Fornetix VaultCore Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures Fornetix VaultCore 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 and asymmetric key identifiers (UUIDs)
- Key algorithms (AES, RSA, EC), lengths, and curve parameters
- Key creation and activation dates
- Key state (Pre-Active, Active, Deactivated, Destroyed)

No raw key bytes are ever retrieved — metadata only.

Prerequisites

- Admin access to the Fornetix VaultCore web console.
- VaultCore 6.0 or later with KMIP 1.2+ enabled.
- Connectivity from the sensor host to TCP 5696.
- The VaultCore CA certificate (downloadable from the UI).
- The Discover_KMIP sensor binary on the sensor host.
- OpenSSL on the host for certificate verification.

Step-by-Step Guide

Step 1: Create a Read-Only Role and Service Account

Under Administration → Roles → Create Role, create cbom-readonly with only Key Read enabled (allows KMIP Locate and Get Attributes); leave Key Create/Update/Delete/Export and Policy Manage unchecked. Then under Administration → Users → Create User, create cbom-sensor with Authentication Type Certificate and the cbom-readonly role.

Step 2: Enable the KMIP Endpoint

Under Services → KMIP, confirm the service is Enabled on port 5696, set Mutual TLS to Required, and ensure KMIP version 1.2+ is allowed. Verify it is listening:

```
openssl s_client -connect vaultcore.example.com:5696 -brief
```

Step 3: Download the Client Certificate Bundle

Open the cbom-sensor user, click Generate Certificate (365-day validity), and Download Certificate Bundle (client certificate, key, and VaultCore CA). Install and verify:

```
mkdir -p /etc/cbom/certs/vaultcore
mv cbom-sensor.crt cbom-sensor.key vaultcore-ca.crt /etc/cbom/certs/vaultcore/
chmod 600 /etc/cbom/certs/vaultcore/cbom-sensor.key
chmod 644 /etc/cbom/certs/vaultcore/cbom-sensor.crt /etc/cbom/certs/vaultcore/vaultcore-ca.crt

openssl verify -CAfile /etc/cbom/certs/vaultcore/vaultcore-ca.crt \
  /etc/cbom/certs/vaultcore/cbom-sensor.crt
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_KMIP
    enabled: true
    type: kmip
    schedule: "0 2 * * *"
    connection:
      host: vaultcore.example.com
      port: 5696
      kmip_version: "1.2"
      tls:
        enabled: true
        mutual_tls: true
        client_cert: /etc/cbom/certs/vaultcore/cbom-sensor.crt
        client_key: /etc/cbom/certs/vaultcore/cbom-sensor.key
        ca_cert: /etc/cbom/certs/vaultcore/vaultcore-ca.crt
        verify_server: true
    authentication:
      type: certificate
      username: cbom-sensor
    discovery:
      object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate]
      locate_batch_size: 100
      max_objects: 50000
    output:
      tags: { source: fornetix-vaultcore, environment: production }
sudo systemctl reload cbom-sensor
```

Step 5: Validate

```
cbom-sensor run --sensor Discover_KMIP --once --verbose
cbom-sensor list --sensor Discover_KMIP
```

Confirm a KMIP connection, authentication as cbom-sensor, and a located-object count. In the VaultCore audit log filtered by cbom-sensor, only Locate and Get Attributes should appear.

Common Errors

certificate verify failed

Cause: ca_cert points to the wrong file, or the VaultCore CA was not downloaded correctly.

Resolution: Re-download vaultcore-ca.crt (Administration → Certificates → CA Certificate), confirm PEM format, and re-verify with openssl.

Permission denied (Locate rejected)

Cause: cbom-sensor lacks Key Read, or the cbom-readonly role was not saved.

Resolution: Confirm Key Read on cbom-readonly and the role assignment on cbom-sensor, then retry.

Connection refused on 5696

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

Resolution: Confirm Services → KMIP is Enabled on 5696, permit inbound TCP 5696 from the sensor host, and test with nc -zv.

Security Recommendations

- Store cbom-sensor.key at chmod 600, owned by the CBOM service account only.
- Rotate the client certificate annually, or immediately on suspected compromise.
- Place the sensor on a management network with a direct allow-list rule to port 5696.
- Review the VaultCore audit log for the cbom-sensor identity monthly.
- Keep cbom-readonly limited to Key Read; create a new role for any future needs.

Conclusion

With a read-only service account, an mTLS-enabled KMIP endpoint, and client certificates, the Discover_KMIP sensor provides continuous, read-only visibility into all VaultCore-managed key metadata — keeping CBOM Secure's inventory of algorithms, lengths, and lifecycle states current without exposing raw key material.