Delinea Platform with AWS XKS

nShield® HSM Integration Guide

2026-08-13

© Entrust Corporation. All rights reserved.

Table of Contents

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

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 with the Delinea Platform.

For a list of supported nShield Security World Software versions and nShield HSMs, including firmware and images, refer to the Amazon Web Services KMS External Key Store (XKS): nShield® HSM Integration Guide, available at https://nshielddocs.entrust.com/.

1.2. 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

- AWS XKS overview
- Connection to the AWS XKS

2.1. AWS XKS 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.

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.

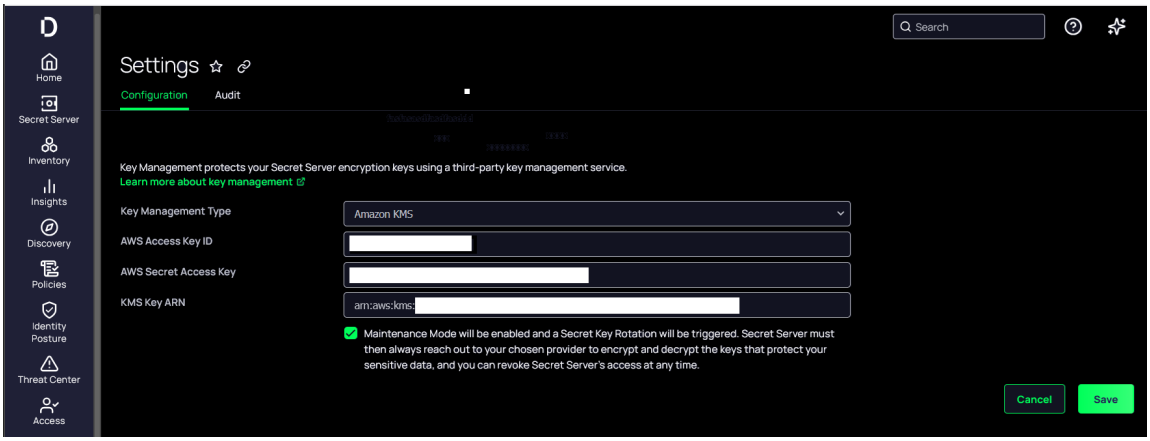
The deployment of the AWS XKS protected by the nShield HSM is covered in a separate document available at nShield Integration Guides.

2.2. Connection to the AWS XKS

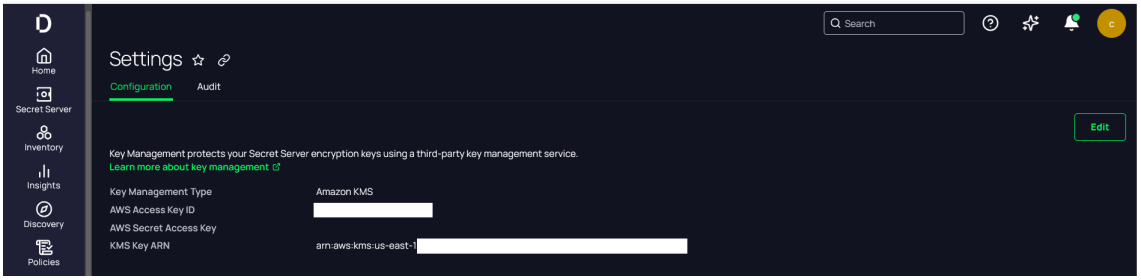
An encryption key was created in the AWS XKS, protected by a key in the nShield HSM. An AWS IAM user was created and granted permissions to the key in the AWS XKS. The key ARN, the IAM user access key, and the secret access key were shared with the Delinea Platform to establish a connection to the AWS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

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

1. In the Delinea Platform, navigate to the Key Management configuration window using an account with administrator privileges. The URL is https://<delinea-platform>/view/vault/admin/key-management/config.
2. Select the **Configuration** tab, then select **Edit**.
3. In the **Key Management Type** pull-down menu, select **Amazon KMS**.
4. Enter the AWS IAM user access key, secret access key, and the key ARN. Then select **Save**.



5. Verify that the configuration completed successfully.

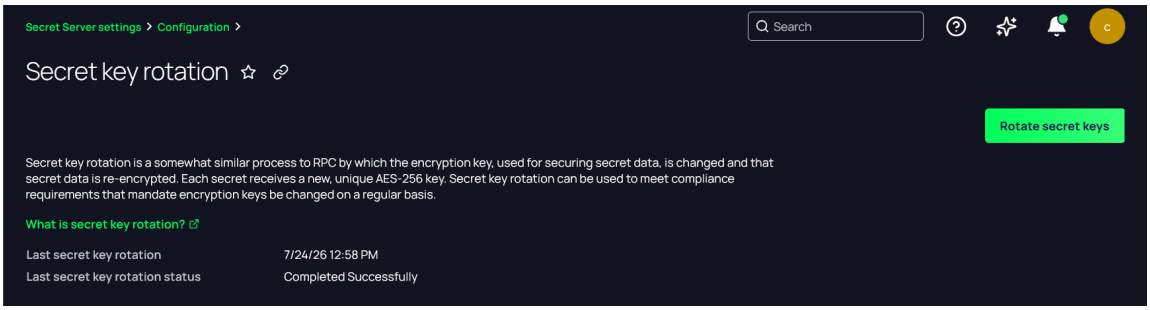


6. Select the **Audit** tab, then hover over the note to view the AWS KMS key ARN.

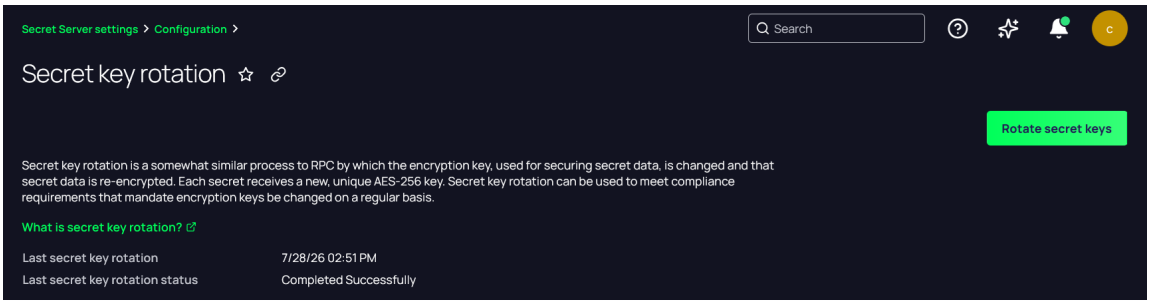
This completes the integration of the Delinea Platform with an AWS XKS protected by the Entrust nShield HSM. Secrets created in the Delinea Platform will use AWS XKS encryption keys protected by the HSM.

Chapter 4. Test the integration

1. In the Delinea Platform, navigate to the Secret Key rotation window using an account with administrator privileges. The URL is https://<delinea-platform>/view/vault/admin/configuration/security-secret-key-rotation.
2. Note the last key rotation date and time. Then select **Rotate secret keys**.



3. In the **Confirm** window, select **Continue**.
4. 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