

Cephable for IT — Deployment & Environment

What your desktop engineering team needs to evaluate and roll Cephable out in a restricted environment.



Install & packaging

- No admin rights required to install
- Installers: user-level (.exe), MSI, MSIX, Microsoft Store
- Deploy via Intune, company portal, or AD groups
- Built-in auto-updater; ships as an automatic update



Identity & access

- Single sign-on via SAML
- SCIM user and seat provisioning
- Integrates with Entra ID / Active Directory
- Seat & license management in the admin portal



Virtual environments

- Runs inside VDI / VM — Citrix, AWS
- Virtualized GPU acceleration = same performance
- CPU fallback where no virtual GPU is present
- Voice needs local audio pass-through (same as Teams mic)



System requirements

- Control + Create: 8 GB RAM
- Automate (full workloads): 16 GB RAM minimum
- Whole-machine compute — CPU, integrated GPU, GPU, NPU
- Windows (lead platform) and macOS



Governance & control

- Admin dashboard blocks or allows apps and sites
- Rules org-wide, per-team, or per-user allow-lists
- Enforced at the tool-call level — not defeatable by prompt injection
- Security by inheritance: only what the signed-in user can do



Data & telemetry

- Only auth, updates, and optional profile sync touch the network
- No inference, documents, or camera/mic ever leave the device
- Local encrypted run history; exports to JSON-L for audit
- Telemetry can be disabled org-wide