



**ENTRUST**

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

Integration Guide

2025-02-07

# Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Requirements	1
2. Deploy and configure KeyControl	2
2.1. Deploy an KeyControl cluster	2
2.2. Additional KeyControl cluster configuration	2
2.3. Configure authentication	3
2.4. Create DNS record for the KeyControl cluster	3
2.5. Create a Cloud Keys Vault in the KeyControl	3
2.6. View the Cloud Keys Vault details	6
3. Create an AWS IAM user service account	8
3.1. Create an AWS BYOK service account policy	8
3.2. Create an AWS IAM user service account	10
4. Integrate BYOK for AWS Key Management Service and KeyControl	14
4.1. Create a CSP account in KeyControl for AWS	14
4.2. Test the CSP account connection to AWS	16
4.3. Create a Key Set in KeyControl for AWS	16
5. Test the integration	19
5.1. Create a single-region cloud key in KeyControl	19
5.2. Create a multi-region cloud key in KeyControl	22
5.3. Create a cloud key in AWS Key Management Service	24
5.4. Import a cloud key created in AWS Key Management Service into KeyControl	27
5.5. Remove a cloud key in KeyControl	28
5.6. Delete a cloud key in KeyControl	30
5.7. Cancel a cloud key deletion in KeyControl	31
5.8. Rotate a cloud key in KeyControl	33
6. Integrating with an HSM	35
7. Additional resources and related products	36
7.1. nShield Connect	36
7.2. nShield as a Service	36
7.3. KeyControl	36
7.4. KeyControl BYOK	36
7.5. KeyControl as a Service	36
7.6. Entrust products	36
7.7. nShield product documentation	36

---

# 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	10.4.1

## 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 an 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.

Node	Status	Server Name	IP Address
Current Node	Online	★ KeyControl-1-2024-11-01-10-00-00	10.10.10.100
	Online	★ KeyControl-2-2024-11-01-10-00-00	10.10.10.101

Name:	★ KeyControl-1-2024-11-01-10-00-00
Status:	Online
Authenticated:	Yes
Domain:	Appliance Management Admin Group
IP Address:	10.10.10.100
Certificate:	Internal Web server: Default External Web server: Default

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.

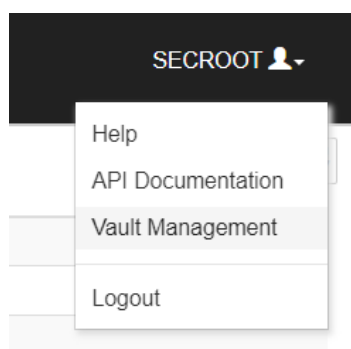
To use hostnames, configure your DNS server giving each node in KeyControl a unique name.

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

For example:

### Create Vault

A vault will have unique authentication and management.

#### Type

Choose the type of vault to create

Cloud Keys

#### Name \*

AWS-BYOK-KC

#### Description

AWS BYOK integration with Entrust KeyControl

Max. 300 characters

#### Email Notifications

**⚠ SMTP needs to be configured to turn on email notifications**

Use email to communicate with Vault Administrators, including their temporary passwords to Vault Admins.

#### Administrator

Invite an individual to have complete access and control over this

#### Admin Name \*

Administrator

#### Admin Email \*

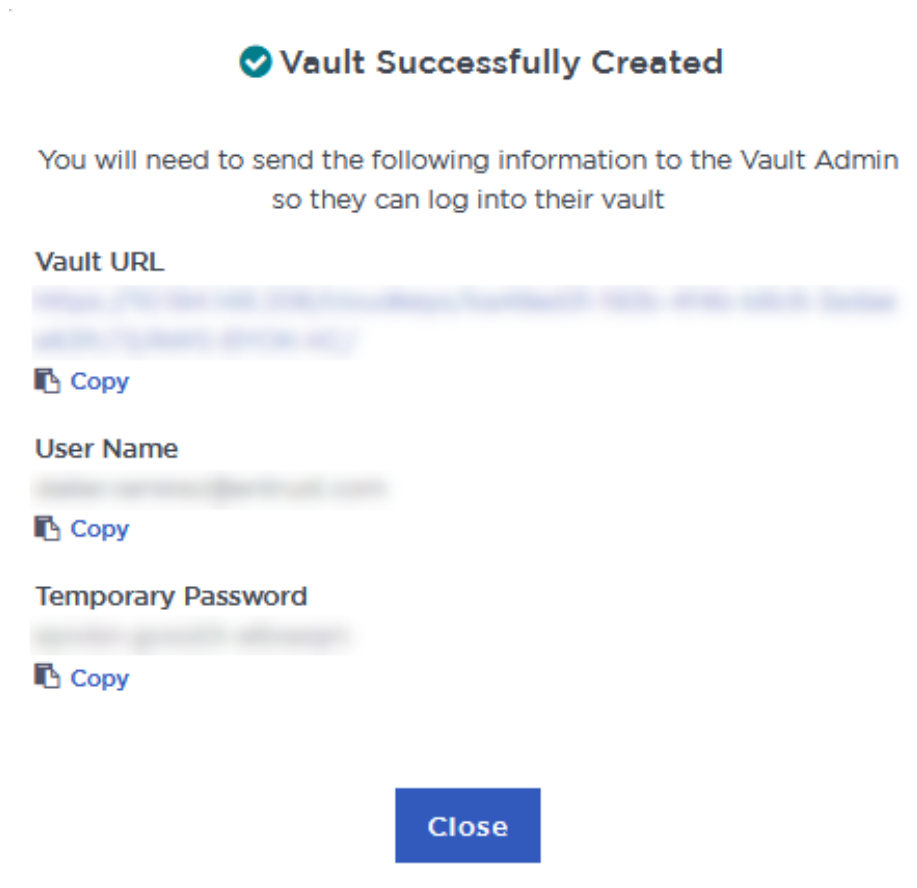
admin@company.com

Create Vault

Cancel

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.

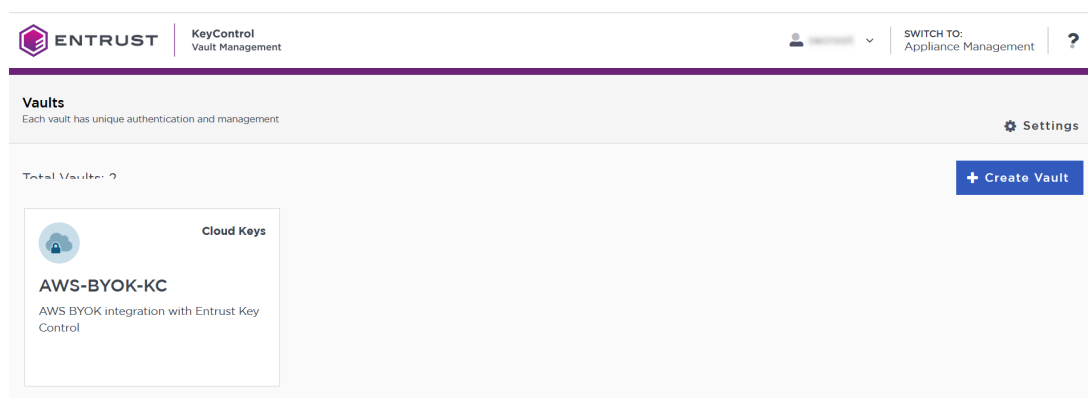
For example:



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

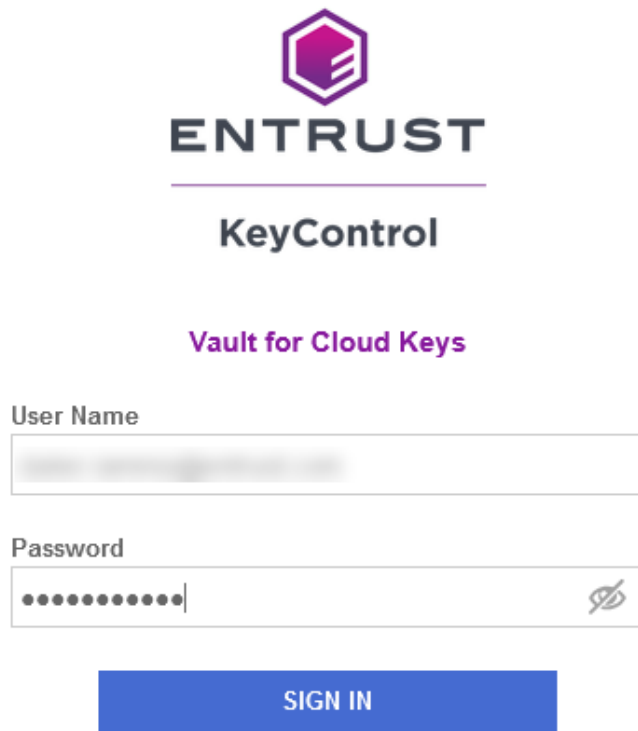
The newly created Vault is added to the **Vault Management** dashboard.

For example:



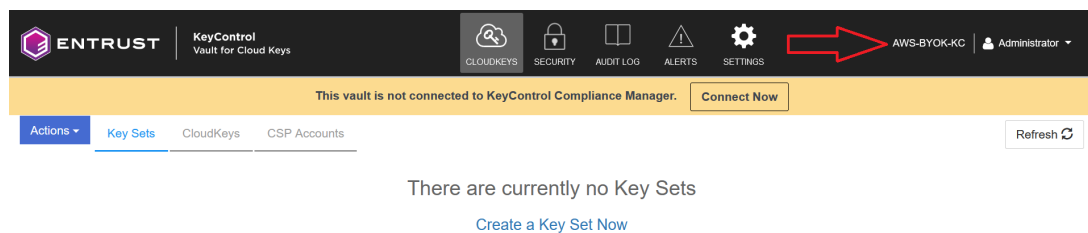
7. Sign in to the **Vault URL** with the temporary password. Change the initial password when prompted. Sign in again to verify.

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:



## Vault Details ✕


**AWS-BYOK-KC**  
AWS BYOK integration with Entrust KeyControl

**Type**  
Cloud Keys


**Created**  
Jan 15, 2025 09:07:11 AM

---

**Vault URL**  
[Redacted]

 [Copy](#)

**API URL**  
[Redacted]

 [Copy](#)

---

**Administrator**

**Admin Name**  
Administrator

**User Name**  
[Redacted]

2. Select **Close** when done.

## Chapter 3. Create an AWS IAM user service account

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

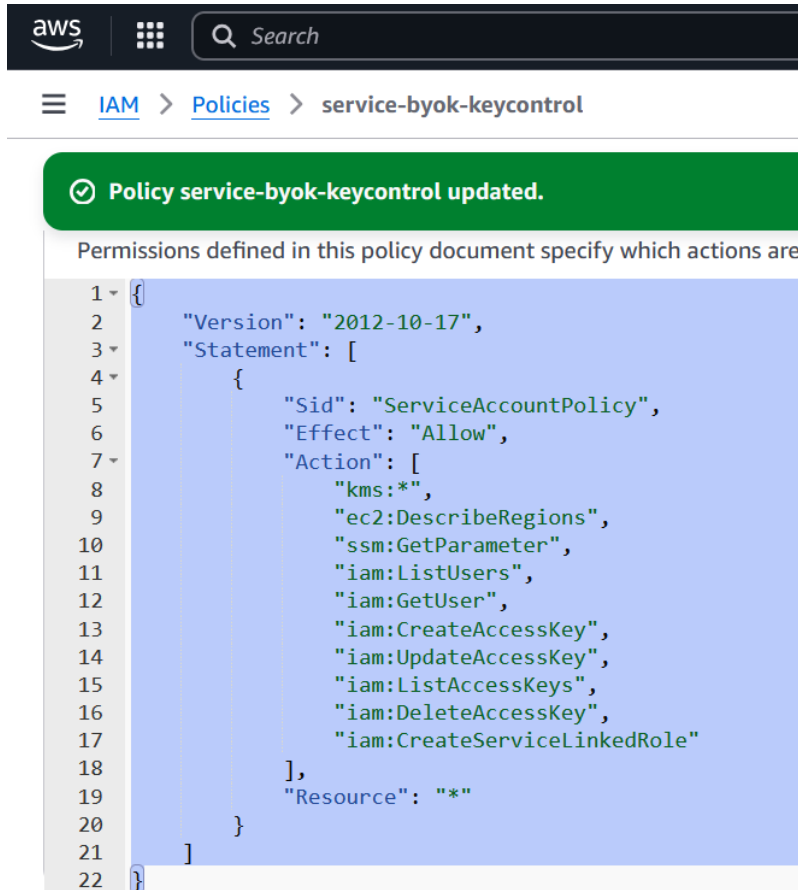
### 3.1. Create an AWS BYOK service account policy

1. In AWS, navigate to **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**

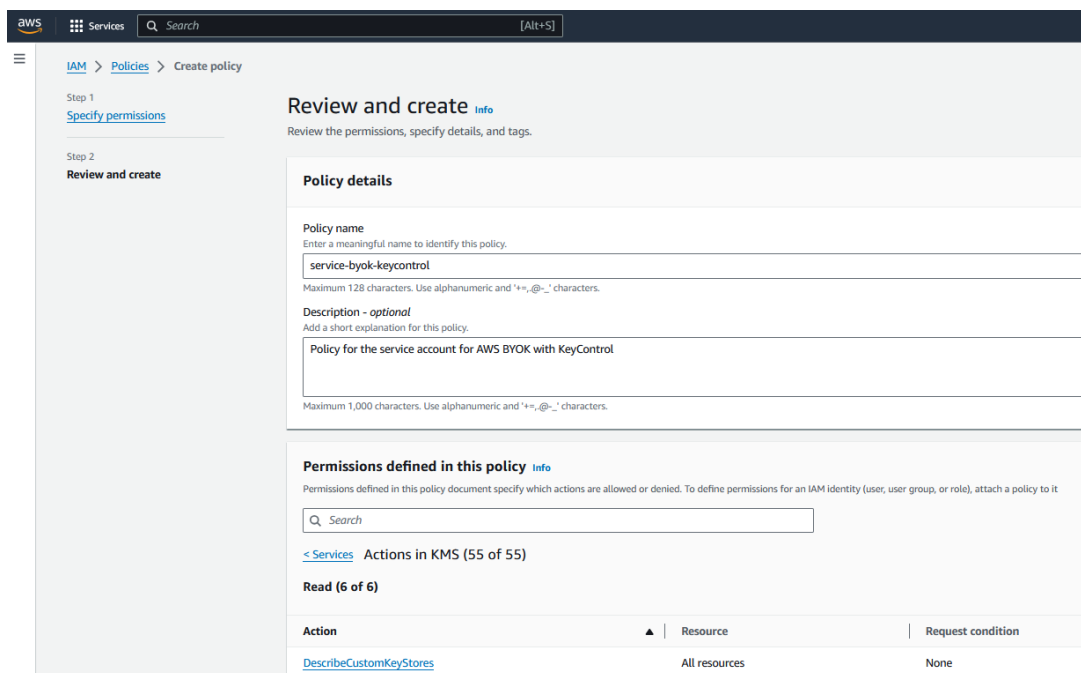
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ServiceAccountPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:*",
        "ec2:DescribeRegions",
        "ssm:GetParameter",
        "iam:ListUsers",
        "iam:GetUser",
        "iam:CreateAccessKey",
        "iam:UpdateAccessKey",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



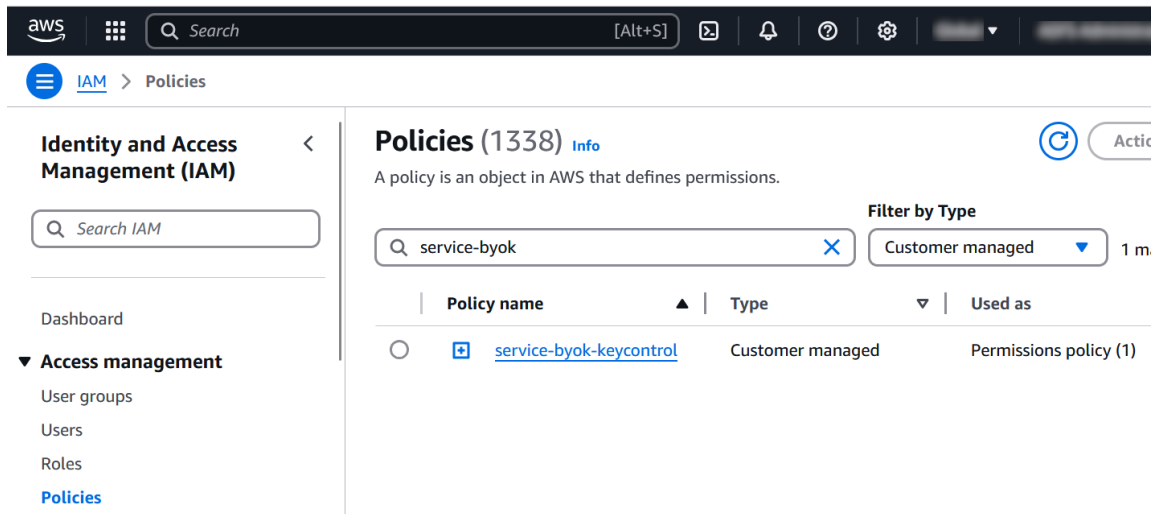
`CreateServiceLinkedRole` is needed to create multi-region keys.



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.



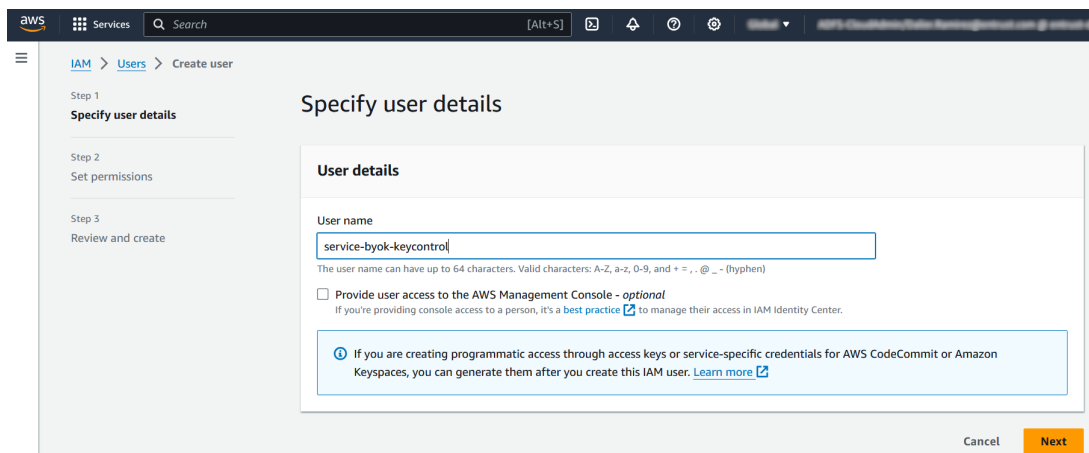
For further information, refer to the [AWS BYOK Service Account Requirements](#).

### 3.2. Create an AWS IAM user service account

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

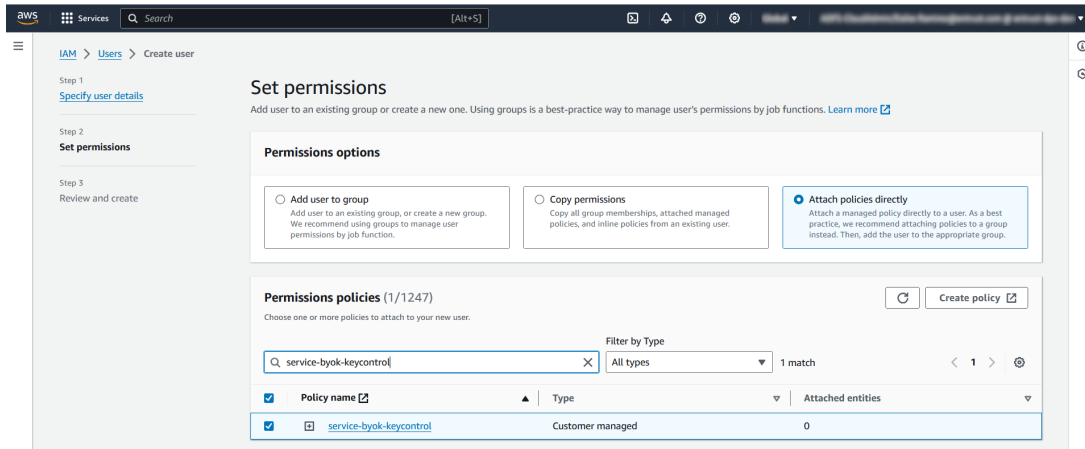
1. In AWS, navigate to **IAM**.
2. In the left pane select **Access management / Users**. Then select the **Create user** icon.
3. Enter the user name. Uncheck **Provide user access to AWS Management Console - optional** since we are creating a service account. Then select **Next**.

For example:



4. In the **Set permissions** window, select the **Attach policies directly** radio button.

- In the **Permissions policy** section, enter the policy created in [Create an AWS BYOK service account policy](#). Check the policy. Then select **Next**.

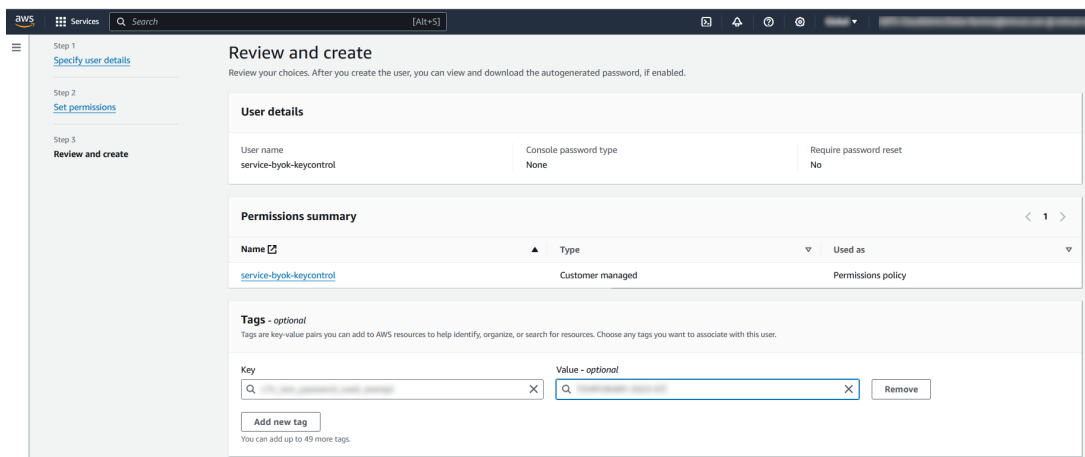


- In the **Review and create** window, go to section **Tags - optional** and select **Add new tag** if required by your organization. Enter the key-value pair. Then select **Create user**.

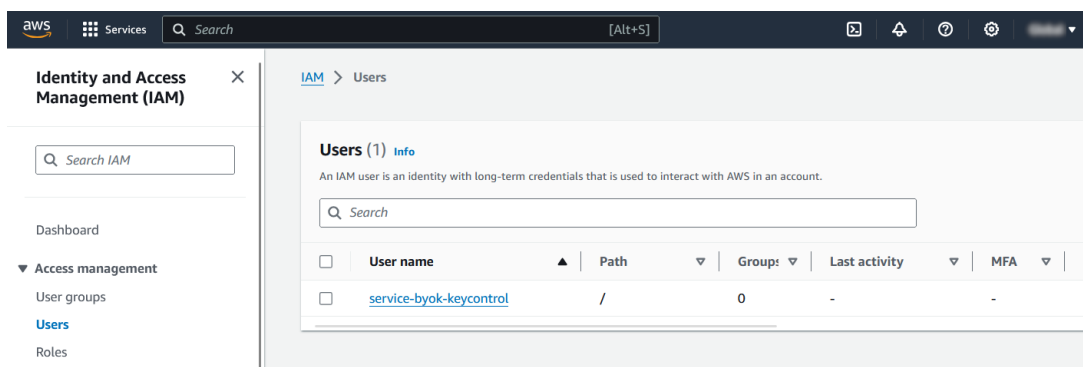


Some organizations uses tags manage IAM users key. Check your organization's policies.


For example:

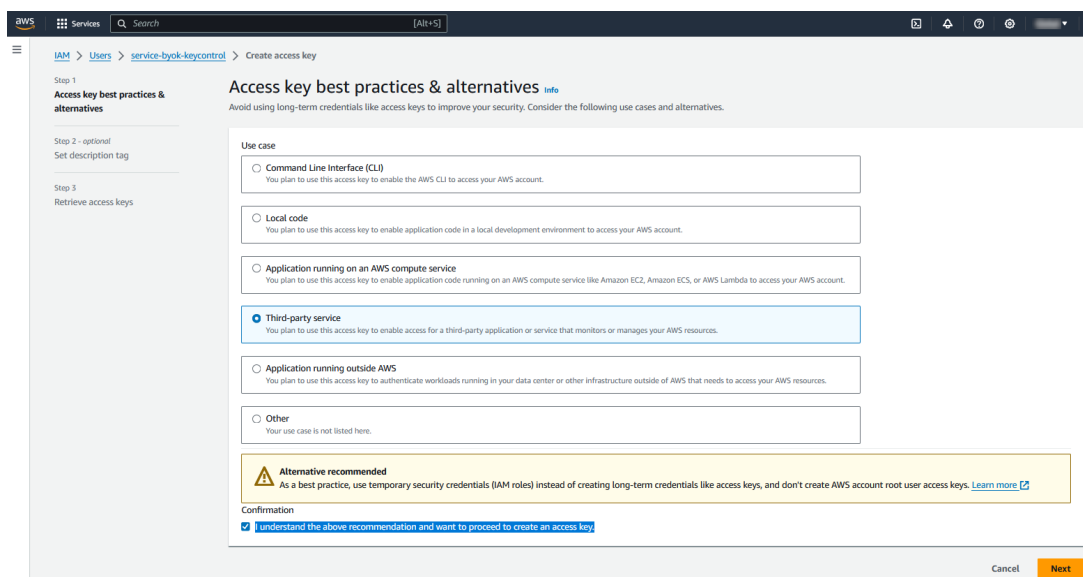


- Notice the new user created.

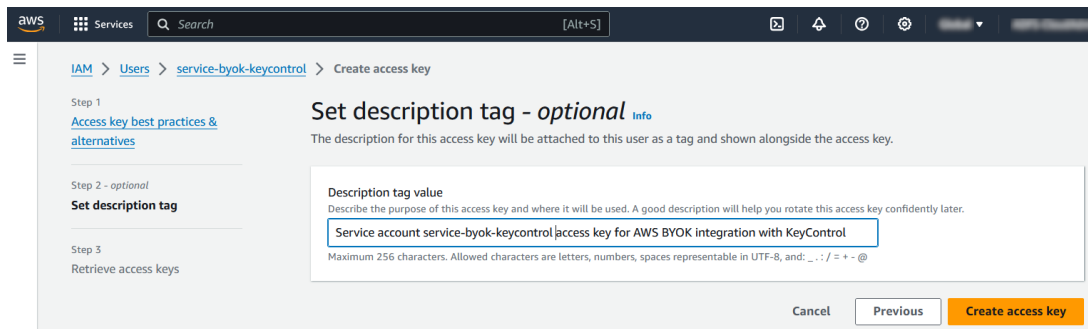


8. Select the new user. Then select the **Security credentials** tab.
9. In the **Access keys (x)** section, select the **create access key** icon.
10. In the **Access key best practices & alternatives** window, select the **Third party service** radio button. Check **I understand the above recommendation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

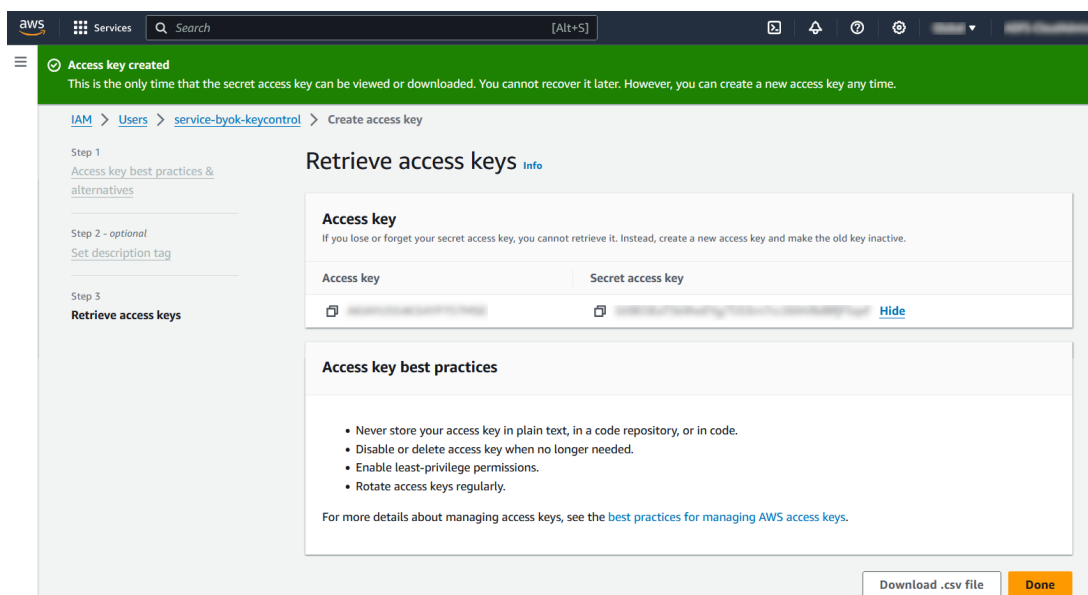
 KeyControl gives you the ability to rotate the access keys. You can set the rotation schedule later on, in [Create a CSP account in KeyControl for AWS](#).



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



- 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 a CSP account in KeyControl for AWS](#). Then select **Done**.



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

## 4.1. Create a CSP account in KeyControl for AWS

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 an AWS IAM user service account](#).
8. In the **AWS Secret Access Key** text box, enter the **Secret access key** created in [Create an AWS IAM user service account](#).
9. In the **Default region**, choose your AWS region. Then select **Continue**.

For example:



Add CSP Account ✕

Details
Schedule

Name \*

Description

Admin Group \*

Type \*

AWS Access Key ID \*

AWS Secret Access Key \*

Default Region ⓘ

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

Add CSP Account ✕

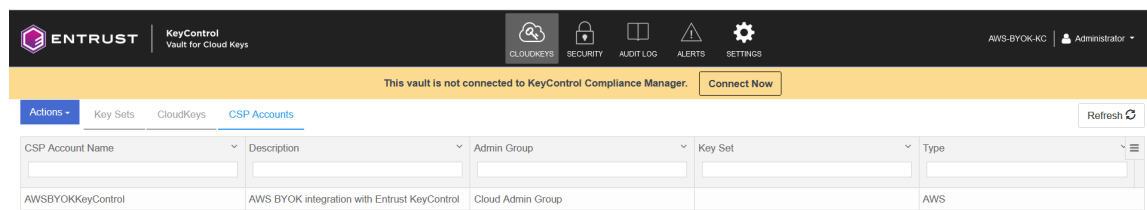
Details
Schedule

Define a schedule for which access keys are rotated.

Rotation Schedule \*  
 Never    Define Schedule

Every   (max limit is 1096 days)

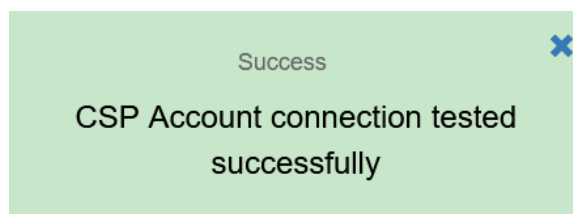
11. Notice the newly created CSP account.



CSP Account Name	Description	Admin Group	Key Set	Type
AWSBYOKKeyControl	AWS BYOK integration with Entrust KeyControl	Cloud Admin Group		AWS

## 4.2. Test the CSP account connection to AWS

1. Select the newly created CSP account.
2. In the **Actions** pull-down menu, select **Test Connection**. The connection tested successfully pop-up windows appears.



## 4.3. Create a Key Set in KeyControl for AWS

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:

×

### Create Key Set

Details
CSP Account
HSM
Schedule

---

Name \*

Description

Admin Group \*

Cloud Admin Group
▼

Cancel
Continue

- In the **CSP Account** tab, select the CSP account created in [Create a CSP account in KeyControl for AWS](#). Uncheck **Use as External Key Store**. Then select **Continue**.

For example:

×

### Create Key Set

Details
CSP Account
HSM
Schedule

---

CSP Account \*

Choose an existing CSP Account or add a new one to use with this Key Set.

AWSBYOKKeyControl
▼

[+ Add CSP Account](#)

External Key Store

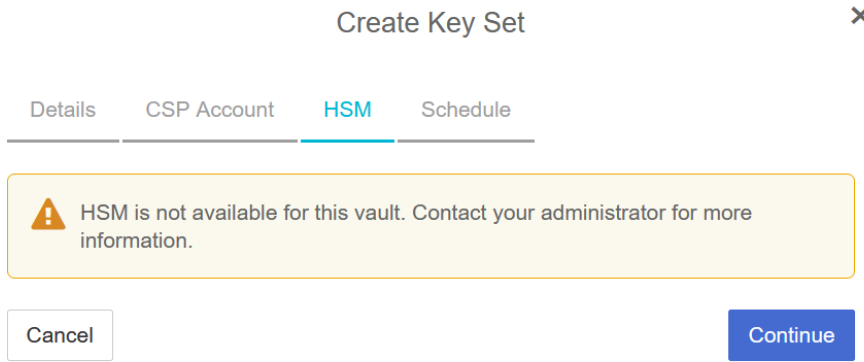
Enabling external key store allows KeyControl to encrypt and decrypt KMS keys.

Use as External Key Store

Cancel
Continue

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

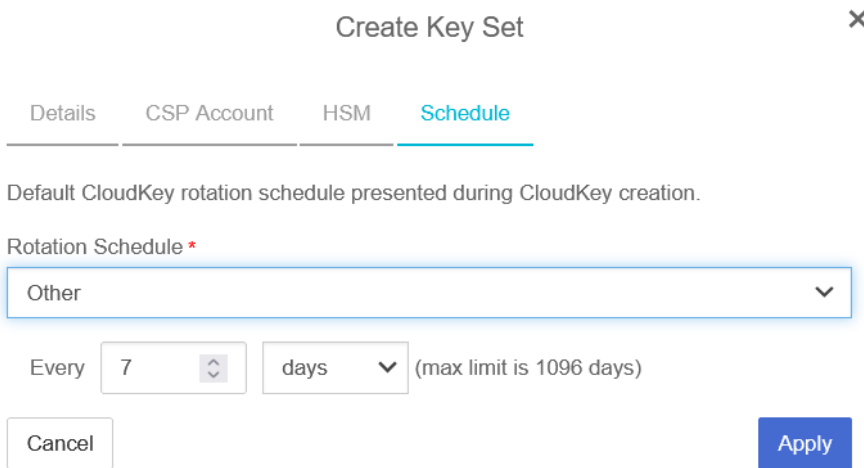
For example:



See [Integrating with an HSM](#) for additional information.

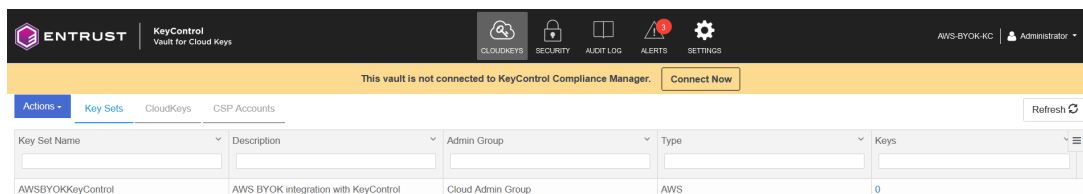
8. In the **Schedule** tab, select a **Rotation Schedule**. Then select **Apply**.

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.

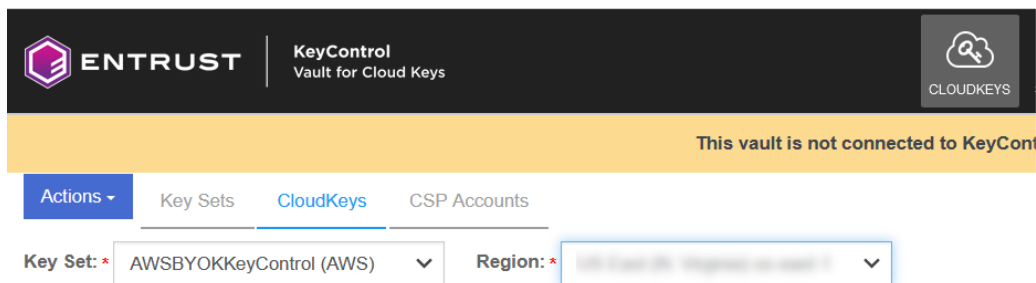
---

# Chapter 5. Test the integration

## 5.1. Create a single-region 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 for AWS](#). In the **Region** pull-down menu, select your region.

For example:



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**. Uncheck **Create as Multi-Region Key**. Then select **Continue**.

For example:

**Create CloudKey** ✕

DetailsPurposeAccessSchedule

Type	<b>AWS</b>
Key Set	<b>AWSBYOKKeyControl</b>
Region	<b>us-east-1</b>

**Create as Multi-Region Key**

Name \*

SingleRegionCloudKeyKeyControl

Description

Single region cloud key created in Entrust KeyControl

CancelContinue

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

For example:

**Create CloudKey** ✕

DetailsPurposeAccessSchedule

Choosing a purpose will determine the key type and algorithm selection

Purpose \*

Symmetric Encrypt and decrypt ▼

Algorithm \*

AES-256 ▼

CancelContinue

7. In the **Access** tab, choose the **Administrators** and **Users**. Then select **Continue**.

For example:

## Create CloudKey



Details **Access** Schedule

### Administrators

Choose users (AWS IAM users) who should have administrative rights to the key.

service-byok-keycontrol x Add an Administrator

### Users

Choose users (AWS IAM users) who can use key to encrypt/decrypt.

service-byok-keycontrol x Add a User

Cancel

Continue

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

For example:

## Create CloudKey



Details Access **Schedule**

### Rotation Schedule \*

Define a schedule for which the CloudKey will be rotated.

Inherit from keyset (Once 7 days) v

### Expiration \*

Define when the CloudKey should be expired.

Never  Choose a date

Cancel

Apply

9. Notice the newly created cloud key.

The screenshot shows the Entrust KeyControl interface. At the top, there's a navigation bar with 'ENTRUST KeyControl Vault for Cloud Keys' and several icons: CLOUDKEYS, SECURITY, AUDIT LOG, ALERTS (with a red '23' notification), and SETTINGS. A yellow banner below the navigation bar states 'This vault is not connected to KeyControl Compliance Manager. Connect Now'. Below the banner, there are tabs for 'Actions', 'Key Sets', 'CloudKeys', and 'CSP Accounts'. The 'CloudKeys' tab is active. Underneath, there are dropdown menus for 'Key Set: AWSBYOKKeyControl (AWS)' and 'Region: All'. A table below displays the list of CloudKeys:

CloudKey Name	Description	Region	Multi-Region	Expires	Cloud Status
SingleRegionCloudKeyKeyControl	Single region cloud key created in Entrust KeyControl	US East (N. Virginia) us-east-1		Never	AVAILABLE

## 5.2. Create a multi-region cloud key in KeyControl

1. Repeat the steps in [Create a single-region cloud key in KeyControl](#), this time checking the box for **Create as Multi-Region Key**.

For example:

Create CloudKey ×

[Details](#) [Purpose](#) [Access](#) [Schedule](#)

Type **AWS**  
Key Set **AWSBYOKKeyControl**  
Primary Region **us-east-1**

Create as Multi-Region Key

Name \*

MultiRegionCloudKeyKeyControl

Description

Multi-region cloud key created in KeyControl

2. Select the multi-region cloud key just created. In the **Actions** pull down menu, select **Create Replica CloudKey**.
3. In the **Create Replica Key** window, select a **Replica Region** from the pull-down menu. Then select **Create Replica Key**.

For example:

Create Replica Key ×

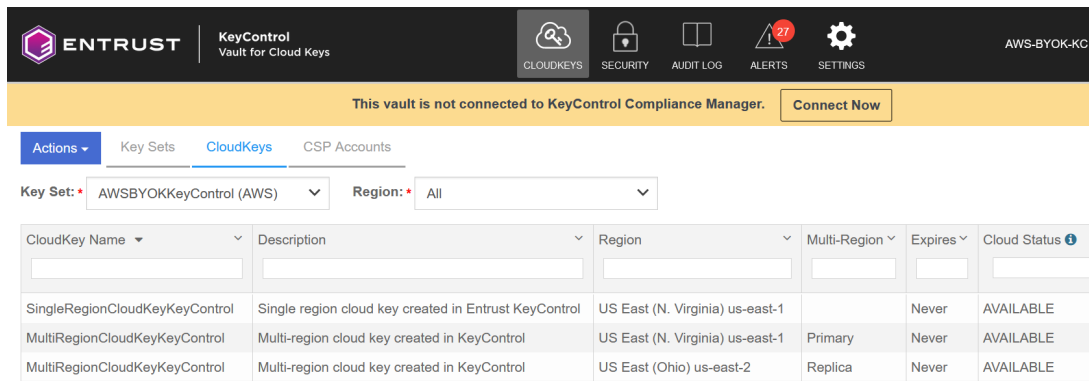
Key Name **MultiRegionCloudKeyKeyControl**  
Primary Region **US East (N. Virginia) us-east-1**

Replica Region \*

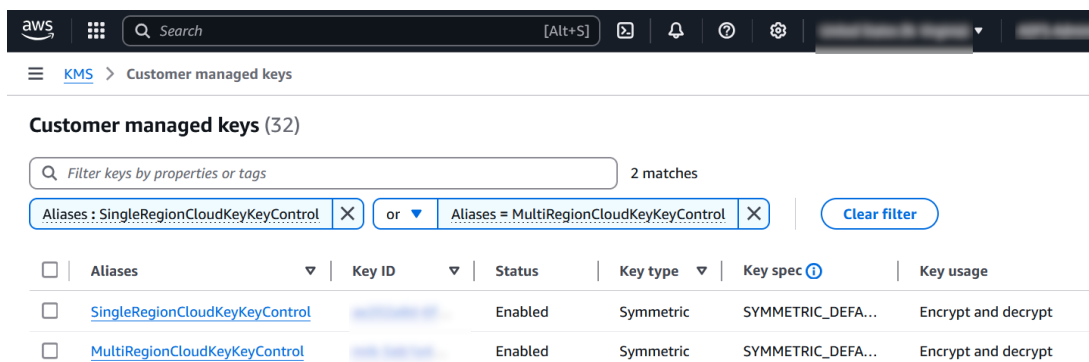
US East (Ohio) us-east-2



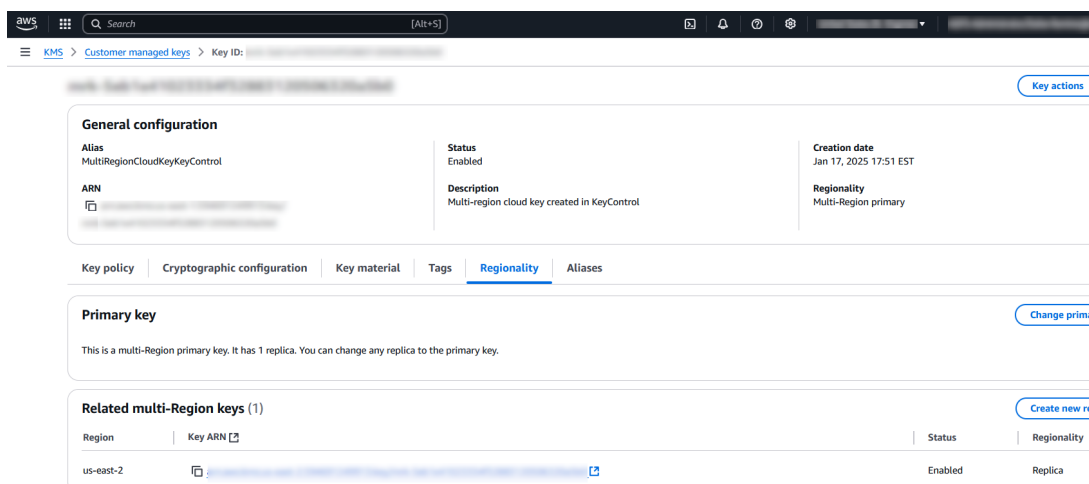
4. Notice the newly created multi-region cloud key.



5. Verify the newly created multi-region cloud key is visible in AWS Key Management Service.



6. Select the newly created multi-region cloud key. In the regionality tab, notice the second region.



For further information, refer to [Creating a CloudKey](#) in the KeyControl online documentation.

## 5.3. Create a cloud key in AWS Key Management Service

1. In AWS, navigate to **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 **Multi-Region key** radio button. Then select **Next**.

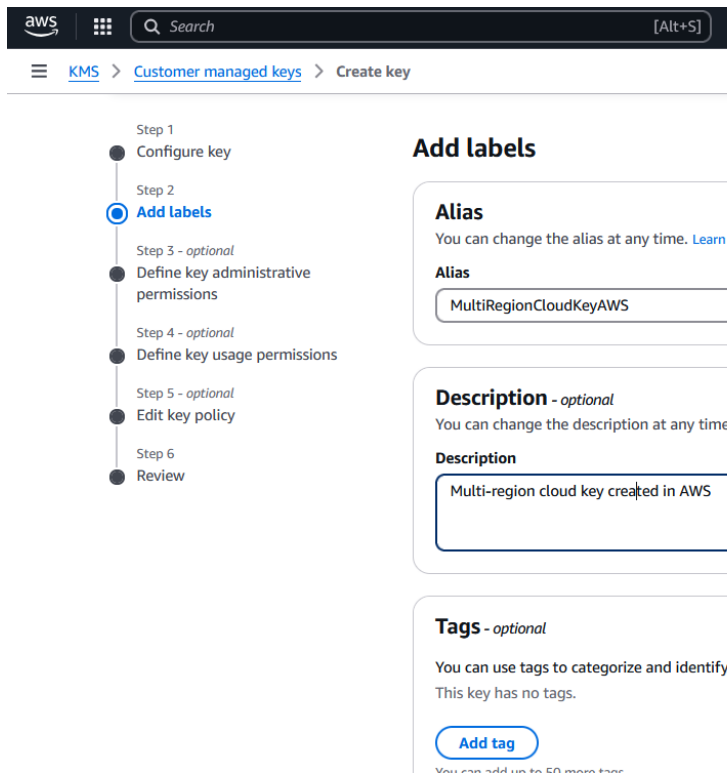
For example:

The screenshot shows the 'Configure key' window in AWS Key Management Service. It is divided into several sections:

- Key type** [Help me choose](#): Two options are shown. 'Symmetric' (selected) is described as 'A single key used for encrypting and decrypting data or generating and verifying HMAC codes'. 'Asymmetric' is described as 'A public and private key pair used for deriving shared secrets'.
- Key usage** [Help me choose](#): Two options are shown. 'Encrypt and decrypt' (selected) is described as 'Use the key only to encrypt and decrypt data.'. 'Generate and verify MAC' is described as 'Use the key only to generate and verify MACs'.
- Advanced options** (expanded):
  - Key material origin**: Described as 'Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. [Help me choose](#)'. Two options are shown: 'KMS - recommended' (selected) with the note 'AWS KMS creates and manages the key material for the KMS key.', and 'External (Import Key material)' with the note 'You create and import the key material'.
  - Regionality**: Described as 'Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. [Help me choose](#)'. Two options are shown: 'Single-Region key' (Never allow this key to be replicated into other Regions) and 'Multi-Region key' (selected) (Allow this key to be replicated into other Regions).

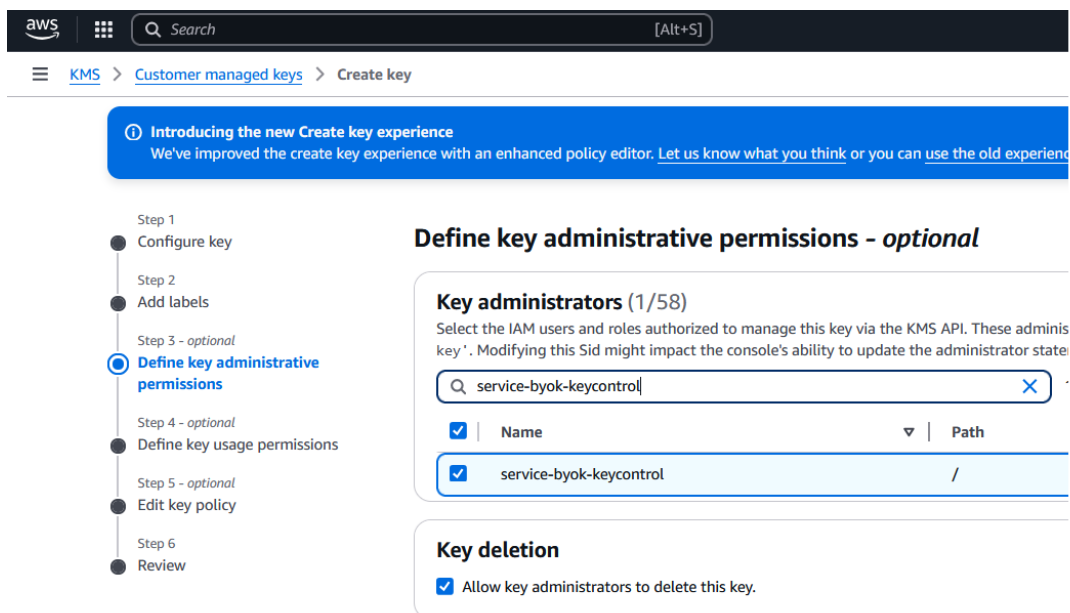
3. In the **Add labels** window, enter the **Alias** and **Description**. Then select **Next**.

For example:



- In the **Define key administrative permissions - optional** window, enter the service account name created in [Create an AWS IAM user service account](#) and select it. In the **Key deletion** section, check **Allow key administrators to delete this key**. Then select **Next**.

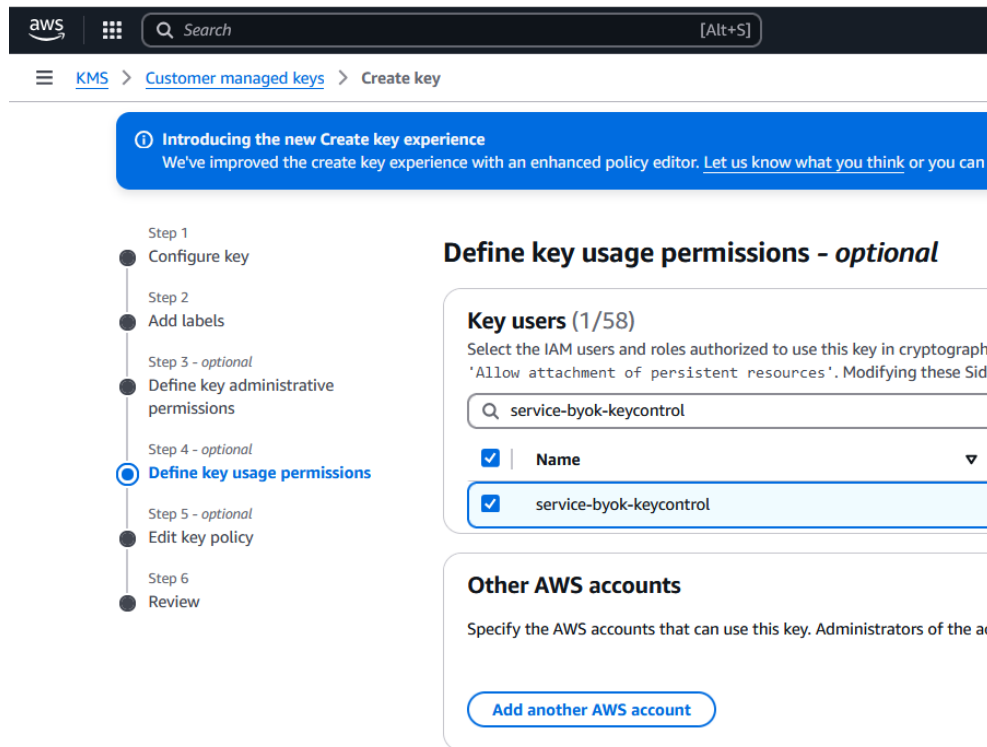
For example:



- In the **Define key usage permissions - optional** window, enter the service account name created in [Create an AWS IAM user service account](#) and select

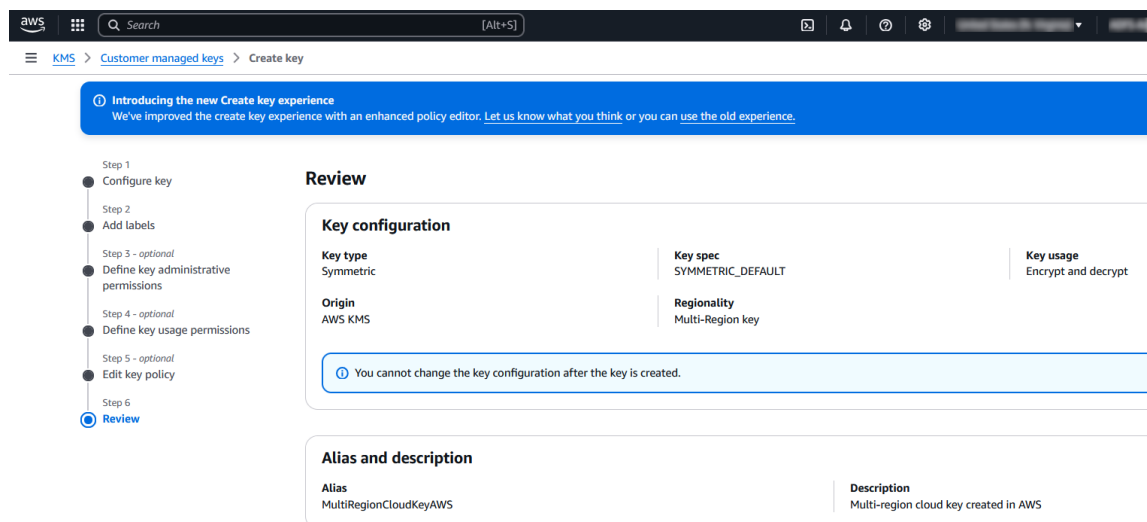
it. Then select **Next**.

For example:

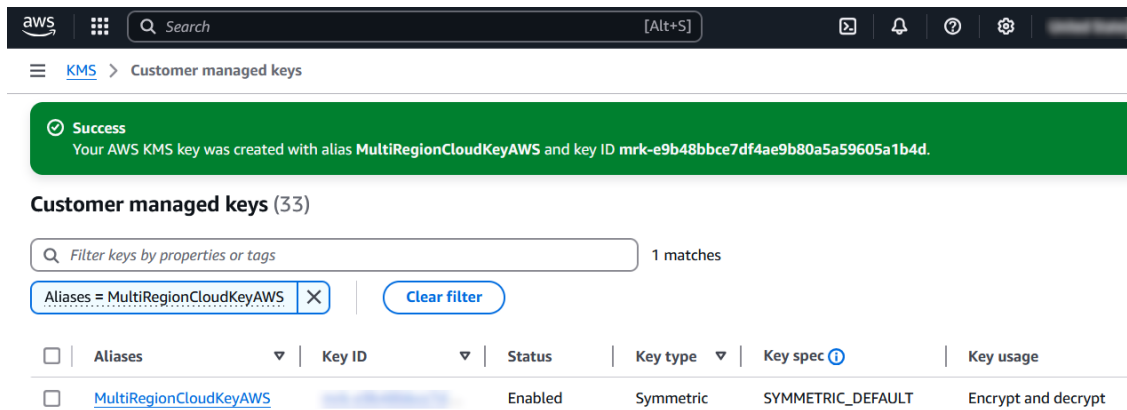


6. In the **Edit key policy - optional** window, select **Next**.

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

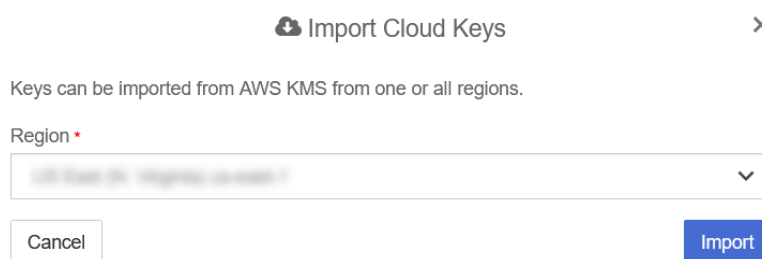


8. Notice the newly created cloud key in AWS Key Management Service.

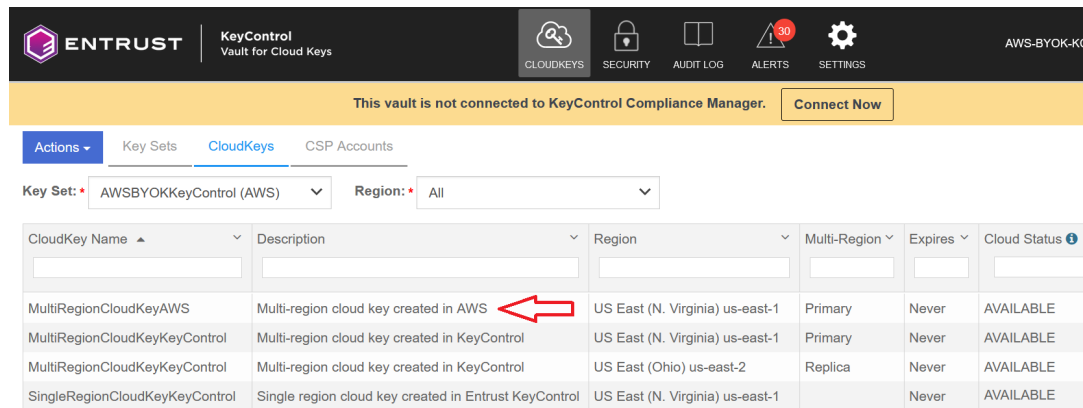


## 5.4. Import a cloud key created in AWS Key Management Service into KeyControl

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 for AWS](#).
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 KeyControl cloud keys vault.



The screenshot shows the Entrust KeyControl interface. At the top, there is a navigation bar with the Entrust logo, 'KeyControl Vault for Cloud Keys', and several icons: CLOUDKEYS, SECURITY, AUDIT LOG, ALERTS (with a red '30' notification), and SETTINGS. A yellow banner below the navigation bar states 'This vault is not connected to KeyControl Compliance Manager.' with a 'Connect Now' button. Below the banner, there are tabs for 'Actions', 'Key Sets', 'CloudKeys', and 'CSP Accounts'. The 'CloudKeys' tab is active. Below the tabs, there are two dropdown menus: 'Key Set: \* AWSBYOKKeyControl (AWS)' and 'Region: \* All'. Below these are two columns of dropdown menus for 'CloudKey Name' and 'Description'. Below the dropdowns is a table with the following data:

CloudKey Name	Description	Region	Multi-Region	Expires	Cloud Status
MultiRegionCloudKeyAWS	Multi-region cloud key created in AWS	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (Ohio) us-east-2	Replica	Never	AVAILABLE
SingleRegionCloudKeyKeyControl	Single region cloud key created in Entrust KeyControl	US East (N. Virginia) us-east-1		Never	AVAILABLE


For further information, refer to [Importing CloudKeys](#) in the KeyControl online documentation.

## 5.5. 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 for AWS](#). 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:

## Remove from Cloud ✕

 Removing the key from the cloud will remove the key material from the KMS. An application will no longer be able to use this key from the cloud.

KeyControl Vault will keep a copy of the key. This copy can always be uploaded back to the cloud.

Are you sure you want to remove the following CloudKey from the cloud?

CloudKey **SingleRegionCloudKeyKeyControl**

KeyId

Type CloudKey Name \*

SingleRegionCloudKeyKeyControl

Cancel

Remove

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

For example:

CloudKey Name	Description	Region	Multi-Region	Expires	Cloud Status
MultiRegionCloudKeyAWS	Multi-region cloud key created in AWS	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (Ohio) us-east-2	Replica	Never	AVAILABLE
SingleRegionCloudKeyKeyControl	Single region cloud key created in Entrust KeyControl	US East (N. Virginia) us-east-1		Never	NOT AVAILABLE

8. Verify the key **Status** changed in AWS Key Management Service.

General configuration	
<p><b>Alias</b> SingleRegionCloudKeyKeyControl</p> <p><b>ARN</b> [Redacted]</p>	<p><b>Status</b> Pending import</p> <p><b>Description</b> Single region cloud key created in Entrust KeyControl</p> <p><b>Creation date</b> Jan 17, 2025 16:10 EST</p> <p><b>Regionality</b> Single Region</p>

For further information, refer to [Removing a CloudKey from the Cloud](#) in the

KeyControl online documentation.

## 5.6. 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 for AWS](#). 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:

Delete CloudKey

The deletion of the following CloudKey will not take effect immediately. However the key will be removed from the cloud and the key will not be available to use by any application.

CloudKey **SingleRegionCloudKeyKeyControl**

KeyId **[REDACTED]**

Define when the CloudKey should be permanently deleted.

30 days

Cancel Delete

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



CloudKey Name	Description	Region	Multi-Region	Expires	Cloud Status
MultiRegionCloudKeyAWS	Multi-region cloud key created in AWS	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (Ohio) us-east-2	Replica	Never	AVAILABLE
SingleRegionCloudKeyKeyControl	Single region cloud key created in Entrust KeyControl	US East (N. Virginia) us-east-1		Never	PENDING DELETE

8. Verify the key **Status** changed in AWS Key Management Service.

**Key Management Service (KMS)**

Customer managed keys > Key ID: **arn:aws:kms:us-east-1:123456789012:key:12345678-9012-3456-7890-123456789012**

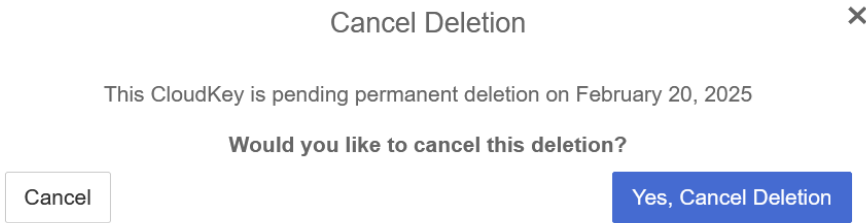
**General configuration**

<b>Alias</b> SingleRegionCloudKeyKeyControl	<b>Status</b> Pending deletion	<b>Creation date</b> Jan 17, 2025 16:10 EST
<b>ARN</b> arn:aws:kms:us-east-1:123456789012:key:12345678-9012-3456-7890-123456789012	<b>Description</b> Single region cloud key created in Entrust KeyControl	<b>Scheduled deletion date</b> Feb 20, 2025 11:43 EST
<b>Regionality</b> Single Region		

For further information, refer to [Deleting a CloudKey](#) in the KeyControl online documentation.

## 5.7. Cancel a cloud key deletion in KeyControl

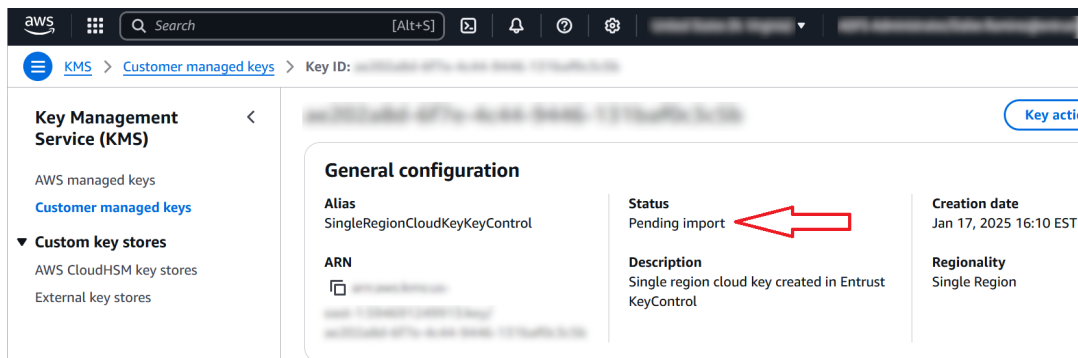
1. Sign in to the cloud keys vault URL created in [Create a Cloud Keys Vault in the KeyControl](#).
2. Select the **CloudKeys** tab.
3. In the **Key Set** pull-down menu, select the key set created in [Create a Key Set in KeyControl for AWS](#). In the **Region** pull-down menu, select your region.
4. 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**.

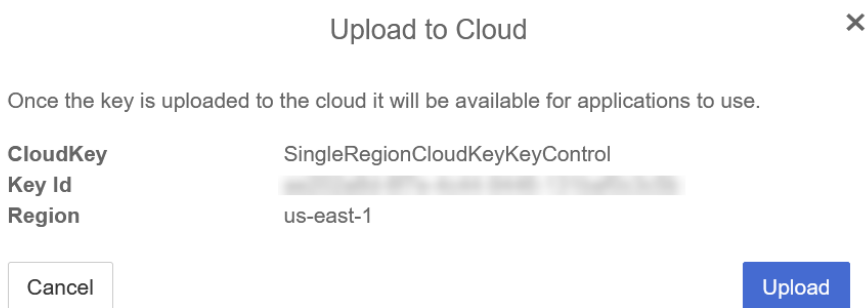
CloudKey Name	Description	Region	Multi-Region	Expires	Cloud Status
MultiRegionCloudKeyAWS	Multi-region cloud key created in AWS	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (Ohio) us-east-2	Replica	Never	AVAILABLE
SingleRegionCloudKeyKeyControl	Single region cloud key created in Entrust KeyControl	US East (N. Virginia) us-east-1		Never	NOT AVAILABLE

8. Verify the key **Status** changed in AWS Key Management Service.



9. Back in 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**.

CloudKey Name	Description	Region	Multi-Region	Expires	Cloud Status
MultiRegionCloudKeyAWS	Multi-region cloud key created in AWS	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (N. Virginia) us-east-1	Primary	Never	AVAILABLE
MultiRegionCloudKeyKeyControl	Multi-region cloud key created in KeyControl	US East (Ohio) us-east-2	Replica	Never	AVAILABLE
SingleRegionCloudKeyKeyControl	Single region cloud key created in Entrust KeyControl	US East (N. Virginia) us-east-1		Never	AVAILABLE

12. Verify the key **Status** changed in AWS Key Management Service.

**Key Management Service (KMS)**

Customer managed keys

**General configuration**

<b>Alias</b> SingleRegionCloudKeyKeyControl	<b>Status</b> Enabled	<b>Creation date</b> Jan 17, 2025 16:10 EST
<b>ARN</b> arn:aws:kms:us-east-1:123456789012:key:abcd1234-5678-9012-3456-789012345678	<b>Description</b> Single region cloud key created in Entrust KeyControl	<b>Regionality</b> Single Region

For further information, refer to [Canceling a CloudKey Deletion](#) in the KeyControl online documentation.

## 5.8. 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 for AWS](#). 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.

The screenshot shows the Entrust KeyControl interface. At the top, there is a navigation bar with the Entrust logo, the text 'KeyControl Vault for Cloud Keys', and icons for 'CLOUDKEYS' and 'SECURITY'. Below this is a detailed view of a key with the following information:

- Name:** MultiRegionCloudKeyKeyControl
- Key Id:** mrk-5eb1e41023334f32883120506320a5b0
- Description:** Multi-region cloud key created in KeyControl
- Cloud Status:** AVAILABLE
- Key Source:** KEYCONTROL
- Key Set:** AWSBYOKKeyControl
- Algorithm:** AES-256
- Key Type:** Symmetric
- Purpose:** Symmetric Encrypt and decrypt
- Region:** US East (N. Virginia) us-east-1
- Multi-Region:** Primary: US East (N. Virginia) us-east-1; Replicas: US East (Ohio) us-east-2. A 'Change Primary Region' button is visible.
- Rotation Schedule:** Every 1 week. A 'Rotate Now' button is visible.
- Key Upload Date:** 01/17/2025

6. Verify the key has been rotated in AWS Key Management Service.

The screenshot shows the AWS Management Console interface for 'Customer managed keys'. The page title is 'Customer managed keys (34)'. A search bar contains the text 'Filter keys by properties or tags' and shows '4 matches'. A filter is applied: 'Regionality = Multi Region'. A 'Clear filter' button is next to it. A 'Key actions' button is in the top right corner. Below the filter, a table lists the keys:

<input type="checkbox"/>	Aliases	▲	Key ID ▼	Status	Key type ▼	Key spec ⓘ	Key usage
<input type="checkbox"/>	-		Old <a href="#">mrk-5eb1...</a>	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt
<input type="checkbox"/>	<a href="#">MultiRegionCloudKeyAWS</a>		<a href="#">mrk-e9b4...</a>	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt
<input type="checkbox"/>	<a href="#">MultiRegionCloudKeyKeyControl</a>	New	<a href="#">mrk-15f2...</a>	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

---

## Chapter 6. Integrating with an HSM

For guidance on integrating the 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](#)