Crypto4A QxEDGE Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures a Crypto4A QxEDGE appliance so the CBOM Secure Discover_KMIP sensor can connect as a read-only KMIP client over mutual TLS on port 5696 and enumerate cryptographic metadata:

- Symmetric keys (AES, 3DES) with key length, algorithm, and activation/deactivation dates
- Asymmetric key pairs (RSA, EC) and public-key metadata
- Certificates in the KMIP object store
- Secret data and opaque data objects
- Key state (Pre-Active, Active, Deactivated, Compromised, Destroyed) and usage masks

No key material is ever retrieved — only metadata attributes are read.

Prerequisites

- A provisioned, powered-on QxEDGE appliance reachable on the network.
- Administrator access to the QxAdmin web interface (default HTTPS port 8443).
- QxEDGE firmware 3.2 or later (KMIP 1.2 support).
- The KMIP service enabled and listening on TCP 5696.
- Connectivity from the sensor host to port 5696, and OpenSSL 1.1.1+ on the host.
- The QxEDGE root CA certificate available from QxAdmin, and the Discover_KMIP sensor binary installed.

Step-by-Step Guide

Step 1: Verify KMIP Service and Export the Root CA

In QxAdmin (https://<appliance-ip>:8443), under Services → KMIP, confirm status Running, port 5696, KMIP 1.2+, and Mutual TLS (mTLS) enabled. Then under PKI → Certificate Authorities, export QxEDGE Root CA as PEM:

```
chmod 640 /etc/cbom/certs/qxedge-root-ca.pem
chown cbom-svc:cbom-svc /etc/cbom/certs/qxedge-root-ca.pem
openssl x509 -in /etc/cbom/certs/qxedge-root-ca.pem -noout -subject -dates
```

Step 2: Create a CryptoAuditor Role

Under Access Control → Roles → Add Role, create CryptoAuditor with only these KMIP operations enabled: Locate, Get Attributes, Get Attribute List, and Query. Ensure all write/destructive operations (Create, Register, Destroy, Activate, Revoke, Archive, Recover) are unchecked, and Save Role.

Step 3: Create the KMIP Service User

Under Access Control → Users → Add User, set Username cbom-auditor, Role CryptoAuditor, and Authentication Method Certificate, then Save.

Step 4: Generate and Export the Client Certificate

Select cbom-auditor → Generate Client Certificate with CN cbom-auditor, O CBOM-Services, RSA 2048 (or EC P-256), 365-day validity. Export the certificate and private key as PEM, transfer to the sensor host, and set permissions:

```
scp cbom-auditor-cert.pem cbom-auditor-key.pem \
    cbom-user@<sensor-host>:/etc/cbom/certs/

chmod 640 /etc/cbom/certs/cbom-auditor-cert.pem
chmod 600 /etc/cbom/certs/cbom-auditor-key.pem
chown cbom-svc:cbom-svc /etc/cbom/certs/cbom-auditor-cert.pem
chown cbom-svc:cbom-svc /etc/cbom/certs/cbom-auditor-key.pem
```

Step 5: Verify mTLS Connectivity

```
nc -zv <qxedge-appliance-ip> 5696

openssl s_client \
  -connect <qxedge-appliance-ip>:5696 \
  -cert /etc/cbom/certs/cbom-auditor-cert.pem \
  -key /etc/cbom/certs/cbom-auditor-key.pem \
  -CAfile /etc/cbom/certs/qxedge-root-ca.pem \
  -verify_return_error
# Expected: Verify return code: 0 (ok)
```

Step 6: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
  schedule: "0 2 * * *"          # daily at 02:00 UTC
connection:
  protocol: KMIP
  kmip_version: "1.2"
  host: 192.168.10.45            # QxEDGE IP or FQDN
  port: 5696
  tls:
    enabled: true
    mutual_tls: true
    ca_cert: /etc/cbom/certs/qxedge-root-ca.pem
    client_cert: /etc/cbom/certs/cbom-auditor-cert.pem
    client_key: /etc/cbom/certs/cbom-auditor-key.pem
    verify_hostname: true
    min_tls_version: "TLSv1.2"
discovery:
  object_types: [SymmetricKey, PublicKey, PrivateKey, Certificate, SecretData, OpaqueData]
  locate_batch_size: 100
  max_objects: 50000
output:
  cbom_endpoint: https://cbom-platform.internal:8443/api/v1/ingest
  api_key_env: CBOM_API_KEY
  tags: { source: Crypto4A-QxEDGE, environment: production }
```

```
export CBOM_API_KEY="<your-cbom-platform-api-key>"
```

Step 7: Validate

```
cbom-sensor run --sensor Discover_KMIP --dry-run --config
/etc/cbom/sensors/discover_kmip.yaml
cbom-sensor run --sensor Discover_KMIP --config /etc/cbom/sensors/discover_kmip.yaml
```

Confirm KMIP connection established … (KMIP 1.2, mTLS verified) and a discovered-object count. Cross-reference against QxAdmin → KMIP → Object Store → Statistics, and confirm the audit log shows only Locate, Get Attributes, Get Attribute List, and Query for cbom-auditor.

Common Errors

TLS handshake failure — certificate verify failed

Cause: ca_cert is incorrect or incomplete (e.g. an intermediate CA is missing).

Resolution: Export the full chain (Root + intermediates) as one bundled PEM from PKI → Certificate Authorities and replace the file.

KMIP permission denied on Locate

Cause: The CryptoAuditor role is missing Locate, or the role was not saved.

Resolution: Confirm Locate, Get Attributes, Get Attribute List, and Query are checked on the role, Save, and retry.

Connection refused on 5696

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

Resolution: Confirm the service is Running, test with nc -zv, and permit TCP 5696 in both directions.

Security Recommendations

- Limit client certificate validity to 365 days or less and rotate annually.
- Store the private key with mode 600, readable only by the sensor account; never commit it.
- Enforce TLS 1.2 minimum and reject TLS 1.0/1.1 on the appliance.
- Review the QxAdmin audit log for any operation beyond the four read operations.
- Use KMIP client IP allowlisting (sensor host only) where supported.

Conclusion

With a least-privilege CryptoAuditor user and a mutual-TLS client certificate, the Discover_KMIP sensor securely enumerates cryptographic key metadata over KMIP 1.2 on the QxEDGE appliance — collecting only attribute information, never key material — keeping CBOM Secure's inventory current.