



**ENTRUST**

SECURING A WORLD IN MOTION

# Entrust KeyControl

nShield® as a Service Integration Guide

**Version: 1.4**

**Date: Monday, January 18, 2021**

Copyright © 2021 Entrust Corporation. All rights reserved.

Copyright in this document is the property of Entrust Corporation. It is not to be reproduced, modified, adapted, published, translated in any material form (including storage in any medium by electronic means whether or not transiently or incidentally) in whole or in part nor disclosed to any third party without the prior written permission of Entrust Corporation neither shall it be used otherwise than for the purpose for which it is supplied.

Words and logos marked with ® or ™ are trademarks of Entrust Corporation or its affiliates in the EU and other countries.

Mac and OS X are trademarks of Apple Inc., registered in the U.S. and other countries.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Information in this document is subject to change without notice.

Entrust Corporation Limited makes no warranty of any kind with regard to this information, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Entrust Security Limited shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

Where translations have been made in this document English is the canonical language.

Entrust

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

Entrust, and the Hexagon Logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

# Contents

1	Introduction .....	4
1.1	About the integration .....	4
1.2	Product configuration.....	5
2	Procedures.....	6
2.1	Prerequisites.....	6
2.2	Initialize nShield as a Service on KeyControl .....	6
2.3	Set up the nShield HSM server.....	7
2.4	Push the KeyControl admin key to nShield as a Service.....	9
2.5	Enable KMIP service and KMIP key wrapping.....	11
	Contact Us.....	12

# 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 compromise 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

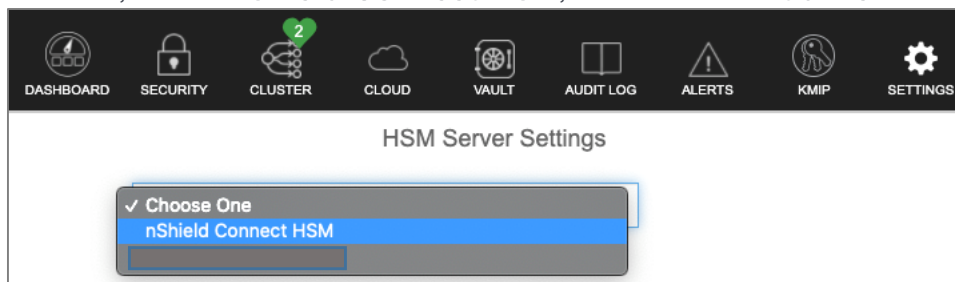
### 2.1 Prerequisites

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

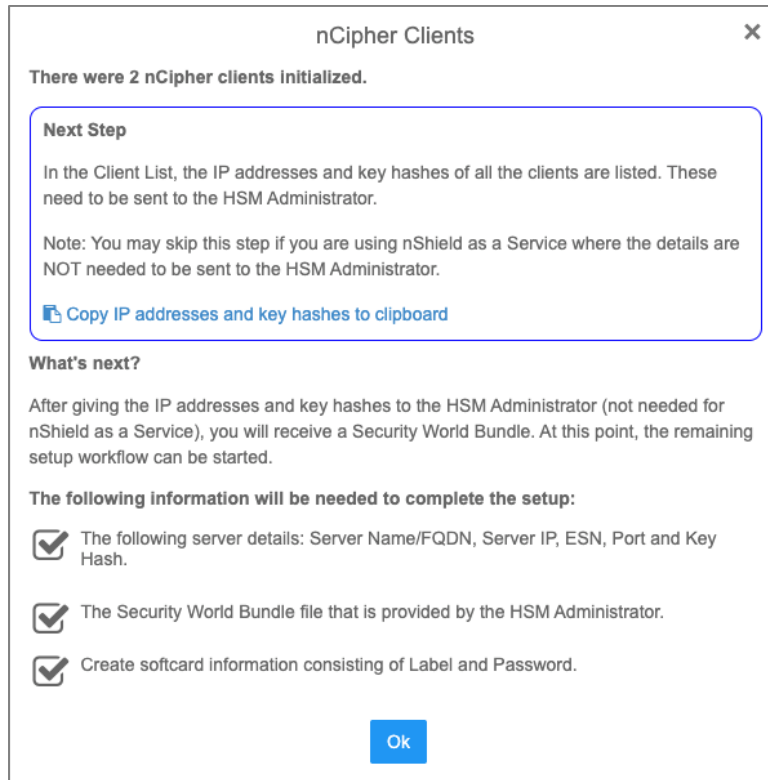
- Entrust KeyControl has been deployed and configured.
- The nShield HSM has been deployed and configured.
- You have rights to add new clients to the HSM configuration.
- You have the following information from the nShield as a Service configuration:
  - A zipped file that contains the nShield Security 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**.

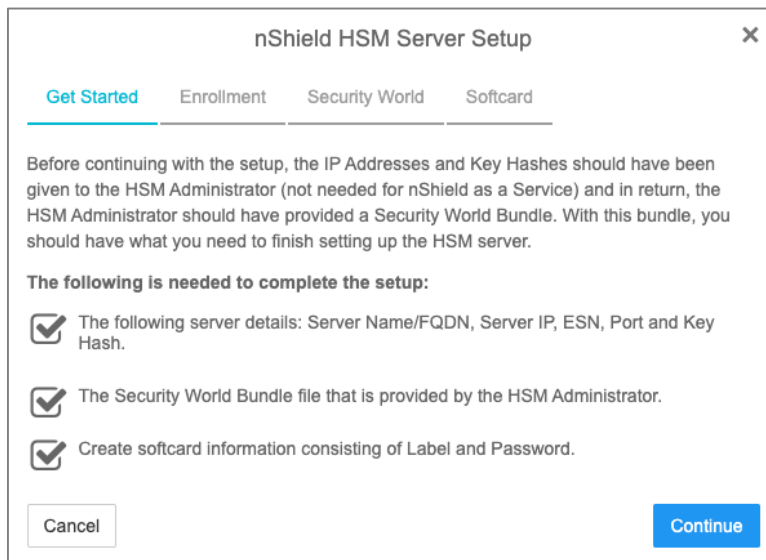


4. When you are using nShield as a Service rather than an on-premise HSM, you are not required to copy the IP addresses and key hashes to the clipboard. Select **OK**.



## 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.

The screenshot shows the 'nShield HSM Server Setup' dialog box with the 'Enrollment' tab selected. The dialog has a title bar with a close button (X) and a navigation bar with four tabs: 'Get Started', 'Enrollment', 'Security World', and 'Softcard'. Below the navigation bar, the section is titled 'Enroll with Server Settings'. It contains five text input fields: 'Server Name \*', 'Server IP \*', 'ESN \*', 'Port \*' (with '9004' entered), and 'Key Hash \*'. At the bottom left is a 'Cancel' button, and at the bottom right is a blue 'Enroll and Continue' button.

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*.

The screenshot shows the 'nShield HSM Server Setup' dialog box with the 'Security World' tab selected. The dialog has a title bar with a close button (X) and a navigation bar with four tabs: 'Get Started', 'Enrollment', 'Security World', and 'Softcard'. Below the navigation bar, the section is titled 'Upload Security World Bundle'. It contains a paragraph of text: 'A security world bundle file needs to be provided from the HSM Administrator. Upload this file in order to enroll the KeyControl nodes.' Below the text are two buttons: 'Load File' and 'Cancel' on the left, and a blue 'Upload and Continue' button on the right.

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.



**nShield HSM Server Setup** ✕

Get Started   Enrollment   Security World   **Softcard**

**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).

Softcard Label \*

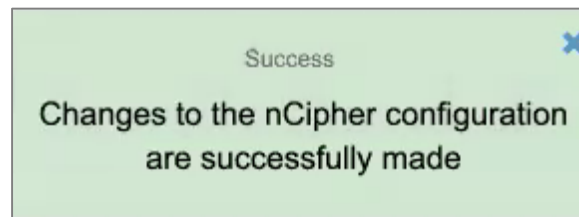
Softcard Password \*

 🗄

Cancel
Complete Setup

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**.

**General Settings** ✕

KeyControl Account   **Admin Key Parts**   Audit Log   Authentication   Mail Server   Session Timeout   SSL Configuration

---

Minimum Key Parts: 1

Email Private Key on Generate Enabled

Verify Current Key
Generate New Key

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

**Download Admin Key**

The system has a new admin key. Please download the key and keep in a safe place for later use. When KeyControl prompts for an admin key to recover your KeyControl system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data. You may also review the passphrase-based authentication mechanism for an alternative recovery option.

[Download](#)

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

The screenshot shows the 'nShield Connect HSM Server Settings' page in the HyTrust KeyControl interface. The page includes a top navigation bar with icons for Dashboard, Security, Cluster, Cloud, Vault, Audit Log, Alerts, KMP, and Settings. Below the navigation bar, there are tabs for 'Actions', 'Server Settings', and 'Client List'. The main content area displays various server configuration parameters such as nCipher State (ENABLED), Server Name, IP/FQDN, ESN, Port, Keyhash, Session Timeout, Softcard Label, and Password. A red circle highlights the 'Locate Admin Key' button located below the 'Admin Key ID' field.

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

This screenshot shows the same 'nShield Connect HSM Server Settings' page, but now the 'Admin Key ID' field is populated with the text: 'Admin key id 3e570d41-9d50-433f-af4e-7c986438b54b located in nshield-01-HSM.cc.ver.hytrust.com with softcard nimhsm'. A red oval highlights this text. The 'Locate Admin Key' button is still visible above the text.

## 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)**.

The screenshot shows the Entrust KeyControl nShield interface. The top navigation bar includes 'DASHBOARD', 'SECURITY', 'CLUSTER', 'CLOUD', 'VMAT', 'ALERT LOG', 'ALERTS', 'KMIP', and 'SETTINGS'. The 'KMIP' tab is selected. The 'Basic' sub-tab is active. The configuration fields are as follows:

State	ENABLED
Host Name:	10.40.15.217
Port:	5696
Auto-Reconnect:	OFF
Verify:	Yes
Protocol:	Version 1.1
Certificate Type:	Default
Nbio:	OFF
Timeout:	<input checked="" type="checkbox"/> Infinite
Log Level:	CREATE-MODIFY
Restrict TLS:	DISABLED
KMIP Key Wrapping:	DISABLED

A dropdown menu for 'KMIP Key Wrapping' is open, showing the following options:

- ✓ DISABLED
- System HSM (nShield Connect HSM: 213.121.187.217)
- IBM HPCS

Buttons for 'Revert' and 'Apply' are visible at the bottom right.

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.

The screenshot shows the Entrust KeyControl nShield interface for the 'KMIP Key Wrapping' configuration. The fields are as follows:

KMIP Key Wrapping:	System HSM (nShield Connect HSM: 213.121.187.217)
HSM Root Key Label:	hsm-test
KEK Cache Timeout:	30 minutes

Buttons for 'Revert' and 'Apply' are visible at the bottom right.

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

# Contact Us

Web site	<a href="https://www.entrust.com">https://www.entrust.com</a>
Support	<a href="https://nshieldsupport.entrust.com">https://nshieldsupport.entrust.com</a>
Email Support	<a href="mailto:nShield.support@entrust.com">nShield.support@entrust.com</a>
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](mailto:nShield.support@entrust.com)  
[nshieldsupport.entrust.com](https://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