

Uplivra IT and security checklist

For the IT and security team: what Uplivra connects to, what to open, what computer to use and what to prepare. Full guides: uplivra.com/docs.html.

Before you install

- A computer or VM for the server (sizes below), with a fixed IP address and a DNS name such as `uplivra.yourcompany.com`.
- SNMP read access on network devices (v3 recommended), and the networks the collector may scan.
- **For names in logs and traps:** an internal DNS server with reverse zones and PTR records for your devices. Without them, logs show IP addresses only.
- A mail server or Teams/Slack webhook for alerts. Optional: AD or LDAP for sign-in (TCP 636), with a read-only service account.
- Firewall rules from the tables below. Only the server needs inbound TCP 443, and only from your users and your own collectors.

Computer sizes

Mode	Minimum	Recommended
Uplivra server (with a collector) The central server: web interface, database and alerts, plus a collector for this site. Most businesses need only this.	2 CPU, 4 GB, 50 GB disk	4 CPU, 8 GB, 100 GB disk
Collector Checks devices at a site and reports to your Uplivra server.	2 CPU, 2 GB, 16 GB disk	2 CPU, 4 GB, 32 GB disk
Log collector Receives logs (syslog) and keeps them in its own encrypted storage. Best on its own computer with its own disk.	2 CPU, 4 GB, 250 GB disk	4 CPU, 8 GB, 500 GB disk
Collector and log collector Both on one computer. Fine for small sites; give logs their own disk.	4 CPU, 8 GB, 250 GB disk	4 CPU, 16 GB, 1000 GB disk
MSP master collector For managed service providers: customer collectors connect through this one to your Uplivra server.	8 CPU, 16 GB, 250 GB disk	16 CPU, 32 GB, 500 GB disk

Mode	Minimum	Recommended
MSP router An MSP master collector that also routes to customers (VRFs, BGP, NAT, firewall, IPsec tunnels, router pairs).	4 CPU, 8 GB, 64 GB disk	8 CPU, 16 GB, 128 GB disk
Packet capture collector Records the traffic from switch SPAN (mirror) ports all the time, so your Uplivra server can pull the packets from any moment. Needs 2 or more network ports: 1 for management, the others for SPAN. Licensed by your Uplivra server.	4 CPU, 8 GB, 500 GB disk	8 CPU, 16 GB, 2000 GB disk

Security in brief

- Monitoring data, logs, flows and passwords stay on your servers; the license check-in sends device counts and the version only.
- Collectors talk to the server over TLS 1.3 with post-quantum hybrid key exchange, pinned to your certificate or your CA.
- Device passwords and SNMP communities stay in an encrypted vault on the collector that uses them.
- Signed updates; tamper-evident, hash-chained logs; auditors can see encryption evidence on demand.
- Remote access is off by default and controlled by you; Uplivra staff can only ask, and you approve each session.
- Roles and access profiles, two-step sign-in, directory sign-in, and an audit log of every change.

Ports and firewall rules

"In" means others connect to that computer. Run `uplivra ports` on an installed computer to print its own list.

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

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	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
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

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
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

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 (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

Direction	Protocol and port	Who	What for	Needed
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

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
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
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
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

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
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	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
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)
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

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	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
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
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