Thales CipherTrust Manager Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures Thales CipherTrust Manager as a read-only KMIP source for the CBOM Secure Discover_KMIP sensor (KMIP 1.2+ over TLS, port 5696):

- Symmetric and asymmetric key identifiers (KMIP UIDs)
- Key algorithms (AES, RSA, EC), lengths, and curve parameters
- Creation/activation dates and state (Pre-Active, Active, Deactivated, Destroyed)
- Key names and custom attributes where accessible

Strictly read-only — only metadata via KMIP Locate and Get Attributes; raw key material is never requested.

Prerequisites

- Admin access to the CipherTrust Manager web UI (2.0+ recommended).
- CipherTrust reachable on TCP 5696 from the sensor host; the KMIP interface licensed.
- OpenSSL on the sensor host; the cbom-sensor binary 1.4.0+ installed.
- The CipherTrust hostname/IP for the sensor config.

Step-by-Step Guide

Step 1: Create a Key User Local User

In Admin → User Management → Users → Create User, add cbom-kmip-readonly with the Key User role (read-only key metadata). Do not assign Key Admin, Admin, or any write-capable role.

Step 2: Enable the KMIP Interface

Under Admin → Services, enable the KMIP service and confirm it is Running on port 5696. Note the CA that signed the KMIP server certificate (export the local root CA under Admin → CA → Local as ciphertrust-ca.pem if internal).

Step 3: Create a Bound Client Certificate

Under Certificates → Client Certificates → Create Client Certificate, set CN cbom-kmip-sensor and Associated User cbom-kmip-readonly (this binds the cert to the Key User role). Download the client certificate, private key, and CA. Stage and verify on the sensor host:

```
chmod 600 /etc/cbom/certs/ciphertrust/cbom-sensor-key.pem
chmod 644 /etc/cbom/certs/ciphertrust/cbom-sensor-cert.pem
/etc/cbom/certs/ciphertrust/ciphertrust-ca.pem
```

```
openssl verify -CAfile /etc/cbom/certs/ciphertrust/ciphertrust-ca.pem \
  /etc/cbom/certs/ciphertrust/cbom-sensor-cert.pem
openssl x509 -noout -modulus -in .../cbom-sensor-cert.pem | md5sum
openssl rsa  -noout -modulus -in .../cbom-sensor-key.pem  | md5sum    # must match
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_KMIP
    type: kmip
    enabled: true
    schedule: "0 2 * * *"
    connection:
      host: ciphertrust.example.internal
      port: 5696
      kmip_version: "1.2"
      tls:
        enabled: true
        ca_cert: /etc/cbom/certs/ciphertrust/ciphertrust-ca.pem
        client_cert: /etc/cbom/certs/ciphertrust/cbom-sensor-cert.pem
        client_key: /etc/cbom/certs/ciphertrust/cbom-sensor-key.pem
        verify_server_cert: true
    discovery:
      operations: [Locate, GetAttributes]
      include_destroyed_objects: false
    output:
      tags: { source: ciphertrust-manager }
```

Step 5: Validate

```
cbom-sensor run --sensor Discover_KMIP --once
journalctl -u cbom-sensor -n 100 --no-pager | grep -i "Discover_KMIP"
```

Confirm a TLS handshake, a Locate returning object identifiers, and forwarded records; filter the inventory by source: ciphertrust-manager. In Admin → Audit Logs, only Locate and Get Attributes should appear for cbom-kmip-readonly.

Common Errors

TLS handshake — unknown CA

Cause: ca_cert doesn't match the CA that signed the KMIP server certificate.

Resolution: Export the correct CA from Admin → Services → KMIP; concatenate intermediate+root into a bundle if needed.

KMIP permission denied on Locate

Cause: The user/cert lacks Key User, or the cert isn't bound to cbom-kmip-readonly.

Resolution: Confirm the Key User role and that the client cert's Associated User is cbom-kmip-readonly; re-issue/redeploy if not.

Connection refused on 5696

Cause: The KMIP service is not running or a firewall blocks 5696.

Resolution: Test nc -zv; confirm the service Running under Admin → Services; allow TCP 5696 (incl. cloud security groups).

Security Recommendations

- Store the client key readable only by cbom-agent (chmod 600); never in source control.
- Use the dedicated Key User account — never an Admin/Key Admin account.
- Rotate the client certificate at least 30 days before expiry and revoke the old one.
- Enable audit logging and alert on any operation other than Locate/Get Attributes.
- Restrict KMIP (5696) by source IP to the sensor host where possible.

Conclusion

With a dedicated Key User, the KMIP interface enabled, and a bound client certificate, the Discover_KMIP sensor safely enumerates CipherTrust Manager key metadata over mutual TLS — providing continuous inventory visibility without accessing raw key material.