



ENTRUST

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

Integration Guide

2024-04-19

Table of Contents

1. Introduction	1
1.1. Documents to read first	1
1.2. Product configurations	1
1.3. Requirements	1
2. Procedures	2
2.1. Install and configure Entrust KeyControl	2
2.2. Create a customer managed policy in AWS	2
2.3. Create IAM User in AWS	5
2.4. Attach a policy to an IAM user in AWS	7
2.5. Create an AWS CSP account	8
2.6. Create a key set in KeyControl	8
2.7. Create a cloud key in KeyControl	10
2.8. Create a cloud key in AWS Key Management Service	12
2.9. Remove a cloud key in KeyControl	15
2.10. Delete a cloud key in KeyControl	16
2.11. Cancel a cloud key deletion in KeyControl	17
2.12. Rotate a cloud key in KeyControl	18
3. Additional resources and related products	19
3.1. Video	19
3.2. nShield Connect	19
3.3. nShield as a Service	19
3.4. KeyControl BYOK	19
3.5. Entrust digital security solutions	19
3.6. nShield product documentation	19

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).

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 it from the [Entrust Document Library](#) and from the [nShield Product Documentation website](#).

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

1.3. Requirements

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 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](#)

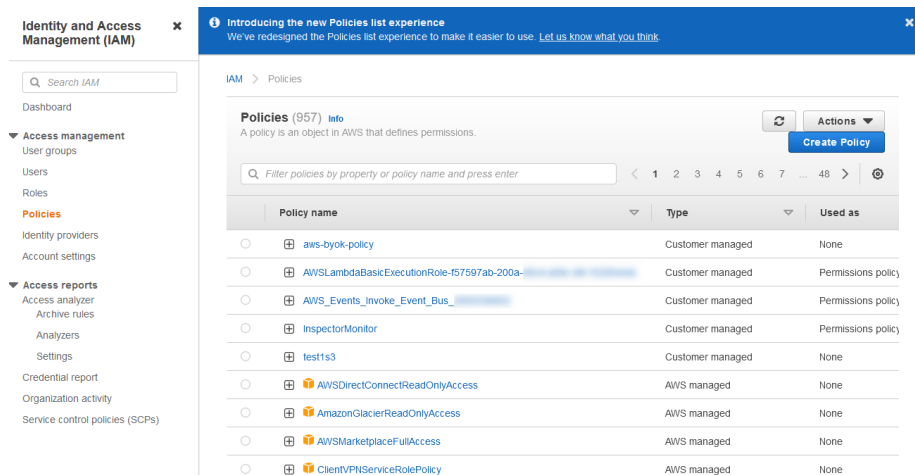
2.1. Install and configure Entrust KeyControl

Follow the installation and set-up instructions in the *Entrust KeyControl nShield HSM Integration Guide*. You can access it from the [Entrust Document Library](#) and from the [nShield Product Documentation website](#).

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:



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.**

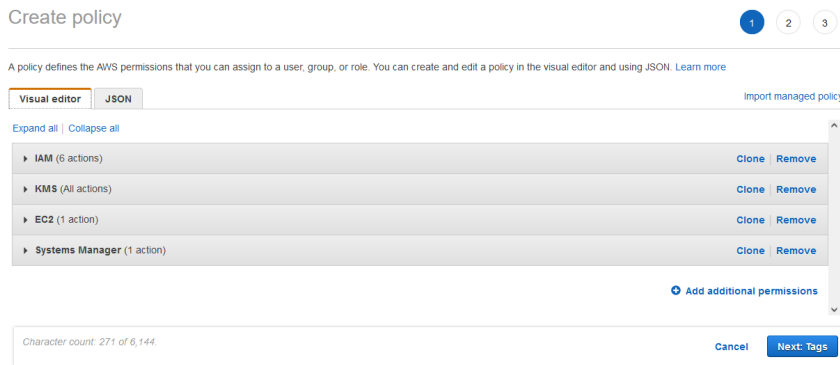
5. Select **Add additional permissions**. Select **Chose a service** and search for **EC2**. Select the following permissions:

- **DescribeRegions.**

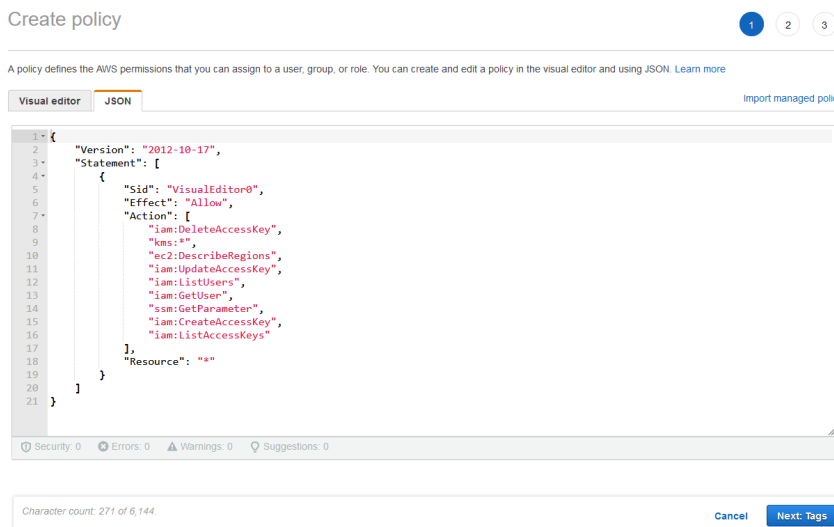
6. Select **Add additional permissions**. Select **Chose a service** and search for **Systems Manager**. Select the following permissions:

- **GetParameter.**

The permissions should be listed as follows:



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



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

- 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 1 2 3

Review policy

Name:
Use alphanumeric and "+=, @, _" characters. Maximum 128 characters.

Description:
Maximum 1000 characters. Use alphanumeric and "+=, @, _" characters.

Summary

Filter

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

Key Value

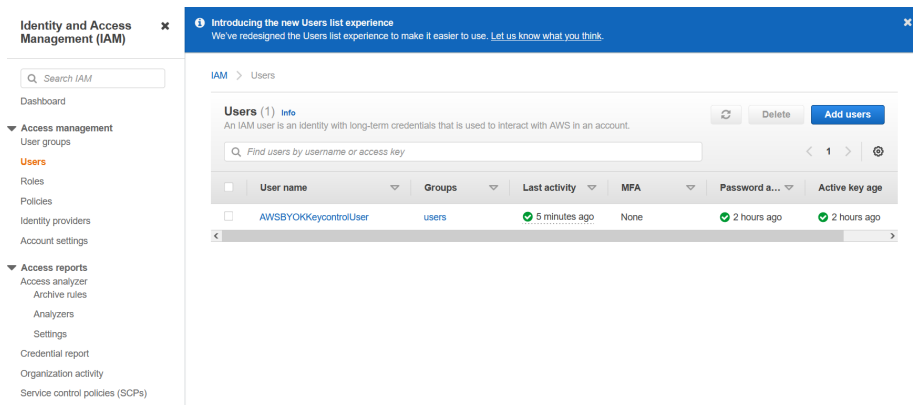
* Required Cancel Previous Create policy

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:



3. Enter values for the following properties:

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

For example:

The screenshot shows the 'Add user' console page at step 1, 'Set user details'. The user name is 'AWSBYOKKeycontrolUser'. Under 'Select AWS access type', both 'Access key - Programmatic access' and 'Password - AWS Management Console access' are selected. Under 'Console password*', 'Custom password' is selected with a masked input field. Buttons for 'Cancel' and 'Next: Permissions' are visible at the bottom.

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

The screenshot shows the 'Add user' console page at step 2, 'Set permissions'. The 'Add user to group' option is selected. A search results table is shown below:

Group	Attached policies
<input type="checkbox"/> Administrator	AdministratorAccess
<input type="checkbox"/> users	AmazonInspectorFullAccess and 2 more

Buttons for 'Cancel', 'Previous', and 'Next: Tags' are visible at the bottom.

5. Add the necessary tags. For example:

The screenshot shows the 'Add user' console page at step 3, 'Add tags (optional)'. It features a table for adding tags:

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	<input type="button" value="Remove"/>

Buttons for 'Cancel', 'Previous', and 'Next: Review' are visible at the bottom.

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

Add user 1 2 3 4 5

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

[Cancel](#) [Previous](#) [Create user](#)

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

Add user 1 2 3 4 5

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>

[Download .csv](#)

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**.

The screenshot shows the AWS IAM console interface. On the left, the navigation menu is open to 'Policies'. The main content area displays a list of policies. The first policy, 'aws-byok-policy', is selected. An 'Actions' menu is open over this policy, showing options: 'Attach', 'Detach', and 'Delete'. The 'Attach' option is highlighted. A notification banner at the top reads '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.'

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

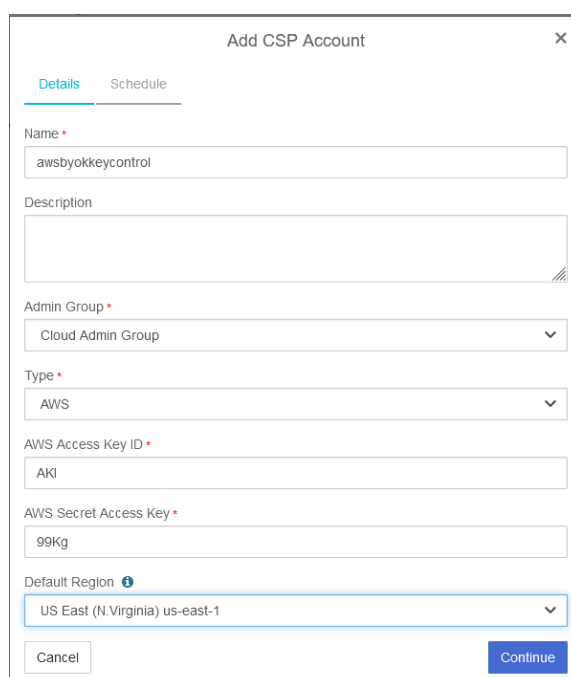
2.5. Create an AWS CSP account

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:



The screenshot shows the 'Add CSP Account' dialog box. The 'Details' tab is active, showing the following fields:

- Name: awsbyokkeycontrol
- Description: (empty)
- 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

Buttons: Cancel, Continue



The region selected has to match your AWS region.

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

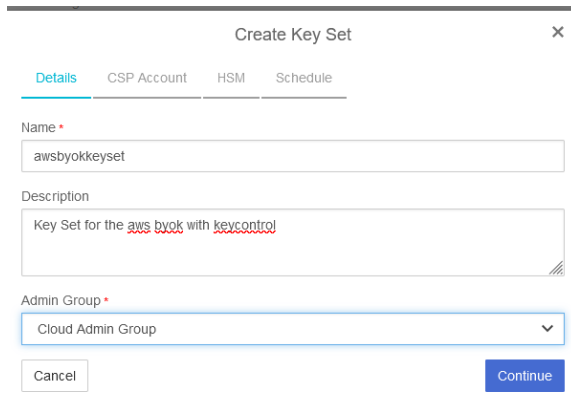
2.6. Create a key set in KeyControl

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**.

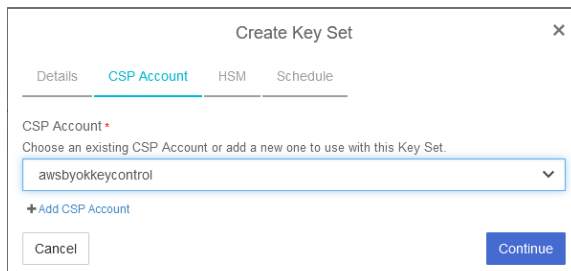
The **Create Key Set** dialog appears.

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



The screenshot shows the 'Create Key Set' dialog with the 'Details' tab selected. The 'Name' field is filled with 'awsbyokkeyset'. The 'Description' field contains 'Key Set for the aws byok with keycontrol'. The 'Admin Group' dropdown menu is set to 'Cloud Admin Group'. There are 'Cancel' and 'Continue' buttons at the bottom.

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

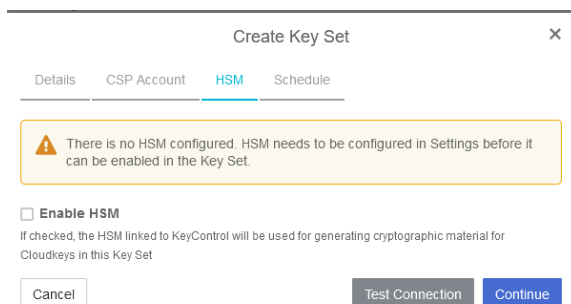


The screenshot shows the 'Create Key Set' dialog with the 'CSP Account' tab selected. The 'CSP Account' dropdown menu is set to 'awsbyokkeycontrol'. There is a '+ Add CSP Account' link below the dropdown. There are 'Cancel' and 'Continue' buttons at the bottom.



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:

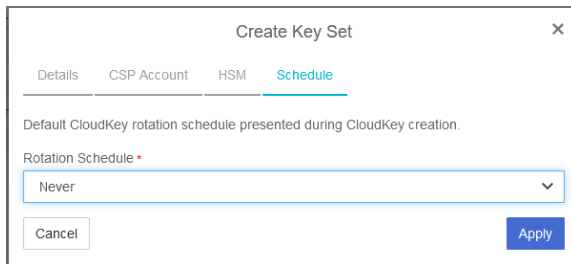


The screenshot shows the 'Create Key Set' dialog with the 'HSM' tab selected. A yellow warning box contains the text: 'There is no HSM configured. HSM needs to be configured in Settings before it can be enabled in the Key Set.' Below the warning, there is an unchecked checkbox labeled 'Enable HSM' and a sub-note: 'If checked, the HSM linked to KeyControl will be used for generating cryptographic material for Cloudkeys in this Key Set'. There are 'Cancel', 'Test Connection', and 'Continue' buttons at the bottom.

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

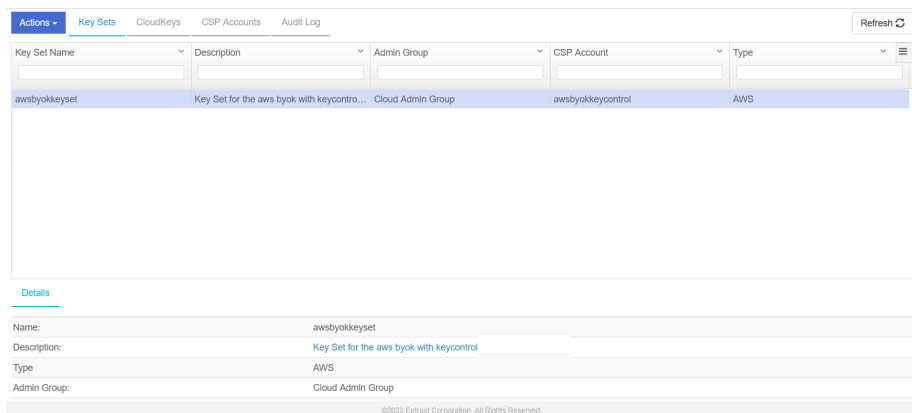
9. Select **Continue**.

10. In the **Schedule** tab, select a **Rotation Schedule** matching the selection made during [Create an AWS CSP account](#). For example:



11. Select **Apply**.

The key set is added. For example:

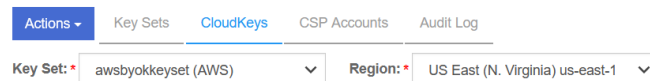


For further information, refer to [Creating a Key Set](#) in the KeyControl online documentation.

2.7. Create a cloud key in KeyControl

To create a cloud key in KeyControl: attach 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:



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

The **Create CloudKey** dialog appears.

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

Create CloudKey

Details Access Schedule

Type **AWS**
 Key Set **awsbyokkeyset**
 Region **us-east-1**

Name *
 AWSCloudKey

Description

Cancel Continue

5. Select **Continue**.

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

Create CloudKey

Details Access Schedule

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

Cancel Continue

7. Select **Continue**.

8. In the **Schedule** tab:

- a. Select a **Rotation Schedule**.
- b. Set **Expiration**.

For example:

Create CloudKey

Details Access Schedule

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

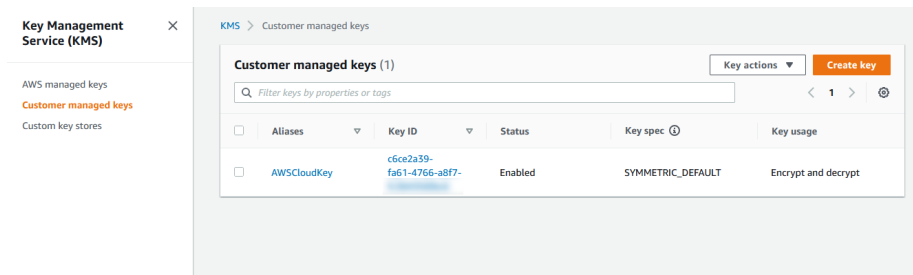
Expiration *
 Define when the CloudKey should be expired.
 Never Choose a date

Cancel Continue

9. Select **Continue**.

The cloud key is created.

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.

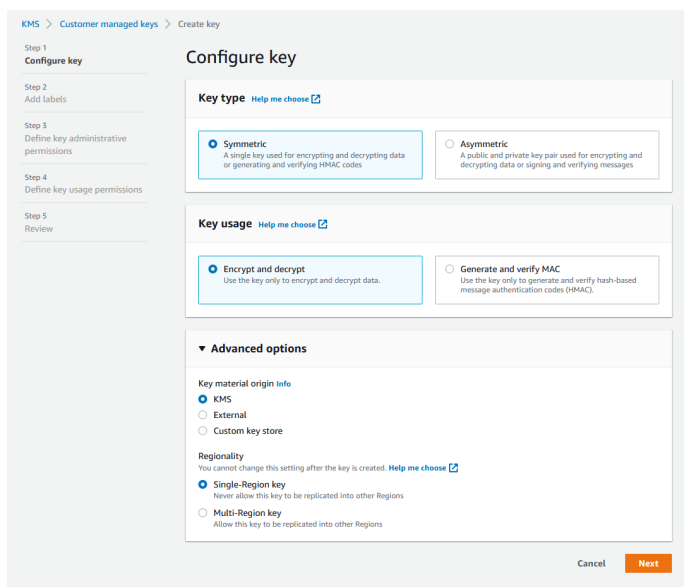
2.8. Create a cloud key in AWS Key Management Service

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**.



3. Select **Next**.

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

5. Select **Next**.

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

Name	Path	Type
<input checked="" type="checkbox"/> AWSBYOKKeycontrolUser	/	User

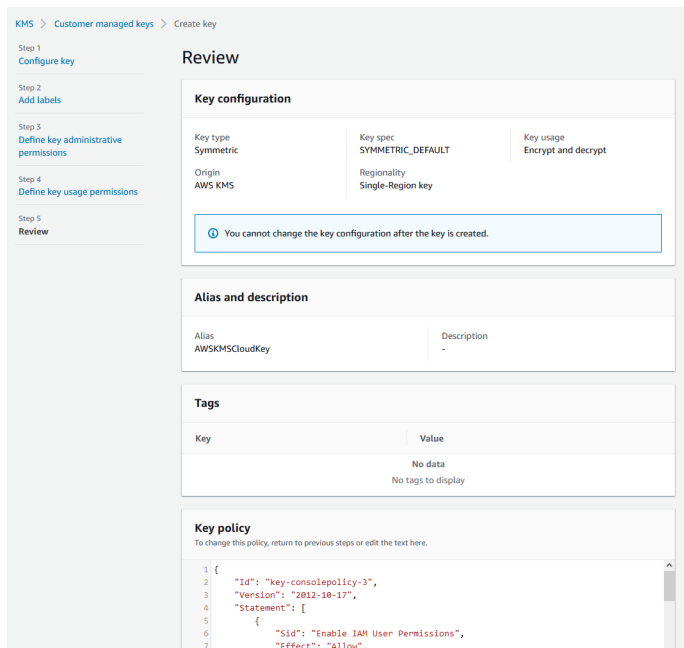
7. Select **Next**.

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

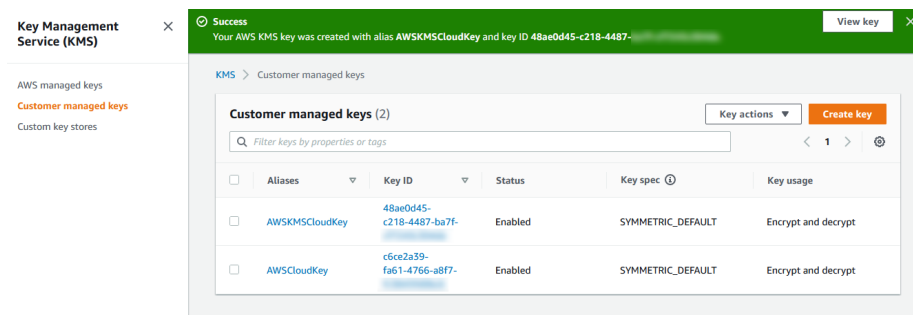
Name	Path	Type
<input checked="" type="checkbox"/> AWSBYOKKeycontrolUser	/	User

9. Select **Next**.

10. Confirm all information in **Step 5: Review**.

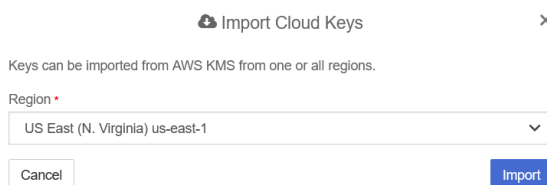


11. Note the new key in the AWS KMS.



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.



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

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. Attach a policy to an IAM user in AWS
3. Select the key to be 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 to 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-██████████**

Type CloudKey Name

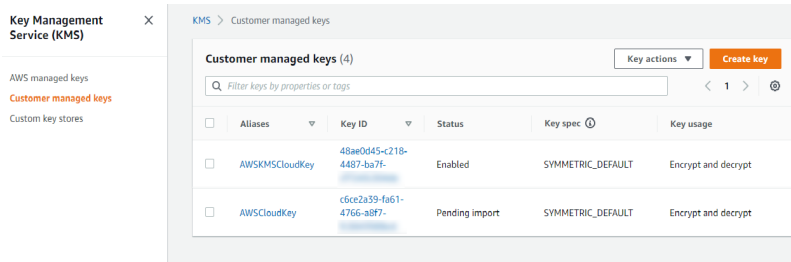
Cancel
Remove

6. Select **Remove**.

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

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

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



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

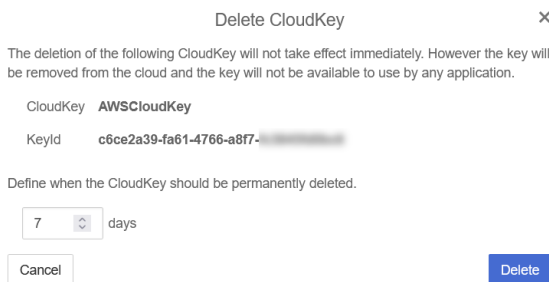
2.10. Delete a cloud key in KeyControl

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 be removed. For example, **AWSCloudKey**.
4. Select **Actions > Delete CloudKey**.

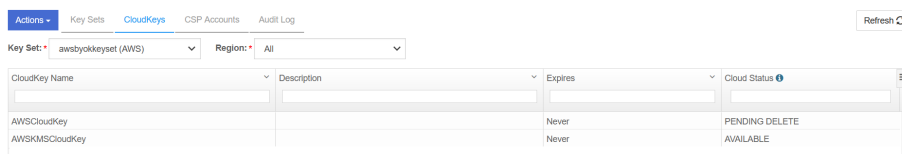
The **Delete CloudKey** dialog appears.

5. Select a time in **Define when the CloudKey should be permanently deleted**. For example:

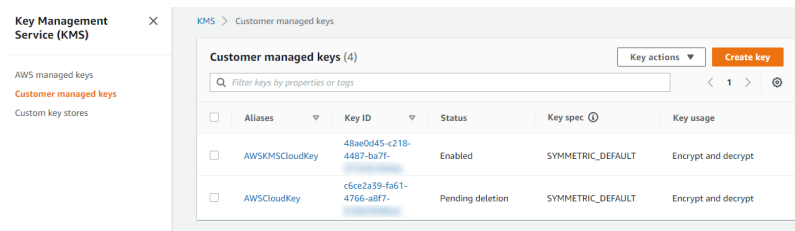


6. Select **Delete**.

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



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



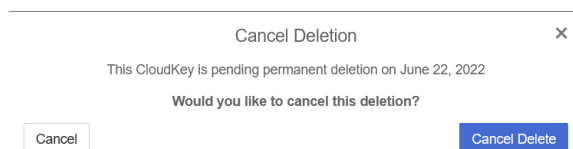
For further information, refer to [Deleting a CloudKey from the Cloud](#) in the KeyControl online documentation.

2.11. Cancel a cloud key deletion in KeyControl

To cancel a cloud key deletion in KeyControl:

1. In KeyControl, select keys **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**.

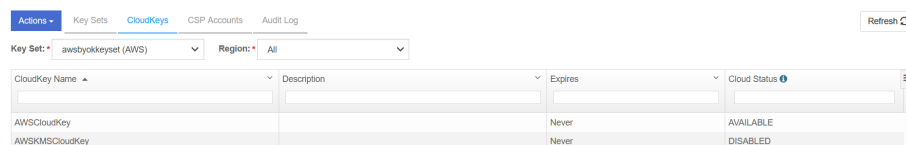
The **Cancel Deletion** dialog appears. For example:



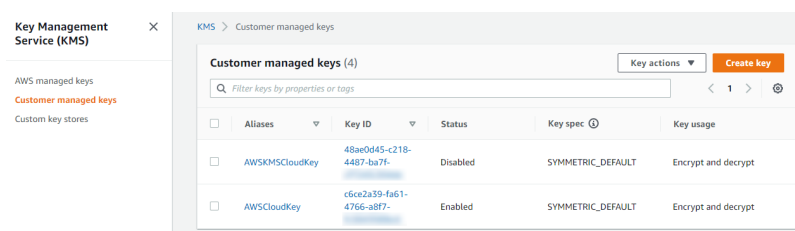
5. Select **Cancel Delete**.

The deletion is cancelled.

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



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





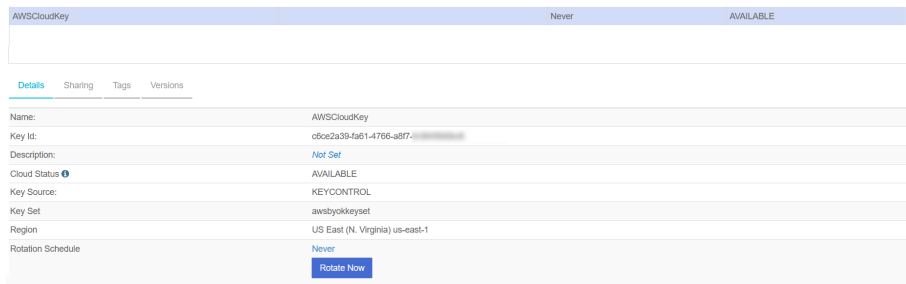
The initial state of the key will be Disabled. You can set the state of the key to Enabled to use it again.

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:

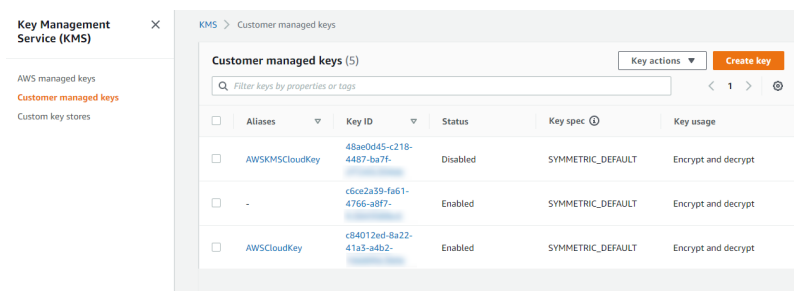
1. In KeyControl, select **BYOK** on the toolbar.
2. Select the **CloudKeys** tab.
3. Select the key you want to rotate. Scroll down and select the **Rotate Now** control. For example:



4. Select **Rotate Now**.

The key is rotated.

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



Chapter 3. Additional resources and related products

[3.1. Video](#)

[3.2. nShield Connect](#)

[3.3. nShield as a Service](#)

[3.4. KeyControl BYOK](#)

[3.5. Entrust digital security solutions](#)

[3.6. nShield product documentation](#)