Bring Your Own Key for AWS Key Management Service and Entrust KeyControl

Integration Guide

2024-11-21

Table of Contents

Chapter 1. Introduction

This document describes the integration of AWS Bring Your Own Key (referred to as AWS BYOK in this guide) with the Entrust KeyControl key management solution (KMS). KeyControl serves as a key manager for cloud keys and KMIP objects.

1.1. Product configurations

Entrust has successfully tested the integration of KeyControl with AWS BYOK in the following configurations:

System	Version
Entrust KeyControl	10.3.1

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- AWS Key Management Service
- Entrust KeyControl Online Documentation Set

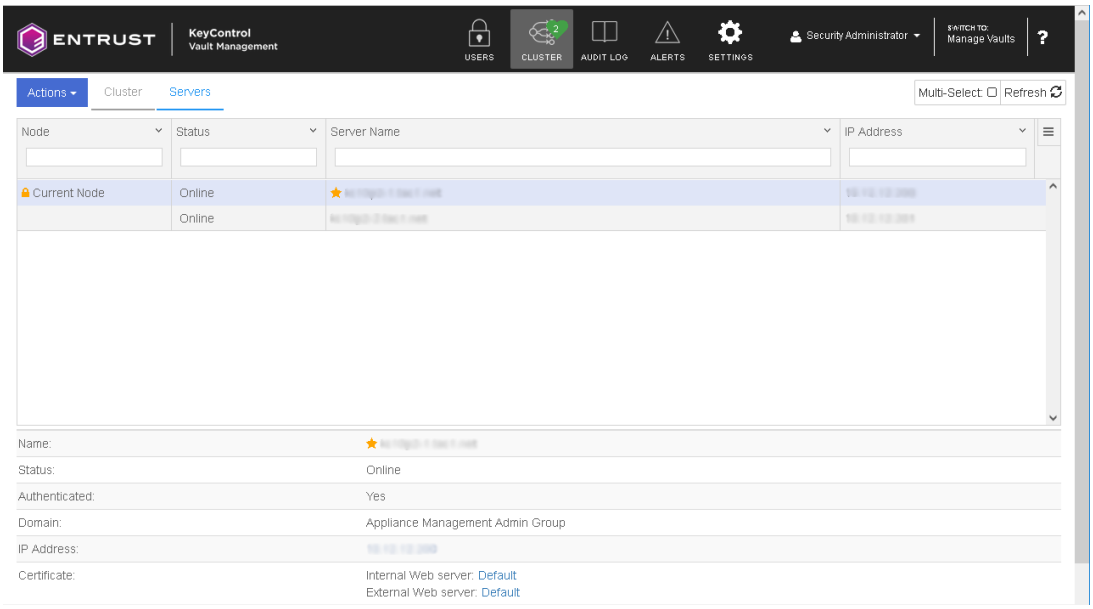
Chapter 2. Deploy and configure KeyControl

2.1. Deploy a KeyControl cluster

For the purpose of this integration, a two-node cluster was deployed as follows:

1. Download the KeyControl software from Entrust TrustedCare. This software is available as an OVA or ISO image. This guide deploys an OVA installation.
2. Install KeyControl as described in KeyControl OVA Installation.
3. Configure the first KeyControl node as described in Configuring the First KeyControl Node (OVA Install).
4. Add second KeyControl node to cluster as described in Adding a New KeyControl Node to an Existing Cluster (OVA Install).

Both nodes need access to an NTP server, otherwise the above operation will fail. Sign in to the console to change the default NTP server if required.



5. Install the KeyControl license as described in Upgrading Your Trial License.

2.2. Additional KeyControl cluster configuration

After the KeyControl cluster is deployed, additional system configuration can be done as described in KeyControl System Configuration.

2.3. Configure authentication

This guide uses local account authentication.

For AD-managed Security groups, configure the LDAP/AD Authentication Server as described in Specifying an LDAP/AD Authentication Server.

2.4. Create DNS record for the KeyControl cluster

This guide uses the individual IP addresses of the KeyControl nodes.

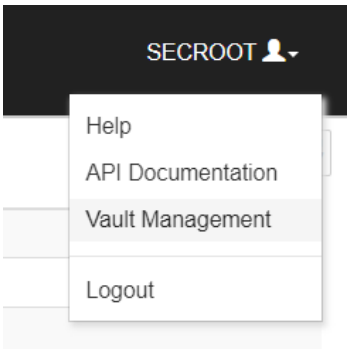
To use hostnames, configure your DNS server giving each node in the KeyControl a unique name.

2.5. Create a Cloud Keys Vault in the KeyControl

The KeyControl Vault appliance supports different type of vaults. For example: cloud key management, KMIP, PASM, database, and others. This section describes how to create a Cloud Keys vault for this integration.

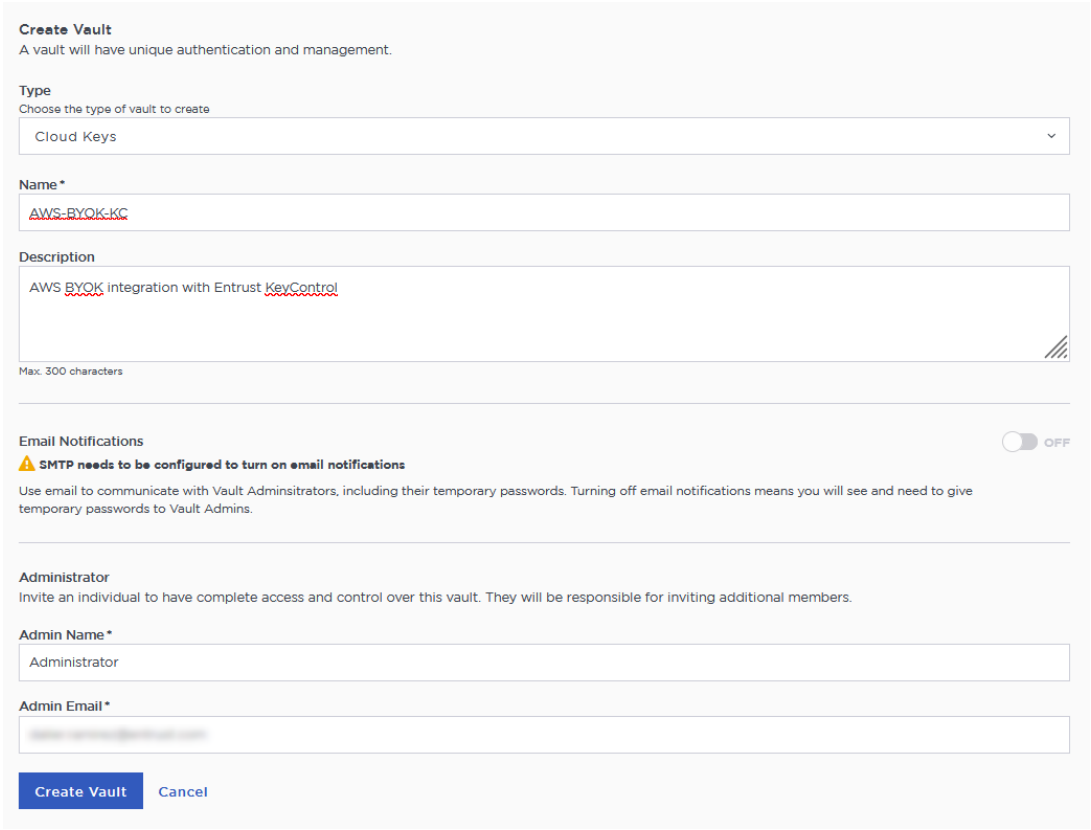
Refer to the Creating a Vault section of the admin guide for more details.

1. Sign in to the KeyControl Vault Server web user interface:
   a. Use your browser to access the IP address of the server.
   b. Sign in using the **secroot** credentials.
2. From the user's dropdown menu, select **Vault Management**.



3. In the KeyControl Vault Management interface, select the **Create Vault** icon.
4. In the **Create Vault** page, select **Cloud Keys**. Then enter your information.

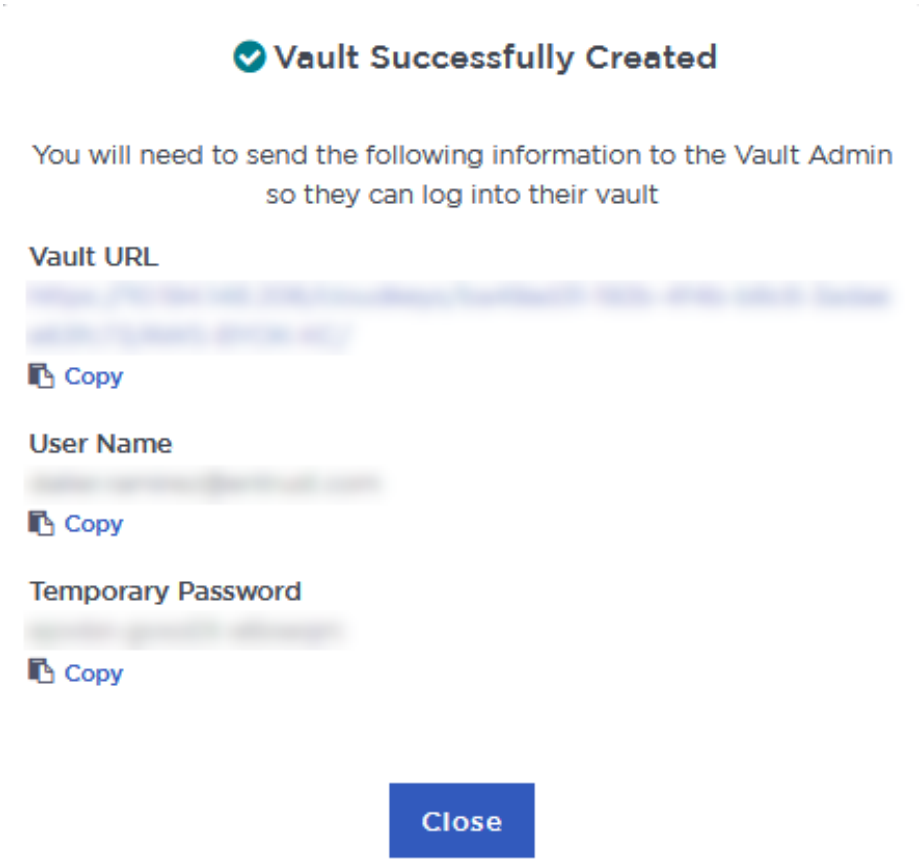
   For example:



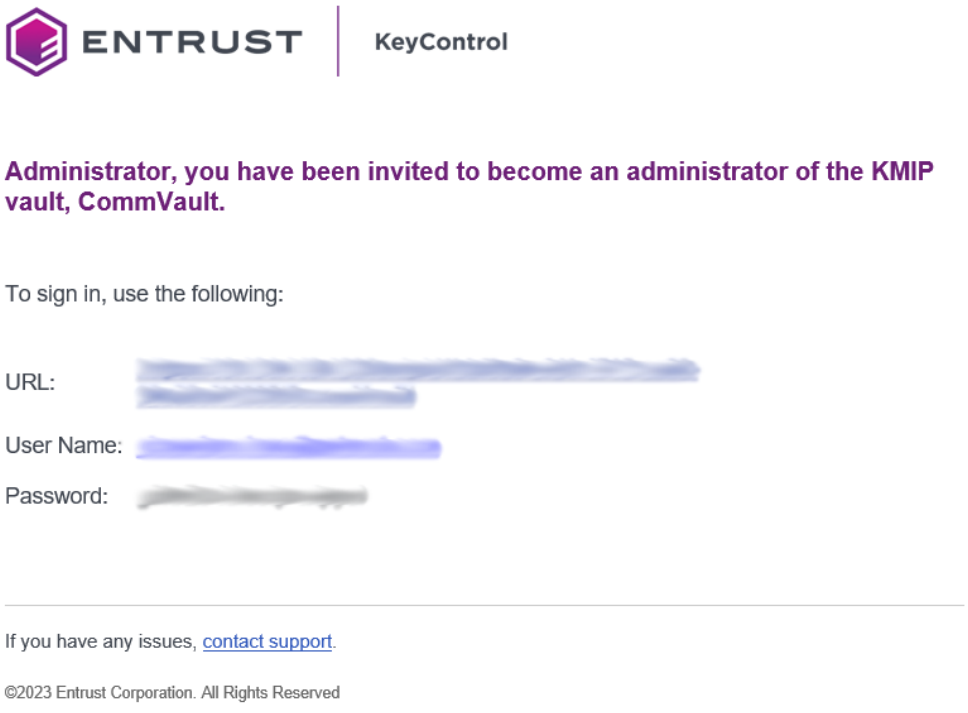
5. Select **Create Vault**, then select **Close**.

   A window with the newly created vault information appears. In addition, an email with the same vault information is sent to the security administrator **secroot**.

   Example vault information window:



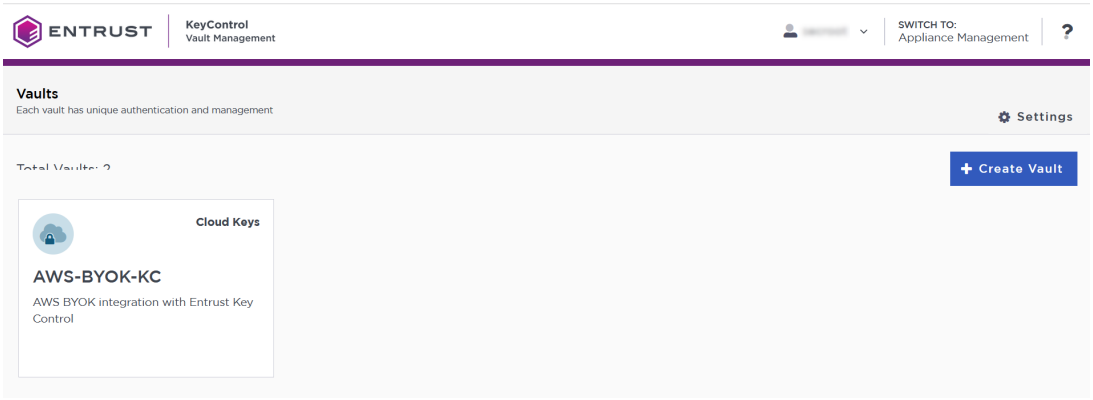
Example email:



6. Bookmark the **Vault URL** listed above.

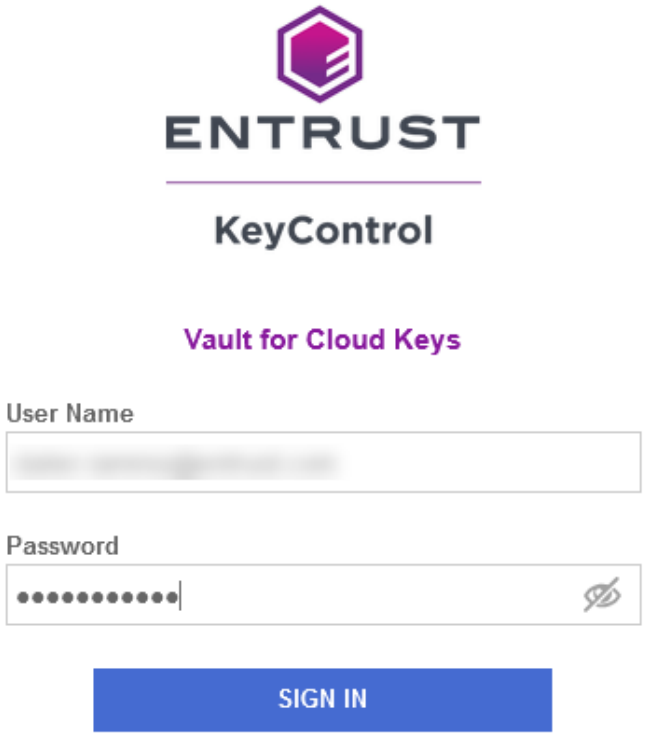
   The newly created Vault is added to the **Vault Management** dashboard.

   For example:



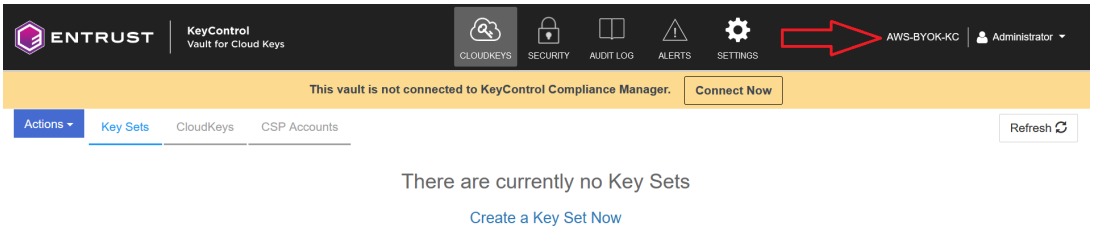
7. Sign in to the **Vault URL** with the temporary password. Change the initial password when prompted. Sign in again to verify.

   For example:



8. Notice the new vault.

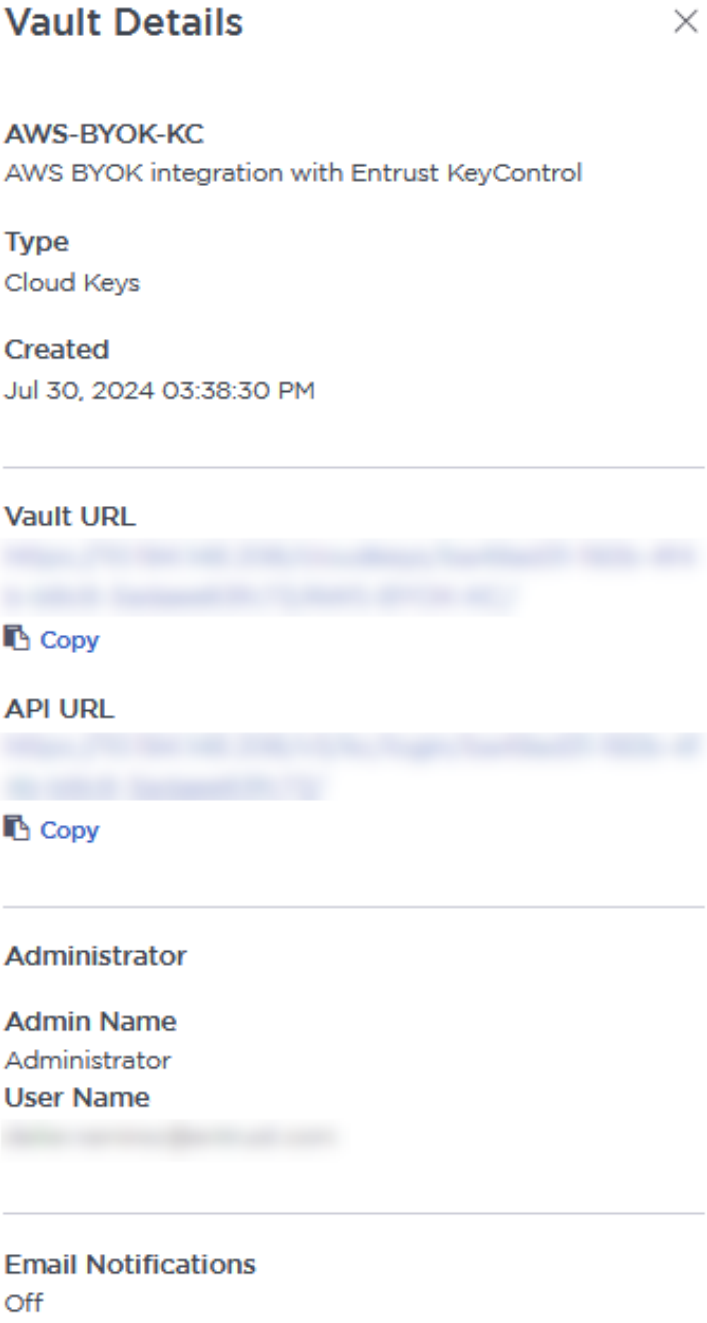
   For example:



2.6. View the Cloud Keys Vault details

1. Back in the **Vault Management** dashboard, hover over the Vault and select **View Details**.

   For example:



2. Select **Close** when done.

Chapter 3. Create a AWS AIM user service account

Entrust KeyControl utilizes an AWS IAM user service account to perform the KMS functionality in BYOK.

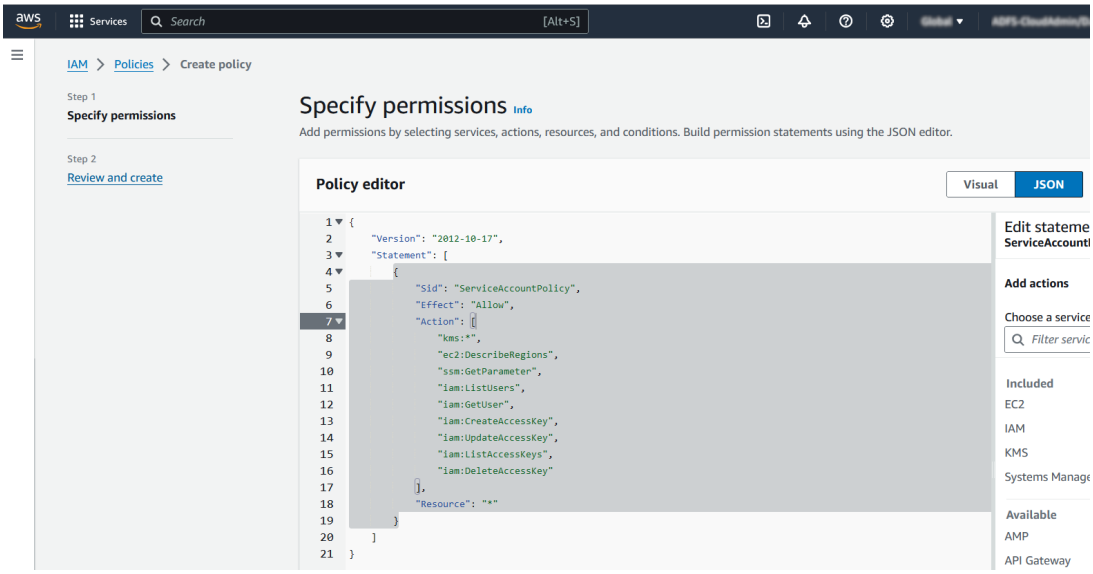
In addition to the IAM user service account, the feature to utilize an AWS domain user to perform the KMS functionality is under consideration for a future release of Entrust KeyControl.

The following steps create a customer managed policy in AWS. Then create an IAM user service account with the customer managed policy.

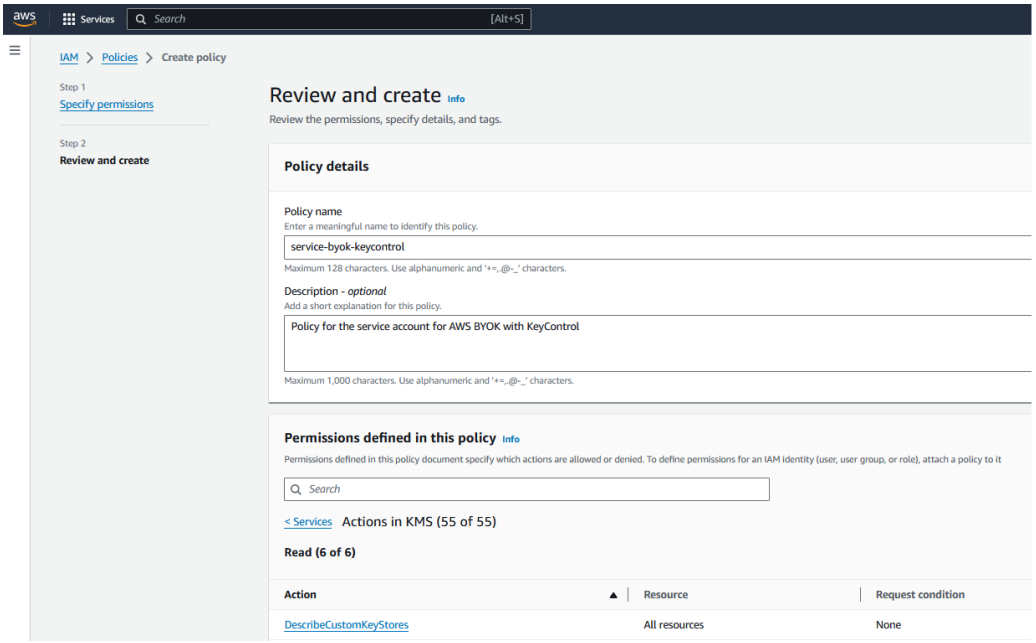
3.1. Create a AWS BYOK service account policy

1. Select **Services** / **IAM**.
2. In the left pane select **Access management** / **Policies**. Then select the **Create policy** icon.
3. In the **Specify permissions** window, select the **JASON** icon.
4. Copy the following in the **policy editor** window. Then select **Next**

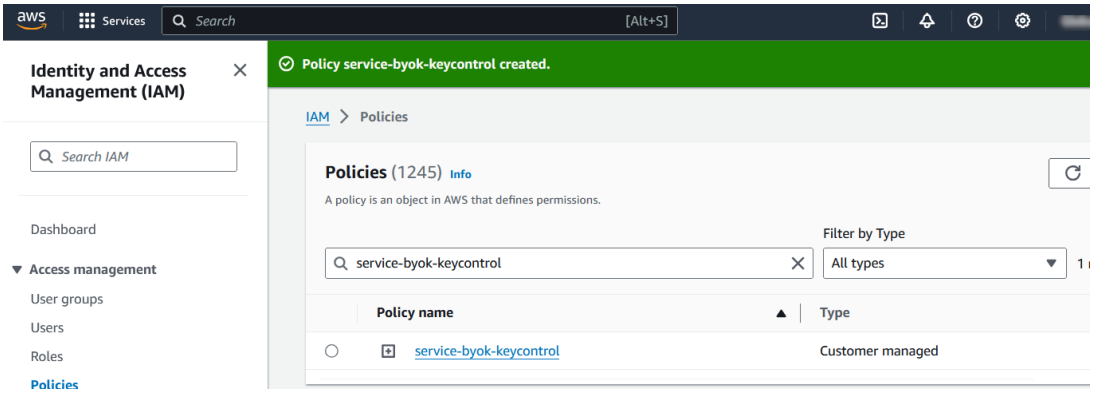
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ServiceAccountPolicy",
            "Effect": "Allow",
            "Action": [
                "kms:*",
                "ec2:DescribeRegions",
                "ssm:GetParameter",
                "iam:ListUsers",
                "iam:GetUser",
                "iam:CreateAccessKey",
                "iam:UpdateAccessKey",
                "iam:ListAccessKeys",
                "iam:DeleteAccessKey"
            ],
            "Resource": "*"
        }
    ]
}
```



5. In the **Review and create** window, enter a name and description.
6. In the **Permissions defined for this policy** section, select **KMS**. Then select **Create policy**.



7. Notice the new policy created.



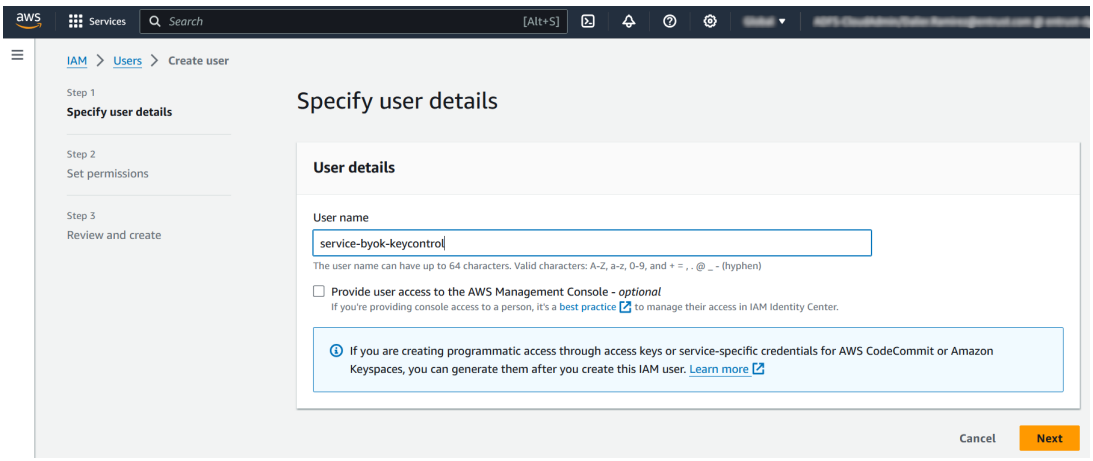
For further information, refer to the AWS BYOK Service Account Requirements.

3.2. Create AWS AIM user service account

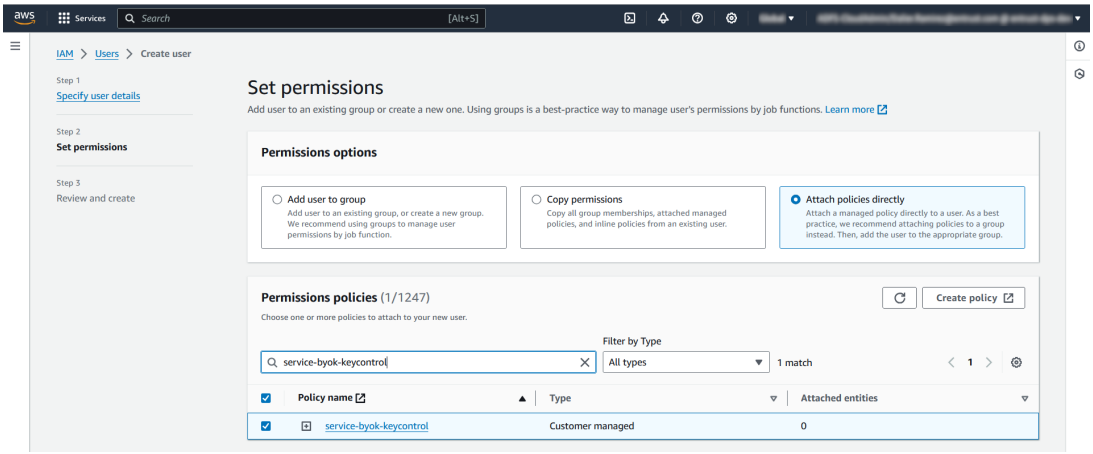
This steps create an AWS IAM user with no console access, a service account, with policy created in Create a AWS BYOK service account policy.

1. Select **Services** / **IAM**.
2. In the left pane select **Access management** / **Users**. Then select the **Create user** icon.
3. Enter the user name. Uncheck **Provide user access to AWS Management Console - optional** since we are creating a service account. Then select **Next**.

   For example:



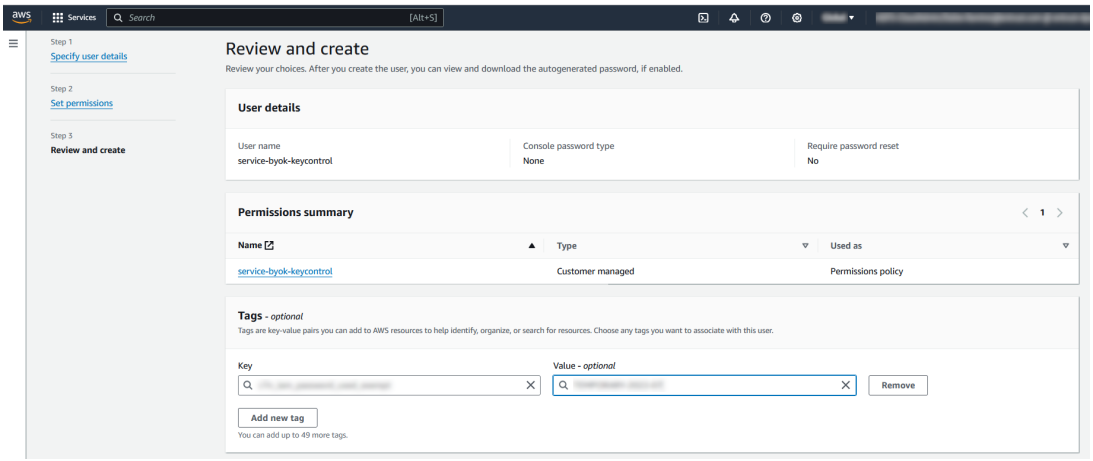
4. In the **Set permissions** window, select the **Attach policies directly** radio button.
5. In the **Permissions policy** section, enter the policy created in Create a AWS BYOK service account policy. Check the policy. Then select **Next**.



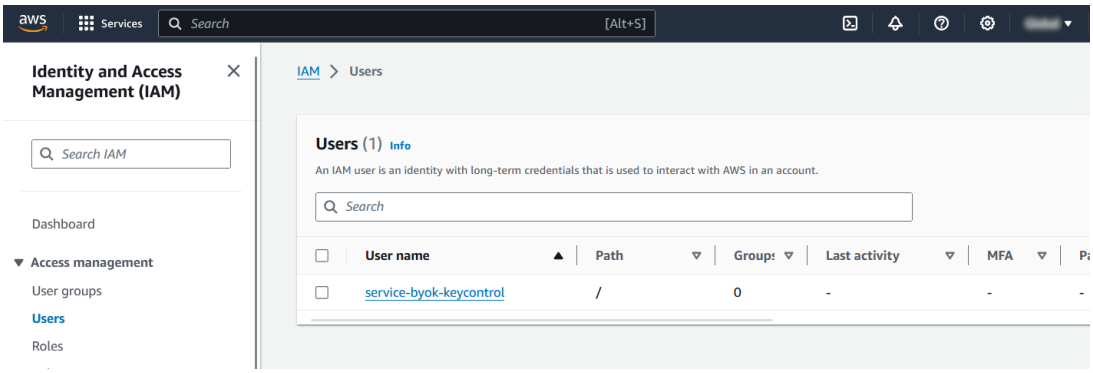
6. In the **Review and create** window, go to section **Tags - optional** and select **Add new tag** if required by your organization. Enter the key-value pair. Then select **Create user**.

> Some organizations uses tags manage IAM users key. Check your organization's policies.

For example:

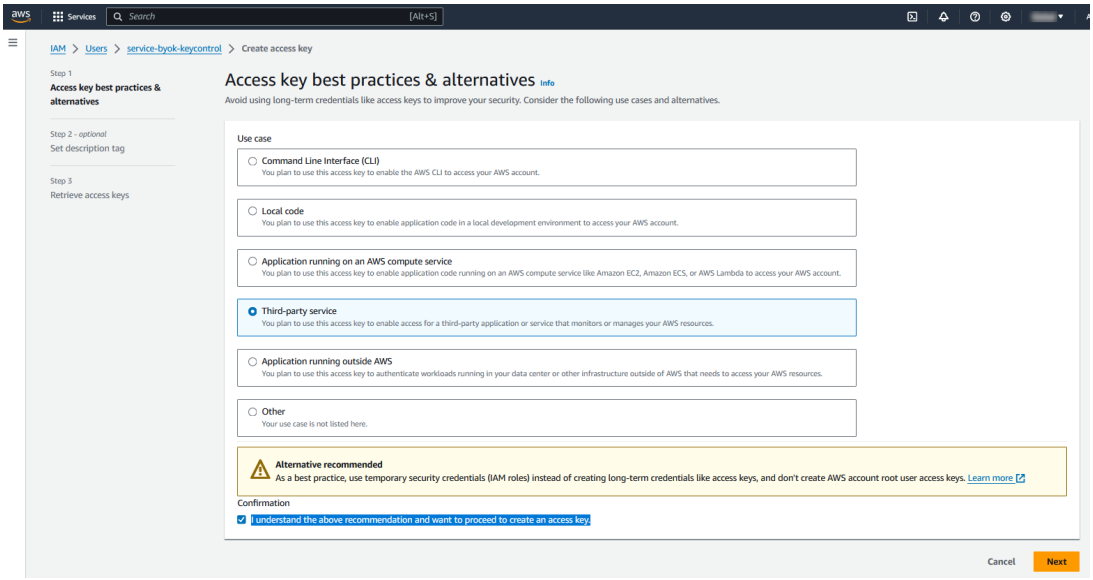


7. Notice the new user created.

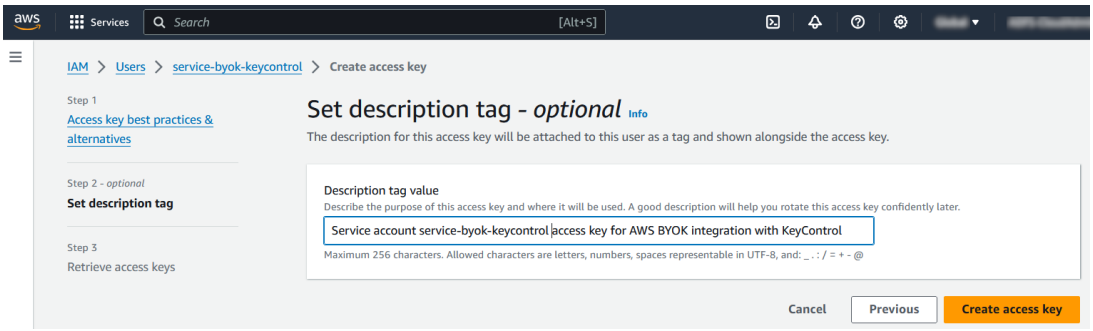


8. Select the new user. Then select the **Security credentials** tab.
9. In the **Access keys (0)** section, select the **create access key** icon.
10. In the **Access key best practices & alternatives** window, select the **Third party service** radio button. Check **I understand the above recommendation and want to proceed to create an access key.** Then select **Next**.

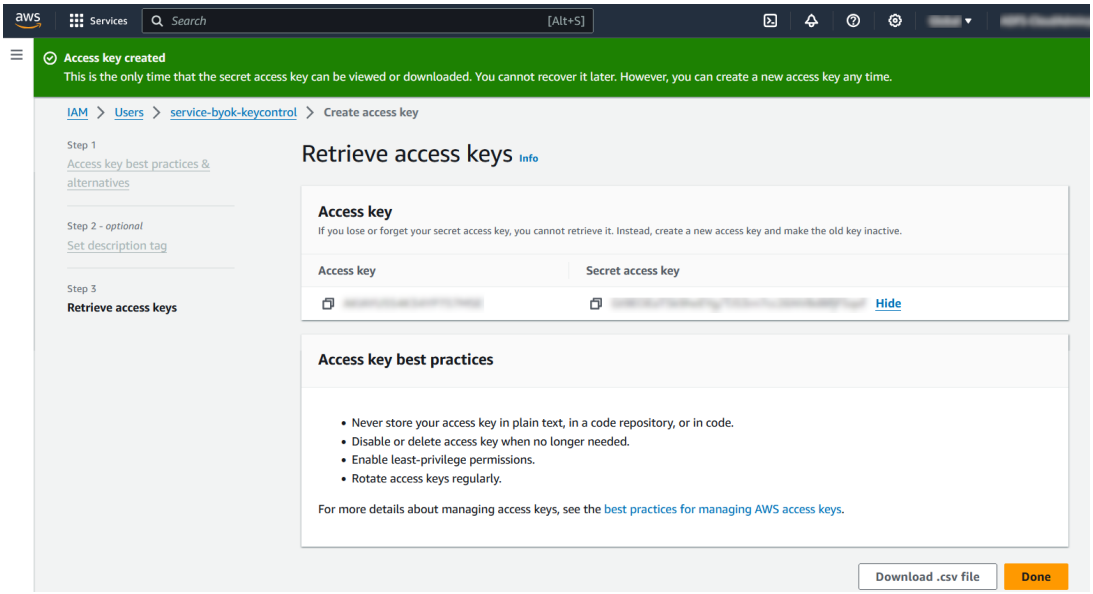
> Entrust KeyControl gives you the ability to rotate the access keys. You can set the rotation schedule later on, in Create an AWS CSP account.



11. In the **Set description tag - optional** window, enter a description tag if desired. Then select **Create access key**.



12. In the **Retrieve access key** window, select **Download .csv file** to download a file containing the **Access key** and **Secret access key**. Save these keys. You will need them to Create an AWS CSP account. Then select **Done**.

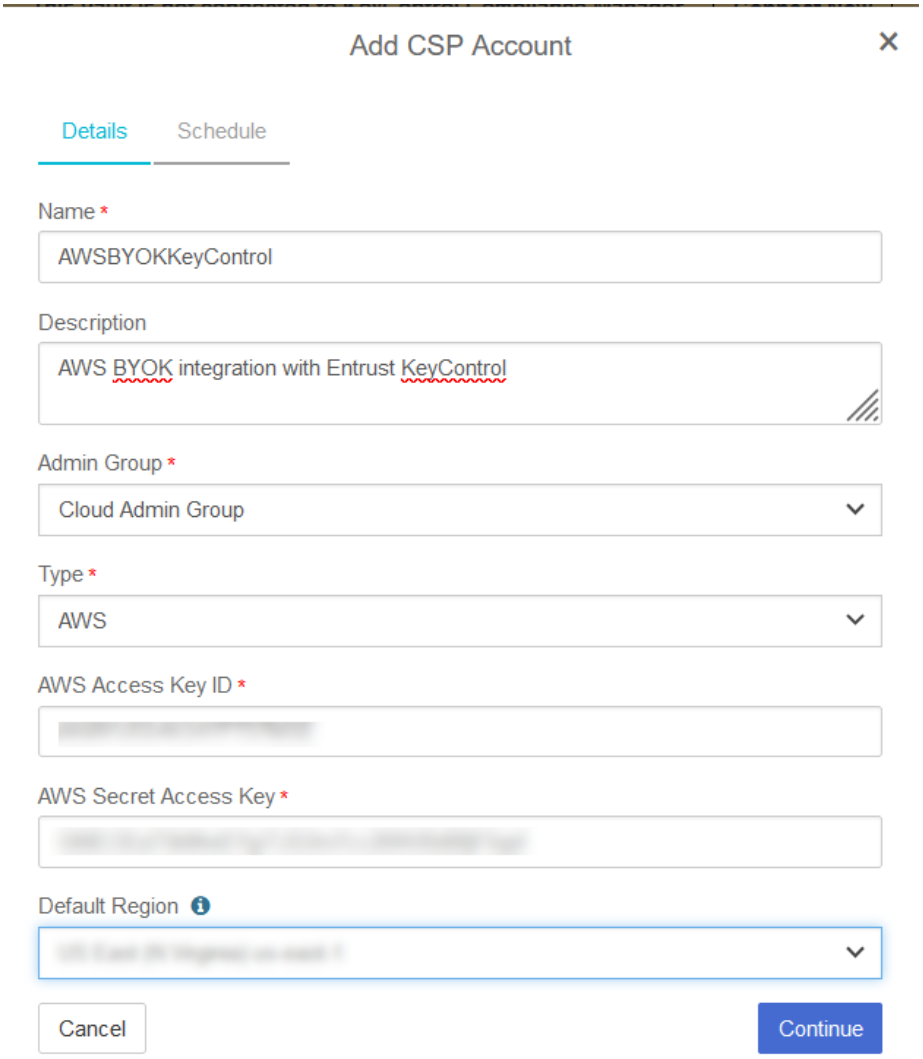

aws
Services
Search
[Alt+S]
Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.
IAM > Users > service-byok-keycontrol > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Retrieve access keys Info
Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key
Secret access key
Hide
Access key best practices
• Never store your access key in plain text, in a code repository, or in code.
• Disable or delete access key when no longer needed.
• Enable least-privilege permissions.
• Rotate access keys regularly.
For more details about managing access keys, see the best practices for managing AWS access keys.
Download .csv file
Done

Chapter 4. Integrate BYOK for AWS Key Management Service and Entrust KeyControl

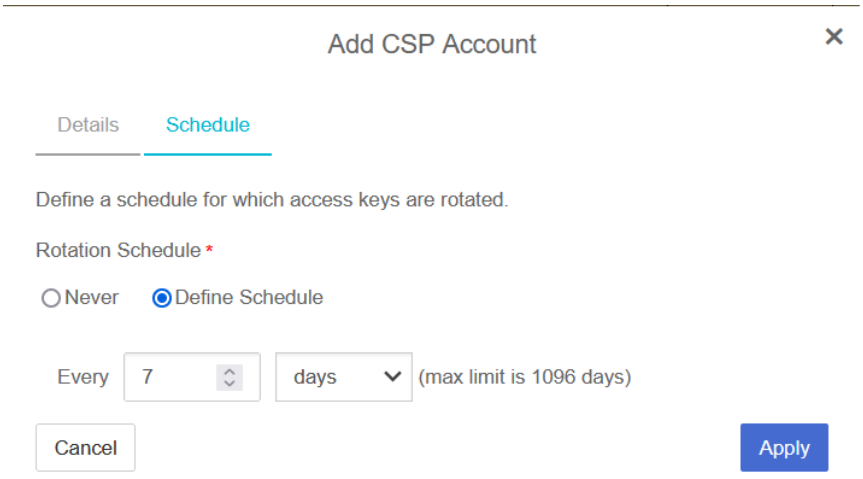
4.1. Create an AWS CSP account

1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **CSP Accounts** tab.
3. In the **Actions** pull down menu, select **Add CSP Account**.
4. In the **Add CSP Account** window, enter the **Name** and **Description**.
5. In the **Admin Group** pull-down menu, select **Cloud Admin Group**.
6. In the **Type** pull-down menu, select **AWS**.
7. In the **AWS Access Key ID** text box, enter the **Access key** created in Create AWS AIM user.
8. In the **AWS Secret Access Key** text box, enter the **Secret access key** created in Create AWS AIM user.
9. In the **Default region**, choose your AWS region. Then select **Continue**.

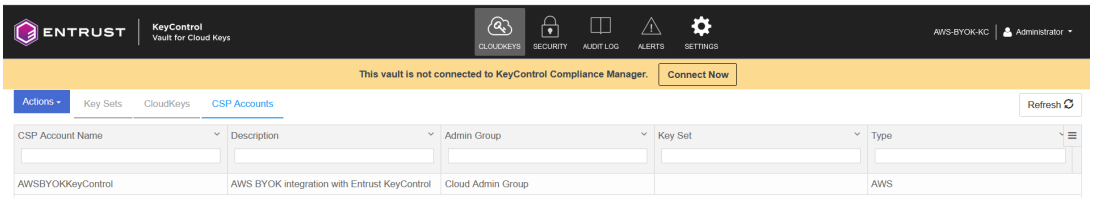
   For example:



10. In the **Schedule** tab, enter your organization's standard rotation schedule for the access keys. Then select **Apply**.



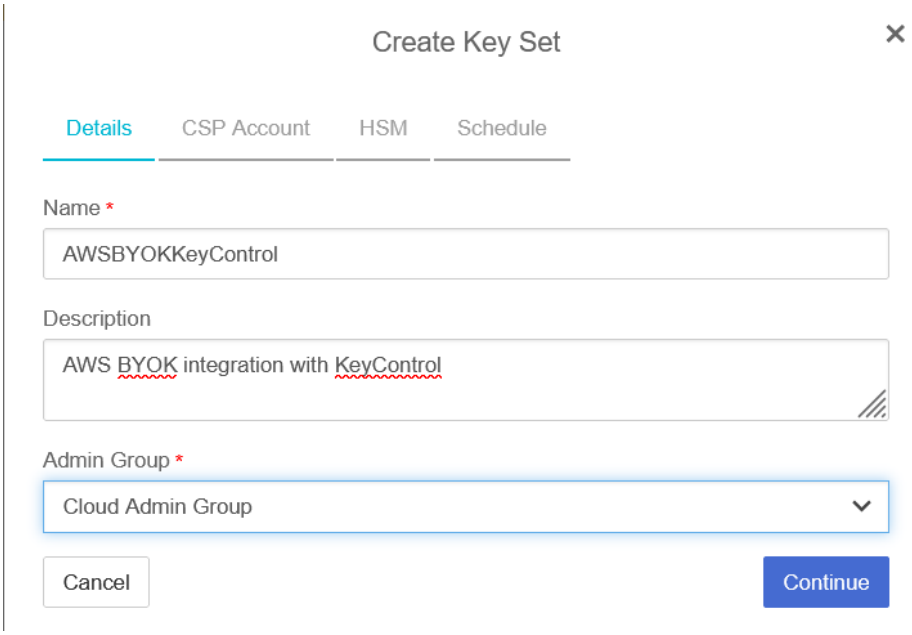
11. Notice the newly created CSP account.



4.2. Create a key set in KeyControl

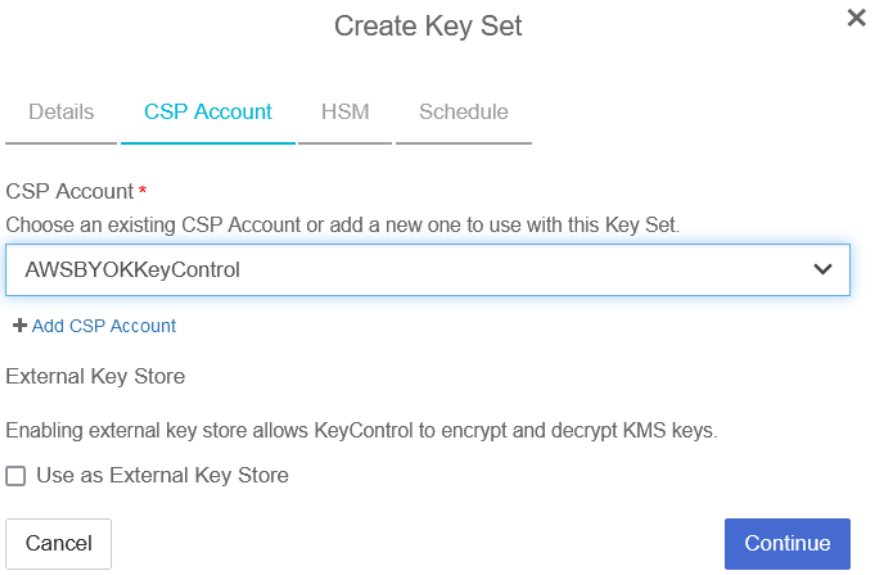
1. sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **Key Sets** tab.
3. In the **Actions** pull down menu, select **Create Key Set**.
4. In the **Choose the type of keys in this key set:** window, select **AWS Key**.
5. In the **Create Key Set** window, enter a **Name** and **Description**. In the **Admin Group** pull-down menu, select **Cloud Admin Group**. Then select **Continue**.

   For example:



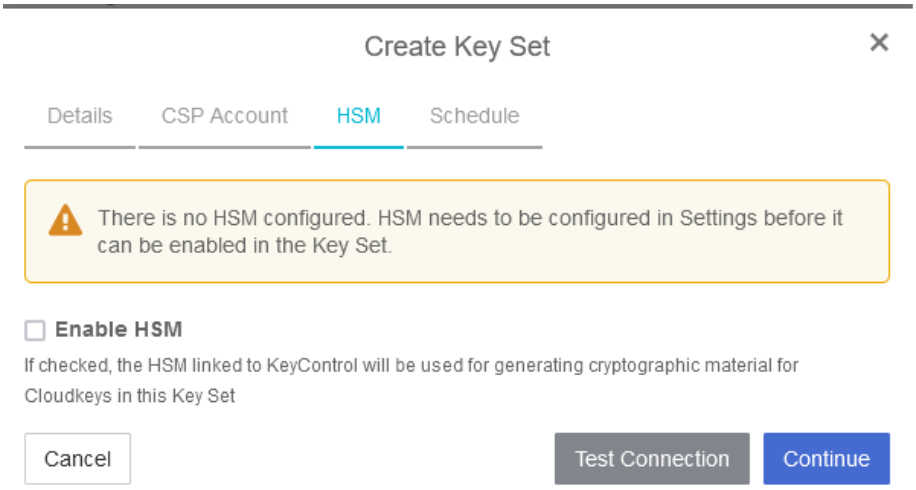
6. In the **CSP Account** tab, select the CSP account created in Create an AWS CSP account. Check **Use as External Key Store** to allow Entrust KeyControl to encrypt and decrypt the KMS keys. Then select **Continue**.

   For example:



7. In the **HSM** tab, check **Enable HMS** if an HSM is configured. Then select **Continue**.

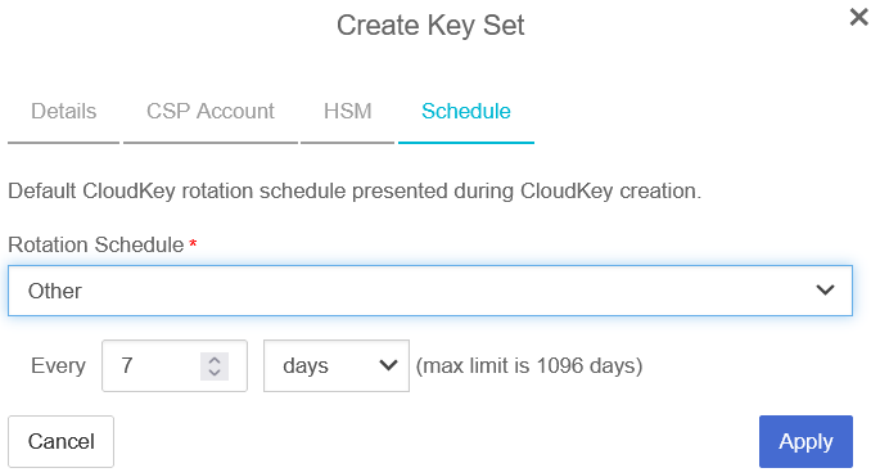
   For example:



   See Integrating with an HSM for additional information.

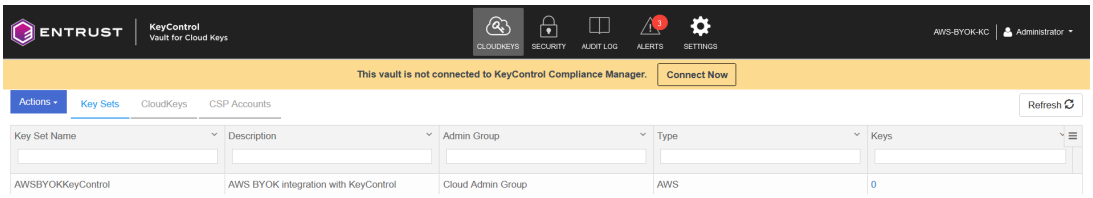
8. In the **Schedule** tab, select a **Rotation Schedule** matching the selection made during Create an AWS CSP account. Then select **Apply**.

   For example:



9. Notice the newly created key set.

   For example:



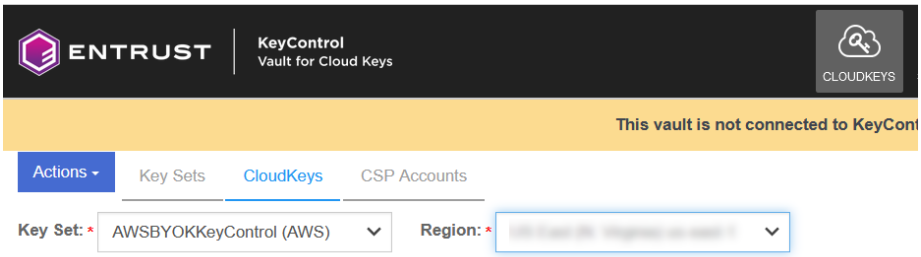
For further information, refer to Creating a Key Set in the KeyControl online documentation.

Chapter 5. Test the integration

5.1. Create a cloud key in KeyControl

1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **CloudKeys** tab.
3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.

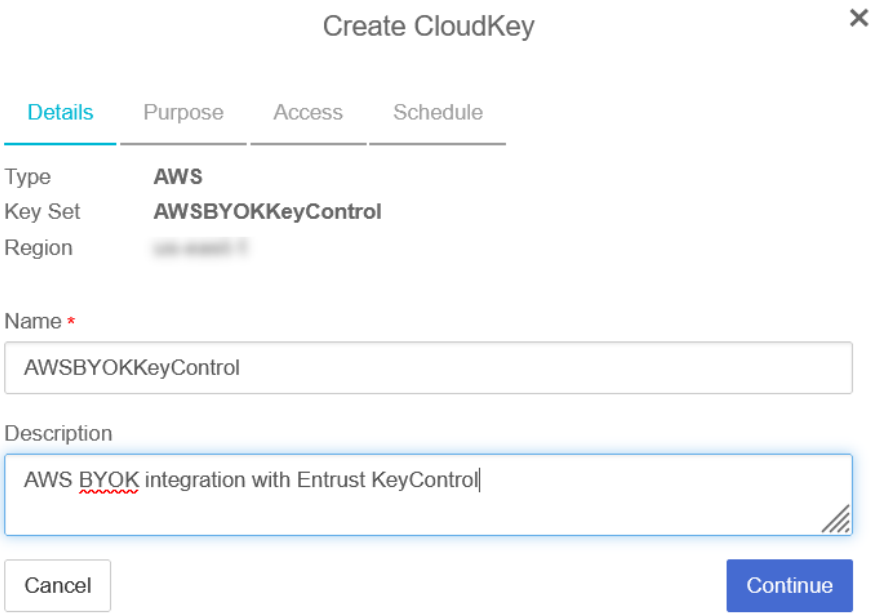
   For example:



> Multi-region keys will be supported in a future release of Entrust KeyControl.

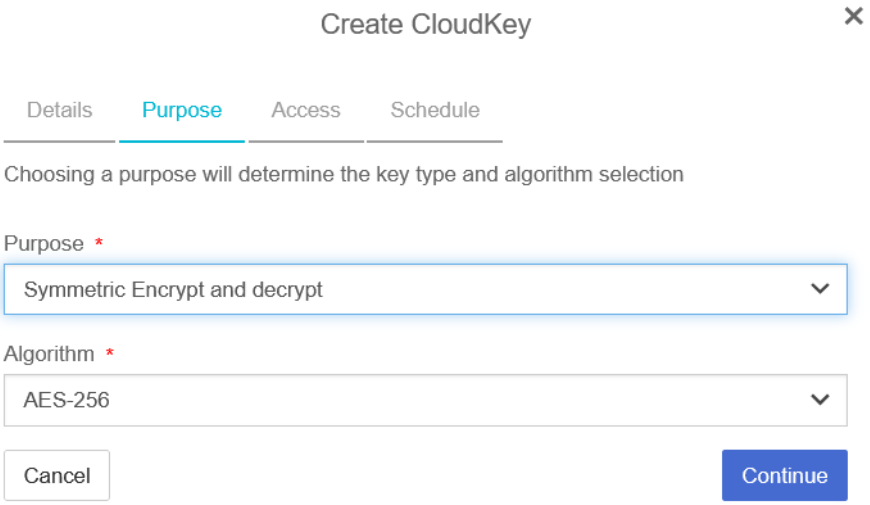
4. In the **Actions** pull down menu, select **Create CloudKey**. The **Create CloudKey** window appears.
5. In the **Details** tab, enter the **Name** and **Description**. Then select **Continue**.

   For example:



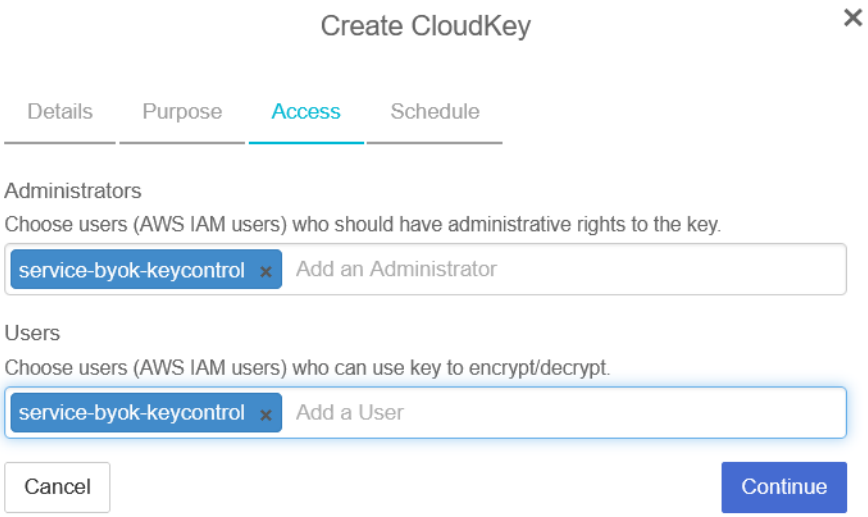
6. In the **Purpose** tab, select from the **Purpose** and **Algorithm** pull-down menus. Then select **Continue**.

   For example:



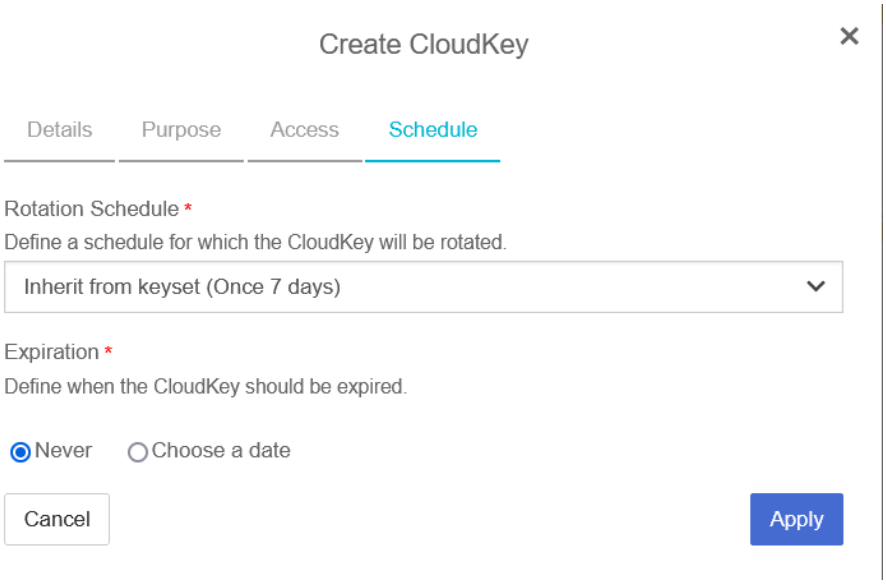
7. In the **Access** tab, select the service account created in Create AWS AIM user in box the **Administrator** and **Users** text box. Then select **Continue**.

   For example:

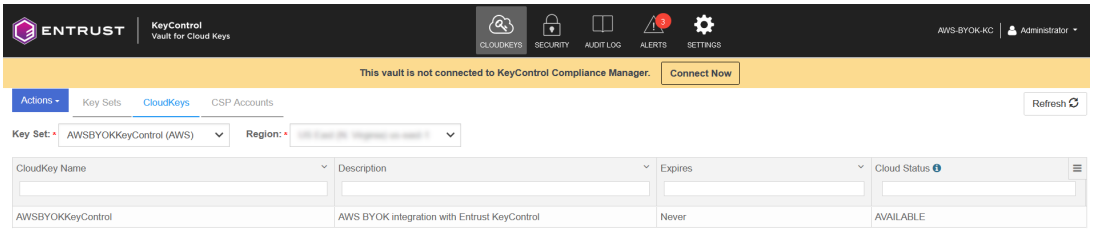


8. In the **Schedule** tab, select your **Rotation Schedule** and **Expiration** date. Then select **Apply**.

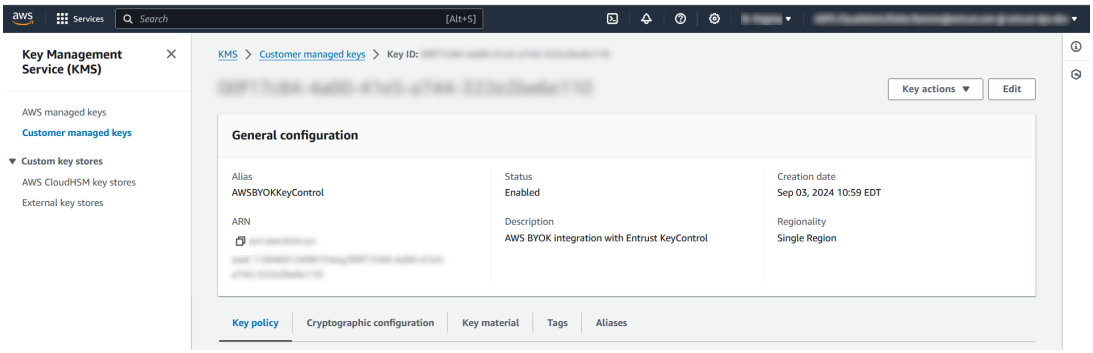
   For example:



9. Notice the newly created cloud key.



10. Verify the cloud key is visible in the AWS Key Management Service (KMS).

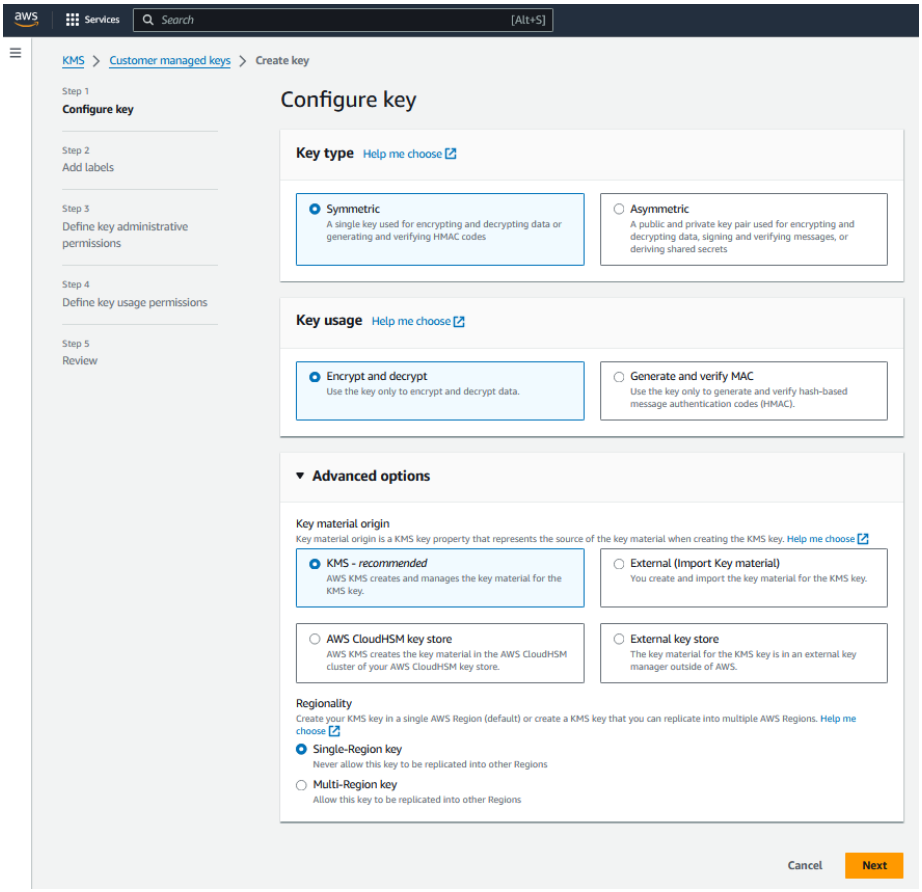


For further information, refer to Creating a CloudKey in the KeyControl online documentation.

5.2. Create a cloud key in AWS Key Management Service

1. In AWS, navigate to **Services** > **Key Management Service** > **Customer managed keys**. Then select the **Create key** icon.
2. In the **Configure key** window, select the **Key type** and **Key usage**. Then expand the **Advance options** and select the **Key material origin**. For **Regionality** select the **Single-Region key** radio button. Then select **Next**.

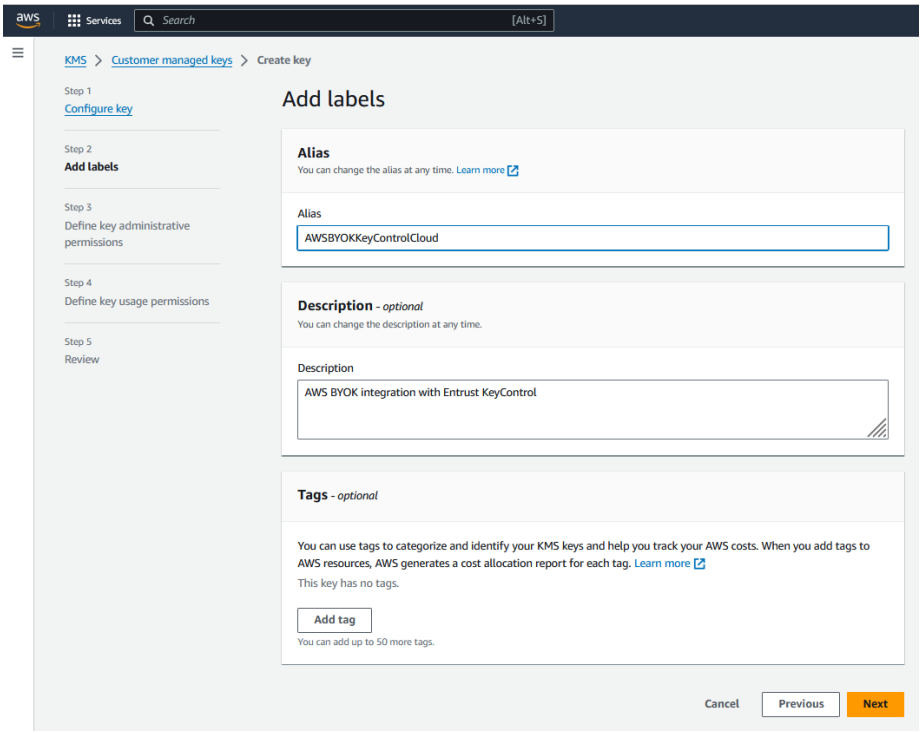
   For example:



Multi-region keys will be supported in a future release of Entrust KeyControl.

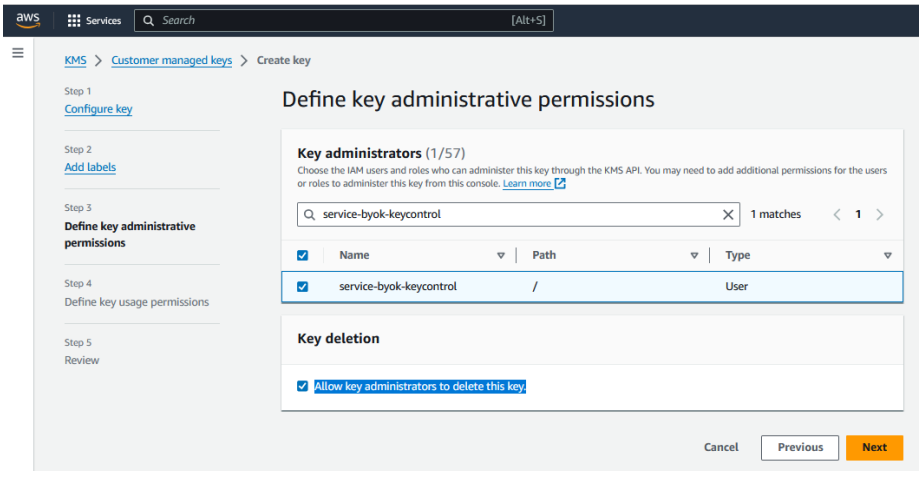
3. In the **Add labels** window, enter the **Alias** and **Description**. Then select **Next**.

   For example:



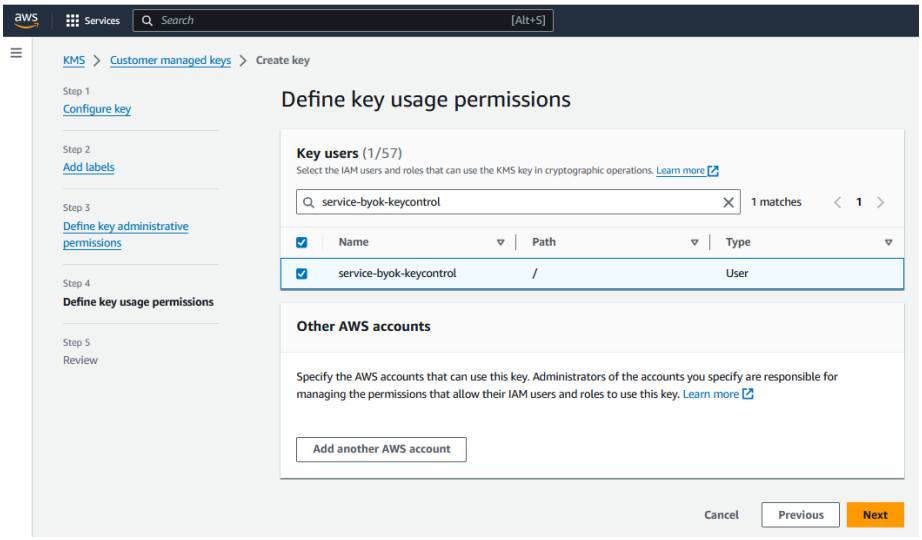
4. In the **Define key administrative permissions** window, enter the service account name created in Create AWS AIM user and select it. In the **Key deletion** section, check **Allow key administrators to delete this key**. Then select **Next**.

   For example:

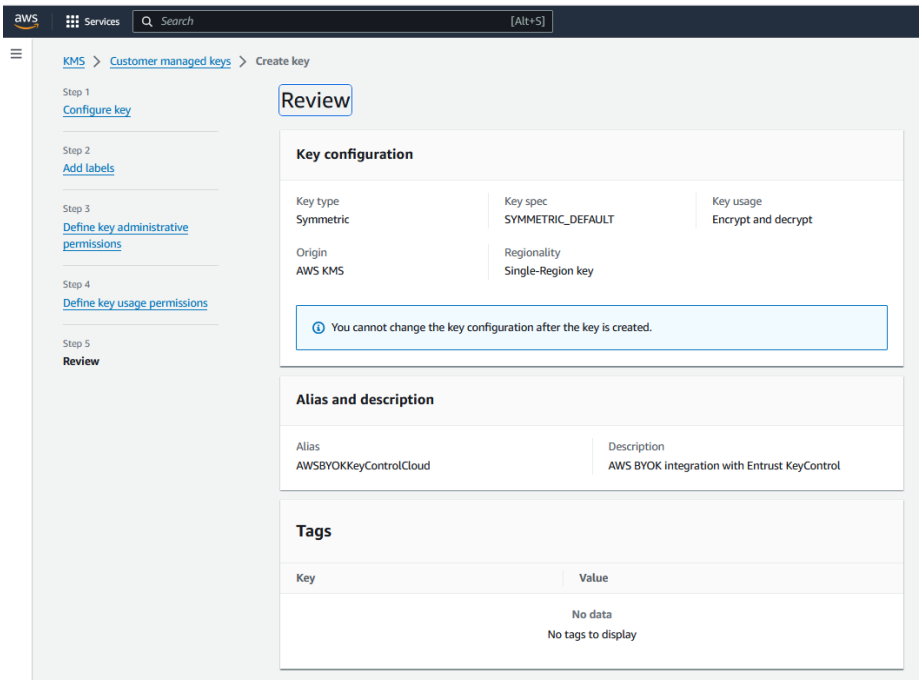


5. In the **Define key usage permissions** window, enter the service account name created in Create AWS AIM user and select it. Then select **Next**.

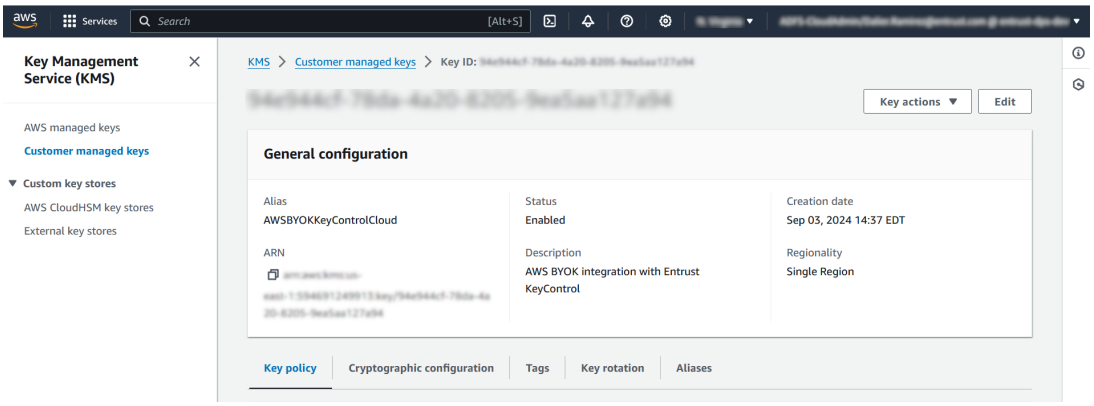
   For example:



6. In the **Review** window, select **Finish**.

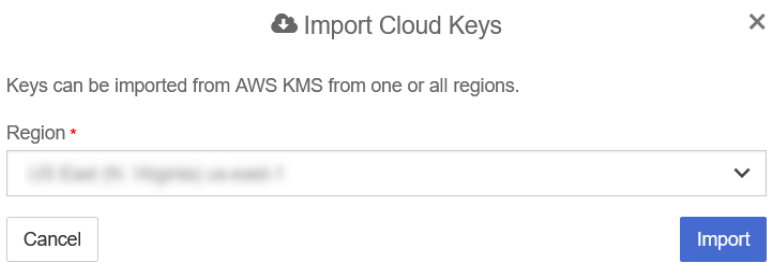


7. Notice the new key in the AWS KMS.

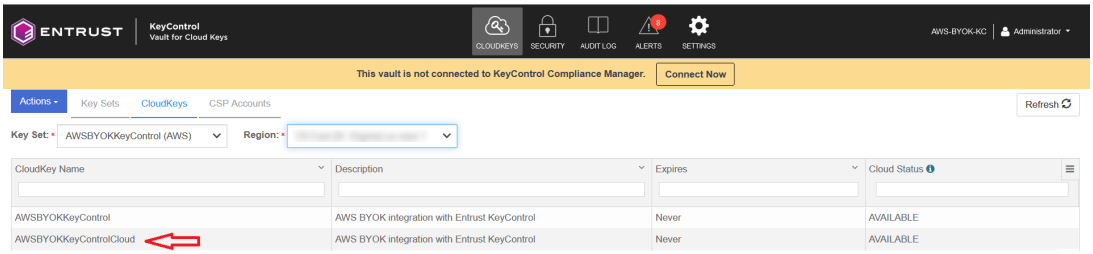


To import the cloud key in KeyControl:

1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **Key Sets** tab. Then select the key set created in Create a key set in KeyControl.
3. In the **Actions** pull down menu, select **Import CloudKeys**. The **Import Cloud Keys** window appears.
4. Select your region. Then select **Import**.



5. Select the **CloudKeys** tab and select **Refresh**.
6. Verify the imported key is visible in the Entrust KeyControl cloud keys vault.



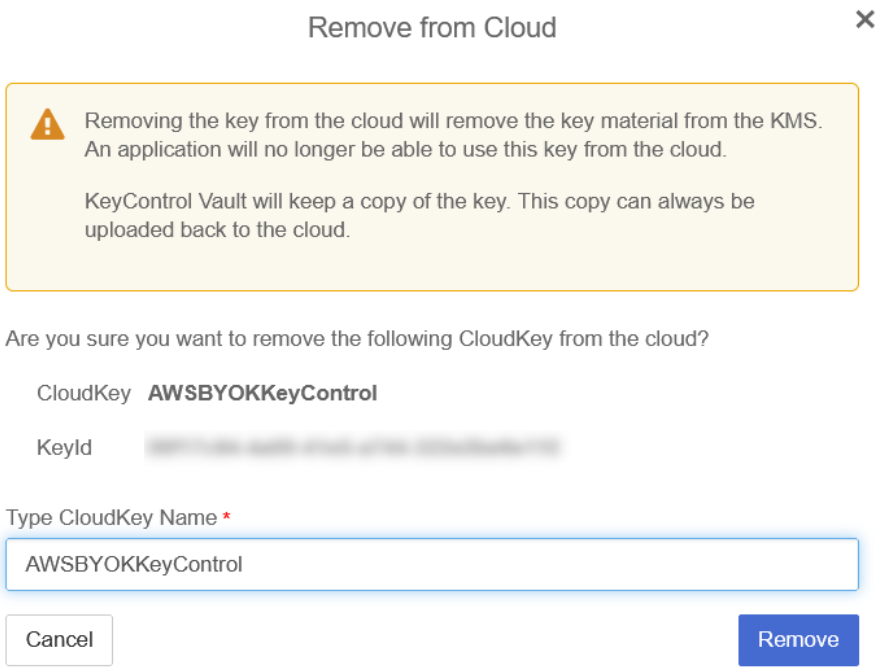
For further information, refer to Importing CloudKeys in the KeyControl online documentation.

5.3. Remove a cloud key in KeyControl

1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **CloudKeys** tab.
3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
4. Select the key to be removed from the cloud.
5. In the **Actions** pull down menu, select **Remove from Cloud**. The **Remove from Cloud** dialog appears.

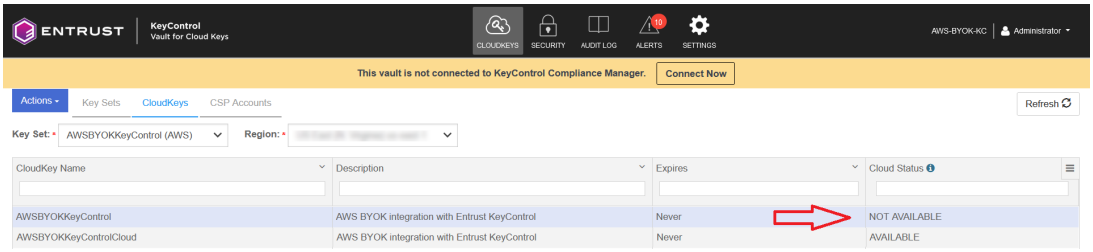
6. Type the name of the key in the **Type CloudKey Name** text box. Then select **Remove**.

   For example:

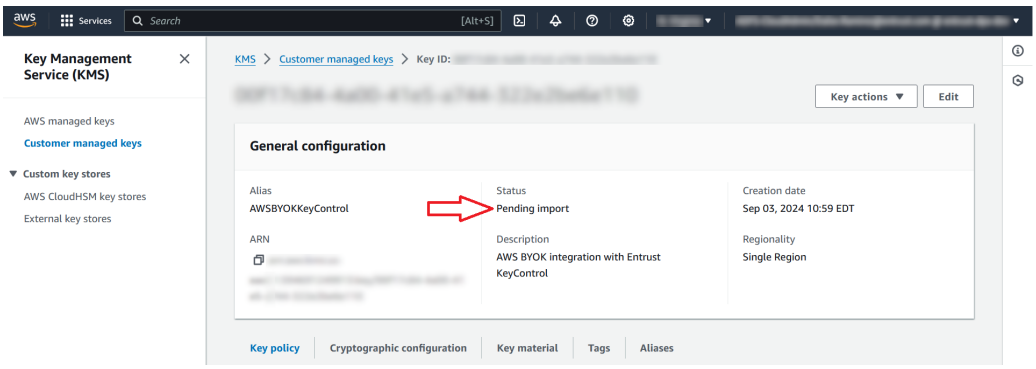


7. Notice the key **Cloud Status** becomes **NOT AVAILABLE**.

   For example:



8. Verify the key **Status** changed in AWS KMS.

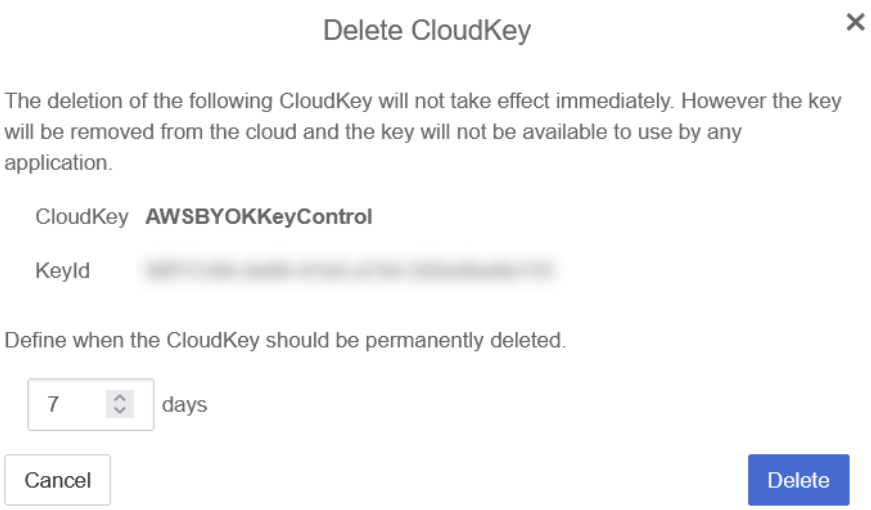


For further information, refer to Removing a CloudKey from the Cloud in the KeyControl online documentation.

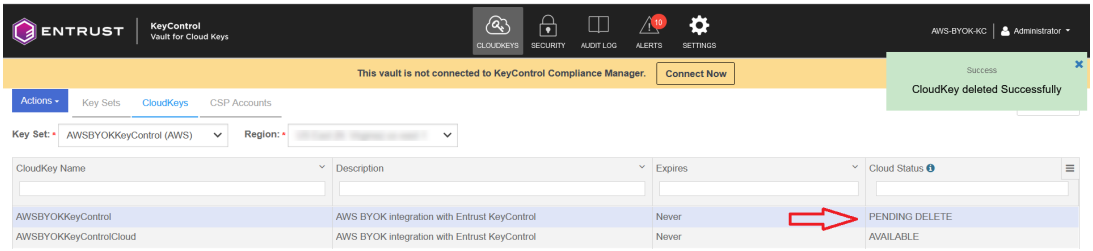
5.4. Delete a cloud key in KeyControl

1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **CloudKeys** tab.
3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
4. Select the key to be deleted.
5. In the **Actions** pull down menu, select **Delete CloudKey**. The **Delete CloudKey** dialog appears.
6. Select a time in **Define when the CloudKey should be permanently deleted**. Then select **Delete**.

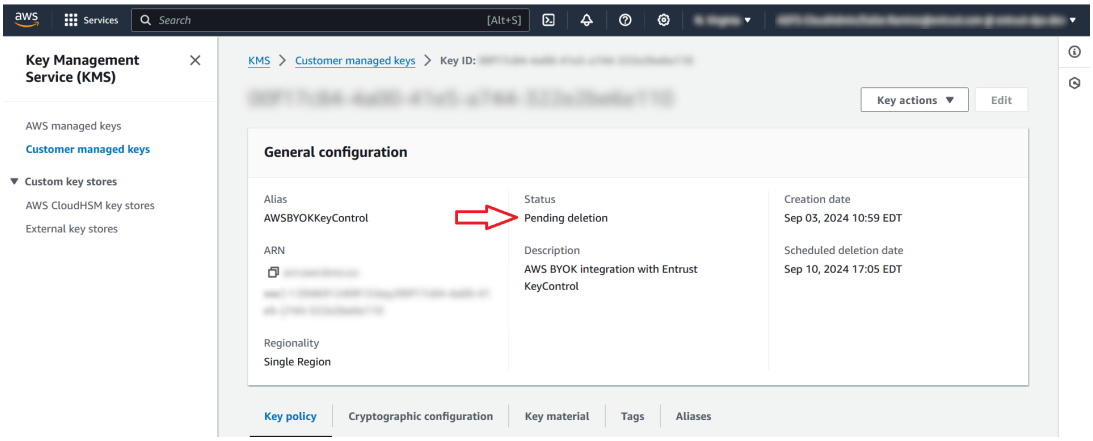
   For example:



7. Notice the key **Cloud Status** becomes **PENDING DELETE**.



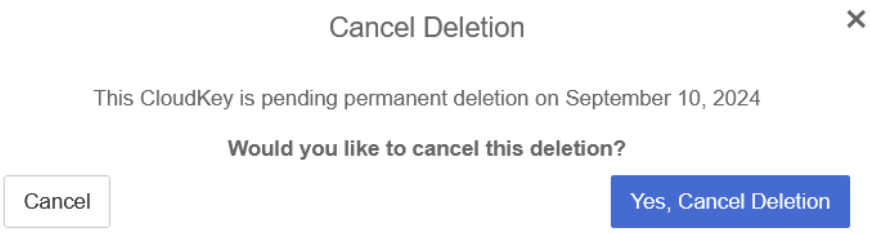
8. Verify the key **Status** changed in AWS KMS.



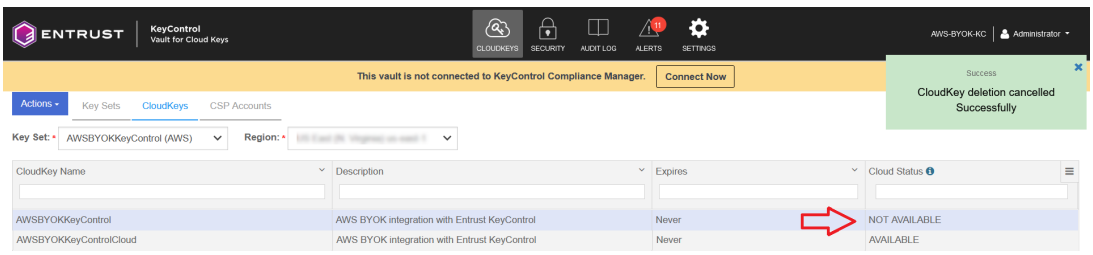
For further information, refer to Deleting a CloudKey in the KeyControl online documentation.

5.5. Cancel a cloud key deletion in KeyControl

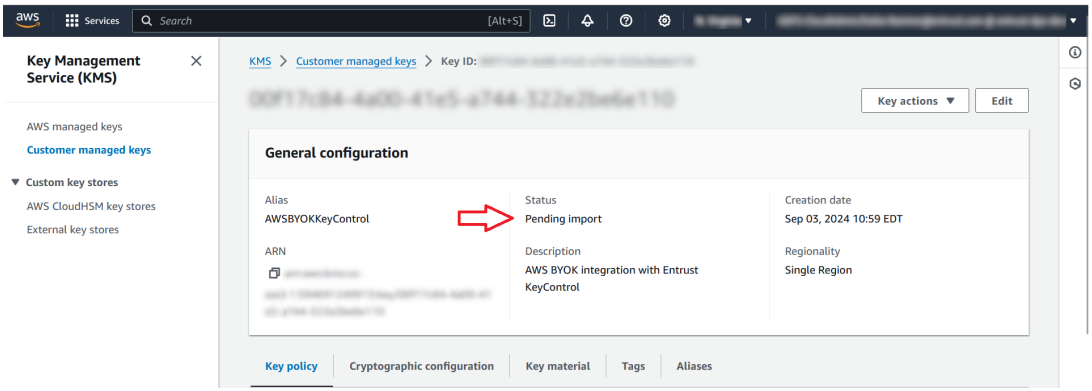
1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **CloudKeys** tab.
3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
4. Select the key who's scheduled deletion is going to be cancelled.
5. In the **Actions** pull down menu, select **Cancel Deletion**. The **Cancel Deletion** dialog appears.
6. Select **Yes, Cancel Deletion**.



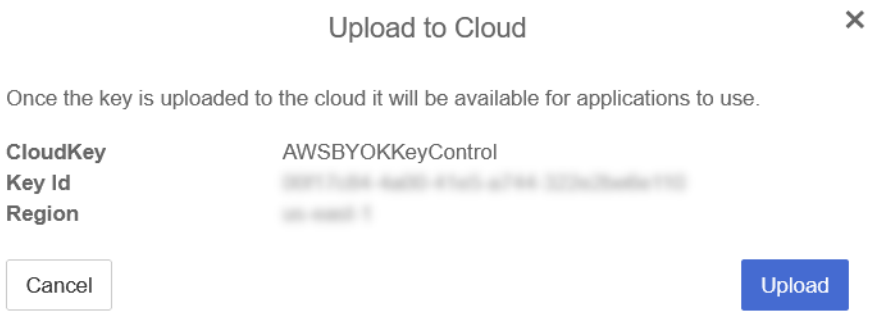
7. Notice the key **Cloud Status** becomes **NOT AVAILABLE**.



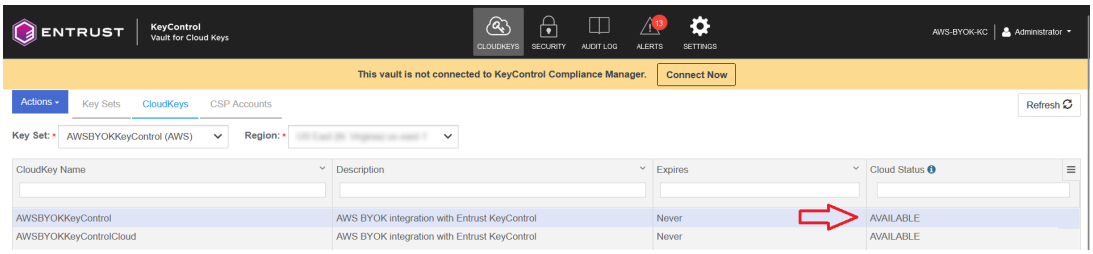
8. Verify the key **Status** changed in AWS KMS.



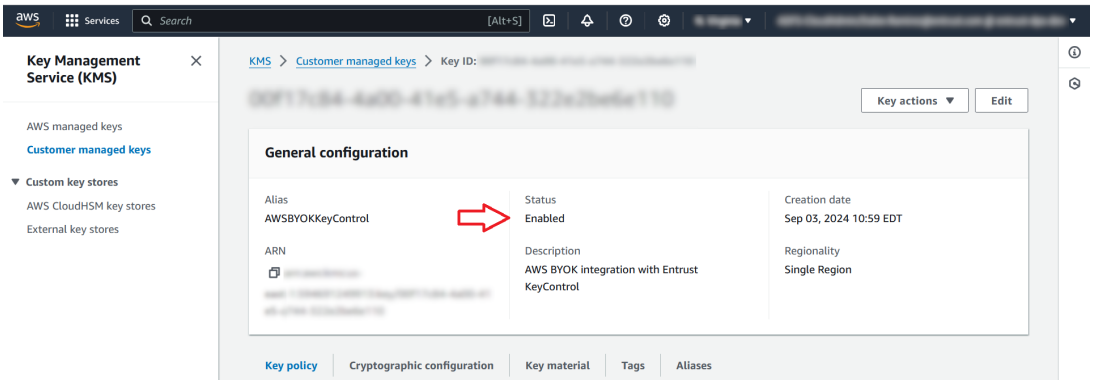
9. Back in Entrust KeyControl, In the **Actions** pull down menu, select **Upload to Cloud**. The **Upload to Cloud** dialog appears.
10. Select **Upload**.



11. Notice the key **Cloud Status** becomes **AVAILABLE**.



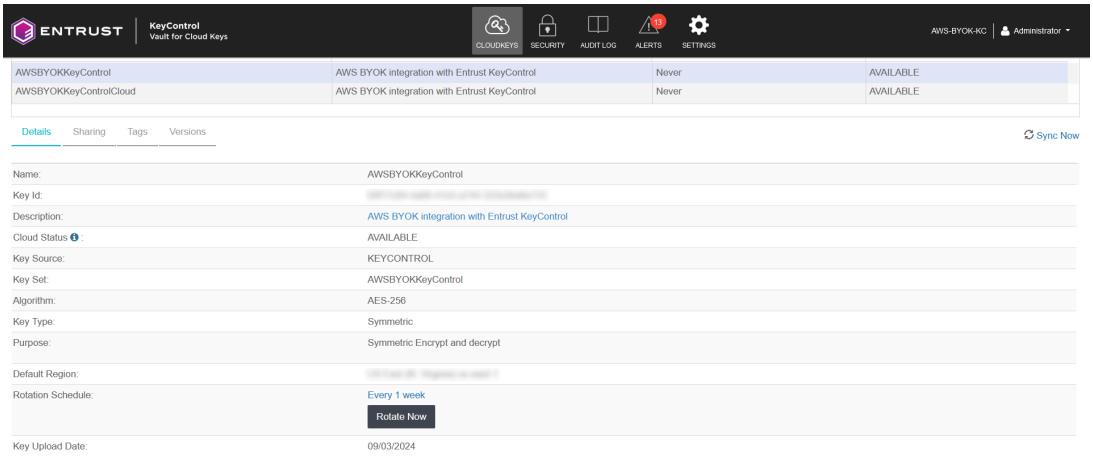
12. Verify the key **Status** changed in AWS KMS.



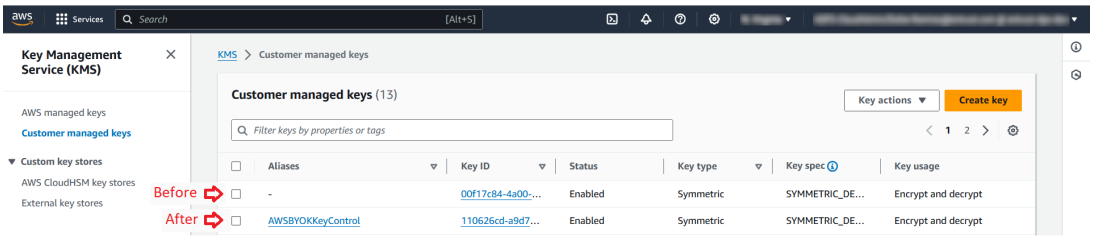
For further information, refer to Canceling a CloudKey Deletion in the KeyControl online documentation.

5.6. Rotate a cloud key in KeyControl

1. Sign in to the cloud keys vault URL created in Create a Cloud Keys Vault in the KeyControl.
2. Select the **CloudKeys** tab.
3. In the **Key Set** pull-down menu, select the key set created in Create a key set in KeyControl. In the **Region** pull-down menu, select your region.
4. Select the key to be rotated.
5. Scroll down, select the **Details** tab, and select the **Rotate Now** icon.



6. Verify that the key has been rotated in AWS KMS.



Chapter 6. Integrating with an HSM

For guidance on integrating the Entrust KeyControl with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the Entrust KeyControl nShield HSM Integration Guide available at Entrust documentation library.

Chapter 7. Additional resources and related products

7.1. nShield Connect

7.2. nShield as a Service

7.3. KeyControl

7.4. KeyControl BYOK

7.5. KeyControl as a Service

7.6. Entrust products

7.7. nShield product documentation