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

Integration Guide

01 Jul 2022

Contents

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).

1.1. Documents to read first

This guide describes how to configure the Entrust KeyControl server as a KMS in AWS BYOK.

To install and configure the Entrust KeyControl server as a KMIP server, see the `Entrust KeyControl nShield HSM Integration Guide`. You can access this in the Entrust Document Library.

Also refer to the documentation and set-up process for AWS Key Management Service (KMS) in AWS Key Management Service.

Also refer to video for the set-up process with IAM at Getting Started with AWS Identity and Access Management.

1.2. Product configurations

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

System	Version
Entrust KeyControl	5.5.1

2. Procedures

Follow these steps to install and configure KeyControl with VSP.

- Install and configure Entrust KeyControl
- Create a customer managed policy in AWS
- Create IAM User in AWS
- Attach a policy to an IAM user in AWS
- Create an AWS CSP account
- Create a key set in KeyControl
- Create a cloud key in KeyControl
- Create a cloud key in AWS Key Management Service
- Remove a cloud key in KeyControl
- Delete a cloud key in KeyControl
- Cancel a cloud key deletion in KeyControl
- Rotate a cloud key in KeyControl

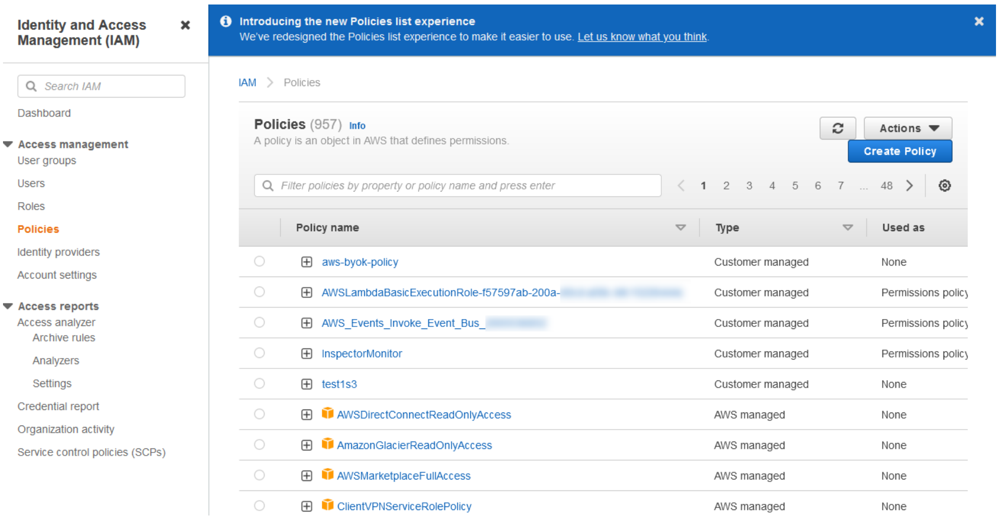
2.1. Install and configure Entrust KeyControl

Follow the installation and set-up instructions in the `Entrust KeyControl nShield HSM Integration Guide`. You can access this in the Entrust Document Library.

2.2. Create a customer managed policy in AWS

To create a customer managed policy in AWS:

1. Go to the IAM Service and select **Access management** > **Policies** from the left menu.
2. On the **Policies** page, select **Actions** > **Create Policy**. For example:



Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

Policies (957) Info
A policy is an object in AWS that defines permissions.

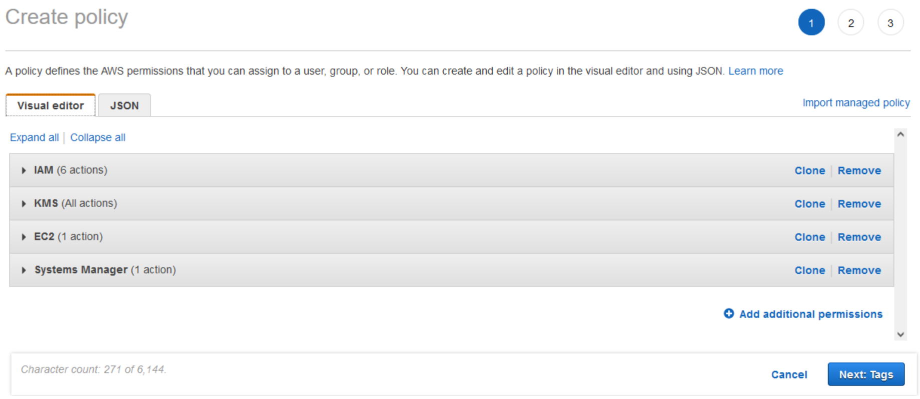
Filter policies by property or policy name and press enter

	Policy name	Type	Used as
○	aws-byok-policy	Customer managed	None
○	AWSLambdaBasicExecutionRole-f57597ab-200a-[redacted]	Customer managed	Permissions policy
○	AWS_Events_Invoke_Event_Bus_[redacted]	Customer managed	Permissions policy
○	InspectorMonitor	Customer managed	Permissions policy
○	test1s3	Customer managed	None
○	AWSDirectConnectReadOnlyAccess	AWS managed	None
○	AmazonGlacierReadOnlyAccess	AWS managed	None
○	AWSMarketplaceFullAccess	AWS managed	None
○	ClientVPNServiceRolePolicy	AWS managed	None

3. On the **Create Policy** page, select **Chose a service** and search for **IAM**. Select the following permissions:
    - **IAM GetUser**.
    - **IAM ListUsers**.
    - **IAM ListAccessKeys**.
    - **IAM CreateAccessKey**.
    - **IAM DeleteAccessKey**.
    - **IAM UpdateAccessKey**.
4. Select **Add additional permissions**. Select **Chose a service** and search for **KMS**. Select the following permissions:
    - **All KMS actions**.
5. Select **Add additional permissions**. Select **Chose a service** and search for **EC2**. Select the following permissions:
    - **DescribeRegions**.
6. Select **Add additional permissions**. Select **Chose a service** and search for **Systems Manager**. Select the following permissions:

    - **GetParameter**.

    The permissions should be listed as follows:



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

IAM (6 actions)

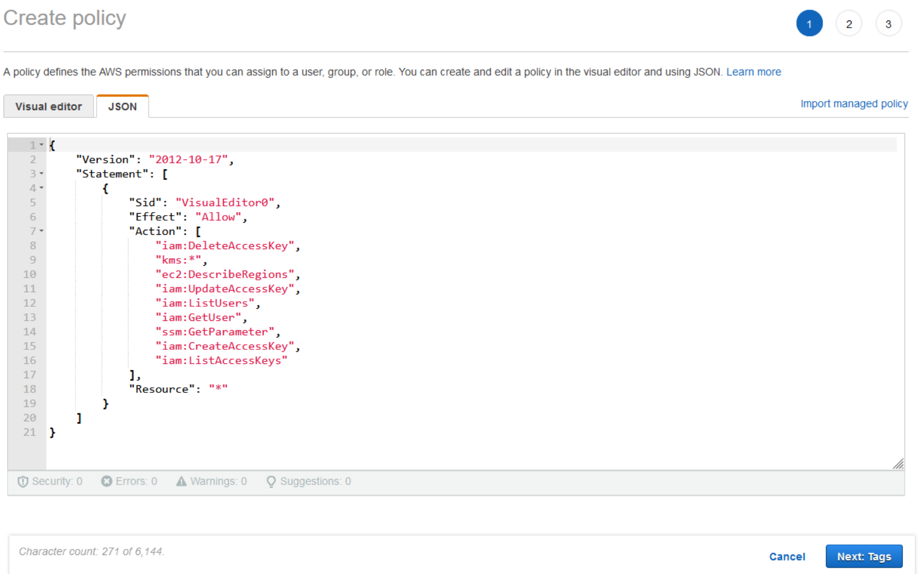
KMS (All actions)

EC2 (1 action)

Systems Manager (1 action)

Character count: 271 of 6,144.

7. Select the **JSON** tab. For example:



Create policy

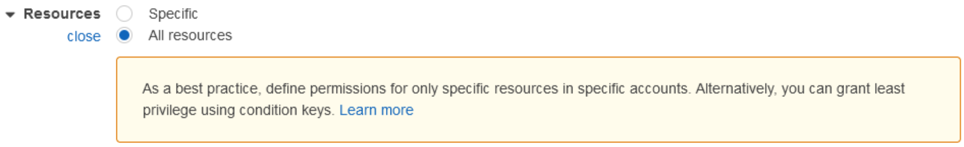
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteAccessKey",
                "kms:*",
                "ec2:DescribeRegions",
                "iam:UpdateAccessKey",
                "iam:ListUsers",
                "iam:GetUser",
                "ssm:GetParameter",
                "iam:CreateAccessKey",
                "iam:ListAccessKeys"
            ],
            "Resource": "*"
        }
    ]
}
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Character count: 271 of 6,144.

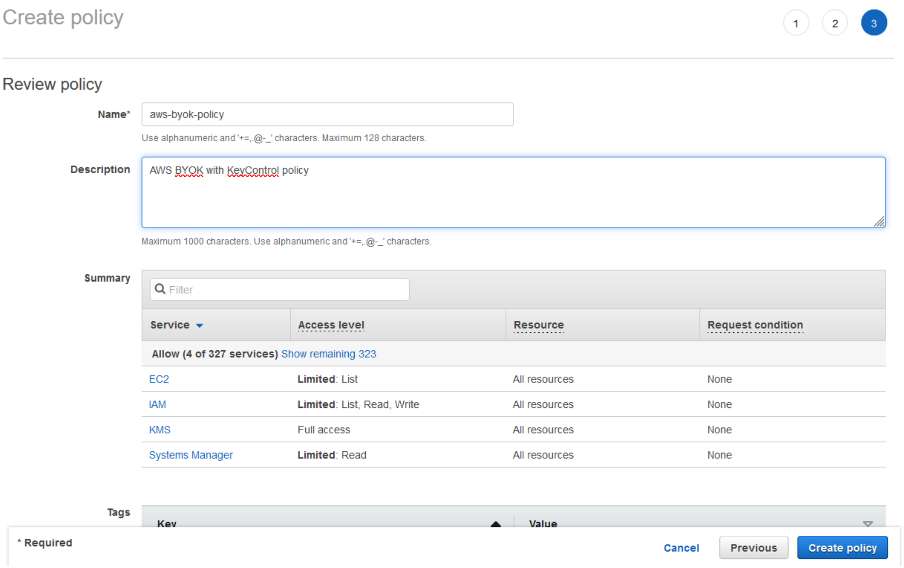
If there are warnings with the resource group, click **All resources**.



○ Specific
● All resources

As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more

8. Select **Next: Tags** and add any appropriate tags.
9. Select **Next: Review** and enter values for the following properties:
   - **Name**.
   - **Description**.
   - **Summary**.
10. Select **Create policy**. For example:



Create policy

Review policy

Name* aws-byok-policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description AWS BYOK with KeyControl policy

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (4 of 327 services) Show remaining 323			
EC2	**Limited**: List	All resources	None
IAM	**Limited**: List, Read, Write	All resources	None
KMS	Full access	All resources	None
Systems Manager	**Limited**: Read	All resources	None

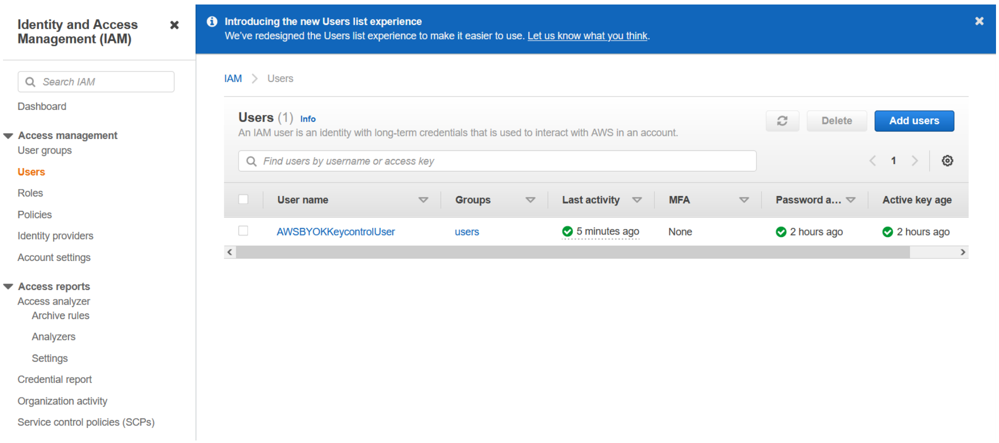
Tags

For further information, refer to the AWS BYOK Service Account Requirements in the KeyControl online documentation.

2.3. Create IAM User in AWS

To create IAM User in AWS:

1. Go to the IAM Service and select **Access management** > **Add users** from the left menu.
2. On the **Users** page, select **Add users**. For example:



Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

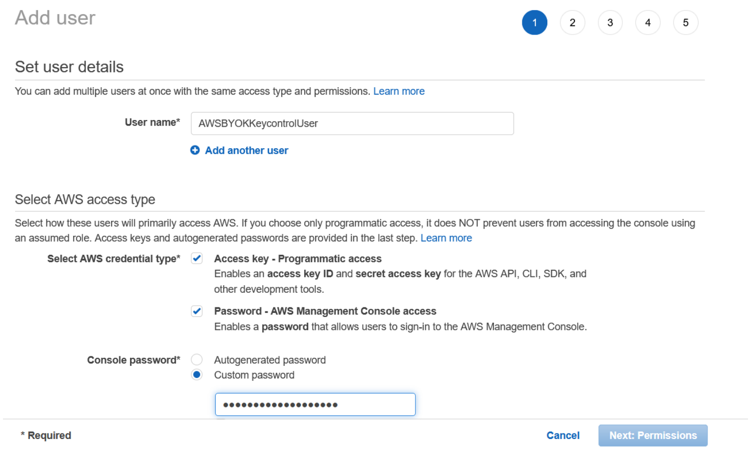
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Groups	Last activity	MFA	Password a...	Active key age
AWSBYOKKeycontrolUser	users	✓ 5 minutes ago	None	✓ 2 hours ago	✓ 2 hours ago

3. Enter values for the following properties:

   - **User name**.
   - **Select AWS credential type**.
   - **Console password**.

   For example:



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* AWSBYOKKeycontrolUser

Select AWS access type

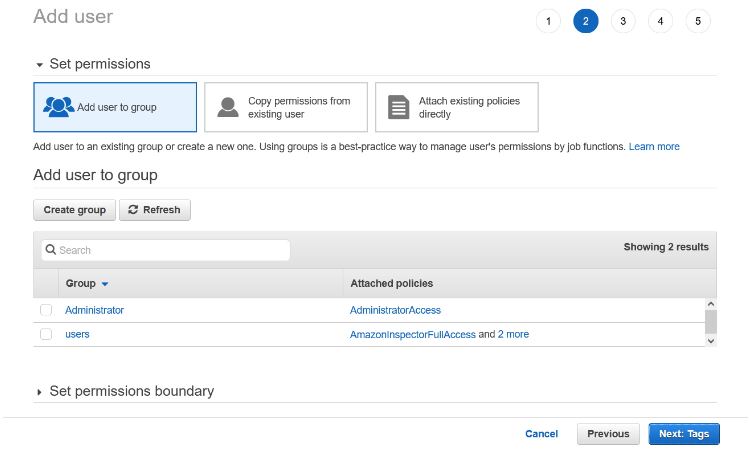
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*
☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
☑ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*
○ Autogenerated password
● Custom password
•••••••••••••••••••

* Required

4. Add the user to a group that complies with your organization's standards.



Add user

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

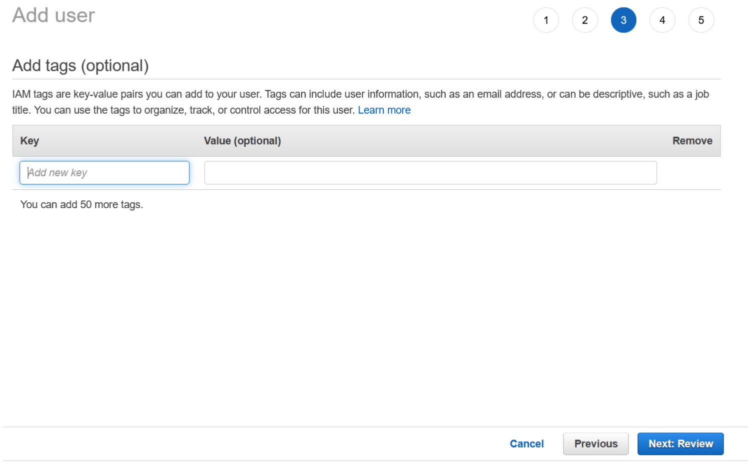
Add user to group

Showing 2 results

	Group	Attached policies
□	Administrator	AdministratorAccess
□	users	AmazonInspectorFullAccess and 2 more

Set permissions boundary

5. Add the necessary tags. For example:



Add user

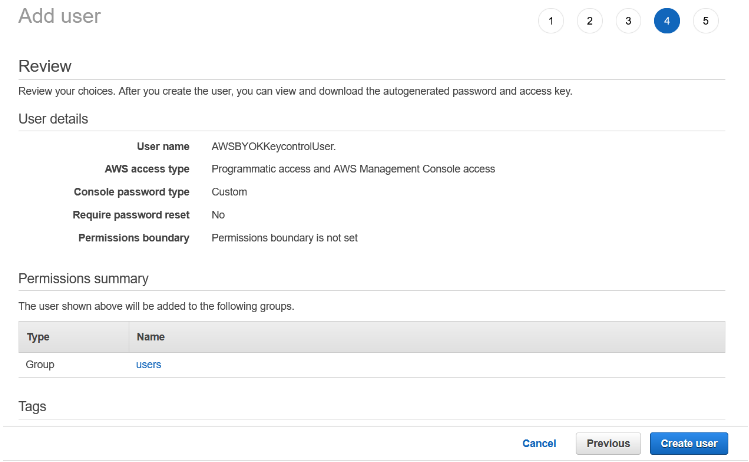
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

6. Review the permissions and then select **Create user**. For example:



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	AWSBYOKKeycontrolUser.
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

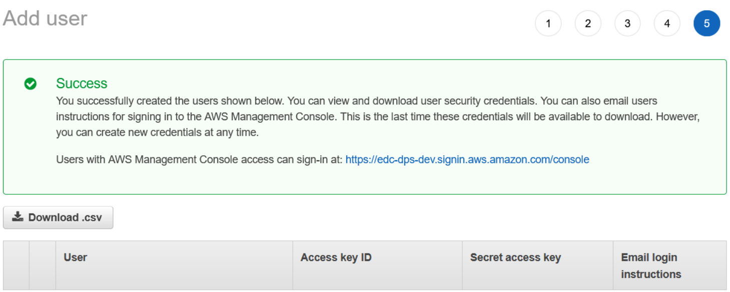
Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	users

Tags

7. Click the hyperlink to download the credentials of the new user. For example:



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

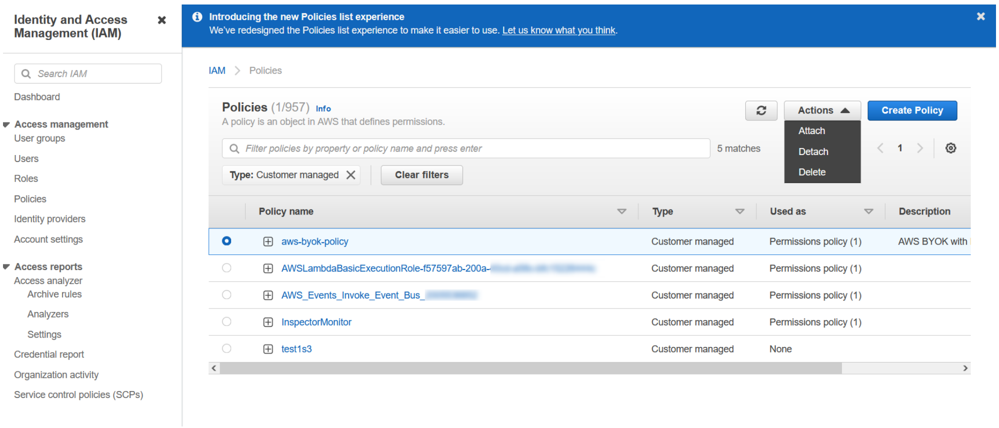
Users with AWS Management Console access can sign-in at: https://edc-dps-dev.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Email login instructions

2.4. Attach a policy to an IAM user in AWS

To attach a policy to an IAM user in AWS:

1. Go to the IAM Service and select **Access management** > **Policies** from the left menu.
2. On the **Policies** page, select your policy (**aws-byok-policy**).
3. Select **Actions** > **Attach**.



Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

Policies (1/957)
A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter

5 matches

Type: Customer managed

	Policy name	Type	Used as	Description
●	aws-byok-policy	Customer managed	Permissions policy (1)	AWS BYOK with
○	AWSLambdaBasicExecutionRole-f57597ab-200a-[redacted]	Customer managed	Permissions policy (1)	
○	AWS_Events_Invoke_Event_Bus_[redacted]	Customer managed	Permissions policy (1)	
○	InspectorMonitor	Customer managed	Permissions policy (1)	
○	test1s3	Customer managed	None	

4. Search for your IAM User (**AWSBYOKKeycontrolUser**) in the search bar and select **Attach policy**.

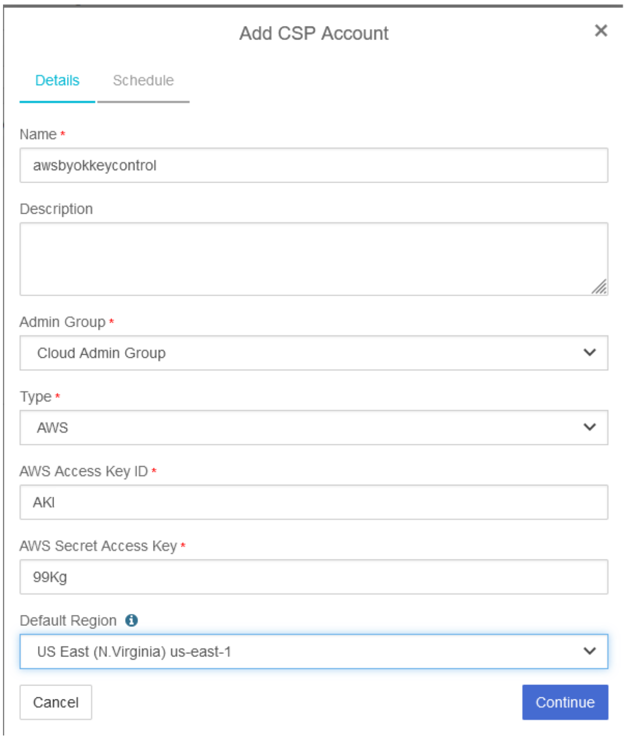
2.5. Create an AWS CSP account

To create an AWS CSP account:

1. In KeyControl, select **BYOK** on the main toolbar.
2. Select the **CSP Accounts** tab.
3. Select **Actions** > **Add CSP Account**.

   The **Add CSP Account** dialog appears.

4. In the **Details** tab, enter the information downloaded during the Create IAM User in AWS process. For example:



Name * awsbyokkeycontrol

Description

Admin Group * Cloud Admin Group

Type * AWS

AWS Access Key ID * AKI

AWS Secret Access Key * 99Kg

Default Region US East (N.Virginia) us-east-1

The region selected has to match your AWS region.

5. In the **Schedule** tab, enter your organization's standard rotation schedule.
6. Select **Apply**.

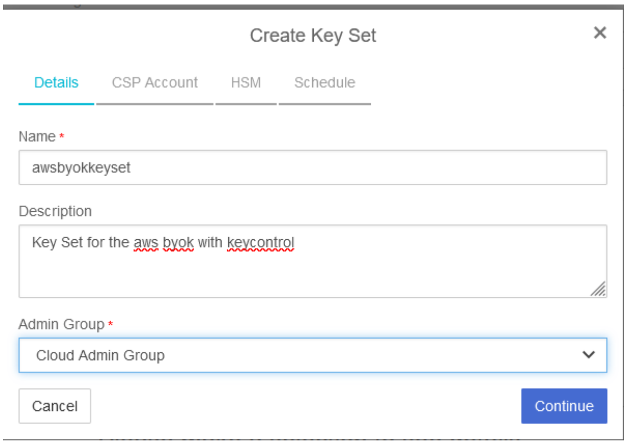
2.6. Create a key set in KeyControl

To create a key set in KeyControl:

1. In KeyControl, select **BYOK** on the main toolbar.
2. Select the **Key Sets** tab.
3. Select **Actions** > **Create Key Set**.

   The **Create Key Set** dialog appears.

4. In the **Details** tab, enter a **Name** and **Description** for the key set. For example:

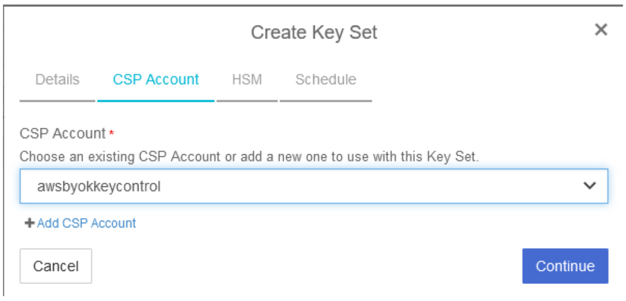


Name *
awsbyokkeyset

Description
Key Set for the aws byok with keycontrol

Admin Group *
Cloud Admin Group

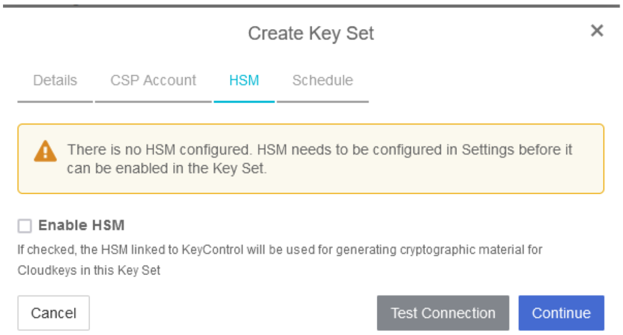
5. Select **Continue**.
6. In the **CSP Account** tab, select the account previously created (**awsbyokkeycontrol**). For example:



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

If no accounts exist, select **Add CSP Account** and add the CSP account, see Create an AWS CSP account.

7. Select **Continue**.
8. In the **HSM** tab, check if an HSM is configured. For example:

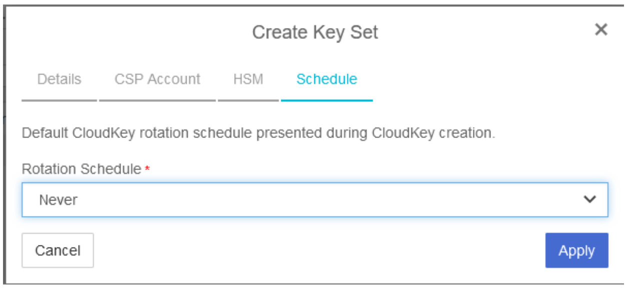


There is no HSM configured. HSM needs to be configured in Settings before it can be enabled in the Key Set.

□ **Enable HSM**
If checked, the HSM linked to KeyControl will be used for generating cryptographic material for Cloudkeys in this Key Set

If no HSM is configured, configure one and then enable it in **Create Key Set**.

9. Select **Continue**.
10. In the **Schedule** tab, select a **Rotation Schedule** matching the selection made during Create an AWS CSP account. For example:

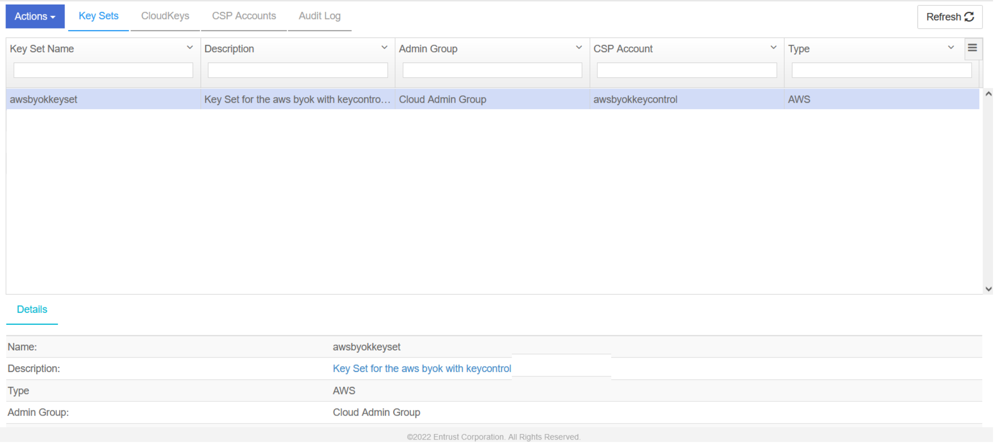


Default CloudKey rotation schedule presented during CloudKey creation.

Rotation Schedule *: Never

11. Select **Apply**.

    The key set is added. For example:



Key Set Name	Description	Admin Group	CSP Account	Type
awsbyokkeyset	Key Set for the aws byok with keycontro…	Cloud Admin Group	awsbyokkeycontrol	AWS

Name:	awsbyokkeyset
Description:	Key Set for the aws byok with keycontrol
Type	AWS
Admin Group:	Cloud Admin Group

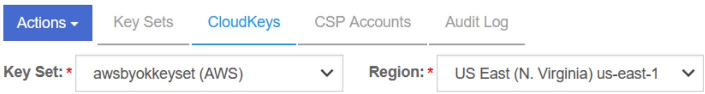
©2022 Entrust Corporation. All Rights Reserved.

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

2.7. Create a cloud key in KeyControl

To create a cloud key in KeyControl: ttach a policy to an IAM user in AWS . In KeyControl, select **BYOK** on the toolbar.

1. Select the **CloudKeys** tab.
2. Select the **Key Set** and **Region**. For example:



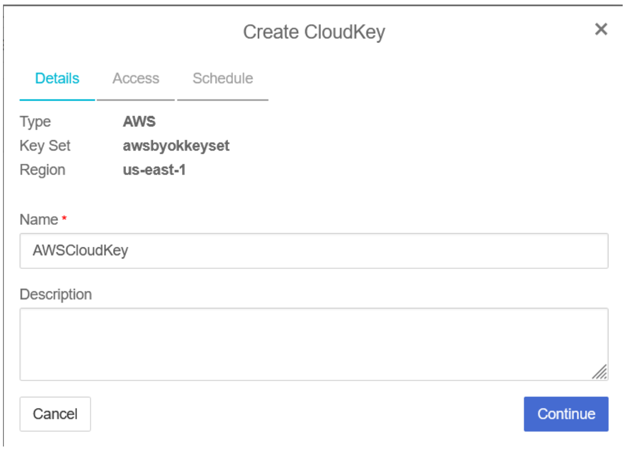
Key Set: * awsbyokkeyset (AWS)

Region: * US East (N. Virginia) us-east-1

3. Select **Actions** > **Create CloudKey**.

    The **Create CloudKey** dialog appears.

4. In the **Details** tab, enter the **Name** and **Description**. For example:

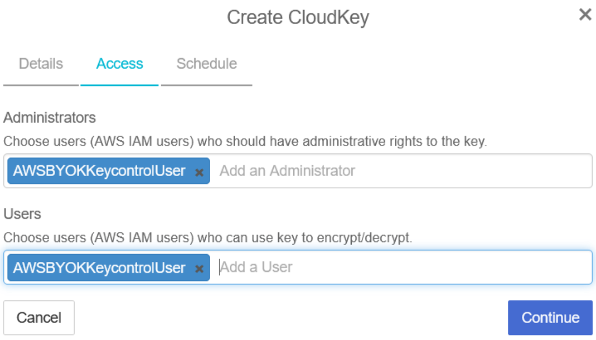


Type AWS
Key Set awsbyokkeyset
Region us-east-1

Name * AWSCloudKey

Description

5. Select **Continue**.
6. In the **Access** tab, select the required access for. For example:



Administrators
Choose users (AWS IAM users) who should have administrative rights to the key.
AWSBYOKKeycontrolUser × Add an Administrator

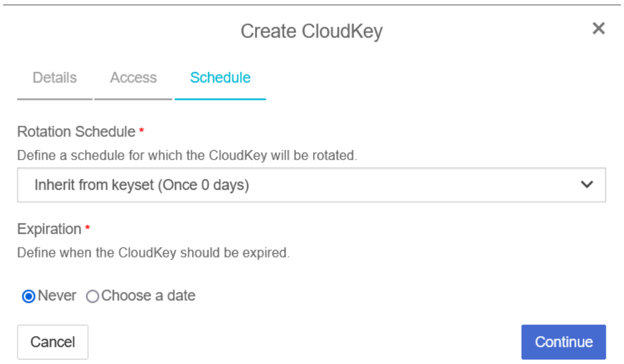
Users
Choose users (AWS IAM users) who can use key to encrypt/decrypt.
AWSBYOKKeycontrolUser × Add a User

7. Select **Continue**.
8. In the **Schedule** tab:

   a. Select a **Rotation Schedule**.

   b. Set **Expiration**.

   For example:



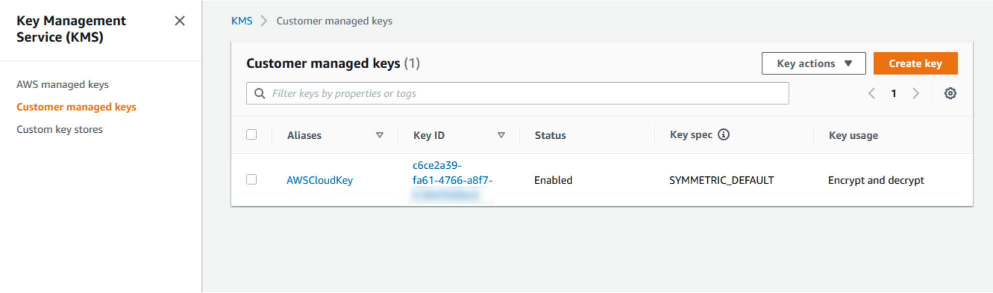
Rotation Schedule *
Define a schedule for which the CloudKey will be rotated.
Inherit from keyset (Once 0 days)

Expiration *
Define when the CloudKey should be expired.
● Never ○ Choose a date

9. Select **Continue**.

   The cloud key is created.

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



Key Management Service (KMS)

- AWS managed keys
- Customer managed keys
- Custom key stores

KMS > Customer managed keys

Customer managed keys (1)

	Aliases	Key ID	Status	Key spec	Key usage
□	AWSCloudKey	c6ce2a39-fa61-4766-a8f7-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

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

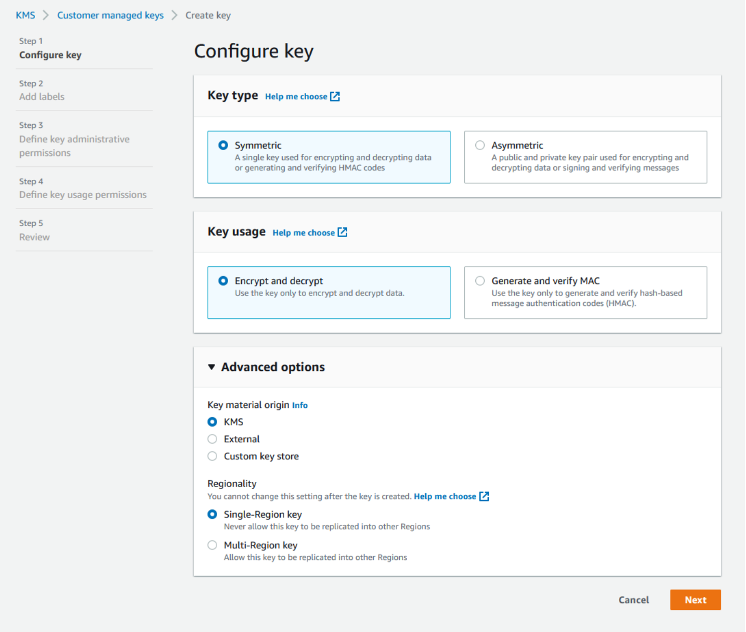
2.8. Create a cloud key in AWS Key Management Service

To create a cloud key in the AWS Key Management Service:

1. Navigate to **Services** > **Key Management Service** > **Customer managed keys** > **Create Key**.

   The **Create a key** dialog appears.

2. Enter the following properties for **Step 1: Configure key**.



KMS > Customer managed keys > Create key

Configure key

Key type

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

○ Asymmetric
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

Key usage

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▼ Advanced options

Key material origin

● KMS

○ External

○ Custom key store

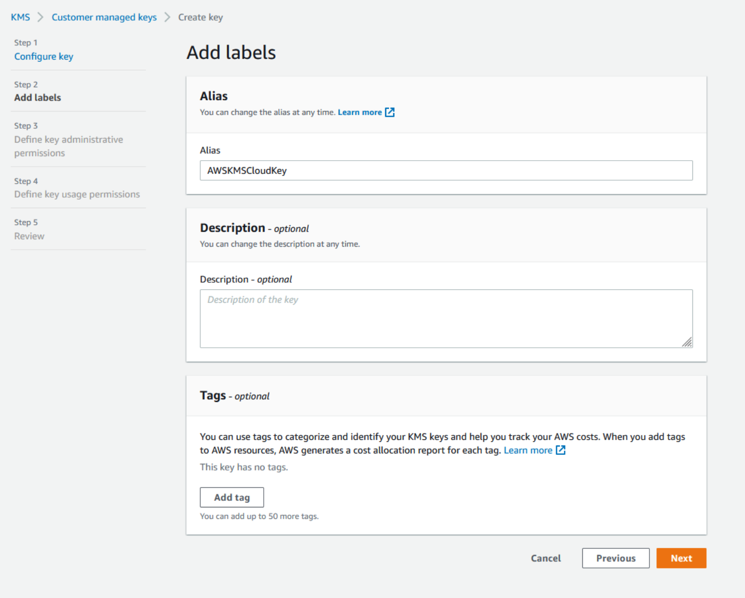
Regionality

You cannot change this setting after the key is created.

● Single-Region key
Never allow this key to be replicated into other Regions

○ Multi-Region key
Allow this key to be replicated into other Regions

3. Select **Next**.
4. Enter the following properties for **Step 2: Add labels**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Add labels

Alias
You can change the alias at any time. Learn more

Alias
AWSKMSCloudKey

Description - *optional*
You can change the description at any time.

Description - *optional*
Description of the key

Tags - *optional*

You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

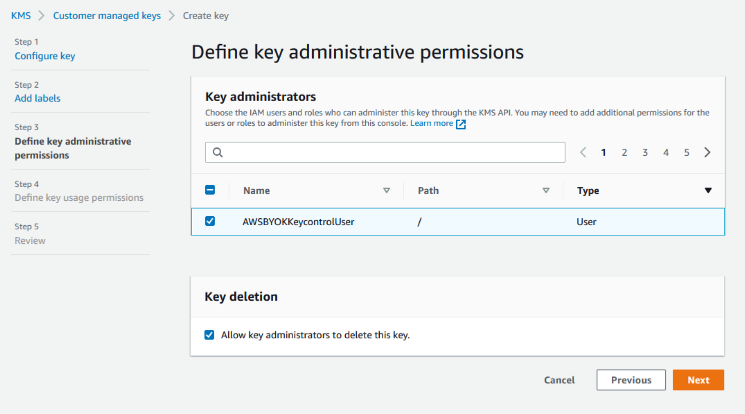
This key has no tags.

Add tag

You can add up to 50 more tags.

Cancel | Previous | Next

5. Select **Next**.
6. Enter the following properties for **Step 3: Define key administrative permissions**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Define key administrative permissions

Key administrators
Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. Learn more

< 1 2 3 4 5 >

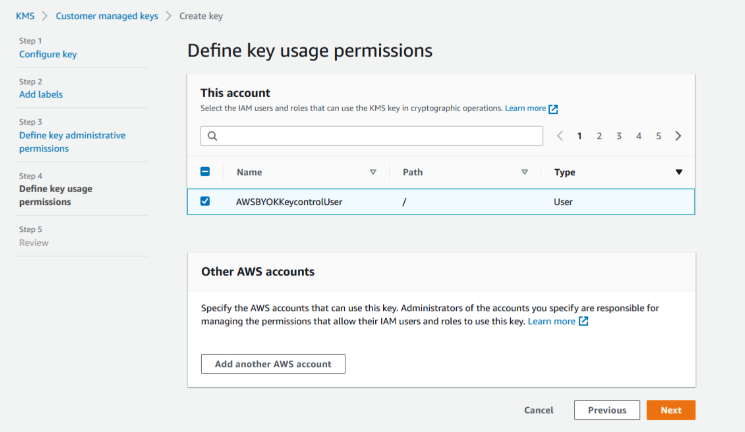
	Name	Path	Type
☑	AWSBYOKKeycontrolUser	/	User

Key deletion

☑ Allow key administrators to delete this key.

Cancel | Previous | Next

7. Select **Next**.
8. Enter the following properties for **Step 4: Define key usage permissions**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Define key usage permissions

This account
Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more

< 1 2 3 4 5 >

	Name	Path	Type
☑	AWSBYOKKeycontrolUser	/	User

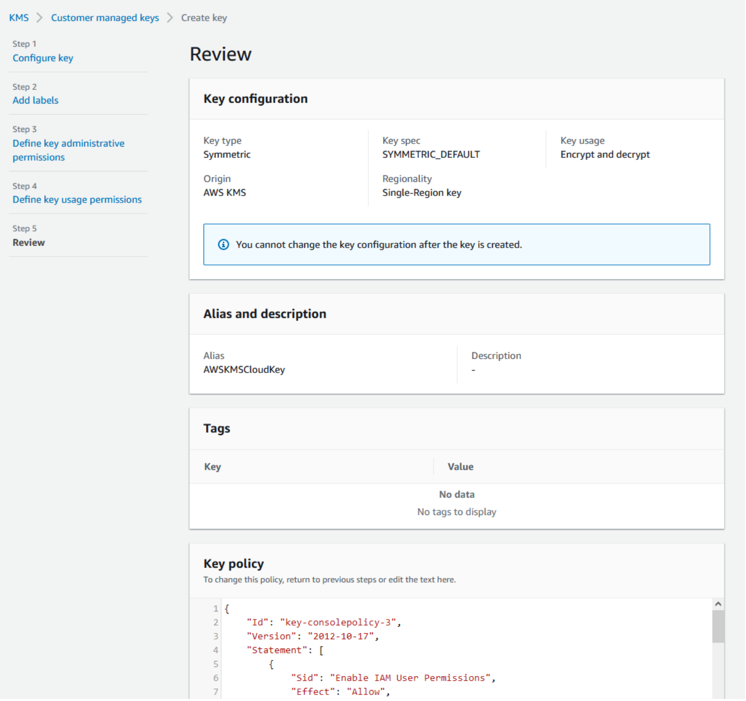
Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more

Add another AWS account

Cancel | Previous | Next

9. Select **Next**.
10. Confirm all information in **Step 5: Review**.



KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review

Review

Key configuration

Key type: Symmetric

Key spec: SYMMETRIC_DEFAULT

Key usage: Encrypt and decrypt

Origin: AWS KMS

Regionality: Single-Region key

You cannot change the key configuration after the key is created.

Alias and description

Alias: AWSKMSCloudKey

Description: -

Tags

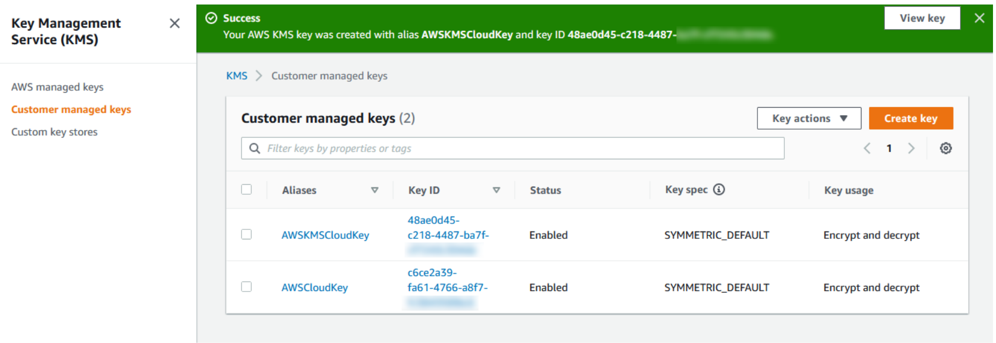
Key	Value
No data No tags to display	

Key policy

To change this policy, return to previous steps or edit the text here.

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
```

11. Note the new key in the AWS KMS.



Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
View key
KMS > Customer managed keys
Key actions
Create key
Filter keys by properties or tags
1

Success

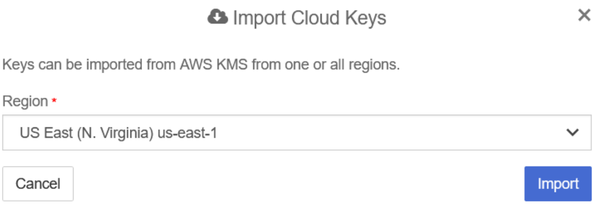
Your AWS KMS key was created with alias **AWSKMSCloudKey** and key ID **48ae0d45-c218-4487-**[redacted]

Customer managed keys (2)

	Aliases	Key ID	Status	Key spec	Key usage
□	AWSKMSCloudKey	48ae0d45-c218-4487-ba7f-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	AWSCloudKey	c6ce2a39-fa61-4766-a8f7-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

To import the cloud key in KeyControl:

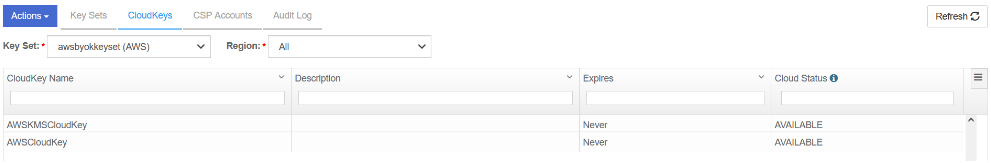
1. Select **BYOK** on the toolbar.
2. Select the **Key Sets** tab and select **awsbyokkeyset**.
3. Select **Actions** > **Import CloudKey**. The **Import Cloud Keys** dialog appears.



Keys can be imported from AWS KMS from one or all regions.

Region *: US East (N. Virginia) us-east-1

4. Select **Import**. The key is imported.
5. Select the **CloudKeys** tab and select **Refresh**.
6. Verify the imported key. For example:



Key Set: * awsbyokkeyset (AWS) Region: * All

CloudKey Name	Description	Expires	Cloud Status
AWSKMSCloudKey		Never	AVAILABLE
AWSCloudKey		Never	AVAILABLE

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

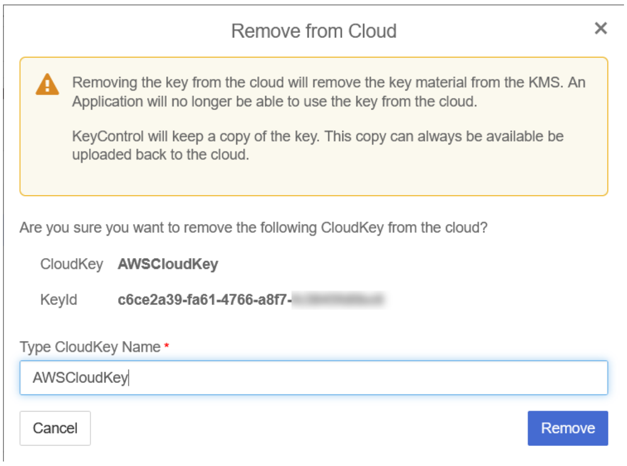
2.9. Remove a cloud key in KeyControl

To remove a cloud key in KeyControl:

1. In KeyControl, select **BYOK** on the main toolbar.
2. Select the **CloudKeys** tab.ttach a policy to an IAM user in AWS
3. Select the key to the removed. For example, **AWSCloudKey**.
4. Select **Actions** > **Remove from Cloud**.

   The **Remove from Cloud** dialog appears.

5. Type the name of the key in **Type CloudKey Name**. 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 the key from the cloud.

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

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

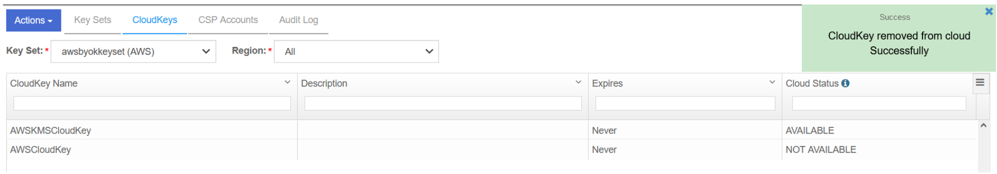
CloudKey **AWSCloudKey**

KeyId **c6ce2a39-fa61-4766-a8f7-**[redacted]

Type CloudKey Name * AWSCloudKey

6. Select **Remove**.

   The cloud key is removed from KeyControl. Its **Cloud Status** becomes **NOT AVAILABLE**. For example:

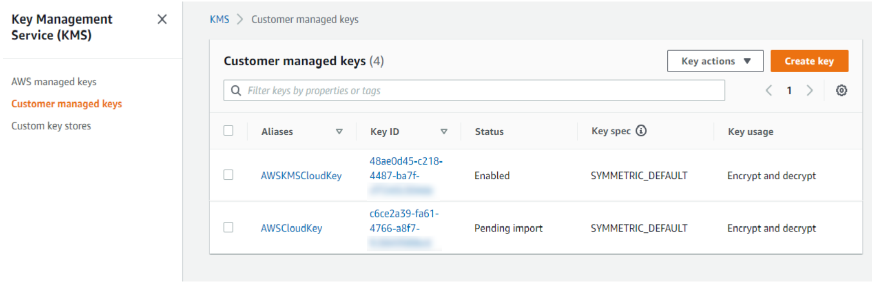


Success
CloudKey removed from cloud Successfully

Key Set: * awsbyokkeyset (AWS) Region: * All

CloudKey Name	Description	Expires	Cloud Status
AWSKMSCloudKey		Never	AVAILABLE
AWSCloudKey		Never	NOT AVAILABLE

7. Verify the key is gone in AWS KMS. For example:



Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
KMS > Customer managed keys
Key actions
Create key
Filter keys by properties or tags
1

Customer managed keys (4)

	Aliases	Key ID	Status	Key spec	Key usage
□	AWSKMSCloudKey	48ae0d45-c218-4487-ba7f-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	AWSCloudKey	c6ce2a39-fa61-4766-a8f7-[redacted]	Pending import	SYMMETRIC_DEFAULT	Encrypt and decrypt

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

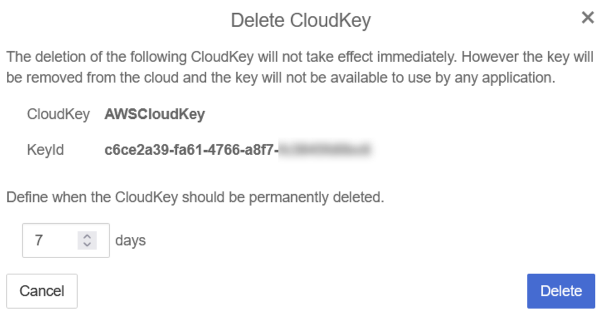
2.10. Delete a cloud key in KeyControl

To delete a cloud key in KeyControl:

1. In KeyControl, select **BYOK** on the toolbar.
2. Select the **CloudKeys** tab.
3. Select the key to the removed. For example, **AWSCloudKey**.
4. Select **Actions** > **Delete CloudKey**.

   The **Delete CloudKey** dialog appears.

5. Select a time in **Define when the CloudKey should be permanently deleted**. 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 **AWSCloudKey**

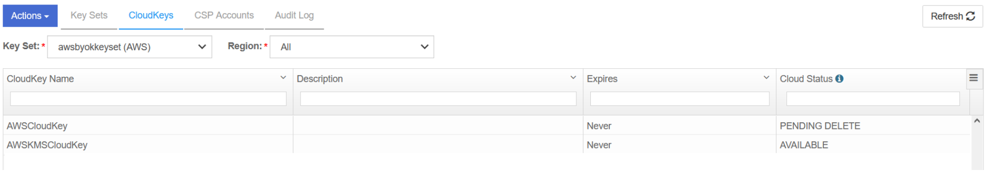
   KeyId **c6ce2a39-fa61-4766-a8f7-**[redacted]

   Define when the CloudKey should be permanently deleted.

   7 days

6. Select **Delete**.

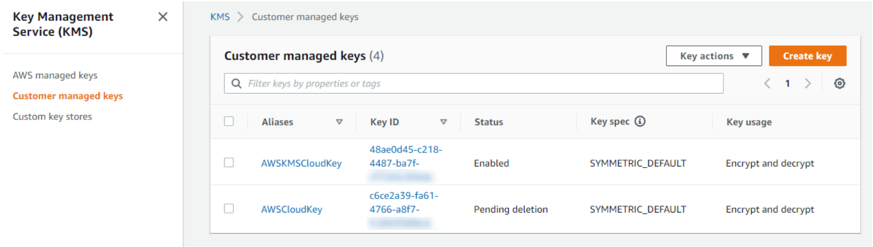
   The cloud key is deleted from KeyControl. The **Cloud Status** becomes **PENDING DELETE**. For example:

   Key Set: * awsbyokkeyset (AWS) Region: * All

CloudKey Name	Description	Expires	Cloud Status
AWSCloudKey		Never	PENDING DELETE
AWSKMSCloudKey		Never	AVAILABLE

7. Verify the key turns into **Pending deletion** in AWS KMS. For example:


Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
KMS > Customer managed keys
Customer managed keys (4)
Key actions ▼
Create key
Filter keys by properties or tags
< 1 >

□	Aliases	Key ID	Status	Key spec	Key usage
□	AWSKMSCloudKey	48ae0d45-c218-4487-ba7f-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	AWSCloudKey	c6ce2a39-fa61-4766-a8f7-[redacted]	Pending deletion	SYMMETRIC_DEFAULT	Encrypt and decrypt

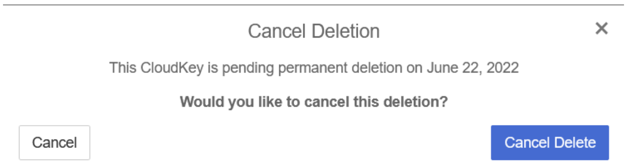
For further information, refer to Deleting a CloudKey from the Cloud in the KeyControl online documentation.

2.11. Cancel a cloud key deletion in KeyControl

To cancel a cloud key deletion in KeyControl:

1. In KeyControl, select **BYOK** on the toolbar.
2. Select the **CloudKeys** tab.
3. Select the key for which you want to cancel a deletion. For example, **AWSCloudKey**.
4. Select **Actions** > **Cancel Deletion**.

   The **Cancel Deletion** dialog appears. For example:



Cancel Deletion

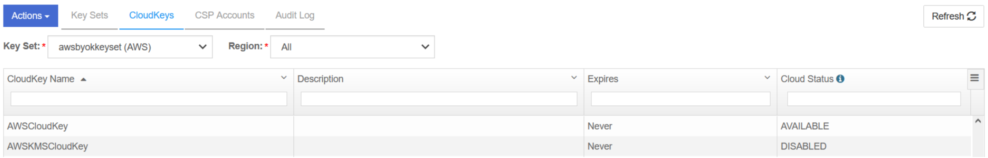
This CloudKey is pending permanent deletion on June 22, 2022

Would you like to cancel this deletion?

5. Select **Cancel Delete**.

   The deletion is cancelled.

6. Verify the status change in KeyControl. For example:

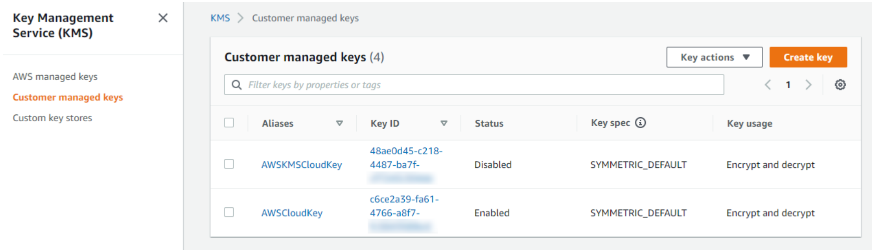


Key Set: * awsbyokkeyset (AWS)

Region: * All

CloudKey Name	Description	Expires	Cloud Status
AWSCloudKey		Never	AVAILABLE
AWSKMSCloudKey		Never	DISABLED

7. Verify the key is now available in Azure. For example:


Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
KMS > Customer managed keys
Customer managed keys (4)
Key actions ▼
Create key
Filter keys by properties or tags
< 1 >

□	Aliases	Key ID	Status	Key spec	Key usage
□	AWSKMSCloudKey	48ae0d45-c218-4487-ba7f-[redacted]	Disabled	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	AWSCloudKey	c6ce2a39-fa61-4766-a8f7-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

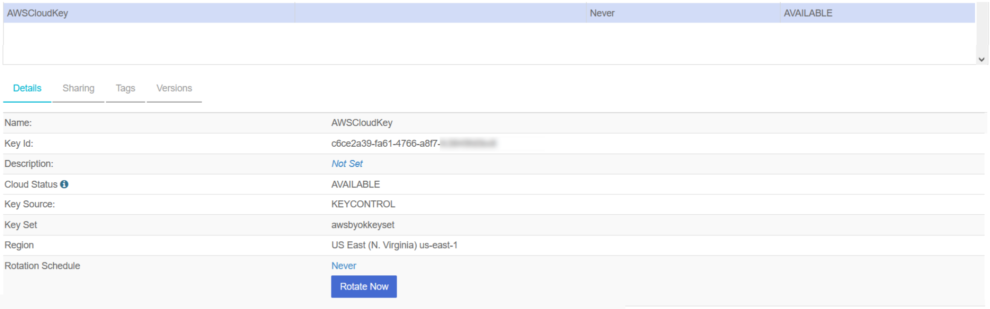
The initial state of the key will be Disabled. You can set the state of the key to Enabled to use it again.

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

2.12. Rotate a cloud key in KeyControl

To rotate a cloud key in KeyControl:

1. In KeyControl, select **BYOK** on the toolbar.
2. Select the **CloudKeys** tab.
3. Select the key you want to rotate. Scroll down and select the **Rotate Now** control. For example:



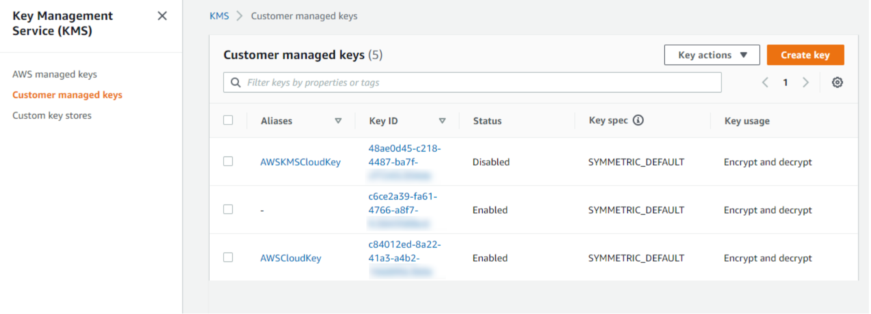
AWSCloudKey		Never	AVAILABLE

Name:	AWSCloudKey
Key Id:	c6ce2a39-fa61-4766-a8f7-[redacted]
Description:	*Not Set*
Cloud Status ℹ	AVAILABLE
Key Source:	KEYCONTROL
Key Set	awsbyokkeyset
Region	US East (N. Virginia) us-east-1
Rotation Schedule	Never Rotate Now

4. Select **Rotate Now**.

   The key is rotated.

5. Verify that the key has been rotated in AWS KMS. For example:



Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
KMS > Customer managed keys
Key actions ▼
Create key
Filter keys by properties or tags
1

Customer managed keys (5)

□	Aliases	Key ID	Status	Key spec ⓘ	Key usage
□	AWSKMSCloudKey	48ae0d45-c218-4487-ba7f-[redacted]	Disabled	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	-	c6ce2a39-fa61-4766-a8f7-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	AWSCloudKey	c84012ed-8a22-41a3-a4b2-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt