

Uplivra is in beta and online purchasing is paused. [Apply to test it](#): testers get a license on request and 10% off when purchasing opens.

INSTALL GUIDE · IT TEAMS AND MSPS

DNS Security

Turn DNS Security on, set policies by network, read the security log, allow a name that shouldn't be blocked, and send blocks to your SIEM.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 9 October 2026 · Latest version:
<https://uplivra.com/guides/dns-security.html>

What you need

- **Uplivra's DNS server** answering for your devices. See [Uplivra's DNS server](#).
- **The DNS Security add-on** in your license: \$1 per protected device per month.
- **Permission: Turn on and change Uplivra's DNS server, zones and records** to change settings. See the [DNS query log](#) to read the security log.
- **Internet access from the Uplivra server** to download the lists (HTTPS to blocklistproject.github.io, dsi.ut-capitole.fr, www.spamhaus.org, www.whoisds.com and raw.githubusercontent.com).

Turn it on

1. Open **Network > DNS server > Security**.
2. Under **Settings**, tick **DNS Security on** and choose **Save**.

Uplivra adds a policy called **Everyone**:

- **Blocked**: malware, phishing, scams, ransomware, crypto mining and bad networks.
- **Only logged (warn)**: newly registered domains, machine-made names and DNS tunnelling.

The server downloads the lists, and the DNS servers load them within a few minutes. Until a list is loaded, the DNS server keeps answering without it.

Check that it works

From a computer that uses Uplivra's DNS server:

```
nslookup use-application-dns.net
```

With **Stop going around this DNS server** on, the answer is "doesn't exist" (Non-existent domain). The block shows in the security log with the reason.

`uplivra dns test <name> -server <collector address>` on the Uplivra server explains the answer, including the block reason.

Policies

The first policy whose networks include the device applies. A policy with no networks covers everyone else. Use the arrows to change the order.

Each policy has:

- **Block:** the categories it blocks.
- **Checks on the name itself:** off, warn or block for newly registered domains, machine-made names and DNS tunnelling. Start with warn and read the log for a week before you block.
- **Stop going around this DNS server:** Firefox's own DNS, iCloud Private Relay and public encrypted-DNS services stop working on this network, so devices use yours. Also block the names in **Encrypted-DNS list for your firewall** on your firewall.
- **SafeSearch:** forced on Google, Bing, YouTube and DuckDuckGo.
- **Sinkhole:** blocked names get the sinkhole address (set under Settings) instead of "doesn't exist".
- **Always allow** and **Always block:** names, with every name under them.

The security log

Every block and warning, with the device, the name and the reason. It is kept for 90 days, even when the query log is off.

- **Allow:** adds the name to the allow list of the policy that covers that device. Devices may remember the block for a minute.

- **Devices to look at:** devices that reached for malware, phishing or other dangerous names in the last 7 days.

Alerts

A device that reaches for dangerous names three times in an hour raises an alert: malware, phishing, ransomware, scams, crypto mining, bad networks, machine-made names or tunnelling. Warnings count too. The alert resolves itself after a quiet day. Use your alert rules to open a ticket.

Laptops away from the office

Laptops and phones can use your Uplivra server's encrypted DNS (DNS over HTTPS) wherever they are, under a policy, with the same blocking, log and alerts. Nothing new is opened: it uses the server's HTTPS port.

1. On the Security page, under **Off-site devices**, choose **Add a device**, name it and pick its policy.
2. The next page shows the device's address and its settings, once: - **Windows 11:** a PowerShell script (or an Intune script). Your own names keep going to the office DNS servers. - **Mac, iPhone, iPad:** a profile to install or send with your device management. - **Chrome, Edge, Firefox:** browser policies.
3. Copy them before you leave the page. The address contains the device's own key.

A lost device: choose **Turn off** next to it, and its address stops working at once. Each device counts as one protected device.

Android's Private DNS needs DNS over TLS with its own name, which isn't offered yet.

Send blocks to your SIEM

Under **Settings > Logs > Log forwarding**, tick **DNS Security events** on a destination. The server sends each block and warning as one message, with the device, name, category and reason as fields.

Your own lists

Under **Block lists**, choose **Add a list by its web address:**

- The address must start with `https://` and be on the internet.
- One name a line, a hosts file or adblock style (`||name^`).

- Pick its category. Policies that block that category use it.

Only add lists your license with their owner allows.

Why a blocked site shows a browser error

Browsers show "can't reach this site" for blocked HTTPS sites. A friendly block page would need Uplivra's certificate on every computer, which we don't do. The security log and the alert say what was blocked and why. Tools like `dig` show the reason (an Extended DNS Error).

Where the lists come from

Downloaded every day by your Uplivra server, only when a policy uses their category:

- The Block List Project (Unlicense)
- UT1 blacklists, Université Toulouse Capitole (CC BY-SA 4.0)
- Spamhaus DROP (credit: The Spamhaus Project)
- StevenBlack hosts (MIT) and 1Hosts (MPL-2.0)
- WhoisDS newly registered domains

The Security page lists each one with its terms and the date it was last updated.