Securosys Primus HSM Setup

CBOM Secure · HSM Sensor (PKCS#11)

Overview

This guide configures a Securosys Primus HSM so the CBOM Secure HSM Sensor can discover cryptographic assets over PKCS#11, read-only:

- Symmetric keys (AES, DES, 3DES)
- Asymmetric key pairs (RSA, EC, Ed25519)
- X.509 certificates
- Secret and data objects in HSM partitions

Prerequisites

- A Securosys Primus HSM (E/S/X-Series), initialized and reachable.
- Security Officer or Administrator credentials for the Primus Management Console (PMC).
- The Primus HSM Client installed on the sensor host, with libprimusP11.so at /usr/local/lib/.
- Network access to the HSM (default TCP 2310); firmware 2.8.0+; a populated primus.cfg.

Step-by-Step Guide

Step 1: Create a Dedicated Partition

In the PMC (https://primus-hsm.example.com:2443) → HSM → Partitions → New Partition, create cbom-discovery with PKCS#11 access enabled and key export disabled. CLI alternative:

```
primusctl partition create \
  --name cbom-discovery \
  --label "CBOM Read-Only Partition" \
  --pkcs11 enabled --key-export disabled
```

Step 2: Create the Partition Security Officer (PSO)

```
primusctl user create \
  --partition cbom-discovery --username cbom-pso --role pso \
  --password "$(openssl rand -base64 24)"
```

Note Store the PSO credential in a vault — the CBOM sensor never uses it. It is only required to create the Crypto User.

Step 3: Create a Read-Only Crypto User

```
primusctl user create \
  --partition cbom-discovery --username cbom-sensor --role crypto-user \
  --password "Cbom-Sensor-Primus-Pw"

primusctl user set-permissions \
```

```
 --partition cbom-discovery --username cbom-sensor \
 --allow find-objects,get-attributes \
 --deny generate,sign,verify,encrypt,decrypt,destroy
```

Step 4: Confirm Slot and Library

```
pkcs11-tool --module /usr/local/lib/libprimusP11.so --list-slots
ls -lh /usr/local/lib/libprimusP11.so
pkcs11-tool --module /usr/local/lib/libprimusP11.so --slot 0 \
 --login --login-type user --pin "Cbom-Sensor-Primus-Pw" --list-objects
```

Confirm the sensor host is listed under HSM → Network → Authorized Clients, and that primus.cfg references the HSM device.

Step 5: Configure the CBOM Secure Sensor

```
sensors:
 - name: Discover_HSM
   type: hsm_pkcs11
   enabled: true
   connection:
     pkcs11_library: /usr/local/lib/libprimusP11.so
     slot: 0
     token_label: CBOM Read-Only Partition
   authentication:
     login_type: user
     username: cbom-sensor
     pin: "${PRIMUS_CBOM_PIN}"
   discovery:
     object_types: [symmetric_keys, asymmetric_keys, certificates, secret_data]
     include_sensitive_attributes: false
   schedule:
     interval: 6h
   tags: { hsm_vendor: securosys, hsm_model: primus }
export PRIMUS_CBOM_PIN="Cbom-Sensor-Primus-Pw"
```

Step 6: Validate

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

Confirm the library loads, the slot connects, Crypto User login succeeds, and objects are enumerated; run live and verify under Assets → HSM.

Common Errors

CKR_PIN_INCORRECT

Cause: The PIN in the config/variable doesn't match the Crypto User password.

Resolution: Reset the cbom-sensor password in the PMC and update PRIMUS_CBOM_PIN.

CKR_SLOT_ID_INVALID

Cause: The slot index doesn't match the cbom-discovery partition (e.g. after a firmware upgrade).

Resolution: Re-run --list-slots and update slot, or use token_label matching.

Cannot open shared object file

Cause: The Primus client is not installed or the library is at a non-standard path.

Resolution: Install the Primus client; locate libprimusP11.so and update pkcs11_library.

Security Recommendations

- Restrict the Crypto User to C_FindObjects and C_GetAttributeValue; disable all generate/sign/encrypt/destroy mechanisms.
- Never configure the sensor with the PSO credential.
- Store the Crypto User PIN in a secrets manager and rotate every 90 days.
- Whitelist only the sensor host under HSM → Network → Authorized Clients.
- Use TLS in primus.cfg with a pinned CA; enable and review the Primus audit log.

Conclusion

The cbom-sensor Crypto User can enumerate all key, certificate, and data objects in the cbom-discovery partition read-only — with no ability to create, modify, export, or delete material — surfacing Securosys Primus assets in CBOM Secure.