INSTALL GUIDE · FIREWALL AND NETWORK TEAMS

Ports and firewall rules

What each kind of Uplivra computer needs open, incoming and outgoing, depending on the modes you choose. Everything runs on HTTPS 443 by default; SSH is optional.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 27 September 2026 · Latest version: https://uplivra.com/guides/ports.html

The short version

- **Everything uses HTTPS on port 443.** The web interface, collectors reporting in, customer collectors connecting to an MSP master collector, and each collector's management page. No odd port numbers in addresses: `https://uplivra.yourcompany.com/`.
- **Collectors only connect out.** A collector reaches your Uplivra server (or your MSP's master collector) on TCP 443. Nothing needs to connect *in* to a collector for it to work; incoming ports on a collector are only for its management page and for devices sending it SNMP traps, logs or traffic flows.
- **SSH is optional.** Incoming SSH to an Uplivra computer is only needed when you manage its Linux system over SSH, when you invite Uplivra support for a session, or on an MSP master collector that other collectors reach over SSH instead of HTTPS (not in router mode, see below; TCP 22, or 2222 when the computer's own SSH has 22).
- **Remote support sessions** (SSH, Remote Desktop and web apps through a collector) need no new ports. They travel inside the collector's HTTPS connection; the collector then connects to the device on the port allowed (22, 3389, 80 or 443 by default). See Remote access.
- **SNMP traps** come in on UDP 162 when you turn them on for a site. See SNMP traps.

To see the rules for a computer that's already installed, run this on it:

```
uplivra ports
```

It reads that computer's settings and prints what it needs, incoming and outgoing. `uplivra ports -all` prints every kind of computer, the same tables as below.

Changing the ports

You can choose different ports during installation, or change them later.

What	During install	Later
Server web interface (and where collectors connect)	"Port for the web interface"	**Settings › Ports and firewall** in the web interface, or `sudo uplivra system ports -port 9443`
A collector's management page	"Port for the management page" (0 turns it off)	`sudo uplivra status-page -port 9443` (Windows: `uplivra.exe status-page -port 9443` in PowerShell as administrator)
Where customer collectors connect to an MSP master collector	"HTTPS port for customer collectors"	`relay.listen` in `/etc/uplivra/collector.json`
SSH for customer collectors (MSP master)	"Also let customer collectors connect over SSH?"	`relay.ssh_listen` in `/etc/uplivra/collector.json`

When the server's port changes, it keeps answering on the old one for a while and tells every collector the new port. Collectors check that the new port answers with the same certificate, switch by themselves, and remember it. **Settings › Ports and firewall** lists anything still using the old port; close it there once that list is empty.

Ports 514, 2055, 4739, 6343 and 9995 are kept for logs and traffic flows, so they can't be chosen for a web page.

Tip: If another program on the computer already uses 443 (a web server such as IIS or nginx), choose another port such as 9443 and add it to addresses: `https://collector.yourcompany.com:9443/`.

MSP master collectors: HTTPS or SSH

Customer collectors connect to a master collector in one of two ways. Both carry the same encrypted HTTPS connection, checked against the master's certificate, and each customer collector still signs in with its own key.

- **HTTPS (normal):** TCP 443 from the customer network to the master. It shares the port with the master's management page; Uplivra tells them apart.
- **SSH:** for customer networks that allow SSH out but not HTTPS. The master listens on TCP 22, or **2222** when its own Linux SSH already uses 22. SSH here is only a carrier: there's no shell, no commands and no forwarding anywhere else.

SSH between collectors uses keys only, never passwords:

- Each collector makes its own SSH key the first time it connects. The key is stored **encrypted**, in a folder only the collector's service account can open (`/var/lib/uplivra-collector/ssh`, mode 700). The key's passphrase is protected like the credential vault's key: a private file on Linux, and Windows' own data protection on Windows.
- A master only lets in keys the Uplivra server knows. The first time, the collector proves who it is with its setup code (or, if it's already connected, its collector key). The master checks that with the server, which then adds the key to the list it sends every master.
- Removing a collector in Uplivra removes its key. Masters drop its SSH connection within a minute.
- The master's own host key is kept the same way. Collectors check it against the host key you give them, so they can't be pointed at an impostor.

Router mode doesn't use SSH: there, customer collectors reach the master through the GRE/IPsec tunnels, over HTTPS.

To set up SSH, choose it on the master during install, or add `ssh_listen` to its `/etc/uplivra/collector.json` and restart it:

```
"relay": { "listen": ":443", "ssh_listen": ":2222" }
```

The master's page in Uplivra (**Settings › Sites and collectors**) then shows its **SSH host key** next to its certificate fingerprint. On the customer collector, choose "SSH, through my MSP's master collector" during install, or add these to its `collector.json`:

```
"server_url": "https://master.yourmsp.com",
"server_fingerprint": "the master's certificate fingerprint",
"server_ssh": "master.yourmsp.com:2222",
"server_ssh_host_key": "SHA256:the master's SSH host key"
```

Customer collectors can also list a second master as a fallback, over HTTPS or SSH:

```
"fallback_servers": [
  { "url": "https://master2.yourmsp.com", "fingerprint": "...",
    "ssh": "master2.yourmsp.com:2222", "ssh_host_key": "SHA256:..." }
]
```

SNMP traps

Turn traps on per site under **Settings › Sites and collectors** ("Receive SNMP traps here"). The site's collector then listens on **UDP 162** (you can pick another port there) for SNMP traps and informs, v1, v2c and v3. Point your devices' trap destination at the collector's address.

A trap is accepted only when it uses one of the site's SNMP logins: a v1/v2c community, or a v3 user whose authentication and encryption check out. Others are dropped. The logins are the ones the site's SNMP checks use, plus any you tick next to the setting.

Traps show on each device's page. A link going down, a restart, failed SNMP logins, a BGP session dropping or a UPS on battery raises an alert straight away. Traps are part of Core; with Log Intelligence they're also searchable with the logs (`app:snmptrap`).

Upgrading from an older version

Older versions used port 8443 for the server and for master collectors, and 8444 for collector management pages. The installer moves them to 443 when you upgrade, if nothing else on the computer uses 443:

- The server moves to 443 and keeps answering on 8443 until every collector has moved. They move by themselves; nothing needs reinstalling.
- Master collectors move to 443 the same way and keep 8443 open for customer collectors until they've moved.
- A collector's management page moves from 8444 to 443 (on the server's own computer it's turned off, because the web interface shows the same).

Remember to allow 443 in any firewall **between** computers (the installer only opens the computer's own firewall). Once **Settings › Ports and firewall** shows nothing using 8443, close it there and remove the old rules from your firewalls.

Rules for each kind of computer

"In" means other computers connect to this one. Optional rules are only needed if you use that feature. The installer opens the incoming ones in Ubuntu's firewall (ufw) or Windows Firewall when it's switched on.

Uplivra server (with its own collector)

The central server: web interface, database, alerts, plus a collector for its own site. Most businesses only need this.

Direction	Protocol and port	Who	What for	Needed
In	TCP 443	People's browsers; every collector and MSP master collector	The Uplivra web interface, and collectors reporting results and fetching their checks (HTTPS)	Always
In	UDP 2055, 6343	Routers, switches and firewalls	Traffic flow records: NetFlow and IPFIX on 2055, sFlow on 6343 (the site's settings in Uplivra can change these)	If you send traffic flows to this collector (Network Pro)

Direction	Protocol and port	Who	What for	Needed
In	UDP 162	Routers, switches, firewalls, UPSs and servers	SNMP traps and informs, v1, v2c and v3 (the site's settings in Uplivra can change the port)	If devices send SNMP traps to this collector
In	UDP 514	Devices and servers	Log messages (syslog; the site's settings in Uplivra can change the port)	If devices send logs to this collector
In	TCP 514	Devices and servers	Log messages (syslog over TCP)	If devices send logs over TCP
In	TCP 22	Your administrators; Uplivra support when you invite them	Managing the Linux system, or a support session	Only if you manage the Linux system this way or allow support sessions
Out	TCP 443	licensing.uplivra.com	License check-ins (monthly), update downloads, and the Uplivra support connection when you turn it on	Not needed for offline licenses and offline updates

Direction	Protocol and port	Who	What for	Needed
Out	TCP 587, 465 or 25	Your mail server	Email alerts	If email alerts are set up
Out	TCP 443	Microsoft Teams, Slack, PagerDuty, webhooks, ticketing systems, cloud accounts (AWS, Azure, Microsoft 365)	Alerts and integrations you turn on	Only the ones you use
Out	TCP 636 or 389	Your domain controllers	Sign-in with Active Directory or LDAP	If directory sign-in is set up
Out	TCP 443	Let's Encrypt and Cloudflare	Trusted certificates for the web interface and management pages	If you use Let's Encrypt
Out	ICMP (ping)	The devices you monitor	Ping checks, traceroute	Always
Out	UDP 161	The devices you monitor	SNMP checks (interfaces, CPU, memory, printers, UPS…)	Always
Out	TCP 22, 80, 443 and the ports you check	The devices you monitor	Service, website, SSH (server health, configuration backups) and port checks	Only for the checks you add

Direction	Protocol and port	Who	What for	Needed
Out	TCP/UDP 6514, 514 or 443	Your SIEM, syslog server, HTTPS log collector or S3/Azure storage	Log forwarding: copies of the logs and traps this collector receives	Only if you set up log forwarding
Out	TCP 22	Network devices being upgraded	Copying firmware images to devices with SFTP or SCP (Upgrade & Lifecycle). Never TFTP, FTP or Telnet	Only when you use Copy to device
Out	UDP 53, 123	Your DNS and time servers	DNS and time (NTP) checks, and name lookups	Always
Out	TCP 22, 3389, 80, 443 (the ones allowed)	Devices on the site's network	Remote support sessions (SSH, Remote Desktop, web apps). They reach the collector inside its HTTPS connection; nothing new is opened incoming	If remote access is turned on for this collector

Collector

Checks devices at a site and reports to the Uplivra server.

Direction	Protocol and port	Who	What for	Needed
In	TCP 443	Your administrators' browsers	The collector's management page (HTTPS)	Can be turned off; you can also limit it to your management networks
In	UDP 2055, 6343	Routers, switches and firewalls	Traffic flow records: NetFlow and IPFIX on 2055, sFlow on 6343 (the site's settings in Uplivra can change these)	If you send traffic flows to this collector (Network Pro)
In	UDP 162	Routers, switches, firewalls, UPSs and servers	SNMP traps and informs, v1, v2c and v3 (the site's settings in Uplivra can change the port)	If devices send SNMP traps to this collector
In	UDP 514	Devices and servers	Log messages (syslog; the site's settings in Uplivra can change the port)	If devices send logs to this collector
In	TCP 514	Devices and servers	Log messages (syslog over TCP)	If devices send logs over TCP
In	TCP 22	Your administrators; Uplivra support when you invite them	Managing the Linux system, or a support session	Only if you manage the Linux system this way or allow support sessions

Direction	Protocol and port	Who	What for	Needed
Out	TCP 443	Your Uplivra server (or your MSP's master collector)	Reporting results and fetching checks (HTTPS). The collector always connects out; nothing connects in to it for this	Always
Out	ICMP (ping)	The devices you monitor	Ping checks, traceroute	Always
Out	UDP 161	The devices you monitor	SNMP checks (interfaces, CPU, memory, printers, UPS…)	Always
Out	TCP 22, 80, 443 and the ports you check	The devices you monitor	Service, website, SSH (server health, configuration backups) and port checks	Only for the checks you add
Out	TCP/UDP 6514, 514 or 443	Your SIEM, syslog server, HTTPS log collector or S3/Azure storage	Log forwarding: copies of the logs and traps this collector receives	Only if you set up log forwarding
Out	TCP 22	Network devices being upgraded	Copying firmware images to devices with SFTP or SCP (Upgrade & Lifecycle). Never TFTP, FTP or Telnet	Only when you use Copy to device

Direction	Protocol and port	Who	What for	Needed
Out	UDP 53, 123	Your DNS and time servers	DNS and time (NTP) checks, and name lookups	Always
Out	TCP 22, 3389, 80, 443 (the ones allowed)	Devices on the site's network	Remote support sessions (SSH, Remote Desktop, web apps). They reach the collector inside its HTTPS connection; nothing new is opened incoming	If remote access is turned on for this collector

Log collector

Receives logs (syslog) and keeps them in its own encrypted storage.

Direction	Protocol and port	Who	What for	Needed
In	TCP 443	Your administrators' browsers	The collector's management page (HTTPS)	Can be turned off; you can also limit it to your management networks
In	UDP 514	Devices and servers	Log messages (syslog; the site's settings in Uplivra can change the port)	If devices send logs to this collector
In	TCP 514	Devices and servers	Log messages (syslog over TCP)	If devices send logs over TCP

Direction	Protocol and port	Who	What for	Needed
In	TCP 22	Your administrators; Uplivra support when you invite them	Managing the Linux system, or a support session	Only if you manage the Linux system this way or allow support sessions
Out	TCP 443	Your Uplivra server (or your MSP's master collector)	Reporting results and fetching checks (HTTPS). The collector always connects out; nothing connects in to it for this	Always

Customer collector connecting to an MSP over SSH

A collector at a customer site that reaches its MSP's master collector through an SSH tunnel instead of HTTPS.

Direction	Protocol and port	Who	What for	Needed
In	TCP 443	Your administrators' browsers	The collector's management page (HTTPS)	Can be turned off; you can also limit it to your management networks

Direction	Protocol and port	Who	What for	Needed
In	UDP 2055, 6343	Routers, switches and firewalls	Traffic flow records: NetFlow and IPFIX on 2055, sFlow on 6343 (the site's settings in Uplivra can change these)	If you send traffic flows to this collector (Network Pro)
In	UDP 162	Routers, switches, firewalls, UPSs and servers	SNMP traps and informs, v1, v2c and v3 (the site's settings in Uplivra can change the port)	If devices send SNMP traps to this collector
In	UDP 514	Devices and servers	Log messages (syslog; the site's settings in Uplivra can change the port)	If devices send logs to this collector
In	TCP 514	Devices and servers	Log messages (syslog over TCP)	If devices send logs over TCP
In	TCP 22	Your administrators; Uplivra support when you invite them	Managing the Linux system, or a support session	Only if you manage the Linux system this way or allow support sessions
Out	TCP 22	Your MSP's master collector	Reporting results and fetching checks, through an SSH tunnel	Always

Direction	Protocol and port	Who	What for	Needed
Out	ICMP (ping)	The devices you monitor	Ping checks, traceroute	Always
Out	UDP 161	The devices you monitor	SNMP checks (interfaces, CPU, memory, printers, UPS…)	Always
Out	TCP 22, 80, 443 and the ports you check	The devices you monitor	Service, website, SSH (server health, configuration backups) and port checks	Only for the checks you add
Out	TCP/UDP 6514, 514 or 443	Your SIEM, syslog server, HTTPS log collector or S3/Azure storage	Log forwarding: copies of the logs and traps this collector receives	Only if you set up log forwarding
Out	TCP 22	Network devices being upgraded	Copying firmware images to devices with SFTP or SCP (Upgrade & Lifecycle). Never TFTP, FTP or Telnet	Only when you use Copy to device
Out	UDP 53, 123	Your DNS and time servers	DNS and time (NTP) checks, and name lookups	Always

Direction	Protocol and port	Who	What for	Needed
Out	TCP 22, 3389, 80, 443 (the ones allowed)	Devices on the site's network	Remote support sessions (SSH, Remote Desktop, web apps). They reach the collector inside its HTTPS connection; nothing new is opened incoming	If remote access is turned on for this collector

MSP master collector

Customer collectors connect through it to the MSP's Uplivra server, over HTTPS or SSH (SSH shown on 2222, since the computer's own SSH usually has 22; 22 works when it's free).

Direction	Protocol and port	Who	What for	Needed
In	TCP 443	Customer collectors; your administrators' browsers	Customer collectors connecting through this master collector, and its management page (HTTPS)	Always
In	TCP 2222	Customer collectors that connect over SSH	Customer collectors connecting through this master collector over SSH (a tunnel for the same HTTPS connection; registered collector keys only, no shell)	Always

Direction	Protocol and port	Who	What for	Needed
In	UDP 2055, 6343	Routers, switches and firewalls	Traffic flow records: NetFlow and IPFIX on 2055, sFlow on 6343 (the site's settings in Uplivra can change these)	If you send traffic flows to this collector (Network Pro)
In	UDP 162	Routers, switches, firewalls, UPSs and servers	SNMP traps and informs, v1, v2c and v3 (the site's settings in Uplivra can change the port)	If devices send SNMP traps to this collector
In	UDP 514	Devices and servers	Log messages (syslog; the site's settings in Uplivra can change the port)	If devices send logs to this collector
In	TCP 514	Devices and servers	Log messages (syslog over TCP)	If devices send logs over TCP
In	TCP 22	Your administrators; Uplivra support when you invite them	Managing the Linux system, or a support session	Only if you manage the Linux system this way or allow support sessions
Out	TCP 443	Your Uplivra server	Reporting results, and passing customer collectors' connections on (HTTPS)	Always

Direction	Protocol and port	Who	What for	Needed
Out	ICMP (ping)	The devices you monitor	Ping checks, traceroute	Always
Out	UDP 161	The devices you monitor	SNMP checks (interfaces, CPU, memory, printers, UPS…)	Always
Out	TCP 22, 80, 443 and the ports you check	The devices you monitor	Service, website, SSH (server health, configuration backups) and port checks	Only for the checks you add
Out	TCP/UDP 6514, 514 or 443	Your SIEM, syslog server, HTTPS log collector or S3/Azure storage	Log forwarding: copies of the logs and traps this collector receives	Only if you set up log forwarding
Out	TCP 22	Network devices being upgraded	Copying firmware images to devices with SFTP or SCP (Upgrade & Lifecycle). Never TFTP, FTP or Telnet	Only when you use Copy to device
Out	UDP 53, 123	Your DNS and time servers	DNS and time (NTP) checks, and name lookups	Always

Direction	Protocol and port	Who	What for	Needed
Out	TCP 22, 3389, 80, 443 (the ones allowed)	Devices on the site's network	Remote support sessions (SSH, Remote Desktop, web apps). They reach the collector inside its HTTPS connection; nothing new is opened incoming	If remote access is turned on for this collector

MSP router

An MSP master collector that also routes to customers over GRE/IPsec tunnels. Customer collectors reach it through the tunnels over HTTPS.

Direction	Protocol and port	Who	What for	Needed
In	TCP 443	Customer collectors; your administrators' browsers	Customer collectors connecting through this master collector, and its management page (HTTPS)	Always
In	UDP 2055, 6343	Routers, switches and firewalls	Traffic flow records: NetFlow and IPFIX on 2055, sFlow on 6343 (the site's settings in Uplivra can change these)	If you send traffic flows to this collector (Network Pro)

Direction	Protocol and port	Who	What for	Needed
In	UDP 162	Routers, switches, firewalls, UPSs and servers	SNMP traps and informs, v1, v2c and v3 (the site's settings in Uplivra can change the port)	If devices send SNMP traps to this collector
In	UDP 514	Devices and servers	Log messages (syslog; the site's settings in Uplivra can change the port)	If devices send logs to this collector
In	TCP 514	Devices and servers	Log messages (syslog over TCP)	If devices send logs over TCP
In	TCP 179	Customer and upstream routers	BGP routing (MSP router mode)	Always
In	UDP 500, 4500	Customer routers and firewalls	IPsec (GRE over IPsec tunnels to customers). Customer collectors reach the master through these tunnels on its HTTPS port	Always
In	TCP 22	Your administrators; Uplivra support when you invite them	Managing the Linux system, or a support session	Only if you manage the Linux system this way or allow support sessions

Direction	Protocol and port	Who	What for	Needed
Out	TCP 443	Your Uplivra server	Reporting results, and passing customer collectors' connections on (HTTPS)	Always
Out	ICMP (ping)	The devices you monitor	Ping checks, traceroute	Always
Out	UDP 161	The devices you monitor	SNMP checks (interfaces, CPU, memory, printers, UPS…)	Always
Out	TCP 22, 80, 443 and the ports you check	The devices you monitor	Service, website, SSH (server health, configuration backups) and port checks	Only for the checks you add
Out	TCP/UDP 6514, 514 or 443	Your SIEM, syslog server, HTTPS log collector or S3/Azure storage	Log forwarding: copies of the logs and traps this collector receives	Only if you set up log forwarding
Out	TCP 22	Network devices being upgraded	Copying firmware images to devices with SFTP or SCP (Upgrade & Lifecycle). Never TFTP, FTP or Telnet	Only when you use Copy to device

Direction	Protocol and port	Who	What for	Needed
Out	UDP 53, 123	Your DNS and time servers	DNS and time (NTP) checks, and name lookups	Always
Out	TCP 22, 3389, 80, 443 (the ones allowed)	Devices on the site's network	Remote support sessions (SSH, Remote Desktop, web apps). They reach the collector inside its HTTPS connection; nothing new is opened incoming	If remote access is turned on for this collector
Out	UDP 500, 4500	Customer routers and firewalls	IPsec tunnels to customers	Always

Packet capture collector

Records switch SPAN (mirror) ports for Packet Capture. Only the management port has an address; the SPAN ports listen and never send, so they need no rules.

Direction	Protocol and port	Who	What for	Needed
In	TCP 443	Your administrators' browsers	The collector's management page (HTTPS)	Can be turned off; you can also limit it to your management networks

Direction	Protocol and port	Who	What for	Needed
In	TCP 22	Your administrators; Uplivra support when you invite them	Managing the Linux system, or a support session	Only if you manage the Linux system this way or allow support sessions
Out	TCP 443	Your Uplivra server (or your MSP's master collector)	Fetching its license and settings, and sending pulled packet captures (HTTPS). Only from the management port; the SPAN ports have no address and send nothing	Always

Checking a connection

From the collector, check it can reach the server:

```
curl -k https://uplivra.yourcompany.com/healthz
```

It should print a short line with `"status":"ok"`. If it times out, a firewall between them is blocking TCP 443. For SSH to a master collector:

```
ssh -p 2222 -o BatchMode=yes uplivra@master.yourmsp.com
```

"Permission denied" or "open failed" means the port is open and the master answered (it doesn't give shells). A timeout means it's blocked.