Active Directory Group Structure for Web Browsing Policy Enforcement

Purpose

This document describes how to structure Active Directory (AD) security groups so Network Box can apply web browsing and proxy policies based on user group membership.

Network Box queries AD via LDAP/LDAPS and builds an internal membership database. Policy enforcement is then applied based on the groups each user belongs to.

How Network Box Uses Group Membership

Network Box reads group membership and builds an internal mapping such as:

user → group membership → policy enforcement

Example internal mapping:

user: users1
group_member: nwb_group1
group_member: nwb_group2

Based on these groups, internet access rules and filtering policies are applied.

Required Group Structure

All web browsing policy groups must be nested under **one parent group**.

Example Structure

CN=WebAll,OU=WebBrowsing,OU=MainOU,DC=yourdomain,DC=local

This parent group acts as the **policy container**.

Policy Groups (Children)

Examples:

CN=Nwb_group1
CN=Nwb_group2
CN=Nwb_group3

Each policy group represents a browsing policy.

Recommended Active Directory Layout

```
OU=MainOU
 └── OU=WebBrowsing
     ├── CN=WebAll        ← Parent container group
     ├── CN=Nwb_group1    ← policy group
     ├── CN=Nwb_group2    ← policy group
     └── CN=Nwb_group3    ← policy group
```

Group Nesting Requirements

Step 1 — Create Policy Groups

Create security groups representing policy roles:

- Nwb_group1
- Nwb_group2
- Nwb_group3
- (additional policy groups as required)

These groups contain **users**.

Step 2 — Create the Parent Container Group

Create a parent group:

WebAll (this is only an example)

This group contains **only the policy groups**, not users.

Step 3 — Nest Policy Groups into Parent Group

Add the policy groups as members of the parent group.

Example:

```
WebAll
 ├── Nwb_group1
 ├── Nwb_group2
 └── Nwb_group3
```

Example LDAP Output

Parent Group

```
CN=WebAll
member:
  CN=Nwb_group1
  CN=Nwb_group2
  CN=Nwb_group3
```

Policy Group Membership

```
CN=Nwb_group2
member:
  CN=User1
```

CN=User2
CN=User3

CN=Nwb_group3
member:
CN=User4
CN=User5

Why This Structure Is Required

Network Box queries the parent group to discover policy groups, then resolves user membership.

This structure ensures:

✔ consistent group discovery

✔ simplified LDAP queries

✔ scalable policy management

✔ clean separation of roles

✔ minimal directory traversal

Policy Assignment Logic

Policy rules are applied based on **policy group membership**.

Example:

Group	Policy
Nwb_group1	standard browsing policy
Nwb_group2	unrestricted access
Nwb_group3	social media allowed

If a user belongs to multiple groups, policy precedence rules may apply (defined during deployment).

Naming Recommendations

Use clear and consistent naming:

Recommended prefix:

NWB_

Examples:

- NWB_Finance
- NWB_HR
- NWB_Executives
- NWB_Restricted
- NWB_IT
- NWB_Marketing

Avoid spaces and special characters.

Important Implementation Rules

✔ Groups must be Security Groups

✔ Groups must be visible to LDAP queries

✔ Nested group membership must be enabled

✔ Users must be direct members of policy groups

✔ Policy groups must be members of the parent group

Common Mistakes to Avoid

- ### Placing users directly inside WebAll

  Users must belong to policy groups, not the parent group.

- ### Creating policy groups outside the container OU

  All policy groups should reside under the designated WebBrowsing OU.

- ### Using Distribution Groups

  Only **Security Groups** are supported.

- ### Relying on cloud-only groups (Azure AD)

  Groups must exist in on-prem AD or be synchronized.

- ### Using deeply nested group structures

  Keep nesting simple: Parent → Policy Group → Users

Testing & Verification

After configuration:

1. Add a test user to a policy group
2. Confirm LDAP membership resolution
3. Verify policy is applied correctly
4. Test removal and reassignment

Scalability & Future Expansion

To add a new policy:

1. Create new policy group (e.g., NWB_Engineering)
2. Add group to WebAll
3. Add users to new group

4. Define policy in Network Box

No structural changes are required.

Security & Best Practices

- Limit modification rights to authorized administrators
- Use least privilege delegation for group management
- Audit group membership changes
- Document policy group purposes

Summary

This structure allows Network Box to efficiently map users to browsing policies using LDAP group membership.

Maintaining a single parent group containing policy groups ensures predictable behavior, simplified management, and scalable policy enforcement.

How Active Directory Groups Are Used in Web Browsing Policy Enforcement

Network Box applies web browsing and proxy policies based on **group membership retrieved from Active Directory**.

LDAP queries determine which policy groups a user belongs to. Those memberships are then mapped to proxy rules that allow or restrict access.

Example Proxy Policy Configuration

Below is a representative proxy rule configuration illustrating how group membership is used to enforce browsing policies:

clear proxy rule webclient

config proxy rule webclient deny isthreat = TRUE with template proxy.malwareblock
config proxy rule webclient deny snidomain inacl custom-BLOCKEDTLD
config proxy rule webclient deny httphost inacl custom-denyall
config proxy rule webclient permit-log httphost inacl custom-allowall

config proxy rule webclient permit-log entitygroup = nwb_group3 httpcategory inacl nwb_group3
config proxy rule webclient permit-log entitygroup = nwb_group3 httphost inacl custom-nwb_group3
config proxy rule webclient deny httphost inacl custom-nwbgroup3 entitygroup != nwb_group3

config proxy rule webclient permit-log entitygroup = nwb_group1 httpcategory inacl nwb_group1

config proxy rule webclient permit-log httpcategory inacl custom-productivity
config proxy rule webclient deny httpcategory inacl custom-core

config proxy rule webclient deny httpurl endswith .exe
config proxy rule webclient permit-log all

What These Rules Do

Threat & Malware Protection

deny isthreat = TRUE
deny snidomain inacl custom-BLOCKEDTLD
deny httphost inacl custom-denyall

Blocks known malicious sites, threat domains, and globally denied hosts.

Global Allow Rules

permit-log httphost inacl custom-allowall

Allows explicitly approved destinations.

Group 3 Exceptions

permit-log entitygroup = nwb_group3 httpcategory inacl nwb_group3
permit-log entitygroup = nwb_group3 httphost inacl custom-nwgroup3
deny httphost inacl custom-nwbit entitygroup != nwb_group3

Meaning:

• Group 3 staff receive expanded access privileges • Certain sites are restricted to Group 3 only
• Non-Group 3 users are denied those resources

Group 1 Department Policy

permit-log entitygroup = nwb_group1 httpcategory inacl nwb_group1

Allows group 1-related categories (e.g., social media, advertising platforms).

Default Productivity Policy

permit-log httpcategory inacl custom-productivity
deny httpcategory inacl custom-core

Allows standard business-use sites while blocking restricted categories.

Executable Download Control

deny httpurl endswith .exe

Prevents direct download of executable files.

Final Rule

permit-log all

Allows remaining traffic and logs activity.

How Group Membership Controls Policy

When a user authenticates or is identified:

1. Network Box queries Active Directory.
2. Group membership is retrieved.
3. Membership is stored internally.
4. Proxy rules evaluate the user's groups.
5. Policies are applied accordingly.

Example

User belongs to:

- Nwb_group2
- Nwb_group1

Result:

✓ Standard browsing allowed

✓ Group 2 browsing sites allowed