INSTALL GUIDE · LOG INTELLIGENCE

# Install a log collector

Set up a computer that receives syslog from your firewalls, switches and servers and keeps it encrypted, searchable and tamper-evident, with off-site copies. Includes how much storage you need.

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

## Separate computer, or together with a collector?

The same Uplivra program can be a collector, a log collector, or both. **We recommend a separate computer (or virtual machine) with its own disk for logs**:

- a burst of log messages can never fill the disk the collector or server needs;
- you can size and back up the log disk on its own;
- in a PCI or HIPAA environment the log store is easier to protect.

**Collector and log collector on one computer** is fine for small sites (up to about 25 devices sending logs), as long as the logs go on their **own disk**.

## How much storage you need

Uplivra keeps logs compressed. A typical mix of firewalls, switches and servers sends about **3 messages a second per device**; after compression, each message takes about 60 bytes on disk.

| Devices sending logs | Stored per day | 90 days | 365 days | Suggested log disk |
|---|---|---|---|---|
| 25 | 0.4 GB | 36 GB | 150 GB | 250 GB SSD |
| 100 | 1.6 GB | 146 GB | 590 GB | 1 TB SSD |

| Devices sending logs | Stored per day | 90 days | 365 days | Suggested log disk |
|---|---|---|---|---|
| 500 | 8 GB | 730 GB | 3 TB | 4 TB, or 1 TB with off-site archive |

These are estimates: a firewall that logs every allowed connection can send ten times more. Setup does this calculation for your numbers, and after a week Uplivra shows your real volume and how many days until the disk is full.

**How long to keep logs:**

| Rule | Keep | Always searchable |
|---|---|---|
| PCI DSS 10.5.1 | 12 months | The last 3 months |
| HIPAA (documentation rule, often applied to logs) | 6 years | Your choice; keep older years off-site |
| SOC 2 | Usually 12 months | — |
| CIS Controls 8.10 | 90 days | 90 days |

**Computer:** for up to 100 messages a second (about 30 devices), 2 CPU cores, 8 GB memory and a 500 GB SSD. For 1,000 a second, 4–6 cores, 16 GB and 2 TB. Always use SSD; never a Raspberry Pi's SD card.

## Step 1: Add a disk for logs

In your virtual machine settings, add a second disk of the size above. On the Linux computer, find it and prepare it (this **erases** that disk, so check the name):

```
lsblk
```

The new disk is the one with no partitions, for example `sdb`. Then:

```
sudo mkfs.ext4 -L uplivra-logs /dev/sdb
sudo mkdir -p /var/lib/uplivra-logs
echo 'LABEL=uplivra-logs /var/lib/uplivra-logs ext4 defaults,noatime 0 2' | sudo tee -a
/etc/fstab
sudo mount -a
df -h /var/lib/uplivra-logs
```

The last line should show the new disk's size.

## Step 2: Install

Follow steps 1–3 of Install the Uplivra server to copy and start the installer (`sudo bash install.sh`). Then:

| Question | Answer |
|---|---|
| What should this computer be? | **Log collector**, or **Collector and log collector** |
| Number of devices sending logs | Your estimate. Setup shows the storage it needs |
| Days of logs to keep | 365 for PCI DSS; 90 for CIS; 2190 for six years |
| Folder for log storage | `/var/lib/uplivra-logs` (the disk from step 1) |
| Server address and setup code | From Uplivra: **Settings › Sites and collectors › your site › Connect a collector** |
| Trust the server's certificate | Check the fingerprint matches the one Uplivra shows, or choose your CA |

The network and time questions are the same as for the server. **Correct time matters for logs**: point it at the same time servers as your devices.

## Step 3: Send logs to it

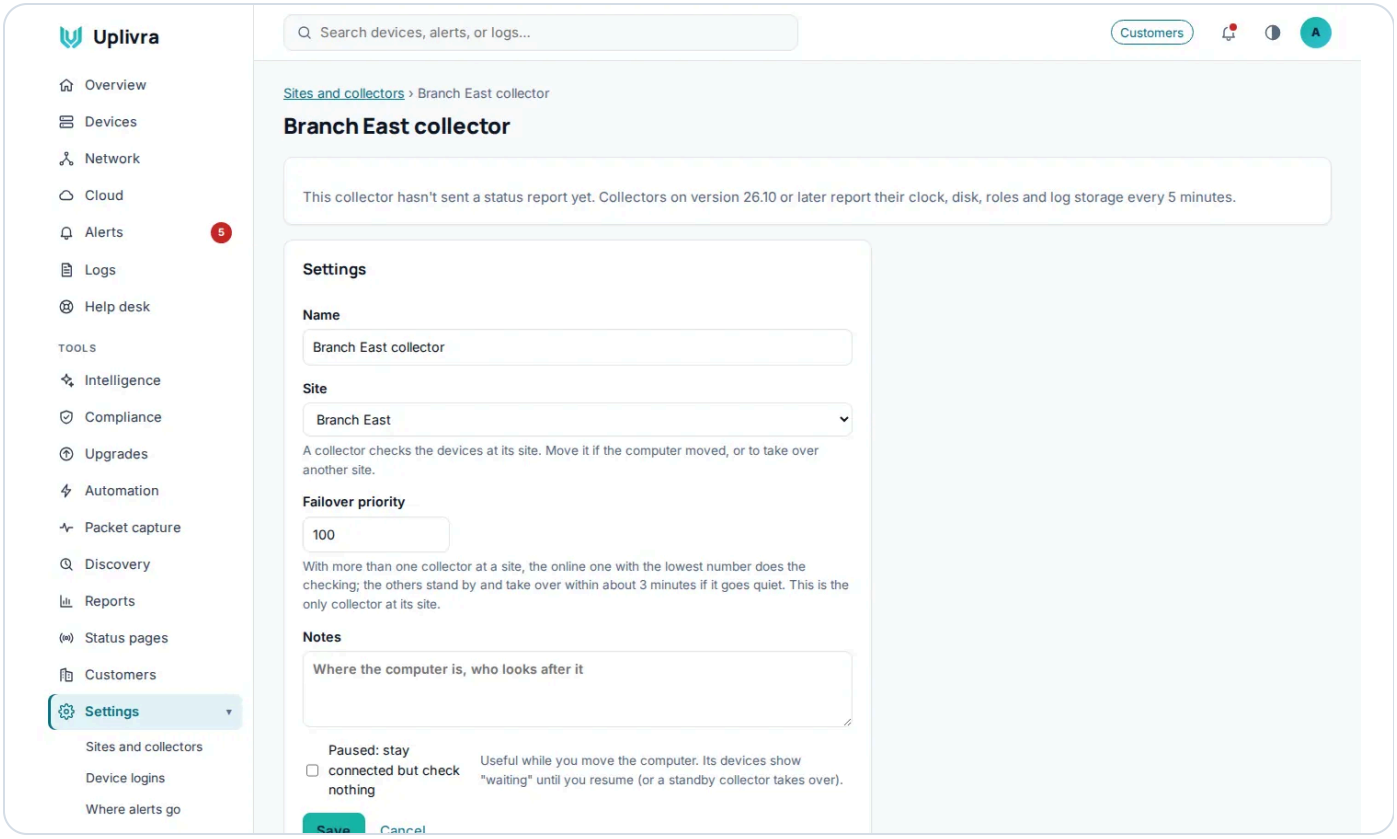
On the site's page in Uplivra (**Settings › Sites and collectors**), tick **Receive syslog here** and save. Then point each device's syslog at the log collector's address, port **514** (UDP or TCP). **Settings › Sites and collectors › How to send logs from common devices** has the exact settings for common firewalls, switches, Windows and Linux.

Messages appear under **Logs** within a minute.

## Step 4: Set retention, warnings and off-site copies

Open the log collector's page (**Settings › Sites and collectors**, click its name):

- **Retention:** pick Recommended, PCI DSS, HIPAA, CIS Controls or your own numbers. The protected period is never deleted to make room; Uplivra warns you instead.
- **Warning level:** a warning when the disk is 75% full (you can change it) or will fill within 30 days.
- **Off-site copy:** Amazon S3 (turn on **Object Lock** on the bucket so copies can't be deleted early), Azure Blob Storage with a SAS link, S3-compatible storage such as Backblaze B2, Wasabi or MinIO, or a network folder. Click **Test** before saving.




The log storage settings on a collector's page. Demo data

## Encryption and the log key

Every hourly archive is encrypted with AES-256-GCM. The key is created on the log collector and a copy is kept, encrypted, on your Uplivra server, so a failed log collector doesn't lose your logs. An administrator can download the key from the collector's page (your password is asked again, and the download is recorded). **Keep a copy offline**, for example in your password manager or safe: without it, off-site copies can't be read.

## Check the archive hasn't been changed

```
sudo uplivra logs verify
```

It checks every archive file against the hash chain and reports any file that's missing or altered. Other useful commands:

```
sudo uplivra logs usage                                  # size, rate and days until full
sudo uplivra logs search -text "failed password" -from 2026-09-01
```

## Troubleshooting

| What you see | What to do |
|---|---|
| No messages arrive | Check "Receive syslog here" is ticked, the device points at the right address and port, and nothing blocks UDP/TCP 514 |
| "The log disk is 80% full" (or any warning) | Add disk space, shorten retention (outside the protected period), or turn on off-site copies |
| "The log archive is full" | New messages are being dropped. Add space now |
| Wrong times on messages | Fix the device's clock or time zone; Uplivra also records when each message arrived |