Microsoft Azure

DKE

Integration Guide (Supplement)

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-2026-0016

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 Abbreviations 4
1.2 Microsoft DKE 5
1.2.1 Prerequisites 5
2 ESKM Configurations 7
3 Azure DKE Configurations 8
3.1 Register Service with Azure 8
3.2 Create Sensitivity Labels using DKE 10
3.3 Publish the Labels 16
3.4 Install Azure Information Protection Unified Labeling Client 21
4 Verify Encryption and Decryption with DKE on Microsoft 365 Client 22
5 Further Information 25
6 Contact and Support Information 26

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All Utimaco SecurityServer product documentation is available from Utimaco's web site at https:// utimaco.com/.

1.1 About This Guide

This guide provides information on how to configure Utimaco ESKM for protecting office 365 documents with Microsoft DKE (Double Key Encryption). Please refer Microsoft Azure DKE_IntegrationGuide_ESKM for ESKM related configurations.

1.1.1 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
AIP	Azure Information Protection
API	Application Programming Interface
Azure AD	Azure Active Directory
CA	Certificate Authority
CSAR	Cloud Service Architecture
CSR	Certificate Signing Request
DKE	Double Key Encryption
FQDN	Fully Qualified Domain Name

Abbreviation	Meaning
GUI	Graphical User Interface
HSM	Hardware Security Module
IP	Internet Protocol
LAN	Local Area Network
PKCS#11	Public-Key Cryptography Standard #11
RSA	Rivest-Shamir-Adleman
URL	Uniform Resource Locator

Table 1: Abbreviations

1.2 Microsoft DKE

Double Key Encryption (DKE) uses two keys together to access protected content. Microsoft stores one key in Microsoft Azure, and the user holds the other key. The user maintains full control of one of their keys using the Double Key Encryption service. The user applies protection using the Azure Information Protection unified labeling client to their highly sensitive content.

Double Key Encryption supports both cloud and on-premises deployments. These deployments help to ensure that encrypted data remains opaque wherever the user stores the protected data.

1.2.1 Prerequisites

- Utimaco ESKM should be hosted publicly,
    - which has a FQDN (the app service URL)
    - which has a verified/registered domain
    - with https port 443 allowed through firewall and reachable from all AIP clients

- The ESKM should be available at the root path and no sub path specified.

2 ESKM Configurations



Please refer Microsoft Azure BYOK_IntegrationGuide_ESKM for the ESKM configurations.

Make sure that the following prerequisites are met:.

1. Login to ESKM Cloud WebUI.
2. Create Microsoft DKE Cloud instance.
3. Create a key in the DKE Cloud instance.

3 Azure DKE Configurations

3.1 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 Example.

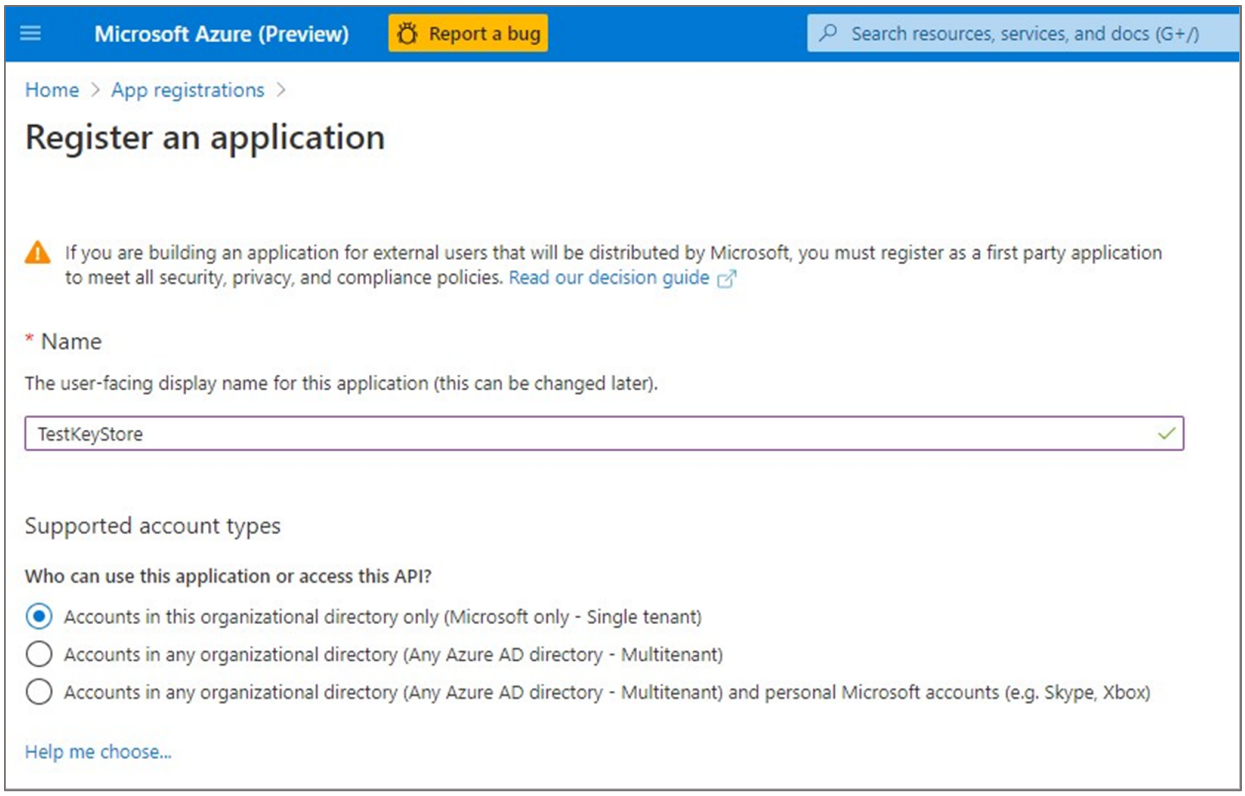


Figure 48: Register an application

Figure 1 : 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.
    a. For example: https://eskm.utimaco.com

The ESKM Public URL needs to be based on the root level, i.e., not a sub directory



*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 Alternatively, follow the below link from Microsoft to register your keystore on Azure https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption?view=o365worldwide%23register-your-key-store.

3.2 Create Sensitivity Labels using DKE

In the Microsoft 365 compliance center, Go to Information Protection section.

1. On Labels page, select + Create a Label to start the new sensitivity label configuration. For example, from the Microsoft 365 compliance center:

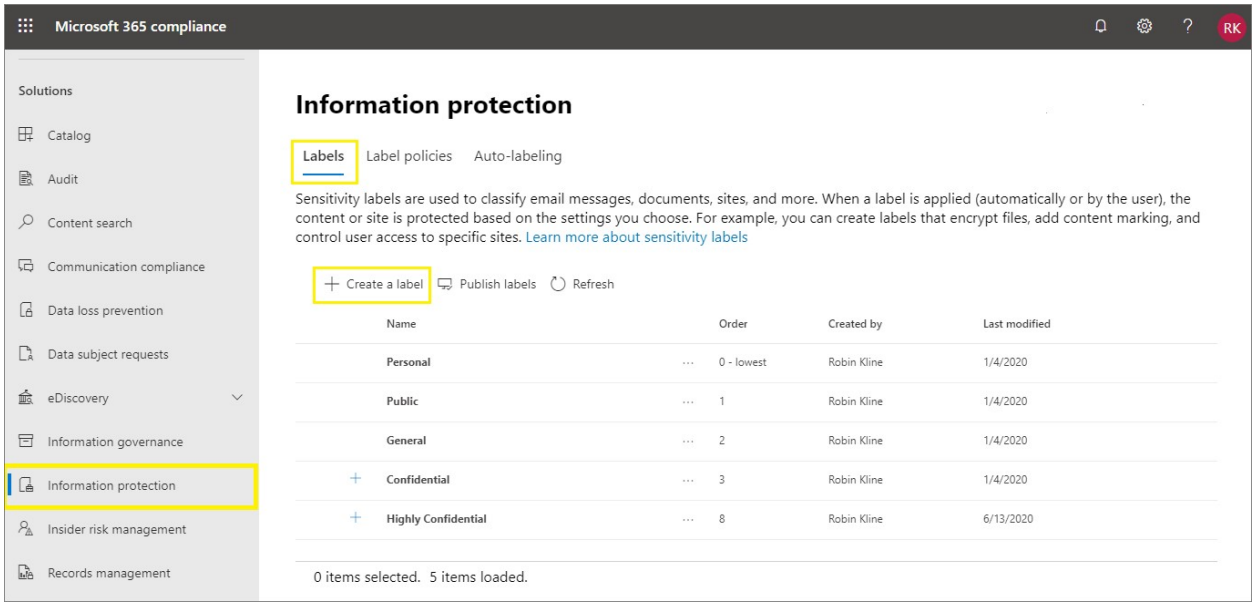


Figure 2 : Create Label

2. On Name and Create a tooltip for your label, specify the following.

- Label name - visible in Microsoft 365 compliance center
- Display name - visible to users in e.g., Microsoft word

- Description for users - the tooltip that appears when users hover over the sensitivity label
- Description for admin - the description available from the Microsoft 365 compliance center

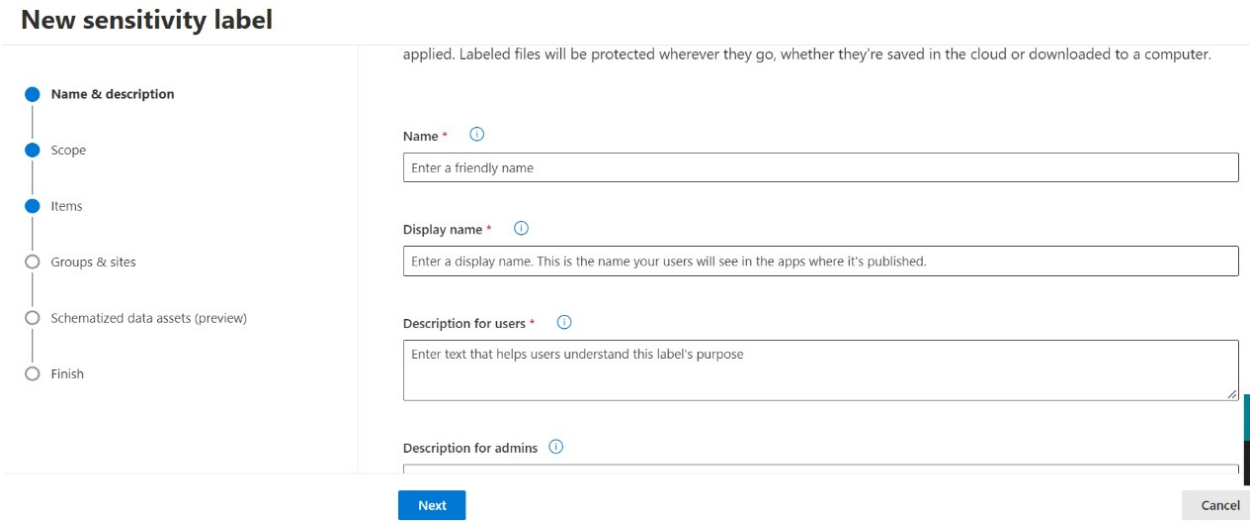


Figure 3 : Name and create a tooltip for your label window

3. Click on Next button.
4. Define the scope of the label. E.g., apply label to files & emails only.

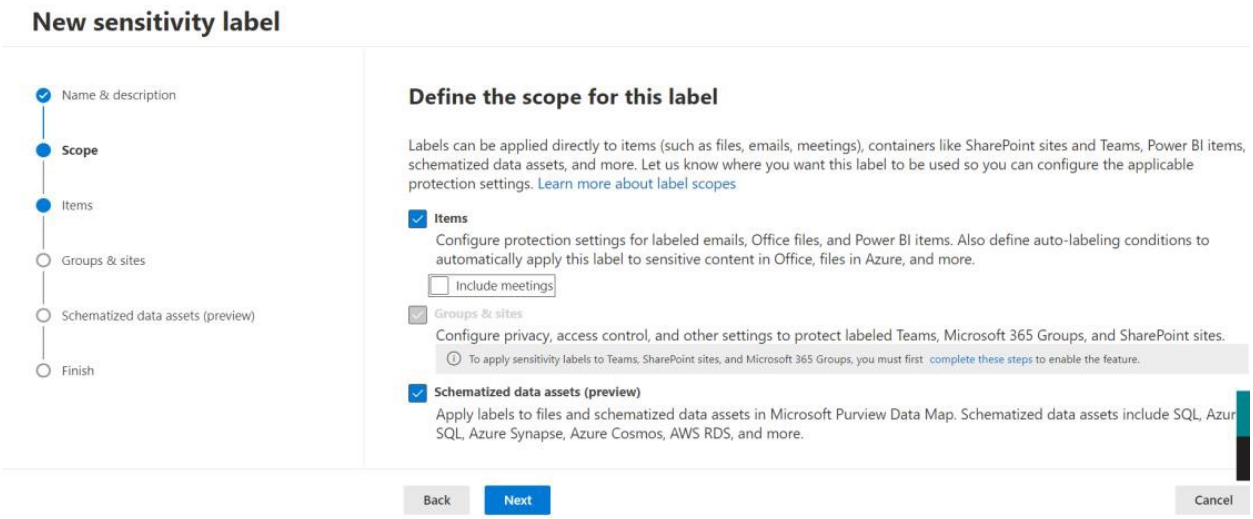


Figure 4 : Define the scope for this label window

5. Click on Next button.
6. Choose protection settings for file and emails.

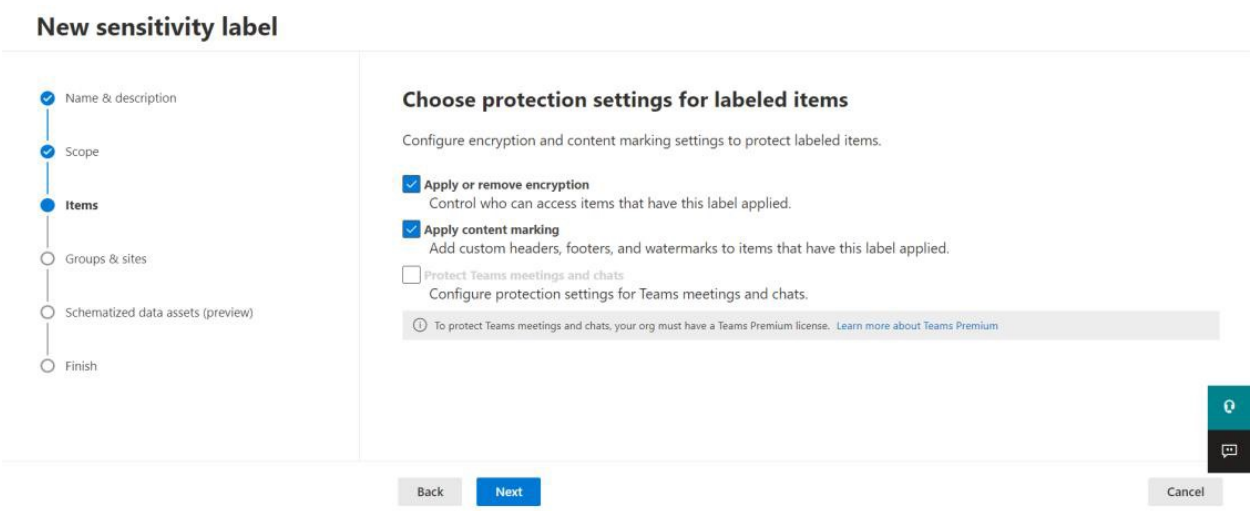


Figure 5 : Choose protection settings for files and emails window

7. In the Encryption step, you can set permissions to content with the label applied. Since the primary reason for this procedure is to secure the files, you'll want to configure encryption settings.

8. In most cases, you will use the Never expires option, since it will let users access files without any time limit.

9. You can also allow or deny offline access to a file. Without the offline access, a user will need to be reauthenticated each time they want to open a document or email.

10. Choose which users or groups should be able to access documents with the label set. Clicking Assign permissions opens a wizard on the right side.

11. Finally, select User Double Key Encryption checkbox and enter correct DKE URL along with key.

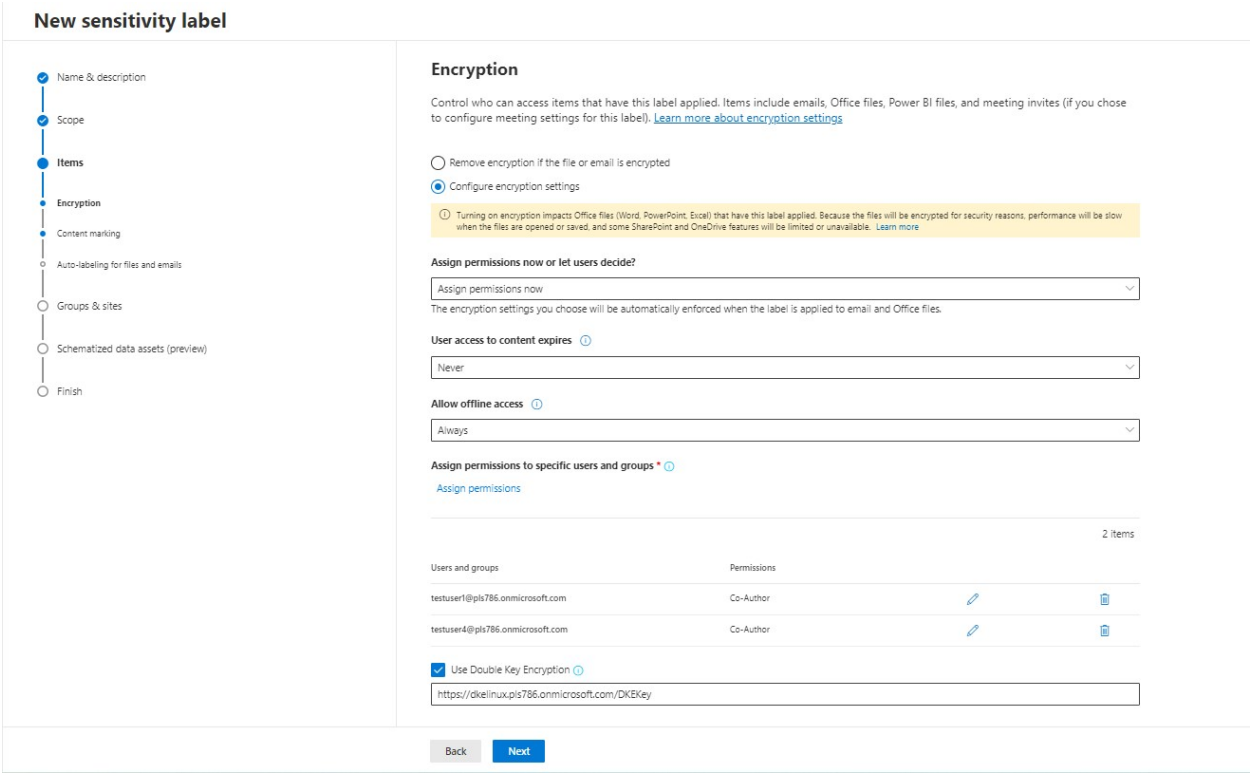


Figure 6 : Files & Emails Access window

Use the DKE Key URL from the ESKM Cloud UI. Refer Viewing Microsoft DKE Key Info in ESKM Cloud Integration document.



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

12. Content marking lets you add clear information about the applied labels directly to a document. You can choose if you want to add a watermark, a header and a footer, and what it should display on Microsoft word document.

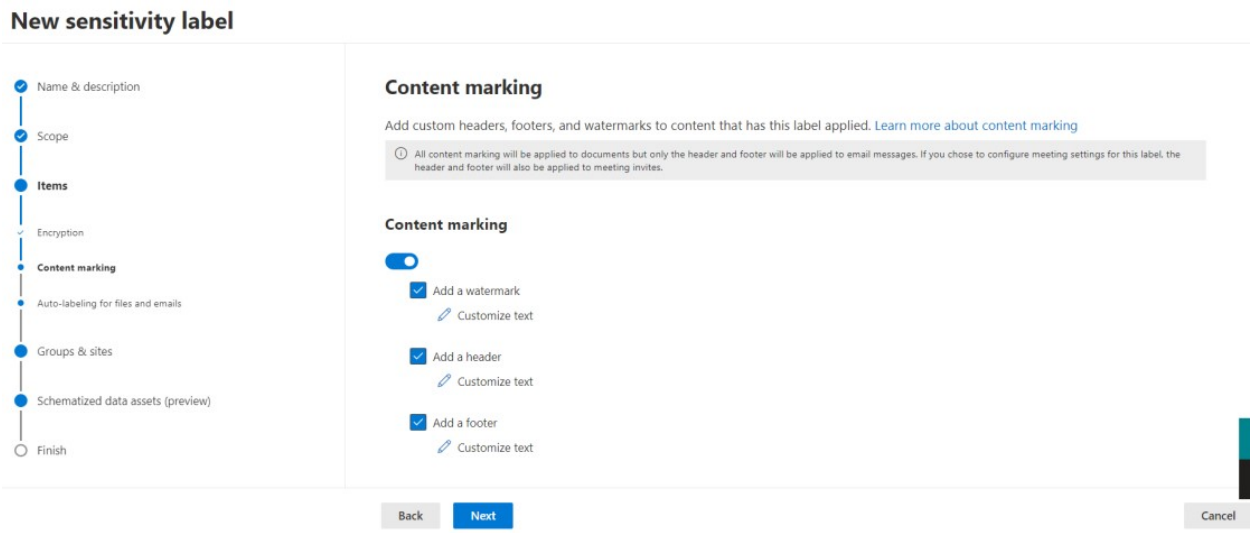


Figure 7 : Content Marking window

13. In the next step, you can turn on auto-labeling. That way certain groups or documents created in certain sites can be automatically marked with your label. This may be useful if you want to make sure nobody forgets about securing documents. On the other hand, auto-labeling can create problems if you intend to share some documents outside your organization.

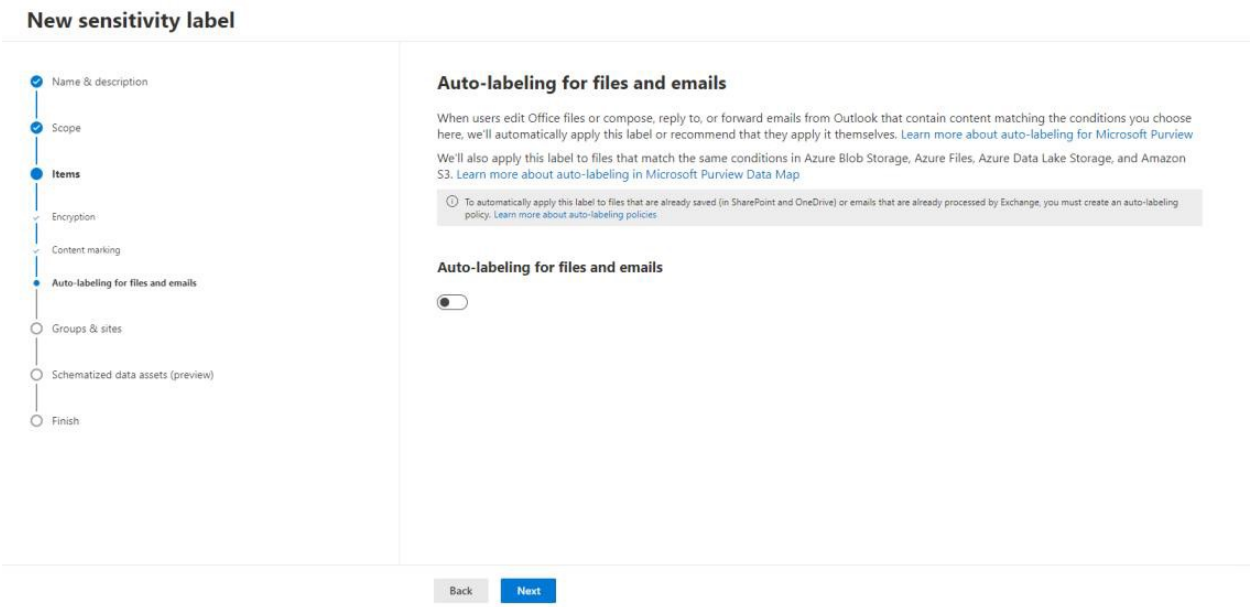


Figure 8 : Auto-Labelling for Files and Emails window

14. Click Next, you can define protection settings for groups and sites. Those settings, unlike the previous ones, apply to teams, groups or sites and not the documents stored in them.

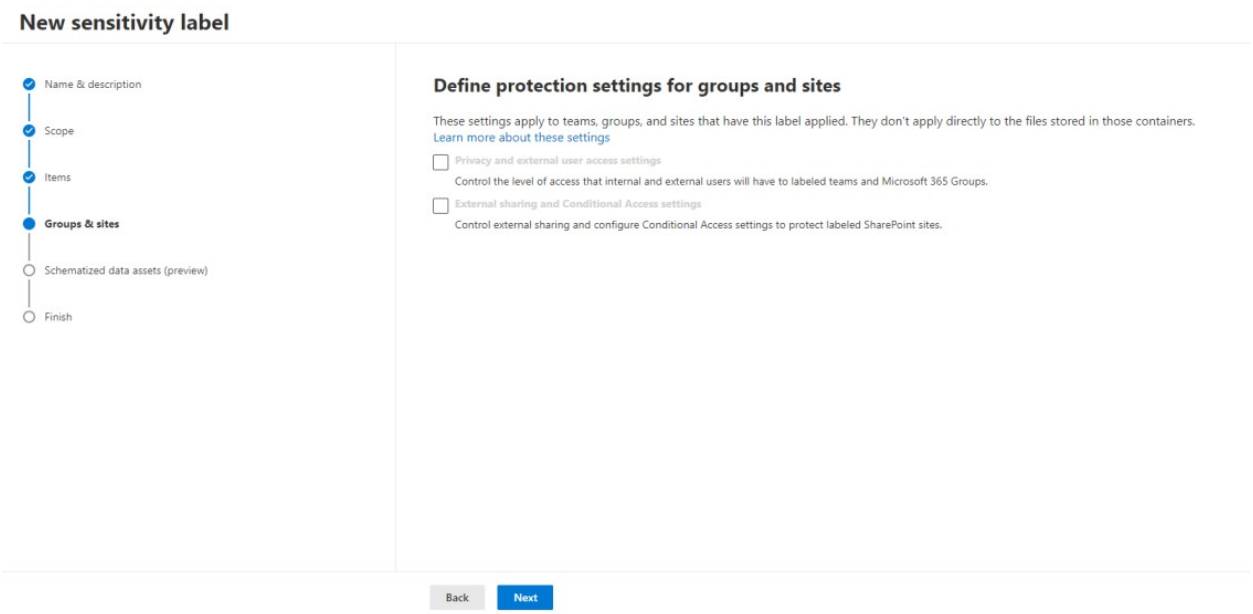


Figure 9 : Define protection settings for groups and sites

15. The last step is about revising the configuration. Revise your settings, click Create label and then Done.

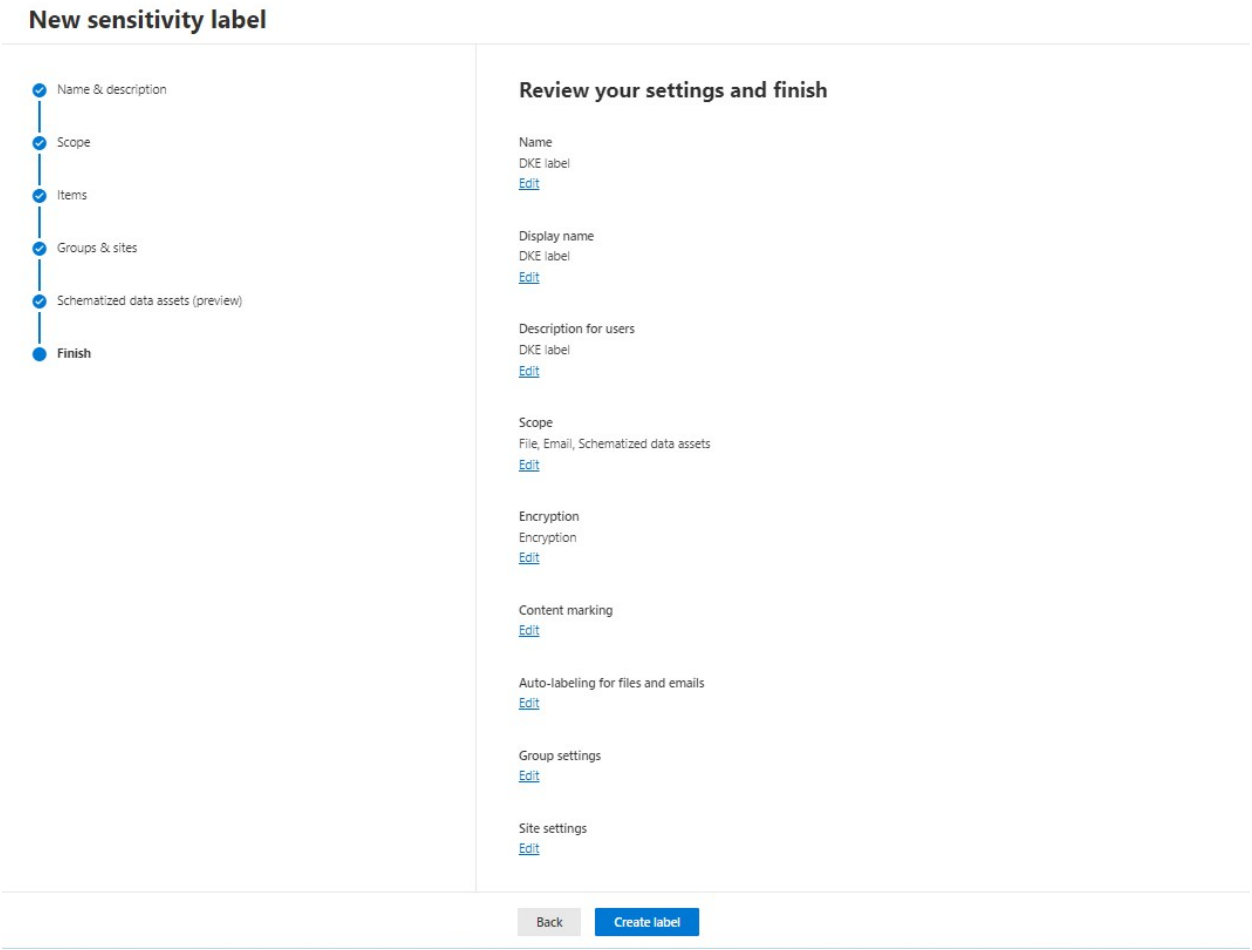


Figure 10 : Review your settings and finish window

3.3 Publish the Labels

1. To publish the label, go to Label policies and click Publish label.

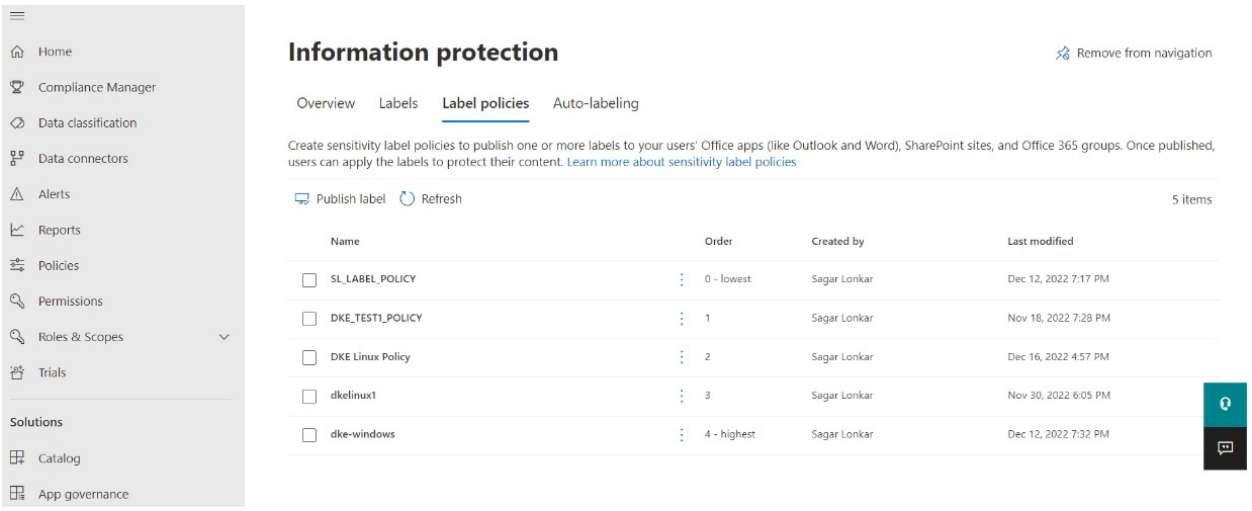


Figure 11 : Information Protection window

2. Click Choose sensitivity labels to publish and pick the label you've created earlier. Click Add and Next.

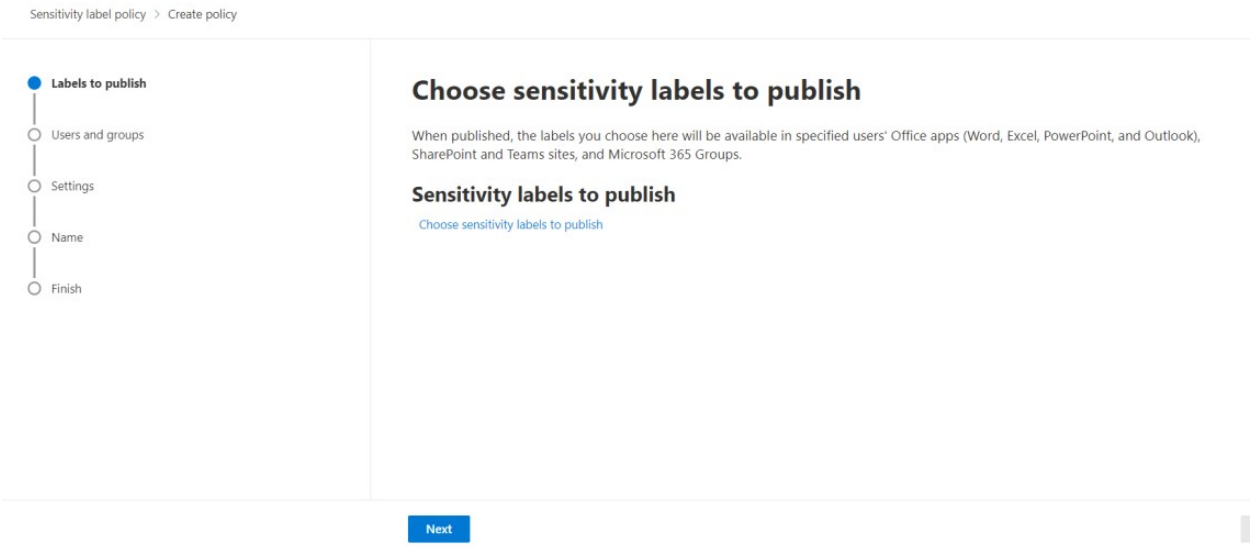


Figure 12 : Choose sensitivity labels to publish

3. Choose which groups or users should have the label available. Again, click Done and Next.

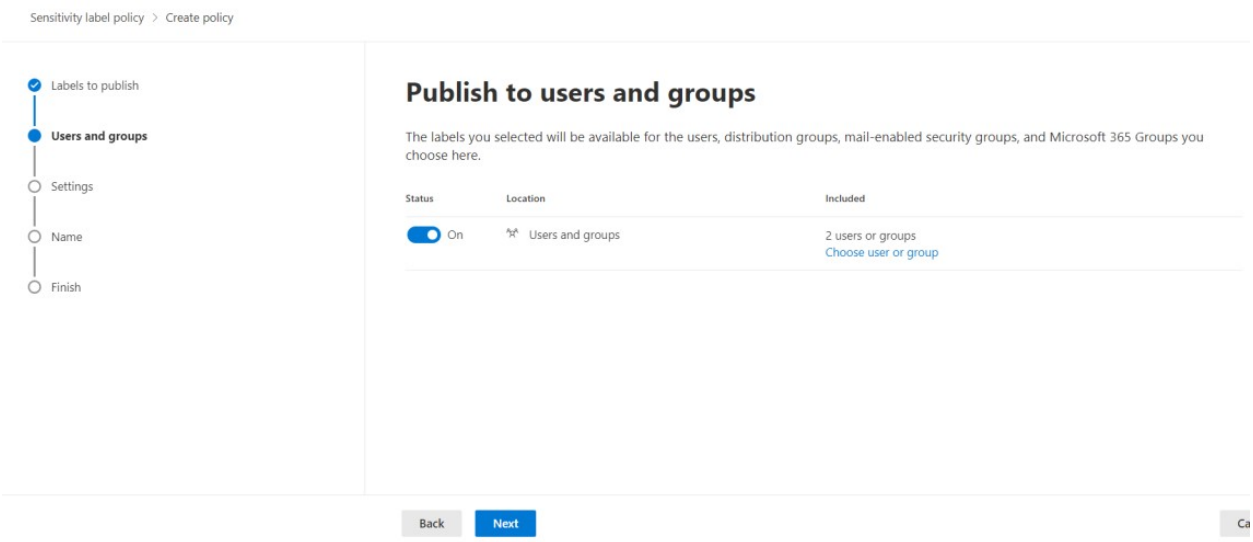


Figure 13 : Publish to users and groups

4. Next, you can choose to use various policy settings:

- Users must provide a justification to remove the label or lower its classification.
- Require users to apply the label to their emails and documents.
- Require users to apply the label to their Power BI content.
- Provide users with a link to a custom help page.

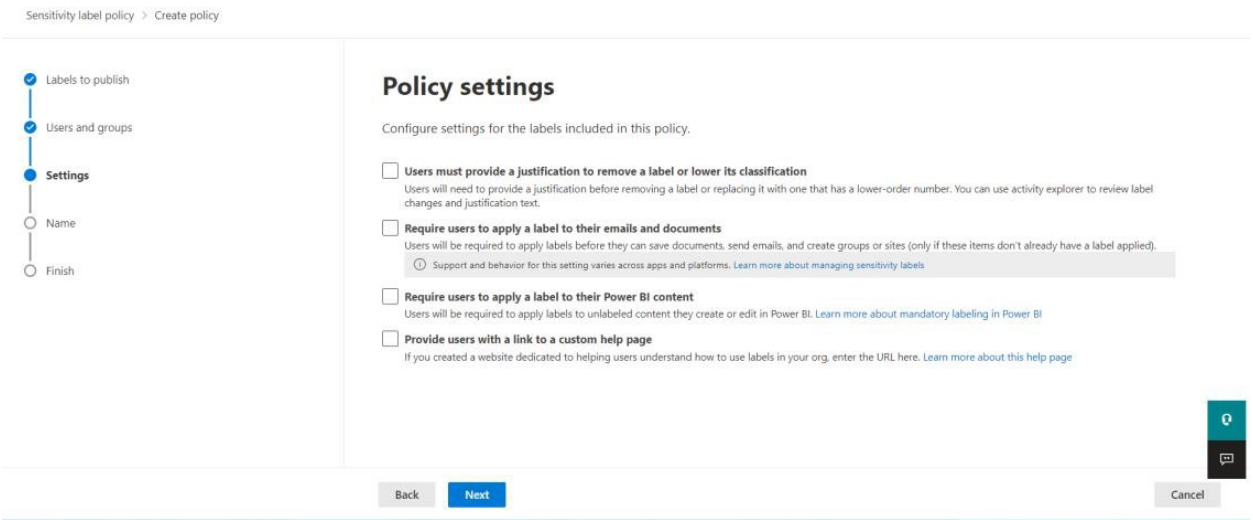


Figure 14 : Policy settings window

5. The next step allows you to apply the default label to documents. If you leave the default None option, users will have the choice to apply the label or use the document without

enhanced protection. Two next steps of the wizard let you configure the default labels for emails and Power BI.

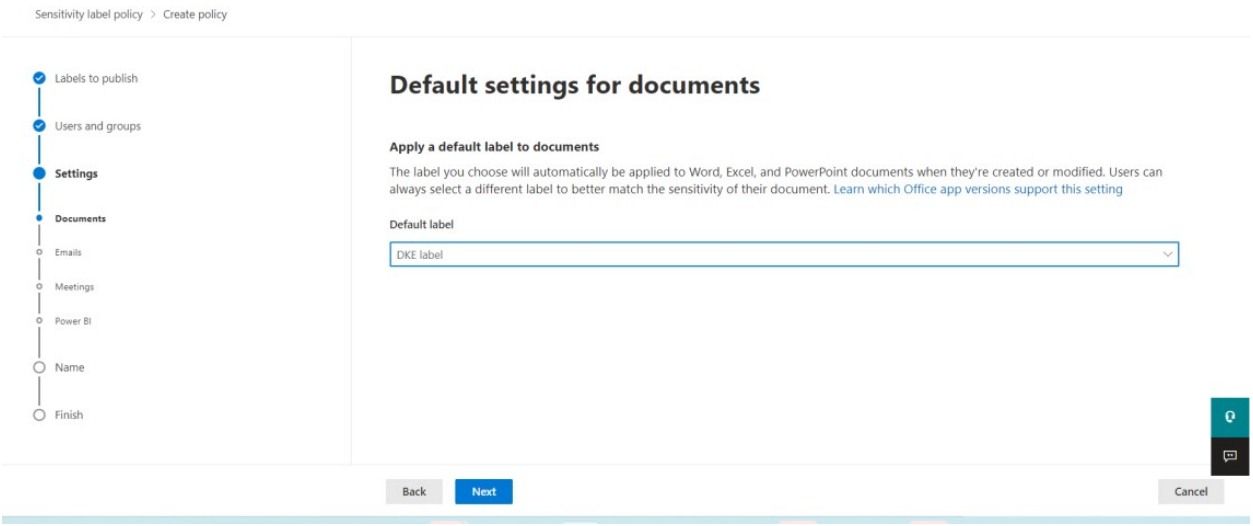


Figure 15 : Apply a default label to documents window

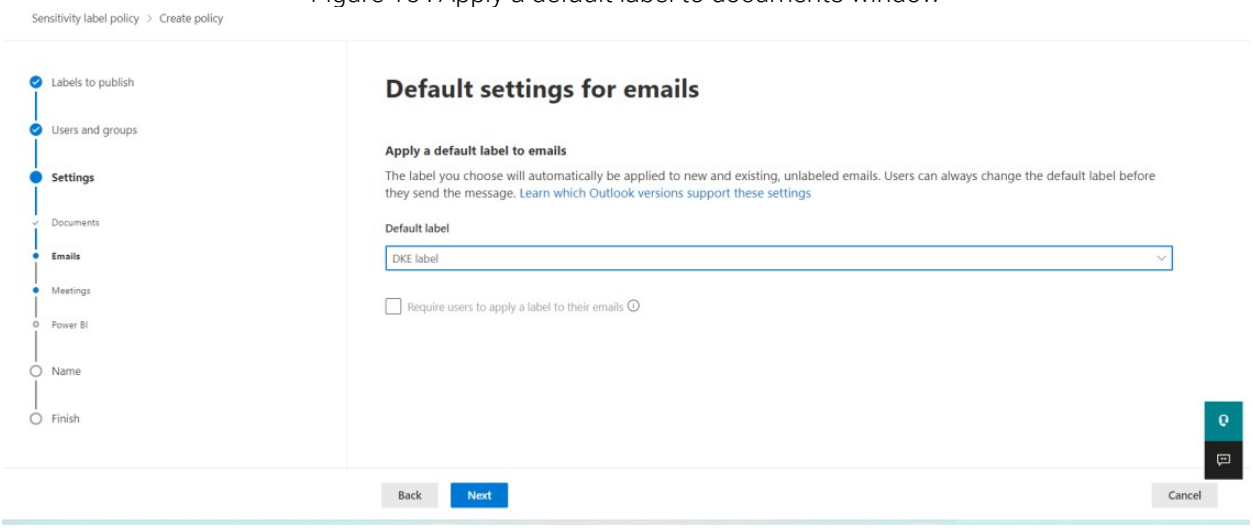


Figure 16 : Apply a default label to emails window

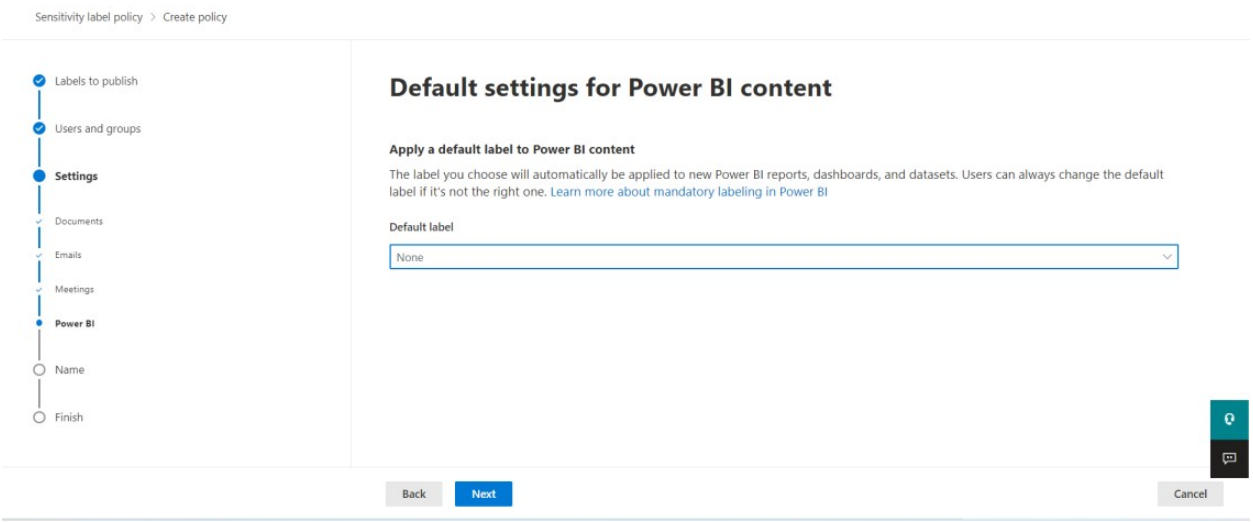


Figure 17 : Apply a default label to Power BI content (preview) window

6. Now you can name your label policy and provide a description.

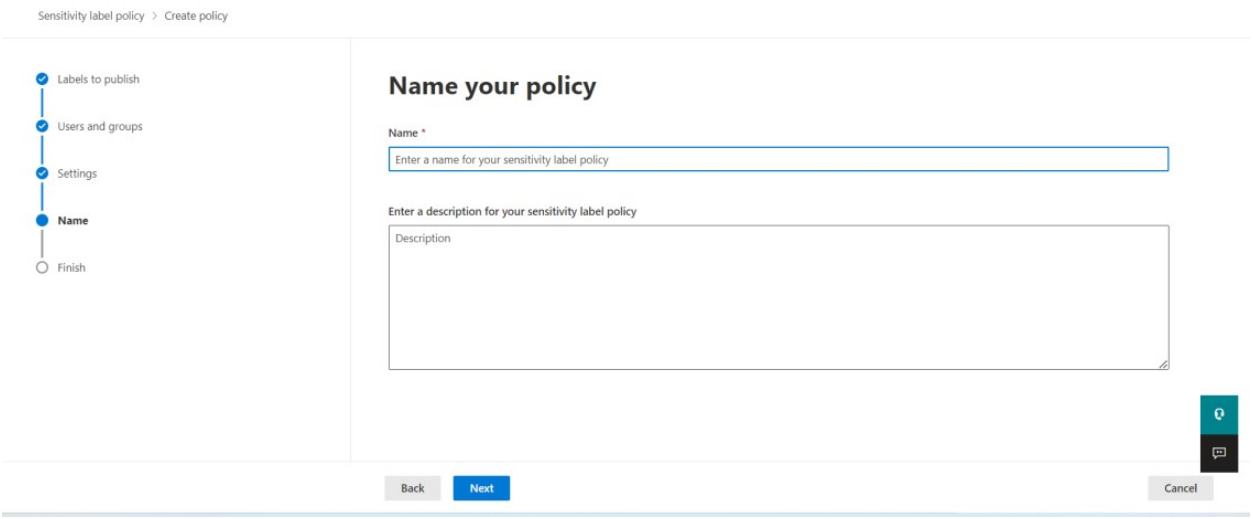


Figure 18 : Name your policy window

7. Finally, review your policy. Click Done when everything is set.

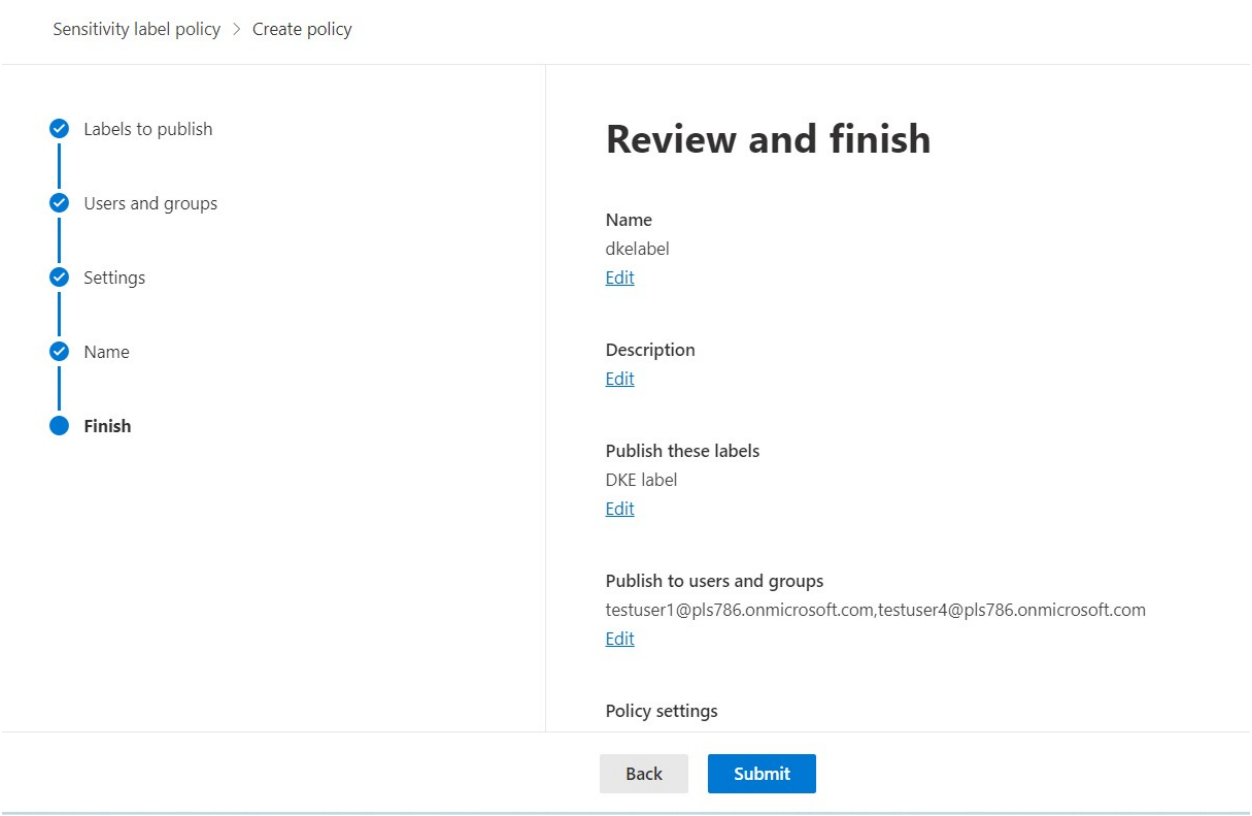


Figure 19 : Review and finish window

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

3.4 Install Azure Information Protection Unified Labeling Client

Please ensure that azure information protection unified labeling client is installed on each client machine. Please use below URL to download the Azure Information protection Unified Labeling client.

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

4 Verify Encryption and Decryption with DKE on Microsoft 365 Client

1. Login to client machine with user to whom access has been provided while creating the key in Microsoft DKE instance. Refer “Microsoft Azure DKE_IntegrationGuide_ESKM > Creating a key on Microsoft DKE".

Make sure before creating any file delete the cache folder data from both client machine on this location: C:\Users\testuser4\AppData\Local\Microsoft\MSIP and MSIPC.

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

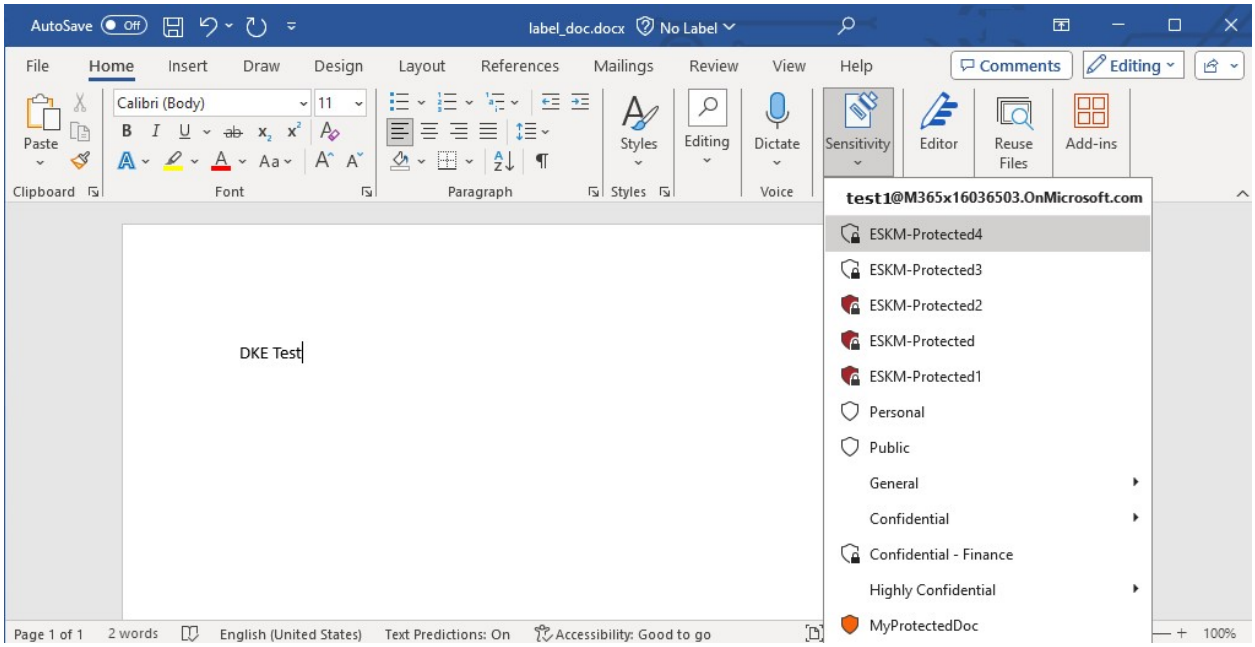


Figure 20 : Word Document

3. Save this file on any location.

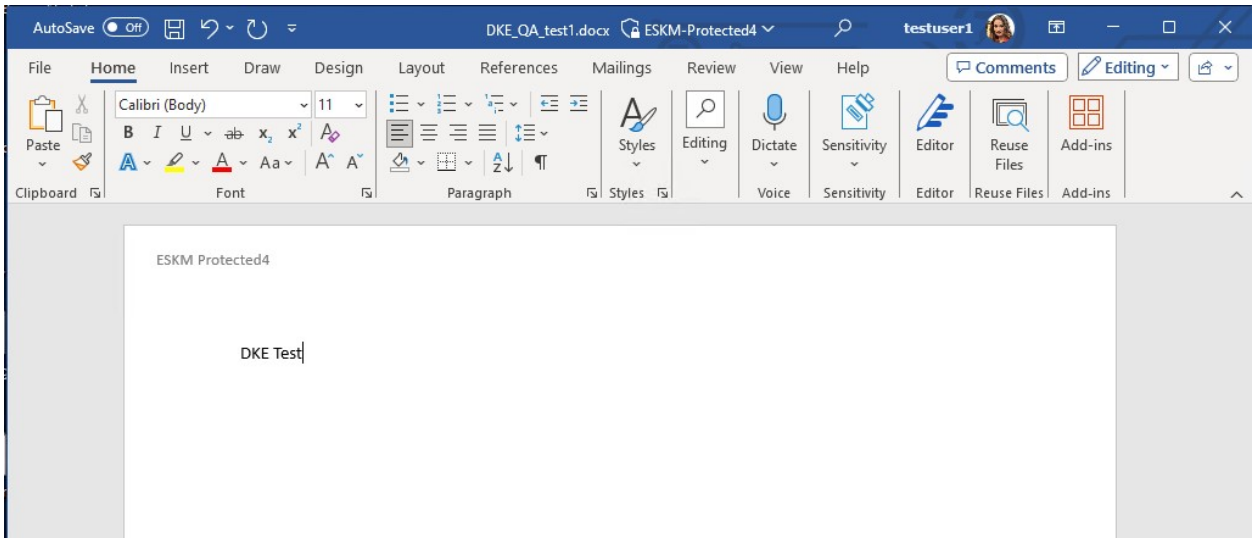


Figure 21 : Encrypted Word Document

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.

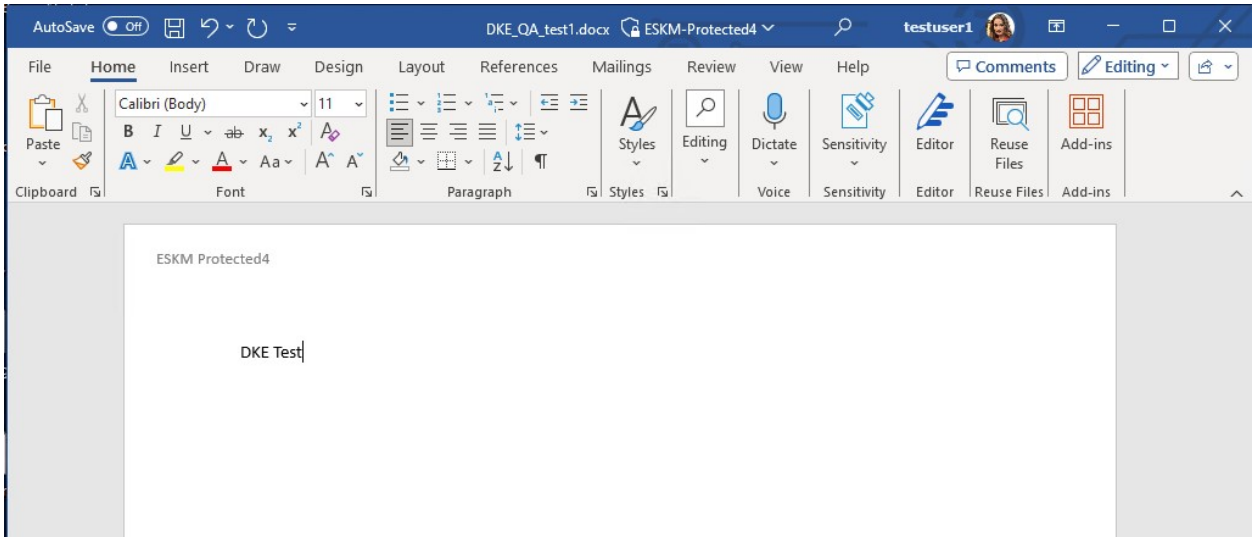


Figure 22 : Encrypted Word Document

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

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

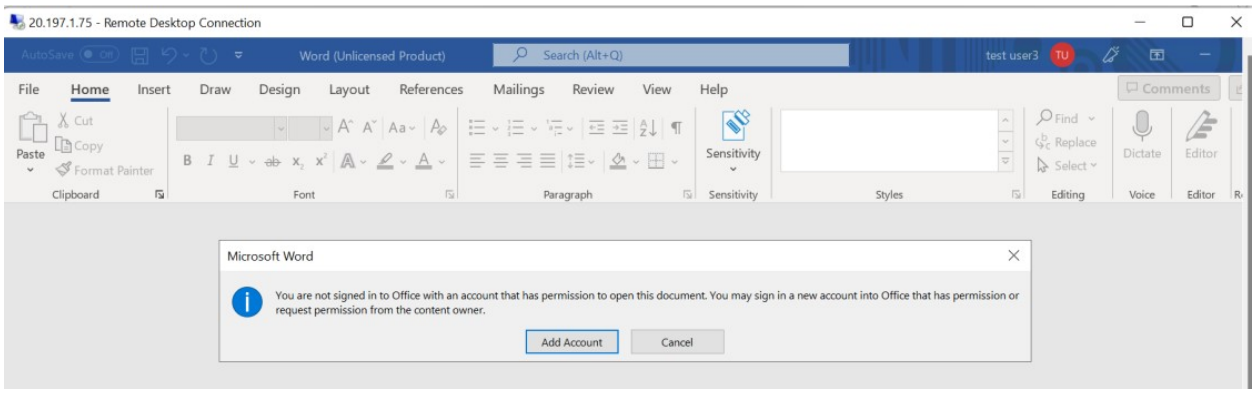


Figure 23 : Access Denied Message

5 Further Information

To refer to Microsoft DKE documentation, see: 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.