Encryption Consulting CertSecure Manager Setup

CBOM Secure · PKI Sensor (Discover_PKI)

Overview

This guide configures the CBOM Secure Discover_PKI sensor to integrate with Encryption Consulting CertSecure Manager via its REST API in read-only mode, cataloging certificate assets across your PKI. The sensor collects:

- Subject DN and Subject Alternative Names (DNS, IP, email)
- Validity period (notBefore / notAfter)
- Issuer DN (issuing CA)
- Key algorithm (RSA, ECDSA, etc.) and key size

No private keys or secret material are accessed; all API calls are read-only and scoped to the certificate inventory endpoint.

Prerequisites

- CertSecure Manager admin access with the Super Admin or User Administrator role.
- CertSecure Manager 4.2.0 or later (REST API v1).
- Connectivity from the sensor host to the CertSecure API on port 443 (HTTPS).
- The CBOM sensor agent installed and running.
- A valid TLS certificate on CertSecure, or its internal CA certificate available for trust.
- Outbound HTTPS allowed from the sensor host to the CertSecure FQDN.

Step-by-Step Guide

Step 1: Create a CertAuditor Service Account

In the CertSecure admin console (https://<host>/admin), go to Admin → Users & Roles → Add User and create cbom-certsecure-svc with Role CertAuditor, Account Type Service Account, Status Active. Uncheck Require password change on first login, then Save. The CertAuditor role grants read-only visibility into the certificate inventory.

Step 2: Generate an API Key

Go to Admin → API Keys → Generate Key, select cbom-certsecure-svc, add a description (e.g. "CBOM PKI Sensor - Read-Only Access"), optionally set an expiry, and Generate. Copy the key immediately (shown once) and store it in a secrets manager. CertSecure authenticates API requests via the X-API-Key header.

Step 3: Verify API Access

```
curl -s -o /dev/null -w "%{http_code}" \
  -H "X-API-Key: <api-key>" \
  "https://<certsecure-host>/api/v1/certificates?limit=1"
# Expected: 200
```

Inspect a sample response and confirm fields such as subject, sans, notBefore, notAfter, issuer, keyAlgorithm, and keySize are present:

```
curl -s -H "X-API-Key: <api-key>" \
  "https://<certsecure-host>/api/v1/certificates?limit=1" | python3 -m json.tool
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_PKI
    type: pki
    enabled: true
    schedule: "0 2 * * *"           # daily at 02:00 UTC
    source:
      provider: certsecure_manager
      endpoint: "https://certsecure-manager.internal.example.com"
      api_version: v1
      tls:
        verify: true
        ca_bundle: "/etc/cbom/certs/certsecure-ca.pem"  # remove if public CA
    auth:
      method: api_key
      header: X-API-Key
      secret_ref: "cbom/certsecure/api-key"             # path in secrets manager
    discovery:
      include_expired: false
      include_revoked: false
      page_size: 500
    filters:
      - field: status
        operator: in
        values: [ACTIVE, EXPIRING_SOON]
    output:
      format: cbom_json
      destination: cbom-collector
      collector_endpoint: "https://cbom-collector.internal.example.com:8443"
    tags: { environment: production, sensor_owner: security-team }
sudo systemctl reload cbom-sensor
sudo systemctl status cbom-sensor
```

Step 5: Validate

```
sudo journalctl -u cbom-sensor -n 50 --no-pager | grep Discover_PKI
cbom-ctl sensor run --name Discover_PKI
cbom-ctl sensor status --name Discover_PKI --last-run
```

Confirm a SUCCESS status with a certificate count, then check Assets → Certificates in the CBOM dashboard for entries tagged sensor_owner: security-team with subject, SANs, validity, issuer, key algorithm, and key size populated.

Common Errors

401 Unauthorized

Cause: The API key is incorrect, expired, or was regenerated after configuration.

Resolution: Verify the key under Admin → API Keys is tied to cbom-certsecure-svc; update the secret at secret_ref and reload the sensor.

TLS certificate verify failed

Cause: CertSecure uses an internal CA not trusted by the sensor host.

Resolution: Export the internal CA to /etc/cbom/certs/certsecure-ca.pem, confirm tls.ca_bundle points to it, and reload.

403 Forbidden — insufficient permissions

Cause: The service account is not assigned the CertAuditor role.

Resolution: Under Users & Roles, set cbom-certsecure-svc to CertAuditor, Save, and re-run the sensor.

Security Recommendations

- Store the API key in a secrets manager and reference via secret_ref — never plaintext.
- Rotate the API key at least every 90 days, and immediately when access changes.
- Restrict network access so only the sensor host IP can reach the CertSecure API on 443.
- Always set tls.verify: true; provide ca_bundle for internal CAs rather than disabling.
- Audit the API key Last Used timestamp and revoke on unexpected usage.

Conclusion

With a dedicated CertAuditor service account and a scoped API key, the Discover_PKI sensor obtains read-only access to the full CertSecure Manager certificate inventory — continuously feeding subject, SANs, validity, issuer, algorithm, and key-size metadata into CBOM Secure for accurate cryptographic asset tracking and compliance reporting.