CHAINNODE · WELCOME PACKAGE

Dashboard Operator's Manual

The complete operator's guide to real-time asset intelligence, blockchain-verified compliance, and fleet optimization.

Version	Audience	Platform	chainnode.pro
1.0	Licensed Operators	ChainNode	Welcome Package

ChainNode Dashboard — Operator's Manual

Version 1.0 · For Licensed Operators of the ChainNode Platform

Welcome to ChainNode. This manual explains every screen, control, and workflow in your dashboard, and shows you how to get the most out of the platform. Read it once end-to-end before deploying agents into production — the five minutes you spend here will save hours later.

---

1. What ChainNode Does (and Why It Matters)

ChainNode is a real-time asset intelligence and compliance platform. It continuously discovers every physical device, IoT sensor, network node, virtual machine, and software license operating inside your environment, records their configuration fingerprints on the **Polygon blockchain**, and alerts you the moment anything changes.

You get three things no traditional asset manager provides:

1. **Tamper-proof evidence.** Every configuration snapshot is hashed and written on-chain. Auditors, insurers, and regulators can independently verify that a device has not been altered since the hash was recorded.
2. **Live discovery.** New devices appear in your fleet within seconds of powering on — no manual registration required.
3. **AI-assisted classification.** Unknown IoT devices are automatically identified, tagged with a confidence score, and assigned a risk level.

Who this is for: Plant managers, IT/OT administrators, compliance officers, and security teams operating industrial, healthcare, financial, or critical-infrastructure environments.

---

2. Logging In

Navigate to your ChainNode URL (typically `https://chainnode.pro/demo/live/` for the demo, or a custom subdomain for licensed deployments).

1. Enter the **email address** issued to you by your administrator.
2. Enter your **password**.
3. Click **Sign In**.

If you see a red error banner, verify the email is correct and check caps-lock. Repeated failures will lock the account — contact your administrator.

Tip: Bookmark the dashboard URL and enable your browser's password manager. ChainNode sessions persist until you explicitly sign out.

---

3. Dashboard Layout

Every page shares two global elements:

3.1 The Sidebar (left column)

Six navigation items, each representing a core workspace:

ICON	ITEM	WHAT IT DOES
▦	**Dashboard**	Real-time overview of the entire fleet
▣	**Assets**	Searchable inventory of every tracked asset
⌘	**Devices**	IoT-only view (sensors, cameras, PLCs, meters, trackers)
✓	**Compliance**	Generate SOC 2, ISO 27001, HIPAA, PCI-DSS, NIST, FDA reports
🔔	**Alerts**	Active alerts, full history, and alert rule management
🔑	**API Keys**	Manage authentication credentials for agents and integrations

A red numeric badge on the **Alerts** item shows the count of unacknowledged alerts. It refreshes every 30 seconds.

Click the **chevron** at the bottom of the sidebar to collapse it to icons only — useful on smaller screens. Hover over a collapsed icon to see its label.

3.2 The Topbar

- **Page title** (left) — tells you which workspace you're in.

- **AI Query button** (right) — opens the natural-language query modal (see §4).
- **Bell icon** (right) — duplicates the sidebar alert badge for visibility.

---

4. The AI Query Modal

This is the fastest way to interrogate your fleet. Click the **AI Query** button in the topbar.

How to use it:

1. Type a question in plain English. Example queries (click to autofill): - *"Show me every device added in the last 30 days without an assigned owner."* - *"List all critical-risk assets."* - *"Which assets have had firmware changes this week?"*
2. Click **Ask**. The response appears in a monospace gray box below the input.
3. Close the modal with the **X** button when finished.

Optimization tips: - Be specific about time ranges ("last 7 days", "since January 1"). - Reference asset attributes ChainNode tracks: hostname, IP, firmware version, location, department, assigned owner, risk level, status. - Use the AI Query as an audit tool — it can surface blind spots faster than manually scanning tables.

---

5. The Dashboard Page

This is your mission-control view. Everything auto-refreshes every 30 seconds.

5.1 The Four Stat Cards (top row)

CARD	WHAT IT COUNTS	WHY IT MATTERS
Active Assets	Every asset with status "Active"	Your live fleet size. Watch for sudden drops — they indicate a network segment going dark.
Changes Today	Configuration or discovery events since midnight	High numbers outside maintenance windows are a red flag.
Active Alerts	Unacknowledged alerts	Should trend toward zero. Anything >0 demands attention.
Blockchain Records Today	Configuration hashes written on-chain today	Confirms your audit trail is being captured. If this is zero but changes are happening, investigate.

5.2 Live Discovery Feed (left panel)

A scrolling stream of the most recent 20 configuration events. A green pulsing **Live** indicator confirms the feed is active.

Each entry shows: - A colored **vertical bar** indicating change type: - **Green** — newly discovered asset - **Amber** — existing asset modified - **Red** — asset removed/gone offline - **Hostname/IP** in bold - **Asset type** underneath - **Relative time** (e.g., "2m ago")

An **amber left border** marks events flagged as anomalous by the AI.

Click any entry to jump directly to that asset's detail page.

5.3 Asset Distribution Chart (right panel)

A doughnut chart breaking down your fleet by asset type. Hover for exact counts. Color-coded: - **Indigo shades** — traditional IT (servers, workstations, VMs, databases) - **Blue/purple** — network devices, software, certificates, cloud resources - **Green shades** — IoT devices (sensors, cameras, controllers, meters, trackers)

Optimization tip: A healthy fleet chart matches your expectations. If "Unknown" or "iot_unknown" dominates, schedule an AI re-classification pass.

5.4 Recent Changes Table

The most recent configuration changes, with four columns: - **Time** — when the change was observed - **Asset** — hostname, IP, and type - **Change** — a pill labeled DISCOVERED,

MODIFIED, REMOVED, or REINSTATED - **Anomaly** — amber "Anomaly" badge if the AI flagged the change as unusual

Click any row to open that asset's detail page.

---

6. The Assets Page

Your master inventory. Every tracked asset lives here.

6.1 Toolbar Controls

From left to right:

1. **Asset Type filter** — narrow to one of 14 types.
2. **Status filter** — Active / Inactive / Removed / Unknown.
3. **Risk Level filter** — Critical / Elevated / Standard / Low.
4. **Search field** — matches hostname or IP address in real time.
5. **Register Asset button** — opens a modal to manually add an asset.

6.2 The Asset Table

COLUMN	WHAT IT SHOWS
Hostname / IP	Icon (per type) + hostname + IP
Type	AI-classified type, or registered type
OS / Firmware	Operating system and firmware version
Risk	Color-coded badge (see §6.4)
Status	Color-coded badge (see §6.4)
Last Seen	Relative time since last check-in
Blockchain	Link to the latest on-chain transaction for this asset

Pagination appears below the table if you have more than 50 assets. Click any row to open the asset's detail page.

6.3 Registering an Asset Manually

Most assets are auto-discovered, but you can register one by hand:

1. Click **Register Asset**.
2. Fill in: Hostname, IP Address, Asset Type, Location, Department, Assigned Owner.
3. Click **Register**.

When to register manually: air-gapped devices, assets on segments the agent cannot reach, or placeholder records for equipment that is on order.

6.4 Badge Color Legend

Status badges: - 🟢 **Active** (green) — checking in normally - ⚫ **Inactive** (gray) — not seen recently but not declared dead - 🔴 **Removed** (red) — confirmed offline or decommissioned - 🟡 **Unknown** (yellow) — status cannot be determined

Risk badges: - 🔴 **Critical** — immediate attention required (unpatched firmware, exposed credentials, compliance violation) - 🟠 **Elevated** — above-baseline risk; review during next maintenance window - ⚪ **Standard** — normal operating risk - 🟢 **Low** — hardened, isolated, or well-protected

Optimization tip: Sort or filter by **Critical** at least once a week. Any asset sitting at Critical for more than 48 hours should have an owner assigned and a remediation ticket open.

---

7. The Asset Detail Page

Open this by clicking any asset. It is the most powerful screen in ChainNode.

7.1 Header

- ← **Assets** link returns you to the inventory.
- Large **hostname/IP** title.
- Secondary line shows IP · MAC address.
- Right side: current **Status** and **Risk** badges.

7.2 Asset Details Panel (left column)

Read-only fields: - **Asset Type** — how ChainNode categorizes the device. - **First Discovered** — when ChainNode saw it for the first time. - **Last Seen** — most recent

heartbeat. - **Operating System** — OS name and version.

Editable fields (hover to reveal the edit icon, click to edit, green ✓ to save, red ✕ to cancel): - Make, Model, Firmware Version - Department, Location, Assigned Owner - Risk Level

A "Saved" label confirms each edit. Errors appear in red.

Best practice: Fill in **Assigned Owner** for every critical asset. In an incident, the owner field is the first thing your response team will read.

7.3 AI Classification Panel

- **Classification dropdown** — override the AI's guess if it's wrong. Your override becomes the new source of truth.
- **Confidence bar** — how sure the AI is (0–100%). Below 60% deserves a manual review.
- **Risk Notes** — plain-English explanation of why the AI assigned this risk.

7.4 Sensor Readings Chart (IoT assets only)

A 24-hour line chart of every sensor reported by the device (temperature, humidity, pressure, etc.). Hover for exact values and timestamps.

Optimization tip: Use this chart to catch drift before alarms fire. A temperature sensor that slowly climbs 2°C over 24 hours is often the earliest sign of HVAC trouble.

7.5 Blockchain Verification Panel (right column)

This is what makes ChainNode unique.

- **Status line:** 🟢 "Verified on Polygon" or 🟡 "Pending."
- **TX Hash** — the Polygon transaction that recorded this asset's latest configuration. Click to open Polygonscan in a new tab. A copy button puts the full hash on your clipboard.
- **Block Number** — the Polygon block containing the transaction.
- **Logged At** — timestamp of the on-chain write.
- **Config Hash** — the SHA-256 fingerprint of the device configuration. If the hash changes, the configuration changed. Period.

How to use this in an audit: 1. Copy the **Config Hash**. 2. Open the asset on Polygonscan via the TX link. 3. Show the auditor the transaction data matches your current hash. 4. The auditor now has independent, cryptographic proof that your record is authentic.

7.6 Change History Timeline

A vertical timeline of every configuration event on this asset, oldest at the bottom. Each event shows: - A colored dot (green/blue/red/purple, or amber if anomalous). - The event label (First Discovered, Configuration Changed, Removed, Reinstated). - Timestamp (relative + absolute). - **Anomaly Detected** badge with AI notes, if applicable. - **Config hash transition** (from → to), so you can see exactly what changed. - **Blockchain link** to the transaction that recorded the change.

Optimization tip: Before approving any firmware or configuration update, take a screenshot of the timeline. After the update, compare — you should see exactly one new MODIFIED event matching your change window. More than one, or any anomaly badges, means something else happened.

---

8. The Devices Page

A focused view of IoT-only assets: sensors, cameras, controllers, meters, trackers, and unclassified IoT. The layout mirrors the Assets page but is pre-filtered.

Use this page when: - You're an OT (Operational Technology) operator who only cares about plant-floor devices. - You're investigating an industrial incident and need to exclude IT noise. - You're auditing IoT-specific compliance (e.g., FDA 21 CFR Part 11 on instrumentation).

All controls (filter, search, pagination, row-click to detail) work identically to the Assets page.

---

9. The Alerts Page

Three tabs: **Active**, **All Alerts**, **Alert Rules**.

9.1 Active Tab

Lists every unacknowledged alert as a card:

- **Severity badge:** 🔴 Critical, 🟠 Warning, 🔵 Info
- **Time fired** (relative)
- **Summary** — what triggered
- **Asset** and **Rule** — what and why

- **Acknowledge button** — opens the acknowledgment modal

Acknowledging an alert: 1. Click **Acknowledge**. 2. Type notes explaining the resolution ("HVAC serviced, sensor back in range" or "Firmware update approved by J. Smith in ticket #4421"). 3. Click **Confirm**. 4. The acknowledgment is **written to the Polygon blockchain**, producing a second TX hash. This gives you an immutable record of who acknowledged what, when, and why. Use these as evidence in post-incident reviews.

9.2 All Alerts Tab

Full historical table of every alert, acknowledged or not. Columns include time, severity, summary, asset, acknowledgment status, and the on-chain acknowledgment TX hash.

9.3 Alert Rules Tab

Lists every rule governing when alerts fire. Columns: rule name, type, severity, sensor, thresholds, status.

Creating a new rule:

1. Click **New Rule** (top right).
2. Fill in: - **Rule Name** — descriptive ("Chiller Temp > 8°C"). - **Rule Type** — Threshold, Anomaly, Change Detection, or Offline Detection. - **Severity** — Info / Warning / Critical. - **Sensor Type** (optional) — e.g., `temperature`, `humidity`, `pressure`. - **Min / Max thresholds** (optional) — numeric bounds. - **Notification Emails** — type each address and press Enter to add it as a tag.
3. Click **Create Rule**.

Rule type reference:

TYPE	FIRES WHEN…	BEST FOR
Threshold	A sensor value crosses min or max	Temperature, pressure, humidity monitoring
Anomaly	The AI detects abnormal behavior	Catching novel issues with no known threshold
Change Detection	A configuration change is recorded	Unauthorized firmware or OS modifications
Offline Detection	An asset stops checking in	Detecting unplugged devices or failed network links

Optimization tip: Start with broad **Warning** rules and tighten them to **Critical** once you've tuned out false positives. A Critical alert that cries wolf is worse than no alert at all.

---

10. The Compliance Page

Generate auditor-ready reports in seconds.

10.1 Framework Tabs

Six horizontal tabs, each corresponding to a compliance regime:

TAB	COVERS	TYPICAL USERS
SOC 2	Service organization controls	SaaS providers, MSPs
ISO 27001	Information security management	Enterprise IT
HIPAA	Protected health information	Hospitals, clinics, medical devices
PCI-DSS	Cardholder data protection	Retail, payment processors
NIST	NIST Cybersecurity Framework	Government contractors, critical infrastructure
FDA	21 CFR Part 11	Pharmaceutical, life sciences, regulated manufacturing

The description below the tabs explains exactly what ChainNode records for that framework.

10.2 Generating a Report

1. Pick a framework tab.
2. Set **Start Date** (defaults to 1 month ago).
3. Set **End Date** (defaults to today).
4. Choose **Format**: PDF (for auditors) or CSV (for downstream analysis).
5. Click **Generate Report**.

When generation completes, a summary appears showing: - Assets in range - Changes detected - Alerts fired

The report itself is an attestation bundle — it contains a **blockchain attestation TX hash** proving the data was not edited after generation.

10.3 Report History

Every report you've generated is logged in a persistent table with its own attestation TX. Auditors can replay any historical report and verify its contents on-chain.

Optimization tip: Run a fresh compliance report on the first business day of every month, whether or not an audit is scheduled. Build the habit now — it's much easier than scrambling the week before an auditor arrives.

10.4 What's On-Chain vs. Off-Chain

One of the most common questions auditors and compliance officers ask is *"what exactly does the blockchain contain?"* Understanding the answer is important — both for defending the model in audits and for knowing what a report actually proves.

ChainNode uses a **hash-anchor** architecture. The blockchain holds a cryptographic fingerprint plus a small metadata envelope for every asset event. The full, human-readable asset record lives in the ChainNode database and is cryptographically linked to the on-chain proof via the transaction hash. This is lightweight, cheap, and sufficient for audit-grade verification — you do *not* need to put every field on-chain to get a tamper-proof trail.

Written to Polygon (per transaction)

Every asset discovery or configuration change writes one Polygon transaction. The payload is a JSON metadata envelope containing:

FIELD	MEANING
`product`	Constant identifier: `"chainnode"`
`organization_id`	Your tenant UUID — proves the record belongs to you
`chainnode_asset_id`	Stable asset identifier (e.g., `cn_line1-plc-01`)
`hostname`	Device hostname at time of write
`ip_address`	IP address at time of write
`asset_type`	Classification (server, iot_controller, network_device, etc.)
`config_hash`	**SHA-256 fingerprint** of the full configuration
`change_type`	`discovered`, `modified`, `removed`, or `reinstated`
`timestamp`	ISO-8601 timestamp of the event

Plus the Polygon block number and the transaction hash itself, which are recorded automatically by the chain.

What the `config_hash` actually covers

The hash is not a hash of a static document — it is a SHA-256 of a canonicalized JSON representation of the device's *entire configuration*, with only volatile timing fields (`last_seen_at`, `scanned_at`, `received_at`, `agent_timestamp`) excluded. Changing **any** of the following will produce a different hash:

- Hostname, IP address, MAC address
- Operating system name and version
- Make, model, firmware version
- Asset type, open ports, protocols
- Every other discovered configuration field

This means a single hash check tells you whether *anything* about the device has drifted since the record was written.

Stored in the ChainNode database (off-chain)

The rich, human-readable data stays off-chain and is linked to the on-chain record by `blockchain_tx_hash`:

- **Identity:** hostname, IPs, MAC, OS name/version, make, model, firmware
- **Governance:** department, assigned owner, location, risk level, status
- **Lifecycle:** first seen, last seen, full change history
- **AI layer:** classification, confidence, risk notes, dependency map
- **Blockchain pointers:** `config_hash`, `blockchain_tx_hash`, `blockchain_block_number`, `blockchain_logged_at`
- **Full discovery payload:** raw metadata captured by the agent at scan time

The compliance report generator joins these two halves. Every row in a generated PDF or CSV includes the rich asset data *and* a clickable Polygonscan link to the transaction that proves it.

What this means for an auditor

An auditor reading a ChainNode compliance report can independently verify each line by:

1. Clicking the Polygonscan link.
2. Decoding the `metadata` JSON on the transaction.
3. Confirming the `config_hash` in the report matches the one on-chain.
4. Confirming the `organization_id` matches your tenant.
5. Confirming the `timestamp` matches the report's logged time.

If anyone tampered with the ChainNode database after the fact, the re-computed hash would no longer match, and the tamper would be immediately visible. That is the property the blockchain is there to guarantee — nothing more, nothing less.

> For a ready-to-hand-an-auditor walk-through of this verification process, see the companion document *"How to Independently Verify a ChainNode Report"* included in your Welcome Package.

---

11. The API Keys Page

This is where you issue, rotate, and revoke the credentials that let agents, devices, and integrations talk to ChainNode.

11.1 The Keys Table

COLUMN	MEANING
Name	Human-readable label
Type	`agent`, `device`, or `dashboard`
Key	Masked prefix (full key never shown after creation)
Last Used	Most recent authentication, or "Never"
Status	Active or Inactive
Actions	"Deactivate" link for active keys

11.2 When to Generate a New Key

Issue a fresh key in any of these situations:

1. **Onboarding a new agent or device** — a new PLC collector, edge gateway, or site-local agent.
2. **New integration** — connecting an ERP, CMMS, historian, BI tool, or custom dashboard.
3. **Third-party/read-only access** — embedded dashboards for customers or executives.
4. **Scheduled rotation** — every 90 days minimum for production credentials.
5. **After suspected compromise** — rotate immediately, then investigate.
6. **Staff turnover** — when an employee or contractor with key access leaves.
7. **Environment separation** — distinct keys per environment (prod / staging / test).
8. **Scope narrowing** — replacing a broad key with one limited to a specific site or function.
9. **Temporary access** — short-lived keys for vendors, auditors, or field technicians.

11.3 How to Generate a Key

1. Click **Generate New Key**.
2. Enter a descriptive **Name** (e.g., "Plant 3 — PLC Collector — Prod").
3. Choose **Type**: Agent (collects telemetry), Device (reports its own state), or Dashboard (read-only display).

4. Click **Generate**.

⚠ **The plaintext key is shown exactly once.** Copy it immediately using the copy button. Store it in your password manager or secrets vault before closing the modal. If you lose it, you must deactivate the key and generate a new one.

11.4 Deactivating a Key

Click **Deactivate** next to any active key. The key stops working instantly. It remains in the table for audit history but cannot authenticate.

Deactivate immediately if: - The key appears in a code commit, screenshot, or Slack message. - A laptop or device holding the key is lost or stolen. - A contractor or employee with key access departs.

---

12. Optimizing Day-to-Day Usage

12.1 A Recommended Daily Routine (5 minutes)

1. Open the **Dashboard**. Scan the four stat cards. Note anything surprising.
2. Glance at **Live Discovery Feed** — any amber anomaly borders?
3. Click **Alerts → Active**. Acknowledge or triage anything new.
4. Return to Dashboard. You're done.

12.2 A Recommended Weekly Routine (20 minutes)

1. **Assets → filter Risk = Critical.** Ensure every critical asset has an assigned owner and a plan.
2. **Assets → filter Status = Unknown.** Investigate anything that has drifted to unknown.
3. **Alerts → Alert Rules.** Review whether any rule is generating too many false positives. Tune or disable.
4. **API Keys.** Check the Last Used column. Any key not used in 30+ days is a candidate for deactivation.

12.3 A Recommended Monthly Routine (1 hour)

1. **Compliance.** Generate a fresh report for your primary framework. Archive it.
2. **API Keys.** Rotate any key older than 90 days.

3. **Assets → filter by Asset Type.** Spot-check the AI Classification confidence scores. Override any below 60%.
4. **AI Query.** Run a few hunt-style questions: *"Show assets without owners," "List devices added this month," "Which assets had multiple changes this week?"*

12.4 Incident Response Checklist

When something goes wrong:

1. Open **Alerts → Active** and identify the triggering alert.
2. Click through to the affected asset.
3. Review the **Change History Timeline** — did a configuration change precede the alert?
4. If yes, compare the **Config Hash** transitions. The before/after tells you exactly what changed.
5. Open the **Blockchain TX** link. Screenshot it for your incident record.
6. After remediation, **Acknowledge** the alert with notes. The acknowledgment is written on-chain as part of your evidence trail.

---

13. Troubleshooting

SYMPTOM	LIKELY CAUSE	FIX
"Signing in..." hangs	Network or Supabase unreachable	Check internet; retry in 60 seconds
Dashboard shows zero assets	No agents running, or wrong API key	Verify the agent is running and its key is Active on the API Keys page
Alert badge never decreases	Unacknowledged alerts accumulating	Clear the Active tab; they persist until acknowledged
Blockchain column shows "—"	Hash pending confirmation on Polygon	Wait 30–60 seconds and refresh
AI Query returns an error	Query service temporarily unavailable	Retry; if persistent, contact support
Inline edit shows red error	Backend rejected the change	Check field format (e.g., firmware version must be text)
New asset doesn't appear	Agent not yet reporting, or type filter active	Clear all filters; wait 30 seconds

14. Glossary

- **Agent** — A lightweight ChainNode collector running on your network that discovers and reports assets. The agent handles only network scanning and fingerprinting — AI classification, anomaly detection, and blockchain writes happen server-side. No AI API keys or third-party credentials are needed on the agent.
- **Asset** — Anything ChainNode tracks: a device, a VM, a software install, a certificate, a sensor.
- **Attestation** — A blockchain-recorded proof that a compliance report was generated from unmodified data.
- **Change Event** — A recorded discovery, modification, removal, or reinstatement of an asset.
- **Config Hash** — A SHA-256 fingerprint of an asset's configuration. Any change alters the hash.

- **Polygon** — The public blockchain ChainNode writes to. Transactions are low-cost and publicly verifiable.
- **Risk Level** — A calculated severity (Critical / Elevated / Standard / Low) based on configuration, exposure, and classification.
- **TX Hash** — A Polygon transaction identifier. Clickable to open Polygonscan.

---

15. Scan Frequency & Tuning

ChainNode's discovery agent sweeps your network on a schedule you control. Understanding this setting — and tuning it to match your environment — is one of the highest-leverage decisions you'll make as an operator.

15.1 How the Agent Schedules Scans

The agent reads a single value, `agent.scan_interval`, from its `config.yaml`. The value is in seconds, and it controls how often a full discovery sweep runs. Between full sweeps, the agent still processes event-driven change signals (a device announcing itself, a link flapping, a telemetry update), so the interval governs **baseline freshness**, not responsiveness to live events.

- **Shipping default:** `3600` seconds — **one full sweep every hour.**
- **Demo / simulator profile:** `120` seconds (every 2 minutes) — tuned for fast visible change on stage.
- **Fallback if unset:** `3600` seconds.

15.2 How This Compares to Legacy Platforms

ChainNode's hourly default is **faster than every major CMDB and discovery platform except agent-on-endpoint tools**. Most legacy CMDB products rely on heavy, credentialed, scheduled sweeps that customers run *daily or weekly* because the scan itself is expensive.

PLATFORM	TYPICAL DEFAULT FULL-DISCOVERY CADENCE
IBM TADDM	Daily (Level 2) / weekly (Level 3), admin-scheduled — no out-of-box continuous interval
ServiceNow Discovery	Daily full sweep, customer-defined
Device42	Daily
Lansweeper	Daily
Qualys / Rapid7 asset discovery	Daily to weekly
Tanium	~15 seconds (agent-on-endpoint, different architecture)
ChainNode	**Hourly, default — tunable to 5 min**

ChainNode's lighter, fingerprint-based scan is what makes hourly sustainable. Legacy CMDBs cannot run hourly without overwhelming the network and the target hosts.

15.3 Recommended Interval by Environment

The shipping default (60 minutes) is a safe middle ground. Tune it to match your operating context:

ENVIRONMENT	RECOMMENDED INTERVAL	WHY
OT / ICS / pharmaceutical / critical infrastructure	**5–15 min**	Change-detection latency matters. Unauthorized firmware or PLC changes must surface fast.
General enterprise IT	**60 min** (default)	Balances freshness against scan noise and bandwidth.
Large fleets (10,000+ assets)	**2–4 hours**	Reduce bandwidth and agent CPU load. Event-driven signals cover gaps.
Cloud / ephemeral workloads	**15 min**	VMs and containers spin up and die between slow scans.
Compliance-only / audit shops	**Daily**	Only need a verifiable snapshot per day for evidence.

15.4 How to Change the Interval

1. Open `config.yaml` on the machine running the ChainNode agent.
2. Locate the `agent:` section and edit the `scan_interval` value (in seconds): `yaml agent: scan_interval: 900 # 15 minutes`
3. Restart the agent service. The new interval takes effect on the next scan cycle.

Common values:

INTERVAL	SECONDS
5 minutes	300
15 minutes	900
30 minutes	1800
1 hour (default)	3600
4 hours	14400
Daily	86400

15.5 Tuning Tips

- **Start conservative, then tighten.** Deploy at the default 60 minutes for the first week. Watch the Changes Today stat card (§5.1) — if you see bursts of change events clustered at scan boundaries, your interval is fine. If critical events are being missed between scans, tighten it.
- **Match your alert rules to your scan interval.** An offline-detection rule with a 5-minute trigger is meaningless if the agent only scans hourly. Set the alert grace period to at least 2× the scan interval.
- **Separate scans for separate segments.** Nothing stops you from running multiple agents on different subnets with different intervals. Use a 5-minute interval for your OT network and a 4-hour interval for your developer VLAN.
- **Monitor the blockchain records counter.** The Dashboard's *Blockchain Records Today* card (§5.1) tells you how many config hashes were written on-chain today. Divide by (24 × 60 ÷ interval-in-minutes) to sanity-check that scans are firing on schedule.

---

16. The ChainNode iPad Companion App

The ChainNode mobile app brings live fleet intelligence, the facility map, alerts, and asset verification to your iPhone and iPad. It is designed as a companion to the web dashboard — ideal for walk-throughs on the plant floor, field audits, and at-a-glance monitoring away from your desk.

> **Status:** The app is currently distributed via **TestFlight** (Apple's beta channel). A public App Store release is planned. Your account manager will send your TestFlight invite as part of the Welcome Package.

16.1 System Requirements

- **iPadOS / iOS 13.0 or newer**
- iPhone or iPad (all modern models supported)
- Active internet connection (Wi-Fi or cellular)
- A valid ChainNode API key of type **dashboard** (see §11)

16.2 Installation (TestFlight Beta)

1. On your iPad or iPhone, install Apple's **TestFlight** app from the App Store if you don't already have it.
2. Open the invitation email from ChainNode and tap the **"View in TestFlight"** button.
3. In TestFlight, tap **Accept**, then **Install**.
4. Once installed, tap **Open** — or launch **ChainNode** from your home screen.

When the app leaves beta, installation will switch to a normal App Store download. Your API key and settings will carry over.

16.3 First-Run Pairing

The first time you launch the app you'll see the **Login Screen**:

- ChainNode ⛓ logo and the tagline *"Blockchain-verified asset intelligence."*
- A single **API Key** field (masked input).
- A **Connect** button.

To pair the device with your tenant:

1. On your web dashboard, go to **API Keys** (see §11).
2. Click **Generate New Key**. Name it descriptively — e.g., *"Plant Manager iPad"* or *"Field Auditor — J. Smith"*. Choose type **Dashboard**.
3. Copy the plaintext key immediately (it is shown only once).
4. On the iPad, paste the key into the **API Key** field and tap **Connect**.
5. The app makes a verification call. On success, you land on the Dashboard tab. On failure you'll see *"Connection failed. Check your API key."* — verify the key is correct, active, and that the iPad has internet access.

The API key is stored securely on-device. **Subsequent launches skip the login screen and auto-connect.**

> **Security tip:** Issue each iPad its own API key. If a device is lost, deactivate just that key on the web dashboard (§11.4) without disrupting anyone else.

16.4 App Layout

The app adapts to screen size:

- **iPad landscape / large screens:** A persistent **left sidebar** shows the ChainNode logo, five navigation items, and a "Powered by Polygon" footer with a purple indicator.
- **iPhone / narrow screens:** A **bottom navigation bar** replaces the sidebar.

Five tabs:

TAB	ICON	PURPOSE
Dashboard	Grid	Fleet overview, live stats, recent changes
Assets	List	Searchable asset inventory
Network Canvas	Account tree	Zoomable floor-plan with live asset status, connections, and tap-to-inspect
Alerts	Bell	Active and historical alerts
Settings	Gear	Connection, display, about

16.5 Dashboard Tab

A mobile-optimized version of the web Dashboard:

- **Four stat cards:** Active Assets, Changes Today, Active Alerts, Blockchain Records. On iPad they appear as a 4-across grid; on iPhone as a 2×2 grid.
- **Recent Changes list:** Ten most recent events with colored status dots (green = discovered, blue = modified, red = removed, amber = anomaly), the TX status badge, and relative time.
- **Asset Distribution chart:** A horizontal stacked bar showing the top six asset types by count.

Pull down on the page to force-refresh.

16.6 Assets Tab

- **Search bar:** Type any hostname or IP fragment — filtering happens instantly.
- **Filter chips:** All / Active / Inactive / Removed.
- **Asset list:** Each row shows the asset-type icon, hostname or IP, type label, and a colored status badge.
- **Tap any row** to open the **Asset Detail** screen (see §16.10).

16.7 Network Canvas Tab

This is the iPad's signature feature — a zoomable, pan-able topology view of your entire fleet, purpose-built for walking the plant with the device in hand. It is the mobile companion to the web dashboard's Network Canvas.

> **Read-only by design.** The iPad Network Canvas shows the layout your administrator designed on the web dashboard. Node positions are **not editable on mobile**. To rearrange the canvas, use the web dashboard. A *"Read-only · Edit layout on web dashboard"* hint is visible in the toolbar so nobody wonders why long-press does nothing.

Visual elements: - A dark canvas background with subtle gridlines. - **Five labeled zones** — **Core Network** (blue), **Production** (purple), **Facilities** (green), **Security** (amber), **Warehouse** (red) — rendered as translucent background regions with corner labels. - **Asset nodes** positioned inside their zones. Each node shows: - A **risk-colored indicator dot** with a soft glow (red = critical, amber = elevated, green = low, gray = standard/unknown). - An **asset-type icon** (PLC, HMI, sensor, camera, switch, server, etc.). - The **hostname** as the primary label. - The **asset type** as a small sublabel. - **Dashed connection lines** between related nodes (for example, every PLC back to the core switch, every HMI back to its PLC), drawn with a `CustomPainter` so they stay crisp at any zoom level.

Gestures & toolbar: - **Pinch to zoom** — range 0.3× to 3.0×, smooth and inertial. - **Drag with one or two fingers to pan** around the canvas. A 400 px boundary margin keeps you from panning fully off the content. - **Fit to Screen button** (top-right, screen-fit icon) — instantly resets the view so the entire canvas is framed, no matter how far you've zoomed or panned. Use this any time you feel lost. - **Live indicator** (top-left, next to the tab title) — a green pulsing dot confirming the canvas is backed by live data. - **Asset count** — a small label in the toolbar shows "*N* assets" so you can confirm everything is loaded.

Tapping a node opens an **Asset Bottom Sheet** showing: - Asset name, status badge, hostname/IP, asset type, last verified time, and blockchain TX hash (if verified). - A **"View Full Details →"** button that opens the full Asset Detail screen (§16.10).

Optimization tip: Mount an iPad in your control room running the Network Canvas tab, set the refresh interval to 15 seconds (Settings → Display), and hit **Fit to Screen**. You now have a live mimic display for the entire facility — without the cost of a traditional SCADA HMI. For a walk-through, pinch into whichever zone you're working in and the canvas becomes a live, labeled map of just that area.

16.8 Alerts Tab

- **Filter chips:** All / Critical / Warning / Info / Unacknowledged.
- **Alert tiles** show a colored left-accent bar (red/amber/blue by severity), the summary text, the alert type, time fired, severity badge, and an **ACK** badge if already acknowledged.
- **Empty state:** A green checkmark and the message *"No alerts — all systems nominal."*
- **Tap any alert** to open a bottom-sheet detail view with the full summary, fired-at timestamp, key/value details, and an **Acknowledge** button (if not already acknowledged).

Pull-to-refresh works on this tab too.

16.9 Settings Tab

Organized into four sections plus a disconnect action:

CONNECTION - **Supabase URL** (read-only). - **API Key** — shows a masked preview (first 12 characters + "..."). Tap to edit in a modal. - **Connection status** — live green/red dot with "Connected" or "Disconnected" text. - **Test Connection** button — runs a verification call and updates the status indicator.

DISPLAY - **Refresh interval** — segmented control: **15s / 30s / 60s / Manual**. Default is 30s. - **Show offline assets** — toggle (default ON). - **Compact asset list** — toggle (default OFF) for denser rows.

NOTIFICATIONS - Placeholder: *"Push notifications coming soon."*

ABOUT - App version (currently 1.0.0). - *"Powered by Polygon Mainnet"* with a tappable link to polygonscan.com. - Footer: *Witty Inventions Digital, LLC.*

DISCONNECT — a red button at the bottom. Tapping it clears the stored API key and returns you to the Login screen. Use this before handing the device to a different user, or if the device will be retired.

16.10 Asset Detail Screen (Mobile)

Opened from Assets, Network Canvas, or Dashboard. It mirrors the web Asset Detail page with a mobile-friendly layout:

- **Header:** Asset name, IP · MAC, and inline badges for Status, Blockchain verification, Risk level, and Asset type.
- **Details grid:** Make, Model, Firmware, Department, Location, Assigned Owner, First Seen, Last Seen. Two-column on iPad, single-column on iPhone.

- **Blockchain Verification panel:** "✅ Verified on Polygon" or "⏳ Pending Verification," followed by TX hash, block number, logged timestamp, config hash, and a **View on Polygonscan** button.
- **AI Classification panel:** Classification label, confidence progress bar, and AI risk notes.
- **Change History Timeline:** Up to 20 recent events with colored dots, anomaly badges, timestamps, config-hash transitions, and Polygonscan links.

The mobile Asset Detail screen is read-only. To edit owner, location, risk level, etc., use the web dashboard.

16.11 Daily Use Scenarios on iPad

- **Plant walk-through:** Open Network Canvas, pinch into the zone you're working in, and verify every asset shows green. Tap anything flagged amber or red to open its Asset Bottom Sheet. Hit **Fit to Screen** between stops to reset the view.
- **Receiving new equipment:** Walk to the equipment, open the Assets tab, wait ~60 seconds, and watch the new device appear in the discovery feed.
- **Incident response:** A critical alert fires. Open Alerts, tap the event, jump to the affected asset, review the change history and blockchain proof, and acknowledge from the device before leaving the scene.
- **Executive briefings:** Hand the iPad to leadership during a tour. The Network Canvas gives a visual story without any technical explanation needed — pinch-zoom makes it feel like a familiar map app.

16.12 Troubleshooting the iPad App

SYMPTOM	LIKELY CAUSE	FIX
"Connection failed" on login	Wrong, inactive, or deactivated key	Verify the key is Active on the web dashboard; regenerate if needed
App opens to Login every launch	Storage reset (e.g., after reinstall)	Re-enter the API key; it will auto-load on future launches
Dashboard shows stale numbers	Refresh interval set to Manual	Settings → Display → set Refresh Interval to 30s
Network Canvas is empty	No assets in tenant, or the API key is inactive	Check the asset count in the toolbar; verify the key on the web dashboard
Lost inside a zoomed-in Network Canvas	Pinched too far in, panned off-screen	Tap **Fit to Screen** in the toolbar to reset the view
Can't move nodes on the Network Canvas	This is intentional — the mobile canvas is view-only	Edit node positions on the web dashboard; the iPad mirrors that layout
Assets missing from list	"Show offline assets" is OFF	Settings → Display → toggle it ON
Can't receive TestFlight invite	Invitation expired or Apple ID mismatch	Ask your ChainNode account manager to re-send

16.13 Roadmap

The following capabilities are planned for future releases of the iPad Companion:

- Push notifications for critical alerts
- Biometric (Face ID / Touch ID) unlock of the API key
- QR-code pairing (scan a QR from the web dashboard to enroll an iPad in one step)
- Apple Pencil annotation on the Network Canvas
- Drag-to-reposition on the Network Canvas (currently web-only)
- Offline caching for use in areas without connectivity

Your feedback during the TestFlight phase directly influences what ships first — use the TestFlight **Send Beta Feedback** option to tell us what you need.

---

17. Support

- **In-app AI Query** — fastest way to answer questions about your fleet.
- **Email support** — provided by your account manager at time of purchase.
- **Documentation portal** — https://chainnode.pro (for licensed customers).
- **Incident hotline** — available on Critical and Enterprise tiers.

ChainNode is a trademark of its respective owner. Polygon is a trademark of Polygon Labs. This manual corresponds to dashboard release 1.0.
