Microsoft
Azure Key Vault Managed HSM (HYOK)

Integration Guide

ESKM

8.54.7

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-09-18
Status	PUBLISHED
Document No.	IG-2026-0037

Table of Contents

1 Introduction

Azure Key Vault Managed HSM (HYOK) allows organizations to protect highly sensitive data while keeping full control of their encryption keys. In this approach, encryption keys are stored and managed only within the organization's own environment and are not stored in the cloud.

When Azure Key Vault Managed HSM (HYOK) is integrated with Enterprise Secure Key Manager (ESKM), ESKM is used to securely create, store, and manage the encryption keys. With Azure Key Vault Managed HSM (HYOK), the encryption key used to protect data in Azure services (the Key Encryption Key, or KEK) is kept entirely outside Microsoft's infrastructure, while cryptographic operations are performed by Azure Managed HSM (MHSM) through its integration with ESKM.

1.1 About This Guide

This guide explains how to integrate Azure Key Vault Managed HSM (HYOK) with Enterprise Secure Key Manager (ESKM).

1.2 Target Audience

This guide is intended for Utimaco ESKM and Azure Key Vault Managed HSM (HYOK) administrators.

1.3 Purpose of the Integration

The purpose of this integration is to enable Azure Key Vault Managed HSM to use encryption keys that are managed externally in Utimaco ESKM. This approach allows organizations to maintain control of key material while integrating with Azure services that support external key management.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
EKM	External Key Management

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
KEK	Key Encryption Key
HYOK	Hold Your Own Key
CA	Certificate Authority
CLI	Command-Line Interface
URL	Uniform Resource Locator
CN	Common Name
DEK	Data Encryption Key
GUI	Graphical User Interface
CMK	Customer-Managed Key
MHSM	Managed Hardware Security Module
REST	Representational State Transfer
SSL	Secure Sockets Layer

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

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

Table 2: Document conventions

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

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

Here you will find additional notes or supplementary information.

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

2 Product Overview

2.1 Overview of Azure Key Vault Managed HSM (HYOK)

Azure Key Vault Managed HSM (HYOK) allows organizations to protect highly sensitive data while keeping full control of their encryption keys. With External Key Management, encryption keys remain in the organization's own environment and are not stored in the cloud.

Azure Information Protection is used for data classification and labeling, while encryption and key operations are performed using on-premises Rights Management Services with customer-controlled keys. This approach helps organizations meet security, compliance, and data ownership requirements without changing the user experience.

2.2 Overview of ESKM

Utimaco Enterprise Secure Key Manager (ESKM) is a solution used to securely manage encryption keys within an organization's own environment. It helps create, store, and control encryption keys in a central and secure way.

ESKM works with Hardware Security Modules (HSMs) to protect keys and meet security and compliance requirements. In the Azure Key Vault Managed HSM (HYOK) integration, ESKM ensures that encryption keys remain fully under the organization's control and are not stored or managed in the cloud.

2.3 Joint Value Proposition

This integration enables Azure Hold Your Own Key (HYOK) by allowing customers to keep their encryption keys outside Azure in a customer-owned Hardware Security Module (HSM) or external key management system (ESKM).

Azure accesses these externally stored keys through ESKM to perform cryptographic operations for supported Azure services using Customer-Managed Keys (CMK), while the key material remains entirely within the customer-controlled environment and is never exposed to Azure.

Azure Key Vault Managed HSM (HYOK) creates the data encryption key (DEK) and securely sends it to ESKM. ESKM protects the DEK by encrypting it with a key that is created and stored only in ESKM. This key never leaves the customer's environment.

Azure stores only the encrypted DEK and cannot access the data without the key held in ESKM. This ensures customers retain full control of their encryption keys while securely integrating with Azure services.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Azure Version	Utimaco ESKM
Azure HYOK	ESKM 8.54.7

Table 3: Tested versions

3.2 Supported Platforms

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

3.3 Software Requirements

Software	Software Requirements
Utimaco ESKM	8.54.7 or later

Table 4: Software requirements

3.4 Prerequisites

- ESKM version 8.54.7 or later is required.
- A valid domain name along with the corresponding SSL certificate is required.
- A Microsoft Azure account with permissions to use EKM is required.
- ESKM must be hosted as an internet-accessible server so that it can be reached by the Azure cloud.
- An Azure Key Vault Managed HSM has been provisioned and activated. Refer to the Microsoft documentation *"Quickstart - Provision and activate an Azure Key Vault Managed HSM using the Azure portal"* for detailed instructions.
- The required certificates and keys are available in Utimaco ESKM.

- Appropriate permissions have been assigned in Azure.
- Azure Key Vault Managed HSM External Key Management (EKM) must be enabled to obtain the client certificate Subject Common Name (CN) required for ESKM configuration.

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** (or **Security → HSM Integration**, depending on the ESKM version) to access the integration configuration page.

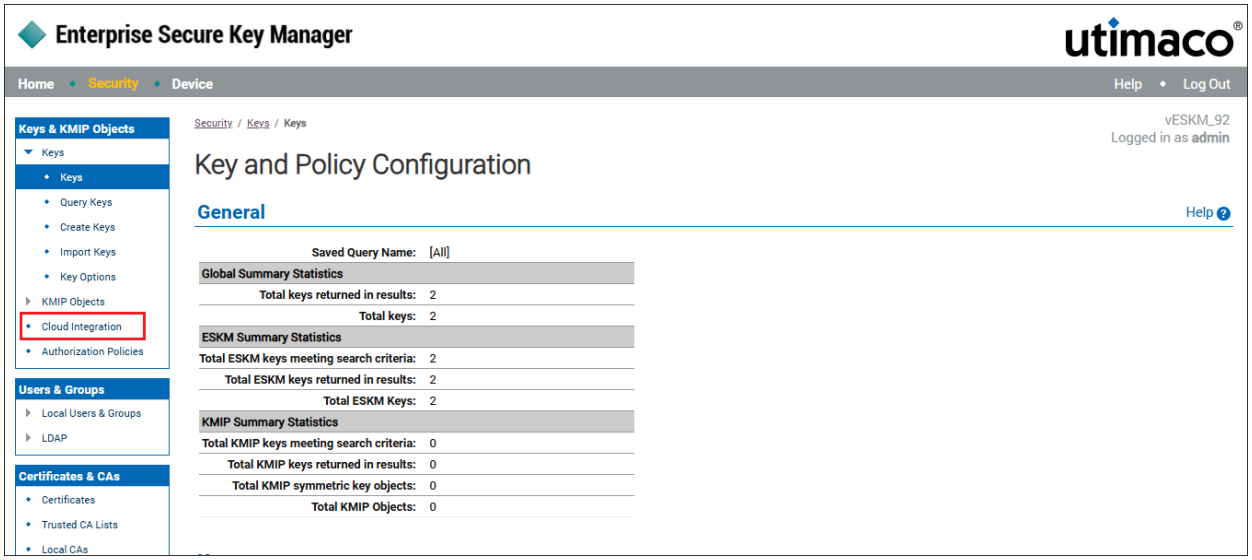

Figure 1 : Cloud Integration

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

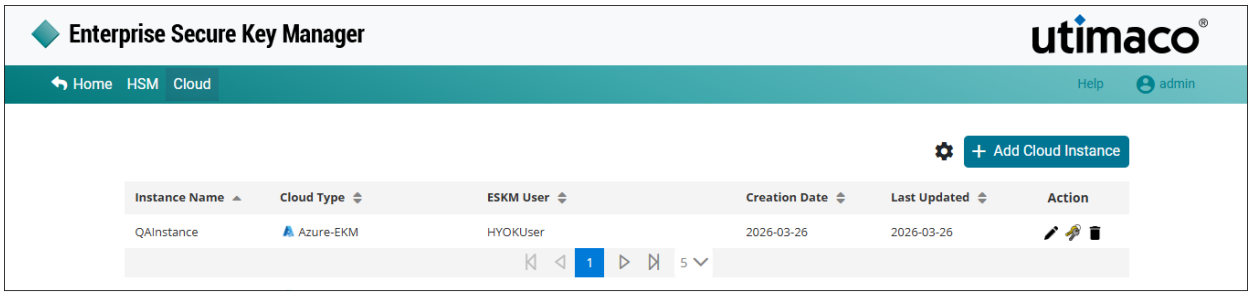

Figure 2 : Cloud Integration Dashboard

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

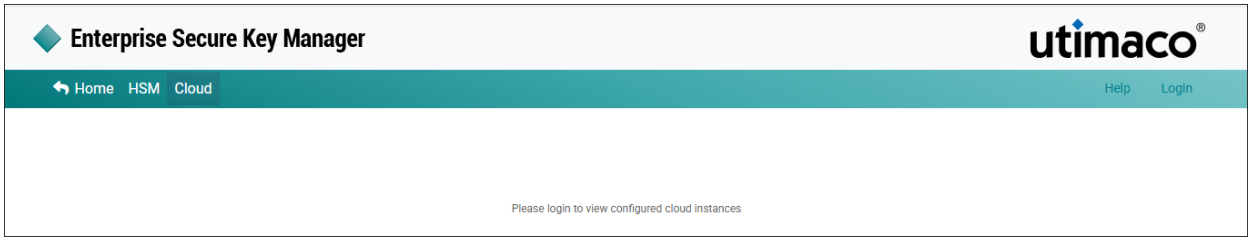

Figure 3 : Cloud Integration login

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

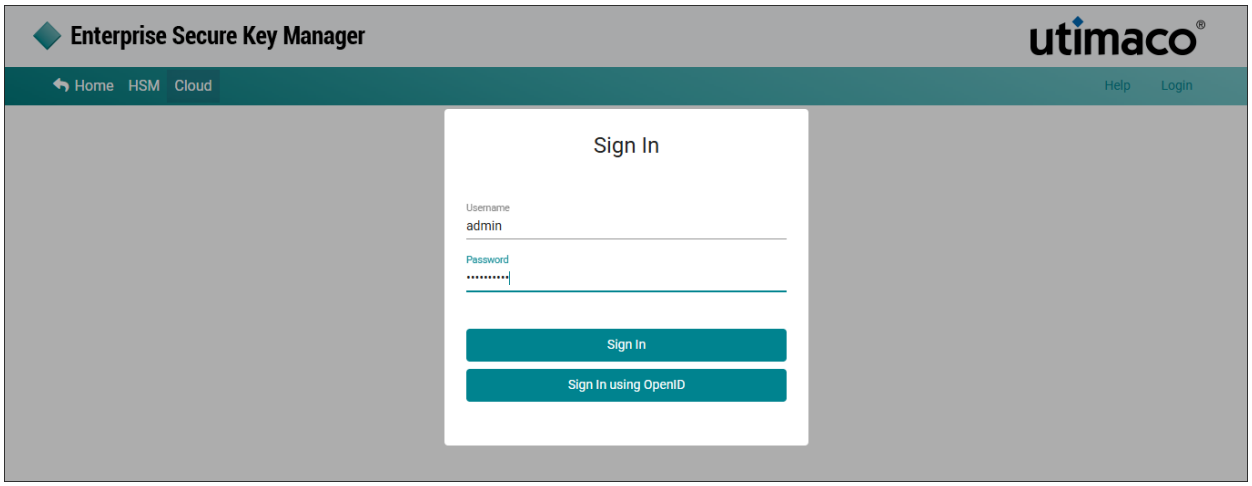

Figure 4 : Cloud Integration Sign In

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

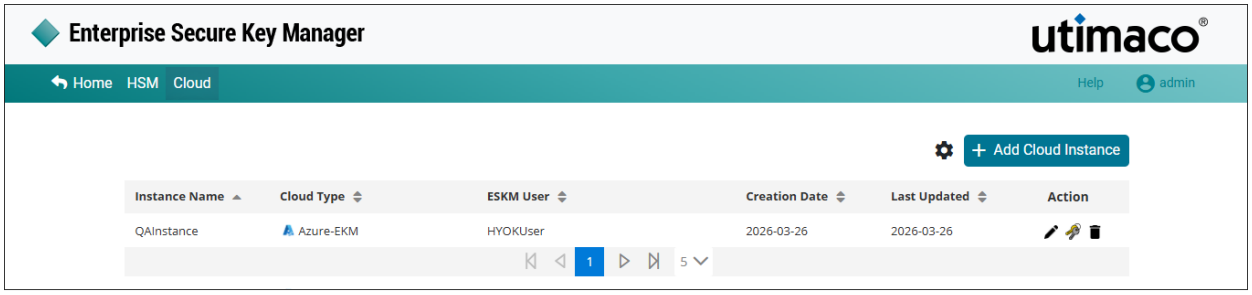

Figure 5 : Cloud ESKM-Logged In page

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, 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 the *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.

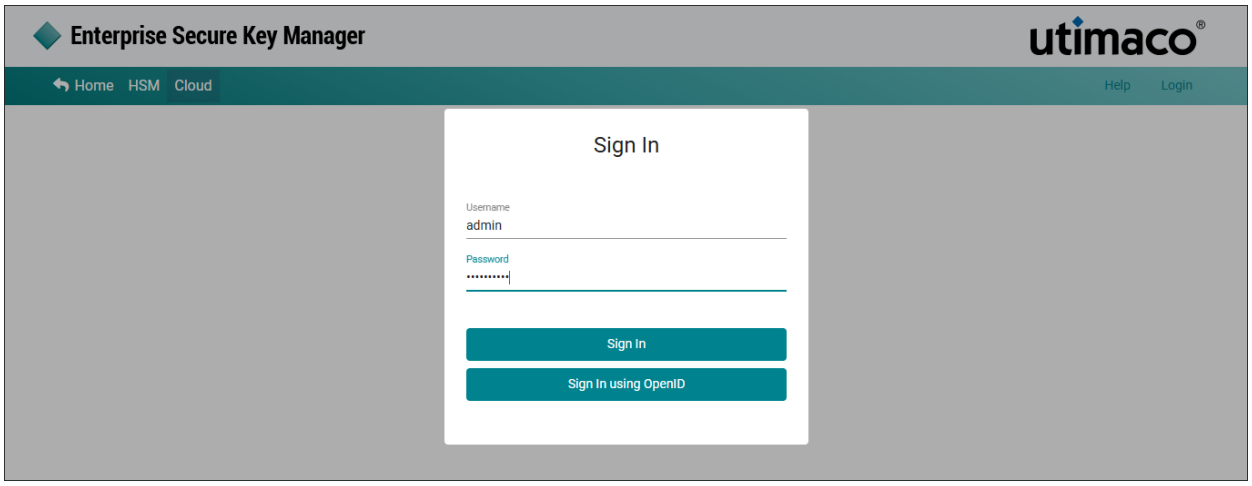

Figure 6 : Sign In Using OpenID

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

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

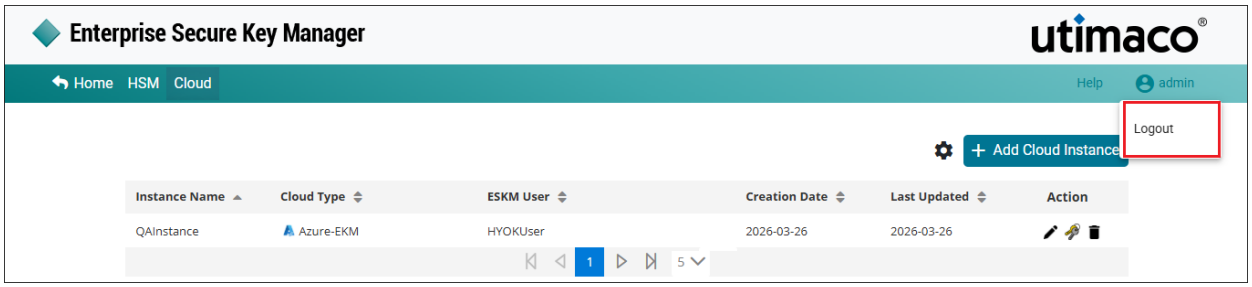

Figure 7 : Logout

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

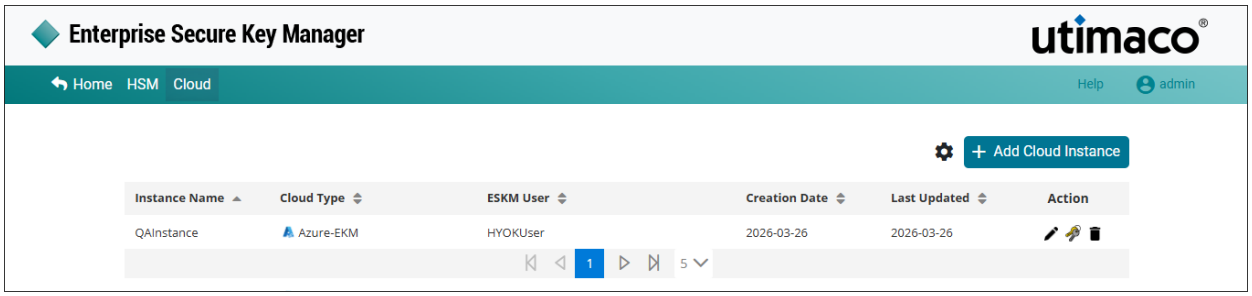

Figure 8 : Cloud Integration Dashboard

5 Integration Steps

5.1 Configuration on ESKM

This section describes the configuration required on ESKM to establish communication with Azure Key Vault Managed HSM External Key Management (EKM). The configuration includes:

- Import the Server Certificate.
- Add the Client Certificate CA as Known CA.
- Advanced REST Settings.
- Create Cloud Instance.
- Create Key.

5.1.1 Import the Server Certificate

This certificate serves as the server certificate for accessing the ESKM. The certificate must be a valid SSL server certificate.

Perform the following steps:

1. Go to **ESKM Management Console**.
2. Go to the **Security** tab and in the **Certificates & CA,** click **Certificates**.
3. In the **Import Certificate** section, select **Upload from browser** and **Choose File**.
4. Enter the **Certificate Name** and **Private Key Password**.
5. Click **Import Certificate**.

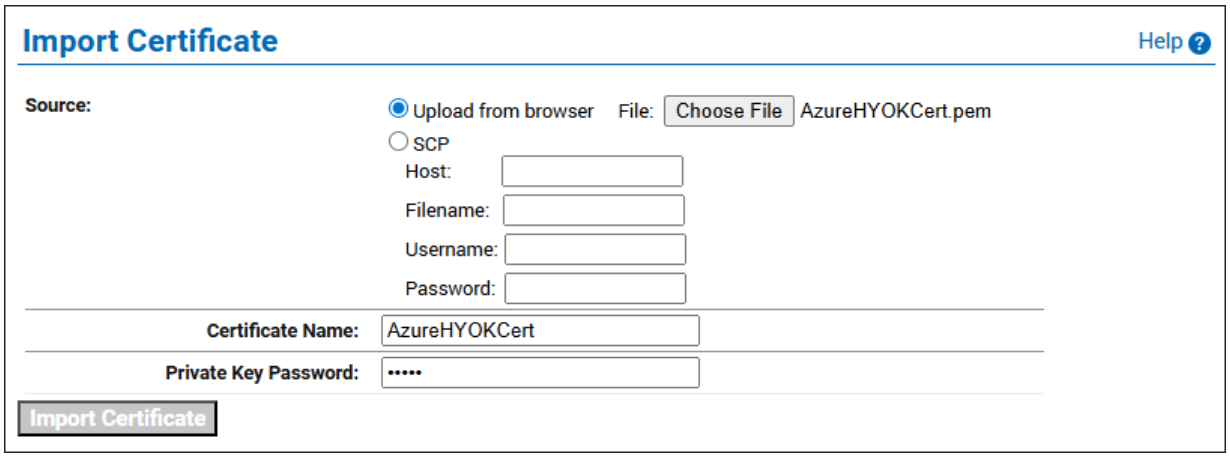

Figure 9 : Import Certificate

Make a note of the Certificate Authority (CA) certificate that issued the server SSL certificate. The CA certificate will be required later when configuring the Root CA Certificates in Azure Managed HSM External Key Management.

5.1.2 Add the Client Certificate CA as Known CA

- Go to **ESKM Management Console**.
- Go to the Security tab and in the Certificates & CA, click **Known CAs**.
- In the **Install CA Certificate** section, enter **Certificate Name** and **Certificate**.

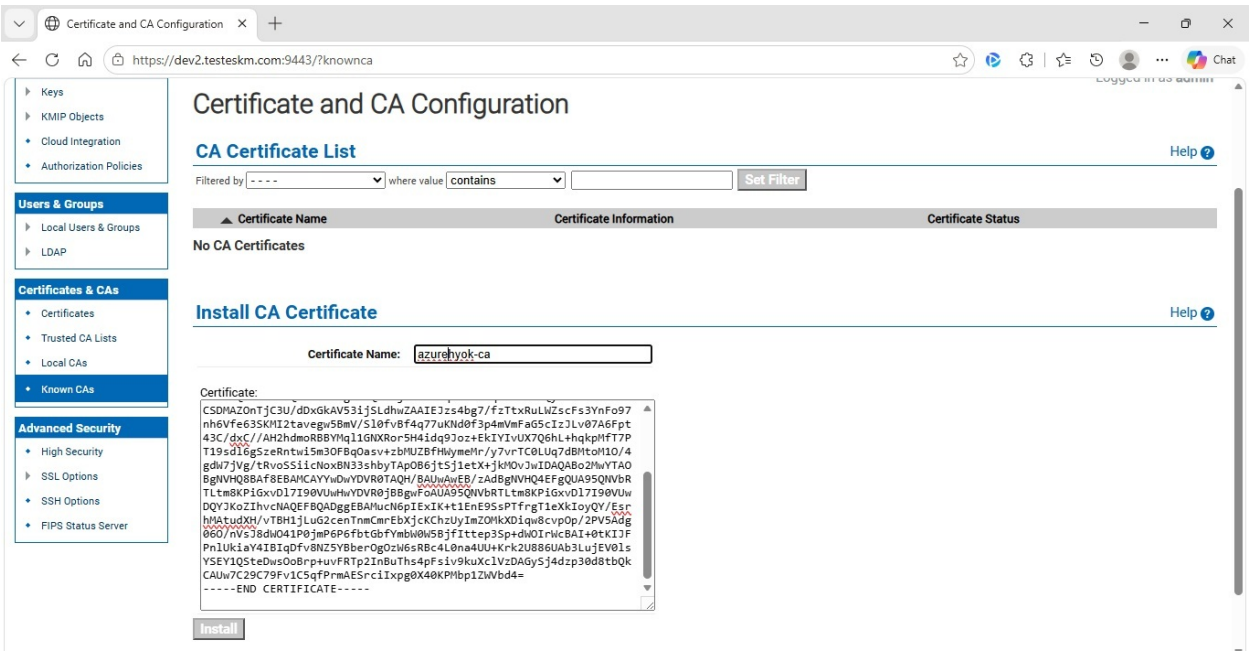

Figure 10 : Install CA Certificate

- Click **Install.** The CA Certificate is create under **CA Certificate List**.

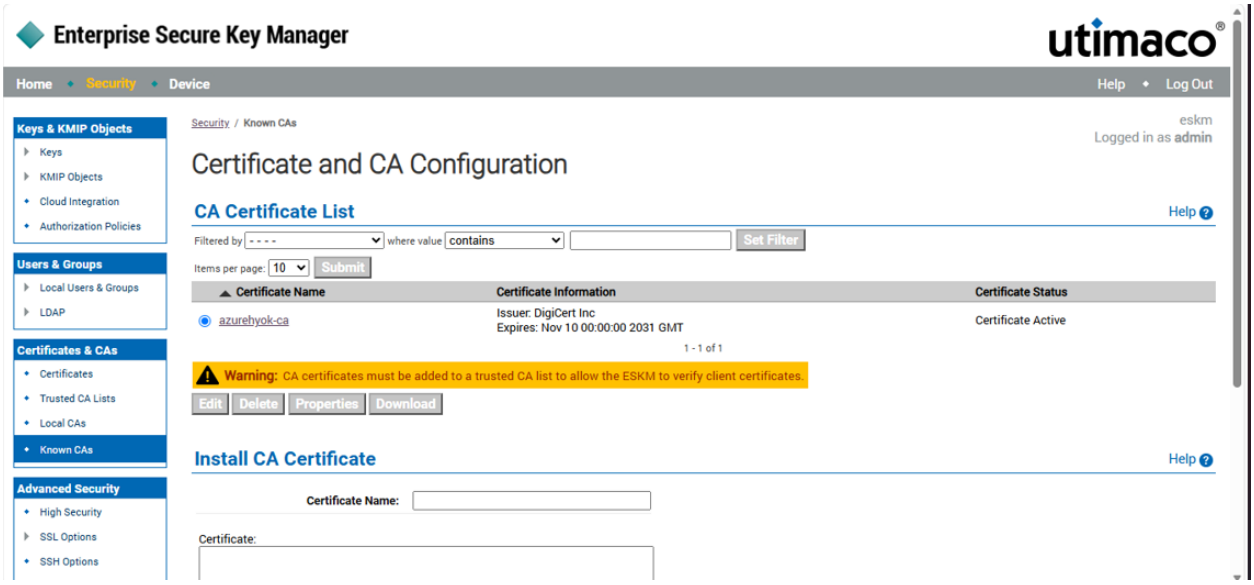

Figure 11 : CA Certificate List

5.1.3 Advanced REST Settings

- Go to **Device** > **Rest Server** > **Advanced REST Settings**. Click **Edit**.

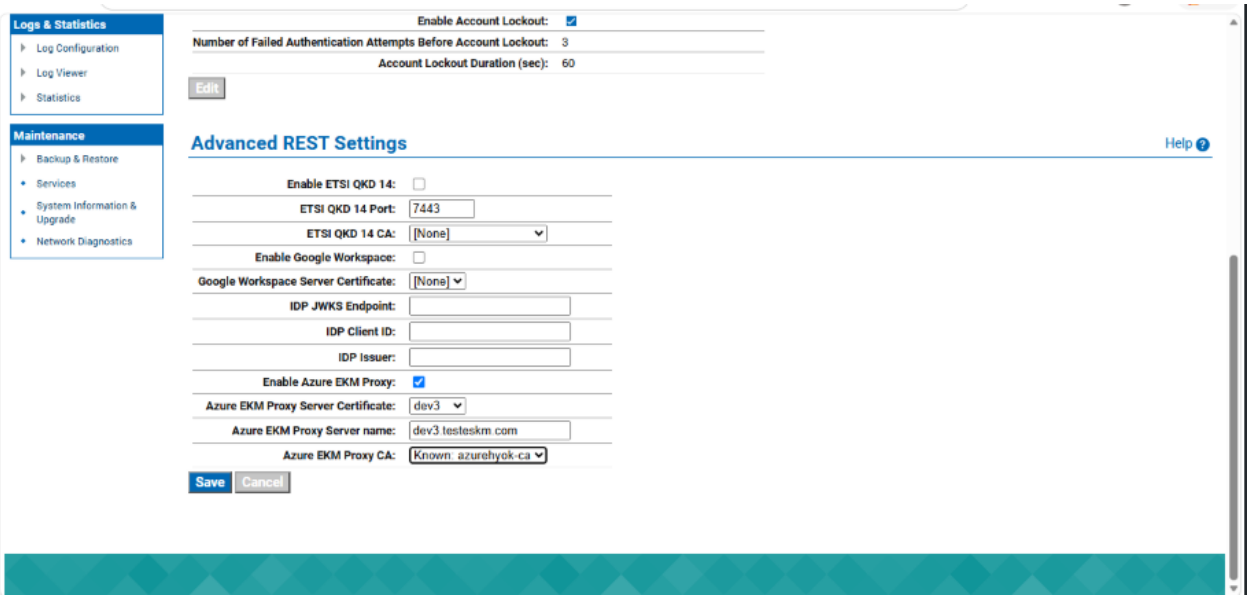

Figure 12 : Advanced REST Settings

- In the **Advanced Rest Settings** section, configure **Enable Azure EKM Proxy, Azure EKM Proxy Server Certificate, Azure EKM Proxy Server name, Azure EKM Proxy CA**.
  - **Azure EKM Proxy Server Certificate**: Select the Imported Server Certificate.
  - **Azure EKM Proxy Server Name**: Server Certificate Common Name.
  - **Azure EKM Proxy CA**: Select the created Local CA.
- Click on **Save**.

Component	Description
Enable Azure EKM Proxy	Indicates whether the Azure EKM Proxy Service is enabled or disabled.
Azure EKM Proxy Server Certificate	The server certificate to be used by the Azure EKM Proxy Service.

Component	Description
Azure EKM Proxy Server name	The host name used by clients to access the Azure EKM Proxy Service.
Azure EKM Proxy CA	The Certificate Authority (CA) used by the Azure EKM Proxy Service to validate client certificates presented to the server.

5.1.4 Create Cloud Instance

- Log in to the Cloud Integration Web Console using any one of the methods described in Accessing the Cloud Integration Web Console.

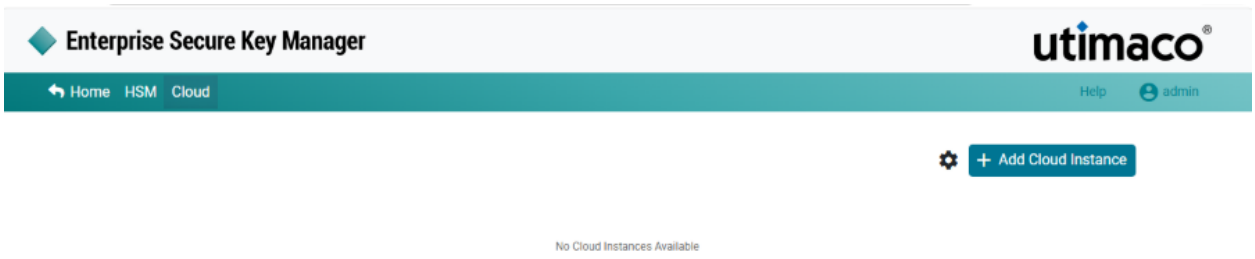

Figure 13 : Add Cloud Instance

- Click on the "**+ Add Cloud Instance**" icon at the top right corner of the page.
- The **Add Cloud Instance** pop-up window will appear.

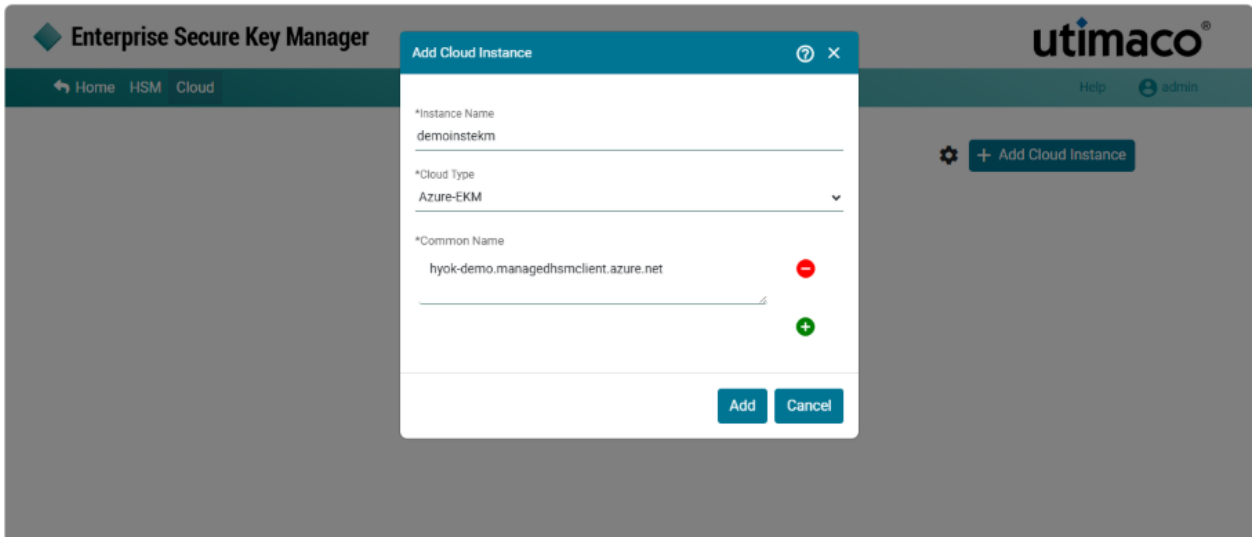

Figure 14 : Add Cloud Instance pop-up

- Enter **Instance Name**, **Cloud Type** and **Common Name** and click **Add**.

Ensure that the Common Name (CN) is the same as the Common Name defined in the client certificate.

5.1.5 Create Key

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

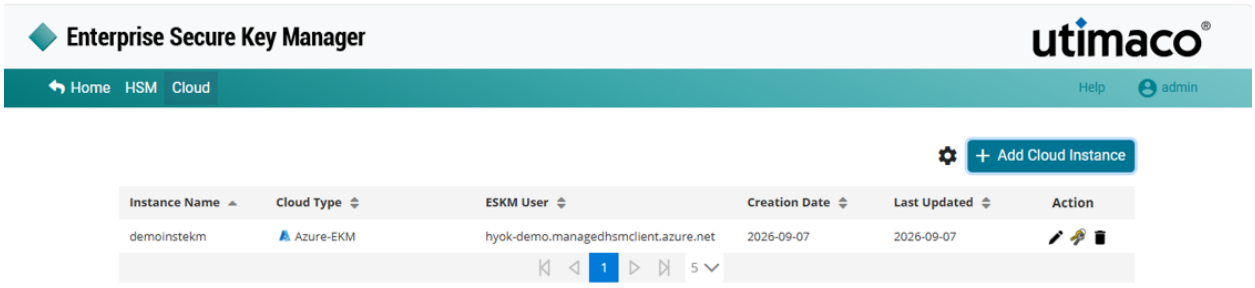

Figure 15 : Manage Keys

- The Keys List dashboard displays.

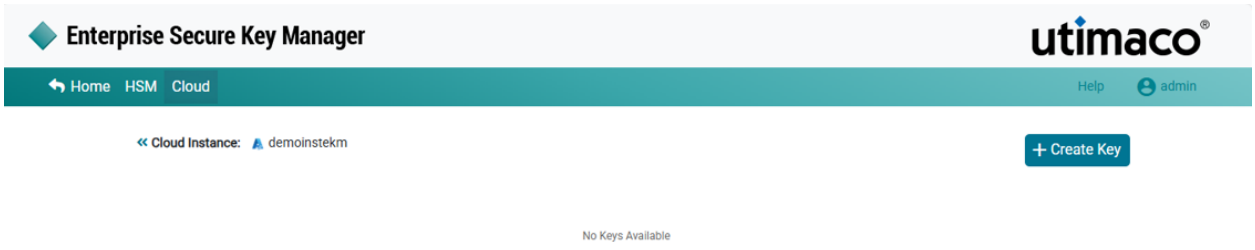

Figure 16 : Key List

- Click **Create Key** at the upper right corner of the page. In the **Create Key** window, enter **ESKM Key Name**, select Algorithm and select **ESKM Key Owner**.

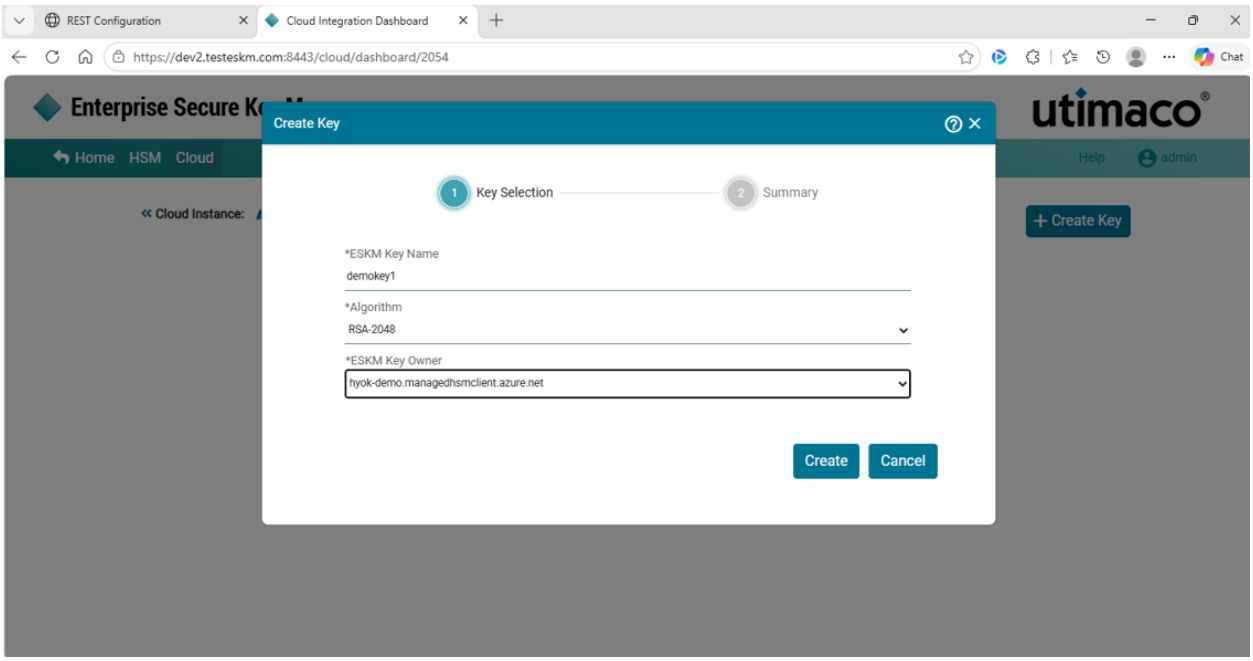

Figure 17 : Create Key

- The following window appears.

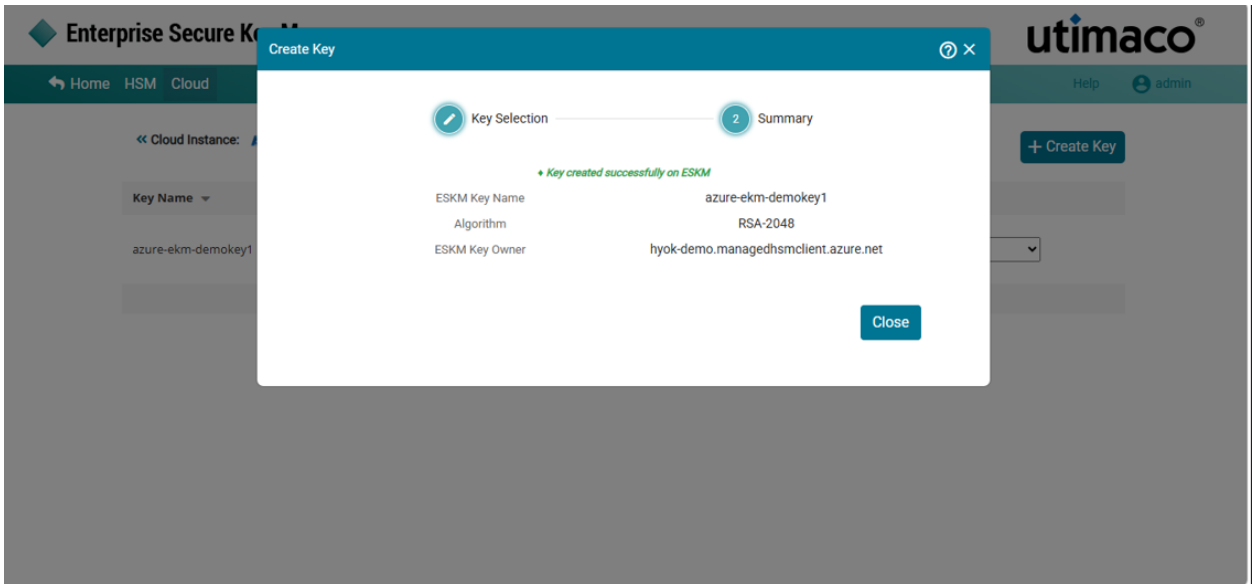

Figure 18 : Summary

- Click **Close**.

5.2 Configuration on Azure

- Navigate to Azure Key Vault Managed HSM → **External Key Management (Preview)**.

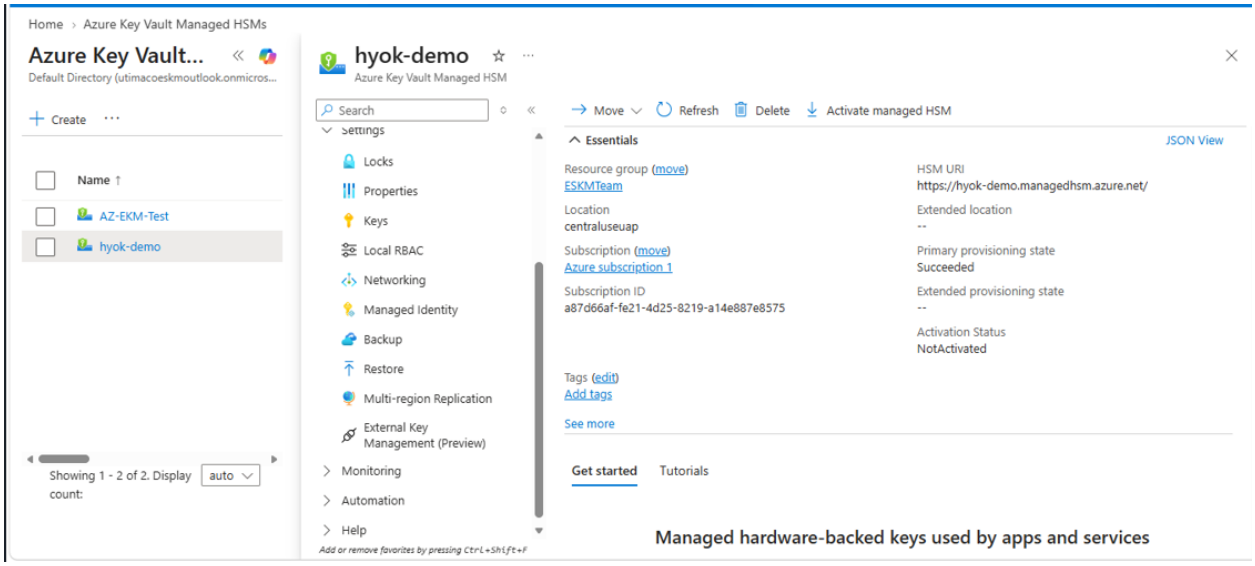

Figure 19 : Azure Key Vault Managed HSM instance

- In the **Client Certificate** section, note the **Subject Common Name** generated by Azure Managed HSM.

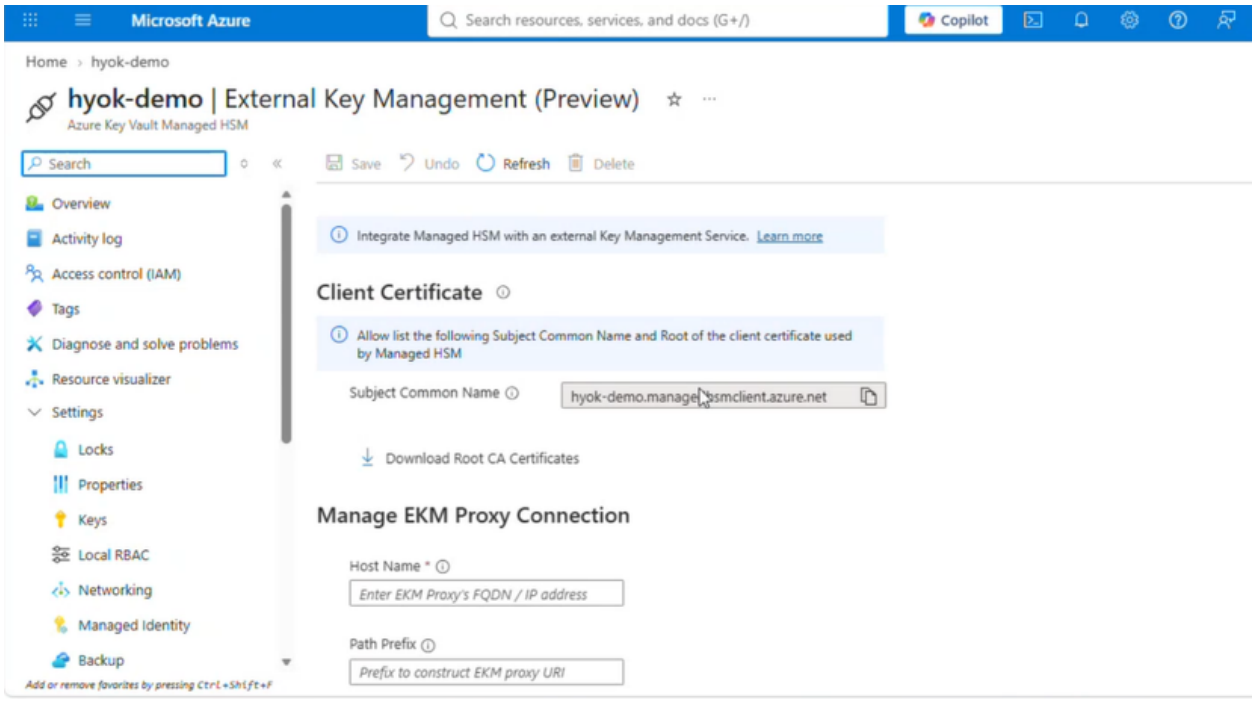

Figure 20 : Azure Managed HSM External Key Management

- Under **Manage EKM Proxy Connection**, specify the ESKM **Host Name** and **path prefix**.
- Provide the **Server Subject Common Name** and upload the required **Server Root CA certificate(s)**.
- Click on **Save** to create the EKM connection.

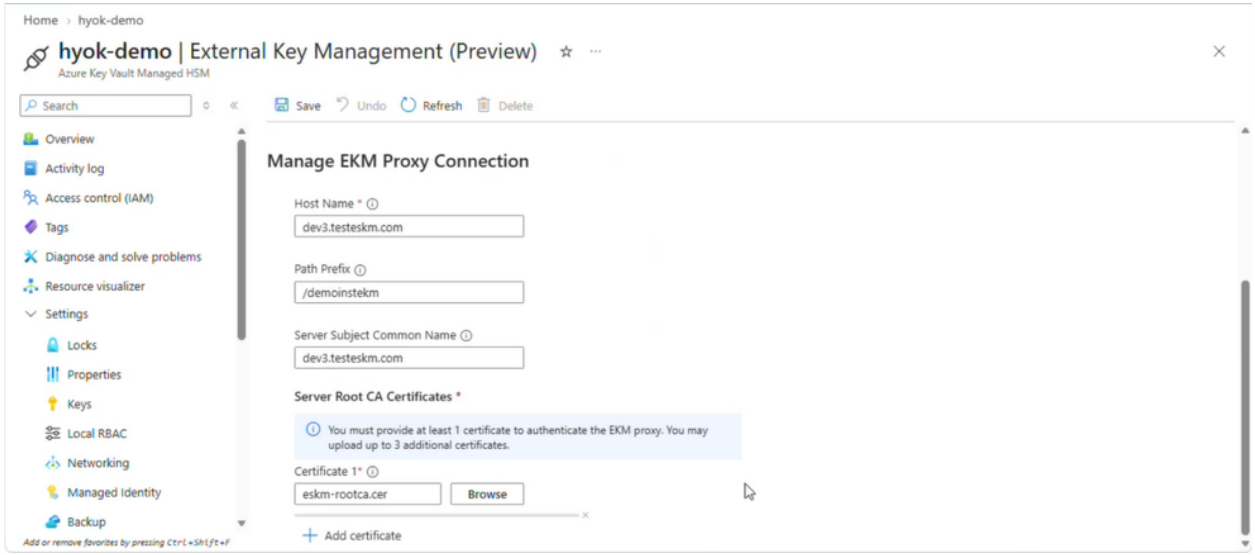

Figure 21 : Configuring the Azure Managed HSM External Key Management connection

- Verify that the **Connection Status** is displayed as successful.

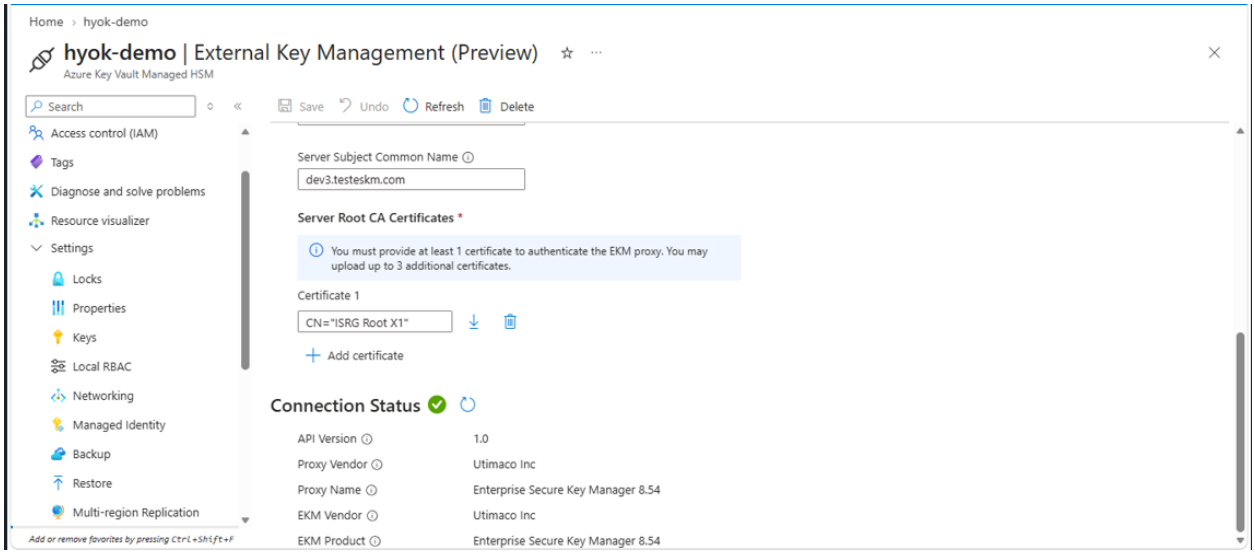

Figure 22 : Azure Managed HSM EKM connection status

5.2.1 Adding Key in Azure

- Navigate to **Keys** and click **Generate/Import/Restore Backup**.

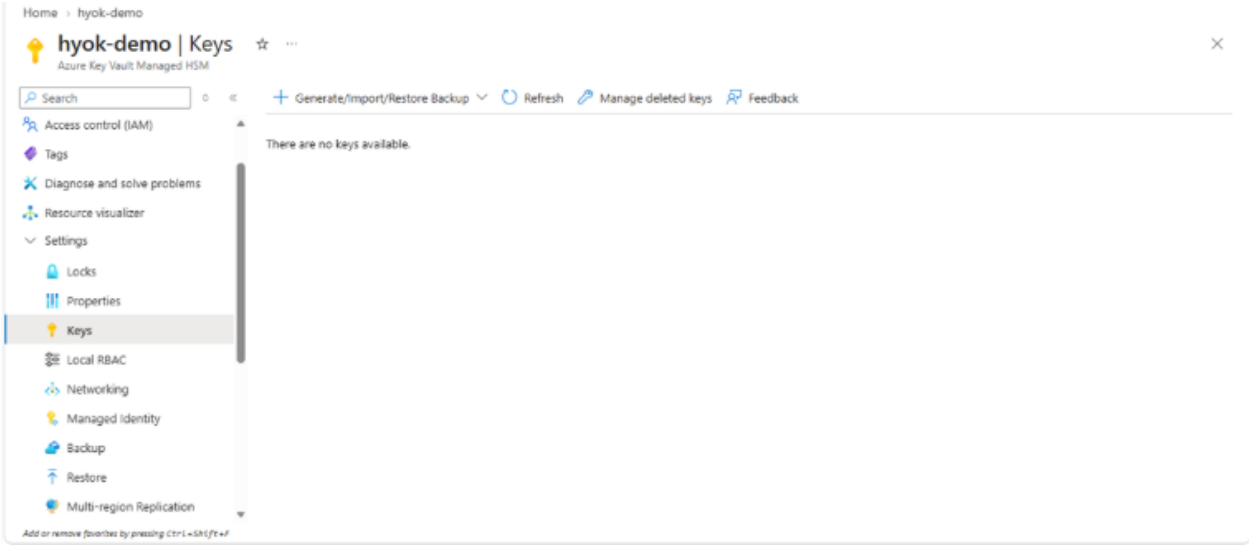

Figure 23 : Azure Managed HSM Keys page

- Select **Generate external key** from the **Options** drop-down list.
- Enter a unique **Name** for the key.
- Specify the **External key identifier** corresponding to the key configured in ESKM.
- Optionally configure the activation and expiration dates.
- Ensure that the key is **Enabled**.
- Click **Create**.

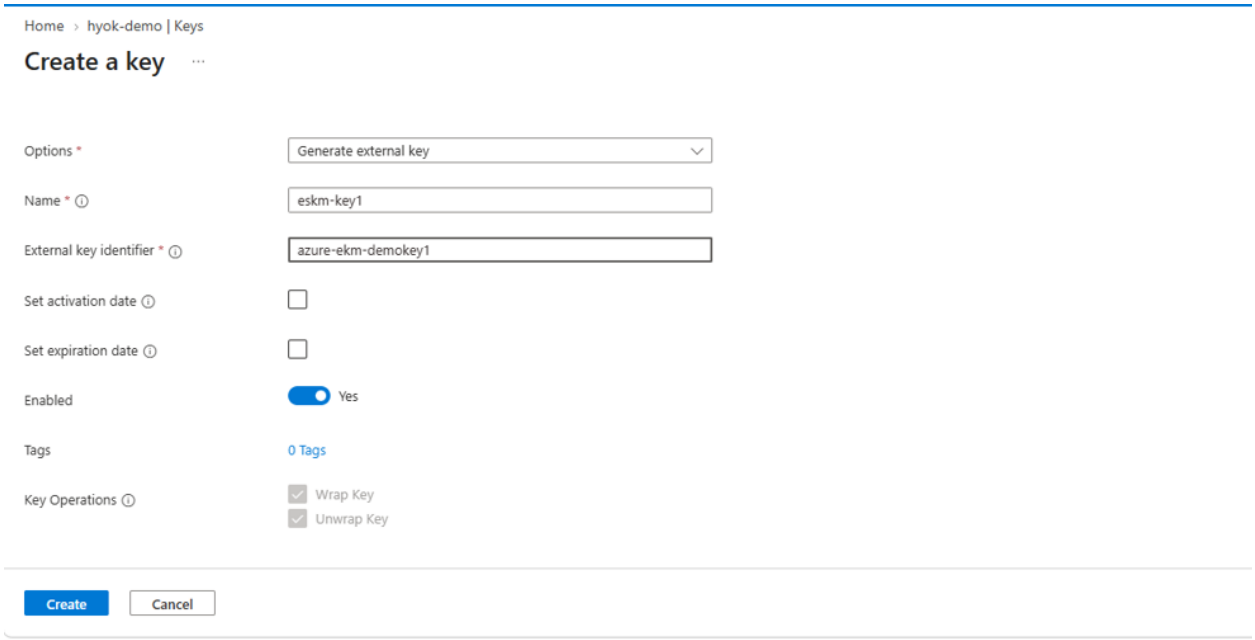

Figure 24 : Creating an external key in Azure Managed HSM

5.2.2 Wrapping/Unwrapping in a Key

After creating the external key, verify that key wrap and unwrap operations are functioning. Refer to the Microsoft documentation,*"Quickstart: Create your first external key in Azure Key Vault Managed HSM using the Azure CLI (Preview)"* .

To confirm that the operations were successfully processed by ESKM, review the ESKM REST log by navigating to: **Device** > **Logs & Statistics** > **Log Viewer** > **REST** .

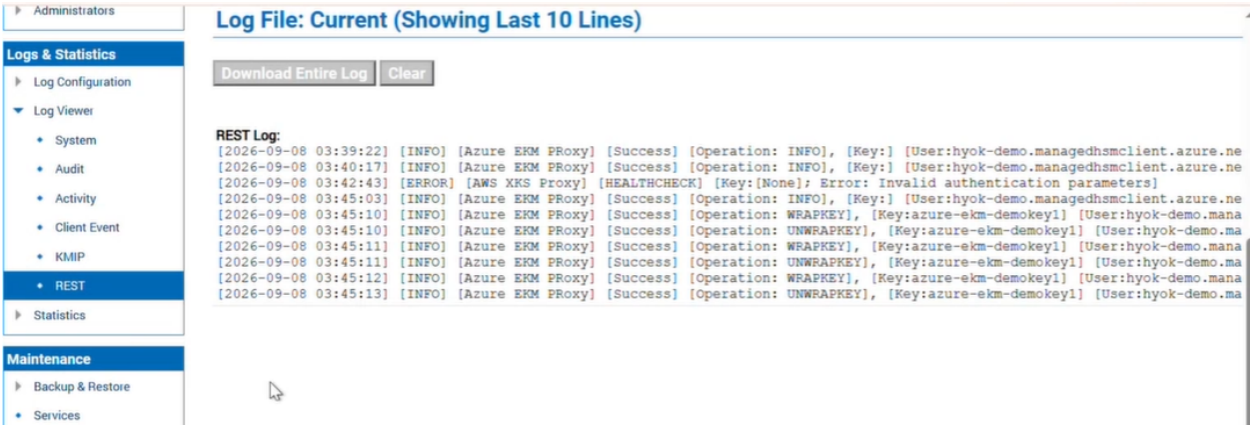

Figure 25 : Successful WRAPKEY and UNWRAPKEY operations in the ESKM REST log

6 Verification and Testing

6.1 Logs and Validation Steps

- In the **ESKM Management Console** > **Security** > **Local Groups**. Verify that the Local Groups are created.

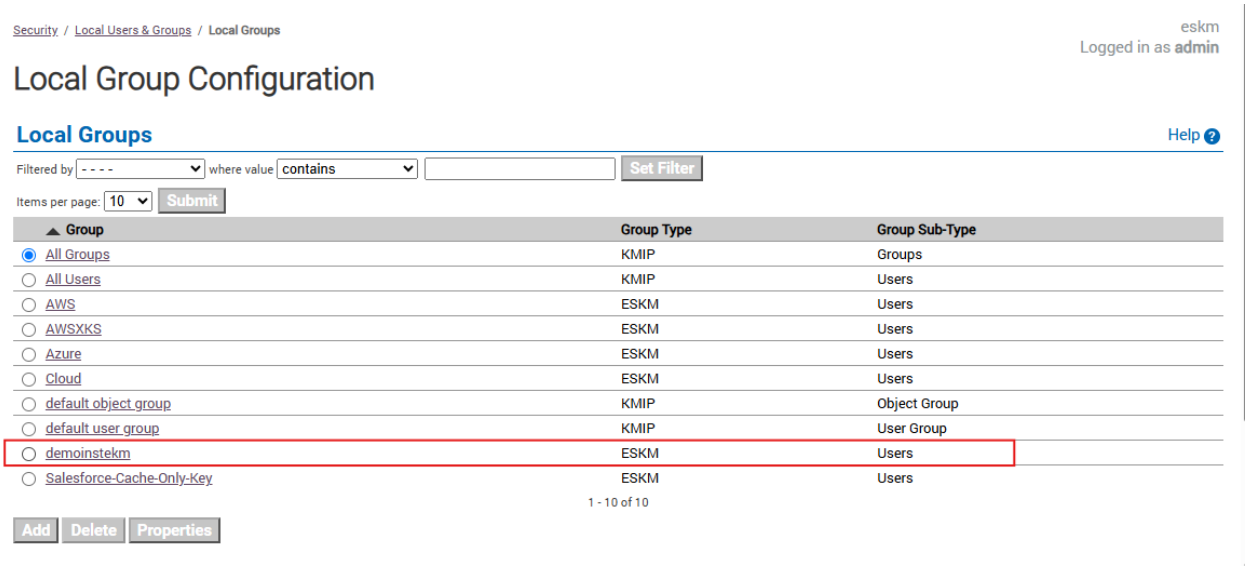

Figure 26 : Local Groups

- In the **ESKM Management Console** > **Security** > **Local Users**. Verify that the Local User is created.

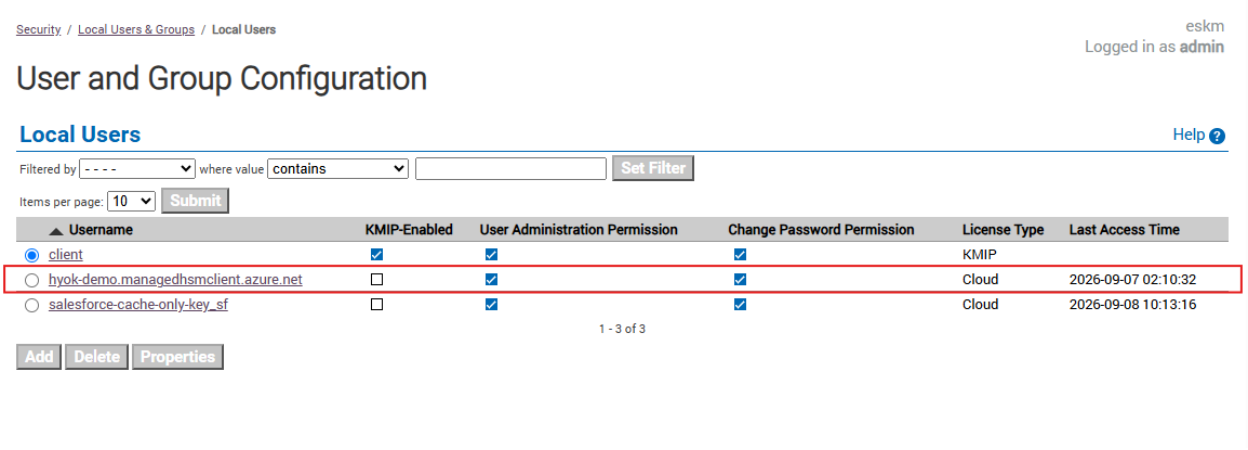

Figure 27 : Local Users

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

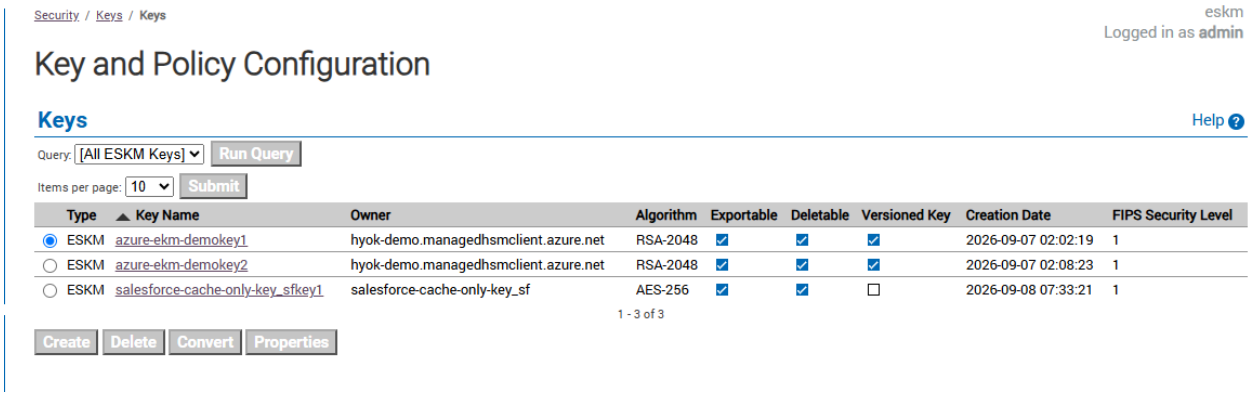

Figure 28 : Key List

- After creating the external key, navigate to **Device** → **Log Viewer** → **REST** in Utimaco ESKM.

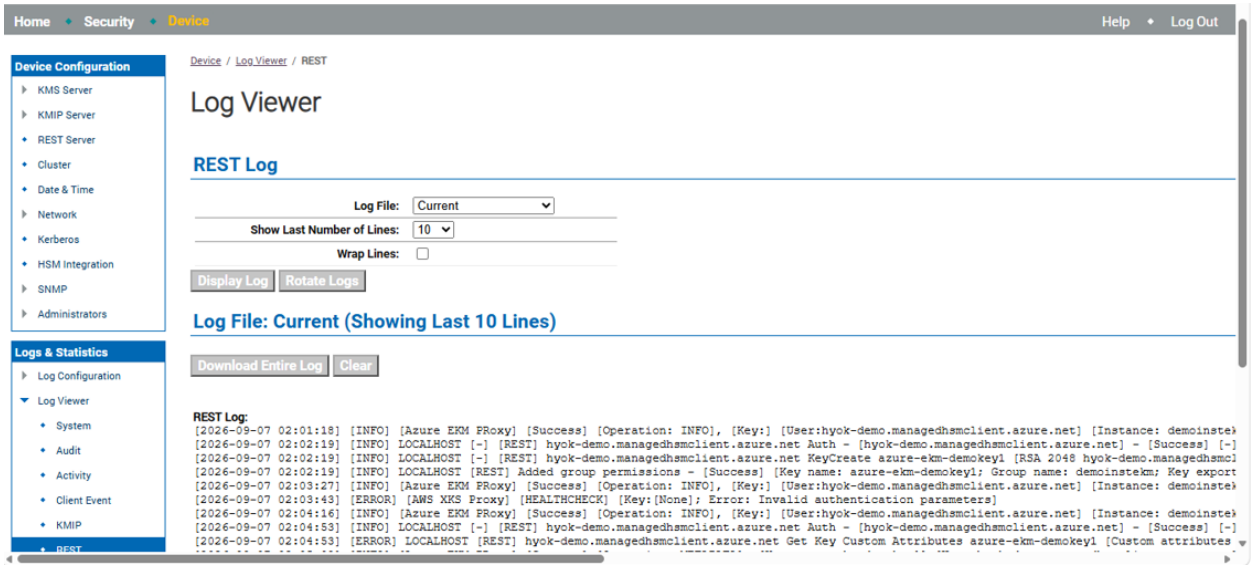

Figure 29 : Utimaco ESKM REST logs showing successful external key creation

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**.

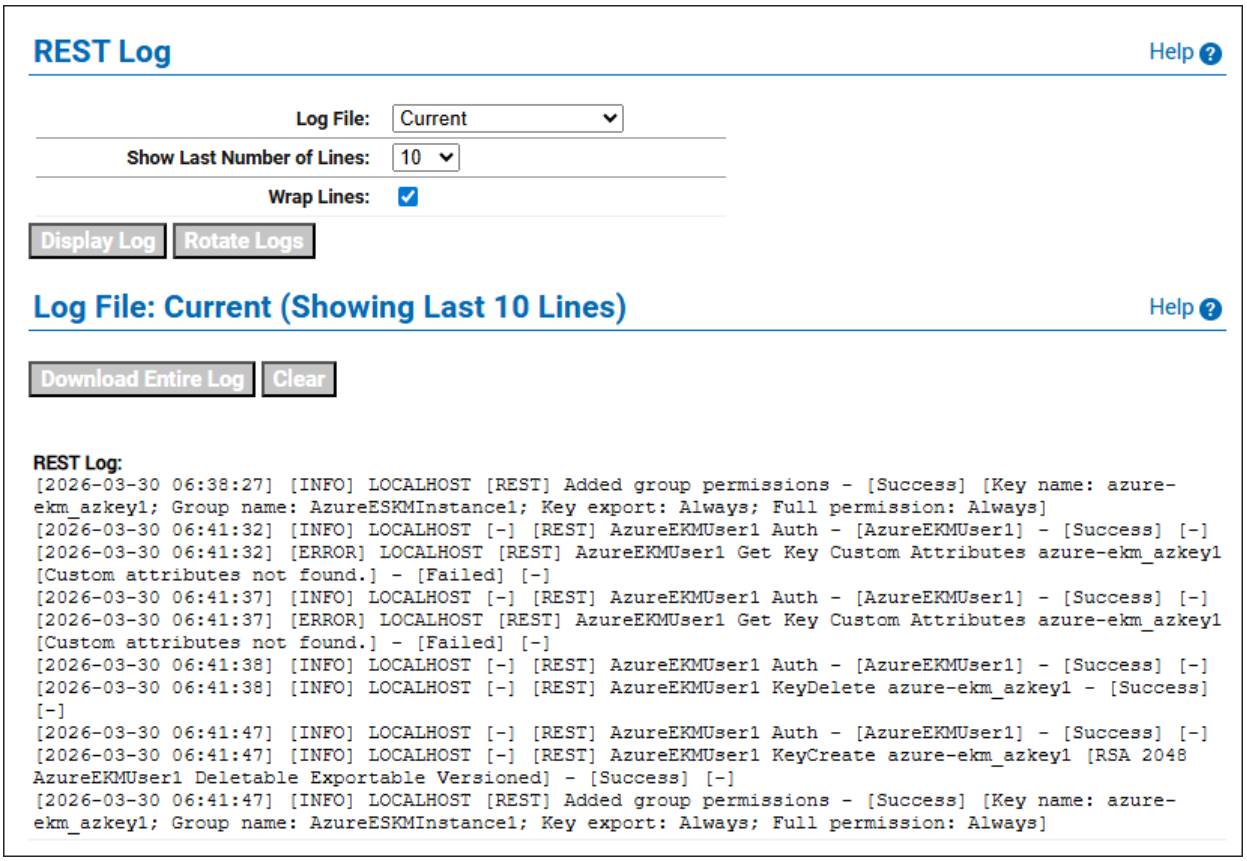

Figure 30 : Rest Log

8 Contact and Support Information

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

Utimaco IS GmbH
Krefelder Straße 220
52070 Aachen
Germany

RMA Query

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

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

Other Support Queries

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

9 Appendices

9.1 References

Title	Description	Document/Link
Azure Key Vault Managed HSM Quickstart	Provides instructions for provisioning and activating an Azure Key Vault Managed HSM instance.	https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/quick-create-portal?source=recommendations
Azure Managed HSM External Key Quickstart	Provides instructions for creating an external key and verifying wrap and unwrap operations.	https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/external-key-management-quickstart-cli#verify-wrapunwrap

Table 5: References