

First-Time Setup Guide

Get the portal production-ready before you onboard your first agent

This guide walks through every setting worth configuring **before** devices start checking in and inventory starts flowing in. Doing these in order means alerts, tickets, asset fields and vulnerability data are all correctly configured from the very first agent check-in — instead of getting confused or stuck partway through onboarding and having to go back and fix things after data has already landed.

How to use this guide: work through the steps in order. Steps marked **Do this before onboarding agents** are the ones that are genuinely hard to fix retroactively (a missing custom field means re-tagging every asset later; misconfigured alerts mean missed notifications during the exact window you need them most). Everything else can be adjusted at any time without disruption.

Contents

- Step 1 — Log in and change the default admin password
- Step 2 — Branding (company name, logo, colour)
- Step 3 — Companies (multi-site or MSP setups)
- Step 4 — Departments
- Step 5 — Users, roles and access
- Step 6 — Security policy
- Step 7 — Single sign-on (optional)
- Step 8 — Email alerts (SMTP)
- Step 9 — Email intake (turn inbound email into tickets)
- Step 10 — Ticketing setup (categories, SLAs, fields, canned responses)
- Step 11 — Asset types and custom fields
- Step 12 — PatchIQ data sources (vulnerability feeds)
- Step 13 — Licensing
- Step 14 — Backups
- Step 15 — Compliance and breach contacts (if applicable)
- Step 16 — Confirm the agent release before you publish it fleet-wide
- Step 17 — Onboard your first agent
- After onboarding — what to check once agents start checking in

Step 1 — Log in and change the default admin password

Where: top-right account menu → Change password

Sign in with the administrator credentials you were given, then change the password immediately — this is standard for any first login, and matters even more once Security Policy (Step 6) enforces password rules for everyone else.

Step 2 — Branding

Where: Administration → Branding

Set your company name, logo and accent colour. This is cosmetic, but it's the first thing end users and technicians see — worth doing before you invite anyone else in, so nobody's first impression is the default theme.

Step 3 — Companies

Where: Administration → Companies

If you support more than one company, site, or client from this one IQDesk instance (an MSP model, or a holding company with separate subsidiaries), create each company record now. Assets, tickets and users can all be tied to a company — setting this up first means every device you onboard later gets filed under the right company from the start instead of needing a bulk re-assignment afterward.

Do this before onboarding agents: If you have more than one company/site, create them all now — every asset, ticket and report can be filtered by company, but only if the company existed when the record was created.

Step 4 — Departments

Where: Administration → Departments

Departments are shared across tickets, assets and user profiles — set up your real org structure (IT, Finance, Operations, etc.) before you start creating users or importing assets, so everything can be tagged correctly from day one.

Step 5 — Users, roles and access

Where: Administration → Users

Create accounts for the rest of your IT team before onboarding begins, so more than one person can respond to tickets and alerts once agents start checking in. Assign the right role per person:

- **Admin** — full access, including all Administration settings covered in this guide.
- **Manager** — day-to-day operational access (tickets, assets, reports) without server-level settings.

- **Technician / Guest** — narrower operational roles for support staff and read-only stakeholders.
-

Step 6 — Security policy

Where: Administration → Security policy

Set idle timeout, password complexity rules and account lockout thresholds before you have a full roster of users logging in daily — changing these later means existing users may suddenly be forced to reset passwords or get logged out mid-work.

Step 7 — Single sign-on (optional)

Where: Administration → Single sign-on

If your organisation uses an OIDC identity provider (Azure AD / Entra ID, Okta, Google Workspace, etc.), configure it now, before you create local accounts for your whole team — it's simpler to onboard everyone through SSO from the start than to migrate local accounts to SSO afterward.

Step 8 — Email alerts (SMTP)

Where: Administration → Email alerts

This is outbound email — SLA breach warnings, MonitorIQ alerts, and (if you enable it) data-breach notifications all go out through this connection. Enter your SMTP host, port, credentials and a From address, then use **Send test email** to confirm delivery before you rely on it.

Do this before onboarding agents: Configure this before onboarding agents. Once devices start checking in, Monitor rules and SLA timers start running immediately — if outbound email isn't configured yet, the first real alerts (a disk filling up, an SLA about to breach) go nowhere and nobody finds out until someone happens to check the portal.

Step 9 — Email intake

Where: Administration → Email intake

Separate from Step 8 — this is inbound. If you want a support mailbox where an email in becomes a ticket, connect it here. Optional, but worth deciding on before you publish a support email address to end users, so the first message they send doesn't disappear into an unmonitored inbox.

Step 10 — Ticketing setup

Where: Administration → Category rules, SLA rules, Location & Branch Fields, Custom Ticket Fields, Quick-ticket tiles, Canned responses

A handful of related settings that shape how every ticket looks and routes from the moment your team starts using the portal:

- **Category rules** — auto-categorise and route new tickets.
- **SLA rules** — response and resolution targets per priority/category.
- **Location & Branch Fields** — the location/branch picklists tickets and assets share.
- **Custom Ticket Fields** — any fields specific to how your organisation tracks work.
- **Quick-ticket tiles** — one-click ticket creation for your most common request types.
- **Canned responses** — reusable reply snippets for tickets and chat.

Tip: If any Custom Ticket Field is marked required, every technician creating a ticket from now on must fill it in — decide on required fields before your team is actively working tickets, not after, to avoid a wave of "why can't I submit this" questions.

Step 11 — Asset types and custom fields

Where: Administration → Asset types & fields

This is the single most important step to get right before onboarding agents. Define any custom asset types and inventory columns you need — asset tags, warranty dates, cost centre, physical location, or anything specific to how your organisation tracks hardware — before the first device checks in.

Do this before onboarding agents: Every agent that checks in creates an asset record immediately using whatever fields exist at that moment. If you add a required custom field after 50 devices have already onboarded, you'll be going back through all 50 by hand to fill it in — there's no bulk backfill from the agent side. Get the field list right first, then start onboarding.

Step 12 — PatchIQ data sources

Where: Administration → Data Sources

If you're using PatchIQ (vulnerability and patch management), every vulnerability feed (CISA KEV, NVD, MSRC, OSV, and the Linux distro feeds) is enabled by default and works without an API key. Adding a free NVD API key here raises its rate limit significantly and is worth doing before you onboard a large fleet, since a bigger fleet means more software to correlate against — a keyless NVD sync can get rate-limited exactly when you have the most data to process. Get a key from the link on that page and save it before mass onboarding.

Step 13 — Licensing

Where: Administration → Licensing

Confirm your license is activated and review what it covers (feature set, seat/device count, expiry). If you're onboarding more devices than your current license covers, sort that out now rather than discovering the limit mid-rollout.

Step 14 — Backups

Where: Administration → Backups

Set a backup schedule, retention period and destination before production data starts accumulating — tickets, asset inventory, chat transcripts and vulnerability findings are all far more valuable (and painful to lose) once real devices are reporting in than they are on a fresh install.

Step 15 — Compliance and breach contacts

Where: Administration → Breach Contacts (and the Data Breach module, if enabled)

If your organisation is subject to a compliance framework (ADHICS or similar), set your breach notification contacts and compliance configuration now. These drive time-sensitive notification clocks the moment an incident is logged — better configured in advance than discovered empty during an actual incident.

Step 16 — Confirm the agent release

Where: Administration → Agent Fleet Updates

Check which agent version is currently published and will be handed to every device that enrolls from this point forward. If you need to publish a newer build first, do it now — once you're actively onboarding, changing the published version means every device that already enrolled will pick up an update shortly after.

Step 17 — Onboard your first agent

Where: Assets → Download Agent Installer / Issue an enrollment token

With everything above in place, install the agent on one test device first:

- Go to the Assets page and download the agent installer, or issue a standalone enrollment token if you're deploying via script/RMM.
 - Install it on a single test machine and confirm it appears in Assets within a few minutes, with inventory, software list and (if applicable) patch data populated.
 - Open that device's asset record and check the custom fields from Step 11 are present and correctly labelled.
 - Only once that one device looks right, roll the installer out to the rest of the fleet — via your RMM, GPO, or however you distribute software today.
-

After onboarding

Once agents are checking in at scale, here's what happens automatically — and what to keep an eye on for the first few days:

- Inventory (hardware, installed software, patch state) populates automatically on every check-in — no manual entry needed.

- Monitor rules start evaluating check-in facts immediately and will alert (via the email set up in Step 8) if something crosses a threshold.
- If PatchIQ is enabled, vulnerability correlation runs on a schedule — expect findings to start appearing within the first sync cycle, not instantly on check-in.
- Spot-check a handful of the first devices against Steps 11 and 12 to confirm fields and vulnerability data look the way you expect before assuming the rest of the fleet will look the same.

This guide covers first-time setup only. For day-to-day usage — creating tickets, using remote support, managing licenses and more — see the in-app User Manual ([Help → User Manual](#)).