

YOUR COMPUTER / YOUR LINUX VM / YOUR S3 STORAGE

Launch here. Install there.

Open **Mantle-Desktop.exe** on your Windows computer. Its desktop wizard installs Matricial-sharding as a **native Linux engine managed through systemd** on your VM, then configures, starts and verifies it.

Connection

Test SSH and sudo access

Administrator + Storage

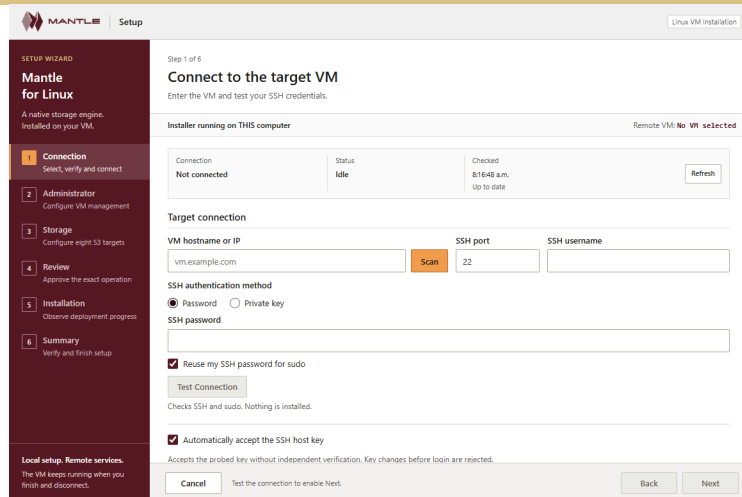
Separate account and S3
pages

Review + Installation

Explicit install and start

Summary

Services, process, mount



Connection in the six-step native desktop installer.

Portable, normal-user launcher. No Go, Node.js, PowerShell or separate SSH client is needed. Keep its window open and your computer awake during setup. Browser alternative: `Mantle-Installer.exe`.

Guide date: **2026-10-21**

Bundled Linux build: `0.3.0-dev+20261020T005000Z`

Remote runtime: October 12 source, `feature/target-repair-migration`

Linux x86-64 / systemd. Source-pinned runtime.

PREPARE ACCESS, STORAGE AND TRUST

Have these ready.

Minimum VM baseline: 4 GB RAM, 50 GB disk, 2 vCPU.

A starting baseline, not a workload-capacity promise. Allow for the OS, other files and the cache free-space requirement below.

On your computer

- ☐ A trusted Windows x86-64 PC with Microsoft Edge WebView2 Runtime.
- ☐ The trusted matching desktop executable and its checksum.
- ☐ VM address, SSH port, username and independent SSH fingerprint information.
- ☐ SSH password or private key/passphrase, plus authorized root/sudo access.
- ☐ A separate VM administrator account and S3 target credentials.

On the remote VM

- ☐ Linux x86-64 with running systemd and reachable SSH.
- ☐ Local ext4/XFS backing storage, correct clock and DNS.
- ☐ Usable kernel FUSE and enough free space for the cache budget below.
- ☐ Outbound HTTPS to all eight S3 target slots and an existing accessible bucket.
- ☐ An available management port, default 8443. No inbound 8443 firewall opening is required.

Remote prerequisites: Ubuntu 24.04 and Debian 12/13 can receive missing fuse3 and ca-certificates through apt. That requires package-network access. Other systems must already satisfy the checks.

The VM needs usable `/dev/fuse` and a trusted `setuid fusermount3`. Packages cannot override a kernel/container policy that prohibits FUSE. Neither the local user nor the VM needs a compiler to use a built launcher.

Cache is not total required space

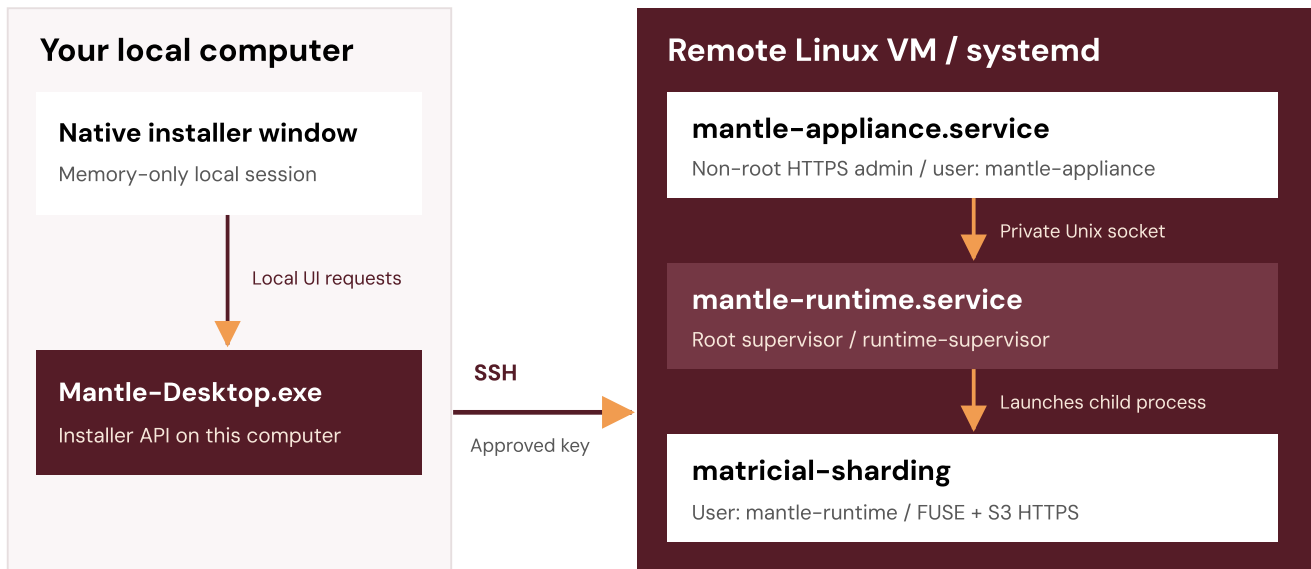
Choose a whole-number cache budget from **1 to 4096 GiB**. Preflight requires **3 × cache + 1 GiB free** for cache, FUSE scratch and reserve. The **8 GiB default needs 25 GiB free** on the backing filesystem.

This check is not a quota, reserved space or maximum file-size promise. Size for the workload and recovery operations; the VM checks available space again before starting. Eight logical S3 slots do not prove independent failure domains.

TWO SYSTEMD UNITS / ONE SUPERVISED STORAGE ENGINE

Native services, not containers.

Matricial-sharding is a native Linux executable. systemd runs a management service and a root supervisor; the supervisor launches the engine as the non-root mantle-runtime user.



The engine mounts /mnt/mantle. Closing the local installer does not stop VM services.

Figure 1. Two systemd units, not three. There is no separate matricial-sharding.service; the engine is the supervisor's child process.

Built once, installed as bytes. The build machine compiles the pinned source; the VM installer validates and extracts the embedded binary. No Docker, Git clone, compiler or automatic branch update on the VM. Management HTTPS is certificate-pinned through SSH; no initial manual tunnel is needed.

REMOTE COMPONENT / LOCATION	RESPONSIBILITY
<code>mantle-appliance.service</code>	Sandboxed, non-root web UI and management API. Default access is VM loopback only.
<code>mantle-runtime.service</code>	Root supervisor; launches the engine as the separate non-root mantle-runtime account.
<code>/opt/mantle/runtime/matricial-sharding</code>	Root-owned engine binary. Upstream LICENSE is in the same directory.
<code>/var/lib/mantle-runtime</code>	Root-private supervisor configuration, credentials and state.
<code>/srv/mantle-runtime</code>	Owned data tree: cache/, state/, tmp/, authority/. Preserve together.
<code>/mnt/mantle</code>	Verified FUSE mount; root/runtime access only.

Existing ext4/XFS storage, no disk formatting. Preserve authority, cache, metadata and storage identity together. No hosted Mantle gateway, enrollment, NFS/SMB export, bucket creation or migration is installed.

SIX STEPS / ONE EXPLICIT DEPLOYMENT

Install, then verify.

On Windows, open bin/Mantle-Desktop.exe as a **normal user**. Keep its window open and computer awake; the wizard runs locally, not on the VM.

WIZARD STEP	WHAT TO DO
1. Connection	Enter the VM address, SSH port (normally 22), user and password or OpenSSH/PEM key. Optional Scan only suggests targets. Automatic host-key acceptance skips independent verification. For manual trust, turn it off, Inspect Host Key , independently compare the full SHA-256 fingerprint and key type, then approve. Select Test Connection to check SSH and sudo without installing. Supply sudo credentials if prompted and test again; select Next only after Connection verified .
2. Administrator	Set the Mantle VM administrator username and password, separate from SSH, and confirm it. Keep management SSH-only (default port 8443); Next validates locally.
3. Storage	Use one existing bucket accessible on all eight ordered HTTPS S3 slots . Enter each access/secret key pair, the cache budget (page 2) and optional public CA PEM , never private keys. Next validates all slots.
4. Review	Check the target, administrator, management access, bucket, slot order, cache and CA. Check consent, type DEPLOY MANTLE and select Install to install, configure and start.
5. Installation	Follow bounded progress through upload, checksum, installation and verification. If interrupted or failed, inspect fresh status before any explicit retry. Upload alone is not success.
6. Summary	Require Local service verified : both systemd services active, matching runtime commit/hash, verified engine process and FUSE mount, expected applied revision and fresh timestamp. Finish disconnects local access; it does not stop the VM or its services.

Already installed? Same-build VERIFY MANTLE is read-only; RESUME MANTLE continues incomplete setup. Both require review/consent and **skip upload/install**. Different builds and unknown state are refused. No automatic retry, upgrade or rollback; inspect fresh status before authorizing recovery.

Later management access

```
ssh -N -L 127.0.0.1:8443:127.0.0.1:8443 USER@VM
```

With a trusted SSH client, replace USER@VM and verify its host key. Keep the tunnel open; visit <https://localhost:8443>. Use the installed port in both tunnel positions and the URL. Compare the full browser TLS certificate SHA-256 fingerprint with the installer's verified handover before trusting it, then sign in with the Mantle administrator. Initial installation needs no manual tunnel.

RESOLVE THE CAUSE, NOT THE SAFETY CHECK

Troubleshoot safely.

OBSERVATION	SAFE NEXT ACTION
Window / session unavailable	For launch failures, check WebView2. For an expired session, select Reopen Session . Accepted work continues; observing it does not replay deployment.
Host key changed / probe expired	For independent verification, disable automatic acceptance, inspect again and approve the full fingerprint. Approval lasts 15 minutes; disconnect before changing targets.
SSH authentication / timeout	Correct credentials and select Test Connection again. In manual mode, reapprove the valid fingerprint or inspect again if expired. For timeout, check VM/network/SSH. A failed connection test does not authorize installation.
Sudo needed / capacity unknown	Provide the separate sudo password or use an authorized root/passwordless account. Unknown preflight is not zero free space. Do not grant broad permissions just to bypass checks.
Unsupported platform / prerequisites	Require Linux x86-64, systemd, supported local storage and usable FUSE. Ubuntu 24.04 / Debian 12/13 package provisioning needs network access. No data disks are formatted.
Existing setup / different build	Same build: explicitly Verify or Resume (page 4). Different bytes, conflicting accounts/units and unknown files are refused. Preserve receipts/data; no upgrade or adoption.
Management TLS / login failure	Never bypass the SSH-derived TLS pin. For a rejected administrator login, correct inputs, reauthorize sudo if consumed, review and authorize again. Verify again is not login retry; no automatic identity reset.
Package lock / upload wait	Read elapsed time, bounded timeout and upload byte/rate/ETA evidence. Wait for apt/dpkg safely; never kill its processes or delete locks. A sent upload still needs checksum confirmation.
Configuration rejected / locked	Next reveals the page/target and its inline field error. Check all origins, paired keys, CA and capacity. First Start locks placement/cache; credential/CA changes require a fully stopped service.
Runtime failed / mount unverified	On the VM, inspect <code>sudo journalctl -u mantle-runtime</code> . Resolve the cause, then explicitly STOP FAILED START before Resume. Healthy runtimes, foreign mounts and persistence failures are excluded.
Busy / stale revision / lost response	Refresh before another explicit action; busy/stale guards still apply. Cancel clears drafts and disconnects; it does not uninstall, stop VM services, undo work or delete data. A lost response is not rollback; never replay it.

Useful support record: public handover plus attempted step, fixed problem code and current revisions. It remains copyable after Finish. Exclude access links/tokens, passwords, private/authority keys, claim codes, S3 credentials and private state.