Active Directory Integration Requirements for Network Box

Overview

Network Box may require connectivity to your Active Directory (AD) environment to enable centralized authentication, authorization, and policy enforcement.

Integration allows Network Box to leverage existing directory identities and group structures, improving access control, operational efficiency, and security posture.

This document describes:

- Functional uses of AD integration
- Supported integration methods
- Security considerations and best practices
- LDAPS and secure binding recommendations
- Operational requirements

Functional Uses

1. Group-Based Policy Enforcement

Network Box queries Active Directory to determine group membership for authenticated users.

This enables:

- Proxy and web filtering policies based on AD groups
- Role-based access enforcement
- Simplified policy management aligned with organizational structure

Without AD integration, policies must be applied based on IP addresses or local accounts, which reduces accuracy and increases administrative overhead.

2. SSL VPN Authentication

Active Directory integration allows SSL VPN users to authenticate using their domain credentials.

Benefits:

- Eliminates separate VPN credentials
- Enforces centralized password and lockout policies
- Enables group-based VPN access control

- Supports rapid user deprovisioning via AD

Users authenticate successfully only if they belong to the designated VPN access group.

3. Email Recipient Verification

During inbound mail scanning, Network Box may verify recipients against Active Directory.

If a recipient does not exist, the message can be rejected during SMTP transaction.

Benefits:

- Prevents backscatter
- Reduces spam processing overhead
- Improves mail hygiene and resource efficiency

Integration Methods

- LDAP / LDAPS (directory queries and authentication)
- RADIUS (authentication passthrough for VPN)

LDAP / LDAPS Integration

Service Account Requirements

A dedicated service account is required for directory queries.

Requirements:

- Standard user account
- No administrative privileges
- Read-only directory access
- Used exclusively by Network Box

Example account name: nbusa

Provide the Distinguished Name (DN), e.g.: CN=nbusa,OU=Users,OU=Company,DC=yourdomain,DC=com

Domain Controller Information

Provide:

- IP addresses or FQDNs of Domain Controllers
- Multiple controllers recommended for redundancy
- Controllers may be used in failover or load-balanced mode

Security Justification

Centralized Identity Control

Authentication uses existing domain credentials.

Password policies, lockouts, and MFA (if deployed) remain enforced.

Immediate Deprovisioning

Disabling a user in AD immediately revokes VPN and policy-based access.

Elimination of Local Credentials

Reduces attack surface created by duplicated credentials.

Least Privilege Service Account

Directory access is read-only.

No administrative privileges are required.

Auditability

Authentication events remain visible in domain controller logs.

LDAPS and Secure Binding (Recommended)

Use LDAPS Instead of LDAP

LDAPS (TCP 636) encrypts directory queries and authentication.

Benefits:

- Protects credentials in transit
- Prevents interception or replay
- Protects group membership data
- Aligns with security best practices and compliance requirements

Certificate Requirements

Domain Controllers must present valid certificates.

Certificates must be trusted by Network Box.

Signing & Channel Binding (Recommended)

If supported in your environment:

- LDAP signing enabled
- Channel binding enabled
- NTLM restrictions enforced where possible

Password & Credential Management

The service account password is stored encrypted within Network Box.

It is not retrievable by personnel after entry.

Because the account is used programmatically, it cannot rotate its password automatically.

When the password is changed:

- Update password in Active Directory
- Provide the new password securely to Network Box support
- Network Box updates stored credentials

Operational Impact if Password Expires

- SSL VPN authentication fails
- Proxy policies fall back to default rules
- Email scanning continues to function

Recommendation: Use a long expiration interval (e.g., annual rotation) and update proactively.

RADIUS Integration (Alternative)

RADIUS may be used for SSL VPN authentication when directory queries are not required.

Advantages:

- Simpler deployment
- No directory bind account required
- Credentials passed through directly

Requirements:

- RADIUS server IP address
- Shared secret
- Network reachability

Network & Security Requirements

Ensure Network Box can reach Domain Controllers over required ports.

- LDAPS (636) preferred
- LDAP (389) only if LDAPS unavailable
- RADIUS (1812/1813) if applicable

Firewall rules should restrict access to required hosts only.

Connectivity & Port Verification

Service	Port	Protocol
LDAP	389	TCP
LDAPS	636	TCP
RADIUS Auth	1812	UDP
RADIUS Accounting	1813	UDP
Global Catalog (optional)	3268 / 3269	TCP

Troubleshooting & Operational Diagnostics

Common Checks

- Review Domain Controller security logs
- Verify bind attempts and authentication events
- Confirm successful LDAP queries
- Review Network Box logs for bind or query errors

Recommended Operational Checks

- Verify service account password before expiration
- Monitor DC certificate expiration dates (LDAPS)
- Confirm group membership changes replicate properly
- Validate LDAPS after domain controller updates
- Test VPN authentication after AD changes

When to Contact Support

- LDAP binds fail despite verified credentials
- LDAPS negotiation errors persist after certificate validation

- Group queries return inconsistent results
- VPN authentication failures occur with no AD log entries

Include timestamps of failure, affected usernames, DC IP addresses used, recent AD changes, and relevant log excerpts.