Microsoft Azure

BYOK

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	2026-03-19
Status	PUBLISHED
Document No.	IG-2026-0007

Table of Contents

1 About this Guide

This document is intended to define the requirements for Microsoft Azure Key Vault Creation and its components. It lists the prerequisites for integrating Utimaco ESKM with Microsoft Azure Cloud Service to support Bring Your Own Key (BYOK) feature.

This document is not intended to be a comprehensive guide to Microsoft Azure and its key valult but a guidance on how to prepare the environment for integration with Utimaco ESKM. For any further questions and changes, please contact your Cloud Administrator or Microsoft Azure Customer Contact services.

2 Introduction

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

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

3 Create a Key Vault

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

To create a key vault:

- Sign in to the Microsoft Azure portal at https://portal.azure.com/.
- In the Microsoft Azure portal Home page, select Create a resource at the left.
- In the Search box, enter Key Vault and select Key Vault.
- On the Key Vault section, choose Create.

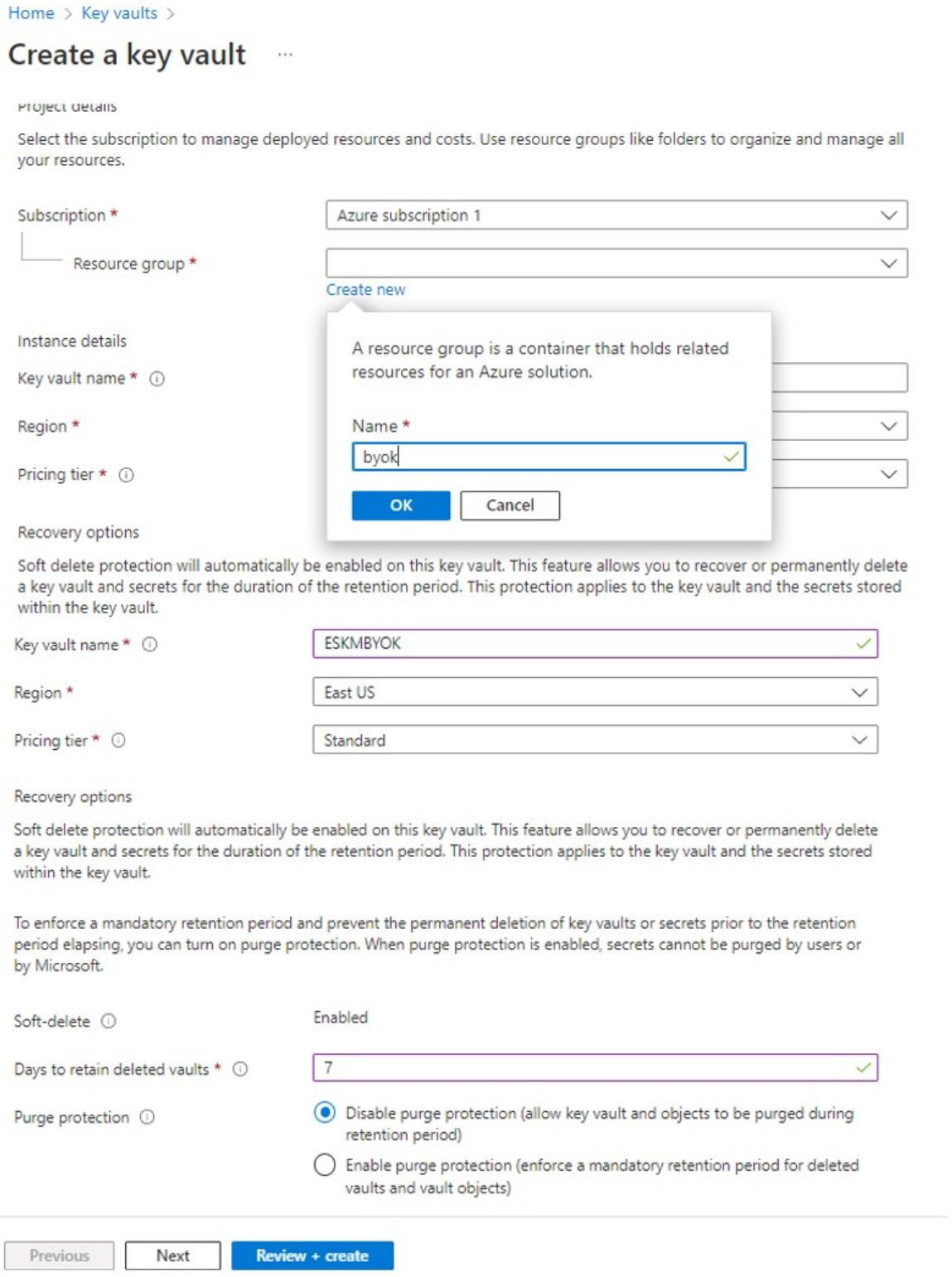


Figure 1 : Create a key vault

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

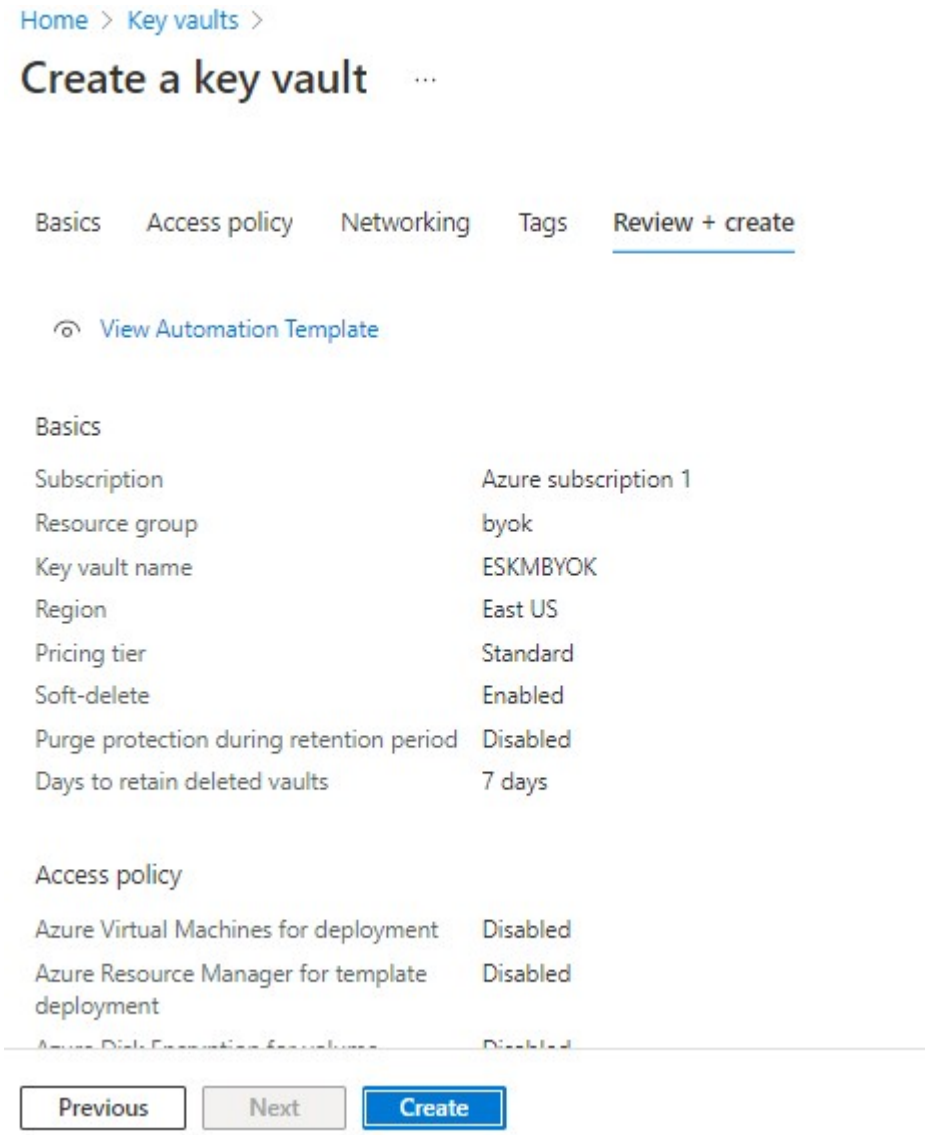


Figure 2 : Review + create

- Review the information provided and click Create.

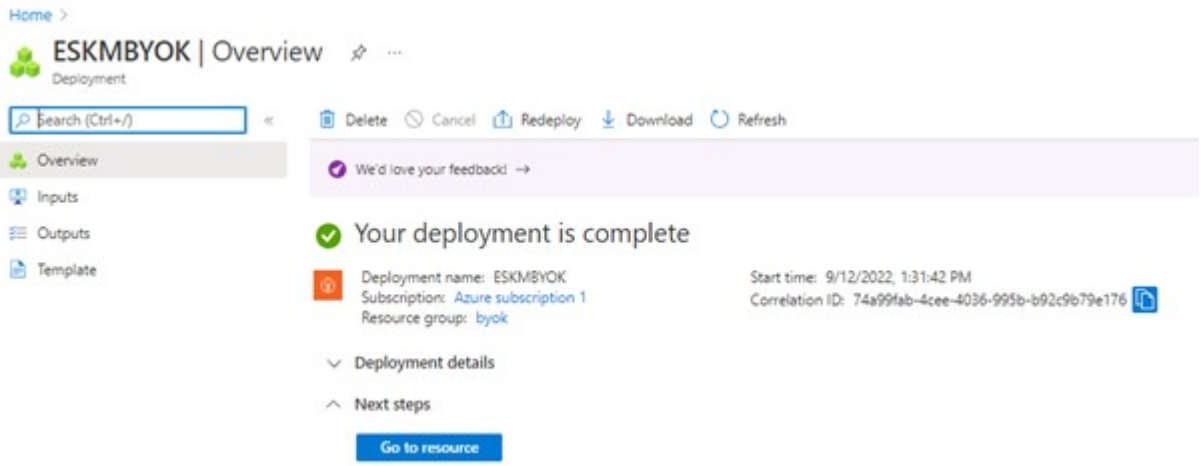


Figure 3 : Your deployment is complete

4 Register an Application

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

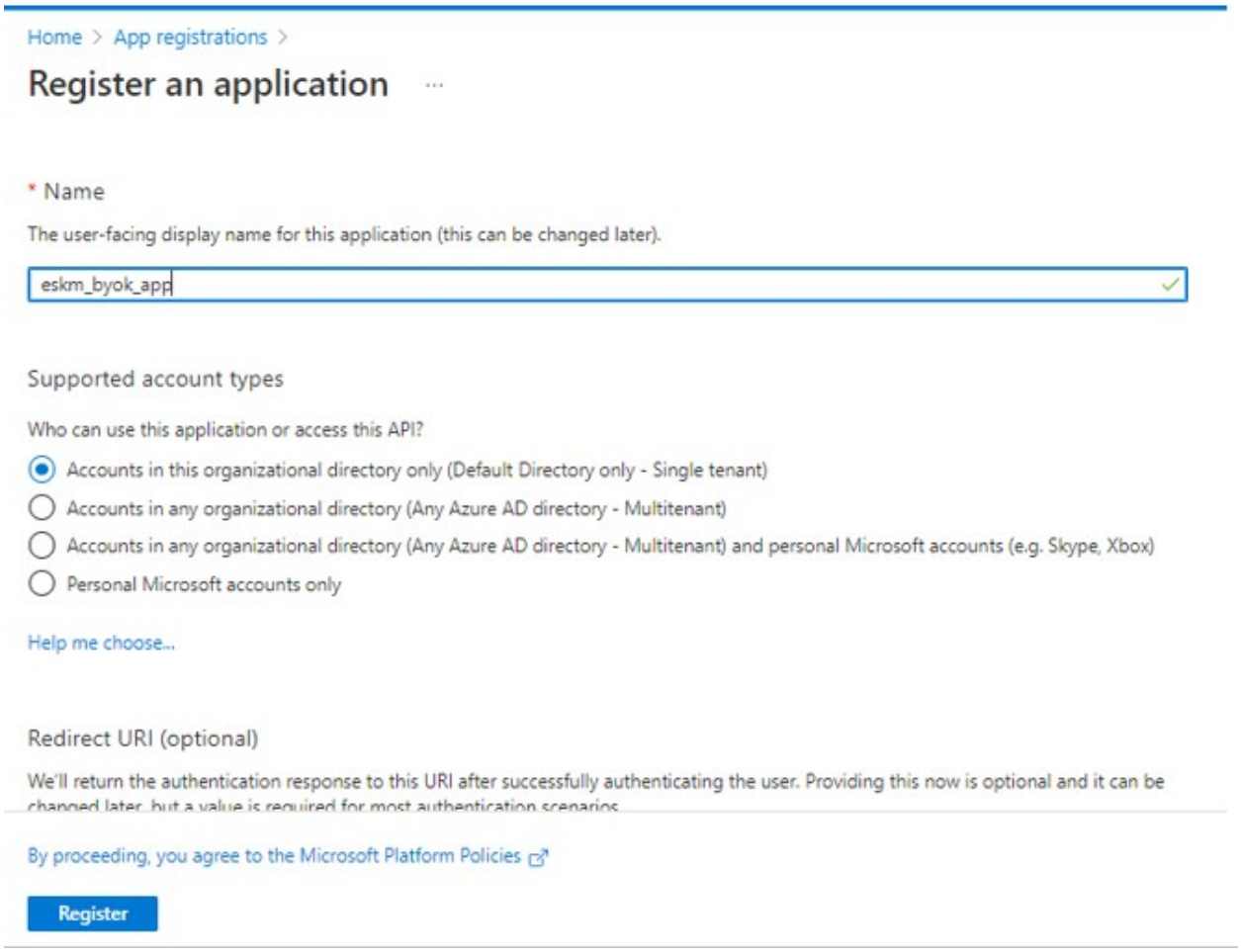
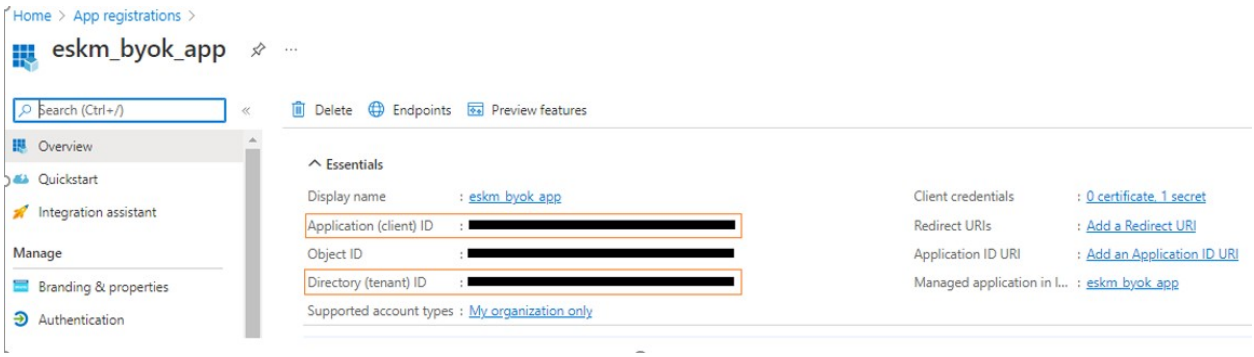


Figure 4 : Register an Application

Click Register. Your Application has created successfully and you can see the details.



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

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

4.1 Create Secret key

In the application page, go to Certificate & Secrets as seen in the screenshot shown below.

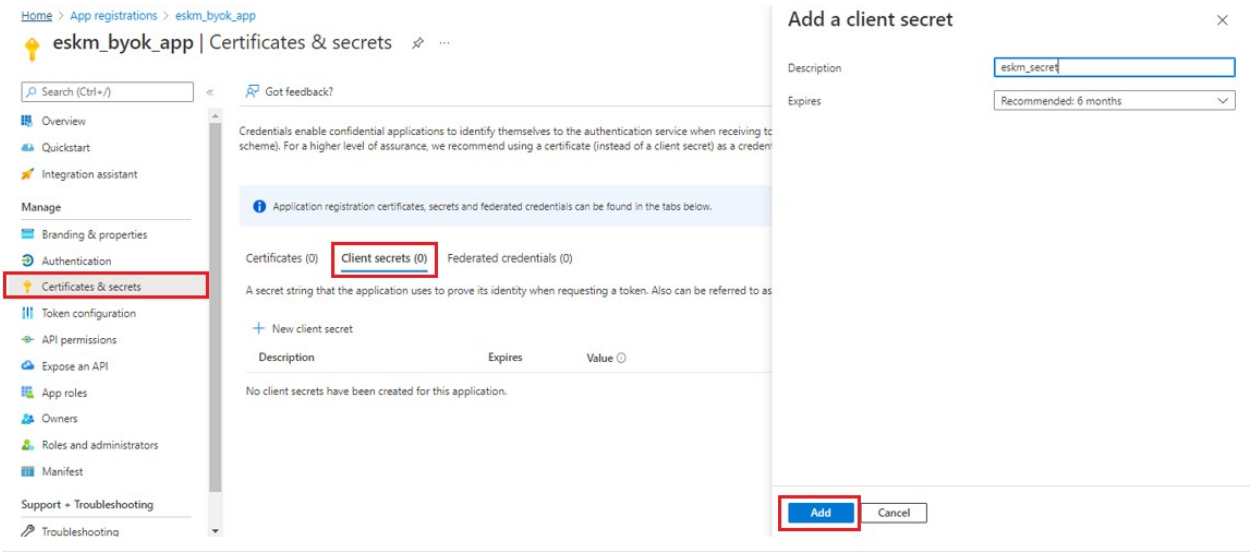


Figure 5 : Certificate & secrets

Enter the required information and click Add.

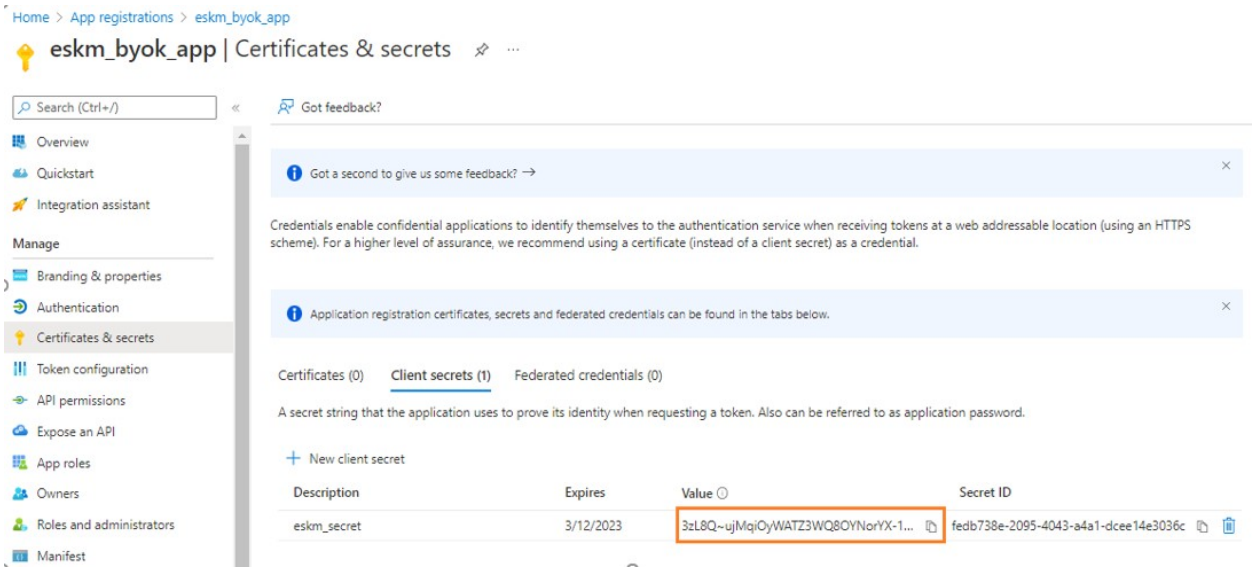


Figure 6 : Secret ID

Secret ID created successfully.

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

5 Access Policy

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

In the Microsoft Azure Portal, Navigate to the key Vault Resource.

Under Settings, select Access Configuration > Access Policies > Create.

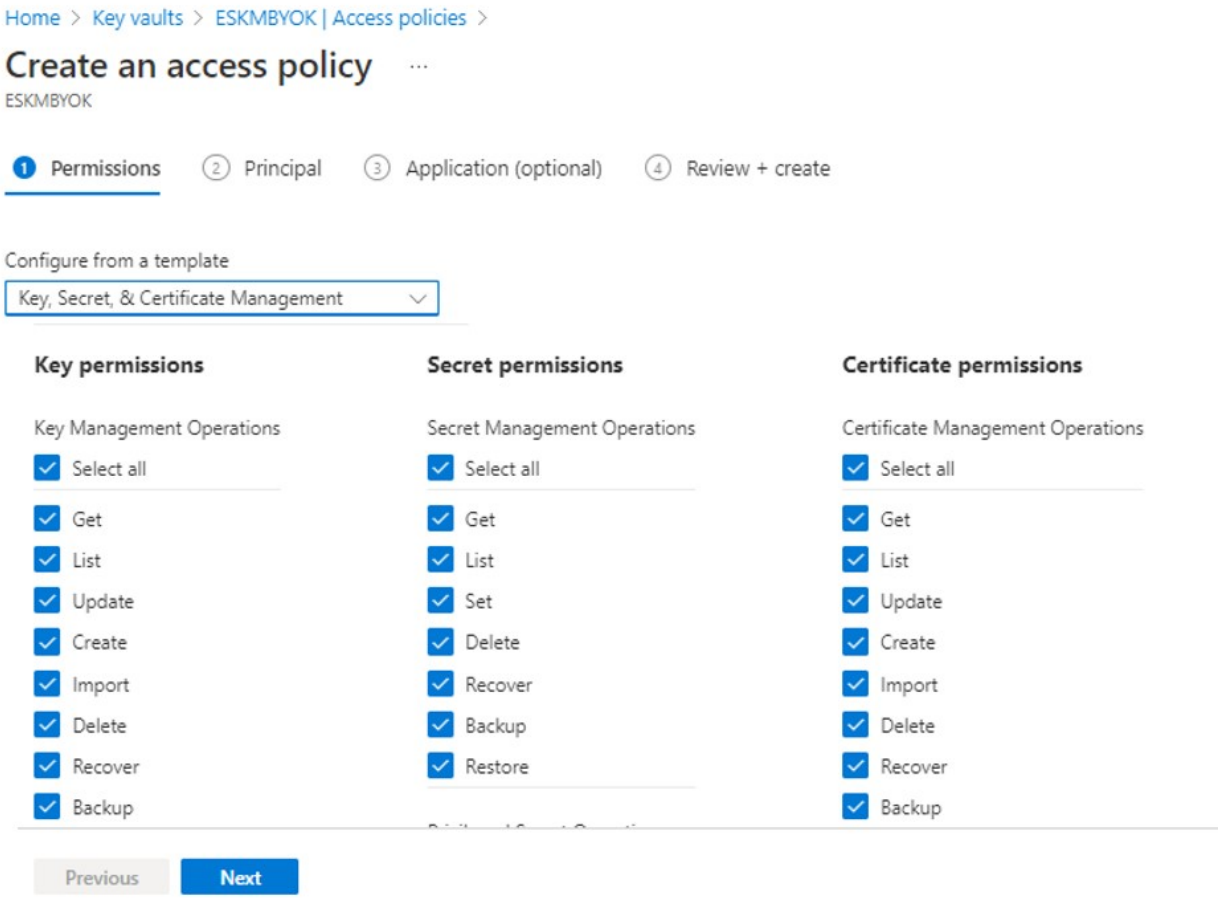


Figure 7 : Create an Access Policy

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

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

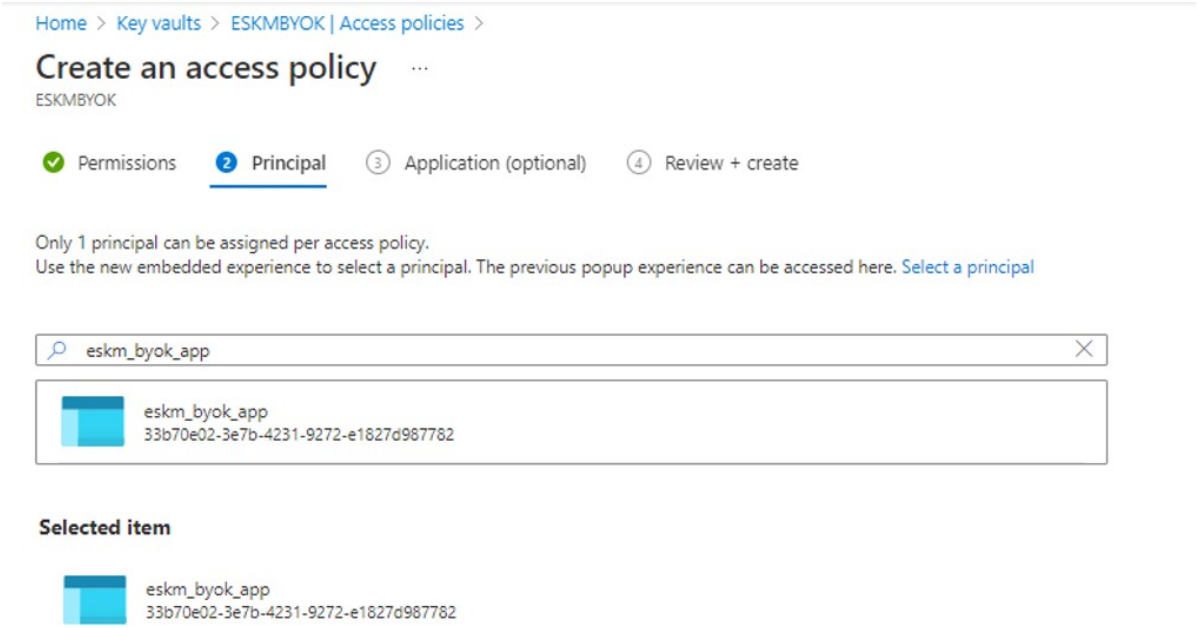


Figure 8 : Principal

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

You will be navigated to the Review Summary and Click Create.

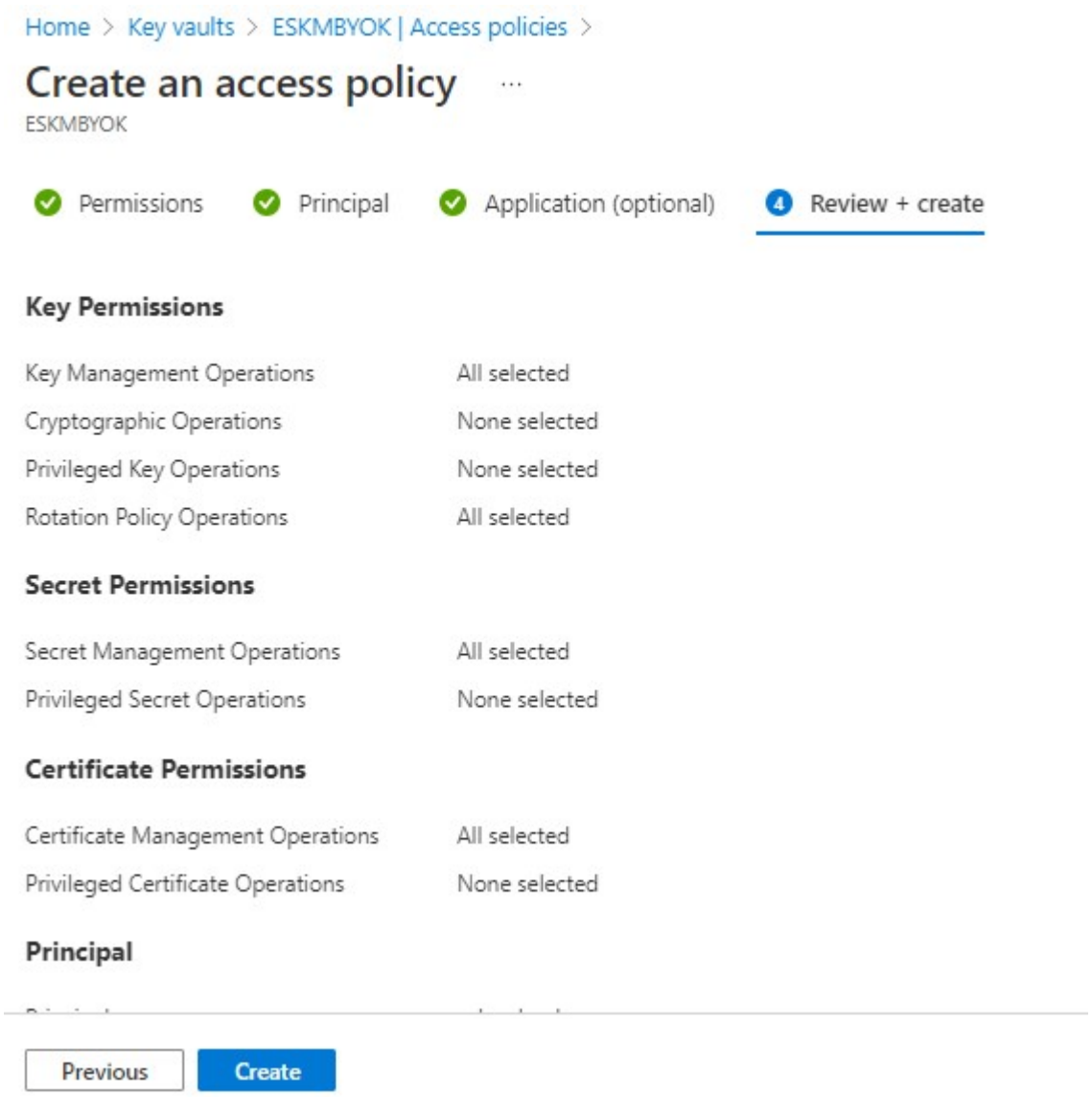


Figure 9 : Review and Create

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.