AWS-BYOK

Integration Guide

ESKM

8.54.7

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-04-09
Status	PUBLISHED
Document No.	IG-2026-0032

Table of Contents

1 Introduction

The **AWS Bring Your Own Key (BYOK)** integration with **Enterprise Secure Key Manager (ESKM)** allows you to use encryption keys that are created and managed in ESKM to protect data in Amazon Web Services (AWS). Using this integration, keys are generated in ESKM and securely imported into **AWS Key Management Service (AWS KMS)**.

This approach helps organizations maintain control over their encryption keys while using AWS services for data encryption and decryption. The integration supports centralized key management and helps meet security and compliance requirements.

1.1 About This Guide

This guide describes how to integrate AWS Bring Your Own Key (BYOK) with Utimaco Enterprise Secure Key Manager (ESKM).

1.2 Target Audience

This guide is intended for Utimaco ESKM and AWS-BYOK administrators.

1.3 Purpose of the Integration

The AWS-BYOK and Enterprise Secure Key Manager (ESKM) integration allows customers to use AWS services while keeping full control of their encryption keys. With this integration, encryption keys are created, stored, and managed in ESKM, ensuring enhanced security and compliance while enabling secure data encryption in AWS.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
AWS	Amazon Web Services
ARN	Amazon Resource Name

Abbreviation	Meaning
BYOK	Bring Your Own Key
KMS	Key Management Service
ESKM	Enterprise Secure Key Manager
IAM	Identity and Access Management
API	Application Programming Interface

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Table 2: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message indicates the expected result after the successful execution of an instruction.

2 Product Overview

2.1 Overview of the AWS-BYOK

AWS Bring Your Own Key (BYOK) allows customers to create and manage their own encryption keys outside the AWS cloud and securely import them into AWS Key Management Service (AWS KMS). This enables customers to maintain control over their encryption keys while using AWS services for data encryption.

2.2 Overview of Utimaco ESKM

Utimaco Enterprise Secure Key Manager (ESKM) is a centralized key management solution that enables organizations to securely generate, store, and manage encryption keys. It provides full control over key lifecycle operations, including key creation, rotation, edit, and deletion.

ESKM integrates with AWS to allow customers to manage encryption keys outside the cloud while maintaining strong security and compliance requirements.

2.3 Joint Value Proposition

Integrating Utimaco ESKM with AWS BYOK enables organizations to generate and control encryption keys within their Utimaco ESKM environment while securely importing them into AWS KMS for cloud workloads. This combined approach strengthens compliance, maintains key ownership, and ensures consistent, high-assurance security across hybrid and multi-cloud deployments, all while supporting seamless cloud adoption without compromising the customer's root of trust.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using, meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured the required software.

3.1 Tested Versions

AWS version	Utimaco ESKM
AWS-BYOK (AWS KMS)	ESKM 8.54.7

3.2 Supported Platforms

- Utimaco ESKM hardware appliance.
- Utimaco ESKM virtual/cloud appliance.

3.3 Prerequisites

- ESKM version must be ESKM 8.54.7 or higher.
- If ESKM has direct internet access without a proxy, a DNS server must be configured on the ESKM appliance. This can be configured from the ESKM Management Console (**Device -> Network -> Hostname & DNS**).
- Must have an AWS account with adequate permissions to use the Key Management Service (KMS) in AWS.
- Access Key ID and Secret Access Key for the IAM user. For more information about Access key ID and Secret access key, refer https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey .

4 Installation and Configuration

4.1 Setting Up ESKM

Cloud Integration Web Console can be accessed using the following methods:

- Log in to the ESKM Management Console as an administrator and navigate to **Security > Cloud Integration** to access the Cloud Integration Web Console.

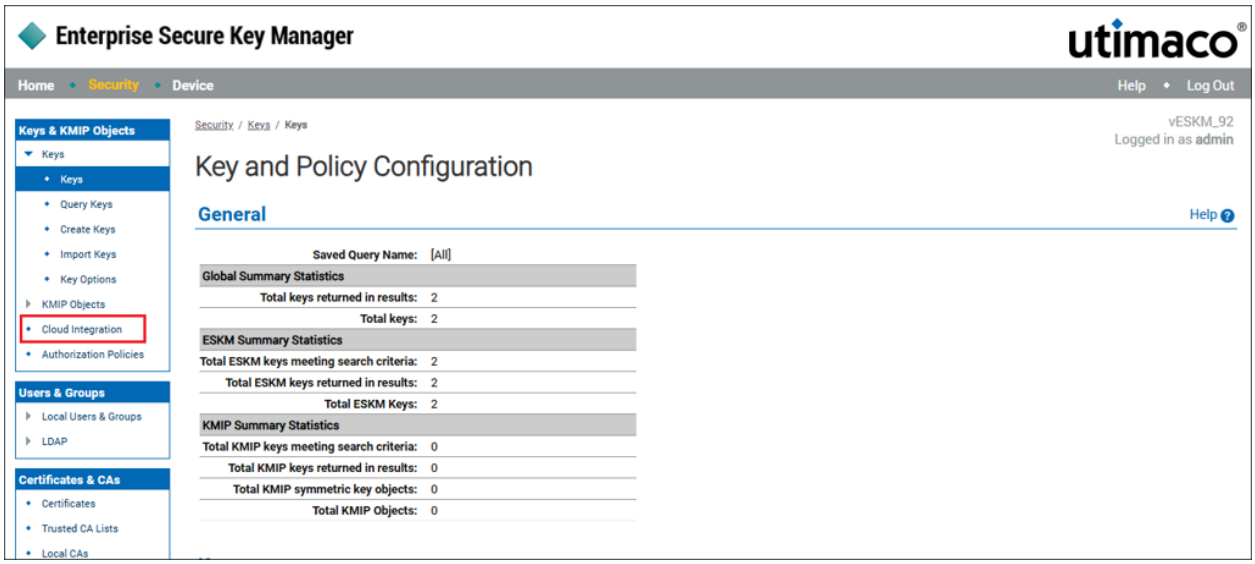

Figure 1 : Cloud Integration

- The Cloud Integration Web Console opens in a new tab and automatically logs you into the cloud ESKM.

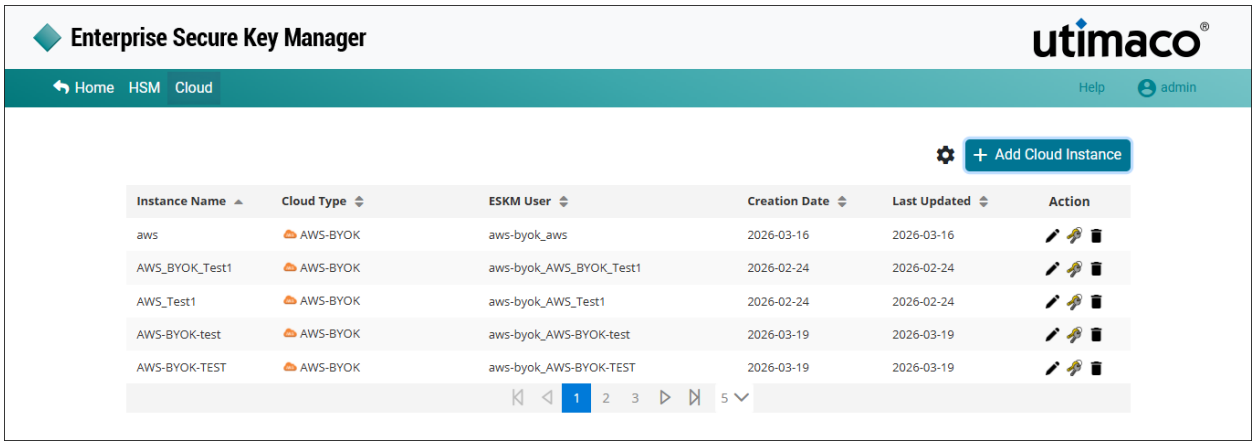

Figure 2 : Cloud Integration Dashboard

- Directly access through a web browser: using IP and port; for example, https://<ESKM IP>:8443/cloud/dashboard.

- The following screen appears.

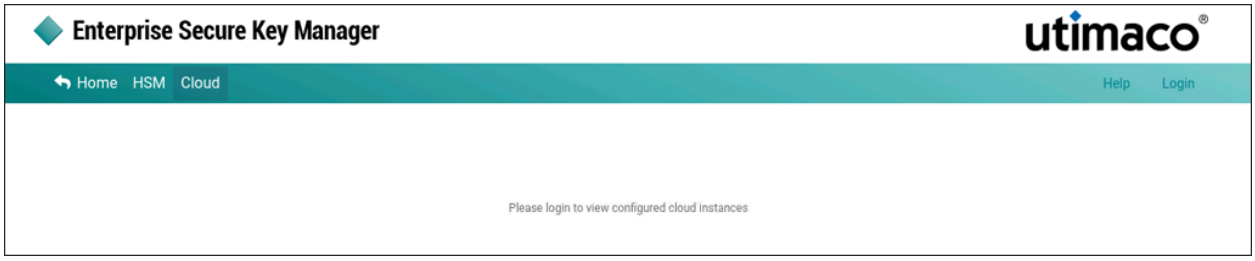

Figure 3 : Cloud Integration Login

- Click **Login** at the top right corner of the page.

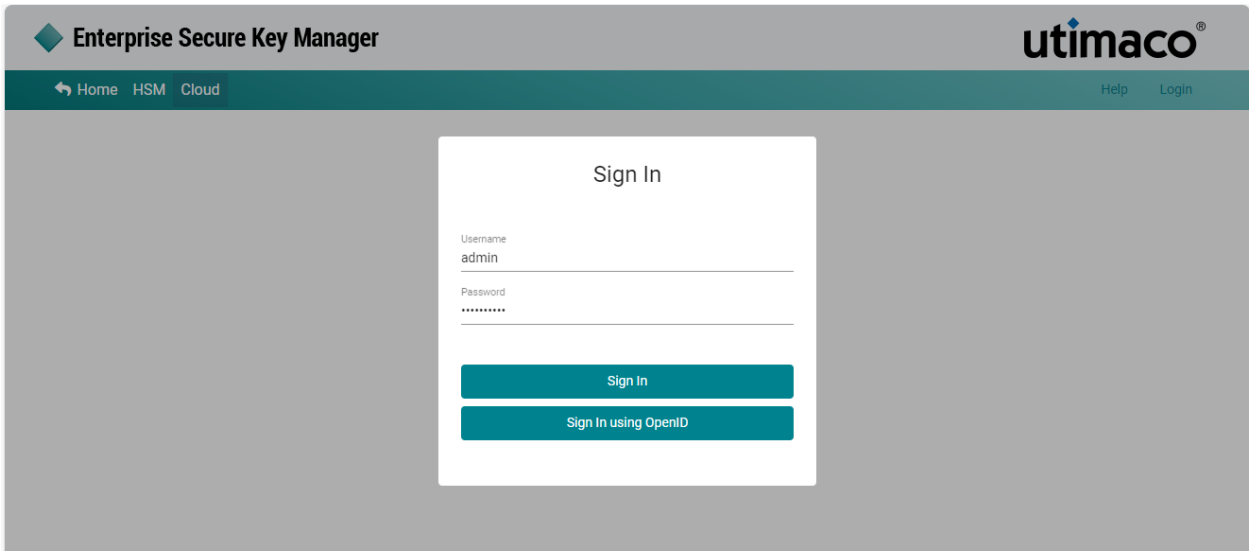

Figure 4 : Cloud Integration Sign In

- Enter the **Administrator Username** and **Password,** and then click **Sign In**.

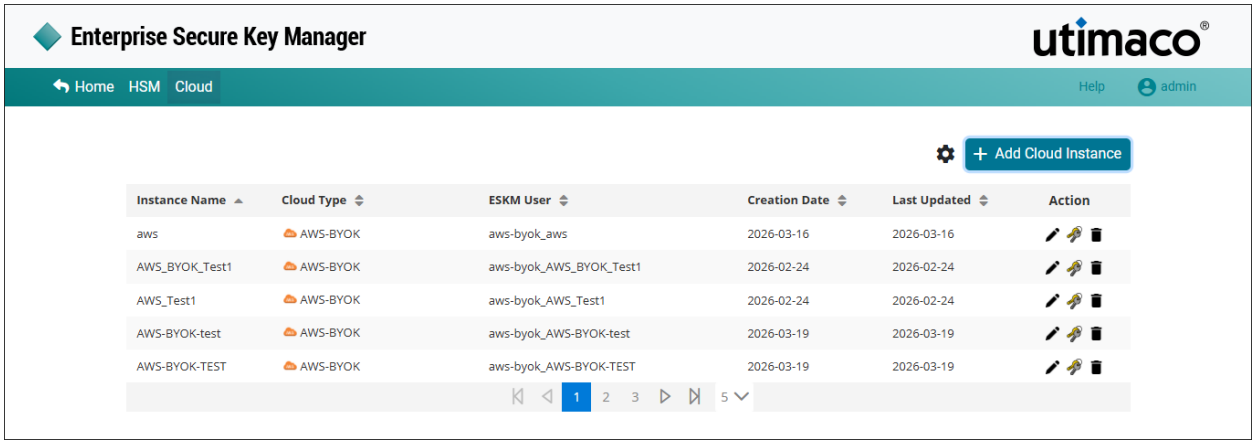

Figure 5 : Cloud ESKM-Logged In page

The cloud integration dashboard enables the user to add cloud instance and view information about the existing instances.

Sign In using OpenID

To log in to the cloud integration dashboard as OpenID administrator, you must configure the OpenID server in ESKM and create OpenID administrator accounts in ESKM. OpenID administrators are users managed by an OpenID provider.

For more information on the OpenID configuration, please refer ESKM_User_Guide_8.54.7

To sign in using OpenID

- In the login page, enter **Username** and **Password** and click on **Sign In using OpenID.** (OR) Click **Sign In using OpenID** without user credentials.

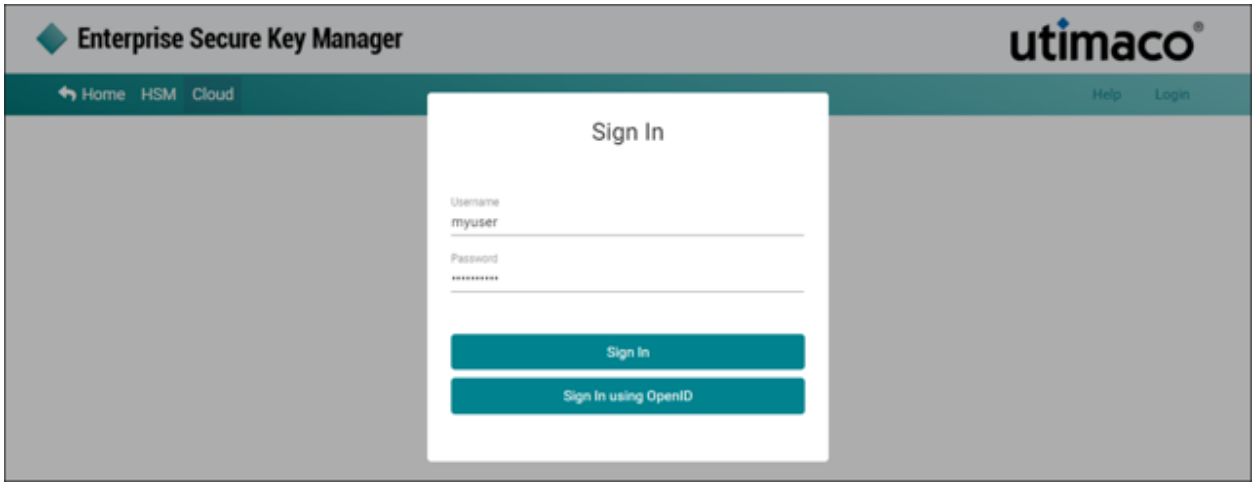

Figure 6 : Sign In Using OpenID

- Enter **Username** and **Password**. Click **Sign In** or **Sign In using OpenID.**
- The **Cloud Integration Dashboard** is displayed.

You can log out of the **Cloud Integration Web Console** at any time using the **Logout option** under **Admin** menu in the upper right corner.

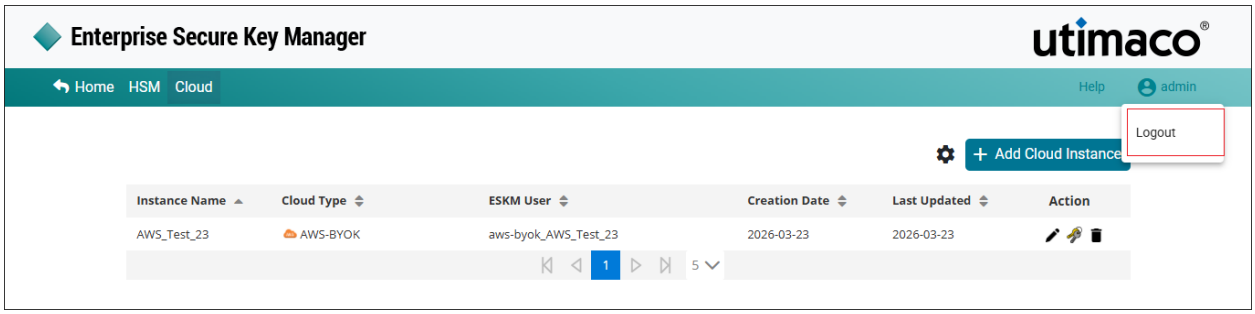

Figure 7 : Logout

- When you **Signed In with Open ID Cloud Integration Web Console**, the **Logout** pop-up window is displayed. Click **Logout**.
- In the Cloud Integration dashboard, click **Left** arrow at the left upper corner of the page to navigate to the ESKM application.

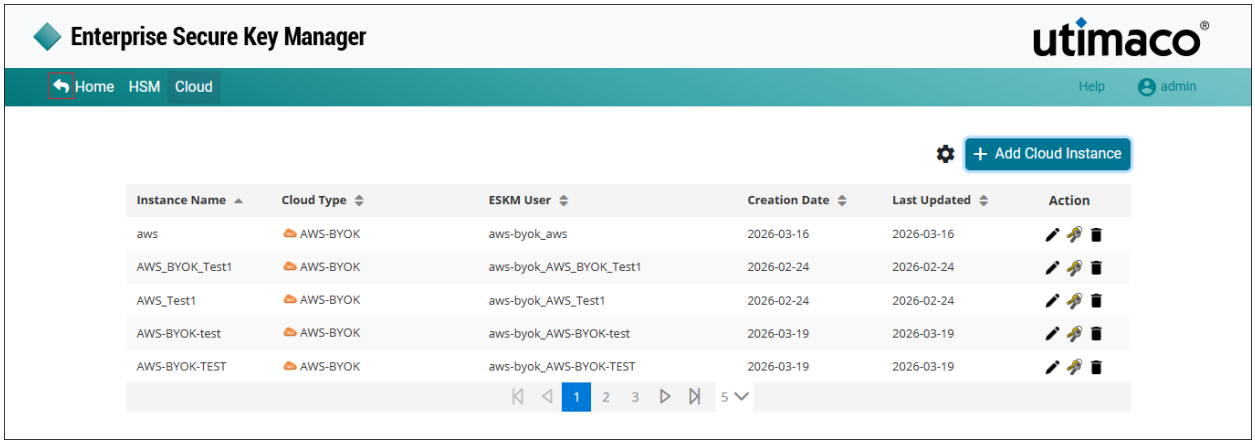

Figure 8 : Cloud Integration Dashboard

4.2 Cloud Settings

The ESKM BYOK service is enabled by default and therefore not displayed in the UI. To access external services, ESKM requires internet connectivity. In environments where direct internet access is restricted, a proxy server can be configured to provide the required connectivity.

To configure the proxy server in ESKM, enable the Proxy Server option, enter the **proxy server address** and **port** number, and then click **Update** to apply the changes.

This section describes the procedure to configure ESKM cloud settings.

To configure proxy settings:

- Click the **Settings** icon on the **Cloud** dashboard.

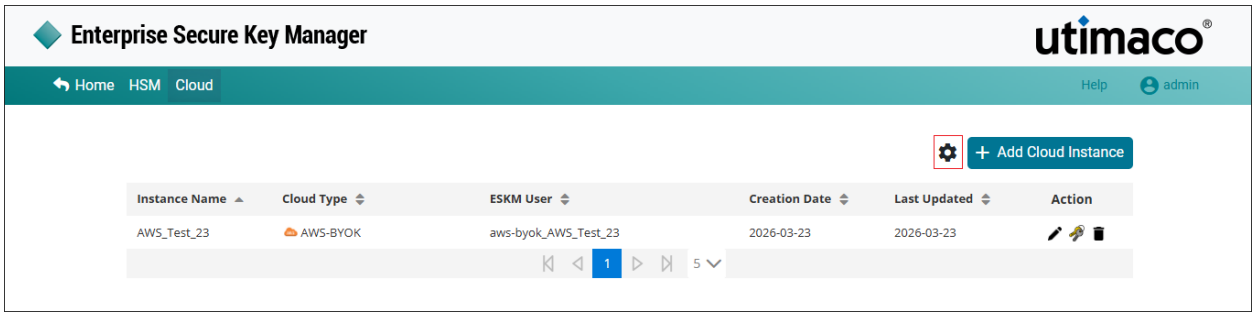

Figure 9 : Cloud Settings

- The **Settings** pop-up window will appear.

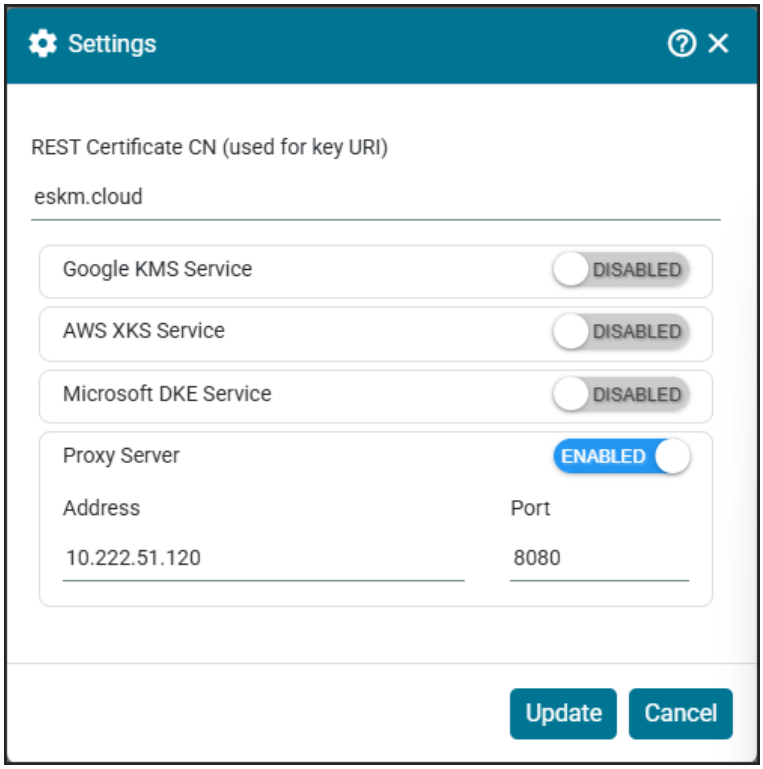

Figure 10 : Update Settings

4.3 Setting Up AWS

1. Sign in to the **AWS Management Console**.
2. Open **IAM (Identity and Access Management)**.
3. Go to **Users** and select **Add users**.
4. Enter a user name and complete the user creation.

5. Copy and save the **Access Key ID** and **Secret Access Key** shown on the screen.

The Secret Access Key is displayed only once and must be stored securely.

5 Integration Steps

5.1 Configuration on ESKM

5.1.1 Adding a AWS-BYOK Cloud Instance

To add a new AWS-BYOK Cloud Instance:

- Click on **+Add Cloud Instance** at the top right corner of the page.

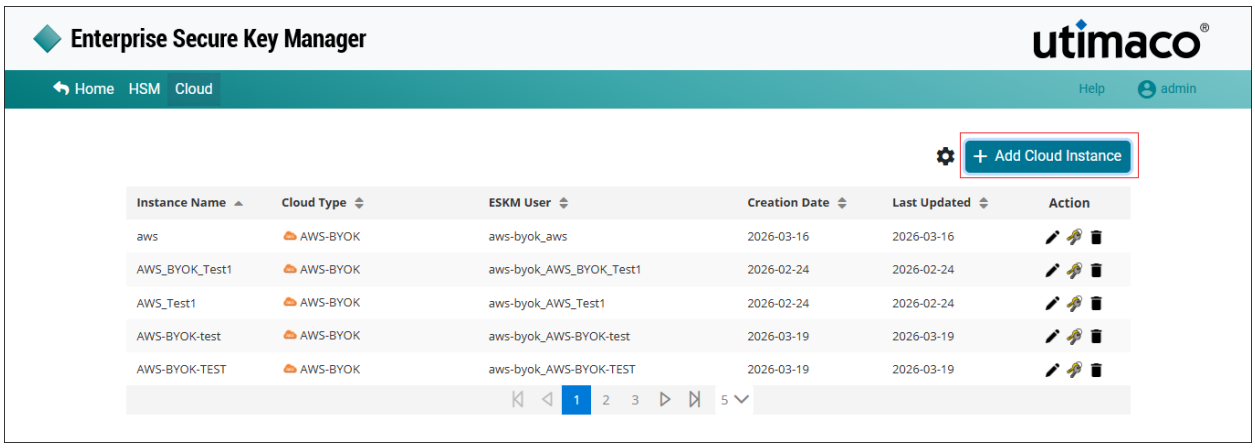

Figure 11 : Add Cloud Instance

- The **Add Cloud Instance** pop-up appears.

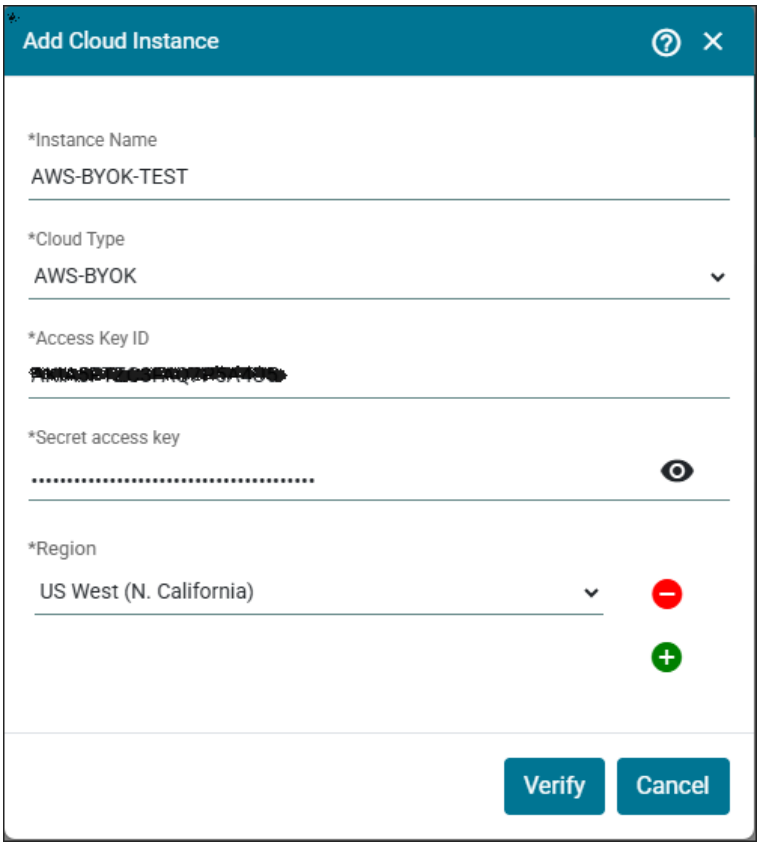

Figure 12 : Verify Cloud Instance

- Enter the **Instance Name**, select **AWS-BYOK** as a Cloud Type and specify **Access Key ID**, **Secret access key** and select **Region** from the list. Click **Verify**.

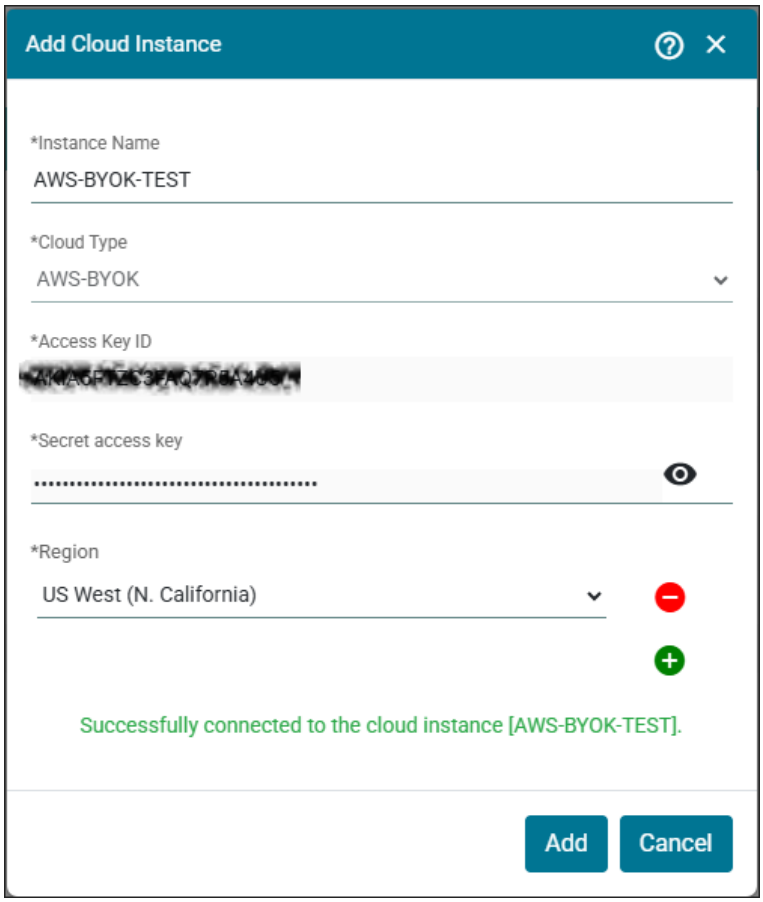

Figure 13 : Add Cloud Instance

- Click **Add**.

Parameters	Description
Instance Name	Name of the Instance.
Cloud Type	The cloud provider with which ESKM is integrated. Here select cloud type as a AWS-BYOK.
Access Key ID	Access key ID is the AWS credential for AWS command line interface.
Secret access key	Secret Access Key is the AWS credential for AWS command line interface.

Parameters	Description
Region	Select the regions to which the key needs to be imported.

Table 3: Add AWS-BYOK Cloud Instance - Parameters

5.1.2 Editing a AWS-BYOK Cloud Instance

- Under **Action** column, click **Edit** icon to edit the existing cloud instances.

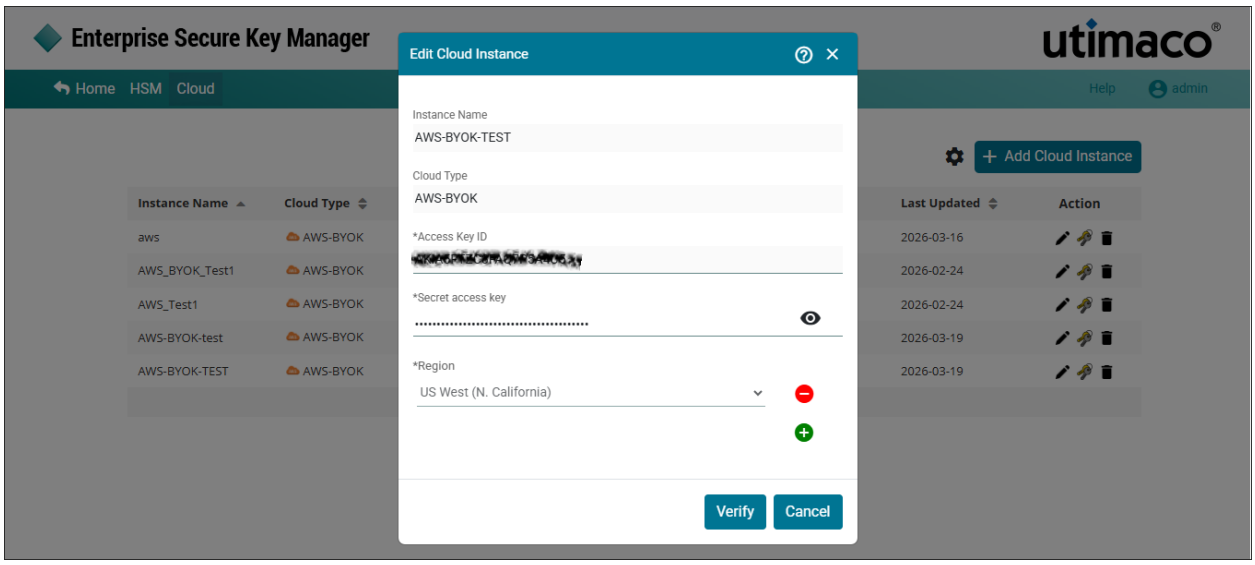

Figure 14 : Verify Cloud Instance

- The **Edit Cloud Instance** pop-up window will appear. Make the necessary changes and click **Verify**.

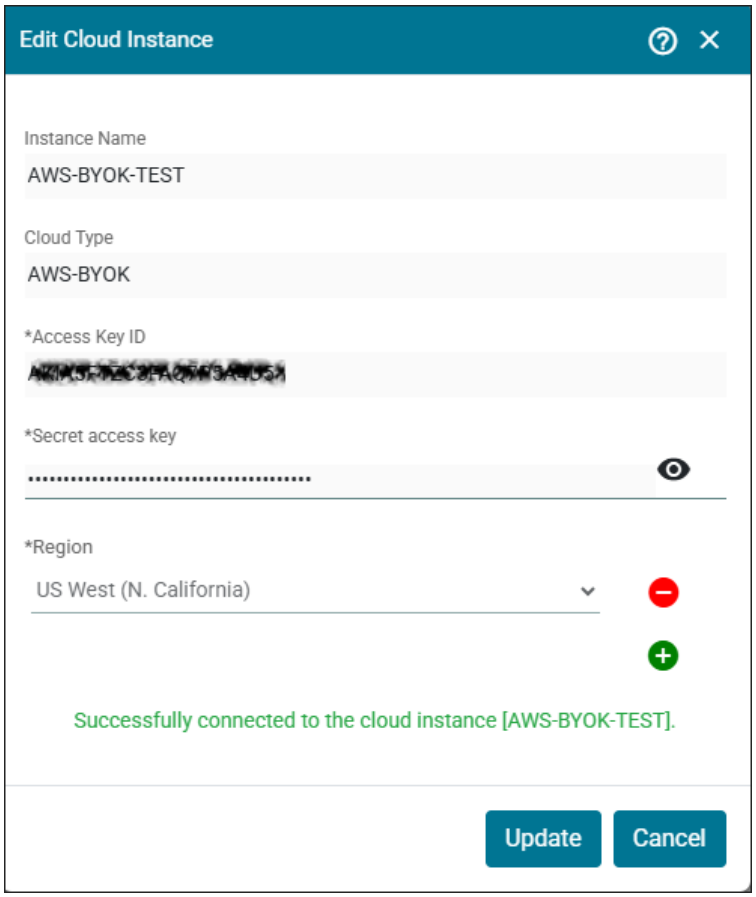

Figure 15 : Edit Cloud Instance

- Click **Update**.

Cloud instance updated successfully.

User can only edit **Secret access key** and **Region** and other fields are disabled for editing.

5.1.3 Deleting a AWS-BYOK Cloud Instance

- Under **Action** column, click **Delete** icon to delete existing AWS-BYOK cloud instance.

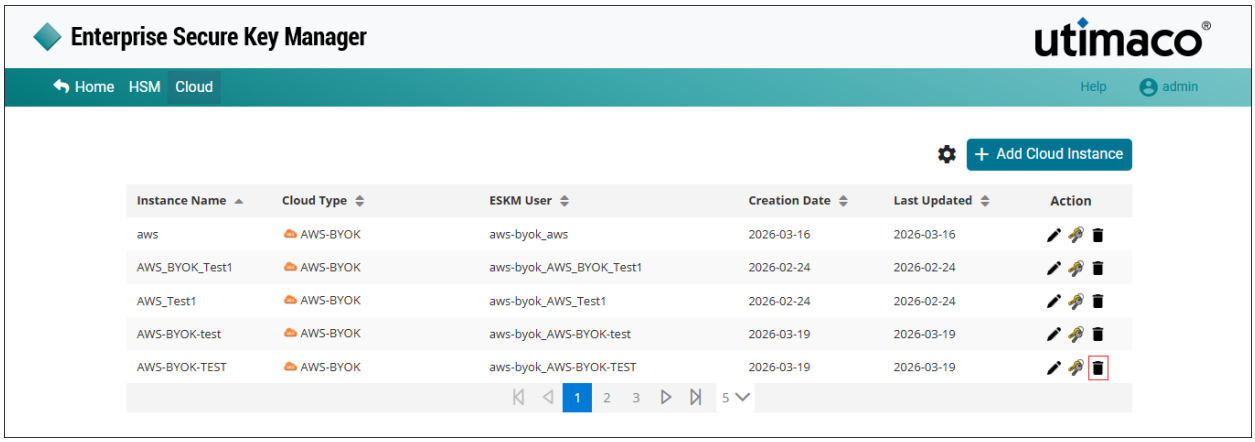

Figure 16 : Delete AWS-BYOK Cloud Instance

- The **Delete Cloud Instance** pop-up window will be displayed asking "**Are you sure you want to delete instance <instance name>?**". Click **Delete**.

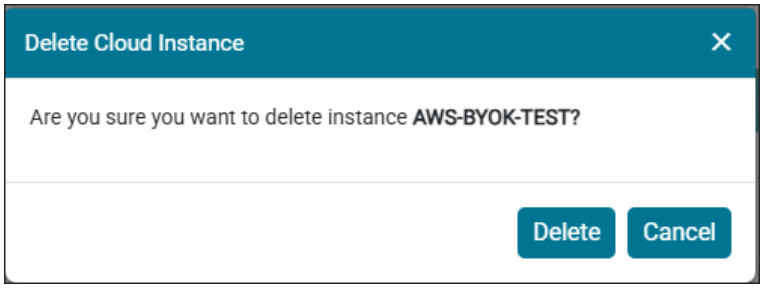

Figure 17 : Delete Cloud Instance Alert

Cloud instance AWS-BYOK-TEST deleted successfully.

You cannot delete a cloud instance if the keys are already associated with it.

5.1.4 Viewing AWS-BYOK Key Dashboard

- Click the **Manage Keys** icon to view keys available in the AWS-BYOK cloud instance.

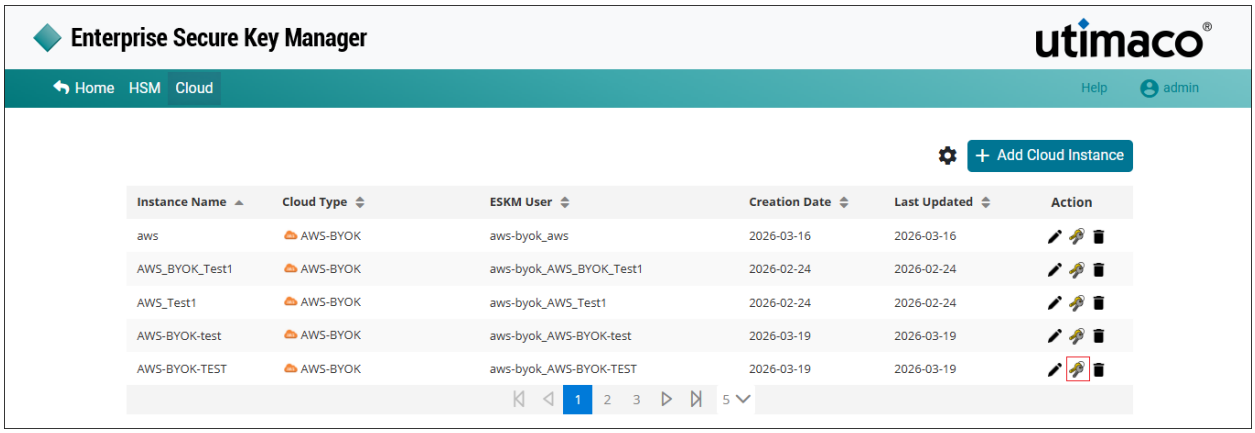

Figure 18 : Manage Keys

- The list of keys for the specified Instance is displayed.

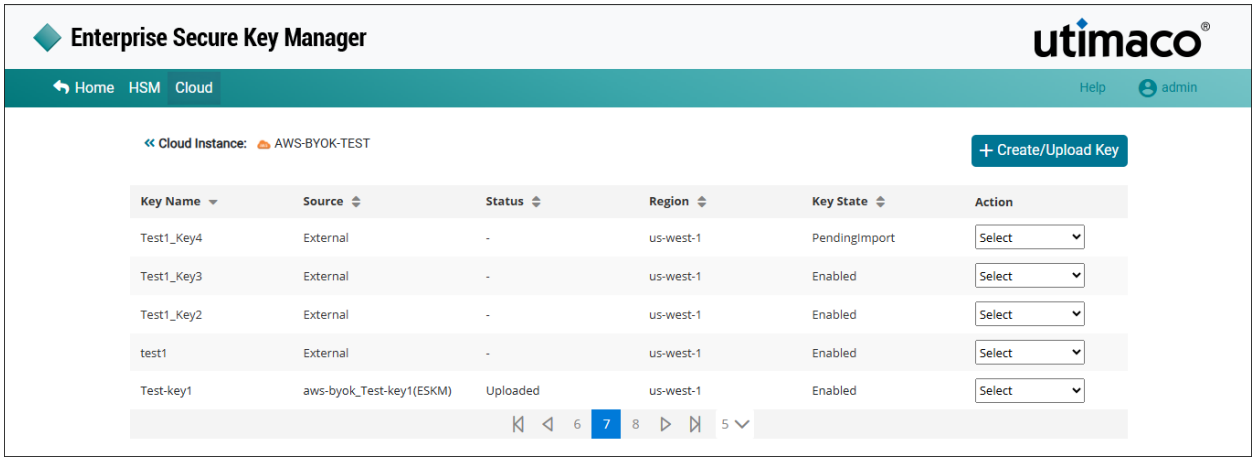

Figure 19 : AWS-BYOK-Key-List

ESKM supports up to 100 keys excluding those which are pending for deletion.

Parameters	Description
Key Name	Name of the key which is created in the AWS-BYOK cloud instance.
Source	The key source indicates where key is generated. If the key was created in the ESKM, the format will be *Instance Name_Key Name(ESKM)*. If the key is created in the cloud, it will appear as external.

Parameters	Description
Status	Status of the key such as Uploaded or Not Uploaded.
Region	Select the regions to which the key needs to be imported.
Key State	key State such as Enabled, Disabled and Pending Import.
Action	It contains various key actions such as Edit, Delete and Upload.

Table 4: AWS_BYOK Keys List Parameters

- Click the required key from the keys list to view its detais and click **Close**.

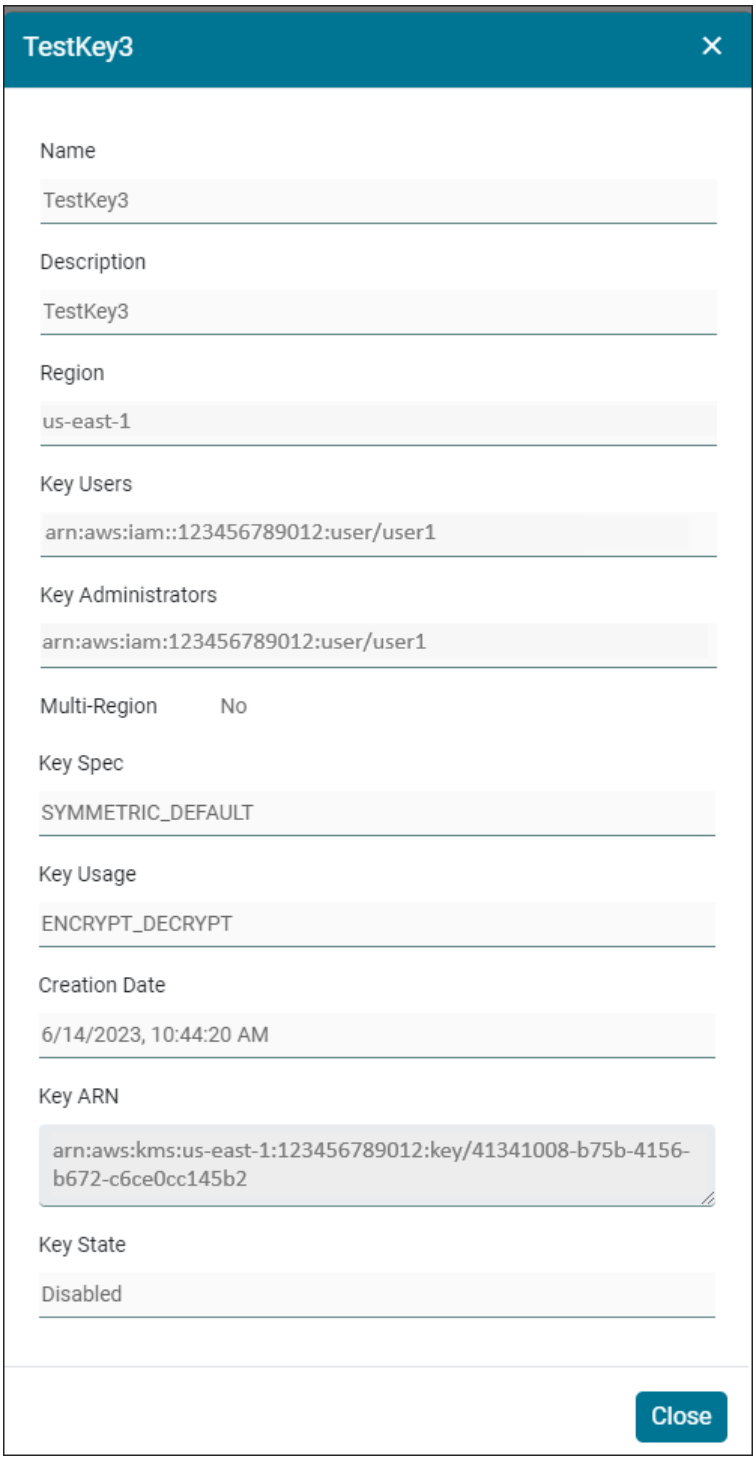

Figure 20 : View Key Details

Parameters	Description
Key Name	Name of the Key created in AWS-BYOK.

Parameters	Description
Description	Detailed information about the key.
Region	Regions to which the key is imported.
Key Users	The AWS IAM users who is responsible and has the access to create the key in AWS BYOK.
Key Administrators	The AWS IAM users who has the right to delete the key in AWS-BYOK.
Multi Region	Enable the Multi Region checkbox if the key to be replicated into other Regions.
Key Spec	The *key spec* determines whether the KMS key is symmetric or asymmetric.
Key Usage	Cryptographic operations supported by the key such as `ENCRYPT_DECRYPT, SIGN_VERIFY, or GENERATE_VERIFY_MAC.`
Creation Date	The date on which AWS-BYOK key is created.
Key ARN	Amazon Resource Name (ARN) of the KMS key. It is used to identify the an AWS KMS key.
Key State	Status of the key such as Enabled or Disabled.

Table 5: View Key Details - Parameters

5.1.5 Creating and Uploading a New Key

- Click the **Manager Keys** to view keys list available in the AWS-BYOK cloud instance.

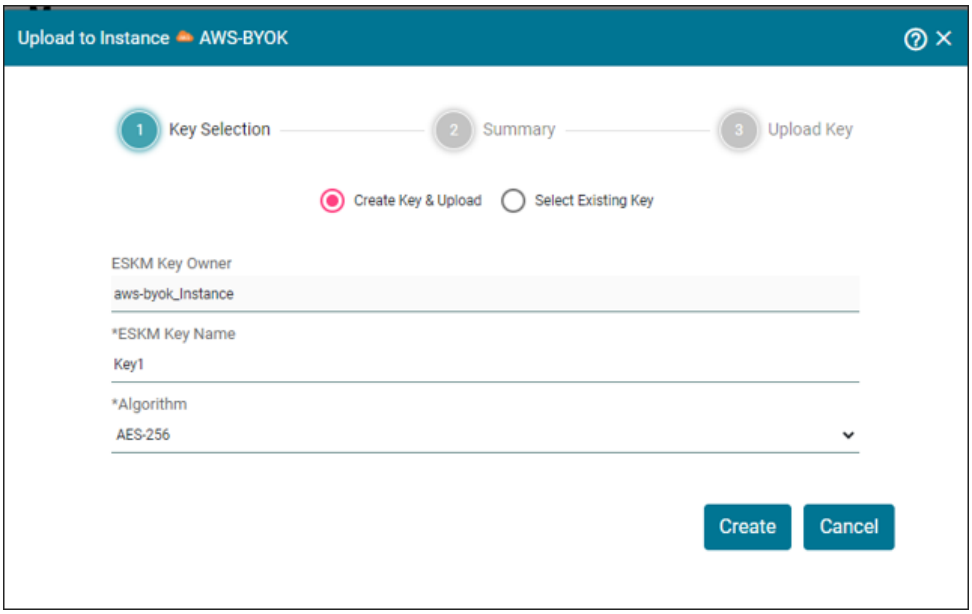

Figure 21 : Key Selection

- Specify the required information and click **Create.**
- The **Upload to Instance AWS-BYOK** pop-up appears and then click **Next**.

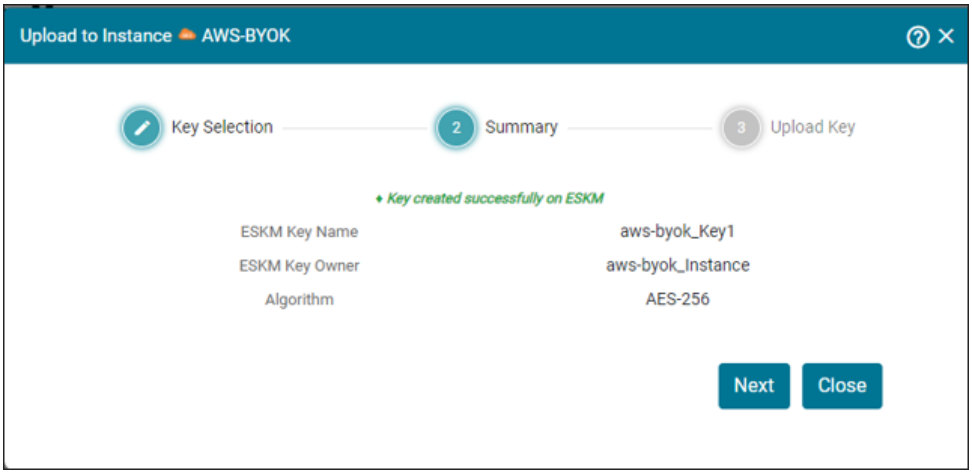

Figure 22 : Summary

- It is navigated to the Upload Key page and specify the required information. Click **Upload**.

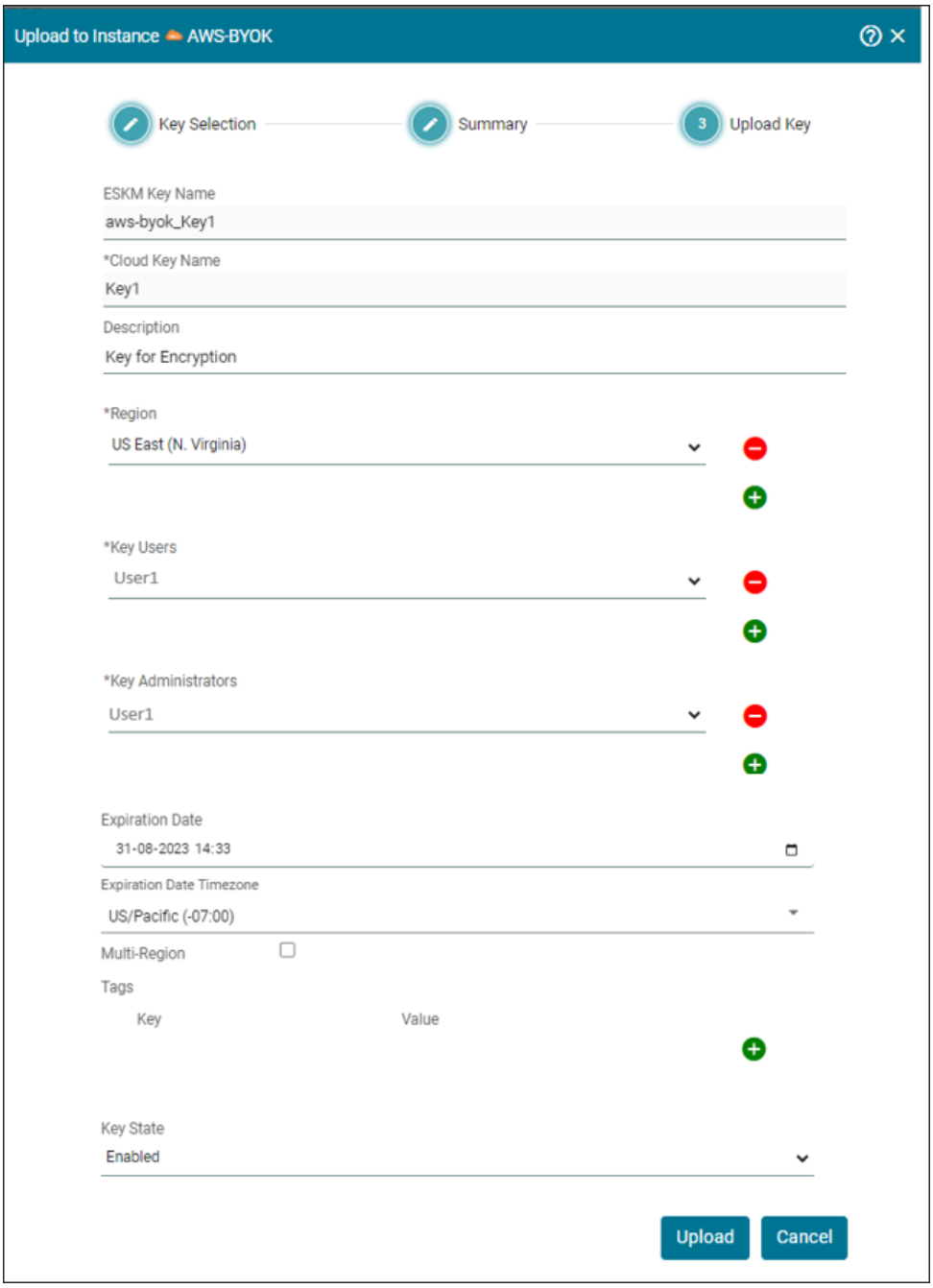

Figure 23 : Upload Key

The key has been successfully uploaded to instance AWS-BYOK.

Parameter	Description
ESKM Key Name	It is combination of Instance name and Key
Cloud Key Name	Name of the key which you want to create in ESKM-BYOK.
Description	Specific reason for what the key is used for in AWS-BYOK.
Region	Select the regions to which the key needs to be imported.
Key Users	Users who creates key for the specific reason.
Key Administrators	admin user who is responsible for deleting the key if necessary. Only administrator has access to delete the key.
Expiration Date	Set the expiration date by which the key must be expired.
Expiration Time Zone	The expiration date time zone is activated based on the current time of the system.
Multi Region	Enable this for allowing the key to be replicated into other Regions.
Tags	Tag is to organize the keys in AWS-BYOK. Multiple Tags can be assigned for a specific key.
Key State	Specify the key status to be enabled or disabled.

Table 6: Create AWS-BYOK Key - Parameters

5.1.6 Uploading an Existing Key

This section describes the procedure to upload existing Keys from Utimaco ESKM to AWS-BYOK KMS.

To upload an existing key:

- Click the **Manage Keys** icon to view keys list available in the cloud instance.

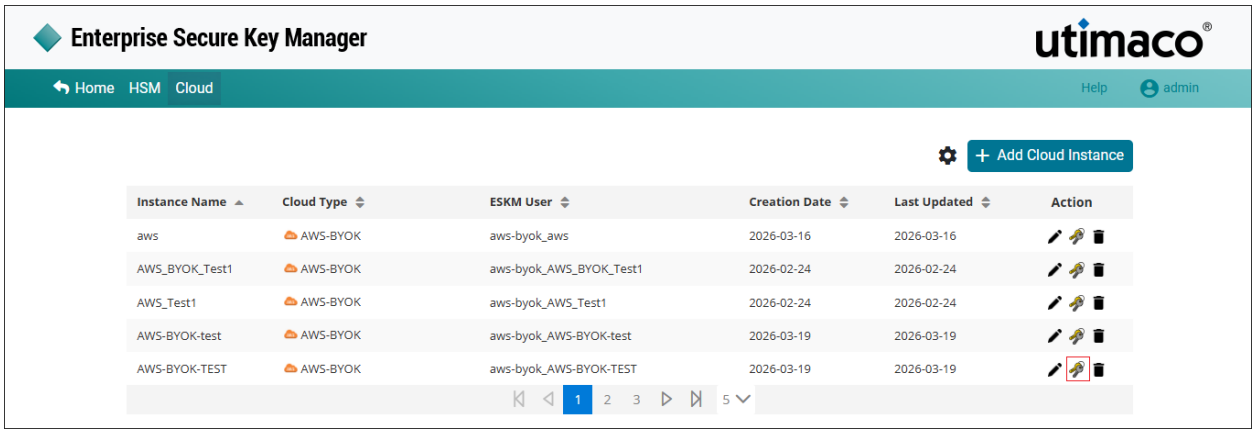

Figure 24 : Manage Keys

- Click **Create/Upload Key** at the right corner of the Cloud Instance page.

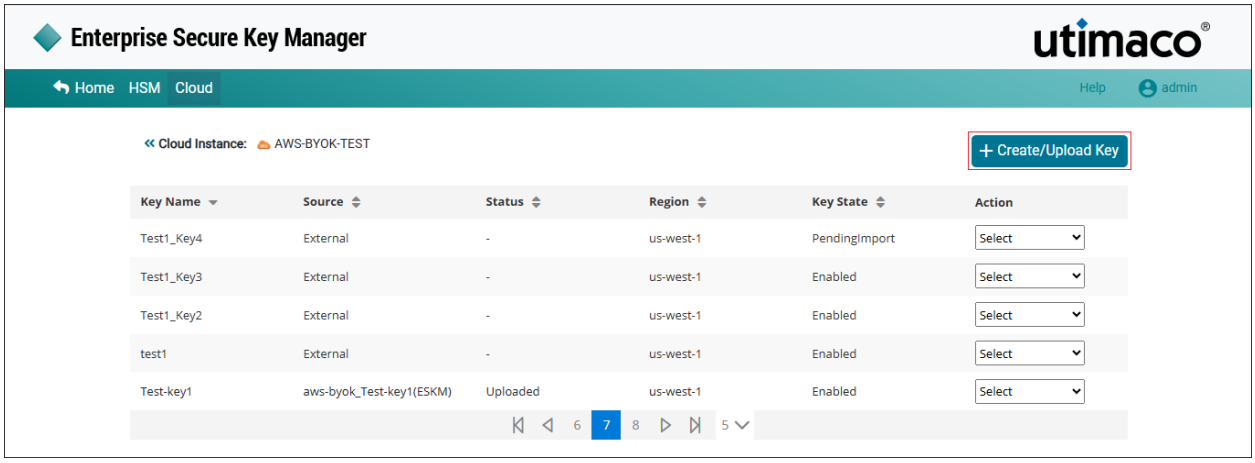

Figure 25 : Create/Upload Key

- The **Upload to Instance AWS-BYOK** pop-up appears. choose **Select Existing Key** option and select the existing key from the list.

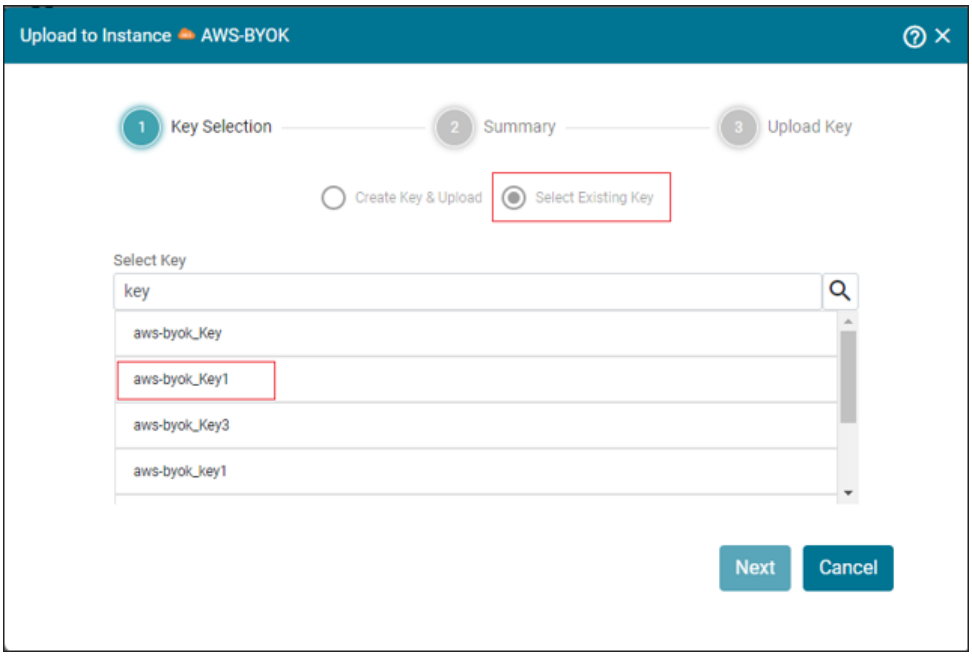

Figure 26 : Select Existing Key

- Click **Next**. The **Upload to Instance AWS-BYOK** Summary pop-up appears.

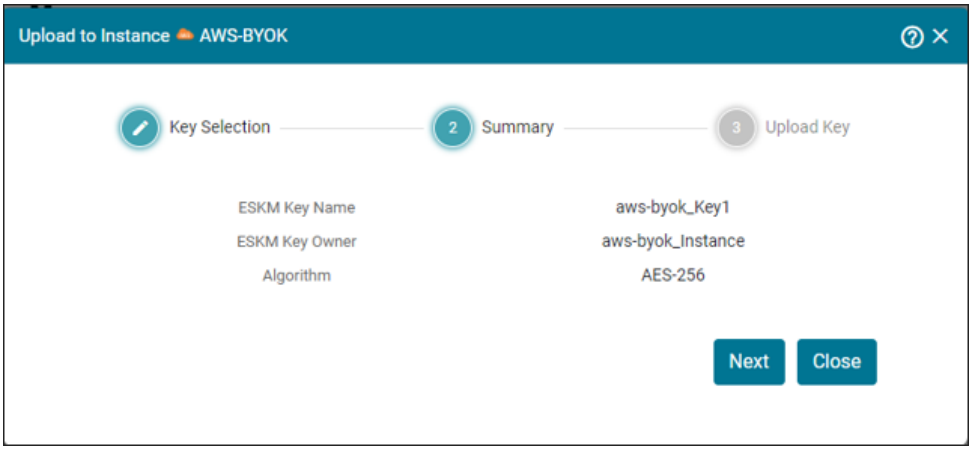

Figure 27 : Upload to Instance AWS-BYOK Summary

- Click **Next**. It navigates to the **Upload to Instance AWS-BYOK** pop-up window. Click **Upload**.

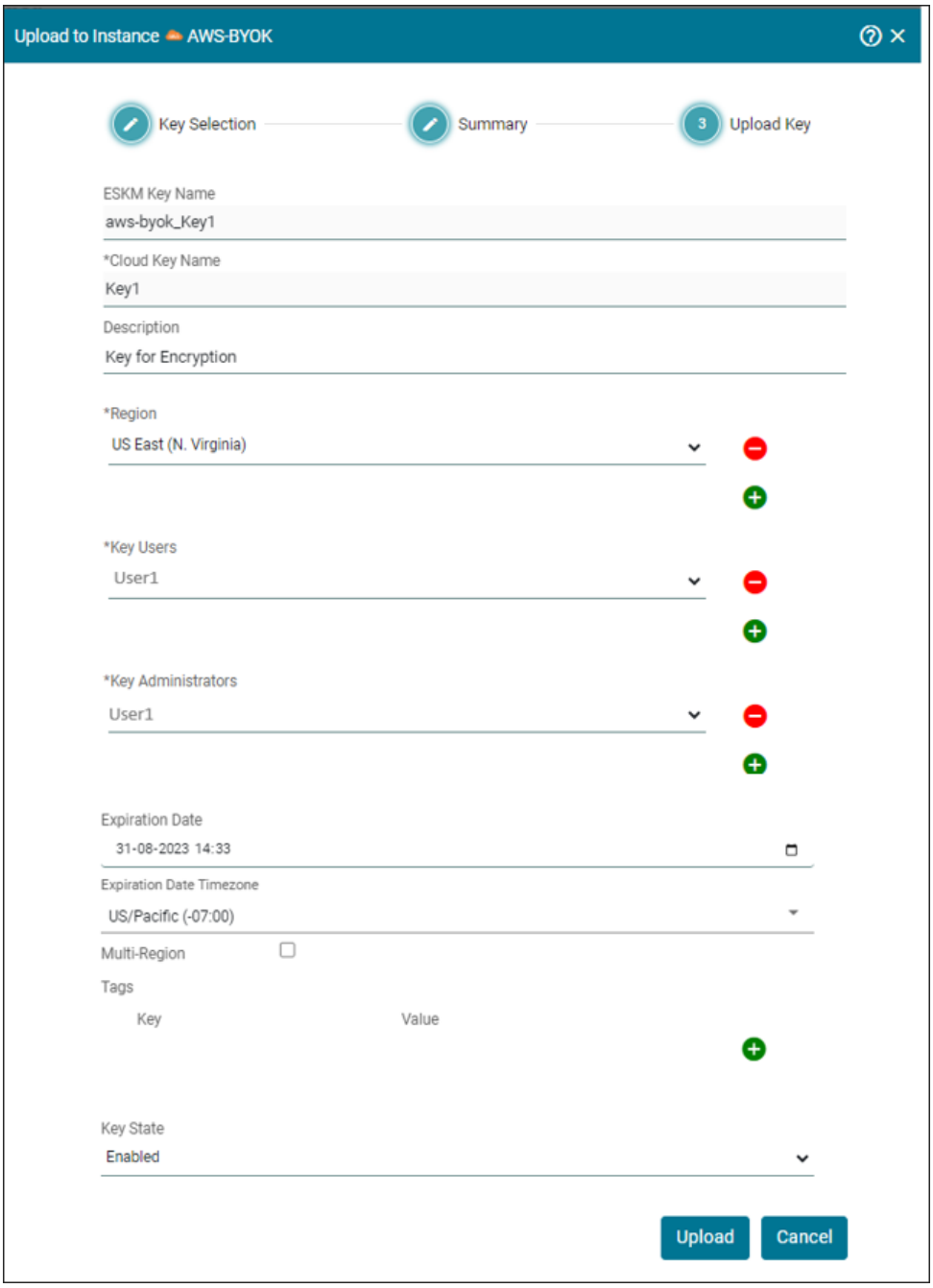

Figure 28 : Upload key

The Key [Key Name] has been successfully uploaded to Instance [AWS-BYOK].

5.1.7 Upload Key from ESKM to AWS-BYOK

- Click the **Manage keys** icon in the cloud instance to view the keys available in the cloud instance.
- If the key is not uploaded from Utimaco ESKM to AWS-BYOK and you wish to upload, select **Upload** from the drop-down.

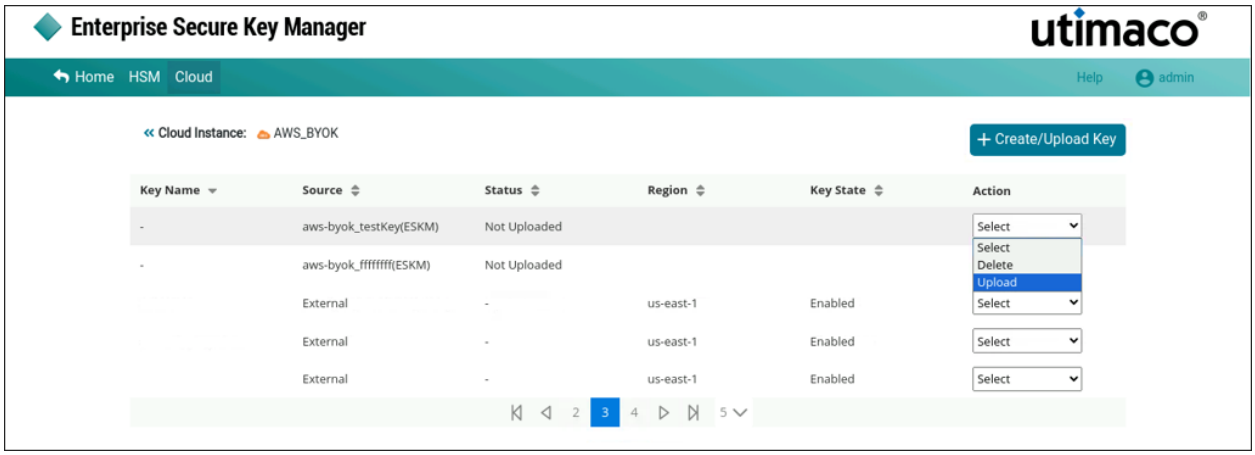

Figure 29 : Upload key from ESKM to AWS-BYOK

- The **Upload key (Key Name) to AWS-BYOK** pop-up window appears. Make the necessary changes and click **Upload**.

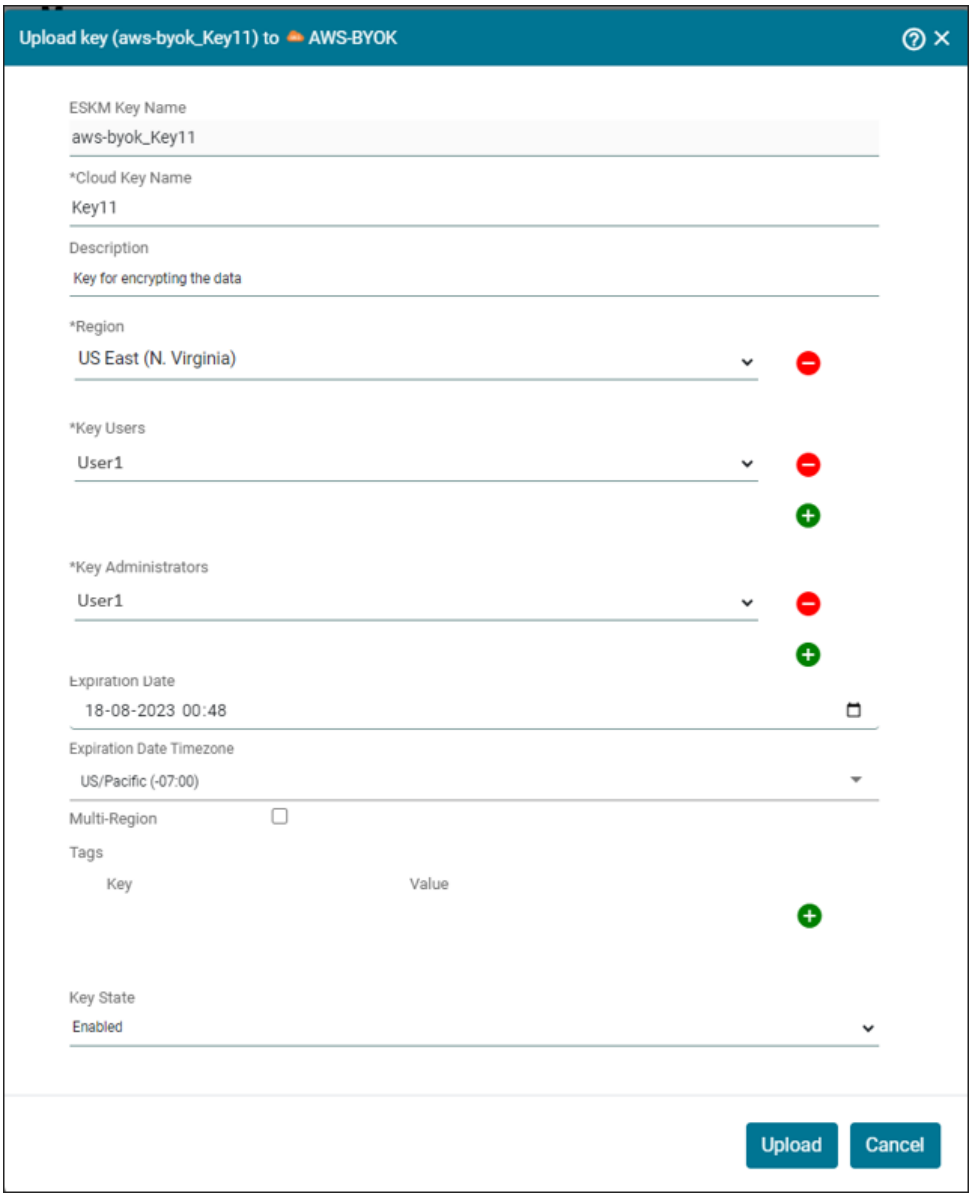

Figure 30 : Upload

Key [key name] has been successfully uploaded to instance [instance name].

5.1.8 Editing AWS-BYOK Key

- Under **Action** column, select **Edit** option to modify the selected key information.

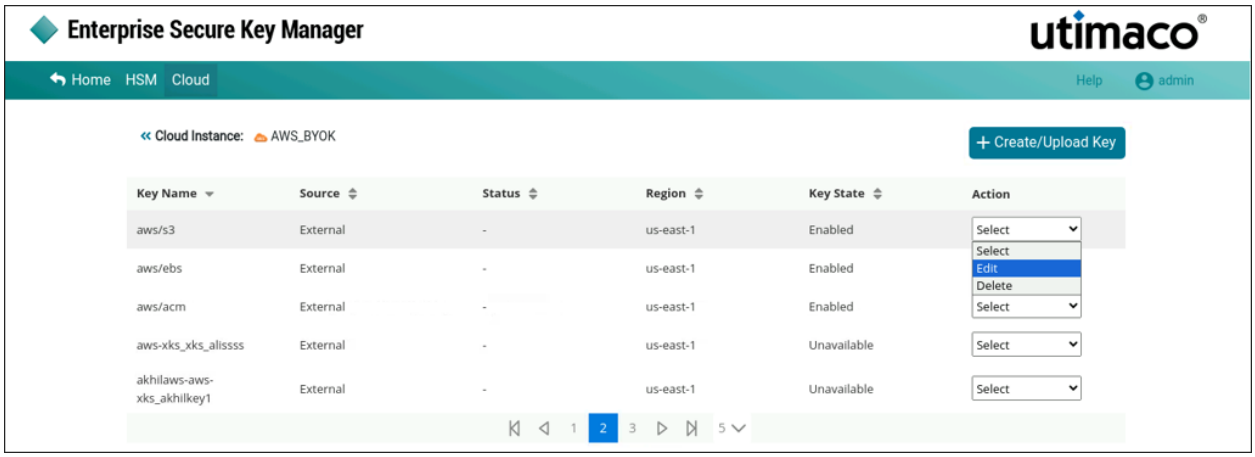

Figure 31 : Edit Key

- The **Edit Key (Key Name) on AWS-BYOK** pop-up window appears.

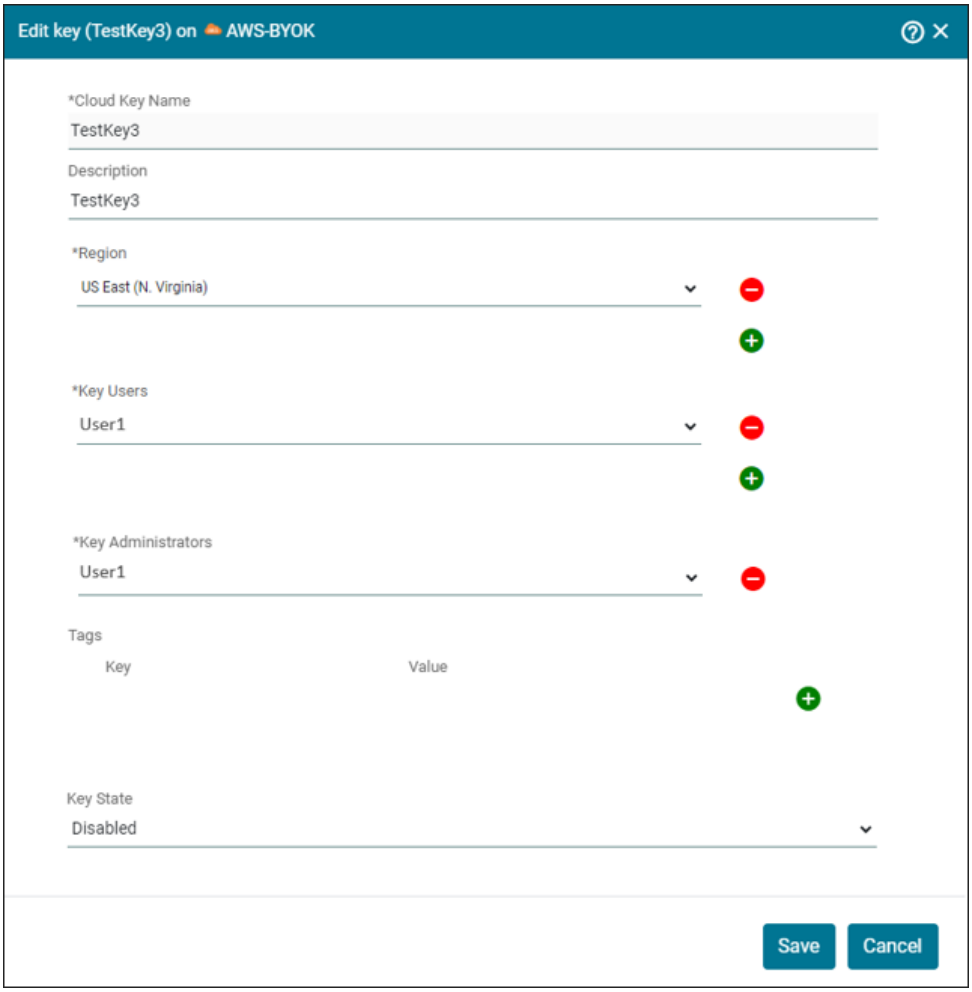

Figure 32 : Edit

- Make the necessary changes and click **Save**.

Cloud Instance Key (key name) updated successfully.

When editing an AWS BYOK key, only the **Description**, **Tags**, and **Key State** can be updated.

5.1.9 Deleting a AWS-BYOK Key

- Under **Action** column, select **Delete** from the drop-down list to delete the existing key.

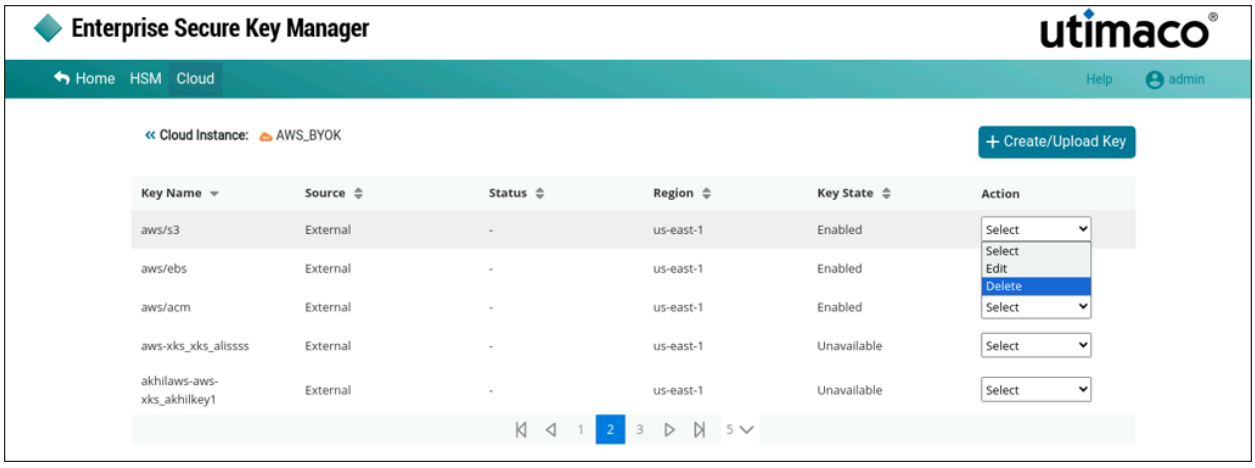

Figure 33 : Deleting AWS Key

- The **Alert** pop-up appears. Enter **Waiting Period (in days)** and click **Yes**.

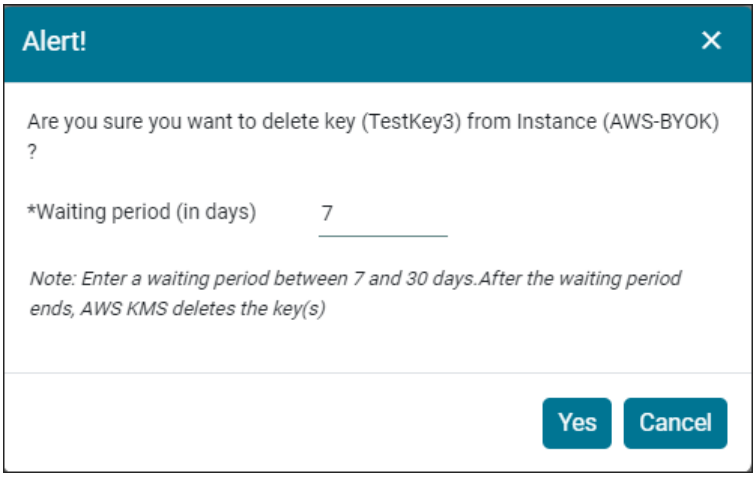

Figure 34 : Delete Key Alert

The user can specify a waiting period between 7 and 30 days. After the waiting periodn has expired, the AWS KMS deletes the key(s). During the waiting period, the key status is shown as “**Pending delete**”.

5.1.10 Create New Version

This section describes the procedure for performing key rotation by creating a new version of an existing key.

To create a new version:

- Under **Action** column, select **New Version** from the drop down to create a new version of the key.

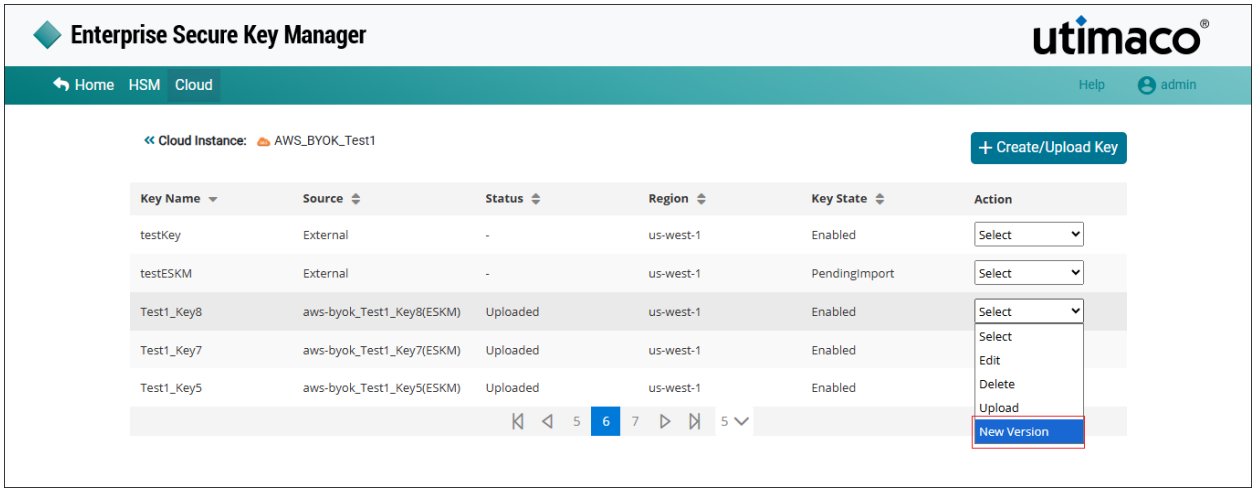

Figure 35 : Create New Version

- The **Alert!** pop-up window appears.

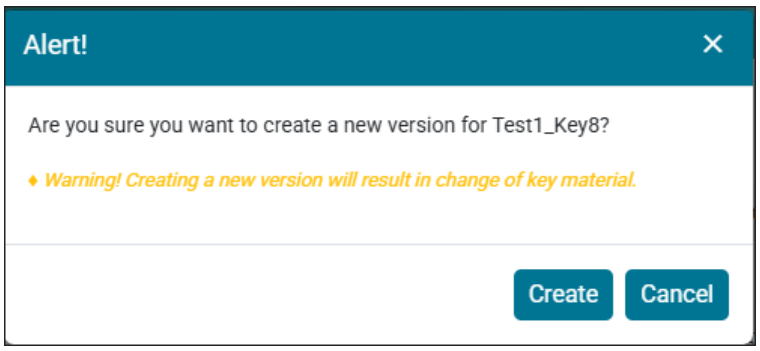

Figure 36 : Alert

- Click **Create** to perform key rotation, or click **Cancel** to cancel the operation.

New version 2 for ESKM key [aws-byok_Test1_Key8] added successfully.

After creating a new version, the key must be uploaded using the Upload option, see Upload Key from ESKM to AWS-BYOK.

The default value for the Number of Active Versions Allowed for a key is 10. To modify this setting, see **6.4.12.1 Active Versions** in the *ESKM User Guide-8.54.7*. If the maximum number of active key versions configured on the **Key Options** page is reached, creating a new key version will fail.

5.1.11 Key Rotation

Key Rotation is the process of creating a new version of an encryption key while retaining older key versions for decrypting existing data.

When a new key version is created in ESKM, the previously created key versions are **retained** and continue to be used for decrypting existing data. The newly created key version becomes the **current (default) key** for encrypting new data.

This capability enables the creation of a new version of the key on-demand for the purposes of compliance or suspected compromise without changing the key ID or disrupting active cloud applications.

To rotate a key in AWS BYOK:

1. After creating a new version of the encryption key, go to the **Actions** column for the key.

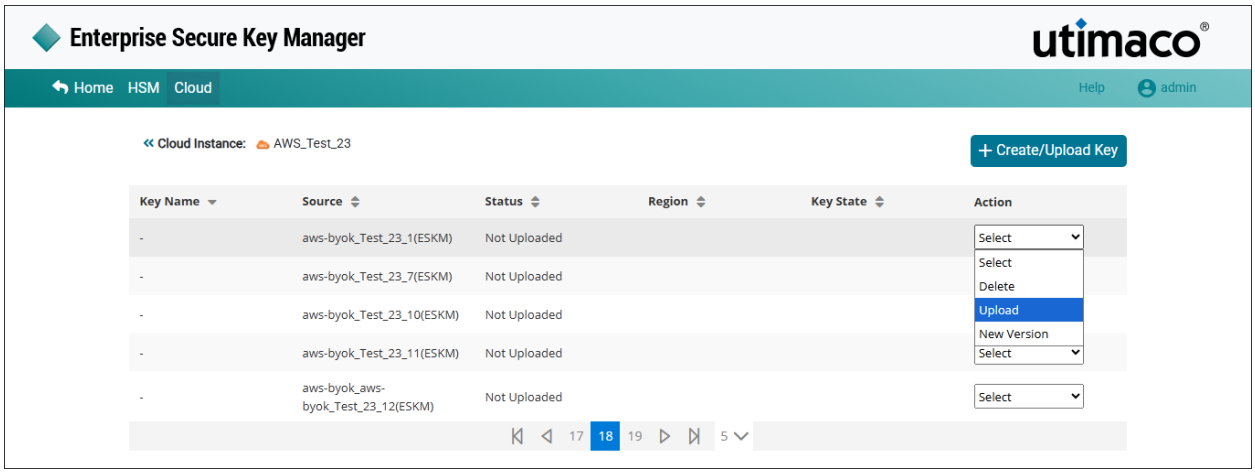

Figure 37 : Upload

2. Select **Upload** to upload the **new key version** to the AWS BYOK console.

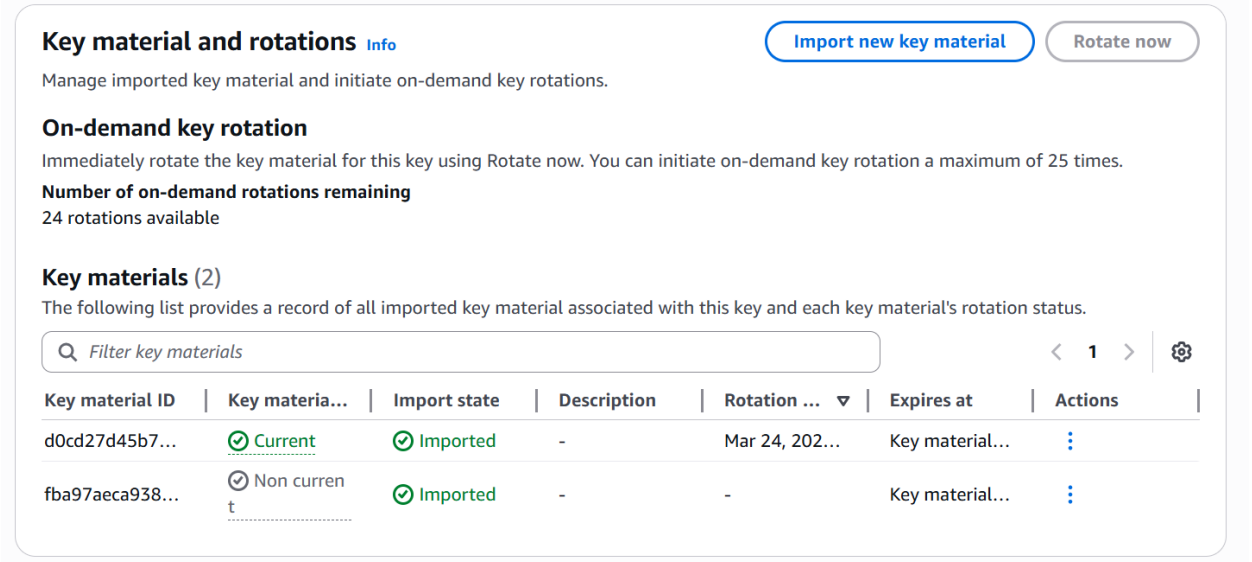

Figure 38 : Key Rotation - AWS-BYOK

For detailed steps, see Upload Key from ESKM to AWS-BYOK.

5.2 Configuration on AWS-BYOK

For more information on configuration on AWS-BYOK, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey.

6 Verification and Testing

6.1 Logs and Validation Steps

1. In the **ESKM Management Console** > **Security** > **Users & Groups** > **Local Groups**. Confirm that **Username** is created.

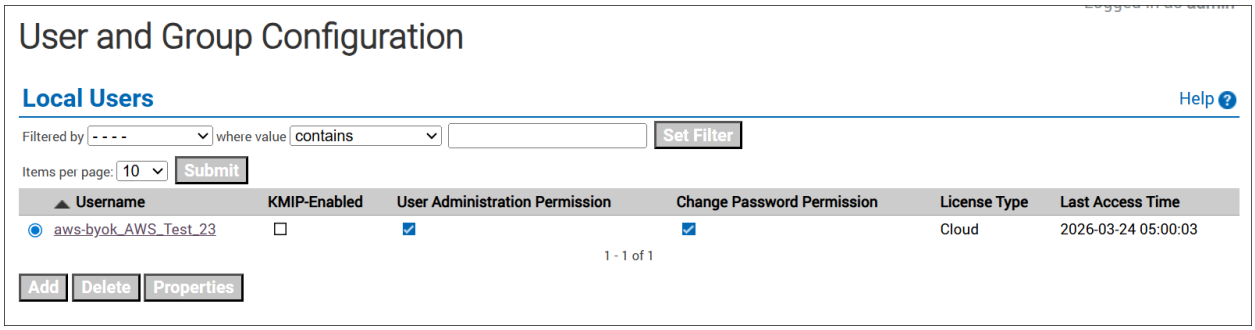

Figure 39 : Local Users

2. In the **ESKM Management Console** > **Security** > **Keys**. Confirm that the created keys are listed.

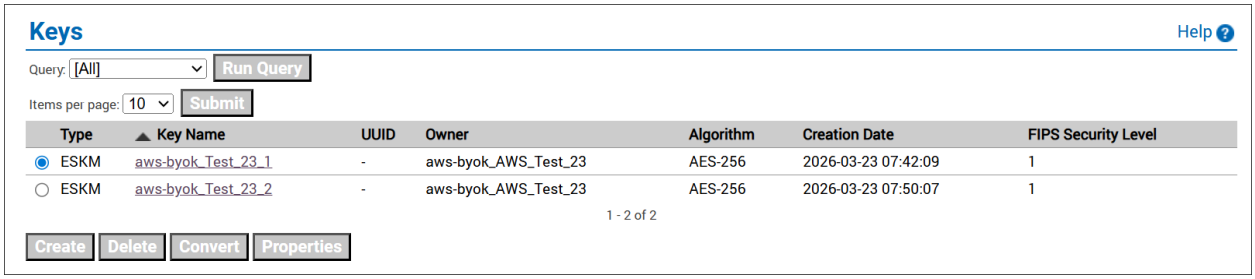

Figure 40 : Keys

3. In the ESKM Management Console, go to **Security > Keys**, select the required key, and then open **Key Versions** to verify that key rotation has been created.

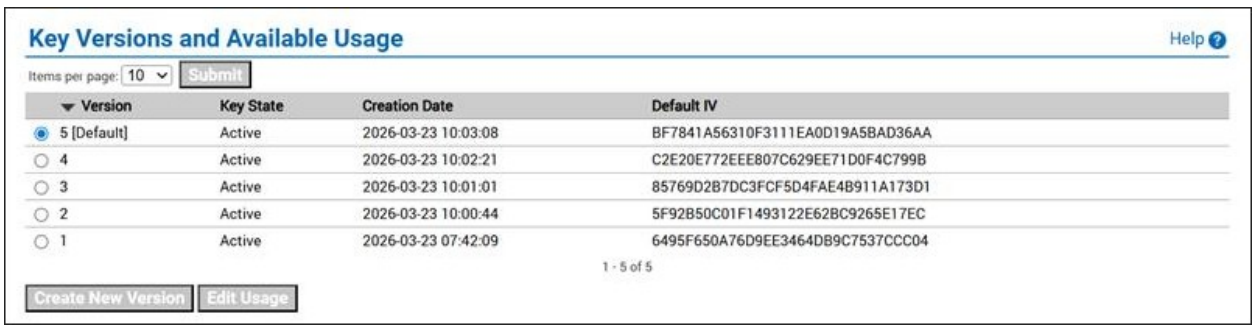

Figure 41 : Key Versions and Available Usage

4. After creating and uploading a key in ESKM, log in to **AWS** page > **Services** > **Key Management Service (KMS)** > **Customer-managed keys** > Search for the uploaded key > Click on **Key material and rotations.** Verify that the key is uploaded in the AWS-BYOK console.

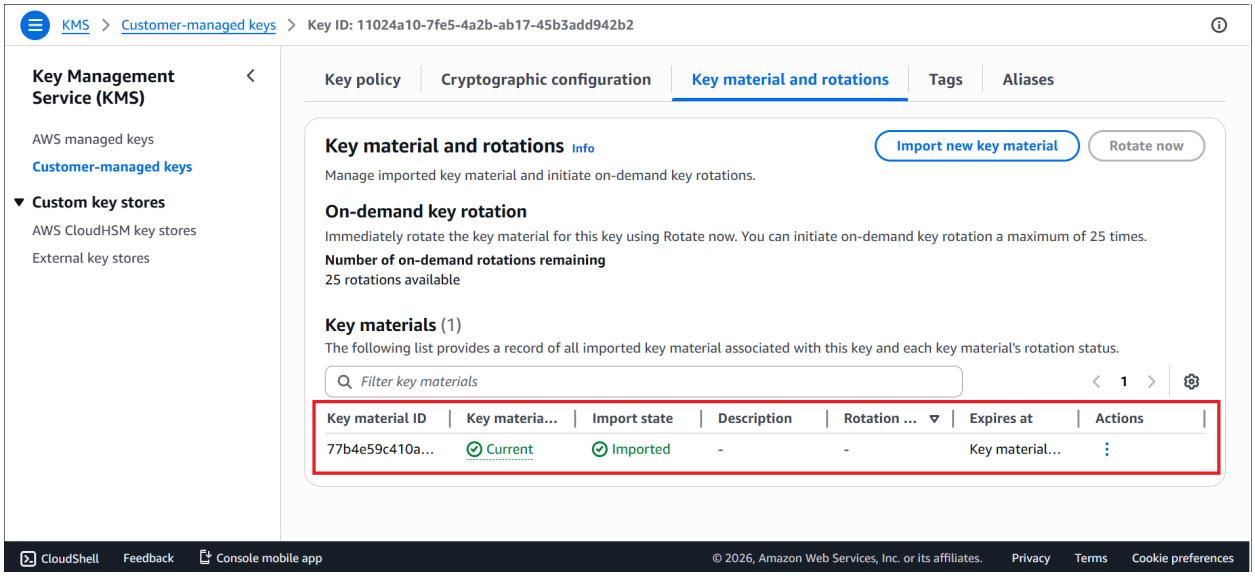

Figure 42 : Key created in AWS-BYOK

5. After creating new version of a key in ESKM, log in to **AWS** page > **Services** > **Key Management Service (KMS)** > **Customer-managed keys** > Search for the uploaded key > Click on **Key material and rotations**. Verify that the key rotation is created in AWS BYOK console.

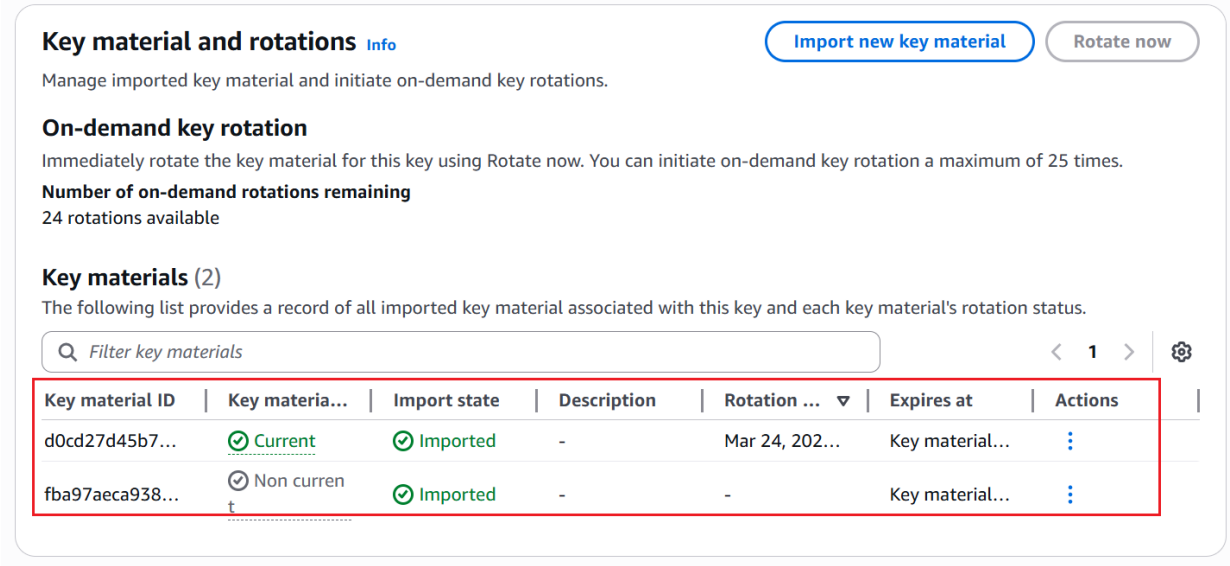

Figure 43 : Key Rotation created in AWS-BYOK

7 Troubleshooting

7.1 Log locations and interpretation

Verify the Utimaco ESKM logs by following the steps below:

1. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **REST**.
2. Review logs related to key rotation performed on the ESKM.

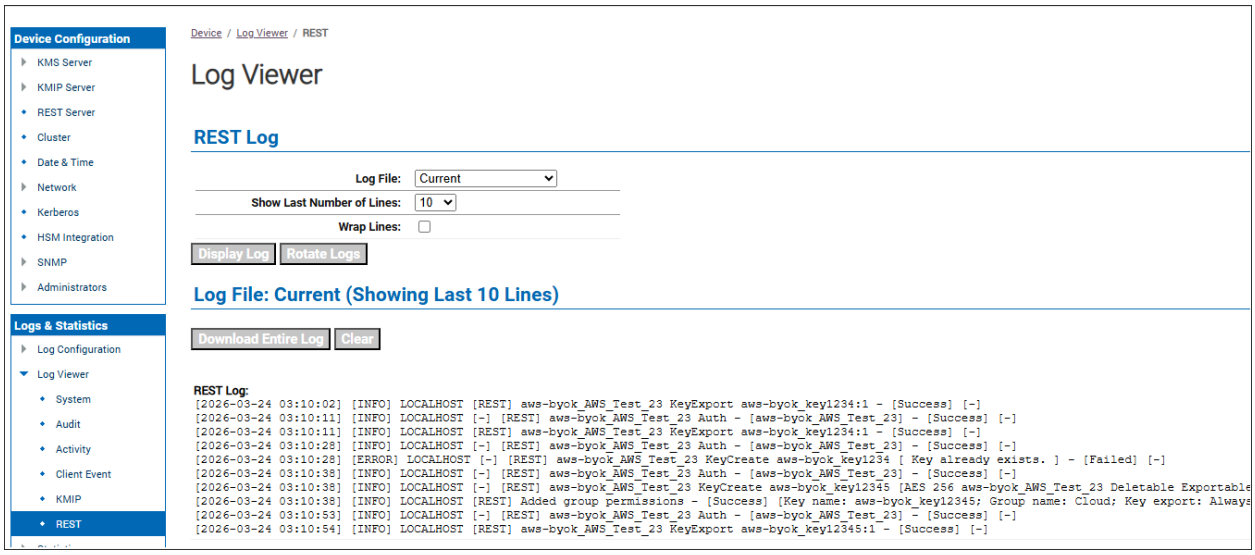

Figure 44 : AWS-BYOK - REST Log

8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Straße 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

9 Appendices

9.1 References

Title	Description	Document/Link
AWS-BYOK	Manage access keys for IAM users	https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey .

Table 7: References

9.2 Glossary

Term	Description
AWS-BYOK	A feature of AWS KMS that allows the use of encryption keys created outside AWS.
ESKM	Utimaco's product used to create and manage encryption keys outside AWS.
IAM (Identity and Access Management)	An AWS service used to manage user access and permissions.
Access Key ID	A credential used to identify a user or application in AWS.
Secret Access Key	A confidential credential used with the Access Key ID to access AWS services.
HSM (Hardware Security Module)	A secure device used to protect encryption keys.