Eperi Cloud Data Protection Gateway Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures the Eperi Cloud Data Protection Gateway as a source for the CBOM Secure Discover_KMIP sensor, which connects over KMIP 1.2+ on TLS port 5696 and reads, read-only:

- Symmetric keys (AES-128, AES-256) managed by the gateway
- Asymmetric key pairs (RSA, EC) in the gateway key store
- Key metadata: identifiers, algorithm, length, state, creation timestamps
- Certificate objects registered with the KMIP server

Prerequisites

- Admin access to the Eperi Gateway management console (typically https://<host>:8443/admin).
- Eperi Gateway 4.x or later (KMIP 1.2+).
- The KMIP port (default 5696) reachable from the sensor host (verify with nc -zv).
- The Discover_KMIP sensor package installed and the agent running.
- A PKI or the gateway's built-in CA to issue a TLS client certificate.
- OpenSSL on the host to generate the CSR.

Step-by-Step Guide

Step 1: Create a Read-Only Service Account

In the management console, under Administration → User Management → Add User, create cbom-sensor-ro with Authentication Certificate and a read-only role. If the KeyViewer role does not exist, create it under Role Management with only Key: List, Key: Get Attributes, Certificate: List, and Certificate: Get Attributes enabled, then assign it.

Step 2: Enable the KMIP Endpoint

Under Services → KMIP, confirm KMIP Status Enabled, Listener Address reachable from the sensor host, Port 5696, and Protocol Version 1.2+. Under KMIP → Access Control, add the sensor host IP (e.g. <cbom-sensor-ip>/32) and Apply.

Step 3: Generate a Client Key and CSR

```
openssl req -new -newkey rsa:2048 -nodes \
  -keyout /etc/cbom/sensors/kmip/cbom-sensor-ro.key \
  -out /etc/cbom/sensors/kmip/cbom-sensor-ro.csr \
  -subj "/CN=cbom-sensor-ro/O=CBOM/OU=Sensors"

chmod 600 /etc/cbom/sensors/kmip/cbom-sensor-ro.key
```

Step 4: Sign the CSR and Download the CA Bundle

In the console under PKI → Certificate Authority → Sign CSR, paste the CSR, set Extended Key Usage clientAuth and a 365-day validity, sign, and download the certificate. Download the CA chain as eperi-ca-bundle.pem. Verify:

```
cp cbom-sensor-ro.crt /etc/cbom/sensors/kmip/cbom-sensor-ro.crt
cp eperi-ca-bundle.pem /etc/cbom/sensors/kmip/eperi-ca-bundle.pem
chmod 644 /etc/cbom/sensors/kmip/cbom-sensor-ro.crt /etc/cbom/sensors/kmip/eperi-ca-
bundle.pem

openssl verify -CAfile /etc/cbom/sensors/kmip/eperi-ca-bundle.pem \
  /etc/cbom/sensors/kmip/cbom-sensor-ro.crt
```

Then, under User Management → cbom-sensor-ro → Certificate Authentication, upload the signed certificate so the gateway maps mTLS connections to the account.

Step 5: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
  schedule: "0 2 * * *"
connection:
  host: "eperi-gateway.example.com"
  port: 5696
  protocol: kmip
  kmip_version: "1.2"
  tls:
    enabled: true
    ca_bundle: "/etc/cbom/sensors/kmip/eperi-ca-bundle.pem"
    client_cert: "/etc/cbom/sensors/kmip/cbom-sensor-ro.crt"
    client_key: "/etc/cbom/sensors/kmip/cbom-sensor-ro.key"
    verify_hostname: true
credentials:
  auth_method: "certificate"
discovery:
  object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate]
  max_objects_per_request: 100
output:
  cbom_endpoint: "https://cbom-server.example.com/api/v1/ingest"
  tags: { source: "eperi-gateway", environment: "production" }
systemctl reload cbom-agent
```

Step 6: Validate

```
cbom-sensor test --sensor Discover_KMIP --config /etc/cbom/sensors/discover_kmip.yaml

openssl s_client -connect eperi-gateway.example.com:5696 \
  -cert /etc/cbom/sensors/kmip/cbom-sensor-ro.crt \
  -key /etc/cbom/sensors/kmip/cbom-sensor-ro.key \
  -CAfile /etc/cbom/sensors/kmip/eperi-ca-bundle.pem -verify_return_error
```

Confirm an mTLS handshake, authentication as cbom-sensor-ro, and a Locate object count. In the gateway audit log, only Locate and Get Attributes should appear for the account.

Common Errors

TLS handshake — certificate unknown

Cause: The client certificate is not uploaded to cbom-sensor-ro, or its CA is not trusted by the gateway.

Resolution: Confirm the cert under Certificate Authentication; ensure the signing CA appears under PKI → Trusted CAs.

KMIP permission denied on Locate

Cause: The KeyViewer role lacks Key: List, or the role was not saved.

Resolution: Confirm Key: List and Key: Get Attributes on KeyViewer and the assignment to cbom-sensor-ro.

Connection refused on 5696

Cause: The KMIP service is not running, a firewall blocks 5696, or the sensor IP is not allow-listed.

Resolution: Confirm Services → KMIP is Enabled, check firewall rules, and add the sensor IP to KMIP → Access Control.

Security Recommendations

- Assign cbom-sensor-ro only the KeyViewer role; audit role assignments quarterly.
- Store the mTLS private key at chmod 600, owned by the cbom-agent user; never in version control.
- Rotate the client certificate annually (validity ≤ 12 months) via your PKI tooling.
- Forward gateway audit logs to your SIEM and alert on anything beyond Locate/Get Attributes.
- Restrict port 5696 to the sensor host IP; never expose KMIP to broad subnets or the internet.

Conclusion

With a dedicated read-only service account, an enabled KMIP endpoint, and certificate-based authentication, the Discover_KMIP sensor safely enumerates keys and certificates managed by the Eperi gateway — providing continuous, read-only visibility into the cryptographic posture of Eperi-protected data without exposing key material.