HowTo Setup LDAP

(Proxmox + LDAP Template)

Updated: July 2026 | napp-it.org | CC-BY-SA 2.0

This guide covers LDAP directory schemas relevant to Windows/SMB authentication (POSIX, Samba, Active Directory mode), when to use which one, and how to set up an LDAP server on Proxmox as a napp-it cs backend member.

Table of Contents

TL;DR — Too Long; Didn't Read

Need Windows clients to log in with a username/password against a central directory? Use OpenLDAP + the Samba schema (NT4-style) for simple NTLM auth, or Samba 4 as a full AD Domain Controller if you also need Kerberos SSO and Group Policy. Recommended path: Proxmox LXC container with the TurnKey LDAP appliance template, then import the Samba schema and add this host as a napp-it cs backend member.

1. The Three LDAP Schema Modes

POSIX / RFC2307 — classic Linux LDAP

Stores Linux UIDs, GIDs, home directories and (with the separate openssh-lpk schema) SSH public keys. On its own it cannot process NTLM hashes for Windows SMB logins.

Samba schema (sambaSamAccount)

Extends the Linux LDAP schema with attributes such as `sambaNTPassword`, letting Samba authenticate Windows clients via NTLM without Kerberos. This is the classic "NT4-style domain" model.

Note: classic NT4-style domain controller support (samba PDC/BDC) has been deprecated in current Samba releases (4.11+). New setups should generally prefer the Active Directory mode below unless there is a specific reason to stay with the legacy model.

Active Directory mode (Samba 4 AD DC)

The LDAP server behaves largely like a Microsoft Windows Domain Controller for Windows clients — it integrates Kerberos, DNS and LDAP in one package. It is highly compatible, though not a byte-for-byte reimplementation of every AD feature.

Mode / Schema	OpenLDAP (plain)	OpenLDAP + Samba3 schema	Samba 4 AD DC
1. POSIX / RFC2307 (native Linux/Unix)	Yes	Yes	Yes (--use-rfc2307)

2. Samba schema (NTLM for SMB)	No	Yes	Handled differently*
3. Active Directory mode (KDC / Kerberos / GPO)	No	No	Yes

* Samba 4 AD DC does not need the classic sambaSamAccount schema import — it still supports NTLM internally for legacy clients, but stores the hash differently (unicodePwd / supplementalCredentials in its own AD schema).

2. Why Plain OpenLDAP Cannot Provide Full Active Directory

A real Active Directory is far more than a directory service — it is a tightly integrated ecosystem of several services:

- **Integrated Kerberos KDC** (Key Distribution Center) — issues Ticket-Granting-Tickets (TGTs)
- **Microsoft-specific LDAP extensions** — e.g. Global Catalog on port 3268, the MS-DRSR replication protocol
- **SMB/RPC server** — for Group Policy Objects (GPOs), NETLOGON and SYSVOL shares
- **DNS server** — BIND-DLZ or Samba-internal DNS for the Kerberos SRV records clients need

OpenLDAP is an excellent, extremely fast and highly flexible pure LDAP server. But out of the box it is missing the Kerberos KDC, the SYSVOL network shares for Group Policy, and the Microsoft-specific RPC interfaces a Windows client expects after joining a domain.

3. When to Use What

Choose OpenLDAP when...

- you primarily need to centrally authenticate Linux/Unix clients, macOS, or web applications (Nextcloud, GitLab, VPN)
- you run a classic Samba 3 ("NT4-style domain") setup with the samba.schema for Windows SMB shares
- you need maximum control over your directory schema and extremely fast queries against a huge number of entries

Choose Samba 4 (Active Directory DC) when...

- you want to natively join Windows clients to a domain (Win key + Pause → Join a domain)
- you want to apply Group Policy Objects (GPOs) to Windows clients
- you want seamless Kerberos Single Sign-On (SSO) across Windows, Linux and Mac clients on your network

Good to know: Samba 4 ships its own integrated LDAP server. Once you set up Samba 4 as an Active Directory Domain Controller (AD DC), you no longer need OpenLDAP at all — Samba 4 answers LDAP, Kerberos and SMB requests entirely on its own.

4. Recommended Installation Path (Proxmox + TurnKey LDAP)

- Proxmox host with an LXC container using the TurnKey LDAP appliance template
- Start the container and install it as Master (read/write)

Install the Samba schema:

```
apt update
apt install smbldap-tools

# Import the Samba schema into the OpenLDAP configuration
ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/share/doc/samba/examples/LDAP/samba.ldif

# Install Samba itself
apt update && apt install -y samba
```

Verify the schema import:

```
ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=schema,cn=config" "(cn=*samba*)" dn
```

As soon as a line such as `dn: cn={X}samba,cn=schema,cn=config` appears in the output, all Samba attributes are available in OpenLDAP and phpLDAPadmin.

Test 2: open `https://ldap-ip` in a browser (napp-it's own webserver.pl must NOT be started here — it would collide with phpLDAPadmin on the same port). This should show the phpLDAPadmin management GUI.

5. Per-User Samba Attributes

Important: you need the Samba schema in OpenLDAP for every single user who is supposed to log in via SMB/NTLM from Windows (or Linux SMB clients).

Why a normal LDAP password entry is not enough:

- **Format mismatch:** by default OpenLDAP stores passwords as ordinary hashes (e.g. SHA-256, SSHA or Bcrypt). Windows, however, sends no plaintext during an SMB/NTLM login — it expects the server to verify the login using a special NTLM hash (sambaNTPassword).
- **Missing attribute:** the OpenLDAP core schema has no sambaNTPassword field at all. Only adding the sambaSamAccount object class from the Samba schema gives a user this field in LDAP.
- **Kerberos vs. NTLM:** in a full Active Directory / Kerberos environment, authentication would run via tickets. Since you are using NTLM without Kerberos here, the Samba server (e.g. acting as a file server) needs to read this sambaNTPassword hash from LDAP to confirm the Windows login.

What this means for your workflow:

Once the schema is imported, every user who is allowed to log in via SMB needs:

- the `sambaSamAccount` object class added
- at minimum these required attributes set: `sambaSID` (a unique Security ID for the user) and `sambaNTPassword` (the generated NTLM hash of the password)

Tip: if you change passwords in phpLDAPadmin or the console, the NTLM hash is often not updated automatically unless you use special overlays (such as smbk5pwd) or tools like smbldap-tools / smbpasswd.

6. napp-it cs: LDAP Server as Backend Member

Set up napp-it cs on the LDAP container as a backend member (autostart via `perl /opt/csweb-gui/autobackend.pl`). This starts only server.pl and monitor.pl on boot — deliberately NOT webserver.pl, since napp-it's own web GUI would collide with phpLDAPadmin on the same port. The actual web GUI stays a manual step if you ever need it directly on this host.

```
perl /opt/csweb-gui/autobackend.pl 1 # enable backend autostart, start now
```

Then add this host as a member in napp-it cs: System menu › add the LDAP container by IP, using the standard member-join flow.

7. Outlook: NTLM Deprecation

Should a future Windows release stop supporting the simple NTLM model by default and require the more secure Kerberos instead, you have two options:

- re-allow NTLM again via a Windows Registry policy, or
- switch to Samba as a full AD DC with DNS/DHCP and Kerberos (considerably more effort)