Utimaco Enterprise Secure Key Manager (ESKM) Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures Utimaco ESKM so the CBOM Secure Discover_KMIP sensor can discover cryptographic assets over KMIP 1.2+ on TLS port 5696, read-only:

- Symmetric keys (AES, 3DES) - identifier, algorithm, length, state, creation date
- Asymmetric key pairs (RSA, EC) - public key attributes, usage masks, validity
- Certificates managed within ESKM - subject, issuer, serial, expiry, key references
- Secret data and opaque data objects in the KMIP namespace

No write, create, delete, or rotate operations are performed. The sensor authenticates with mutual TLS using a client certificate issued by the ESKM CA.

Prerequisites

- Utimaco ESKM 3.2 or later (KMIP 1.2 introduced in 3.2), initialized and licensed.
- ESKM Management Console access (typically https://<eskm-host>:2760) with Security Officer or Administrator role.
- Network reachability to the sensor host on TCP 5696; verify with openssl s_client -connect <eskm-host>:5696.
- The Discover_KMIP sensor module installed on the sensor host.
- The ESKM root CA certificate (or full chain) for server verification.
- The sensor host IP added to the KMIP allowlist if ESKM enforces IP allowlisting.

Step-by-Step Guide

Step 1: Create a Read-Only KMIP User

In User Management > Users > Add User, create cbom-kmip-sensor with the Auditor role (or Key Viewer). Confirm on the user detail page that the allowed KMIP operations include Locate, Get, Get Attributes, Get Attribute List, and Query - and that Create, Register, Destroy, Revoke, Archive, and Recover are not present.

Step 2: Enable the KMIP Service on Port 5696

- Go to Administration > Services and Edit the KMIP Service.
- Set Status to Enabled and confirm Port 5696.
- Set TLS Version to 1.2 or 1.3 (disable 1.0/1.1).

- Set Client Authentication to Mutual TLS (mTLS).
- Ensure KMIP 1.2 (and optionally 2.0) is allowed, then Save.

Confirm the listener with openssl s_client -connect <eskm-host>:5696 -tls1_2; the service should show Status: Running.

Step 3: Export the Client Certificate Bundle

In Certificate Manager > Client Certificates, generate a certificate with CN cbom-kmip-sensor, associated user cbom-kmip-sensor, RSA 2048 or EC P-256, 365-day validity. Download the PKCS#12 and split it, and export the ESKM root/intermediate CA:

```
openssl pkcs12 -in cbom-kmip-sensor.p12 -clcerts -nokeys -out cbom-kmip-sensor.crt.pem
openssl pkcs12 -in cbom-kmip-sensor.p12 -nocerts -nodes  -out cbom-kmip-sensor.key.pem


mkdir -p /etc/cbom/certs/eskm && chmod 700 /etc/cbom/certs/eskm
chmod 600 /etc/cbom/certs/eskm/cbom-kmip-sensor.key.pem
chmod 644 /etc/cbom/certs/eskm/cbom-kmip-sensor.crt.pem /etc/cbom/certs/eskm/eskm-
ca.crt.pem
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_KMIP
    enabled: true
    schedule: "0 2 * * *"
    targets:
      - id: utimaco-eskm-prod
        label: "Utimaco ESKM Production"
        vendor: utimaco
        product: eskm
        host: eskm.example.internal
        port: 5696
        kmip_version: "1.2"
        tls:
          ca_cert: /etc/cbom/certs/eskm/eskm-ca.crt.pem
          client_cert: /etc/cbom/certs/eskm/cbom-kmip-sensor.crt.pem
          client_key: /etc/cbom/certs/eskm/cbom-kmip-sensor.key.pem
          verify_hostname: true
          min_tls_version: "TLSv1.2"
        auth:
          method: mtls
          username: cbom-kmip-sensor      # must match the client cert CN
        discovery:
          object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate, SecretData]
          max_objects: 50000
          batch_size: 200
        output:
          backend: cbom-api
          endpoint: https://cbom.example.internal/api/v1/ingest
          api_key_env: CBOM_API_KEY
```

Reload after saving: cbom-sensor reload.

Step 5: Validate

```
cbom-sensor run --sensor Discover_KMIP --target utimaco-eskm-prod --dry-run
cbom-sensor run --sensor Discover_KMIP --target utimaco-eskm-prod
```

Confirm authentication as cbom-kmip-sensor and a Locate object count. Verify assets under Assets > Key Management, and check the ESKM audit log shows only Locate/Get Attributes for the user - no writes.

Common Errors

TLS Handshake Failed - unable to get local issuer certificate

Cause: ca_cert is wrong or the CA file is missing intermediate certificates.

Resolution: Re-export the full chain from Certificate Manager > CA Certificates, update ca_cert, and reload.

KMIP PermissionDenied

Cause: The user lacks Locate or Get Attributes, or its role was modified.

Resolution: Confirm the Auditor/Key Viewer role and restore Locate/Get/Get Attributes; add explicit per-operation grants if ESKM requires them.

Connection Refused on Port 5696

Cause: The KMIP service is not running, uses another port, or a firewall/allowlist blocks the sensor.

Resolution: Confirm the service under Administration > Services, verify the port, test with nc -zv, open TCP 5696, and add the sensor IP to Allowed Clients.

Security Recommendations

- Restrict the sensor user to Auditor/Key Viewer - never grant Create, Destroy, Revoke, or Archive.
- Rotate the client certificate annually before expiry.
- Store the client private key with chmod 600 (or inject via a secrets manager at runtime).
- Enable ESKM audit logging for the sensor user and forward to your SIEM; alert on any write.
- Enforce TLS 1.2 minimum on both ends and disable weak ciphers (RC4, 3DES, export).

Conclusion

With a read-only Auditor user, mutual TLS, and Get Attributes/Locate operations only, the Discover_KMIP sensor enumerates ESKM keys, certificates, and secret objects with no risk of modification - continuously populating CBOM Secure with an up-to-date inventory for compliance reporting and cryptographic risk visibility.