Microsoft
Azure OpenID Connect (OIDC)

Integration Guide

ESKM

8.54.7

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	2026-08-17
Status	PUBLISHED
Document No.	IG-2026-0090

Table of Contents

1 About This Guide

This guide describes how to integrate Utimaco Enterprise Secure Key Manager (ESKM) with an OpenID Connect (OIDC) identity provider using Microsoft Entra ID. The integration enables users to authenticate to ESKM through the OIDC protocol, providing centralized authentication and Single Sign-On (SSO) capabilities.

1.1 Target Audience

This guide is intended for Microsoft Entra ID administrators and Utimaco ESKM administrators responsible for configuring, deploying, and managing OpenID Connect (OIDC)-based authentication integration between the two systems.

1.2 Purpose of the Integration

The integration of Utimaco Enterprise Secure Key Manager (ESKM) with an OIDC identity provider enables centralized user authentication for ESKM. By leveraging OIDC authentication, organizations can provide users with a secure and streamlined sign-in experience while reducing the need for local credential management within ESKM.

In this integration, Microsoft Entra ID acts as the OIDC Identity Provider (IdP), authenticating users and providing identity information to ESKM.

Benefits of the integration include:

- Centralized authentication using organizational credentials.
- Single Sign-On (SSO) access to the ESKM Management UI.
- Simplified user identity management through a centralized identity provider.
- Reduced administrative overhead associated with local account management.
- Enhanced security through centralized authentication policies and Multi-Factor Authentication (MFA), where configured.
- Improved user experience by allowing users to authenticate using their existing organizational accounts.

1.3 Scope of the Integration

This guide covers the configuration required to integrate Utimaco Enterprise Secure Key Manager (ESKM) with Microsoft Entra ID using OIDC authentication. The guide describes the creation and configuration of an application registration in Microsoft Entra ID, the configuration of OIDC settings in ESKM, and the validation of user authentication through the identity provider.

1.4 Abbreviations

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
OIDC	OpenID Connect
IdP	Identity Provider
SSO	Single Sign-On
MFA	Multi-Factor Authentication
GUI	Graphical User Interface
UI	User Interface
URL	Uniform Resource Locator
KMIP	Key Management Interoperability Protocol
NTP	Network Time Protocol
DNS	Domain Name System

Abbreviation	Meaning
ID	Identifier

Table 1: 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	Under **Client secrets**, click **New client secret**.
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	ESKM 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 indicates the expected result after the successful execution of an instruction.

2 Product Overview

2.1 Overview of Microsoft Azure OIDC

Microsoft Azure OpenID Connect (OIDC) is an identity authentication protocol provided through Microsoft Entra ID that enables applications to securely authenticate users and obtain identity information using standardized tokens. Built on the OAuth 2.0 framework, Azure OIDC supports enterprise security features such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), Conditional Access, and centralized identity management. In this integration, Microsoft Entra ID acts as the OpenID Connect Identity Provider (IdP), authenticating users and issuing identity tokens that enable secure access to Utimaco Enterprise Secure Key Manager (ESKM).

2.2 Overview of ESKM

ESKM is a centralized key management solution that securely stores, distributes, and manages encryption keys throughout their lifecycle. It supports industry standards, including the KMIP, enabling integration with various enterprise applications and storage systems.

2.3 Joint Value Proposition

The integration of Utimaco Enterprise Secure Key Manager (ESKM) with Microsoft Azure OpenID Connect (OIDC) combines the secure key management capabilities of ESKM with standards-based user authentication and identity services. By leveraging Azure OIDC as the authentication mechanism, organizations can provide secure and centralized access to ESKM while simplifying identity management. Key benefits of the integration include:

- Centralized authentication – Users can authenticate to ESKM using their existing enterprise identities.
- Single Sign-On (SSO) – Provides a seamless authentication experience and reduces the need for multiple credentials.
- Simplified user management – User identities and access policies can be managed centrally through the identity provider.
- Enhanced security – Authentication can leverage advanced security controls such as Multi-Factor Authentication (MFA) and Conditional Access policies.
- Reduced administrative overhead – Eliminates the need to maintain separate authentication credentials for ESKM users

2.4 Integration Architecture

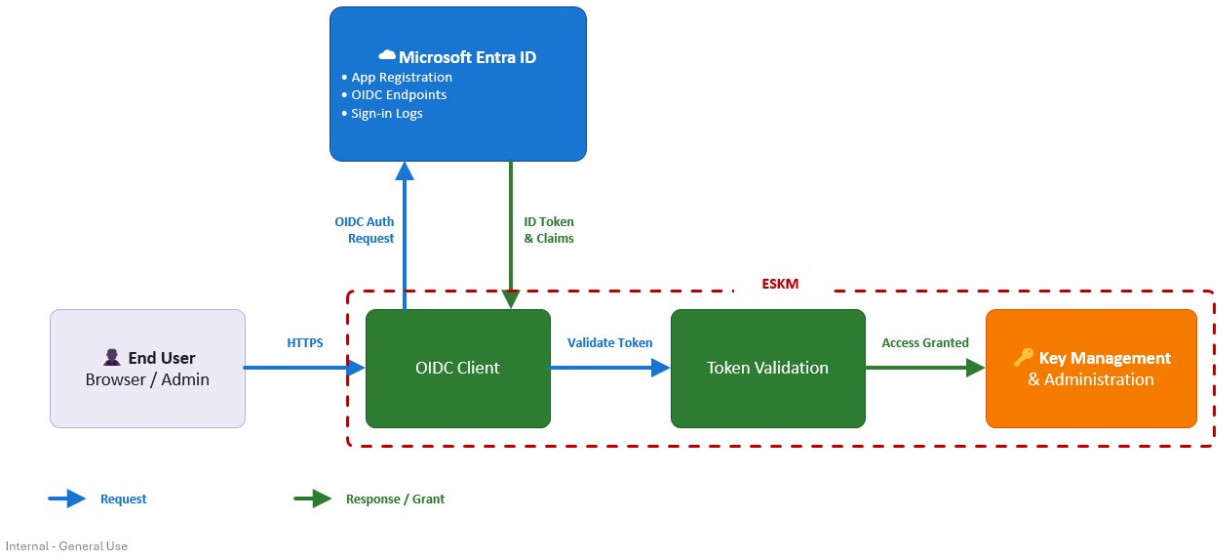

Figure 1 : Integration architecture

The integration architecture enables users to authenticate to Utimaco Enterprise Secure Key Manager (ESKM) using Microsoft Entra ID through the OpenID Connect (OIDC) protocol. When a user accesses the ESKM Management UI, ESKM initiates an OIDC authentication request and redirects the user to Microsoft Entra ID. After successful authentication, Microsoft Entra ID returns an ID token containing the user's identity claims. ESKM validates the token and associated claims before granting access to the ESKM management and administration functions.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Microsoft Entra ID	Utimaco ESKM Version
Cloud Service	8.54.7

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	8.54.7
Microsoft Entra ID	Azure Cloud Service

Table 4: Hardware and software requirements

3.4 Prerequisites

Before starting the integration, ensure that the following prerequisites are met:

- ESKM listed in *Tested Versions*.
- Administrative access to ESKM is available.
- A Microsoft Entra ID tenant is available.
- Permissions to create and manage App Registrations in Microsoft Entra ID are available.
- The ESKM server has network connectivity to Microsoft Entra ID endpoints.

- DNS resolution is properly configured on the ESKM server.
- The ESKM server time is synchronized with a reliable NTP source.

4 Installing and Configuring ESKM

The following section outlines the procedures required to configure ESKM.

The initial phase involves configuring the ESKM before proceeding to Microsoft OIDC.
For detailed configuration steps, refer to the *"ESKM_Installation and Replacement_Guide_8.54.0"*.

After successful installation and configuration, log in to the ESKM.

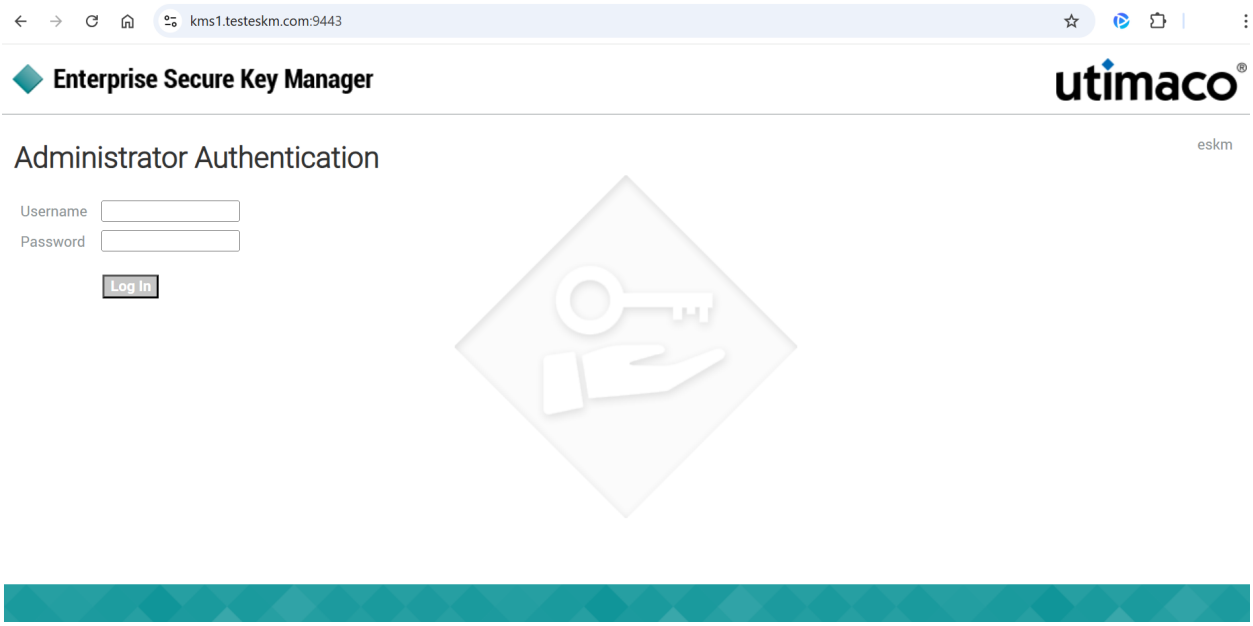

Figure 2 : ESKM login page

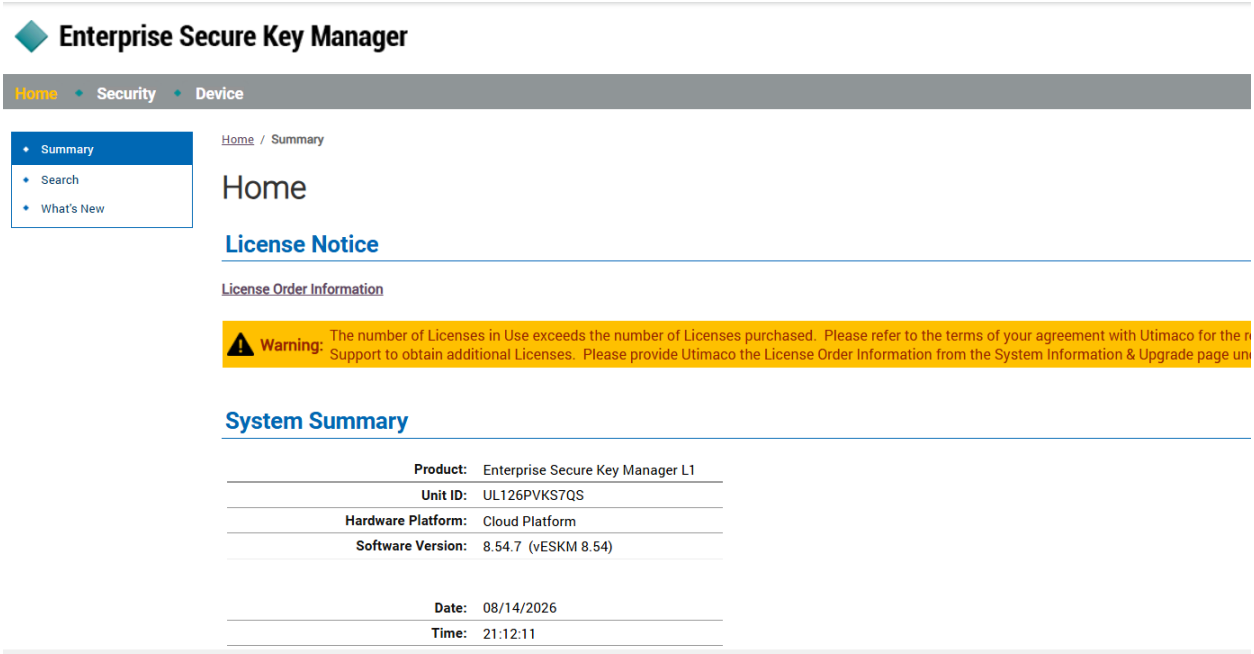

Figure 3 : ESKM home page

5 Integration Steps on Microsoft Entra ID

To enable OpenID Connect (OIDC) authentication between Microsoft Azure and Utimaco Enterprise Secure Key Manager (ESKM), an application registration must be created in Microsoft Entra ID. The application registration establishes the trust relationship between Microsoft Entra ID and ESKM and provides the identifiers and credentials required for OIDC authentication.

5.1 Creating an App Registration

1. Sign in to the **Azure Portal**.
2. Navigate to **Microsoft Entra ID** → **Manage** → **App registrations**.
3. Click **New registration**.
4. In the **Register an application** page, configure the following settings:

- **Name**: Enter a descriptive name for the application, for example, **ESKM-OIDC**.
- **Supported account types**: Select the appropriate supported account type based on your organization's requirements. In this example, **Single tenant only - Default Directory** is selected.
- **Redirect URI**: Leave this field blank during initial creation.

5. Click **Register**.

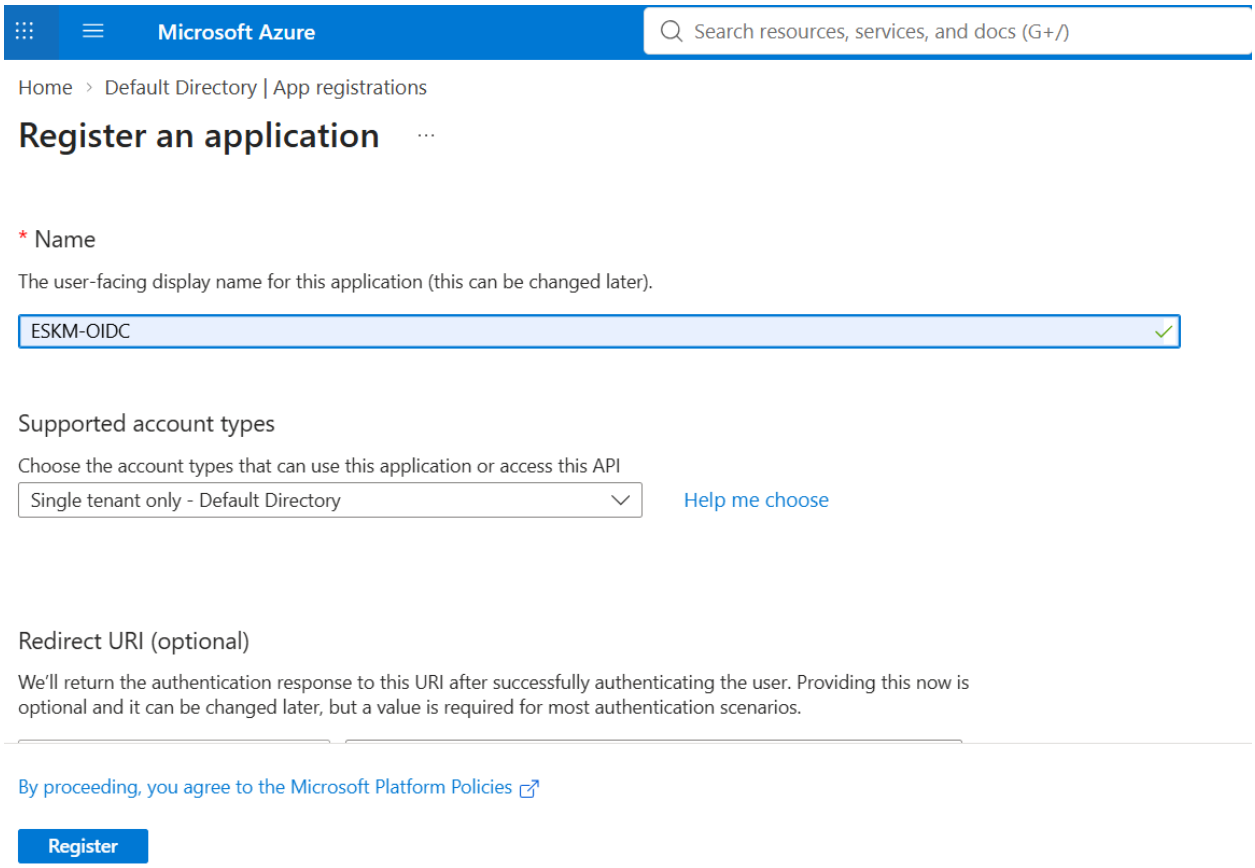

Figure 4 : Register an application

After the application registration is created, Microsoft Entra ID redirects to the **Overview** page. Record the following values, as they will be required when configuring OpenID Connect authentication in ESKM:

- Application (client) ID
- Directory (tenant) ID
- Display Name

The Application (client) ID uniquely identifies the application, while the Directory (tenant) ID identifies the Microsoft Entra ID tenant in which the application is registered.

5.2 Creating a Client Secret

A client secret is required to allow Utimaco Enterprise Secure Key Manager (ESKM) to authenticate with Microsoft Entra ID during the OpenID Connect (OIDC) authentication process.

1. From the application registration **Overview** page, navigate to **Manage** → **Certificates & secrets**.
2. Under **Client secrets**, click **New client secret**.

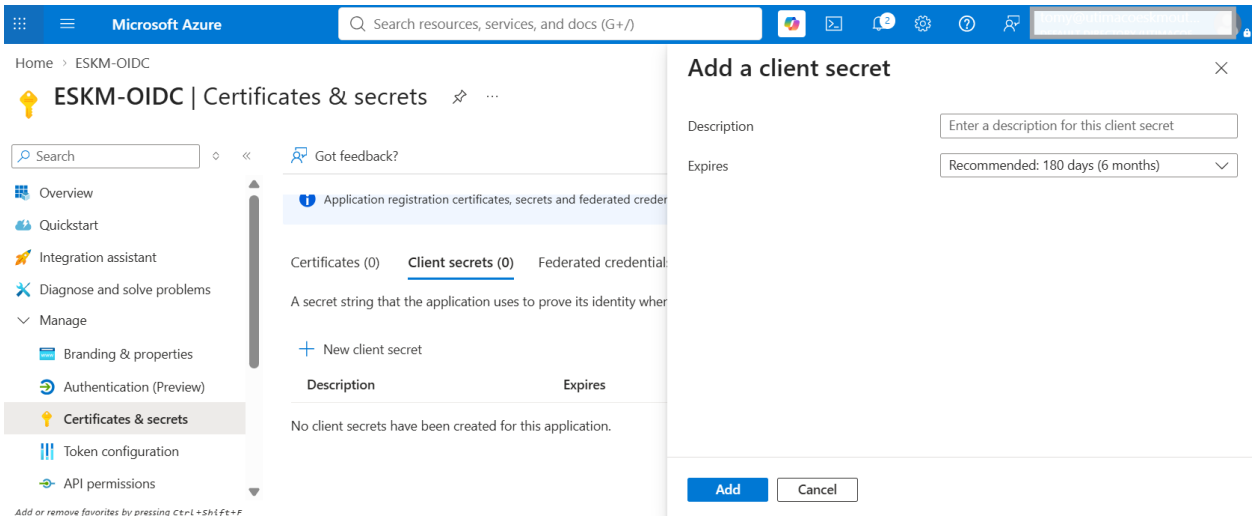

Figure 5 : Add a client secret

3. In the **Add a client secret** pane:
   a. Enter a meaningful description for the secret.
   b. Select the desired expiration period.
4. Click **Add**.

Once the client secret is created, copy and securely store the value displayed in the **Value** field.

> The client secret value is displayed only once after creation. Ensure the value is copied and stored securely before leaving the page.

5.3 Configuring Authentication Settings

Configure the application authentication settings and add the redirect URI that will be used by Utimaco Enterprise Secure Key Manager (ESKM).

1. From the application registration page, navigate to **Manage** → **Authentication**.
2. In the **Redirect URI configuration** section, click **Add Redirect URI**.
3. In the **Select a platform to add redirect URI** pane, select **Web**.
4. In the **Redirect URI** field, enter the callback URL generated by ESKM (For example: *https://<ESKM_HOSTNAME>:8443/byok/login/oauth2/code/<Application_Client_ID>*)
5. Click **Configure**.

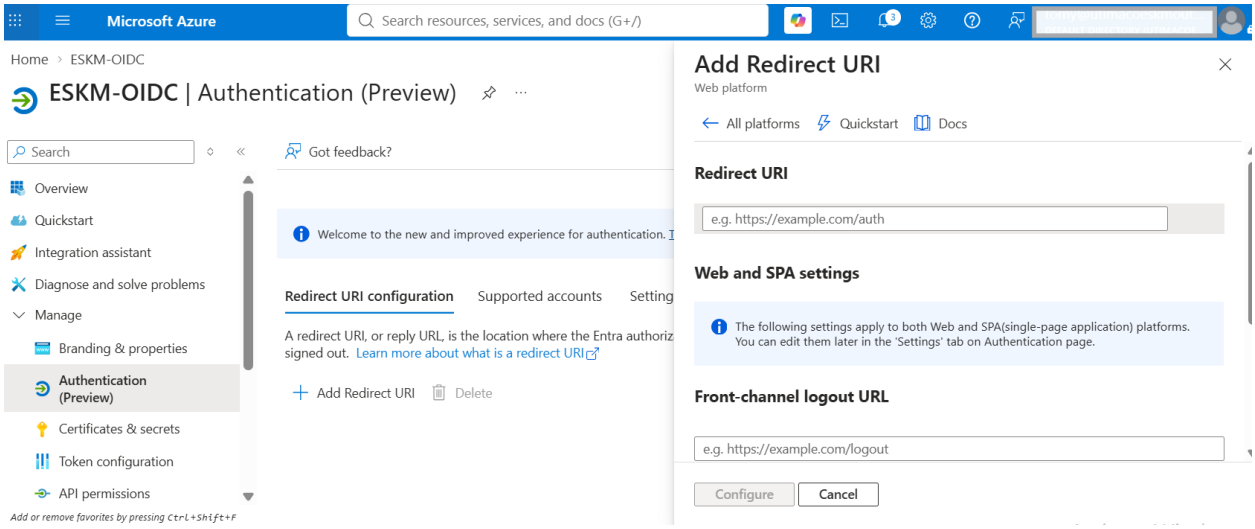

Figure 6 : Add redirect URI

In this integration, the ESKM *Registration ID* is configured with the same value as the Microsoft Entra ID *Application (Client) ID* during the OIDC configuration process described in the subsequent steps. Therefore, the callback URL includes the *Application (Client) ID* as the final path component.

6 Integration Steps on Utimaco ESKM

6.1 Configuring the OpenID Server

After completing the Microsoft Entra ID configuration and obtaining the required application details, configure the OpenID Server settings in ESKM.

1. Log in to the ESKM Administration Portal using an administrator account.
2. Navigate to **Device** → **Administrators** → **OpenID Server Configuration**.
3. Click **Edit**.
4. Enable **OpenID Authentication**.
5. Configure the parameters listed in the table below.
6. Click **Save** to apply the configuration.

Parameter	Description
Configuration URL	*https://login.microsoftonline.com/<Tenant-ID>/v2.0/.well-known/openid-configuration*
Client ID	<Application Client ID>
Client Name	<Display name>
Client Secret	<Client Secret value>
Registration ID	<Application Client ID>
Scope	openid,profile,email

Parameter	Description
Username Attribute Name	email

Table 5: OpenID server configuration parameters

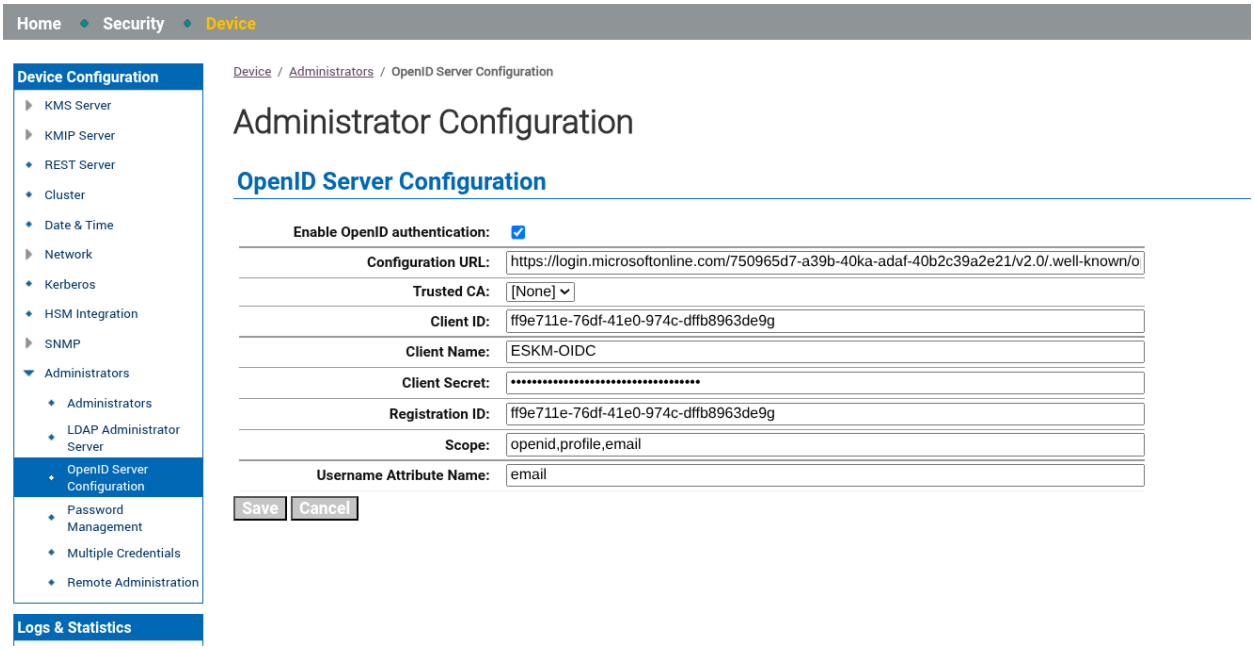

Figure 7 : OpenID server configuration

After saving the configuration, ESKM restarts the required services and enables OIDC-based authentication.

The *Configuration URL, Client ID, Registration ID*, and *Client Secret* values are obtained from the Microsoft Entra ID application registration created in the previous section.

The value specified for *Username Attribute Name* must correspond to a claim provided by Microsoft Entra ID. In this example, *email* is used to identify authenticated users.

6.2 Creating an OIDC Administrator in ESKM

After configuring the OpenID Server settings, create an OpenID administrator account in ESKM that corresponds to a Microsoft Entra ID user.

1. Navigate to **Device** → **Administrators** → **Administrators**.
2. Click **Create OpenID Administrator**.
3. In the **Username** field, enter the *email address* of the Microsoft Entra ID user that will be granted access to ESKM. Ensure that the value matches the email claim returned by Microsoft Entra ID during authentication.
4. Assign the required administrative privileges and access rights.
5. Click **Create** to create the OpenID administrator.

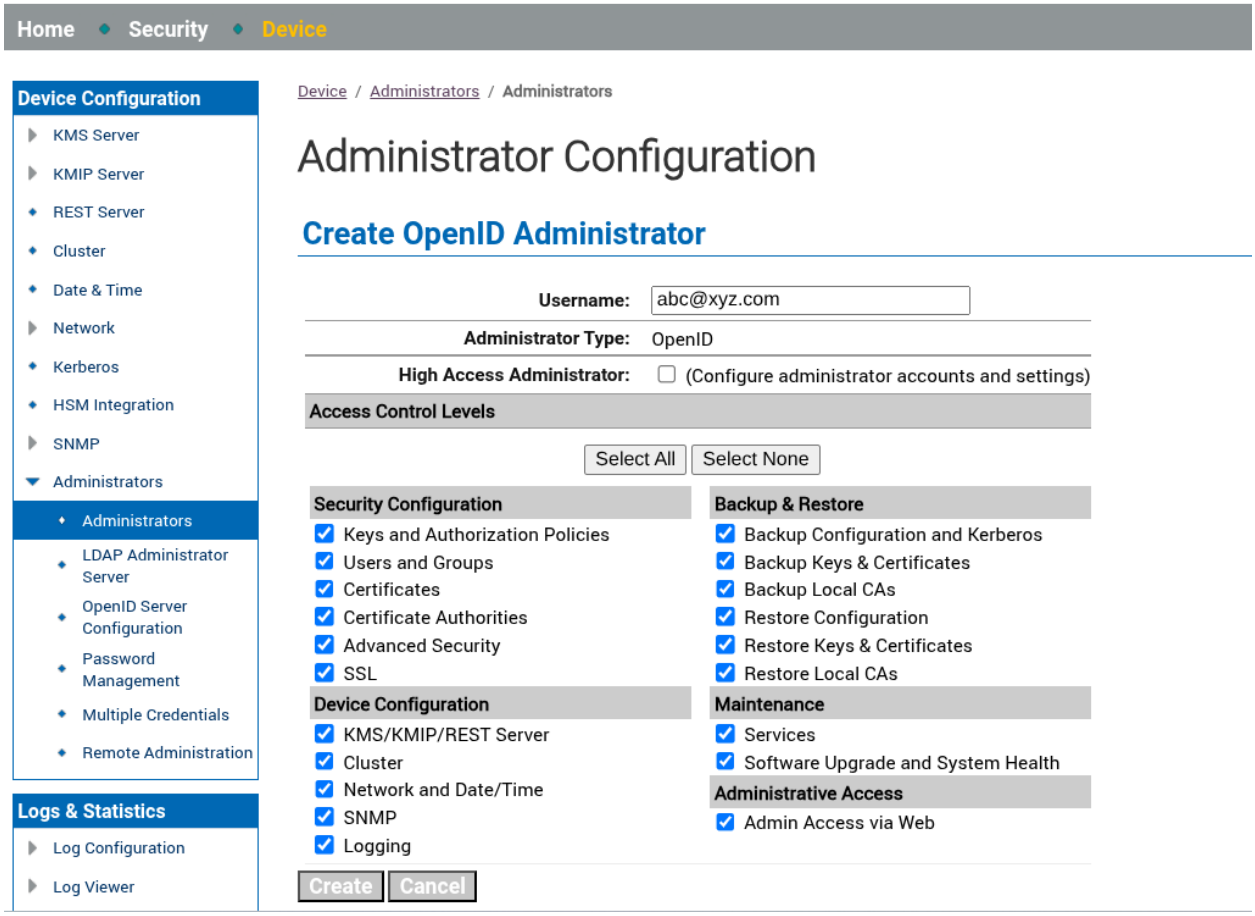

Figure 8 : Administrator configuration

The OpenID administrator username must exactly match the value returned by the claim specified in the *Username Attribute Name* field of the OpenID Server Configuration. In this guide, the *Username Attribute Name* is configured as *email*.

After completing this step, the configured user can authenticate to ESKM using Microsoft Entra ID credentials through OIDC authentication.

7 Verification and Testing

After completing the configuration, validate the integration by authenticating to ESKM using Microsoft Entra ID credentials.

7.1 Logging in to ESKM Using OIDC Authentication

1. Launch a web browser and navigate to the ESKM Management UI using port 8443. Example: *https://<ESKM_HOSTNAME>:8443*
2. Click on **Login**.
3. On the ESKM login page, click **Sign In using OpenID**.

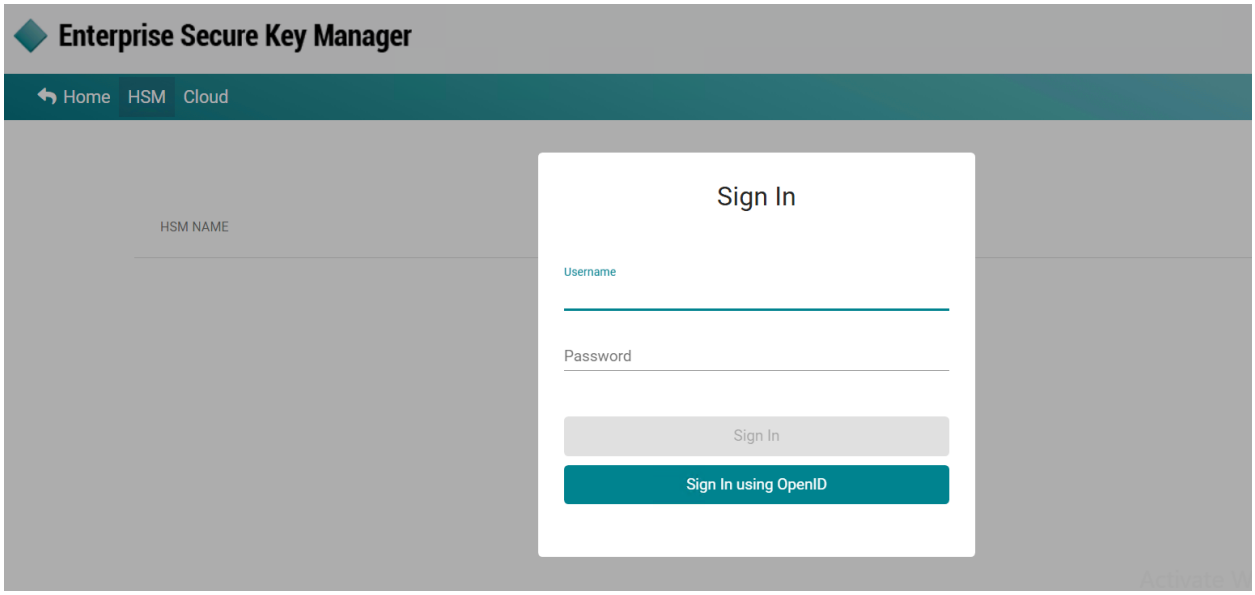

Figure 9 : ESKM OIDC login page

4. The browser is redirected to the Microsoft Entra ID sign-in page.
5. Enter the credentials of the Microsoft Entra ID user that was configured as an OpenID administrator in ESKM.
6. Complete any Multi-Factor Authentication (MFA) verification steps, if applicable.
7. After successful authentication, Microsoft Entra ID redirects the user back to ESKM.
8. Verify that the user is successfully logged in to the ESKM Management UI.

7.1.1 Verifying Successful Authentication

Perform the following validation checks:

- Verify that the user is successfully authenticated through Microsoft Entra ID and redirected to the ESKM Management UI.
- Verify that the authenticated user is granted the expected administrative privileges configured in ESKM.
- Verify that the user can successfully perform ESKM administrative operations according to the assigned permissions.
- Verify successful Single Sign-On (SSO) behavior:
    - Click **Home** in the ESKM Management UI and verify that ESKM redirects the user to the Home page on port *9443*.
    - Confirm that the user remains authenticated and is not prompted to log in again after the redirection.

7.2 Logs and Validation Steps

The integration can be validated by reviewing authentication events in Microsoft Entra ID and ESKM.

7.2.1 Reviewing Authentication Logs in Microsoft Entra ID

Microsoft Entra ID records authentication attempts performed through OIDC.

1. Sign in to the Azure Portal.
2. Navigate to **Microsoft Entra ID** → **Monitoring** → **Sign-in logs**.
3. Locate the authentication event corresponding to the ESKM login attempt.
4. Verify that the sign-in status is reported as successful.
5. Review additional details such as:
    - User
    - Application
    - Status

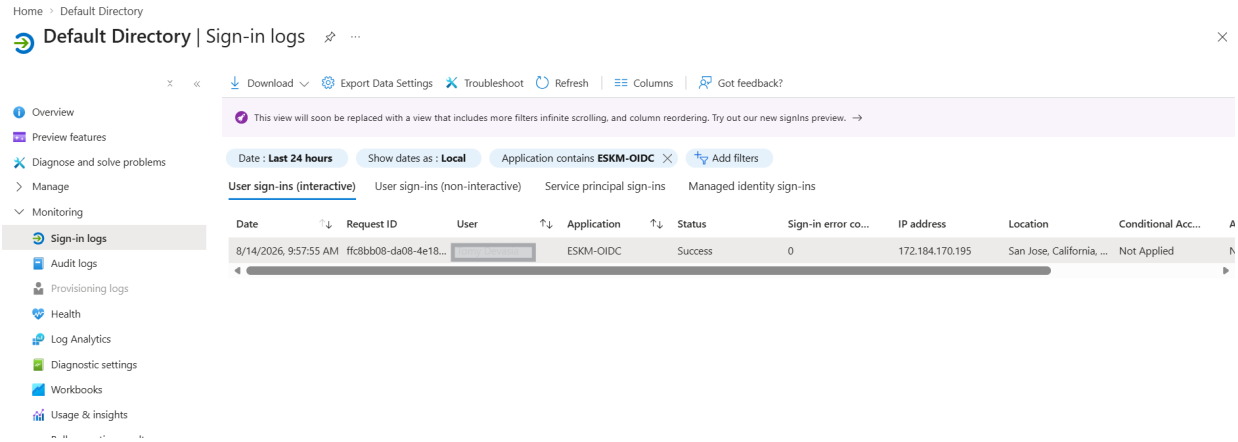

Figure 10 : Sign-in logs

7.2.2 Reviewing Authentication Logs in ESKM

ESKM records OIDC authentication events and administrator login activities.

1. Log in to the ESKM Administration Console.
2. Navigate to **Device** → **Log Viewer** → **Audit**.
3. Select the desired log file.
4. Click **Display Log** and verify that an entry similar to the following is present.

```
[abc@xyz.com] [Login] Logged in from <IP Address> via web
```

8 Troubleshooting

8.1 Common issues and how to resolve them

The following table lists common issues that may be encountered during the integration and the corresponding resolution steps.

Issue	Possible Cause	Resolution
Authentication fails and the user is not redirected back to ESKM	Redirect URI mismatch between Microsoft Entra ID and ESKM	Verify that the Redirect URI configured in Microsoft Entra ID exactly matches the callback URL configured in ESKM.
User is not redirected to Microsoft Entra ID after clicking Sign In using OpenID	OpenID authentication is not enabled or the OpenID Server configuration is incorrect	Verify that OpenID Authentication is enabled and that the OpenID Server configuration has been saved successfully.
Authentication fails with an "Invalid Client" error	Incorrect Client ID or Client Secret configured in ESKM	Verify that the Client ID and Client Secret values in ESKM match those configured in Microsoft Entra ID.
User successfully authenticates with Microsoft Entra ID but cannot access ESKM	OpenID administrator account is not configured or username mapping is incorrect	Verify that an OpenID administrator account exists in ESKM and that the username matches the configured user attribute returned in the OIDC token.
Authentication fails after renewing the client secret	Expired or updated client secret has not been updated in ESKM	Generate a new client secret in Microsoft Entra ID and update the value in the ESKM OpenID Server Configuration.

Issue	Possible Cause	Resolution
Authentication fails with token validation or token expiry errors	Time synchronization issue between ESKM and Microsoft Entra ID	Verify that the ESKM server date, time, and timezone are correctly configured and synchronized with a reliable NTP source.
Authentication succeeds but the user is not authorized to access ESKM	The OpenID administrator username does not match the configured OIDC claim value	Verify that the username configured for the OpenID administrator exactly matches the value returned in the claim configured by the Username Attribute Name parameter. In this guide, the email claim is used.
ESKM cannot reach Microsoft Entra ID endpoints or authentication fails during redirection	DNS resolution failure on the ESKM server	Verify that the ESKM server can resolve Microsoft Entra ID endpoints such as *login.microsoftonline.com*. Check the DNS server configuration and confirm successful name resolution before retrying authentication.

Table 6: Troubleshooting

9 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.

10 Appendices

10.1 References (links to external docs)

Title	Description	Document/Link
Microsoft Entra ID Documentation	Official Microsoft documentation for Microsoft Entra ID identity and access management services.	*https://learn.microsoft.com/en-us/entra/identity/*
App Registration in Microsoft Entra ID	Microsoft documentation for creating and managing application registrations.	*https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app*
OpenID Connect Protocol	Microsoft documentation for OpenID Connect authentication using the Microsoft identity platform.	https://learn.microsoft.com/en-us/entra/identity-platform/v2-protocols-oidc
Microsoft Entra ID Sign-In Logs	Documentation for monitoring and troubleshooting authentication using sign-in logs.	https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-ins

Table 7: References