Installation and configuration

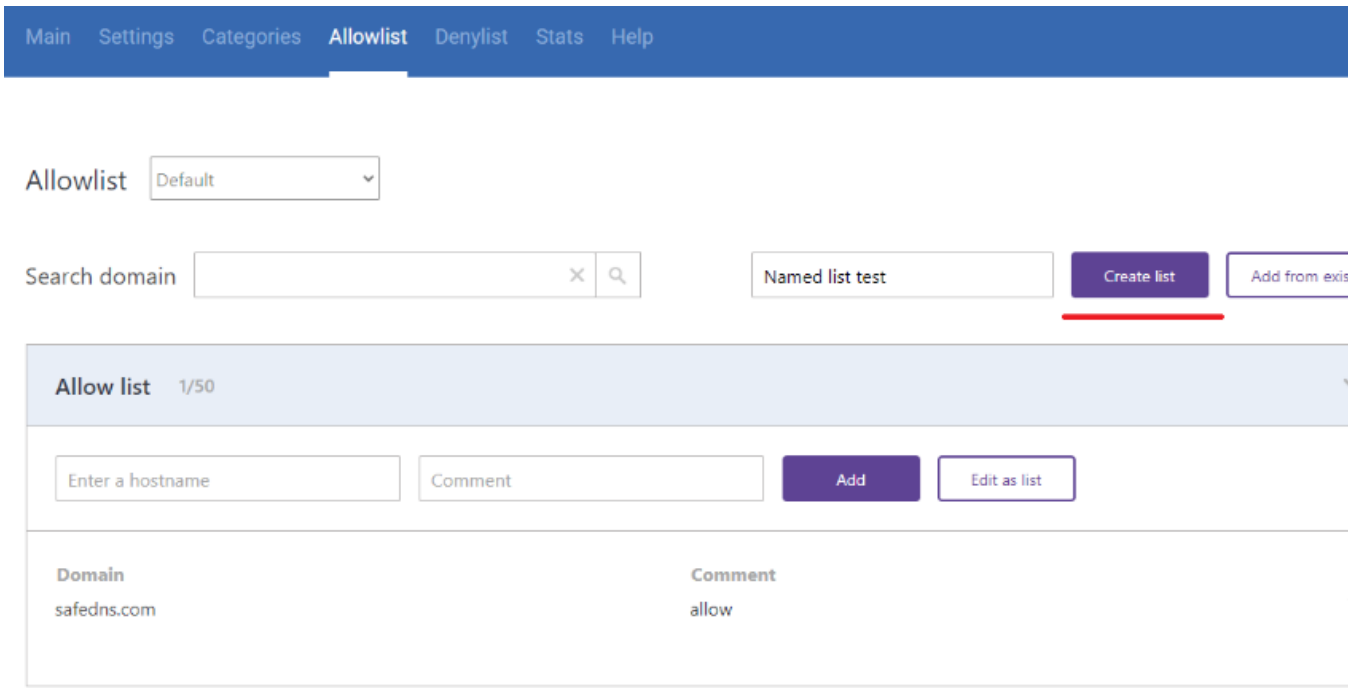
Allow/Denylists And Named Lists

This feature comes in handy when you need to add the same list of domains to the different policies (filtering profiles). You can create or edit a list and then apply it to any of your filtering policies. You can manage lists of allowed or blocked hosts and domains for all of your profiles or group of profiles.

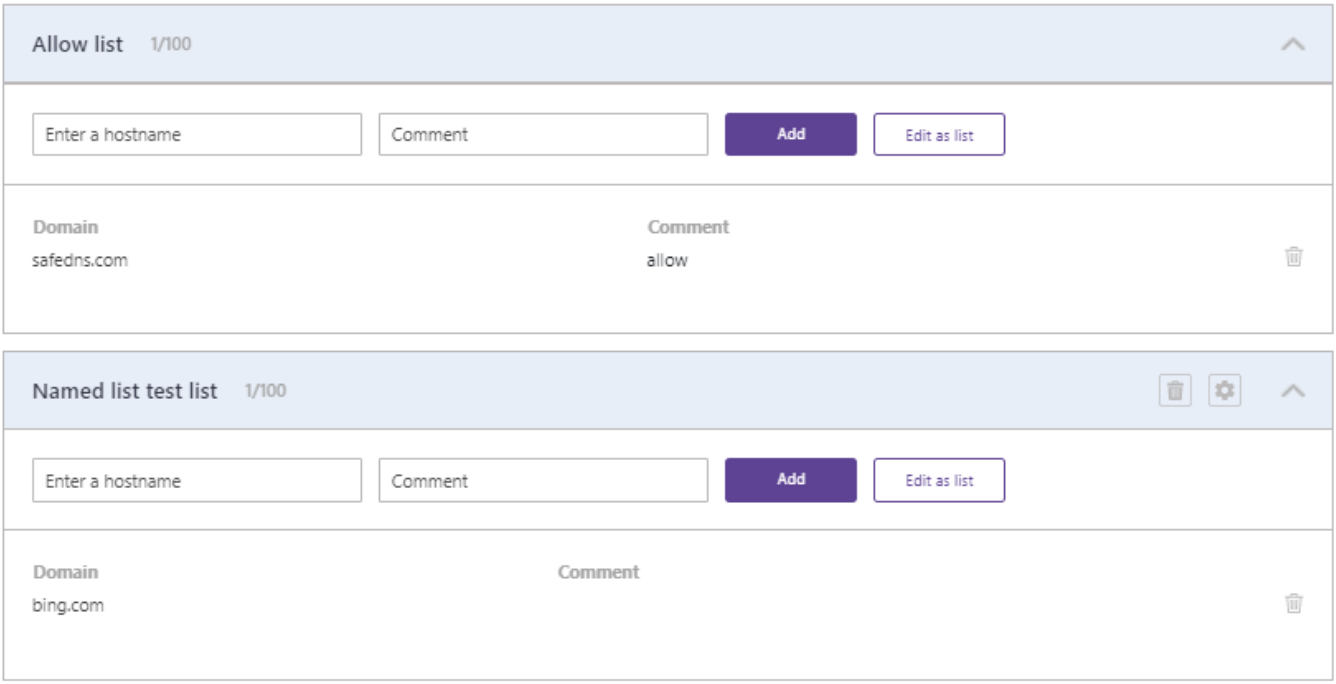
> Blocking/allowing a domain automatically blocks/allows all its subdomains, overriding Categories settings.

> It is possible to simultaneously block a domain and allow its subdomain(s), and vice versa.

1. Navigate to the "**Allowlist**" or "**Denylist**" tab to create a new named list.
2. Find the "**Create list**" button and enter the name of the new list into the "**List name**" box on the right and click "**Create list**". It will appear at the bottom of the page.



3. Click the **Cogwheel** button on the right, then click "**Save**" to add the newly created named list to the multiple policies (profiles).



The same steps work for the **Denylist** section.

Wildcards are not supported at the moment.

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

General Setup via OpenVPN

Some devices are not yet supported by the SafeDNS Agent or cannot have it installed for various reasons. In this case, you can configure the SafeDNS filtering via the third-party app OpenVPN.

Download OpenVPN

> OpenVPN creates a VPN connection using the SafeDNS **Configuration file** that contains all settings of chosen filtering policy.

OpenVPN does not change or hide your Public IP, as regular VPN services do, it only receives filtering rules from your dashboard.

Multiple devices can use the same filtering policy, but **each device should use its own Configuration file**.

Devices filtered via OpenVPN remain protected in any network.

The installation process is the same for all platforms: you need to download the Configuration file, install OpenVPN, and import the **Configuration file.**

Guides for the platforms supported by OpenVPN

1. Windows Filtering Setup via OpenVPN
2. Mac Filtering Setup via OpenVPN
3. Linux Filtering Setup via OpenVPN
4. iOS and Android Filtering Setup via OpenVPN

Schedule Setup

Unlike other content filtering systems that use simple schedules with complete blocking of internet access based on time, SafeDNS uses a complex system of schedules that can be flexibly configured for any needs and any scenario. However, greater flexibility brings more complexity to the setup of a schedule.

> Schedule logic: selected custom Policy (profile) is applied at the selected time; Default policy is applied at all other times.

This system allows a much more flexible schedule, that you can apply in advanced scenarios such as:

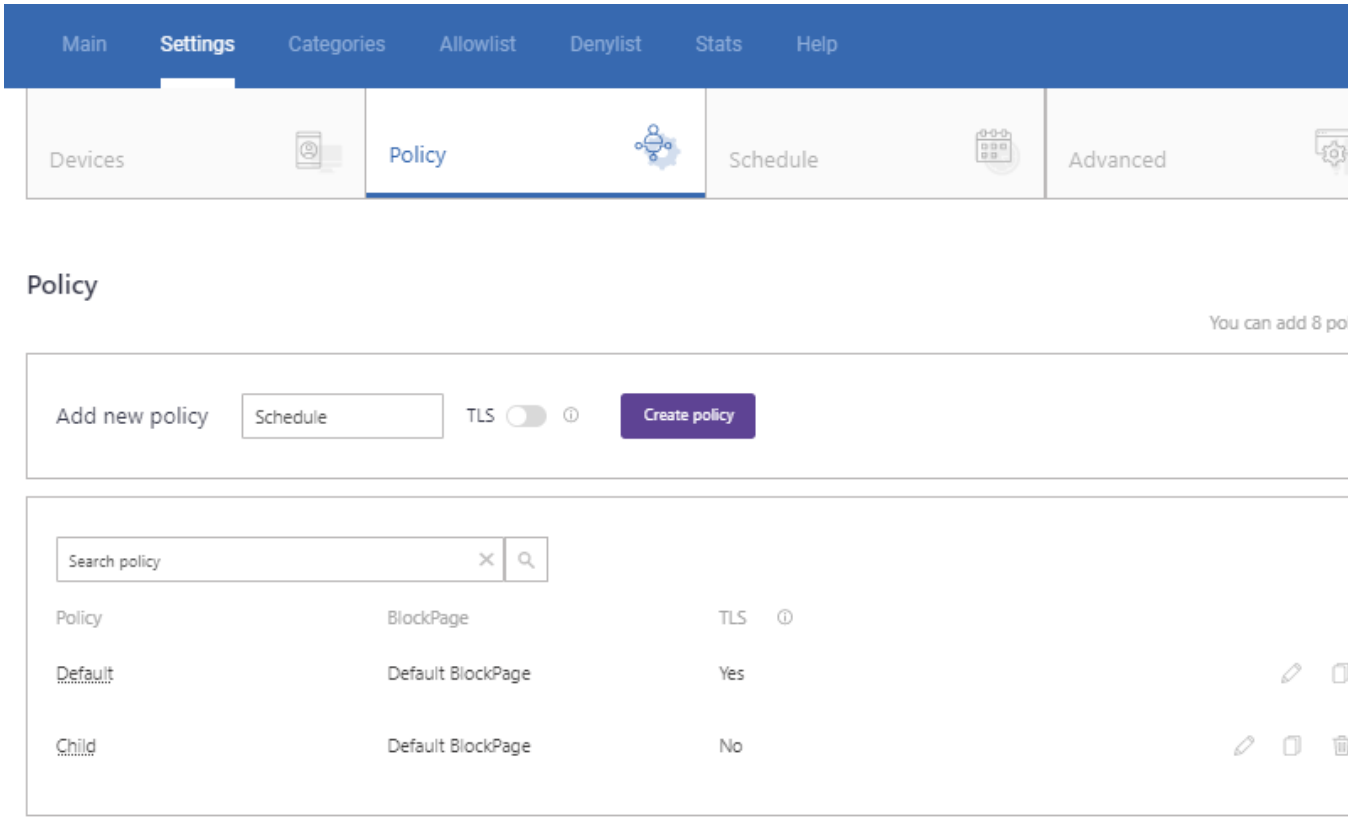
1. Turning off the internet on schedule, with the filtered internet at the other time. This option is often used by parents to limit kids during school hours.
2. Filtering of unproductive websites at the workplace, with unfiltered access during lunch break, and before and after the workday. This type of scheduling is suitable for use within organizations.
3. Filtered internet in the hours when the computer is used by a child, with different filtering rules in the hours when the computer is used by adults.

Schedule setup

To set the schedule, you must create an additional Policy (profile) for which the schedule will be enabled.

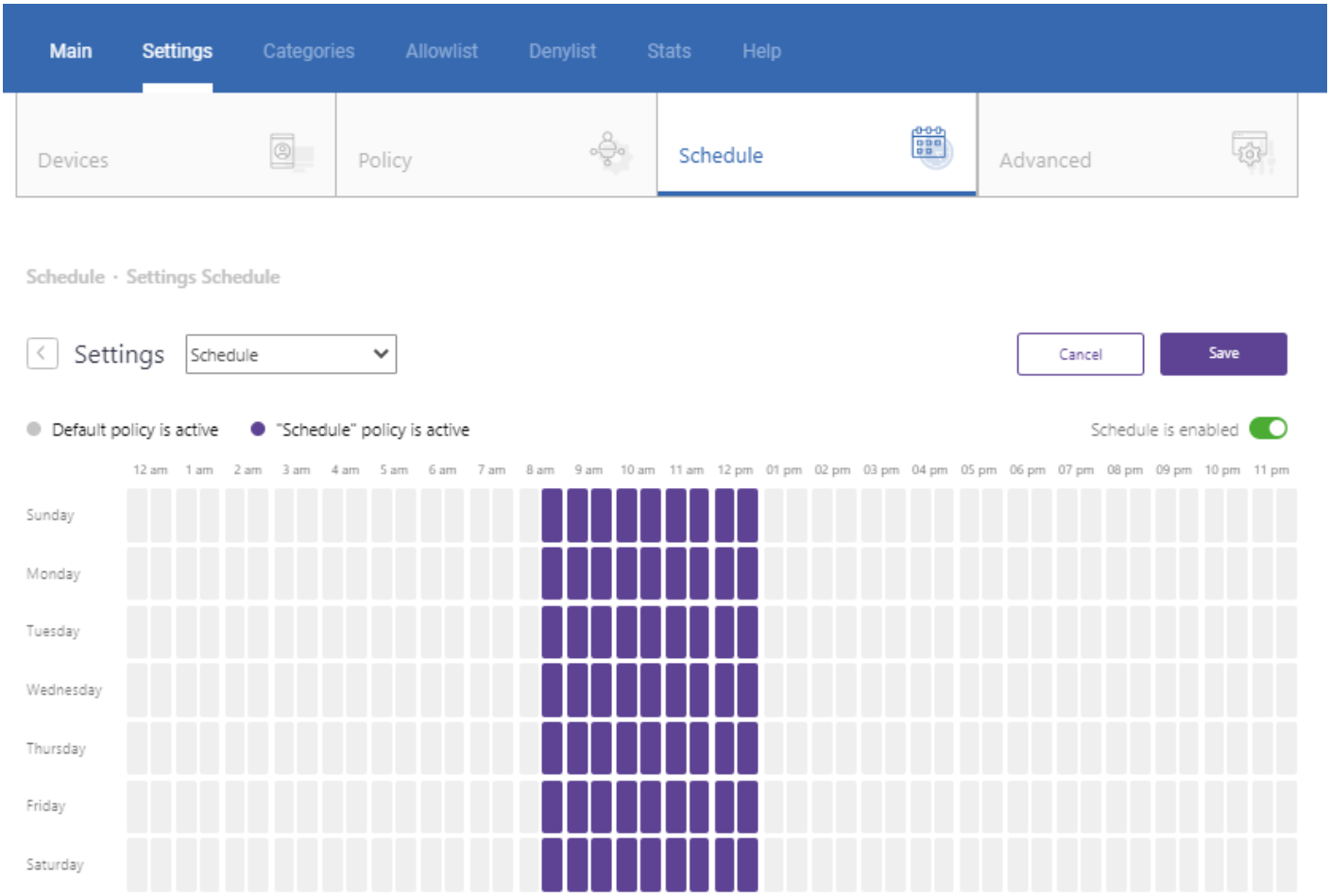
1. Log in to your SafeDNS Dashboard
2. Go to **Settings > Policy**

3. Enter the name of the policy (e.g. "*Schedule*"), and click "**Create policy**".



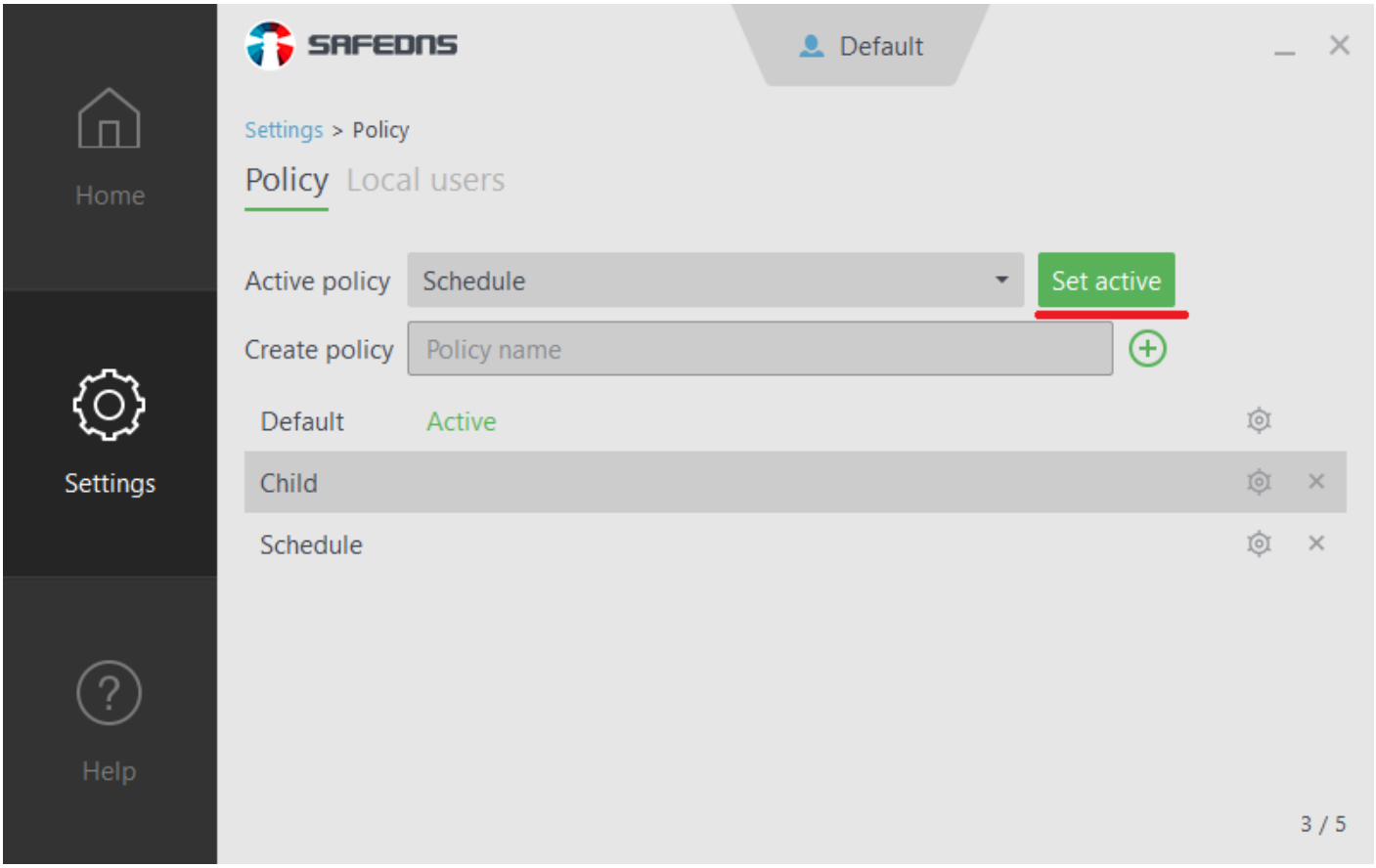
After creating a policy, you can start setting up the schedule.

1. Go to **Settings > Schedule**.
2. Select the newly created policy "*Schedule*" from the dropdown menu on the left.
3. Set the time at which the policy "*Schedule*" should be active. The rest of the time the Default policy will be active. The appearance and functionality of the Schedule depend on your service plan.
4. Switch on the **Schedule is enabled** on the right.
5. Click "**Save**".



After setting the schedule, you need to apply it to your network or individual computers.

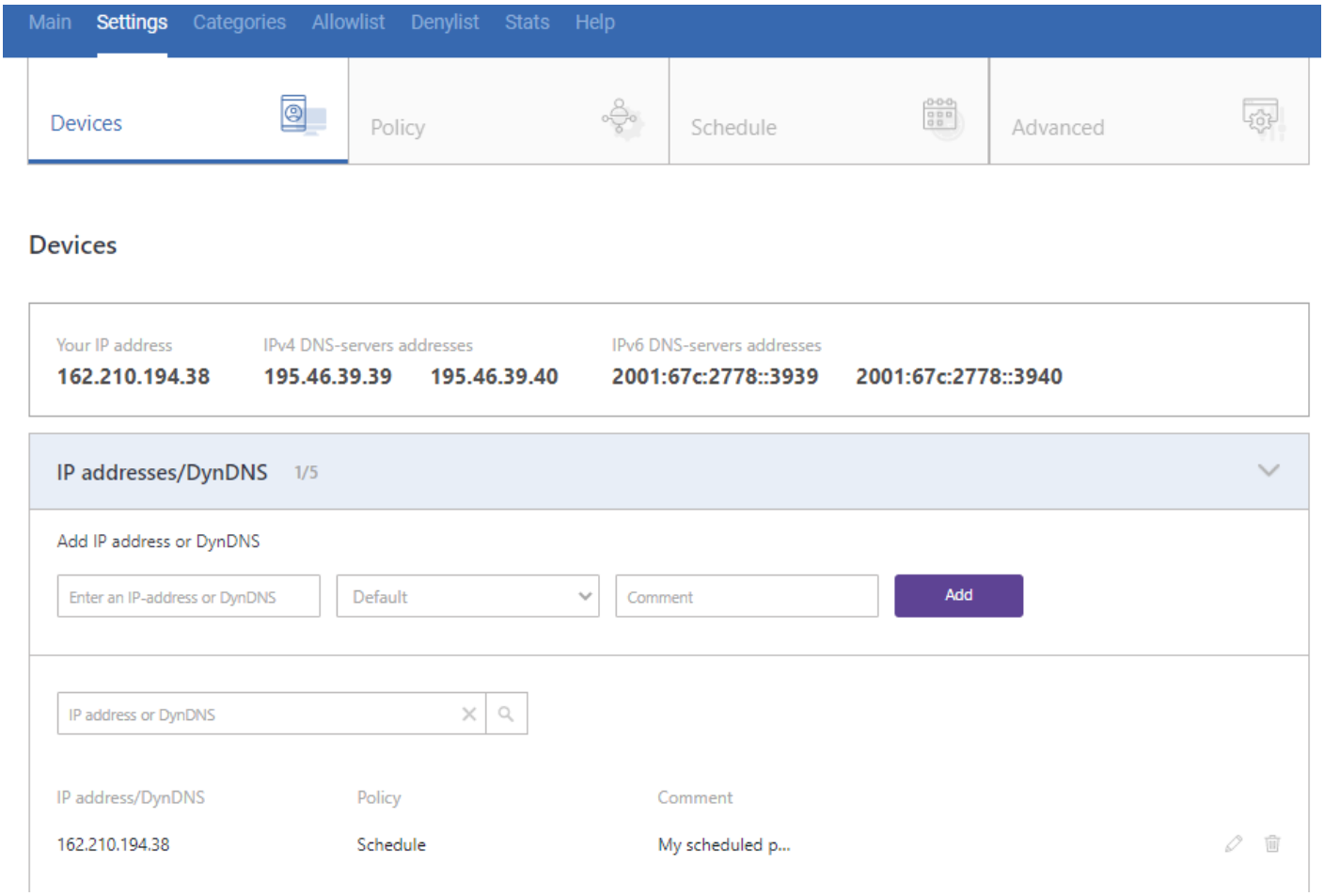
If you use the SafeDNS Agent, you need to open **Settings > Policy** and set the "*Schedule*" policy as active.



If you use an unattended installation of the Agent for computers in a corporate network, you will need to reinstall it with the scheduling policy as the main policy parameter.

If your filtering is set up at the router/modem, proxy, or gateway, you need to bind your external (public) IP address to the custom "*Schedule*" policy.

1. Go to **Settings > Devices**
2. Navigate to your IP address/DynDNS and click on the edit icon on the right.
3. Change the Policy to the custom "*Schedule*" using the dropdown menu.
4. Click on the green checkmark on the right to apply changes.



After the settings are applied, the Schedule will be active.

You can have multiple policies with different schedules for different users and networks, but note that the switch will always be between the current policy and the "*Default*" policy.

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

Possible problems with the schedule

Scheduled settings switch at the wrong time

Make sure that you have the correct time zone applied. In the Dashboard, click on the **Cogwheel** icon in the top right corner, select the correct time zone and click **"Save changes"**.

> Please note that settings take 5-7 minutes to apply.

Because of the cache of DNS queries at the system level and in the browser, your computer can not immediately respond to the newly applied settings. To eliminate this, we recommend disabling automatic control of the browser cache.

The schedule is not working at all

Make sure that you have followed all steps above. If everything is done correctly and the problem persists, please contact our technical support.

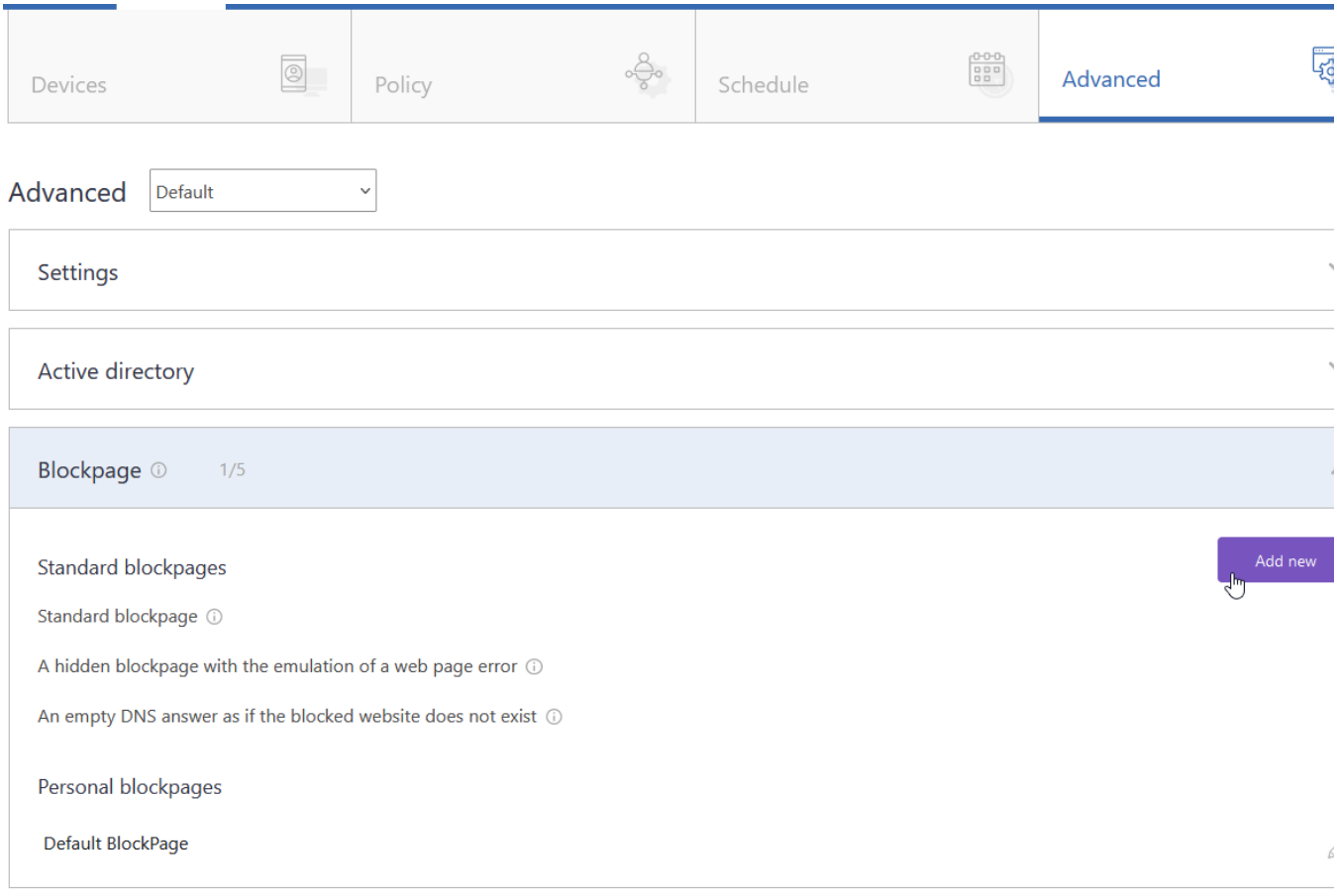
Block Page Setup

The block page is displayed when a user is trying to access a website blocked by the filtering rules. SafeDNS provides instruments to customize the block page. For example, you can add your logo and contact details on the block page, and an explanation why the website site is blocked.

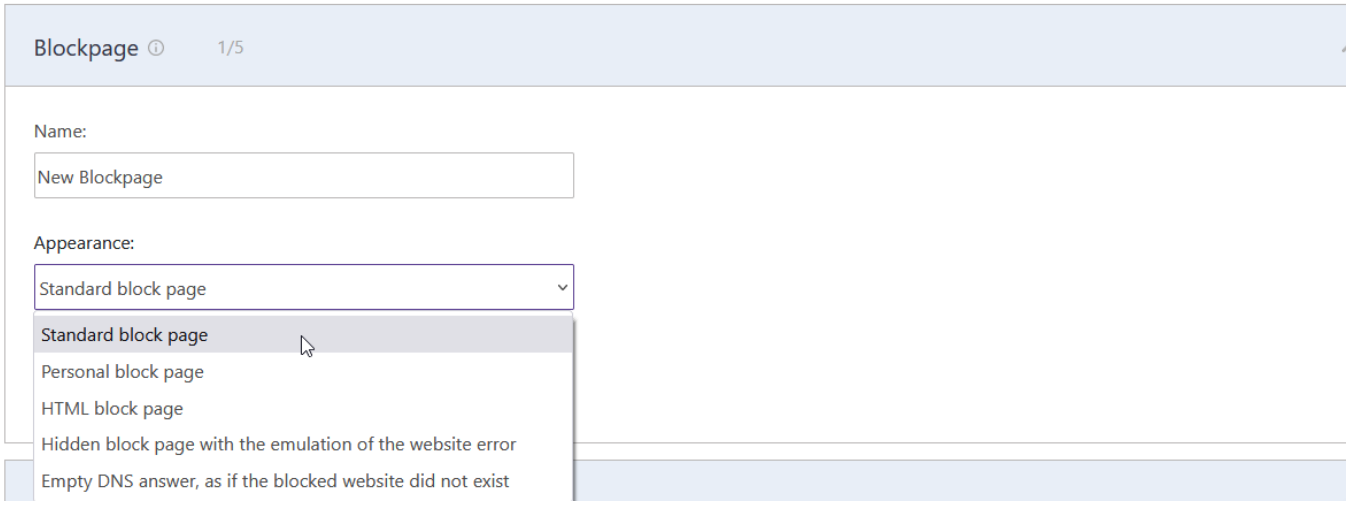
Creating custom block page

To create a custom block page, do the following:

1. Log in to SafeDNS Dashboard.
2. Navigate to **Settings > Advanced** and scroll down to the **block page** section.
3. Click "**Add new**".

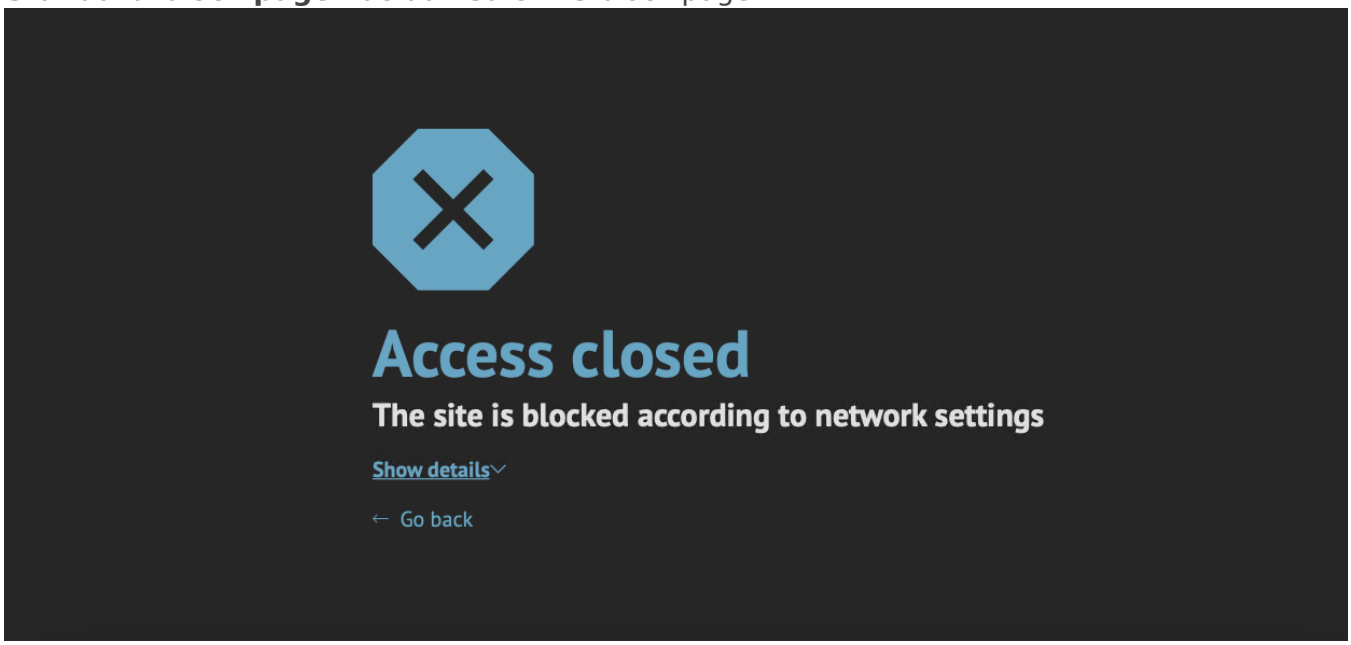


4. Enter the name of the new block page and choose its type from the dropdown menu. Click "Add".



Block page types

- **Standard block page** - default SafeDNS block page.



- **Personal block page** - simple block page with the customizable image and description.
- **HTML block page** - block page with the HTML support.
  The following variables are supported:
  - *$website* - shows the address of a blocked website.
  - *$domain* - shows the domain part of the *$website*.
  - *$reason* - shows the reason of the block, supports language prefix.
  - *$category* - shows the filtering category(-ies) of the blocked *$domain*, supports language prefix.

You can add a language prefix to translate the *$reason* and *$category* variables (e.g *$fr:reason, $ar:category*).

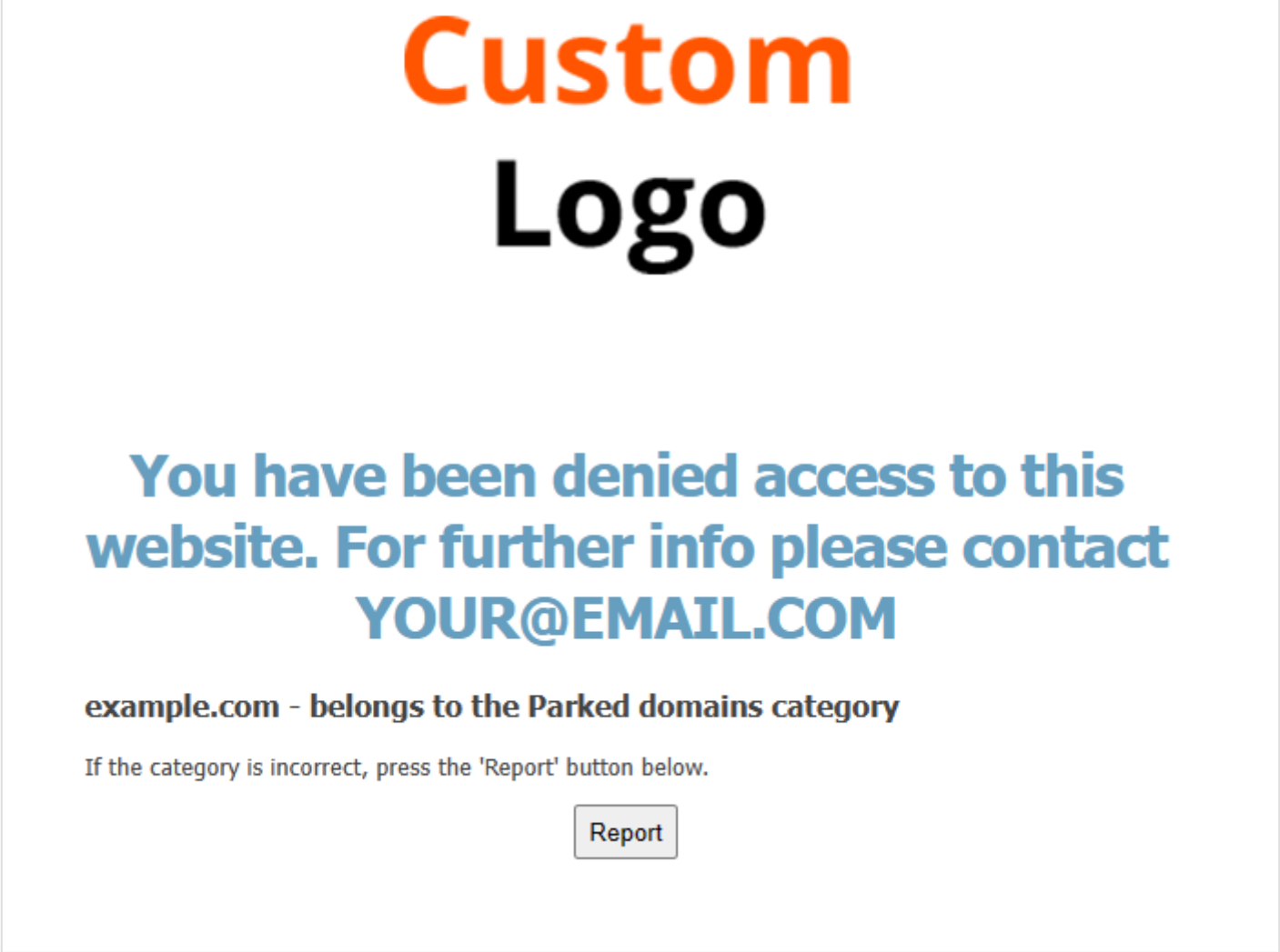
List of available languages: sq (Albanian), ar (Arabic), es (Spanish), sv (Swedish), tr (Turkish), it (Italian), en (English), ur (Urdu), pt_BR (Brazilian Portuguese), fr (French), de (German).

HTML blockpage example

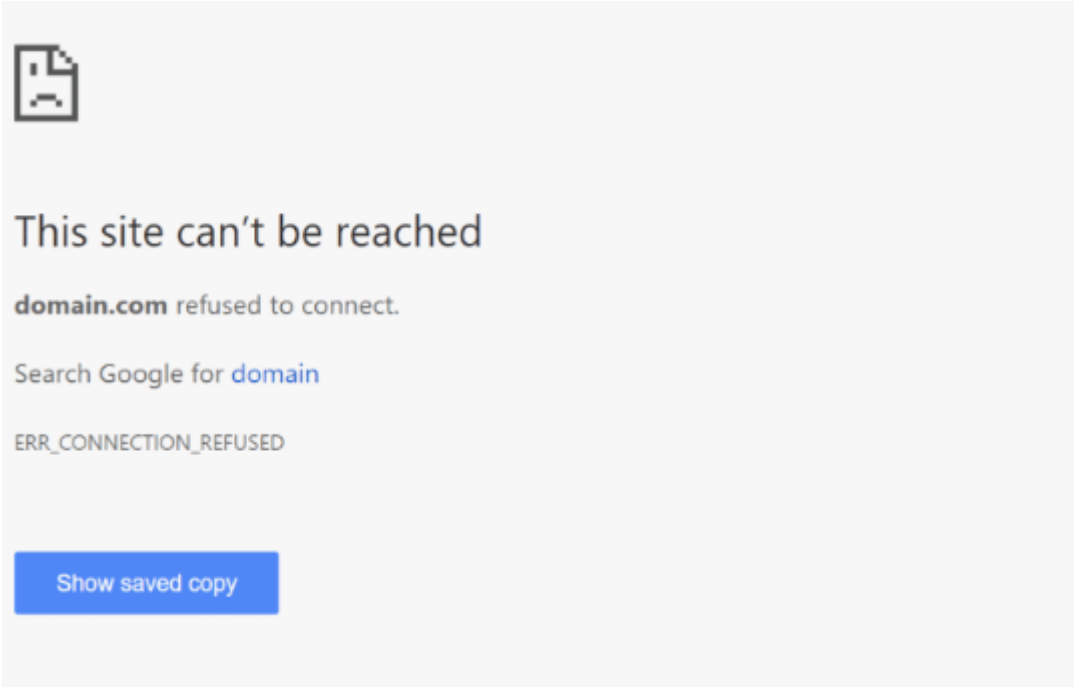
```
<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<title>Website Blocked</title>
<style media="screen" type="text/css">
body { font-family: Tahoma, sans-serif; font-size: 16px; color: #444; text-align: left;
background-color: white; width: 100%; height: 100%; margin: 0; padding: 0; }
h1 { font-size: 32px; letter-spacing: -1px; font-weight: bold; color: #659ebf; text-align:
center; margin-top: 20px; margin-bottom: 20px; }
a { color: #659ebf; font-weight: bold; text-decoration: none; }
.micro { font-size: 13px; text-align: center; }
.med { font-size: 13px; }
</style>
</head>
<body>
<table id="f" style="width: 100%; height: 100%; border: 1px solid black; display: none;">
<tbody>
<tr><td style="font:normal 10px Tahoma, sans-serif;color:#333;text- align:center;">Content
is Blocked</td></tr>
</tbody>
</table>
<table id="b" style="width: 600px;" align="center">
<tbody>
<tr>
<td>
<div align="center">
<img src="//YOUR.WEBSITE/YOUR-LOGO.PNG" border="0">
</div>
<h1>You have been denied access to this website. For further info please contact
YOUR@EMAIL.COM</h1>
<div id="detailed-info">
<p><strong>$website $reason</strong></p>
</div>
```

```
<div class="report-form">
<p class="med">If the categories are listed incorrectly, press the 'Report' button
below.</p>
<form method="post" action="mailto:YOUR@EMAIL.COM?subject=$website">
<div align="center">
<input name="send" value="Report" style="height:30px;" type="submit">
</div>
</form>
</div>
</td>
</tr>
</tbody>
</table>
</body>
</html>
```

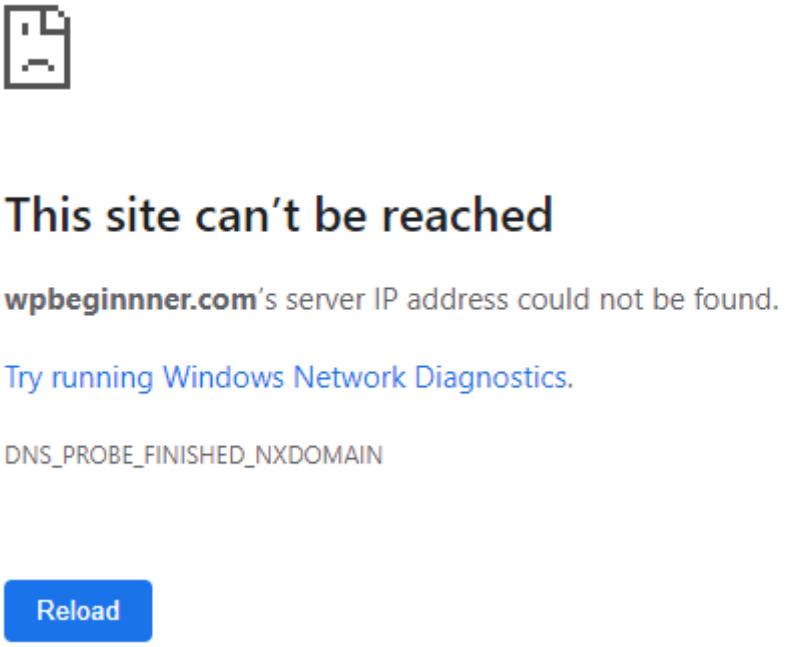
Please change the "**//YOUR.WEBSITE/YOUR-LOGO.PNG**" and "**YOUR@EMAIL.COM**" in the lines 25, 27, and 33 accordingly.



- **Hidden block page with the emulation of the website error** - block page that imitates browser's website error.

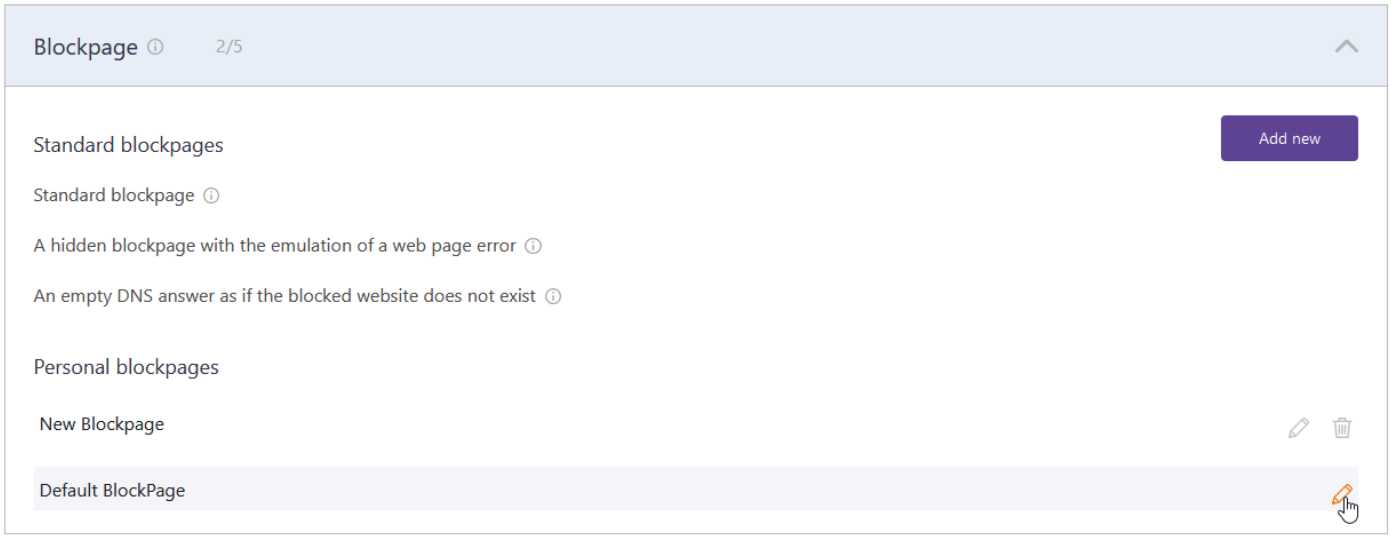


- **Empty DNS answer, as if the blocked website does not exist** - block page that imitates NXDOMAIN browser error.



The availability of a certain block page type depends on your billing plan.

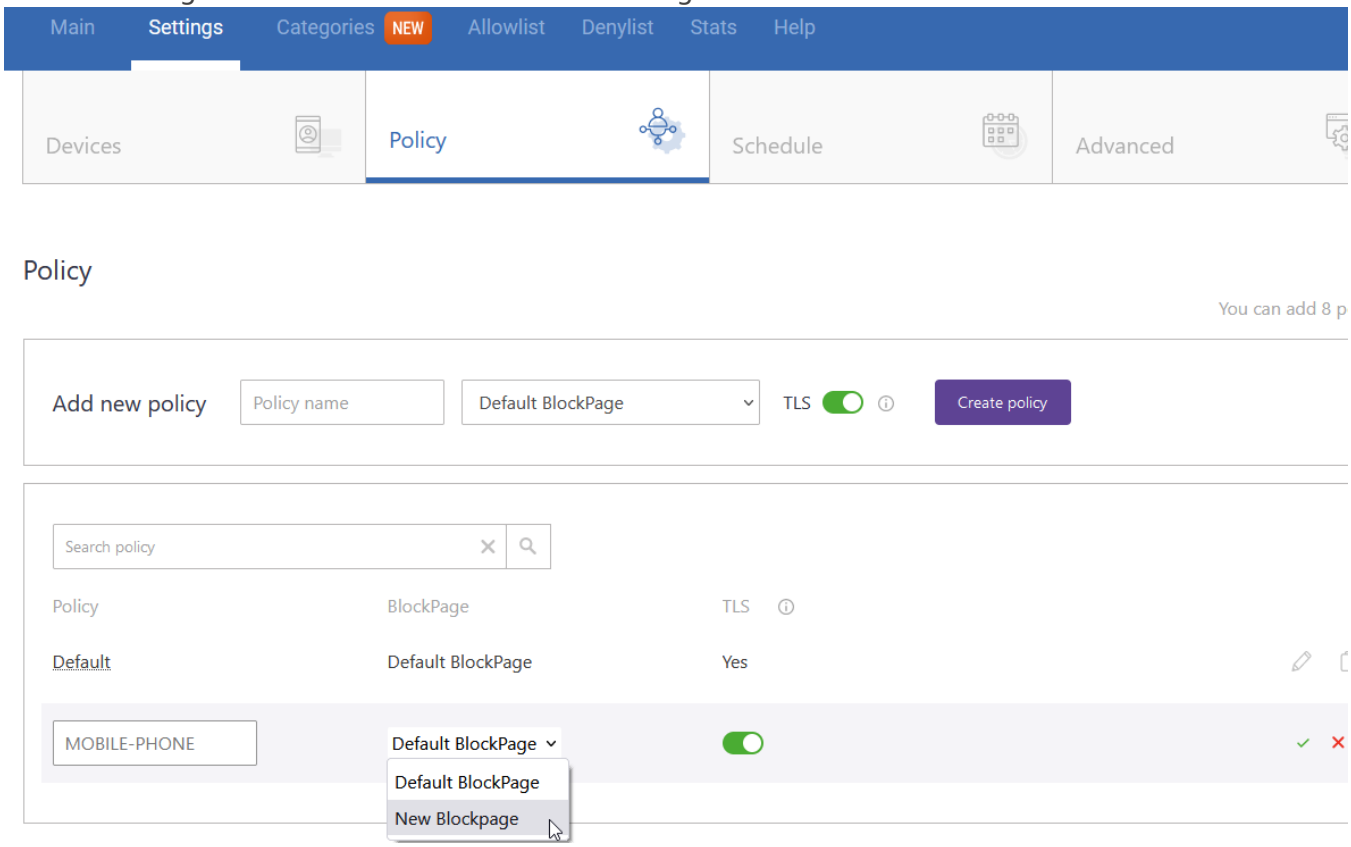
You can always edit the block page type by clicking on the pencil icon to the right.



Applying custom block page

To create a custom block page, do the following:

1. Navigate to **Settings > Policy**.
2. Click on the pencil icon to the right from the filtering policy.
3. Select the custom block page from the dropdown menu.
4. Click on the green check mark to save the changes.



Please note that the SafeDNS TLS certificate should be installed on each end device where you want HTTPS pages to display correctly. Without the certificate, block page will be displayed for

HTTP websites only.

SafeDNS Root CA certificate installation guide.

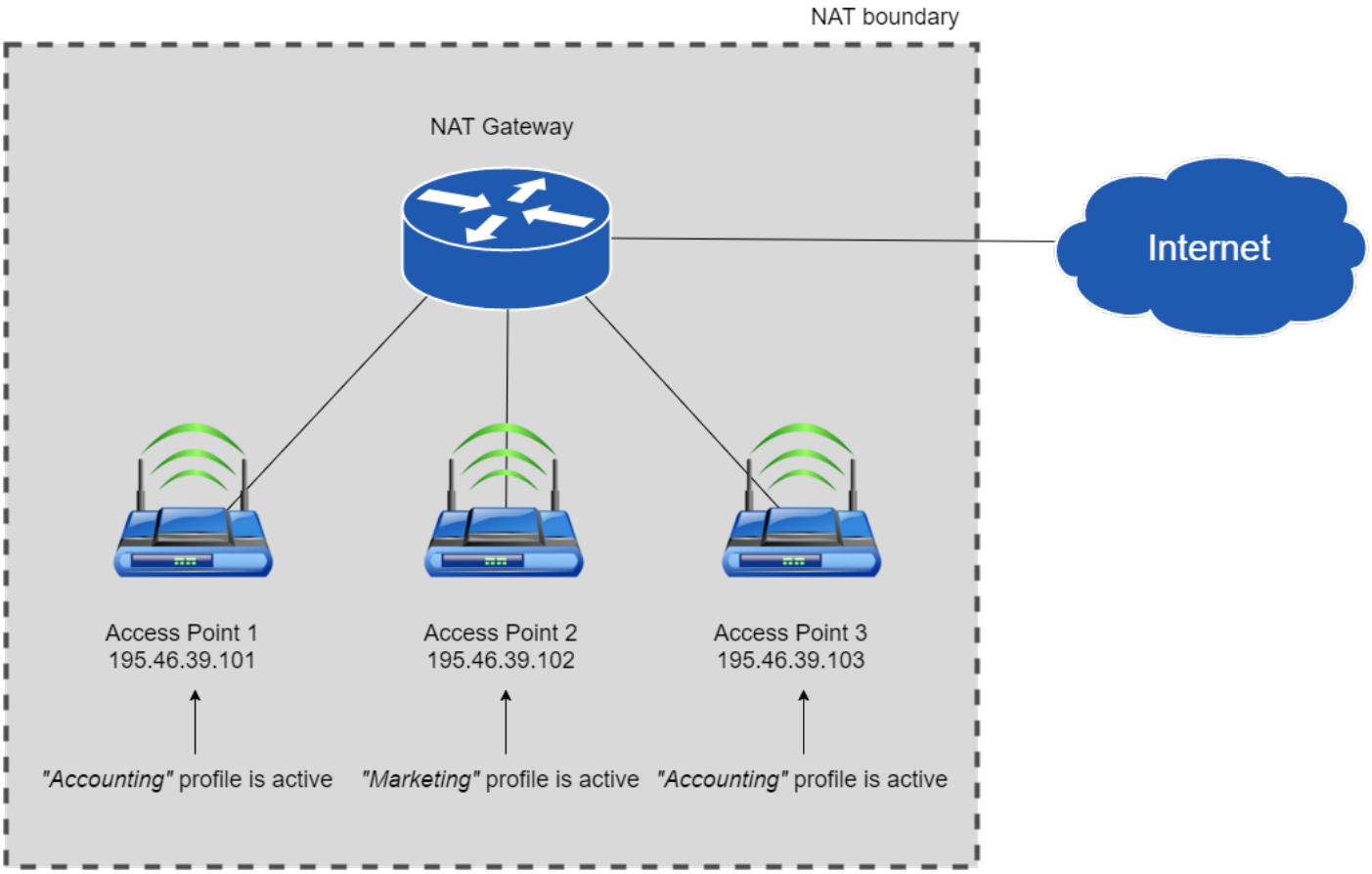
NAT DNS Setup

This feature is not available for the Safe@Home plan.

- Network Address Translation or NAT is frequently used in corporate networks. It allows network owners and administrators to:
  - decrease the number of static IPs
  - secure local networks
  - prevent unwanted external access to the local hosts
  - hide the entire internal network structure

NAT DNS is a SafeDNS service feature designed to apply different filtering policies to different networking hardware (routers, gateways, etc.) behind NAT with one public IP.

Your networking hardware should be set up according to the SafeDNS instructions.



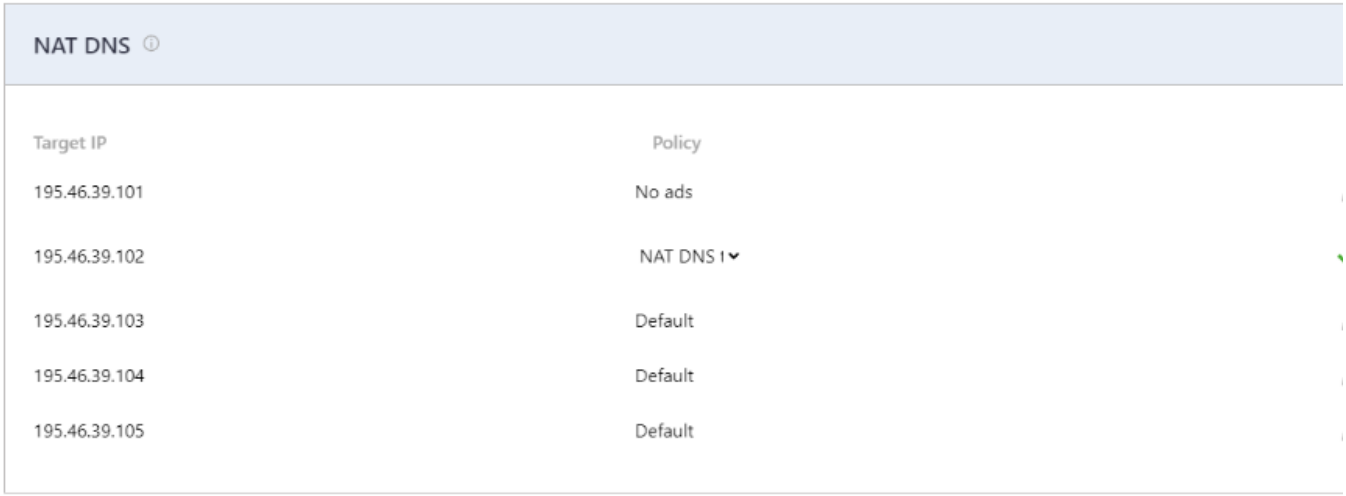
NAT DNS setup

1. Enter the **Dashboard > Settings**. Assign the **Public IP** of a NAT device to one of the existing filtering policies under the “IP addresses / DynDNS” section. (to use NAT DNS you must have 2 or more policies).
2. Manually or via DHCP set up the **target DNSes** on the end devices (routers or gateways behind NAT).

   List of target DNS addresses:

   195.46.39.101
   195.46.39.102
   195.46.39.103
   195.46.39.104
   195.46.39.105

3. In the **Dashboard > Settings**, scroll down to the bottom, and assign policies to the **Target IPs** (one IP = one policy). Click on the green checkmark to apply settings.



After that, all devices behind NAT will be filtered by the chosen policy.

You can view the stats for each **Target IP** by selecting its policy in the **Stats** tab.

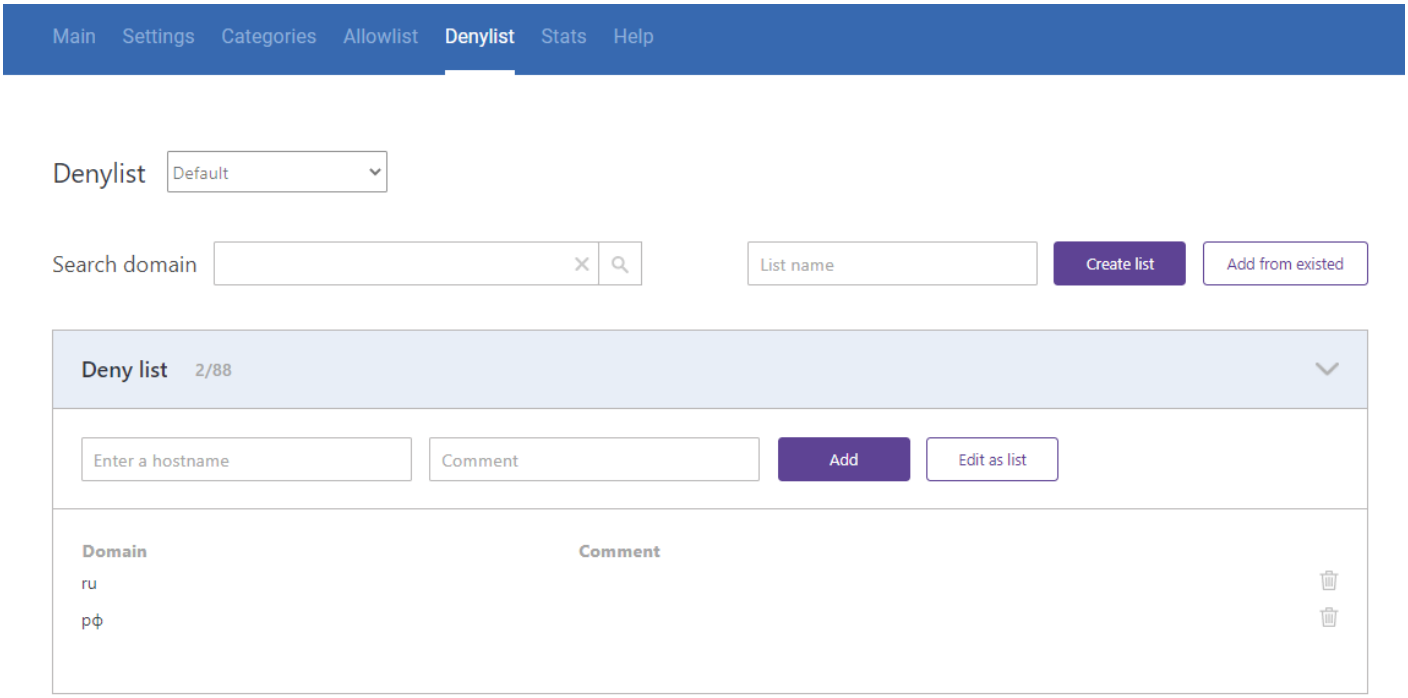
> This feature works only for networks behind NAT. If you use a proxy server, the NAT DNS filtering option will not work, because in proxy server’s settings will be applied instead.

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

Top-level Domains Blocking

If you want to block any top-level domain, just add it without a leading dot to your **Denylist**.

For example, if you want to block access to all websites in the RU domain zone, add **ru** to your Denylist.



Internationalized country code top-level domains should be added to the Denylist list in the IDN form:
(Chinese IDN ccTLD), **рф** (Russian IDN ccTLD), etc.

A full list of top-level domains can be found on the IANA website and Wikipedia.

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