Microsoft
Azure 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	3.0.0
Date	2026-07-10
Status	PUBLISHED
Document No.	IG-2026-0038

Table of Contents

1 Introduction

The Azure Bring Your Own Key (BYOK) and Utimaco Enterprise Secure Key Manager (ESKM) integration enables customers to generate and manage encryption keys outside Microsoft Azure and securely import them into Azure Key Vault. This integration helps maintain customer control over encryption keys while using Azure services for data protection.

1.1 About This Guide

This document provides information on integrating Azure Bring Your Own Key (BYOK) with Utimaco Enterprise Secure Key Manager (ESKM). It explains the key concepts, prerequisites, and configuration steps required to manage encryption keys outside Azure using ESKM and securely import them into Azure Key Vault for use with Azure services.

1.2 Target Audience

This document is intended for Utimaco ESKM and Azure BYOK administrators.

1.3 Purpose of the Integration

The purpose of the Azure-BYOK and Utimaco ESKM integration is to enable customers to generate and manage encryption keys outside Microsoft Azure while securely using those keys with Azure Key Vault. This integration helps customers retain control over key ownership and lifecycle management while meeting security and compliance requirements for protecting data in Azure.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
Azure	Microsoft Azure
BYOK	Bring Your Own Key

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
Key Vault	Azure Key Vault
API	Application Programming Interface
CMK	Customer-Manager-Key

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	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

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 marks the result expected after the successful execution of an instruction.

2 Product Overview

2.1 Overview of Azure-BYOK

Azure Bring Your Own Key (BYOK) is a capability of Azure Key Vault that allows customers to use encryption keys generated and managed outside Microsoft Azure. Using BYOK, customers can import externally created keys into Azure Key Vault and use them for encrypting Azure resources while retaining ownership and control of the key material.

2.2 Overview of Utimaco ESKM

Utimaco Enterprise Secure Key Manager (ESKM) is a centralized key management solution used to generate, store, and manage encryption keys in the customer environment. It provides secure control over key lifecycle operations such as key creation, usage, rotation, and deletion, helping organizations maintain strong security governance and compliance.

2.3 Joint Value Proposition

The Azure BYOK and Utimaco ESKM integration enables organizations to keep full ownership and control of encryption keys while protecting data in Azure. By managing keys in ESKM outside Azure, customers strengthen security governance and meet compliance requirements, while still using Azure Key Vault for cloud encryption operations.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Azure Version	Utimaco ESKM
Azure BYOK	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.
- ESKM must have internet connectivity.
- 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**).
- Microsoft Azure Key Vault, Client ID, Tenant ID and Secret ID are required to integrate Utimaco ESKM keys with Microsoft Azure Cloud Service Provider. Ensure that the Key Vault and its credentials are created in Microsoft Azure portal and keep them readily available.

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.

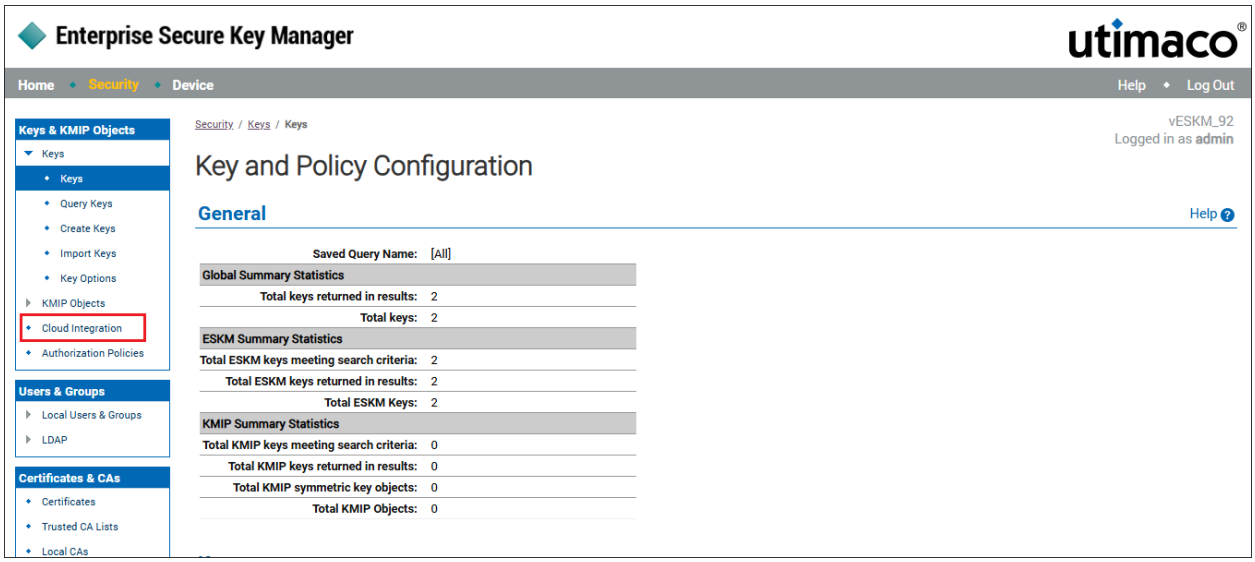

Figure 1 : Cloud integration

- The **Cloud Integration Web Console** is opened in a new browser window and auto logged in to the cloud ESKM.

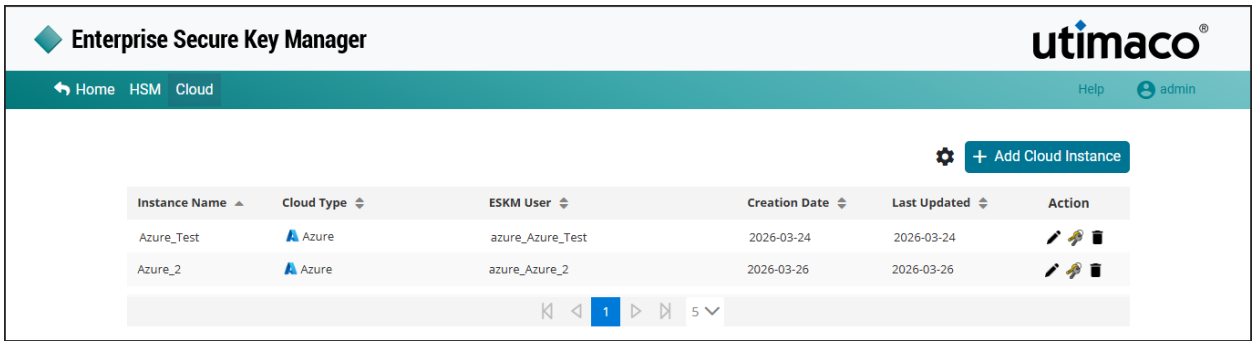

Figure 2 : Cloud integration dashboard

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

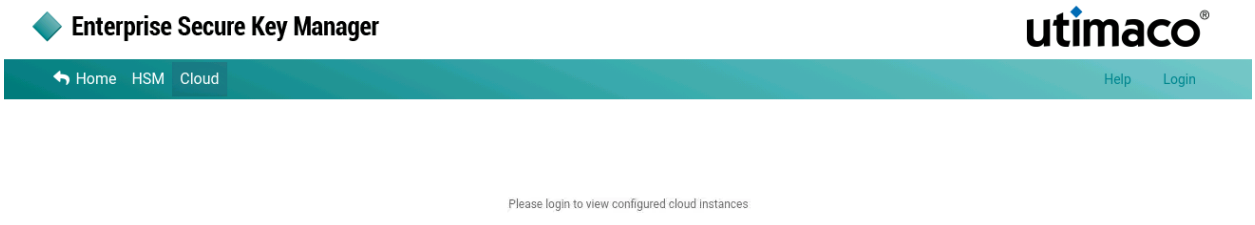

Figure 3 : Cloud integration login

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

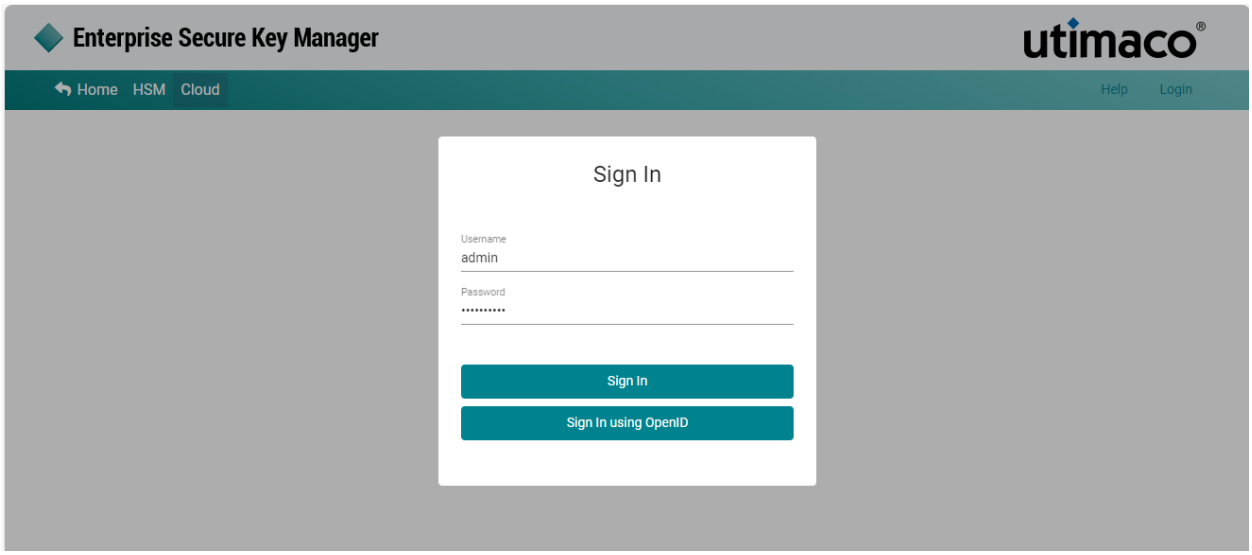

Figure 4 : Cloud integration sign in

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

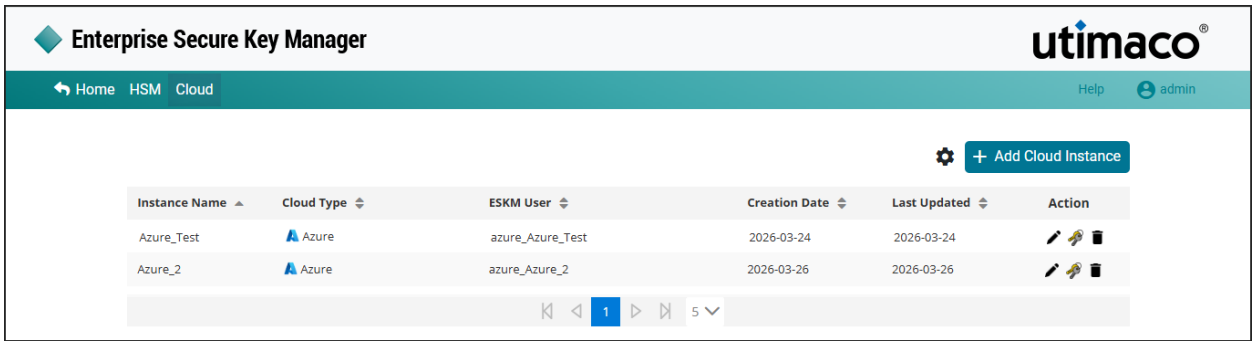

Figure 5 : Cloud ESKM logged in page

- 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, the OpenID server must be configured in ESKM and OpenID administrator accounts must be created 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 **User Name** and **Password** and click on **Sign In using OpenID.** (OR) Click **Sign In using OpenID** without user credentials.

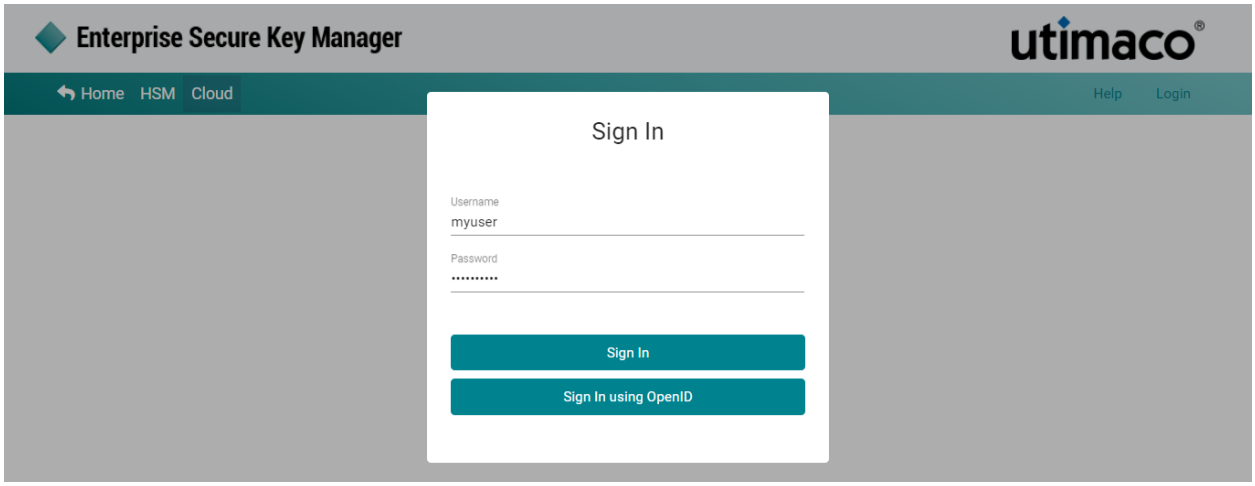

Figure 6 : Sign in using OpenID

- Enter **User Name** and **Password**. Click **Sign In** or **Sign In using OpenID**.
- The **Cloud Integration Dashboard** is displayed.
- Log out of the **Cloud Integration Web Console** at any time using the **Logout** link in the upper right corner.

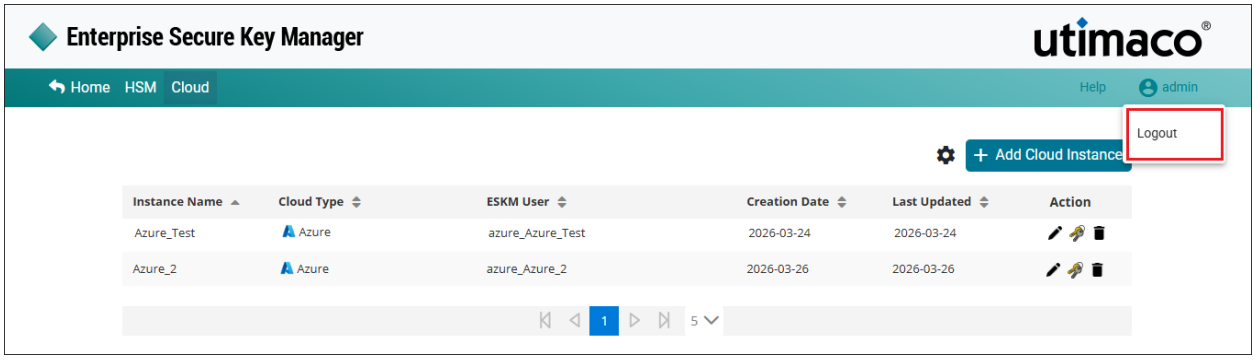

Figure 7 : Logout

- 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.

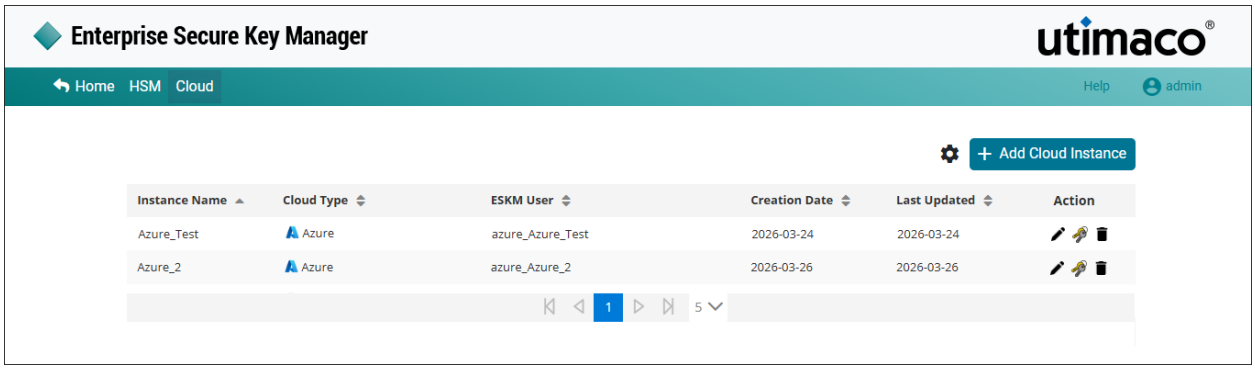

Figure 8 : Cloud integration dashboard

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 cloud settings

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

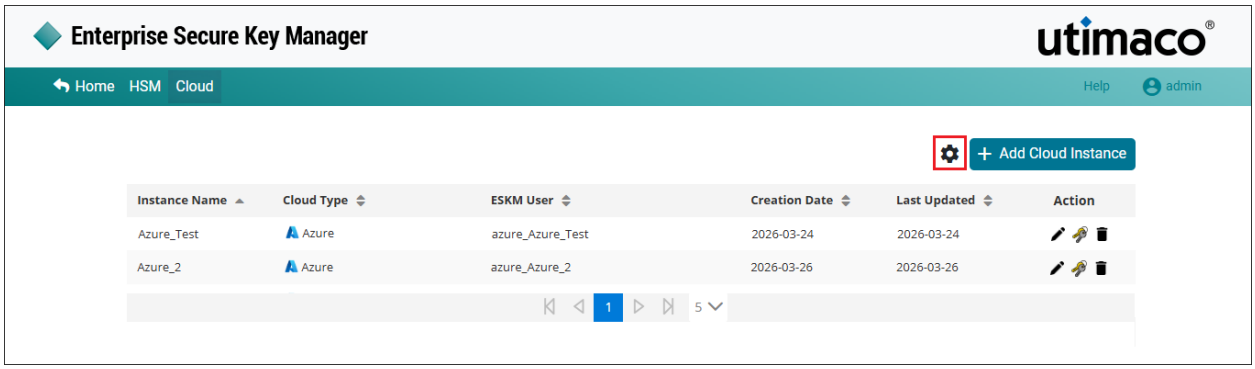

Figure 9 : Cloud settings

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

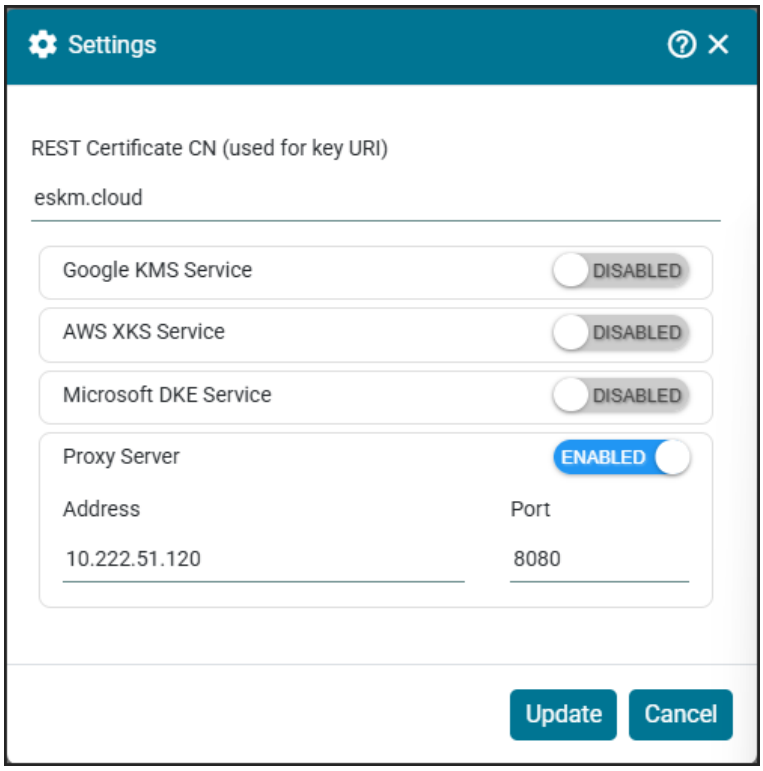

Figure 10 : Update settings

- Enable the **Proxy Server**, enter the proxy **Address** and **Port**, and then click **Update**.

4.3 Setting Up Azure-BYOK

- Go to *Microsoft Azure*.
- Sign in using your **Microsoft (Azure AD) administrator account**.
- In the Azure portal, search for **Key Vaults**.
- Click **Create**.

For more information on setting up Azure-BYOK, refer to *Create an Azure Key Vault with the Azure portal*.

5 Integration Steps

5.1 Configuration on Azure-BYOK

The Microsoft Azure BYOK helps the user to use the ESKM to generate keys and import them into Microsoft Azure Key Vault. It allows the user to encrypt various kinds of keys, secrets and certificates. Before uploading a keys from Utimaco ESKM to the cloud, make sure that the key vault and its credentials are created in the Microsoft Azure portal. Following are the steps to be followed to create the Microsoft Azure Key Vault and authorize Utimaco ESKM to upload the keys to the Microsoft Azure Key Vault.

- Create a Key Vault
- Register an Application
- Create a Secret Key
- Access Policy

5.1.1 Create a Key Vault

Microsoft Azure Key Vault is a managed secret solution within the Microsoft Azure Cloud that offers authentication and authorization for ESKM keys in the Microsoft Azure Key Vault for BYOK protection. Follow the instructions below to create a Key Vault.

To create a key vault:

- Sign in to the Microsoft Azure portal at *Microsoft Azure*.
- In the Microsoft Azure portal **Home** page, select **Create a resource** on the left.
- In the search box, enter **Key Vault** and select **Key Vault**.
- In the **Key Vault** section, choose **Create**.

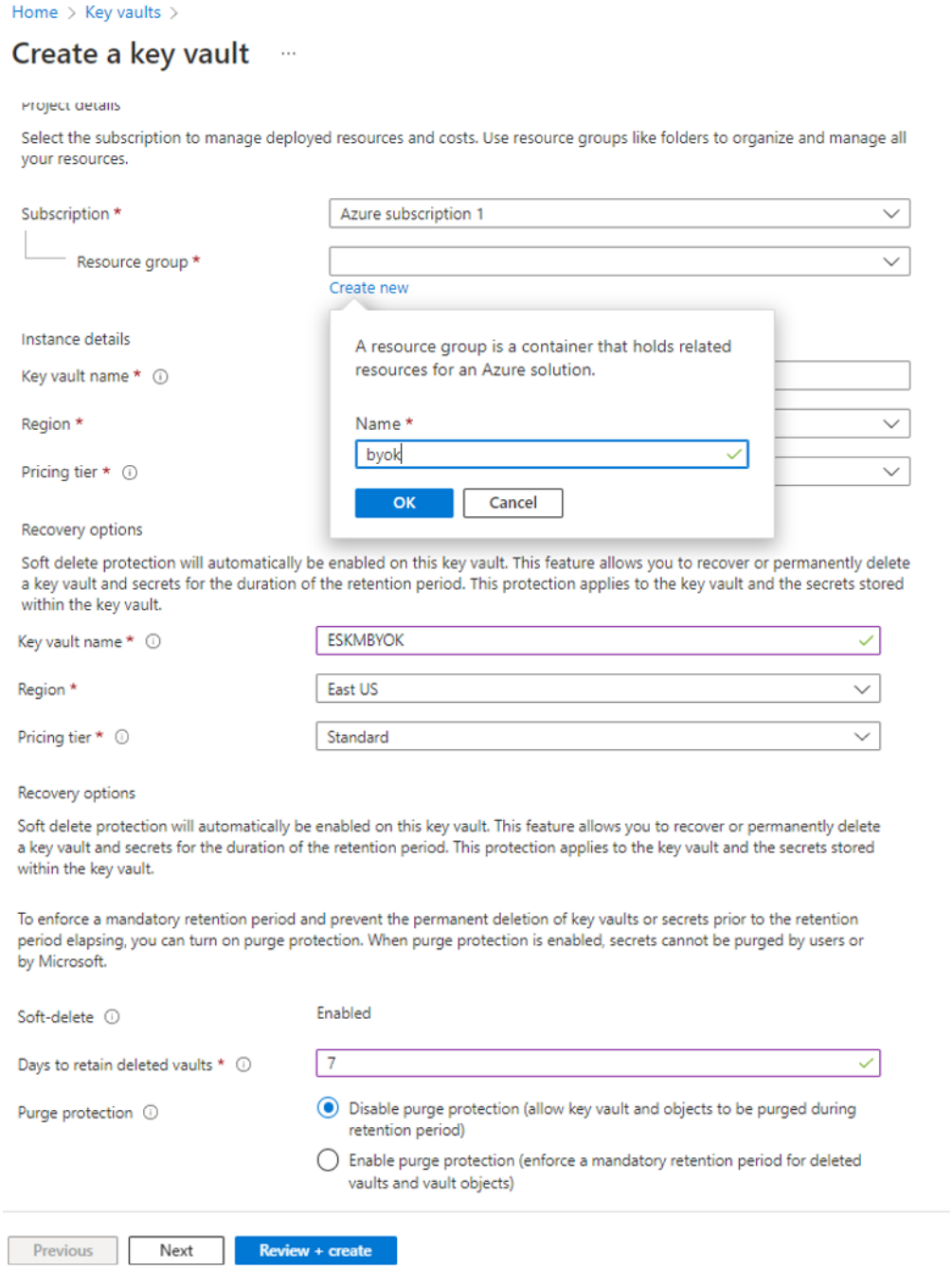

Figure 11 : Go to create a Key Vault

- In the **Create a key vault** section, provide the necessary information and click **Review + Create**.

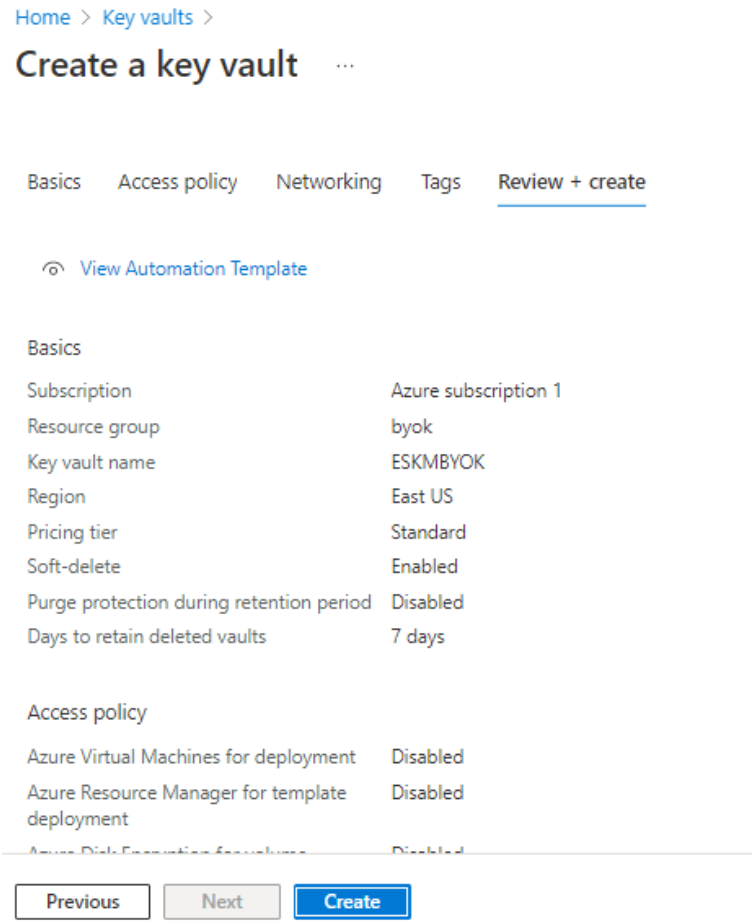

Figure 12 : Review and Create

- Review the information provided and click **Create**.

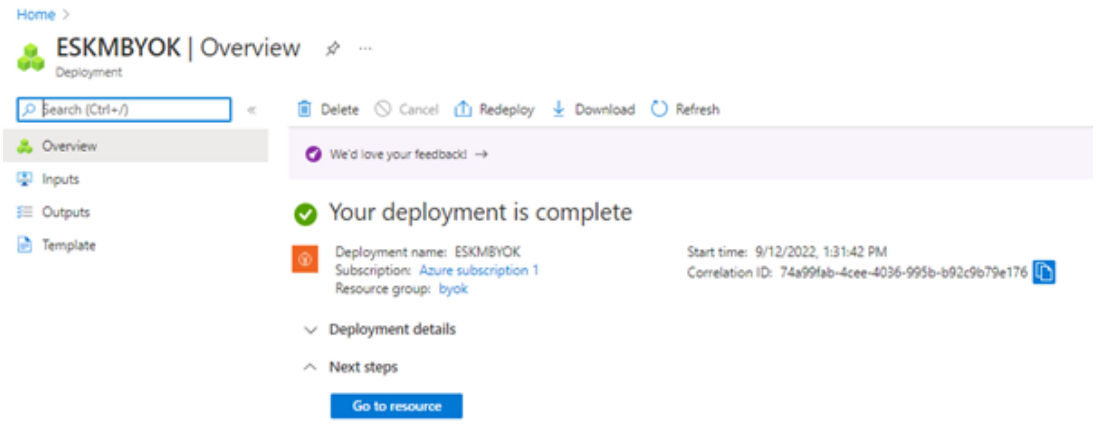

Figure 13 : Deployment is complete

5.1.2 Register an Application

After logging into the Microsoft Azure Portal, navigate to Microsoft Azure AD and **App registrations**. Click on **New Registration** to start the process of creating the application and you will be presented with a few options to be filled out based on how the application works.

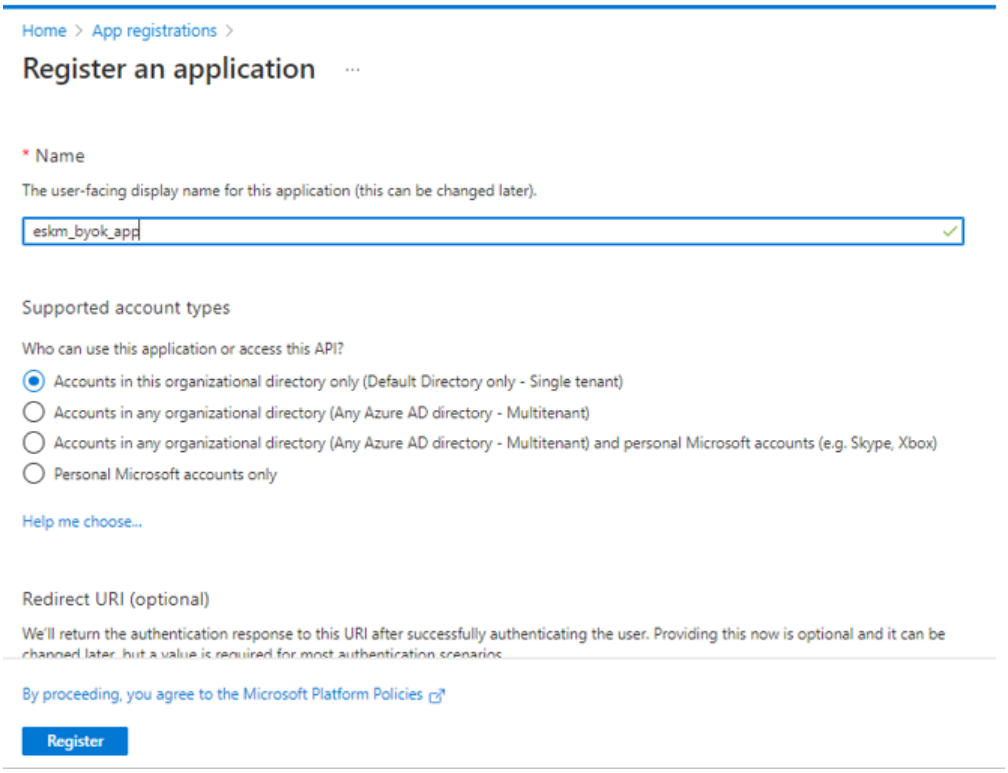

Figure 14 : Register an application

Click **Register**. Your application has been created successfully and you can see the details.

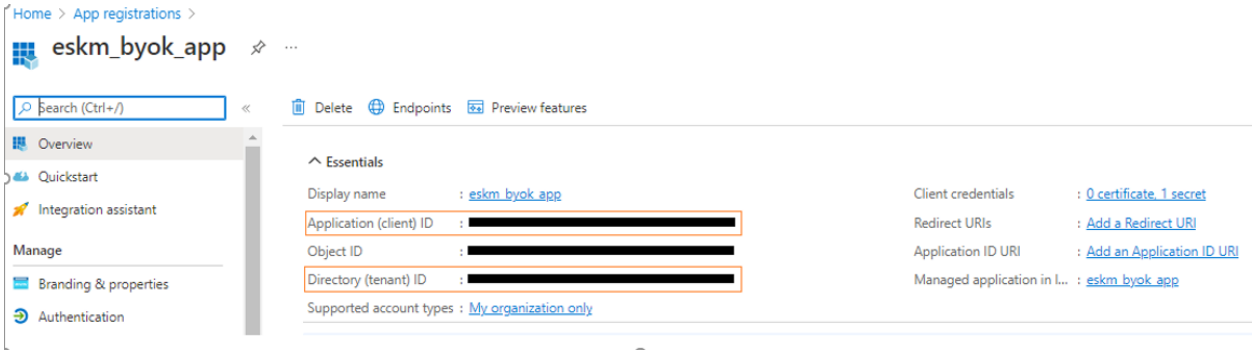

Figure 15 : Application created

When the application is created, the Tenant ID(Directory ID) and Client ID(Application ID) are generated.

Once the application is registered, copy the Tenant ID and Client ID to configure the Utimaco ESKM with Microsoft Azure Key Vault.

5.1.3 Create a Secret Key

In the application page, go to **Certificate & secrets** as seen in the screenshot below.

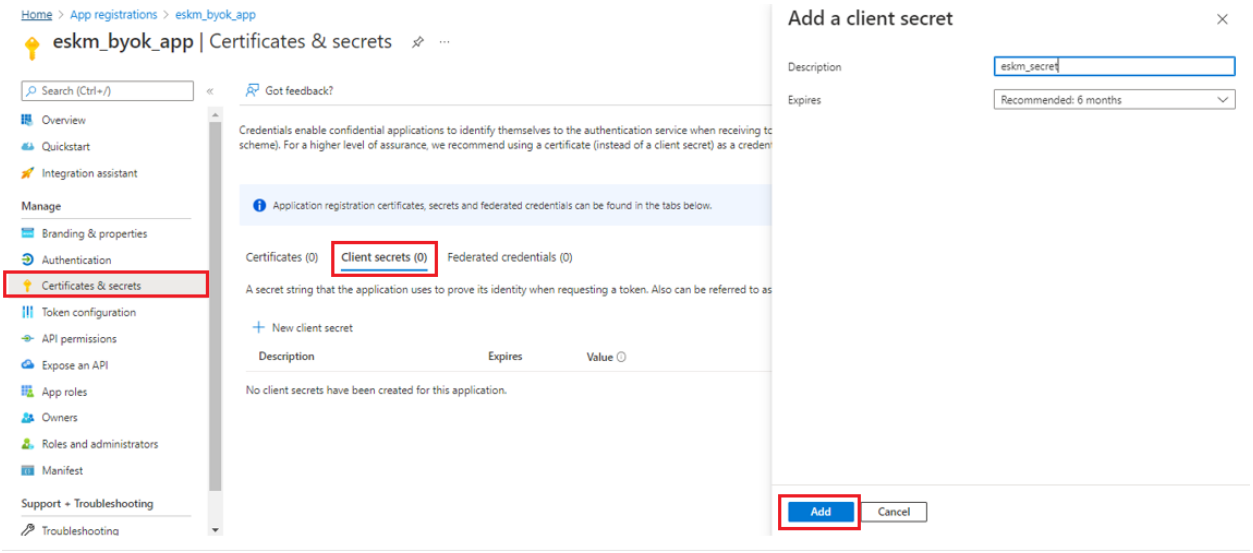

Figure 16 : Add a client secret

Enter the required information and click **Add**.

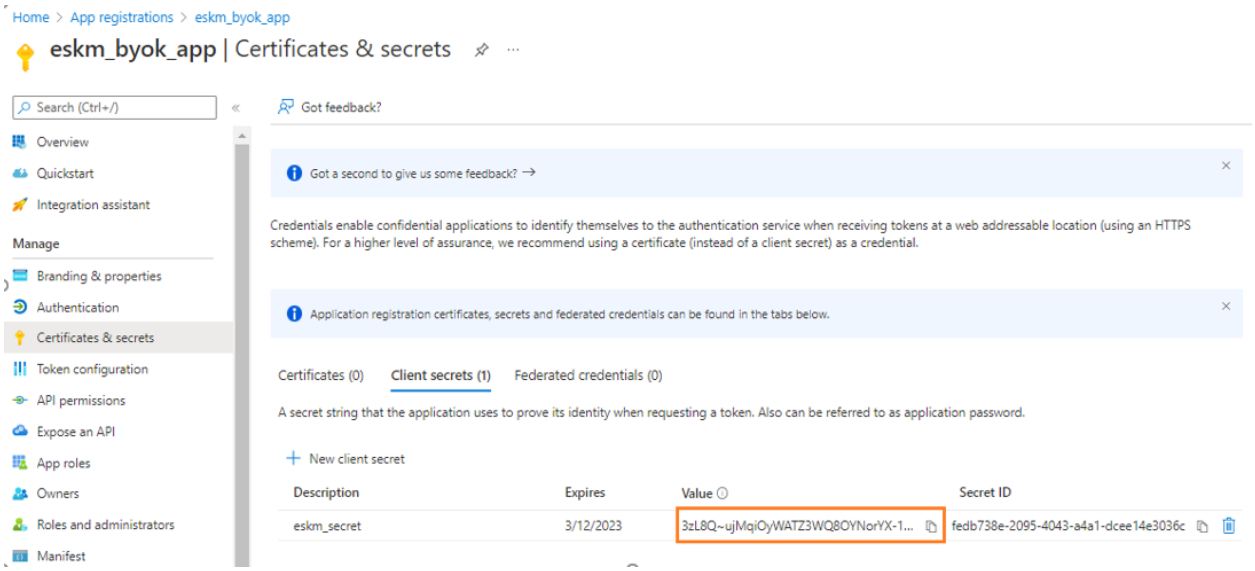

Figure 17 : Secret ID

Secret ID created successfully.

Before leaving the page, ensure that the Secret ID has been copied and saved. After leaving the page, the Secret ID is no longer accessible.

5.1.4 Access Policy

A Key Vault access policy allows a security principal, such as a user, application, or user group, to perform various operations on Key Vault secrets, keys, and certificates. User can assign access policies using Microsoft Azure portal.

- In the **Microsoft Azure Portal**, Navigate to the **Key Vault Resource**.
- Under **Settings**, select **Access Configuration** > **Access Policies** > **Create**.

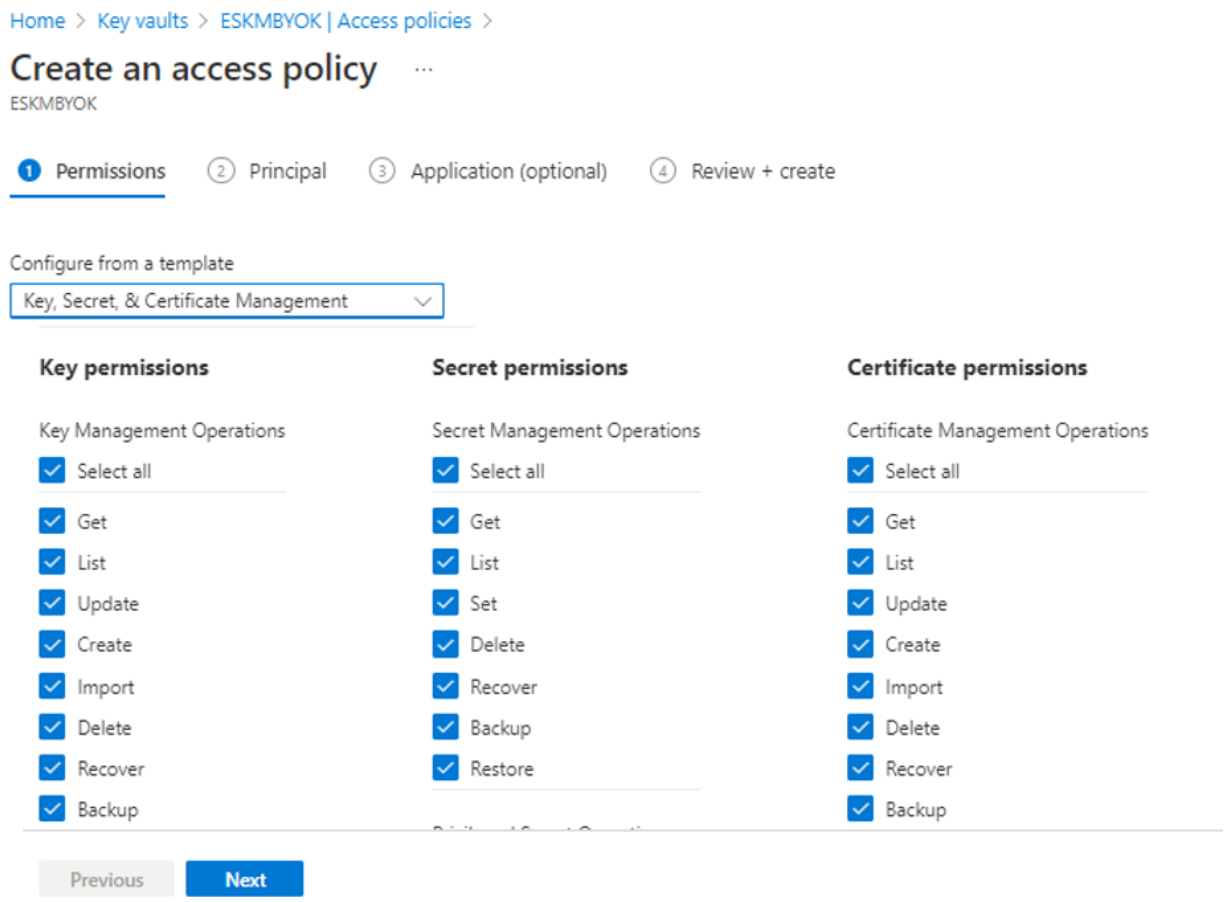

Figure 18 : Create an access policy

Select the permissions you want under **Certificate permissions**, **Key permissions**, and **Secret permissions**. You can also select the template from the drop-down that contains common permissions. Click **Next**.

Under the **Principal** tab, search for the user from the Active Directory to provide access to the key vault as a Manager. Click **Next**.

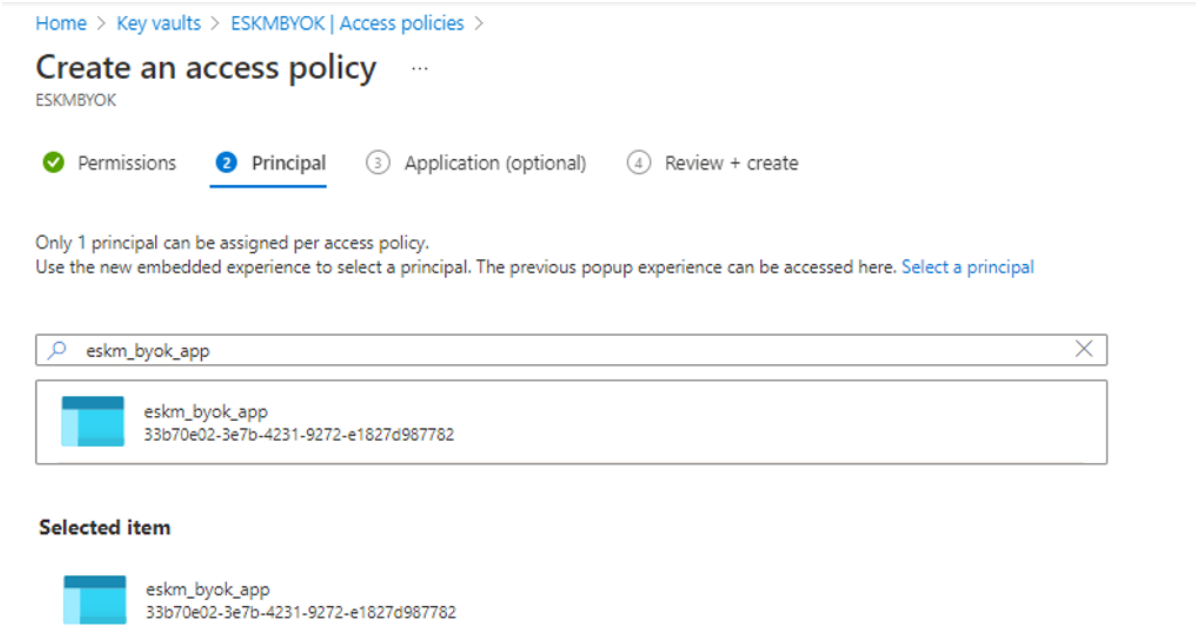

Figure 19 : Principal

Under **Application (optional)** tab, search for and select the name of the app to provide the access at the application level grants. With your application identity, you can let your application connect to the vault. Click **Next**.

You will be navigated to the **Review Summary** and click **Create.**

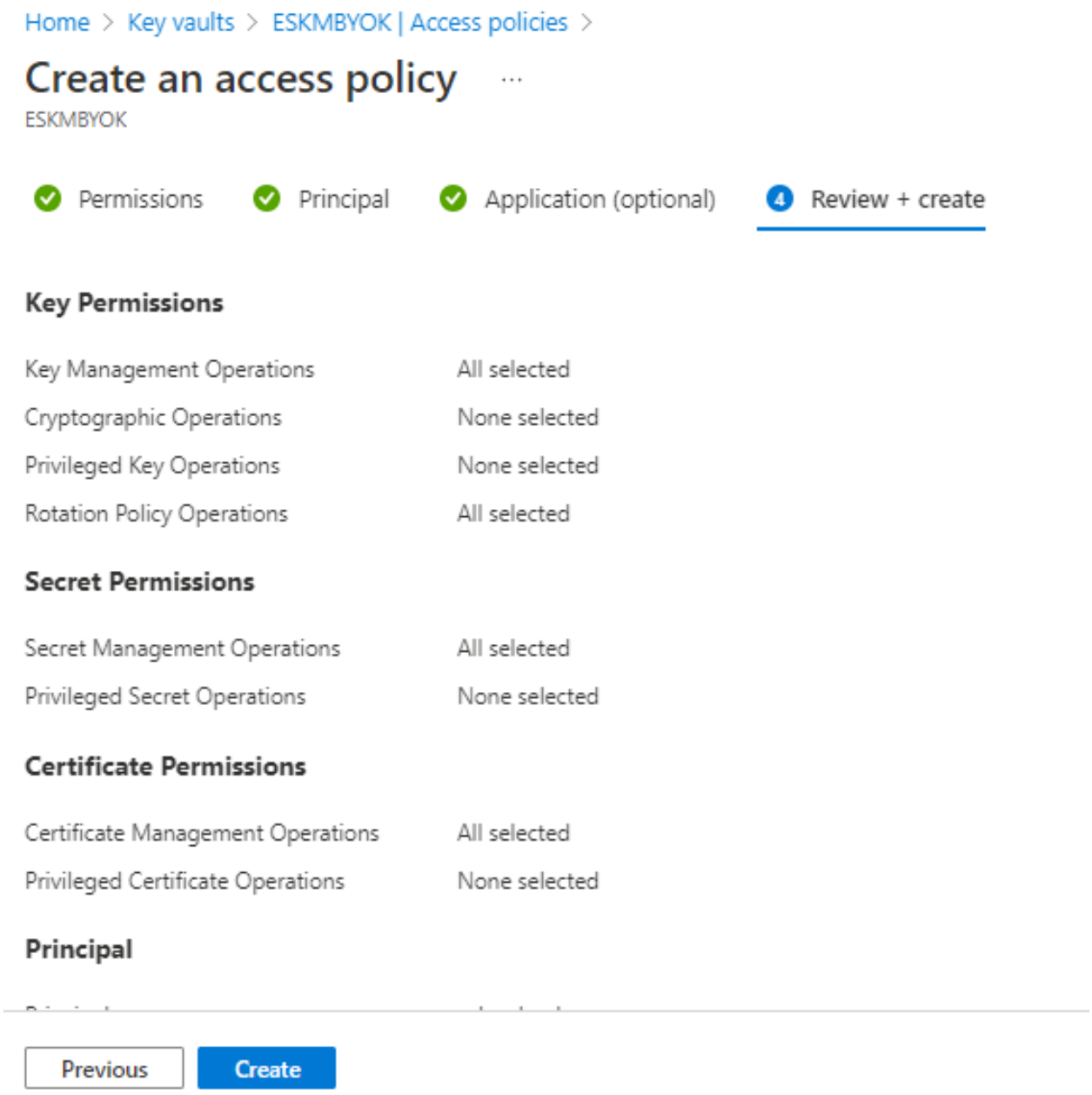

Figure 20 : Review and create

5.2 Configuration on Utimaco ESKM

5.2.1 Adding a New Cloud Instance

This section describes the procedure of adding a new cloud instance.

To add a new cloud instance

- Log in to the Cloud Integration Web Console using any one of the methods described in the *Accessing the Cloud Integration Web Console* chapter of *ESKM_Installation and Replacement_Guide_8.54.0*.
- Click on the "+ **Add Cloud Instance**" button in the top right corner of the page.

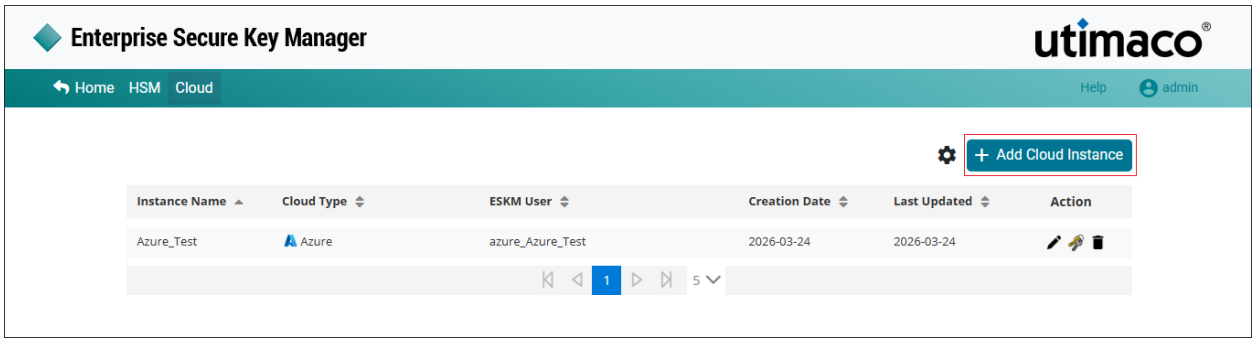

Figure 21 : Add new cloud instance

- The **Add Cloud Instance** pop-up window will appear.

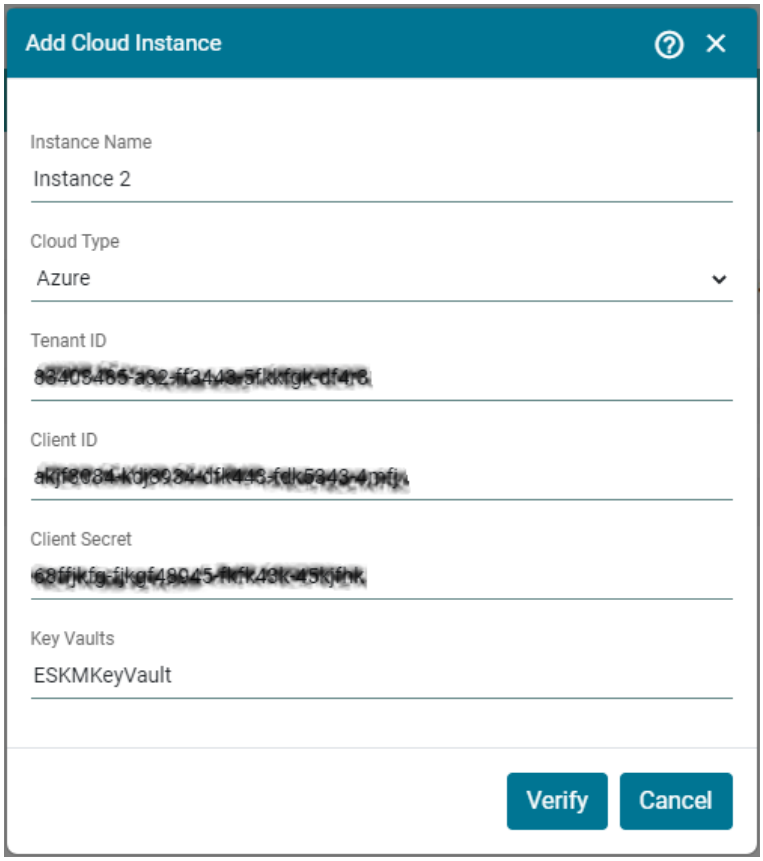

Figure 22 : Verify cloud instance

- Enter the **Instance Name** and select **Cloud Type**. On selection of cloud type, respective configuration fields will be loaded. In case of Microsoft Azure cloud type, enter values for **Tenant ID**, **Client ID**, **Client Secret** and **Key Vaults**. Click **Verify**.

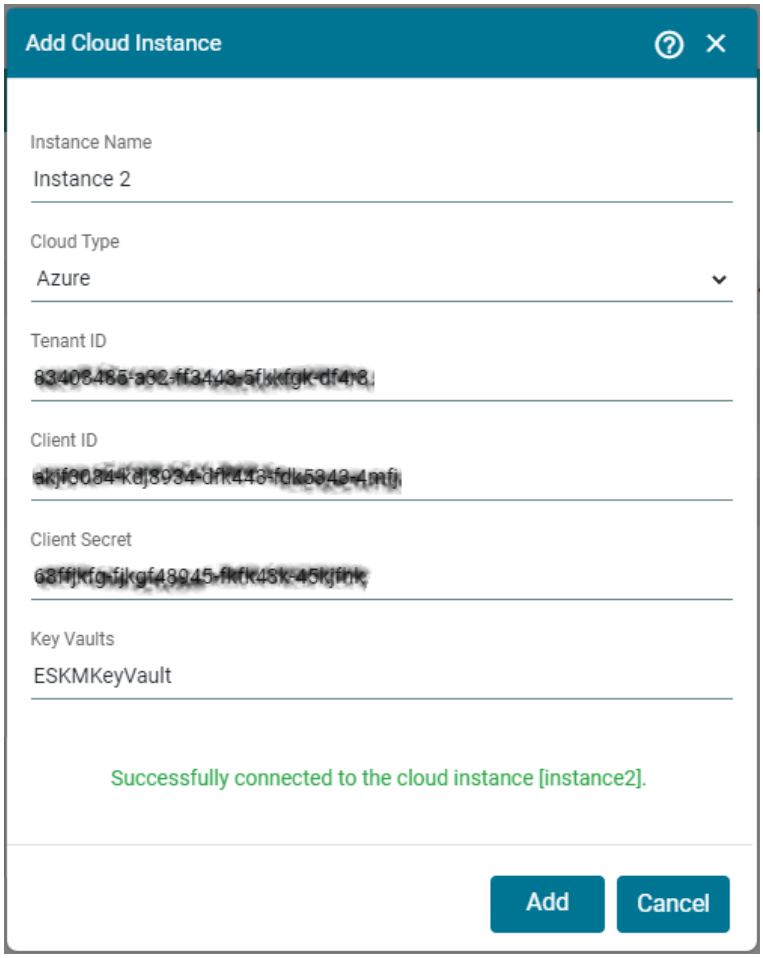

Figure 23 : Azure cloud instance

When an instance is verified without an internet connection, the error message "**Invalid key vault name or failed to connect with the cloud instance"** is displayed.

Components	Description
Instance Name	Instance Name is a Key Vault identifier created in Microsoft Azure Key Vault.

Components	Description
Cloud Type	The cloud provider with which ESKM is integrated. Here select the Cloud Type as Azure.
Tenant ID	Tenant ID is generated when Application is created in Microsoft Azure Key Vault. Copy the Tenant ID to configure the ESKM with Microsoft Azure Key Vault.
Client ID	Client ID is generated when Application is created in Microsoft Azure Key Vault. Copy the Client ID to configure the ESKM with Microsoft Azure Key Vault.
Client Secret	Secret value is generated when Client Secret is created in Microsoft Azure Key Vault. This key cannot be viewed once user exits from the page. Copy the secret value to configure the ESKM with Microsoft Azure Key Vault.
Key Vaults	Key Vault Name created in Microsoft Azure.

Table 4: Add Cloud Instance - parameters

Cloud Instance inst2 [Azure] created successfully.

5.2.2 Editing a Cloud Instance

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

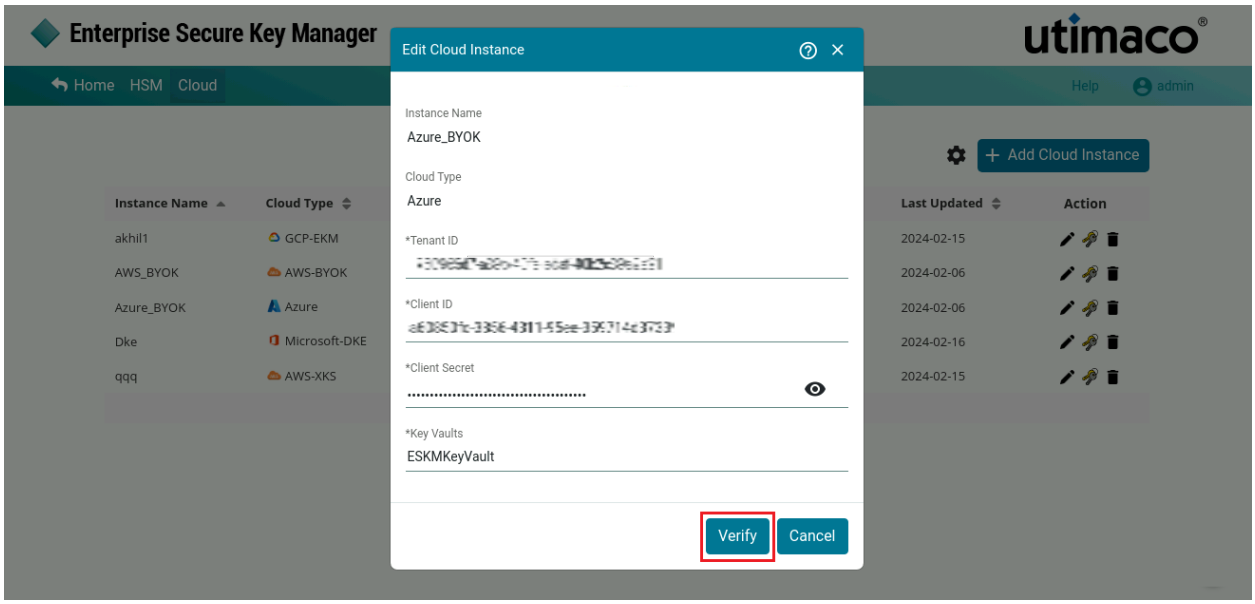

Figure 24 : Verify cloud instance

- The **Edit Cloud Instance** pop-up window will appear. Modify the existing cloud instance details if necessary and click **Verify**.

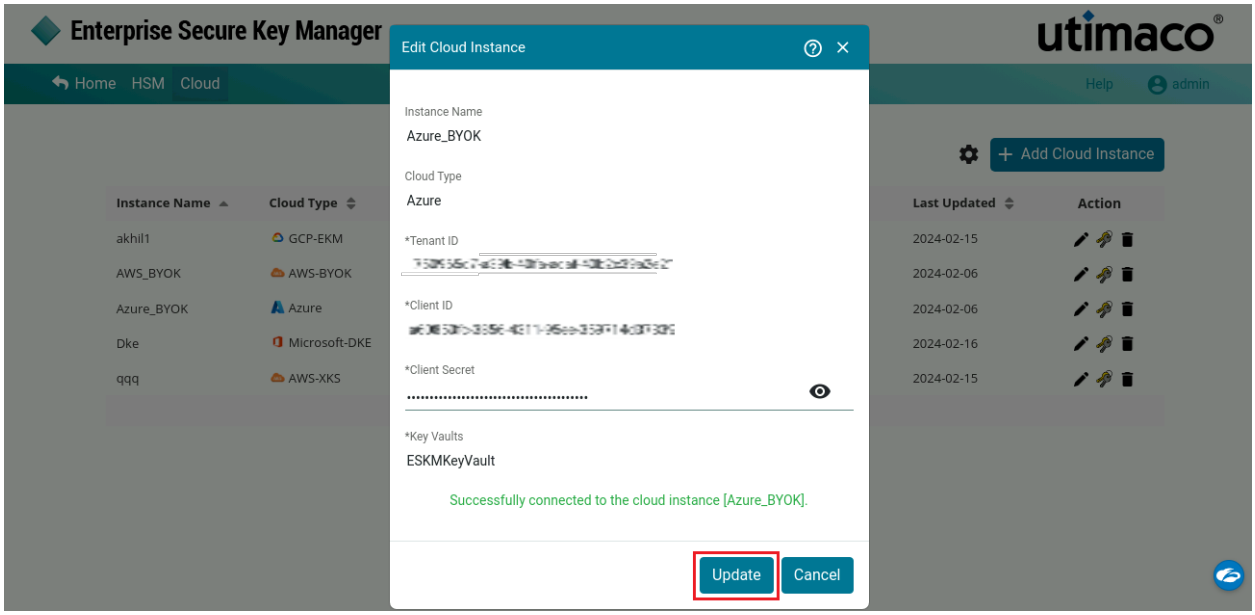

Figure 25 : Update cloud instance

- Click **Update**.

Cloud Instance Instance 2[Azure] updated successfully.

While editing an Azure-BYOK cloud instance, the **Instance** and **Cloud Type** fields cannot be modified.

5.2.3 Deleting a Cloud Instance

1. Under **Action** column, click the **Delete** icon to delete the existing cloud instance.

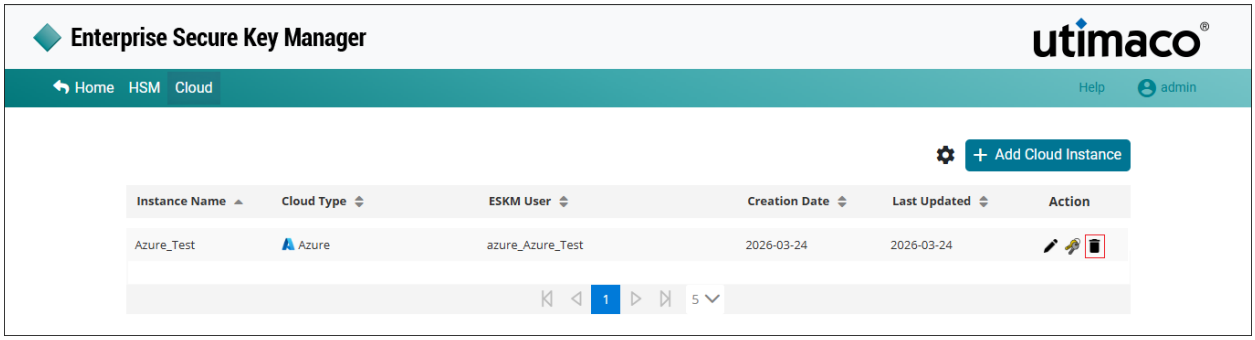

Figure 26 : Delete cloud instance

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

Cloud Instance instance name[Azure] deleted successfully.

Cannot delete Cloud Instance Azure_Test [Azure] as keys are already associated with it.

5.2.4 Key Dashboard

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

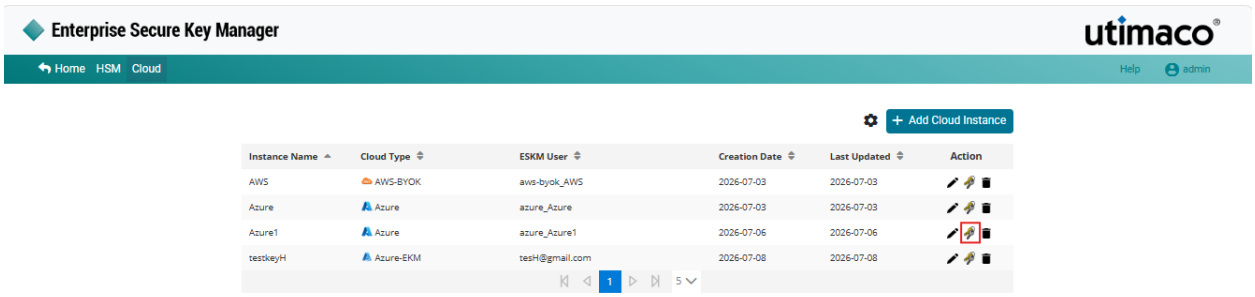

Figure 27 : Manage keys

- Select the key from the keys list to view a key's detailed information.

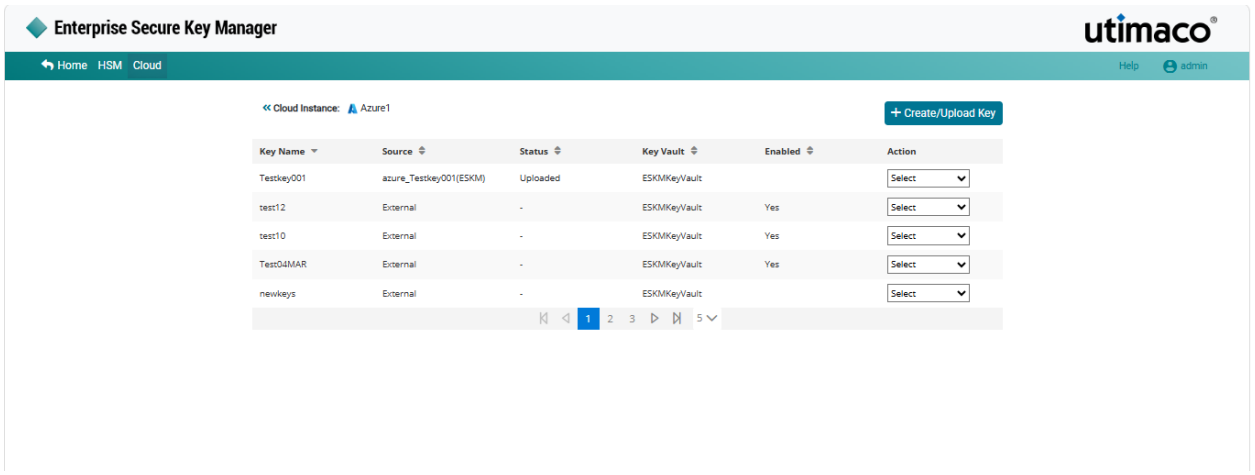

Figure 28 : Key list in the ESKM key dashboard

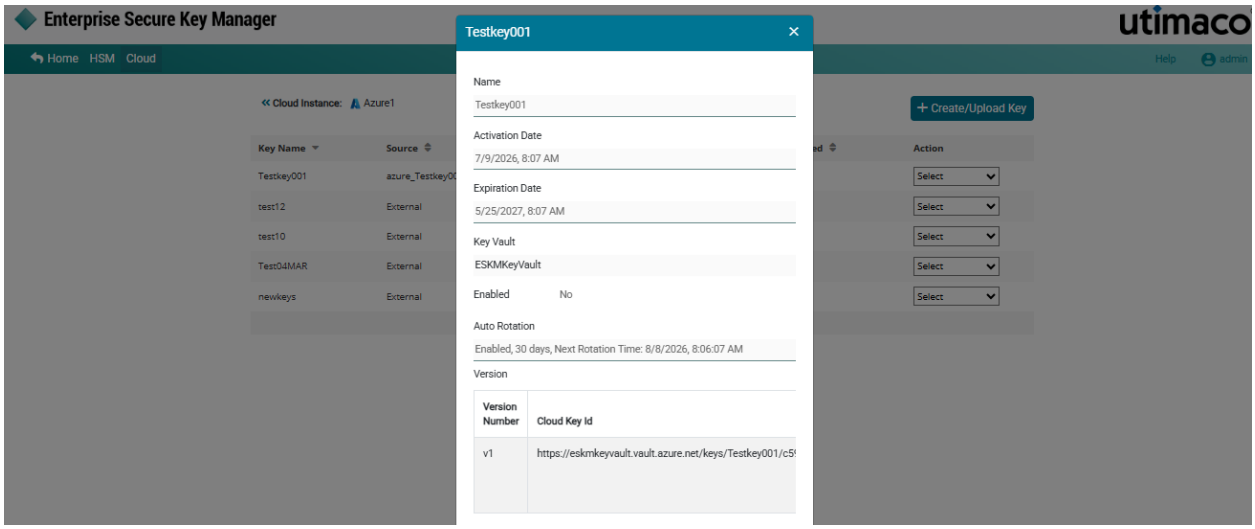

Figure 29 : Key details

Parameters	Description
Key Name	Name of the key.
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.
Status	Status of the key such as Uploaded or Not Uploaded.
Enabled	Displays either “Yes” if the key is enabled in Microsoft Azure Key Vault or “No” if the key is disabled.
Key Vault	Key Vault Name created in Microsoft Azure.
Action	It contains various key actions such as Edit, Delete and Upload.

Parameters	Description
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 5: Cloud instance - keys list parameters

5.2.5 Azure Cloud Integration

The Cloud Integration console provides you with two ways to integrate ESKM keys: Create a new key in ESKM and upload it to Microsoft Azure Key Vault, or upload an existing key from ESKM to Microsoft Azure Key Vault.

This section provides the information on the following topics:

- Creating a New Key
- Uploading an Existing Key
- Upload a Key from ESKM to Azure Cloud
- Deleting an ESKM Key
- Editing an ESKM Key
- Create a New Version
- Azure BYOK Key Rotation

5.2.5.1 Creating a New Key

This section describes the procedure to create a new key to the ESKM Cloud.

To create a new key

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

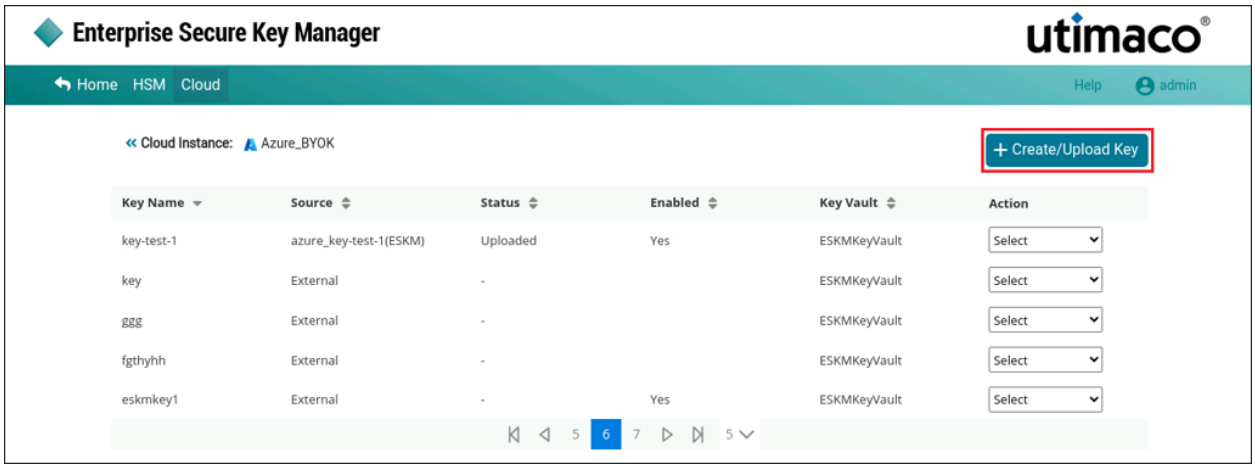

Figure 30 : Create/Upload Key

- Click the **+ Create/Upload Key** button in the top right corner of the page.

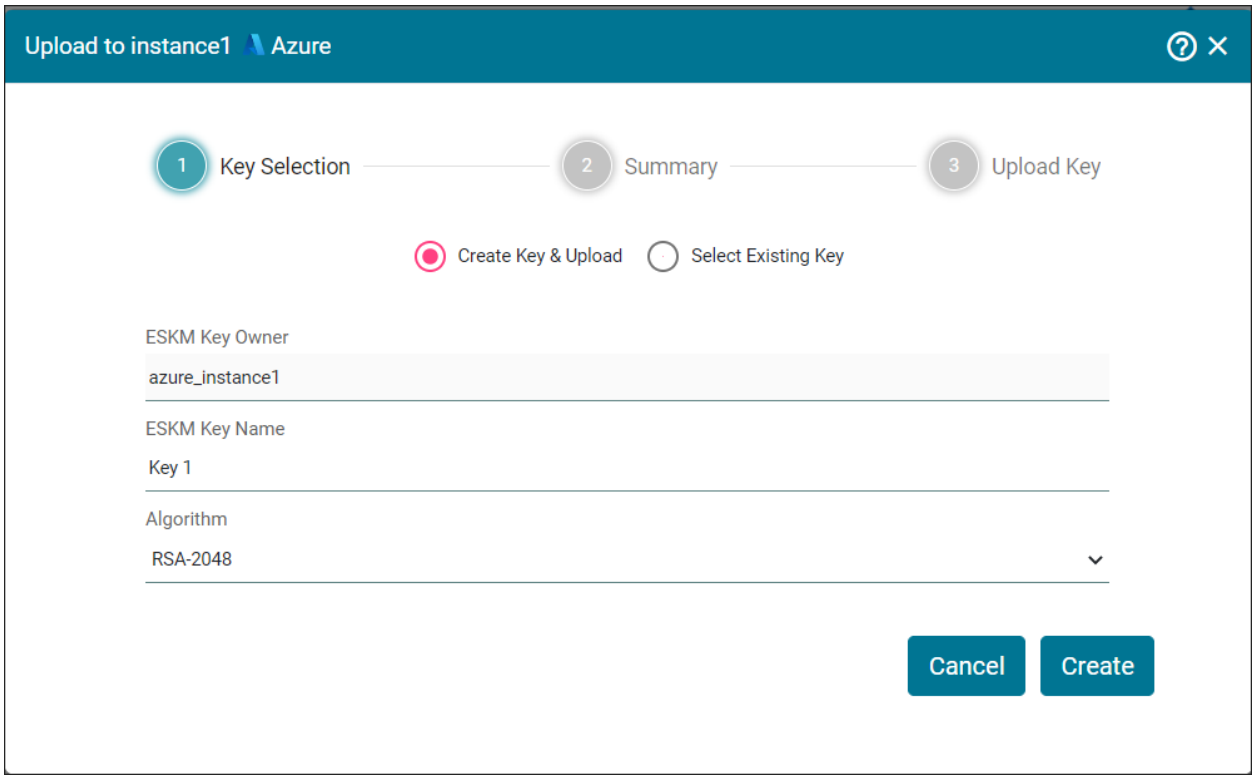

Figure 31 : Key Selection

Provide a valid key name. Key names can only contain alphanumeric characters and dashes.

Parameters	Description
ESKM Key Owner	It is a key vault identifier created in Microsoft Azure key Vault.
ESKM Key Name	Name of the key.
Algorithm	Algorithm used to generate the key in ESKM.

Table 6: Key selection - parameters

- Select **Create New Key & Upload** option (selected by default) to create/upload a new key.
- Enter **ESKM Key Name** and select **Algorithm** from the drop down. Click **Create.**

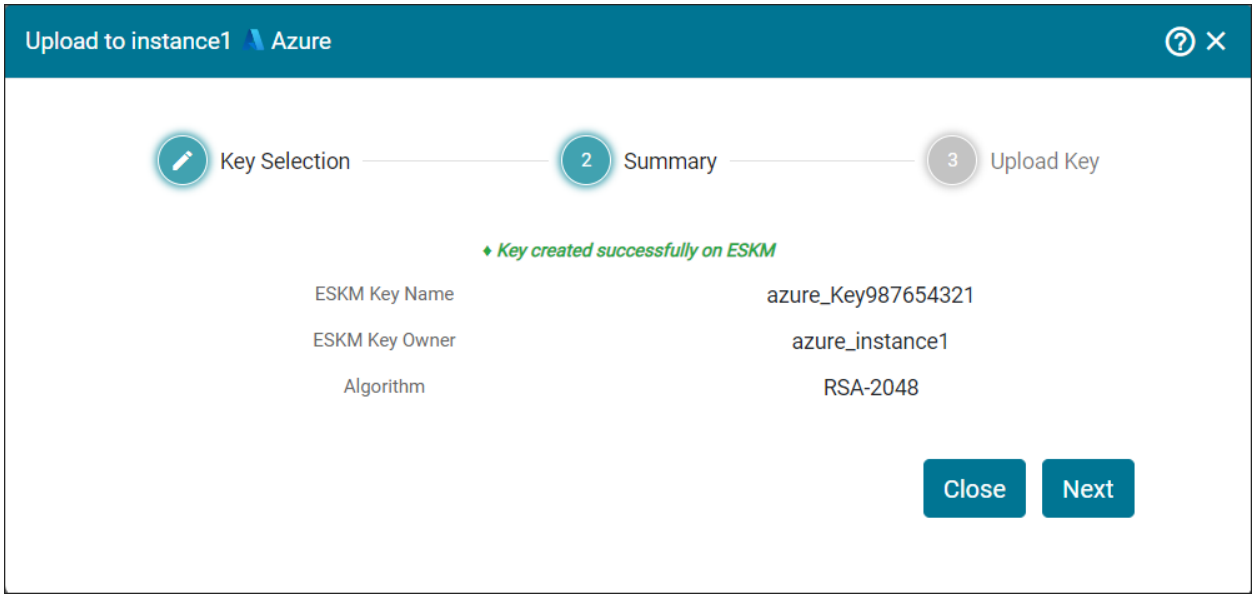

Figure 32 : Review Summary

- Review the **Summary** and click **Next.** You will be navigated to the **Upload Key** section.

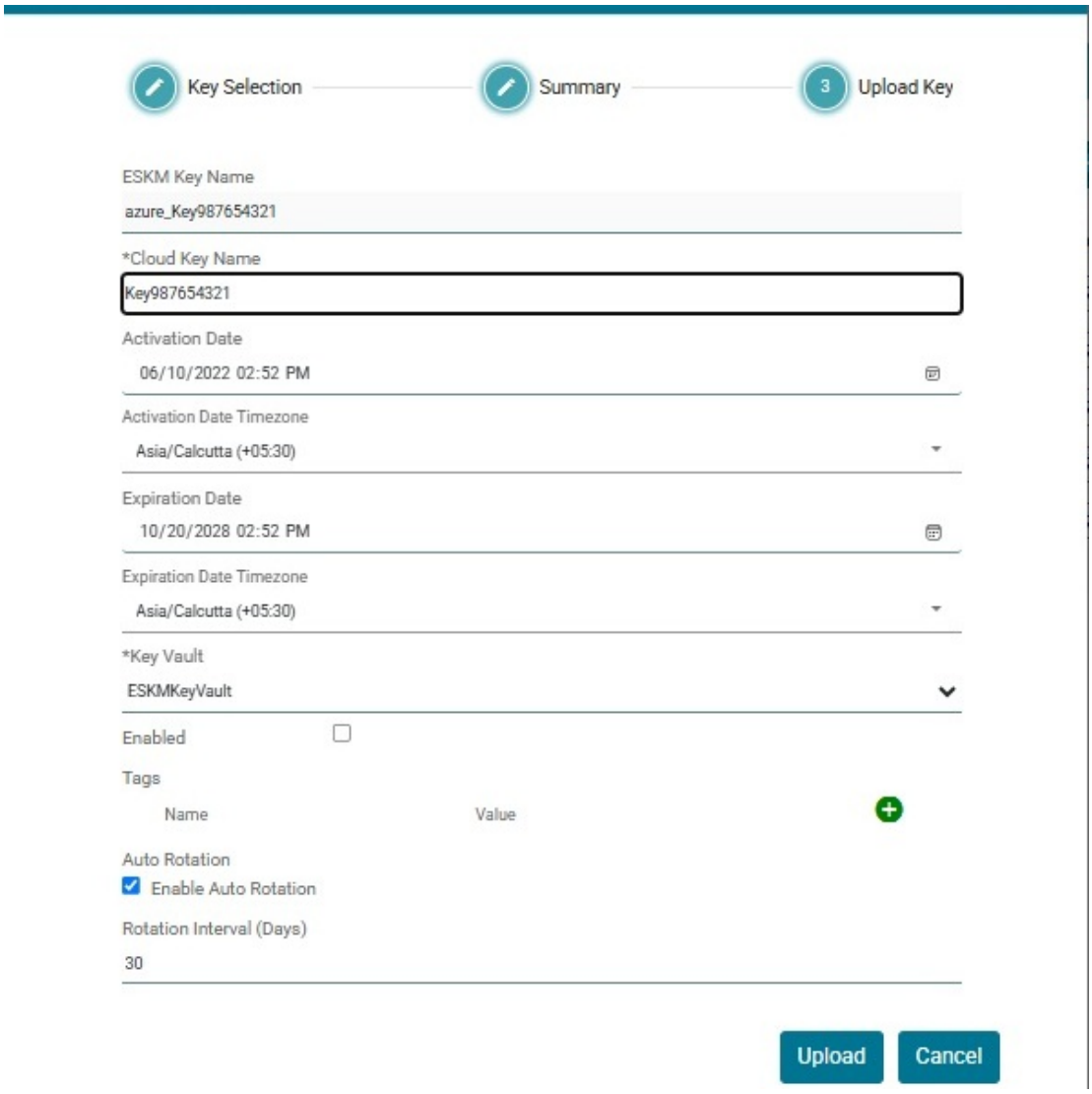

Figure 33 : Upload Key

- Select the **Vault Key Name** (by default, its value is “select”) and fill the details such as **Key Vault**, **Enabled**, **Activation Date** and **Expiration Date**. Optionally, enable **Auto Rotation** and specify the **Rotation Interval (Days)**. Click **Upload**.

Parameters	Description
ESKM key Name	Name of the key. It combines cloud type with the ESKM key name.

Parameters	Description
Cloud Key Name	The name of the ESKM Key to be uploaded to the Microsoft Azure cloud.
Activation Date	Set the date on which the key must be activated.
Activation Date Timezone	The activation date timezone is activated based on the current time of the system.
Expiration Date	Set the expiration date by which the key must be expired.
Expiration Date Timezone	The expiration date timezone is activated based on the current time of the system.
Key Vault	Name of the Key Vault created in Microsoft Azure.
Enabled	Check this box to activate the ESKM key in the Microsoft Azure key vault.
Tags	Tag is to organize the keys in Microsoft Azure Key Vault. Multiple Tags can be assigned for a specific key.
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: Parameters

Key [key_name] has been successfully uploaded to Inst1 [Azure].

5.2.5.2 Uploading an Existing Key

This section describes the procedure to upload existing Keys from Utimaco ESKM to Microsoft Azure Cloud.

To upload an existing key

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

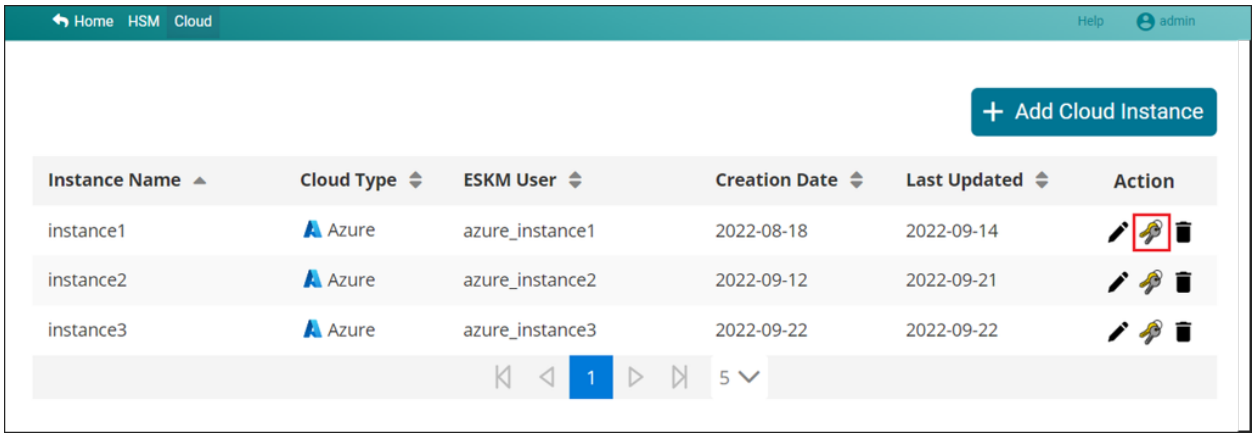

Figure 34 : Manage Keys

- Click the **+ Create/Upload Key** button in the top right corner of the page.

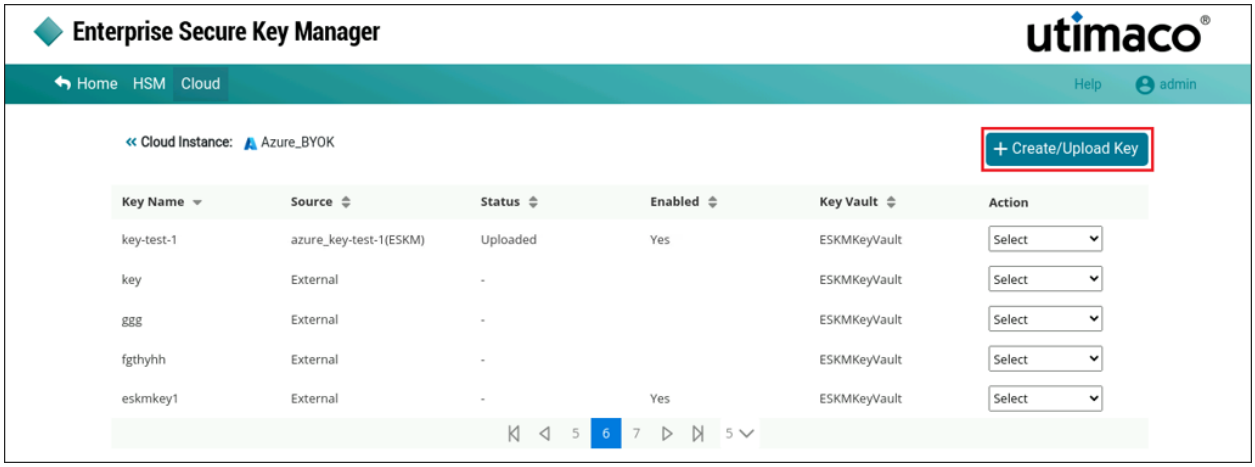

Figure 35 : Keys list

- Choose the **Select Existing Key** option to upload existing keys to the Cloud Instance.

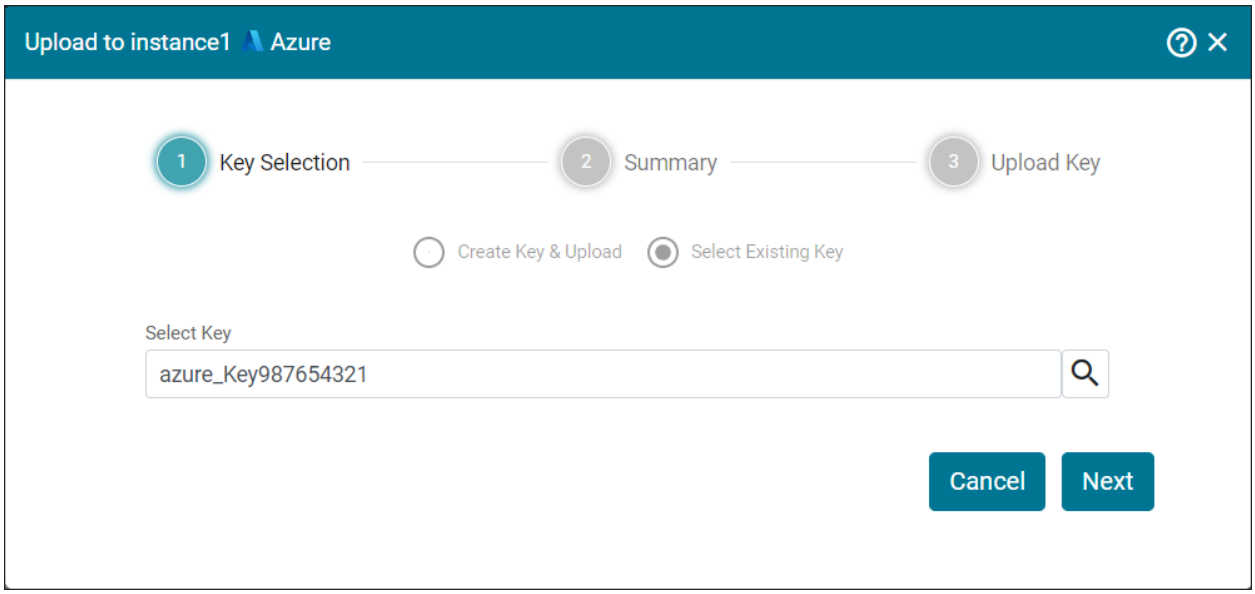

Figure 36 : Select Key

- Search for and select the key that you want to upload. Click **Next**.

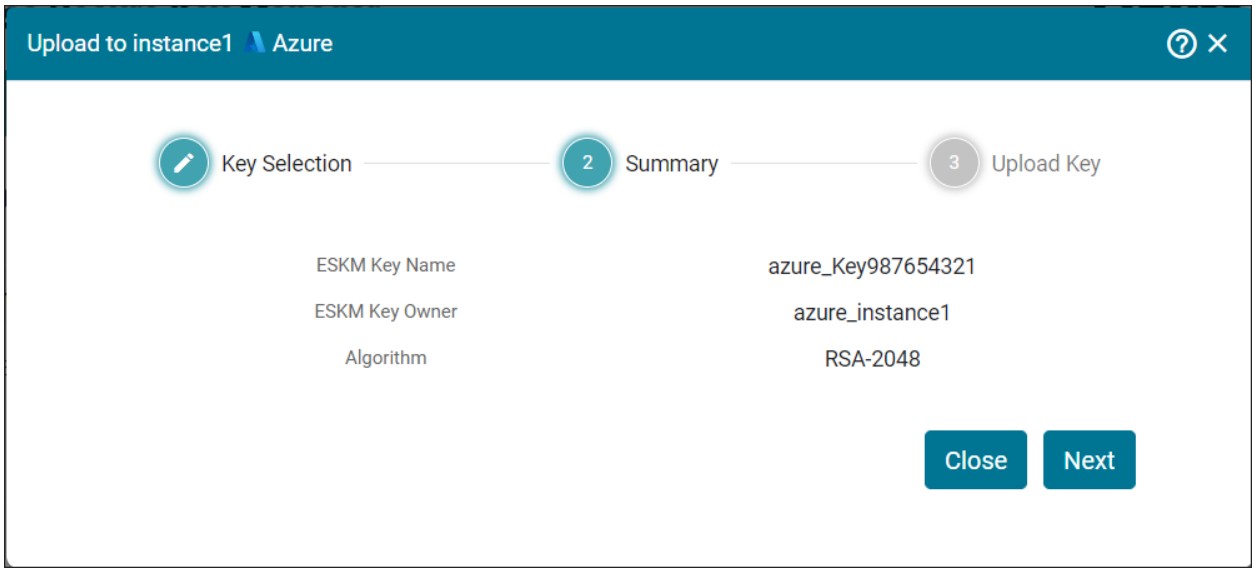

Figure 37 : Review Summary

- Now, you will be navigated to the **Summary** section. Review the **Summary** and click **Next**.
- Enter the details such as **Key Vault Name**, **Key Vault, Enabled**, **Activation Date** and **Expiration Date**. Optionally, enable **Auto Rotation** and specify the **Rotation Interval (Days)**. Click **Upload**.

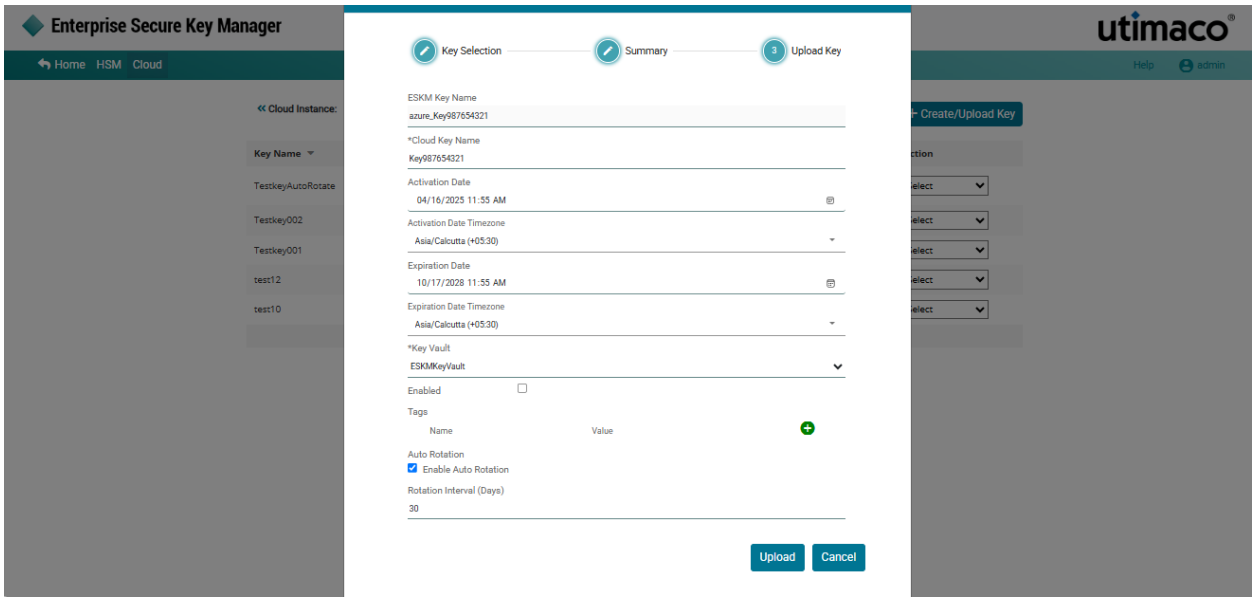

Figure 38 : Upload existing key

Key [Key987654321] has been successfully uploaded to instance1 [Azure].

5.2.5.3 Upload a Key from ESKM to Azure Cloud

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

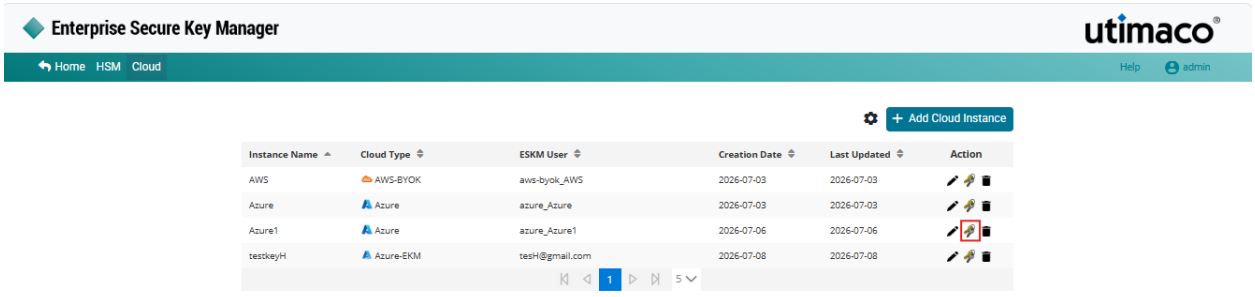

Figure 39 : Manage keys

- If the key is not uploaded from ESKM to cloud and you wish to upload it, select **Upload** from the drop-down.

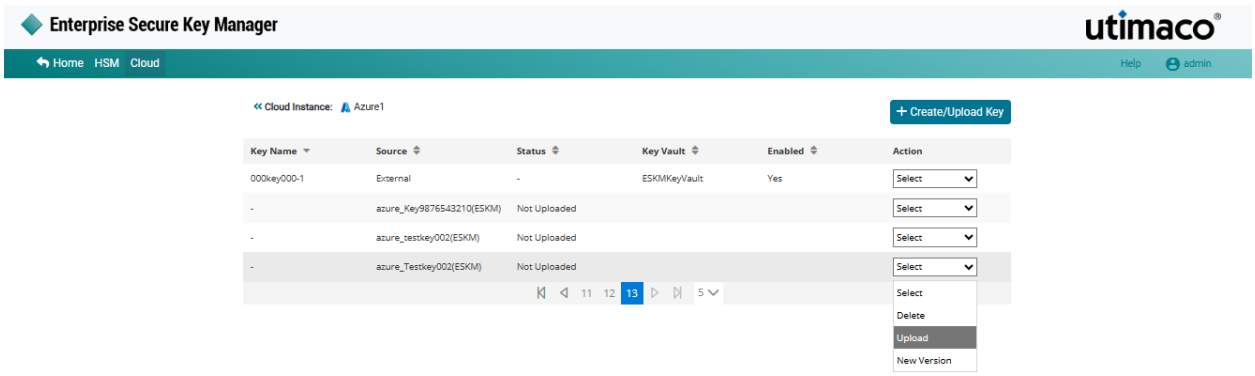

Figure 40 : Upload key from ESKM to cloud

- The **Upload key** pop-up window appears. Make the necessary changes and click **Upload**.

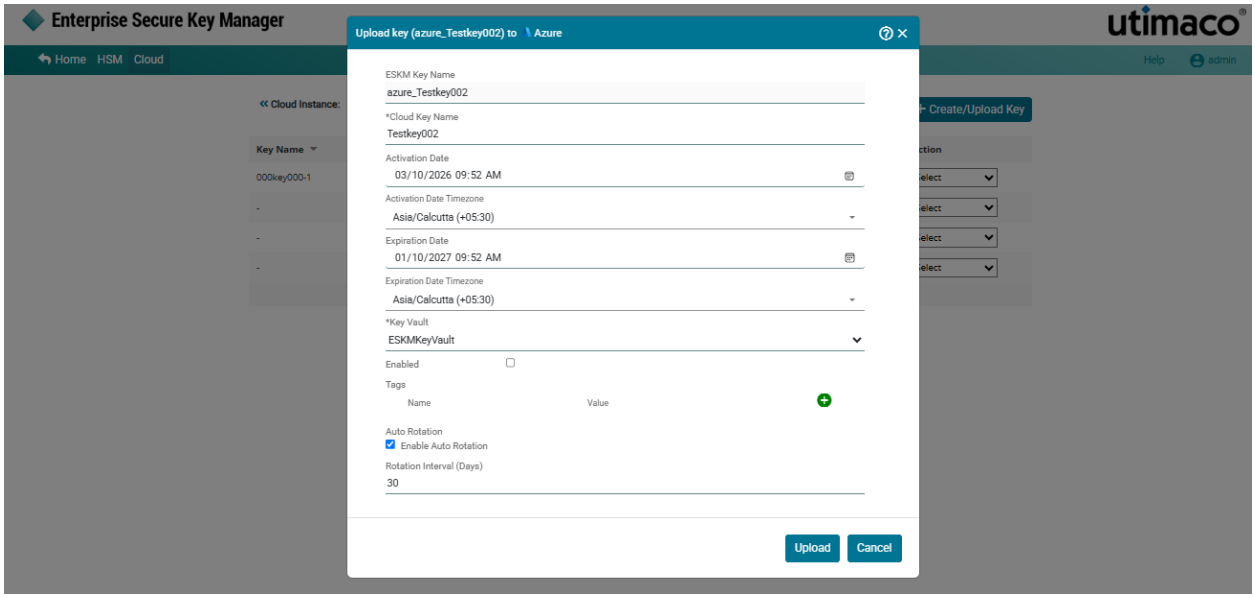

Figure 41 : Upload Azure key

Cannot upload the same key that has been deleted and purged from the cloud.

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

5.2.5.4 Deleting an ESKM Key

- Click the **Manage keys** icon in the cloud instance and select **Delete** from the drop down.

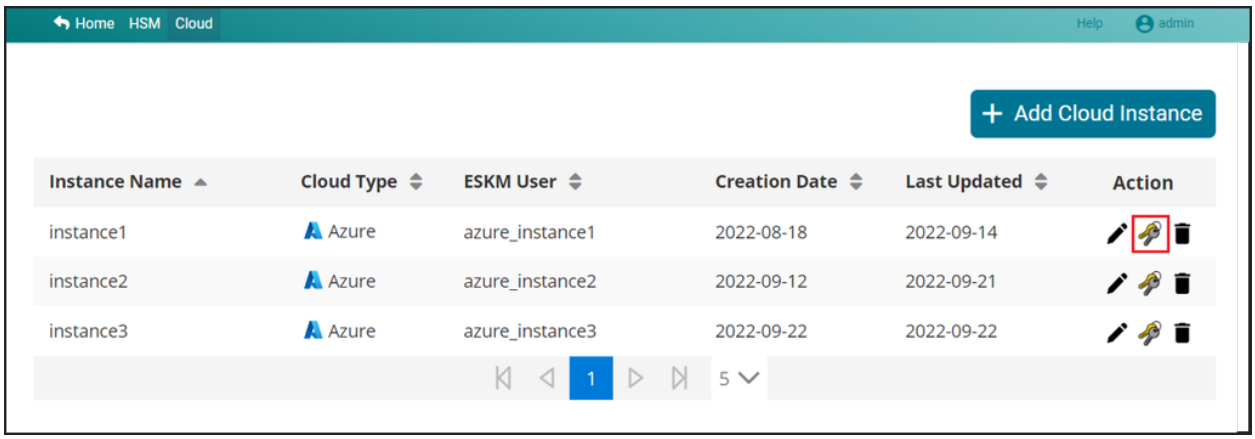

Figure 42 : Manage keys

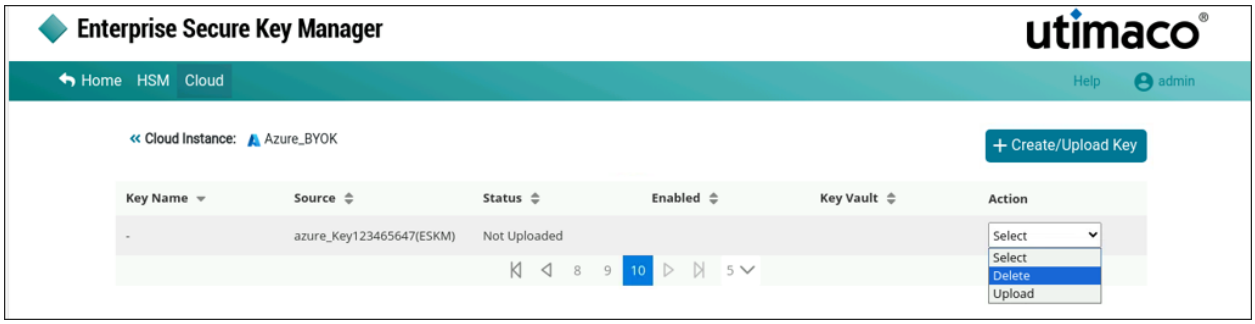

Figure 43 : Delete keys

- If the selected key is uploaded and is not associated with any other instance, a pop-up window will appear with a message "**Are you sure you want to delete key<keyname> from <Cloud Instance Name>(Azure)?**".

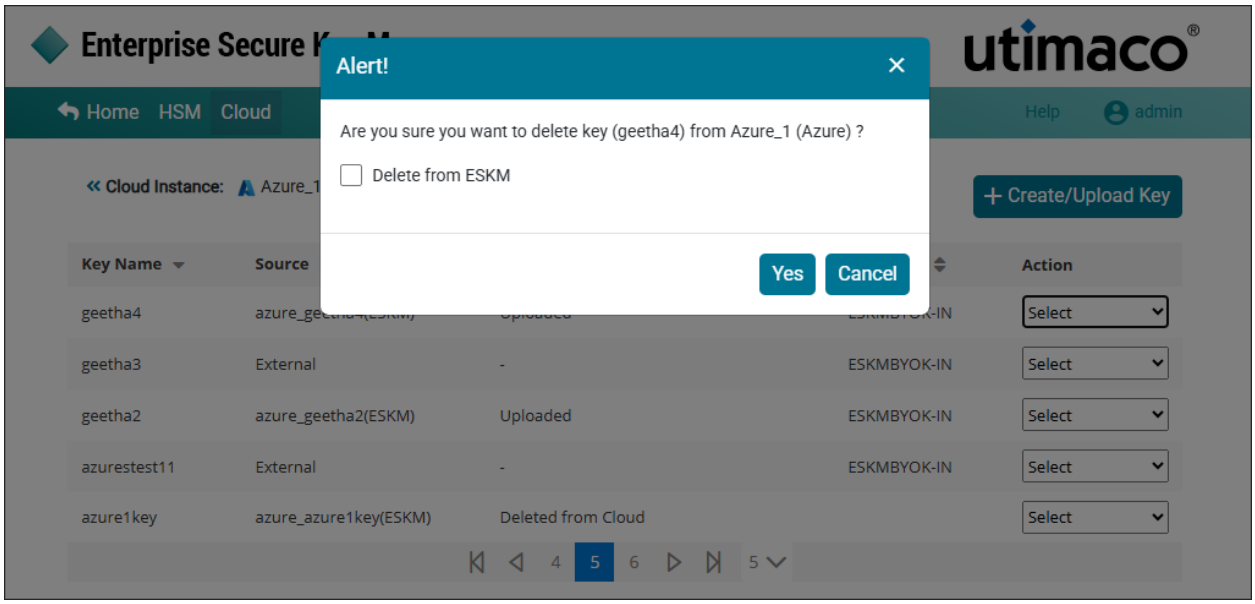

Figure 44 : Delete key alert

- Click **Yes** and the key will be deleted from the cloud.
- If the key is uploaded and associated with another instance (locally created from another instance), a pop-up window will appear with a message "**Are you sure you want to delete key <keyname> from <Cloud Instance Name> (Azure)?**".

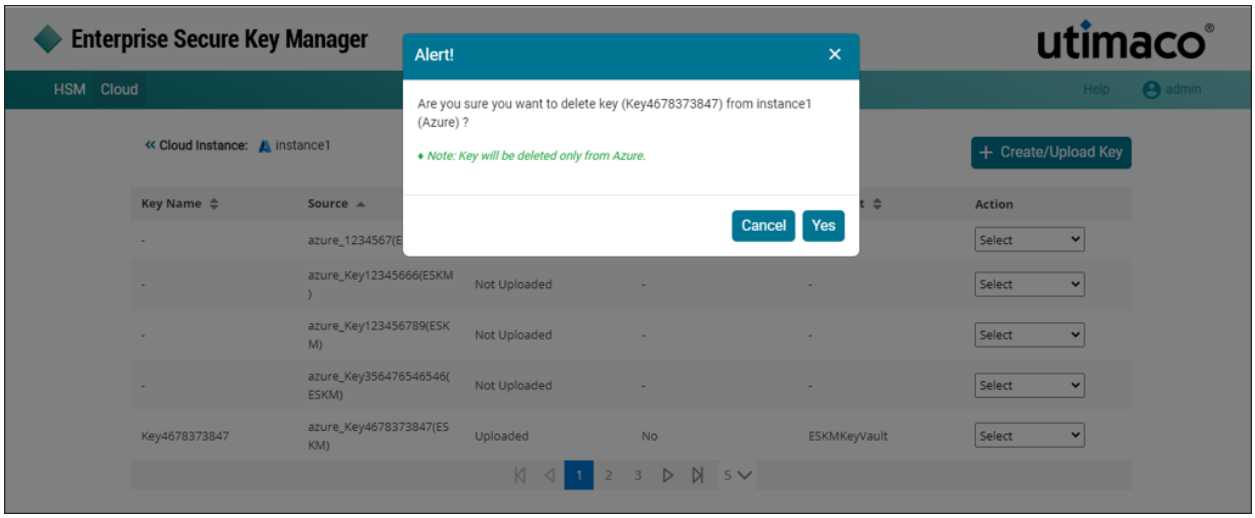

Figure 45 : Delete key from cloud

- Click **Yes** and the key will be deleted from Cloud.

- If the selected key is not uploaded and is not associated with any other instance (locally created in ESKM), a confirmation pop-up appears with the message: **"Are you sure you want to delete key <keyname> from ESKM?"**.

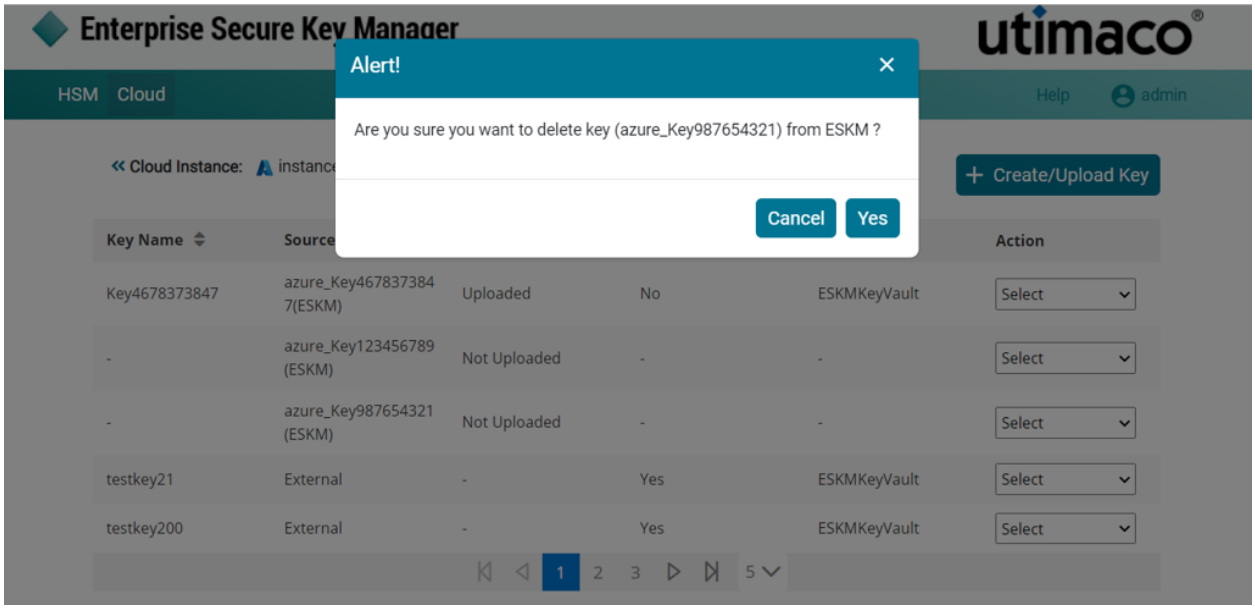

Figure 46 : Delete key from ESKM

- Click **Yes** and the key will be deleted from **ESKM**.
- When deleting an external key that is not created in ESKM, the system displays a confirmation pop-up with the message: "**Are you sure you want to delete key<keyname> from <Cloud Instance Name>(Azure)?**".

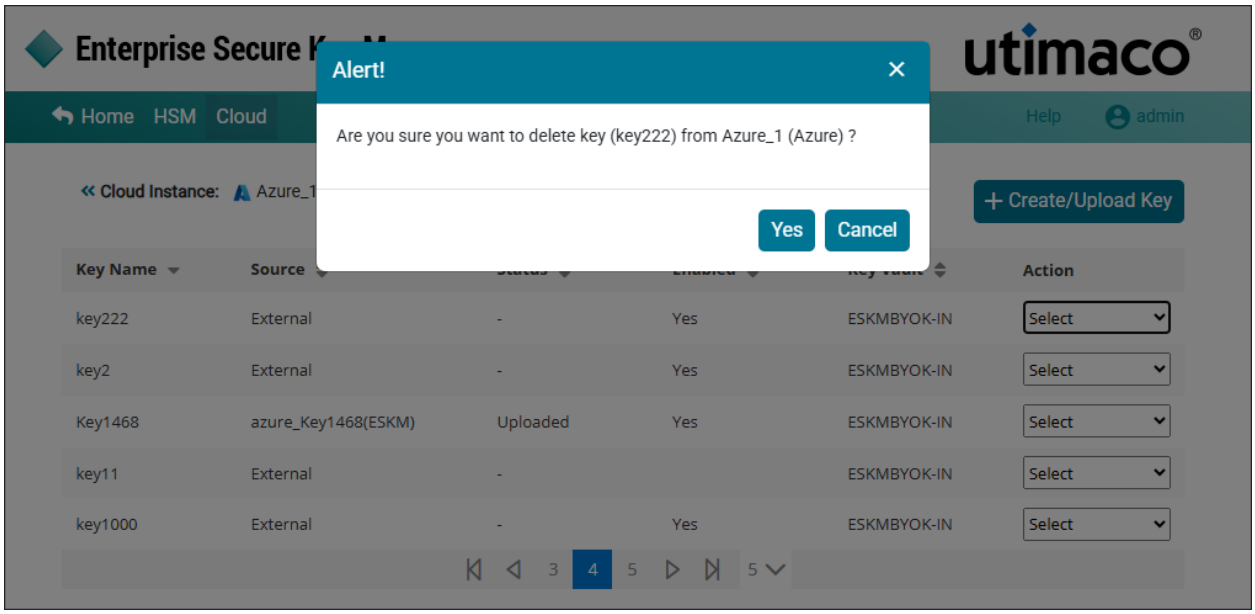

Figure 47 : Delete external key

- Click **Yes** and the key will be deleted from **Azure**.

Cloud Instance key [key222] removed successfully from Azure_1 [Azure].

5.2.5.5 Editing an ESKM Key

- Select **Edit** from the drop-down on the cloud instance page to modify the selected key information.

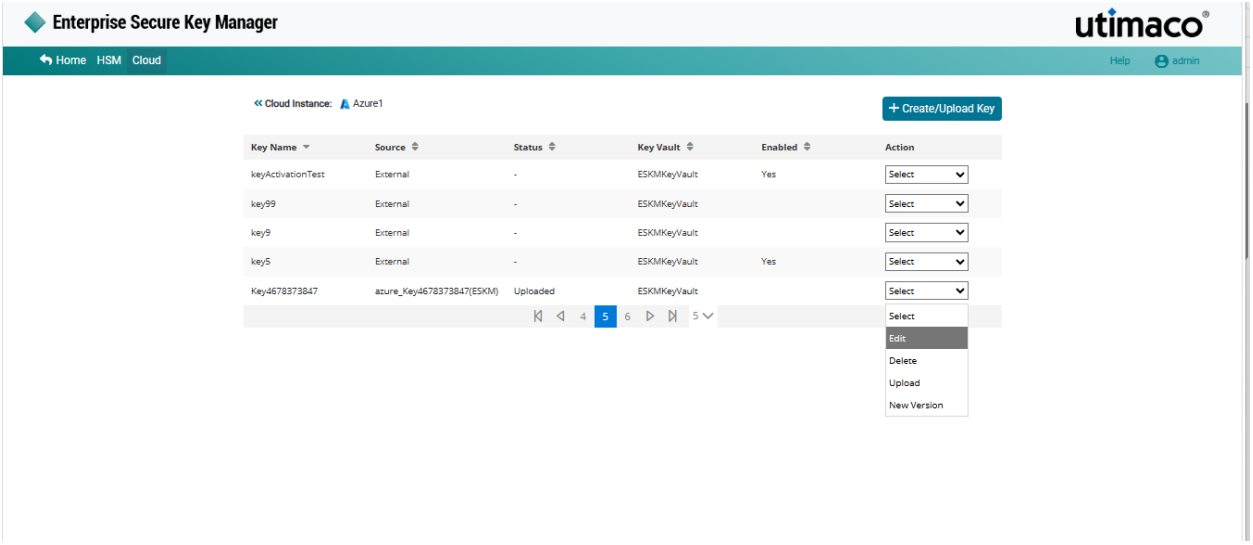

Figure 48 : Edit key

- Make the required modifications and enable or disable the selected key.

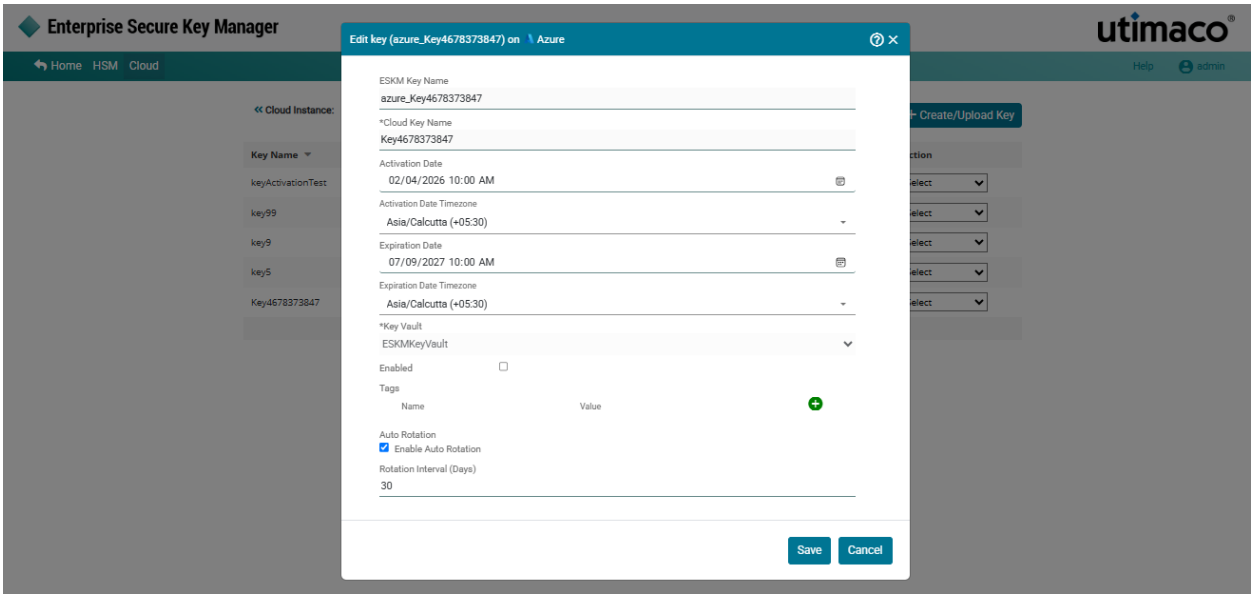

Figure 49 : Editing a key

- Click **Save**.

Cloud Instance key [azure_key4678373847] updated successfully.

While editing a key in ESKM, you cannot modify the **ESKM Key Name**, **Cloud Key Name** and **Key Vault**. Additionally, external keys created directly in the Azure console cannot be edited in ESKM. **Auto Rotation** settings can be configured or modified for existing keys as required.

5.2.5.6 Create a New Version

This section describes the procedure to create a new version of a key which has already been created.

To create a new version

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

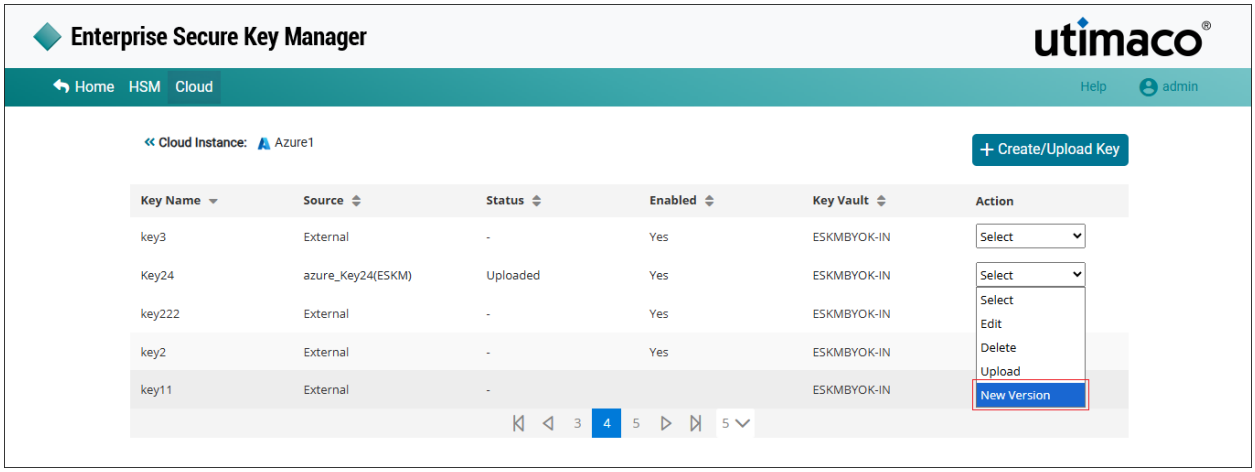

Figure 50 : New version

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

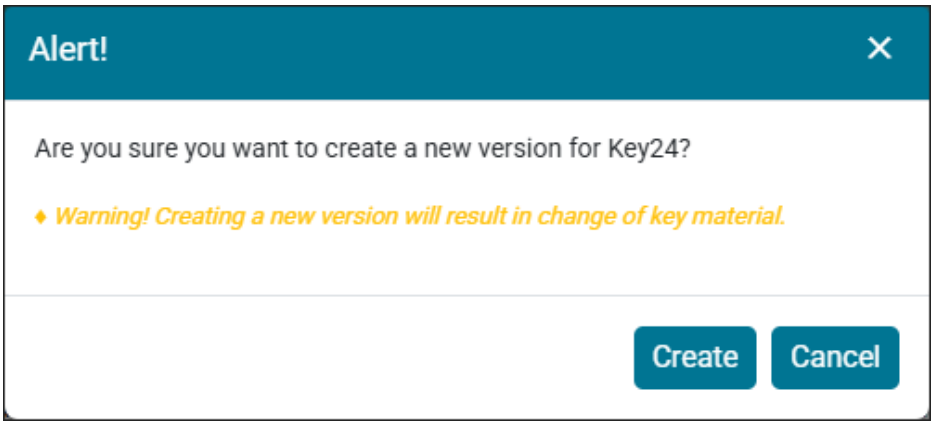

Figure 51 : Alert window

Click **Create**.

New version 3 for ESKM key [azure_Key24] added successfully.

After creating a new version, the key must be uploaded using the Upload option (refer to *Upload Key from ESKM to Azure Cloud*).

The default value for the Number of Active Versions Allowed for a key is 10. To modify this setting, refer to the *Active Versions (Section 6.4.12.1)* 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.

5.2.5.7 Azure BYOK 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 Azure Cloud

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

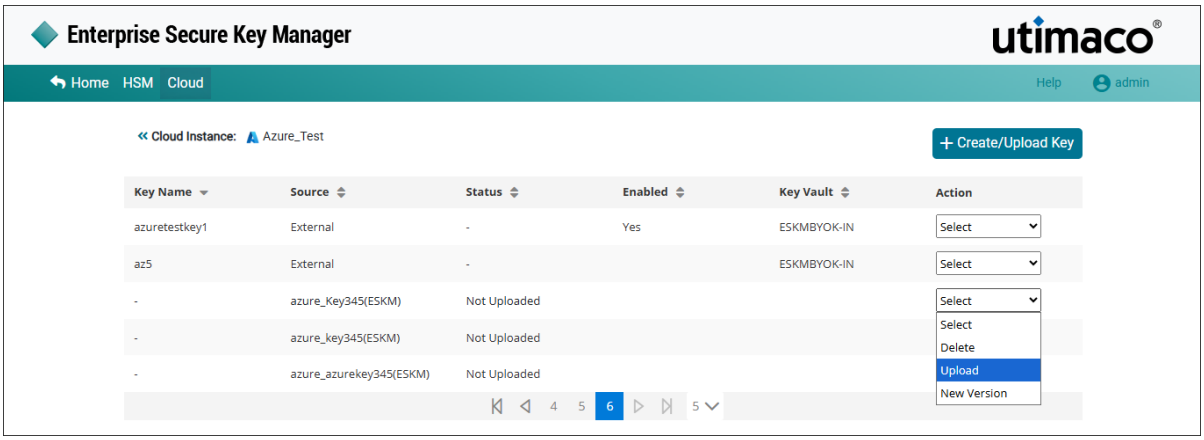

Figure 52 : Upload key

- Select **Upload** to upload the **new key version** to the Azure Cloud console.

For detailed steps, refer to *Upload Key from ESKM to Azure Cloud*.

5.2.5.7.1 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 Azure Key Vault. Older key versions are retained and continue to be available for decrypting previously encrypted data.

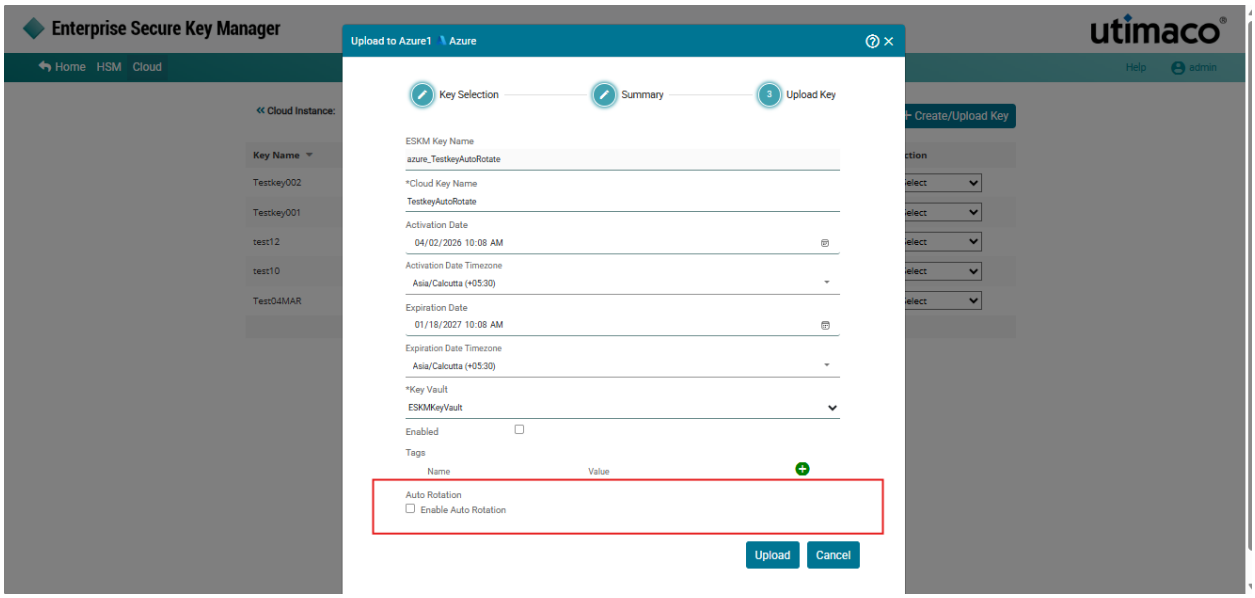

Figure 53 : Auto rotation

Note: 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.

6 Verification and Testing

6.1 Logs and Validation Steps

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

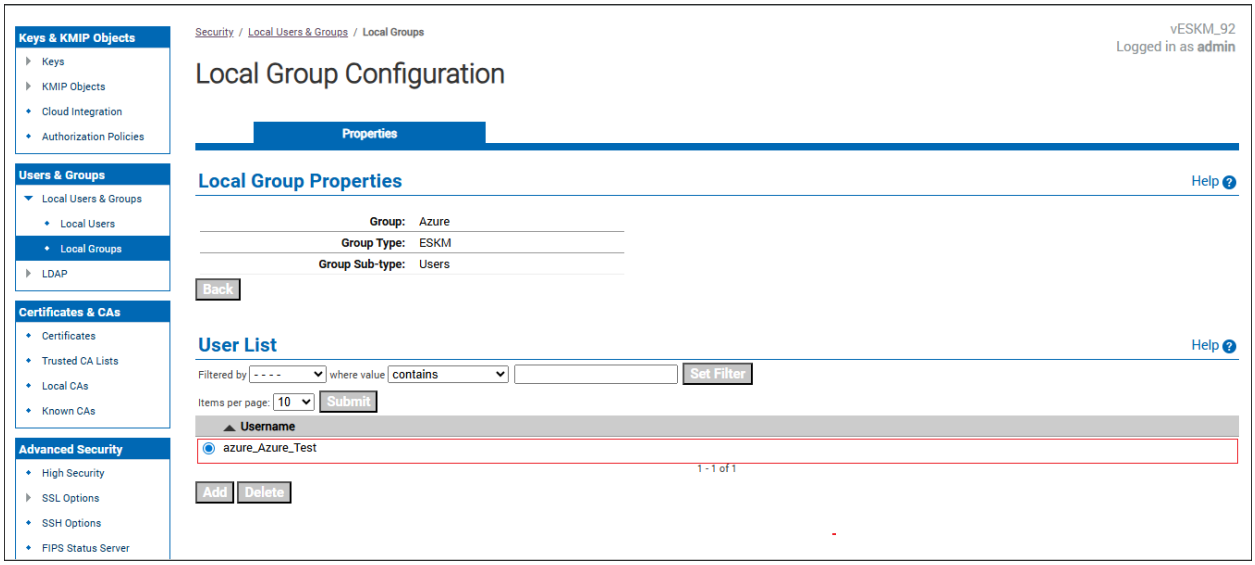

Figure 54 : User list

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

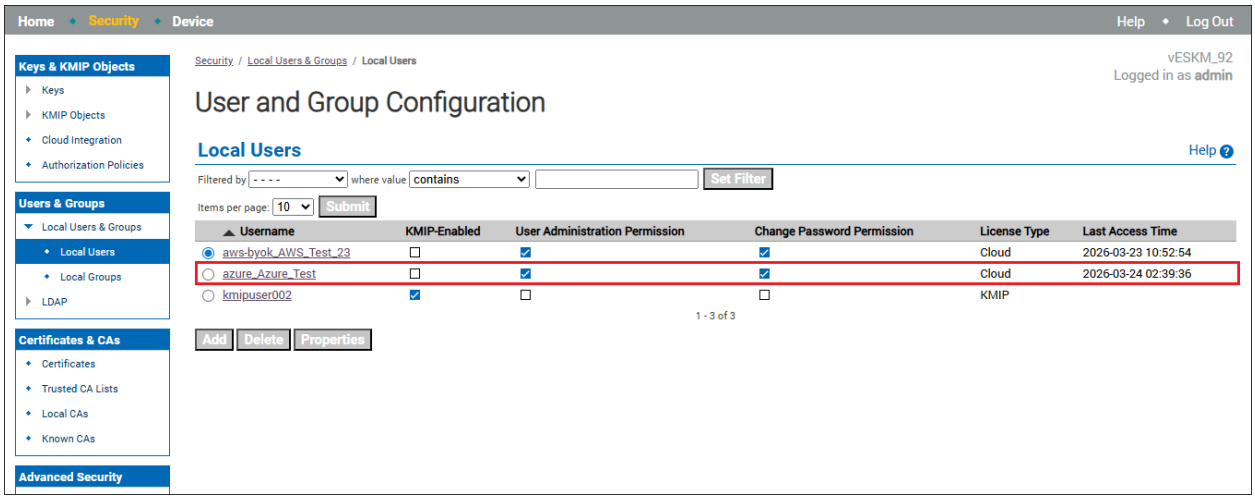

Figure 55 : Local users

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

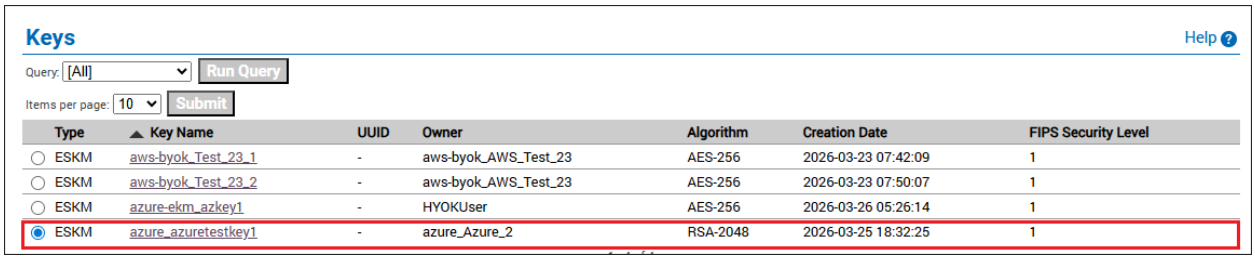

Figure 56 : Keys

- 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.

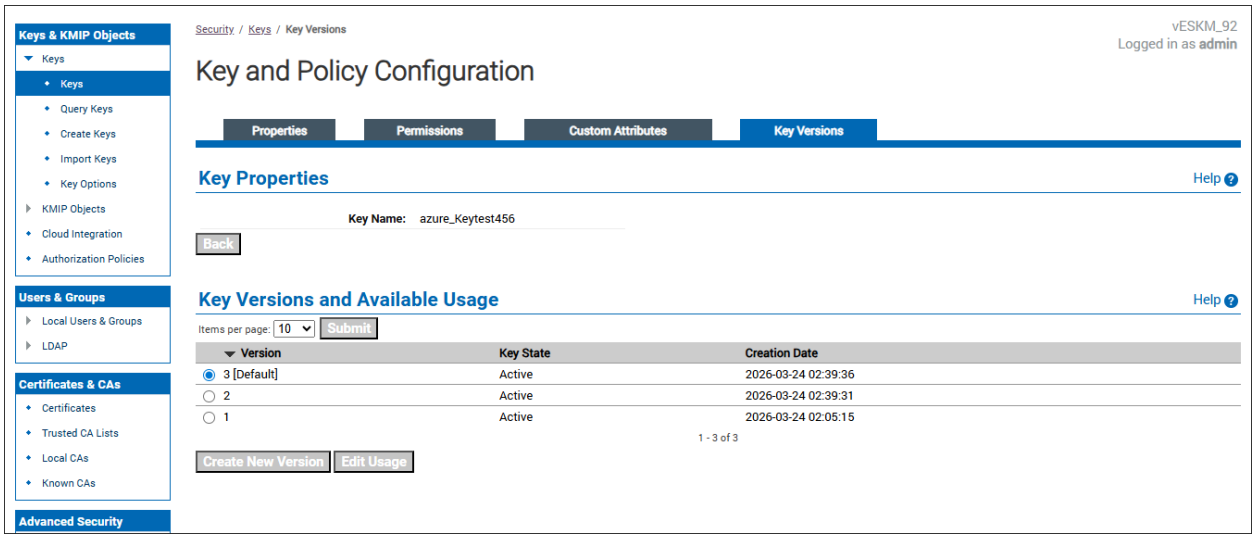

Figure 57 : ESKM key rotation

- In the **Azure Portal**, go to **Key Vaults**, select the required **Key Vault**, and select **Keys** from the left navigation pane. Verify that the key is created.

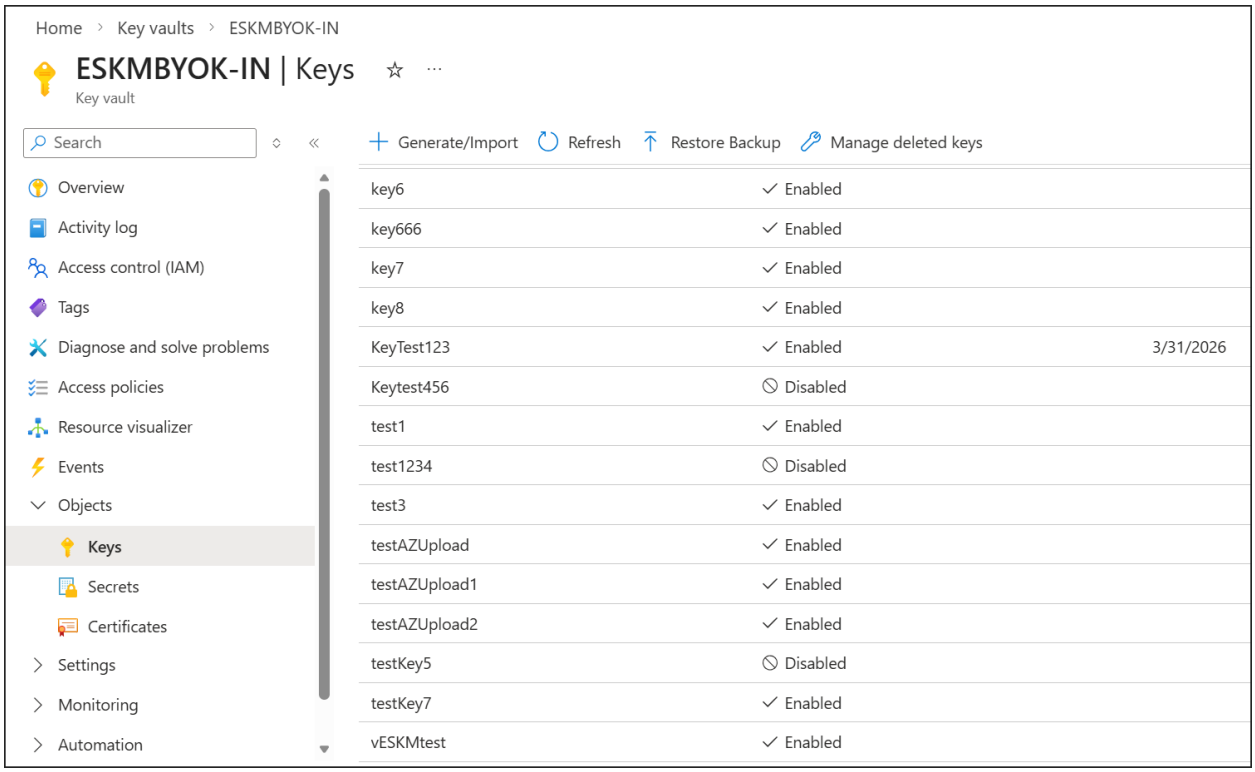

Figure 58 : Keys uploaded in Azure console

- Log in to the **Azure Portal**, navigate to **Key vaults** and select the required **Key Vault**. Select **Keys** and select the required **Key**. Verify that the key rotation is created after uploading in ESKM Console.

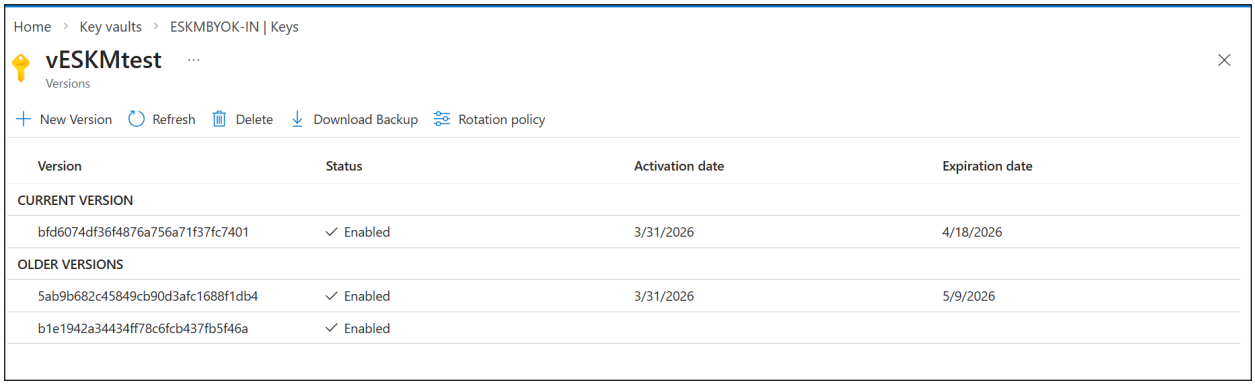

Figure 59 : Key rotation in Azure console

7 Troubleshooting

7.1 Log Locations and Interpretation

Verify the Utimaco ESKM logs by following the steps below:

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

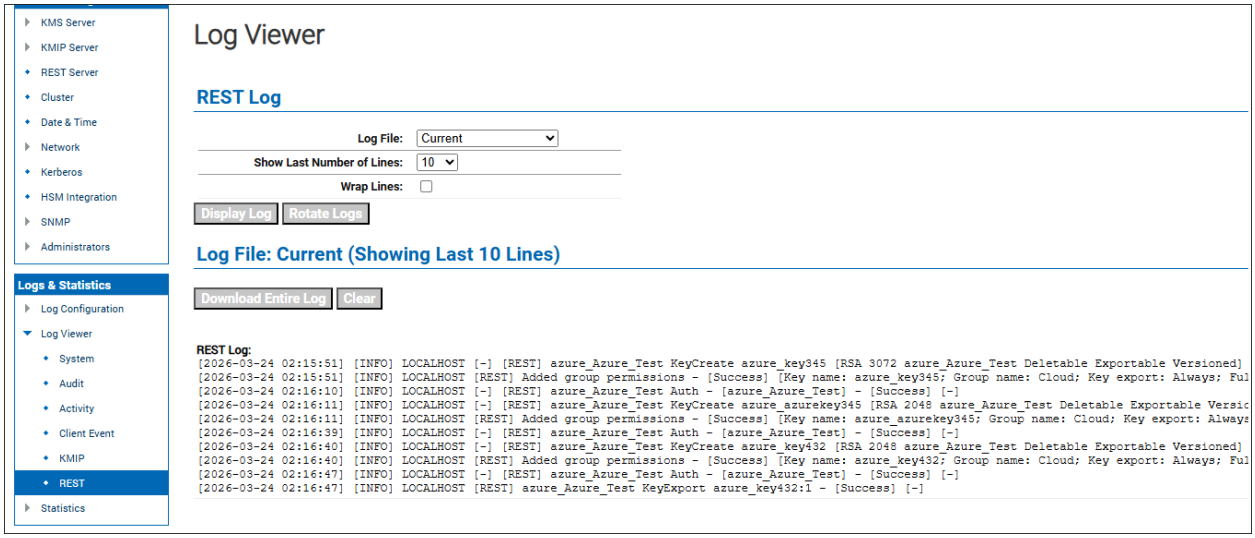

Figure 60 : Rest log

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.

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 Str. 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
Azure-BYOK	Create Key Vault, Secret ID and Client ID	https://learn.microsoft.com/en-us/azure/key-vault/general/quick-create-portal

Table 8: References

10 Appendix B: Glossary

Term	Description
Azure BYOK	Allows customers to use their own encryption keys in Azure.
ESKM	Utimaco system used to create and manage encryption keys outside Azure.
Customer-Managed Key (CMK)	An encryption key owned and controlled by the customer.
Azure Key Vault	Azure service that stores and manages encryption keys.
Key Import	Process of importing an external key into Azure Key Vault.
Key Rotation	Creating a new version of a key to replace an old one.

Table 9: Glossary