LDAP Integration Guide

CBOM Secure · LDAP Discovery Sensor

Overview

This guide describes how to configure the CBOM Secure LDAP Discovery Sensor to discover certificates and keys held in a directory server over LDAP / LDAPS (ports 389 / 636). It works with OpenLDAP, FreeIPA / 389-Directory, and other standards-based directories, and supports scanning user-declared custom attributes.

The sensor discovers:

Discovered material	Source
Server TLS certificate	The LDAPS server's own certificate (TLS handshake)
User & CA certificates	userCertificate, cACertificate
S/MIME certificates	userSMIMECertificate (PKCS#7 bundles)
Cross-certificate pairs	crossCertificatePair
PKCS#12 bundles	userPKCS12 (passwords supplied in config)
SSH public keys	altSecurityIdentities, sshPublicKey, ipaSshPubKey
Custom attributes	Any user-declared attribute (format auto-detected)

Prerequisites

- An LDAP / LDAPS server reachable from the sensor host on port 389 or 636.
- A bind account (full bind DN and password) with read access to the entries to be scanned — or anonymous bind if the directory permits it.
- For LDAPS with verification enabled: the issuing CA certificate available to the sensor (via the OS trust store or a PEM file). Self-signed lab servers may instead disable verification.
- Passwords for any PKCS#12 bundles you want the sensor to open.
- The CBOM Secure LDAP Discovery Sensor package ready for configuration.

Step-by-Step Guide

Step 1: Confirm Connectivity and Port

Confirm the sensor host can reach the directory. If you set port to 0, the sensor auto-detects the transport in the order LDAPS/636 → StartTLS/389 → plain/389.

Step 2: Identify a Read-Only Bind Account

Use a dedicated service account with read access, expressed as a full bind DN — for example, CN=svc-ldap,OU=ServiceAccounts,DC=corp,DC=example,DC=com. Anonymous bind may be used where the directory allows it.

Step 3: Determine the Base DN

Set base_dn to the search root (for example, DC=corp,DC=example,DC=com). Leave it empty to auto-discover the naming contexts from the server's Root DSE.

Step 4: Configure TLS Verification

For production directories, keep verify_ssl: true. For an internal or self-signed CA, set ca_cert_path to the PEM CA certificate rather than disabling verification. Use verify_ssl: false only in throwaway lab environments.

Step 5: Prepare the Minimal Configuration

```
ExtName: Discover_LDAP
host: ldap.corp.example.com
port: 636
use_ssl: true
verify_ssl: true
auth_method: simple
username: "CN=svc-ldap,OU=ServiceAccounts,DC=corp,DC=example,DC=com"
password: "s3cr3t!"
base_dn: "DC=corp,DC=example,DC=com"
```

Step 6: (Optional) PKCS#12 Passwords, Custom Attributes, Page Size

Add passwords for encrypted bundles, declare custom attributes to scan, and tune the page size for slow or throttled servers. Raw symmetric keys in a custom attribute require a type: secret_key hint.

```
ca_cert_path: /etc/ssl/certs/internal-ca.pem   # pin internal CA
page_size: 500                                 # reduce if the server throttles

pkcs12_passwords:
 - "changeit"
 - "export123"
 - ""

custom_attributes:
 - name: pgpKey
 - name: myAESKey
   type: secret_key       # hint required for raw symmetric bytes
   algorithm: AES
   key_size: "256"

custom_protected_attributes:
 - name: companyPKCS12
   passwords:
    - "export123"
    - ""
```

Step 7: (Optional) Scan Multiple Hosts

```
ExtName: Discover_LDAP
```

```
username: "cn=admin,dc=corp,dc=example,dc=com"
password: "s3cr3t!"
auth_method: simple
page_size: 1000

hosts:
  - host: ldap1.corp.example.com
    port: 636
    use_ssl: true
    base_dn: "dc=corp,dc=example,dc=com"
  - host: ldap2.corp.example.com
    port: 636
    use_ssl: true
    base_dn: "dc=eu,dc=corp,dc=example,dc=com"
```

Step 8: Run Discovery

Run the LDAP discovery task from CBOM Secure. The sensor scans the server TLS certificate once, then enumerates stored certificates, SSH keys, and any configured custom attributes for each base DN, streaming results to CBOM Secure.

Step 9: Validate Results

On completion, the sensor emits a status document per target with the detected vendor, per-phase counts, total documents, and any errors. Confirm the totals match expectations and that no errors are reported.

Configuration Reference

Key	Default	Description
host	—	Hostname or IP of the LDAP server.
port	0	0 = auto-detect (LDAPS → StartTLS → plain).
use_ssl	true	Use LDAPS. Ignored when port=0.
verify_ssl	true	Validate the server TLS certificate against trusted CAs.
ca_cert_path	""	PEM CA certificate to verify the server cert (internal CAs).
auth_method	simple	simple / anonymous / ntlm / sasl.
username	""	Full bind DN (simple/NTLM) or username (SASL).
base_dn	""	Search base. Empty = auto-discover from Root DSE.
page_size	1000	Entries per LDAP round-trip. Reduce for throttled servers.
pkcs12_passwords	[]	Passwords tried in order for encrypted userPKCS12 bundles.

Known Limitations

- Raw symmetric keys in custom attributes have no detectable structure — they require a type: secret_key hint, otherwise they are not parsed.
- PKCS#12 key material is reported as existence and algorithm only; private-key bytes are never extracted.
- NTLM hashes and Kerberos TGT key bytes are never exposed over LDAP and are out of scope by design.