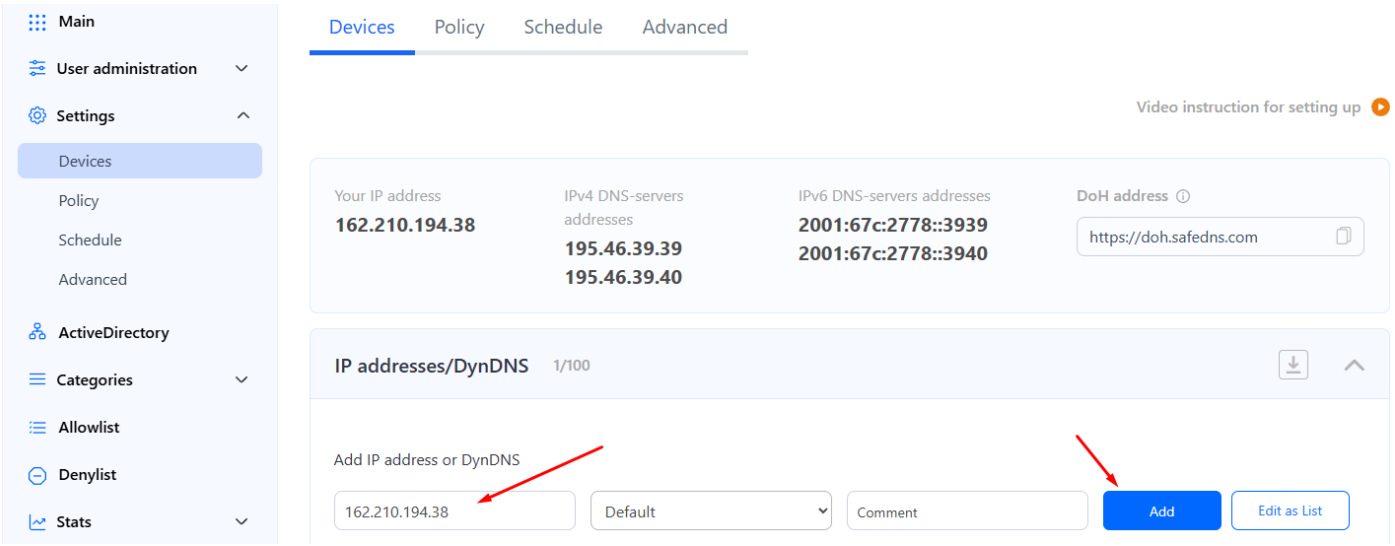
Peplink Router Setup

Router with Static IP address configuration

1. Go to SafeDNS **Dashboard > Settings > Devices** and copy your IP address to the "**IP addresses / DynDNS**" box, choose a policy, and click "**Add**".



2. Change your router's DNS servers to SafeDNS addresses - **195.46.39.39** and **195.46.39.40**:

1. Log in to the **Peplink Web Admin** interface.
2. Navigate to **Network > WAN** and click on your active WAN connection.
3. Under **DNS Servers**, set the DNS assignment mode to custom/manual.
4. Enter the primary and secondary SafeDNS server addresses:
   Primary DNS: **195.46.39.39**
   Secondary DNS: **195.46.39.40**
5. Click **Save** and **Apply Changes**.

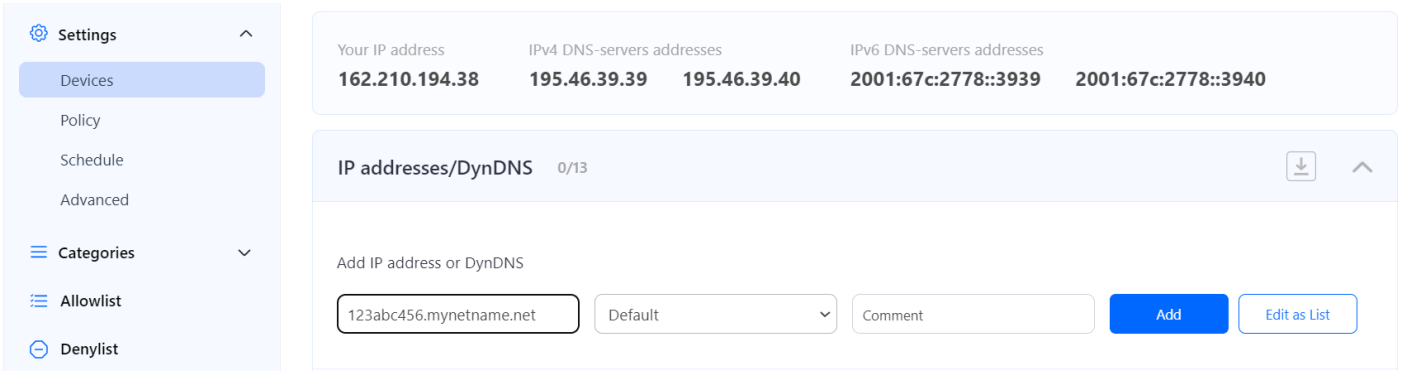
You have successfully configured your router.

> Please note that settings take 5-7 minutes to apply.
> Stats and filtering status update every 10 minutes.

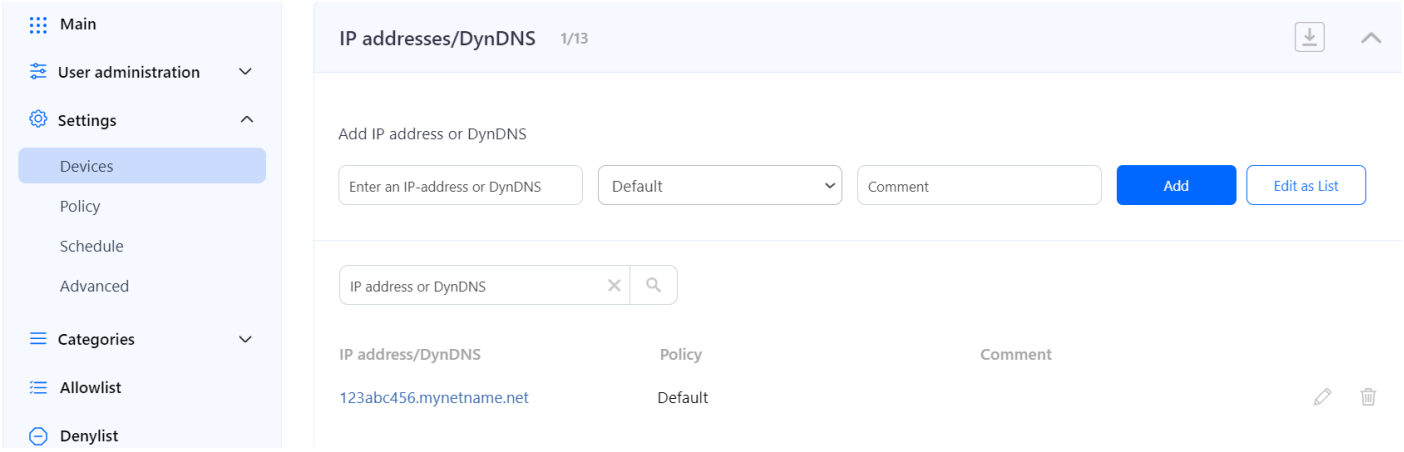
Router with Dynamic IP address configuration

Peplink routers have the built-in feature of the Dynamic DNS setup named **Find My Peplink**.
It can be activated easily from the router with no configuration needed on any DDNS service.

1. Log into **InControl 2** portal, navigate to your organization/group, and click on your Peplink device to open its **Device Details** page.
2. Click the **Edit** button near the top-left corner.
3. Scroll down to **Find My Peplink Service** and toggle the switch to **On**.
4. Enter your preferred unique prefix for the `mypep.link` address and click **Save**.
5. Go to SafeDNS **Dashboard > Settings > Devices** and copy your DynDNS hostname to the "**IP addresses / DynDNS**" box, choose a policy, and click "**Add**".



Once added, you will see it in the DynDNS section of the Dashboard.



6. Change your router's DNS servers to SafeDNS addresses - **195.46.39.39** and **195.46.39.40**

1. Log in to the **Peplink Web Admin** interface.
2. Navigate to **Network > WAN** and click on your active WAN connection.
3. Under **DNS Servers**, set the DNS assignment mode to custom/manual.
4. Enter the primary and secondary SafeDNS server addresses:
   Primary DNS: **195.46.39.39**
   Secondary DNS: **195.46.39.40**
5. Click **Save** and **Apply Changes**.

You have successfully configured your router.

> Please note that settings take 5-7 minutes to apply.
> Stats and filtering status update every 10 minutes.

DoH setup

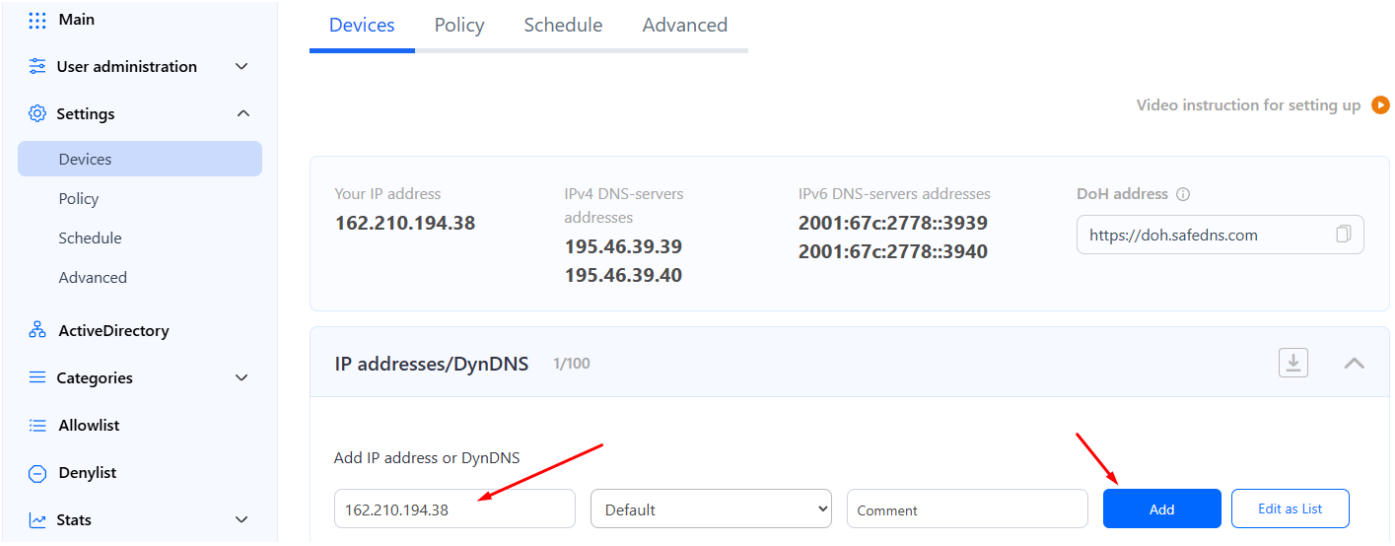
> DoH is supported on all paid plans.
> DoH links with policy are available on Education & Non-Profit, Pro, and Pro Plus plans only.

MikroTik router allows setting up the DoH connection to SafeDNS.

DoH link without policy

With this setup, all devices connected to the network with the IP address added in the SafeDNS Dashboard will be filtered with the selected policy. If the IP address of the router is changed, you need to add a new IP address in the SafeDNS Dashboard.

Navigate to SafeDNS **Dashboard > Settings > Devices**, and make sure your IP address or DynDNS has been set up.



Configure the internal LAN interface and the DHCP service:

1. In Peplink Web Admin, navigate to **Network > LAN** and select your client LAN or VLAN.
2. Locate **DNS Proxy Settings** and check the box to **Enable DNS Proxy**. Leave **Include Google Public DNS Servers** unchecked.
3. If Peplink manages DHCP for the network, locate **DHCP Server Settings** and set **DNS Servers > Assign DNS server automatically**. This advertises the Peplink LAN IP address as the default DNS server to DHCP clients.
4. If an external device manages DHCP, set **DHCP Option 6** (DNS servers) on that server to the reachable Peplink LAN IP address.
5. Save and apply changes, then renew client network leases.

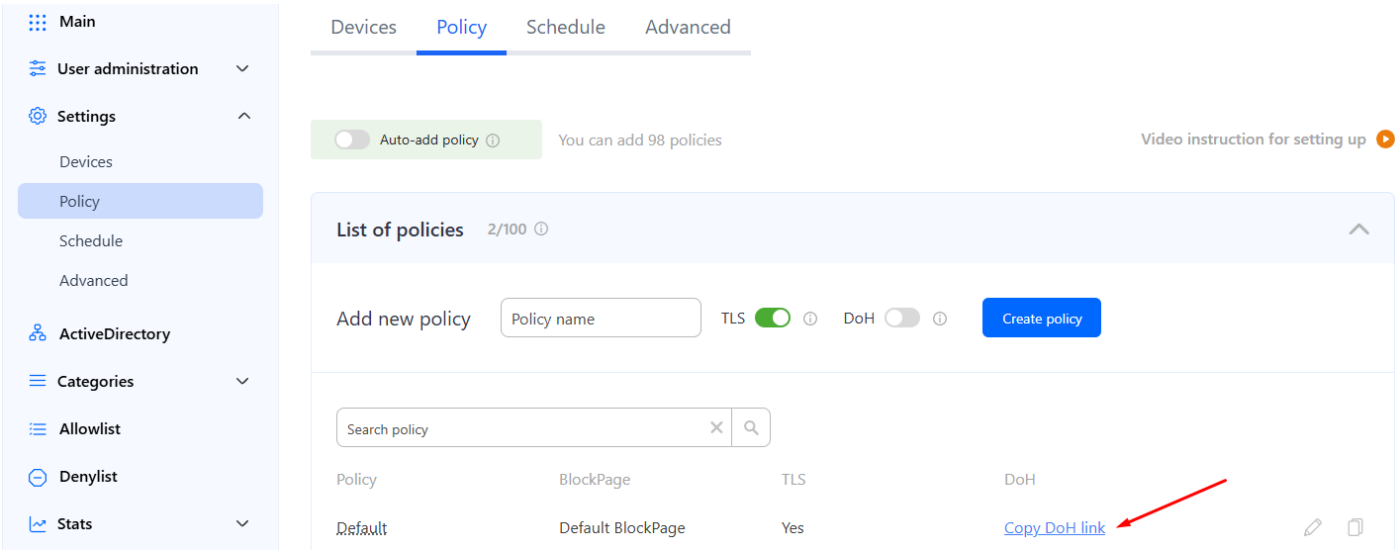
With the LAN proxy active, configure the Peplink DoH engine to connect to your SafeDNS custom URL:

1. In Peplink Web Admin, navigate to **Network > WAN > DNS over HTTPS**.
2. Enable the **DNS over HTTPS** feature.
3. Set **Server** to **Custom URL**.
4. In the **URL** field, paste your copied SafeDNS token link `https://doh.safedns.com/`
5. In the **IP Address** field, enter `195.46.39.41`.
6. Click **Save and Apply Changes**.

DoH link with policy

With this setup, all devices connected to the router will be filtered with the selected policy.
The Router is identified by the policy token in the link. If the IP address of the router changes, it will not affect the filtering.

Navigate to SafeDNS **Dashboard > Settings > Policy**, and copy the DoH link with the policy.



Click **Copy Link** to retrieve your unique DoH URL. The default link format appears as `https://<token>.doh.safedns.com/`

Configure the internal LAN interface and the DHCP service:

1. In Peplink Web Admin, navigate to **Network > LAN** and select your client LAN or VLAN.
2. Locate **DNS Proxy Settings** and check the box to **Enable DNS Proxy**. Leave **Include Google Public DNS Servers** unchecked.
3. If Peplink manages DHCP for the network, locate **DHCP Server Settings** and set **DNS Servers > Assign DNS server automatically**. This advertises the Peplink LAN IP address as the default DNS server to DHCP clients.
4. If an external device manages DHCP, set **DHCP Option 6** (DNS servers) on that server to the reachable Peplink LAN IP address.
5. Save and apply changes, then renew client network leases.

With the LAN proxy active, configure the Peplink DoH engine to connect to your SafeDNS custom URL:

1. In Peplink Web Admin, navigate to **Network > WAN > DNS over HTTPS**.
2. Enable the **DNS over HTTPS** feature.
3. Set **Server** to **Custom URL**.
4. In the **URL** field, paste your copied SafeDNS token link `https://doh.safedns.com/`
5. In the **IP Address** field, enter `195.46.39.41`.
6. Click **Save and Apply Changes**.

Bypass Prevention

To prevent unmanaged clients or network users from bypassing SafeDNS filtering policies, enforce additional security rules within Peplink Web Admin and the SafeDNS Dashboard.

Redirect Traditional DNS Requests

Configure Peplink to intercept standard DNS queries sent directly to external resolvers (such as `8.8.8.8` or `1.1.1.1` on port 53):

1. Open **Advanced > Misc. Settings > Service Forwarding > DNS Forwarding**.
2. Enable **Forward Outgoing DNS Requests to Local DNS Proxy**.
3. Save and apply changes. Standard UDP/TCP port 53 requests are automatically redirected to the local Peplink DNS proxy.

Block Outbound DNS-over-TLS (DoT)

Prevent devices from establishing encrypted DNS-over-TLS sessions to third-party resolvers:

1. Open **Advanced > Firewall > Access Rules > Outbound Firewall Rules**.
2. Add a new outbound rule positioned above general allow rules:

- **Rule Name / Action:** Block Outbound DoT / Deny
- **Protocol:** TCP
- **Destination Port:** `853`
- **Source Subnet:** Client Wi-Fi LAN / VLAN subnets
- **Destination:** Any external address

3. Save and apply rules to drop outbound TCP port 853 traffic.

Block Public Encrypted Resolvers in SafeDNS AppBlocker

Restrict browser-based DoH fallback options inside the SafeDNS Dashboard:

1. In **SafeDNS Dashboard**, edit the filtering policy assigned to your Peplink device.
2. Under **AppBlocker > VPN and Proxy**, block **Chrome/Firefox Secure DNS** and **Apple Private Relay**.

3. As appropriate, enable blocking for the **Proxies & Anonymizers** category and add known public DoH bootstrap hostnames to the policy Denylist.
4. Save the policy settings.

Created 2026-11-17 19:15:51 UTC by Val Redman
Updated 2026-11-22 19:57:13 UTC by Val Redman