CALLLUME · A NURIQ TECHNOLOGIES PRODUCT

Deployment & Sizing Guide

Supported install paths, hardware sizing, network requirements and backup/DR for CallLume.

PREPARED FOR	DATE	DOCUMENT
CallLume Stakeholders	October 2026	OPS-DEPLOY-01

CallLume

Confidential
© 2026 NurIQ Technologies LLP

Supported install paths

PATH	DETAIL
Windows Server	MSI installer (`CallCentreOps-<version>.msi`), self-contained: bundles its own .NET runtime, PostgreSQL 16 and a VC++ runtime — no separate database install needed. Windows Server 2022 or later, 64-bit.
Linux containers	Podman (rootless, preferred) or Docker, via `docker compose` / `podman compose`. Five build targets from one multi-stage Dockerfile: api, collector, bi-gateway, tools, proxy.

Hardware sizing

4 vCPU
MINIMUM

8 GB
RAM MINIMUM

One installation serves one organisation. These are the documented minimums for the self-hosted install; call volume, retention window and recordings-index size (if the quality module is enabled) are the main drivers of storage beyond the minimum.

Network requirements

- The collector host needs access to the Avaya IP Office's SMDR port (8085) only — read access to the call-record feed, nothing else is opened toward the PBX.
- HTTPS for the application itself (`CCOPS_PUBLIC_URL` must be HTTPS for setup links to work).
- Outbound access is opt-in per feature: SMTP, Telegram, WhatsApp and browser-push are each off until an administrator configures them. No feature requires outbound access to function at a basic level — a fully offline licence file is available for sites with no internet connectivity at all.
- Optional: Tableau/BI gateway, its own bind address and port, enabled via `--profile bi`.

Installation and onboarding

1. Install (MSI or container compose); migrations are versioned and checksum-protected, applied automatically by the `migrate` service in the container path.
2. Open the private, one-time setup link (Windows: Start menu shortcut; container: `ccops setup-link`). The token is never logged and is removed from the browser's history by the wizard itself.
3. Sign in, enrol MFA, complete the onboarding checklist (groups, numbers, hours, capabilities) — or hand the customer the offline **Site Setup Questionnaire** (one HTML file, no network required) to fill

© 2026 NurIQ Technologies LLP — Deployment Guide

in beforehand; every answer is reviewed, source-badged and confirmed inside the product before anything is applied.

4. Connect the phone system (optional at setup time — "Connect later" is supported).

Upgrade

Pull/rebuild and restart (containers) or run the new MSI (Windows, in-place upgrade). Migrations never edit an already-applied migration; settings, applied presets and audit history are preserved. Exporting settings first (Settings > Presets > Export) is the documented fallback. `scripts/init-secrets.sh` is re-run after every upgrade to add any new secret a release introduces, without ever overwriting an existing one.

Backup and disaster recovery

Backups are AES-256-GCM encrypted and chunked, with a built-in restore test proving round-trip integrity rather than assuming the backup file is good. The Windows installer runs the backup agent as a scheduled task. A damaged line in the spool no longer stops the collector; an interrupted retention purge is recorded as failed rather than silently appearing to still be running.

© 2026 NurIQ Technologies LLP — Deployment Guide