entro | DATASHEET

Securing On-Prem Active Directory Service Accounts with NHI Control

Entro connects to your on-premises AD DS to discover and classify service accounts, visualize access paths and permissions, and enable remediation with unified non-human identities (NHI) inventory, posture, and real-time threat detection.

AD Service Accounts = Active NHI Attack Surface

Released over a quarter of a century ago, Active Directory is still the core identity backbone for many enterprises, especially across Windows servers, legacy applications, and critical on-prem infrastructure. This also means AD DS service accounts remain one of the most common "quiet control planes" in your environment. They power business critical services, hold "everlasting" passwords, and are frequently the first identities attackers go for post-breach for persistence, lateral movement and privilege escalation.

The hard part for security is not "do we have svc accounts?" It's "do we know what they can access, who owns them, and whether they're being misused?"

Service Accounts outlive their purpose and creators.

They often stay enabled for years, drift into privileged groups, and accumulate access via OU scope, delegation, and GPO-driven local group assignments.

Critical access is buried in nested groups.

A seemingly harmless non-human identity may inherit powerful Access Rights through multi-level group membership.

Security posture risks go both ways.

Human users get configured for programmatic use and service accounts get used interactively (RDP, console, unusual hosts).

Permissions sprawl across OUs and object ACLs.

Delegated access, granular ACEs, and inherited permissions create unexpected access (attack) paths.

No clear owner, no quick remediation.

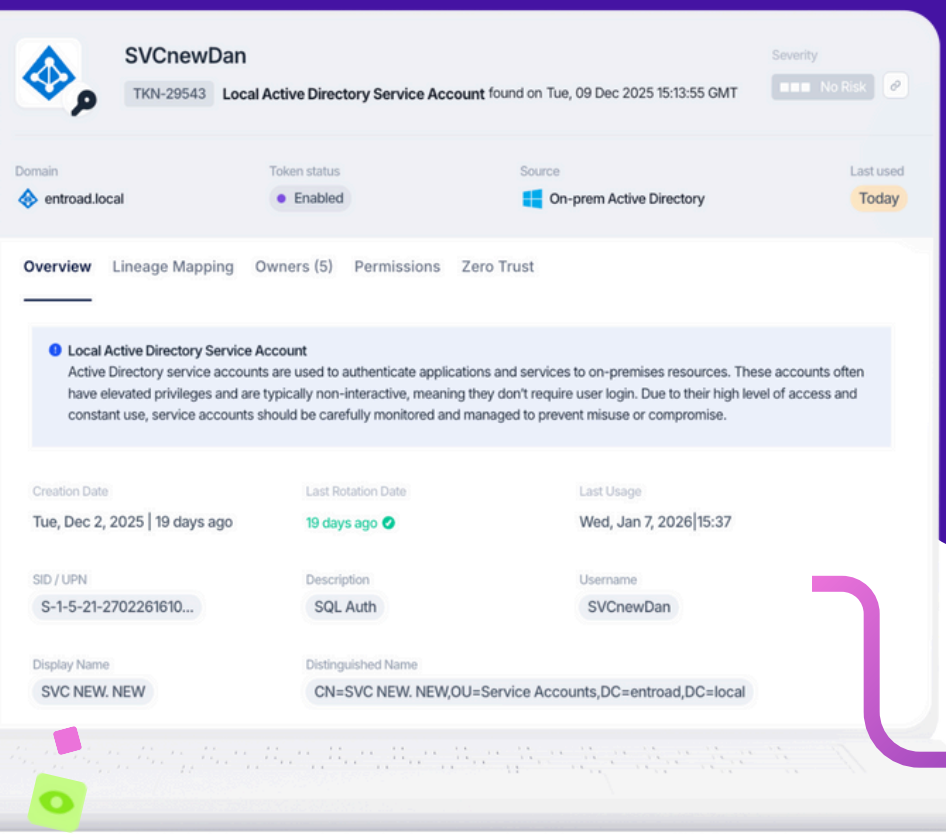
Without clear ownership and context, security teams can't rotate, right-size, or disable accounts confidently without breaking production.

entro

Entro for On-Prem AD DS

The platform ingests AD DS objects, users and ACLs to turn service accounts into governed NHIs by mapping their effective access (nested groups, OUs, ACEs) and their potential exposure paths (lateral movement and privilege escalation).

Findings are then tied to human ownership, anomaly detection, and automated remediation workflows.



Unify on-prem Active Directory service accounts with your NHI security program.

Detect misuse in real time. Spot interactive logons and unusual behavior that signal credential theft or compromise.

Deployment is non-disruptive, Entro uses a dedicated read-only LDAP bind account and does not make changes to AD.

Full Contextual Visibility

Access Rights

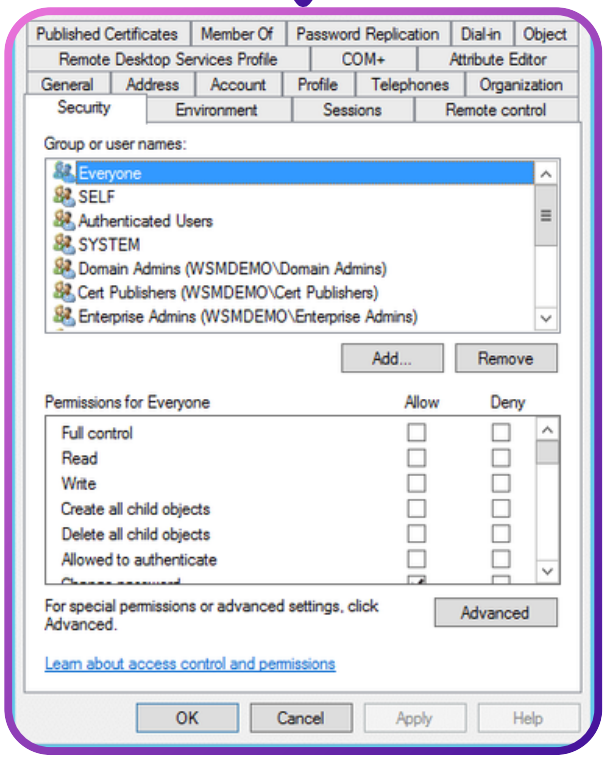
Understand what service accounts can access and where they pose risk (object ACL/ACE analysis).

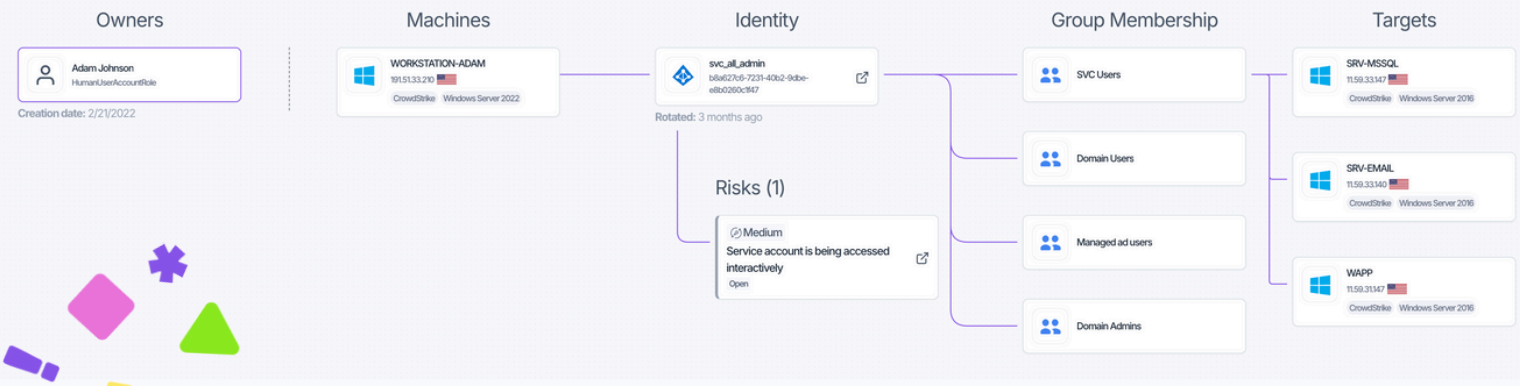
Nested Groups

Expand multi-level group membership to reveal hidden effective permissions.

Identity Classification

Distinguish humans acting as service accounts (programmatic access) vs service accounts used interactively.





Continuous Risk Management

Lineage Map Visuals

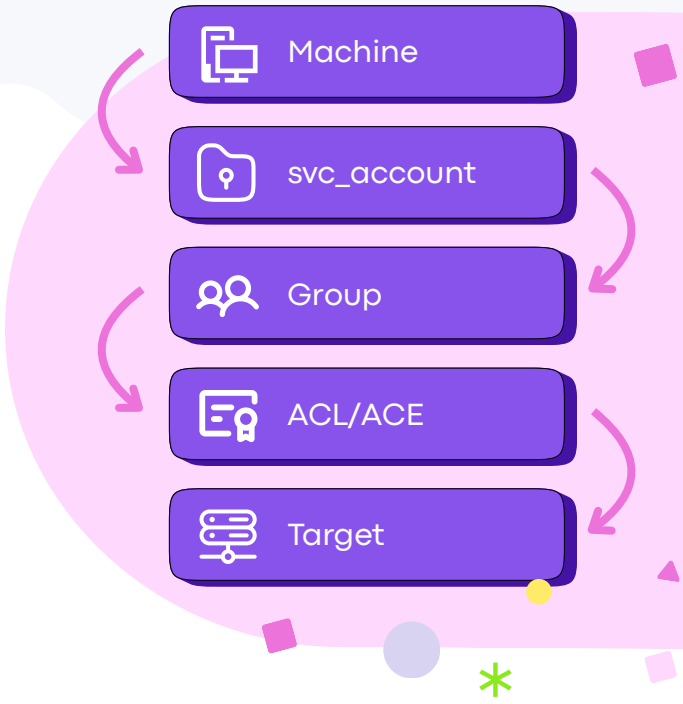
Map relationships between service accounts, human users, machines, permissions, target resources and exposed secrets.

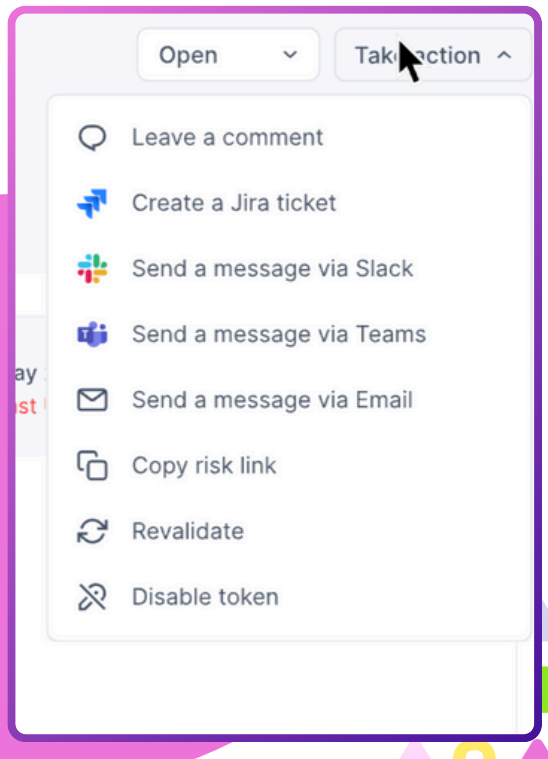
Attack Path Mapping

Identify how your service accounts can be leveraged in lateral movement chains.

Privilege Escalation Detection

Surface risky permission paths that could potentially lead to domain-level compromise.





Simplified Investigation & Remediation

Custom Query Analysis

Investigate exposures, identity behavior, and anomalies across AD DS objects, groups, and permissions.

Hybrid Correlation

Correlate on-prem AD DS identities and access paths with cloud identity sources for end-to-end context.

Remediation Workflows

Route high-risk findings into security operations using native integrations (Tines, Torq etc.), to assign ownership and drive resolution.

entro

Technical Appendix: On-Prem AD DS Integration

Entro lets you choose the deployment method that fits your architecture best. All options can be used independently or combined for richer context.

Entra ID ingestion (for synced on-prem environments)

Ingests AD-related identity objects that are synchronized to Entra ID to accelerate baseline visibility in hybrid deployments.

CrowdStrike Identity module (EDR context)

Adds domain controller and device context and identity activity signals to enrich service account behavior and usage analysis.

Entro Outpost (agent) via LDAP/LDAPS

Connects directly to on-prem AD DS over LDAP/LDAPS to ingest AD objects and object ACLs/ACEs for deep permissions, effective access, and attack path analysis.

Purpose	Ingest AD DS objects and object ACLs to identify identity risk, excessive permissions, and lateral movement paths.
Supported environments	• On-premises Active Directory forests (single-domain or multi-domain) • Hybrid environments where local AD data is synced to Entra ID
Data Entro scans	Entro requires a single read-only LDAP bind account. The account must be able to enumerate users, groups, computers, and basic attributes. No administrative or write privileges are needed. • User accounts and attributes • Groups and nested group membership • Group Policy Objects (GPO metadata) • ACLs on AD objects (where accessible via LDAP/LDAPS) • Computer accounts and Service Principal Names (SPNs) • Password and lockout policies (metadata) • Last logon signals, account status, privileged group membership • Authentication method summary
Requirements	• Network reachability from chosen Worker Group (Outpost) to a Domain Controller (view Onboarding in our doc center) • Service account UPN for LDAP bind (example: svc_entro@corp.local) Must have read access to directory objects and attributes within all required target domains.
Security and compliance	TLS 1.2+ required for LDAPS connections. Read-only directory access. Stored tokens encrypted using AES-256. Applicable standards: SOC 2 Type II, ISO 27001, GDPR (data retention and export controls apply).

Ready to secure your legacy NHIs?

Get a personalized Entro demo with our experts to assess your on-prem Active Directory service account exposure, risks, and remediation paths.

entro

Get a Demo