QuietAD

User Guide — Active Directory Management Tool

Version 2.0.0 · quietad.online

Contents

1. Introduction

QuietAD is a Windows desktop tool for managing Active Directory — users, computers, groups, and LAPS passwords — from one signed, offline-activated application. It's built for IT administrators and helpdesk technicians who handle the same recurring set of AD tasks daily and want them handled faster than switching between ADUC, PowerShell, and separate LAPS lookup tools allows.

QuietAD only ever talks to the domain controller you configure it against. There is no cloud service, no telemetry, and no dependency on QuietAD's developer for the application to function — your Active Directory data never leaves your network.

> This guide covers QuietAD 2.0.0. Screens and menu names described here match this version; a small number of details may differ in earlier or later releases.

2. Getting Started

2.1 Installing QuietAD

QuietAD is available two ways:

- **Microsoft Store** (recommended) — search "QuietAD" in the Store, or visit the listing directly. Store installs are signed by Microsoft and update automatically.
- **Direct download (.zip)** — available at quietad.online for networks where the Microsoft Store is restricted. Extract the downloaded folder completely before running `QuietAD.exe` from inside it — the application will not run correctly if the `_internal` folder is separated from the executable.

2.2 Activating Your License

On first launch, QuietAD shows an activation screen if no valid license is present. Click **Import License File...** and select the `.lic` file you received by email after purchasing a trial or perpetual license.

> Activation is entirely offline — QuietAD verifies the license file's digital signature locally and never contacts a server to check it. No internet connection is required to activate or to use the application afterward.

Once activated, your license file is stored securely on your machine and the application opens directly to the main window on subsequent launches.

2.3 Connecting to Active Directory

The **AD Connection Settings** panel at the top of the main window is always visible, regardless of which tab you're on:

Field	Description
DC IP / Hostname	The IP address or DNS name of a domain controller to connect to.
Base DN	The distinguished name of your domain, e.g. `DC=example,DC=com`.
Admin User	An account with appropriate Active Directory permissions for the actions you intend to perform.
Admin Password	That account's password.

Click **Save Credentials Securely** to encrypt and store these locally so you don't need to re-enter them every launch. Saved credentials are cleared automatically after 2 hours of inactivity, requiring re-entry before further changes can be made — this is a deliberate security measure, not an error.

> QuietAD only performs actions that the account you connect with is already authorized to perform under Active Directory's own permission and delegation model. It has no permissions of its own and cannot grant capability an account doesn't already have — an account without appropriate delegated rights will be rejected by Active Directory itself, the same as it would in ADUC or PowerShell.

3. User & Group Tab

3.1 Target Operations

Enter or browse for a **Target Username** (the Browse button opens a live search matching username, email, display name, or employee ID) and a **Target Group Name** to enable:

Add to Group / Remove from Group
Adds or removes the target user from the target group.

Unlock Account
Clears the account lockout flag for the target user.

Enable Account / Disable Account
Enables or disables the target user's account.

3.2 Move User

Enter or browse for a **Destination OU** (full distinguished name) and click **Move User to OU** to relocate the target user. The ★ button next to Browse opens your saved Favorite OUs (see Section 6.2) for one-click selection.

3.3 Group Lookup

Enter or browse for a group name and click **View Members** to see its full membership list, along with the group's description if one is set. From the results window you can **Export to CSV** — useful for audits or attaching to a support ticket.

3.4 Bulk Group Membership

Paste a list of usernames (one per line) into the text box, specify a **Target Group**, and use **Bulk Add to Group** or **Bulk Remove from Group** to apply the change to every listed user in one action. A results log shows the outcome for each username individually — useful when onboarding a group of new hires or cleaning up access after a reorganization.

4. Computer Tab

4.1 Computer Operations

Enter or browse for a **Target Computer Name** and a **Destination OU** to enable:

Move Computer to OU
Relocates the target computer object.

Delete Computer
Permanently removes the computer object from Active Directory. This action cannot be undone.

Enable Computer / Disable Computer
Enables or disables the target computer's account.

4.2 Retrieving LAPS Passwords

Click **Retrieve LAPS Password** to look up the local administrator password for the target computer. QuietAD supports both legacy LAPS (`ms-Mcs-AdmPwd`) and the newer Windows LAPS attribute, including detection of encrypted Windows LAPS passwords (which QuietAD will report as present but cannot decrypt, since decryption requires infrastructure beyond a simple LDAP read).

> LAPS retrieval requires an encrypted (LDAPS, port 636) connection to the domain controller — Active Directory itself refuses this operation over plain LDAP regardless of the connecting account's permissions. Ensure port 636 is reachable from the machine running QuietAD.

4.3 Bulk Computer Operations

Build a list of computers by pasting names directly, using **Browse & Add...** to search and add them individually, or **Import CSV/TXT...** to load a list from a file. **Bulk Move to Destination OU** and **Bulk Delete** apply to every computer in the list, using the Destination OU field from Section 4.1 for moves. A results log reports success or failure for each computer.

5. Helpdesk Tab

The Helpdesk tab is designed for the specific, recurring workflow of a support call: understanding an account or computer's current status before taking any action on it.

5.1 User Lookup

Search by username, email, display name, or employee ID. If more than one result matches, a picker lets you choose the correct one. The results window shows:

- Enabled/disabled status and lockout status (color-coded)
- Email, title, department, manager, and OU
- Description, password-last-set date, and last logon
- Full list of group memberships
- Copy buttons for the username and full distinguished name

5.2 Computer Lookup

Search by computer name or DNS hostname. Results show enabled/disabled status, operating system and version, DNS name, OU, description, last logon, and creation date.

5.3 Locked-Out Accounts

Click **Refresh Locked-Out List** to see every currently locked-out account under your Base DN in one list, rather than checking usernames individually. Select an account and click **Unlock Selected** to clear its lockout directly from this list.

> This report is based on the `lockoutTime` attribute. It may briefly still list an account whose lockout has just expired naturally but hasn't yet had an authentication attempt against it — this is standard Active Directory behavior, not a QuietAD defect.

5.4 New User

Create a new Active Directory user by providing:

Field	Notes
First Name / Last Name	Used to build the display name and CN.
Username (sAMAccountName)	Must be unique in the domain.
Initial Password	Set over an encrypted connection (see note below).
Destination OU	Full distinguished name; supports Browse and the ★ Favorites picker.

Check **User must change password at next logon** to require the new user to set their own password on first login — enabled by default and recommended for most use cases.

> Like LAPS retrieval, creating a user with a password requires an encrypted (LDAPS, port 636) connection — Active Directory refuses password-related writes over plain LDAP.

6. Settings Tab

6.1 OU Restrictions

By default, QuietAD is unrestricted — a fresh install can move, enable, or disable objects in any OU the connecting account has permission to touch. The Settings tab lets an administrator optionally scope this down, independently for Users & Groups and for Computers:

1. Check **Restrict Move User / Enable / Disable Account to specific OUs** (or the Computers equivalent)
2. Click **Add OU...** and browse to select one or more allowed OUs
3. Once enabled, any Move or Enable/Disable action outside the allowed OUs is blocked, and OU browse pickers only show the allowed locations

> This setting is a convenience layer for delegating safe, limited use of QuietAD to junior staff — it is not a replacement for Active Directory's own permission model, which remains the actual security boundary regardless of this setting.

6.2 Favorite OUs

Bookmark frequently-used OUs here to make them available as a one-click ★ quick-pick next to every Destination OU field in the application, avoiding repeated tree navigation for the same locations.

7. Security & Data Handling

- **Credentials** — saved admin credentials are encrypted on disk and never transmitted anywhere.
- **Audit logging** — every action is logged to a shared folder you choose on first run, with automatic local fallback if that folder is unreachable. Logs are never sent to QuietAD's developer.
- **Idle timeout** — saved passwords clear automatically after 2 hours of inactivity.
- **License verification** — fully offline, using Ed25519 digital signatures; no network call is made to validate a license.
- **Confidential operations** — password resets, new-user password creation, and LAPS retrieval use an encrypted LDAPS connection, as required by Active Directory itself.

Full detail is published at quietad.online/security.php, including known limitations (no third-party security audit has been performed to date, and the application is not yet code-signed for direct downloads outside the Microsoft Store).

8. Verifying Your Copy of QuietAD

Click **About / Verify Integrity** in the footer of the main window to see your license details and a live SHA-256 hash of the running executable. Compare this hash against the one published for your version at quietad.online to confirm your copy hasn't been modified or corrupted since release.

9. Troubleshooting

Symptom	Likely cause / fix
Cannot connect to domain controller	Confirm the DC IP/Hostname is reachable from this machine and that LDAP (389) is not blocked by a firewall.
"Access denied" performing an action	The connecting account lacks delegated AD permissions for that object or OU. This is Active Directory's own permission check, not a QuietAD error — verify delegation for the account you're using.
LAPS retrieval or New User creation fails	These require LDAPS (port 636). Confirm this port is open between this machine and the domain controller.
License not recognized after reinstalling or updating	QuietAD stores its license and settings in `%LOCALAPPDATA%\QuietAD\`. If this folder was cleared, re-import your license file.
An OU-restricted action is blocked unexpectedly	Check the Settings tab — an admin may have scoped Move/Enable/Disable actions to specific OUs.

10. Frequently Asked Questions

Does QuietAD require an internet connection?
No, other than during initial download/installation. Both AD operations and license activation are fully offline.

Can one license cover multiple machines?
Yes — a perpetual license covers unlimited machines within a single organization, with no per-seat counting.

Does QuietAD send any data to its developer?
No. QuietAD has no telemetry. Your Active Directory data, credentials, and logs never leave your network.

Can QuietAD do more than my AD account already allows?
No. Every action is checked by Active Directory's own permission system; QuietAD cannot bypass or exceed the connecting account's actual delegated rights.

11. Getting Support

Email support@quietad.online with questions, issues, or feedback. Include your license's organization name and the QuietAD version (visible in About / Verify Integrity) to help us assist you faster.