

AWS
BYOK

Integration Guide

ESKM

8.54.7



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	2.0.0
Date	2026-07-13
Status	PUBLISHED
Document No.	IG-2026-0032
All rights reserved	No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems. Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1	About this Guide	5
1.1	Target Audience	5
1.2	Purpose of the Integration	5
1.3	Abbreviations	5
1.4	Document Conventions	6
2	Product Overview.....	8
2.1	Overview of the AWS-BYOK.....	8
2.2	Overview of Utimaco ESKM.....	8
2.3	Joint Value Proposition.....	8
3	Integration Requirements and Prerequisites	9
3.1	Tested Versions.....	9
3.2	Supported Platforms.....	9
3.3	Prerequisites	9
4	Installation and Configuration.....	10
4.1	Setting Up ESKM	10
4.2	Cloud Settings.....	14
4.3	Setting Up AWS-BYOK.....	15
5	Integration Steps	16
5.1	Configuration on ESKM	16
5.1.1	Adding a AWS-BYOK Cloud Instance.....	16
5.1.2	Editing an AWS-BYOK Cloud Instance.....	19
5.1.3	Deleting an AWS-BYOK Cloud Instance.....	20
5.1.4	Viewing AWS-BYOK Key Dashboard.....	21
5.1.5	Creating and Uploading a New Key	26
5.1.6	Uploading an Existing Key.....	30
5.1.7	Upload Key from ESKM to AWS-BYOK	34
5.1.8	Editing AWS-BYOK Key	36
5.1.9	Deleting an AWS-BYOK Key.....	38
5.1.10	Create New Version.....	39
5.1.11	Key Rotation.....	41
5.1.11.1	Auto-Key Rotation	42

5.2 Configuration on AWS-BYOK..... 44

6 Verification and Testing45

6.1 Logs and Validation Steps..... 45

7 Troubleshooting.....48

7.1 Log Locations and Interpretation 48

8 Contact and Support Information49

9 Appendix A: References.....50

10 Appendix B: Glossary51

1 About this Guide

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

The AWS BYOK integration with 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 Target Audience

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

1.2 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.

1.3 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
AWS	Amazon Web Services
ARN	Amazon Resource Name
BYOK	Bring Your Own Key

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

Table 1: Abbreviations

1.4 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
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chsm-create</code>
<i>Italic</i>	References and important terms	See <i>Sample Chapter</i> in the <i>CryptoServer - Sample Manual</i>

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

Table 3: Tested versions

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 to [Manage access keys for IAM users](#).

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.

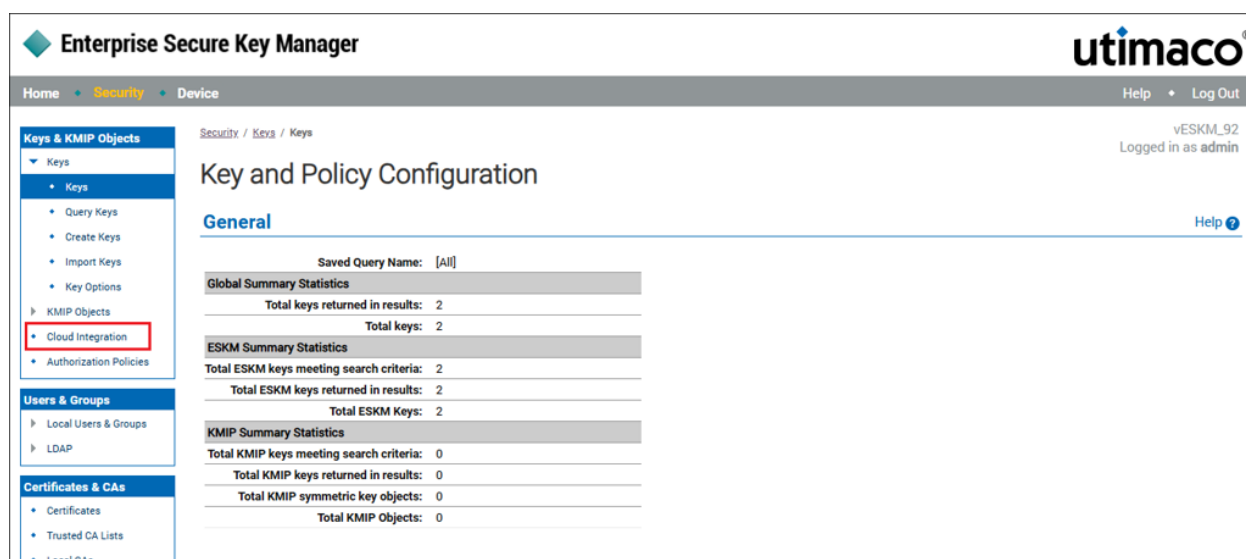


Figure 1 : Cloud integration

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

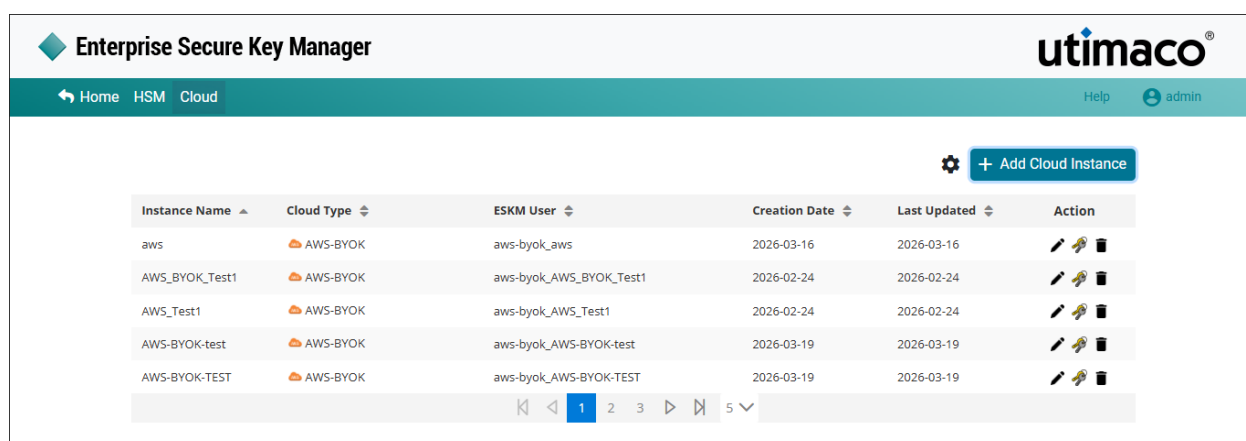


Figure 2 : Cloud integration dashboard

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

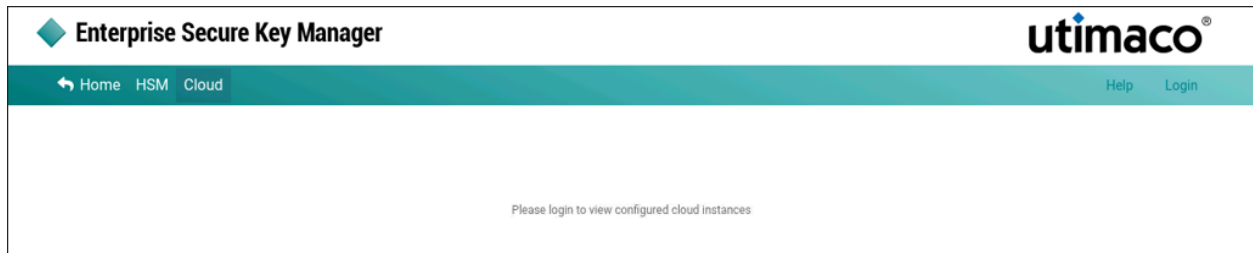


Figure 3 : Cloud integration login

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

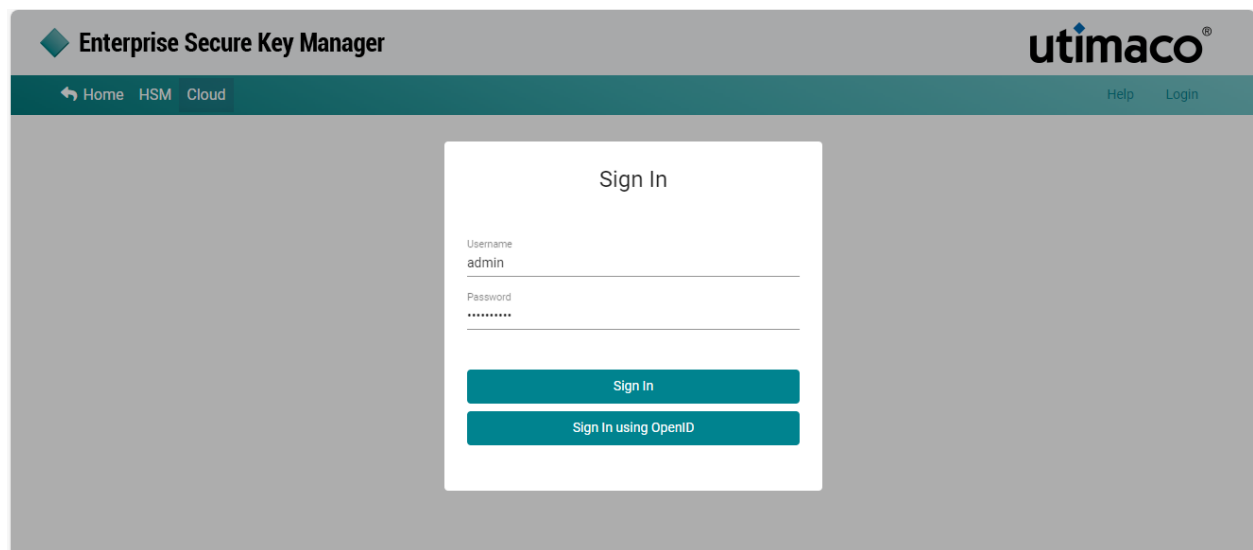
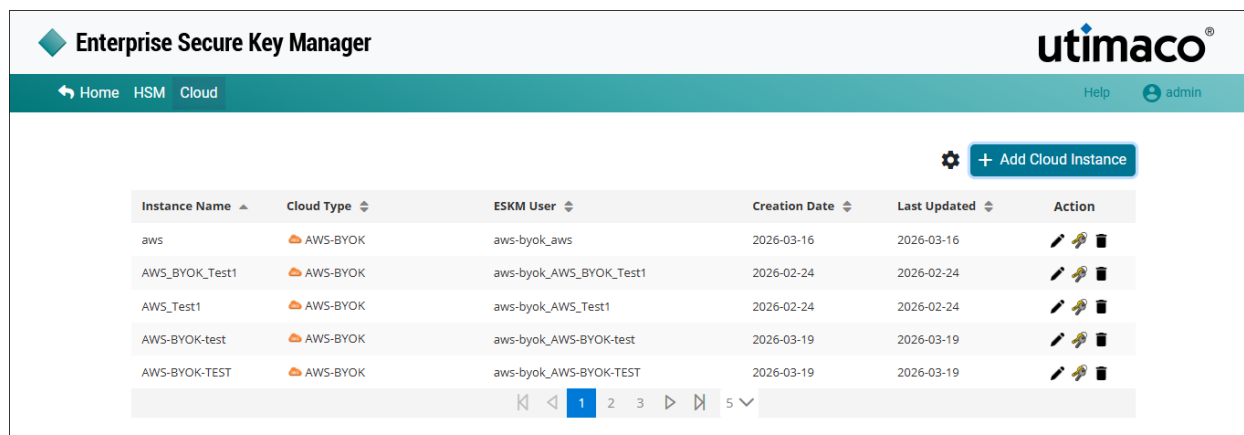


Figure 4 : Cloud integration Sign In

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



Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action
aws	AWS-BYOK	aws-byok_aws	2026-03-16	2026-03-16	[Edit] [Delete] [Refresh]
AWS_BYOK_Test1	AWS-BYOK	aws-byok_AWS_BYOK_Test1	2026-02-24	2026-02-24	[Edit] [Delete] [Refresh]
AWS_Test1	AWS-BYOK	aws-byok_AWS_Test1	2026-02-24	2026-02-24	[Edit] [Delete] [Refresh]
AWS-BYOK-test	AWS-BYOK	aws-byok_AWS-BYOK-test	2026-03-19	2026-03-19	[Edit] [Delete] [Refresh]
AWS-BYOK-TEST	AWS-BYOK	aws-byok_AWS-BYOK-TEST	2026-03-19	2026-03-19	[Edit] [Delete] [Refresh]

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 to *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.

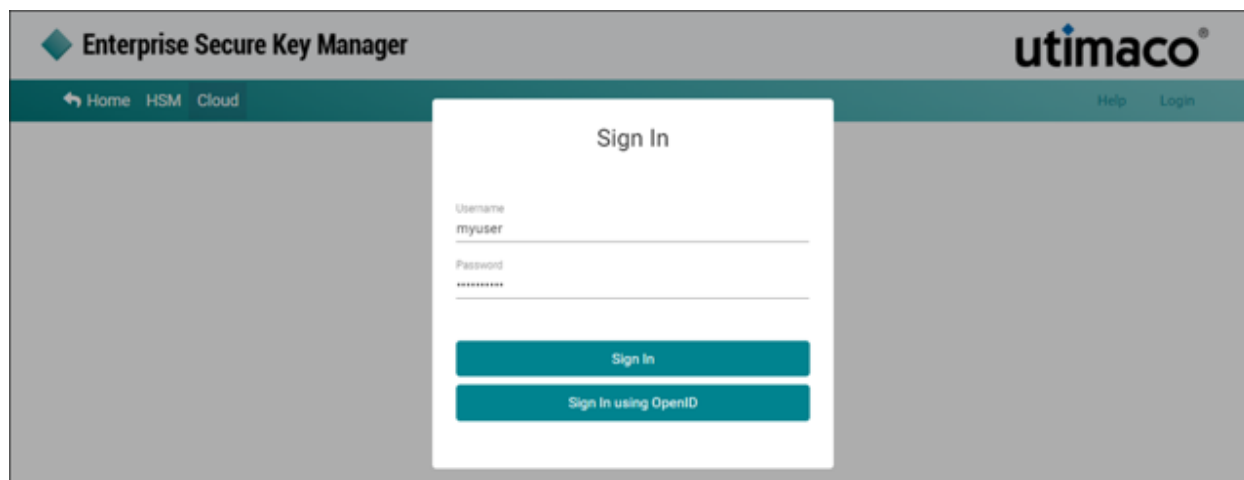


Figure 6 : Sign in using OpenID

- 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.

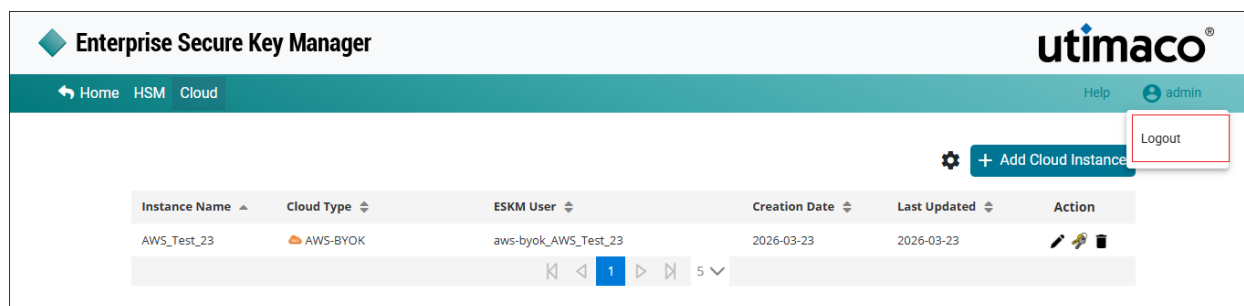


Figure 7 : Logout

- 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 the **Left** arrow at the left upper corner of the page to navigate to the ESKM application.

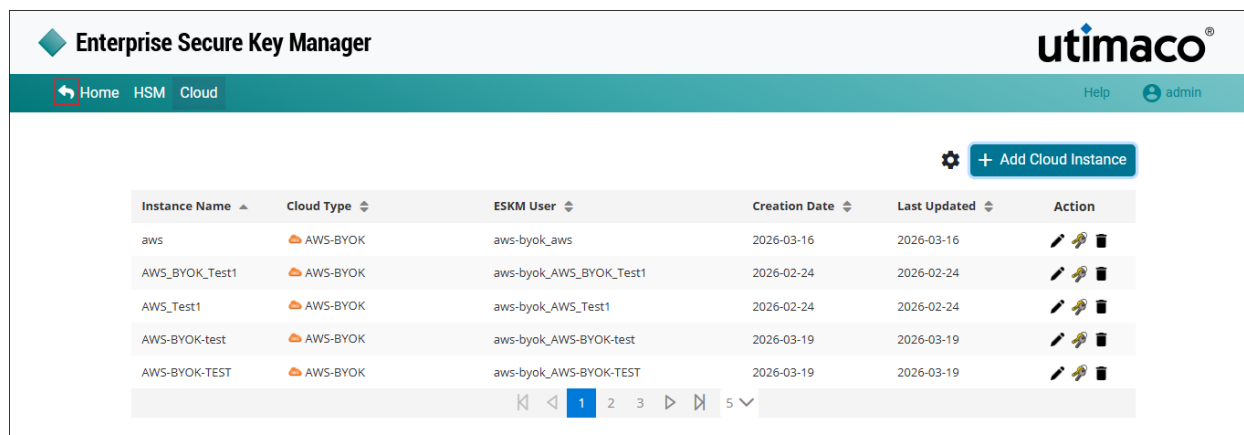


Figure 8 : Cloud integration dashboard

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.

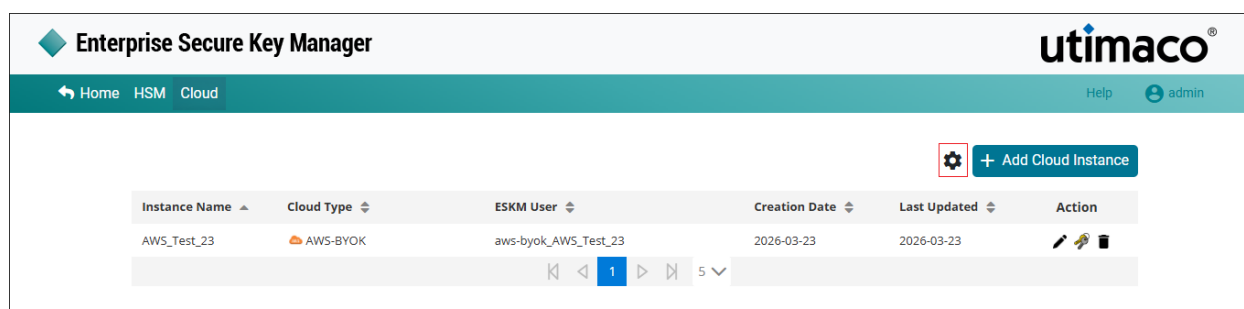
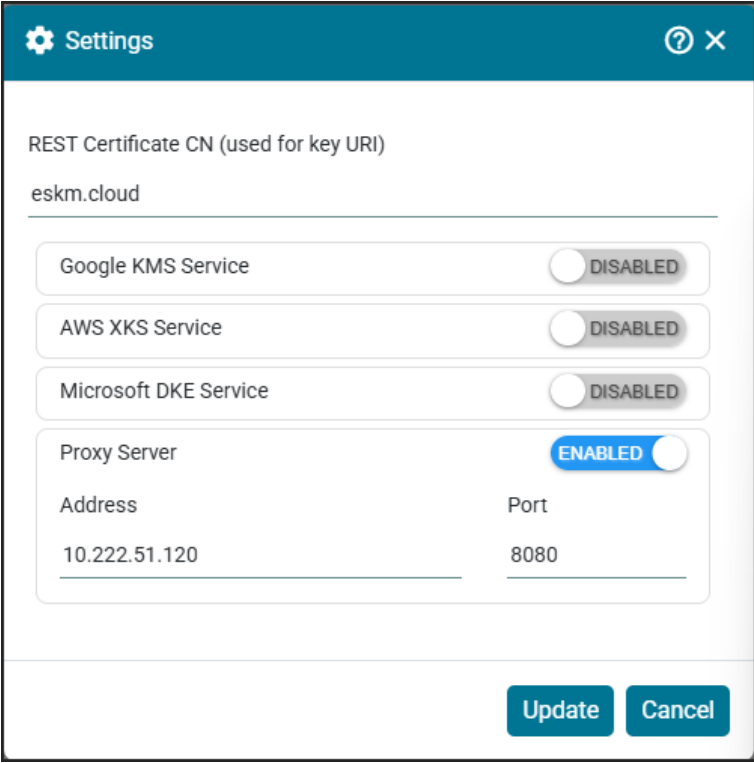


Figure 9 : Cloud settings

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



Settings

REST Certificate CN (used for key URI)

eskm.cloud

Google KMS Service ☐ DISABLED

AWS XKS Service ☐ DISABLED

Microsoft DKE Service ☐ DISABLED

Proxy Server ☒ ENABLED

Address Port

10.222.51.120 8080

Update Cancel

Figure 10 : Update settings

4.3 Setting Up AWS-BYOK

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 username 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.

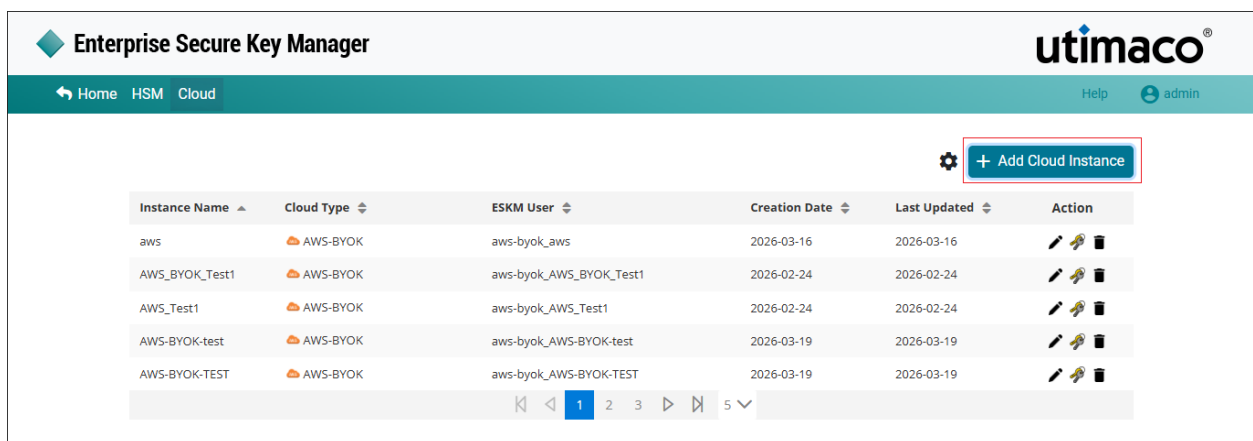
5 Integration Steps

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.

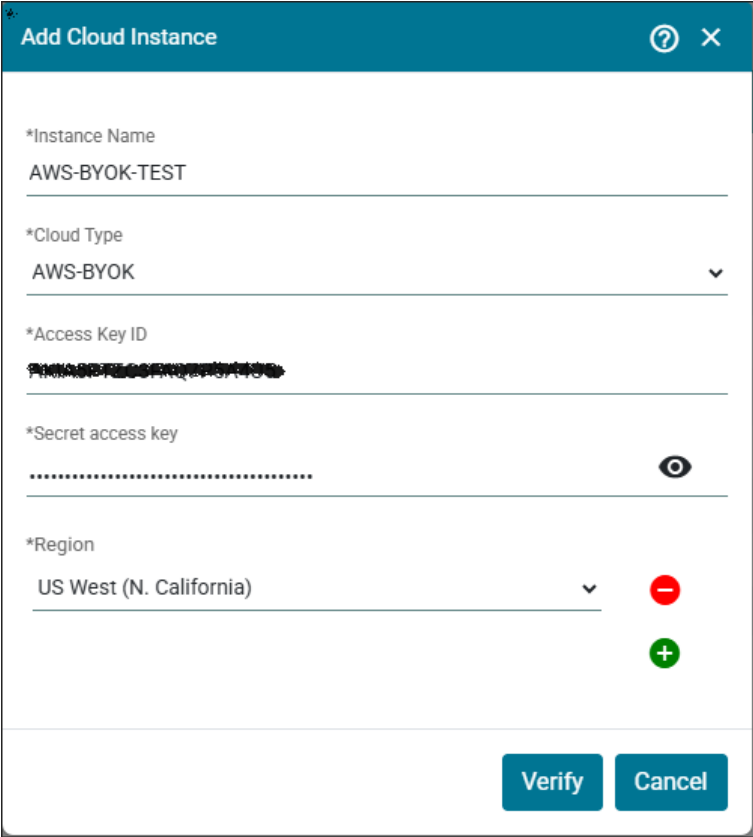


The screenshot displays the 'Enterprise Secure Key Manager' interface. At the top, there is a navigation bar with 'Home', 'HSM', and 'Cloud' tabs. The 'Cloud' tab is active. In the top right corner, there is a 'Help' link and a user profile icon labeled 'admin'. Below the navigation bar, there is a table of cloud instances. The table has columns for 'Instance Name', 'Cloud Type', 'ESKM User', 'Creation Date', 'Last Updated', and 'Action'. There are five rows of data, all with 'AWS-BYOK' as the cloud type. A red box highlights the '+ Add Cloud Instance' button in the top right corner of the table area. Below the table, there is a pagination bar showing '1' of 5 items.

Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action
aws	AWS-BYOK	aws-byok_aws	2026-03-16	2026-03-16	[Edit] [Refresh] [Delete]
AWS_BYOK_Test1	AWS-BYOK	aws-byok_AWS_BYOK_Test1	2026-02-24	2026-02-24	[Edit] [Refresh] [Delete]
AWS_Test1	AWS-BYOK	aws-byok_AWS_Test1	2026-02-24	2026-02-24	[Edit] [Refresh] [Delete]
AWS-BYOK-test	AWS-BYOK	aws-byok_AWS-BYOK-test	2026-03-19	2026-03-19	[Edit] [Refresh] [Delete]
AWS-BYOK-TEST	AWS-BYOK	aws-byok_AWS-BYOK-TEST	2026-03-19	2026-03-19	[Edit] [Refresh] [Delete]

Figure 11 : Add cloud instance

- The Add Cloud Instance pop-up appears.



Add Cloud Instance

*Instance Name
AWS-BYOK-TEST

*Cloud Type
AWS-BYOK

*Access Key ID
AKIAI44QH8DHBEXAMPLE

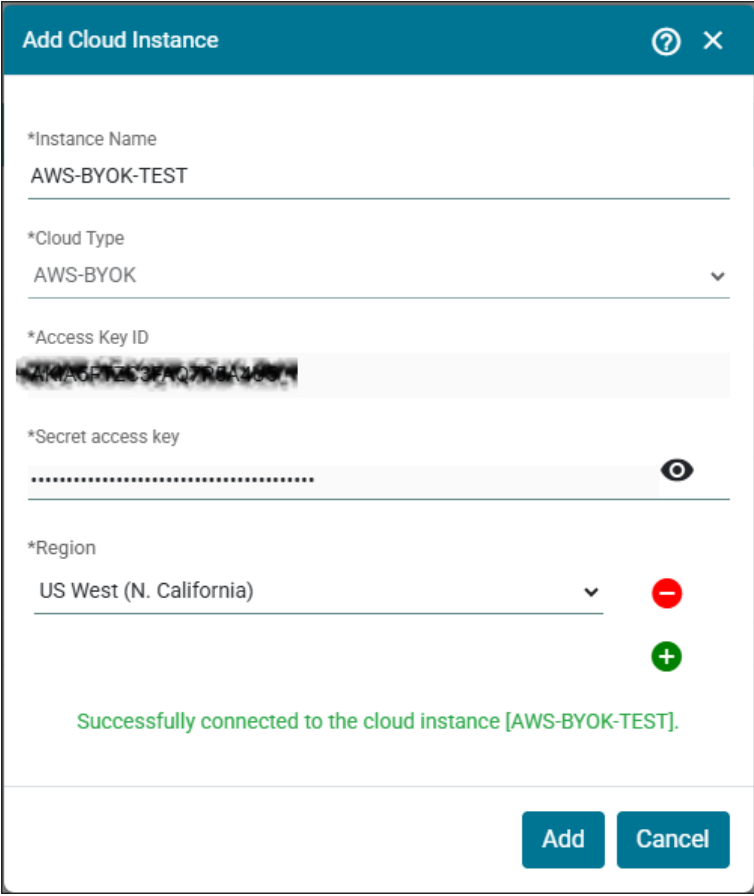
*Secret access key
.....

*Region
US West (N. California)

Verify Cancel

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**.



Add Cloud Instance

*Instance Name
AWS-BYOK-TEST

*Cloud Type
AWS-BYOK

*Access Key ID
AKIAQF7ZC37AQT7R8A3007

*Secret access key
.....

*Region
US West (N. California)

Successfully connected to the cloud instance [AWS-BYOK-TEST].

Add Cancel

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 4: Add AWS-BYOK cloud instance - parameters

5.1.2 Editing an AWS-BYOK Cloud Instance

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

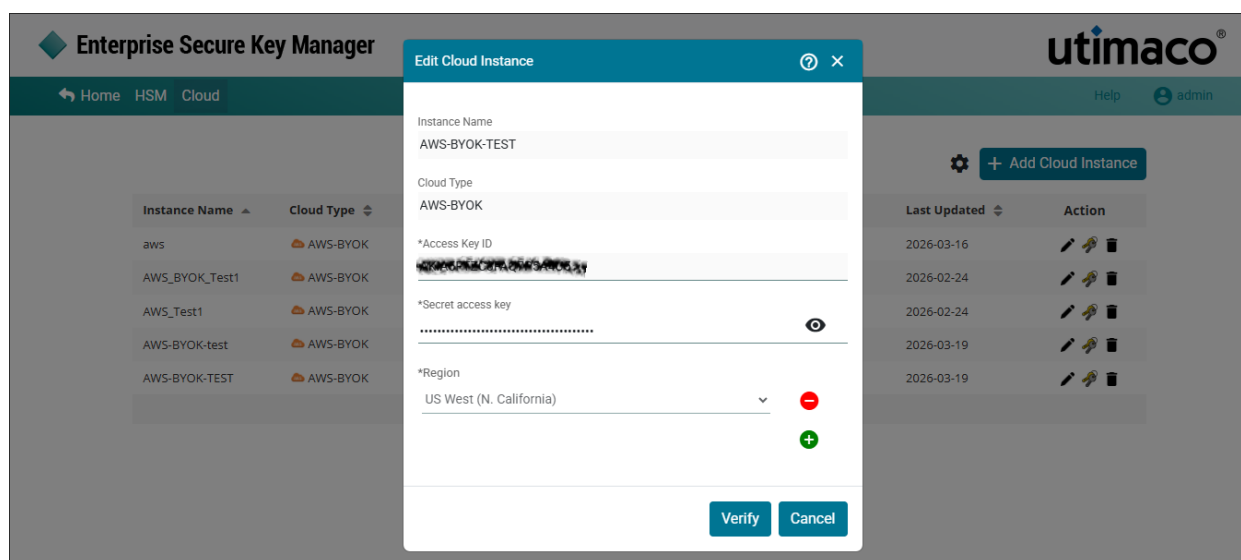
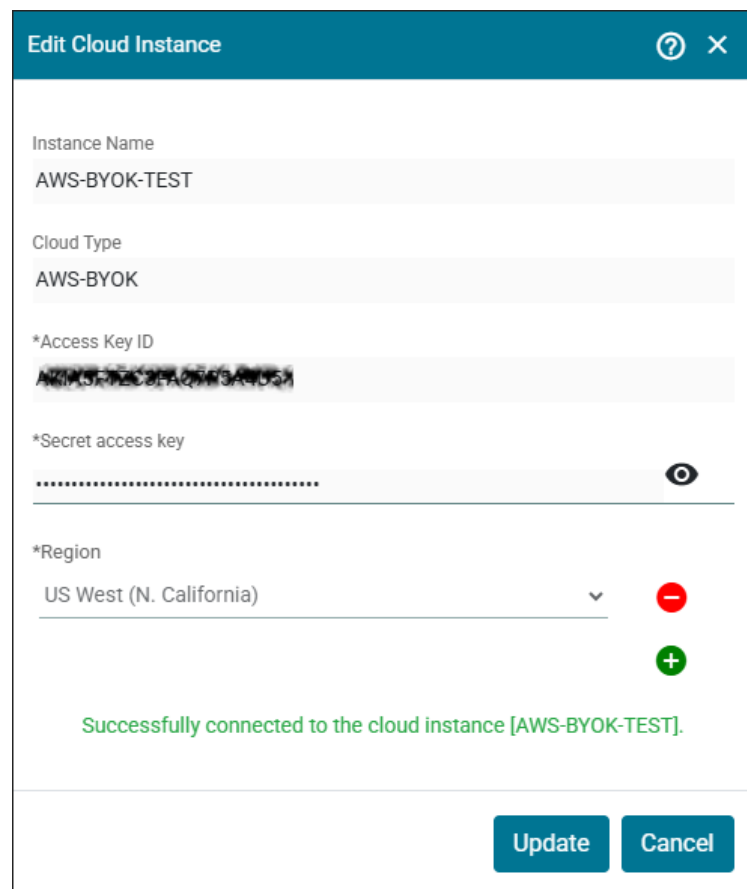


Figure 14 : Verify cloud instance

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



Edit Cloud Instance

Instance Name
AWS-BYOK-TEST

Cloud Type
AWS-BYOK

*Access Key ID
AKIA5F72C3FAQ993A9051

*Secret access key
.....

*Region
US West (N. California)

Successfully connected to the cloud instance [AWS-BYOK-TEST].

Update Cancel

Figure 15 : Edit Cloud Instance

- Click **Update**.



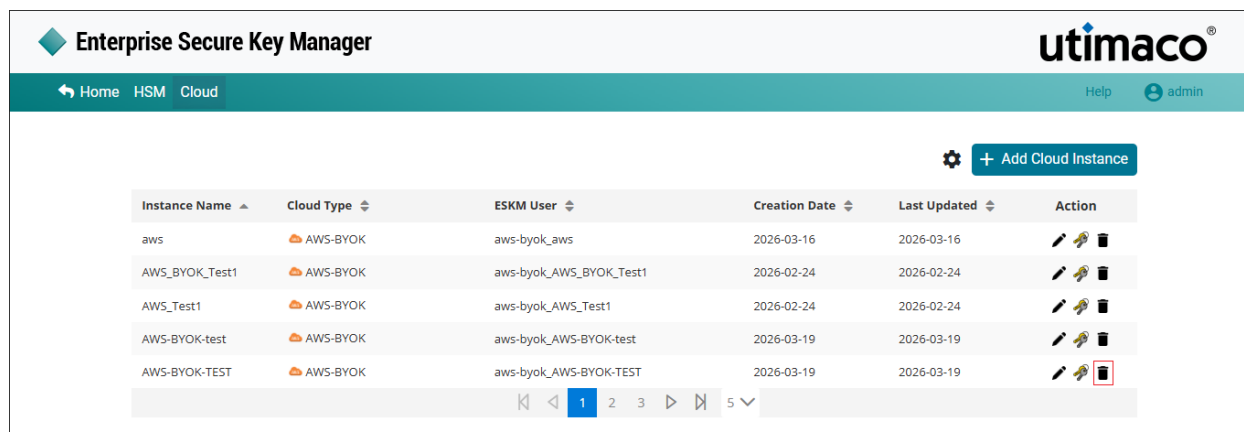
Cloud instance updated successfully.



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

5.1.3 Deleting an AWS-BYOK Cloud Instance

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



Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action
aws	AWS-BYOK	aws-byok_aws	2026-03-16	2026-03-16	 
AWS_BYOK_Test1	AWS-BYOK	aws-byok_AWS_BYOK_Test1	2026-02-24	2026-02-24	 
AWS_Test1	AWS-BYOK	aws-byok_AWS_Test1	2026-02-24	2026-02-24	 
AWS-BYOK-test	AWS-BYOK	aws-byok_AWS-BYOK-test	2026-03-19	2026-03-19	 
AWS-BYOK-TEST	AWS-BYOK	aws-byok_AWS-BYOK-TEST	2026-03-19	2026-03-19	 

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**.

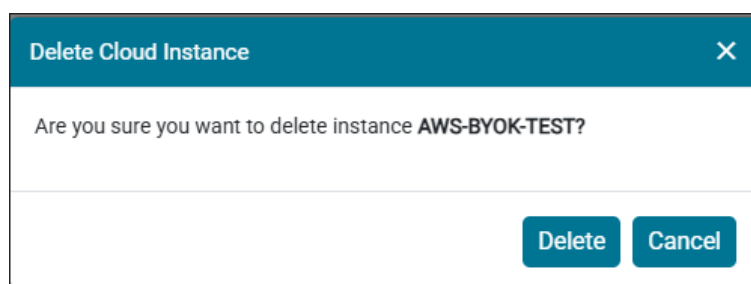


Figure 17 : Delete Cloud Instance alert



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.

Enterprise Secure Key Manager						utimaco®
Home HSM Cloud						Help admin
						+ Add Cloud Instance
Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action	
aws	AWS-BYOK	aws-byok_aws	2026-03-16	2026-03-16		
AWS_BYOK_Test1	AWS-BYOK	aws-byok_AWS_BYOK_Test1	2026-02-24	2026-02-24		
AWS_Test1	AWS-BYOK	aws-byok_AWS_Test1	2026-02-24	2026-02-24		
AWS-BYOK-test	AWS-BYOK	aws-byok_AWS-BYOK-test	2026-03-19	2026-03-19		
AWS-BYOK-TEST	AWS-BYOK	aws-byok_AWS-BYOK-TEST	2026-03-19	2026-03-19		
1 2 3 5						

Figure 18 : Manage keys

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

Enterprise Secure Key Manager						utimaco®
Home HSM Cloud						Help admin
<< Cloud Instance: AWS-BYOK-TEST						+ Create/Upload Key
Key Name	Source	Status	Region	Key State	Action	
Test1_Key4	External	-	us-west-1	PendingImport	Select	
Test1_Key3	External	-	us-west-1	Enabled	Select	
Test1_Key2	External	-	us-west-1	Enabled	Select	
test1	External	-	us-west-1	Enabled	Select	
Test-key1	aws-byok_Test-key1(ESKM)	Uploaded	us-west-1	Enabled	Select	
6 7 8 5						

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.

Parameters	Description
Source	The key source indicates where key is generated. If the key was created in the ESKM, the format will be <i>Instance Name_Key Name(ESKM)</i> . If the key is created in the cloud, it will appear as external.
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 5: AWS_BYOK keys list parameters

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

Name

Testkey001

Description

Testkey

Key State

Enabled

Multi-Region

No

Region

us-west-1

Key Users

Key Administrators

Key Spec

SYMMETRIC_DEFAULT

Key Usage

ENCRYPT_DECRYPT

Creation Date

7/9/2026, 3:03:46 PM

Key ARN

Auto Rotation

Enabled, 30 days, Next Rotation Time: 8/8/2026, 3:02:12 PM

Version

Version Number	Cloud Key Id	Rotation Type	Status	Creation Time
v1	b2731020-7191-434a-b04a-3917801ff430	MANUAL	ACTIVE	Jul 9, 2026, 3:02:1 PM

◀

▶

Close

Figure 20 : View key details

Parameters	Description
Key Name	Name of the Key created in AWS-BYOK.
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 <i>key spec</i> determines whether the KMS key is symmetric or asymmetric.
Key Usage	Cryptographic operations supported by the key such as <code>ENCRYPT_DECRYPT</code> , <code>SIGN_VERIFY</code> , or <code>GENERATE_VERIFY_MAC</code> .
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.

Parameters	Description
Auto Rotation	Displays the Auto Rotation status for the key. When enabled, the configured rotation interval and the next scheduled rotation time are displayed.
Version	Displays the available key versions along with version details such as Version Number, Cloud Key Id, Rotation Type, Status, Creation Time and Uploaded Time. Versions created through Auto Rotation are displayed as AUTO, while manually created versions are displayed as MANUAL.

Table 6: 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.

Upload to AWS  **AWS-BYOK**  

1 Key Selection

2 Summary

3 Upload Key

☒ Create Key & Upload ☐ Select Existing Key

ESKM Key Owner

aws-byok_AWS

*ESKM Key Name

Testkey002

*Algorithm

AES-256

▼

Create

Cancel

Figure 21 : Key Selection

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

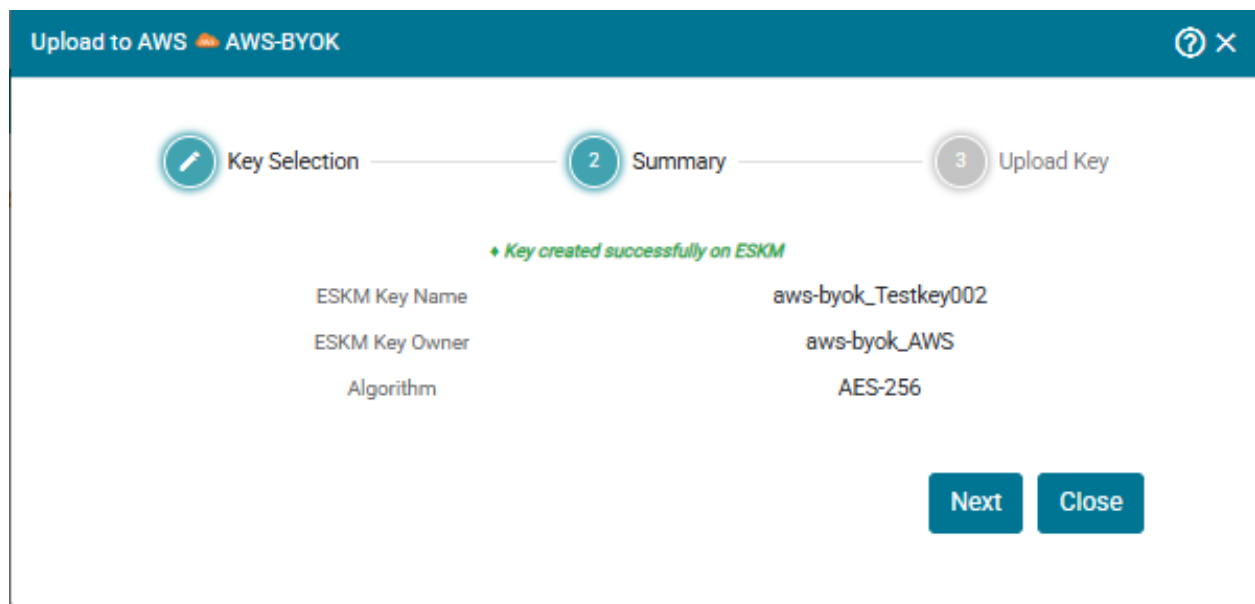


Figure 22 : Summary

- You will be navigated to the **Upload Key** page. Specify the required information and click **Upload**.

Key Selection

Summary

3 Upload Key

ESKM Key Name

aws-byok_Testkey002

*Cloud Key Name

Testkey002

Description

Key State

Enabled

▼

Multi-Region

☐

*Region

US West (N. California) ▼

+

+

*Key Users

▼

+

+

*Key Administrators

▼

+

+

Expiration Date

05/20/2027 03:49 PM

📅

Expiration Date Timezone

Asia/Calcutta (+05:30) ▼

Tags

Key	Value

+

Auto Rotation

☒ Enable Auto Rotation

Rotation Interval (Days)

30

Upload

Cancel

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.

Parameter	Description
Key State	Specify the key status to be enabled or disabled.
Enable Auto Rotation	Enables automatic creation of new key versions.
Rotation Interval (Days)	Specifies the frequency at which a new key version is automatically generated. Supported values range from 30 to 365 days.

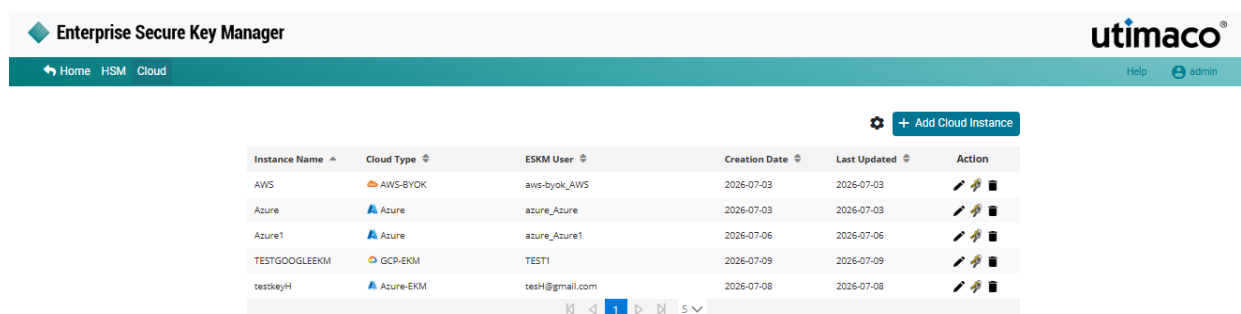
Table 7: Create AWS-BYOK key - parameters

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.



The screenshot displays the 'Enterprise Secure Key Manager' web application. The header includes the 'utimaco' logo and navigation links for 'Home', 'HSM', and 'Cloud'. A '+ Add Cloud Instance' button is visible in the top right. The main content area features a table with the following columns: Instance Name, Cloud Type, ESKM User, Creation Date, Last Updated, and Action. The table lists five instances: AWS, Azure, Azure1, TESTGOOGLEKIM, and testkeyH, each with its respective cloud type (AWS-BYOK, Azure, or GCP-EKM), user, and dates. The 'Action' column contains icons for editing, deleting, and other operations. A pagination bar at the bottom shows '1' of 5 items.

Instance Name	Cloud Type	ESKM User	Creation Date	Last Updated	Action
AWS	AWS-BYOK	aws-byok_AWS	2026-07-03	2026-07-03	[Edit] [Delete] [Info]
Azure	Azure	azure_Azure	2026-07-03	2026-07-03	[Edit] [Delete] [Info]
Azure1	Azure	azure_Azure1	2026-07-06	2026-07-06	[Edit] [Delete] [Info]
TESTGOOGLEKIM	GCP-EKM	TEST1	2026-07-09	2026-07-09	[Edit] [Delete] [Info]
testkeyH	Azure-EKM	testH@gmail.com	2026-07-08	2026-07-08	[Edit] [Delete] [Info]

Figure 24 : Manage keys

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

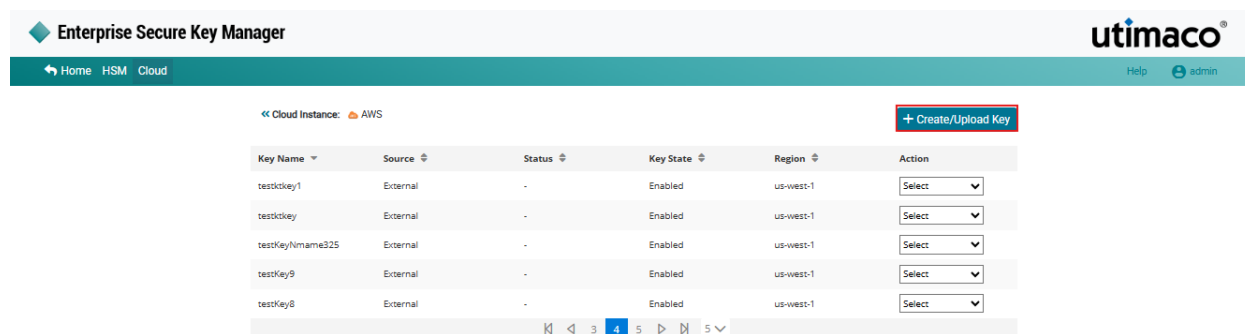


Figure 25 : Create/Upload key

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

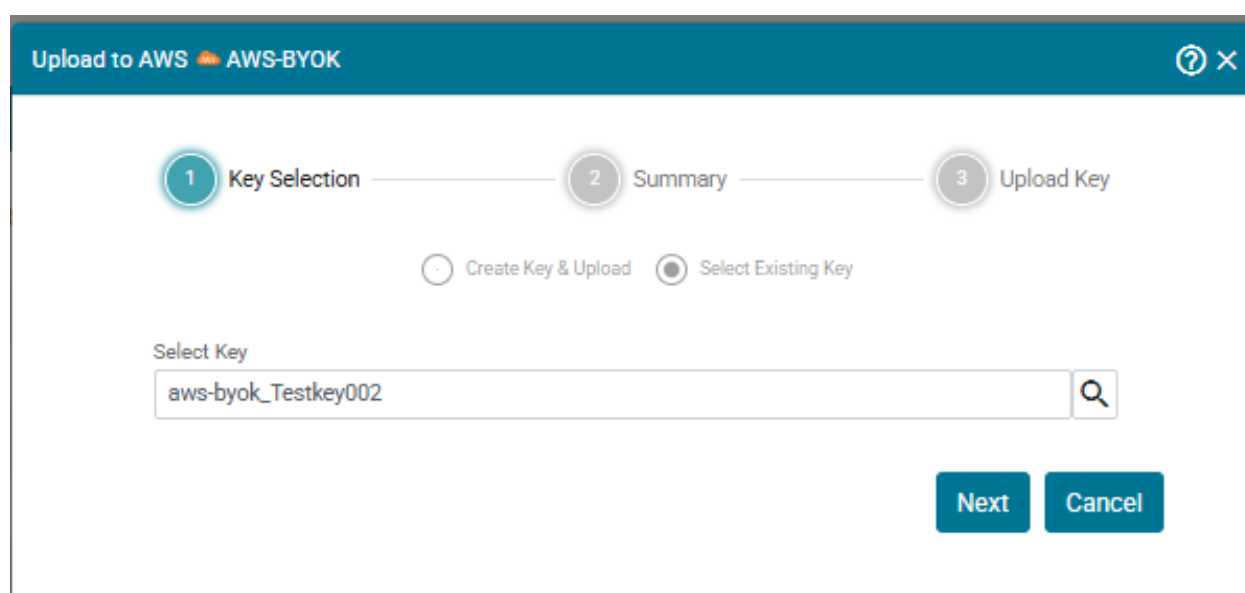


Figure 26 : Select Existing Key

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

The screenshot shows a dialog box titled "Upload to AWS" with a sub-header "AWS-BYOK". The dialog contains a progress bar with three steps: "Key Selection", "2 Summary", and "3 Upload Key". The "Summary" step is currently active and highlighted. Below the progress bar, the following information is displayed:

ESKM Key Name	aws-byok_Testkey002
ESKM Key Owner	aws-byok_AWS
Algorithm	AES-256

At the bottom right of the dialog, there are two buttons: "Next" and "Close".

Figure 27 : Upload to instance AWS-BYOK Summary

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

Key Selection

Summary

3 Upload Key

ESKM Key Name

aws-byok_Testkey002

*Cloud Key Name

Testkey002

Description

Key State

Enabled

Multi-Region

☐

*Region

US West (Oregon)

*Key Users

*Key Administrators

Expiration Date

05/27/2027 08:00 PM

Expiration Date Timezone

Asia/Calcutta (+05:30)

Tags

Key	Value

Auto Rotation

☒ Enable Auto Rotation

Rotation Interval (Days)

30

Upload

Cancel

Figure 28 : Upload key



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



Uploading an existing key will fail if the key already exists in the target AWS instance. Keys that are not already present in the instance can be uploaded successfully. If a newer key version is available in ESKM and has not yet been uploaded, that version can be uploaded to the instance.

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 one, select **Upload** from the drop-down.

<< Cloud Instance: AWS + Create/Upload Key

Key Name ▾	Source ⚙	Status ⚙	Key State ⚙	Region ⚙	Action
345	External	-	Disabled	us-west-1	Select ▾
123Key1	External	-	PendingImport	us-west-1	Select ▾
-	aws-byok_Key1(ESKM)	Not Uploaded			Select ▾
-	aws-byok_Testkey1(ESKM)	Not Uploaded			Select ▾
-	aws-byok_Testkey002(ESKM)	Not Uploaded			Select ▾
-	aws-byok_Testkey003(ESKM)	Not Uploaded			Select ▾
	External	-	PendingImport	us-west-1	Select
	External	-	PendingImport	us-west-1	Delete
	External	-	PendingImport	us-west-1	Upload
					New Version

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**.

ESKM Key Name	
aws-byok_Testkey003	
*Cloud Key Name	
Testkey003	
Description	
Key State	
Enabled	
Multi-Region ☐	
*Region	
US West (N. California)	
*Key Users	
*Key Administrators	
Expiration Date	
04/14/2027 04:36 PM	
Expiration Date Timezone	
Asia/Calcutta (+05:30)	
Tags	
Key	Value
Auto Rotation	
☒ Enable Auto Rotation	
Rotation Interval (Days)	
30	

Upload

Cancel

Figure 30 : Upload



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

5.1.8 Editing AWS-BYOK Key

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

The screenshot shows the 'Enterprise Secure Key Manager' interface. At the top, there's a header with the utimaco logo and navigation links: Home, HSM, Cloud, Help, and admin. Below the header, there's a section for 'Cloud Instance: AWS' with a '+ Create/Upload Key' button. The main area contains a table with columns: Key Name, Source, Status, Key State, Region, and Action. The table lists several keys, including 'testkey1', 'testkey03', 'Testkey004', 'Testkey002', and 'Testkey001'. The 'Testkey001' row is highlighted, and its 'Action' dropdown menu is open, showing options: Select, Edit, Delete, Upload, and New Version. The 'Edit' option is highlighted.

Key Name	Source	Status	Key State	Region	Action
testkey1	External	-	Enabled	us-west-1	Select
testkey03	External	-	Pendingimport	us-west-1	Select
Testkey004	aws-byok_Testkey004(ESKM)	Uploaded	Enabled	us-west-1	Select
Testkey002	External	-	Pendingimport	us-west-1	Select
Testkey001	aws-byok_Testkey001(ESKM)	Uploaded	Enabled	us-west-1	Edit

Figure 31 : Edit key

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

Edit key (aws-byok_Testkey004) on  **AWS-BYOK**?x

ESKM Key Name

aws-byok_Testkey004

*Cloud Key Name

Testkey004

Description

Key State

Enabled

*Region

US West (N. California)

*Key Users

*Key Administrators

Tags

Key

Value

Auto Rotation

☒ Enable Auto Rotation

Rotation Interval (Days)

30

Save

Cancel

Figure 32 : Editing a key

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



Cloud Instance Key (key name) updated successfully.



When editing an AWS BYOK key, only the **Description**, **Tags**, **Key State** and **Auto Rotation** can be updated. **Auto Rotation** settings can be configured or modified for existing keys as required.

5.1.9 Deleting an AWS-BYOK Key

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

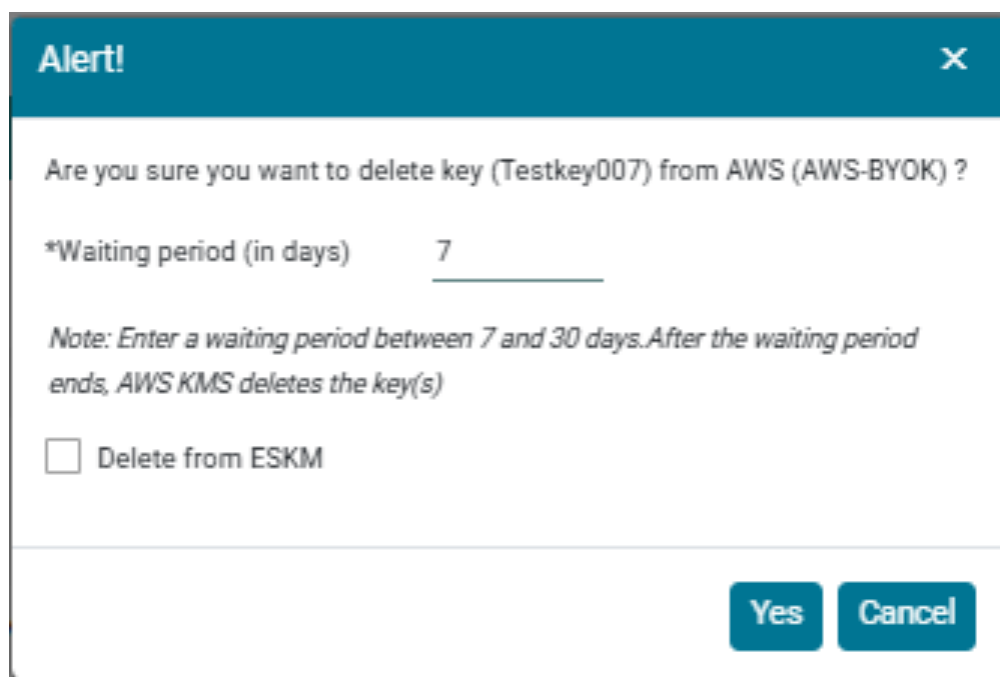
<< Cloud Instance: AWS + Create/Upload Key

Key Name	Source	Status	Key State	Region	Action
testkey1	External	-	Enabled	us-west-1	Select
testkey03	External	-	PendingImport	us-west-1	Select
Testkey007	aws-byok_Testkey007(ESKM)	Uploaded	Enabled	us-west-1	Select
Testkey005	External	-	PendingImport	us-west-1	Select
Testkey004	aws-byok_Testkey004(ESKM)	Uploaded	Enabled	us-west-1	Edit Delete Upload New Version

Navigation: < > 7 8 9 > 5

Figure 33 : Deleting a key

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



The image shows a modal dialog box titled "Alert!" with a close button (X) in the top right corner. The main text asks: "Are you sure you want to delete key (Testkey007) from AWS (AWS-BYOK) ?". Below this is a label "*Waiting period (in days)" followed by a text input field containing the number "7". A note in italics states: "Note: Enter a waiting period between 7 and 30 days. After the waiting period ends, AWS KMS deletes the key(s)". There is a checkbox labeled "Delete from ESKM" which is currently unchecked. At the bottom right, there are two buttons: "Yes" and "Cancel".

Figure 34 : Delete key alert



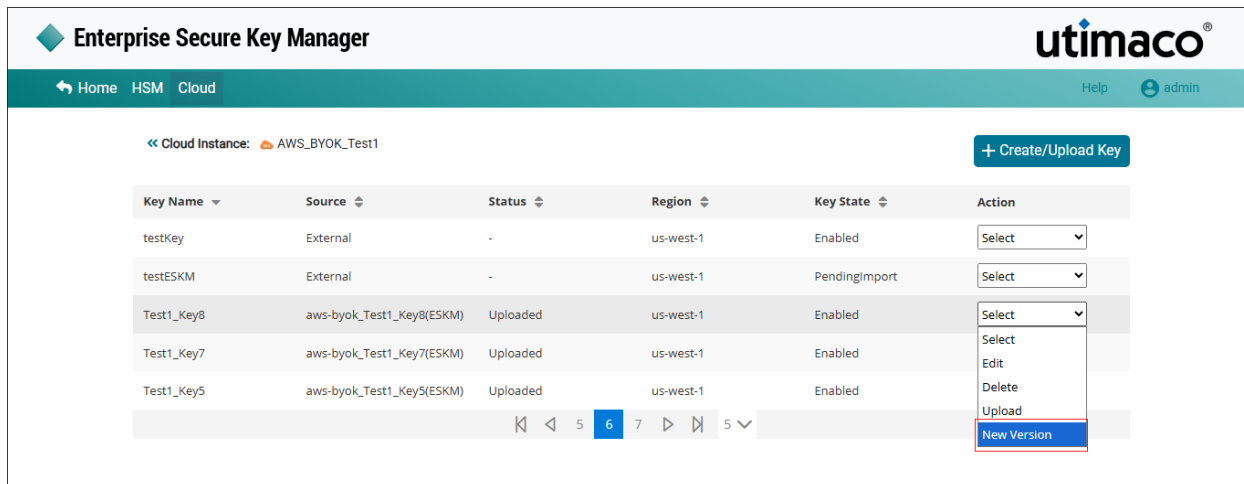
The user can specify a waiting period between 7 and 30 days. After the waiting period has expired, the AWS KMS deletes the key(s). During the waiting period, the key status is shown as **Pending delete**.

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



Enterprise Secure Key Manager

Home HSM Cloud Help admin

Cloud Instance: AWS_BYOK_Test1 + Create/Upload Key

Key Name	Source	Status	Region	Key State	Action
testKey	External	-	us-west-1	Enabled	Select
testESKM	External	-	us-west-1	PendingImport	Select
Test1_Key8	aws-byok_Test1_Key8(ESKM)	Uploaded	us-west-1	Enabled	Select
Test1_Key7	aws-byok_Test1_Key7(ESKM)	Uploaded	us-west-1	Enabled	Select
Test1_Key5	aws-byok_Test1_Key5(ESKM)	Uploaded	us-west-1	Enabled	Edit Delete Upload New Version

Figure 35 : Create new version

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

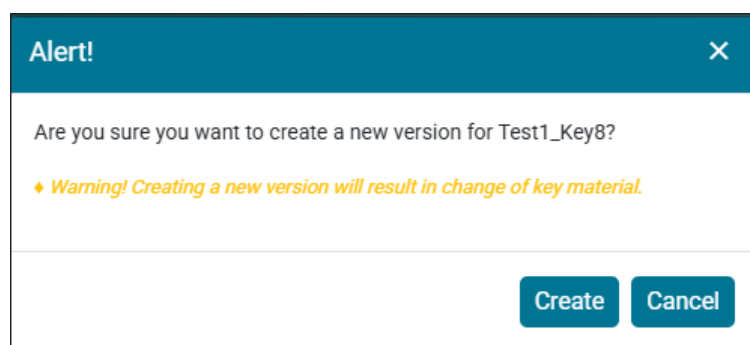


Figure 36 : Alert

- 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 new key version is created and uploaded during version creation. If the key is not uploaded, upload the key version using the **Upload** option under the **Action** column. For detailed steps, 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

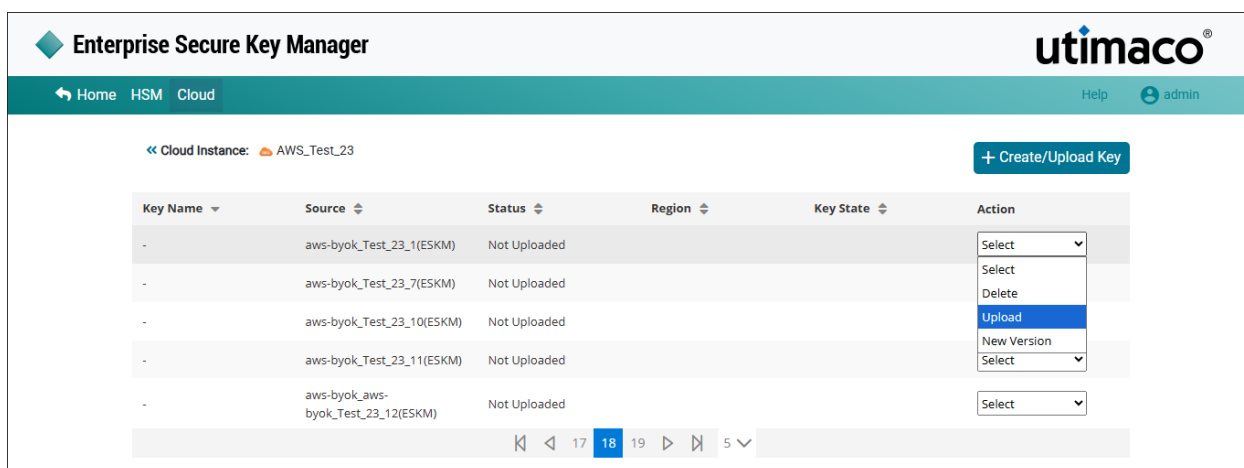
Key Rotation is the process of creating a new version of an encryption key while retaining older key versions for decrypting existing data.

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.

Manual key rotation in AWS BYOK:

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



The screenshot shows the 'Enterprise Secure Key Manager' interface. At the top, there's a navigation bar with 'Home', 'HSM', and 'Cloud' tabs. Below this, a breadcrumb trail shows 'Cloud Instance: AWS_Test_23'. A '+ Create/Upload Key' button is visible. The main content is a table with columns: Key Name, Source, Status, Region, Key State, and Action. The table lists five keys, all with a status of 'Not Uploaded'. The 'Action' column for the first key is expanded, showing options: Select, Select, Delete, Upload (highlighted), New Version, and Select. A pagination bar at the bottom shows page 18 of 5.

Key Name	Source	Status	Region	Key State	Action
-	aws-byok_Test_23_1(ESKM)	Not Uploaded			Select
-	aws-byok_Test_23_7(ESKM)	Not Uploaded			Select
-	aws-byok_Test_23_10(ESKM)	Not Uploaded			Delete
-	aws-byok_Test_23_11(ESKM)	Not Uploaded			Upload
-	aws-byok_Test_23_12(ESKM)	Not Uploaded			New Version
-	aws-byok_aws-byok_Test_23_12(ESKM)	Not Uploaded			Select

Figure 37 : Upload

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

Key material and rotations [Info](#)

[Import new key material](#)[Rotate now](#)

Manage imported key material and initiate on-demand key rotations.

On-demand key rotation

Immediately rotate the key material for this key using Rotate now. You can initiate on-demand key rotation a maximum of 25 times.

Number of on-demand rotations remaining
24 rotations available

Key materials (2)

The following list provides a record of all imported key material associated with this key and each key material's rotation status.

Key material ID	Key materia...	Import state	Description	Rotation ...	Expires at	Actions
d0cd27d45b7...	✓ Current	✓ Imported	-	Mar 24, 202...	Key material...	⋮
fba97aeca938...	✓ Non curren t	✓ Imported	-	-	Key material...	⋮

Figure 38 : Key Rotation - AWS-BYOK

For detailed steps, see [Upload Key from ESKM to AWS-BYOK](#).

5.1.11.1 Auto-Key Rotation

Automatic Key Rotation enables scheduled creation of new key versions without manual intervention. Based on the configured rotation policy, ESKM automatically generates a new version of the selected key and uploads it to AWS Key Management Service. Older key versions are retained and continue to be available for decrypting previously encrypted data.

ESKM Key Name

aws-byok_Testkey003

*Cloud Key Name

Testkey003

Description

Key State

Enabled

▼

Multi-Region

☐

*Region

US West (N. California)

▼

+

+

*Key Users

▼

+

+

*Key Administrators

▼

+

+

Expiration Date

04/14/2027 04:36 PM

📅

Expiration Date Timezone

Asia/Calcutta (+05:30)

▼

Tags

Key	Value
-----	-------

+

Auto Rotation

☒ Enable Auto Rotation

Rotation Interval (Days)

30

Upload

Cancel

Figure 39 : Auto Rotation



Automatic Rotation can be configured during key creation or enabled later by editing an existing key. Administrators can modify the rotation settings by enabling/disabling **Auto Rotation** for the desired key.

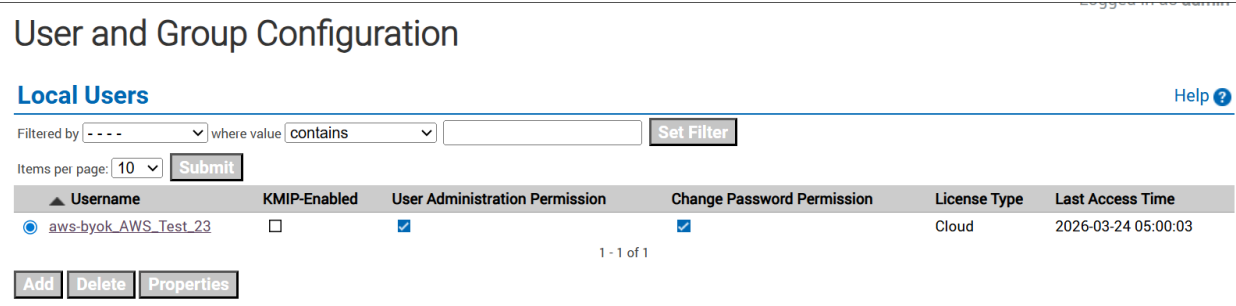
5.2 Configuration on AWS-BYOK

For more information on configuration on AWS-BYOK, see [Manage access keys for IAM users](#).

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.



User and Group Configuration

Local Users [Help ?](#)

Filtered by: --- where value: contains [Set Filter](#)

Items per page: 10 [Submit](#)

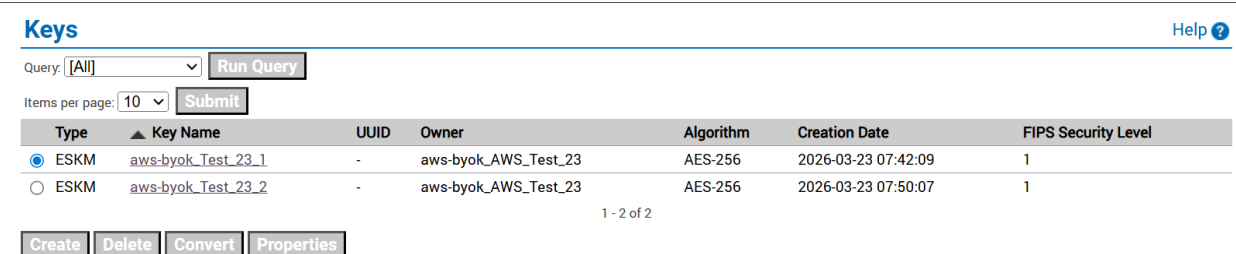
Username	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
☒ aws-byok_AWS_Test_23	☐	☒	☒	Cloud	2026-03-24 05:00:03

1 - 1 of 1

[Add](#) [Delete](#) [Properties](#)

Figure 40 : Local Users

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



Keys [Help ?](#)

Query: [All] [Run Query](#)

Items per page: 10 [Submit](#)

Type	Key Name	UUID	Owner	Algorithm	Creation Date	FIPS Security Level
☒ ESKM	aws-byok_Test_23_1	-	aws-byok_AWS_Test_23	AES-256	2026-03-23 07:42:09	1
☐ ESKM	aws-byok_Test_23_2	-	aws-byok_AWS_Test_23	AES-256	2026-03-23 07:50:07	1

1 - 2 of 2

[Create](#) [Delete](#) [Convert](#) [Properties](#)

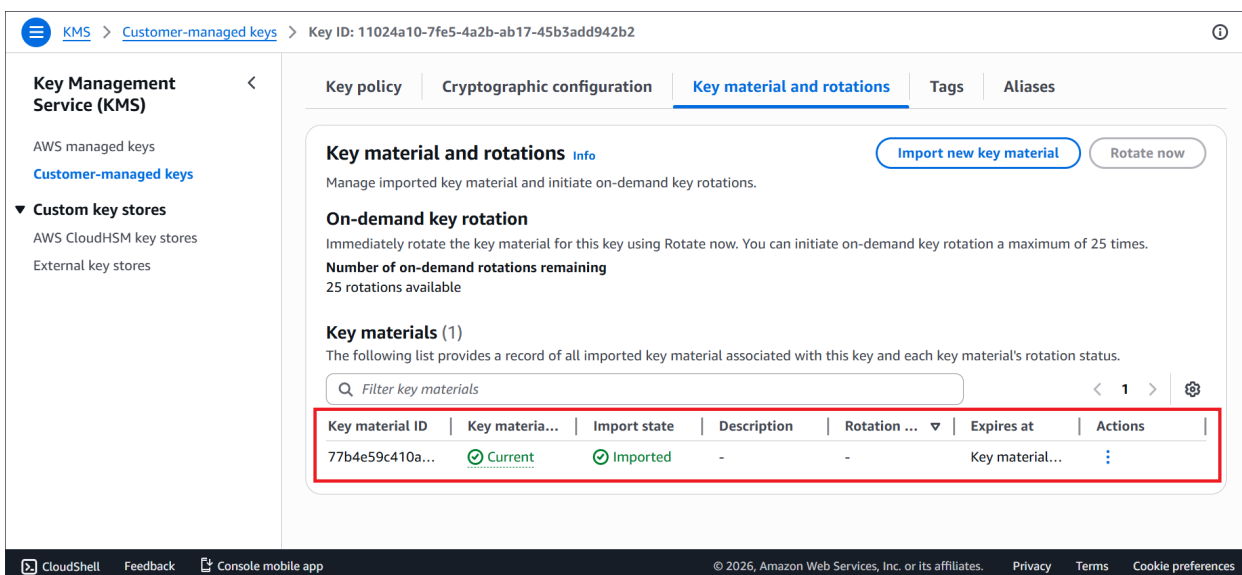
Figure 41 : Keys

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.

Key Versions and Available Usage				Help ?
Items per page: 10 Submit				
Version	Key State	Creation Date	Default IV	
☒ 5 [Default]	Active	2026-03-23 10:03:08	BF7841A56310F3111EA0D19A5BAD36AA	
☐ 4	Active	2026-03-23 10:02:21	C2E20E772EEE807C629EE71D0F4C799B	
☐ 3	Active	2026-03-23 10:01:01	85769D2B7DC3FCF5D4FAE4B911A173D1	
☐ 2	Active	2026-03-23 10:00:44	5F92B50C01F1493122E62BC9265E17EC	
☐ 1	Active	2026-03-23 07:42:09	6495F650A76D9EE3464DB9C7537CCC04	
1 - 5 of 5				
Create New Version Edit Usage				

Figure 42 : Key Versions and Available Usage

- 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.



Key Management Service (KMS)

Key ID: 11024a10-7fe5-4a2b-ab17-45b3add942b2

Key policy | Cryptographic configuration | **Key material and rotations** | Tags | Aliases

Key material and rotations Info

Manage imported key material and initiate on-demand key rotations.

On-demand key rotation
Immediately rotate the key material for this key using Rotate now. You can initiate on-demand key rotation a maximum of 25 times.

Number of on-demand rotations remaining
25 rotations available

Key materials (1)
The following list provides a record of all imported key material associated with this key and each key material's rotation status.

Filter key materials

Key material ID	Key materia...	Import state	Description	Rotation ...	Expires at	Actions
77b4e59c410a...	Current	Imported	-	-	Key material...	

CloudShell Feedback Console mobile app © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Figure 43 : Key created in AWS-BYOK

- 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.

Key material and rotations [Info](#)

Manage imported key material and initiate on-demand key rotations.

On-demand key rotation

Immediately rotate the key material for this key using Rotate now. You can initiate on-demand key rotation a maximum of 25 times.

Number of on-demand rotations remaining
24 rotations available

Key materials (2)

The following list provides a record of all imported key material associated with this key and each key material's rotation status.

< 1 > ⚙

Key material ID	Key materia...	Import state	Description	Rotation ... ▼	Expires at	Actions
d0cd27d45b7...	✓ Current	✓ Imported	-	Mar 24, 202...	Key material...	⋮
fba97aeca938...	✓ Non curren t	✓ Imported	-	-	Key material...	⋮

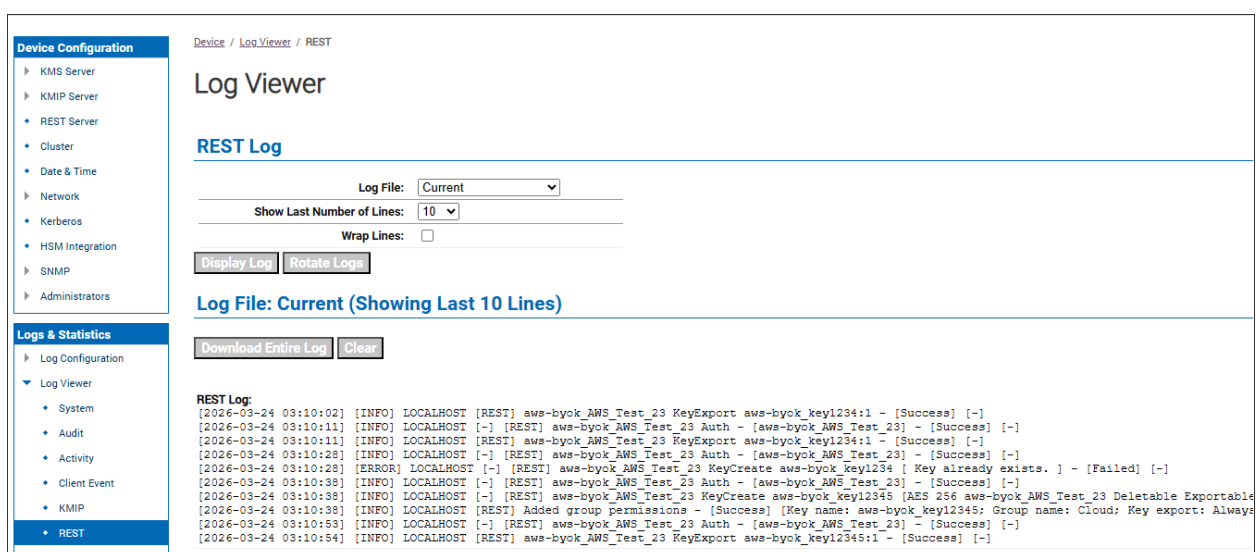
Figure 44 : Key Rotation created in AWS-BYOK

7 Troubleshooting

7.1 Log Locations and Interpretation

Verify the Utimaco ESKM logs by following these steps:

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



The screenshot displays the Utimaco ESKM Management Console interface. On the left, there is a navigation menu with two main sections: 'Device Configuration' and 'Logs & Statistics'. Under 'Device Configuration', options include KMS Server, KMIP Server, REST Server, Cluster, Date & Time, Network, Kerberos, HSM Integration, SNMP, and Administrators. Under 'Logs & Statistics', options include Log Configuration, Log Viewer, System, Audit, Activity, Client Event, KMIP, and REST (which is currently selected).

The main content area is titled 'Log Viewer' and shows the 'REST Log'. It includes a 'Log File' dropdown set to 'Current', a 'Show Last Number of Lines' dropdown set to '10', and a 'Wrap Lines' checkbox. There are buttons for 'Display Log' and 'Rotate Logs'. Below these controls, the log file is named 'Log File: Current (Showing Last 10 Lines)'. At the bottom of the log viewer, there are buttons for 'Download Entire Log' and 'Clear'.

The log entries are as follows:

```

REST Log:
[2026-03-24 03:10:02] [INFO] LOCALHOST [REST] aws-byok_AWS_Test_23 KeyExport aws-byok_key1234:1 - [Success] [-]
[2026-03-24 03:10:11] [INFO] LOCALHOST [-] [REST] aws-byok_AWS_Test_23 Auth - [aws-byok_AWS_Test_23] - [Success] [-]
[2026-03-24 03:10:11] [INFO] LOCALHOST [REST] aws-byok_AWS_Test_23 KeyExport aws-byok_key1234:1 - [Success] [-]
[2026-03-24 03:10:28] [INFO] LOCALHOST [-] [REST] aws-byok_AWS_Test_23 Auth - [aws-byok_AWS_Test_23] - [Success] [-]
[2026-03-24 03:10:28] [ERROR] LOCALHOST [-] [REST] aws-byok_AWS_Test_23 KeyCreate aws-byok_key1234 [ Key already exists. ] - [Failed] [-]
[2026-03-24 03:10:38] [INFO] LOCALHOST [-] [REST] aws-byok_AWS_Test_23 Auth - [aws-byok_AWS_Test_23] - [Success] [-]
[2026-03-24 03:10:38] [INFO] LOCALHOST [-] [REST] aws-byok_AWS_Test_23 KeyCreate aws-byok_key12345 [RES 256 aws-byok_AWS_Test_23 Deletable Exportable] - [Success] [-]
[2026-03-24 03:10:38] [INFO] LOCALHOST [REST] Added group permissions - [Success] [Key name: aws-byok_key12345; Group name: Cloud; Key export: Always]
[2026-03-24 03:10:53] [INFO] LOCALHOST [-] [REST] aws-byok_AWS_Test_23 Auth - [aws-byok_AWS_Test_23] - [Success] [-]
[2026-03-24 03:10:54] [INFO] LOCALHOST [REST] aws-byok_AWS_Test_23 KeyExport aws-byok_key12345:1 - [Success] [-]

```

Figure 45 : 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 Appendix A: 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 8: References

10 Appendix B: 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.

Table 9: Glossary