Microsoft Sentinel

Integration Guide

ESKM

8.54.15

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	2.0.0
Date	2026-08-13
Status	PUBLISHED
Document No.	IG-2026-0061

Table of Contents

1 Introduction

This guide is part of the support provided by Utimaco. Additional documentation produced to support your Utimaco Enterprise Secure Key Manager (ESKM) product can be found in the utimaco ESKM product documentation.

All Utimaco product documentation is available from Utimaco's website at *https://utimaco.com/*.

1.1 About This Guide

This guide describes how to integrate Utimaco Enterprise Secure Key Manager (ESKM) with Microsoft Sentinel, using the official Utimaco ESKM solution published in the Microsoft Sentinel Content Hub. The Utimaco ESKM solution ingests KMIP server logs from the ESKM management API into a Microsoft Sentinel Log Analytics workspace using the Codeless Connector Framework (CCF) RestApiPoller. Once data is flowing, the solution provides analytic rules, hunting queries, and a workbook for operational visibility and threat detection over key management activity.

1.2 Target Audience

This guide is intended for Microsoft Sentinel administrators and Utimaco ESKM administrators responsible for deploying and operating the integration.

1.3 Purpose of the Integration

The integration of Utimaco ESKM with Microsoft Sentinel serves a critical role in enhancing the security and compliance posture of cryptographic key management operations. By forwarding KMIP server logs to Sentinel, security operations teams gain:

- Centralized visibility into all KMIP operations, authentication events, and state changes.
- Automated detection of anomalous behavior such as brute-force authentication attempts, privilege escalation probing, and mass key destruction.
- Proactive threat hunting capabilities to identify rare users, new source IPs, high-volume key retrievals, and after-hours activity.
- An operational dashboard (workbook) for day-to-day monitoring of the KMIP plane.

1.4 Scope of the Integration

This integration enables monitoring and visibility of ESKM KMIP activity through Microsoft Sentinel by ingesting KMIP server logs from the ESKM management API. The solution provides real-time monitoring, automated threat detection, and proactive threat hunting capabilities for key management operations and security events.

1.5 Abbreviations

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
KMIP	Key Management Interoperability Protocol
HSM	Hardware Security Module
CCF	Codeless Connector Framework
DCR	Data Collection Rule
KQL	Kusto Query Language
API	Application Programming Interface
REST	Representational State Transfer
TLS	Transport Layer Security
HTTPS	Hypertext Transfer Protocol Secure
JSON	JavaScript Object Notation

Abbreviation	Meaning
ARM	Azure Resource Manager
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
QPS	Queries Per Second
RBAC	Role-Based Access Control
CA	Certificate Authority
NTP	Network Time Protocol
IP	Internet Protocol
URL	Uniform Resource Locator
VA	Virtual Appliance

Table 1: Abbreviations

1.6 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	Navigate to **Threat management** → **Hunting** → **Queries**
`Monospaced`	Code that is given for explanation or as an example, file paths	`UtimacoESKMKmipServerLogs_CL| where TimeGenerated > ago(24h)| take 100`
Italic	References and important terms	Rows arriving check (*Rows Are Arriving*)

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 marks the result expected after the successful execution of an instruction.

2 Product Overview

2.1 Overview of Microsoft Sentinel

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) solution built on Azure. It collects data at cloud scale across all users, devices, applications, and infrastructure (both on-premises and in multiple clouds), uses analytics and threat intelligence to detect attacks, and provides tools for threat investigation and response.

Microsoft Sentinel's Codeless Connector Framework (CCF) enables ingestion of data from external REST APIs into Log Analytics tables without requiring custom code, using polling-based data collection governed by a Data Collection Rule (DCR).

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 ESKM with Microsoft Sentinel combines the robust key management and audit capabilities of ESKM with the advanced threat detection and investigation features of Microsoft Sentinel. Organizations benefit from:

- Automated log ingestion - KMIP server logs are automatically polled every 5 minutes and ingested without manual intervention.
- Threat detection - Built-in analytic rules detect brute-force attacks, privilege probing, and mass key destruction in real time.
- Proactive hunting - Hunting queries allow security analysts to investigate anomalous patterns before they escalate.
- Operational dashboards - A purpose-built workbook provides at-a-glance visibility into key management activity.

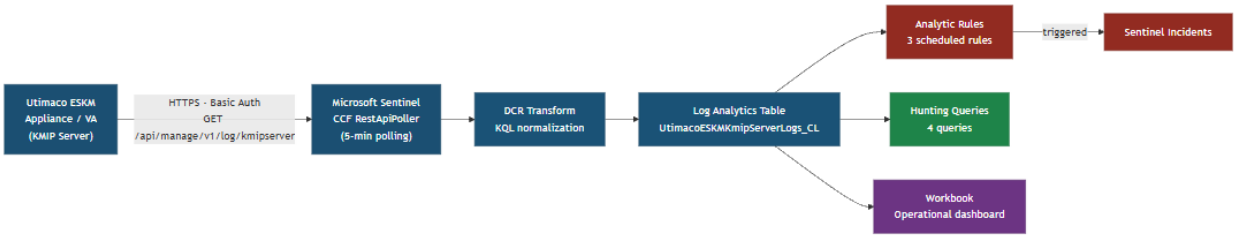

Figure 1 : Integration architecture overview

The ESKM appliance generates KMIP server logs that are polled every 5 minutes via HTTPS by the Sentinel CCF RestApiPoller using basic authentication. The raw logs are ingested into a custom stream, transformed by the DCR using KQL normalization, and written to the Log Analytics table. From there, the data flows to three detection channels: scheduled analytic rules that generate security incidents, proactive hunting queries for manual investigation, and an operational workbook for real-time dashboarding.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Enterprise Secure Key Manager (ESKM) from Content Hub	Utimaco ESKM Version
3.0.0	8.54.15

Table 3: Tested versions

3.2 Software Requirements

Software	Software Requirements
Utimaco ESKM	8.54.15 or later

Table 4: Software requirements

3.3 Prerequisites

Before you begin:

- Ensure that the Utimaco ESKM appliance (physical or virtual) is set up, initialized, and reachable from the internet over HTTPS on the management port (default 8443). Refer to the ESKM product documentation for setup instructions.
- Ensure that the Microsoft Sentinel workspace is provisioned and that you hold Microsoft Sentinel Contributor (or equivalent) permissions.
- Ensure that you have Active subscription in Azure with contributor rights at the resource group level.
- Collect the following information before starting the connector configuration wizard:

Information	Example
ESKM API Base URL	https://<eskm-host>:8443

Information	Example
username	admin
password	xxxxx

Table 5: Required connection information

4 Installing and Configuring ESKM

The initial phase involves configuring the ESKM before proceeding to Microsoft Sentinel. 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.

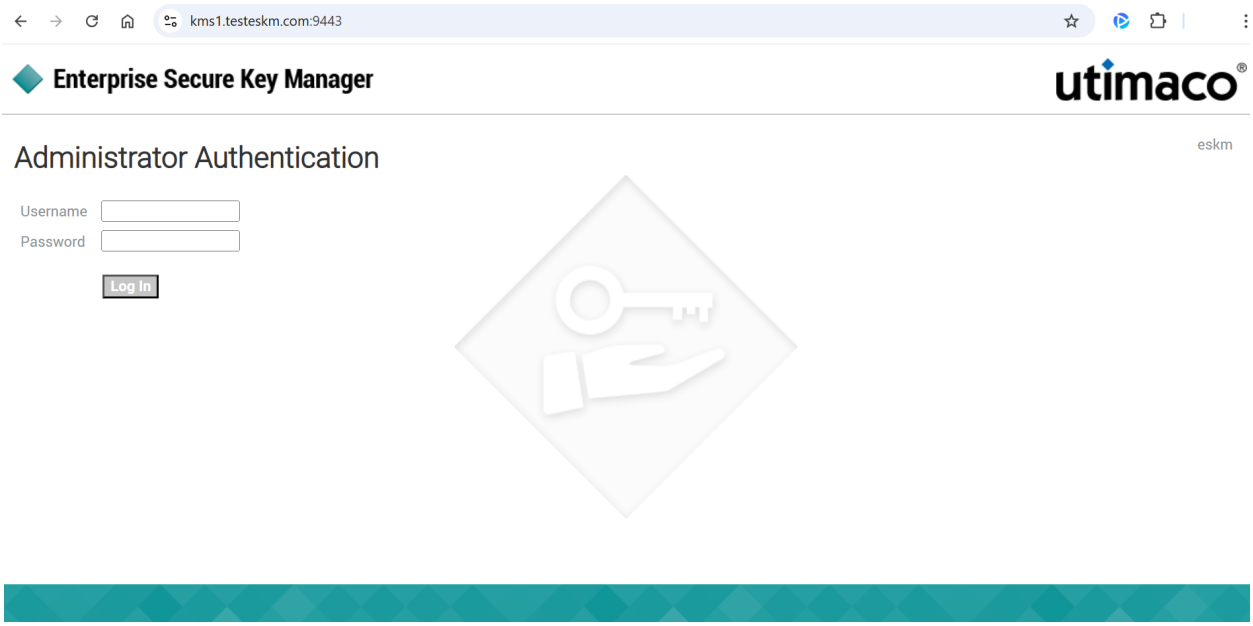

Figure 2 : ESKM login page

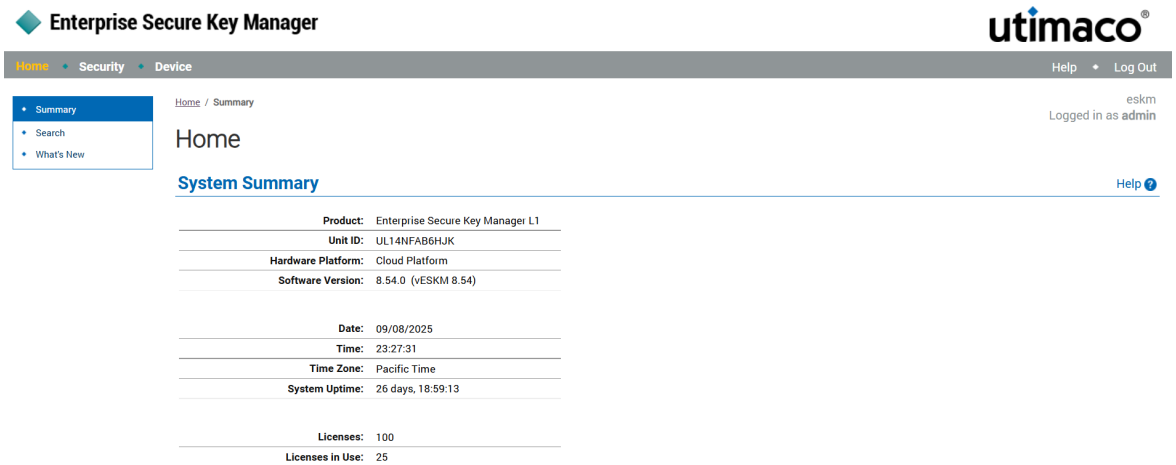

Figure 3 : ESKM home page

5 Verify KMIP Logs are Generated in ESKM

Ensure that the ESKM appliance is actively generating KMIP server logs. This verifies that the logging infrastructure is operational and will provide data to the connector.

1. Sign in to the ESKM Management Console as an administrator.
2. Navigate to **Device** → **Logs & Statistics** → **Log Viewer** → **KMIP** (path may vary by ESKM version).
3. Check that **KMIP Logs** are present and contain recent entries.
4. Verify the logs include operational events such as authentication, key operations, and connection events.

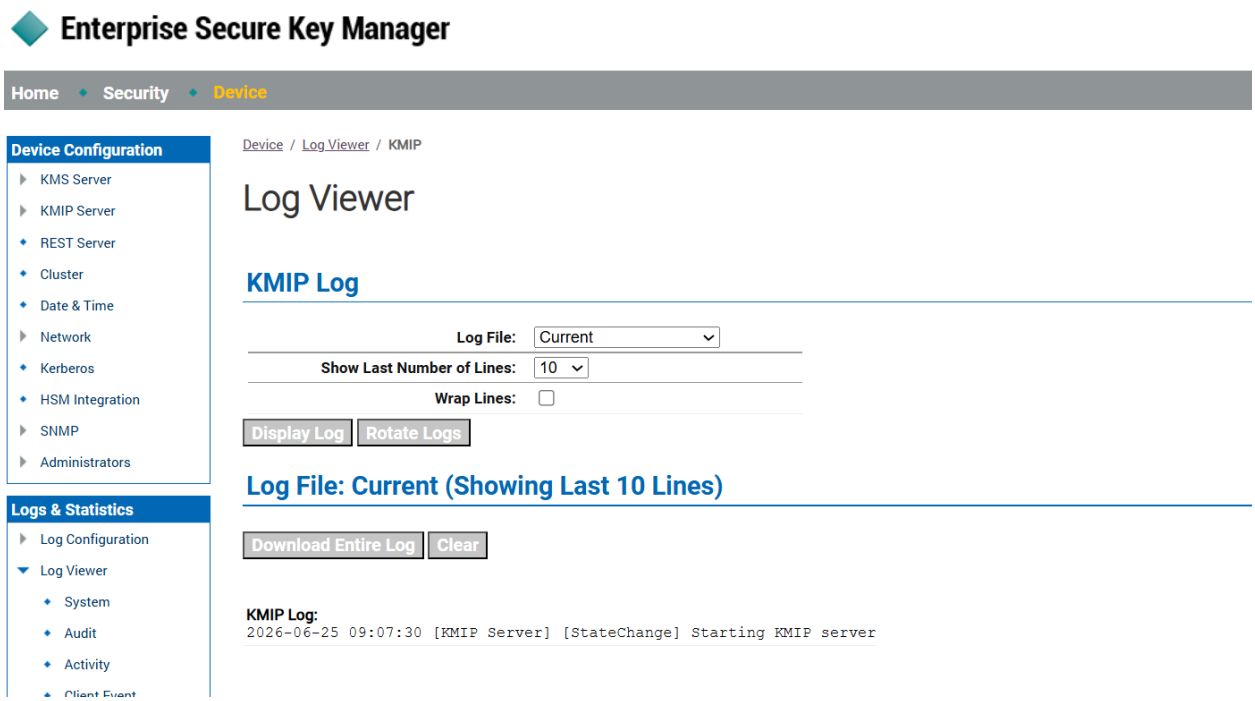

Figure 4 : KMIP logs

KMIP server logs are visible with recent entries.

KMIP logs are generated when a KMIP client is configured and interacts with the KMIP server. If logs are empty, ensure that a KMIP client is configured to connect to the server. For testing purposes, you can also disable and then enable the KMIP server to generate a startup/shutdown log entry.

6 Installing and Configuring Sentinel Solution

Follow these steps in the Azure Portal to deploy the Sentinel Solution:

1. Open the **Azure portal** → **Microsoft Sentinel** → select your workspace.
2. Go to **Content management** → **Content hub**.
3. Search for "**Utimaco Enterprise Secure Key Manager**".
4. Select the solution and click **Install**.
5. After installation, open **Manage** to see the included content (data connector, analytic rules, hunting queries, workbook).

The solution installs successfully, and all content items - one data connector, three analytic rules, four hunting queries and one workbook - appear in the Manage view.

7 Verify Network Connectivity

1. Ensure the ESKM appliance is reachable from the internet on port 8443 (or your configured management API port).
2. From an external host, test connectivity to verify the port is open.

If you cannot reach the appliance from outside your network, coordinate with your network team to open the required firewall rules.

8 Integration Steps

8.1 Configuration on Connector

1. In **Microsoft Sentinel**, go to **Configuration → Data connectors**.
2. Search for "Utimaco Enterprise Secure Key Manager (ESKM)" and click **Open connector page**. The connector page exposes a guided form. Provide the following details:

Field	Value
API Base URL	https://<eskm-host>:8443
Username	admin
Password	xxxxx

Table 6: Connector configuration fields

3. Click **Connect**. Sentinel will:
    a. Validate the credentials against {BaseUrl}/api/manage/v1/log/kmipserver.
    b. Provision the Data Collection Rule (UtimacoESKMDCR).
    c. Activate the RestApiPoller(UtimacoESKMKmipServerLogsConnector) on a 5-minute query window.

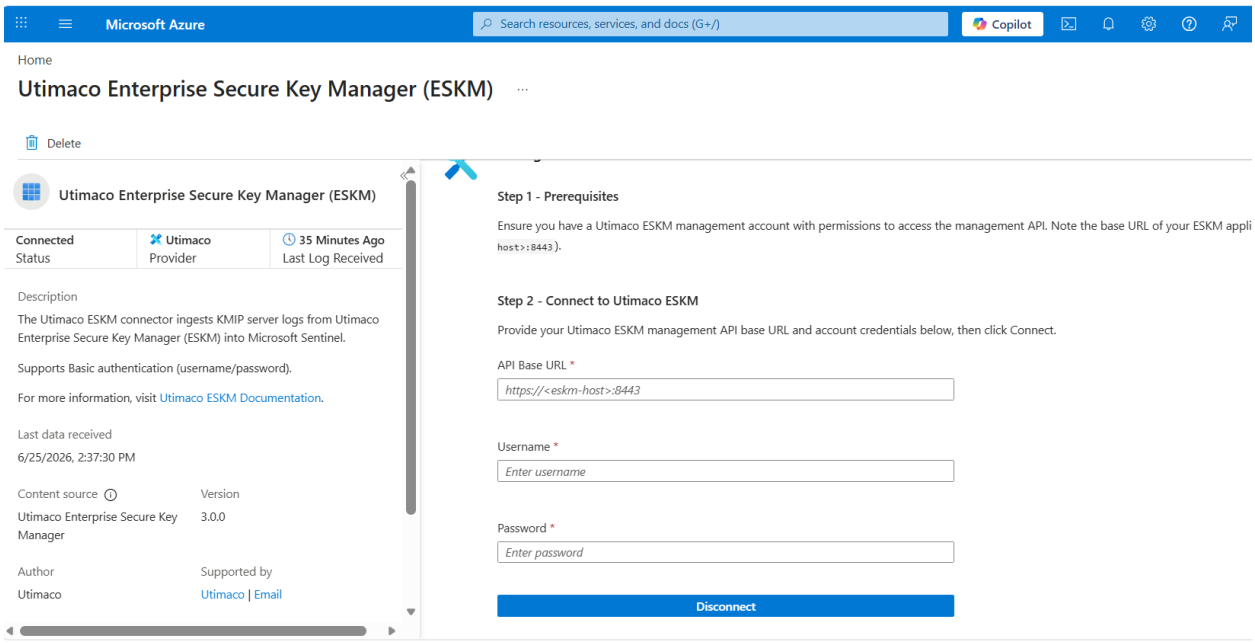

Figure 5 : ESKM connector

The connector status changes to Connected.

9 Verification and Testing

After connecting, allow 15–20 minutes for the first batch of events to land in the Log Analytics workspace.

9.1 Validate the Data Flow

Before validating data flow to Sentinel, first verify that ESKM is generating and forwarding logs to the data connector. This validation process confirms the complete data pipeline: from KMIP server logging through the Management API to Sentinel ingestion.

1. Navigate to **ESKM Management Console → Device → Logs & Statistics → Log Viewer → KMIP**.
2. Verify that KMIP events are being logged (authentication, operations, access attempts, etc.)
3. If no events appear, generate test traffic (e.g., a KMIP authentication or key operation) and verify it appears in the log viewer.

KMIP events are visible in the ESKM log viewer and recent timestamps are present.

Once you've confirmed KMIP logging is active, run the following queries in **Microsoft Sentinel → Logs** to validate data ingestion into Sentinel.

9.1.1 Rows Are Arriving

This query verifies that the Microsoft Sentinel connector is actively ingesting logs from Utimaco ESKM. It checks whether events have been received within the last hour and provides a summary of the total number of events along with the most recent ingestion timestamp.

```
UtimacoESKMKmipServerLogs_CL| where TimeGenerated > ago(1h)| summarize Events =
count(), LastSeen = max(TimeGenerated)
```

The query returns at least one row with a recent `LastSeen` timestamp. If no rows are returned after 30 minutes, refer to *Troubleshooting*.

9.1.2 Sample Events

This query retrieves a sample set of up to 100 events ingested in the last 24 hours. It allows you to inspect the raw log records generated by ESKM and verify that the data is being correctly parsed and stored in the custom Sentinel table.

```
UtimacoESKMKmipServerLogs_CL| where TimeGenerated > ago(24h)| take 100
```

These logs typically include fields such as event type, operation, user, result, and timestamps, which are mapped during ingestion. When reviewing the sample events, verify that all expected columns are populated with meaningful data, that timestamps are recent and accurate, and that user and IP information is correctly captured.

9.1.3 Event Distribution

This query provides a breakdown of events by type (e.g., authentication, key operations). It helps validate that different categories of ESKM activities are being ingested and that the connector is not restricted to a single event type.

```
UtimacoESKMKmipServerLogs_CL
| summarize count() by Event
| order by count_ desc
```

Review the results to identify the distribution of different KMIP event types in your environment. Expected event types include Authentication, Get, Create, Destroy, and StateChange operations. If you notice that certain expected operations (such as Destroy) have zero or significantly lower counts than anticipated, this may indicate a logging configuration issue or that those operations are not being performed during the monitoring period. A healthy data flow should show a balanced distribution of events representing the normal operations on your KMIP plane.

9.1.4 Connector Health Status

This step verifies the operational health of the data connector. It ensures that the connector is successfully authenticated, actively polling the ESKM API, and sending logs to Sentinel.

Navigate to **Configuration → Data connectors → Utimaco Enterprise Secure Key Manager (ESKM)**.

In the connector details, verify the following:

- **Status** should display **Connected** (indicating successful authentication and API communication).
- **Last Data received** should show a recent timestamp (typically within the last 10–15 minutes, depending on your polling interval).

10 Analytic Rules

10.1 Overview of Analytic Rules

Analytic rules are scheduled queries that automatically monitor your KMIP logs for predefined threat patterns and anomalies. Unlike hunting queries which are run on-demand, analytic rules execute continuously and generate incidents when they detect suspicious activities. This enables real-time alerting and automated incident creation for your security team.

Three scheduled analytic rules ship with the solution to detect threats targeting your KMIP plane. Rules must be individually enabled from **Configuration** → **Analytics** → **Rule templates**.

Rule	Severity	Detection Logic
Multiple KMIP authentication failures from same IP	Medium	≥ 5 authentication failures from one IP in 15 min
`PERMISSION_DENIED` burst for a KMIP user	Medium	≥ 10 permission denied events for one user in 30 min
Burst of `KMIP DESTROY` operations by a single user	High	≥ 20 successful destroy operations by one user in 10 min

Table 7: Analytic rules

10.2 How to Enable the Rules

Follow these steps to activate each analytic rule in your Microsoft Sentinel workspace:

1. Navigate to **Configuration** → **Analytics** → **Rule templates**.
2. Search for `Utimaco ESKM` to find the available rules.
3. Select a rule to view its detection logic.
4. Click **Create rule** to enable it in your workspace.

5. Configure notifications and automation playbooks as needed.

The rules will begin running on schedule and automatically generate incidents in **Threat management** → **Incidents** when they detect suspicious patterns. Configured notifications will alert your team, and linked automation playbooks will trigger as needed.

11 Run Hunting Queries

11.1 Overview of Hunting Queries

Hunting queries are proactive, on-demand searches that help uncover suspicious patterns and potential threats in your KMIP environment. Four pre-built queries are available under **Threat management → Hunting → Queries**.

Query	Purpose
Rare KMIP users	Detect newly provisioned or unknown service accounts
New source IPs	Surface unauthorized clients reaching the KMIP API
High-volume key retrievals	Identify credential harvesting or data exfiltration staging
After-hours activity	Catch insider or opportunistic activity outside business hours

Table 8: Hunting queries

Run queries weekly as part of your threat hunting routine to proactively search for emerging threats. Correlate findings with analytic alerts and workbook trends to build a complete picture of potential threats and validate your concerns.

11.2 How to Run the Queries

Follow these steps to execute a hunting query against your ESKM data.

1. Navigate to **Threat management → Hunting → Queries**.
2. Search for `Utimaco ESKM` to find the available queries.
3. Select a query to view its KQL logic.
4. Click **Run Selected Queries** to execute it against your data.
5. Click **View results** to review the results in the Log Analytics editor.

11.3 Using Results

After running a query, systematically review and action the results to strengthen your threat hunting process and incident response workflow:

- Select significant result rows from the results table to review the details.
- Link to incident from the toolbar options for findings that warrant investigation and team assignment.
- Run queries weekly as part of your threat hunting routine to proactively search for emerging threats.

12 Use the Workbook

The Enterprise Secure Key Manager Workbook is a pre-built operational dashboard that provides real-time visibility into KMIP operations, security events, and anomalies. Access it from your workspace to monitor traffic patterns, user activity, and authentication trends daily.

12.1 Save the Workbook from Templates

The Workbook is available as a template in Sentinel's Workbooks gallery. Save it to your workspace:

1. Navigate to **Threat management** → **Workbooks** → **Templates**.
2. Search for and select the **Utimaco Enterprise Secure Key Manager** template.
3. Click **Save** and select the location.

The workbook is now available in **My workbooks**.

12.2 Access and Daily Use

Access your saved workbook at **Threat management** → **Workbooks** → **My workbooks**. Select **Utimaco Enterprise Secure Key Manager** and click on **View saved workbook**.

The workbook provides:

- Event volume over time – track KMIP traffic patterns.
- Top users and source IPs – identify key operational sources.
- Operation distribution and failure ratios – monitor success vs. failure metrics.
- Authentication trends – detect credential or brute-force issues.

Figure 6 : ESKM operational dashboard

Use the workbook as daily operational dashboard for the KMIP plane. Filter by time range, users, or operations as needed for investigations and trend analysis.

13 Troubleshooting

13.1 Common Issues and How to Resolve Them

Symptom	Probable Cause	Resolution
Connector status: Disconnected immediately after Connect	Wrong Base URL, wrong port, bad credentials	Test the API endpoint with `curl` from a public host.
Connector connects, no data after 30 min	KMIP logs empty, polling window too narrow, or time skew on the appliance	Check ESKM appliance time synchronization (NTP). Generate test KMIP traffic and re-check `UtimacoESKMKmipServerLogs_CL`
Some events have an empty Operation field	Log entry is StateChange or Authentication Failure, which legitimately omit operation fields	Expected behavior. Use `where isnotempty(Operation)` to filter for client operations.

Table 9: Troubleshooting reference

13.2 Log Locations and Interpretation

Log locations may vary based on configuration. The primary diagnostic sources are:

Source	Location
Microsoft Sentinel connector status	**Configuration → Data connectors → Utimaco Enterprise Secure Key Manager → Status**
Sentinel ingestion logs	_LogOperation table in the Log Analytics workspace

Source	Location
DCR activity	Azure Monitor → Data Collection Rules → UtimacoESKMDCR → Activity Log
ESKM KMIP logs	In the ESKM Management Console, click Device -> Logs & Statistics -> Log Viewer -> KMIP

Table 10: Log locations

14 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.

15 Appendix A: KQL Query Reference

Query	Purpose
Rows arriving check (*Rows Are Arriving*)	Confirm events are being ingested
Sample events (*Sample Events*)	Browse recent raw events
Event distribution (*Event Distribution*)	Understand event type breakdown

Table 11: KQL query reference

16 Appendix B: References

Title	Description	Document/Link
Enterprise Secure Key Manager v8.54.0 Installation and Replacement Guide	Setup and configuration steps for Utimaco ESKM.	ESKM_Installation and Replacement_Guide.pdf

Table 12: References