

FOR IT & INFRASTRUCTURE TEAMS

Corvexa — Technical Specification & System Requirements

A reference for what it actually takes to host and run Corvexa: runtime and server requirements, network and security architecture, data storage, and the web interfaces operators, administrators, and visitors use — so your team can plan a deployment before a single license is signed.

Deployment Model

Corvexa is a self-hosted application that runs on infrastructure your organization controls — it is not a multi-tenant SaaS product. It's deployed on a server or virtual machine on the same network (or a routed/VPN-connected network) as the video, access control, intrusion, and life-safety subsystems it integrates with, since those systems typically live on a private site network rather than the public internet.

On-premises — the primary, expected model: a server or VM inside your own facility network, alongside the subsystems it connects to.

Customer-controlled cloud — a VM in AWS, Azure, or any other cloud is fully supported, provided network connectivity back to on-site subsystems is solved (site-to-site VPN, Direct Connect / ExpressRoute, etc.).

Server & Runtime Requirements

COMPONENT	REQUIREMENT
Runtime	Node.js $\geq$ 18.0.0
Operating system	Any OS Node.js runs on (Linux, Windows, macOS). Linux is the typical production target.
Application dependencies	express, qrcode
Database server	None required. Persistence is file-backed (append-only NDJSON event/audit logs plus JSON configuration files) under one data directory — no separate database to install, patch, or back up.
Web server (application)	Built-in Node/Express HTTP server. Speaks plain HTTP only — TLS is terminated externally (see Network & Security).
Reverse proxy	Required for production. A ready-to-adapt nginx reference configuration is provided.
Outbound connectivity	To each integrated subsystem's own network endpoint (VMS, access control, intrusion, BAS) — scoped per connector, not a blanket internet requirement.

Dependency footprint is deliberately minimal by design — everything beyond HTTP routing (express) and visitor-pass QR generation (qrcode) is built on Node's own standard library, so there are fewer third-party packages to patch or audit.

Suggested Hardware Starting Point

Not a vendor-certified minimum. No fixed CPU/RAM/disk requirement is published — Corvexa is a lightweight, single-process application, and the right size depends on device count, event volume, and how many operator/admin sessions stay connected simultaneously. The figures below are a reasonable starting point for a planning conversation; our Site Assessment (see back page) right-sizes this to your actual environment.

DEPLOYMENT SIZE	ILLUSTRATIVE STARTING POINT	TYPICAL FIT
Single site	2 vCPU · 4 GB RAM · 20 GB disk	One facility, a few dozen devices, one operator console at a time
Multi-site / campus	4 vCPU · 8 GB RAM · 50+ GB disk	Several buildings or sites, higher event volume, multiple concurrent consoles

Disk usage grows with event-log retention and uploaded floor-plan images (see Data & Storage) — size for your retention policy, not just today's footprint.

Network & Security Architecture

ASPECT	DETAIL
Default listen port	4000 (HTTP)
TLS	Not terminated by the application. Terminate HTTPS at a reverse proxy (nginx reference config provided) and proxy plain HTTP to the app.
Real-time updates	Server-Sent Events (SSE) on /api/stream — no WebSockets are used anywhere, which simplifies firewall and proxy rules. Your reverse proxy must disable response buffering and allow a long read timeout on this route , or real-time push breaks silently.
Request body limit	15 MB, sized to fit a base64-encoded floor-plan image upload (~11 MB max image).
Authentication	HMAC-signed session tokens (JWT-alike, not a general-purpose JWT library). No password store — the sign-in directory is a stand-in for your real identity provider (AD/SAML/OIDC) until that integration is scoped.
Authorization	Three-tier role model — operator < supervisor < admin — enforced on every route.
Admin workstation restriction	Optional: restrict the admin role to a single allow-listed source IP.
Console IP allowlist	Optional: restrict the entire authenticated console/API to a set of allow-listed source IPs (the public visitor-kiosk endpoints are exempt by design).
Production safety check	The server refuses to start in production if default signing secrets or a development auth bypass are still in place — a misconfiguration can't accidentally reach production silently.

Key Configuration Variables

VARIABLE	PURPOSE	REQUIRED?
PORT	HTTP listen port	Optional — default 4000
NODE_ENV	Set to production to enable startup safety checks	Optional — default development
DATA_DIR	Root directory for all persisted data	Optional — default ./data
JWT_SECRET	Signs session tokens	Required in production
LICENSE_SIGNING_SECRET	Signs/verifies the license key	Required in production
SESSION_TTL_HOURS	Session token lifetime	Optional — default 12
TRUST_PROXY	Enable when running behind a reverse proxy, so client IPs resolve correctly	Optional
CONSOLE_ALLOWED_IPS	Comma-separated console/API IP allowlist	Optional
ADMIN_WORKSTATION_IP	Single IP the admin role is restricted to	Optional
*_MODE	Per-connector mock/live switch (video, access control, intrusion, BAS) — lets a connector run simulated before it's pointed at a live system	Optional — default mock

Each live connector (video management, access control, intrusion receiver, BAS email ingestion) takes its own endpoint and credential configuration once you're ready to point it at a real subsystem — scoped during systems integration, not listed exhaustively here.

Data & Storage

Everything Corvexa persists lives under a single configurable data directory — there is no external database to provision, patch, or back up separately.

DATA	FORMAT	NOTES
Event log	Append-only NDJSON	Every raw event from every connected subsystem
Audit trail	Append-only NDJSON	Every user and system action, from detection to resolution
SOPs, users, org settings	JSON	Loaded at boot, flushed to disk on every change
Floor plan images	PNG / JPG / SVG	One per building, up to ~11 MB each
License key	Signed key file	Installed once per deployment

Backup is a file-level operation. Because every piece of state lives under one directory on disk, backing up Corvexa is the same as backing up any other application data folder — no database dump/restore procedure to script separately.

Web Interfaces & Browser Requirements

Corvexa is delivered entirely as web pages — there is no desktop or mobile app to install. Every interface runs in a standard, current browser.

INTERFACE	WHO USES IT	BROWSER / DEVICE REQUIREMENT
Operator Console	Operators, supervisors, admins	Any current evergreen browser (Chrome, Edge, Firefox, Safari) with Server-Sent Events support — standard in all of them.
Visitor Kiosk	Front-desk / lobby tablet	Same, plus camera access (getUserMedia) when the organization requires a badge photo — this also requires the page be served over HTTPS, which the standard reverse-proxy setup already provides.
Guard Tour App	Patrol / mobile guard staff	Any current mobile or desktop browser — a lightweight page, no camera or location APIs required.
On-Call App	On-call / after-hours staff	Any current mobile or desktop browser with Server-Sent Events support.

No native app install

No plugins

No WebSockets to allowlist

Licensing

Corvexa's license is time-based (a fixed term or perpetual, tied to your organization name) — it is **not** metered by device count, connector count, or concurrent user seats under the current licensing model. Scaling to more devices, more sites, or more operators does not require a new license tier on that basis alone; capacity planning is a hardware/network conversation (see Suggested Hardware Starting Point), not a licensing one.

What This Means for Your Rollout

- No database server to stand up, patch, or license separately.
- A single reverse proxy (config provided) handles TLS and the one SSE-specific setting that matters.
- New connectors run in simulated mode first — your team validates correlation logic and SOPs before a single credential touches a live system.
- Everything your operators, admins, and visitors use is a web page — no fleet of native apps to package, sign, or push updates to.

Ready to scope your environment?

Our Site Assessment reviews your subsystems, network topology, and expected event volume, and right-sizes the deployment before anything is installed.

info@e2securityconsulting.com
(754) 732-8290