IBM Security Key Lifecycle Manager (SKLM) Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures IBM Security Key Lifecycle Manager (SKLM) so the CBOM Secure Discover_KMIP sensor can enumerate key metadata over KMIP 1.2+ on mutual TLS port 5696, read-only:

- Symmetric and asymmetric key metadata (key ID, algorithm, length, dates, state)
- Managed object types (SecretData, PrivateKey, PublicKey, Certificate)
- Key lifecycle states (Pre-Active, Active, Deactivated, Destroyed)
- Key group and device group associations

Prerequisites

- IBM SKLM 3.0+ with the admin console accessible and the KMIP endpoint licensed.
- Admin credentials for the SKLM Admin GUI.
- Connectivity from the sensor host to TCP 5696.
- The Discover_KMIP sensor installed; OpenSSL on the host; the SKLM keystore password.

Step-by-Step Guide

Step 1: Create a Dedicated KMIPAdmin User

In the SKLM Admin GUI (https://<host>:9443/SKLM/login.jsp), under Access Management → Users → Add User, create cbom-kmip-svc with the KMIPAdmin role. CBOM uses only Locate and Get Attributes, which the role includes. Do not use the built-in SKLMAdmin account.

Step 2: Enable the KMIP Endpoint

Under Administration → Server Configuration → KMIP, enable the service with Port 5696, TLS 1.2+, and Require Client Authentication = Yes; restart the KMIP service. Confirm it is listening:

```
ss -tlnp | grep 5696
```

Step 3: Generate Client and CA Certificates

```
keytool -genkeypair -alias cbom-kmip-client -keyalg RSA -keysize 2048 -validity 730 \
  -keystore /opt/IBM/SKLM/keystore/sklmKeystore.jks -storetype JKS \
  -storepass <keystore-password> -dname "CN=cbom-kmip-client, O=YourOrg, C=US"

keytool -exportcert -alias cbom-kmip-client -rfc \
  -keystore /opt/IBM/SKLM/keystore/sklmKeystore.jks -storepass <keystore-password> \
  -file /tmp/cbom-kmip-client.pem
```

```
keytool -importkeystore -srckeystore /opt/IBM/SKLM/keystore/sklmKeystore.jks \
  -destkeystore /tmp/cbom-kmip-client.p12 -deststoretype PKCS12 \
  -srcalias cbom-kmip-client -srcstorepass <keystore-password> -deststorepass <p12-
password>
openssl pkcs12 -in /tmp/cbom-kmip-client.p12 -nocerts -nodes \
  -passin pass:<p12-password> -out /tmp/cbom-kmip-client-key.pem

keytool -exportcert -alias <sklm-ca-alias> -rfc \
  -keystore /opt/IBM/SKLM/keystore/sklmKeystore.jks -storepass <keystore-password> \
  -file /tmp/sklm-ca.pem
```

Transfer the three PEM files to the sensor host and set permissions (key 600, certs 644). Remove the temporary files from the SKLM server.

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
connection:
  host: sklm-prod.internal.example.com
  port: 5696
  protocol: kmip
  kmip_version: "1.2"
  tls:
    enabled: true
    verify_server_cert: true
    ca_cert: /etc/cbom/certs/sklm-ca.pem
    client_cert: /etc/cbom/certs/cbom-kmip-client.pem
    client_key: /etc/cbom/certs/cbom-kmip-client-key.pem
authentication:
  method: certificate
  username: cbom-kmip-svc
discovery:
  object_types: [SymmetricKey, PrivateKey, PublicKey, Certificate, SecretData]
  max_objects: 50000
output:
  collector_url: https://cbom-collector.internal.example.com:8443/api/v1/ingest
  collector_token_env: CBOM_COLLECTOR_TOKEN
```

Step 5: Validate

```
openssl s_client -connect sklm-prod.internal.example.com:5696 \
  -CAfile /etc/cbom/certs/sklm-ca.pem \
  -cert /etc/cbom/certs/cbom-kmip-client.pem \
  -key /etc/cbom/certs/cbom-kmip-client-key.pem
cbom-sensor run --config /etc/cbom/sensors/ibm-sklm-kmip.yaml --dry-run
```

Confirm a return code 0 handshake and a Locate object count; run live and verify records under the SKLM source label.

Common Errors

TLS handshake — unknown ca

Cause: SKLM does not trust the client cert's CA, or the alias is not in the SKLM truststore.

Resolution: Import the signing CA under SSL Certificates → Signer Certificates and restart the KMIP service.

Permission Denied (Locate)

Cause: cbom-kmip-svc lacks KMIPAdmin, or the KMIP access policy blocks Locate.

Resolution: Confirm the KMIPAdmin role and that the access policy permits Locate and Get Attributes.

Connection refused on 5696

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

Resolution: Confirm ss -tlnp | grep 5696, restart the service, and open TCP 5696 to the sensor host.

Security Recommendations

- Require mutual TLS; never allow unauthenticated or password-only KMIP sessions.
- Rotate the client certificate before its 730-day expiry.
- Restrict cbom-kmip-svc to KMIPAdmin with no GUI admin rights; scope to Locate/Get Attributes.
- Store the client key at mode 600, readable only by the sensor process.
- Enable KMIP audit logging and review the account's operations.

Conclusion

With a scoped KMIPAdmin account, the KMIP endpoint enabled, and mutual TLS certificates deployed, the Discover_KMIP sensor continuously discovers SKLM key metadata in read-only mode — no impact to key lifecycle operations.