Fortanix Data Security Manager (DSM) Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures Fortanix Data Security Manager (DSM) so the CBOM Secure Discover_KMIP sensor can discover cryptographic assets over KMIP 1.2+ on mutual TLS port 5696, read-only:

- Symmetric and asymmetric managed cryptographic objects (keys)
- Certificates stored within DSM security objects
- Security-object metadata: algorithm, key length, state, lifecycle dates
- Group and application associations for discovered objects

Prerequisites

- An active Fortanix DSM account with Account or Group Administrator privileges.
- The DSM instance (SaaS or on-prem) reachable on port 5696 from the sensor host.
- The Discover_KMIP sensor binary installed and configured to run.
- Access to the DSM web console (e.g. https://<account>.smartkey.io for SaaS).
- OpenSSL on the sensor host for certificate verification.
- The KMIP endpoint licensed on your DSM subscription tier.

Step-by-Step Guide

Step 1: Create a Dedicated Group

In the DSM console, under Groups → + Add Group, create CBOM-KMIP-ReadOnly with a description, leaving cryptographic policy at defaults. Note the Group UUID for audit records.

Step 2: Create an App with KMIP Access

Under Apps → + Add App, create CBOM-Sensor with Interface KMIP, assign it to CBOM-KMIP-ReadOnly, and set the group permission to Read only (no Create, Export, Delete, or Manage). Save.

Step 3: Generate the API Key

Open the App detail page → Credentials → Add API Key, label it cbom-sensor-key, and Generate. Copy the key immediately (shown once) and store it in a secrets manager.

Step 4: Enable the KMIP Endpoint and Download the CA

Under Settings → Account Settings → Integrations/Endpoints, toggle KMIP to Enabled and confirm port 5696. Under the TLS / CA Certificate section, Download CA Certificate to the sensor host:

```
openssl s_client -connect <dsm-hostname>:5696 -showcerts   # confirm handshake
```

```
chmod 640 /etc/cbom/certs/fortanix-dsm-ca.pem
chown cbom-service:cbom-service /etc/cbom/certs/fortanix-dsm-ca.pem
```

Step 5: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
  description: "Fortanix DSM KMIP sensor"
connection:
  protocol: kmip
  version: "1.2"
  host: "<your-account>.smartkey.io"
  port: 5696
  tls:
    enabled: true
    ca_cert: "/etc/cbom/certs/fortanix-dsm-ca.pem"
    verify_server_cert: true
authentication:
  type: api_key
  api_key: "${CBOM_FORTANIX_API_KEY}"
discovery:
  groups: ["CBOM-KMIP-ReadOnly"]
  object_types: [SymmetricKey, PrivateKey, PublicKey, Certificate, SecretData]
  fetch_key_material: false        # never retrieve raw key bytes
  batch_size: 100
output:
  format: cbom_json
  destination: "/var/cbom/output/fortanix-dsm-discovery.json"
schedule:
  cron: "0 */6 * * *"
export CBOM_FORTANIX_API_KEY="<paste-api-key>"
```

Step 6: Validate

```
systemctl start cbom-discover-kmip
tail -f /var/log/cbom/fortanix-kmip-sensor.log
```

Confirm a TLS handshake, KMIP authentication as App CBOM-Sensor, and an objects-found count. In the DSM console, Apps → CBOM-Sensor → Activity should show only Locate and GetAttributes (no Get / key-material retrieval).

Common Errors

certificate verify failed

Cause: The CA certificate path is wrong/missing, or the cert does not match the DSM issuer chain.

Resolution: Verify the path, re-download the CA from DSM Settings, and confirm PEM format with openssl x509 -noout -subject.

AuthenticationNotSuccessful

Cause: The API key is invalid/expired, or the App is not assigned to the expected group.

Resolution: Confirm the key under Apps → CBOM-Sensor → Credentials (regenerate if needed) and the group assignment.

ECONNREFUSED on 5696

Cause: The KMIP endpoint is not enabled, or a firewall blocks 5696.

Resolution: Enable KMIP under Account Settings → Integrations, allow TCP 5696 from the sensor host, and (on-prem) confirm the local firewall.

Security Recommendations

- Assign the CBOM App only to CBOM-KMIP-ReadOnly; never to groups holding unrelated production keys.
- Keep fetch_key_material: false so the sensor uses only Locate and GetAttributes.
- Rotate the App API key at least every 90 days; automate via your secrets manager.
- Restrict TCP 5696 to the sensor host IP at the network perimeter.
- Review the CBOM-Sensor Activity log for any unexpected Get/Destroy/Create operations.

Conclusion

With a dedicated group, a KMIP App, an enabled endpoint, and the DSM CA certificate, the Discover_KMIP sensor maintains a current, read-only inventory of all cryptographic objects in Fortanix DSM without exposing key material — backed by least-privilege group membership and regular activity-log review.