

GateBeacon

Documentation

Official documentation for GateBeacon: account setup, device enrollment, application publishing, and support.

- [About GateBeacon](#)
- [Prerequisites](#)
- [Supported Operating Systems](#)
- [Creating Your GateBeacon Account](#)
- [Subscription Plans](#)
- [Enrolling a Linux Device](#)
- [Enrolling a Windows Device](#)
- [Publishing an App over HTTPS](#)
- [Publishing IIS Websites](#)
- [Other Catalog Applications](#)
- [Feedback & Support](#)
- [Frequently Asked Questions](#)

About GateBeacon

About GateBeacon

What GateBeacon Is

GateBeacon is a multi-tenant reverse-tunnel gateway platform. It lets you take an application running on a private device — a laptop, a home server, a small office machine — and publish it to the public internet as a secure HTTPS URL, without opening any inbound firewall port and without a static public IP address.

Once a device is enrolled, it connects **outbound only** to GateBeacon's cloud tunnel infrastructure:

- **Linux devices** connect using a lightweight [Rathole](#) client.
- **Windows devices** connect using a native SSH reverse tunnel (`ssh -R`).

From that point on, any local application you choose to publish is reachable through GateBeacon's edge, which terminates TLS and routes traffic back down the tunnel to your device.

Why It Exists

Traditionally, exposing a self-hosted application to the internet requires:

- A public IP address or port forwarding on your router.
- Manually obtaining and renewing a TLS certificate.
- Firewall changes that widen your attack surface.
- Extra effort if the device is behind CGNAT, a mobile hotspot, or a restrictive corporate network.

GateBeacon removes all of this. The device never accepts inbound connections — it only reaches out — so there is nothing new to open on your firewall, router, or ISP connection.

Key Benefits

Benefit	Detail
No inbound firewall changes	The device only makes outbound connections to GateBeacon.

Benefit	Detail
Automatic HTTPS	TLS certificates are issued and renewed by GateBeacon at the edge — you never touch a certificate.
Works behind NAT / CGNAT	No public IP or port forwarding required, including on mobile or carrier-grade NAT networks.
Cross-platform	Both Linux and Windows endpoints are supported.
One-click application catalog	Dozens of ready-to-run self-hosted applications (Nextcloud, Gitea, Grafana, and more) install with a single click.
Multi-tenant isolation	Each customer's devices, published applications, and data are logically isolated from every other customer.

Who GateBeacon Is For

GateBeacon is built for individuals, teams, and small businesses who want to self-host applications on hardware they already control — and reach those applications securely from anywhere — without taking on cloud hosting costs, networking expertise, or certificate management.

Where to Go Next

- New to GateBeacon? Continue to [Prerequisites](#) and [Supported Operating Systems](#) to confirm your device is compatible.
- Ready to sign up? See [Creating Your GateBeacon Account](#).
- Already have an account? Jump to [Enrolling a Linux Device](#) or [Enrolling a Windows Device](#).

Prerequisites

Prerequisites

Before enrolling a device, confirm it meets the requirements below. The install scripts perform some of these checks automatically and will stop with a clear error if a hard requirement is missing.

Hardware

- Any machine capable of running your target application(s) is sufficient — GateBeacon's own footprint is a lightweight background connector process.
- As a practical minimum, keep at least **1 vCPU and 1 GB of RAM** free beyond what your published applications need.
- If you plan to install multiple catalog applications, budget more — each one runs as its own Docker container.

Software

Linux

- Root or `sudo` access to run the installer.
- One of the [supported distributions](#) (see Supported Operating Systems).
- `systemd` — GateBeacon's background services run as systemd units.
- Docker — installed automatically by the setup script if not already present.
- The installer also provisions its own supporting utilities (`curl`, `tar`, `unzip`, `ufw`, `iproute2`, `jq`, `kmod`) if missing.

Windows

- Administrator rights to run the installer.
- The **Windows OpenSSH Client** optional feature — installed automatically if not already enabled.
- PowerShell (built in to all supported Windows versions).

Network

- **Outbound HTTPS (443) connectivity** from the device to GateBeacon's API and tunnel endpoints. No inbound port needs to be opened on your router or firewall.
- Working DNS resolution on the device — the Linux installer explicitly checks IP configuration, internet reachability, and DNS resolution before proceeding, and will stop with an error if any of these fail.
- If the device sits behind a network that blocks outbound 443 (some locked-down corporate networks or proxies), the tunnel cannot be established — check with your network administrator first.

Things That Are Not Supported

- **Non-apt Linux distributions.** RHEL, CentOS, Fedora, openSUSE, Arch, and similar are not currently supported by the automated installer — see [Supported Operating Systems](#) for the exact distribution list.
- **Offline / air-gapped installation.** Both the installer and the ongoing tunnel connection require internet access; there is no offline install path.
- **Cloned VM images with a shared identity.** Linux device identity defaults to `/etc/machine-id`. If you clone a VM or disk image and enroll multiple copies without regenerating this file, GateBeacon detects the collision and issues the second device a new identity automatically — this is handled safely, but it means the second device will **not** appear as the same device record as the first. If you intend to enroll multiple devices from the same image, regenerate `/etc/machine-id` on each clone before enrollment (for example, `sudo rm /etc/machine-id && sudo systemd-machine-id-setup`).

Before You Continue

Once your device meets the above, proceed to [Creating Your GateBeacon Account](#) if you don't have one yet, or straight to [Enrolling a Linux Device](#) / [Enrolling a Windows Device](#).

Supported Operating Systems

Supported Operating Systems

Linux

The Linux installer identifies your distribution from `/etc/os-release` and only proceeds on an explicitly supported combination:

Distribution	Supported Versions
Ubuntu	20.04, 22.04, 24.04
Debian	11, 12, 13
Linux Mint	20, 21, 22
Pop!_OS	20.04, 22.04, 24.04
Zorin OS	16, 17, 18
elementary OS	6, 7, 8

Any other distribution ID causes the installer to stop immediately with an unsupported-OS error, rather than attempting a best-effort install.

Additional Linux requirements:

- **apt-based systems only.** The installer uses `apt-get` for package management and Docker's Ubuntu/Debian repositories (with derivative distributions falling back to the underlying Ubuntu codename). RHEL/CentOS/Fedora/openSUSE/Arch and other non-apt distributions are not currently supported.
- **systemd is required.** GateBeacon's background services (tunnel client, terminal access, route sync) run as systemd units.

Windows

There is no hard-coded Windows version check in the installer, but functionality depends on the **Windows OpenSSH Client** optional feature, which is available starting with:

- Windows 10, version 1809, or later
- Windows Server 2019, or later

Earlier Windows releases are not supported. The installer will attempt to enable the OpenSSH Client feature automatically if it is not already present, but this requires the underlying Windows version to support it.

Additional Windows requirements:

- Administrator rights are required to run the installer.

Known Limitations

- **ARM devices are not officially validated.** There is no documented ARM-specific packaging for either platform. If you plan to enroll ARM hardware (for example, a Raspberry Pi), check with support before relying on it in production.
- **Platform-specific catalog apps.** The **IIS Web Server** catalog application is Windows-only. Most other catalog applications are Docker-based and Linux-only. **App Publishing HTTPS** is the one catalog entry that works identically on both platforms. See [Other Catalog Applications](#) for the full per-app platform matrix.

Next Steps

Confirm your device matches the table above, then continue to [Enrolling a Linux Device](#) or [Enrolling a Windows Device](#).

Creating Your GateBeacon Account

Creating Your GateBeacon Account

Follow these steps to create a new GateBeacon account and organization.

Step 1 — Start Sign-Up

Go to www.gatebeacon.com and click **Sign Up**.

Step 2 — Enter Your Details

Provide the following:

- **Email address** — used as your login and for account verification.
- **Password** — minimum 10 characters.
- **Full name**
- **Organization details** — company name, company size, job title, and a contact phone number.

An organization (referred to internally as a *tenant*) is created for you automatically from these details — you don't need to set anything up separately.

Step 3 — Verify Your Account

GateBeacon sends a one-time verification code to the email address you provided. Enter the code (or follow the verification link, depending on the sign-up flow you're shown) to activate your account.



Important: your account cannot log in until verification is complete. If you don't receive a code within a few minutes, check your spam folder, or use the resend option on the verification screen. Use a real, reachable email address when signing up.

Step 4 — Log In

Once verified, log in at www.gatebeacon.com with your email and password.

Step 5 — You're In

You'll land on the customer portal dashboard. New accounts start on the free **Community** plan by default. See [Subscription Plans](#) to compare tiers and upgrade if you need more devices or published applications.

Next Steps

- Confirm your device meets the [Prerequisites](#) and is a [supported operating system](#).
- Continue to [Enrolling a Linux Device](#) or [Enrolling a Windows Device](#) to connect your first device.

Subscription Plans

Subscription Plans

GateBeacon offers three plans. Pricing is in INR and excludes GST.

Plan Comparison

	Community (Free)	Standard	Premium
Price	Free	₹199 / month or ₹2,220 / year	₹399 / month or ₹4,500 / year
Devices	1	1	3
Published applications	1	10	10
App units	6	50	50
Bandwidth per app	20 Mbps	100 Mbps	200 Mbps
Total reserved bandwidth	—	—	600 Mbps
Premium data policy	No	No	Yes

"App units" is GateBeacon's internal capacity measure covering catalog application installs; each catalog app consumes a share of your plan's app-unit allowance.

Choosing a Plan

- **Community** is a good fit for trying GateBeacon out, or for a single always-on personal project.
- **Standard** suits a single device running several published applications.
- **Premium** is intended for setups that span multiple devices — for example, a home server and a small office machine — with higher bandwidth needs.

Upgrading

1. In the customer portal, go to **Subscription**.
2. Choose the plan you want and click **Choose Standard** or **Choose Premium**.
3. You'll be redirected to a secure Cashfree checkout page. A coupon code field is available if you have one.

4. Complete payment. Your new plan limits apply immediately — no manual activation step is required.

Downgrading

- From **Premium**, use **Downgrade to Standard**.
- To move to the free **Community** plan, use the guided **Community Downgrade** flow. If your current usage exceeds Community's limits (for example, more than one enrolled device or published app), you'll need to reduce usage to fit before the downgrade can complete.

Cancelling

Use **Cancel Subscription** in the Subscription section, then confirm with **Yes, cancel subscription**. Your paid plan remains active until the end of the current billing period, after which your account reverts to Community limits.

Next Steps

Once you're on the plan you need, continue to [Enrolling a Linux Device](#) or [Enrolling a Windows Device](#).

Enrolling a Linux Device

Enrolling a Linux Device

This guide walks through connecting a Linux device to GateBeacon. Confirm your distribution is listed in [Supported Operating Systems](#) before you begin.

Step 1 — Start the Enrollment Wizard

1. Log in to the customer portal and go to **Devices**.
2. Click **Add your device**.
3. On **Step 1 — Select device operating system**, choose **Linux**.
4. Review and check the box agreeing to GateBeacon's Terms & Conditions and Acceptable Use Policy.
5. Click **Next**. This generates a one-time enrollment token and moves you to Step 2.

Step 2 — Run the Installation Command

1. On **Step 2 — Installation command**, click **Copy command** to copy the one-line install command to your clipboard.
2. Open a terminal on the target Linux machine with root or `sudo` access.
3. Paste and run the command.

The installer will, in order:

1. Check IP configuration, internet connectivity, and DNS resolution.
2. Install required packages (`curl`, `tar`, `unzip`, `ufw`, `iproute2`, `jq`, `kmod`) and Docker, if not already present.
3. Register the device with GateBeacon using your enrollment token.
4. Start the Rathole tunnel client and GateBeacon's background systemd services.

Step 3 — Confirm Enrollment

Back in the portal wizard, **Step 3** will show "**Congratulations. NovaEdge Device enrolled successfully.**" once the device checks in. Click **Close**. Your device now appears in the **Devices** list with an **Online** status.

Notes

- **Enrollment tokens are single-use and time-bounded.** If the command expires before you run it, go back to Devices and generate a new one.
- **Re-running the installer is safe.** If you run the install command again on a device that's already enrolled, it re-uses the device's existing identity and tunnel token rather than creating a duplicate — useful for updating or repairing an existing installation.
- **Cloned VMs:** if this device was cloned from another machine's disk image, regenerate

`/etc/machine-id` first — see [Prerequisites](#).

Next Steps

With your device online, you can:

- Install a ready-made application from the catalog — see [Other Catalog Applications](#).
- Publish an application you already run on the device — see [Publishing an App over HTTPS](#).

Enrolling a Windows Device

Enrolling a Windows Device

This guide walks through connecting a Windows device to GateBeacon using a native SSH reverse tunnel. Confirm your Windows version meets the minimum in [Supported Operating Systems](#) before you begin.

Step 1 — Start the Enrollment Wizard

1. Log in to the customer portal and go to **Devices**.
2. Click **Add your device**.
3. On **Step 1 — Select device operating system**, choose **Windows**.
4. Review and accept the Terms & Conditions and Acceptable Use Policy.
5. Click **Next** to generate a one-time enrollment token and advance to Step 2.

Step 2 — Run the Setup Command

1. Click **Copy full command** to copy the one-time PowerShell setup command.
2. On the Windows device, open **PowerShell as Administrator**.
3. Paste and run the command.

The installer will:

1. Install the **Windows OpenSSH Client** optional feature, if it isn't already enabled.
2. Generate a dedicated ed25519 SSH keypair directly on the device. The private key never leaves the device, and its file permissions are restricted to the Administrators group so the background scheduled task (which runs as SYSTEM) can use it.
3. Register the device with GateBeacon, sending the newly generated public key.
4. Receive back an assigned SSH username, a dedicated remote port, and the tunnel server's host-key fingerprint — the device pins this fingerprint rather than trusting it on first use.
5. Install and start a scheduled task that keeps the reverse SSH tunnel connected in the background.

Step 3 — Confirm Enrollment

The wizard will show the same success confirmation once the device checks in, and the device will appear in **Devices** with an **Online** status.

How the Tunnel Is Secured

Each device's SSH key is scoped so it can **only** open its one assigned remote port — it cannot open an interactive shell on GateBeacon's infrastructure, and it cannot reach any other device's tunnel. This scoping happens automatically; there's nothing to configure.

Next Steps

- Publishing an IIS website: see [Publishing IIS Websites](#).
- Publishing any other local HTTP application: see [Publishing an App over HTTPS](#).

Publishing an App over HTTPS

Publishing an App over HTTPS

App Publishing HTTPS converts any local HTTP port on an enrolled device into a public HTTPS URL. GateBeacon handles SSL entirely at the edge — the application itself does not need to know anything about TLS.

It is available on both Linux and Windows devices, and is one of the few catalog entries you can install more than once on the same device — so you can publish several independent local ports as separate public URLs.

Step by Step

1. In the customer portal, go to your device's application list and choose **App Publishing HTTPS** from the catalog (or **Publish a custom app**, if shown separately).
2. Enter:
 - **Local port** — the port your application listens on, on that device. If left blank, it defaults to `127.0.0.1:8080`.
 - **Label** — becomes part of your generated public hostname.
3. Save. GateBeacon automatically provisions a DNS record and a routing rule for the new hostname — you don't create either manually.
4. Your app becomes reachable at the generated HTTPS URL within roughly **10 seconds**, once the tunnel VM picks up the new route. First-time TLS certificate issuance can add a little more time on top of that.

Multiple Publishing Deployments

Unlike most catalog apps — which can only be installed once per device — App Publishing HTTPS supports multiple independent installs on the same device. Use this to publish, for example, a personal wiki on one port and a media server on another, each as its own HTTPS URL.

Limits

The number of applications you can publish is capped by your subscription plan:

Plan	Published apps
Community	1
Standard	10
Premium	10

See [Subscription Plans](#) for full plan details.

Defaults

- Local target defaults to `http://127.0.0.1:8080` if you don't specify a port.
- Point the local port field at whatever port your application actually listens on — it does not have to be 8080.

Understanding the Limitations

- **Route propagation is not instant.** Allow up to about 10 seconds for a new route to go live, and a little longer for first-time certificate issuance, before troubleshooting further.
- **Large uploads.** Very large file uploads through a published app can be sensitive to network-level timeouts. If you consistently see uploads fail partway through, contact support — this may need a longer timeout configured on your specific route.
- **The device must actually be listening.** Publishing a port doesn't start anything on the device — the local application must already be running and bound to the port you configured.

Basic Troubleshooting

Symptom	Check
App unreachable at its public URL	Confirm the device shows Online in the portal.
App unreachable at its public URL	Confirm the local application is actually running and listening on the configured port (not just installed).
App unreachable at its public URL	Confirm no local firewall on the device is blocking loopback/local traffic to that port.
New route seems to not exist yet	Wait roughly a minute after saving before troubleshooting — propagation and certificate issuance are not instantaneous.

Symptom	Check
Upload fails partway through on a large file	Contact support — large uploads can hit network-level timeouts that may need adjustment for your route.

Next Steps

Looking to publish an IIS website specifically? See [Publishing IIS Websites](#) instead — it uses a dedicated catalog app tailored to IIS.

Publishing IIS Websites

Publishing IIS Websites

GateBeacon includes a dedicated **IIS Web Server** catalog application for publishing Microsoft IIS sites from a Windows device. This app is **Windows-only**.

Step by Step

1. On an already-enrolled Windows device (see [Enrolling a Windows Device](#)), open the catalog in the customer portal and choose **IIS Web Server**, then **Install**.
2. The installer checks for an existing IIS installation:
 - If IIS is **already installed**, it is left as-is and simply connected to GateBeacon's routing.
 - If IIS is **not installed**, GateBeacon installs the required Windows features (Web Server Role, Common HTTP Features, Default Document, Directory Browsing, and related IIS sub-features) automatically via DISM.
3. On a fresh install, GateBeacon replaces the default IIS welcome page with a GateBeacon-branded placeholder page, then restarts IIS.
4. GateBeacon publishes the site securely over HTTPS on port 443 at the network edge. **IIS itself continues to serve plain HTTP on `127.0.0.1:80` locally** — you do not configure a certificate inside IIS at all.
5. Deploy your website content into IIS as you normally would (default site root, or your own site and bindings). GateBeacon forwards public HTTPS traffic to whatever IIS serves on port 80.

Defaults

- Local target: `http://127.0.0.1:80`.
- If your IIS site is bound to a different local port, update the port field when installing/configuring the app to match.

Limitations

- **One IIS publish per device.** Unlike App Publishing HTTPS, the IIS Web Server catalog app is not designed for multiple installs on the same device. To serve multiple sites, use IIS's own host headers or bindings under a single site rather than expecting separate GateBeacon entries per site.
- **Health checks use a basic TCP connect**, not an HTTP status check — IIS can legitimately return a wide range of status codes for its default or a custom page, so GateBeacon only verifies that

something is listening on the port rather than checking for a specific response.

- **Do not configure HTTPS bindings inside IIS.** Public visitors never connect to IIS directly — GateBeacon's edge is what terminates TLS. Keep IIS itself on plain HTTP; adding your own HTTPS binding inside IIS has no effect on what the public sees and is unnecessary.

Basic Troubleshooting

Symptom	Check
Site unreachable after install	Confirm the World Wide Web Publishing Service is running (<code>services.msc</code>).
Site unreachable after install	Confirm your site is actually bound to port 80 — not a different port than the one GateBeacon is targeting.
Placeholder GateBeacon page still showing	Your own content hasn't been deployed to the IIS site root yet — deploy your site files, IIS will serve them once in place.
Device shows Online but site is down	Check IIS locally on the device first (<code>http://127.0.0.1</code> on the device itself) before assuming a GateBeacon-side issue.

Next Steps

Need to publish something other than an IIS site — a custom app, another local service — from this same device? See [Publishing an App over HTTPS](#).

Other Catalog Applications

Other Catalog Applications

Beyond App Publishing HTTPS and IIS Web Server, GateBeacon's catalog includes over 45 additional one-click applications. Each runs as a Docker container on a Linux device and is published over HTTPS automatically, the same way as App Publishing HTTPS.

How Installation Works

1. On an enrolled Linux device, open the catalog in the customer portal.
2. Choose an application and click **Install**.
3. GateBeacon pulls the container image, starts it on your device, and provisions a public HTTPS URL for it — no manual Docker commands required.

Most catalog applications can only be installed **once per device**. If you need multiple instances of the same application, enroll an additional device.

Catalog by Category

Category	Applications
Collaboration	Nextcloud, Immich, Excalidraw, ONLYOFFICE Docs, Mattermost, HedgeDoc
Productivity	Paperless-ngx, Joplin Server, Plane, Formbricks
Finance	Actual Budget, Firefly III, Invoice Ninja
Security	Vaultwarden, Authentik, Wazuh
Analytics	Metabase, Grafana, Apache Superset, Prometheus
AI	Open WebUI, SearXNG, Langflow, Flowise
Development	Gitea, Forgejo, code-server, Hoppscotch, pgAdmin
Infrastructure	Portainer, Jenkins, Headlamp
Automation	n8n, Node-RED
Web / CMS	WordPress, October CMS
Education	Moodle, OpenSIS, Anki Sync Server
Healthcare	OpenEMR

Category	Applications
Community	ChurchCRM
Storage	MinIO
Knowledge base	Wiki.js
CRM / ERP	Twenty CRM, ERPNext

The exact catalog available to your account may vary slightly by plan and platform — check the **Catalog** section in the portal for the current, complete list.

A Note on Single Sign-On

Authelia is not currently offered as a catalog application. If you're evaluating GateBeacon and were expecting a site-wide single sign-on layer across all your published apps, that specific capability isn't available today.

Authentik is available as a standalone identity-provider application — it offers SSO, OAuth2, SAML, and LDAP — but it is a self-contained app you install and configure yourself, like any other catalog entry. It is not automatically wired into your other published applications as a shared login layer.

Next Steps

- Have feedback on an app you'd like to see added? See [Feedback & Support](#).
- Common questions about catalog apps and publishing are answered in the [FAQ](#).

Feedback & Support

Feedback & Support

We want to hear about anything that isn't working the way you expect, and any capability you wish GateBeacon had.

Submitting Feedback

1. Log in to the customer portal.
2. Go to the **Feedback** section in the sidebar.
3. Submit a new ticket describing your question, issue, or suggestion.
4. Track the status and any replies directly in the same section — you don't need a separate email thread.

This is the fastest way to reach the GateBeacon team, since your ticket is automatically tied to your account and device context, which helps us investigate faster.

What to Include

To help us resolve issues quickly, include where relevant:

- The **device name** (as shown in the portal) involved.
- The **application or catalog app** affected.
- What you expected to happen, and what actually happened.
- Any error message shown, verbatim.
- Roughly when the issue occurred.

Before You Submit

For common questions, check the [FAQ](#) first — many day-to-day questions about devices, publishing, and plans are already answered there.

Feature Requests

Feature requests (including requests for new catalog applications) are welcome through the same Feedback section. We review these regularly when prioritizing the catalog and platform roadmap.

Frequently Asked Questions

Frequently Asked Questions

Do I need to open any ports on my router or firewall?

No. Devices connect to GateBeacon **outbound only**. There is nothing to forward or open inbound.

Does my device need a public or static IP address?

No. GateBeacon works behind NAT, CGNAT, and most home or mobile connections, as long as outbound HTTPS (443) is reachable.

What operating systems are supported?

Ubuntu, Debian, Linux Mint, Pop!_OS, Zorin OS, and elementary OS on specific versions for Linux; Windows 10 (1809+) and Windows Server 2019+ for Windows. See [Supported Operating Systems](#) for the exact version list.

Can I enroll a Raspberry Pi or other ARM device?

ARM hardware is not officially validated today. Check with support before relying on it for production use.

Why does my second cloned VM show up as a different device?

Linux device identity is derived from `/etc/machine-id`. If you clone a VM or disk image without regenerating this file, GateBeacon detects the collision and automatically assigns the second device a fresh identity rather than merging it with the first. Regenerate `/etc/machine-id` on clones before enrolling — see [Prerequisites](#).

How long does it take for a newly published app to go live?

Typically around 10 seconds for the routing rule to propagate, plus a little more time on the very first publish while a TLS certificate is issued.

Can I publish more than one application from a single device?

Yes, using **App Publishing HTTPS**, which supports multiple independent installs on the same device — each with its own local port and public URL. Most other catalog apps are limited to one install per device.

What happens if I exceed my plan's device or app limit?

You won't be able to enroll an additional device or publish an additional application beyond your plan's limit. Upgrade your plan from the **Subscription** section in the portal — see [Subscription Plans](#).

How do I downgrade from Premium or Standard to the free Community plan?

Use the guided **Community Downgrade** flow in **Subscription**. If your current usage (devices, published apps) exceeds Community's limits, you'll need to reduce it first before the downgrade can complete.

Does GateBeacon manage TLS certificates for me?

Yes, entirely. TLS is terminated at GateBeacon's edge; your application and device never need a certificate of their own.

Is there a single sign-on option across all my published apps?

Not currently. Authelia (which previously provided this) is no longer offered. **Authentik** is available as a standalone identity-provider catalog app you can install and configure yourself, but it does not automatically apply to your other published apps.

My published app is unreachable — where do I start?

Check, in order: (1) the device shows **Online** in the portal, (2) the local application is actually running and listening on the port you configured, (3) no local firewall on the device is blocking loopback traffic to that port, (4) you've waited roughly a minute since publishing or making changes. See [Publishing an App over HTTPS](#) for the full troubleshooting table.

How do I get help beyond this documentation?

Submit a ticket through the **Feedback** section of the customer portal — see [Feedback & Support](#).