Entrust KeyControl Vault

nShield® HSM Integration Guide

2024-11-21

Table of Contents

Chapter 1. Introduction

This guide describes:

- The procedure to install and configure KeyControl Vault.
- The procedure to integrate Entrust KeyControl Vault and Entrust nShield HSM for establishing a hardware root of trust for all encryption keys.
- The procedure to protect the KeyControl Vault 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.
- Until and including v13.4.5 firmware, all nShield HSMs require specific activation to utilize the elliptic curve features. See the nShield Security World documentation at nShield Product Documentation website.

1.1. Product configuration

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

Product	Version
KeyControl Vault	10.4.1
nShield HSM hardware	Connect XC, nShield 5C

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

Feature	Support
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:

HSM	Security World Software	Firmware	Image	FIPS 140 Level 3
nShield 5c	13.6.3	13.4.5 (FIPS 140-2 Certified)	13.6.5	Yes
Connect XC	13.6.3	12.72.3 (FIPS 140-2 certified)	13.6.5	Yes

Chapter 2. Install and configure the Entrust KeyControl Vault server

2.1. Install the KeyControl Vault server

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

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

After the KeyControl Vault server is deployed, configure the first KeyControl Vault node as described in the Entrust Configuring the First KeyControl Vault Node (OVA Install) online documentation.

After completing this procedure, add the second node as described in the Entrust Adding a New KeyControl Vault 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 Vault node can be deployed to perform its functions, Entrust strongly recommends deploying the solution with a minimum of four nodes in an active-active cluster solution.

Your KeyControl Vault license determines how many KeyControl Vault nodes you can have in a cluster. KeyControl Vault requires the deployment of KeyControl Compliance Manager (KCM). KCM manages licenses for the various KeyControl Vaults in the organization. For full information about the KeyControl Vault licensing, see the Entrust Upgrading Your Trial License online documentation.

2.2. Configure the KeyControl Vault Server

After the Entrust KeyControl Vault server is deployed and the initial installation is complete, you can configure the network settings, e-mail server preferences and cluster. For these procedures, see the KeyControl System Configuration in the Administration Guide.

Chapter 3. Integrate Entrust Key Control Vault server and Entrust nShield HSM

This chapter describes the procedure to integrate Entrust KeyControl Vault server 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 vault support, KMIP key wrapping is set at the vault level. Each KMIP vault will set up according to their requirements. Refer to Enable KMIP key wrapping (KMIP Vaults only) for details.

3.1. Prerequisites

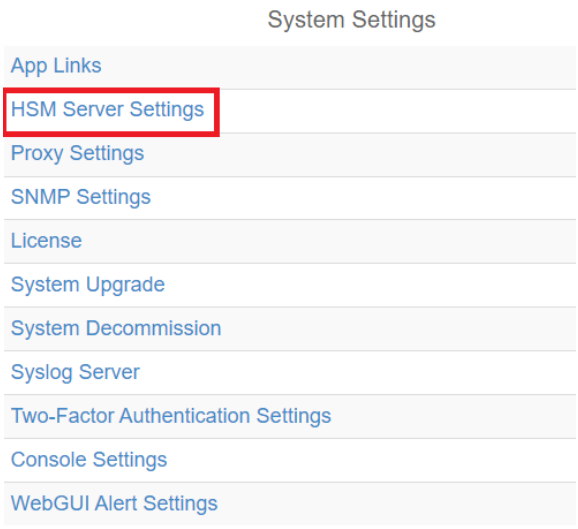
Before you integrate Entrust Key Control Vault server and Entrust nShield HSM, complete the following tasks:

- Entrust KeyControl Vault server has been deployed and configured. For details, see Install and configure the Entrust KeyControl Vault server.
- Entrust KeyControl Compliance Manager has been deployed and configured.
- 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.

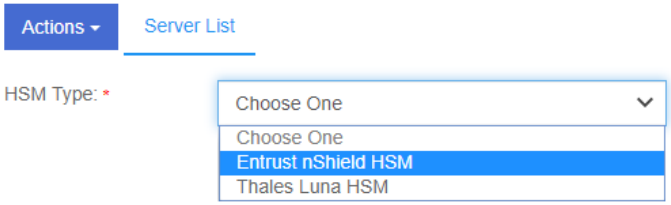
3.2. Initialize the HSM on KeyControl Vault server

To initialize the HSM on KeyControl Vault server:

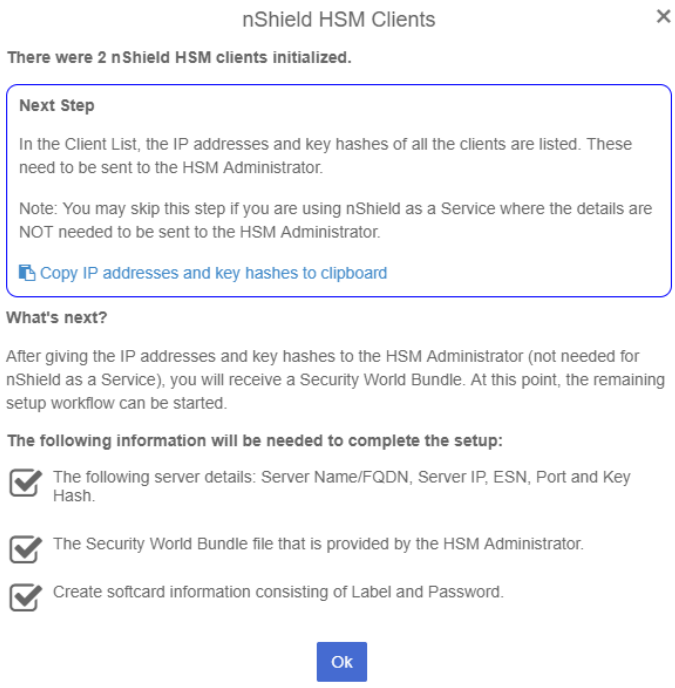
1. Log into the KeyControl Appliance Manager web user interface using an account with Security Admin privileges.
2. In the top menu bar, select **Settings** and then select **System Settings** > **HSM Server Settings**.



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 Vault cluster:

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

6. Save the file.

3.3. Add one or more KeyControl Vault nodes to the HSM

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

The HSM administrator adds each KeyControl Vault 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:

  ```
  world
  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):

  ```
  world
  module_5F08-02E0-D947
  card_1296a68c901427d44bf68a029c0b72b8f4fb2e15_1
  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:

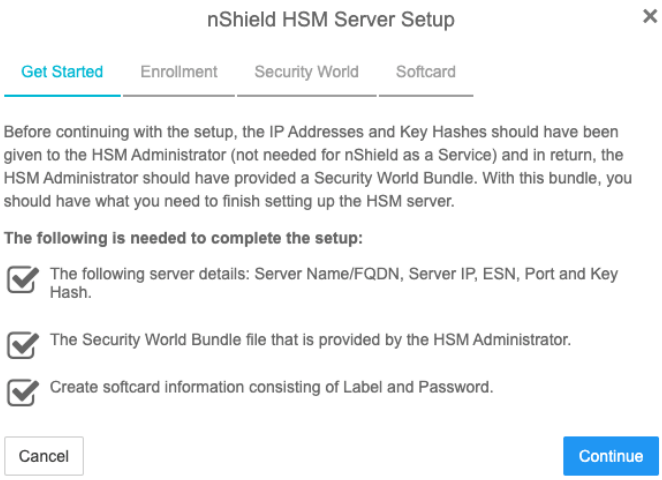
```
[anonkneti <hsm-ip-address>]
```

- The network port number that the HSM uses.

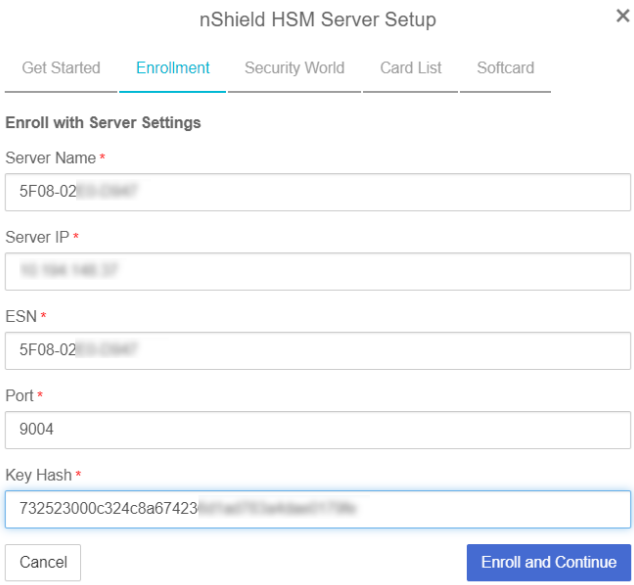
3.4. Set up the nShield HSM Server

To set up the nShield HSM Server:

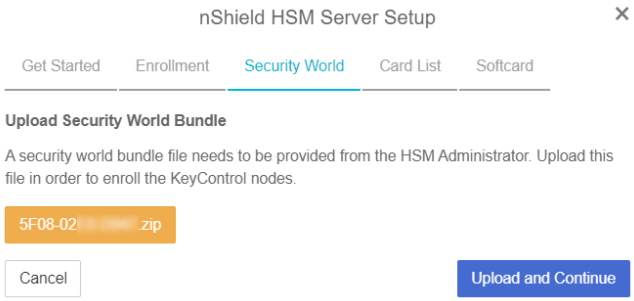
1. In the **Get Started** step of the **nShield HSM Server Setup** dialog, select **Continue**.



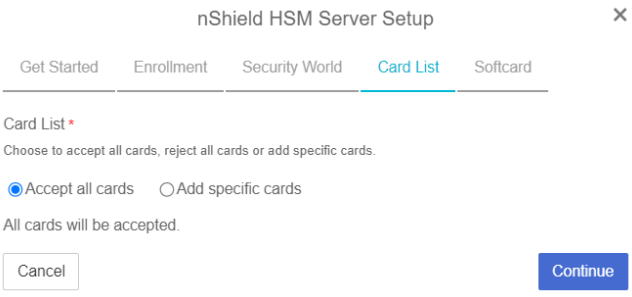
2. In the **Enrollment** step of the dialog:
    a. For **Server Name**, enter the server FQDN for the HSM (if defined) or the ESN of the HSM.
    b. For **Server IP**, enter the IP address of the HSM.
    c. For **ESN**, enter the ESN of the HSM.
    d. For **Port**, enter the required port. The default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



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 Vault nodes to the HSM.
   c. Select **Upload and Continue**.

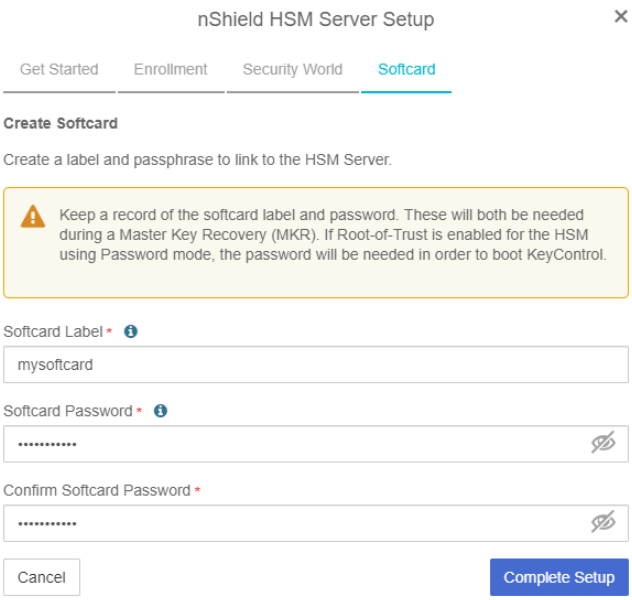


4. In the **Card List** step of the dialog:
   a. Only used if using FIPS Level 3 world file with an OCS card.
   b. Select **Accept All Cards**

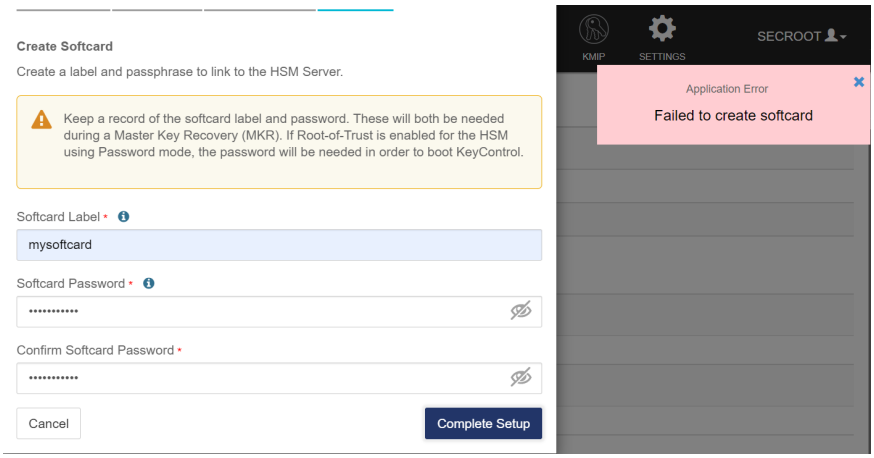


c. Select **Continue**

5. 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:



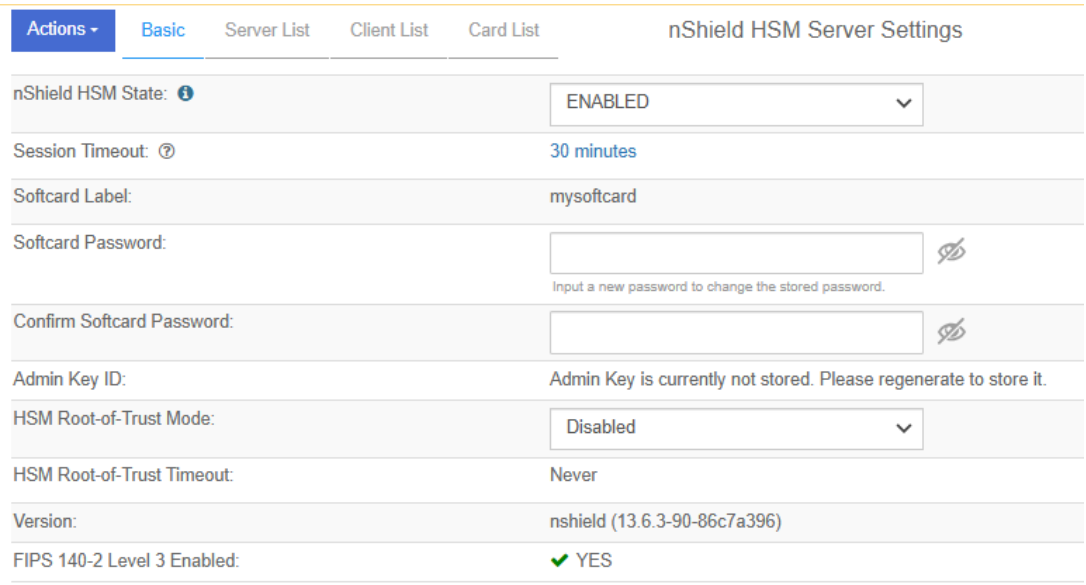
   d. Keep a record of the Softcard label and password. These will be needed during a Master Key Recovery (MKR). If Root-of-Trust is enabled for the HSM using Password mode, the password is also needed to boot KeyControl.
   e. If using a FIPS Level 3 world file, the OCS card must be inserted in the HSM for the setup to complete successfully. If not inserted, you will get an error message at this stage. For example:



   Insert the OCS card.

f. Select **Complete Setup**.

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

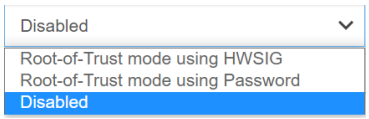


3.4.1. Enable HSM Root-of-Trust mode

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

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

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



Once you **Enable** ROT, **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 the KeyControl Vault hardware configuration, booting

KeyControl Vault 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 Vault Masterkey Recovery procedure is used which requires the admin key that had been downloaded when KeyControl Vault was installed.

- Root-of-Trust mode using Password:

  The HSM's softcard password is used to wrap the HSM configuration file. When KeyControl Vault boots, the UI will prompt for the HSM password. Only when the password is correctly entered is KeyControl Vault 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.

If you enable **Root-of-Trust**, you cannot reset the HSM configuration through the GUI unless you destroy the Root-of-Trust configuration using the console. Please contact Entrust support for details on how to destroy the Root-of-Trust configuration to be able to reset the HSM configuration.

3.4.2. Test HSM connectivity

To test HSM connectivity:

1. Access the **nShield HSM Server Settings** screen.
2. Select the **Actions** menu.
3. In the **Basic** tab, select **Test Connection** to ensure that the HSM is fully connected to KeyControl Vault.

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 Vault Administration guide.

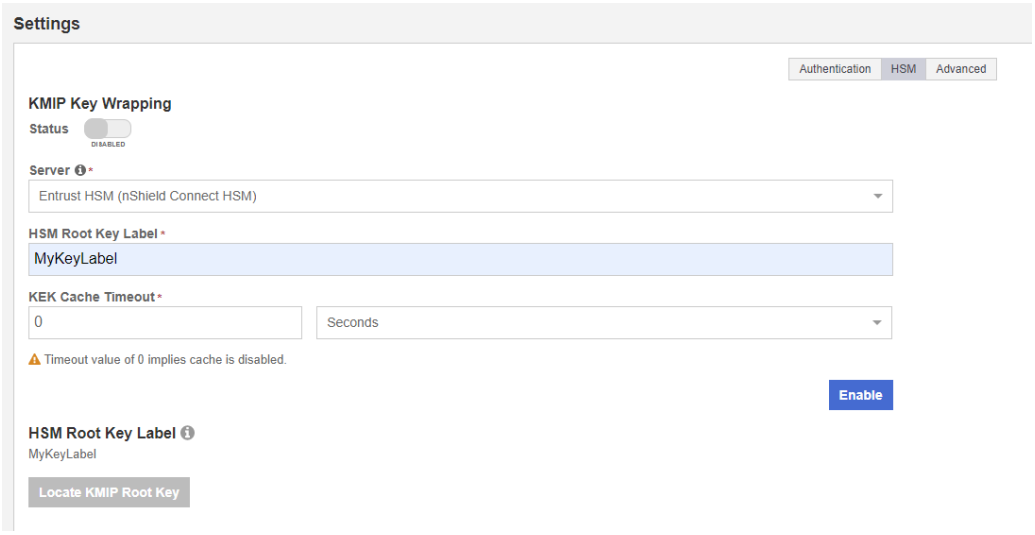
3.5. Enable KMIP key wrapping (KMIP Vaults only)

KMIP key wrapping is set at the vault level. Each vault will be configured according to its requirements.

1. Log into the KMIP Vault web user interface using the **Login** URL.

> The KMIP Vault **Login** URL is available by clicking the Vault **View Details** link available in the KeyControl **Vault Management** interface. This URL is different from the standard KeyControl Vault 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. 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**. 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

Recommendations 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. Enable KMIP key wrapping at the KMIP Vault.

3.7. TLS Configuration

Beginning with KeyControl Version 10.4.1, Secure Sockets Layer (SSL) has been replaced with Transport Layer Security (TLS). Support has also been added for Extended Master Secret (EMS).

The online documentation for this can be found here:

TLS Configuration section of the KeyControl Administration Guide.

By default, KeyControl comes setup with **TLS 1.3** and **EMS enforced**. These settings may cause problems during the integration where the client software fails to communicate with KeyControl because either it does not support **TLS 1.3** or **EMS**.

To change these settings:

1. Log into the KeyControl Appliance Manager web user interface.
2. Select **Settings** in the top level menu.
3. Under **General Settings**, select **TLS Configuration**.
4. To change the protocol version use the **Protocol Tab**. Supported options are:

   a. TLSv1.2, TLSv1.3
   b. TLSv1.3 only (default)
5. Adjust the protocol according to what the client software supports.
6. Under the **TLS Extended Master Secret** tab, you can change the **EMS** settings. They are:
   a. Enforce EMS (default)
   b. Do not enforce EMS (Not Recommended - has known vulnerabilities)
7. Adjust the EMS settings according to what the client software supports.

When you change the **EMS** settings, the KeyControl nodes in the cluster will reboot and you will have to log back in.

Chapter 4. Additional resources and related products