Google
Workspace Client Side Encryption

Integration Guide

ESKM

8.54.0 or higher

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	2026-03-20
Status	PUBLISHED
Document No.	IG-2026-0010

Table of Contents

1 Introduction 4
1.1 Prerequisites 4
1.2 About this Guide 4
1.3 Target Audience 5
1.4 Document Coventions 5
1.5 Abbreviations 6
2 Accessing the Cloud Integration Web Console 7
3 Google Workspace Integration 11
3.1 Configure ESKM 11
3.2 Adding Google Workspace Cloud Instance 12
3.3 Editing Google Workspace Cloud Instance 13
3.4 Deleting Google Workspace Cloud Instance 14
3.5 Google Workspace Keys Dashboard 15
3.6 Creating Google Workspace Keys 17
3.7 Deleting Google Workspace Keys 19
4 Google Workspace Configuration 21
4.1 Configuring Gmail to work with ESKM 22
4.2 Configuring ESKM for migration 23
5 Contact and Support Information 24

1 Introduction

Google Workspace Client Side encryption allows you to secure Drive, Docs, Sheets, and Slides data with an external encryption key that Google servers cannot access. File content is encrypted in the browser before being sent to Google. Decryption requires explicit customer authorization on a per-file basis, and Google cannot unilaterally access file content.

This integration enhances security by giving administrators the ability to protect sensitive data stored and processed within Google Workspace, ensuring it's encrypted and that only authorized users or systems can access the decryption keys.

This guide covers the integration of Google Cloud Workspace with ESKM.

1.1 Prerequisites

Before using ESKM Cloud, make sure that the following prerequisites are met:

- ESKM version must be ESKM 8.54.0 or higher.
- A DNS server must be configured in ESKM. This can be done in the ESKM management console (Device->Network->Hostname & DNS).
- Admin Access to Google Workspace with Assured Controls must be possible.
- An OpenID-based identity provider, such as Keycloak, with the necessary users added, must be available.
- A domain name and the corresponding SSL certificate for Google Workspace must be available.
- ESKM must be connected to the Internet, and DNS must be configured.
- GCP project is required for Gmail.

1.2 About this Guide

This guide describes the following:

- Google Workspace Integration
- Google Workspace Configuration

1.3 Target Audience

This guide is intended for Google Workspace administrators.

1.4 Document Coventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Table 1: 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.

1.5 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
PKI	Public Key Infrastructure
TDE	Transparent Data Encryption
PKCS	Public Key Cryptography Standards
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
SO	The PKCS#11 cryptographic slot Security Officer
DB	Database
JRE	Java Runtime Environment
MBK	Master backup key
P11CAT	the PKCS#11 graphical interface tool
CXI	Cryptographic eXtended Interface
FIPS	Federal Information Processing Standards

Table 2: Abbreviations

2 Accessing the Cloud Integration Web Console

The Cloud Integration Web Console can be accessed in the following ways:

- Log in to the ESKM Management Console as an administrator and go to **Security** > **Cloud Integration**.
    - The Cloud Integration Web Console opens in a new tab and you will be automatically logged in to Cloud ESKM.

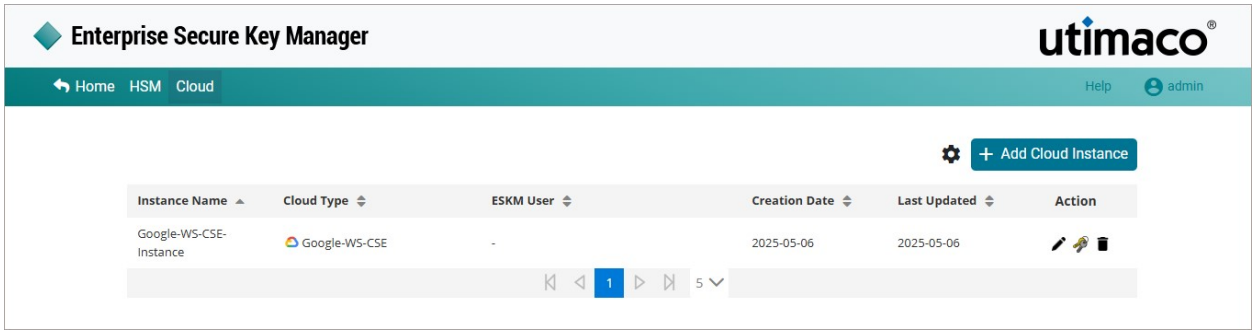


Figure 1 : Cloud Integration Dashboard

- Direct access via a web browser using IP address and port. For example, `https://<ESKM IP>:8443/cloud/dashboard`.

The following screen will be displayed:

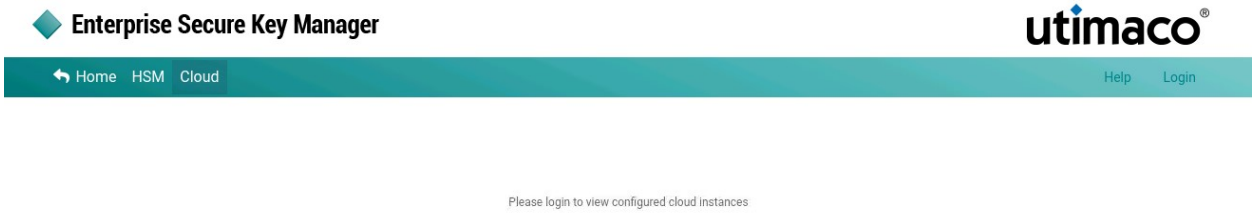
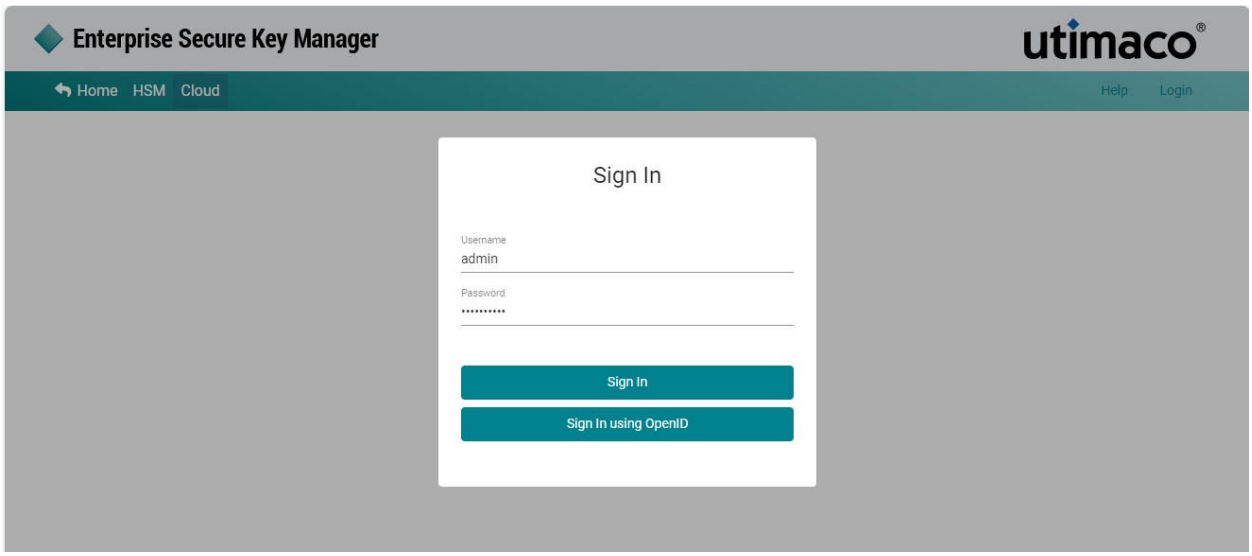


Figure 2 : Cloud Integration Login

Click **Login** at the top right corner of the page.



Enter the administrator username and password, and click on **Sign In**.

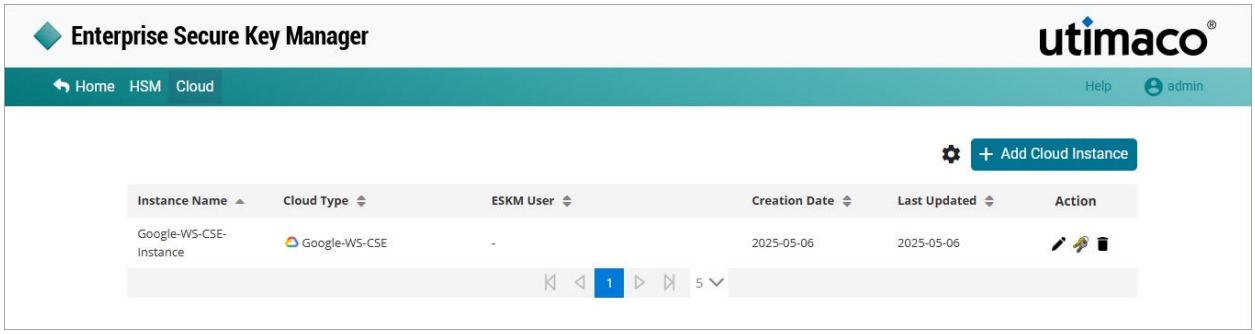


Figure 3 : Cloud ESKM-Logged In Page

The Cloud Integration Dashboard allows users to add cloud instances and view information about 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:

- On the login page, enter username and password and click on **Sign In using OpenID**.
  OR
  Click **Sign In using OpenID** without user credentials.

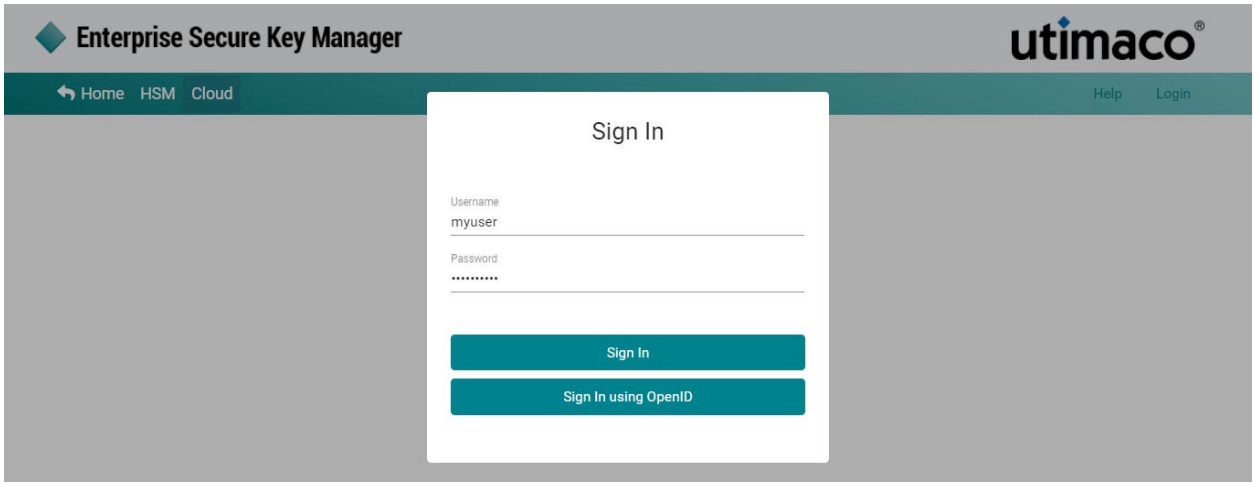


Figure 4 : Sign In Using OpenID

- Enter username and password and click on **Sign In or Sign In using OpenID**.
- The Cloud Integration Dashboard is displayed.

You can log out of the Cloud Integration Web Console at any time using the **Logout** option in the upper right corner.

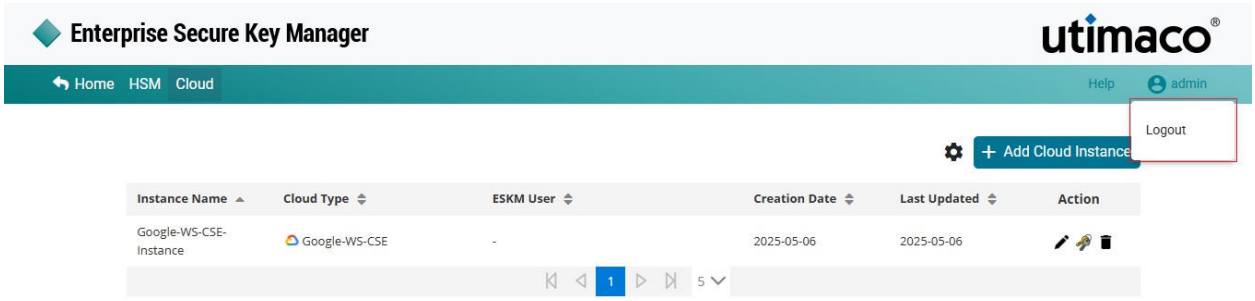


Figure 5 : Logout

- When you signed in with OpenID Cloud Integration Web Console, the **Logout** pop-up window is displayed. Click on **Logout**.
- In the Cloud Integration Dashboard, click the left arrow at the upper left corner of the page to navigate to the ESKM application.

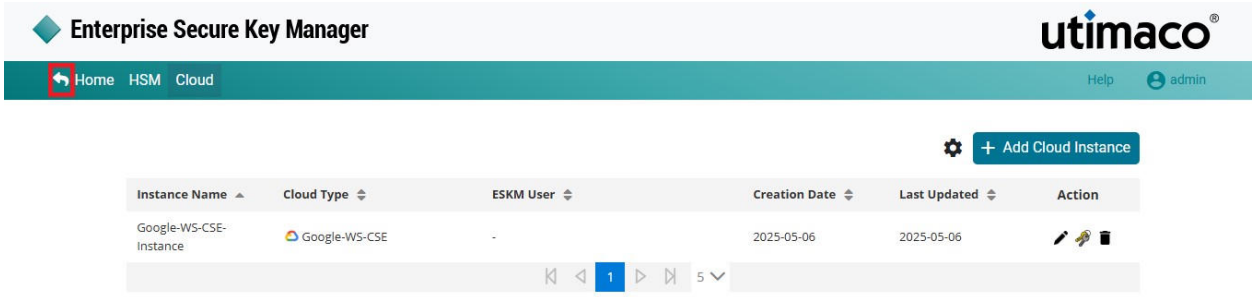


Figure 6 : Cloud Integration Dashboard

3 Google Workspace Integration

3.1 Configure ESKM

- Configure the following information in the ESKM management console.
- Navigate to the **Advanced Rest Settings** on the Rest Configuration page (**Device** > **Rest Server** >**Advanced Rest Settings**).

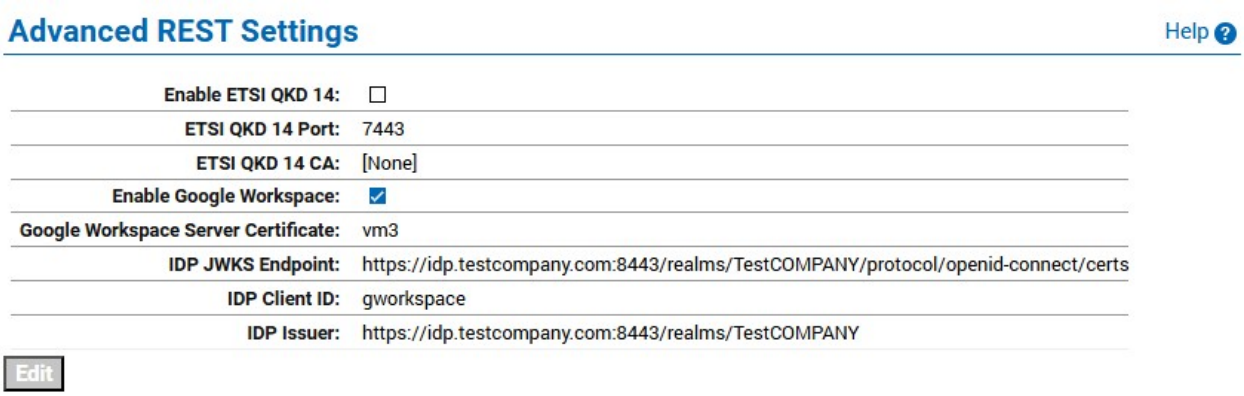


Figure 7 : Advanced Rest Settings

- Select the **Enable Google Workspace** checkbox.
- Select the **Google Workspace Server Certificate** from the drop-down list.
  This certificate should be different from the **Server Certificate** configured in the **Rest Server Settings**.
- Specify the **IDP JSON Web Key Set (JWKS) Endpoint URL**.
  ESKM uses this URL to fetch JWKS to validate authentication token.

> This URL is likely in the following format:
> `https://<idp-domain-name>/realms/ <realm-name>/protocol/openid-connect/certs`

- Specify the **IDP Client ID**.
  The Client ID should match the one configured in both the Identity Provider (IDP) and the Google Workspace Admin Console.
- Specify the **IDP issuer** of the authentication token and it is checked against the 'iss' claim to verify the token's origin.

3.2 Adding Google Workspace Cloud Instance

This section describes how to add a Google Workspace Cloud Instance.

To add a new cloud instance:

- Log in to the Cloud Integration Web Console using any one of the methods described in Accessing the Cloud Integration Web Console.
- Click on **+ Add Cloud Instance** at the top right corner of the page.

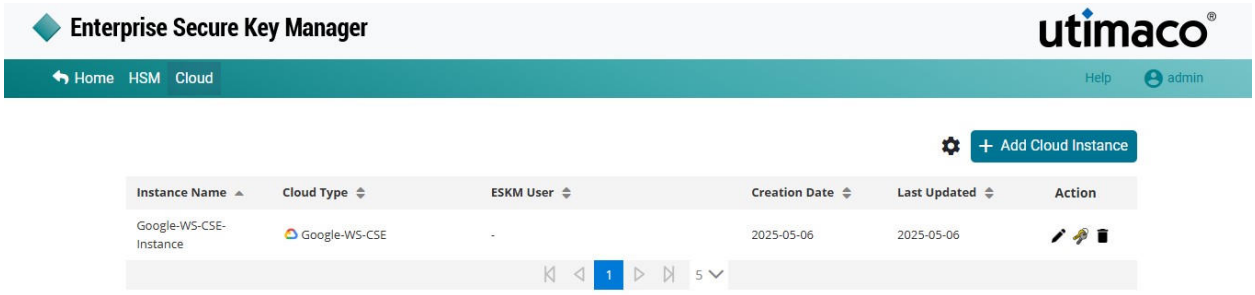


Figure 8 : Add Cloud Instance

- The **Add Cloud Instance** dialog is displayed.

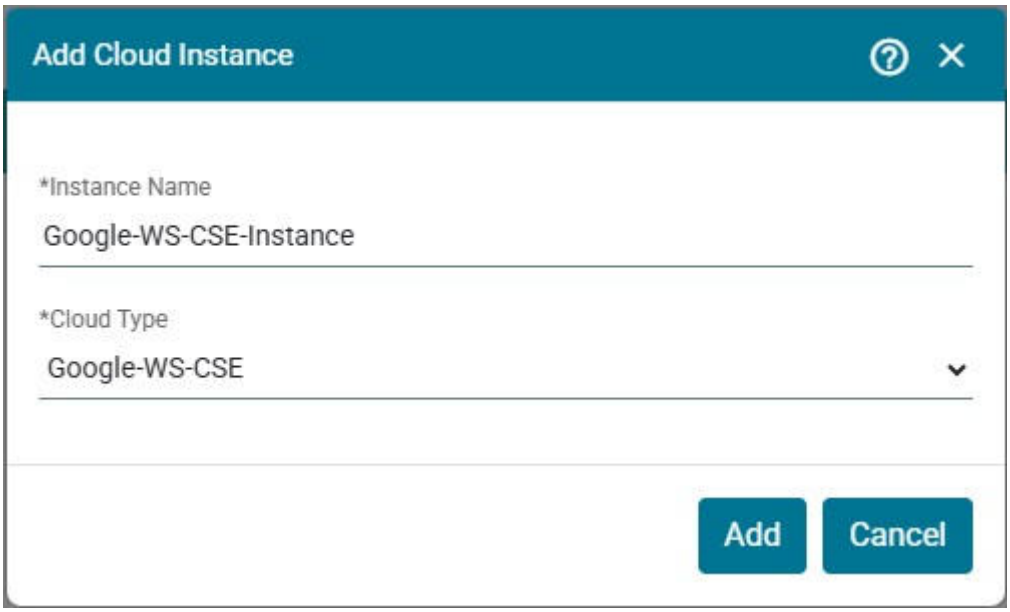


Figure 9 : Add Google Workspace Cloud Instance

- Select **Google-WS-CSE** as the **Cloud Type** and click on **Add**.

The Cloud Instance Instance1 **[Google-WS-CSE]** has been created successfully.

The **Instance Name** cannot be edited.

Only one Google Workspace instance can be added for **Cloud Type [Google-WS-CSE]**.

3.3 Editing Google Workspace Cloud Instance

- To edit an existing Google Workspace Cloud Instance, click on the **Edit** icon in the **Action** column.

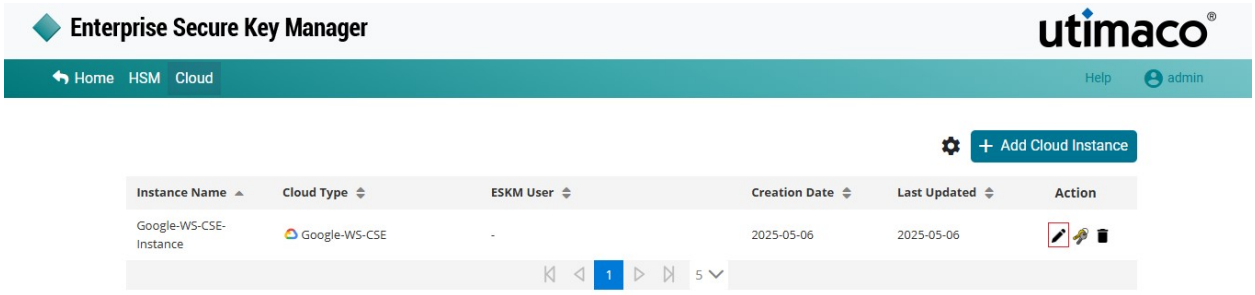


Figure 10 : Edit an Instance

- The **Edit Cloud Instance** dialog is displayed.

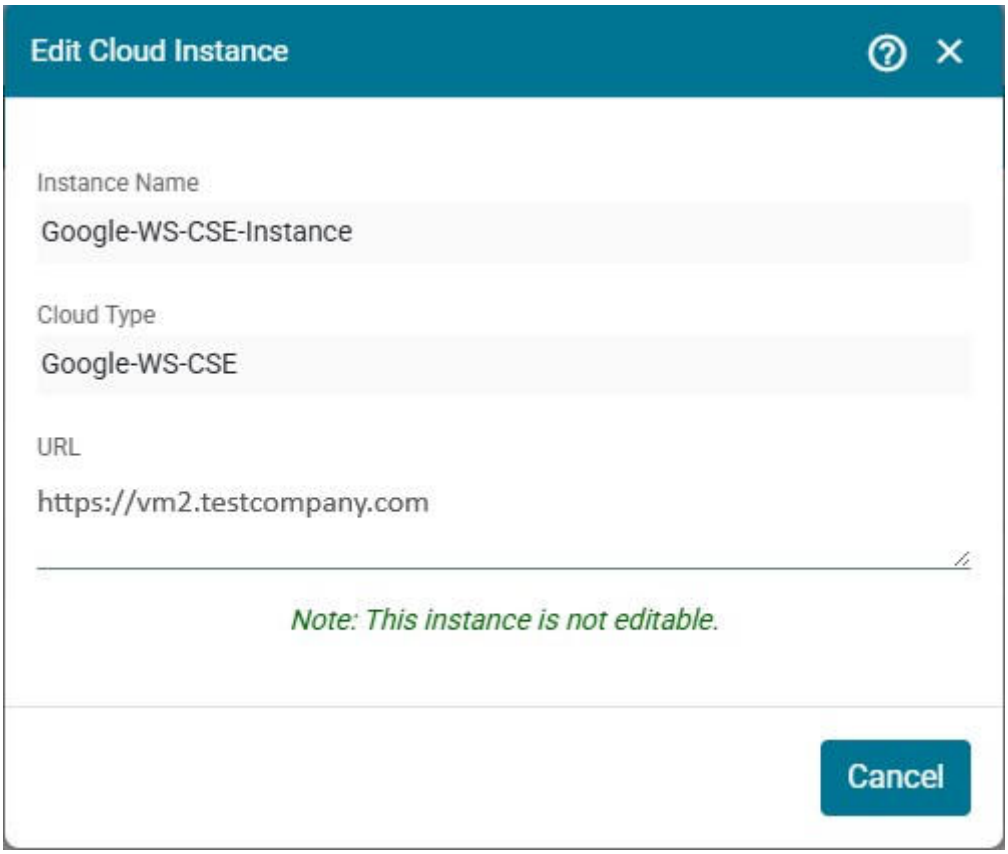


Figure 11 : Edit Cloud Instance

- The displayed URL is the External Key Service URL. This URL is constructed using the Common Name of the Google WS certificate configured under **Advanced REST Settings**.

The Google Workspace Instance is read-only and cannot be edited.

3.4 Deleting Google Workspace Cloud Instance

- To delete the existing cloud instance, click on the **Delete** icon in the **Action** column.

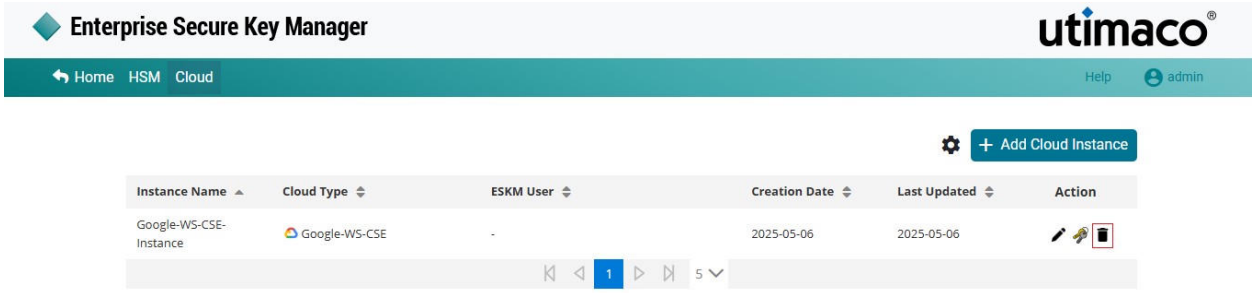


Figure 12 : Google Workspace Cloud Instance

- The Delete Cloud Instance dialog is displayed. Click on **Delete**.

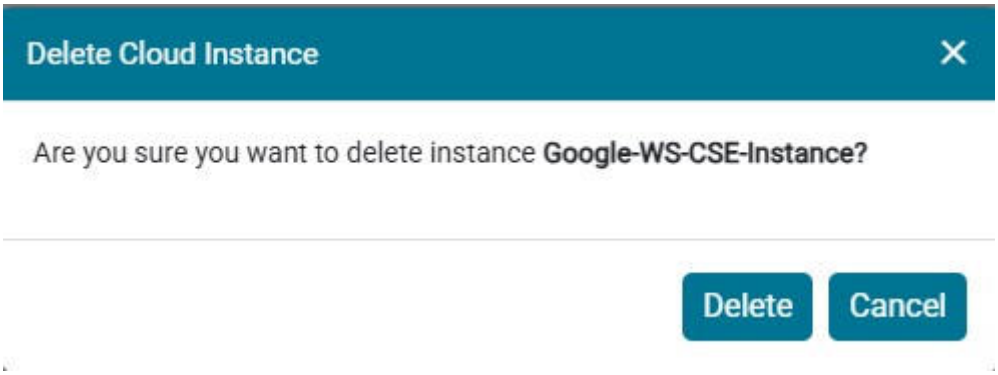


Figure 13 : Delete Google Workspace Cloud Instance

The Cloud Instance Instance1 [Google-WS-CSE] has been deleted successfully.

You cannot delete the Cloud Instance **Google-WS-CSE-Instance [Google-WS-CSE]** if keys

are already associated with it.

3.5 Google Workspace Keys Dashboard

- To list all keys created for Google Workspace, click on the **Manage Keys** icon in the **Action** column.

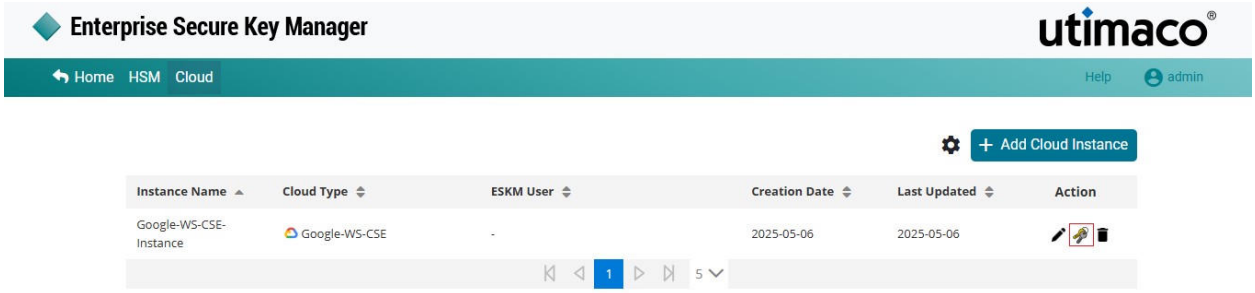


Figure 14 : Google Workspace - Manage Keys

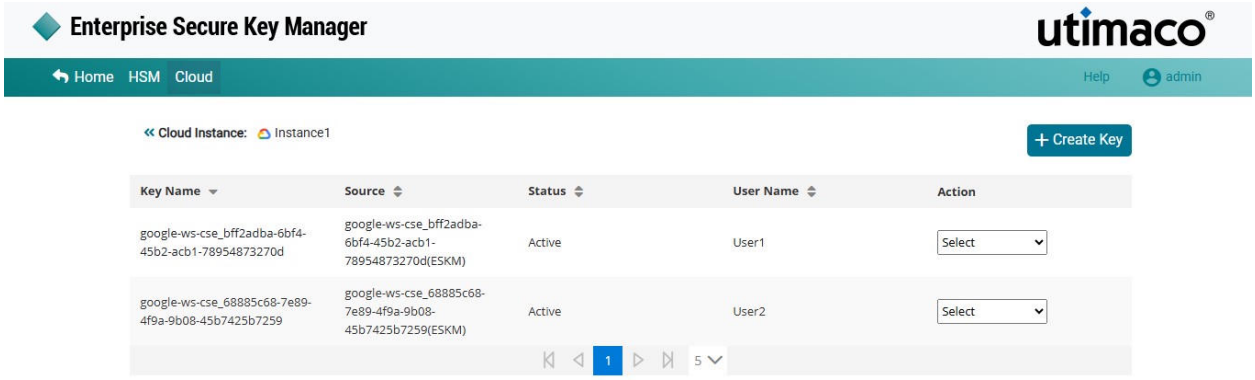


Figure 15 : Google Workspace - Key List

- Select a key from the list to view its details.

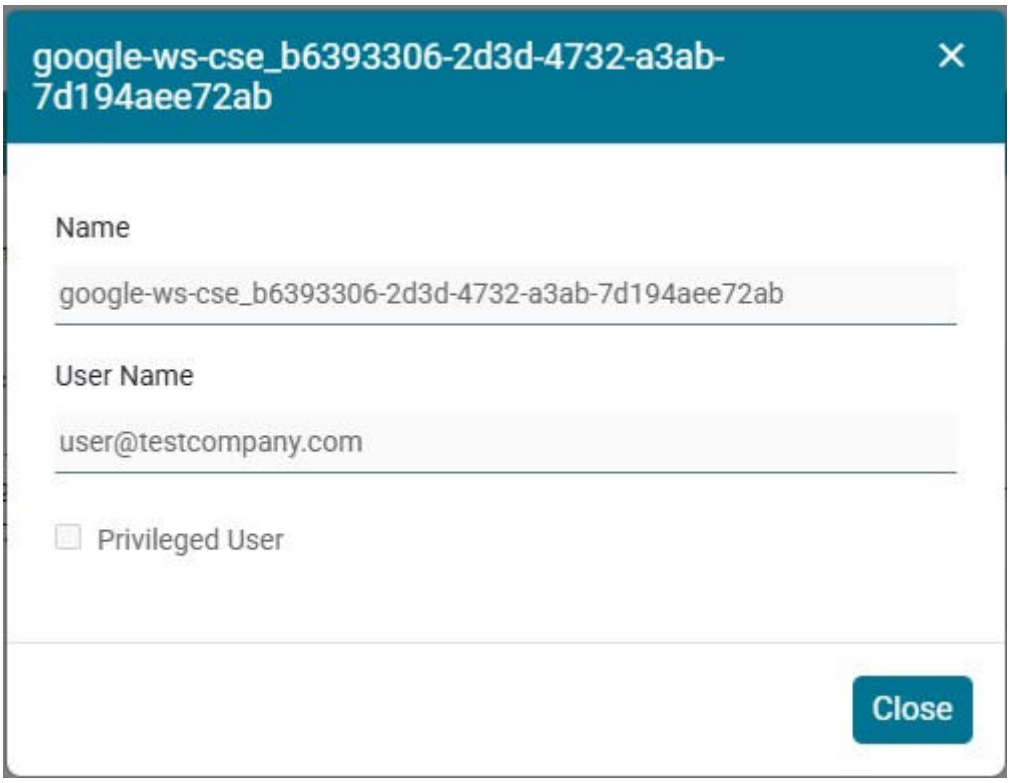
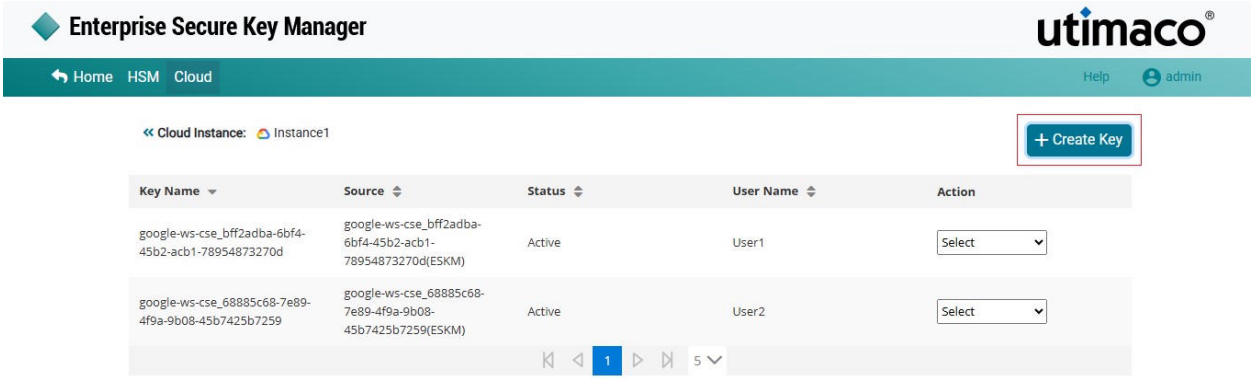


Figure 16 : Key Information

3.6 Creating Google Workspace Keys

This section describes how to create a key in the Cloud ESK.

- Click on the **Manage Keys** icon to display a list of keys created in the Cloud instance.



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

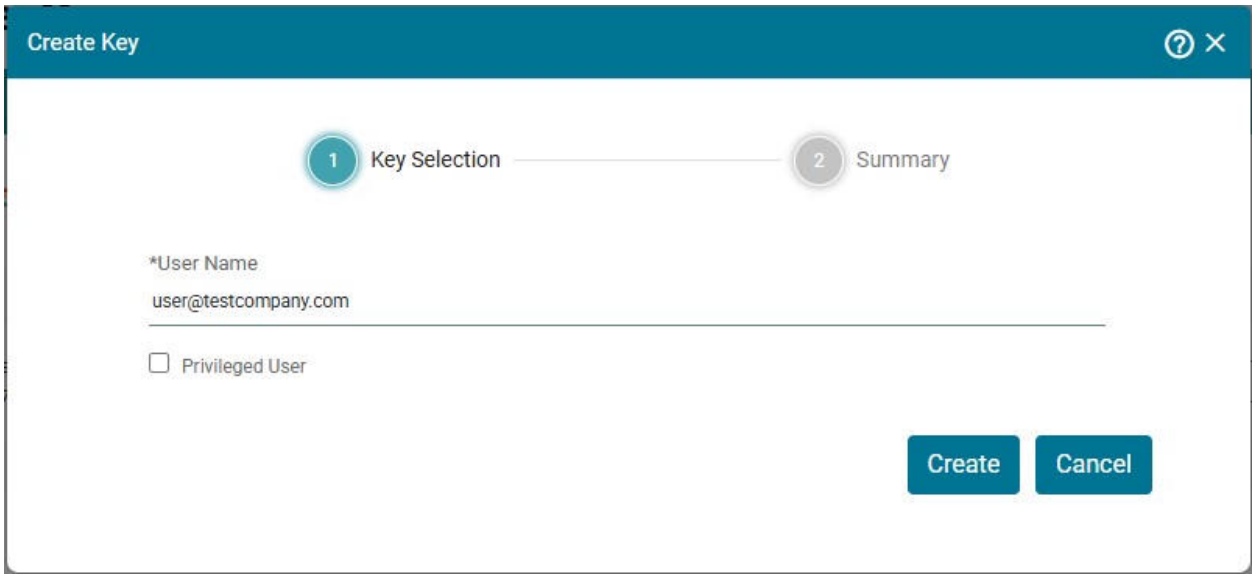


Figure 17 : Create Key - Key Selection

- Enter a username and click on **Create**.

Check **Privileged User** only if the user needs to call privileged APIs, namely `PrivilegedWrap`, `PrivilegedUnwrap`, and `PrivilegedPrivateKeyDecrypt`. Privileged requests do not require Google authorization and can be initiated from any application, requiring only authentication. For detailed information, see https://developers.google.com/workspace/cse/reference. ESKM will reject all privileged API requests from users not marked as privileged.

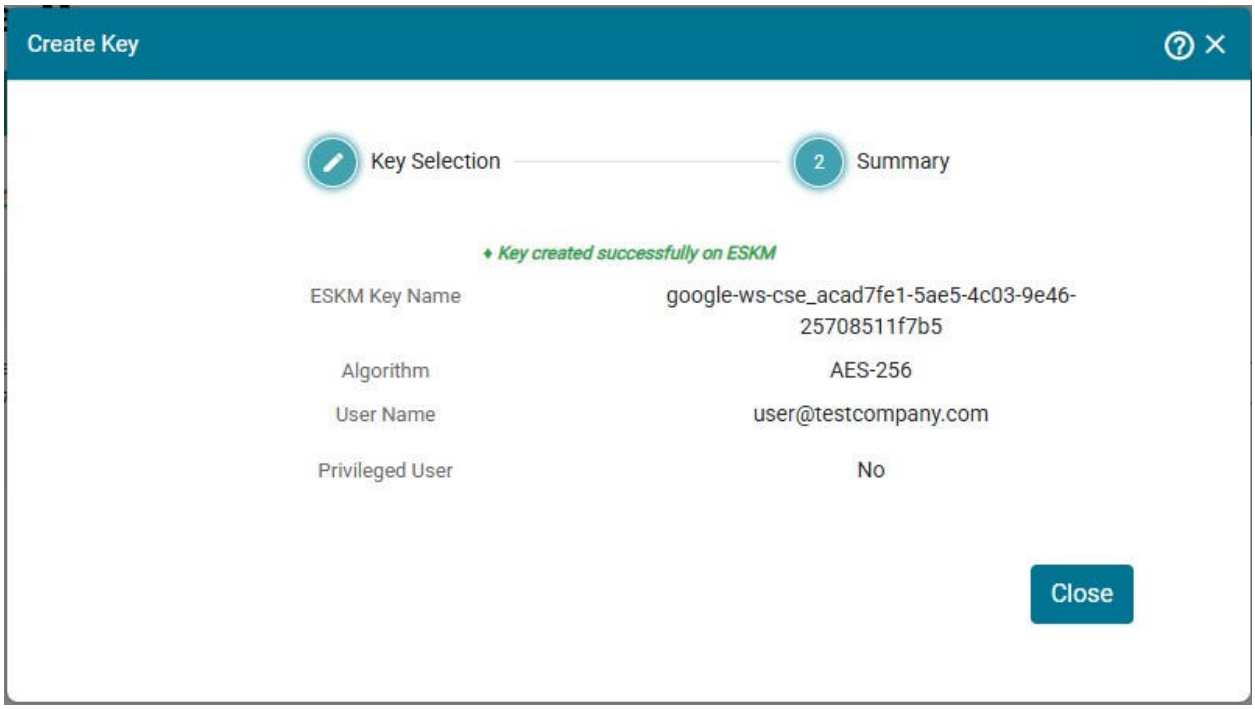


Figure 18 : Key Summary

- A **Create Key** summary page is displayed. Review the summary and click on **Close**.

3.7 Deleting Google Workspace Keys

- Select **Delete** from the drop-down list in the column of the key you want to delete.

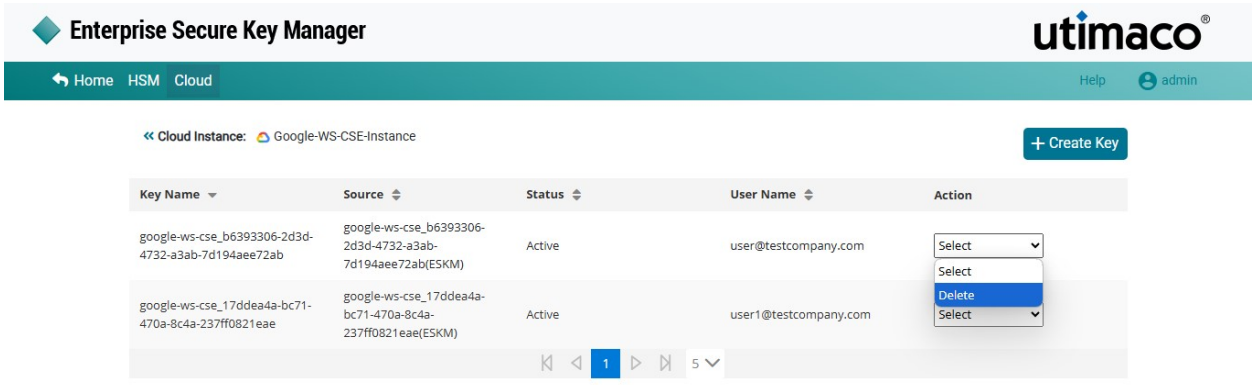


Figure 19 : Google Workspace - Delete Key

- An alert window will pop up asking *Are you sure you want to delete key (<key source>) from ESKM ?*

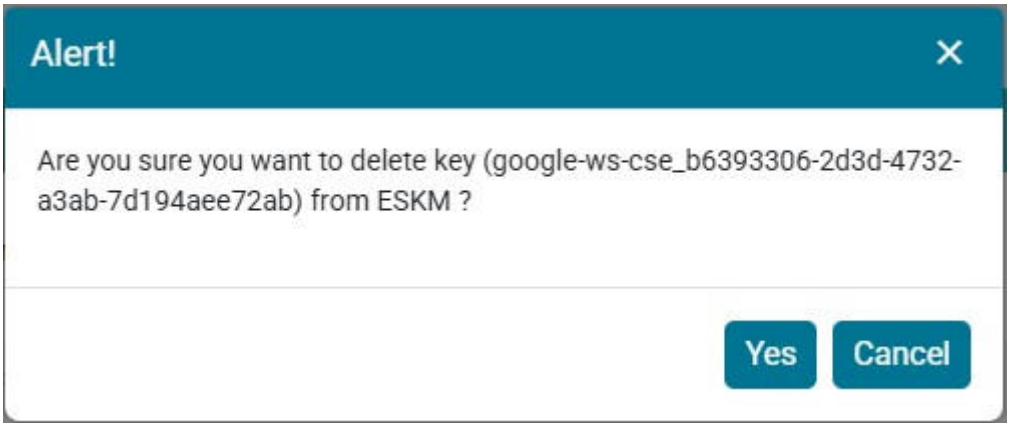


Figure 20 : Delete Key - Alert

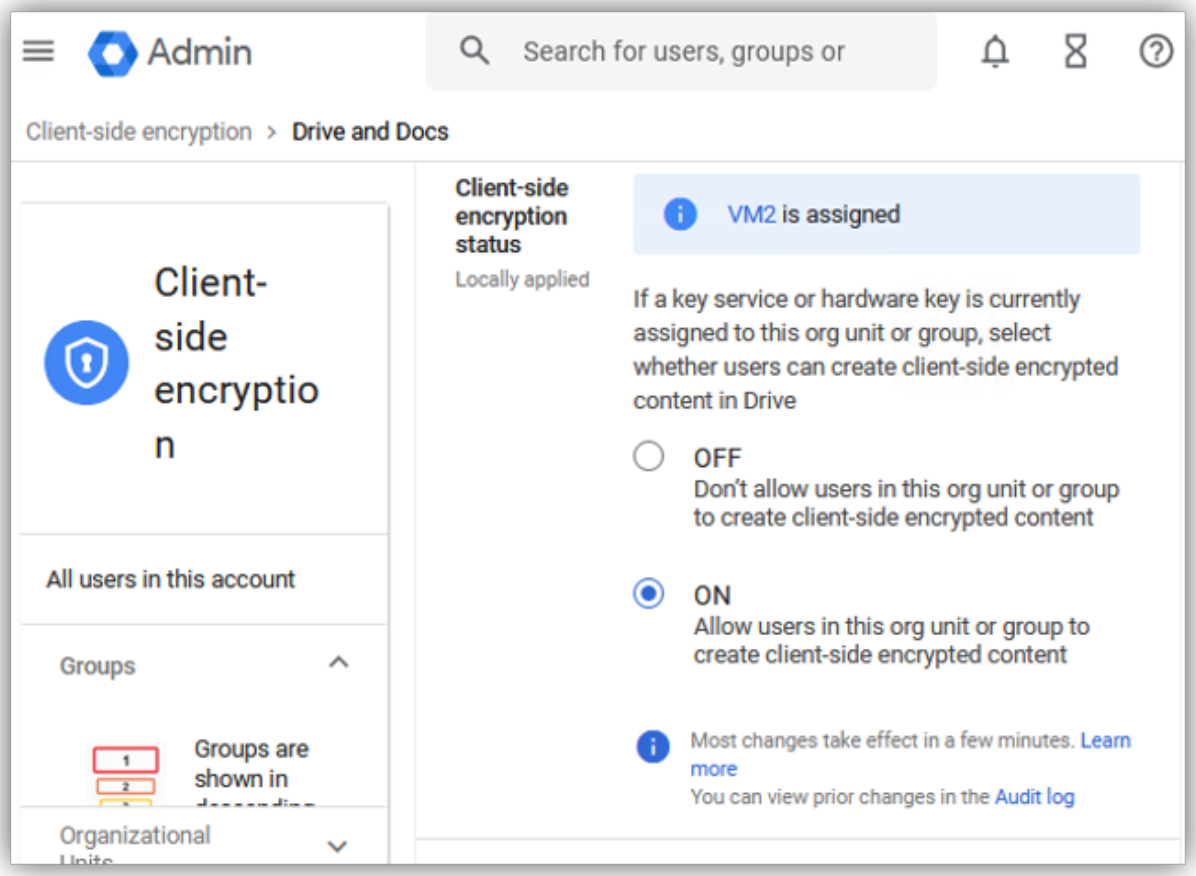
- Click on **Yes**.

The key will be deleted from ESKM.

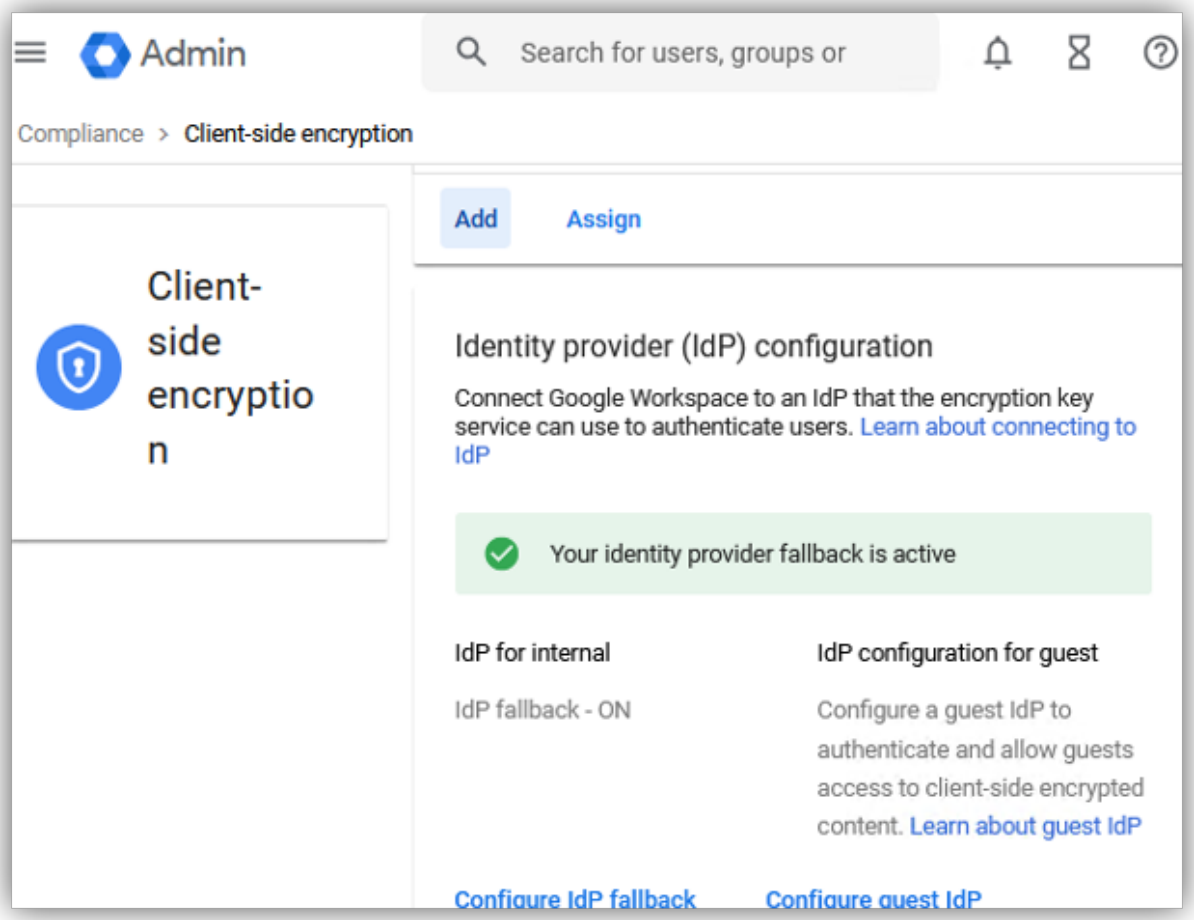
4 Google Workspace Configuration

To configure the Identity Provider in the Google Workspace Admin Console (https://admin.google.com/):

- Go to **Data** > **Compliance** > **Client-side encryption**.
- Add the ESKM URL (for examle https://vm2.testcompany.com) as the External Key Manager in the Google Workspace Admin Console.
- Assign the key manager to apply authentication methods for various Google Workspace applications such as Gmail, Meet, Calendar, and Drive & Docs.



- Go to to **Security** > **Access and data control** > **Client-side encryption** and select **Configure IdP fallback** under **Identity provider configuration.**



- Enter the **IDP Client ID**, which is obtained from the IDP Admin Console. The same Client ID should also be configured in the **Advanced Rest Settings**. For more information, see Configure ESKM.

4.1 Configuring Gmail to work with ESKM

ESKM can be used to sign and encrypt emails sent using Gmail. The workspace admin should get the private key of the S/MIME certificate encrypted for each user by submitting a privileged wrap request to ESKM. This wrapped private key can then be configured in Google by following the steps here: https://support.google.com/a/answer/13069736?sjid=9318445332644748151-NC.

4.2 Configuring ESKM for migration

To migrate encrypted content to a new key service, the current key service should be configured as the backup for the new service. ESKM can be added as a backup key manager for other key managers, and other key managers can also be added as backup key managers for ESKM.

To add ESKM as a backup key manager, create a key with the following username, in ESKM Google-WS-CSE-Instance:

`apps-security-cse-kaclscommunication@system.gserviceaccount.com`

This key will be used to encrypt data for all users. To add another key service as a backup to ESKM, include the `Issuer` value expected in privileged requests from the other key manager in the `IDP Issuer` section of the **Advanced REST Settings**.

5 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.