AppViewX

nShield® 5c HSM Integration Guide

2025-04-15

© 2025 Entrust Corporation. All rights reserved.

Table of Contents

Chapter 1. Introduction

AppViewX is a certificate lifecycle management platform that provides visibility, automation, and control of certificates and keys. Integrating HSMs with AppViewX means you do not need to deploy vendor-specific SDK or JAR files.

1.1. Supported nShield hardware and software versions

We have successfully tested AppViewX SaaS version 24.1, using the AppViewX Cloud Connector, with the following nShield hardware and software versions:

1.1.1. nShield 5

Security World Software	Firmware	FIPS 140
13.6.3	13.2.2	Unrestricted world

Throughout this guide, the term HSM refers to the nShield 5c. Other product configurations might work, but not all possible combinations have been tested by Entrust.

For help integrating AppViewX Platform with an Entrust HSM, see Entrust HSM in the AppViewX documentation library.

1.2. More information

- nShield HSM and Security World documentation
- AppViewX documentation
- Lightweight Kubernetes (K3s) documentation

For further information or support, contact your AppViewX sales representative or Entrust nShield Support, https://nshieldsupport.entrust.com.

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

Chapter 2. Procedures

The AppViewX Cloud Connector was set up using the AppViewX Virtual Image, which is an OVA containing all the required software, network, and Docker prerequisites that runs as a deployable virtual machine. It contains a lightweight Kubernetes distribution (K3s). This integration installs nShield Security World software on to the virtual machine, where it can interact with the K3s pods.

2.1. Set up the AppViewX virtual machine

1. Deploy the AppViewX OVA virtual image into VMware, see Setting up the AppViewX Cloud Connector via OVA using AppViewX User Interface.
2. Install the nShield Security World software (Linux version) into the AppViewX virtual machine you created in the previous step, see the nShield Security World Software Installation Guide.
3. Add all the relevent nShield 5c HSMs to the Security World, see Add HSMs to a Security World.
4. Add the following line to the `cknfastrc` file:

   ```
   CKNFAST_LOADSHARING=1
   ```

   See CKNFAST_LOADSHARING for more information.

5. Create a new softcard and give it a password:

   ```
   ppmk --new <name>
   ```

   Where <name> is the name you give to the new softcard. See Create a softcard with ppmk for more information.

6. Run the following commands to update permissions on the virtual machine:

   ```
   usermod -aG nfast appviewx
   chmod 644 /opt/nfast/chnfastrc
   chown -Rf appviewx:nfast /opt/nfast/kmdata/local
   cd /opt/nfast/kmdata/local
   chmod 644 *
   ```

7. Run `ckinfo` to get the slot number and name. This should be slot 1 and the softcard name that you specified in a previous step.
8. Run kubectl get to list the K3s pods.

9. Delete the AppViewX pod.

   After you delete the pod, Kubernetes automatically redeploys it with the new host files and permission changes.

10. Get a shell to the AppViewX pod using kubectl exec.
11. In the AppViewX shell, run `ckinfo` to check that the output is good and that there are no permission issues.

2.2. Add an HSM in the AppViewX user interface

After you integrate AppViewX with an nShield Security World, you can add HSMs to AppViewX. This enables you to use AppViewX to manage and utilise the HSM for tasks such as private key encryption and certificate management.

1. In the AppViewX web client menu, select **Inventory** > **Device**.
2. On the **HSM** tab, select **Entrust** and then **Add HSM**.
3. Complete the wizard as required.
   - For **HSM usage**, select **CSR Generation**.
   - For **Protect type**, select **Soft card**.
   - For the **So File Location**, enter the path to the `nfast/toolkits/pkcs11/libcknfast.so` file, including any symlinks.
   - For the **Config file Location** field, enter the path to the `nfast/kmdata/config/config` file, including any symlinks.

When the connection is ready, it appears as "Available" in the HSM list and the status indicator next to the name turns green.

Chapter 3. Additional resources and related products

3.1. nShield 5c

3.2. Entrust products

3.3. nShield product documentation