



Delinea Platform with AWS XKS

nShield® HSM Integration Guide

2026-08-03

Table of Contents

1. Introduction	1
1.1. Product configurations.....	1
1.2. Supported nShield hardware and software versions.....	1
1.3. Supported nShield features	1
1.4. Requirements	1
2. Architecture overview	3
2.1. AWS XKS overview.....	3
2.2. Delinea Platform overview.....	3
2.3. Connection to the AWS XKS	4
3. Integrate the Delinea Platform with the AWS KMS XKS.....	5
4. Test the integration.....	6
5. Additional resources and related products	7
5.1. nShield HSMs	7
5.2. nShield as a Service.....	7
5.3. Entrust products.....	7
5.4. nShield product documentation	7

Chapter 1. Introduction

This document describes how to integrate the Delinea Platform with the AWS Key Management Service (KMS) External Key Store (XKS) supported by the Entrust nShield Hardware Security Module (HSM).

1.1. Product configurations

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

Product	Version
Delinea Platform	12.1.000024

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

HSM	Security World Software	Firmware	Netimage
Connect 5c	13.9.5	13.8.4	13.9.5
nShield XC	13.9.5	13.8.3	13.9.5

1.3. Supported nShield features

Entrust has successfully tested nShield HSM integration with the following features:

Feature	Supported
Module Only Key	Yes
nSaaS	Supported but not tested

1.4. Requirements

- Access to Delinea Platform from your Delinea sales representative.
- Access to the [Entrust TrustedCare Portal](#).

- Access to an AWS XKS (External Key Store) supported by the Entrust nShield Hardware Security Module (HSM).

Familiarize yourself with the [nShield Documentation](#).

- The importance of a correct quorum for the Administrator Card Set (ACS).
- Whether your Security World must comply with FIPS 140 Level 3 or Common Criteria standards. For more information, see [FIPS 140 Level 3 compliance](#).
- Whether to instantiate the Security World as recoverable or not.

Chapter 2. Architecture overview

An AWS XKS protected by the nShield HSM was deployed for this integration testing. The AWS XKS has a public domain name and a publicly trusted certificate. The Delinea Platform connects to the AWS XKS using shared secrets.

- [AWS XKS overview](#)
- [Delinea Platform overview](#)
- [Connection to the AWS XKS](#)

2.1. AWS XKS overview

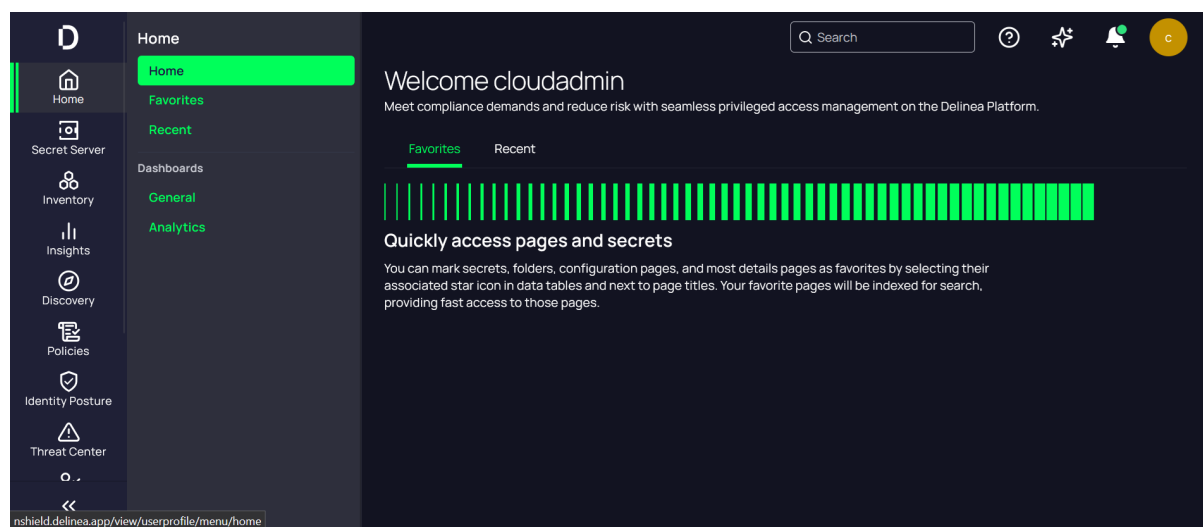
The AWS XKS consisted of an AWS Linux EC2 instance running the Security World software. The HSM was physically located at an Entrust test lab.

The AWS XKS endpoint was fronted by an AWS Network Load Balancer (NLB). A public DNS record was created. A publicly trusted TLS certificate was issued to connect to the XKS via the NLB.

The deployment of the AWS XKS protected by the nShield HSM is covered in a separate document available at [nShield Integration Guides](#).

2.2. Delinea Platform overview

Delinea provided a link via email to register with their platform. A tenant was created through the registration process, which in turn created a URL to access the tenant. Access to the URL is secured using credentials and multifactor authentication.

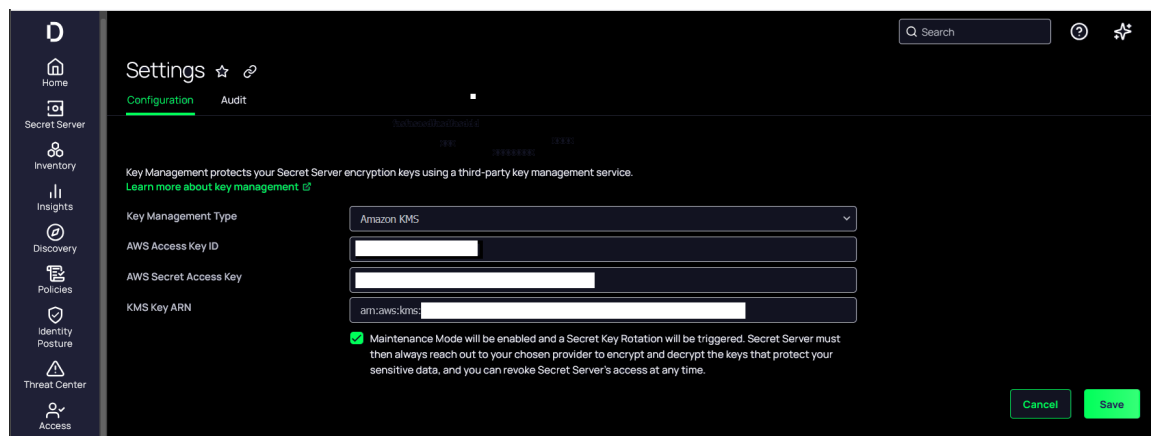


2.3. Connection to the AWS XKS

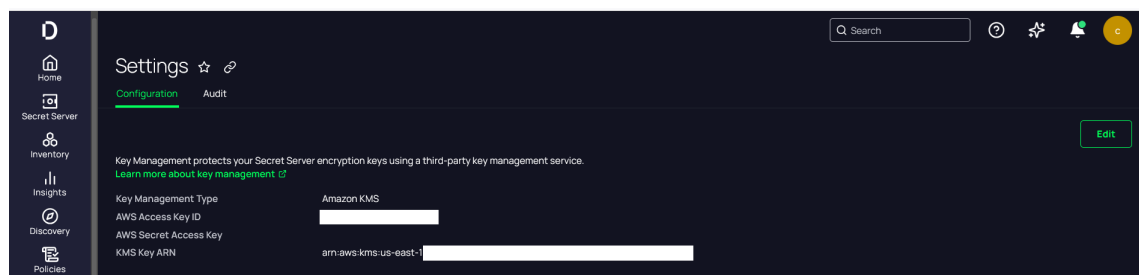
An encryption key was created in the AWS XKS. An AWS IAM user was created and granted permissions to use the key. The key ARN, the IAM user access key, and the secret access key were shared with the Delinea Platform to establish a connection to the AWS XKS.

Chapter 3. Integrate the Delinea Platform with the AWS KMS XKS

1. Open a browser, navigate to the Delinea Platform, and sign in.
2. Type "Key Management" in the search box. Then select **Key Management** in the search results. Alternatively, in the browser navigate to <https://<delinea-platform>/view/vault/admin/key-management/config>.
3. In the **Configuration** tab, select **Edit**.
4. In the **Key Management Type** pull-down menu, select **Amazon KMS**.
5. Enter the AWS IAM user access key, secret access key, and the key ARN. Then select **Save**.



6. Verify that the configuration completed successfully.

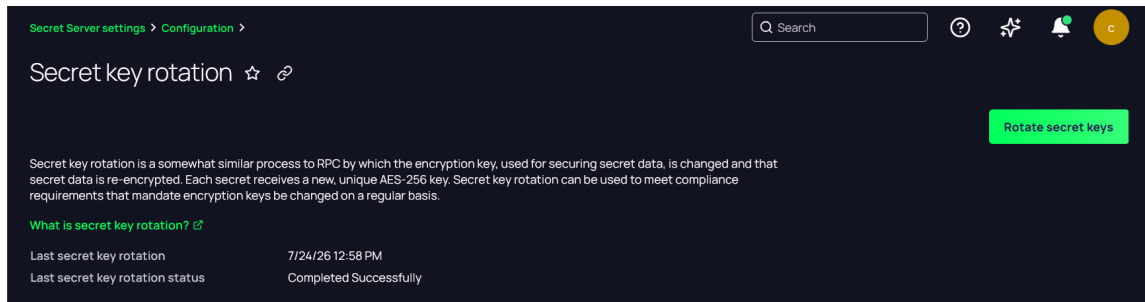


7. Select the **Audit** tab, then hover over the note to view the AWS KMS key ARN.

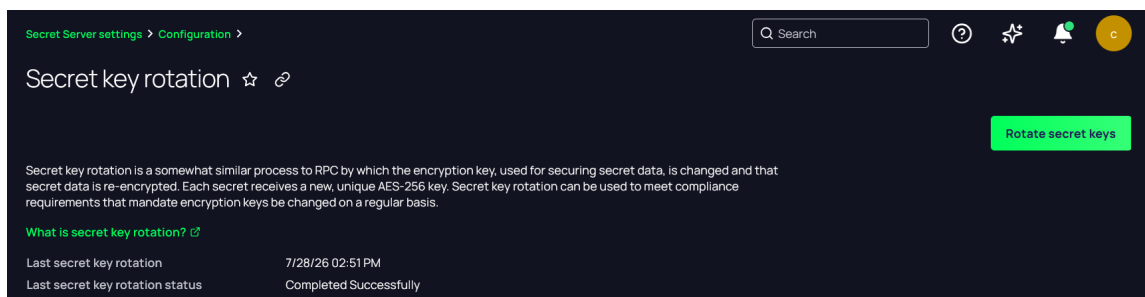
This completes the integration of the Delinea Platform with an AWS XKS protected by the Entrust nShield HSM. Secrets created in the Delinea Platform will use AWS XKS encryption keys protected by the HSM.

Chapter 4. Test the integration

1. Open a browser, navigate to the Delinea Platform, and sign in.
2. Type "Secret Key Rotation" in the search box. Then select **Secret Key Rotation** in the search results. Alternatively, in a browser navigate to <https://<delinea-platform>/view/vault/admin/configuration/security-secret-key-rotation>.
3. Note the last key rotation date and time. Then select **Rotate secret keys**.



4. In the **Confirm** window, select **Continue**.
5. Verify that the **Last secret key rotation** date has been updated.



Chapter 5. Additional resources and related products

5.1. nShield HSMs

5.2. nShield as a Service

5.3. Entrust products

5.4. nShield product documentation