HyTrust KeyControl Integration with nCipher nShield-as-a-Service

Why use Hytrust Keycontrol with nCipher nShield-as-a-Service?

Complications of Managing High Volumes of Encryption Keys for Workloads Across Multiple Clouds
As more enterprises today use multi-cloud computing environments to conduct business, managing encrypted workloads become increasingly difficult. Handling the encryption from each cloud management platform is complex and increases the risk of inconsistent policies. Migrating workloads and data between clouds requires them to be decrypted first, then migrated in clear-text, and subsequently re-encrypted, which creates a security gap.

Challenges of Securely Managing Key Lifecycles Centrally While Supporting Multi-Cloud Settings
Centralizing key management across multi-cloud deployments enables consistent security policy enforcement and reduced risks. However, aggregating keys in one central location requires additional security. Establishing a root of trust that protects the centralized key management platform is critical to ensure that the organization has access to encrypted workloads across a variety of on-premises and cloud environments.

Seamless Integration Between HyTrust KeyControl and nCipher 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. nCipher’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.

HyTrust KeyControl and nCipher nShield-as-a-Service seamlessly integrate to provide comprehensive protection of admin 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

HyTrust KeyControl
HyTrust 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.

Once a trusted connection between KeyControl and nCipher nShield-as-a-Service is established admin keys and key encryption keys used by the KMS are securely stored and protected by nCipher nShield-as-a-Service. The combined solution enhances security and facilitates regulatory compliance with a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust.
nCipher Security
nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity, and control to their business-critical information and applications. By using the same proven technology customers depend on today to protect against threats and meet compliance, nCipher underpins the trust of tomorrow.

Prerequisites
This document assumes the following:
- You have already deployed and configured HyTrust KeyControl version 5.2 or later
- You have access to the nShield-as-a-Service running firmware 12.6.x or later

Initialize HSM on KeyControl
1. Log into the KeyControl WebGUI using an account with Security Admin privileges
2. In the top menu bar, click Settings and then click HSM Server Settings
3. Select nShield Connect HSM from the drop-down box then click the Initialize button
4. When using the nShield-as-a-Service you are not required to copy the IP addresses and key hashes to the clipboard. Click OK.
NOTE: You still need the following information from the nShield-as-a-Service

1. A zipped file that contains the nShield Security World and HSM module files
2. The FQDN of the nShield-as-a-Service
3. The IP Address of the nShield-as-a-Service
4. The Electronic Serial Number (ESN) and the Key Hash of the nShield-as-a-Service
5. The network port the nShield-as-a-Service is using

**nShield HSM Server Setup**

1. Click **Continue** at this dialog

![nShield HSM Server Setup dialog](image)

2. In the **Enrollment** step of the configuration:
   a. Enter the Server FQDN of the nShield-as-a-Service in the **Server Name** field
   b. Enter the IP Address of the nShield-as-a-Service in the **Server IP** field
   c. Enter the ESN of the nShield-as-a-Service in the **ESN** field
   d. Enter the port in the **Port** field if it is different from 9004
   e. Enter the Key Hash of the nShield-as-a-Service in the **Key Hash** field
3. In the Security World step of the configuration:
   a. Click the Load File button and select the zipped file you obtained from the nShield-as-a-Service back in section: Initialize HSM on KeyControl
   b. Click Upload and Continue

4. In the Security World step of the configuration:
   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)
c. Click **Complete Setup**

5. The nShield Connect HSM is now configured to work with HyTrust KeyControl

**Push KeyControl Admin Key to HSM**

1. In the top menu bar, click **Settings** and click **Admin Key Parts**
2. Click **Generate New Key**
3. Click **Download** and securely save the new Admin Key part to your computer

4. In the top menu bar, click **Settings** and click **HSM Server Settings**

5. Click **Locate Admin Key**

6. The Admin Key ID from the nShield-as-a-Service will be displayed along with the Softcard label that was entered previously
Enable KMIP Service and KMIP Key Wrapping

1. In the top menu bar, click KMIP and click the Basic tab
2. Click the State dropdown box and select Enable
3. Make sure the Protocol is set to version 1.1
4. Click the KMIP Key Wrapping dropdown box and 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 a value for how long you want KeyControl to cache the HSM-derived Key Encryption Keys (KEKs). The maximum length is 24 hours.
7. Click Apply and confirm the changes when prompted

Summary

This quick start guide described the procedure on how to integrate HyTrust KeyControl and nCipher nShield-as-a-Service for establishing a hardware root of trust for all encryption keys. Next, the procedure for securely protecting the KeyControl Admin Key in the HSM was described. Finally, the procedure for enabling vSAN and vSphere, VM-based encryption can now be enabled using HyTrust KeyControl as the Key Management Server (KMS). Please refer to the HyTrust Quick Start guides at https://www.hytrust.com to learn more.