Refine — LDAP / Active Directory Setup Guide

Connect Refine to your on-premises Active Directory so employees can sign in with their corporate credentials.

For an architectural overview of how directory integration fits with each network topology (public ALB, internal ALB + NAT, air-gapped, etc.), see `NETWORK_ARCHITECTURE.md`.

Network Requirements

What: Refine's EC2 must reach your LDAP/AD server on port 389 (LDAP) or 636 (LDAPS).

Why: LDAP authentication is a server-to-server bind from Refine to your AD. There is no public-internet dependency, so this works in private subnets and air-gapped deployments — but your VPC must have a route to the AD host.

How:

- The LDAP server can be a private IP. Configure `Server URL` as `ldaps://<private-IP-or-hostname>:636`.
- VPC must resolve the AD hostname. If you use a corporate DNS name (e.g., `ad.corp.com`), configure a Route 53 Resolver outbound endpoint forwarding to your on-prem DNS, or use the AD server's IP directly.
- Network path: VPN, AWS Direct Connect, VPC peering, or Transit Gateway must connect Refine's VPC to the AD network.
- Refine EC2's security group must allow outbound TCP to `<AD host>:636` (or `:389`).
- **TLS verification:** v2.19+ defaults to verifying the AD server's TLS certificate against the system trust store. If your AD uses a self-signed corporate CA cert, either install the cert in the EC2's trust store or set `tls_verify=false` in the LDAP config (with a security risk acknowledgment — this disables MITM protection).
- **Cross-partition:** LDAP works across partitions if VPN/peering provides reachability. Refine's LDAP code is partition-agnostic.
- **Air-gapped:** LDAP works in fully air-gapped deployments because no public-internet endpoints are called.

Topology	Works?
A — Internet-facing ALB	Yes, if AD is reachable via VPN/peering
B — Internal ALB + NAT	Yes
C — Internal ALB + VPC endpoints (no NAT)	Yes
D — Air-gapped GovCloud	Yes (use on-prem AD via VPN/peering)

---

1. Overview

Refine supports on-prem AD/LDAP authentication:

- Employees sign in with their AD username and password on the Refine login page
- Users are **auto-provisioned** on first login (no manual account creation needed)
- AD groups can be **mapped to Refine account groups** so team members automatically see the right AWS accounts
- The **ROOT** user (setup script runner) always uses local email/password — LDAP is for additional users only

2. Prerequisites

Requirement	Details
Refine instance	Running and accessible, ROOT user logged in
Network access	Docker container can reach the AD server (port 636 for LDAPS, 389 for LDAP)
Service account	An AD account with read access to user objects (for search-then-bind authentication)
Service account DN	The full Distinguished Name of the service account
User Search Base	The OU containing your user accounts (e.g., `OU=Users,DC=corp,DC=com`)
Email domain	The domain used by your AD users (e.g., `corp.com`)

> ***Security:*** *Use LDAPS (port 636) whenever possible. Plaintext LDAP (port 389) transmits passwords unencrypted.*

3. Option A: Configure via Refine UI (Recommended)

1. Log in to Refine as the **ROOT** user
2. Go to **Directory Settings** in the sidebar (lock icon)
3. Select the **LDAP** tab
4. Fill in the required fields:
   - **Server URL** — e.g., `ldaps://ad.corp.com:636`
   - **Bind DN** — service account DN (e.g., `CN=svc-refine,OU=Service Accounts,DC=corp,DC=com`)
   - **Bind Password** — service account password
   - **User Search Base** — e.g., `OU=Users,DC=corp,DC=com`
   - **User Domain** — e.g., `corp.com`
5. Click **Test Connection** to verify connectivity
6. Click **Save LDAP Configuration**
7. Optionally set up **Group Mapping** (see Section 5)

After saving, employees can immediately sign in with their AD credentials.

4. Option B: Configure During Setup Script

When running `setup.sh` or `setup.bat`, the wizard offers an optional directory integration step:

```
Directory Integration (Optional)
[1] Skip — I'll set this up later
[2] On-Prem Active Directory (LDAP)
[3] Azure AD / Entra ID

Your choice [1]: 2
```

If you choose option 2, the wizard prompts for Server URL, Bind DN, Bind Password, Search Base, and User Domain. The values are written to `.env` and automatically seeded into the database on first boot.

> *You can always change the configuration later from the Directory Settings page.*

---

5. Group Mapping

Map AD groups to Refine account groups so users automatically get access to the right AWS accounts:

1. Go to **Directory Settings** > **Group Mapping** section
2. Click **Fetch Directory Groups** to load groups from your AD server
3. For each AD group, select the corresponding **Refine account group** from the dropdown
4. Optionally set a **Role Override** — members of this AD group will be provisioned as Admin instead of User
5. Click **Save Mappings**

On each login, the user's Refine group memberships are synced with their current AD group memberships. If a user is removed from an AD group, they lose access to those AWS accounts on their next Refine login.

> ***No mapping configured?*** *Users are still provisioned on login with the default role (User), but they won't be assigned to any account groups. ROOT can manually assign them from the User Management page.*

---

6. How It Works

1. User enters their AD email and password on the Refine login page
2. Refine detects the email domain matches the configured LDAP user domain
3. Refine's service account searches AD for the user by `sAMAccountName`
4. The user's password is verified via an LDAP bind with their own credentials
5. On first login, a Refine user account is auto-created (JIT provisioning)
6. AD group memberships are synced to Refine groups per the mapping table
7. A JWT session token is issued — the rest of the session works identically to local auth

The ROOT user is never affected by LDAP — ROOT always uses local email/password authentication.

---

7. Finding Your LDAP Values

Server URL

Check with your IT team. Common formats:

- **LDAPS (recommended):** `ldaps://ad.yourcompany.com:636`
- **LDAP (plaintext):** `ldap://ad.yourcompany.com:389`

Bind DN (Service Account)

The full Distinguished Name of the service account. Example:

```
CN=svc-refine,OU=Service Accounts,DC=corp,DC=com
```

To find it from a domain-joined Windows machine:

```
dsquery user -name svc-refine
```

User Search Base

The Organizational Unit containing your user accounts. Example:

```
OU=Users,DC=corp,DC=com
```

In Active Directory Users and Computers: right-click the Users OU → Properties → Object tab → see the full path.

User Search Filter

Default: `(sAMAccountName={username})` — works for most AD setups. The `{username}` placeholder is replaced with the part before `@` in the user's email.

Email Domain

The domain portion of your users' email addresses (e.g., `corp.com` if users sign in as `jane@corp.com`).

---

8. Troubleshooting

Problem	Solution
Connection refused	Verify server URL and port. Check firewall rules between Docker host and AD server.
Invalid credentials (bind)	Verify the Bind DN and password. Check that the service account isn't locked or expired.
User not found	Check the User Search Base DN. Verify the user exists in that OU. Try the search filter with a known username.
SSL certificate error	Refine uses permissive TLS by default (accepts self-signed certs). For strict validation, contact support.
Users can't log in but test succeeds	Verify the User Domain matches your users' email domain. Check that users are in the Search Base OU.
LDAP server is down	ROOT can always log in with local credentials. Directory users see a clear error message ("Directory server unavailable").
Groups not mapping	Click "Fetch Directory Groups" to verify groups are visible. Check that the mapping table has been saved.
Role not syncing	If ROOT manually changed a user's role, it won't be overridden by AD sync (role is "locked"). Clear the lock from User Management if needed.

Need Help?

Contact Blacktip Solutions at **support@blacktipsolutions.com**