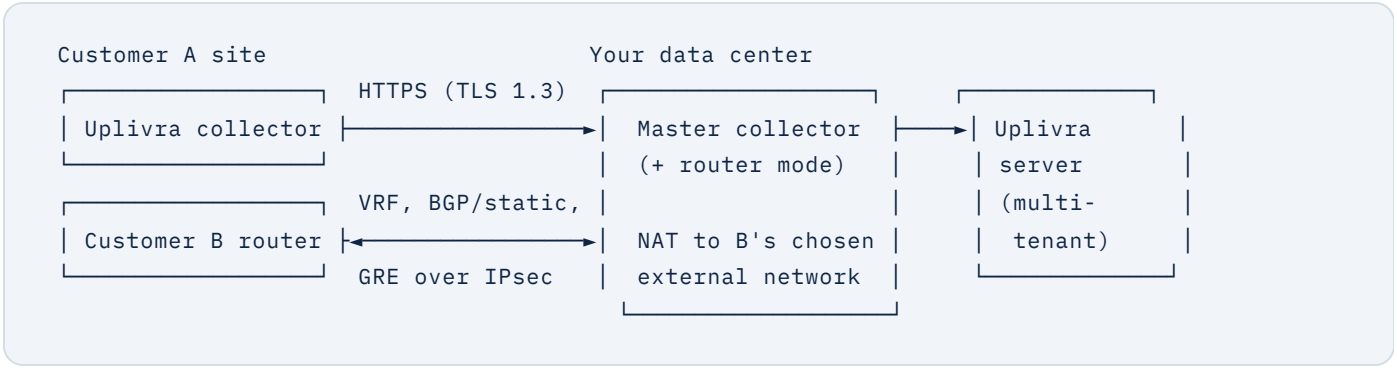
INSTALL GUIDE · MANAGED SERVICE PROVIDERS

MSP master collector and router

Build the MSP side of Uplivra: a multi-tenant server, master collectors your customers' collectors connect through, and router mode to reach customer networks with VRFs, BGP, NAT, firewall and IPsec-protected GRE tunnels.

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

The design



- The **Uplivra server** holds every customer as a separate tenant (the MSP multi-tenant module).
- **Master collectors** in your data center relay for customer collectors, so customers only need outbound HTTPS to you, and your server is never exposed to them.
- **Router mode** on a master collector lets it reach into customer networks directly: each customer gets a VRF, and your monitoring traffic is translated (NAT) into an **external network the customer chooses**, which you advertise to them by BGP, or they reach by a static route. Overlapping customer networks are no problem.

Use two master collectors (and a router pair) for redundancy: customer collectors fail over between masters automatically, and routers share connection state.

Sizing

Role	Minimum	Recommended
MSP master collector, 25 customers / 2,500 devices	8 cores, 16 GB, 250 GB	16 cores, 32 GB, 500 GB NVMe
MSP master collector, 100 customers / 10,000 devices	16 cores, 32 GB, 500 GB	Scale out: add masters rather than growing one
Router mode	4 cores, 8 GB, 64 GB	8 cores with AES-NI, 16 GB, 128 GB, 2–4 × 10 GbE NICs

Plan one CPU core per 1 Gbps of IPsec traffic (with AES-NI) plus two spare, and about 330 MB of memory per million tracked connections. Full internet BGP tables need 8 GB or more; partial or default routes need very little.

Use **Ubuntu 24.04 LTS** or the **MSP edition** of the virtual appliance. Give router VMs multi-queue virtual NICs (VMXNET3 or virtio) and pass through AES-NI.

Step 1: The multi-tenant server

1. Install the server as in Install the Uplivra server.
2. Add the **MSP multi-tenant** module to your license (partners get it with their discount).
3. Open **Customers** and add each customer. Switch to a customer to create their sites and people.

Step 2: Master collectors

On a computer in your data center, run the installer and choose **MSP master collector**. Answer:

Question	Answer
Also collect logs for customers?	**yes** only if it has its own large log disk (see the log collector guide)
Server address and setup code	Your Uplivra server, from **Settings › Sites and collectors** (your own company's site)

Question	Answer
Trust	Fingerprint, or your CA
Port customer collectors connect to	Enter for **8443**, or the HTTPS port you publish (for example 443 if the master has its own address)
Port for the status page	Enter for **8444**; choose a password. Limit it to your NOC network later with `sudo uplivra status-page -allow`

The master collector listens on the port you chose (8443 by default) for customer collectors. On its page in Uplivra you'll see its relay fingerprint. By default it uses a certificate Uplivra makes; to use your own public or internal CA certificate, upload it under **Settings › Certificates** on the server and it's sent to the relays automatically.

Repeat on a second computer for redundancy.

Step 3: Customer collectors through the master

When you install a collector for a customer (Linux or Windows, as in the collector guides), use the **master collector's address** as the server address, for example `https://collect.yourmsp.com:8443`. The setup code still comes from the customer's site in Uplivra.

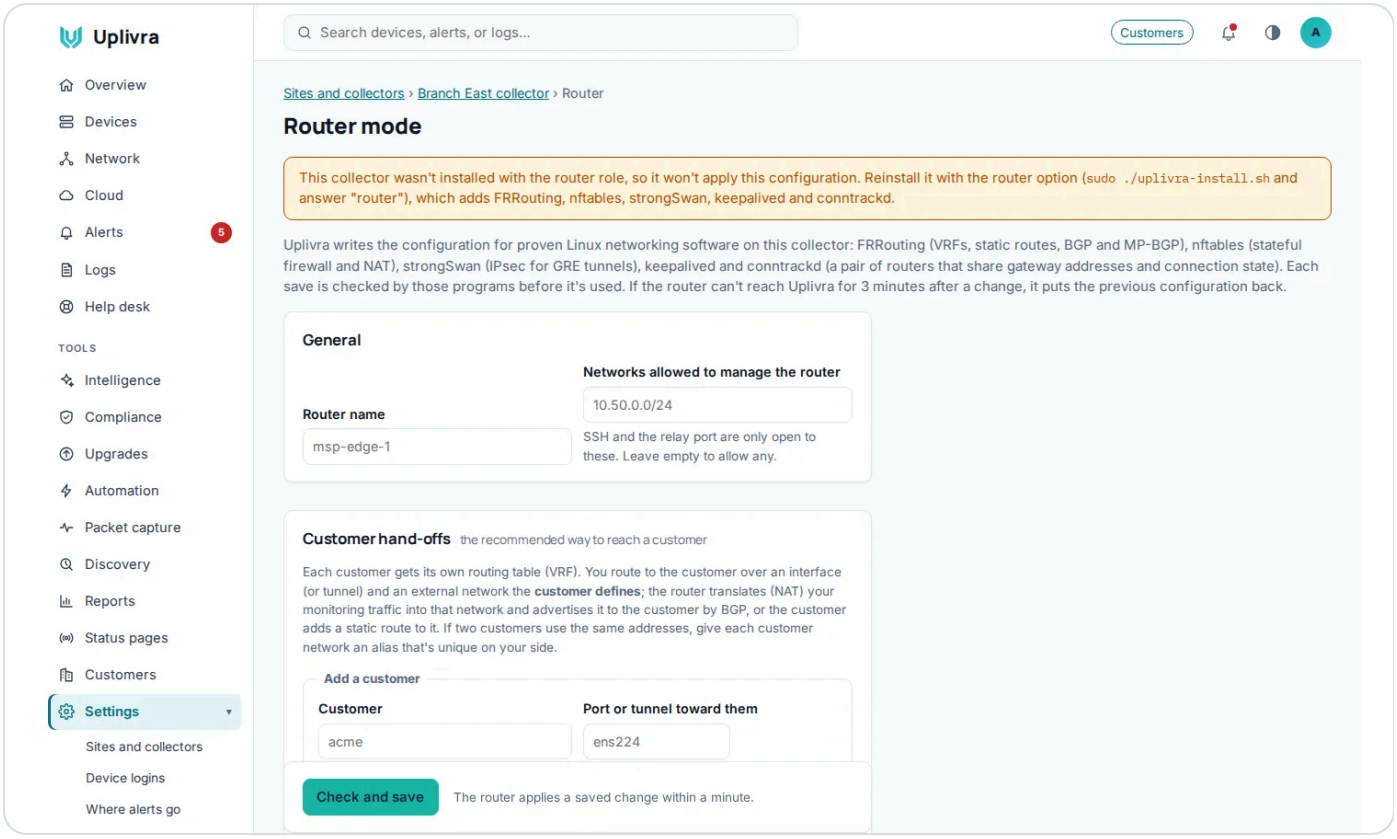
To give a Linux collector a second master to fail over to, add it to `/etc/uplivra/collector.json` and restart the collector:

```
"fallback_servers": [
  { "url": "https://collect2.yourmsp.com:8443", "fingerprint": "the second master's
fingerprint" }
]
```

```
sudo systemctl restart uplivra-collector
```

Step 4: Router mode

Install on the router computer and choose **MSP router**. Setup installs FRRouting, nftables, strongSwan, keepalived and conntrackd. Then in Uplivra open the collector's page and click **Router**.



The router editor. Demo data

Customer hand-offs (recommended)

For each customer:

Field	Meaning
Customer	A short name; becomes the VRF `c-name`
Port or tunnel toward them	An interface, VLAN or GRE tunnel
MTU	1500, or 9000 for jumbo frames if the whole path supports it

Field	Meaning
Your address on the hand-off	For example `169.254.10.1/30`
Customer's router	Their side of the link
External network	**The customer chooses it**, unique on their side, for example `100.64.10.0/28`. Your traffic appears to come from here
Your networks that reach them	Your monitoring networks, translated into the external network
Their networks to reach	The customer networks you monitor
Aliases	If their networks overlap another customer's, give them an alias range
Routing	**BGP** (your AS, their AS, password) or **static routes only**

Uplivra builds the VRF, the NAT, the routes and prefix filters, and the BGP session that advertises the external network to them.

Tunnels, firewall and pairs

- **GRE tunnels** protected by **IPsec**: pick the suite. *Strongest* (AES-256-GCM, SHA-384, ECP-384) is the default; *post-quantum hybrid* adds ML-KEM-768; *compatible* is for older customer firewalls.
- **Firewall:** a stateful firewall per VRF: allow only what monitoring needs.
- **Router pair:** two routers share a virtual address (keepalived) and connection state (conntrackd) over a dedicated sync link, so a failover doesn't drop sessions.

Applying safely

Click **Check and save**. Uplivra checks the whole configuration with the routing and firewall tools themselves before applying it. **If the router can't reach Uplivra for 3 minutes after a change, it puts**

the previous configuration back. Every version is kept under **Earlier versions**, and you can preview the generated files first.

On the router you can also run:

```
sudo uplivra system status      # interfaces, BGP peers, tunnels, sessions
sudo uplivra system rollback    # go back to the previous version now
```

Troubleshooting

What you see	What to do
"This collector wasn't installed with the router role"	Re-run `sudo bash install.sh -reconfigure` and choose MSP router
BGP stays down	Check AS numbers and password match the customer's, and TCP 179 is allowed on the hand-off
Tunnel won't come up	Both ends must use the same suite; try *compatible* for older firewalls, and allow UDP 500 and 4500
Customer collector can't connect	It must reach the master on TCP 8443; check the fingerprint or CA it trusts