PrimeKey EJBCA Enterprise (KMIP) Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide connects the CBOM Secure Discover_KMIP sensor to a PrimeKey EJBCA Enterprise instance exposing a KMIP 1.2+ interface over TLS on port 5696, read-only:

- Symmetric and asymmetric keys in the KMIP key store
- Key attributes: algorithm, length, state, activation/deactivation dates, UIDs
- Managed objects: certificates, secret data, and opaque objects
- Lifecycle metadata: creation timestamps and cryptographic usage masks

Note: this is the KMIP add-on path; for EJBCA's REST API certificate discovery see the separate EJBCA guide.

Prerequisites

- EJBCA Enterprise 7.4+ with an active KMIP module license.
- Super Administrator or RA Administrator access to the EJBCA Admin web UI.
- An internal CA in EJBCA to sign the client certificate (referenced as Internal-TLS-CA).
- Inbound TCP 5696 permitted from the sensor host; the CA chain (PEM) exported for server verification.
- OpenSSL or keytool available; the Discover_KMIP sensor (2.0+) installed.

Step-by-Step Guide

Step 1: Create an End Entity Profile and Certificate Profile

In the Admin UI → RA Functions → End Entity Profiles, add CBOM_KMIP_Client with CN required, Default CA Internal-TLS-CA, and Token = P12 file (password required). Create a certificate profile CBOM_KMIP_TLS_Client (End Entity type, Key Usages Digital Signature + Key Encipherment, EKU TLS Web Client Authentication, 365d validity).

Step 2: Issue the Client Certificate

Under RA Functions → Add End Entity, create username cbom-kmip-sensor with CN cbom-kmip-sensor using the profiles above and a temporary enrollment password. Enroll via the EJBCA public web (Enroll with username) generating an RSA 2048 (or EC P-256) key, and download cbom-kmip-sensor.p12. Verify and stage it:

```
openssl pkcs12 -in cbom-kmip-sensor.p12 -nokeys -clcerts \
  -passin pass:'Cbom@TmpP12!2025' | openssl x509 -noout -subject -dates
```

```
chmod 640 /etc/cbom/certs/cbom-kmip-sensor.p12
chmod 644 /etc/cbom/certs/internal-tls-ca-chain.pem
chown cbom-service:cbom-service /etc/cbom/certs/cbom-kmip-sensor.p12
```

Step 3: Enable the KMIP Service

Under System Functions → Services, edit the KMIP Service, confirm Active, set the worker interval, Save, and Run. Verify the listener:

```
openssl s_client -connect <ejbca-host>:5696 \
  -cert /etc/cbom/certs/cbom-kmip-sensor.p12 -certform P12 \
  -pass pass:'Cbom@TmpP12!2025' \
  -CAfile /etc/cbom/certs/internal-tls-ca-chain.pem
```

Step 4: Grant KMIP Read Permissions

Under System Functions → Roles and Access Rules, create a role CBOM_KMIP_ReadOnly granting KMIP/Locate, KMIP/Get, and KMIP/GetAttributes, and add a role member matching the client certificate DN CN=cbom-kmip-sensor. Never grant Create, Destroy, Register, or Activate.

Step 5: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_KMIP
    enabled: true
    type: kmip
    schedule: "0 2 * * *"
    connection:
      host: ejbca.internal.example.com
      port: 5696
      tls:
        enabled: true
        client_cert: /etc/cbom/certs/cbom-kmip-sensor.p12
        client_cert_format: pkcs12
        client_cert_password: "${CBOM_EJBCA_P12_PASSWORD}"
        ca_bundle: /etc/cbom/certs/internal-tls-ca-chain.pem
        verify_server_cert: true
    kmip:
      protocol_version: "1.2"
      operations: [Locate, Get, "Get Attributes", "Get Attribute List"]
      object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate, SecretData,
OpaqueObject]
    output:
      format: cbom-json
      label: ejbca-prod-kmip
```

Step 6: Validate

```
cbom-sensor run --sensor Discover_KMIP --config /etc/cbom/sensors/ejbca-kmip.yaml --dry-run
tail -100 /var/log/cbom/discover_kmip.log | grep -E "ERROR|WARN"
```

Confirm a KMIP Locate returns objects and no ERROR lines appear; verify the ejbca-prod-kmip source populates in the CBOM dashboard.

Common Errors

TLS handshake — certificate verify failed

Cause: ca_bundle is incomplete (missing intermediate).

Resolution: Download the full CA chain (CA Functions → Download CA Certificate Chain PEM) and replace the bundle.

KMIP operation not allowed — Permission Denied

Cause: The client DN is not mapped to a role permitting Locate/Get/GetAttributes.

Resolution: Create/verify the CBOM_KMIP_ReadOnly role with a member matching CN=cbom-kmip-sensor.

Connection refused on 5696

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

Resolution: Confirm the service under System Functions → Services, check ss -tlnp | grep 5696, and open the firewall to the sensor host.

Security Recommendations

- Store the P12 password in a secrets manager (the sensor supports vault:// references).
- Restrict the P12 to the cbom-service account at mode 0640.
- Rotate the client certificate annually and update the config.
- Limit the KMIP role to Locate/Get/GetAttributes only.
- Enable EJBCA KMIP audit logging for a tamper-evident query trail.

Conclusion

The Discover_KMIP sensor authenticates to PrimeKey EJBCA over mutual TLS and enumerates all KMIP-managed objects read-only, with an auditable, revocable client identity issued from the internal CA — feeding continuous cryptographic asset discovery into CBOM Secure.