

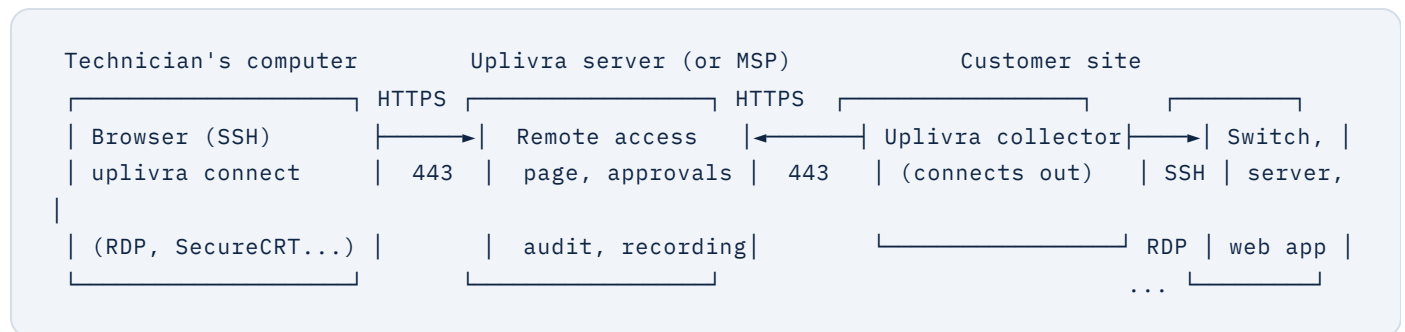
INSTALL GUIDE · MSPS AND IT TEAMS

Remote access and collector administration

Administer collectors (restart, diagnostics, tests, upgrades) and reach a customer's devices through their Uplivra collector. SSH in the browser, and Remote Desktop, SSH and web apps with your own programs, all inside HTTPS on port 443. The customer decides whether sessions are always allowed or need their approval each time.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 28 September 2026 · Latest version:
<https://uplivra.com/guides/remote-access.html>

How it works



- The collector **only connects out**, as it always does. When a session is approved, it opens a second HTTPS connection to the server for each connection and passes it to the device. Nothing is opened in the customer's firewall.
- Everything is **TLS-encrypted end to end on the Uplivra side**: technician to server, and server to collector. SSH and RDP add their own encryption on top.
- **SSH in the browser** needs nothing installed. For **Remote Desktop, SSH with your own program (SecureCRT, PuTTY) and web apps**, run the small `uplivra connect` app on your computer. It is the same `uplivra` program you install collectors with.
- Every session is written to the audit log with who asked, why, what it reached, when, and how much traffic passed. Browser SSH sessions are also recorded (what the device showed), and you can replay or download them from the session's page.

Who decides

Two sides have a say, and **the stricter one applies**.

The collector's computer. Remote access is **off** until someone turns it on *on that computer*. It can't be turned on from the web interface, by an MSP or by an upgrade. There are three choices:

Setting	What sessions may reach
<code>off</code> (default)	Nothing
<code>this-computer</code>	Only the collector's own computer (for example, SSH to it)
<code>network</code>	The collector's computer and devices on private networks (10.x, 172.16–31.x, 192.168.x, 100.64.x). Never the internet

The collector's computer also sets **which ports** may be used (22, 3389, 80 and 443 by default) and whether it asks for approval:

Approval on the collector	Meaning
<code>always</code> (default)	No approval needed from the collector
<code>ask</code>	Every session needs an approval, either in Uplivra by the customer's administrators or on the collector's management page
<code>ask-local</code>	Every session must be approved on the collector's own management page, by someone at the site

The customer's administrators in Uplivra choose on the **Remote access** page, under "Who may connect":

- **Always allow:** technicians can start sessions whenever they need to.
- **Ask each time:** every session waits for one of the customer's own administrators to approve it. They're notified wherever their alerts go (email, Teams, Slack...), and approve it on the Remote

access page or on the collector's page.

- **Off:** no sessions at all.

Only the customer's own administrators can change this. An MSP's staff can't, even when switched into the customer. A technician can never approve their own session.

Step 1: Turn it on at the customer's collector

On a **new** collector the installer asks "Allow remote support through this collector?" and whether each session must be approved. Pressing Enter keeps it off.

On a collector that's **already installed**, sign in to that computer and run:

```
sudo uplivra remote-access on
```

It asks what sessions may reach, which ports, and how approval works, then restarts the collector. Or give the choice directly:

```
sudo uplivra remote-access network -approval ask
```

Check the settings any time with `sudo uplivra remote-access`, and turn it off with `sudo uplivra remote-access off`.

On Windows, open **PowerShell as administrator** in `C:\Program Files\Uplivra` and use `.\uplivra.exe remote-access on`.

Upgrading never turns remote access on. A collector upgraded from an older version stays off until someone runs the command above.

Step 2: Start a session

1. In Uplivra, open **Remote access > New session**, or press **Connect** on a device's page.
2. Choose the collector, **the collector itself** or **a device on its network** (name or address), the kind of connection, how long you need (1 to 8 hours) and the reason (a ticket number helps the customer).
3. Press **Start the session**. The session page shows its status. If approval is needed, it says who it's waiting for and updates by itself.

Step 3: Connect

SSH in the browser: press **Open a terminal**, and sign in to the device with a username and password, or choose one of the SSH logins saved in Uplivra (the password is never sent to your browser). The first time, Uplivra remembers the device's host key and warns you if it ever changes.

Remote Desktop, SSH with your own program, and web apps:

1. Download `uplivra.exe` (Windows) or `uplivra` (Mac/Linux) from **Settings > Updates** if you don't have it.
2. On the session's page, press **Get the connect command** and copy it. It's shown only once, works only for that session and for you, and stops working when the session ends.
3. Open PowerShell (or Terminal) in the folder with the program and paste it, for example:

```
.\uplivra.exe connect "https://uplivra.yourcompany.com/remote/.../connect#t=..."
```

1. Leave that window open while you work, and point your program at your own computer:

Kind	Connect to	Notes
Remote Desktop	<code>127.0.0.1:13389</code>	On Windows, Remote Desktop opens by itself. The session page also has a <code>.rdp</code> file
SSH (SecureCRT, PuTTY)	host <code>127.0.0.1</code> , port <code>2222</code>	
HTTPS web app	<code>https://127.0.0.1:8443/</code>	Your browser warns about the certificate's name. That's expected
HTTP web app	<code>http://127.0.0.1:8080/</code>	
Other TCP	<code>127.0.0.1:10022</code>	

If a port is already in use on your computer, add `-port 23389` (for example) before the link.

Press **Ctrl+C** in the window to stop. **End session** on the session's page closes every connection straight away, for you and for the customer.

Administering collectors

Each collector's page (**Settings > Sites and collectors**, then the collector, or **Manage** on **Settings > Updates**) has an **Administration** section. Every action goes to the collector over its own outgoing connection and is written to the audit log.

Action	What it does
Fetch checks again	The collector reloads its checks and settings now instead of within the minute, and reports its status
Diagnostics report	A text report: version, system, disk, clock, connection to the server with a live health check, work queues, remote access settings and the last 200 messages. It never contains passwords, keys or device logins. View it on the page or download it
Restart	The collector restarts (checks pause for about a minute)
Test from this collector	Ping, port, DNS lookup or traceroute to any address, run from the collector's network
Upgrade this collector	Upgrades just this collector to the newest release, ahead of the others. Settings > Updates still upgrades them all at once
SSH to this computer	Starts a remote access session to the collector itself (remote access must be on at the collector)

There's no "run any command" button on purpose. For a shell on the collector, use **SSH to this computer**, which follows the collector's remote access settings.

Uplivra support connection

When you need help from Uplivra, the support connection lets Uplivra staff ask for things on your installation. It's **off** until one of your administrators turns it on under **Settings > Uplivra support**, and **nothing happens until one of your administrators approves each request** there. You're notified wherever your alerts go.

- Your server connects **out** to the licensing service over HTTPS (443), the same place it already checks its license. Nothing connects in, and no new firewall rules are needed.
- Uplivra staff can ask for a collector's diagnostics report, a fresh fetch of its checks, a restart, an upgrade to the current release, or a **support terminal** (SSH) through a collector to the collector itself or a device behind it.
- A support terminal runs from **your** server, through the collector, under the collector's own remote access settings (including approval on the collector's page if it asks for that). Your server records what the device shows and keeps the recording. The session shows on your **Remote access** page, where you can end it at any time.
- While it's on, your server tells Uplivra its version, device and company counts, and each collector's name, site, version, system and last contact. Never device names, addresses, passwords or monitoring data.

The support connection needs an online license (not an offline or free one). On MSP servers, only the MSP's own administrators manage it.

Limits worth knowing

- Sessions end at the time you chose, even if a connection is still open. A browser terminal also closes after 15 minutes without typing.
- The collector checks every connection itself: the session must be approved on its side, the target must be the one requested, and the port and network must be allowed by its settings.
- Recordings of browser SSH sessions are kept on the Uplivra server with the session (up to 50 MB each).
- The web interface needs to be reachable on its HTTPS port by technicians. No other port is used. See [Ports and firewall rules](#).

Troubleshooting

What you see	What to do
"doesn't allow remote access"	Turn it on at the collector (Step 1)
"doesn't allow port ..."	Add the port on the collector: <code>sudo uplivra remote-access network -ports 22,3389,443,8006</code>

What you see	What to do
"only allowed to private network addresses"	The collector never connects to internet addresses. Use the device's inside address
Waiting a long time	The customer's policy or the collector asks for approval. The session page says who needs to approve
"the device's host key has CHANGED"	Expected after a device is reinstalled. If so, press Forget the remembered host key on the terminal's sign-in page. If not, stop and check
<code>uplivra connect</code> says the certificate isn't trusted	Copy the command again from the session's page. It includes the server's certificate fingerprint