

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

Uplivra's DNS server

A collector answers your network's DNS. It serves your own zones, names made from DHCP leases and IP reservations, and forwards your AD domain to its domain controllers. Everything else is looked up over encrypted DNS through Quad9, which blocks known malware and phishing sites.

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

What you need

- **Uplivra:** 26.10.70 or later. The DNS server is part of **Core**, so it's free in every edition, including the free plan for up to 15 devices.
- **A collector on the network:** two is better, so devices have a backup DNS server.
- **Permission: Turn on and change Uplivra's DNS server, zones and records.** Administrators have it. Seeing the query log needs **See the DNS query log**.

Turn it on

1. Go to **Network > DNS server** and pick **Set up** next to a collector.
2. Tick **Answer DNS on this collector**, then tick the network ports it should answer on.
3. Leave **Quad9 (recommended)** for other names. Quad9 is free for organisations, encrypted, blocks known malware and phishing domains, and keeps no device addresses. You can pick Cloudflare, or list your own resolvers.
4. **Save.** The collector starts answering within a minute and opens port 53 on those ports in its own firewall.
5. Give devices the collector's address as their DNS server. In Uplivra's DHCP server, that's the **DNS servers** field of the scope. Hand out two collectors' addresses for a backup.

The overview shows each collector's state, how many questions it answered, how many came from its cache, and whether its upstream resolvers are answering.

Who can use it

It is **never an open resolver**:

- **Who it answers:** only the networks you allow. By default that's private networks only: 10/8, 172.16/12, 192.168/16, 100.64/10 and IPv6 private addresses. Everyone else gets "refused".
- **Rate limit:** each device can ask 200 questions a second by default, more than any normal computer needs.
- **No zone transfers,** and "ANY" questions get a one-line answer, so the server can't be used to flood someone else.
- **Rebinding protection** (on by default): a public name that points at a private address is dropped. This stops a known trick for attacking routers and printers from a web page.
- **Privacy:** which device asked is never passed on to Quad9 or any other upstream.

Zones and records

A **zone** is a domain your DNS servers answer for themselves.

- **Choosing a name:** use a sub-domain of a domain you own, like `office.example.com`, or a name ending in `.internal`.
- **Not your public domain itself:** don't use `example.com` unless every name in it is listed in Uplivra too. Otherwise devices inside would stop finding your website and email.

Network > DNS server > Add a zone, then add records:

Type	Value	Example
A	IPv4 address (the reverse name is made automatically)	<code>printer</code> → <code>192.168.10.20</code>
AAAA	IPv6 address	<code>printer</code> → <code>fd00::20</code>
CNAME	another name (nothing else can share the name)	<code>www</code> → <code>printer</code>

Type	Value	Example
MX	mail server, with a priority	@ → 10 mail.example.com.
TXT	text	@ → v=spf1 -all
SRV	server, with priority, weight and port	_sip._tcp → 10 5 5060 pbx
CAA	who may issue certificates	@ → 0 issue "letsencrypt.org"
NS	hand a sub-domain to other servers	lab → ns1.lab.example.com.

@ means the zone itself. A name ending in a dot is a full name; one without a dot is inside the zone. A * name (*.lab) answers for every name under it that isn't listed.

Automatic names

Tick **Add names from Uplivra's DHCP leases** and **Add names from IP address reservations** on a zone:

- **DHCP leases:** a device that tells the DHCP server its name gets a name in the zone while its lease lasts (ams-laptop.office.example.com).
- **IP reservations:** each reservation with a name on the IP addresses page gets one too.

A record you add yourself with the same name always wins. The zone page lists the automatic names.

Active Directory

Keep your domain controllers as the DNS servers for the AD domain. In the collector's DNS settings, under **Forwarded zones**, write the domain and its domain controllers:

```
corp.example.com 10.0.0.5 10.0.0.6
```

Names in corp.example.com are asked of the domain controllers, so sign-ins and group policy keep working. Everything else is answered by Uplivra.

Names from Windows DHCP or Kea (dynamic updates)

If another DHCP server hands out addresses (Windows DHCP, ISC Kea, a router), it can add and remove names in a zone by itself (RFC 2136):

1. Open the zone and choose **Allow a DHCP server to update this zone**.
2. Write the DHCP server's address. - **Windows DHCP**: choose **No key**. Windows sends unsigned updates, so only that address is accepted. - **ISC Kea**: choose **Make a key**. Uplivra shows the key once, with the settings for `kea-dhcp-ddns.conf`.
3. In the DHCP server, turn dynamic DNS updates on for the scope.

A DHCP server can change only the names it wrote. Names you made in Uplivra, and names another DHCP server wrote, are refused. The zone page lists the names each DHCP server wrote, and you can remove any of them. Every DNS server of yours gets the change within a minute.

Uplivra's own DHCP server doesn't need this: tick **Add names from Uplivra's DHCP leases** on the zone instead.

Secondary DNS servers

A secondary keeps a copy of a zone, so names still work if the collector is down. It can be a DNS server at another site, your DNS host, or BIND.

1. Open the zone and choose **Add a secondary**.
2. Write the secondary's IP address.
3. Keep **Make a new key** ticked. Uplivra shows the key once, with the settings to paste into BIND. Copy it before you leave the page.
4. In the secondary, set the primary to the collector's address (the zone page lists it).

How it is kept safe:

- **Who can copy**: only the addresses listed. Everyone else is refused.
- **The key**: with a key, the copy request must be signed with it (TSIG). Uplivra keeps the key encrypted.
- **Address only**: use this only on a private network you trust.

When the zone changes, Uplivra tells the secondary (NOTIFY), and it copies the new version. The secondary connects to TCP port 53. If it is outside your network, open TCP port 53 from its address on your firewall.

To change a secondary, remove it and add it again. `uplivra dns secondaries <zone>` lists them on the server.

The query log

Tick **Keep a query log** in a collector's DNS settings. **Network > DNS server > Query log** then shows which device looked up which name, with the answer and where it came from:

- **cache:** answered from the collector's memory.
- **upstream:** looked up through Quad9 or your own resolvers.
- **local:** answered from one of your zones.
- **forward:** sent to a forwarded zone's servers.
- **refused:** a network that isn't allowed.
- **rebind:** blocked by rebinding protection.
- **transfer:** a secondary copied a zone.

It is kept for 30 days. The log shows people's browsing by name, so only give the permission to people who need it.

Why a blocked site shows a browser error

Uplivra (and Quad9) answer "doesn't exist" for blocked names, with a reason code that tools like `dig` show (an Extended DNS Error). Browsers show their usual "can't find this site" page. A friendly block page would need Uplivra's own certificate installed on every computer, which we don't do.

DNS Security

The **DNS Security** add-on adds its own blocking on top:

- **What it blocks:** malware, phishing and scams by default; categories you choose; newly registered and machine-made domains; DNS tunnelling.
- **Logs and alerts:** a security log of every block with its reason, alerts for devices that keep trying, and SIEM forwarding.

See [DNS Security](#).