

INSTALL GUIDE · EVERY EXTRA SITE

Add a collector on Linux

Put a collector at another office, data closet or customer site so Uplivra can check the devices there. One copy-and-paste command on any Linux computer, including a Raspberry Pi.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 25 September 2026 · Latest version:
<https://uplivra.com/guides/collector-linux.html>

What a collector does

A **collector** is the Uplivra program running on an always-on computer at a site. It checks the devices at that site and sends the results to your Uplivra server over encrypted HTTPS. The collector always connects **out** to the server, so you don't need to open ports at the remote site.

Your server already has a collector for its own site. Add one for each other location.

Before you start

- **A computer at the site** that stays on: a small PC, a virtual machine, or a Raspberry Pi 4 or 5. For up to 100 devices, **2 CPU cores, 4 GB memory and a 32 GB disk** is plenty (minimum 2 GB and 16 GB).
- **Linux** on it: Ubuntu 22.04, 24.04 or 26.04, or Debian 12. Raspberry Pi OS (64-bit) works too.
- It must reach your Uplivra server's address on port **8443**, for example across a site-to-site VPN or the internet.
- An administrator sign-in to the Uplivra web interface.

Step 1: Create the site

In Uplivra, open **Settings > Sites and collectors**. If the site isn't there yet, add it (for example "Branch East").

Step 2: Get the install command

On the site, click **Connect a collector**, then **Linux computer**. Uplivra shows a single line starting with `curl`. Click **Copy to clipboard**.

The line contains a **one-time setup code** that works for 24 hours, and your server's certificate fingerprint, so the collector only ever downloads from, and connects to, your server.

Step 3: Run it on the collector computer

Open a terminal on that computer, or connect to it with `ssh` from your PC. Paste the line and press Enter. If it asks for a password, type your password for that computer (nothing shows while you type).

It asks you to accept the terms of service (type `I agree`) and which port to use for the collector's own status page (press Enter for 8444, see below), then installs and connects. If you chose a port, it asks for a password for that page. After about 30 seconds you'll see:

```
Done. This computer appears under Settings > Sites and collectors in Uplivra within a minute.
```

Step 4: Check it's connected

Back in Uplivra, **Settings > Sites and collectors** shows the collector with its version and "just now" under **Last report**. Now add devices at that site, or run a Discovery scan there.

Sites and collectors

A **site** is a location, such as an office or a data closet. Each site needs a **collector**: the Uplivra program running on any always-on computer there. It does the checking and reports back here.

Branch East ► Rename

COLLECTOR	COMPUTER	VERSION	LAST REPORT
Branch East collector	h	test	just now

[Edit](#)

Connect a collector at Branch East

☐ Receive traffic flows here

NetFlow / IPFIX port: sFlow port: [Save](#)

The collector listens on these UDP ports. Point your router or firewall's flow export at h.

☐ Receive syslog here

Port (UDP and TCP): [Save](#) Point your devices' syslog at h. [How to send logs from common devices.](#)

Data Center ► Rename

COLLECTOR	COMPUTER	VERSION	LAST REPORT
Data Center collector	h	test	just now

[Edit](#)

Connect a collector at Data Center

☐ Receive traffic flows here

NetFlow / IPFIX port: sFlow port: [Save](#)

The collector listens on these UDP ports. Point your router or firewall's flow export at h.

Sites and collectors, each with its collector and when it last reported. Demo data

The collector's status page

During install you're asked for a **port for the collector's HTTPS status page** (press Enter for **8444**, or type **0** to leave it off) and a password for it. Open `https://<collector address>:<port>/` in a browser, accept the certificate warning the first time (the collector made its own certificate), and sign in. The page shows:

- whether the collector is reaching your Uplivra server, when it last did, and the last error if not, with a **Check the connection now** button;
- its version, roles, clock, disk space and, for log collectors, log storage;
- `/healthz`, which answers "ok" without signing in while the server is reachable, for load balancers or other monitoring.

It's most useful exactly when the collector can't reach the server. Sessions end after 30 minutes without activity, and five wrong passwords lock that address out for 15 minutes. To change the port or password, turn it off, or limit it to your admin network:

```
sudo uplivra status-page -port 8444
sudo uplivra status-page -allow 10.0.0.0/24
sudo uplivra status-page -port 0
```

A trusted certificate for the status page

To stop the browser's "not private" warning, give the page a real certificate. On the collector's page in Uplivra (**Settings > Sites and collectors**, click the collector), under **Status page certificate**, choose one:

- **Let's Encrypt, automatic (recommended)**: free and trusted everywhere. Uplivra gets and renews it through your Cloudflare DNS, so the collector never needs to be reachable from the internet. Set up the Cloudflare token once under **Settings > Certificates > Let's Encrypt**, then type a name such as `status.yourcompany.com` and save.
- **Let's Encrypt with certbot on the collector**: for a collector that certbot can already reach, for example one running nginx with port 80 open to the internet. Save the choice, then run on the collector: `sudo uplivra status-page -certbot status.yourcompany.com`. Certbot renews it and every renewal reaches the page.
- **Your company certificate**: the one marked for collectors under **Settings > Certificates**.

Then open the page by that name, for example `https://status.yourcompany.com:8444/`. Inside your network the name must point at the collector's address: add a DNS record for it in your router or domain controller (or in Cloudflare, pointing at the collector's inside address).

Two collectors for one site (failover)

Install a second collector at the same site the same way. Both connect; the one with the **lowest failover priority** (on the collector's page) does the checking, and the other stands by. If the active one goes quiet for about 3 minutes, the standby takes over, and hands back when the first returns.

Using a public or company certificate

If your Uplivra server uses a certificate from a public or internal certificate authority (see **Settings > Certificates**), the collector can trust that instead of a fingerprint. Run the collector setup by hand and choose "My company's certificate authority" or "A public certificate authority":

```
sudo uplivra setup
```

Choose **Collector**, give the server address and setup code, and pick the trust option you need.

Note: Choose "no" at "Use TLS 1.3 only with post-quantum key exchange" only if a firewall or proxy between the collector and the server inspects HTTPS traffic and can't handle it.

Running it together with a log collector

To also receive logs on this computer, choose **Collector and log collector** in `sudo uplivra setup`. See [Install a log collector](#) for sizing: logs need their own disk.

Troubleshooting

What you see	What to do
"Could not download from ..."	This computer can't reach the server on port 8443. Check the VPN, firewall, or the address
"The setup code is missing"	Copy the whole line again; codes are one-time and expire after 24 hours
Collector stays "never"	Check <code>systemctl status uplivra-collector</code> and <code>sudo journalctl -u uplivra-collector -n 50</code>
Status page doesn't open	Check the port with <code>sudo uplivra status-page</code> , that a firewall between you and the collector allows it, and that you used <code>https://</code>
Clock warnings	The collector's clock is off. It uses the time servers you set; see Settings > Time

Remove a collector

On its page in Uplivra, remove it; then on the computer:

```
sudo systemctl disable --now uplivra-collector
```