Entrust KeyControl Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures Entrust KeyControl as a source for the CBOM Secure Discover_KMIP sensor, which connects over KMIP 1.2+ on TLS port 5696 using mutual certificate authentication and reads key metadata read-only:

- Symmetric keys (AES, 3DES) stored in KeyControl vaults
- Asymmetric key pairs (RSA, EC) in KMIP security domains
- Key attributes: algorithm, length, state, creation/expiration dates, and UIDs
- Certificate objects registered as KMIP managed objects

All operations are strictly read-only KMIP Locate and Get Attributes.

Prerequisites

- Entrust KeyControl 6.2 or later, reachable from the sensor host on TCP 5696.
- KeyControl web console access (https://<host>/vault) with an admin or Security Officer account.
- The Discover_KMIP sensor binary on the sensor host.
- The KeyControl CA certificate available for download, and the sensor host trusts it.
- OpenSSL on the sensor host for certificate verification.
- A KeyControl vault licensed for KMIP (KMIP service enabled under System → Services).

Step-by-Step Guide

Step 1: Create a KMIP-Enabled Vault and Security Domain

In the KeyControl console, under Vaults → Add Vault, create cbom-discovery-vault. Within it, go to Security Domains → Add Security Domain, name it cbom-kmip-domain, set Protocol KMIP and version 1.2+ (1.4 if supported), confirm Mutual TLS (mTLS) is enabled, and Save.

Step 2: Create a Read-Only Service Account

Under Users → Add User, create cbom-sensor-svc with the least-privileged role that allows Locate and Get Attributes (KMIP User or Security Officer Read-Only), assign it to cbom-kmip-domain, and Save. Under Security Domains → cbom-kmip-domain → Users, confirm the assignment.

Step 3: Download the KMIP Client Certificate Bundle

Under Security Domains → cbom-kmip-domain → Certificates (or KMIP Clients), generate a client certificate with CN cbom-sensor-svc and a 365-day validity, then download the bundle (client certificate, private key, and CA certificate). Install on the sensor host:

```
sudo mkdir -p /etc/cbom/sensors/kmip/certs
sudo chmod 700 /etc/cbom/sensors/kmip/certs
sudo cp client_certificate.pem client_key.pem ca_certificate.pem
/etc/cbom/sensors/kmip/certs/
sudo chown -R cbom:cbom /etc/cbom/sensors/kmip/certs
sudo chmod 600 /etc/cbom/sensors/kmip/certs/client_key.pem
```

Confirm the certificate matches the key and the handshake succeeds:

```
openssl x509 -noout -modulus -in /etc/cbom/sensors/kmip/certs/client_certificate.pem |
md5sum
openssl rsa  -noout -modulus -in /etc/cbom/sensors/kmip/certs/client_key.pem        | md5sum


openssl s_client -connect <keycontrol-host>:5696 \
  -CAfile /etc/cbom/sensors/kmip/certs/ca_certificate.pem \
  -cert   /etc/cbom/sensors/kmip/certs/client_certificate.pem \
  -key    /etc/cbom/sensors/kmip/certs/client_key.pem -brief
```

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
  description: "KMIP key discovery from Entrust KeyControl vault"
connection:
  host: keycontrol.example.com
  port: 5696
  protocol: kmip
  kmip_version: "1.2"
tls:
  ca_cert: /etc/cbom/sensors/kmip/certs/ca_certificate.pem
  client_cert: /etc/cbom/sensors/kmip/certs/client_certificate.pem
  client_key: /etc/cbom/sensors/kmip/certs/client_key.pem
  verify_server: true
authentication:
  method: certificate
  username: cbom-sensor-svc        # must match the certificate CN
discovery:
  vault: cbom-discovery-vault
  security_domain: cbom-kmip-domain
  object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate]
schedule:
  interval: 6h
output:
  format: cbom-json
  destination: /var/cbom/output/entrust-keycontrol/
```

Step 5: Validate

```
cbom-sensor run --config /etc/cbom/sensors/entrust-keycontrol.yaml --once
cbom-cli list assets --source entrust-keycontrol --limit 10
```

Confirm a successful KMIP handshake, authentication as cbom-sensor-svc, and a located-object count; verify assets appear with algorithm, length, and state populated.

Common Errors

certificate signed by unknown authority

Cause: ca_certificate.pem does not match the CA that signed the KeyControl server certificate, or the path is wrong.

Resolution: Re-download the CA cert under System → Certificates, verify the path, and re-run the openssl s_client test.

AuthenticationNotSuccessful

Cause: The certificate CN does not match the username, or the user is not assigned to cbom-kmip-domain.

Resolution: Confirm cbom-sensor-svc is in the domain and the CN is exactly cbom-sensor-svc; regenerate the cert if needed.

Connection refused on 5696

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

Resolution: Confirm the KMIP service under System → Services, permit TCP 5696 from the sensor host, and test with nc -zv.

Security Recommendations

- Restrict the certs directory to chmod 700 and the key to 600, owned by the cbom user.
- Rotate the KMIP client certificate annually with a brief overlap to avoid downtime.
- Use a dedicated read-only KMIP role; review the assignment in the audit log.
- Enable KeyControl audit logging and review Locate/Get Attributes calls.
- Isolate the sensor host and permit only outbound TCP 5696 to KeyControl.

Conclusion

With a dedicated vault, a KMIP-enabled security domain, a least-privileged service account, and a client certificate bundle, the Discover_KMIP sensor performs secure, read-only discovery of all KeyControl-managed key metadata — feeding continuous cryptographic-posture visibility into CBOM Secure.