Atos Trustway KMS Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures Atos Trustway Key Management Server (KMS) so the CBOM Secure Discover_KMIP sensor can discover cryptographic assets via KMIP 1.2+ over TLS on port 5696. The sensor performs read-only enumeration of:

- Symmetric keys (AES, 3DES) with key length, dates, and state
- Asymmetric key pairs (RSA, EC) and associated attributes
- X.509 certificates in the KMS object store
- Secret and opaque managed objects
- Key lifecycle state and cryptographic usage-mask attributes

The sensor connects read-only and never modifies, creates, or deletes key material.

Prerequisites

- Atos Trustway KMS / Proteccio NetHSM with KMIP 1.2+ enabled (verify under System → About).
- Administrator or Security Officer role in the Trustway Administration Console.
- Network access from the sensor host to TCP port 5696 (verify with nc -zv <host> 5696).
- A configured TLS server certificate on the KMS and its CA chain.
- Mutual TLS (mTLS) supported and enabled on the KMIP interface; the internal CA accessible under PKI → Internal CA.
- The Discover_KMIP sensor binary or container image installed on the scanning host.

Step-by-Step Guide

Step 1: Create a Read-Only Key Auditor Account

Log in to the Trustway Administration Console (https://<host>:8443/admin). Under User Management → Users → Add User, create cbom-kmip-auditor with role Key Auditor and Certificate-Based Authentication (mTLS), then Save.

Step 2: Issue a Client Certificate

- Go to PKI → Client Certificates → Issue Certificate and select cbom-kmip-auditor.
- Set the validity period per policy (recommended 1 year) and click Generate.
- Download the PEM bundle: the client certificate, the private key, and the Trustway CA chain.

```
chmod 600 cbom-kmip-auditor.key
chmod 644 cbom-kmip-auditor.crt trustway-ca-chain.pem
```

Step 3: Enable and Verify the KMIP Interface

Under Services → KMIP Interface, ensure the service is enabled with: Protocol KMIP 1.2+, Port 5696, TLS 1.2 minimum, Client Authentication Required (mTLS), Status Running. Download the server CA under PKI → Internal CA as trustway-server-ca.pem. Then verify the mTLS handshake from the sensor host:

```
openssl s_client -connect <trustway-kms-host>:5696 \
  -cert cbom-kmip-auditor.crt \
  -key cbom-kmip-auditor.key \
  -CAfile trustway-server-ca.pem
# Expected: Verify return code: 0 (ok)
```

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
  description: "Read-only KMIP discovery against Atos Trustway KMS"
connection:
  host: trustway-kms.example.internal
  port: 5696
  protocol: KMIP
  kmip_version: "1.2"
  tls:
    enabled: true
    min_version: TLS1_2
    ca_cert: /etc/cbom/certs/trustway-server-ca.pem
    client_cert: /etc/cbom/certs/cbom-kmip-auditor.crt
    client_key: /etc/cbom/certs/cbom-kmip-auditor.key
    verify_hostname: true
discovery:
  scope: ALL_OBJECTS
  object_types: [SYMMETRIC_KEY, ASYMMETRIC_KEY, CERTIFICATE, SECRET_DATA,
OPAQUE_DATA]
  attributes_to_collect: [Name, Cryptographic_Algorithm, Cryptographic_Length,
    State, Initial_Date, Activation_Date, Deactivation_Date, Compromise_Date,
    Destroy_Date, Cryptographic_Usage_Mask, Link, Last_Change_Date]
credentials:
  auth_method: certificate
  username: cbom-kmip-auditor
output:
  format: cbom_json
  platform_endpoint: https://cbom-platform.example.internal/api/v1/ingest
  api_key_env: CBOM_PLATFORM_API_KEY
  tags: { vendor: atos, system: trustway-kms, environment: production }
scheduling:
  interval_minutes: 60
export CBOM_PLATFORM_API_KEY="your-cbom-platform-api-key"
cbom-sensor start --config /etc/cbom/sensors/discover-kmip-trustway.yaml
```

Step 5: Validate

```
cbom-sensor status --config /etc/cbom/sensors/discover-kmip-trustway.yaml
tail -n 100 /var/log/cbom/discover-kmip-trustway.log
```

Confirm a successful TLS handshake and object enumeration (e.g. Discovery complete. Total objects: 347). In the Trustway audit log, all operations for cbom-kmip-auditor should be Locate and Get Attribute only.

Common Errors

TLS handshake failure — certificate unknown

Cause: The client certificate is not correctly associated with the account, or it does not match the CA the KMIP interface trusts.

Resolution: Under PKI → Client Certificates, confirm the certificate for cbom-kmip-auditor matches the .crt used in the config; re-issue if needed.

KMIP operation denied — permission denied

Cause: The account has a role other than Key Auditor, or a KMIP ACL blocks Locate / Get Attributes.

Resolution: Confirm the Key Auditor role; add an explicit allow rule for Locate and Get Attribute under Policies → KMIP Access Control.

Connection refused / timeout on 5696

Cause: The KMIP interface is not running, the port is firewalled, or DNS resolves incorrectly.

Resolution: Confirm KMIP Interface status is Running, test with nc -zv …:5696, and verify DNS resolution.

Security Recommendations

- Restrict the Key Auditor account to the sensor host IP via Network Restrictions.
- Rotate the client certificate at least annually and update the config before expiry.
- Store the private key with chmod 600 (or inject from a secrets manager).
- Enable KMIP audit logging (90-day retention) and confirm only Locate / Get Attribute operations.
- Use TLS 1.2+ with forward-secrecy cipher suites; disable TLS 1.0/1.1.

Conclusion

Using a dedicated Key Auditor account with certificate-based authentication, the Discover_KMIP sensor gains read-only visibility into all Trustway KMS object metadata over mutual TLS — without any risk of modifying key material — and continuously populates CBOM Secure for risk assessment and compliance reporting.