

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
All rights reserved	<p>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.</p> <p>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.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>

Table of Contents

1	About this Guide	4
2	Introduction	5
3	Create a Key Vault	6
4	Register an Application	10
4.1	Create Secret key	11
5	Access Policy	13
6	Contact and Support Information	16

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.

Home > Key vaults >

Create a key vault

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

[Create new](#)

Instance details

Key vault name *

Region *

Pricing tier *

A resource group is a container that holds related resources for an Azure solution.

Name *

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

Key vault name *

Region *

Pricing tier *

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete Enabled

Days to retain deleted vaults *

Purge protection Disable purge protection (allow key vault and objects to be purged during retention period)

Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Figure 1 : Create a key vault

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

[Home](#) > [Key vaults](#) >

Create a key vault ...

[Basics](#) [Access policy](#) [Networking](#) [Tags](#) [Review + create](#)

[View Automation Template](#)

Basics

Subscription	Azure subscription 1
Resource group	byok
Key vault name	ESKMBYOK
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	7 days

Access policy

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volumes	Disabled

[Previous](#) [Next](#) **[Create](#)**

Figure 2 : Review + create

- Review the information provided and click Create.

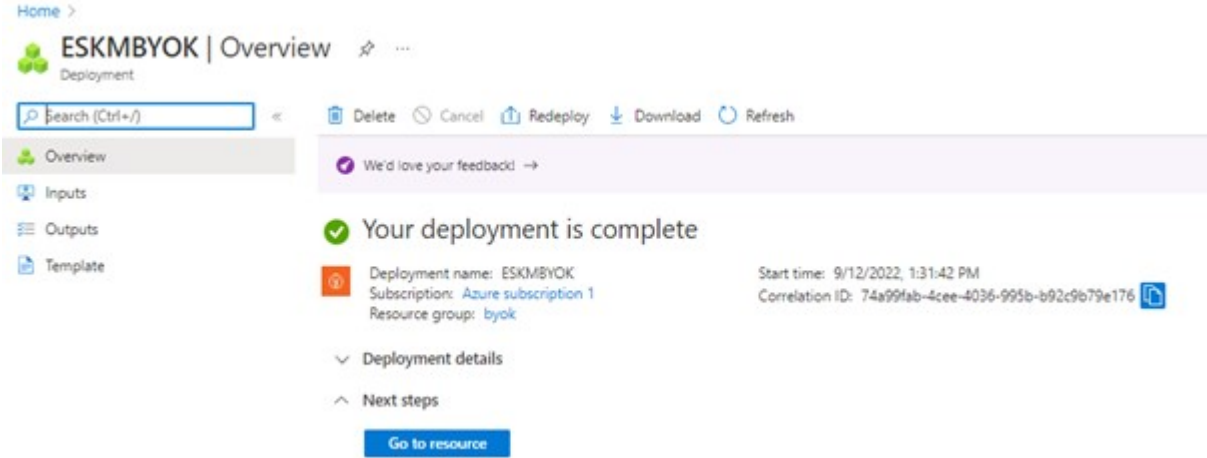


Figure 3 : Your deployment is complete

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.

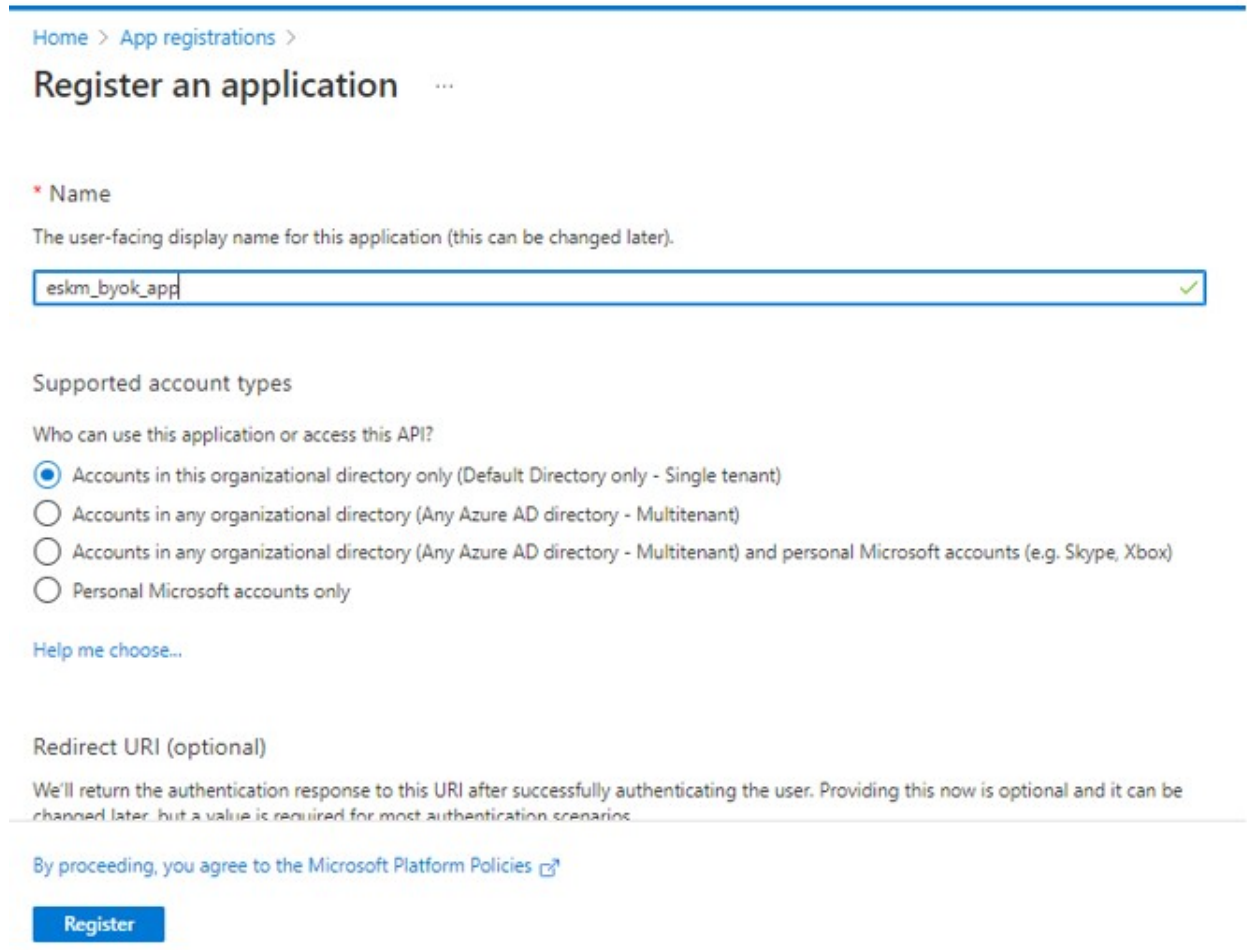
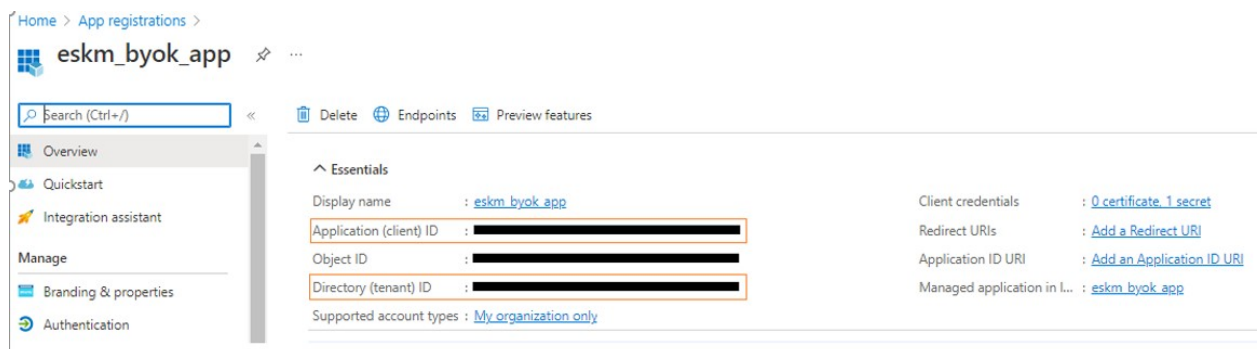


Figure 4 : Register an Application

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.

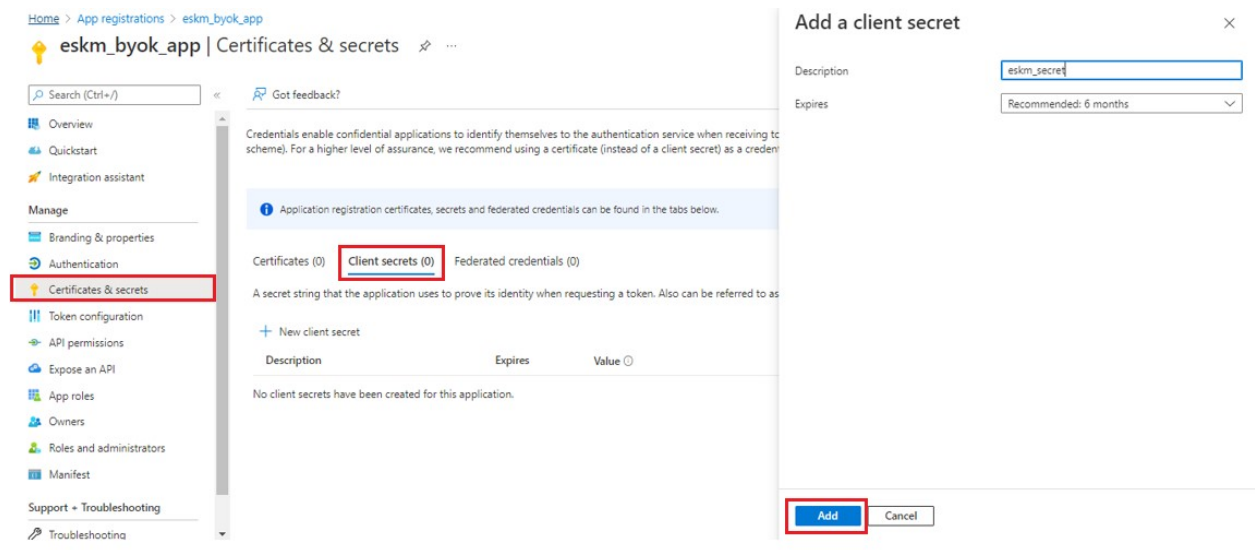


Figure 5 : Certificate & secrets

Enter the required information and click Add.

Home > App registrations > eskm_byok_app

eskm_byok_app | Certificates & secrets

Search (Ctrl+/) << Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
eskm_secret	3/12/2023	3zL8Q--ujMqjOyWATZ3WQ8OYNorYX-1...	fedb738e-2095-4043-a4a1-dcee14e3036c

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.

Home > Key vaults > ESKMBYOK | Access policies >

Create an access policy ...

ESKMBYOK

1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions	Secret permissions	Certificate permissions
Key Management Operations	Secret Management Operations	Certificate Management Operations
<input checked="" type="checkbox"/> Select all	<input checked="" type="checkbox"/> Select all	<input checked="" type="checkbox"/> Select all
<input checked="" type="checkbox"/> Get	<input checked="" type="checkbox"/> Get	<input checked="" type="checkbox"/> Get
<input checked="" type="checkbox"/> List	<input checked="" type="checkbox"/> List	<input checked="" type="checkbox"/> List
<input checked="" type="checkbox"/> Update	<input checked="" type="checkbox"/> Set	<input checked="" type="checkbox"/> Update
<input checked="" type="checkbox"/> Create	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Create
<input checked="" type="checkbox"/> Import	<input checked="" type="checkbox"/> Recover	<input checked="" type="checkbox"/> Import
<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Backup	<input checked="" type="checkbox"/> Delete
<input checked="" type="checkbox"/> Recover	<input checked="" type="checkbox"/> Restore	<input checked="" type="checkbox"/> Recover
<input checked="" type="checkbox"/> Backup		<input checked="" type="checkbox"/> Backup

Previous Next

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.

Home > Key vaults > ESKMBYOK | Access policies >

Create an access policy ...

ESKMBYOK

① Permissions ② **Principal** ③ Application (optional) ④ Review + create

Only 1 principal can be assigned per access policy.

Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

 eskm_byok_app 33b70e02-3e7b-4231-9272-e1827d987782

Selected item

 eskm_byok_app
33b70e02-3e7b-4231-9272-e1827d987782

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.

[Home](#) > [Key vaults](#) > [ESKMBYOK | Access policies](#) >

Create an access policy ...

ESKMBYOK

- ✓ Permissions
- ✓ Principal
- ✓ Application (optional)
- 4** Review + create

Key Permissions

Key Management Operations	All selected
Cryptographic Operations	None selected
Privileged Key Operations	None selected
Rotation Policy Operations	All selected

Secret Permissions

Secret Management Operations	All selected
Privileged Secret Operations	None selected

Certificate Permissions

Certificate Management Operations	All selected
Privileged Certificate Operations	None selected

Principal

Principal:

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.