
IQOPS · NURIQ TECHNOLOGIES

Deployment & Sizing Guide

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

PREPARED FOR
NurIQ Technologies Leadership

DATE
September 2026

DOCUMENT
OPS-DEPLOY-01

UPDATE NOTICE — CHANGES SINCE THE AUGUST 22 EDITION

This guide was refreshed on September 2, 2026 to reflect one material change since the original edition: a native, opt-in fleet capacity-monitoring capability shipped that is directly relevant to sizing and disk-capacity planning (see the note at the end of §2). Every other section reflects the original assessment and remains accurate as written — in particular, RHEL real (non-container) hardware verification is still pending, unchanged since the original edition.

Contents

1. Supported Deployment Paths

2. Hardware Sizing

3. Network & Ports

4. Backup & Disaster Recovery

5. Upgrades

1. Supported Deployment Paths

PATH	PLATFORMS	DATABASE	STATUS
Docker Compose	Any Linux host with Docker	Bundled PostgreSQL container	Primary/reference deployment
Native package, bundled database	Ubuntu 24.04+, Debian 12+	Companion iqdesk-postgresql-bundled package, provisioned automatically	Verified on real hardware
Native package, bundled database	RHEL / Rocky / Alma 9	Same companion-package model	Verified in a clean-room container; real (non-container) hardware verification pending — see Risk Assessment Report, R1/R8
Native package, external database	Ubuntu/Debian/ RHEL	Customer-provided PostgreSQL 16	Supported via environment configuration
Windows MSI	Windows Server 2022/2025	Windows-specific PostgreSQL vendoring (ADR-0026)	Verified on real hardware

All native paths (Debian-family and RHEL-family) resolve the same PostgreSQL/Redis/ClamAV companion-package dependency at the package-manager level — there is no nested package-manager invocation, which was a real architectural defect found and fixed earlier in the product's history (see the R16 remediation record in the engineering risk log).

2. Hardware Sizing

The platform is a single ASP.NET Core process plus PostgreSQL, Redis, and ClamAV. The starting points below are conservative recommendations for a healthy baseline, not lab-benchmarked ceilings — validate against your own endpoint count and ticket volume before a large rollout, and scale up if PatchIQ/vulnerability correlation runs against a very large software inventory.

FLEET SIZE	VCPU	RAM	DISK
Up to 100 endpoints	4	8 GB	100 GB SSD
100–500 endpoints	8	16 GB	250 GB SSD
500–2,000 endpoints	16	32 GB	500 GB SSD, consider a separately-hosted PostgreSQL instance
2,000+ endpoints	Contact NurlQ Technologies for a sizing consultation		

Endpoint agent footprint is deliberately lightweight: a background service plus a per-user tray process, no continuous high-frequency polling by default — check-in interval and bandwidth are both configurable.

Endpoint disk capacity — a separate concern from the platform's own sizing above — is monitored natively via the optional, per-tenant Capacity Management area (Agents → Capacity Management, off by default). It tracks free space per drive across the managed fleet, raises threshold-based alerts (an absolute GB floor or a free-space percentage), forecasts days-until-full from a rolling trend, and can send a scheduled digest email — no separate agent, script, or third-party monitoring tool required to plan ahead of an endpoint running out of disk.

3. Network & Ports

PORT	PURPOSE
8444 (default, configurable)	HTTPS — portal UI + REST API + agent check-in. IQOps always serves HTTPS; a self-signed certificate is auto-provisioned on first boot if none is supplied
5432 / 5433	PostgreSQL (internal to the deployment; not required to be externally reachable)

A NAT'd or Docker deployment reachable at a different address than its container's own auto-detected interfaces needs its externally-reachable address explicitly set (`IQDESK_CERT_SAN`) so the auto-provisioned TLS certificate's Subject Alternative Name list actually matches what agents connect to — documented as ADR-0027, not an oversight.

4. Backup & Disaster Recovery

A scheduled backup service runs on a configurable interval, using a dedicated backup database role (`BYPASSRLS`, used only for backup, never by the running application) so a backup is always complete regardless of tenant-scoping. Backups are protected by a crash-safe advisory-lock mechanism preventing two backup jobs from racing each other across a multi-process deployment. Cloud-provider backup targets (AWS/Azure/GCP) are supported at the provider-logic level. On-demand rollback is available for PatchIQ-managed deployments specifically, independent of the general backup schedule.

5. Upgrades

Native-package upgrades use the platform's own package manager (`apt/dnf`) against the same companion-package dependency chain as install. The Windows MSI uses a major-upgrade path that preserves machine identity and configuration. The endpoint agent's own self-update uses a blue-green atomic directory swap with automatic rollback on a failed health check after the swap — not an in-place file overwrite — so a bad agent build cannot leave a managed endpoint in a half-updated state.