Keyfactor Command Setup

CBOM Secure · PKI Sensor (Discover_PKI)

Overview

The CBOM Secure Discover_PKI sensor integrates with Keyfactor Command via its REST API (/KeyfactorAPI/Certificates) in read-only mode, collecting certificate metadata: Subject DN and SANs, validity period, Issuer DN, certificate template, issuing CA, key algorithm and size, and serial number / thumbprint.

Prerequisites

- Keyfactor Command web portal access with an Administrator account.
- Keyfactor Command 10.x+ with the REST API enabled.
- HTTPS connectivity from the sensor host to the API (port 443).
- A valid TLS cert on the Keyfactor server, or its CA trusted by the sensor.
- The Keyfactor base URL and the Discover_PKI sensor installed.

Step-by-Step Guide

Step 1: Create a Service Account

In Admin → Security → Users, add cbom-sensor-svc (local or AD). Under Roles, add it to the Certificate Read role (read-only GET on the Certificates endpoint). Do not assign Administrator, CA Administrator, or Enrollment roles.

Step 2: Generate API Credentials

Use an API key (on-premises) under Admin → API Keys → Add, associated with cbom-sensor-svc, with a 90/365-day expiry — or OAuth2 client credentials (cloud) with a client_credentials grant and KeyfactorAPI:Read scope. Store the secret in a secrets manager.

Step 3: Verify API Access

Keyfactor requires the x-keyfactor-requested-with: APIClient header on all API calls — omitting it returns 401 even with valid credentials.

```
# OAuth2 token, then query Certificates
TOKEN=$(curl -s -X POST "https://keyfactor.example.com/connect/token" \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -d "grant_type=client_credentials&client_id=cbom-discover-
pki&client_secret=<SECRET>&scope=KeyfactorAPI" \
  | python3 -c "import sys,json; print(json.load(sys.stdin)['access_token'])")

curl -s "https://keyfactor.example.com/KeyfactorAPI/Certificates?
pageReturned=1&returnLimit=5" \
  -H "Accept: application/json" \
```

```
  -H "x-keyfactor-requested-with: APIClient" \
  -H "Authorization: Bearer $TOKEN" | python3 -m json.tool
```

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_PKI
  vendor: Keyfactor
  enabled: true
  schedule: "0 2 * * *"
connection:
  base_url: "https://keyfactor.example.com"
  api_version: "v1"
  verify_ssl: true
  ca_bundle: "/etc/ssl/certs/internal-root-ca.pem"
auth:
  method: "oauth2_client_credentials"   # or "basic" / "api_key"
  token_endpoint: "https://keyfactor.example.com/connect/token"
  client_id: "cbom-discover-pki"
  client_secret: "${KEYFACTOR_CLIENT_SECRET}"
  scope: "KeyfactorAPI"
discovery:
  endpoint: "/KeyfactorAPI/Certificates"
  page_size: 100
  include_expired: true
  include_revoked: false
output:
  format: "cbom-json"
  destination: "/var/cbom/output/keyfactor_pki_discovery.json"
```

Step 5: Validate

```
export KEYFACTOR_CLIENT_SECRET="your-client-secret"
cbom-sensor run --config /path/to/keyfactor_pki.yaml --dry-run
cbom-sensor enable Discover_PKI
```

Confirm successful authentication, paginated retrieval, and a total certificate count, then enable the scheduled job.

Common Errors

401 Unauthorized on all requests

Cause: Wrong/expired credentials, or the missing x-keyfactor-requested-with header.

Resolution: Verify the secret, check key expiry, and ensure the header is sent on every request.

403 Forbidden on Certificates

Cause: cbom-sensor-svc lacks the CertificateRead permission, or role membership has not propagated.

Resolution: Confirm membership in the Certificate Read role and the Effective Permissions; re-run after caching expires.

SSL CERTIFICATE_VERIFY_FAILED

Cause: The Keyfactor server uses an internal CA not trusted by the sensor host.

Resolution: Set ca_bundle to the root CA PEM; never set verify_ssl: false in production.

Security Recommendations

- Prefer OAuth2 client credentials (short-lived tokens) over Basic Auth.
- Rotate API keys / client secrets every 90 days via your secrets manager.
- Restrict the account to the Certificate Read role — never enrollment, revocation, or admin.
- Store secrets in a secrets manager and inject via env vars — never plaintext YAML.
- Enable Keyfactor audit logging and confirm only GET operations occur.

Conclusion

With a read-only Certificate Read service account and secure API credentials, the Discover_PKI sensor maintains a continuously updated inventory of Keyfactor-managed certificate metadata — subject, SAN, validity, issuer, template, and CA — feeding CBOM Secure.