KEYper Enterprise Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide integrates KEYper Enterprise (a KMIP-compliant key management server) with the CBOM Secure Discover_KMIP sensor over KMIP 1.2+ on TLS port 5696, read-only:

- Symmetric keys (AES, 3DES) and asymmetric key pairs (RSA, EC)
- X.509 certificates registered as KMIP managed objects
- Secret data objects and opaque cryptographic blobs
- Key metadata: algorithm, length, activation/expiration dates, state, owning application

The sensor performs only read-only KMIP operations (Locate, Get Attributes, Query).

Prerequisites

- KEYper Enterprise 6.0+ with KMIP 1.2+ enabled and TLS on port 5696.
- Admin access to the KEYper management console.
- Connectivity from the sensor host to TCP 5696; OpenSSL on the host.
- The KEYper CA certificate available for download.

Step-by-Step Guide

Step 1: Create a KeyAudit Service Account

In the console (https://<host>:8443/keyper/admin) → Administration → Users & Accounts → Add User, create cbom-sensor with Account Type Service Account, Permission Level KeyAudit, and Interactive Login Disabled. KeyAudit allows Locate, Get Attributes, Get Attribute List, Query, and Discover Versions — and denies Get (raw key material), Create, Register, Destroy, and Revoke.

Step 2: Confirm the KMIP TLS Listener

Under Configuration → Network Services, ensure the KMIP Service is running with KMIP 1.2, port 5696, TLS 1.2 minimum, and Client Auth Required (mTLS). Verify reachability:

```
openssl s_client -connect <keyper-host>:5696 -tls1_2
```

Step 3: Issue a Client Certificate

```
openssl req -newkey rsa:2048 -keyout cbom-sensor.key -out cbom-sensor.csr \
  -subj "/CN=cbom-sensor/O=<Your-Org>/C=US" -nodes
chmod 600 cbom-sensor.key
```

In the console → Administration → Client Certificates → Issue Certificate, paste the CSR, set Associated User cbom-sensor, Use KMIP Client Authentication, and a 365-day validity. Download

cbom-sensor.crt and the CA (Configuration → Certificate Authority → Download CA Certificate as keyper-ca.crt). Place all three at /etc/cbom/sensors/kmip/ with key 600, certs 644.

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
  schedule: "0 2 * * *"
connection:
  host: keyper-enterprise.internal.example.com
  port: 5696
  protocol: kmip
  kmip_version: "1.2"
  tls:
    enabled: true
    min_tls_version: "TLS1_2"
    ca_cert: /etc/cbom/sensors/kmip/keyper-ca.crt
    client_cert: /etc/cbom/sensors/kmip/cbom-sensor.crt
    client_key: /etc/cbom/sensors/kmip/cbom-sensor.key
    verify_server_cert: true
authentication:
  method: certificate
  username: cbom-sensor
discovery:
  operations: [Locate, GetAttributes, GetAttributeList, Query, DiscoverVersions]
  object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate, SecretData, OpaqueData]
output:
  cbom_endpoint: https://cbom-platform.internal.example.com/api/v1/ingest
  api_token: ${CBOM_API_TOKEN}
```

Step 5: Validate

```
sudo systemctl start cbom-sensor-kmip
sudo tail -f /var/log/cbom/discover_kmip.log
```

Confirm a TLS handshake, authentication as cbom-sensor (KeyAudit), and a located-object count; verify keys/certs under Assets filtered by sensor_source: keyper-enterprise, with no raw key material present.

Common Errors

TLS handshake failure

Cause: ca_cert is incorrect/incomplete (e.g. missing intermediate).

Resolution: Download the full CA chain and verify with openssl verify -CAfile keyper-ca.crt cbom-sensor.crt.

KMIP authorization denied (Locate)

Cause: cbom-sensor lacks the KeyAudit permission level.

Resolution: Confirm KeyAudit and that Locate is Allowed on the Permissions tab; restart the sensor.

Connection refused on 5696

Cause: The KMIP listener is stopped or a firewall blocks 5696.

Resolution: Confirm the service is Running, test with nc -zv, and open TCP 5696 to the sensor host.

Security Recommendations

- Rotate the client certificate annually and restart the sensor after rotation.
- Store the CBOM API token in a secrets manager, injected at runtime.
- Restrict the KeyAudit account by IP allowlist to the sensor host.
- Enable KEYper audit logging for cbom-sensor's KMIP operations.
- Never grant the account the Get permission (raw key material).

Conclusion

With a read-only KeyAudit account, the KMIP TLS listener, and mutual TLS certificates, the Discover_KMIP sensor provides continuous, automated discovery of cryptographic objects in KEYper Enterprise — surfacing them in CBOM Secure without ever retrieving key bytes.