Bring Your Own Key for Microsoft Azure Key Vault and Entrust CSP

Integration Guide

2026-11-02

Member of
Microsoft Intelligent Security Association

Microsoft Security

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Product configurations . . . 1
    1.2. Features tested . . . 1
    1.3. Requirements . . . 1
2. Install and configure the Entrust Key Management Vault . . . 3
    2.1. Deploy a Key Management Vault cluster . . . 3
    2.2. Create a vault for cloud keys in Key Management Vault . . . 3
3. Create an Azure key vault . . . 5
4. Configure Key Management Vault as a Microsoft Azure cryptographic service provider . . . 6
    4.1. Create an Azure client secret . . . 6
    4.2. Create a CSP account for Azure in Key Management Vault . . . 7
5. Test the integration . . . 9
    5.1. Create a key set in Key Management Vault . . . 9
    5.2. Create a cloud key in Key Management Vault . . . 11
    5.3. Create a cloud key in Azure Key Vault . . . 14
    5.4. Rotate a cloud key in Key Management Vault . . . 15
    5.5. Remove a cloud key in Key Management Vault . . . 16
    5.6. Upload a removed cloud key to Azure . . . 18
    5.7. Delete a cloud key in Key Management Vault . . . 19
    5.8. Cancel a cloud key deletion in Key Management Vault . . . 20
6. Additional resources and related products . . . 22
    6.1. nShield HSMs . . . 22
    6.2. nShield as a Service . . . 22
    6.3. KeyControl BYOK . . . 22
    6.4. Entrust products . . . 22
    6.5. nShield product documentation . . . 22

Chapter 1. Introduction

This document describes how to integrate Microsoft Azure Key Vault Bring Your Own Key (BYOK) with the Entrust Cryptographic Security Platform Key Management Vault (Key Management Vault). It provides instructions for configuring the Key Management Vault as a Key Management Service (KMS) for Azure BYOK.

The Key Management Vault provides a comprehensive solution for managing the lifecycle of cryptographic keys. In addition, it can be integrated with Entrust nShield HSMs to help organizations meet security and compliance requirements.

1.1. Product configurations

Entrust has successfully integrated the Key Management Vault with Azure BYOK in the following configurations:

System	Version
Entrust Cryptographic Security Platform	1.6.1

1.2. Features tested

Entrust has successfully tested the following features:

- Create cloud key
- Rotate cloud key
- Remove cloud key
- Upload removed cloud key
- Delete cloud key
- Cancel cloud key deletion

1.3. Requirements

- A Microsoft Azure subscription.
- Access to the Entrust TrustedCare Portal.
- A virtual environment or servers on which to deploy the Entrust CSP.

Familiarize yourself with the following:

- Microsoft Azure Key Vault online documentation.
- Cryptographic Security Platform 1.6 - Vault 10.6.1 installation, administration, and user guide online documentation.

Chapter 2. Install and configure the Entrust Key Management Vault

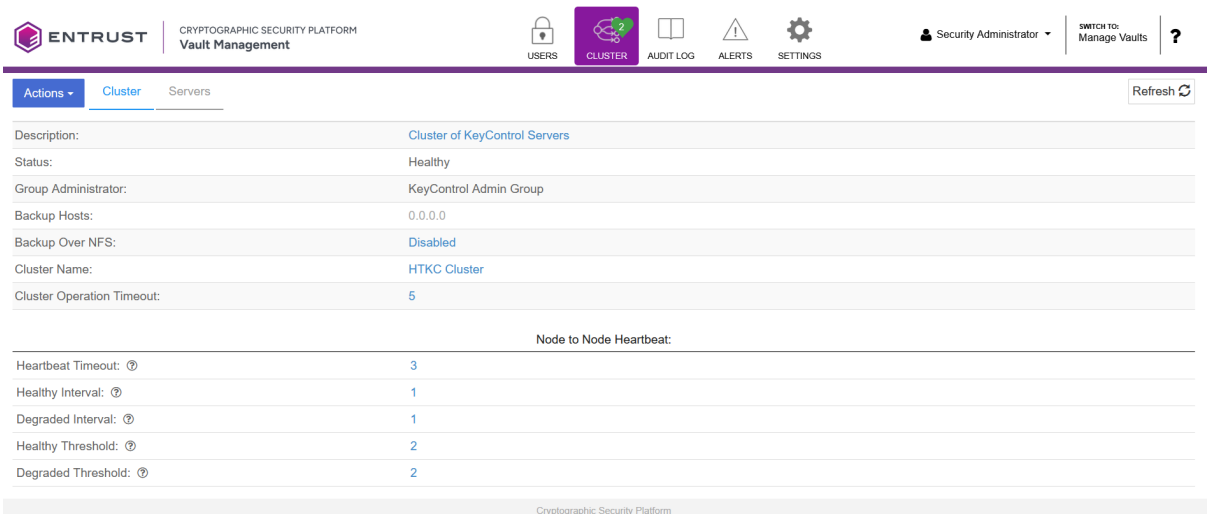
- Deploy a Key Management Vault cluster
- Create a vault for cloud keys in Key Management Vault

2.1. Deploy a Key Management Vault cluster

For this integration, Key Management Vault was deployed as a two-node vault cluster along with an Entrust Cryptographic Security Platform Compliance Manager (Compliance Manager) server. The vault cluster was configured in an active-active deployment and licensed with a 30-day trial license.

The Key Management Vault and Compliance Manager are software-based solutions available as either OVA or ISO images. Both components were deployed as virtual machines using the OVA images. For more details, see Installation Overview.

If you are using an HSM, see the Entrust Cryptographic Security Platform Key Management Vault: nShield® HSM Integration Guide for more information about integrating with the Entrust nShield HSM.

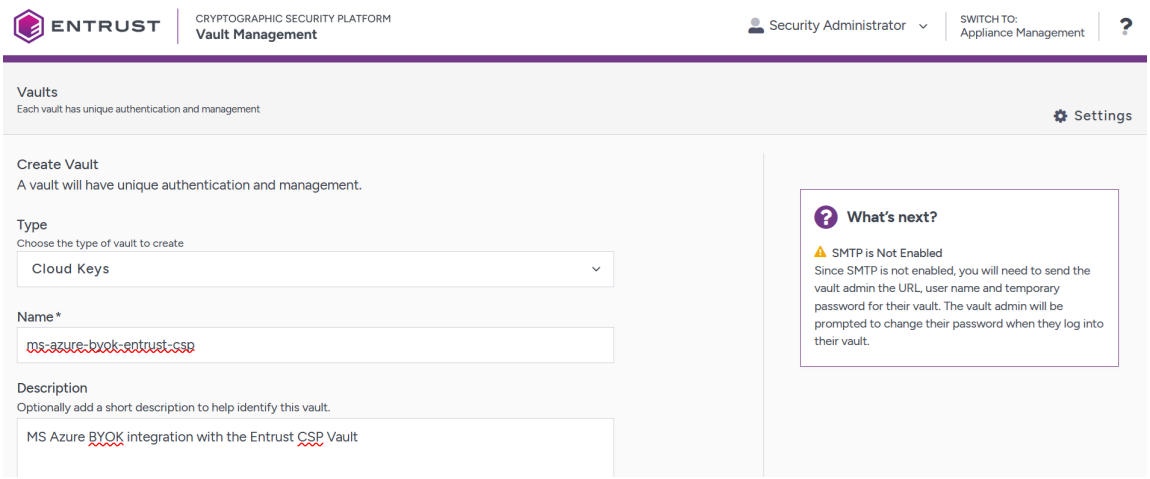


2.2. Create a vault for cloud keys in Key Management Vault

1. Sign in to Appliance Manger on the Key Management Vault server.
2. Select **Create Vault**.
   The **Create Vault** dialog appears.
3. From the **Type** drop-down menu, select **Cloud Keys** and enter the required

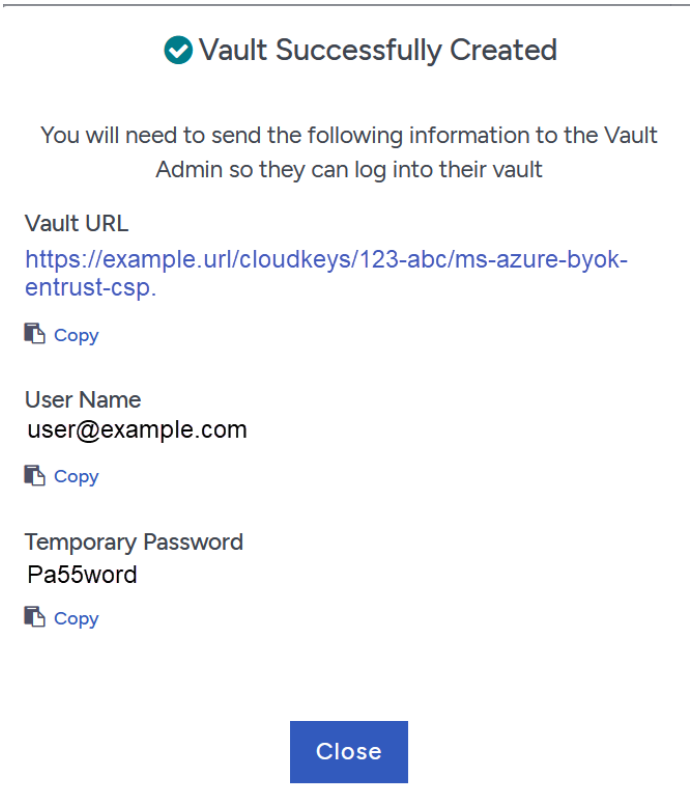
information, then select **Create Vault**.

For example:



4. Bookmark the URL and save the credentials displayed in the **Vault Successfully Created** window, then select **Close**.

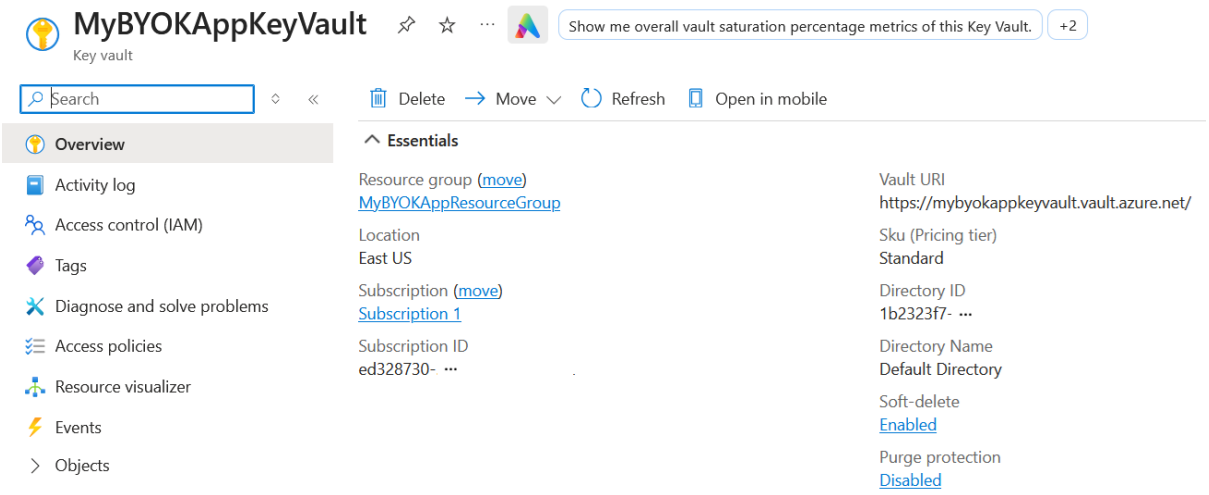
   For example:



5. Sign in to the bookmarked URL.
   Change the one-time password when prompted.

Chapter 3. Create an Azure key vault

For this integration, we created a Microsoft Azure service key vault. See Configuring Azure for Vault BYOK for details.



Chapter 4. Configure Key Management Vault as a Microsoft Azure cryptographic service provider

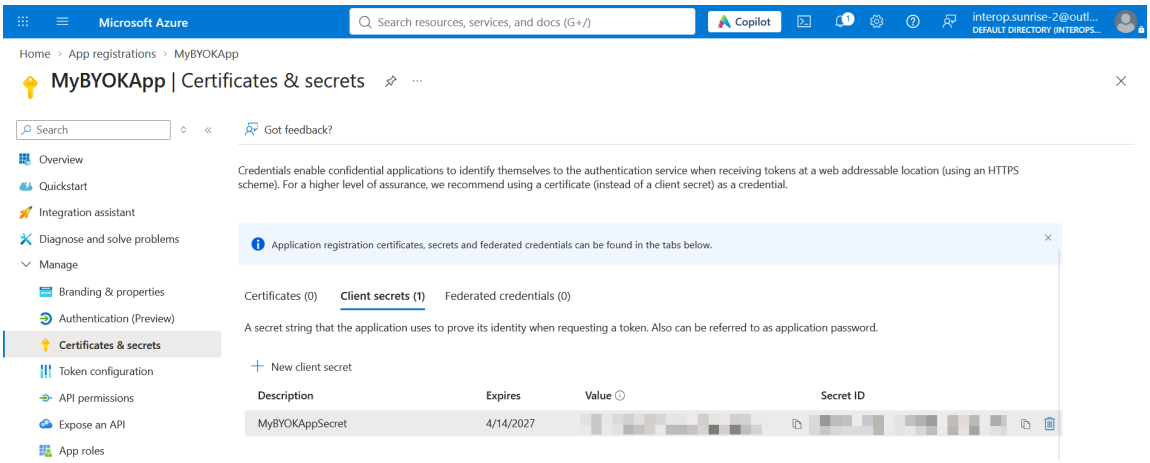
- Create an Azure client secret
- Create a CSP account for Azure in Key Management Vault

4.1. Create an Azure client secret

This secret is required to create a CSP account for Azure in Key Management Vault. It expires after a set period. You must create the CSP account for Azure in Key Management Vault before the secret expires.

1. Navigate to **App registrations** and select your App registration.
2. Select **Certificates & secrets** and create a **New client secret**.
   The **Add a client secret** dialog appears.
3. Enter a **Description** and select the expiration date.
4. Select **Add**.
   The **Certificates & secrets** window appears.

   For example:



5. Copy the **Value** of the new client secret and save it somewhere secure.

> You will not be able to retrieve this value again after navigating away from this page and must create a new secret if you lose it.

For additional information, see Creating a client secret in Azure Active Directory.

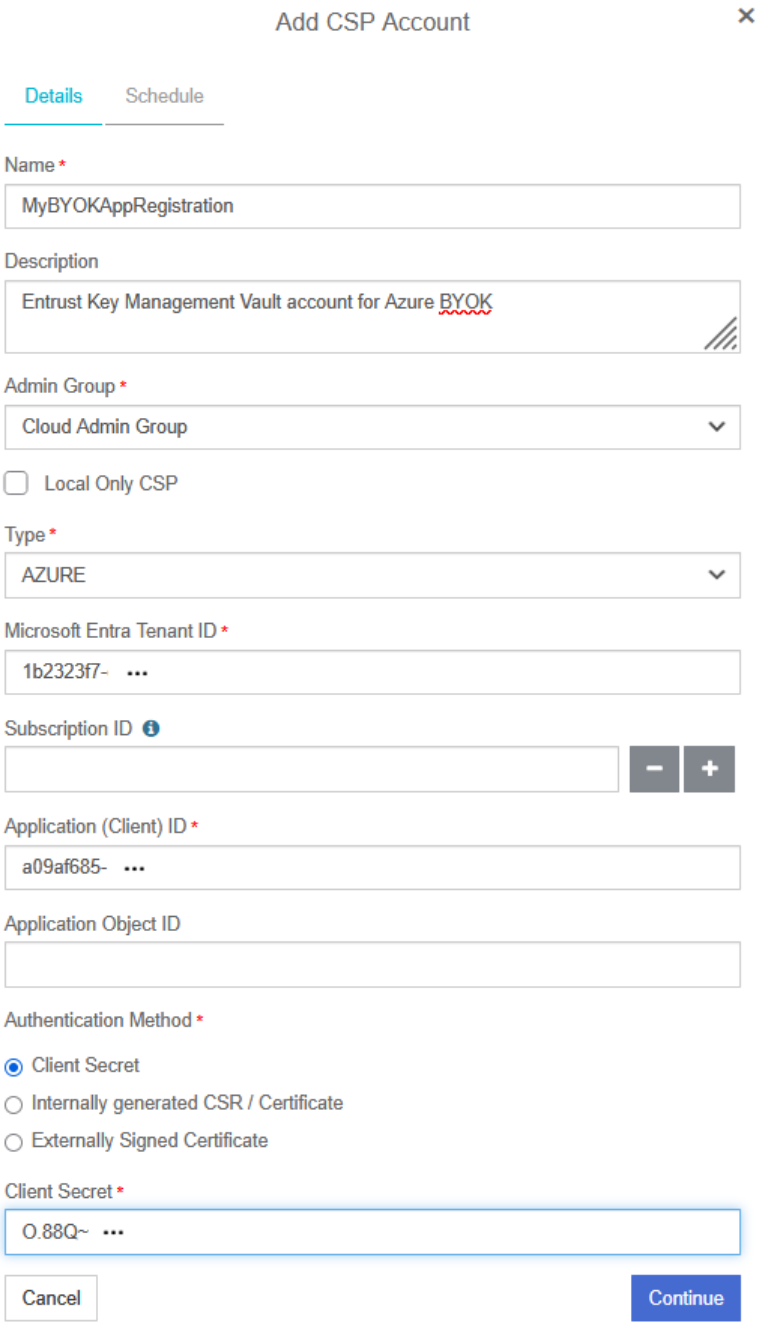
4.2. Create a CSP account for Azure in Key Management Vault

The following steps establish a connection between Key Management Vault and Azure, making Key Management Vault the cryptographic service provider of the Azure application.

1. Sign in to the Key Management Vault URL bookmarked from Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CSP Accounts** tab.
4. Select the **Action** icon, and then select **Add CSP Account** from the drop-down menu. The **Add CSP Account** dialog appears.
5. In the **Details** tab, enter a **Name** and **Description**.
6. From the **Admin Group** drop-down menu, select **Cloud Admin Group**.
7. From the **Type** drop-down menu, select **Azure**.
8. Enter the following values from the Azure account:

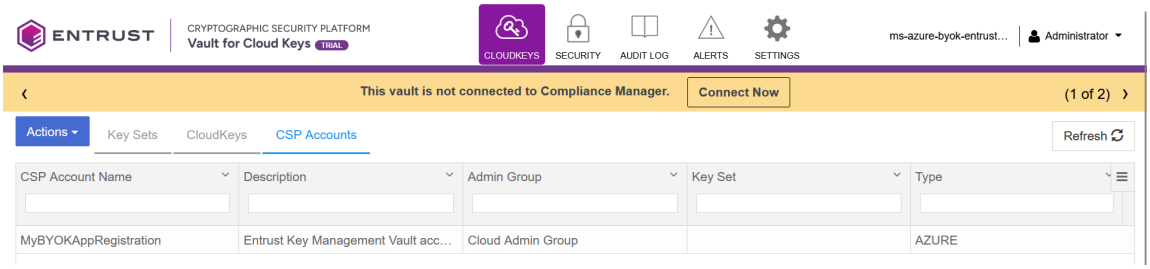
Item	Value
Microsoft Entra Tenant ID	**App registrations** / <app-registration> / Directory (tenant) ID
Application (Client) ID	**App registrations** / <app-registration> / Application (client) ID
Client Secret	**Value** of the secret created in Create an Azure client secret

For example:



9. Select **Continue**.
10. In the **Schedule** tab, define the rotation schedule and then select **Apply**.

    The new CSP account is created.



Chapter 5. Test the integration

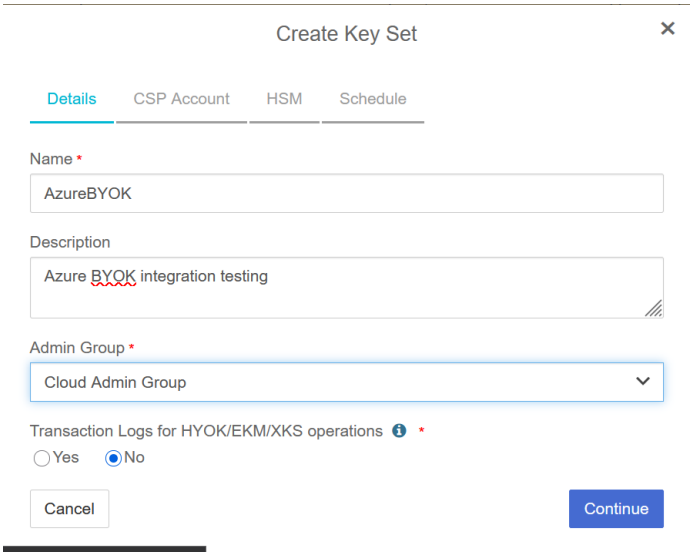
- Create a key set in Key Management Vault
- Create a cloud key in Key Management Vault
- Create a cloud key in Azure Key Vault
- Rotate a cloud key in Key Management Vault
- Remove a cloud key in Key Management Vault
- Upload a removed cloud key to Azure
- Delete a cloud key in Key Management Vault
- Cancel a cloud key deletion in Key Management Vault

5.1. Create a key set in Key Management Vault

This key set is used to create a cloud key in Key Management Vault.

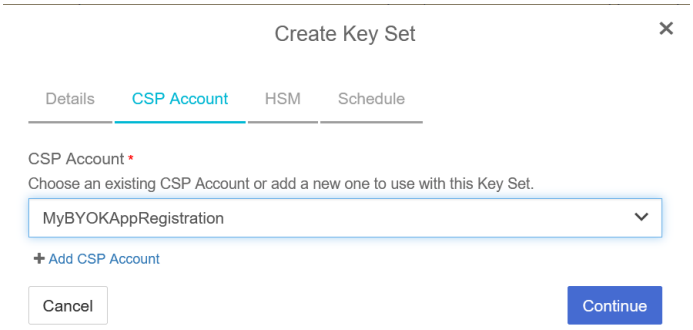
1. Sign in to the Key Management Vault you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **Key Sets** tab.
4. Select **Actions** > **Create Key Set**.
   The **Choose the type of keys...** dialog appears.
5. Choose **Azure Key**.
   The **Create Key Set** dialog appears.
6. In the **Details** tab, enter a **Name** and **Description**.
7. From the **Admin Group** drop-down menu, select **Cloud Admin Group**.

   For example:



8. Select **Continue**.
9. In the **CSP Account** tab, select the CSP account created in Create a CSP account for Azure in Key Management Vault.

   For example:



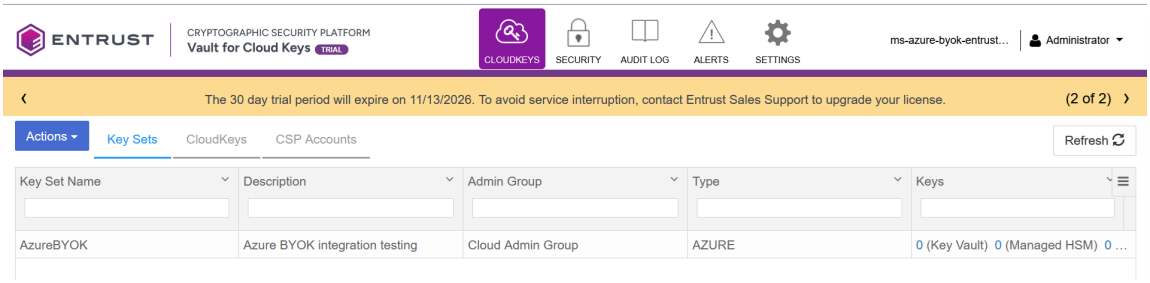
10. Select **Continue**.
11. If you are using an HSM, in the **HSM** tab, select **Enable HSM**, then select **Continue**.

    You must have configured the HSM before performing this step.

12. In the **Schedule** tab, select a **Rotation Schedule** matching the selection made during Create an Azure client secret then select **Apply**.

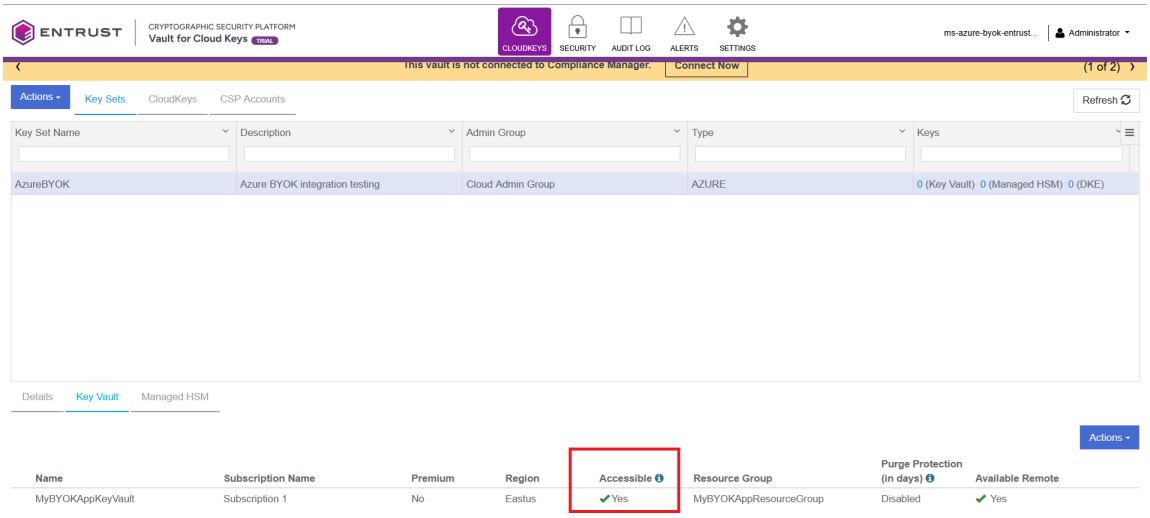
    The key set is added.

    For example:



13. Verify that the Azure Key Vault created in Create an Azure key vault is listed in the **Key Vault** tab with the setting **Accessible** set to **Yes**.

    For example:



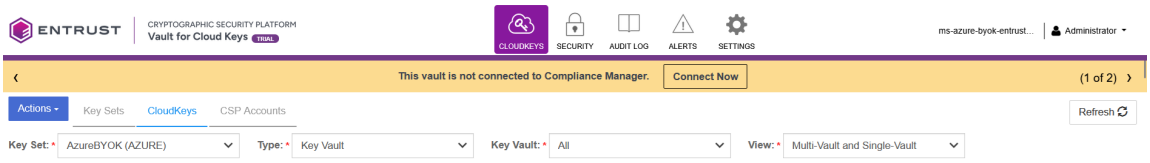
For more information, see Creating a Key Set.

5.2. Create a cloud key in Key Management Vault

The following steps create a cloud key in Key Management Vault and verify that it is available in Azure Key Vault.

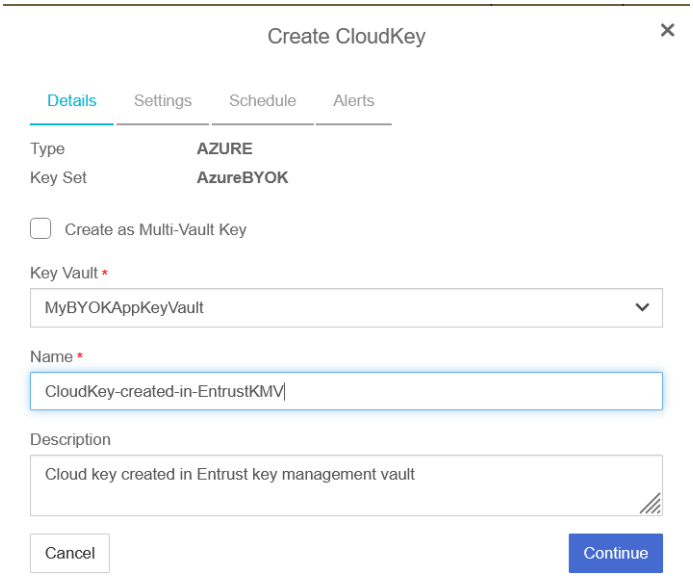
1. Sign in to the Key Management Vault you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in Create a key set in Key Management Vault.
5. In the **Type** menu, select **Key Vault**.

   For example:



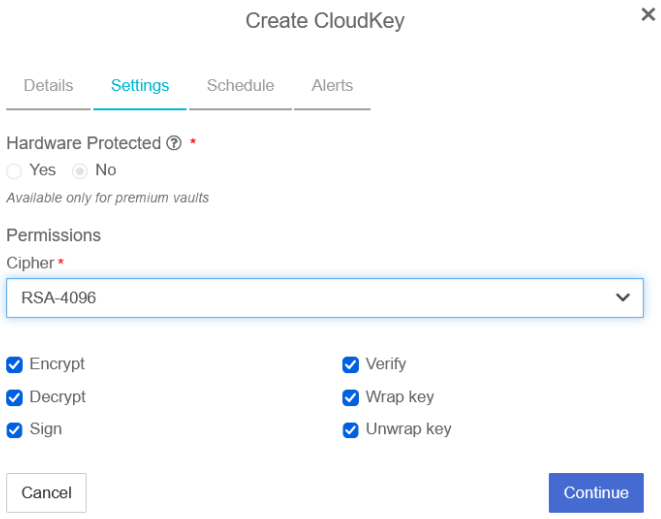
6. Select **Actions** > **Create CloudKey**. The **Create CloudKey** dialog appears.
7. In the **Key Vault** menu, select your Azure Key Vault.
   For this integration test, select the vault created in Create an Azure key vault.
8. In the **Details** tab, enter a **Name** and **Description**. Then select **Continue**.

   For example:



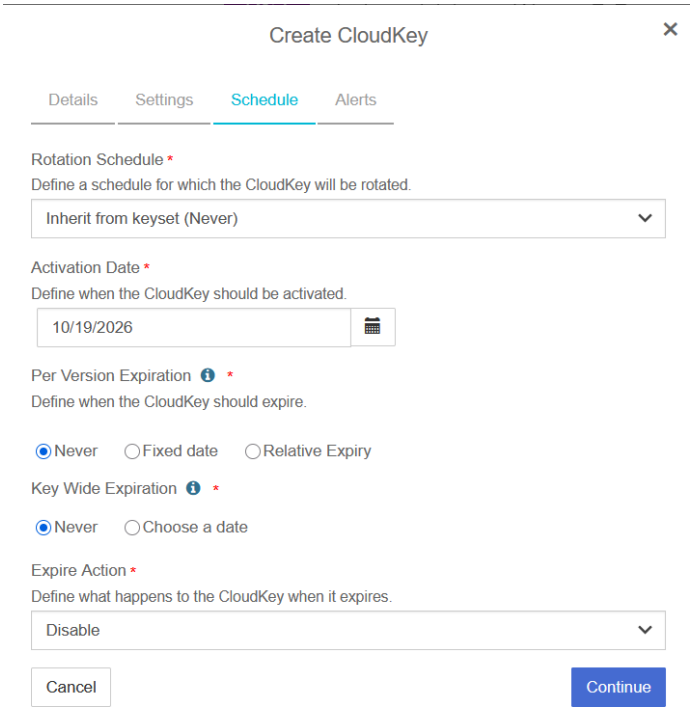
9. In the **Settings** tab, select the required **Cipher** and then select **Continue**.

   For example:



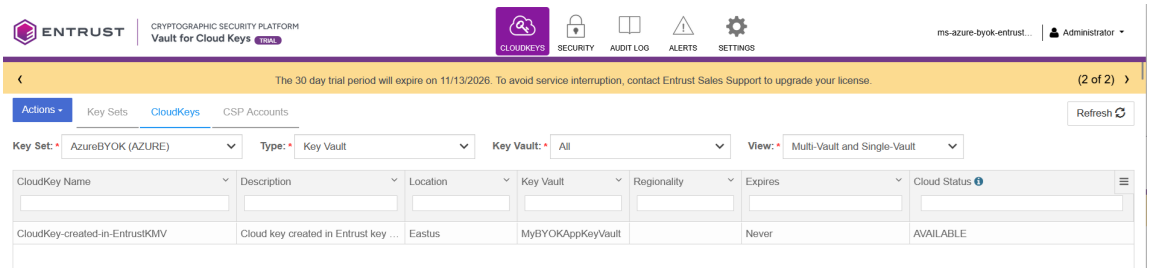
10. In the **Schedule** tab, select the **Rotation Schedule**, **Activation Date**, and **Expiration**, and then select **Continue**.

    For example:

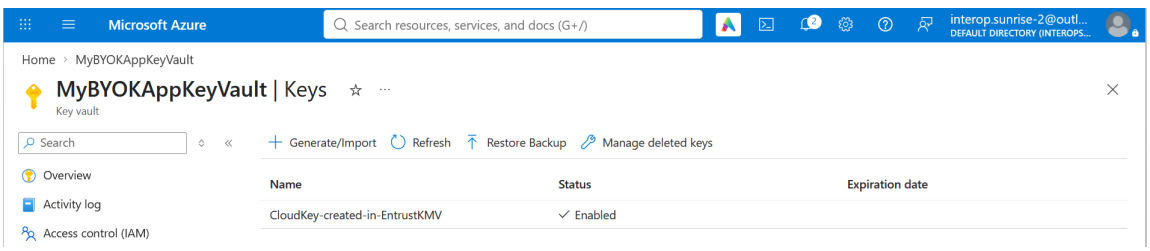


11. In the **Alerts** tab, configure the alerts as required then select **Apply**.

    The cloud key is created.



12. Verify that the cloud key created in Key Management Vault is available in Azure Key Vault.



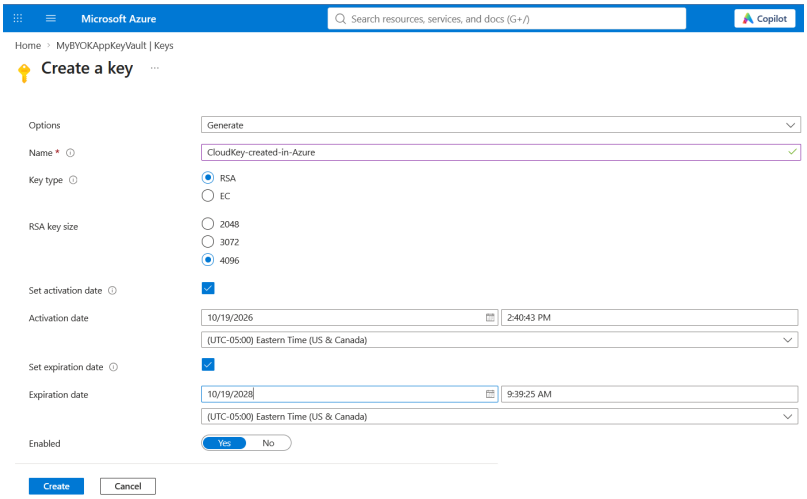
For additional information, see Creating a CloudKey.

5.3. Create a cloud key in Azure Key Vault

The following steps create a cloud key in Azure Key Vault and import it into Key Management Vault.

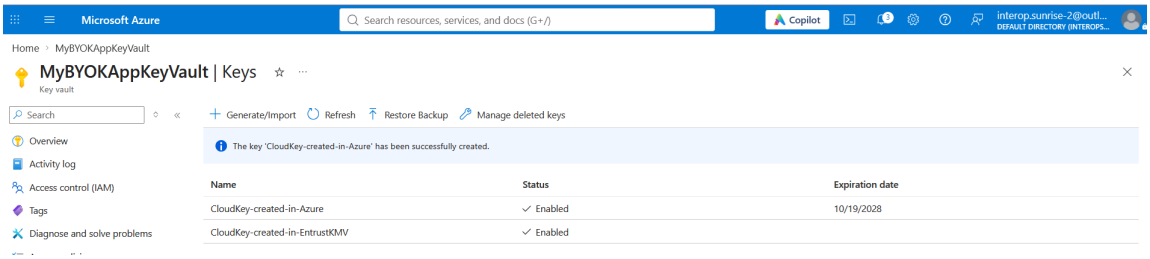
1. Navigate to **Home** > **Key vaults** > **<key-vault>** > **Keys** > **Generate/Import**.
   The **Create a key** dialog appears.
2. Enter a **Name** and configure the required key properties, then select **Create**.

   For example:



3. Verify the newly created key.

   For example:

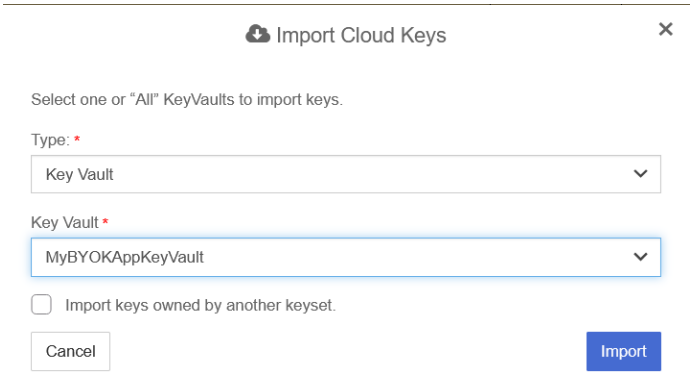


To import the cloud key created in Azure into Key Management Vault:

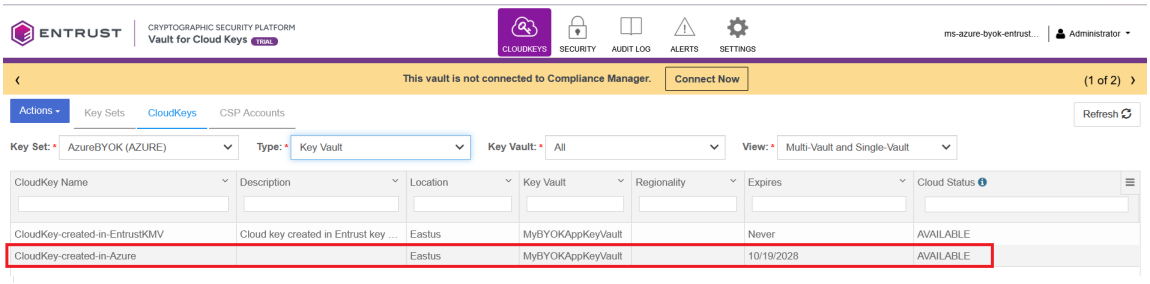
1. Sign in to the Key Management Vault URL you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **Key Sets** tab.
4. Select the key set created in Create a key set in Key Management Vault.
5. Select **Actions** > **Import CloudKey**.
   The **Import Cloud Keys** dialog appears.

6. In the **Type** menu, select **Key Vault**.
7. In the **Key Vault** menu, select your Azure Key Vault then select **Import**.
   For this integration test, select the vault created in Create an Azure key vault.

   For example:



8. Verify that the cloud key created in Azure Key Vault is available in Key Management Vault.

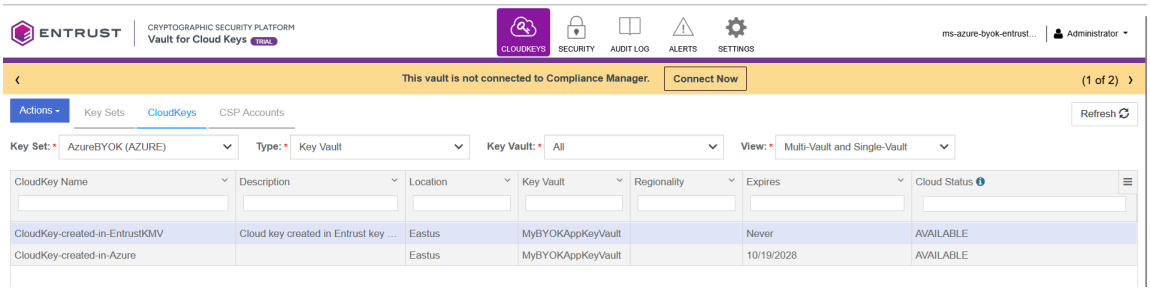


5.4. Rotate a cloud key in Key Management Vault

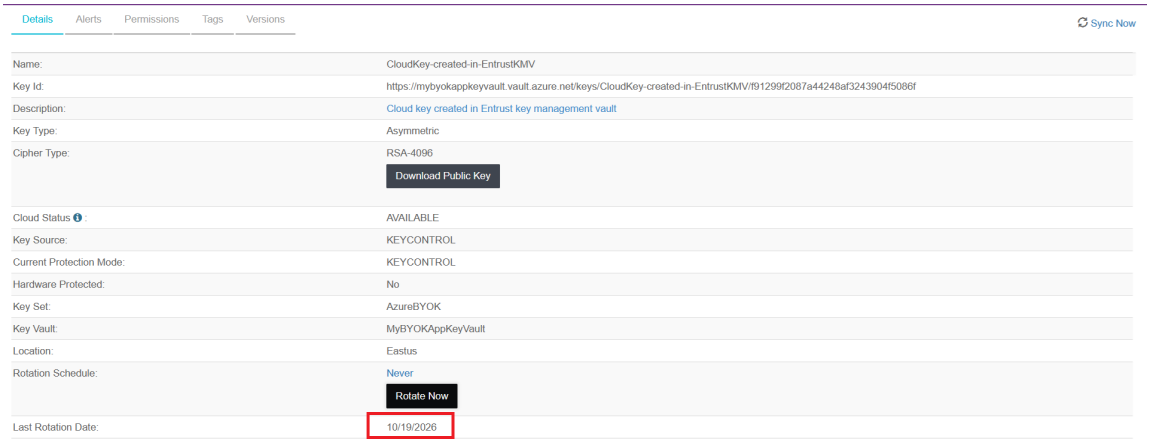
1. Sign in to the Key Management Vault URL you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in Create a key set in Key Management Vault.
5. In the **Type** menu, select **Key Vault**.
6. Select the key to rotate and then scroll down until you see the **Rotate Now** control. Make a note of the **Last Rotation date**.
7. Select **Rotate Now**.

   Verify that the **Last Rotation date** has been updated.

For example:

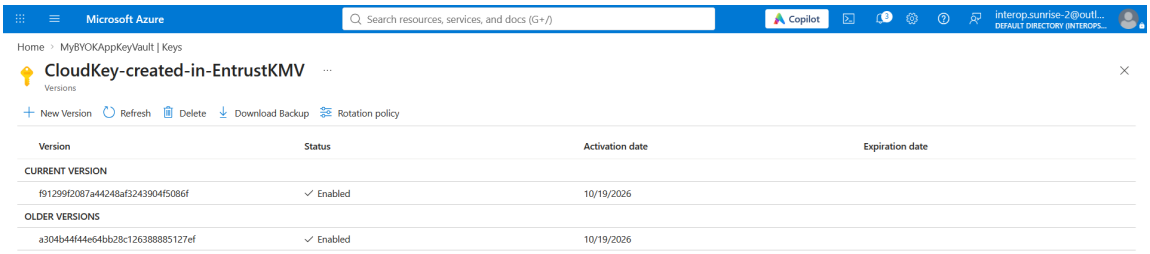


...



8. In Azure, navigate to **Home** > **Key vaults** > **<key-vault>** > **Keys**.
9. Select the key that you rotated in Key Management Vault.
10. Compare the **OLDER VERSIONS** with the **CURRENT VERSION** to verify that the key has been rotated.

    For example:



For additional information, see Rotating keys.

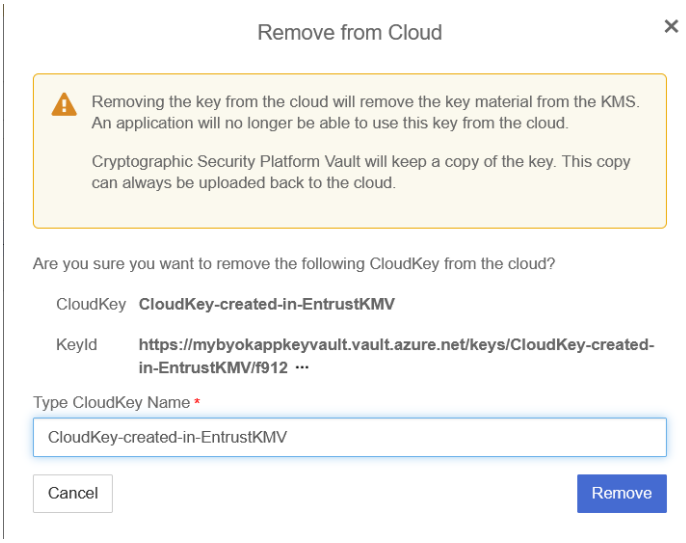
5.5. Remove a cloud key in Key Management Vault

A removed cloud key is no longer be available for use in Azure. However, Key Management Vault keeps a copy of the removed cloud key, which can be reloaded to Azure and will be

available for use again.

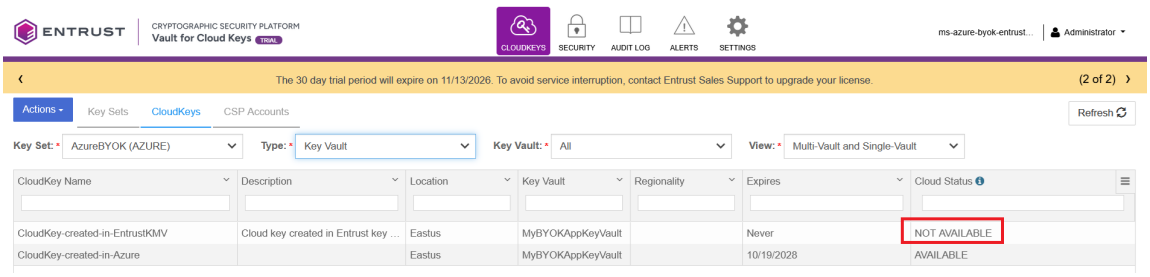
1. Sign in to the Key Management Vault URL you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in Create a key set in Key Management Vault.
5. In the **Type** menu, select **Key Vault**.
6. Select the key to be removed.
7. Select **Actions** > **Remove from Cloud**.
   The **Remove from Cloud** dialog appears.
8. Enter the name of the cloud key in **Type CloudKey Name**, then select **Remove**.

   For example:



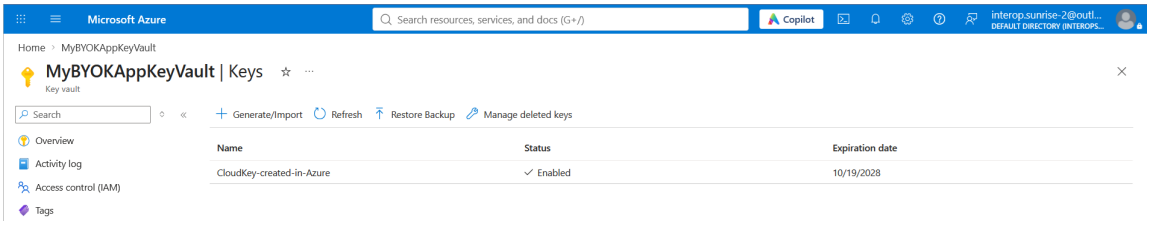
9. Verify the status change in Key Management Vault.

   For example:



10. Verify that the key is no longer available in Azure.

For example:

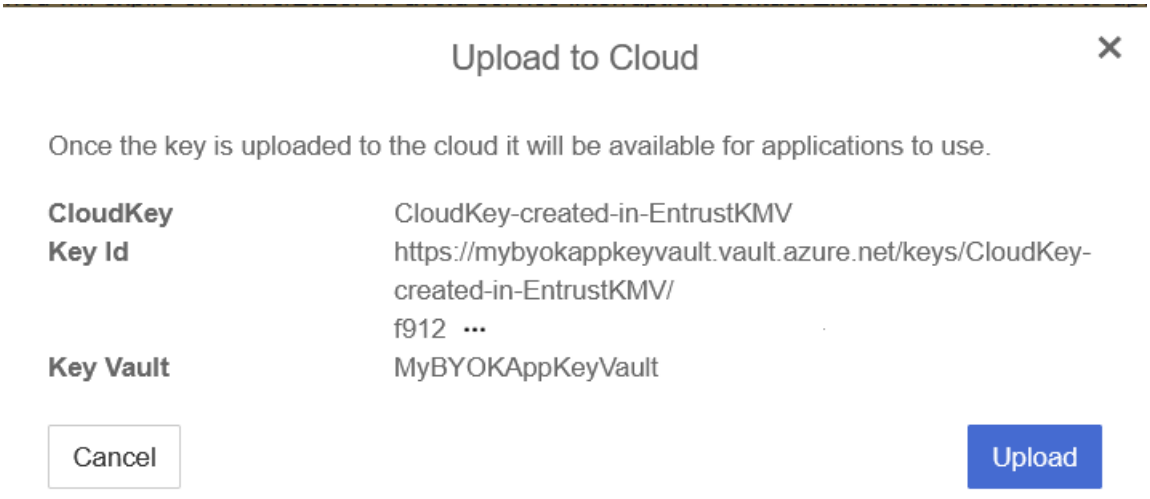


For additional information, see Removing a CloudKey.

5.6. Upload a removed cloud key to Azure

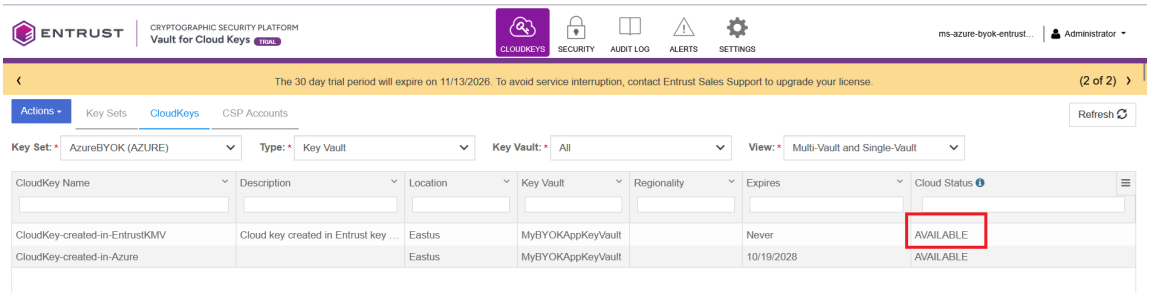
1. Sign in to the Key Management Vault you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in Create a key set in Key Management Vault.
5. In the **Type** menu, select **Key Vault**.
6. Select the key to be uploaded.
7. Select **Actions** > **Upload to Cloud**.
8. In the **Upload to Cloud** dialog, select **Upload**.

   For example:



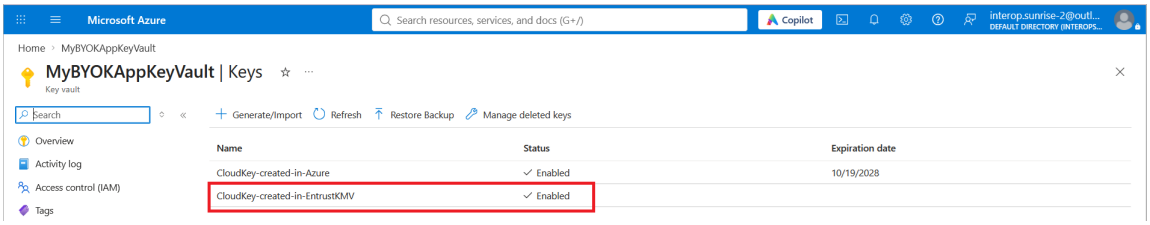
9. Verify the status change in Key Management Vault.

   For example:



10. Verify that the key is now available in Azure.

    For example:

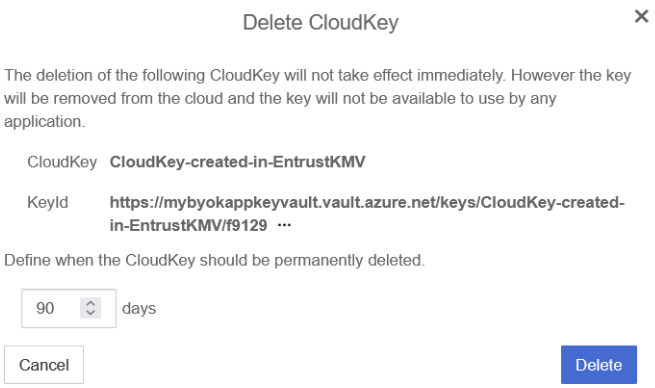


5.7. Delete a cloud key in Key Management Vault

The deletion of a cloud key does not take effect immediately. When deleting a key, you specify the period after which the key will be permanently deleted.

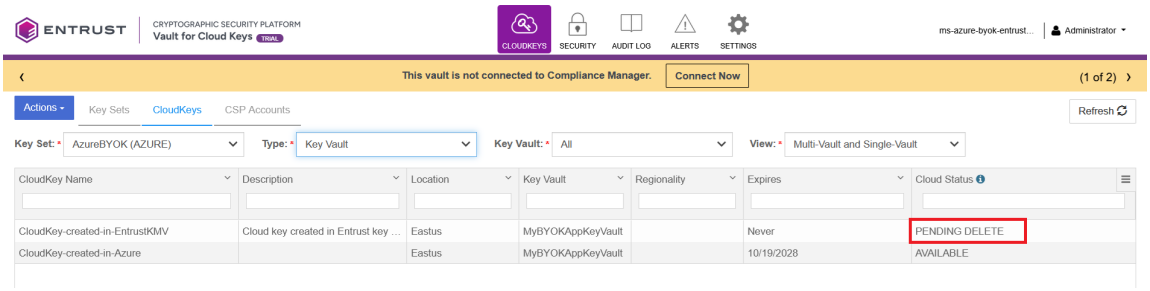
1. Sign in to the Key Management Vault you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in Create a key set in Key Management Vault.
5. In the **Type** menu, select **Key Vault**.
6. Select the key to be deleted.
7. Select **Actions** > **Delete CloudKey**.
   The **Delete CloudKey** dialog appears.
8. Select a period of time after which the key will be permanently deleted in **Define when the CloudKey should be permanently deleted**, then select **Delete**.

   For example:



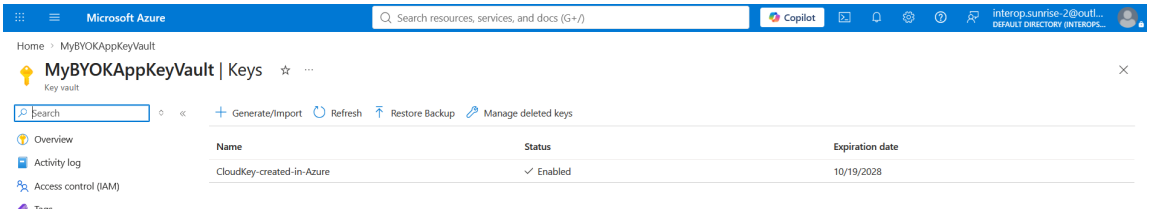
9. Verify that the status has changed to "PENDING DELETE" in Key Management Vault.

   For example:



10. Verify that the key is no longer available in Azure.

    For example:



For additional information, see Deleting a CloudKey.

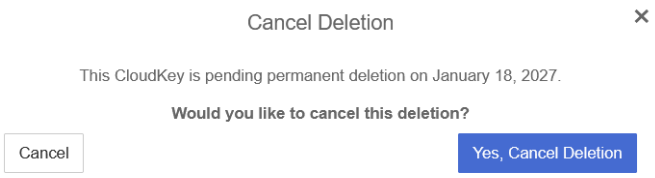
5.8. Cancel a cloud key deletion in Key Management Vault

You can cancel key deletion before the period specified in **Define when the CloudKey should be permanently deleted** expires.

1. Sign in to the Key Management Vault you created a bookmark for in Create a vault for cloud keys in Key Management Vault.
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.

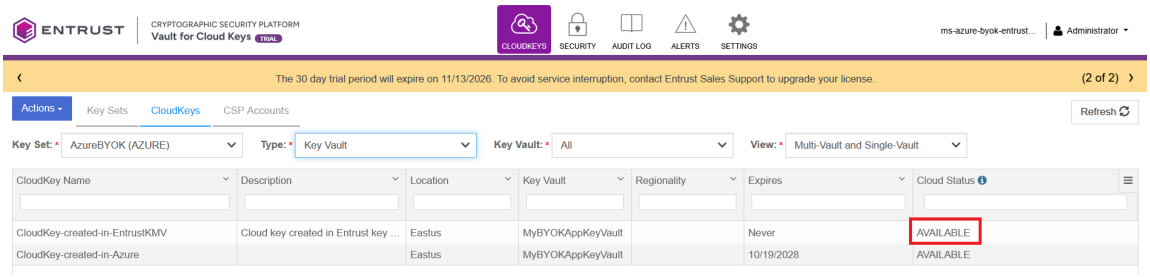
4. In the **Key Set** menu, select the **Key Set** created in Create a key set in Key Management Vault.
5. In the **Type** menu, select **Key Vault**.
6. Select the key that you no longer want to delete.
7. Select **Actions** > **Cancel Deletion**.
8. In the **Cancel Deletion** dialog, select **Yes, Cancel Deletion**.

   For example:



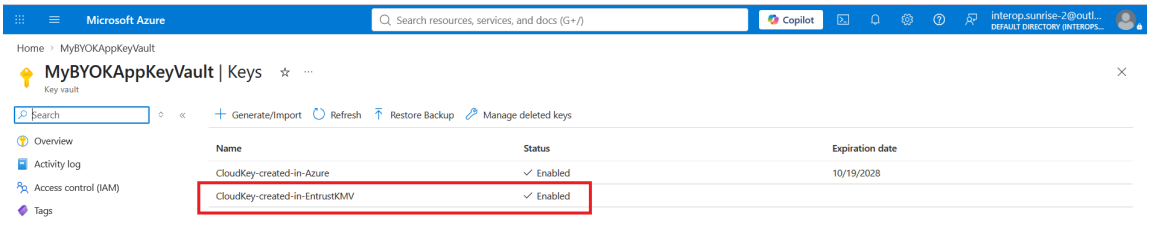
9. Verify that the status has changed back to "AVAILABLE" in Key Management Vault.

   For example:



10. Verify the key is now available in Azure.

    For example:



For additional information, see Canceling a CloudKey Deletion.

Chapter 6. Additional resources and related products

6.1. nShield HSMs

6.2. nShield as a Service

6.3. KeyControl BYOK

6.4. Entrust products

6.5. nShield product documentation