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

Network Box supports integration using:

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

Architecture Overview

Directory Query Flow (LDAP/LDAPS)

User → Network Box → AD Domain Controller
(Bind & Query)
↓
Group Membership Retrieved
↓
Policy Enforcement Applied

SSL VPN Authentication Flow

Remote User
↓
SSL VPN Client
↓
Network Box
↓
Active Directory (LDAP/LDAPS bind)
↓
Authentication + Group Validation
↓
VPN Access Granted / Denied

RADIUS Authentication Flow (Alternative)

Remote User
↓
SSL VPN Client
↓
Network Box
↓
RADIUS Server (Pass-through authentication)
↓
Accept / Reject

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
  - Multiple controllers are recommended for redundancy
  - Controllers may be used in failover or load-balanced mode

Security Justification

Active Directory integration improves security rather than weakening it.

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.

Elimation 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
- is not retrievable by personnel after entry

Important

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

When the password is changed:

1. Update password in Active Directory
2. Provide the new password securely to Network Box support
3. Network Box updates stored credentials

Operational Impact if Password Expires

If the service account password becomes invalid:

Function	Impact
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

When to Use RADIUS

RADIUS is appropriate when:

- VPN authentication is required
- group-based policy enforcement is not needed via LDAP
- centralized authentication infrastructure already exists

Network & Security Requirements

To enable AD integration, 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 restrict access to required hosts only

Summary

Active Directory integration enables secure, centralized authentication and policy enforcement while improving operational efficiency and access control.

LDAP/LDAPS enables directory queries and policy enforcement, while RADIUS provides streamlined authentication for VPN access.

Use of LDAPS, least-privilege service accounts, and centralized identity controls ensures integration aligns with enterprise security best practices.

Executive Summary

Active Directory integration allows Network Box to leverage your organization's existing identity infrastructure to provide centralized authentication, authorization, and policy enforcement.

This integration enables:

- secure SSL VPN authentication using domain credentials
- group-based policy enforcement aligned with organizational roles
- immediate access revocation when users are disabled in AD
- improved mail hygiene through recipient verification

Security is maintained through the use of least-privilege service accounts, encrypted credential storage, and support for secure directory binding using LDAPS.

Where supported, LDAPS, LDAP signing, and channel binding should be enabled to ensure directory communications are encrypted and resistant to interception or tampering.

Active Directory integration reduces administrative overhead, eliminates duplicate credentials, and strengthens access control while maintaining full auditability within the domain environment.

Troubleshooting & Operational Diagnostics

This section helps administrators quickly identify and resolve common integration issues.

1. SSL VPN Authentication Failures

Symptoms

- Users cannot authenticate to VPN
- Authentication errors returned immediately
- Previously working users now failing

Possible Causes

Service account password expired or changed

- Verify bind account credentials
- Update password in Network Box configuration if needed

User not in VPN access group

- Confirm group membership in AD
- Verify correct group configured on Network Box

Domain Controller unreachable

- Verify network connectivity
- Confirm firewall rules allow LDAP/LDAPS traffic

Account lockout policy triggered

- Check AD security logs
- Verify user account status

2. Group-Based Policy Not Applying

Symptoms

- Users authenticate but receive incorrect proxy policies
- Default rules applied unexpectedly

Possible Causes

Directory query failure

- Verify LDAP bind account credentials
- Confirm DC connectivity

Incorrect group DN configured

- Confirm full distinguished name (DN)
- Verify nested group membership behavior

Replication delay in AD

- Verify group membership has replicated across DCs

3. LDAPS Connection Failures

Symptoms

- Cannot bind using LDAPS
- TLS/SSL handshake errors
- Connection timeout on port 636

Possible Causes

Invalid or untrusted certificate

- Verify DC certificate validity
- Ensure issuing CA is trusted

LDAPS not enabled on Domain Controllers

- Confirm LDAPS service is active
- Verify certificate installed in NTDS store

Firewall blocking LDAPS

- Confirm TCP 636 allowed between Network Box and DC

4. Email Recipient Verification Not Working

Symptoms

- Messages to invalid recipients accepted
- No recipient validation occurring

Possible Causes

Directory lookup failure

- Verify LDAP connectivity
- Confirm bind credentials

Incorrect domain scope

- Verify AD domain matches scanned email domain

5. LDAP Bind Failures

Symptoms

- Authentication errors in logs
- Directory queries fail
- VPN auth fails simultaneously

Possible Causes

Incorrect Distinguished Name

- Verify DN syntax and OU path

Password expired

- Update password and re-test

Account disabled

- Verify service account status

6. Connectivity & Port Verification

Ensure required ports are reachable:

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

Test connectivity:

```
telnet DC_IP 636
```

or

```
openssl s_client -connect DC_IP:636
```

7. Diagnostic Logging & Verification

When troubleshooting:

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

8. Recommended Operational Checks

To ensure reliability:

✔ 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

9. When to Contact Support

Contact Network Box support if:

- 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
- relevant log excerpts

Excellent choices — these are exactly the sections admins and architects look for when deploying.

Below are three additions you can append to the document:

Quick Deployment Checklist

Use this checklist to ensure a smooth and secure Active Directory integration.

Pre-Deployment

- ✓ Confirm Network Box can reach Domain Controllers
- ✓ Identify primary and secondary Domain Controllers
- ✓ Verify firewall rules allow required ports
- ✓ Confirm LDAPS availability (recommended)
- ✓ Verify DC certificates are valid and trusted

Service Account Setup (LDAP / LDAPS)

- ✓ Create dedicated service account (e.g., **nbusa**)
- ✓ Assign **no administrative privileges**
- ✓ Ensure account has read access to directory
- ✓ Set password expiration policy (annual recommended)
- ✓ Document Distinguished Name (DN)
- ✓ Store credentials securely

Directory & Group Preparation

- ✓ Create VPN access group (if required)
- ✓ Confirm group naming conventions

✓ Verify nested group membership (if used)

✓ Confirm group replication across domain controllers

Network Configuration

✓ Allow outbound access from Network Box to DCs

✓ Open required ports:

Service	Port
LDAPS	636
LDAP (fallback)	389
RADIUS (optional)	1812/1813

✓ Restrict access to DC IPs only (least exposure)

LDAPS Security Configuration (Recommended)

✓ Install valid certificate on DCs

✓ Confirm certificate trust chain

✓ Test LDAPS connectivity

✓ Enable LDAP signing (if environment supports)

✓ Enable channel binding (if supported)

Network Box Configuration

- ✓ Enter service account DN
- ✓ Enter credentials securely
- ✓ Configure DC IPs / FQDNs
- ✓ Configure group DN(s) for policy enforcement
- ✓ Test bind & query

Validation & Testing

- ✓ Test VPN authentication with test user
- ✓ Confirm group-based policy enforcement
- ✓ Test login with non-authorized user
- ✓ Verify logs show successful bind and query
- ✓ Test failover using secondary DC

Post-Deployment

- ✓ Document configuration
- ✓ Record password rotation date
- ✓ Monitor authentication logs
- ✓ Test authentication after domain changes

One-Page Implementation Guide

Objective

Integrate Network Box with Active Directory to enable centralized authentication and group-based policy enforcement.

Step 1 — Prepare Domain Controllers

- Ensure DCs are reachable from Network Box
- Install and validate LDAPS certificates (recommended)
- Confirm required ports are open

Step 2 — Create Service Account

Create a read-only directory account:

Example: nbusa

Requirements:

- no admin privileges
- used only for directory queries
- password stored securely

Record Distinguished Name:

CN=nbusa,OU=Users,OU=Company,DC=domain,DC=com

Step 3 — Prepare Groups

Create and document groups used for:

- VPN access control
- policy enforcement

Verify membership and replication.

Step 4 — Configure Network Box

Enter:

- Domain Controller IPs / FQDNs
- service account DN
- password
- group DN(s)

Select **LDAPS** if available.

Step 5 — Validate Authentication

Test with:

✓ authorized user

✓ unauthorized user

✓ multiple DC failover

Confirm logs show successful bind and group retrieval.

Step 6 — Verify Policy Enforcement

- confirm proxy rules apply correctly
- confirm VPN access restricted by group
- verify fallback behavior

Step 7 — Document & Monitor

- record configuration details
- track password expiration date
- monitor logs for authentication failures

Azure AD / Microsoft Entra ID Hybrid Considerations

Organizations using hybrid identity environments (on-prem AD synchronized to Azure AD / Microsoft Entra ID) should consider the following.

Supported Scenarios

Network Box integrates with **on-prem Active Directory**.

In hybrid environments:

✓ Authentication occurs against on-prem AD

✓ Azure AD sync does not affect LDAP queries

✓ Group membership is sourced from on-prem directory

Azure AD Domain Services (AAD DS)

If using **Azure AD Domain Services**, Network Box may integrate using LDAP/LDAPS against the managed domain.

Requirements:

- LDAPS enabled in AAD DS
- secure certificate configuration

- network connectivity to Azure virtual network

Azure AD (Entra ID) Only Environments

Pure cloud-only Azure AD environments **do not support LDAP**.

In these cases, options include:

Option 1 — RADIUS Authentication

Use NPS or Azure MFA NPS extension to provide RADIUS authentication.

Option 2 — Azure AD Domain Services

Deploy AAD DS to provide LDAP/LDAPS compatibility.

MFA Considerations

When Azure MFA or conditional access is used:

- LDAP authentication does **not** enforce MFA
- RADIUS with Azure MFA extension can enforce MFA
- VPN MFA enforcement may require RADIUS-based architecture

Group Synchronization Considerations

When groups originate in Azure AD and sync to on-prem AD:

✔ ensure groups are synchronized back to on-prem directory

✔ verify membership replication before testing policies

✔ avoid relying on cloud-only groups for LDAP queries

Conditional Access Policies

Conditional access policies in Azure AD do not apply to LDAP authentication.

To enforce location, device, or risk-based controls:

- use VPN policy controls
- use RADIUS with MFA
- enforce endpoint compliance controls

Recommended Hybrid Best Practices

✓ Keep identity source authoritative in on-prem AD for LDAP use

✓ Use LDAPS for secure directory communication

✓ Consider RADIUS + Azure MFA for VPN MFA enforcement

✓ Monitor synchronization health between AD and Azure AD

✓ Document identity architecture for operational clarity