ENTRUST

SECURING A WORLD IN MOTION

Entrust KeyControl

nShield® as a Service Integration Guide

Version: 1.4

Date: Monday, January 18, 2021

Entrust
Registered Office: One Station Square,
Cambridge, CB1 2GA, United Kingdom
Registered in England No. 11673268

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 and how vSAN and vSphere, VM-based encryption can be enabled using Entrust KeyControl as the Key Management Server (KMS).

1.1 About the integration

1.1.1 KeyControl

KeyControl includes a fully functional KMIP (Key Management Interoperability Protocol) server that can serve as a KMS (Key Management Server) for vSphere and many other products that support the KMIP protocol.

1.1.2 nShield HSMs

nShield HSMs are designed to safeguard and manage cryptographic keys and processes within a certified hardware environment to establish a root of trust. Critical keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can compromize confidential information. nShield HSMs, offered as an appliance deployed at an on-premises datacenter or leased through an as-a-service subscription, provide enhanced key generation, signing, and encryption to protect sensitive container data and transactions. Using HSMs as part of an enterprise encryption or key management strategy is considered a best practice among cybersecurity professionals.

nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management.

After a trusted connection between KeyControl and an nShield Connect HSM is established, administrator keys and key encryption keys used by the KMS are securely stored and protected by the HSM. The combined solution enhances security and facilitates regulatory compliance with a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust.

For more information about KeyControl and nShield products, see https://www.Entrust.com.

1.1.3 KeyControl integration with nShield as a Service

Keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise through internal and external key theft. Entrust's nShield as a Service is a subscription-based solution for generating, accessing and protecting cryptographic key

material, separately from sensitive data, using dedicated FIPS 140-2 and eIDAS certified against EN 419 221-5 certified nShield Connect HSMs.

Subscribed customers interact with the cloud-based nShield HSMs in the same way that they would with appliances in their own dark data centers, but have no need to receive, install and maintain physical hardware

Entrust KeyControl and nShield as a Service integrate to provide comprehensive protection of administration and key encryption keys. The combination delivers an auditable method for enforcing security policies for foundational keys. By providing a mechanism to enforce security policies and a secure tamper resistant environment, customers can:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose.
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed.
- Deliver superior performance to support demanding multi-cloud workload deployments.
- Support hybrid cloud deployments and offer easy key migration should data repatriation from a Cloud Service Provider to on-premises be required.

1.2 Product configuration

Product	Version
KeyControl	5.2 or later
nShield HSM hardware	Connect + Connect XC
nShield firmware	12.50.11 or later

2 Procedures

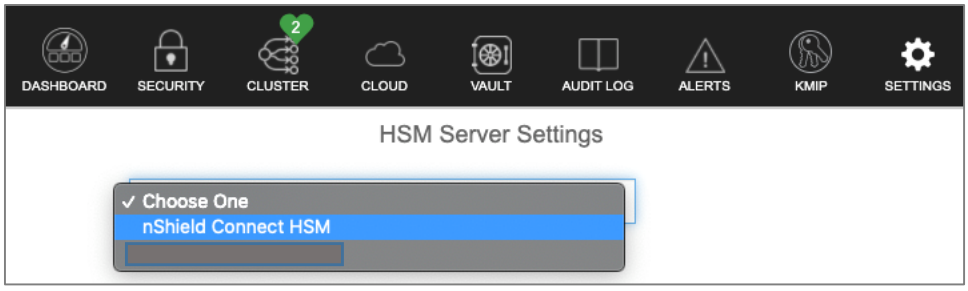
2.1 Prerequisites

For supported product versions, see section *1.2 Product configuration*.

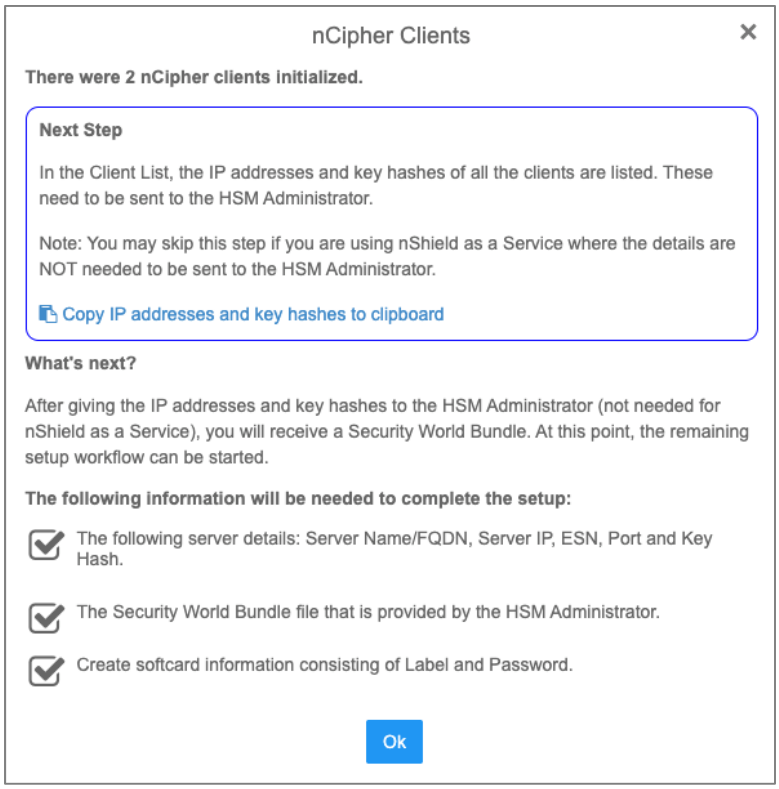
- Entrust KeyControl has been deployed and configured.
- The nShield HSM has been deployed and configured.
- You have rights to add new clients to the HSM configuration.
- You have the following information from the nShield as a Service configuration:
    - A zipped file that contains the nShield Security World and HSM module files.
    - The FQDN of nShield as a Service.
    - The IP Address of nShield as a Service.
    - The Electronic Serial Number (ESN) and the key hash of nShield as a Service.
    - The network port number that nShield as a Service uses.

2.2 Initialize nShield as a Service on KeyControl

1. Log in to the KeyControl web user interface using an account with Security Admin privileges.
2. In the top menu bar, select **Settings**, and then select **HSM Server Settings**.
3. From the list, select **nShield Connect HSM**, then select **Initialize**.

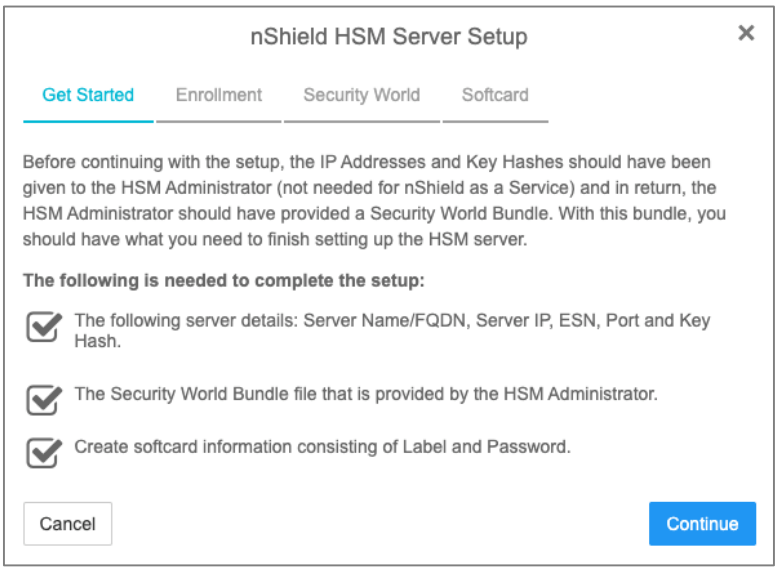


4. When you are using nShield as a Service rather than an on-premise HSM, you are not required to copy the IP addresses and key hashes to the clipboard. Select **OK**.

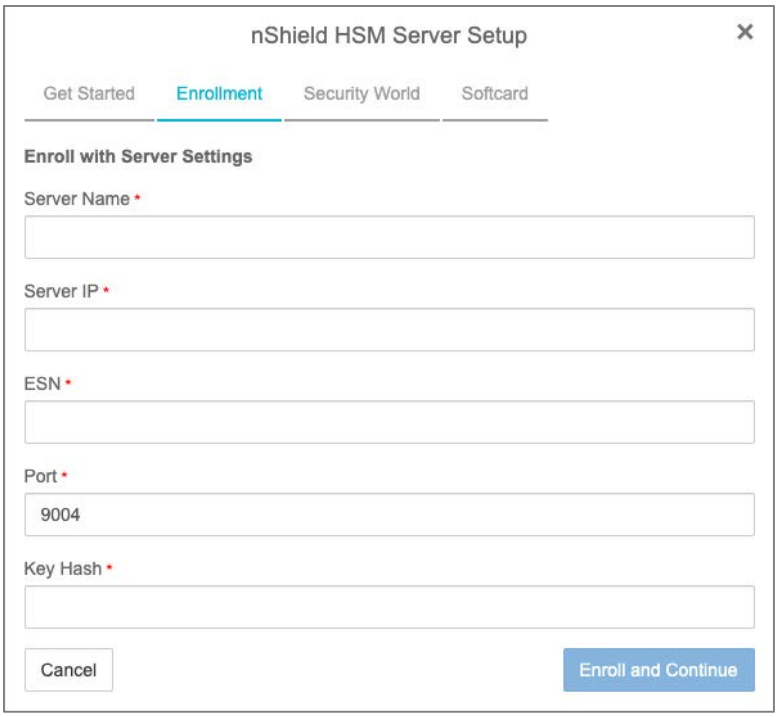


2.3 Set up the nShield HSM server

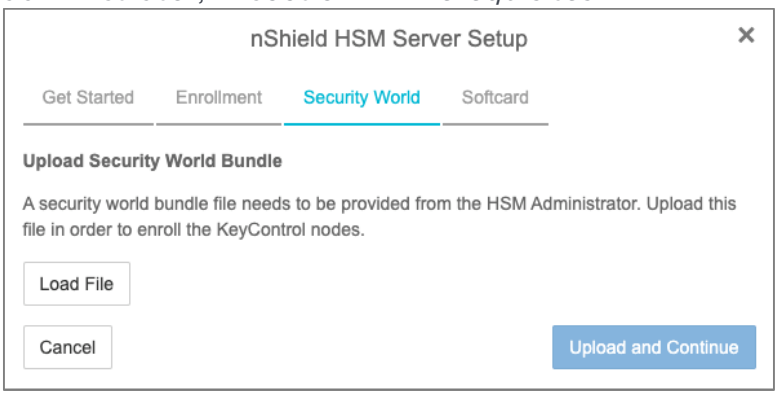
1. Select **Continue**.



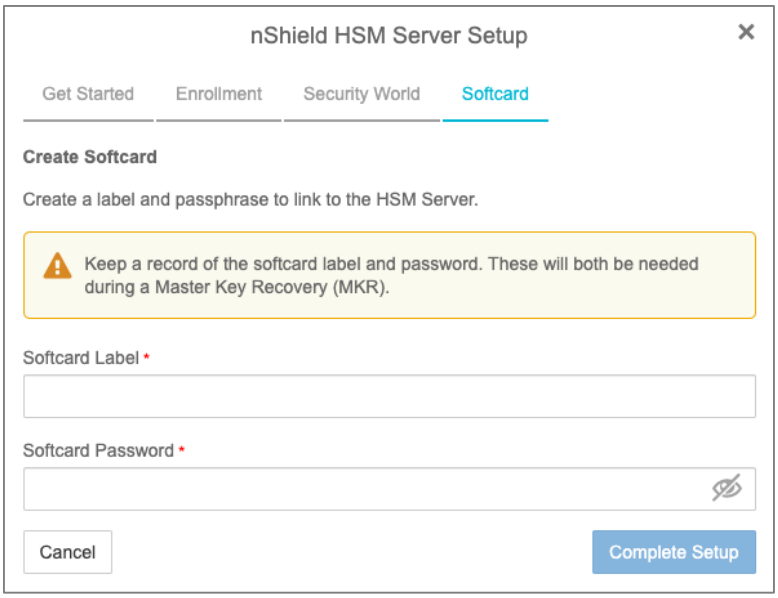
2. In the **Enrollment** step of the configuration:
   - Enter the server FQDN of nShield as a Service in the **Server Name** field.
   - Enter the IP address of nShield as a Service in the Server IP field.
   - Enter the ESN of nShield as a Service in the **ESN** field.
   - Enter the port in the **Port** field if it is different from 9004.
   - Enter the key hash of nShield as a Service in the **Key Hash** field.



3. Select **Enroll and Continue**.
4. In the **Security World** step of the configuration, select **Load File**, then browse to the zipped file that you received from the nShield as a Service administrator, in section *2.1 Prerequisites*.

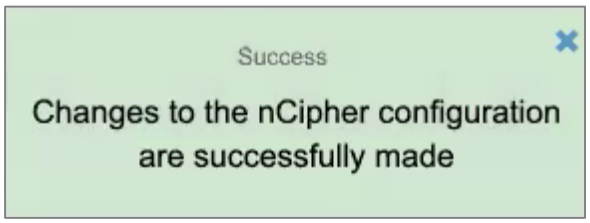


5. Select **Upload and Continue**.
6. In the **Softcard** step:
    a. Enter a unique name in the **Softcard Label** field. This value is user-defined.
    b. Enter a password in the **Softcard Password** field. This value is user-defined.



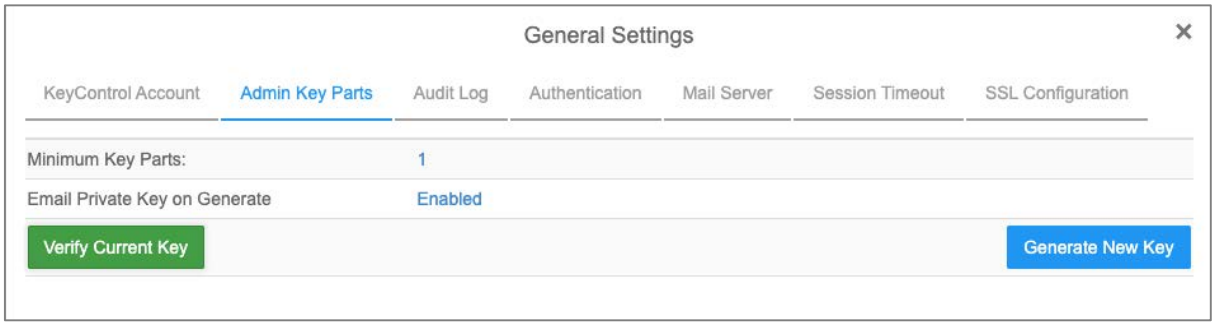
7. Select **Complete Setup**.

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

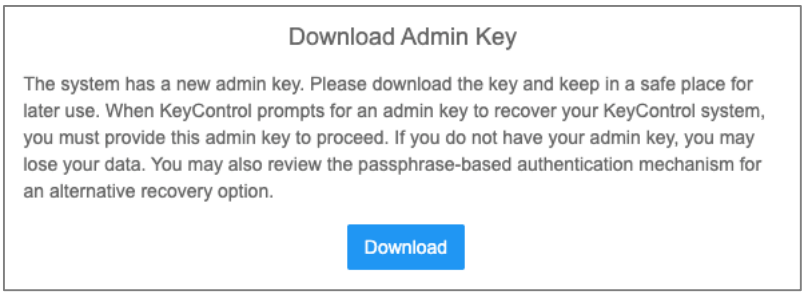


2.4 Push the KeyControl admin key to nShield as a Service

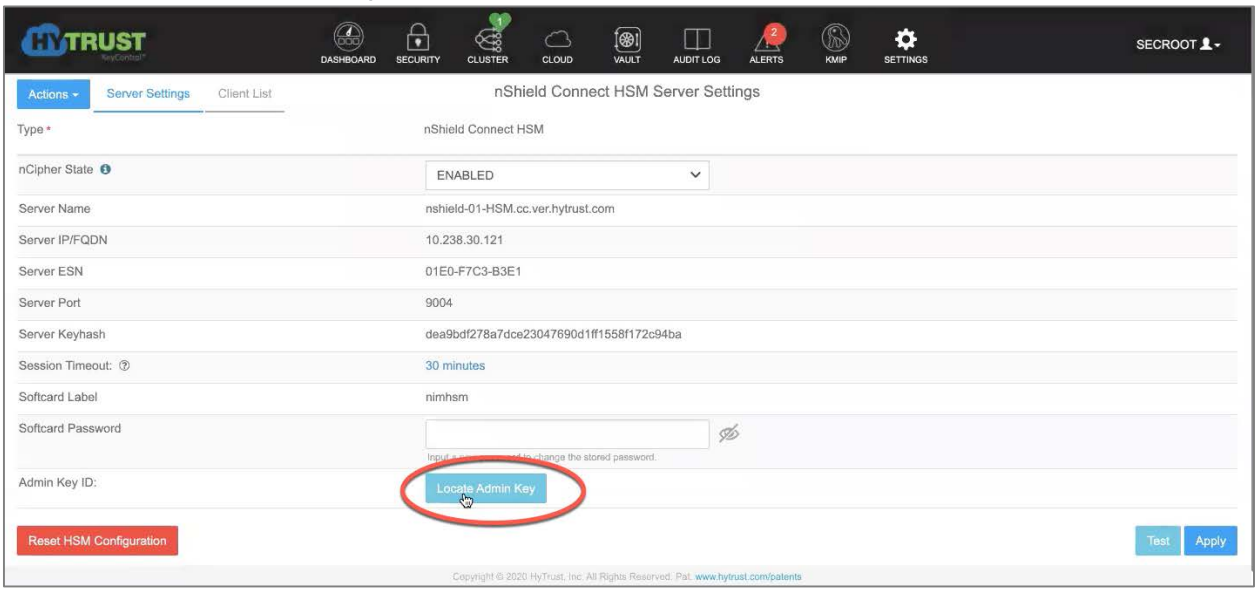
1. In the top menu bar, select **Settings**, then select **Admin Key Parts**.
2. Select **Generate New Key**.



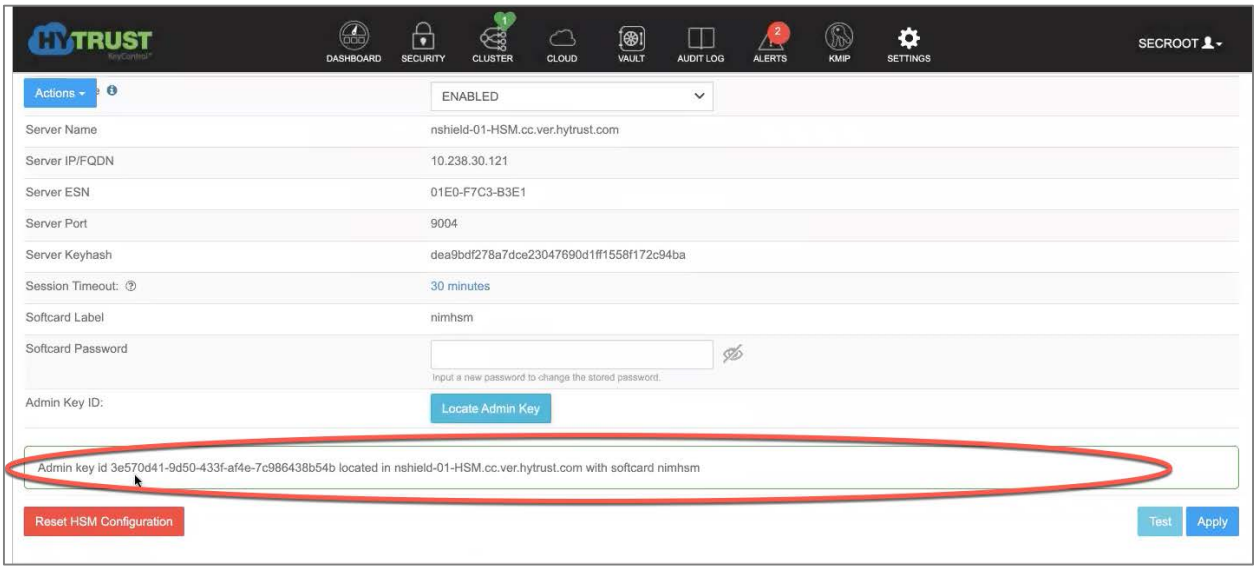
3. Select **Download**, and securely save the new Admin Key part to your computer.



4. In the top menu bar, select **Settings**, then select **HSM Server Settings**.
5. Select **Locate Admin Key**.

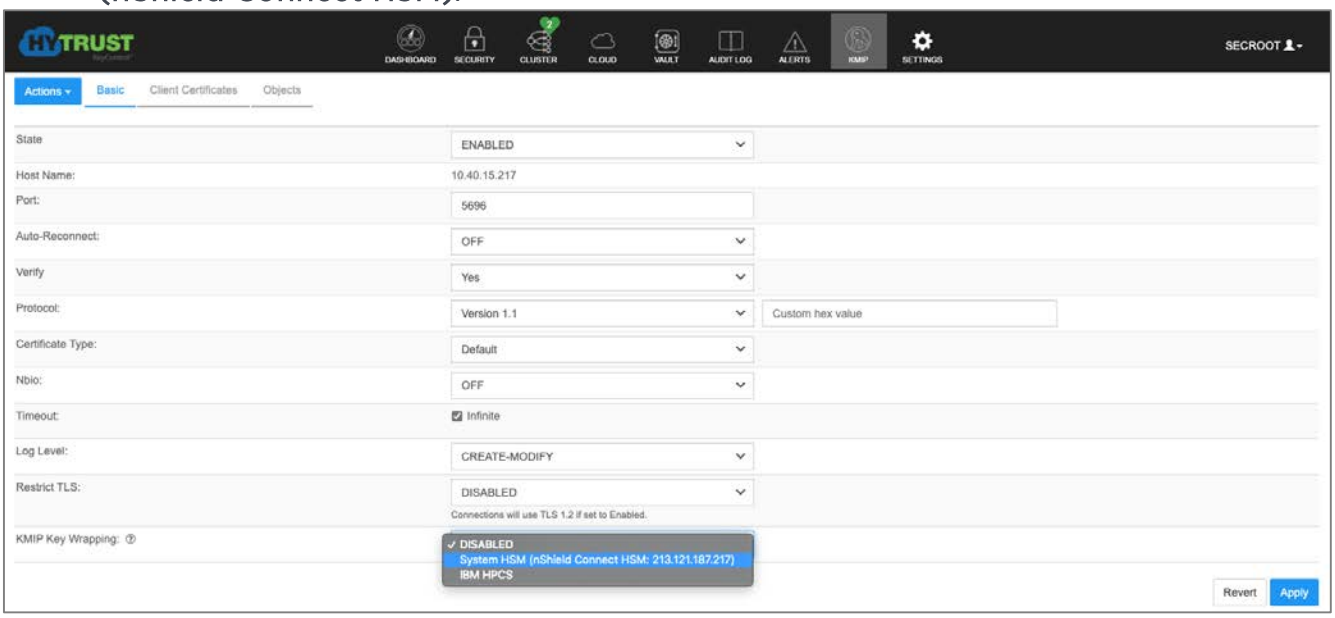


The **Admin Key ID** from the HSM is displayed, with the Softcard label that you defined:

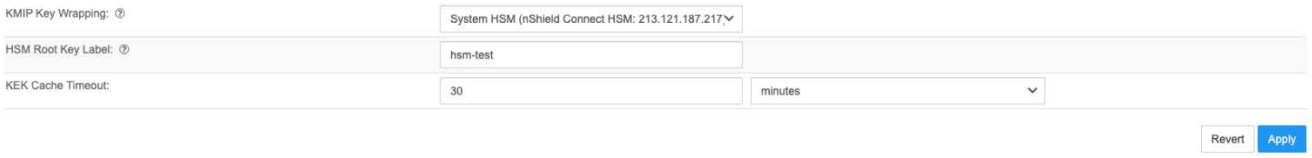


2.5 Enable KMIP service and KMIP key wrapping

1. In the top menu bar, select **KMIP,** then select the **Basic** tab.
2. From the list, select **State**, then select **Enable**.
3. Make sure that **Protocol** is set to version 1.1.
4. From the list, select **KMIP Key Wrapping**, then **select System HSM (nShield Connect HSM)**.



5. In the **HSM Root Key Label** field, enter a unique name for the **HSM Root Key**.
6. In the **KEK Cache Timeout** field, enter how long you want KeyControl to cache the HSM-derived Key Encryption Keys (KEKs). The maximum length is 24 hours.



7. Select **Apply**, and confirm the changes when prompted.

Contact Us

Web site	https://www.entrust.com
Support	https://nshieldsupport.entrust.com
Email Support	nShield.support@entrust.com
Online documentation:	Available from the Support site listed above.

You can also contact our Support teams by telephone, using the following numbers:

Europe, Middle East, and Africa

United Kingdom:	+44 1223 622 444 One Station Square Cambridge CB1 2GA UK

Americas

Toll Free:	+1 833 425 1990
Fort Lauderdale:	+1 954 953 5229 Sawgrass Commerce Center – A Suite 130, 13800 NW 14 Street Sunrise FL 33323 USA

Asia Pacific

Australia:	+61 9126 9070 World Trade Centre Northbank Wharf Siddeley St Melbourne VIC 3005 Australia
Japan:	+81 50 3196 4994
Hong Kong:	+852 3008 4994 31/F, Hysan Place 500 Hennessy Road Causeway Bay Hong Kong

To get help with
Entrust nShield HSMs

nShield.support@entrust.com

nshieldsupport.entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

ENTRUST

SECURING A WORLD IN MOTION