Microsoft Azure

DKE

Integration Guide

ESKM

8.54.0

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	2.0.0
Date	2026-11-06
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 5
1.1 About this Guide 5
1.2 Target Audience 6
1.3 Purpose of this Integration 6
1.4 Abbreviations 6
1.5 Document Conventions 7
2 Product Overview 9
2.1 Overview of Microsoft DKE 9
2.2 Overview of Utimaco ESKM 9
2.3 Joint Value Proposition 9
3 Integration Requirements and Prerequisites 10
3.1 Tested Versions 10
3.2 Supported Platforms 10
3.3 Hardware and Software Requirements 10
3.4 Prerequisites 10
4 Accessing the Cloud Integration Web Console 12
5 Cloud Settings 16
6 Microsoft DKE Integration 19
6.1 Adding a Microsoft DKE Cloud Instance 19
6.2 Editing a Microsoft DKE Cloud Instance 21
6.3 Deleting a Microsoft DKE Cloud Instance 22
6.4 Creating a Key on Microsoft DKE 23
6.5 Editing a Microsoft DKE key 25
6.6 Deleting a Microsoft DKE Key 26
6.7 Create New Version 27
6.8 Viewing Microsoft DKE Key Information 28
7 Configurations on Azure and Microsoft Purview 32
7.1 Register Service with Azure 32
7.2 Create Sensitivity Labels using DKE 34
7.3 Publish the Sensitivity Label 40
7.4 Install Azure Information Protection Unified Labelling Client 47

7.5 Verify Encryption and Decryption with DKE on Microsoft 365 Client 47
8 Contact and Support Information 50
9 Appendices 51
9.1 Microsoft Azure DKE API Commands 51

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.

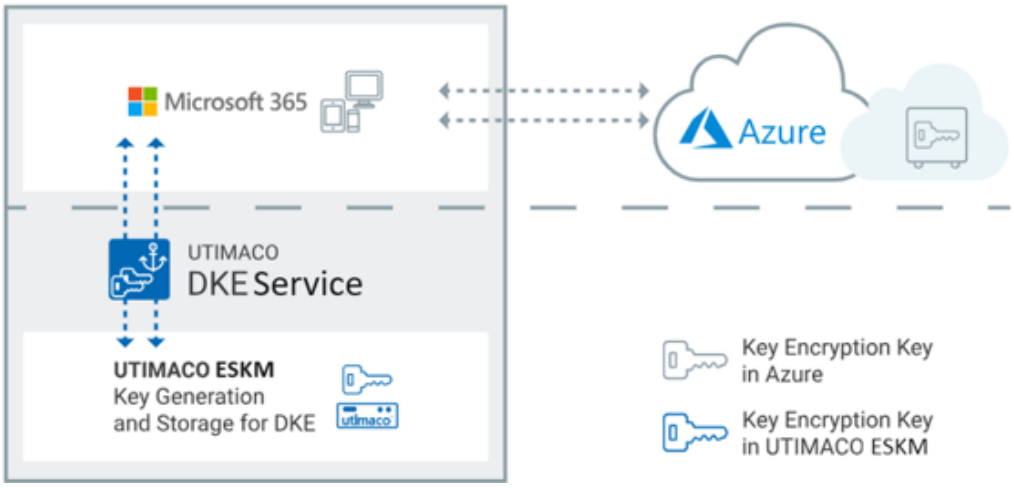


Figure 1 : Azure DKE

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
- Configurations on Azure and Microsoft Purview
- Verification of encryption and decryption with DKE

1.2 Target Audience

This guide is intended for administrators of Microsoft DKE and Utimaco ESKM.

1.3 Purpose of this Integration

The purpose of this integration is to integrate Microsoft Double Key Encryption (DKE) with Utimaco ESKM to provide an additional layer of protection for sensitive Microsoft 365 data while maintaining control of the encryption key within Utimaco ESKM.

1.4 Abbreviations

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
DKE	Double Key Encryption
API	Application Programming Interface
CA	Certificate Authority
UI	User Interface
URL	Uniform Resource Locator

Abbreviation	Meaning
RSA	Rivest, Shamir, Adleman
GUI	Graphical User Interface
SSL	Secure Sockets Layer
CN	Common Name
IP	Internet Protocol
FQDN	Fully Qualified Domain Name

Table 1: List of 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 Microsoft DKE

Microsoft Double Key Encryption (DKE) provides additional protection for highly sensitive data by using two encryption keys. One key is controlled by Microsoft, while the second key remains under the organization's control. Both keys are required to access DKE-protected content.

2.2 Overview of Utimaco ESKM

Utimaco Enterprise Secure Key Manager (ESKM) is a centralized key management solution used to securely generate, store, and manage encryption keys. In the Microsoft DKE integration, ESKM provides the customer-controlled key used as part of the Double Key Encryption process.

2.3 Joint Value Proposition

The integration of Microsoft DKE with Utimaco ESKM combines Microsoft's Double Key Encryption capability with customer-controlled key management through ESKM. ESKM manages the customer-controlled key required for DKE, enabling organizations to retain control of their encryption key while using DKE to protect sensitive Microsoft 365 data.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Microsoft Double Key Encryption (DKE)	Utimaco ESKM Version
Cloud Service	8.54.0

Table 3: Tested versions

3.2 Supported Platforms

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

3.3 Hardware and Software Requirements

Software	Software Requirements
Utimaco ESKM	8.54.0

Table 4: Hardware and software requirements

3.4 Prerequisites

Please make sure that the following prerequisites are met:

- ESKM version mentioned in *Tested Versions* or higher.
- ESKM must be publicly accessible.
- Register a domain name/FQDN for ESKM and configure it as the audience (REST Certificate CN) in Cloud Settings.
- Configure a valid SSL certificate signed by a trusted external CA in REST Server Settings.
- Allow HTTPS communication on port 443 and ensure ESKM is reachable from the required clients.

- ESKM must be available at the root path without a sub path.
- Enable the Microsoft DKE Service in Cloud Settings.

4 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.

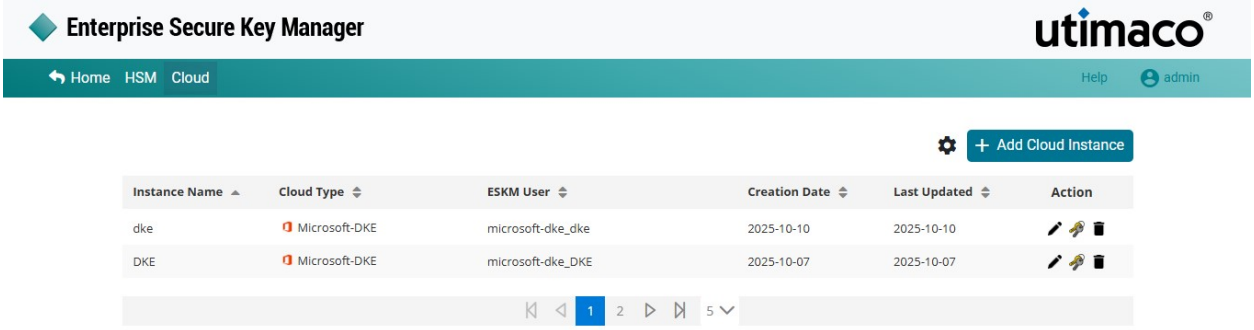


Figure 2 : Cloud integration dashboard

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

The following screen appears.

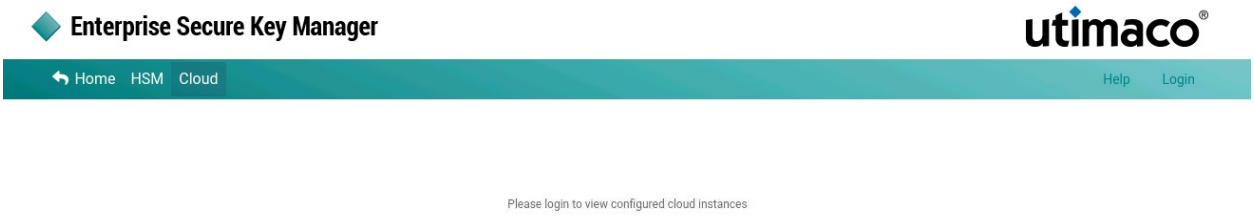


Figure 3 : Cloud Integration login

Click Login at the top right corner of the page.

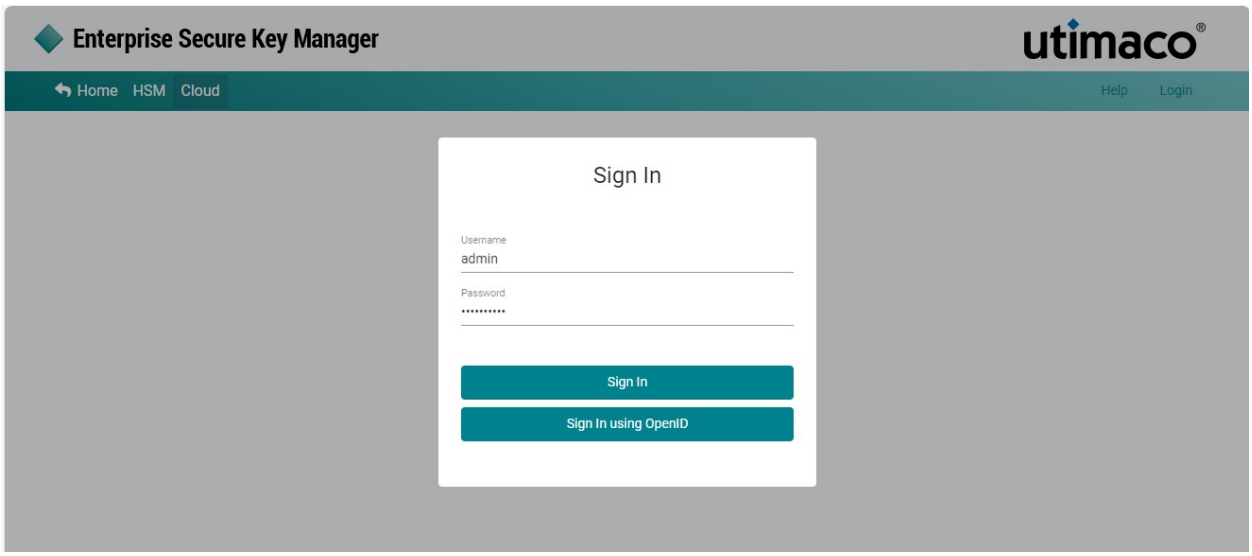


Figure 4 : Cloud Integration sign-in

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

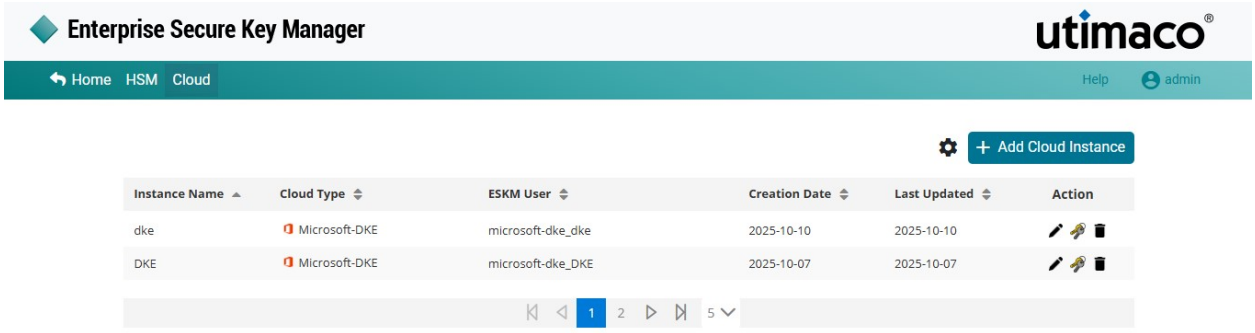


Figure 5 : Cloud ESKM log-in page

The cloud integration dashboard enables the user to add cloud instances 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.

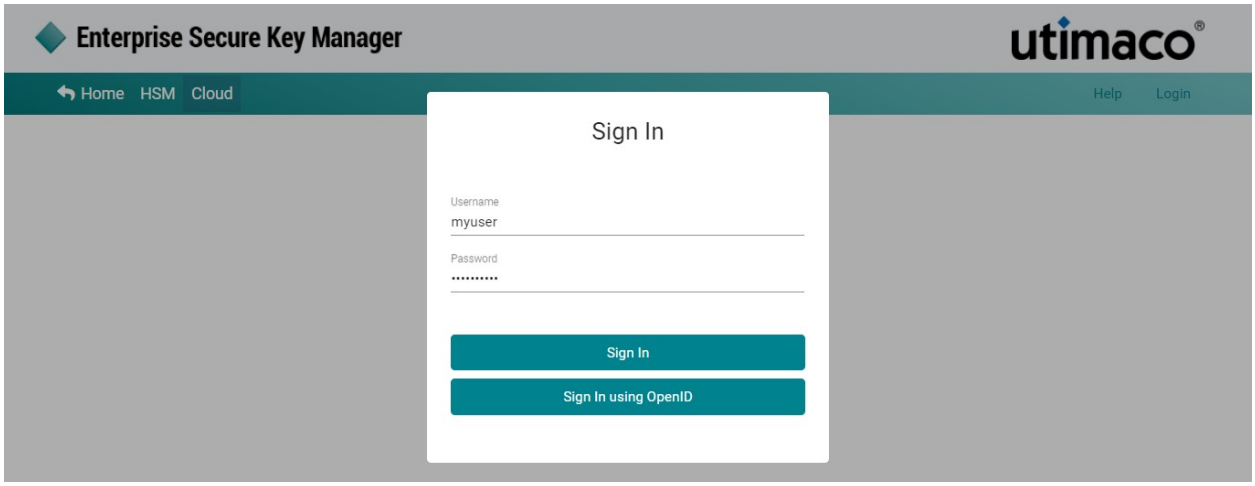


Figure 6 : Sign-in using OpenID

- 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.

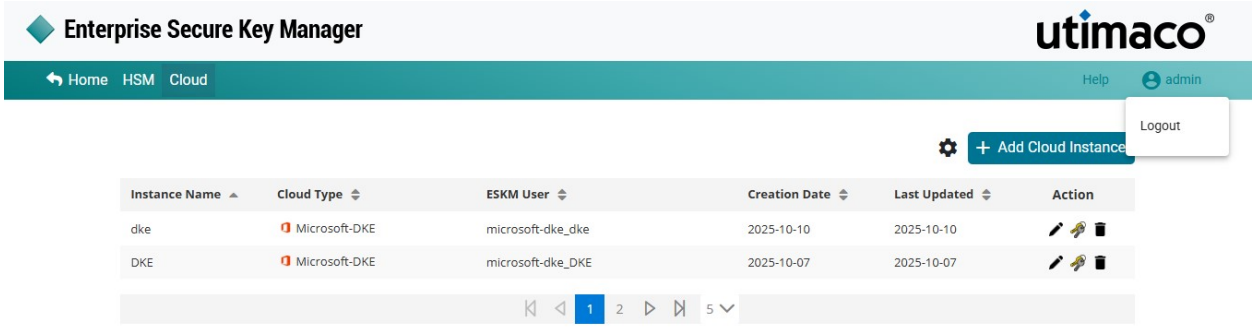


Figure 7 : Logout

- When you are signed in with the 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 upper left corner of the page to navigate to the ESKM application.

5 Cloud Settings

This section describes the procedure to enable ESKM cloud settings.

To enable cloud settings

- Click the Settings icon on the Cloud dashboard.

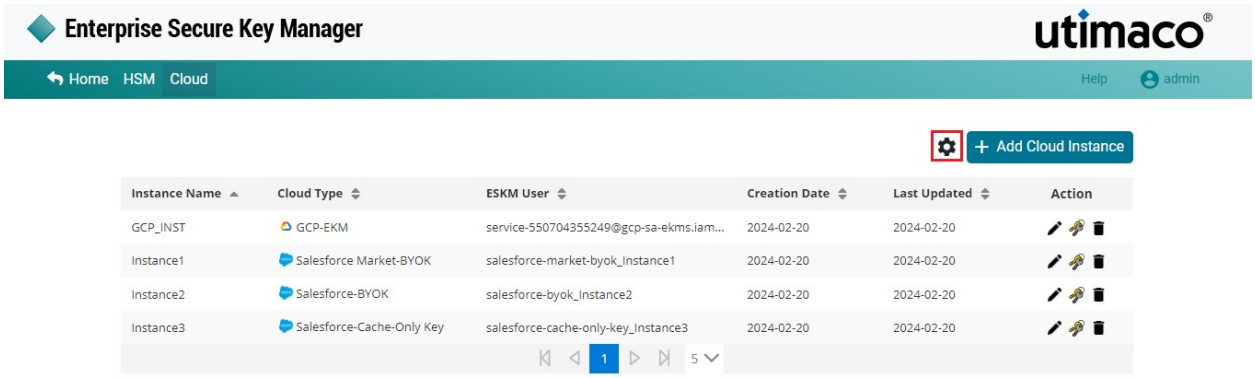


Figure 8 : Cloud settings

- The Settings pop-up window will appear.

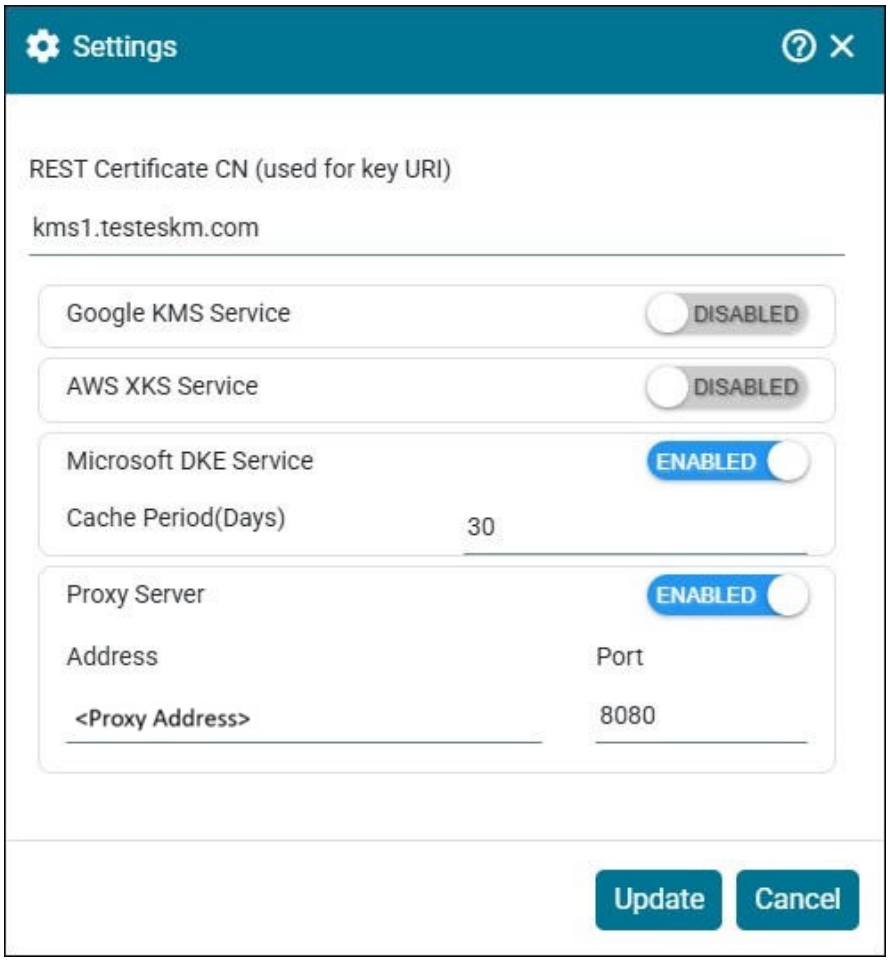


Figure 9 : Microsoft DKE - Cloud Settings

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(Days)	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 5: Settings - Parameters

6 Microsoft DKE Integration

6.1 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.

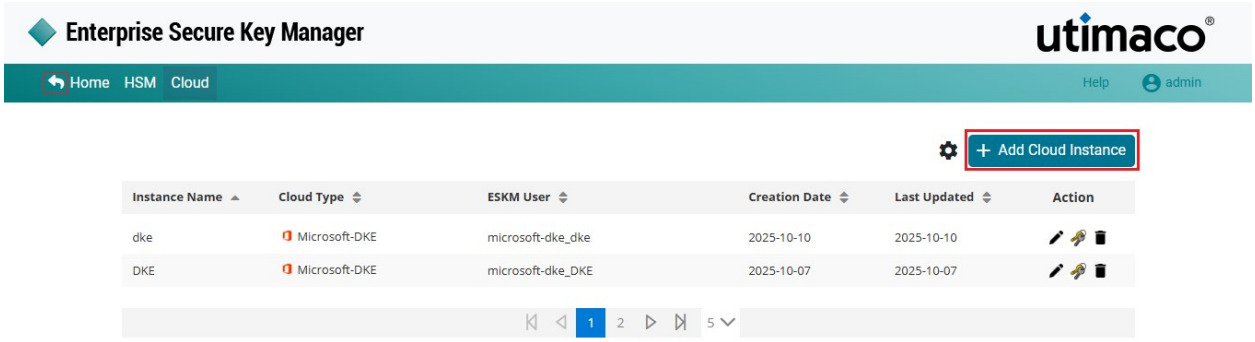


Figure 10 : Microsoft DKE Cloud Instance

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

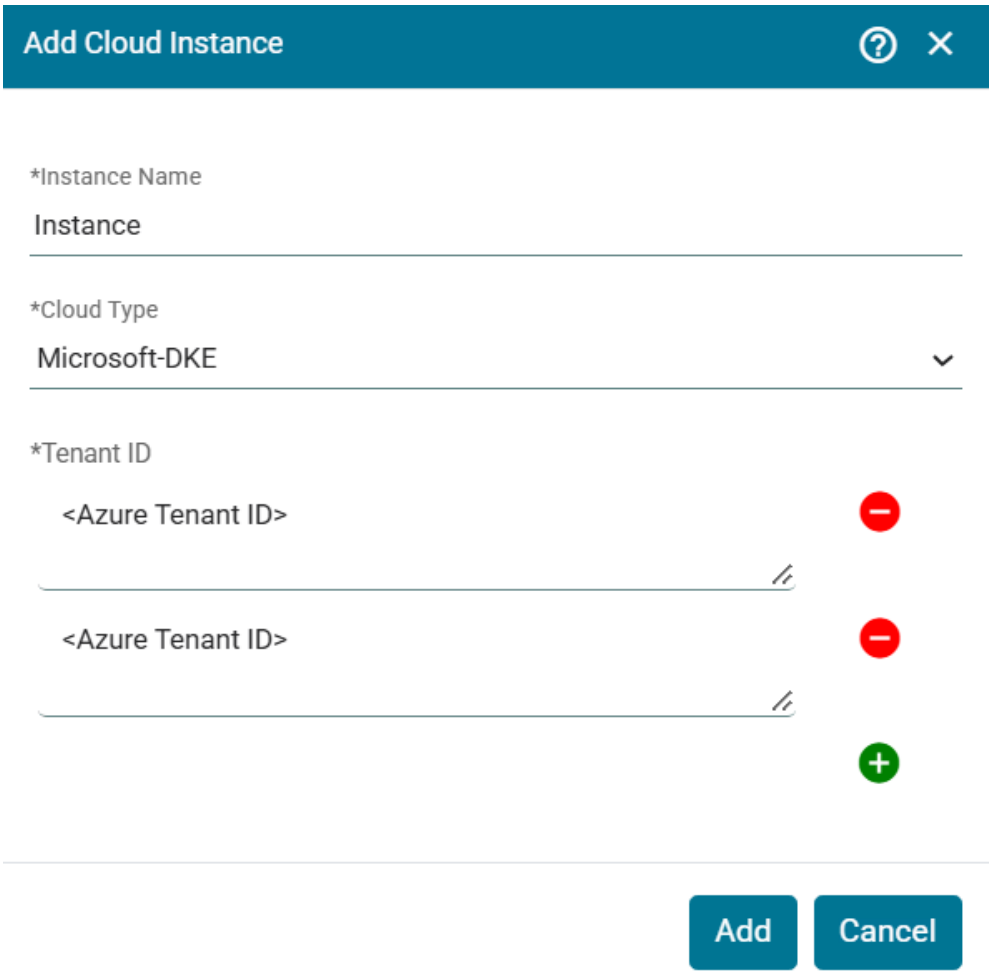


Figure 11 : Add Cloud Instance

- 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. Here 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 6: Add Microsoft DKE Cloud Instance - parameters

6.2 Editing a Microsoft DKE Cloud Instance

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

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

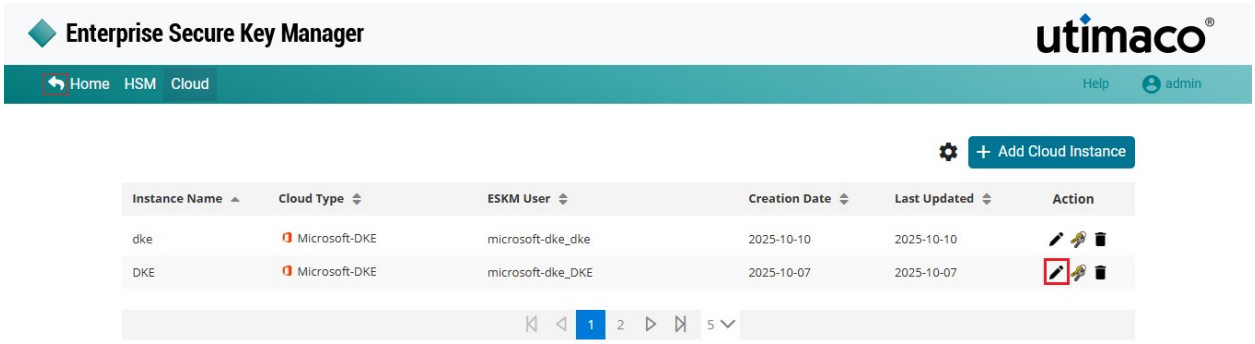


Figure 12 : Edit Key

- The Edit Cloud Instance pop-up window appears.

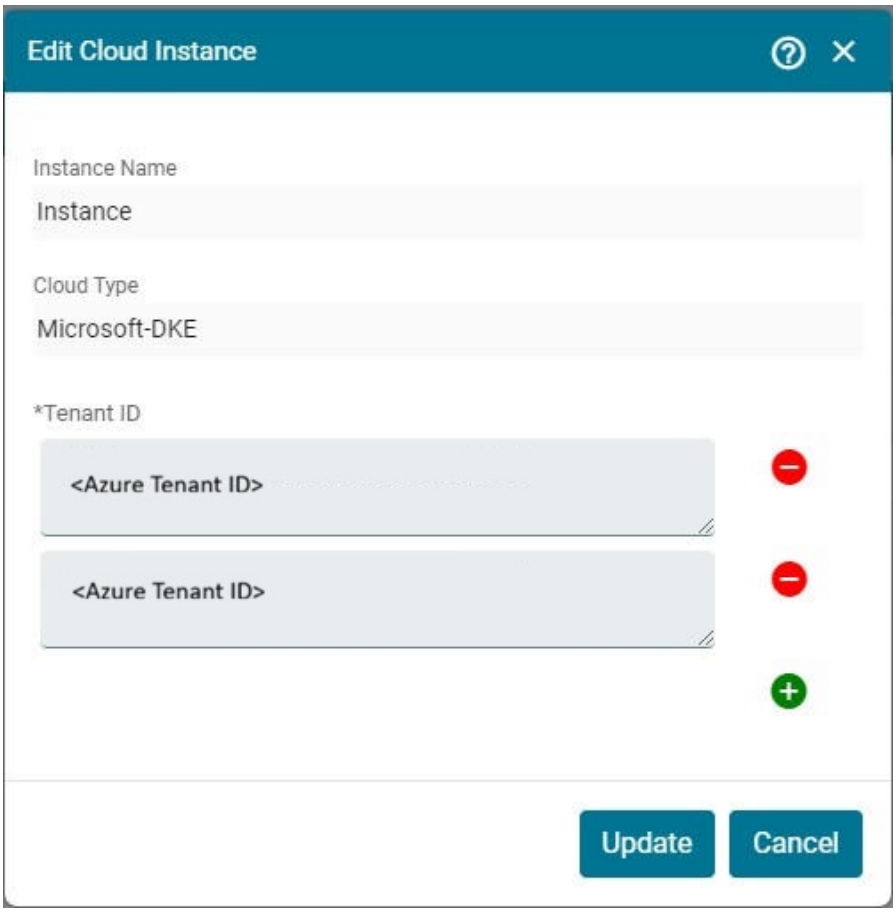


Figure 13 : Edit Cloud Instance

- Make the necessary changes and click Update.

Cloud Instance Name [Microsoft-DKE] updated successfully.

6.3 Deleting a Microsoft DKE Cloud Instance

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

To delete a Microsoft DKE cloud instance:

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

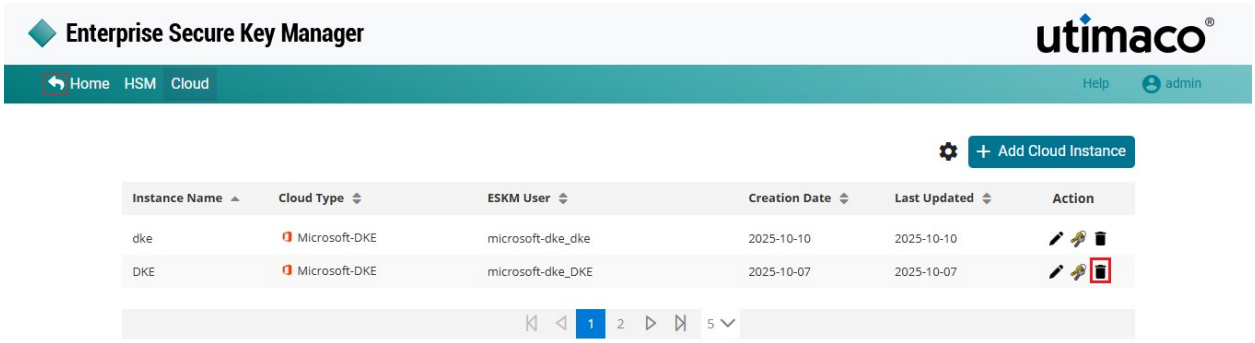


Figure 14 : Delete Cloud Instance

- 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.

The Cloud Instance name [Microsoft DKE] was deleted successfully.

6.4 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 the keys list available in the cloud instance.

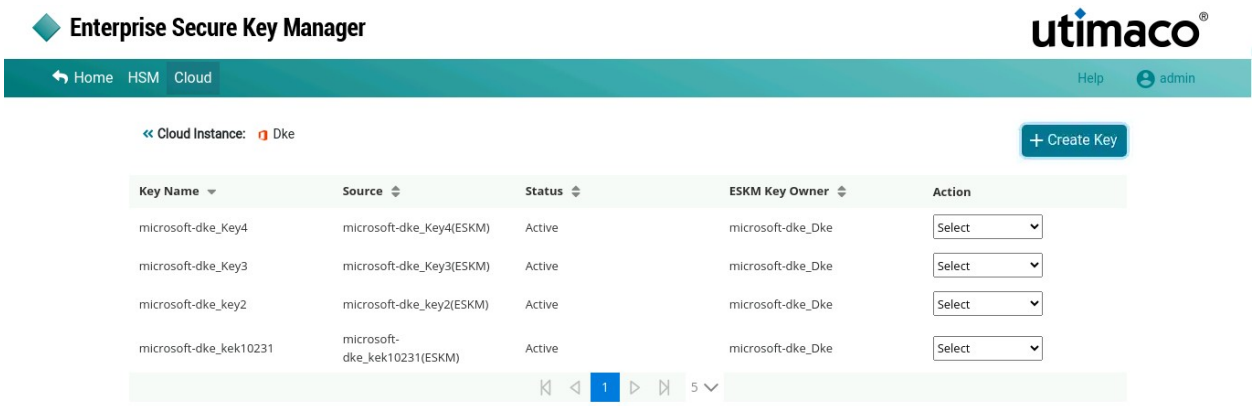


Figure 15 : Keys List

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

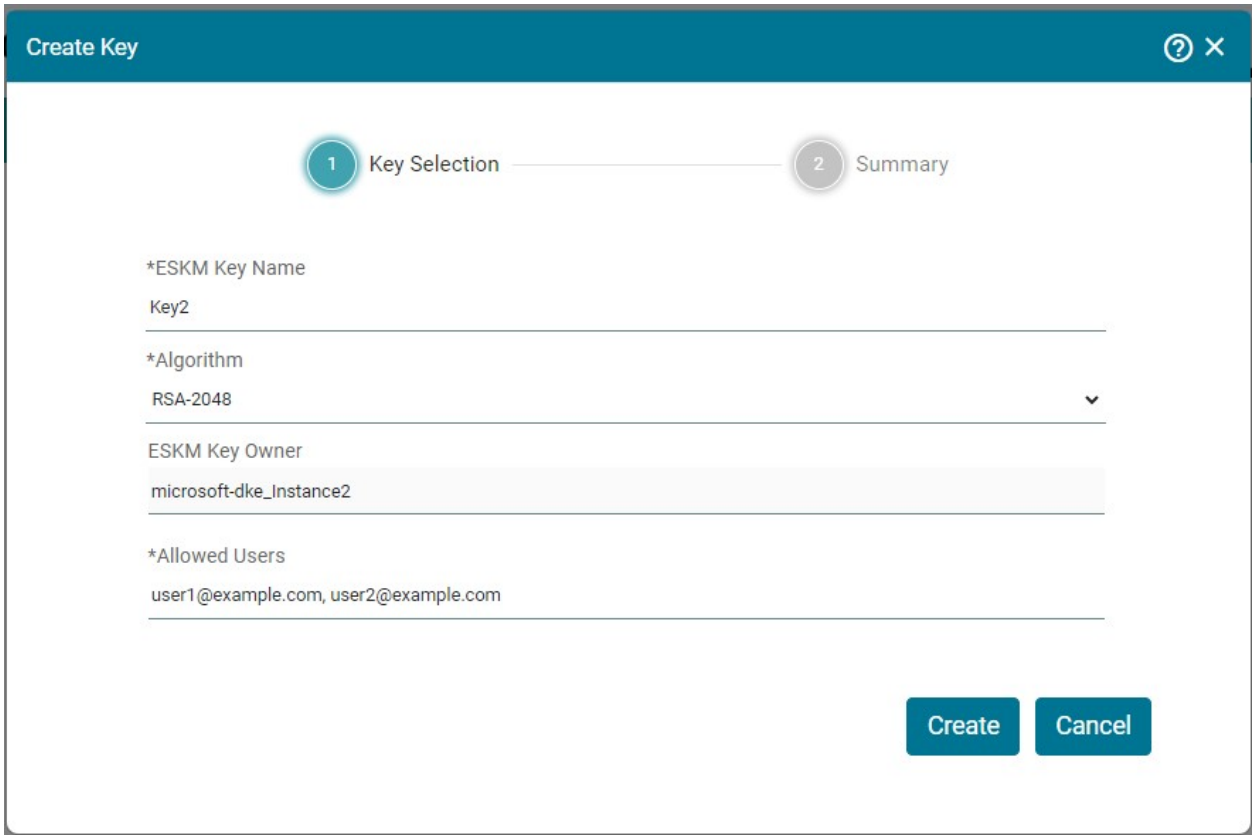


Figure 16 : Create Key

- Fill out the necessary details and then 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 7: Create Key - Parameters

6.5 Editing a Microsoft DKE key

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

To edit key

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

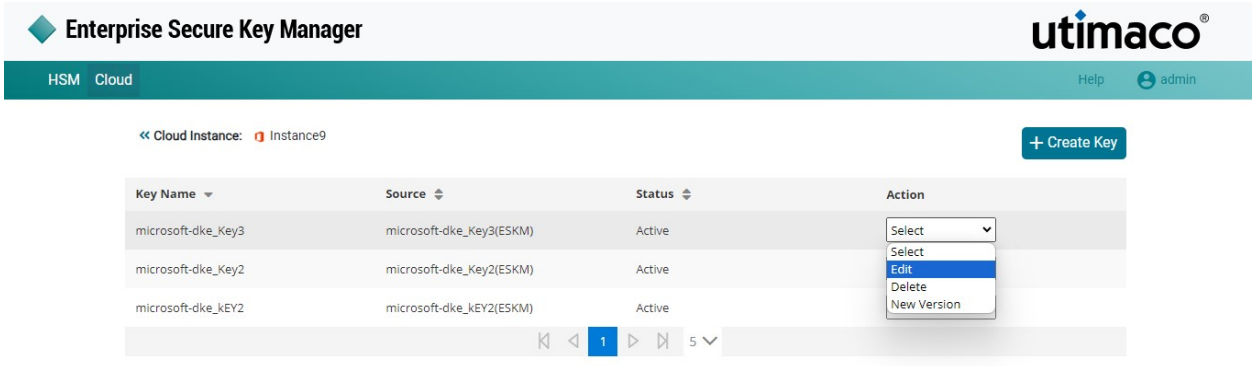


Figure 17 : Edit Key

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

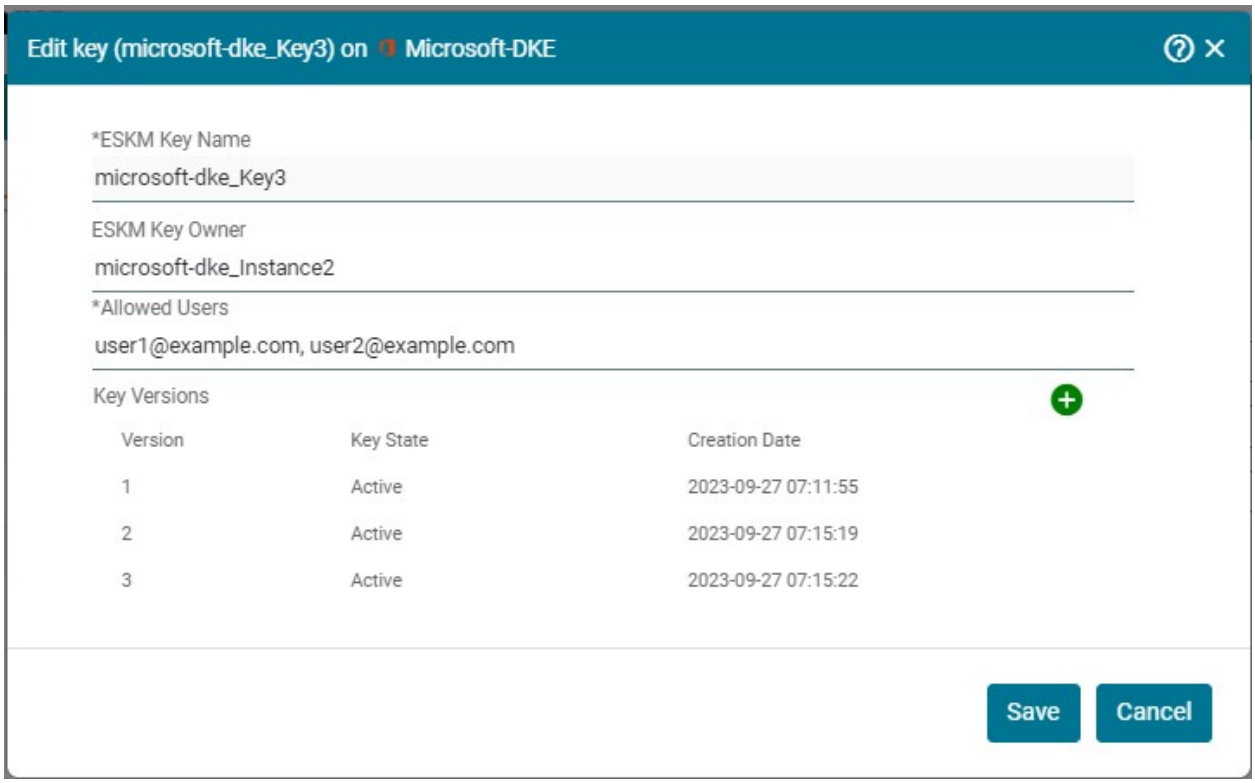


Figure 18 : Edit Key

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

6.6 Deleting a Microsoft DKE Key

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

To delete a key

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

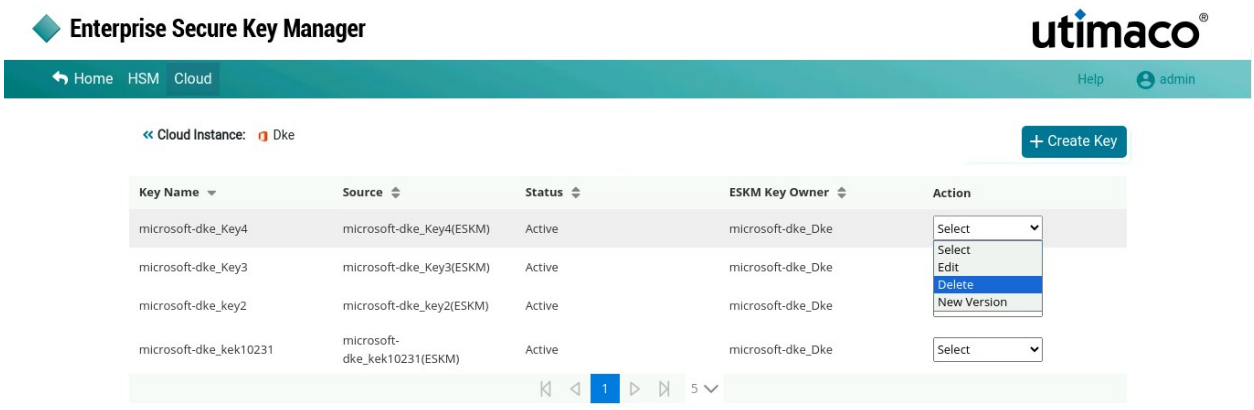


Figure 19 : Delete Key

- 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.

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

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

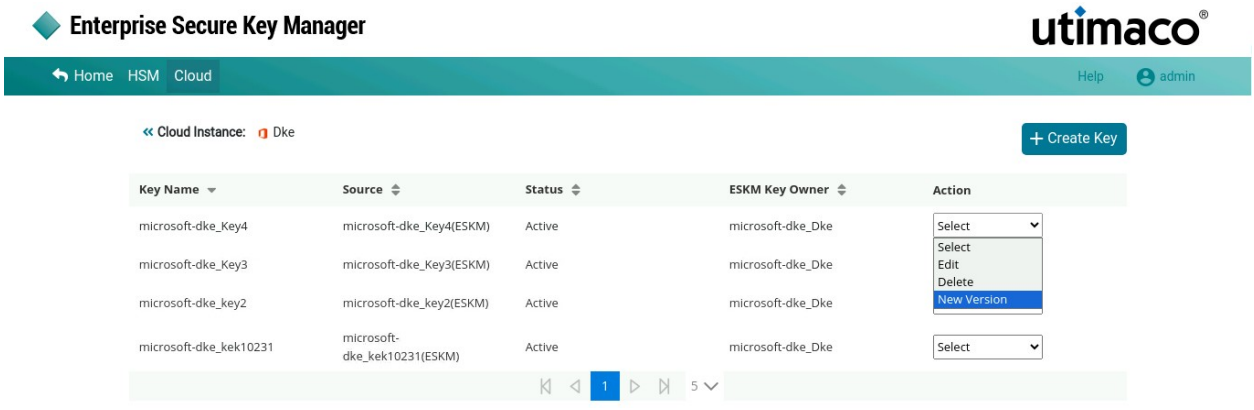


Figure 20 : Create New Version

- The Alert pop-up appears.

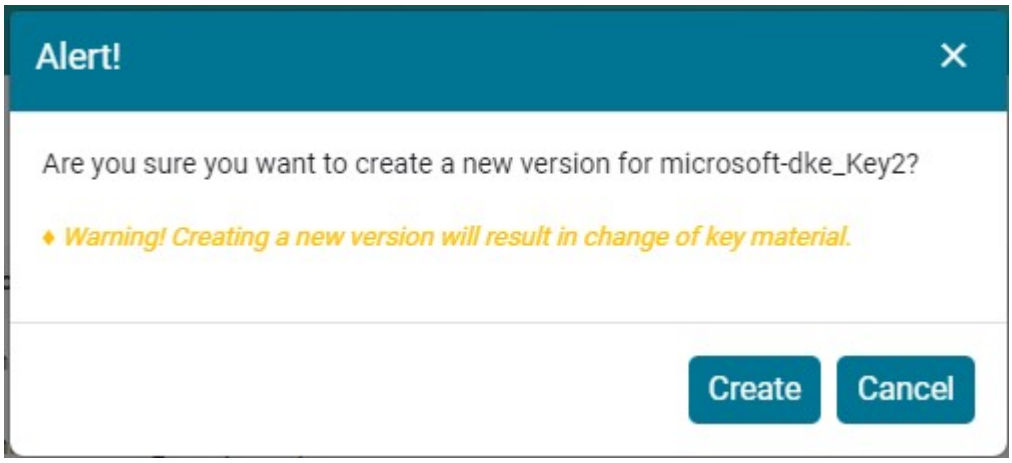


Figure 21 : Alert

- Click Create.

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

6.8 Viewing Microsoft DKE Key Information

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

To view key information

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

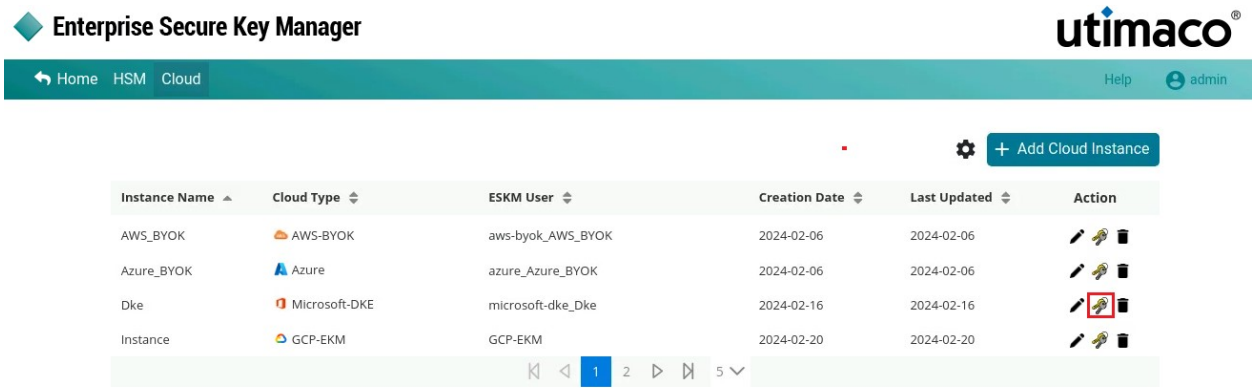


Figure 22 : Manage Keys

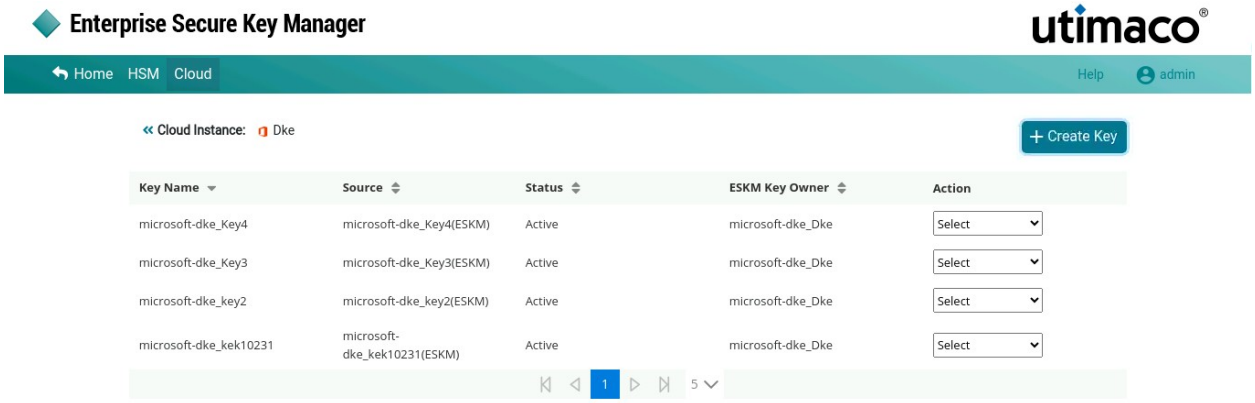


Figure 23 : Keys List

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

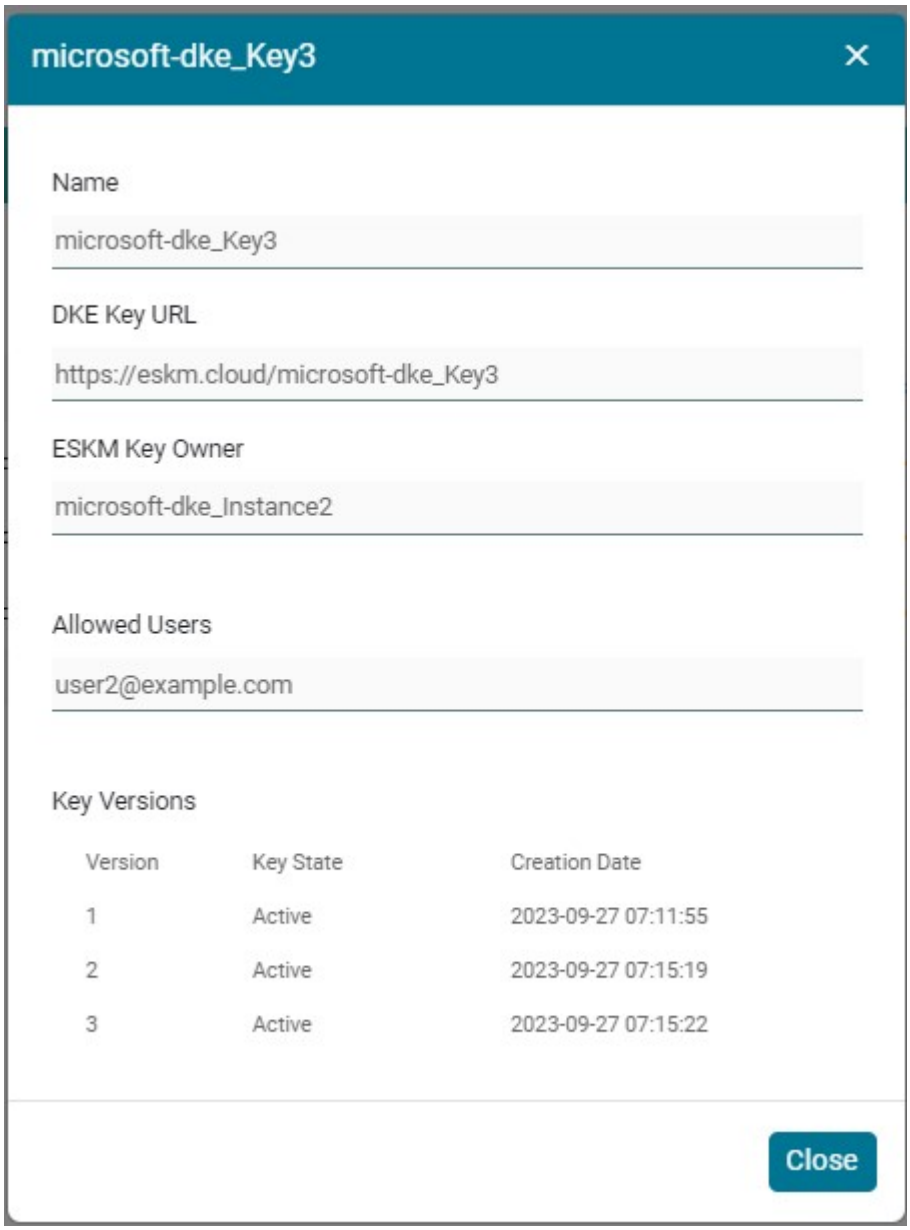


Figure 24 : Key Information

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 8: Microsoft DKE - Key details

7 Configurations on Azure and Microsoft Purview

Follow the procedures below to complete the configurations outside ESKM that are required for the integration.

7.1 Register Service with Azure

The following steps enable you to register your ESKM DKE service. Registering your ESKM DKE service is the last step in deploying DKE before you can start creating labels.

To register ESKM DKE service:

1. In your browser, open the **Microsoft Azure portal**, and go to **All Services > Identity > App Registrations**.
2. Select **New registration** and enter a meaningful name.
3. Select an account type from the options displayed either single or multi-tenant.

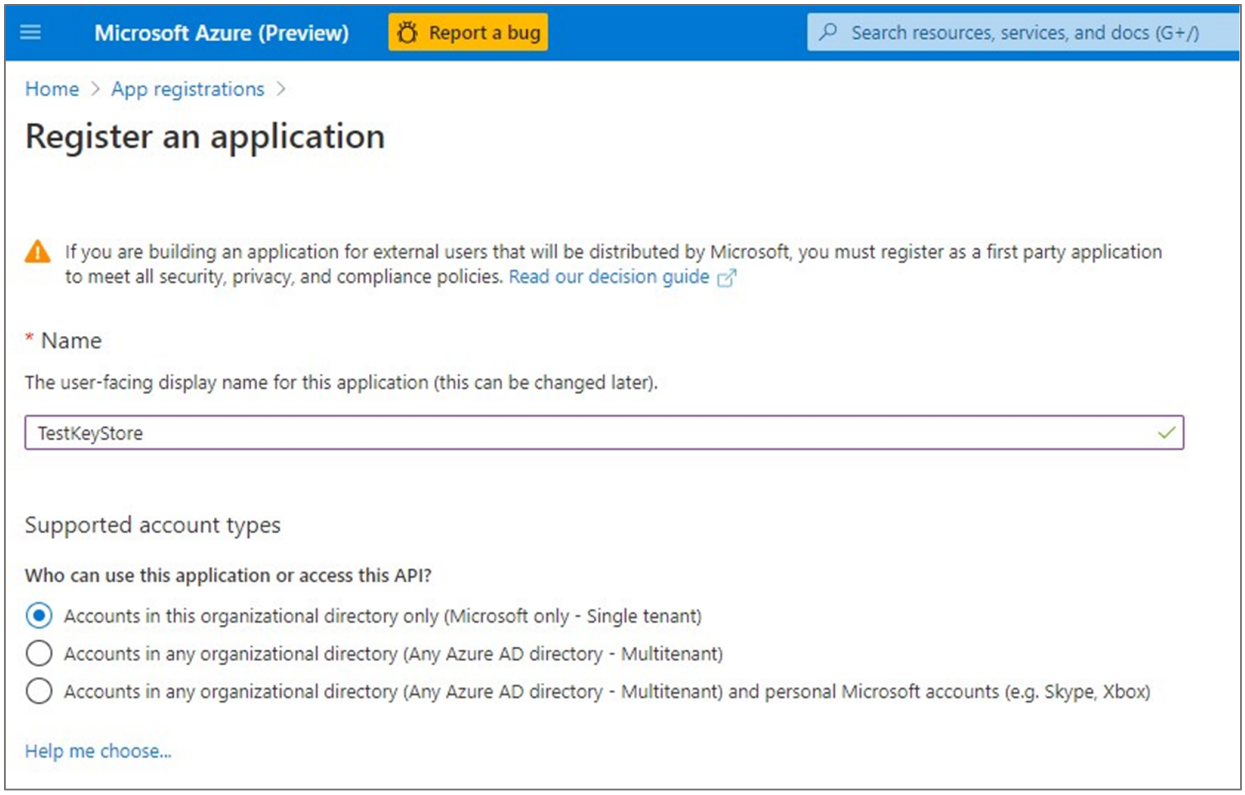


Figure 25 : Register an application

4. At the bottom of the page, select **Register** to create the new App Registration.
5. In your new App Registration, in the left pane, under **Manage**, select **Authentication**.
6. Select **Add a platform**.
7. On the **Configure platforms** popup, select **Web**.
8. Under **Redirect URIs**, enter the URI of your double key encryption service. Enter the App Service URL, including both the hostname and domain and click on **Configure** button. For example: *https://eskm.utimaco.com*



The ESKM Public URL needs to be based on the root level, i.e., not a sub directory
example: `https://eskm.utimaco.com/mykey`
This example does not work: `https://eskm.utimaco.com/dkeservice/mykey`



No trailing slash in DKE URL. The DKE URL must not contain a trailing slash:
example: `https://eskm.utimaco.com/mykey`
This example does not work: `https://eskm.utimaco.com/mykey/`

9. Under **Implicit grant**, select the **ID tokens** checkbox.
10. Select **Save** to save your changes.
11. On the left pane, select **Expose an API**, next to **Application ID URI**, click on **Set** and enter your App Service URL, including both hostname and domain and click on **Save**.
12. Still on the **Expose an API** page, in the **Scopes defined by this API** area, select **Add a scope**. In the new scope:
    a. Define the scope name as `user_impersonation`.
    b. Select the administrators and users who can consent.
    c. Define any remaining values required.
    d. Select **Add scope.**
    e. Select **Save** at the top to save your changes.
13. Still on the **Expose an API** page, in the **Authorized client applications** area, select **Add a client application**. In the new client application:

a. Define the **Client ID** as `d3590ed6-52b3-4102-aeff-aad2292ab01c`. This value is the Microsoft Office client ID and enables Office to obtain an access token for your key store.

b. Under **Authorized scopes**, select the `user_impersonation` scope.

c. Select **Add application.**

d. Select **Save** at the top to save your changes.

e. Repeat these steps, but this time, define the client ID as `c00e9d32-3c8d-4a7d-832b-029040e7db99`.

This value is the Azure Information Protection unified labeling client ID.

7.2 Create Sensitivity Labels using DKE

In the **Microsoft Purview portal**, navigate to the **Information Protection** section.

1. On Sensitivity **Labels** page, select **+ Create** to start the new sensitivity label configuration.
2. On **Provide basic details for this label**, specify the following:

   a. **Name** – The name used to identify the sensitivity label in Microsoft Purview.

   b. **Display name** – The name displayed to users in applications where the label is published.

   c. **Description for users** – A description that helps users understand the purpose of the sensitivity label.

   d. **Description for admins** – A description for administrators who manage the sensitivity label.

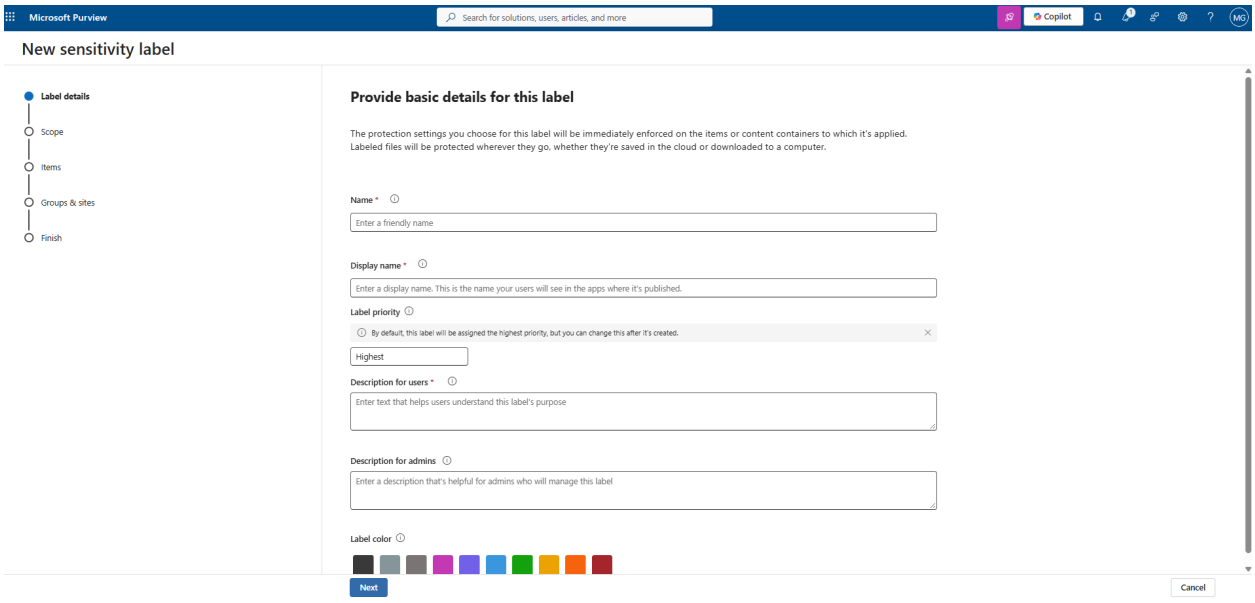


Figure 26 : Create label

3. Click on **Next** button.

4. On **Define the scope for this label**, select the required scope for the sensitivity label. For example, select **Files & other data assets** and click on **Next** button.

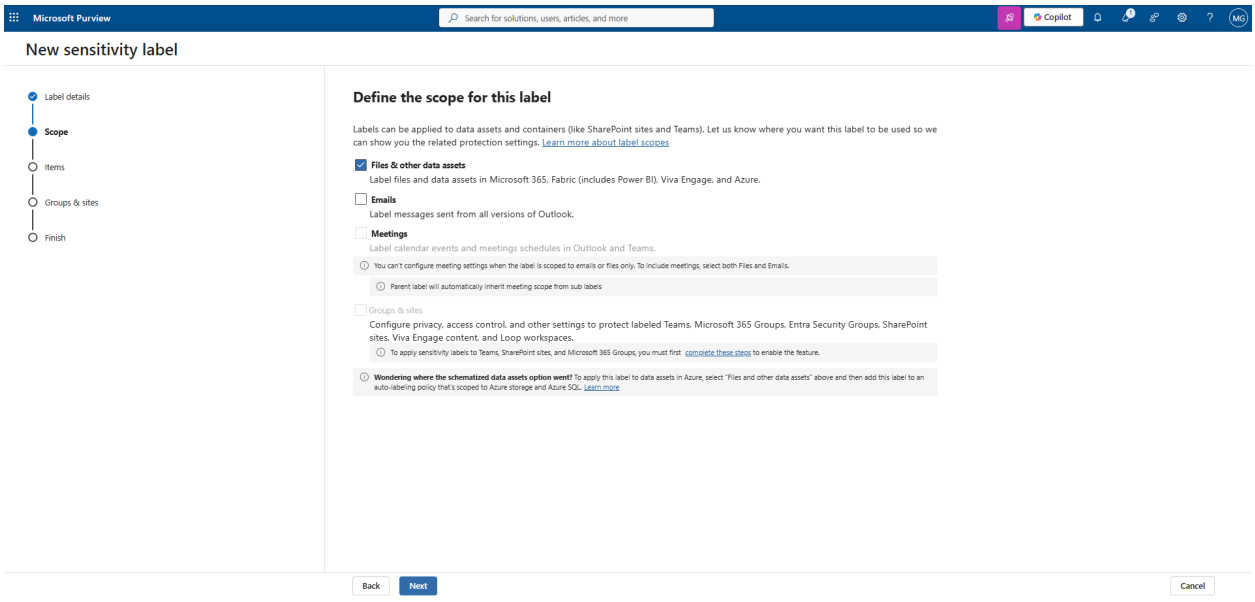


Figure 27 : Define the scope for this label

5. On **Choose protection settings for the types of items you selected**, select **Control access** to configure permissions for content to which the label is applied. Since the primary purpose of this procedure is to secure the files, configure the appropriate access control settings. Select **Apply content marking**, and then select **Next**.

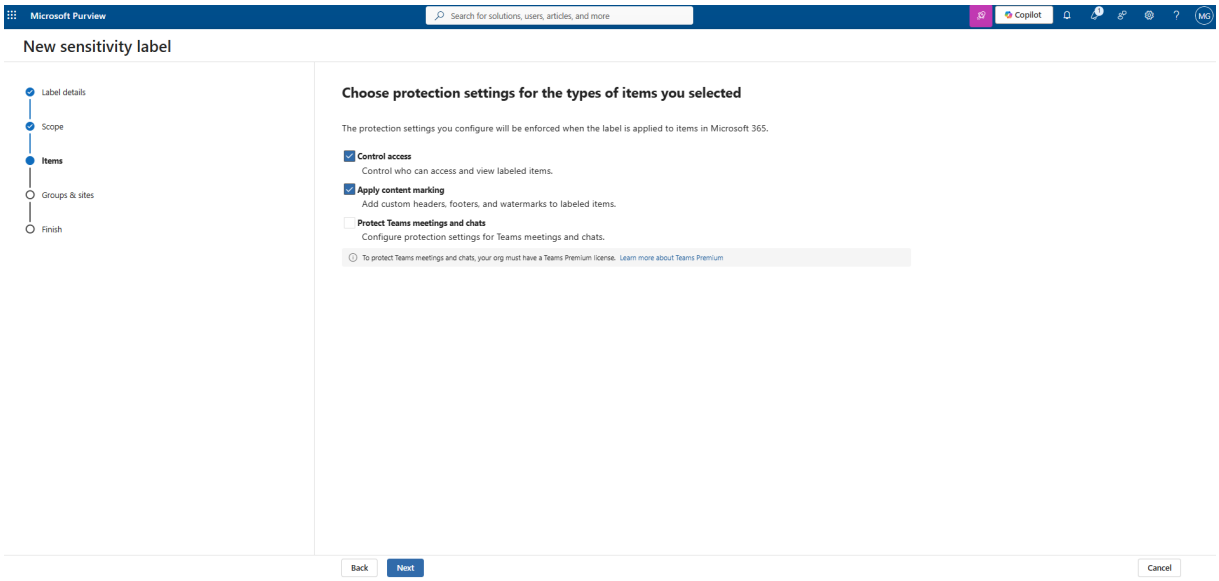


Figure 28 : Choose protection settings

6. On **Access control**, configure the access settings as follows:

    a. **Assign permissions now or let users decide?** – Select **Assign permissions now**.

    b. **User access to content expires** – Select **Never** to allow users to access protected files without an expiration period.

    c. **Allow offline access** – Select **Always**.

    d. Under **Assign permissions to specific users and groups**, select **Assign permissions** and specify the users or groups that require access to the protected content.

    e. Select **Use Double Key Encryption** and enter the appropriate **DKE Key URL** obtained from the ESKM Cloud UI and select **Next**.

Use the DKE Key URL from the ESKM Cloud UI. Refer to Section *Viewing Microsoft DKE Key Information.*

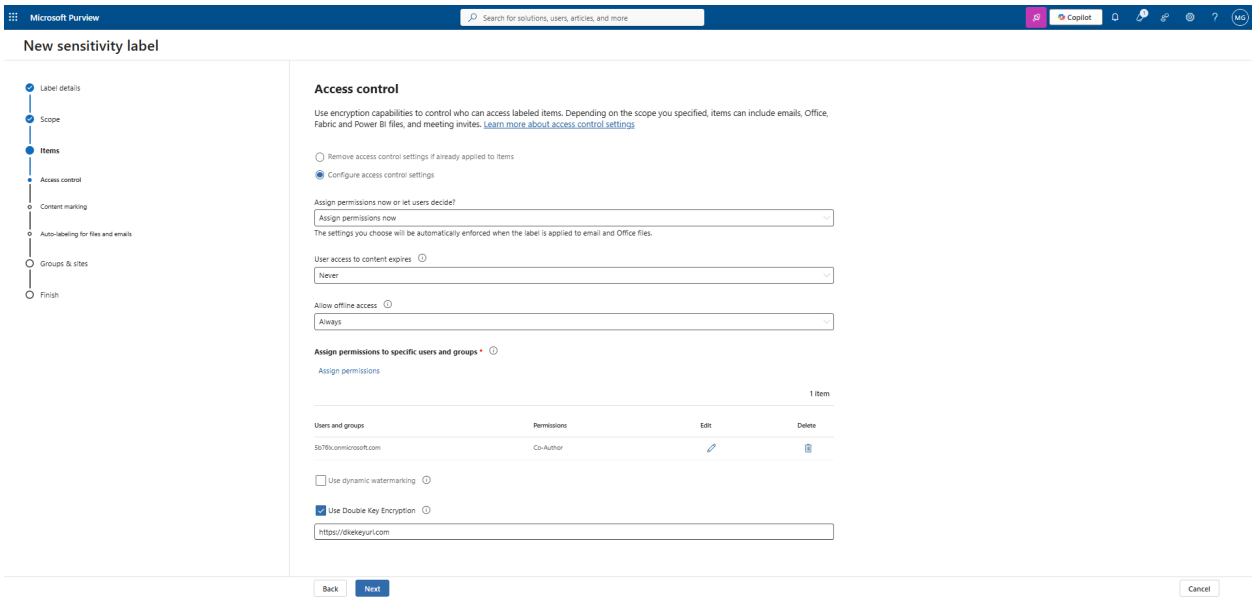


Figure 29 : Access control



The sensitivity label used for DKE protection needs to provide sufficient permissions for all intended recipients of the documents.

7. On **Content marking**, configure how the sensitivity label is displayed on protected content. Enable **Content marking**, and configure the required **watermark**, **header**, and **footer** settings. Select **Next**.

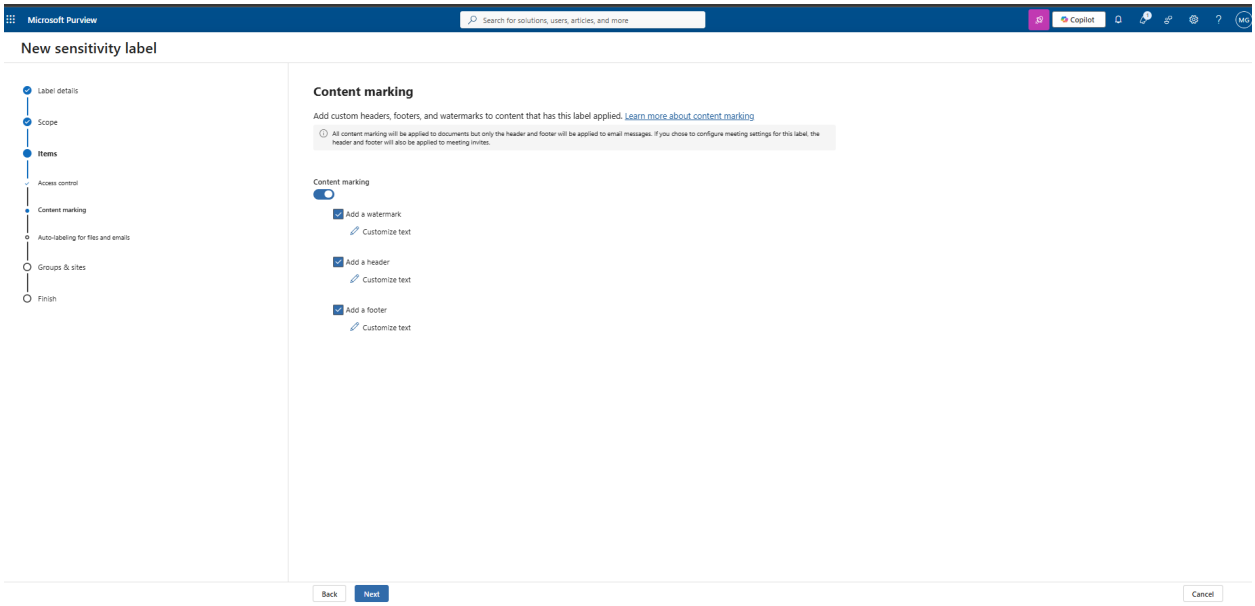


Figure 30 : Content marking settings

8. On **Auto-labeling for files and emails**, enable **Auto-labeling for files and emails**. Configure the required conditions for detecting content and select the action to be performed when the content matches the specified conditions. Then select **Next**.

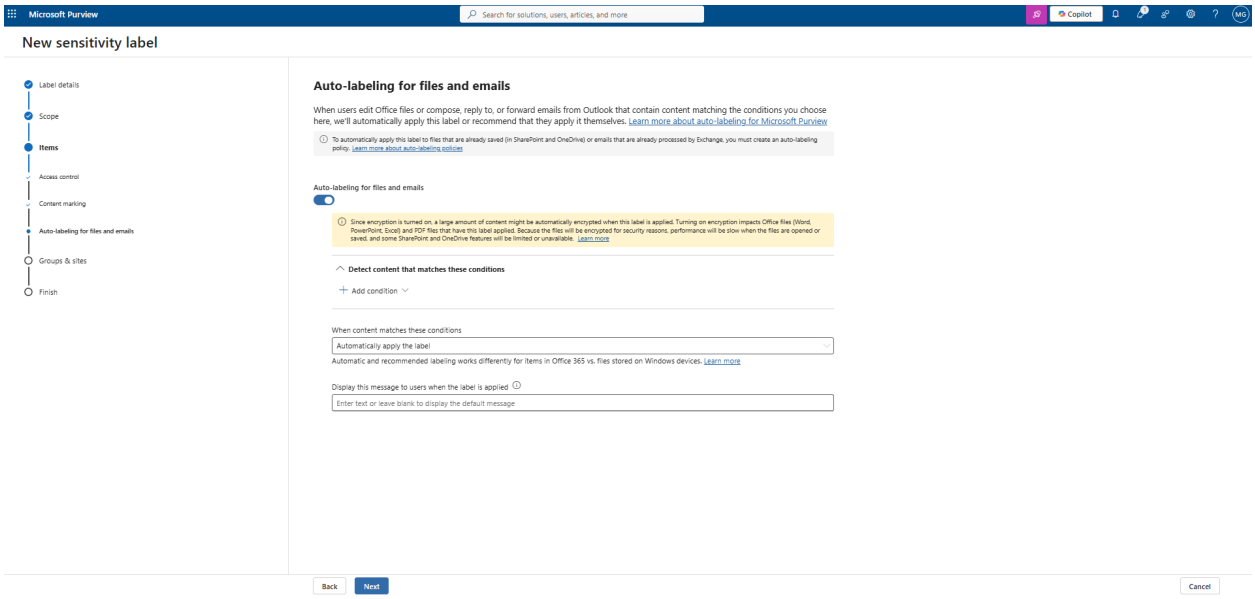


Figure 31 : Auto-labeling for files and emails

9. On **Define protection settings for groups and sites**, configure the required protection settings for groups and sites. These settings apply to teams, groups, and sites, and not directly to the files stored in them. Then select **Next**.

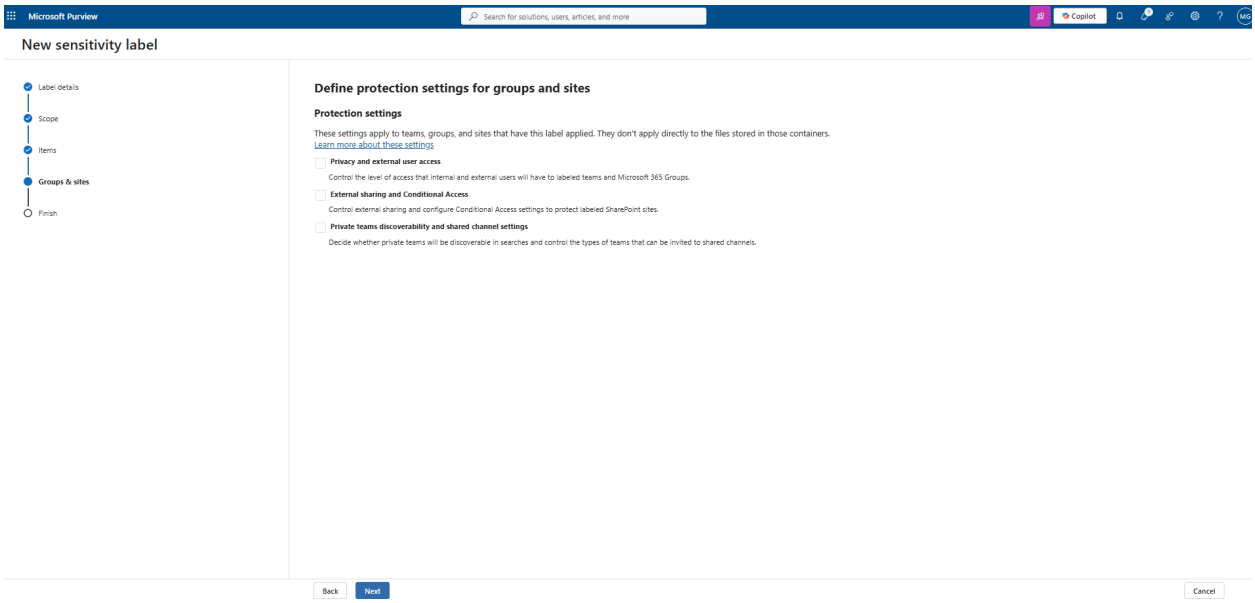


Figure 32 : Define protection settings for groups and sites

10. On **Review your settings and finish**, review the configured settings and make any required changes. Select **Create label** to create the sensitivity label, and then select **Done**.

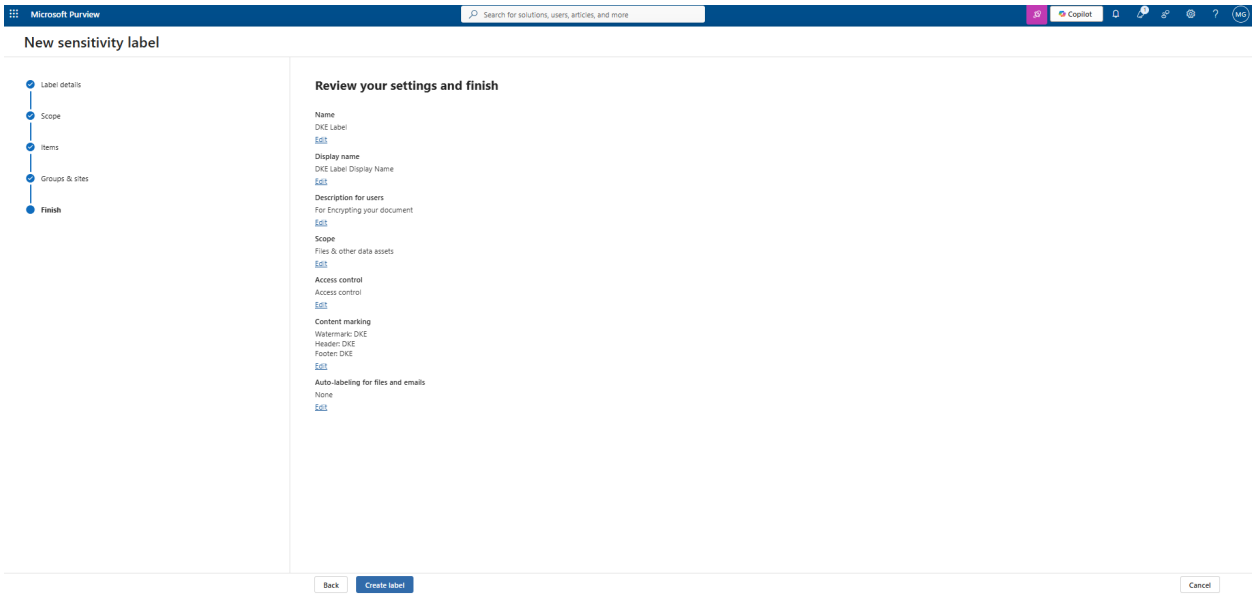


Figure 33 : Review label settings

7.3 Publish the Sensitivity Label

After the sensitivity label is created, it must be published to make it available to users.

1. On **Your sensitivity label was created**, select **Publish label to users' apps**, and then select **Done**.

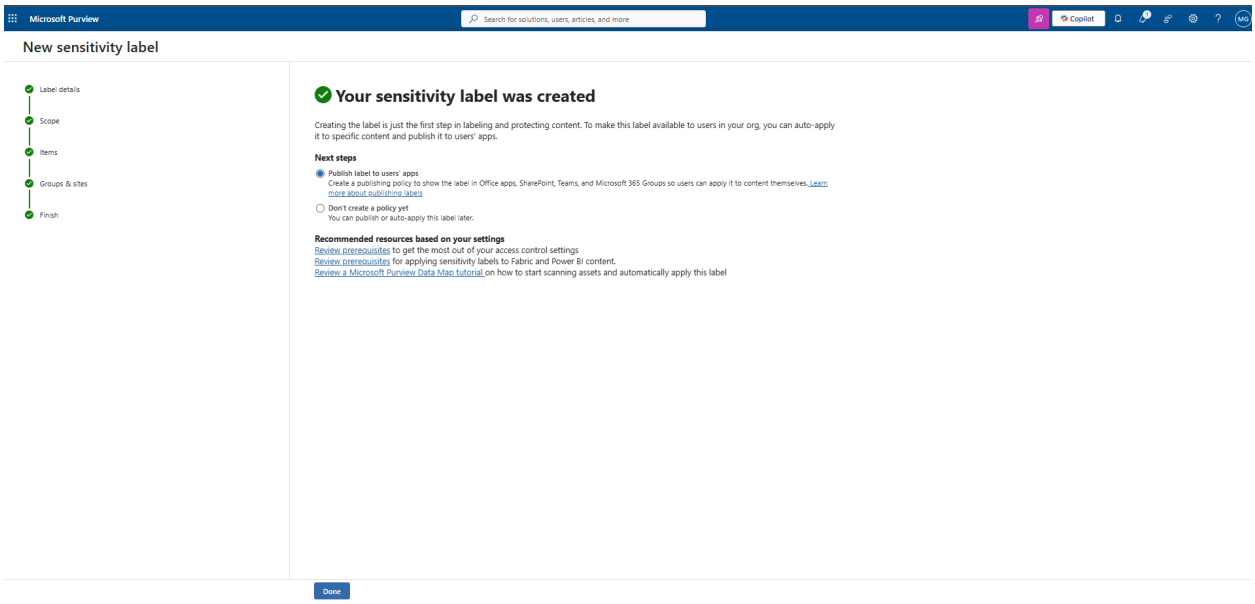


Figure 34 : Sensitivity label created

2. On **Publish label**, select **Create new label policy** to create a new publishing policy, or select an existing **Label Policy** if an appropriate policy is already available.

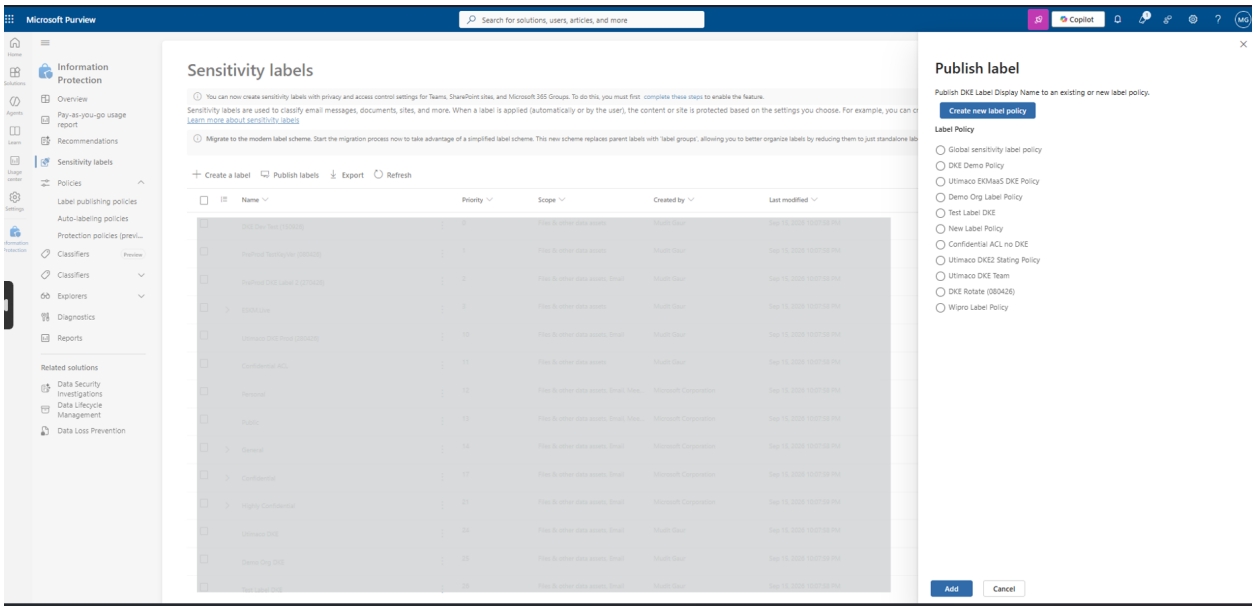


Figure 35 : Publish label

3. On **Choose sensitivity labels to publish**, select **Choose sensitivity labels to publish**, select the sensitivity label created earlier, and then select **Add,** and then select **Next**.

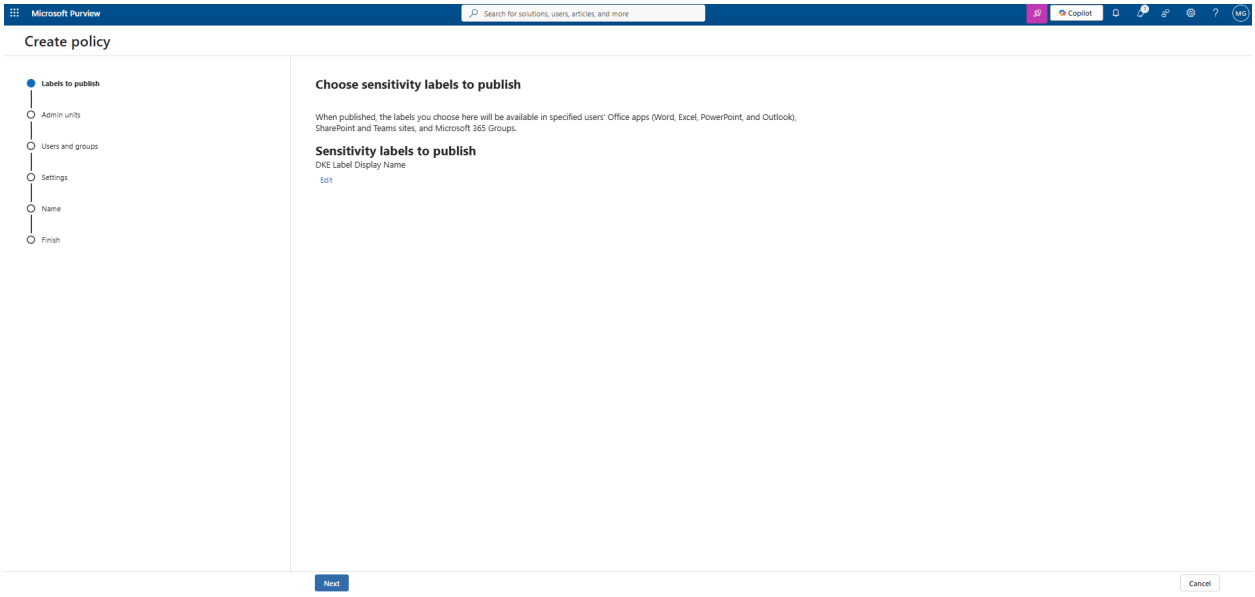


Figure 36 : Choose sensitivity labels to publish

4. On **Publish to users and groups**, specify the users or groups for which the sensitivity label should be available, and then select **Next**.

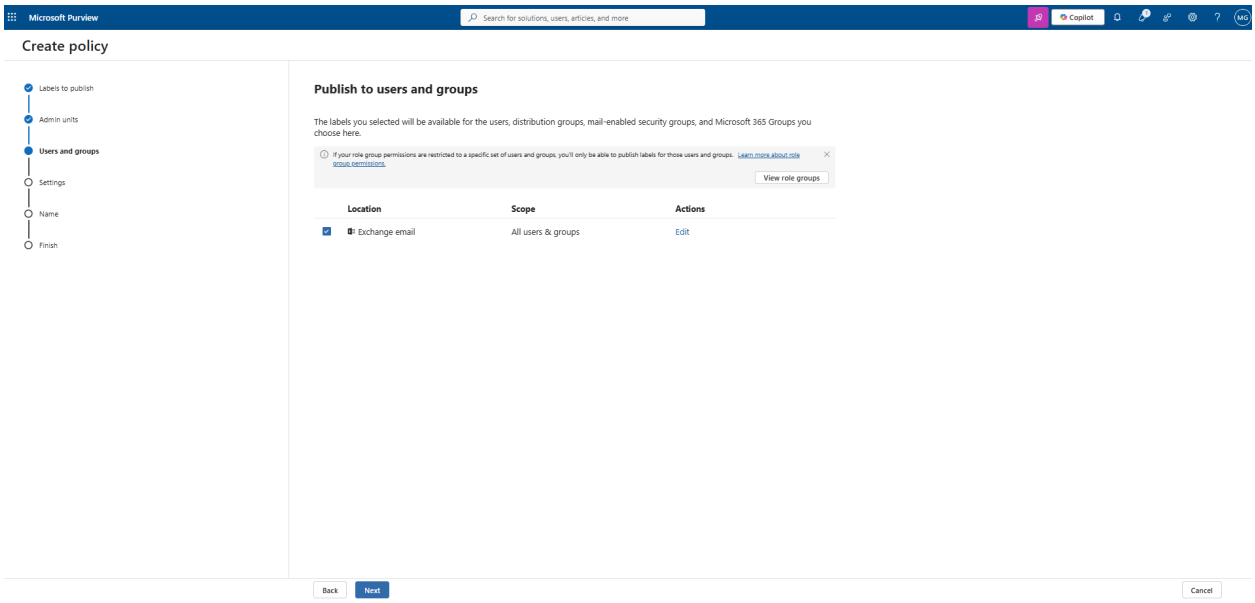


Figure 37 : Publish to users and groups

5. On **Policy settings**, configure the required policy settings as applicable:
    a. Users must provide a justification to remove a label or lower its classification.
    b. Require users to apply a label to their emails and documents.
    c. Require users to apply a label to their Fabric and Power BI content.
    d. Provide users with a link to a custom help page.

Then select **Next**.

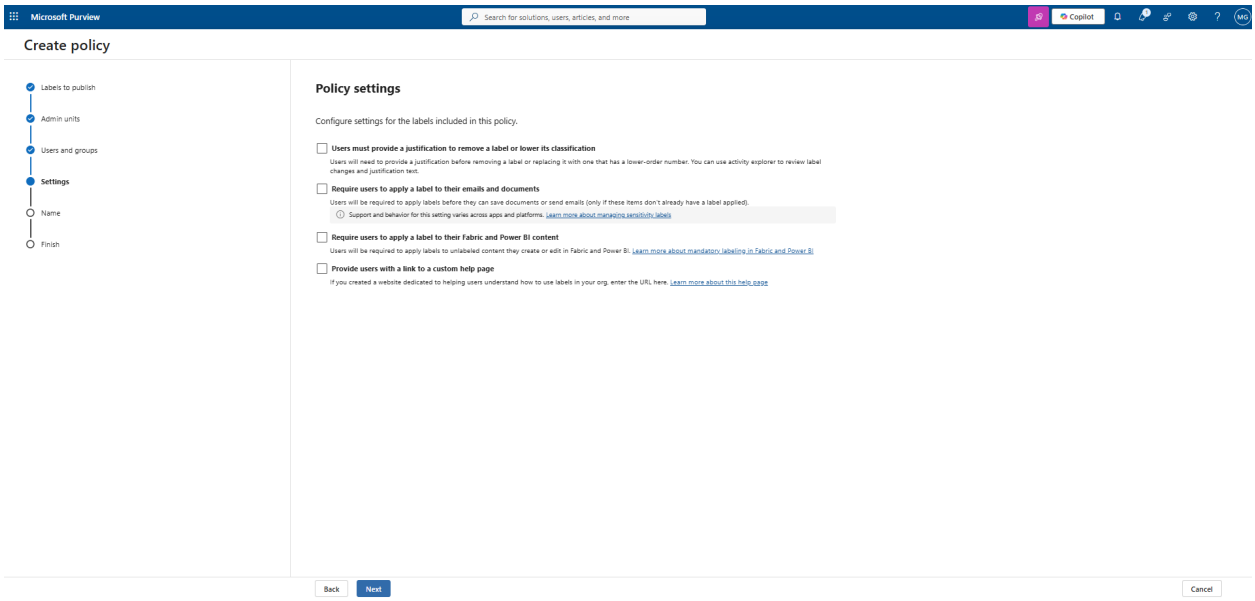


Figure 38 : Policy settings

6. Configure the default label settings for **Documents**, **Emails**, **Meetings**, and **Fabric and Power BI** as required **on the subsequent pages**, selecting **Next** after each configuration.

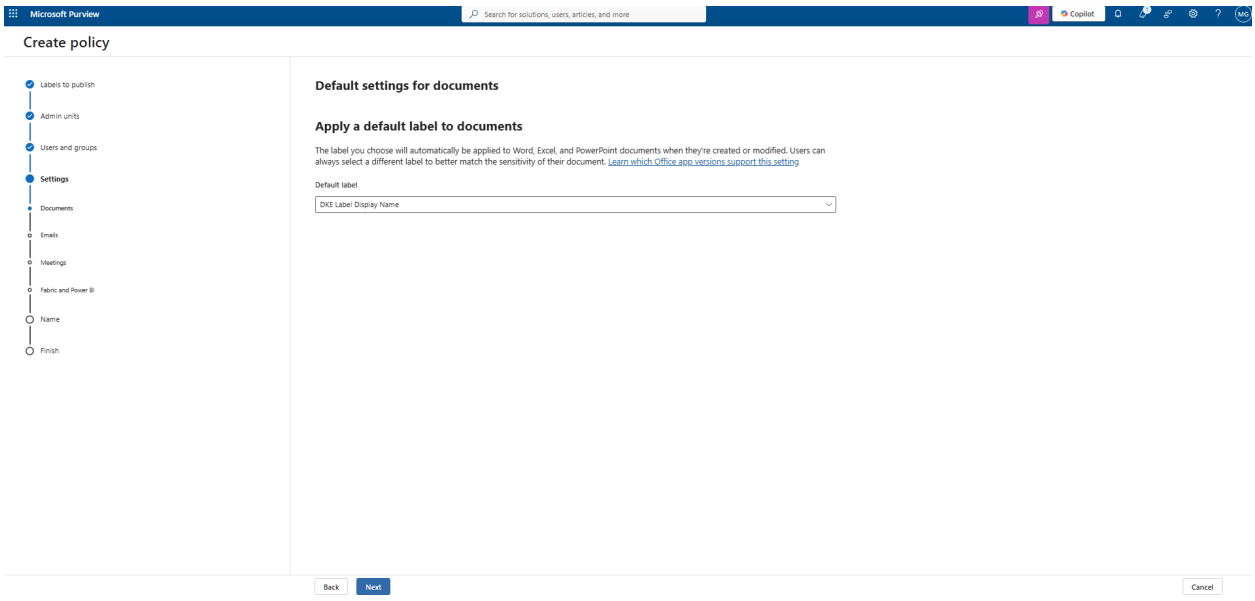


Figure 39 : Default settings for documents

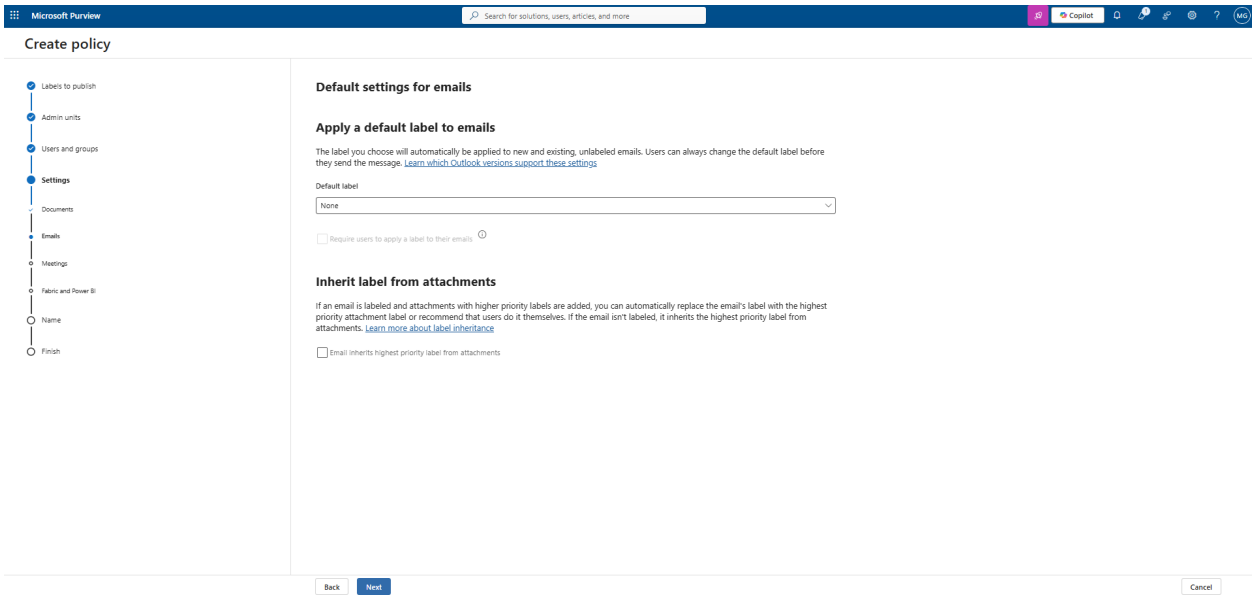


Figure 40 : Default settings for emails

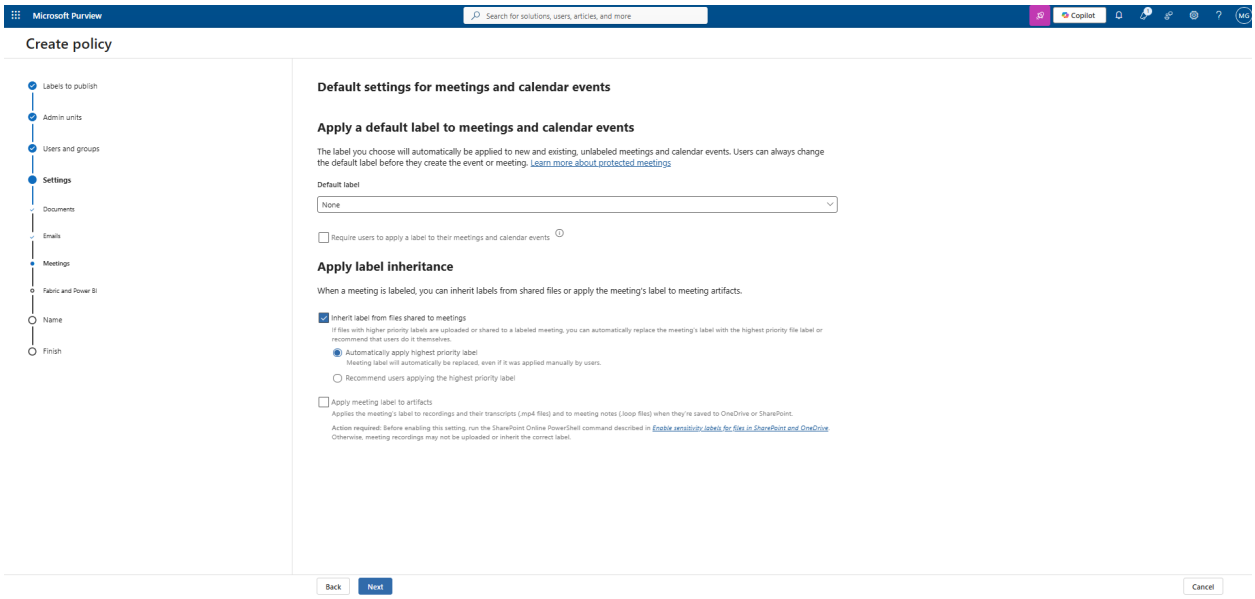


Figure 41 : Default settings for meetings and calendar events

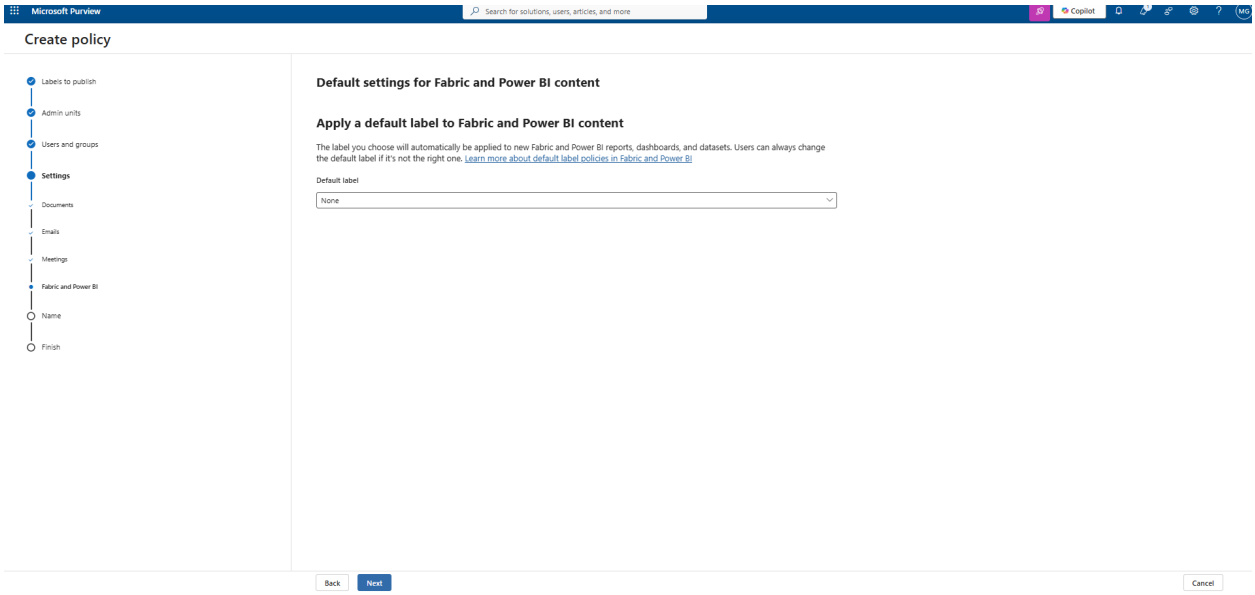


Figure 42 : Default settings for Fabric and Power BI content

7. On **Name your policy**, enter a **Name** for the sensitivity label policy and, optionally, provide a **Description**. Select **Next**.

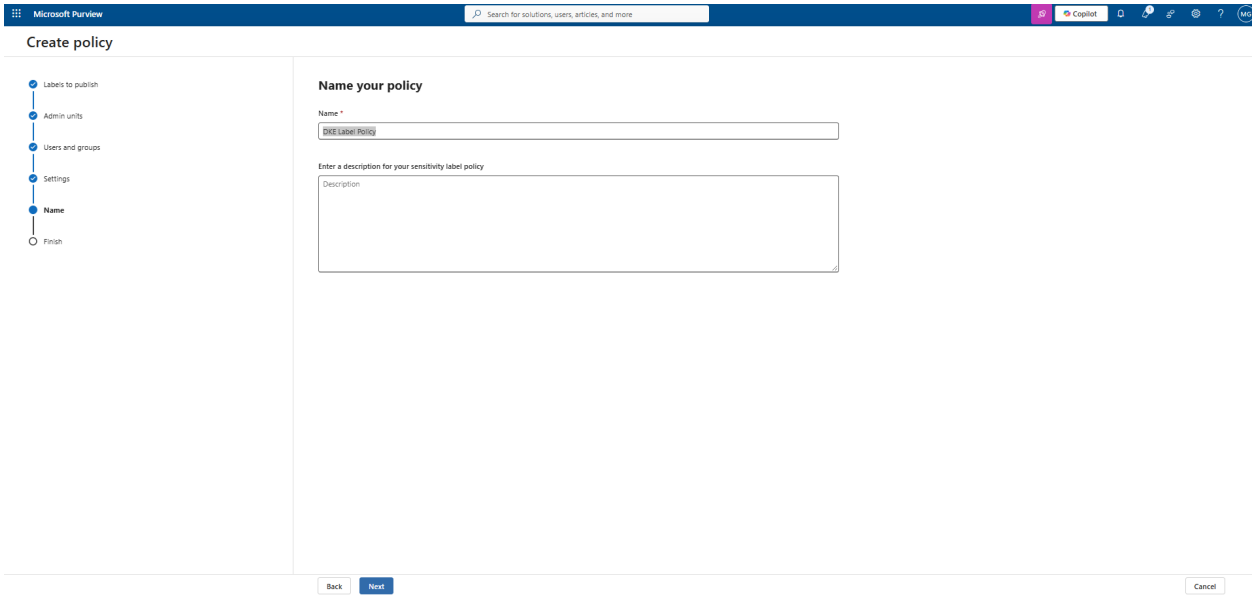


Figure 43 : Name your policy

8. On **Review and finish**, review the policy configuration and make any required changes. Select **Submit** to create the policy.

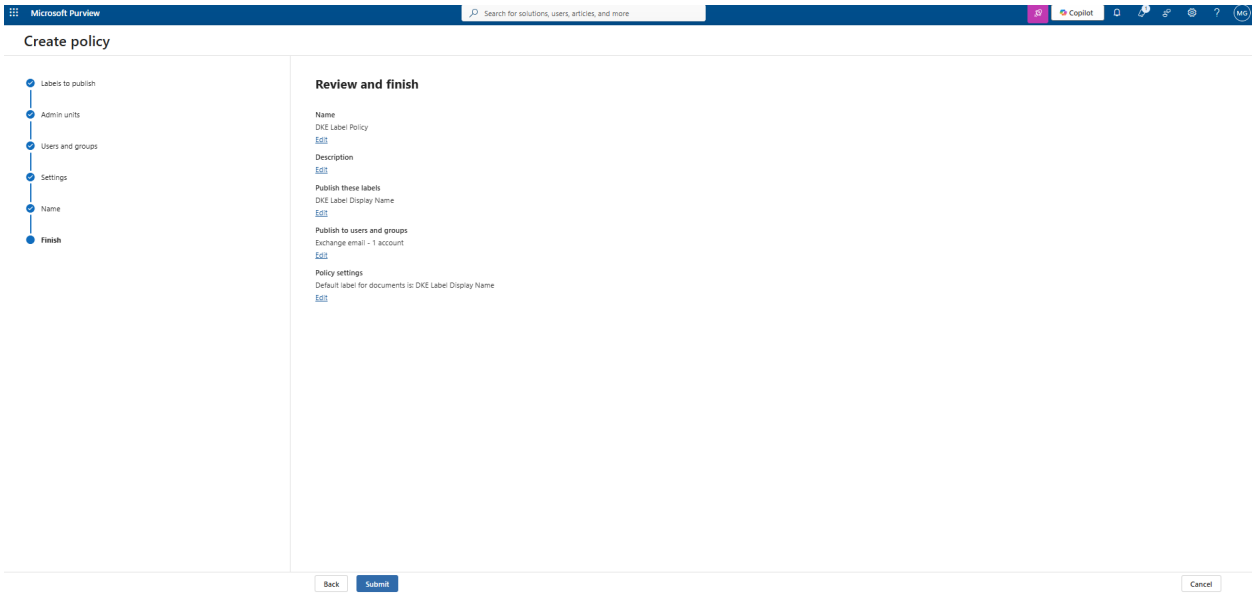


Figure 44 : Review and finish

9. On **New policy created**, verify that the policy was created successfully, and then select **Done**.

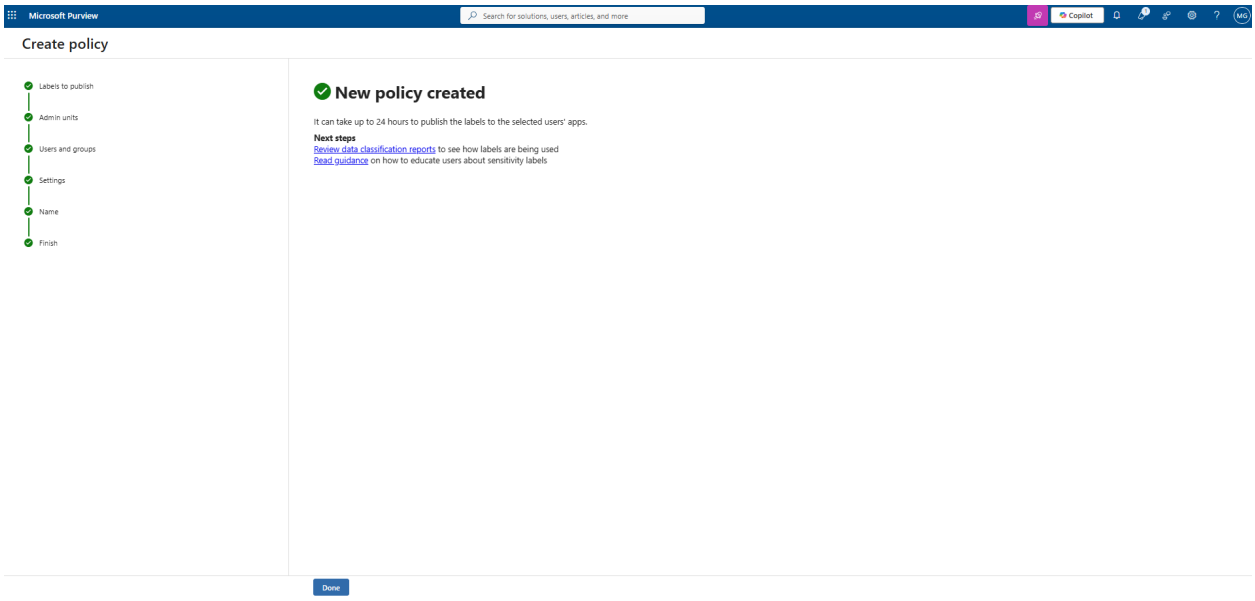


Figure 45 : New policy created



It may take up to 24 hours for the clients to refresh with the new labels.

7.4 Install Azure Information Protection Unified Labelling Client

Please ensure that the Azure Information Protection Unified Labeling Client is installed on each client machine. Use the following URL to download the Azure Information Protection Unified Labeling Client:

https://www.microsoft.com/en-us/download/details.aspx?id=53018

7.5 Verify Encryption and Decryption with DKE on Microsoft 365 Client

1. Log in to the client machine as a user for whom access has been provided while creating the key in Microsoft DKE instance. Refer to *Creating a Key on Microsoft DKE*.



Make sure before creating any file delete the cache folder data from both client machines on this location: C:\Users\<username>\AppData\Local\Microsoft\MSIP and MSIPC

2. Create a word document and assign a sensitivity label. (e.g., DKE).

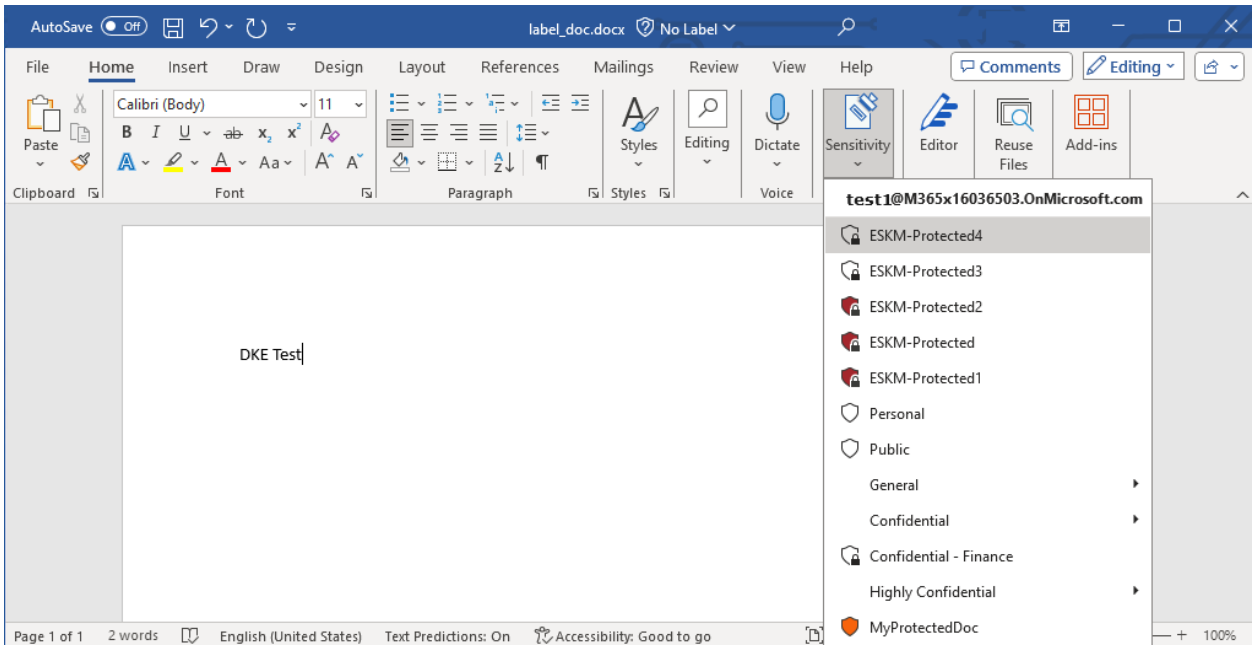


Figure 46 : Word Document

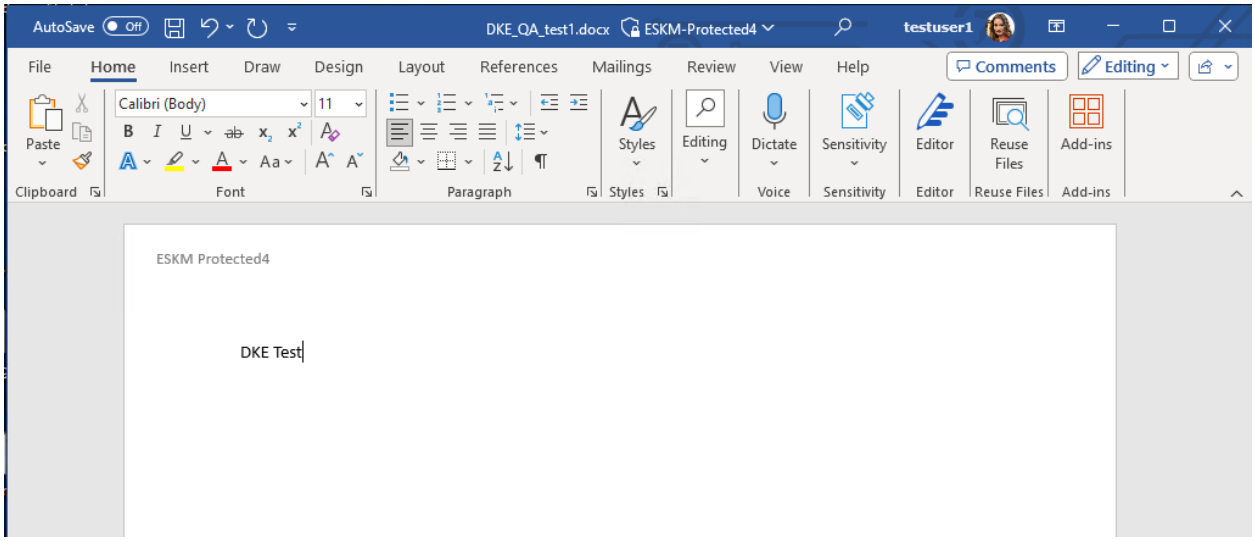


Figure 47 : Encrypted word document

3. Save this file to any location.

4. Copy this file to another client machine and user with allowed access to this sensitivity label and DKE.

5. Open the file and verify that this authorized user is able to open the document.

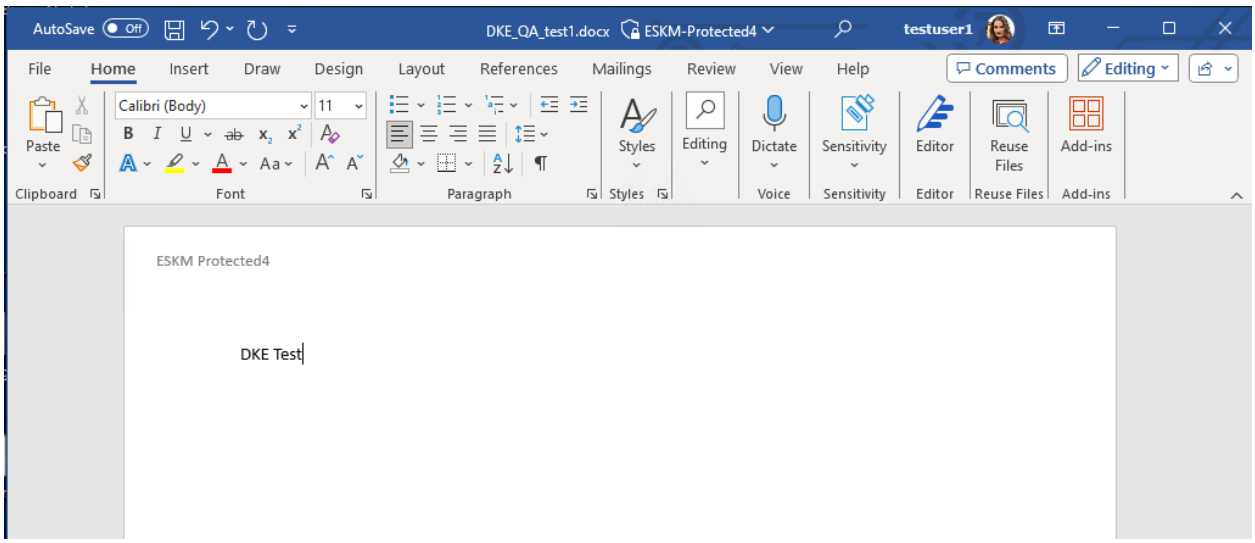


Figure 48 : Encrypted Word Document

6. Copy the same file to another client machine with a user who is not authorized to this sensitivity label and DKE.

7. Try to open the document. You will get an error with the below permission message.

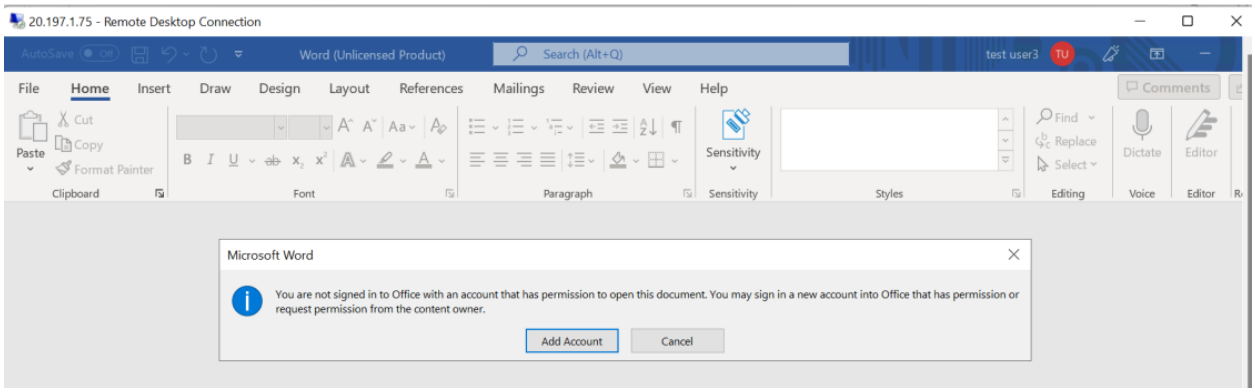


Figure 49 : Access denied message

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 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 Appendices

9.1 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 .