Isovara Ecosystem program

Isovara
ECOSYSTEM

Oct 10, 2026 · Program overview for device makers, operators and their customers

Build the device. The cloud, the apps and the sales channel are already here.

Isovara Cloud already runs monitoring businesses for operators: companies that sell environmental monitoring under their own brand, as a hosted service or on their own servers. Their customers sign in to a branded portal, get alerts by text and email, set rules, read charts, and keep their monitors up to date with signed firmware.

The **Isovara Ecosystem program** opens that platform to hardware from other makers. A device that meets the published device contract enrolls with a claim code, gets its own encrypted connection, and shows up in every operator's portal next to Isovara v3. It gets the same alerts, rules, charts, firmware rollouts, branding and billing. Operators can sell it from day one.

Three groups gain from the program:

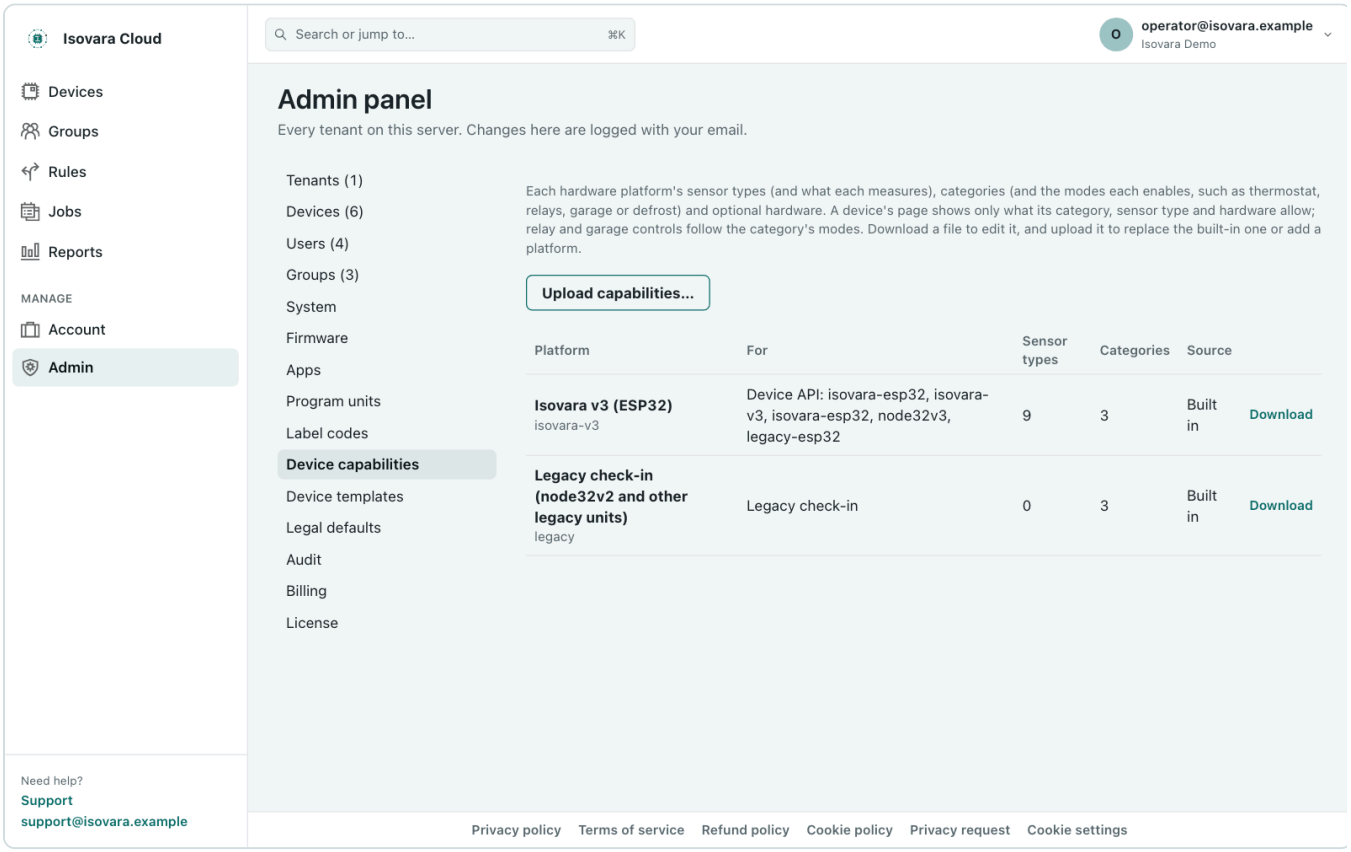
	What they get
Device makers	A market and a cloud, without building either. Your hardware joins a platform operators already sell
Operators	A wider catalog to sell under one portal, with the same tools for every device
Customers	One account and one app for every monitor, with security requirements they can count on

Why device makers join

Building an IoT product means building a cloud behind it: enrollment, credentials, a broker, dashboards, alerting, user accounts, billing and an update system. Most makers would rather build the device. With the Ecosystem program, the cloud work is already done and tested at scale. A single server handled 10,000 simulated devices at 1% of one CPU core.

- **No cloud to build or run.** Enrollment, per-device credentials and broker accounts, alerts by email and SMS, rules, charts and CSV export, user roles, read-only viewers, groups, scheduled jobs and subscription billing are already there.
- **A ready sales channel.** Operators resell monitoring to restaurants, clinics, IT teams, growers and homeowners. Certified devices are offered to operators on the hosted service and included in the device catalog of licensed installs.
- **Your measures, first class.** A device capabilities file declares your sensor types, operating modes and optional hardware. Extra values your device reports (up to 32 per reading) can drive rules as `extra.<name>`, and numeric values you mark for storage get history and charts.

- **Your device page.** A device management template defines the tabs operators and technicians see for your device. It is backed by an OpenAPI document of your channel operations, so there is no portal code to write.
- **Your keys stay yours.** You sign firmware with your own Ed25519 key, kept offline. You register only the public key. Every update is checked by signature and SHA-256 before it can boot, and two key slots let you rotate keys safely.
- **Rollouts handled for you.** Operators publish your signed releases to production and beta channels, then roll out to a share of devices or named groups first.
- **Brand-ready.** If your firmware supports the brand template, operators can sell your device under their own name, with no separate build.
- **Room for small devices.** Battery-powered and sleeping devices can certify as Reporting (Class B) without holding a cloud connection open.

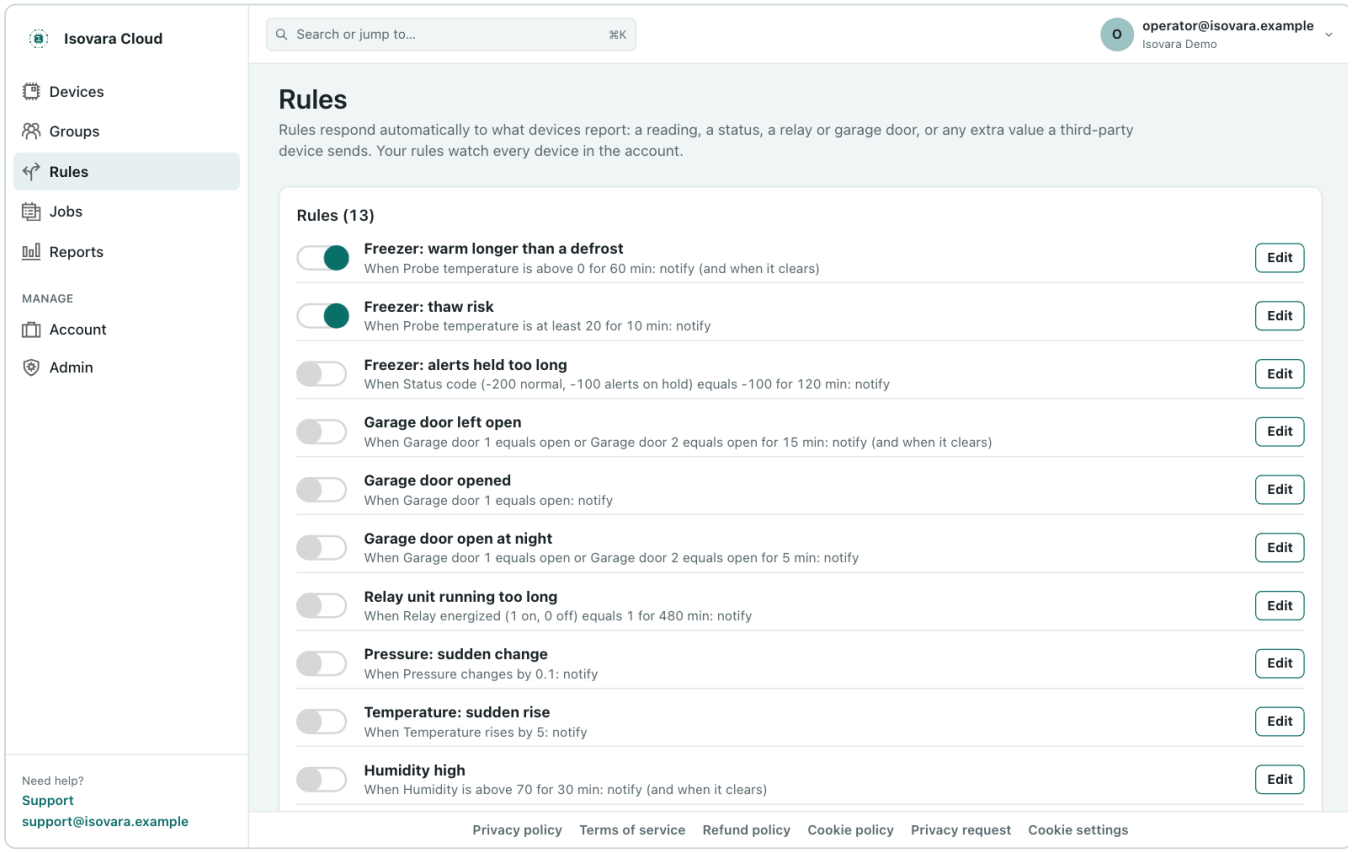


Each hardware platform is registered with a capabilities file. Operators' screens show only the sensors, modes and controls that platform declares.

Why operators want certified devices

- **A wider catalog, one portal.** Offer sensors Isovara v3 does not have, such as air quality, water leaks or power, without a second platform, a second app or a second bill.
- **The same tools for every device.** Alerts, the 13 ready-made rules plus your own, groups, jobs, label codes, staged firmware rollouts and plans work the same way across certified hardware.
- **Lower risk.** A certified device has passed the published conformance checklist, the platform's test scenarios and a 72-hour run. It updates only with signed firmware and never exposes its secrets.

- **The same business model.** Per-device plans, your own Stripe account and your own branding apply to every certified device.



Rules work on built-in measures and on the extra values a certified device reports.

What certification tells customers

Customers rarely read protocol documents. The Isovara Certified mark tells them four things:

1. **It works with their provider's app.** They add it with the code on its label, and it appears next to their other monitors.
2. **Its connection is private.** Every certified device verifies the cloud's certificate, uses TLS for every connection and has its own credentials.
3. **Its updates are safe.** It installs only firmware signed for its own model and rolls back if a new version cannot connect.
4. **It is safe to pass on.** A factory reset erases its credentials, and a new owner can add it to their own account.

Participation levels

	Developer	Certified	Partner
For	Any company building a device for Isovara Cloud	Each product (platform and firmware line) that passes certification	Makers with certified products and a shared go-to-market plan

	Developer	Certified	Partner
You get	Hardware Developer Guide and OpenAPI documents; a staging tenant; a reserved platform ID; factory and enrollment codes for test units; technical support	Use of the Isovara Certified mark; a catalog listing for operators; production registration on the hosted service and in licensed-install releases; a certificate number	Co-marketing and introductions to operators; early access to protocol changes; a seat on the roadmap council; priority lab slots; a named engineer
You commit to	Test only against staging installs; keep the guide confidential (NDA); no use of the mark	Keep the product conformant; recertify when triggers apply; answer security reports within [N] days; publish your extra fields with units and ranges	An annual joint plan; reference customers or operators
Cost	[program fee or free]	[certification fee per product]	[by agreement]

The mark belongs to a product, not to a company. A Developer may say "built for Isovara Cloud" while the product is in development, but may not use the Isovara Certified mark until it is certified.

Certification classes

Certification follows the device classes in the Hardware Developer Guide. Legacy check-ins (Class C) exist only for units already in the field and cannot be certified.

	 **Native (Class A)**	**Reporting (Class B)**
Connects through	Device API over HTTPS, then its own MQTT-over-TLS cloud channel	Device API over HTTPS only
What operators get	Enrollment, live commands with acknowledgments, full configuration, remote console, signed cloud updates, brand pushes	Enrollment, readings, settings in each reply, configuration by polling
Best for	Mains-powered monitors and controllers	Battery-powered, sleeping or very small devices
Required for	Any new design that can hold a connection	Designs that cannot

What certification checks

A device is ready for certification when every item of the conformance checklist passes against a staging installation. The checklist is section 11 of the Hardware Developer Guide; in summary:

Area	We verify	Why it matters
Identity and hardware	A 12-character device ID from hardware, unique and printed on the label; a truthful hardware report; enough memory to run safely; A/B firmware slots	Customers add the right device; screens show only what is fitted; updates cannot brick the unit
Enrollment and trust	Enrollment with factory and enrollment codes; correct handling of refusals; trust bootstrap for private installs; no plain-HTTP cloud addresses	Only the rightful owner can claim a device, on public or private installs
Cloud channel	Online and offline status; one path for reports at a time; credential refresh; reconnect with backoff	Accurate online status and alerts; no storms of reconnects after an outage
Messages	Heartbeat, readings and configuration reports in the published formats; documented extra fields	Charts, alerts and rules work without special cases
Commands	Every command acknowledged within 2 seconds; expired and repeated commands dropped; relays refused when absent; configuration applied atomically	Actions from the app do what they say, once
Updates	Signed images for its own platform only; progress reported; automatic rollback	A bad or foreign image never becomes the running one
Security	No secret in any report, log, console or crash dump; local changes need the admin password; sign-in lockout; setup mode times out	Customers' networks and accounts stay private

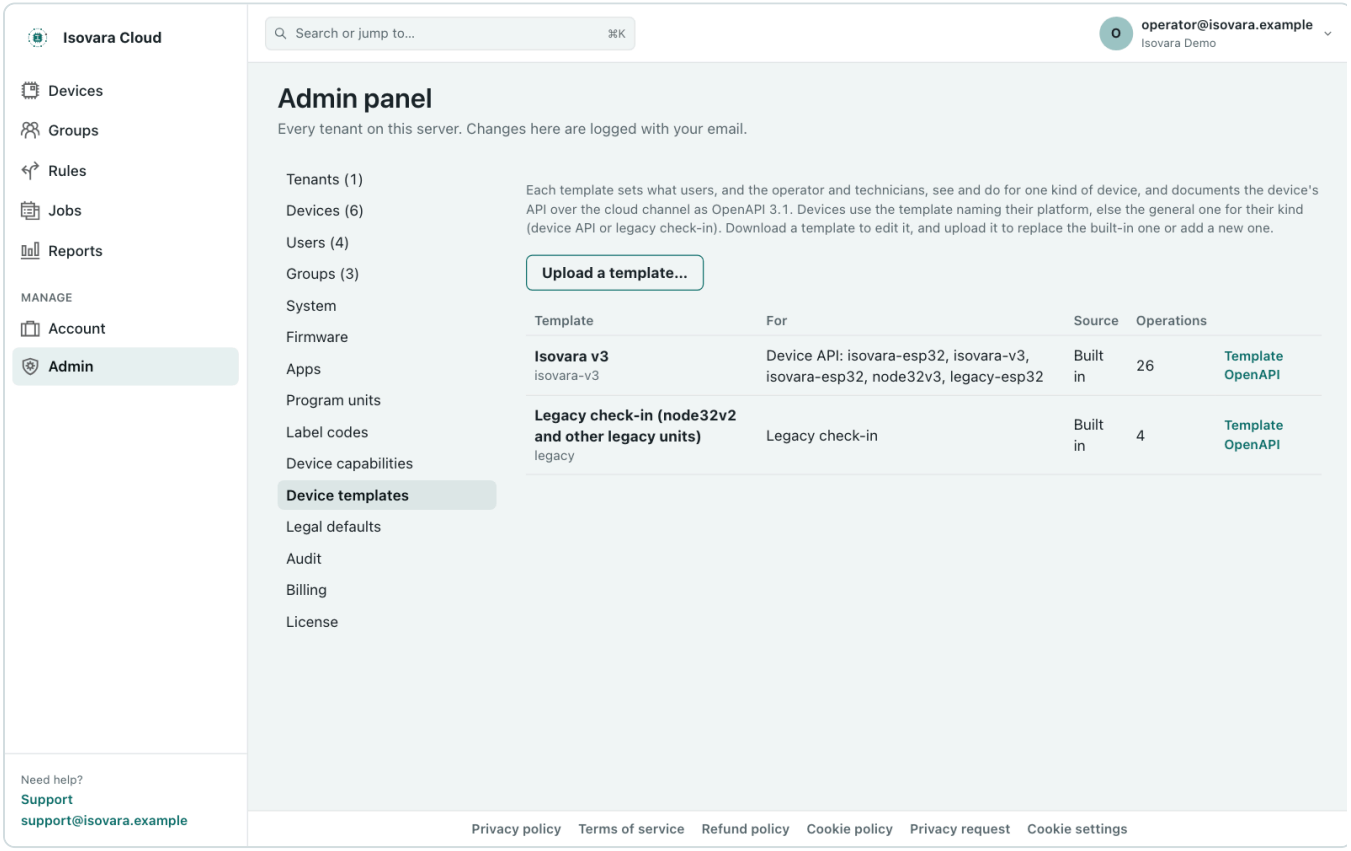
Certification also runs ten test scenarios, from "power on a factory unit and enter the label code" (enrolled within one minute) to "cut power during a download" (boots the old image and retries) and a 72-hour run with readings every 15 minutes (no missed reports, no memory leak).

What certification does not cover. Electrical safety, radio approvals (FCC, ISED, CE, UKCA), environmental ratings, measurement accuracy and product warranty remain the maker's responsibility. Certification states how the device behaves with Isovara Cloud, not that it is fit for a particular use.

The path to certification

1. **Join.** Sign the program agreement and NDA. You receive the Hardware Developer Guide, a staging tenant and a reserved platform ID such as `acme-t1`.
2. **Register your platform on staging.** Upload your capabilities file and device management template, and register your firmware's public signing key.
3. **Build and self-test.** Work through the checklist and the ten scenarios. The staging Admin panel shows what your device reports, its configuration and its update status.
4. **Submit.** Send the completed checklist, logs from the scenarios, the 72-hour run report, a signed release and [three] sample units.
5. **Lab review.** We repeat the scenarios on our staging install and send findings. Fix and resubmit as needed. Typical review time: [N weeks].

6. **Certified and listed.** You receive a certificate number and a license to use the mark. Your platform is registered in production and listed for operators.
7. **Stay certified.** Ship signed releases through the cloud and recertify when a trigger below applies.



A device management template gives each platform its own device page, built from an OpenAPI document of its operations.

Staying certified

Change	What you do
Minor firmware release (bug fixes, new extra fields)	Self-attest with the checklist changes; publish new extra fields
Major firmware version, or any change to enrollment, trust, credentials or the update path	Recertify the affected checklist areas
New hardware revision that changes radio, memory, storage or power	Recertify, including the 72-hour run
New device API protocol version	Recertify within [N months] of its release
Every year	Renewal attestation

If a certified product has an unresolved security problem after [N] days, its listing and the mark are suspended and operators are told. **Devices already in the field keep working.** The platform never cuts off customers' devices over a certification status.

Using the mark



- Use the seal that matches the product's class (Native or Reporting), with its certificate number nearby, for example "Isovara Certified Native · N32C-0001".
- Use it only on the certified product and its packaging, product page and datasheet. Not for uncertified variants, and not as a company badge.
- Do not redraw, recolor, stretch or crop it. Keep clear space of a quarter of its width on every side. Minimum size: 20 mm in print, 96 pixels on screen.
- Do not suggest that Isovara makes, sells or warrants your product.

The Isovara Ecosystem logo and its rules for use are in the logo kit.

Questions makers ask

Do we have to use an ESP32? No. Any microcontroller or embedded Linux device that meets the minimums in the guide qualifies. For a Native device that means holding one TLS session and an MQTT client open with room to spare. The Isovara v3 reference design is a floor, not a target.

Where do our devices connect? To whichever Isovara Cloud the operator runs: the hosted service or a licensed install on their own servers. Both run the same software.

Can operators put their own brand on our device? Yes, if your firmware supports the brand template and the `brand` and `brandfile` commands. One signed image serves every brand.

Who signs our firmware? You do, with your own offline key. We never hold your private key.

Our device has sensors Isovara doesn't know about. Declare them in your capabilities file and report them as extra fields. Operators can chart them and write rules on them.

What about devices we already shipped? Units already in the field with legacy firmware keep reporting through the legacy check-in. Certification applies to Class A and B firmware.

Get started

Apply to the Isovara Ecosystem program: [program contact: email, phone, web address to be added]

Read first: the Isovara Hardware Developer Guide (available under NDA) and the Isovara Cloud API guide.