QuintessenceLabs qCrypt Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures a QuintessenceLabs qCrypt KMS so the CBOM Secure Discover_KMIP sensor can discover cryptographic assets over KMIP 1.2+ on mutual TLS port 5696, read-only:

- Symmetric and asymmetric managed keys (AES, RSA, EC)
- Key metadata: algorithm, length, state, creation/activation/expiry dates
- Named key objects and key groups, plus associated certificates
- Key lifecycle states (Pre-Active, Active, Compromised, Destroyed)

The sensor issues only KMIP Locate and Get Attributes; no keys are exported, modified, or destroyed.

Prerequisites

- A qCrypt appliance on firmware 3.0+ with the KMIP service available.
- A qCrypt administrator account able to create service accounts and manage the KMIP interface.
- Connectivity from the sensor host to TCP 5696; OpenSSL 1.1.1+ on the host.
- The qCrypt CA certificate (Admin → Certificates → CA Bundle).
- The Discover_KMIP plugin enabled in the CBOM sensor manager.

Step-by-Step Guide

Step 1: Create a Key User Service Account

In the qCrypt console (https://<appliance-ip>), under Admin → Users & Groups → Users → Add User, create cbom-sensor-svc with Role Key User and Authentication Method Certificate. Then under Admin → Policies → Access Control, add a policy cbom-kmip-readonly for that principal allowing Locate, Get, Get Attributes, Get Attribute List, and Discover Versions (deny all write/destroy operations); scope it to All Managed Objects or specific key groups.

Step 2: Enable the KMIP Interface

Under Admin → Services → KMIP, ensure the service is Running with Port 5696, TLS 1.2/1.3 only, Client Certificate Authentication Required, and KMIP 1.2 minimum.

Step 3: Provision the Client Certificate

```
openssl req -newkey rsa:2048 -nodes \
  -keyout /etc/cbom/certs/cbom-sensor-client.key \
  -out /etc/cbom/certs/cbom-sensor-client.csr \
  -subj "/CN=cbom-sensor-svc/O=CBOM/OU=Security"
```

In Admin → Certificates → Client Certificates → Issue Certificate, upload the CSR (CN cbom-sensor-svc, 365-day validity) and download the signed cert as cbom-sensor-client.crt. Download the CA bundle (Admin → Certificates → CA Bundle) as qcrypt-ca.pem, then set permissions (key 600, certs 644).

Step 4: Verify mTLS Connectivity

```
openssl s_client -connect <qcrypt-appliance-ip>:5696 \
  -CAfile /etc/cbom/certs/qcrypt-ca.pem \
  -cert /etc/cbom/certs/cbom-sensor-client.crt \
  -key /etc/cbom/certs/cbom-sensor-client.key
```

Step 5: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
  schedule: "0 2 * * *"
target:
  vendor: QuintessenceLabs
  product: qCrypt
  host: 192.168.10.50
  port: 5696
  kmip_version: "1.2"
auth:
  method: mutual_tls
  client_cert: /etc/cbom/certs/cbom-sensor-client.crt
  client_key: /etc/cbom/certs/cbom-sensor-client.key
  ca_cert: /etc/cbom/certs/qcrypt-ca.pem
discovery:
  object_types: [SymmetricKey, PrivateKey, PublicKey, Certificate, SecretData]
  include_compromised: false
output:
  format: cbom_json
  tags: { sensor_source: quintessencelabs_qcrypt }
```

Step 6: Validate

```
systemctl restart cbom-sensor
cbom-sensor run --sensor Discover_KMIP --once
tail -n 100 /var/log/cbom/discover_kmip.log
```

Confirm a TLS handshake, a KMIP session, and a located-object count. In the qCrypt audit log, only Locate and Get Attributes should appear for cbom-sensor-svc.

Common Errors

TLS handshake — certificate verify failed

Cause: ca_cert doesn't match the chain qCrypt presents, or the bundle is incomplete.

Resolution: Re-download the CA bundle and verify with openssl verify -CAfile qcrypt-ca.pem cbom-sensor-client.crt.

KMIP permission denied on Locate

Cause: The cbom-kmip-readonly policy doesn't permit Locate, or wasn't applied to the target groups.

Resolution: Confirm Locate under Operations Allowed, Save and Apply, and include the target key groups in scope.

Connection refused on 5696

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

Resolution: Enable the service (Admin → Services → KMIP) and test with nc -zv.

Security Recommendations

- Scope the read-only policy to only the relevant key groups where possible.
- Rotate the client certificate before expiry; monitor with openssl x509 -enddate.
- Store the private key at chmod 600, readable only by the sensor process.
- Forward the qCrypt audit log to your SIEM and alert on write/destroy operations.
- Enforce TLS 1.2 minimum; disable TLS 1.0/1.1 on the KMIP interface.

Conclusion

With a Key User service account, a read-only access policy, and mutual TLS, the Discover_KMIP sensor provides continuous, read-only visibility into the qCrypt cryptographic key inventory — keeping CBOM Secure's bill of materials accurate without ever exporting key material.