QUICK START V26.07.27.1120 DENSEDEFENSE · FORTEFIDE

ForteFide Quick Start

Install, license, and run your first engagement — recon, scan, remediate, signed evidence — in about 30 minutes.

- Technical scan · Free tier
- Auto-remediation · licensed
- Signed evidence package · licensed
- Online license check · off by default

How to install and open the dashboard

LINUX

`sudo dpkg -i ForteFide_Setup_26.07.27.1120_linux.deb` — native ELF, no Python runtime needed on the host

WINDOWS

Run `ForteFide_Setup_26.07.27.1120_Windows.exe` as Administrator (Inno Setup wizard; installs to `C:\Program Files\ForteFide`)

OPEN

Browse to `http://127.0.0.1:5000` — first launch, set a password for the built-in ForteFideAdmin account (loopback-only; sign-in remembered 30 days)

LICENSE

Drag your `license.key` onto the LICENSE panel top-right, or use the claim link in your purchase email

CONTENTS

---

1 · Pre-flight check

ForteFide runs on one machine and reaches out to your CMMC-scoped systems over SSH (Linux) or WinRM (Windows). It does not need internet connectivity once licensed.

ITEM	LINUX HOST	WINDOWS HOST
OS	Ubuntu 22.04 / 24.04, Debian 12 (or compatible)	Windows 10 / 11, Server 2016–2025
RAM	1 GB free	1 GB free
Disk	500 MB	500 MB
Privileges	sudo / root for install	Administrator for install
Inbound	TCP 5000 (loopback only)	TCP 5000 (loopback only)
Outbound	TCP 22 to Linux targets, TCP 5985/5986 to Windows targets	Same

Tip — The dashboard binds to `127.0.0.1:5000`. Nothing is exposed to your network until you explicitly change the bind address. Browse from the same machine ForteFide is installed on.

What you should have on hand

- Your ForteFide `license.key` file (sent by email after purchase)
- An admin credential for at least one target (used once during Prep, then never again)
- Either your Active Directory domain + a DC IP + domain-admin credentials (recommended — ForteFide queries AD for the authoritative computer inventory), or a CIDR / host list for the systems in your CMMC scope (fallback when AD is not the source of truth)

2 · Install ForteFide

Linux (.deb)

ForteFide v26.07.27.1120 ships a single self-contained Linux .deb bundling Layer 1 airgap packages for the major distro families (Windows + RHEL + Ubuntu + Debian + SUSE + Arch). One download, every supported distro covered.

```
sudo dpkg -i ForteFide_Setup_26.07.27.1120_linux.deb
```

- Native ELF binary — no Python runtime needed on the host
- Installs to `/opt/fortefide`, with state under `/var/lib/fortefide` and logs under `/var/log/fortefide`
- Unattended (`DEBIAN_FRONTEND=noninteractive`) installs accept the EULA implicitly; otherwise you'll be prompted

Outlier distros: download an expansion bundle (Debian / SUSE / Arch)

If you installed CORE and your fleet has Debian, SUSE, or Arch hosts, ForteFide detects this during recon and tells you which expansion to download.

1. Run discovery / recon against your fleet (see §4)
2. Visit `/api/expansions/required` in the dashboard, or via curl — ForteFide enumerates uncovered distros and emits exact download URLs
3. On a connected machine, download the bundle + `.sig` from `densedefense.com/expansions/`
4. Sneakernet to the airgapped scanner
5. Drop the `.tar.xz` onto the dashboard (or `POST /api/expansions/install`). ForteFide verifies the Ed25519 signature locally and extracts to `/opt/fortefide/packages/`
6. Re-scan; the new distro support is picked up automatically

Note — ForteFide on the scanner never reaches densedefense.com — not for the .deb, not for the bundle, not for the license, not for updates. Your connected machine downloads; you sneakernet to the scanner. 100% standalone airgap is the canonical mode.

Windows (.exe)

Supported: Windows Server 2012 R2, 2016, 2019, 2022, 2025; Windows 10 (Pro / Enterprise); Windows 11. The .exe is Nuitka-compiled and Inno Setup wrapped, ships the full Layer 1 distro packages bundle, and has zero Python runtime dependency on the host.

- **Interactive install** — right-click `ForteFide_Setup_26.07.27.1120_Windows.exe` and "Run as Administrator". The wizard prompts for the install path (default `C:\Program Files\ForteFide`), then completes; the browser auto-opens to `http://localhost:5000`.
- **Silent / scripted install** — `ForteFide_Setup_26.07.27.1120_Windows.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /LOG=ff-install.log`. Append `/DIR="D:\Apps\ForteFide"` to override the binary path. Exit code 0 = success.
- **Install layout** — binary at `C:\Program Files\ForteFide\fortefide.exe`. State (license, scans.db, keys, journal, reversion, certs) under `C:\ProgramData\ForteFide\`. Logs at `C:\ProgramData\ForteFide\logs\`.
- **Process model** — the dashboard is a foreground process, not a Windows Service in this version. On Server / RDP the .exe detaches from the console — closing the console window does not stop it. Stop cleanly with `Stop-Process -Name fortefide -Force`. For boot-survival, wrap with Task Scheduler ("Run whether user is logged on or not") or NSSM.
- **Firewall** — Inno Setup adds an inbound "ForteFide Dashboard" rule scoped to `fortefide.exe` on the chosen port. Loopback-only by default.

High-impact — Back up your license before reinstalling the .exe. Unlike Linux `dpkg -i` (which preserves `/var/lib/fortefide` during upgrade), the Windows installer is a fresh install every time — it proactively deletes any `license.key` from `C:\ProgramData\ForteFide\`, `C:\Program Files\ForteFide\`, and `%USERPROFILE%\.fortefide\` before extracting the new build. Keep `license.key` off the scanner host — USB stick, password manager, wherever — before running the installer a second time.

Pre-accept the EULA (optional, Linux only)

If you're scripting the install or running it from a CI runner:

```
sudo mkdir -p /var/lib/fortefide
sudo bash -c 'date > /var/lib/fortefide/.eula_accepted'
```

Verify the service is up

```
# Liveness — the login page is public (no token needed); expect HTTP 200:
curl -s -I http://127.0.0.1:5000/login | head -1
```

```
# Health + version — /api/* is for automation; pass the internal API token:
TOKEN=$(sudo fortefide --show-token)
curl -s -H "X-Auth-Token: $TOKEN" http://127.0.0.1:5000/api/health
# Expect: {"status":"ok","version":"26.07.27.1120",...}
```

3 · Open the dashboard and activate

The dashboard is protected by a login. Every action — scan, remediate, rollback, license import — is behind it, so neither a second person on your network nor a website you happen to visit can drive ForteFide even though it's running.

- **First launch** — open `http://127.0.0.1:5000` on the scanner host and set a password for the built-in **ForteFideAdmin** account (at least 12 characters). You don't pick a username — there's one account. One-time step.
- **After that** — sign in as ForteFideAdmin with that password. Your sign-in is remembered for 30 days on each machine, so day-to-day you won't be asked again.

> **Tip — From another computer.** The dashboard is loopback-only, so tunnel the port over SSH first — `ssh -L 5000:localhost:5000 <scanner-host>` — then browse to `http://localhost:5000` and sign in as ForteFideAdmin with the same password.

Without a license

- ForteFide runs in scanner-only mode: a 79-control technical scan over NIST SP 800-171 Rev. 2 (of 110 CMMC L2 practices), no time limit
- Remediation, evidence collection, and endpoint preparation are gated behind a license

Activate

Your `license.key` file is the literal cryptographic anchor that makes evidence verifiable — not a license number you copy somewhere. Treat it like a private key, because it is one. Three ways to activate; pick whichever matches what you got:

- **File (most common)** — click the LICENSE panel in the topbar. A compact popup opens; drag your `license.key` onto the dashed box, or click it to open a file picker.
- **Online claim link** (post-purchase email) — click "Claim your license". The dashboard auto-detects the `?claim=<token>` URL parameter, POSTs to `/api/claim-license`, exchanges your machine fingerprint + token with license-api, and the signed key arrives automatically.
- **Activation code** (legacy flow) — click "Manage license" (full screen), paste the code in the activation field.

Verification happens locally on your machine for the file path — no outbound network call required.

- Linux: `/var/lib/fortefide/license.key`
- Windows: `C:\ProgramData\ForteFide\license.key`

- Your license is cryptographically bound to this machine's fingerprint (hostname + machine_id + disk_serial + cpu_id + system_uuid + mac + os) and cannot be used elsewhere without a support-mediated transfer

> **High-impact —** License = key = proof. `license.key` is the trust anchor for every signed evidence package you generate — the math simply fails if it's used anywhere else. Before any uninstall, back up two things to durable storage: (1) `license.key`, (2) the signed evidence package(s) you need to retain. Uninstall (`dpkg --remove` or `--purge`) wipes both by design — leave-no-trace doctrine. Upgrade (`dpkg -i` over existing) preserves everything.

Optional: online license verification

ForteFide is offline by default. If your environment allows outbound HTTPS and you'd like the dashboard to surface license status changes from DenseDefense (cancellation, refund, warranty withdrawal), enable Online license verification in Settings.

- Off by default — airgap-safe and CMMC-classified-environment-safe out of the box
- When on, ForteFide periodically asks `verify.densedefense.com` whether your license is still active
- Does not change how scans, remediation, or evidence generation work
- Adds one outbound destination: `verify.densedefense.com` on HTTPS / port 443
- Can be turned off again at any time

4 · The 6-step customer journey

ForteFide is structured around a single end-to-end flow. You walk it once per engagement. Every step is reversible, and the host is left in its original state when you're done — the leave-no-trace doctrine.

#	STEP	WHAT HAPPENS
1	Recon	Three modes in one panel: Active Directory (LDAP query against your DC — recommended), Network Scan (CIDR probe), or Jump Host (proxy through a bastion). Results render in the same panel for review before you advance.
2	Prep	Create a service account on each target and deploy a cert + SSH key. One-time use of the admin password. The click to advance from Recon is explicit ("Continue to Prepare →").
3	Scan	Run the 79-control technical scan over the prepared (or manually-credentialed) targets. Authenticated mode auto-flips to Certificate (Zero Trust) once Prep succeeds.
4	Remediate	Apply automated fixes for failed controls. Smart ordering runs safe controls first, connectivity-affecting ones last.
5	Evidence	Baseline is auto-collected after the first scan; after the rescan you click COLLECT FINAL EVIDENCE for the Ed25519-signed final package — SSP, POA&M, SPRS scorecard, per-control evidence, 14 family policies, and signed attestation PDFs. Sealed for C3PAO.
6	Out (rollback / teardown)	Rollback restores any remediated control to its baseline. No-op rollbacks (target already at baseline) are labeled "no-op" instead of "FAIL". Auto-rescan runs after rollback so the scorecard reflects current state.

Step 1 — Recon

Three discovery modes in one panel. Pick the tab that matches where your authoritative inventory lives:

TAB	USE WHEN	WHAT YOU PROVIDE
Active Directory	Your fleet is domain-joined (the common case for any CMMC contractor). AD has the authoritative computer list.	DC IP + domain name + admin username + password
Network Scan	AD is not the source of truth, or you want a port-and-OS sweep across a subnet to find unmanaged endpoints.	CIDR range (e.g. 10.0.0.0/24) or comma-separated host list
Jump Host	Targets are behind a bastion / not directly reachable from the scanner. ForteFide tunnels discovery through SSH.	Jump host address + SSH creds, then a remote CIDR or AD config to enumerate behind it

- When discovery completes, review the results and deselect anything that isn't yours, then click "Continue to Prepare →" — ForteFide never auto-jumps past the recon results

- ForteFide identifies live hosts and best-guesses their OS family from open ports + service banners + AD attributes
- Persistent out-of-scope list: mark IPs or hostnames as out-of-scope once (build hosts, jump boxes, printers) and ForteFide filters them out of every future discovery

Step 2 — Prep

Prep sets up ForteFide's 3-tier auth chain on each target. ForteFide deploys all three and tries them in order on every subsequent operation, falling back automatically:

TIER	LINUX ORDER	WINDOWS ORDER	USED WHEN
1	SSH client cert (FF CA)	SSH key over OpenSSH + PowerShell	Default for all post-Prep ops
2	SSH key (authorized_keys)	WinRM certificate (HTTPS 5986)	When the Tier-1 method is rejected
3	Password (SSH)	Password (WinRM NTLM)	Bootstrap during Prep; fallback when 1+2 fail

- Enter the admin credential once in the sidebar. ForteFide uses it to bootstrap Prep, install `fortefide-svc`, deploy Tier 1 (cert) + Tier 2 (ssh key), arm the watchdog, then drops back to its installed identity. Your admin password doesn't transit the network again after Prep.
- Prepare deploys the in-OS watchdog (Linux). If a remediation later breaks SSH for 15+ minutes, the watchdog reverts the change so you're never stranded. Reverse-commands run LIFO, and a heartbeat every 5 minutes means walking away after Remediate no longer triggers a revert.
- Firewall remediations (AC.L1-3.1.20, SC.L1-3.13.1, SC.L2-3.13.6, SC.L1-3.13.5) require a signed operator acknowledgment via `POST /api/firewall-ack` before they'll run.
- Free / scanner-only tier: skip Prep, enter scan credentials manually in Step 3 — ForteFide will still try Tier 3 (password) but not deploy Tier 1/2.

Step 3 — Scan

- Pick Full (79 controls scanned) or Quick (light port-only) and press EXECUTE SCAN
- Live progress streams into the right pane; results land in the score cards on completion
- If you prepped, no credentials needed here — ForteFide reuses the deployed auth

Step 4 — Remediate

- After a scan, the Remediate panel summarizes auto-remediable vs manual-only failures
- Click REMEDIATE ALL AUTO CONTROLS to apply every safe fix in one batch

- Each change is journalled to `/var/lib/fortefide/journal/remediation.jsonl` so it can be rolled back later (durable across restarts)
- Manual-only controls (AT/PE/PS family items) get attestation prompts in Step 5

COVERAGE	COUNT
Automated technical scan	79 of 110
Manual attestation only (AT / PE / PS)	31
Safe auto-remediation available on Linux	67
Safe auto-remediation available on Windows	66
Auto-remediable on both Linux and Windows	51
Auto-remediable on at least one OS	82

Lockout-warning controls (read carefully before clicking ACK)

Four Linux controls — SSH cipher hardening (SC.L2-3.13.8), SHA512 password hashing (IA.L2-3.5.10), password expiry (IA.L2-3.5.8), and session-locking (AC.L2-3.1.11) — could lock you out of the target if applied wrong. ForteFide pauses with a prominent modal:

```
If this change is made, you will lose rollback option
```

These four controls intentionally have no rollback path — because if they break access, ForteFide can't roll them back for you either. Read the prompt. If you're sure, click ACKNOWLEDGE. If not, skip the four and remediate them by hand later. Rollback works for every other auto-control.

Tracking remediations — the ROLLBACK button

When the journal has open entries, the topbar shows a ROLLBACK button with a count badge. Click it for a side-panel with per-target breakdown and "Rollback all" or per-target rollback. Survives restart; the count is read from the durable journal, not browser state.

Diagnosing failures — the REPORT button

The topbar REPORT button opens the Failure Report modal: every failure ForteFide has recorded (across scan, remediate, prepare, watchdog deploy) bucketed into 11 categories — timeout, ssh-fail, auth-fail, sudo-fail, command-not-found, network, layer1-missing, exit-code, permission, watchdog-deploy, license. Download as CSV. Backed by `GET /api/failure-report` (also reachable via the standalone `lab_tools/failure_report.py` without the FF service running).

Step 5 — Evidence

- Baseline evidence is auto-captured the moment your first scan finishes
- After remediation + rescan, click COLLECT FINAL EVIDENCE on the green banner
- Output is a signed ZIP with SSP, POA&M, SPRS scorecard, per-control evidence, and 14 family policies. The entire package is Ed25519-signed with your license-derived key. Your C3PAO verifies offline — no vendor server in the trust path.
- Manual-control attestation: the 31 organizational controls (AT/PE/PS/Other families) are not auto-passed. ForteFide emits ATTESTATION_REQUIRED for each and generates signed per-family attestation PDFs for your wet-ink sign-off, plus a sealed Attestation Index. The 79-control automated score is unchanged — manual controls are excluded from the denominator.
- Scanner-only tier captures unsigned baseline only; signed evidence requires a license

Step 6 — Out (rollback / teardown)

- ROLLBACK ALL on the Remediate panel reverts every change applied in this session
- ROLLBACK ALL FROM JOURNAL covers changes from earlier sessions (durable journal)
- TEARDOWN removes the ForteFide service account from every prepared target

Tip — Auto-teardown is off by default. Earlier builds tore down service accounts at the end of every scan — that broke multi-target remediation. Teardown is operator-triggered: click the Teardown button, or `POST /api/teardown-endpoint`, when the engagement is done.

High-impact — If a remediation locks you out of a host: console into the target as root (vSphere web console, IPMI, iDRAC, BMC, or physical keyboard) and run `sudo /var/lib/fortefide/emergency-revert.sh`. The script restores the pre-engagement snapshot ForteFide took during Prepare, reload-restarts sshd, verifies port 22 is listening, disarms the watchdog, and prints a status summary — pure POSIX shell, no ForteFide running required, no network required, no hypervisor adapter required. After SSH is back, click ROLLBACK in the dashboard to flush the journal.

5 · Reading your first scan result

When the scan finishes, the asset scorecard above the tab nav fills in. Each prepared host is one asset scorecard; the overall fleet roll-up sits across the top. These are your top-line numbers.

CARD	WHAT IT TELLS YOU
Compliance %	Pass rate across the 79 scanned controls in scope for this scan. SPRS-aligned: each NOT MET deducts 1, 3, or 5 points by severity.
Controls Passed	Raw count out of 110.
Total Findings	Number of failed-control + manual-attestation rows.
Critical	5-point deductions. Address these first.
High	3-point deductions.
Medium	1-point deductions.
Low	Informational; usually no SPRS impact.

Tabs under the score cards

- Overview — donut chart, host list, family pass-rate bars
- Family Breakdown — every one of the 110 NIST 800-171 r2 controls, grouped by family (AC, AU, CM, …)
- Findings — failed controls, sortable by severity
- Attestations — the 31 manual-only controls in AT/PE/PS
- Delta / Trends — compare the latest scan to the previous one
- Compliance Timeline — score over time across all scans

Tip — Scan history is in an encrypted SQLite database at `/var/lib/fortefide/scans.db` (`C:\ProgramData\ForteFide\scans.db` on Windows). Browser refresh, service restart, even reboot — everything reloads on next dashboard open.

6 · Auth tiers in plain English

Step 2 (Prep) asks how ForteFide should authenticate to your targets going forward. There are three options. Higher tier = stronger; ForteFide falls back automatically if a higher tier is unavailable on a given target.

TIER	MECHANISM	WHEN TO USE	LONG-TERM ROLE
1	Certificate (recommended)	Default. Per-target 30-day cert signed by your license-derived CA.	Steady-state. Auto-renews.
2	SSH key (Ed25519)	Cert path unavailable; legacy SSH-only targets.	Steady-state fallback.
3	Password	Bootstrap only — only used to install the cert + key in Step 2.	Not a steady-state mode.

Tip — Tier 1 SSH cert authentication lands on 100% of supported Linux targets (Ubuntu 20/22/24, Debian 11, RHEL/Rocky/Alma/Oracle 7-9, SLES 12/15, Arch rolling, AL2023) and 100% of supported Windows targets, including Server 2012R2, 2016, 2019, 2022, 2025, Windows 10, and Windows 11. If you complete Prep and a target is still on password auth, the bootstrap didn't fully complete — re-run Prep on that target.

Note — Tier 3 is bootstrap, not operating mode. If you finish Prep and a target is still on password auth, re-run Prep — the goal is to land every target on Tier 1 (cert) or Tier 2 (key) for steady-state scanning.

7 · Common first-timer questions

What does the Teardown button do?

It removes the ForteFide service account from every target you prepared, deletes the per-target cert directory, and closes out the local journal entries. After teardown the targets look exactly as they did before Prep — leave-no-trace, both sides of the wire.

What does the Clear History button do? (top-bar, orange)

Wipes the scanner's in-memory engagement state: scans, inventory, prepared service-account records, self-heal/watchdog state, customer-action banners, and the activity log. Your license file is preserved. Two-step confirmation; if you still have prepared endpoints out there, it'll warn you that clearing without Teardown orphans those accounts on the targets. The right rhythm is Teardown first (cleans the targets), then Clear History (cleans the scanner).

What does "verified via admin-cred fallback" mean?

After remediation, ForteFide runs a verification scan to confirm each control actually moved from NOT MET to MET. Most of the time that scan authenticates as the `fortefide-svc` service account. Occasionally a hardening control locks that account out for the next connection — the verification scan falls back one step and retries using the admin credential you supplied at Prepare time. The evidence package marks the affected controls as verified-via-admin-fallback so a C3PAO auditor sees the full provenance; on the dashboard the host renders with an orange border and a "Verified-by-Admin" label.

How many SSH connections does ForteFide make to each target?

One per (engagement, Linux target). The scan and the remediation engine share a single already-authenticated SSH session that covers preflight, every control executed, every post-control liveness probe, every auto-rollback, and the post-remediation verification scan. On the wire, your network team sees a single TCP connection on port 22 per target, alive for the duration of the engagement, closed at the end — this avoids tripping sshd MaxStartups, connection -rate firewall rules, and fail2ban-style IDS, and lets remediation keep working through controls that restart sshd. Windows targets currently use one WinRM session per call.

Where are the logs?

- Linux: `/var/log/fortefide/fortefide.log`
- Windows: `%ProgramData%\ForteFide\logs\fortefide.log`
- Live tail in the dashboard: bottom-right Activity Log panel

- Run with `--debug` for verbose logging (default level is INFO)

Where is my license / cert / journal data?

- Linux: `/var/lib/fortefide/` (license.key, scans.db, keys/, journal/, reversion/)
- Windows: `%ProgramData%\ForteFide\`

Who do I email for help?

- License + billing: densedefense.com/account
- Support: support@densedefense.com
- Security disclosures: security@densedefense.com

How do I uninstall without losing my license?

```
# Back up first
sudo cp /var/lib/fortefide/license.key ~/license.key.bak
# Then upgrade in place (preserves state):
sudo dpkg -i ForteFide_Setup_<version>_linux.deb
```

Use `dpkg -i` (upgrade), not `dpkg --purge`, when reinstalling. Purge wipes `/var/lib/fortefide` and your `license.key` with it. The PRERM gate refuses uninstall when the journal has open entries unless you set `FORTEFIDE_UNINSTALL_ACK` to `rollback` / `abandon` / `cancel` — the leave-no-trace doctrine self-enforcing at the OS level.

My distro isn't in the supported list — what now?

ForteFide ships airgap-clean Layer 1 packages for Ubuntu 20/22/24, Debian 11/12, RHEL 7/8/9 (incl. Rocky/Alma/Oracle/CentOS), SUSE 15/16, and Windows. Amazon Linux 2023 is supported in connected-only mode (EC2 hosts always reach AWS internal repos — no Layer 1 staging needed). SUSE 12 and Arch Linux have partial Layer 1 today; install may succeed but specific controls might fall through to Customer Action Required. Email support@densedefense.com to request a thicken-up roadmap entry for your distro variant.

DDWitness upload returns 503 vault_not_configured

You haven't set the vault upload token yet. Sign in to densedefense.com, navigate to Account → Vault, copy your vault upload token, and POST it to `/api/vault/configure` on this scanner. DDWitness is optional — you can also skip the cloud handoff entirely and use sneakernet for evidence delivery.

DDWitness upload returns 502 vault_unreachable

Network or DNS issue between your scanner and the vault. ForteFide built the signed package locally — it's still in `/tmp/fortefide_vault_upload/`. Retry the POST manually, or switch to sneakernet evidence delivery for this engagement. The vault is optional; failing to reach it does not block your assessment.

My customer says they "lost their license.key" — now what?

Bad news: any signed evidence package they produced under that license is now cryptographically unverifiable. The packages still exist as files; the signature chain has no key to anchor against. DenseDefense does not escrow license files — this is doctrine, not an oversight. Restore from their backup if available. If not: import a new license and re-run the full prepare → scan → remediate → evidence cycle to rebuild the chain under the new license.

8 · Standalone / airgap operation

ForteFide is 100% standalone. No admin accounts beyond your existing bootstrap user. No outbound network. Licensing and updates are sneakernet.

License delivery via sneakernet

1. On a connected machine (your usual office laptop), sign in to densedefense.com and download your `license.key` file.
2. Copy `license.key` to authorized removable media (USB stick, encrypted external drive, optical media — whatever your CUI environment policy allows).
3. On the airgapped scanner host, copy `license.key` to `/var/lib/fortefide/license.key` (Linux) or `C:\ProgramData\ForteFide\license.key` (Windows). Or POST it via `/api/import-license`.
4. Restart ForteFide (stop and relaunch the process). License activation is fully offline — no callout to license.densedefense.com required. The Ed25519 signature is verified locally.

High-impact — License = key = proof. Your `license.key` file is the trust anchor for every signed evidence package you produce. Back it up to durable storage outside the scanner. Lose it and your assessor cannot cryptographically verify your evidence. DenseDefense does not escrow license files.

Updates via sneakernet

1. On a connected machine, download the new `ForteFide_Setup_<version>_linux.deb` (or .exe) from densedefense.com.
2. Copy to authorized removable media.
3. On the scanner: `dpkg -i ForteFide_Setup_<version>_linux.deb` (Linux) or run the installer (Windows). Existing `license.key`, scan history, and journal are preserved across upgrade.

ForteFide v26.07.27.1120 — CMMC Level 2 / NIST SP 800-171 Rev. 2 compliance readiness scanner, remediation engine, and signed evidence generator. Runs on one host you control and reaches your scoped targets over SSH / WinRM; no internet connectivity is required once licensed.