VPN Access Troubleshooting Procedure (KB)

Version: 1.0 | Last updated: 2026-01-22 | Owner: IT Support

Purpose

Provide a consistent first-line procedure for resolving VPN access issues reported via email/tickets.

Scope

Applies to all employees using the corporate VPN client on Windows/macOS.

Symptoms (common)

- Cannot connect / connection timed out
- "Authentication failed" / wrong password
- "Account locked" / MFA failure
- VPN connects but internal apps are unreachable

Required info to collect

1) Username / email
2) Device OS (Windows/macOS) + VPN client version
3) Error message (exact text or screenshot)
4) Network type (home/corporate/mobile hotspot)
5) Time issue started + whether it worked before

Step-by-step resolution

Step 1 — Check service status
- Verify if there is an ongoing incident or planned maintenance.
- If incident exists, link ticket to incident and stop at Step 6.

Step 2 — Basic client checks
- Ask user to restart VPN client and try again.
- Confirm correct VPN profile/hostname is selected.

Step 3 — Credentials & MFA
- Confirm password reset was not recently performed.
- Ask user to re-authenticate and complete MFA.
- If repeated MFA failures → proceed to Step 5.

Step 4 — Network/DNS checks
- Ask user to try a different network (hotspot) if possible.
- If only corporate Wi■Fi fails, escalate as network issue.

Step 5 — Account lock / access verification
- Check if the account is locked in IdP/AD.
- Unlock account if policy allows; otherwise escalate to IAM.

Step 6 — Escalation criteria
Escalate to L2/Network if ANY:
- multiple users affected
- VPN service appears down