Active Directory Integration Guide

CBOM Secure · Active Directory Discovery Sensor

Overview

This guide describes how to configure the CBOM Secure Active Directory Discovery Sensor to discover cryptographic material held in an Active Directory environment over LDAP / LDAPS (ports 389 / 636) and the Global Catalog (ports 3268 / 3269).

The sensor discovers the following, across the domain and configuration partitions and, for multi-forest environments, across all domains reachable through the Global Catalog:

Discovered material	Source
User & computer certificates	userCertificate on user / computer objects
SSH public keys	altSecurityIdentities (RSA, ECDSA, Ed25519)
Windows Hello (NGC) keys	msDS-KeyCredentialLink — TPM-backed key pairs
CA & cross-certificates	cACertificate, crossCertificatePair (PKI hierarchy)
KDS root keys	msKds-ProvRootKey (gMSA password derivation)
Kerberos krbtgt metadata	krbtgt account — KVNO and last rotation
Domain trust keys	trustedDomain inter-realm key metadata
BitLocker / DPAPI / TPM metadata	Existence and metadata only (no key bytes)

Note Certificate revocation is enriched at scan time: certificates whose serial appears in the directory CRL are flagged as revoked.

Prerequisites

- A domain user account the sensor can bind with. Standard directory read access covers most certificates and public keys; a delegated read or Domain Admin account is required to read elevated objects such as KDS root keys and DPAPI backup-key metadata.
- LDAPS (port 636) enabled on the domain controllers. Plain LDAP (389) is supported but LDAPS is strongly recommended.
- Network connectivity from the sensor host to DC ports 389 / 636 and, for multi-forest discovery, Global Catalog ports 3268 / 3269 (both 3269 and 636 must be reachable on the GC).
- For tree domains in a multi-forest setup: DNS resolution of the tree-domain hostnames (a conditional forwarder on the parent-forest DC).
- The CBOM Secure Active Directory Discovery Sensor package ready for configuration.

Step-by-Step Guide

Step 1: Create a Read-Only Service Account

Create a dedicated domain account for the sensor to bind with (for example, svc-cbom-ad). Use it exclusively for discovery so its activity is easy to audit and its credentials can be rotated independently.

Step 2: Grant Directory Read Permissions

Grant the service account read access to the directory. For most material, membership in Domain Users is sufficient. To discover KDS root keys, DPAPI backup-key metadata, and configuration-partition objects, delegate read access to those containers or use an account with the necessary rights.

Step 3: Verify Connectivity and Ports

Confirm the sensor host can reach the required ports on each target.

Port	Protocol	Used for
389	LDAP	Plain or StartTLS directory queries
636	LDAPS	TLS directory queries (recommended)
3268	Global Catalog	Forest-wide queries (plain)
3269	Global Catalog	Forest-wide queries over TLS

Step 4: Choose an Authentication Method

The sensor supports simple, NTLM, and Kerberos binds. Simple bind (over LDAPS) is the verified, recommended path. If you use NTLM, the domain field is required in the configuration.

Step 5: Prepare the Sensor Configuration

The sensor uses a forests block. Each forest entry defines credentials shared by all domains inside it; any field can be overridden at the domain level. Minimal example — one forest, one DC:

```
Name:    ActiveDirectoryDiscovery
ExtName: Discover_ActiveDirectory
Config:
  scan_name: "corp-scan"
  page_size:  500
  forests:
    - name:       "corp.test.local"
      auth_type:  simple          # simple | ntlm | kerberos
      username:   "CORP\\Administrator"
      password:   "<secret>"
      use_ssl:    true
      verify_ssl: false
      domains:
        - server:  "192.168.1.138"
          base_dn: "DC=corp,DC=test,DC=local"
```

Step 6: (Multi-Forest) Add Global Catalog Discovery

To scan an entire forest, add a gc_servers entry. The Global Catalog auto-discovers all child and tree domain controllers and appends them to the scan queue.

```
Config:
 scan_name: "enterprise-scan"
 page_size: 500
 forests:
  - name:       "partner.local"
    auth_type:  ntlm
    domain:     "PARTNER"        # required for ntlm
    username:   "Administrator"
    password:   "<secret>"
    use_ssl:    true
    verify_ssl: false
    gc_servers:
     - server: "192.168.1.24"   # auto-discovers all child/tree DCs
    domains:
     - server:  "192.168.1.24"
       base_dn: "DC=partner,DC=local"
     - server:  "192.168.1.157"
       base_dn: "DC=child,DC=partner,DC=local"
```

Step 7: (Optional) Skip a Domain or Override Credentials

Mark a known-unreachable domain to skip it, or override credentials for a specific domain:

```
domains:
 - server:  "192.168.1.141"
   base_dn: "DC=isolated,DC=corp,DC=example,DC=com"
   skip:    true

 - server:   "dc01.us.corp.example.com"
   base_dn:  "DC=us,DC=corp,DC=example,DC=com"
   username: "US\\Administrator"   # overrides forest-level credential
   password: "<secret>"
```

Step 8: Run Discovery

Run the Active Directory discovery task from CBOM Secure using the prepared configuration. The sensor connects to each target, runs its scan phases, and streams results to CBOM Secure.

Step 9: Validate Results

On completion, the sensor emits a status document per target (outcome and per-phase counts) and a single traversal document for the whole run that lists every target, the resolved IP and FQDN, and the outcome. Confirm:

- Each target shows an Ok (or expected Partial) outcome.
- Certificate and key counts are non-zero where material is expected.
- Any connection or phase errors in the traversal log are understood and resolved.

Step 10: Known Limitations

Limitation	Detail
TLS verification	With verify_ssl: true, the DC certificate must be issued by a CA trusted by the scanning machine. Use

	verify_ssl: false only for internal/self-signed DC certs in controlled environments.
DNS for tree domains	Tree domains require a conditional DNS forwarder on the parent-forest DC; without it, hostname resolution fails.
Key bytes never exposed	krbtgt, BitLocker, DPAPI, and KDS material is reported as existence + metadata only — actual key bytes are never available over LDAP.

Out of scope by design: NTLM password hashes, AD CS archived private keys, certificate-template analysis, and EFS recovery-agent certificates (these are not available over LDAP).