Townsend Alliance Key Manager (AKM) Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures Townsend Alliance Key Manager (AKM) so the CBOM Secure Discover_KMIP sensor can connect over mutual TLS (port 5696, KMIP 1.2+) and enumerate managed cryptographic assets, read-only:

- Symmetric keys (AES-128, AES-256) used for SQL Server and Oracle TDE
- Asymmetric key pairs (RSA, ECC) in the KMIP object store
- Certificate objects stored in the KMIP object store
- Key metadata: algorithm, length, state, creation/modification dates, names, and custom attributes

All connections are read-only - no keys or key material are exported or modified.

Prerequisites

- AKM 8.0 or later, reachable from the sensor host.
- The KMIP module licensed and enabled (contact Townsend Security if absent).
- Administrator access to the AKM web console (default https://<akm-host>:8443).
- TCP 5696 reachable from the sensor host; verify with nc -zv <akm-host> 5696.
- CBOM platform 2.4 or later with the Discover_KMIP module.
- A valid CBOM API token for result ingestion.

Step-by-Step Guide

Step 1: Create a KMIP Audit User

In the AKM console, go to Security > Users > Add User and create a dedicated read-only account:

- Username: cbom-kmip-auditor
- Full Name: CBOM KMIP Sensor
- Role: Key Audit (read-only metadata; no use, export, or modify)
- Enable the Allow KMIP Access checkbox

If Key Groups isolate keys, add cbom-kmip-auditor to the Authorized Users list of each in-scope group under Security > Key Groups.

Step 2: Enable KMIP on Port 5696

- Go to Configuration > KMIP and confirm the service status is Running (Start Service if stopped).
- Confirm the listening port is 5696.

- Set TLS Version to 1.2 minimum (1.3 preferred).
- Set Client Authentication > Require Client Certificate to Enabled (mutual TLS).
- Note the CA certificate AKM uses to sign KMIP client certificates, then Apply.

Step 3: Download the KMIP Client Certificate

Go to Security > KMIP Certificates > Generate Client Certificate with CN cbom-kmip-sensor, associated user cbom-kmip-auditor, and a 365-day validity. Download the ZIP (client cert, private key, AKM CA cert) and place them on the sensor host:

```
/etc/cbom/certs/akm/cbom-kmip-sensor.crt
/etc/cbom/certs/akm/cbom-kmip-sensor.key
/etc/cbom/certs/akm/akm-ca.crt

chmod 600 /etc/cbom/certs/akm/cbom-kmip-sensor.key
chown cbom-sensor:cbom-sensor /etc/cbom/certs/akm/cbom-kmip-sensor.key
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_KMIP
    enabled: true
    schedule: "0 */6 * * *"          # every 6 hours
    type: kmip
    connection:
      host: akm.example.com
      port: 5696
      tls:
        enabled: true
        min_version: "TLS1.2"
        client_cert: /etc/cbom/certs/akm/cbom-kmip-sensor.crt
        client_key: /etc/cbom/certs/akm/cbom-kmip-sensor.key
        ca_cert: /etc/cbom/certs/akm/akm-ca.crt
        verify_server: true
    auth:
      username: cbom-kmip-auditor
      password: "${AKM_KMIP_PASSWORD}"
    discovery:
      object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate]
      include_states: [PreActive, Active, Deactivated, Compromised]
      max_objects: 10000
    cbom_backend:
      api_endpoint: https://cbom.example.com/api/v1/ingest
      api_token: "${CBOM_API_TOKEN}"
      asset_source_label: akm-production
```

Note Never store passwords or API tokens in plaintext. Use ${} environment substitution or a secrets manager.

Step 5: Validate

```
openssl s_client -connect akm.example.com:5696 \
  -cert /etc/cbom/certs/akm/cbom-kmip-sensor.crt \
  -key /etc/cbom/certs/akm/cbom-kmip-sensor.key \
  -CAfile /etc/cbom/certs/akm/akm-ca.crt -verify_return_error
cbom-sensor run --sensor Discover_KMIP --dry-run
cbom-sensor run --sensor Discover_KMIP
```

A handshake returning Verify return code: 0 (ok) plus a dry-run object list confirms the setup. Then filter by Source: akm-production in Assets > Cryptographic Keys.

Common Errors

TLS Handshake Failed - certificate signed by unknown authority

Cause: The AKM CA certificate is missing or wrong in the ca_cert field.

Resolution: Re-download the CA from Configuration > KMIP > Download CA Certificate, confirm PEM format, and restart the sensor.

KMIP NotAuthorized - Access Denied

Cause: cbom-kmip-auditor lacks KMIP access, has a wrong password, or is not in the relevant Key Groups.

Resolution: Confirm Allow KMIP Access and the Key Audit role, add the user to each Key Group, and re-verify the password.

Connection Refused on Port 5696

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

Resolution: Start the service, test with nc -zv, open TCP 5696, and confirm the listener with ss -tlnp | grep 5696.

Security Recommendations

- Use the cbom-kmip-auditor account exclusively for the sensor.
- Rotate the KMIP client certificate annually - expired certs cause silent failures.
- Inject the AKM password and CBOM token via a secrets manager, never plaintext YAML.
- Restrict the client private key to the sensor service account (chmod 600).
- Enable AKM KMIP audit logging so sensor reads are recorded for compliance.

Conclusion

With a Key Audit user, mutual TLS on port 5696, and read-only Locate/Get Attributes operations, the Discover_KMIP sensor continuously inventories all KMIP-managed objects in Townsend AKM - including SQL Server and Oracle TDE keys - without modifying or exporting any key material.