Microsoft Azure

DKE

Integration Guide

ESKM

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	2026-03-17
Status	PUBLISHED
Document No.	IG-2026-0009

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 Introduction 4
1.1 About this Guide 4
1.1.1 Intended Audience 5
1.2 Prerequisites 5
2 Accessing the Cloud Integration Web Console 6
3 Cloud Settings 9
4 Microsoft DKE Integration 12
4.1 Adding a Microsoft DKE Cloud Instance 12
4.2 Editing a Microsoft DKE Cloud Instance 14
4.3 Deleting a Microsoft DKE Cloud Instance 15
4.4 Creating a Key on Microsoft DKE 16
4.5 Editing a Microsoft DKE key 18
4.6 Deleting a Microsoft DKE Key 19
4.7 Create New Version 19
4.8 Viewing Microsoft DKE Key Information 21
5 Microsoft Azure DKE API Commands 24
6 Contact and Support Information 25

1 Introduction

Enterprise Secure Key Manager (ESKM) can be used as an external key manager for Microsoft Double Key Encryption (DKE) to provide enhanced data protection and key control. In this setup, Microsoft manages one encryption key, and the second key is securely stored and managed in ESKM by the organization.
When a user opens DKE-protected content in Microsoft 365, the DKE service connects to ESKM to request access to organization's key. ESKM authorizes the request and allows decryption only if the organization approves it. This ensures that Microsoft cannot access the protected data without the organizations consent.

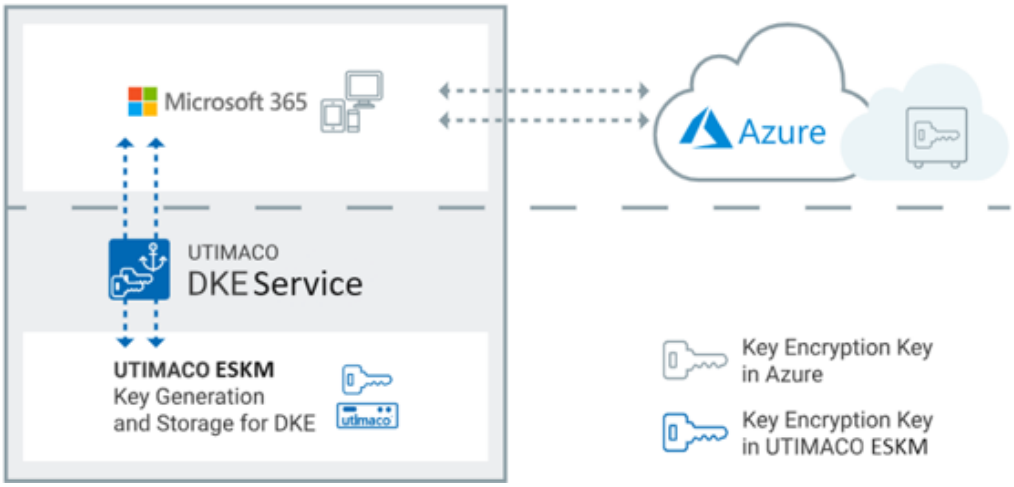


Figure 1 : Azure DKE

Using ESKM as the external key manager allows organizations to:

- Maintain full control over encryption keys.
- Enforce internal security and access policies.
- Meet compliance and data requirements.

1.1 About this Guide

This guide outlines the following features:

- Accessing the Cloud Integration Web Console
- Cloud Settings
- Microsoft DKE Integration

- Microsoft Azure DKE API Commands

1.1.1 Intended Audience

This guide is intended for Microsoft DKE administrators.

1.2 Prerequisites

Before using ESKM Cloud, make sure that the following prerequisites are met:

- ESKM version must be ESKM 8.52 or higher.
- Host ESKM Publicly.
- Register Domain name for the ESKM and configure it as audience (Rest Certificate CN) in 'Cloud Settings'.
- Valid SSL certificate, signed by a trusted external CA - import to ESKM and configure it in 'REST Server Settings'.
- Enable Microsoft DKE Service in the Cloud Settings.



Refer to the Microsoft DKE-Utimaco ESKM Integration Supplement for additional prerequisites.

2 Accessing the Cloud Integration Web Console

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

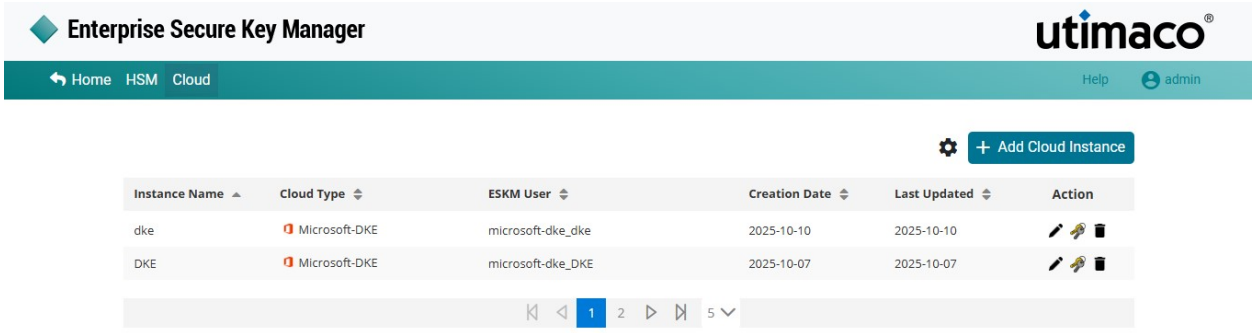


Figure 2 : Cloud integration dashboard

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

The following screen appears.

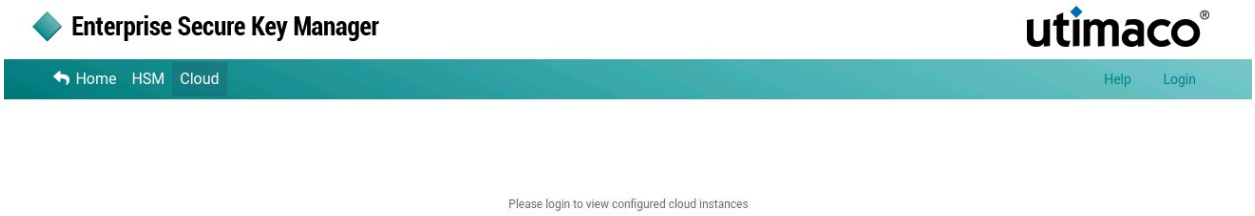


Figure 3 : Cloud Integration login

Click Login at the top right corner of the page.

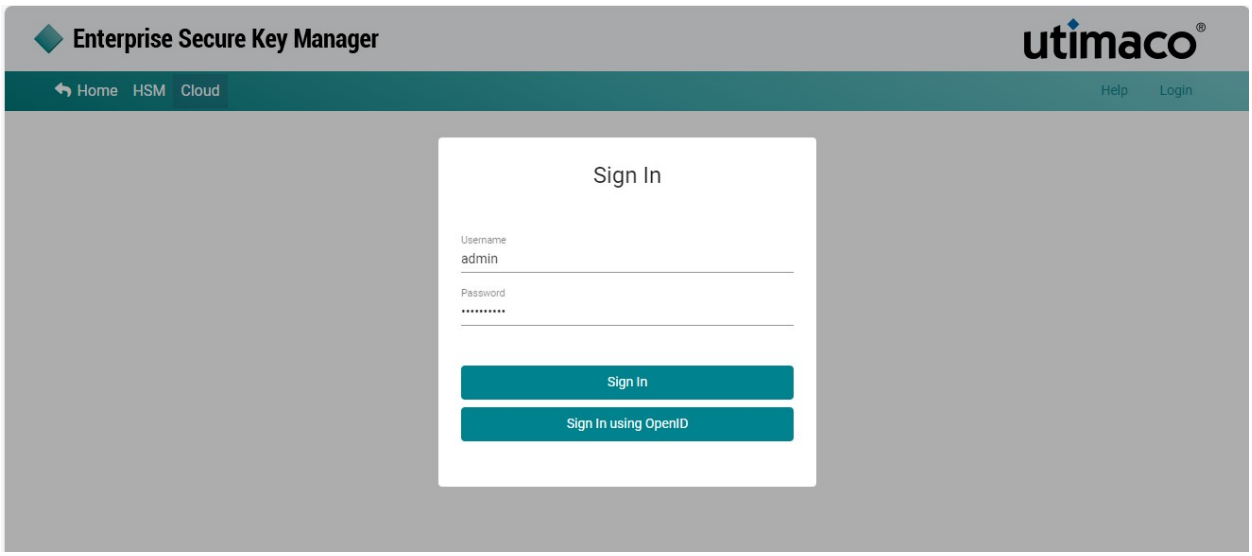


Figure 4 : Cloud Integration sign-in

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

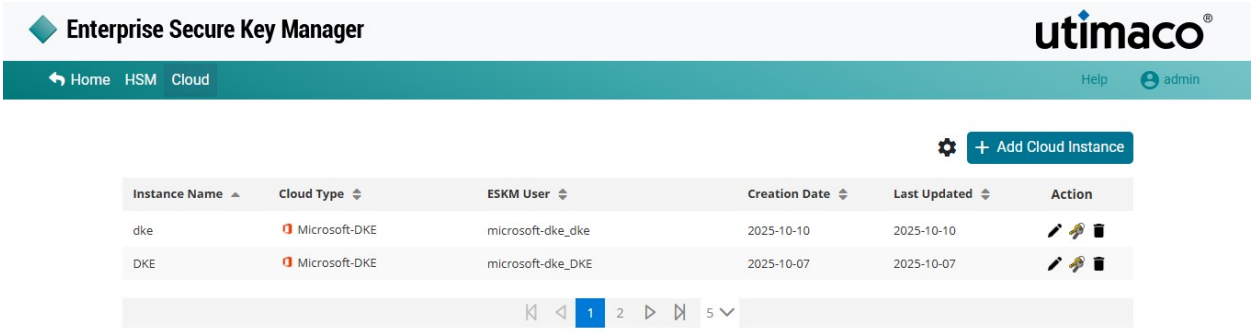


Figure 5 : Cloud ESKM log-in page

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_8.54.0.

To sign in using OpenID

Click Sign In using OpenID without user credentials.

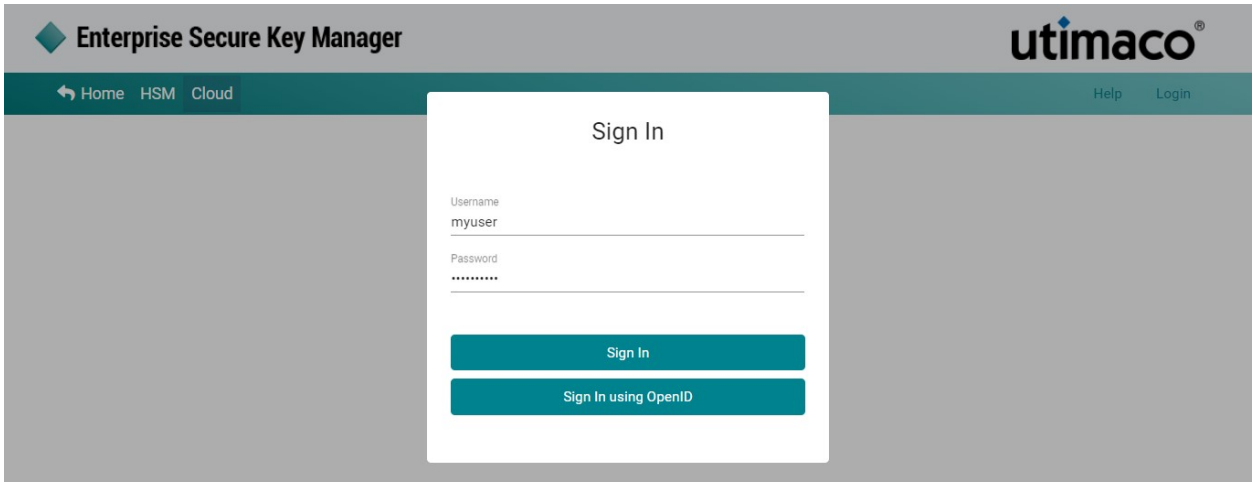


Figure 6 : Sign-in using OpenID

- You will be navigated to the Open ID Provider. Enter Username and Password. Click Sign In.
- The Cloud Integration Dashboard is displayed.

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

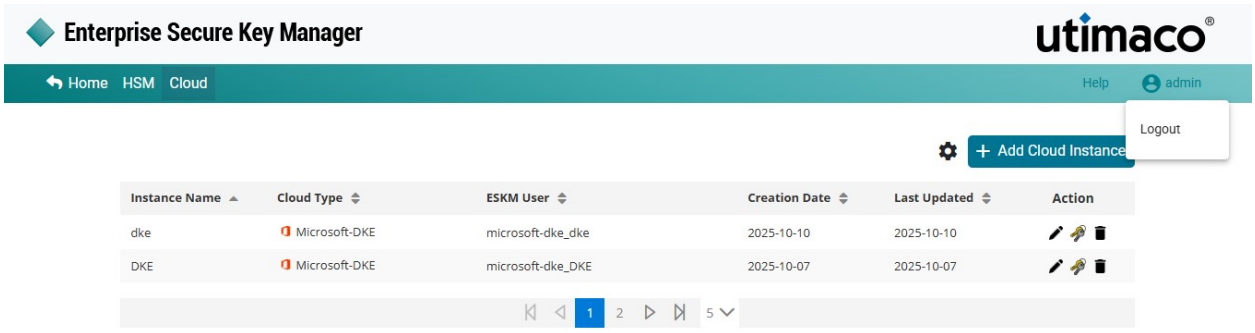


Figure 7 : Logout

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

3 Cloud Settings

This section describes the procedure to enable ESKM cloud settings.

To enable cloud settings

- Click the Settings icon on the Cloud dashboard.

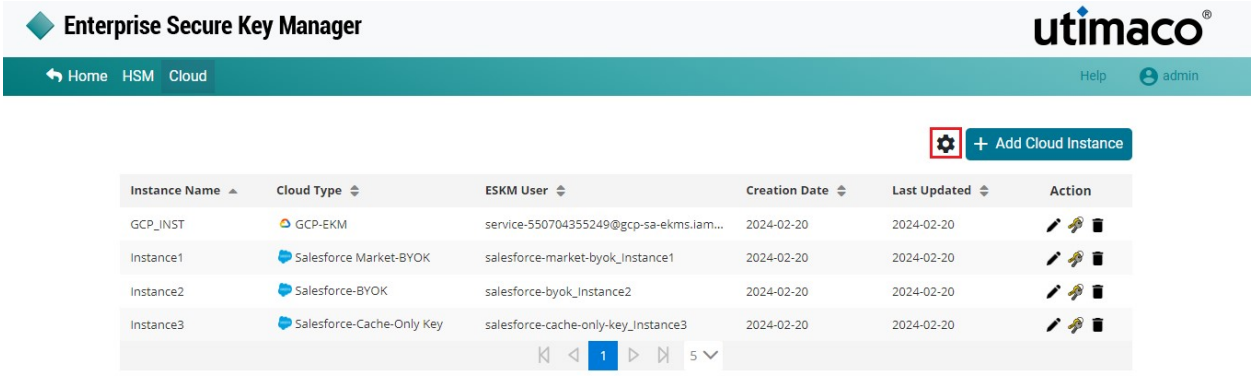


Figure 8 : Cloud settings

- The Settings pop-up window will appear.

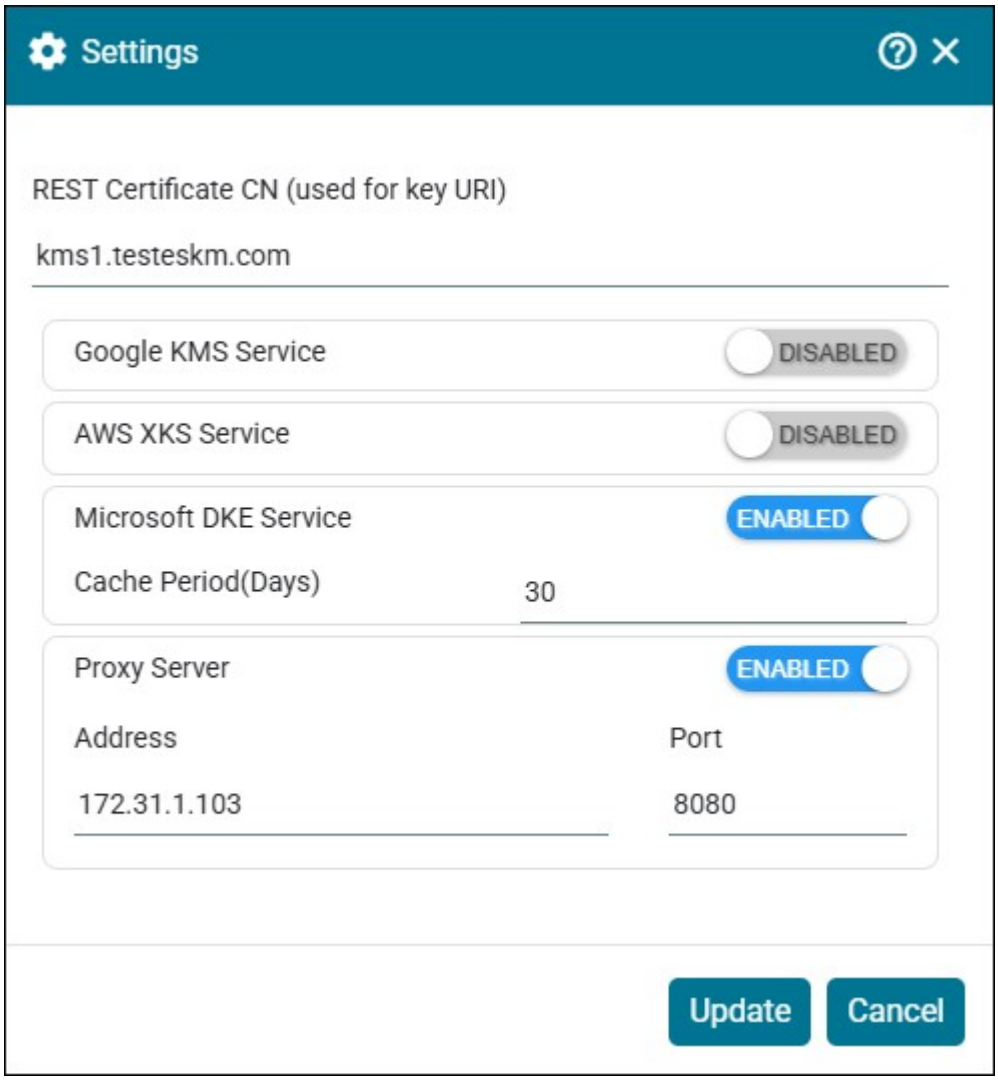


Figure 9 : Microsoft DKE - Cloud Settings

By default, cloud services are disabled; users must enable cloud settings as required.

- Enable the Microsoft DKE Service and Proxy Server. Click Update.

Parameters	***Description***
Microsoft DKE Service	Enable the Microsoft DKE Service to integrate Microsoft DKE with ESKM.

Parameters	***Description***
Cache Period(s)	Cache period refers to the number of days a key is stored (Cached) by the client. During this period, the key can be used without requiring ESKM availability until it expires.
Proxy Server	Enable this to configure Proxy Server with address and port number for internet access.

Table 1: Settings - Parameters

4 Microsoft DKE Integration

4.1 Adding a Microsoft DKE Cloud Instance

This section describes the procedure to add a new cloud instance for Microsoft DKE.

To add new Microsoft DKE Cloud Instance:

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

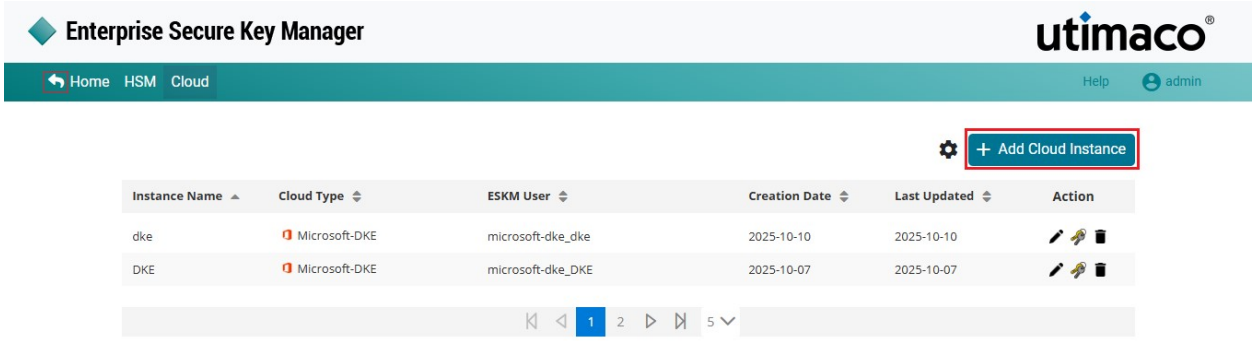


Figure 10 : Microsoft DKE Cloud Instance

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

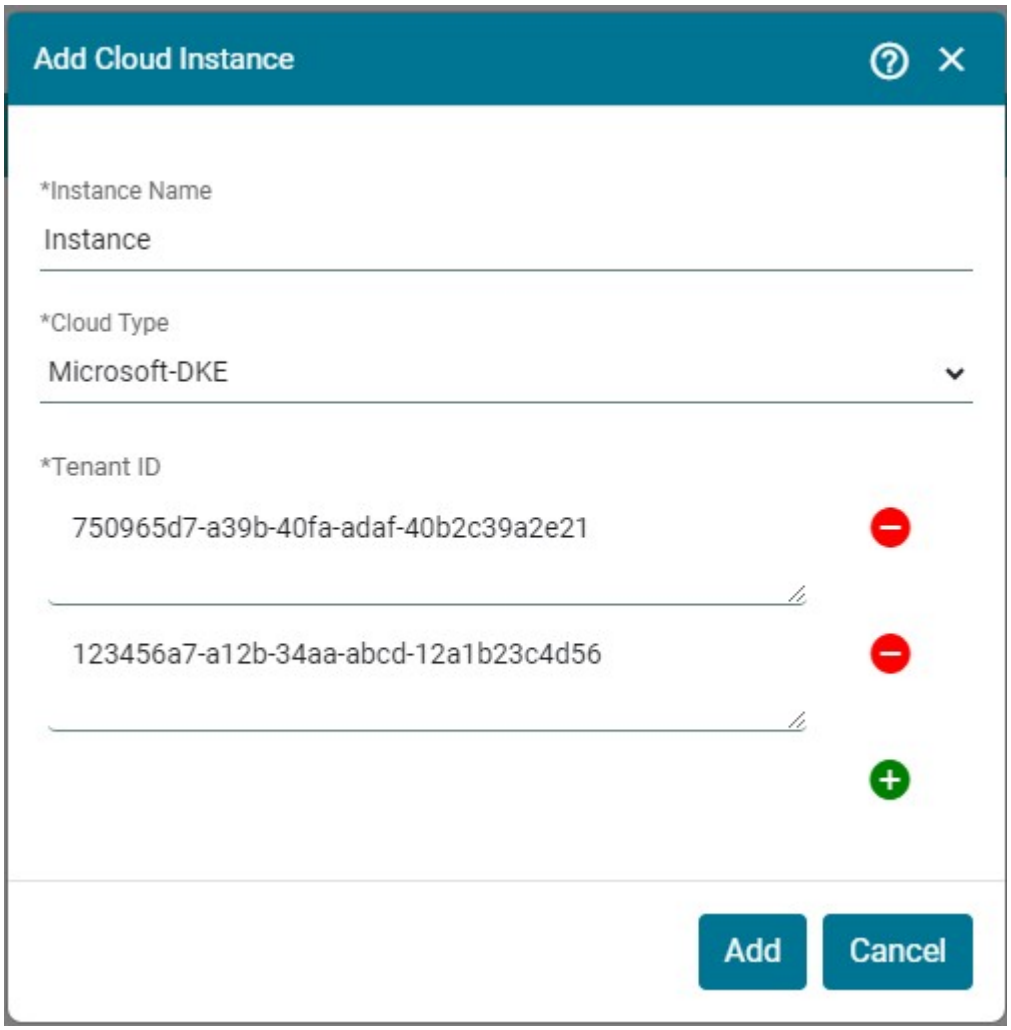


Figure 11 : Add Cloud Instance

- Enter the Instance Name, select Microsoft DKE as the Cloud Type, and then enter the Tenant ID created in Microsoft DKE.

Cloud Instance [Instance Name] Microsoft DKE created successfully.

Parameters	***Description***
Instance Name	Name of the Instance

Parameters	Description
Cloud Type	The cloud provider with which ESKM is integrated. ere select cloud type as a Microsoft DKE.
Tenant ID	Tenant ID for the Azure cloud account being used for DKE integration. Search for Tenant Properties in the azure portal to get the tenant ID. You can add multiple tenant IDs to a single Instance.

Table 2: Add Microsoft DKE Cloud Instance - parameters

4.2 Editing a Microsoft DKE Cloud Instance

This section describes the procedure to edit Microsoft DKE Cloud Instance.

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

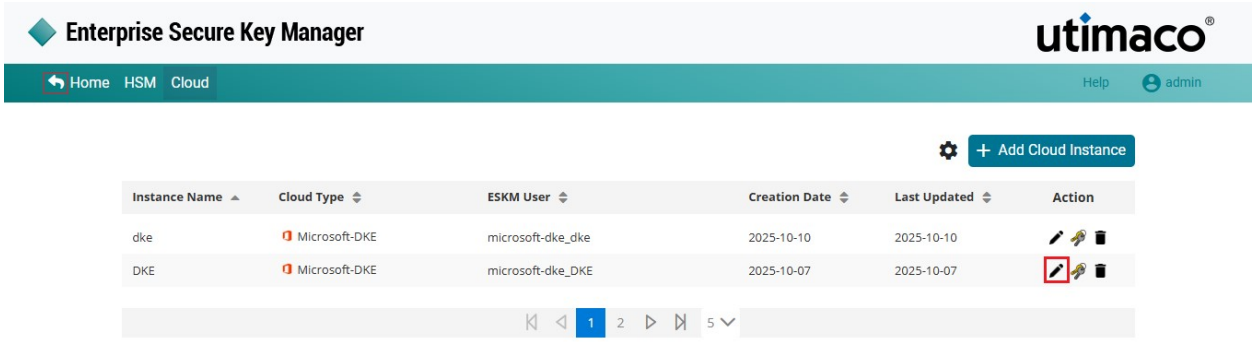


Figure 12 : Edit Key

- The Edit Cloud Instance pop-up window appears.

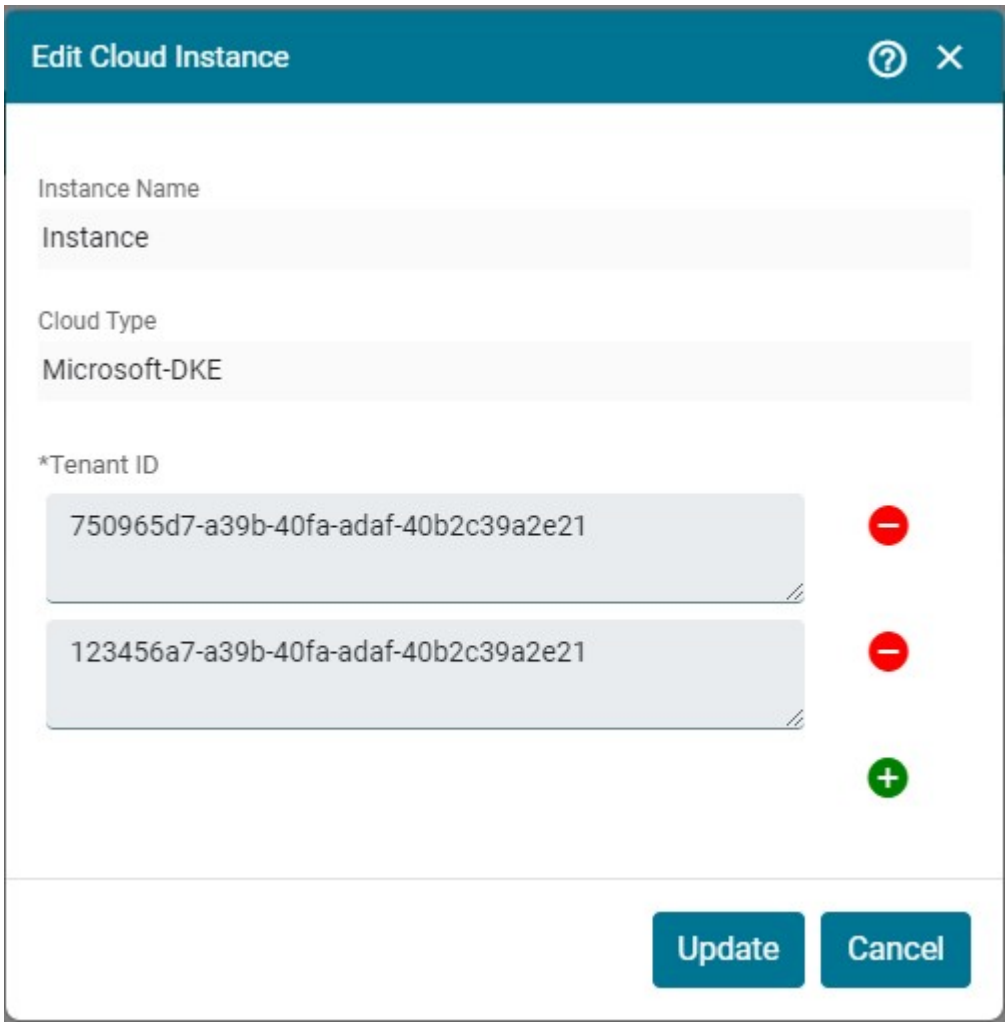


Figure 13 : Edit Cloud Instance

- Make the necessary changes and click Update.

Cloud Instance Instance Name [Microsoft-DKE] updated successfully.

4.3 Deleting a Microsoft DKE Cloud Instance

This section describes the procedure to delete Microsoft DKE cloud instance.

To delete a Microsoft DKE cloud instance:

- Under Action column, click Delete icon to delete existing Microsoft DKE cloud instance.

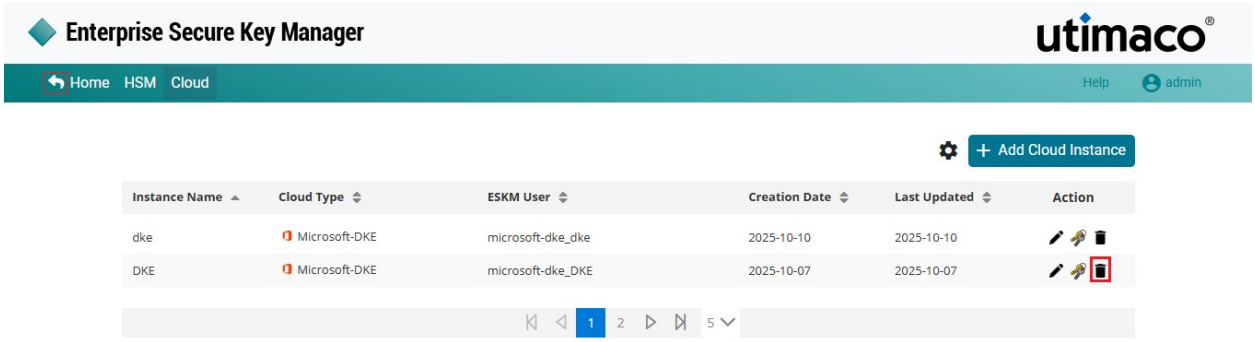


Figure 14 : Delete Cloud Instance

- 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[Microsoft DKE] deleted successfully.

4.4 Creating a Key on Microsoft DKE

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

To create a new key

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

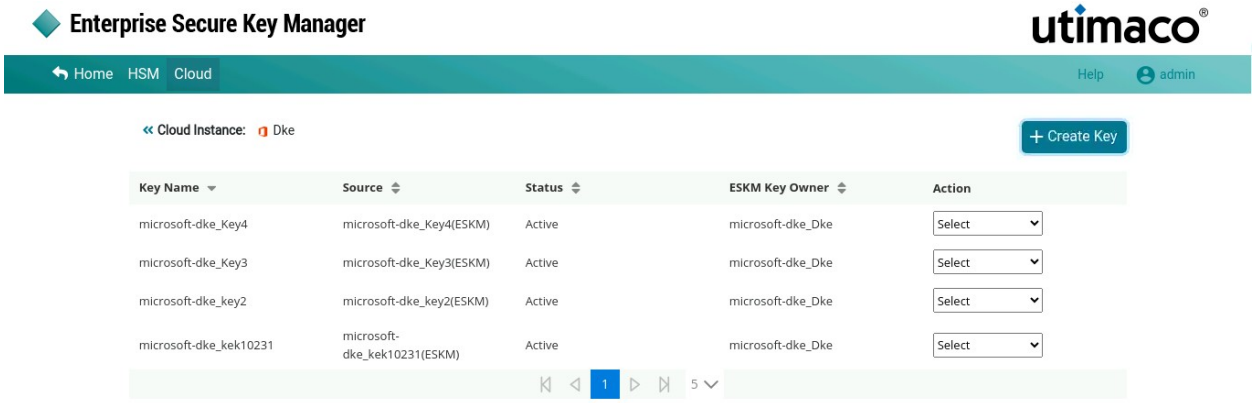


Figure 15 : Keys List

- Click +Create Key button at the top right corner of the page.

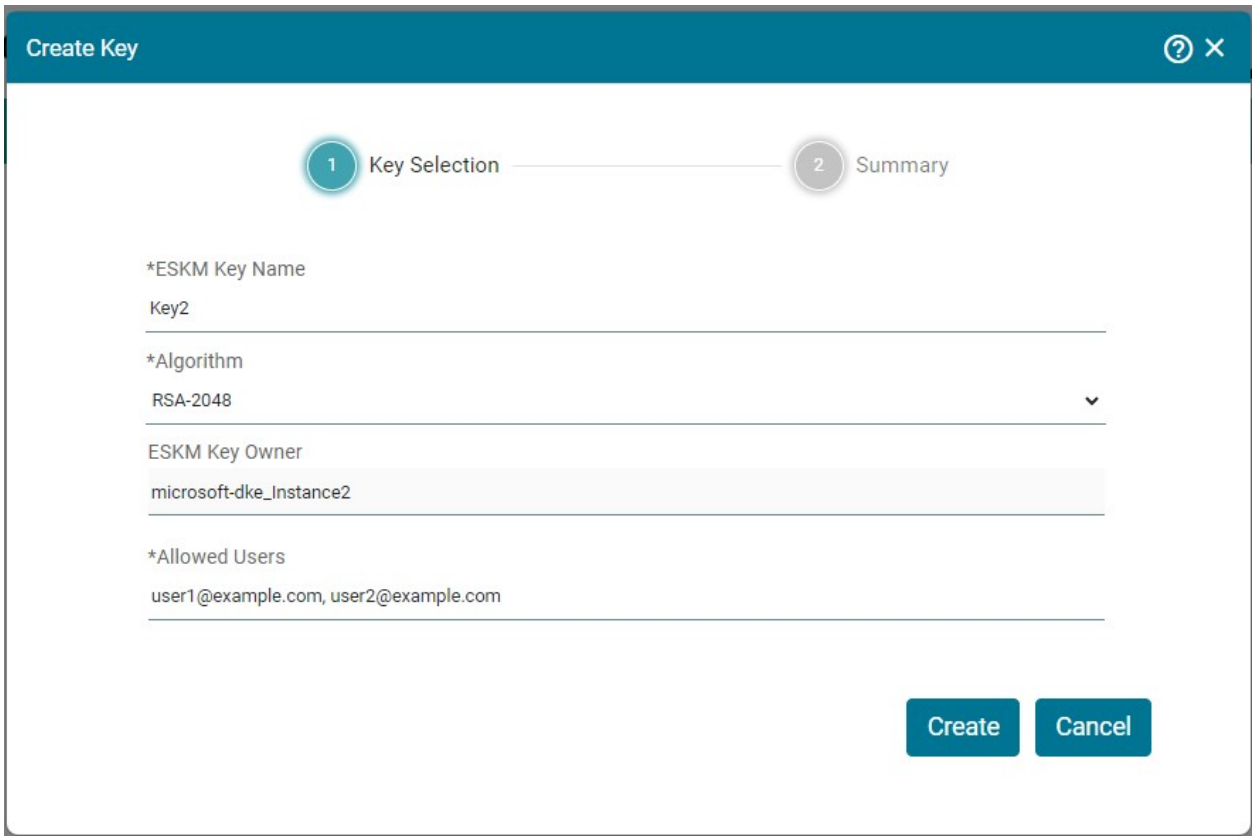


Figure 16 : Create Key

- Fill up the necessary details and the click Create.
- Now, you will be navigated to the Summary section. Review Summary and click Close.

Parameters	***Description***
ESKM Key Name	Name of the key
Algorithm	Algorithm used to create the key. Only RSA-2048 is supported currently.
ESKM Key Owner	Microsoft DKE instance name is the key owner.
Allowed Users	Users who are allowed to use this key for DKE.

Table 3: Create Key - Parameters

4.5 Editing a Microsoft DKE key

This section describes the procedure to edit key information on Microsoft DKE cloud instance.

To edit key

- Under Action column, select Edit from the drop-down to modify key information.

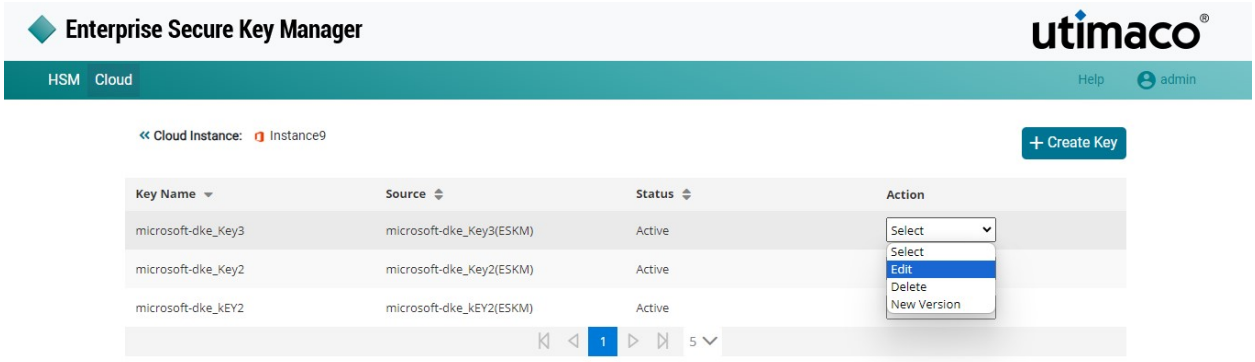


Figure 17 : Edit Key

- The Edit key on Microsoft DKE pop-up window appears.

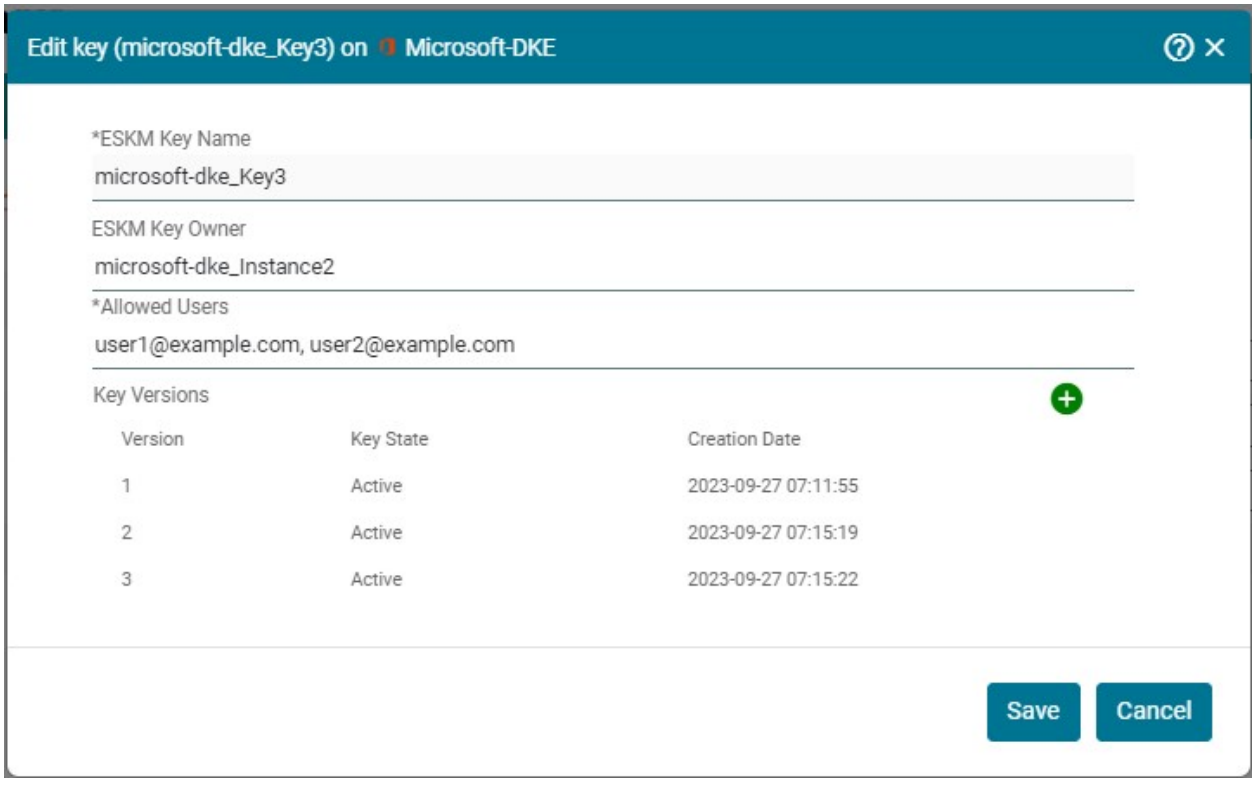


Figure 18 : Edit Key

- Make the necessary changes and click + icon to create a new key version.

- Click Save.

4.6 Deleting a Microsoft DKE Key

This section describes the procedure to delete a key in Microsoft DKE cloud instance.

To delete a key

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

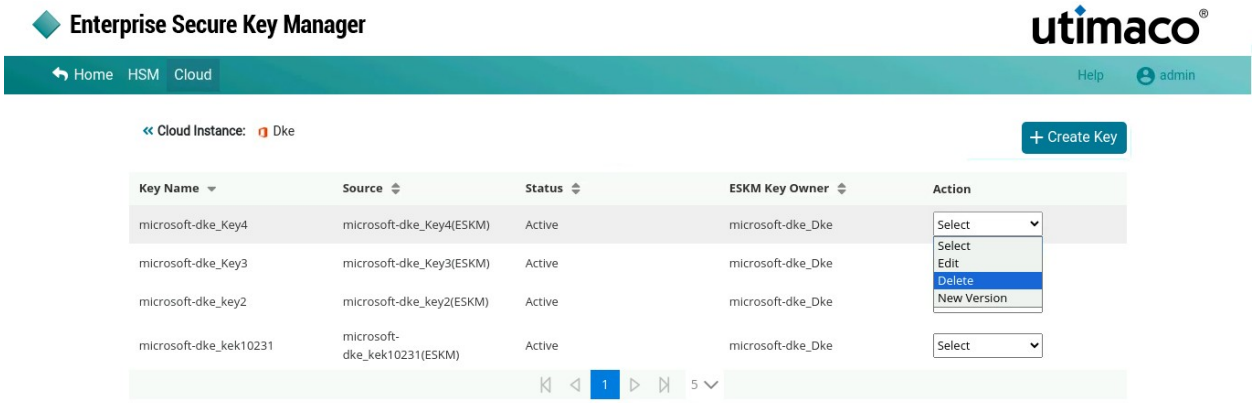


Figure 19 : Delete Key

- The pop-up window will be displayed with a message reading "Are you sure you want to delete key (microsoft-dke_Key3) from ESKM ?". Click Yes.

Cloud Instance key [microsoft-dke_Key3] removed successfully from ESKM.

4.7 Create New Version

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

To create a new version of the key

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

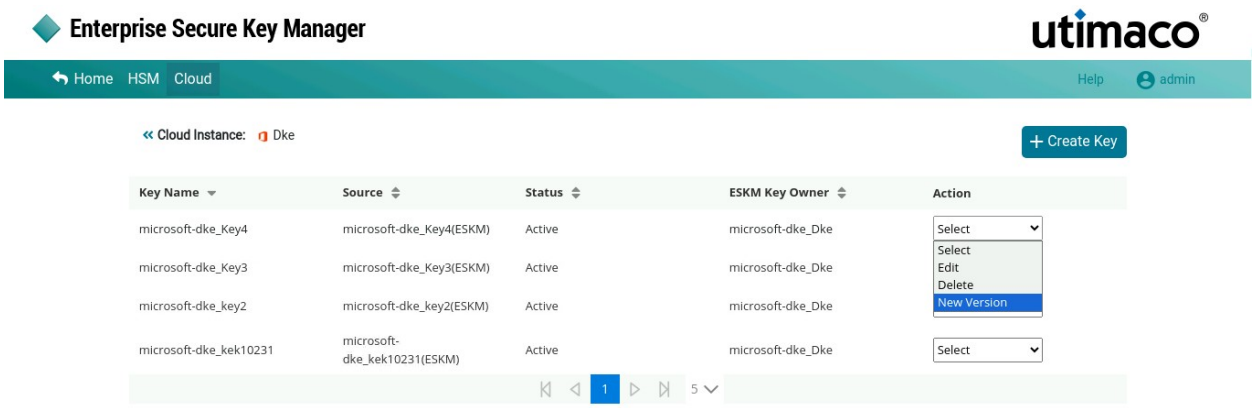


Figure 20 : Create New Version

- The Alert pop-up appears.

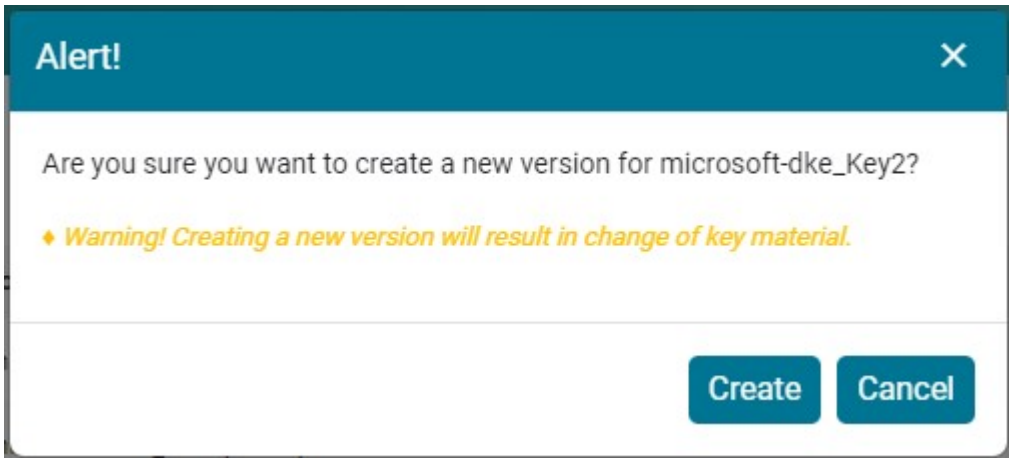


Figure 21 : Alert

- Click Create.

New version 2 for ESKM key [microsoft-dke_Key2] added successfully.

Please refer to the Microsoft DKE-Utimaco ESKM Integration Supplement for the configurations listed below outside of the ESKM.

- Register DKE service with Azure
- Create Sensitivity Labels using DKE
- Publish the Sensitivity Labels
- Verify Encryption and Decryption with DKE on Microsoft 365 Client

4.8 Viewing Microsoft DKE Key Information

This section describes the procedure to view key's information in Microsoft DKE cloud instance.

To view key information

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

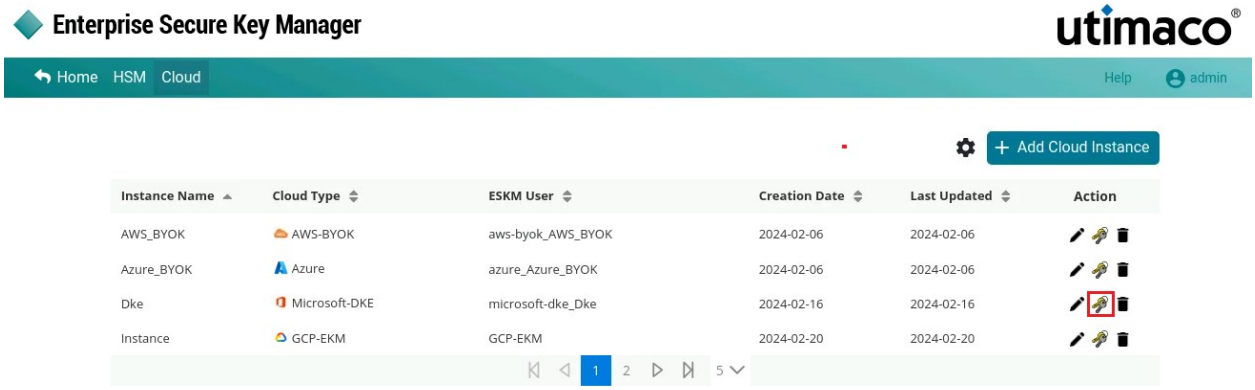


Figure 22 : Manage Keys

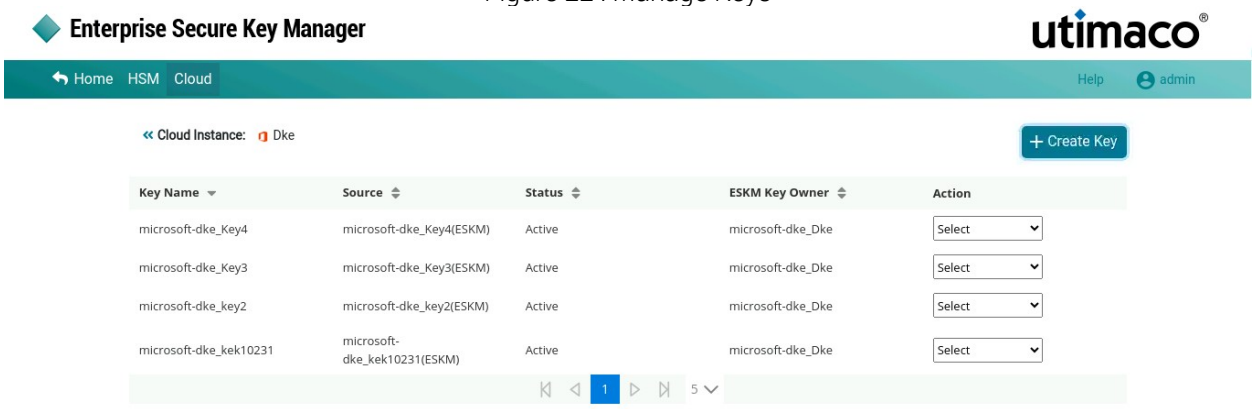


Figure 23 : Keys List

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

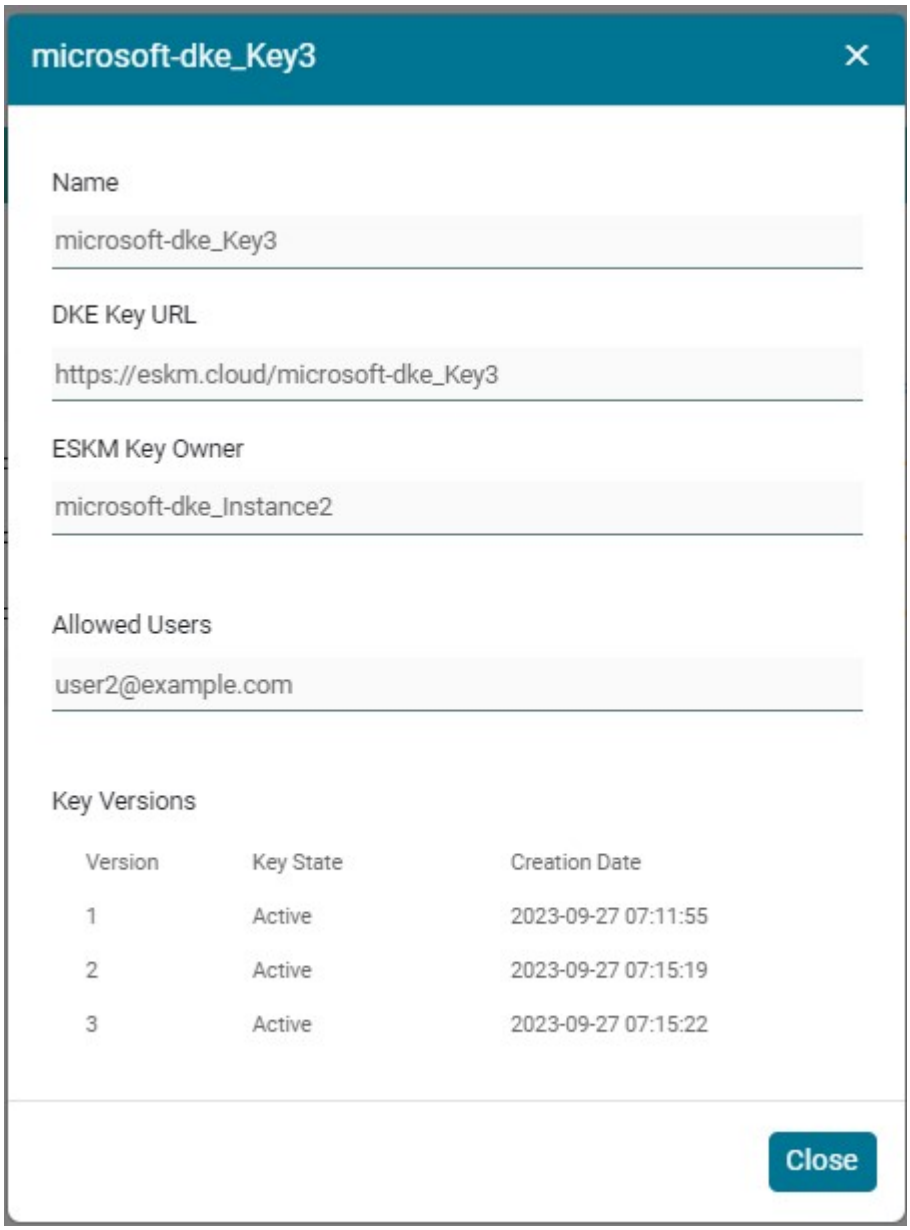


Figure 24 : Key Information

Parameters	***Description***
Key Name	Name of the Key created in Microsoft DKE
DKE Key URL	DKE Key URL in the ESKM Cloud

Parameters	***Description***
ESKM Key Owner	Microsoft DKE Instance Name is the ESKM Key Owner
Allowed users	Users who are allowed to use this key for Microsoft DKE
Key Versions	It displays number of versions created for a specific key. User can create multiple key versions based on the Number of Active Versions Allowed for a Key in ESKM Management Console (Security > Keys > Key Options).

Table 4: Microsoft DKE - Key details

5 Microsoft Azure DKE API Commands

The following APIs have been implemented to support Microsoft Double Key Encryption (DKE).

- Get Public Key API
- Decrypt Data API

For more information, please see the following link: https://learn.microsoft.com/en-us/ purview/ double-key-encryption.

6 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 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.