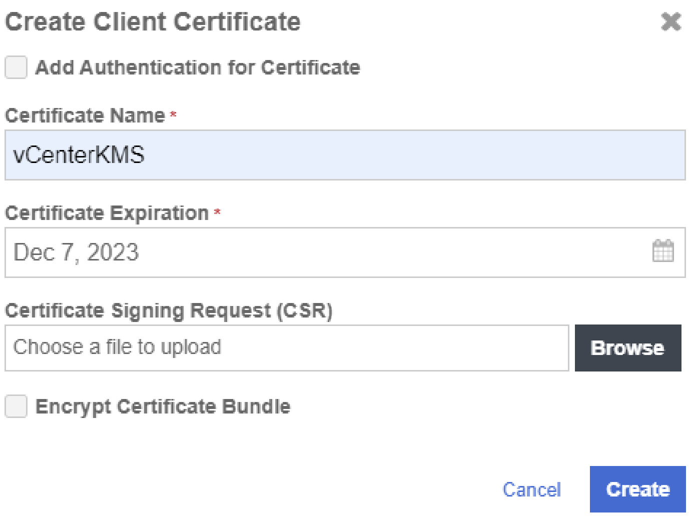
Password: •••••••••••

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

□ Add Authentication for Certificate

Certificate Name *

vCenterKMS

Certificate Expiration *

Dec 7, 2023

Certificate Signing Request (CSR)

Choose a file to upload

□ Encrypt Certificate Bundle

   d. Select **Create**.
5. After it is created, select the new certificate 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.

ℹ 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 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.

These procedures are optional but the combined solution facilitates regulatory compliance with a FIPS 140 Level 3 and Common Criteria EAL4+ root of trust.

The guide covers FIPS 140 Level 2 compliance and will note when different instructions are needed for compliance with FIPS 140 Level 3.

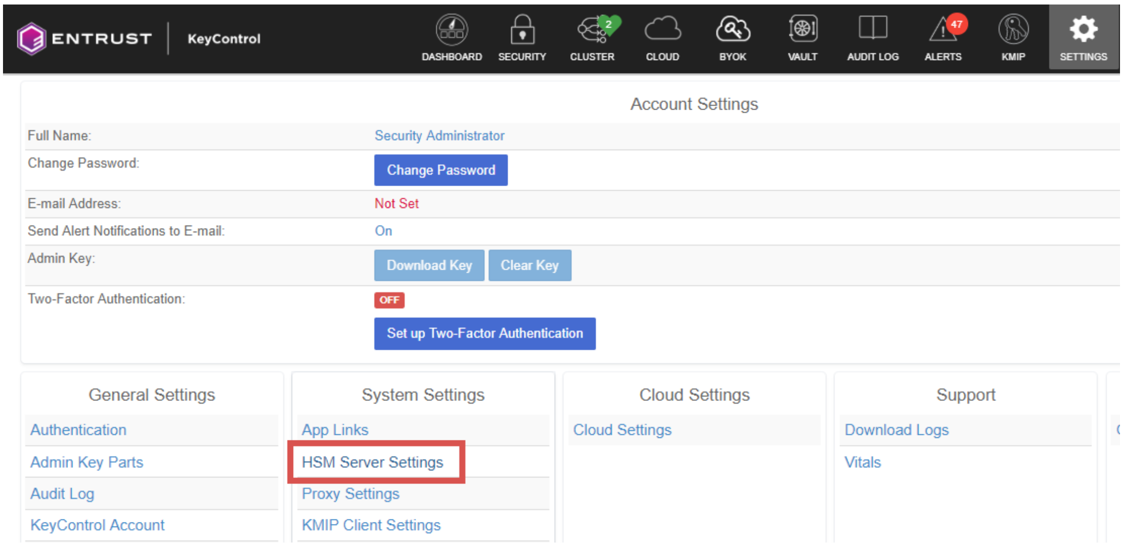
> With Multi Tenancy support, KMIP key wrapping is set at the tenant level. Each tenant will set up according to their requirements. Refer to Enable KMIP key wrapping for details.

3.1. Prerequisites

- Entrust KeyControl has been deployed and configured. For details, see Install the KeyControl server.
- 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**.



Account Settings

Full Name: Security Administrator

Change Password:

E-mail Address: Not Set

Send Alert Notifications to E-mail: On

Admin Key:

Two-Factor Authentication: OFF

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.

  Zipped file content example:

  ```
  -rwxrwxrwx. 1 root   nfast 40632 Dec 20 12:01 world
  -rwxrwxrwx  1 root   nfast  5000 Dec 20 12:01 module_5F08-02E0-D947
  ```

  When multiple HSMs are used there will be a `module_NNN` file for each HSM.

> The zipped file should contain the Security World and HSM module files. For a level 3 world, FIPS authorization is required. Entrust recommends that an OCS card is used to provide FIPS authorization for the generation of keys. The card and cards files in this case should also be included in the zipped file and the OCS card to be left inserted in the HSM. If more than one HSM is used, have the OCS card inserted in each HSM. Keep in mind that the OCS is only used for FIPS authorization and does not protect any keys.

Zipped file content example with OCS card (FIPS Level 3 world file):

```
-rwxrwxrwx. 1 root   nfast 40632 Dec 20 12:01 world
-rwxrwxrwx  1 root   nfast  5000 Dec 20 12:01 module_5F08-02E0-D947
-rw-rw-r--  1 root   nfast   104 Dec 20 12:06 card_1296a68c901427d44bf68a029c0b72b8f4fb2e15_1
-rw-rw-r--  1 root   nfast  1352 Dec 20 12:06 cards_1296a68c901427d44bf68a029c0b72b8f4fb2e15
```

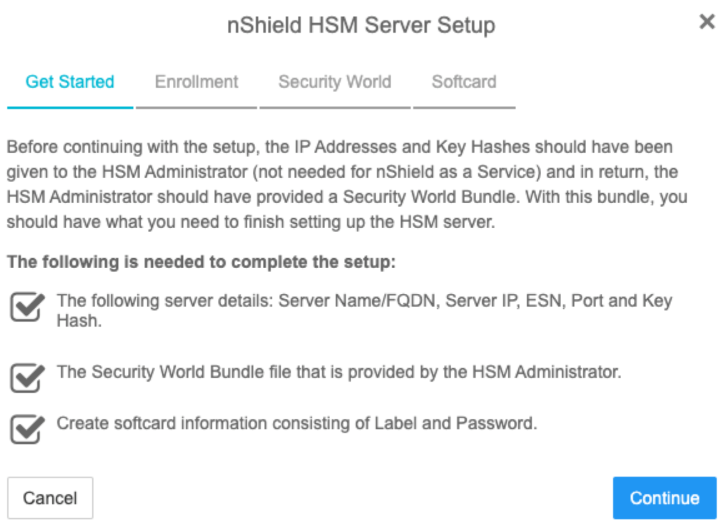
- The HSM server name. This can be the FQDN if defined, If an FQDN is not defined, it can be the ESN of the HSM.
- The IP address of the HSM.
- The Electronic Serial Number (ESN) and the key hash of the HSM. This can be obtained by running the following command on the nShield RFS server:

```
[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.

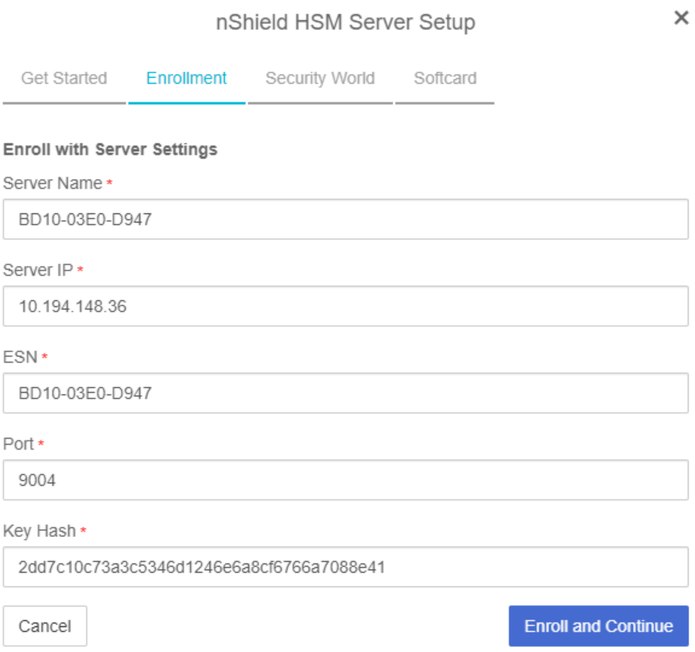
The following is needed to complete the setup:

☑ 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 for the HSM (if defined) or the ESN 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**.



nShield HSM Server Setup

Enroll with Server Settings

Server Name *: BD10-03E0-D947

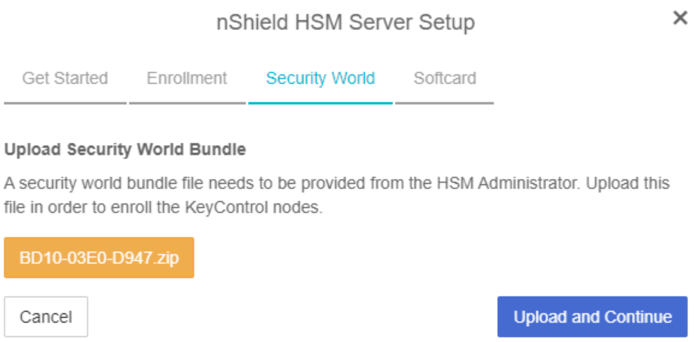
Server IP *: 10.194.148.36

ESN *: BD10-03E0-D947

Port *: 9004

Key Hash *: 2dd7c10c73a3c5346d1246e6a8cf6766a7088e41

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**.



nShield HSM Server Setup

Upload Security World Bundle

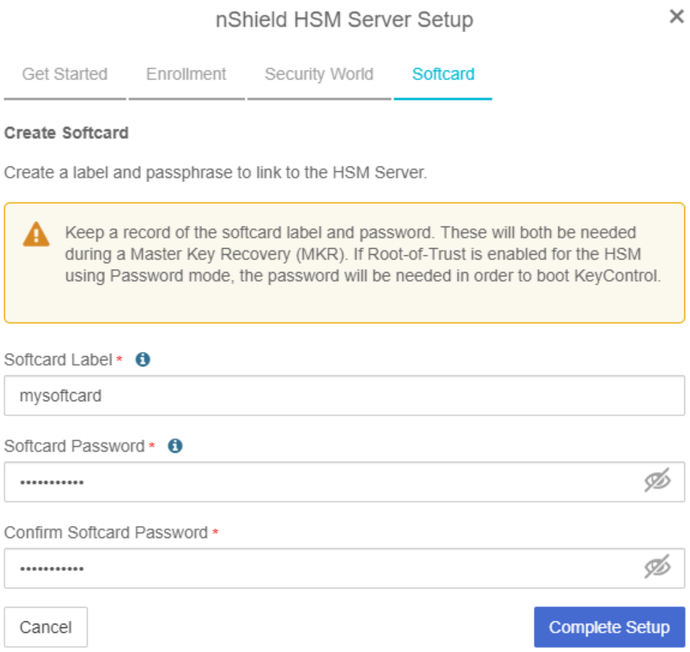
A security world bundle file needs to be provided from the HSM Administrator. Upload this file in order to enroll the KeyControl nodes.

BD10-03E0-D947.zip

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.

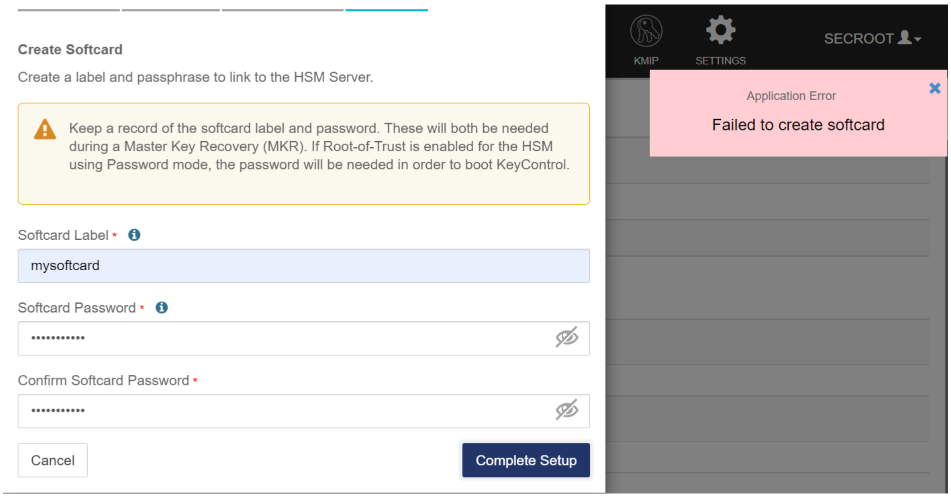
Softcard Label *: mysoftcard

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. If using a FIPS Level 3 world file, the OCS card must be inserted in the HSM for the setup to complete sucessfully. If not inserted, you will get an error message at this stage. 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 *: •••••••••••

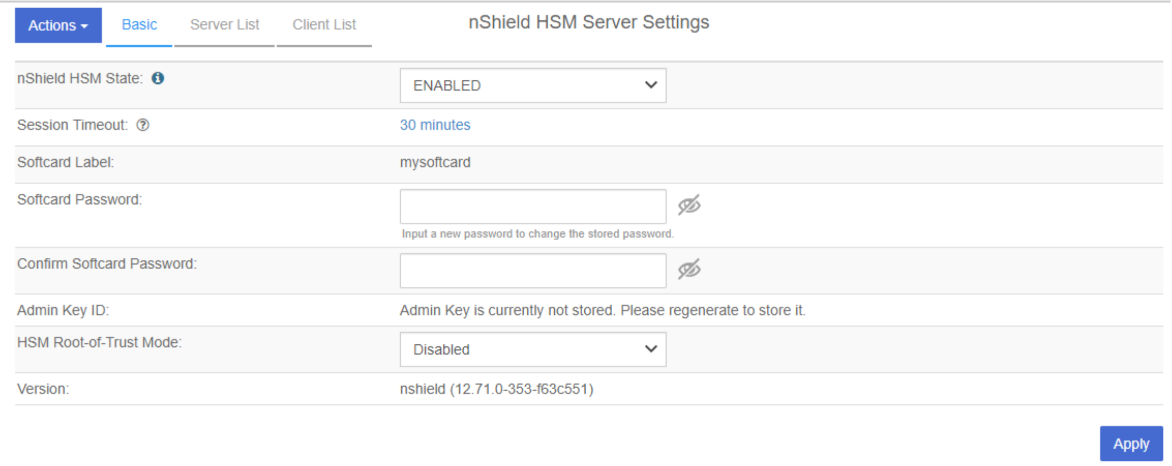
Application Error

Failed to create softcard

Insert the OCS card.

f. Select **Complete Setup**.

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



nShield HSM Server Settings

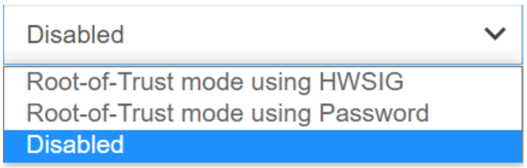
nShield HSM State:	ENABLED
Session Timeout:	30 minutes
Softcard Label:	mysoftcard
Softcard Password:	Input a new password to change the stored password.
Confirm Softcard Password:	
Admin Key ID:	Admin Key is currently not stored. Please regenerate to store it.
HSM Root-of-Trust Mode:	Disabled
Version: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

3.4.1. Enable HSM Root-of-Trust mode

HSM Root-of-Trust is disabled by default. HSM Root-of-Trust provides enhanced protection for the contents of the object store. HSM Root-of-Trust is gained when the HSM provides the cryptographic keys necessary to unlock the object store.

If the HSM cannot be contacted when KeyControl boots, or if the correct keys cannot be located, trust cannot be established with the HSM and KeyControl is not allowed to begin servicing key requests.

If you remove the HSM from the KeyControl configuration, the HSM Root-of-Trust configuration is also destroyed. Entrust strongly recommends enabling it by selecting one of the modes available. For example:


Disabled
Root-of-Trust mode using HWSIG
Root-of-Trust mode using Password
Disabled

Once you **Enable** Root-of-Trust, **Apply** the new configuration by selecting **Apply**.

- Root-of-Trust mode using HWSIG:

  The hardware signature is used to wrap the HSM configuration file. Unless there is a change to KeyControl's hardware configuration, booting KeyControl will require no user intervention before it can begin servicing requests.

  Virtual machine configuration changes may result in a need to recover the HSM configuration changes. When this happens, the normal KeyControl Masterkey Recovery procedure is used which requires the admin key that had been downloaded when KeyControl was installed.

- Root-of-Trust mode using Password:

  The HSM's softcard password is used to wrap the HSM configuration file. When

KeyControl boots, the UI will prompt for the HSM password. Only when the password is correctly entered is KeyControl allowed to begin booting.

The HSM password must be entered on each node of the cluster. For instance, if the entire cluster is restarted, it will only begin servicing requests once the password has been entered on all of the nodes in the cluster.

3.4.2. Test HSM connectivity

In the **nShield HSM Server Settings** screen:

1. Select **Actions** menu.
2. In the **Basic** tab, select **Test Connection** to ensure that the HSM is fully connected to KeyControl.

3.4.3. Generate new Admin Key

To make proper use of the HSM integration, regenerate the Admin Key in the HSM. Follow the instructions in the Generating the Admin Key section of the KeyControl Administration guide.

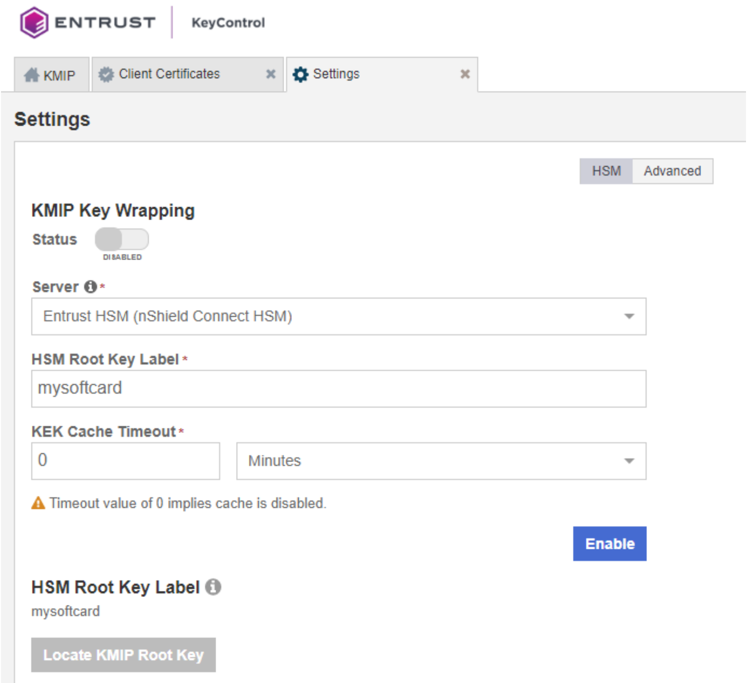
3.5. Enable KMIP key wrapping

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.

   > ℹ The **Tenant Login** URL was displayed at the end of the Create a KMIP tenant procedure. This URL 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: DISABLED

Server *: Entrust HSM (nShield Connect HSM)

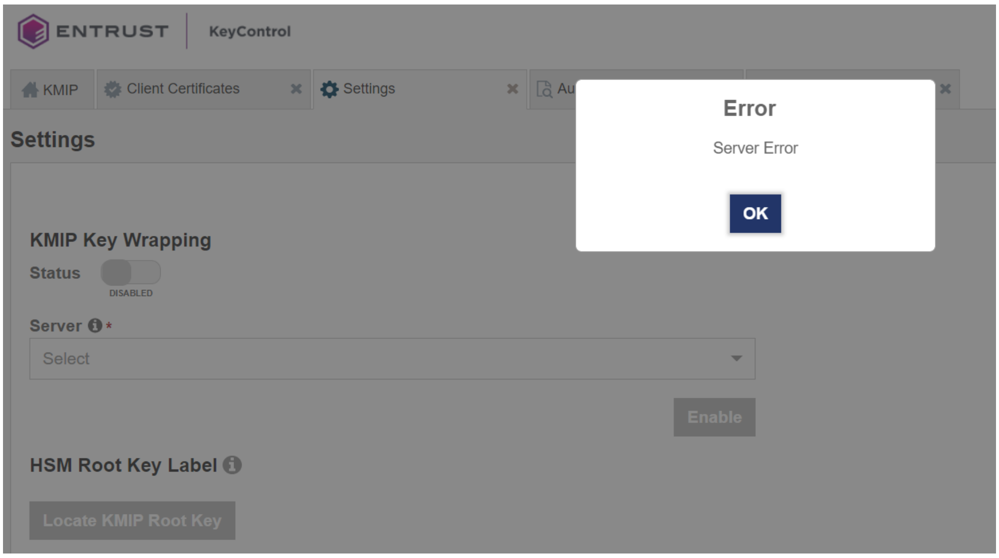
HSM Root Key Label *: mysoftcard

KEK Cache Timeout *: 0 Minutes

⚠ Timeout value of 0 implies cache is disabled.

HSM Root Key Label: mysoftcard

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. This guide uses **0** for the value so that no cache is used, which forces KeyControl to use the HSM every time.
8. If a FIPS level 3 world file is used, insert the OCS card in the HSM. If the OCS card is not inserted, an error appears when you select **Enable**.



Settings

Error

Server Error

KMIP Key Wrapping

Status: DISABLED

Server *: Select

HSM Root Key Label

To resolve this, select **OK** and insert the OCS card in the HSM.

9. 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.

3.6. FIPS Level 3 remarks and recommendations

Recomendations for when a FIPS Level 3 world file is used for the HSM configuration:

1. Create an OCS card 1/N where N is at least the number of HSMs being used in the configuration.
2. All HSMs in the configuration must use the same world file.
3. Leave the OCS card inserted on each HSM used in the configuration. This will prevent issues in case of a failure of one of the HSMs configured.
4. The zipped bundle file used in the configuration must have the world, module, card and cards files in the bundle.
5. The OCS card is only used for FIPS authorization and not to protect the keys.
6. The OCS card must be present any time new key material is created (FIPS authorization).
7. Regenerate the Admin Key.
8. Enable HSM Root of Trust.
9. Create KMIP tenant domain KEK.