



SafeDNS

Content Filtering Service Guide

August 2018

Contents

| | |
|--|----|
| 1. What is SafeDNS and what it is made for..... | 7 |
| 1.1. What SafeDNS is made for | 7 |
| 1.2. Solutions for Web Filtering and Network Security..... | 7 |
| 1.3. How SafeDNS works | 8 |
| 1.4. The basis of SafeDNS database | 9 |
| 2. How to set up content filtering..... | 10 |
| 2.1. How to start using SafeDNS | 10 |
| 2.2. How to protect your computer | 11 |
| 2.3. How to protect your laptop with SafeDNS..... | 13 |
| 2.4. How to protect your mobile device | 13 |
| 2.5. How to protect the entire network..... | 13 |
| 2.6. How to add multiple IP addresses..... | 13 |
| 2.7. How to enable filtering on a dynamic IP address | 13 |
| 3. Blocking categories of websites | 14 |
| 3.1. How to block porn sites or other site categories..... | 14 |
| 3.2. How to block banner ads, advertisement videos, pop-up windows | 14 |
| 4. Black and White lists..... | 15 |
| 4.1. How to block access to specific domains..... | 15 |
| 4.2. How to block all subdomains for main domains | 15 |
| 4.3. How to allow access to the specific domain from a blocked category | 16 |
| 4.4. How to allow access only to websites in your whitelist (Whitelist-only mode)..... | 17 |
| 4.5. Named Black / white lists | 17 |
| 5. Additional features | 20 |

| | |
|--|----|
| 5.1. Forcing Safe Search | 20 |
| 5.2. How to enable Safe Search Agent..... | 21 |
| 5.3. How to forcibly turn on Restricted mode on YouTube | 22 |
| 6. Botnets, Phishing and Virus propagation | 23 |
| 6.1. How to turn on notifications in botnet activity in my network..... | 23 |
| 6.2. Blocking access to botnet control nodes | 23 |
| 6.3. Blocking access to phishing sites | 24 |
| 6.4. Blocking access to virus propagation sites | 25 |
| 7. Profiles | 27 |
| 7.1. How to add a filtering profile | 27 |
| 7.2. How to change the name of the profile settings | 28 |
| 7.3. How to copy profile settings | 28 |
| 7.4. How to change profile settings for the selected static or dynamic IP address..... | 29 |
| 7.5. How to make different filters for different users of the same computer | 29 |
| 8. Schedule..... | 30 |
| 8.1. How to set up schedule for filtering..... | 30 |
| 8.2. Possible issues with the schedule | 32 |
| 9. Customizing appearance of the service..... | 33 |
| 9.1. How to use custom text and picture on the block page..... | 33 |
| 9.2. How to change the design of the whole block page..... | 34 |
| 9.3. How to conceal that blocking is in effect | 37 |
| 10. Statistics | 38 |
| 10.1. How do I view statistics in my account queries..... | 38 |
| 10.2. How to see list of the most popular sites | 39 |
| 10.3. How to view list of blocked sites..... | 40 |

| | |
|--|----|
| 10.4. How to see a list of the most popular website categories..... | 40 |
| 10.5. How to view statistics for a selected period | 41 |
| 10.6. How to view statistics for a specific profile..... | 41 |
| 10.7. How to view detailed statistics..... | 42 |
| 10.8. How to export statistics | 42 |
| 10.9. How to get automatic statistic reports by email | 43 |
| 10.10. How to view statistics for different computers, devices and networks..... | 43 |
| 11. Local resources | 45 |
| 11.1. How to make local resource easily available. Use aliases..... | 45 |
| 11.2. How to temporarily suspend filtering | 45 |
| 11.3. Does SafeDNS work with proxy servers? | 48 |
| 11.4. How to change time zone for schedule and statistics..... | 48 |
| 11.5. How to see reason for blocking a website on block page..... | 49 |
| 11.6. How to check website category | 50 |
| 12. Active Directory and Administrators | 51 |
| 12.1. Service settings in Active Directory network through the cloud | 51 |
| 12.2. Working with Active Directory through a special version of the agent | 52 |
| 12.3. Working with Active Directory for single filtering settings | 52 |
| 12.4. How to enable multiple account administrators | 53 |
| 12.5. How to see Administrator activity log | 54 |
| 12.6. How to install Agent on a corporate network | 54 |
| 13. Other modes of service..... | 56 |
| 13.1. How to turn on monitor mode | 56 |
| 13.2. How to completely block access to the internet..... | 57 |
| 14. Pricing policy | 58 |

| | |
|--|----|
| 14.1. SafeDNS billing plans..... | 58 |
| 14.2. How to calculate the number of licenses required..... | 59 |
| 14.3. How to buy premium services | 59 |
| 14.4. How to extend premium services..... | 60 |
| 14.5. How to see list of fees and plan switching | 60 |
| 14.6. How to change paid billing plan to another | 61 |
| 14.7. What happens when paid period ends of plan..... | 61 |
| 15. Technical support..... | 62 |
| 15.1. How to get support | 62 |
| 15.2. What is SafeDNS Help Desk portal | 62 |
| 15.3. How to completely disable content filtering | 62 |
| 15.4. How to change email account..... | 63 |
| 15.5. How do I change my account password | 63 |
| 15.6. My IP address is already used by someone else..... | 63 |
| 16. Clearing cache | 64 |
| 16.1. Windows..... | 64 |
| 16.2. OS X | 64 |
| 16.3. Linux (major distributions)..... | 65 |
| 16.4. Debian | 65 |
| 16.5. Ubuntu Linux..... | 66 |
| 16.6. Clearing your cache in Google Chrome | 67 |
| 16.7. Clearing your cache in Opera..... | 68 |
| 16.8. Clearing your cache in Microsoft Edge and Internet Explorer..... | 69 |
| 16.9. Clearing your cache in Safari | 71 |
| 16.10. Clearing your cache in Mozilla Firefox | 72 |

| | |
|--------------------|----|
| About SafeDNS..... | 73 |
|--------------------|----|

1. What is SafeDNS and what it is made for

1.1. What SafeDNS is made for

SafeDNS is a cloud-based content filtering service based on the domain name technology – DNS, domain name system. The DNS protocol is used to map the IP address of the site and its domain name. Computers and websites work with IP addresses but for us as customers, it is more convenient to use names of sites – domains. For example, it is easier to remember google.com, not the 8.8.8.8 IP address.

1.2. Solutions for Web Filtering and Network Security

We offer a wide selection of secure, fast and reliable solutions for content and web filtering. You can find an appropriate solution for your industry or type of organization – from small business to enterprise. Work with us to make the internet safe. Contact us if you want to know more about our content filtering solutions.

Home/Parental Control

- Protect your family from threats and dangers on the internet.
- Block inappropriate websites.
- Protect every internet-connected device from tablets, laptops to gaming consoles.
- Use SafeDNS Agent, a SafeDNS software agent for Windows-based PCs, to protect your family even when you are away.
- Get protection for the entire home network with no software required.

Business

- Protect your company and maximize employees' productivity.
- Block inappropriate and insecure websites.
- Get centralized protection and management for your decentralized infrastructure.

Educational Institutions and Libraries

- Reliable protection for all educational institutions from K-12 schools to higher education.
- Full CIPA compliance.

- Safe Internet for your campus networks and every connected device in your school or college.

Telecoms and Internet Service Providers (ISPs)

- Protect your infrastructure and users.
- Get a standalone solution with the ability to serve millions of users.
- Launch your own branded protection for your customers (parental control and content filtering services).
- Follow government regulations.

Wi-Fi Hotspots and Wireless ISPs

- Protect your infrastructure and users in few minutes.
- Provide centralized protection and management for your decentralized infrastructure.
- Secure access without excessive filtering to your customer satisfaction.

Service Providers and VARs

- Join our partnership program and earn money with us.
- Protect your customers' networks and devices against threats with less service overheads.
- Get reseller panel for centralized management of all your customers' networks and registration of users.
- Show your own brand for your customers.

OEM Partners

- Use our database of categorized websites in your own software and systems.
- Integrate a white-labeled version of SafeDNS Agent.
- Install SafeDNS parental control software on your PCs or other devices.

1.3. How SafeDNS works

Pretty simple. As a registered user you choose the categories of websites you wish to block in your SafeDNS filtering service Dashboard at safedns.com. A few minutes later the changes will come into effect on SafeDNS DNS servers, and the filtering rules that

you have set will be applied to the protected networks and devices.

Once you have done that, all DNS requests from these networks and devices are redirected to the SafeDNS servers, where each request is categorized and checked against the content categories you have previously blocked. If there's a request for a site not included in any of the blocked categories or in any blacklist, the IP address of the site will be returned, and the web page will be opened. If the request is for a site from a blocked category, then the answer will contain IP address of the SafeDNS block page. At the same time, the quality of content filtering in many respects depends on the relevance of a website database, used for site categorization, as well as on the coverage of the internet by the database.

1.4. The basis of SafeDNS database

SafeDNS provides the best categorization database on the market. Now the database contains over 100 million sites, which covers approximately 3/4 of the existing and working internet resources.

The SafeDNS categorization database is based on:

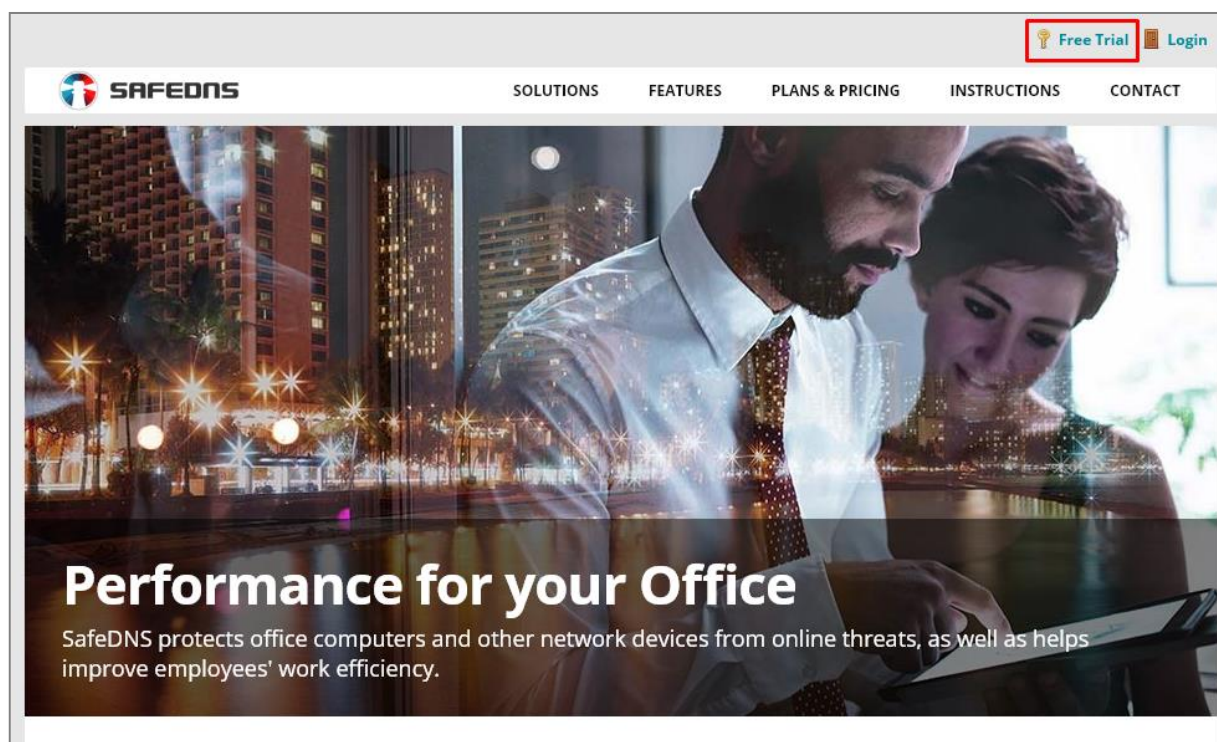
- Automatic categorization by the SafeDNS crawler
- Detection of virus propagation sites by a special module for detecting malicious resources
- Manual categorization by SafeDNS specialists
- DNS logs of SafeDNS users
- Custom categorization.

[Back to the Contents](#)

2. How to set up content filtering

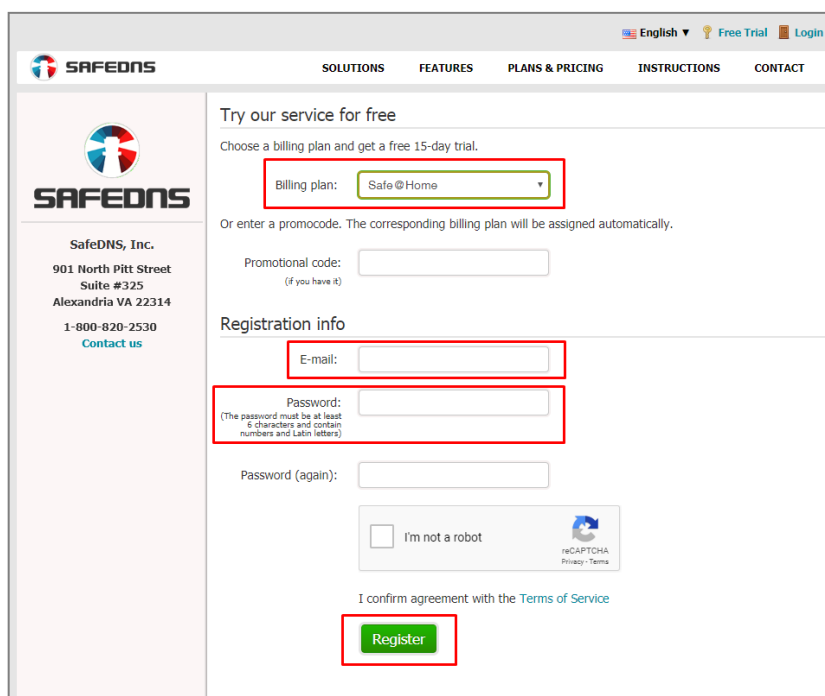
2.1. How to start using SafeDNS

First of all, you need to register at the SafeDNS website. Please, click the **Free Trial** link in the upper right corner of the website.



On the registration page select a billing plan you need. You can use a 15-day trial period (for any of the 'Home', 'School', 'Office' plans). Next, you need to create your login credentials – **email** and **password** which will be used for identification. After that, enter the captcha and accept rules for using the SafeDNS service and click the **Register** button.

Confirmation of your registration in the SafeDNS service will be sent to your email. Also, you can immediately pay any paid plan on our website (for more details about the billing plans and payments – [see this guide, §14](#))



The screenshot shows the SafeDNS registration page. On the left is a sidebar with the SafeDNS logo and contact information for SafeDNS, Inc. (901 North Pitt Street, Suite #325, Alexandria VA 22314, 1-800-820-2530, and a 'Contact us' link). The main content area is titled 'Try our service for free' and includes a dropdown menu for 'Billing plan' (set to 'Safe@Home'), a 'Promotional code' field, and a 'Registration info' section with fields for 'E-mail', 'Password' (with a note: 'The password must be at least 8 characters and contain numbers and Latin letters'), and 'Password (again)'. There is also a checkbox for 'I'm not a robot' with a reCAPTCHA logo, a link to 'Terms of Service', and a green 'Register' button. The top navigation bar includes links for 'SOLUTIONS', 'FEATURES', 'PLANS & PRICING', 'INSTRUCTIONS', and 'CONTACT', along with language and login options.

2.2. How to protect your computer

To protect your computer, you can install SafeDNS Agent or configure filtering through **DDClient** in case your computer has a dedicated external dynamic IP address.

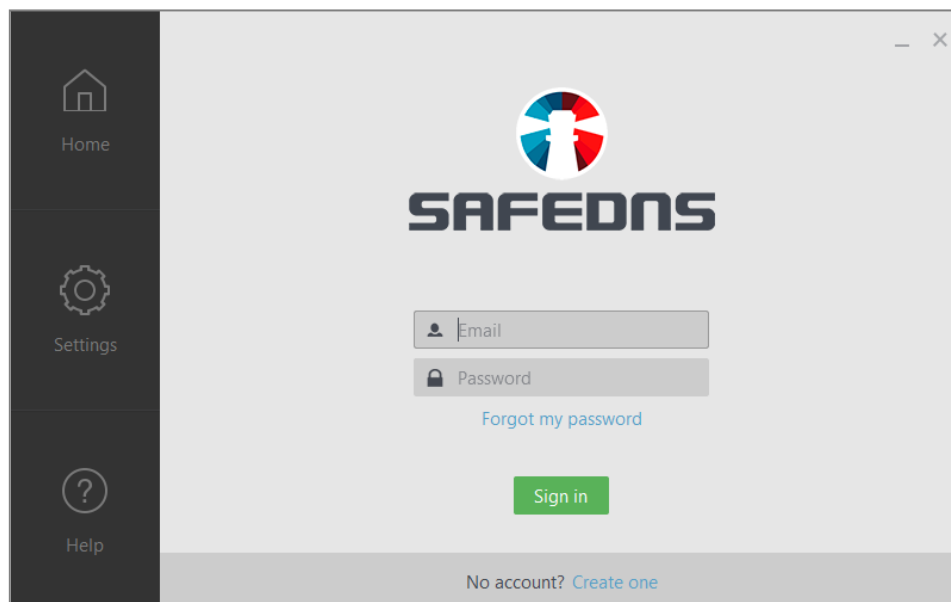
How to install SafeDNS Agent

Download an installation file from your Dashboard or by the link:
<https://www.safedns.com/downloads/SafeDNS-Agent-Setup.exe>

Upon launching the file, you will see SafeDNS Agent setup window.



Installation of SafeDNS Agent is intuitive and straightforward. After installation is complete you can run SafeDNS Agent and log in. To sign in to Agent use the credentials you have created on the SafeDNS website.



More detailed instructions on SafeDNS Agent installation and configuration can be found on the SafeDNS website: <https://www.safedns.com/en/safedns-agent-how-to-guide/>

2.3. How to protect your laptop with SafeDNS

To protect your laptop, you can install SafeDNS Agent or configure the filtering through **DDClient** if your computer has a dedicated external dynamic (White) IP address.

2.4. How to protect your mobile device

In order to protect your mobile phone against any inappropriate material on the internet, you can install and configure an OpenVPN application following instructions on our website: https://www.safedns.com/en/guides/mobile_vpn_guide/

2.5. How to protect the entire network

You can use the following options to configure filtering to protect the network:

- Custom filtering on any other router, gateway, router
- Custom filtering by setting SafeDNS Agent on each computer in the network

2.6. How to add multiple IP addresses

If you have multiple networks with static IP address, you can add each network to Dashboard. You can make notes for your convenience in the **Comment section** (when adding your network in **Dashboard**). If necessary, you can choose different policies (profiles) on your network.

To add a network, go to **Dashboard -> Settings -> Nets**.

2.7. How to enable filtering on a dynamic IP address

There are several options:

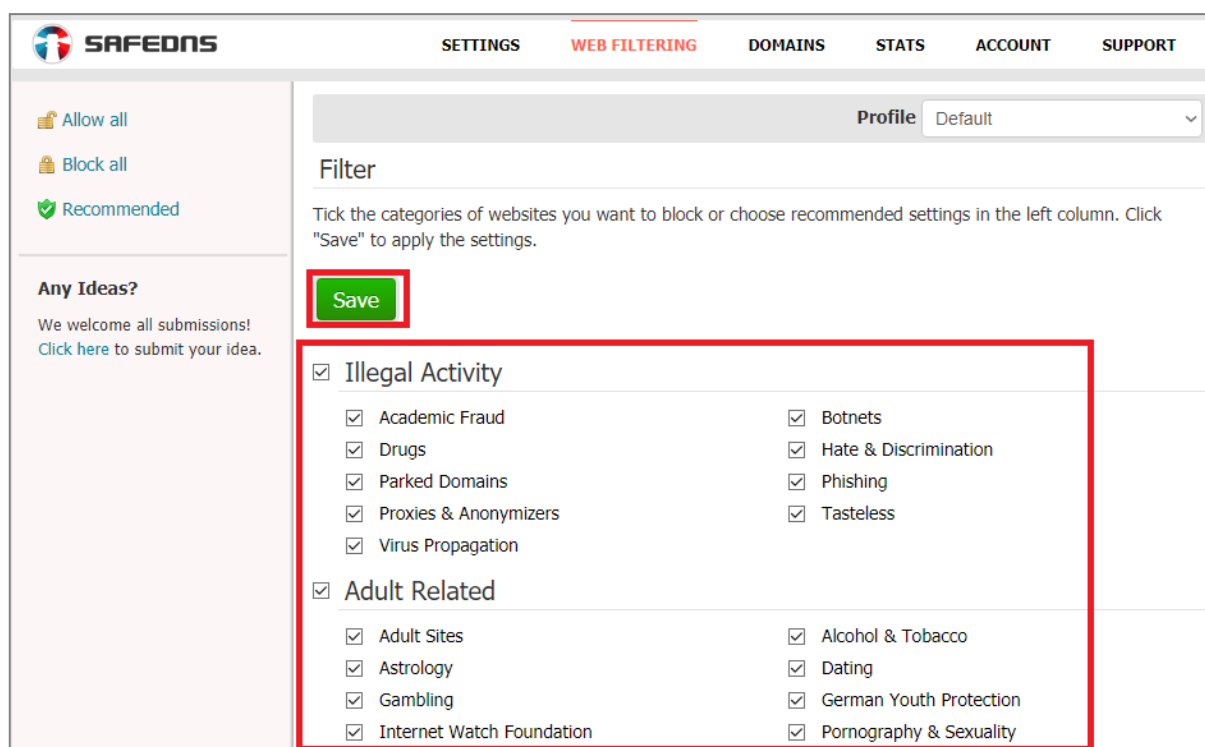
- Install and configure SafeDNS Agent.
- If your router supports any of DynDNS services, you can configure filtering by using this service. You can see the instruction on how to configure the filtering on the SafeDNS website: <https://www.safedns.com/en/setup-on-dsl-wi-fi-routers/#dynamic>.

[Back to the Contents](#)

3. Blocking categories of websites

3.1. How to block porn sites or other site categories

To block pornography and other categories of sites, you need to go to **Dashboard -> Web Filtering section**, tick the checkbox next to the category/categories or their groups you wish to block and save the settings (click the green **Save** button). To unblock a category, untick it and save the settings. The settings will be distributed to all of the SafeDNS servers in 3-5 minutes.



SAFEDNS SETTINGS **WEB FILTERING** DOMAINS STATS ACCOUNT SUPPORT

Profile Default

Filter

Tick the categories of websites you want to block or choose recommended settings in the left column. Click "Save" to apply the settings.

Save

- ☒ **Illegal Activity**
 - ☒ Academic Fraud
 - ☒ Drugs
 - ☒ Parked Domains
 - ☒ Proxies & Anonymizers
 - ☒ Virus Propagation
 - ☒ Botnets
 - ☒ Hate & Discrimination
 - ☒ Phishing
 - ☒ Tasteless
- ☒ **Adult Related**
 - ☒ Adult Sites
 - ☒ Astrology
 - ☒ Gambling
 - ☒ Internet Watch Foundation
 - ☒ Alcohol & Tobacco
 - ☒ Dating
 - ☒ German Youth Protection
 - ☒ Pornography & Sexuality

3.2. How to block banner ads, advertisement videos, pop-up windows

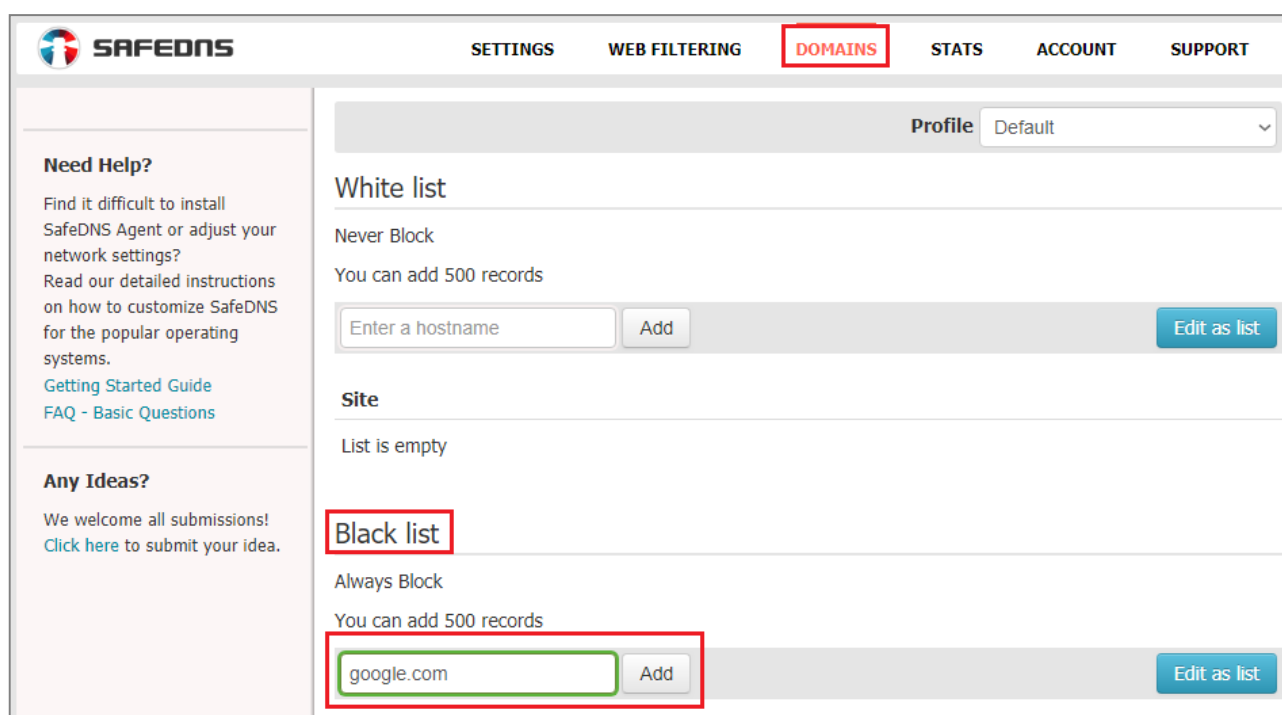
To block banner ads, you need to go to **Dashboard -> Web Filtering -> Time Wasters** group and tick the category **Banner Ads**, then click **Save** to apply the settings.

[Back to the Contents](#)

4. Black and White lists

4.1. How to block access to specific domains

To block certain sites, go to **Dashboard -> Domains tab -> Blacklist section**, enter the domain you want to block and click **Add** button. To block a site, its domain should be entered without 'www' (for example, **google.com**). In this case, the whole domain will be blocked, including its subdomains. If you want to block only a particular subdomain (for example, **maps.google.com**), you just need to add this subdomain to your blacklist. In this case, the remaining subdomains of the domain **google.com** will be available.



The screenshot shows the SafeDNS web interface. The top navigation bar includes 'SETTINGS', 'WEB FILTERING', 'DOMAINS' (highlighted with a red box), 'STATS', 'ACCOUNT', and 'SUPPORT'. On the left, there is a sidebar with 'Need Help?' and 'Any Ideas?' sections. The main content area is titled 'Profile Default' and contains two sections: 'White list' and 'Black list' (highlighted with a red box). The 'White list' section is currently empty, showing 'Never Block' and 'You can add 500 records'. The 'Black list' section is also empty, showing 'Always Block' and 'You can add 500 records'. In the 'Black list' section, the input field 'google.com' is highlighted with a green box, and the 'Add' button is highlighted with a red box. An 'Edit as list' button is visible at the end of each section.

Once the domain is added, it will be shown in the list below. These changes will be applied approximately in 3-5 minutes and the domain will be blocked.

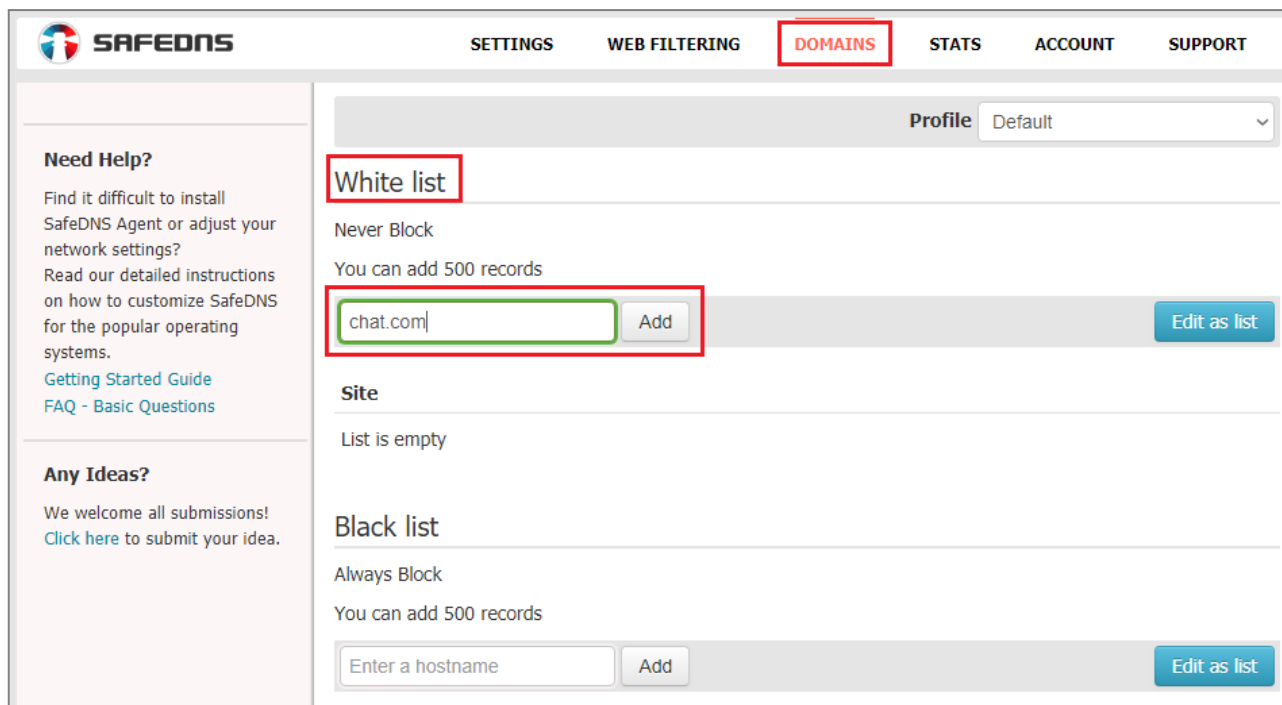
4.2. How to block all subdomains for main domains

To block all subdomains of a domain, you should block the primary domain. For example, if you need to block **maps.google.com**, **docs.google.com**, etc., you should add the root domain **google.com** to your blacklist.

4.3. How to allow access to the specific domain from a blocked category

To access a domain from a blocked category you have to add this domain to your whitelist. For example, if you need to open access **to chat.com** but block all other messengers, block the category **Chat & Messengers** and add **chat.com** domain to your whitelist.

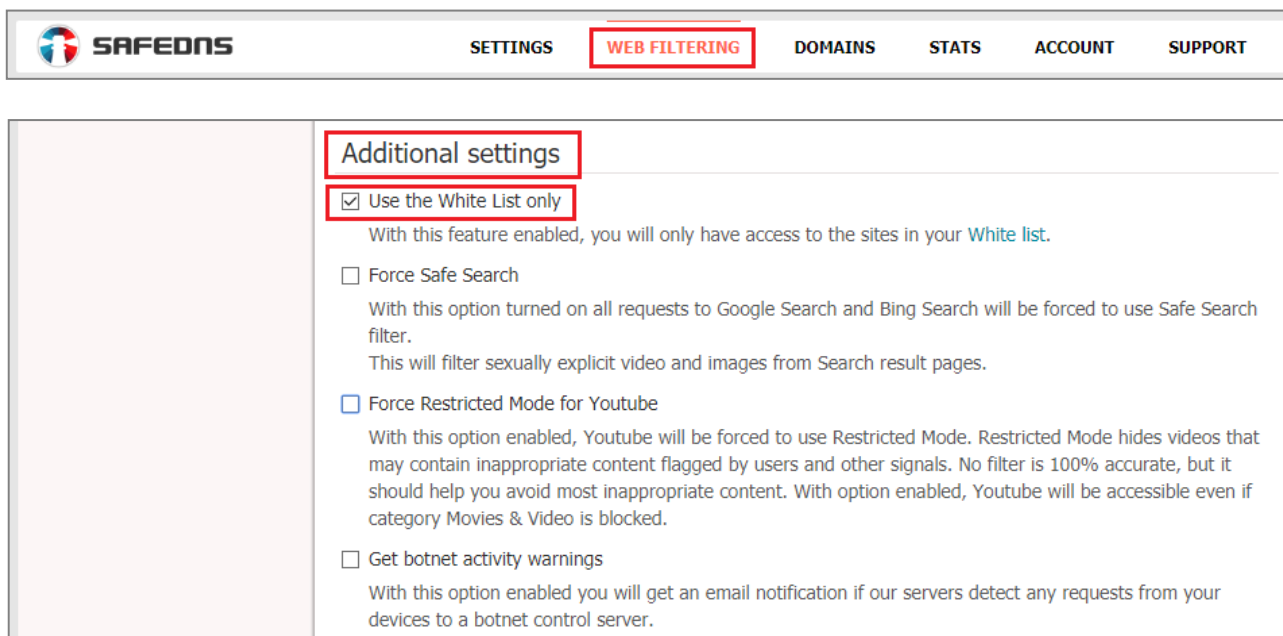
To unblock a certain site from a restricted category, go to **Dashboard -> Domains tab**, find the **White list** section and enter the website address you want to allow.



The screenshot shows the SafeDNS web interface. The top navigation bar includes 'SETTINGS', 'WEB FILTERING', 'DOMAINS' (highlighted with a red box), 'STATS', 'ACCOUNT', and 'SUPPORT'. On the left sidebar, there is a 'Need Help?' section with links to 'Getting Started Guide' and 'FAQ - Basic Questions', and an 'Any Ideas?' section with a link to submit an idea. The main content area is titled 'Profile Default' and features a 'White list' section (highlighted with a red box). This section is labeled 'Never Block' and states 'You can add 500 records'. It contains a text input field with 'chat.com' (highlighted with a green box) and an 'Add' button (highlighted with a red box). To the right of the input field is an 'Edit as list' button. Below the 'White list' section is a 'Black list' section, labeled 'Always Block' and also stating 'You can add 500 records'. It features a text input field with the placeholder 'Enter a hostname' and an 'Add' button, with an 'Edit as list' button to the right.

4.4. How to allow access only to websites in your whitelist (Whitelist-only mode)

To allow access only to whitelisted sites go to **Dashboard -> Web filtering**. Scroll down to the **Additional settings section**, tick the **Use the White List only** checkbox and **Save** the settings.



SAFEDNS

SETTINGS WEB FILTERING DOMAINS STATS ACCOUNT SUPPORT

Additional settings

☒ Use the White List only

With this feature enabled, you will only have access to the sites in your [White list](#).

☐ Force Safe Search

With this option turned on all requests to Google Search and Bing Search will be forced to use Safe Search filter.

This will filter sexually explicit video and images from Search result pages.

☐ Force Restricted Mode for Youtube

With this option enabled, Youtube will be forced to use Restricted Mode. Restricted Mode hides videos that may contain inappropriate content flagged by users and other signals. No filter is 100% accurate, but it should help you avoid most inappropriate content. With option enabled, Youtube will be accessible even if category Movies & Video is blocked.

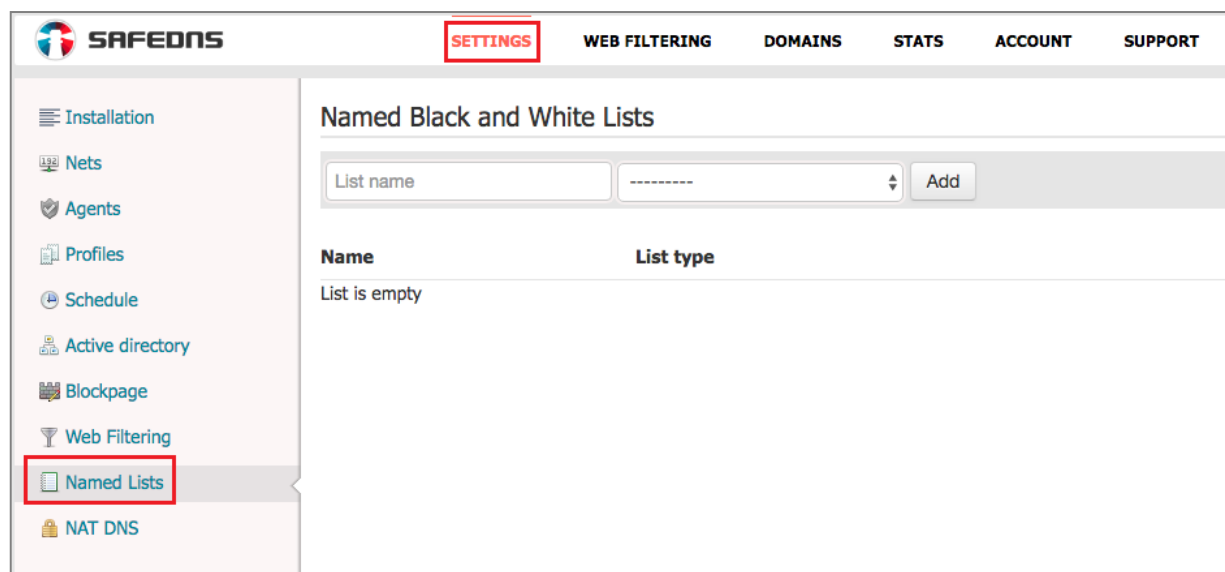
☐ Get botnet activity warnings

With this option enabled you will get an email notification if our servers detect any requests from your devices to a botnet control server.

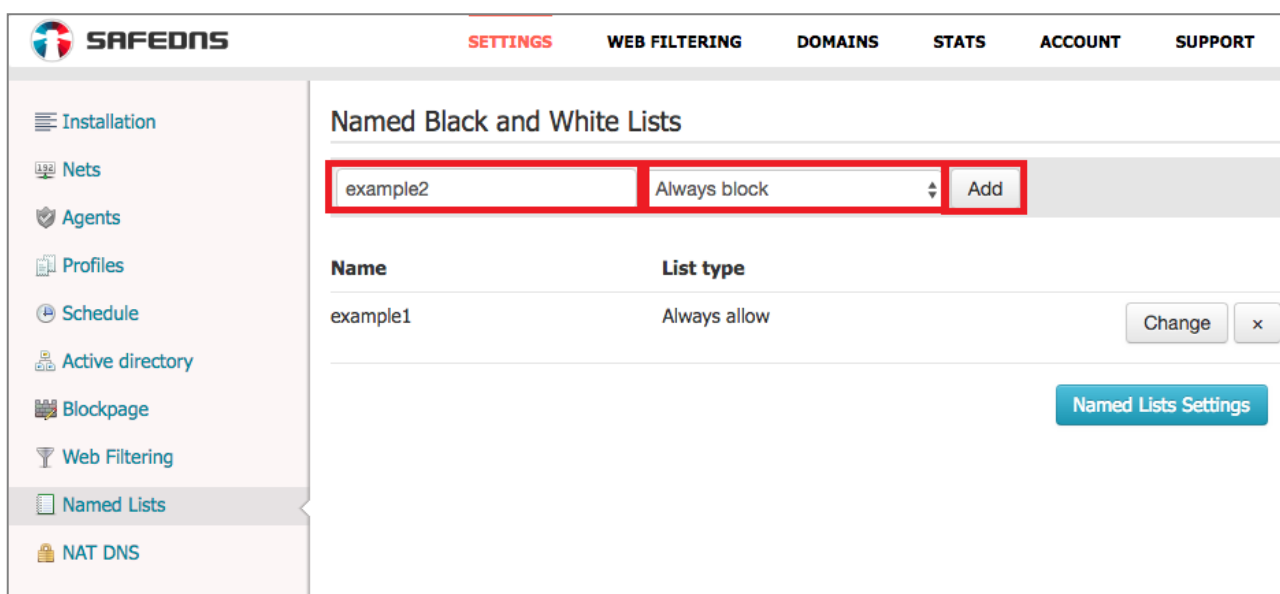
4.5. Named Black / white lists

Named Lists is a convenient feature for the Education, Hotspot, Office and Enterprise billing plans. It is designed to be installed on different filtering policies (profiles) at the same time. Now you can edit one named list and then apply it to any of your filtering policies. Named lists will also increase the limit for black and white lists according to your billing plan. You also can manage lists of allowed or blocked hosts and domains for all of your profiles or groups of profiles via this convenient feature.

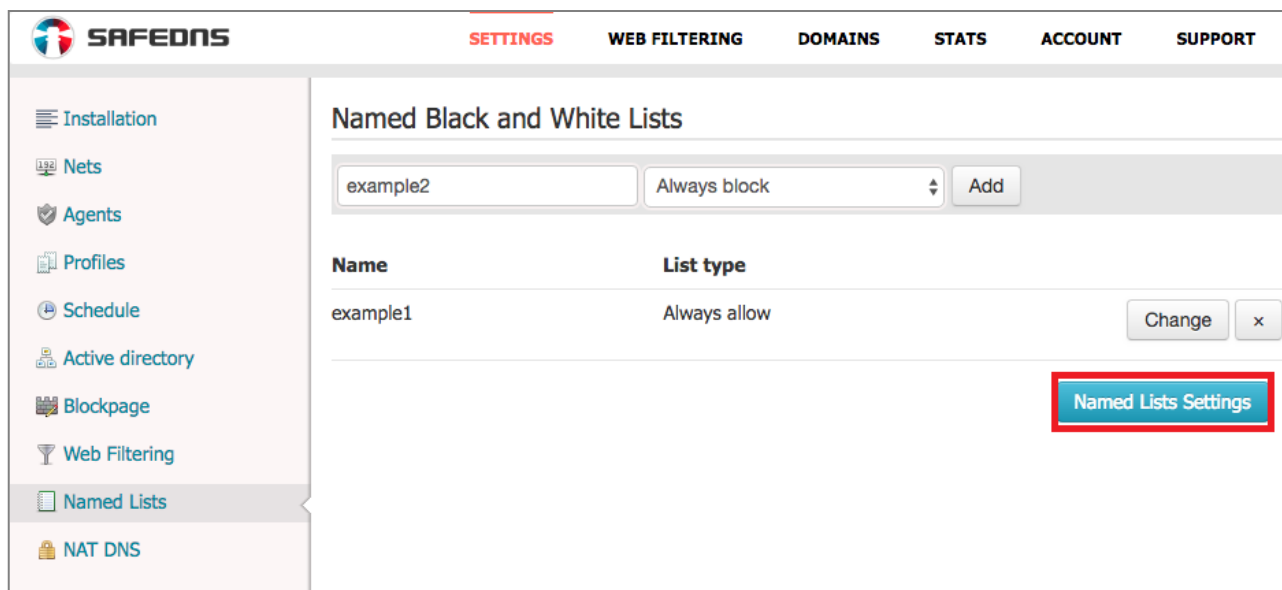
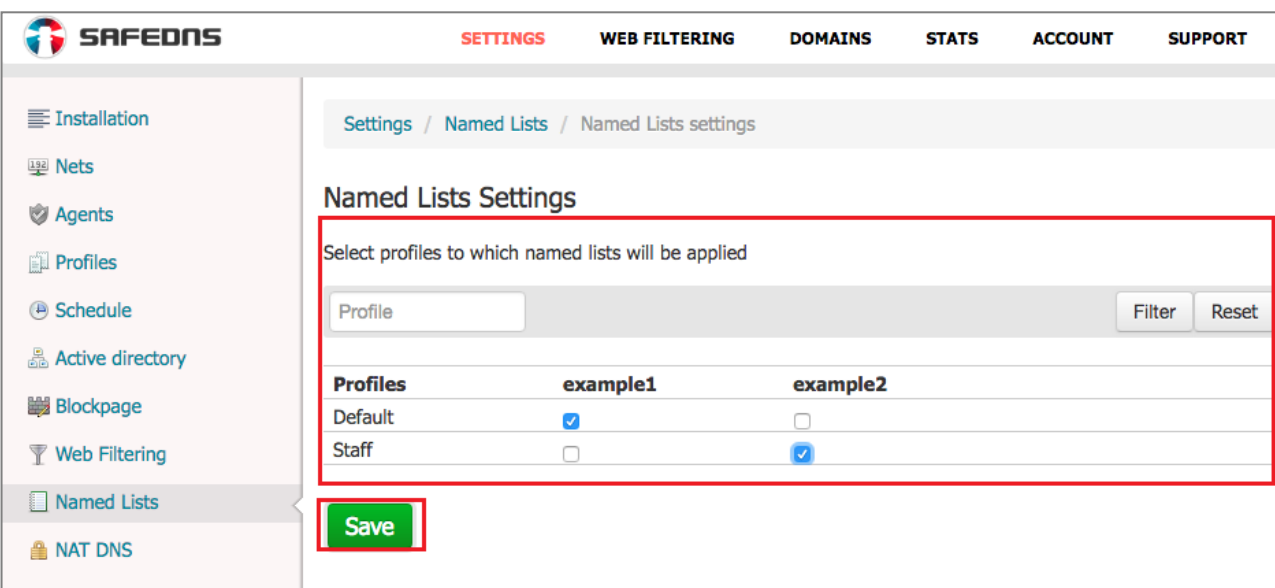
Click the **Settings tab** and choose **Named Lists** in the menu:



Then enter the most convenient name for the list and choose an appropriate action: **Always allow** (for the White list) or **Always block** (for the Black list).



Use the **Named Lists Settings** button to select profiles to which the named lists will be applied:

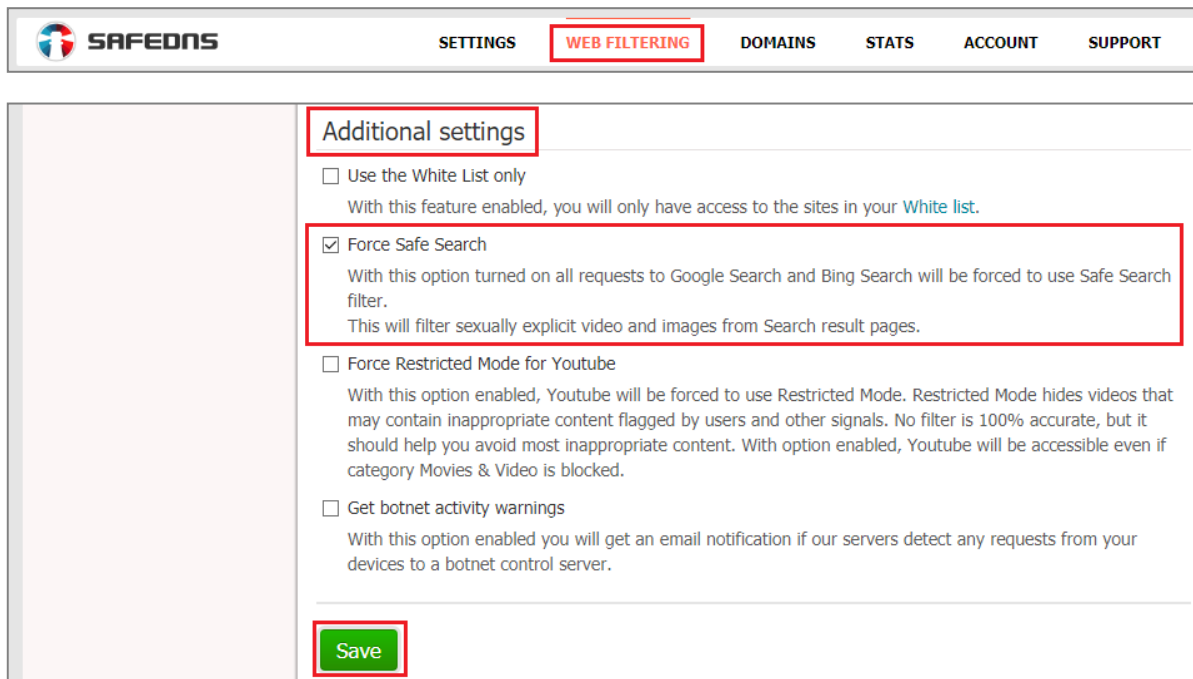
Save the settings and go to the **Domains** tab. Choose a filtering profile for which the Named list is active, put hosts and domains in the appropriate field. Alternatively, you can press **Edit as list** button to edit a list of records for the selected named list.

[Back to the Contents](#)

5. Additional features

5.1. Forcing Safe Search

To enable **Safe Search** go to **Dashboard -> Web Filtering tab** (top menu). Scroll down to the **Additional settings section** tick the **Force Safe Search** checkbox and click **Save**.



SAFEDNS SETTINGS **WEB FILTERING** DOMAINS STATS ACCOUNT SUPPORT

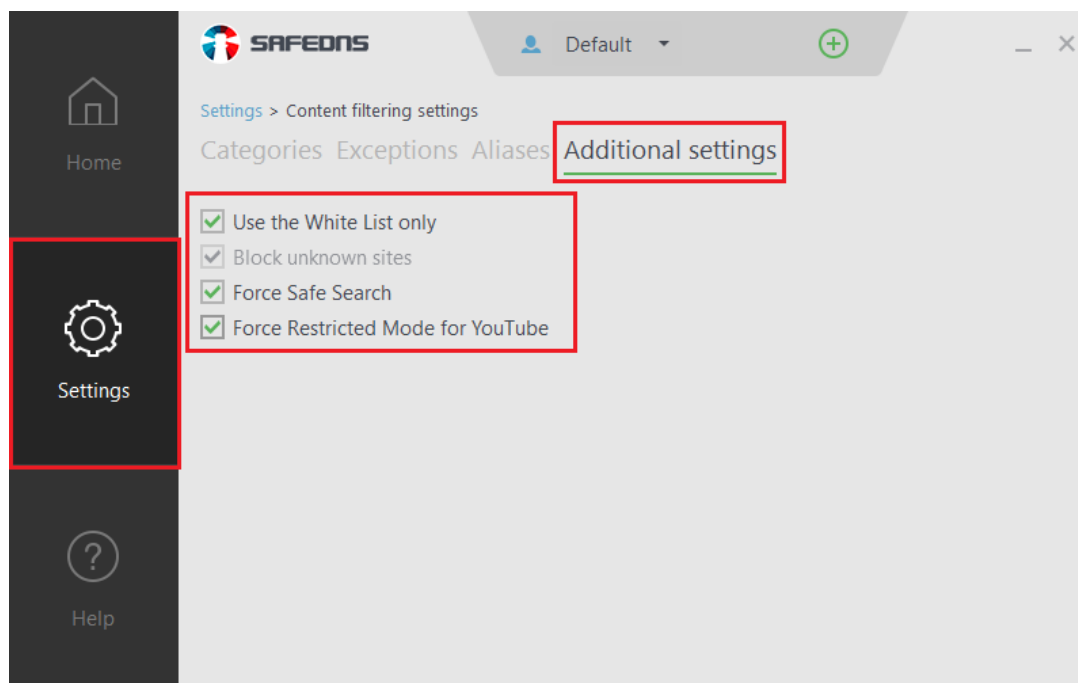
Additional settings

- ☐ Use the White List only
With this feature enabled, you will only have access to the sites in your [White list](#).
- ☒ Force Safe Search
With this option turned on all requests to Google Search and Bing Search will be forced to use Safe Search filter.
This will filter sexually explicit video and images from Search result pages.
- ☐ Force Restricted Mode for Youtube
With this option enabled, Youtube will be forced to use Restricted Mode. Restricted Mode hides videos that may contain inappropriate content flagged by users and other signals. No filter is 100% accurate, but it should help you avoid most inappropriate content. With option enabled, Youtube will be accessible even if category Movies & Video is blocked.
- ☐ Get botnet activity warnings
With this option enabled you will get an email notification if our servers detect any requests from your devices to a botnet control server.

Save

5.2. How to enable Safe Search Agent

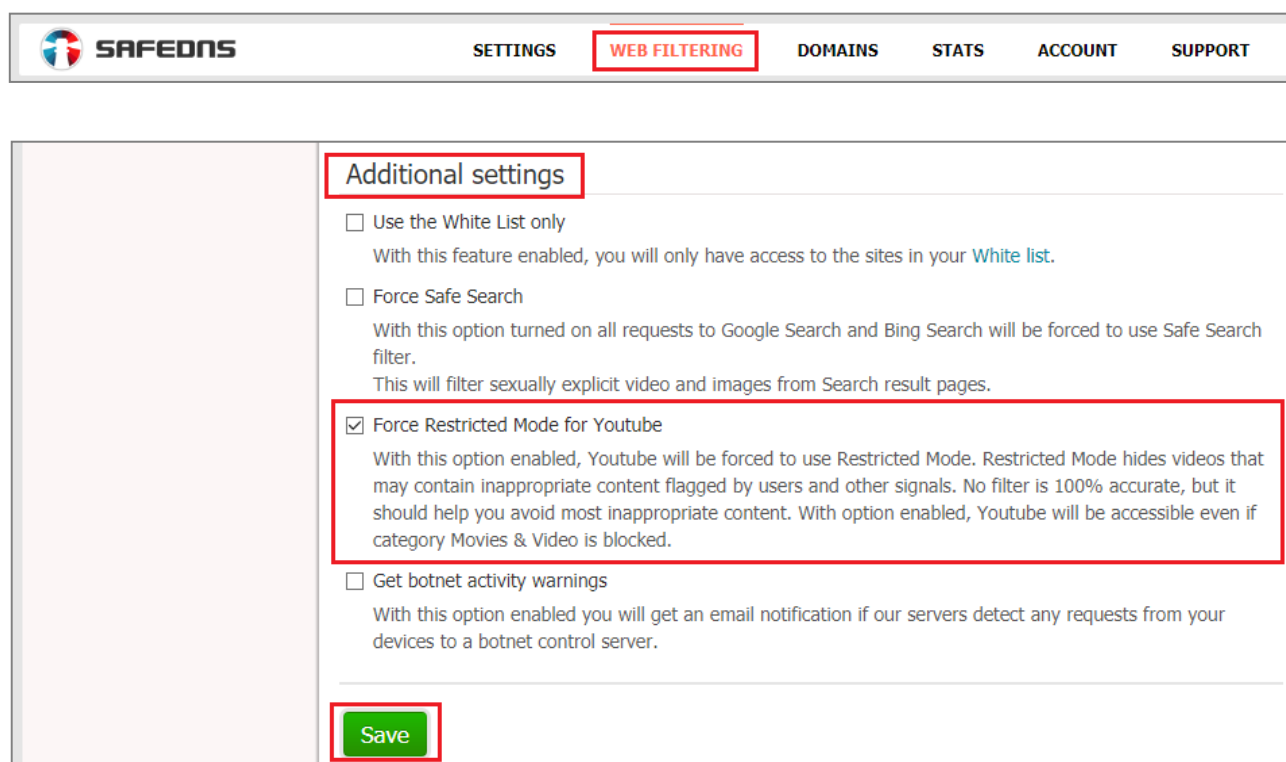
You can manage such settings as **Force Safe Search**, **Force Restricted Mode for YouTube** and others in the **Additional settings** tab.



5.3. How to forcibly turn on Restricted mode on YouTube

With **Force Restricted mode** option enabled, YouTube will be forced to use Restricted Mode. This mode hides videos that may contain inappropriate content flagged by users. No filter is 100% accurate, but it should help you avoid the most inappropriate content. With the option enabled, YouTube will be accessible even if the **Movies & Video** category is blocked.

To force YouTube Restricted mode, go to **Dashboard -> Web Filtering tab** (top menu) and in the **Additional settings** section tick the **Force Restricted Mode for Youtube** checkbox and click **Save**.



SAFEDNS SETTINGS **WEB FILTERING** DOMAINS STATS ACCOUNT SUPPORT

Additional settings

- ☐ Use the White List only
With this feature enabled, you will only have access to the sites in your [White list](#).
- ☐ Force Safe Search
With this option turned on all requests to Google Search and Bing Search will be forced to use Safe Search filter.
This will filter sexually explicit video and images from Search result pages.
- ☒ Force Restricted Mode for Youtube
With this option enabled, Youtube will be forced to use Restricted Mode. Restricted Mode hides videos that may contain inappropriate content flagged by users and other signals. No filter is 100% accurate, but it should help you avoid most inappropriate content. With option enabled, Youtube will be accessible even if category Movies & Video is blocked.
- ☐ Get botnet activity warnings
With this option enabled you will get an email notification if our servers detect any requests from your devices to a botnet control server.

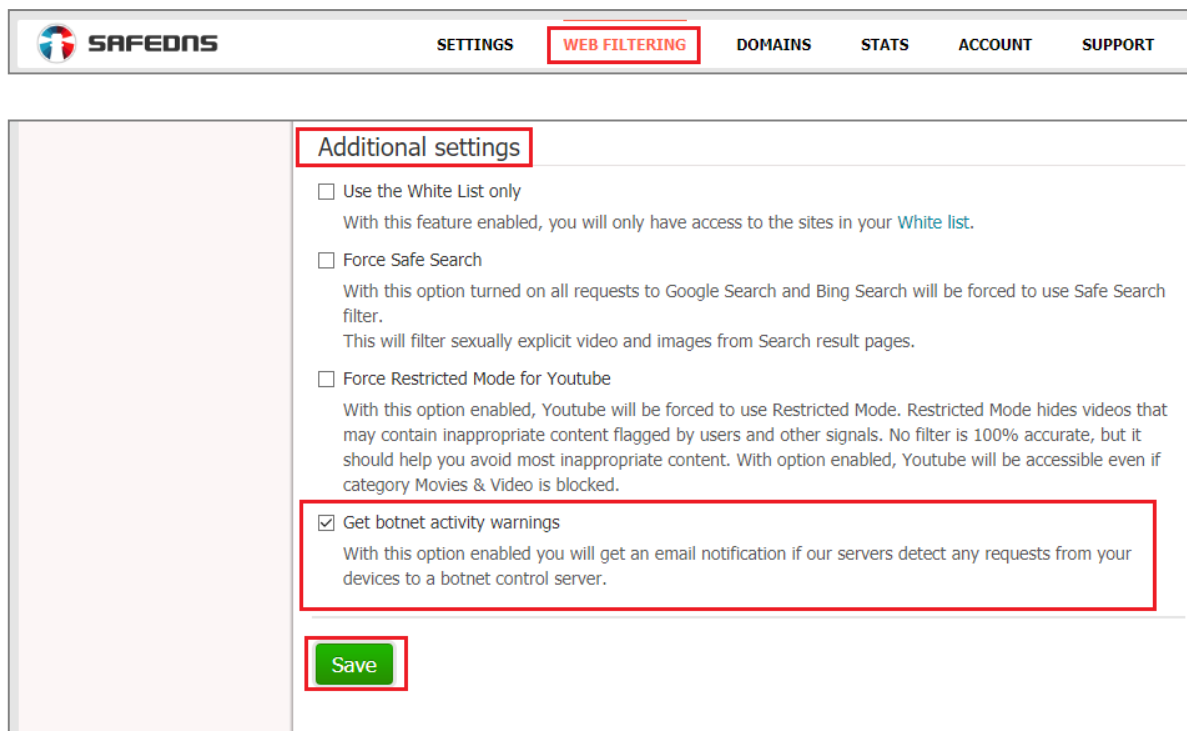
Save

[Back to the Contents](#)

6. Botnets, Phishing and Virus propagation

6.1. How to turn on notifications in botnet activity in my network

To receive notifications of botnet activity, go to **Dashboard -> Web Filtering** (top menu) -> **Additional settings**, tick the **Get botnets activity** checkbox and click **Save**. When this is done, you will get email notifications of any botnet activity from the protected networks and devices.



SAFEDNS

SETTINGS **WEB FILTERING** DOMAINS STATS ACCOUNT SUPPORT

Additional settings

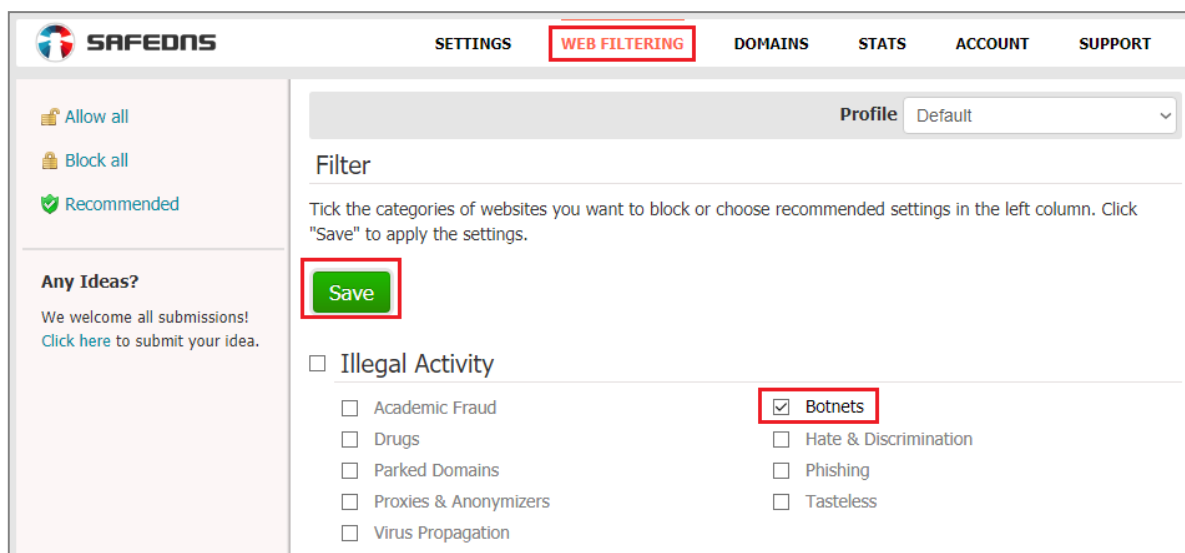
- ☐ Use the White List only
With this feature enabled, you will only have access to the sites in your [White list](#).
- ☐ Force Safe Search
With this option turned on all requests to Google Search and Bing Search will be forced to use Safe Search filter.
This will filter sexually explicit video and images from Search result pages.
- ☐ Force Restricted Mode for Youtube
With this option enabled, Youtube will be forced to use Restricted Mode. Restricted Mode hides videos that may contain inappropriate content flagged by users and other signals. No filter is 100% accurate, but it should help you avoid most inappropriate content. With option enabled, Youtube will be accessible even if category Movies & Video is blocked.
- ☒ Get botnet activity warnings
With this option enabled you will get an email notification if our servers detect any requests from your devices to a botnet control server.

Save

6.2. Blocking access to botnet control nodes

Botnet is a computer network consisting of a number of hosts from running bots – standalone software.


To block access to the control nodes of botnets go to **Dashboard -> Web Filtering tab** and block the **Botnets** category. Then click **Save**.




6.3. Blocking access to phishing sites


Phishing is a form of an internet fraud used for getting access to confidential data – logins and passwords.


In order to block access to phishing sites go to **Dashboard -> Web Filtering tab** and block the **Phishing** category. Then click **Save**.

 SAFEDNS

SETTINGSWEB FILTERINGDOMAINSSTATSACCOUNTSUPPORT

 Allow all

 Block all

 Recommended

Any Ideas?
We welcome all submissions!
[Click here](#) to submit your idea.

ProfileDefault

Filter

Tick the categories of websites you want to block or choose recommended settings in the left column. Click "Save" to apply the settings.

Save

☐ Illegal Activity

☐ Academic Fraud

☐ Drugs

☐ Parked Domains

☐ Proxies & Anonymizers

☐ Virus Propagation

☐ Botnets

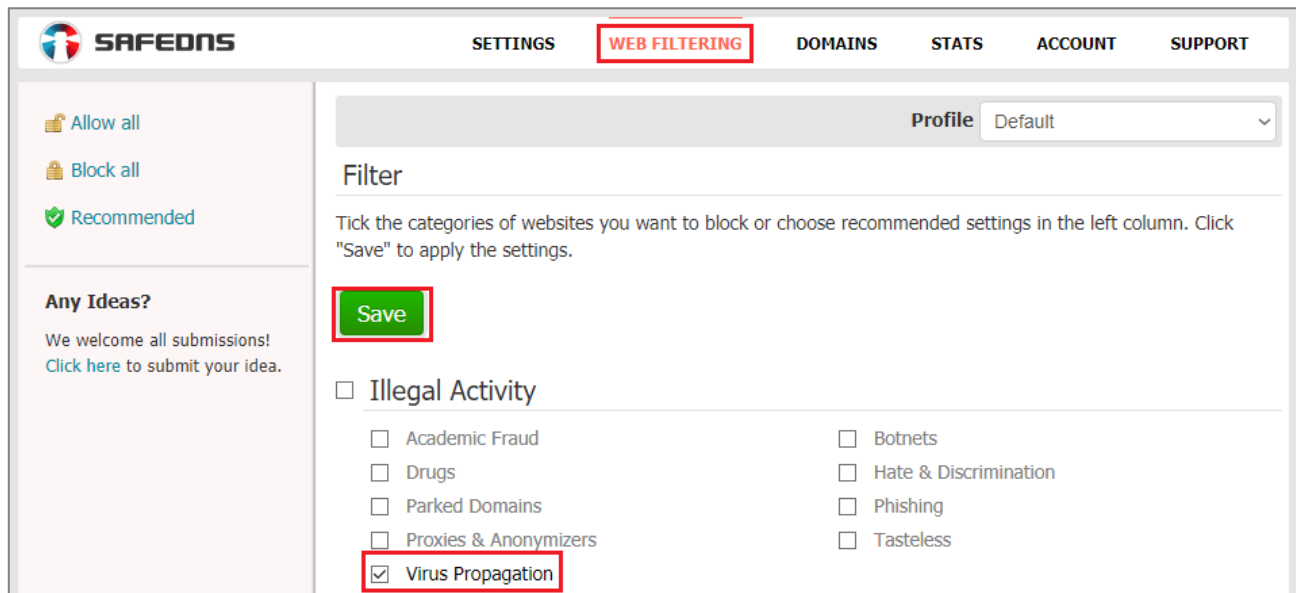
☐ Hate & Discrimination

☒ Phishing

☐ Tasteless

6.4. Blocking access to virus propagation sites

To block access to infected sites, go to **Dashboard -> Web Filtering tab** and block the **Virus propagation** category. Then click **Save**.



SAFEDNS

SETTINGS **WEB FILTERING** DOMAINS STATS ACCOUNT SUPPORT

Allow all
Block all
Recommended

Any Ideas?
We welcome all submissions!
[Click here](#) to submit your idea.

Profile: Default

Filter

Tick the categories of websites you want to block or choose recommended settings in the left column. Click "Save" to apply the settings.

Save

☐ **Illegal Activity**

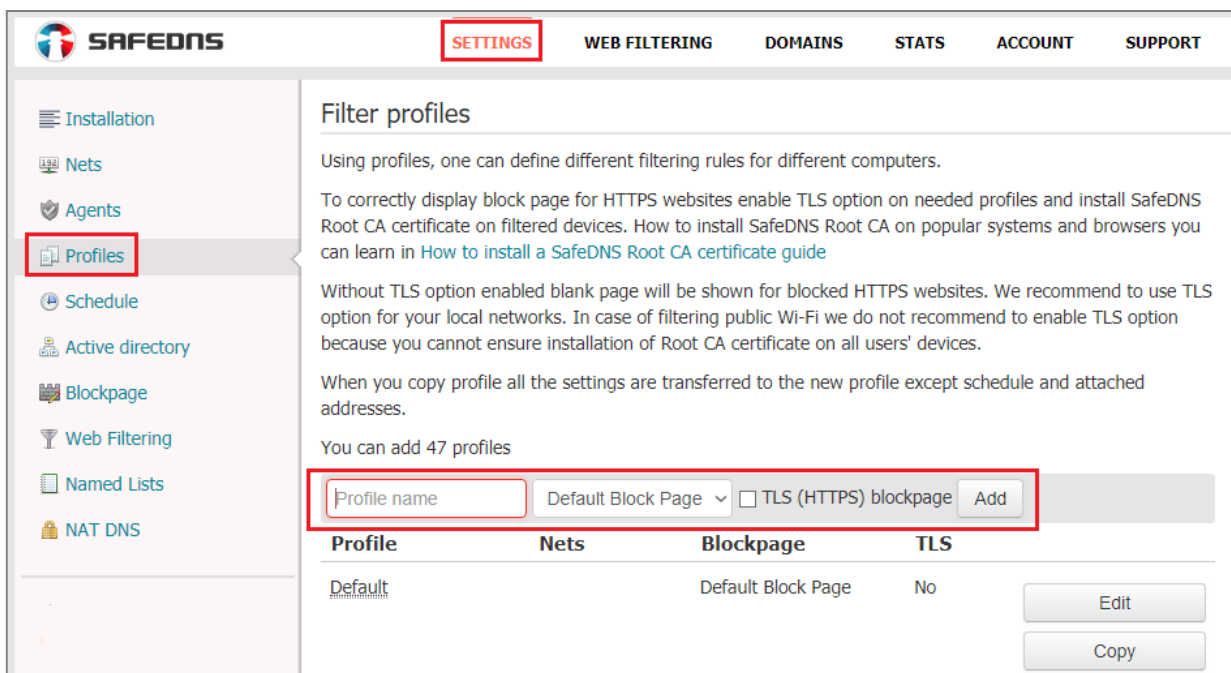
| | |
|--|--|
| <input type="checkbox"/> Academic Fraud | <input type="checkbox"/> Botnets |
| <input type="checkbox"/> Drugs | <input type="checkbox"/> Hate & Discrimination |
| <input type="checkbox"/> Parked Domains | <input type="checkbox"/> Phishing |
| <input type="checkbox"/> Proxies & Anonymizers | <input type="checkbox"/> Tasteless |
| <input checked="" type="checkbox"/> Virus Propagation | |

[Back to the Contents](#)

7. Profiles

7.1. How to add a filtering profile

A filtering profile is a set of filtering options with an assigned name. It is necessary if you have different filtering policies for different network users (or groups of users). Also, profiles are used when you are setting a filtering schedule. The *Default profile* cannot be deleted or renamed and you cannot set any filtering schedule for it. Additional profiles can be created in the **Settings -> Profiles tab** in **Dashboard**.



The screenshot shows the SafeDNS dashboard with the 'SETTINGS' tab selected. The left sidebar contains various settings categories, with 'Profiles' highlighted. The main content area is titled 'Filter profiles' and contains instructions on how to use profiles, including enabling TLS for HTTPS websites and a warning about blank pages without TLS. Below the instructions, it states 'You can add 47 profiles'. A form for adding a new profile is visible, with fields for 'Profile name', 'Default Block Page' (a dropdown menu), and a checkbox for 'TLS (HTTPS) blockpage'. An 'Add' button is next to the form. Below the form is a table showing the existing 'Default' profile.

| Profile | Nets | Blockpage | TLS | |
|----------------|------|--------------------|-----|---------------------------------|
| <u>Default</u> | | Default Block Page | No | <div>Edit</div> <div>Copy</div> |

7.2. How to change the name of the profile settings

Change the name of the profile settings in **Settings -> Profiles**. Next to any existing profile click **Edit**. After editing click **Save**.

You can add 47 profiles

Profile name Default Block Page ☐ TLS (HTTPS) blockpage

| Profile | Nets | Blockpage | TLS | |
|------------------|---------------|--------------------|-----|---|
| <u>Default</u> | | Default Block Page | No | <input type="button" value="Edit"/> <input type="button" value="Copy"/> |
| <u>Marketing</u> | | Default Block Page | No | <input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> |
| <u>Sales</u> | 10.91.159.213 | Default Block Page | No | <input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> |

7.3. How to copy profile settings

Profile copying will be important in situations when there's an extensive white- or blacklist created for a particular profile. To save you time, you can copy the profile instead of manually adding the necessary sites to white- or blacklists of a new profile. Remember, only the existing profile's filtering settings are copied (**Web filtering** and **Domains sections**). To copy the settings of the profile, go to **Profiles** and click **Copy**.

You can add 47 profiles

Profile name Default Block Page ☐ TLS (HTTPS) blockpage

| Profile | Nets | Blockpage | TLS | |
|------------------|---------------|--------------------|-----|---|
| <u>Default</u> | | Default Block Page | No | <input type="button" value="Edit"/> <input type="button" value="Copy"/> |
| <u>Marketing</u> | | Default Block Page | No | <input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> |
| <u>Sales</u> | 10.91.159.213 | Default Block Page | No | <input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> |

7.4. How to change profile settings for the selected static or dynamic IP address

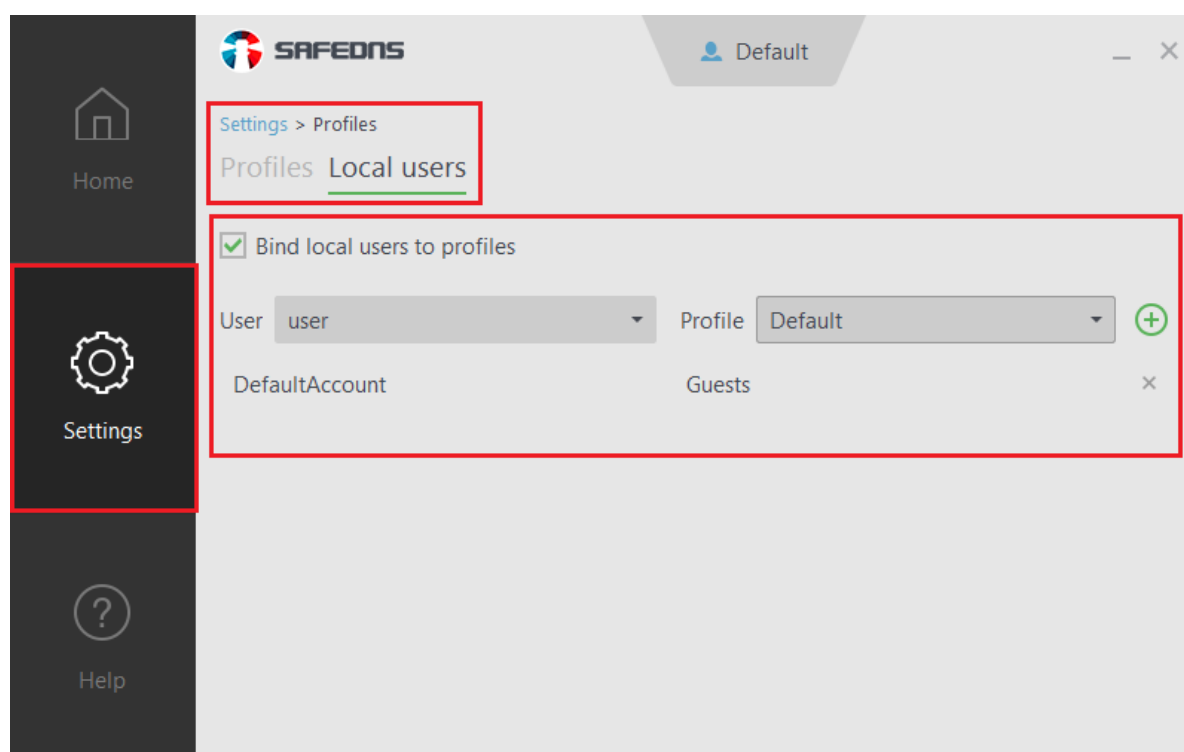
Go to **Settings -> Nets** (section on the left) and find the static IP address or a hostname in the appropriate section. To the right of the IP address or name of the dynamic DNS host, you can click **Change** and select the desired profile. After that click **Save**.

7.5. How to make different filters for different users of the same computer

To create different filters for different local users you need two or more filtering profiles (for example, 'Children' and 'Parents').

Application of such settings is possible only with the use of SafeDNS Agent. To set it up you need to have two or more local user accounts created on the computer.

In **SafeDNS Agent** go to **Settings -> Profiles -> Local users**, select the user and the corresponding filtering profile and tick the box '**Bind local users to profiles**'.



The corresponding profile is used when the user logs into the system.

[Back to the Contents](#)

8. Schedule

8.1. How to set up schedule for filtering

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

Profile settings will come into effect during active hours and during the rest of the time *Default profile* settings will be applied.

This system allows for a flexible schedule, so you can apply more advanced scenarios like:

1. 'Turning off the internet' schedule, with the filtered internet for the rest of the time. This option is often used by parents to limit kids' access to the internet during school hours.
2. 'Filtering of unproductive websites in the workplace', with unlimited access during lunch break, before and after the working hours. Obviously, this scheduling is suitable for use within organizations.
3. A more rigorous filtering in the hours when the computer is used by a child and less strict filtering (or lack of it) in the hours when the computer is used by adults.

Now we will look at how to set up and enable a schedule, and then look at common scenarios of the filtering schedule usage at home and in the organization.

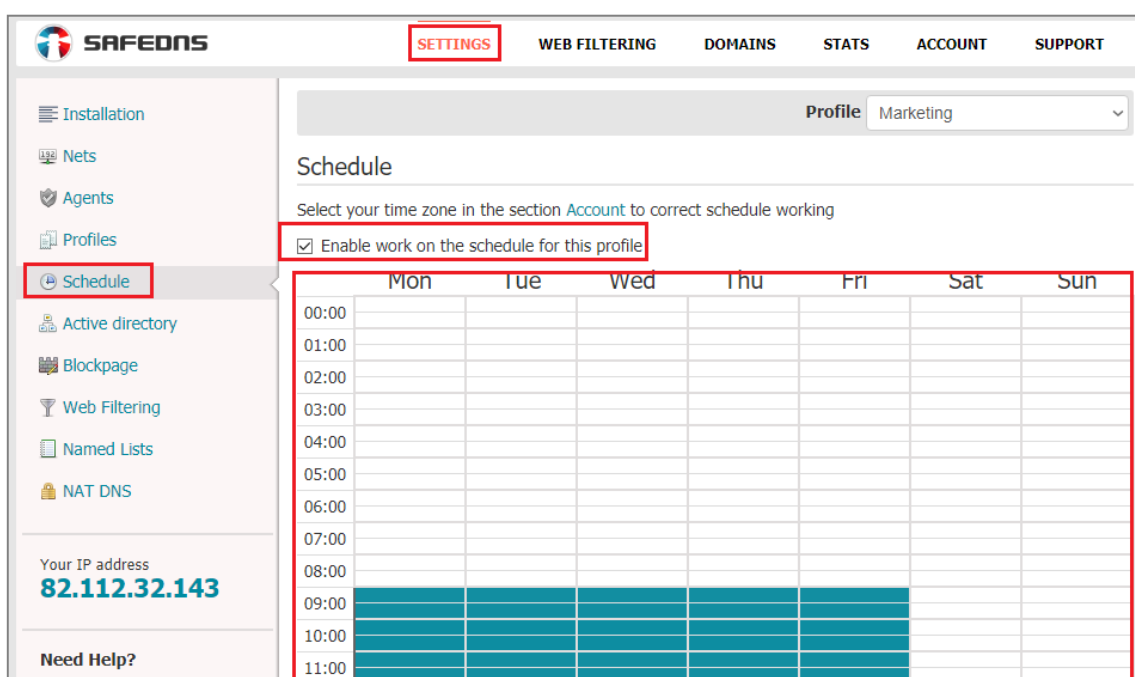
To set up a schedule, you are supposed to have at least one additional profile on which you will enable the schedule.

1. Log in to **Dashboard**.
2. Go to **Settings -> Profiles**.
3. Enter the name of the profile (e.g. *Schedule profile*) and click **Add**.

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

1. Go to Settings -> Schedule

2. In the list of your profiles (upper right corner), select the recently created profile *Schedule profile*. Note that the *Default profile* does not appear in the list because no separate schedule can be enabled on it.
3. Set the time during which *Schedule profile* should be active. The rest of the time the *Default profile* will be active. The appearance and functionality of the schedule depends on your service plan.
4. Tick the checkbox **Enable work on the schedule** for this profile.
5. Click **Save**.



SAFEDNS

SETTINGS WEB FILTERING DOMAINS STATS ACCOUNT SUPPORT

Profile Marketing

Schedule

Select your time zone in the section [Account](#) to correct schedule working

☒ Enable work on the schedule for this profile

| | Mon | Tue | Wed | Thu | Fri | Sat | Sun |
|-------|-----|-----|-----|-----|-----|-----|-----|
| 00:00 | | | | | | | |
| 01:00 | | | | | | | |
| 02:00 | | | | | | | |
| 03:00 | | | | | | | |
| 04:00 | | | | | | | |
| 05:00 | | | | | | | |
| 06:00 | | | | | | | |
| 07:00 | | | | | | | |
| 08:00 | | | | | | | |
| 09:00 | | | | | | | |
| 10:00 | | | | | | | |
| 11:00 | | | | | | | |

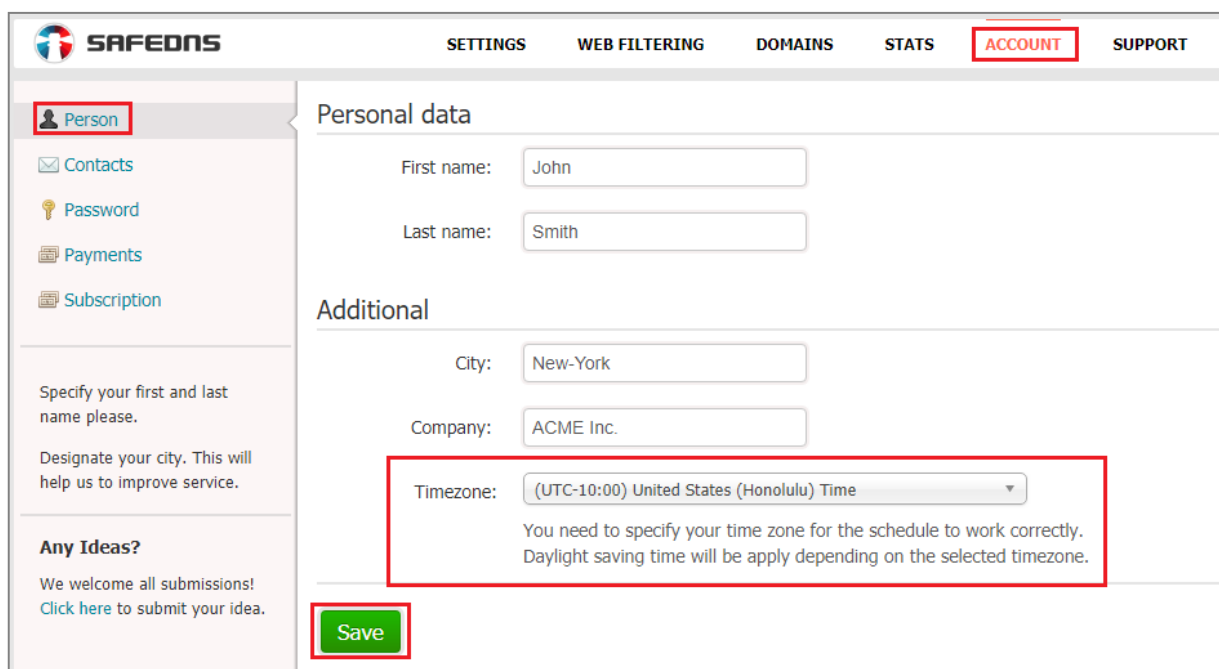
After setting up the schedule you need to apply it to your network or individual computers.

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

8.2. Possible issues with the schedule

Scheduled settings switch at the wrong time:

Make sure that you have the correct time zone applied. In **Dashboard** go to **Account** - > **Person**, select the correct time zone and click **Save**.



SAFEDNS SETTINGS WEB FILTERING DOMAINS STATS **ACCOUNT** SUPPORT

Person

Contacts
Password
Payments
Subscription

Specify your first and last name please.
Designate your city. This will help us to improve service.

Any Ideas?
We welcome all submissions!
[Click here](#) to submit your idea.

Personal data

First name:

Last name:

Additional

City:

Company:

Timezone:

You need to specify your time zone for the schedule to work correctly.
Daylight saving time will be apply depending on the selected timezone.

Save

The schedule works but blocking and unblocking occur with a delay:

Due to the caching of DNS queries at the system and browser level, your computer cannot immediately respond to blocking or unblocking issued by our service. To eliminate this, we recommend disabling automatic control of the browser cache.

The schedule isn't working at all:

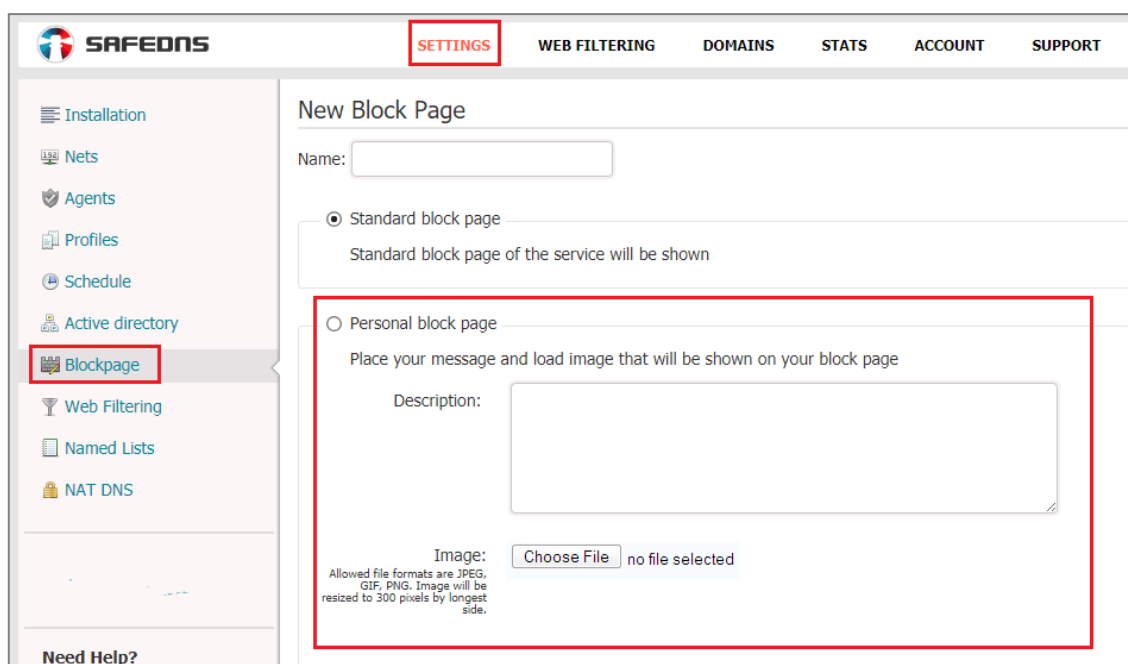
Make sure that you have followed all of the above-mentioned steps on configuring the schedule. If everything is done correctly and the issue persists, contact our technical support team.

[Back to the Contents](#)

9. Customizing appearance of the service

9.1. How to use custom text and picture on the block page

To place your custom text and picture on the block page, go to **Dashboard -> Settings** (top level menu) -> **Block page** (section on the left), then select **Personal block page**. Then you can write your text in the **Description** field. To upload your picture instead of the SafeDNS logo, you need to prepare a picture (Image formats: JPEG, GIF, PNG. The picture will automatically be reduced to 300 points as the maximum size) and upload it through the **Choose File** field. Then click **Save** to apply the changes.



SAFEDNS **SETTINGS** WEB FILTERING DOMAINS STATS ACCOUNT SUPPORT

Installation
Nets
Agents
Profiles
Schedule
Active directory
Blockpage
Web Filtering
Named Lists
NAT DNS

Need Help?

New Block Page

Name:

☒ Standard block page
Standard block page of the service will be shown

☐ Personal block page
Place your message and load image that will be shown on your block page

Description:

Image: no file selected
Allowed file formats are JPEG, GIF, PNG. Image will be resized to 300 pixels by longest side.

You can see a preview of your customized block page by clicking the **View** button next to the name of the page type. The preview of your block page will open in the new window.

9.2. How to change the design of the whole block page

With any of a host of Safe@Office billing plans you can completely change the appearance of your block page by inserting your HTML-code in the settings of the block page.

You can use the following variables in HTML block page:

\$website - requested website address

\$domain - name of categorized domain for \$website

\$reason - reason of blocking, is available for translate

\$category - list of categories for \$domain, is available for translate

Also, you can add a language prefix before the variable name to translate it to another language.

Also, you can add language prefix before variable name to translate it to another language.

e.g: **\$fr:reason**

List of available languages: **fr, en, pt_BR, de, tr, it, sv, ar, ur, es**

Example of HTML code of the block page:

```
<!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">
                        
                    </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 $reason</strong></p>
                    </div>
                    <div class="compain-form">
                        <p class="med">If the categories are listed incorrectly, press the 'Complain'
button below. We shall investigate the situation.</p>
                        <form method="post"
action="mailto:your@email.com?subject=$website">
                            <div align="center">
                                <input name="send" value="Complain" style="height:30px;"
type="submit">
                            </div>

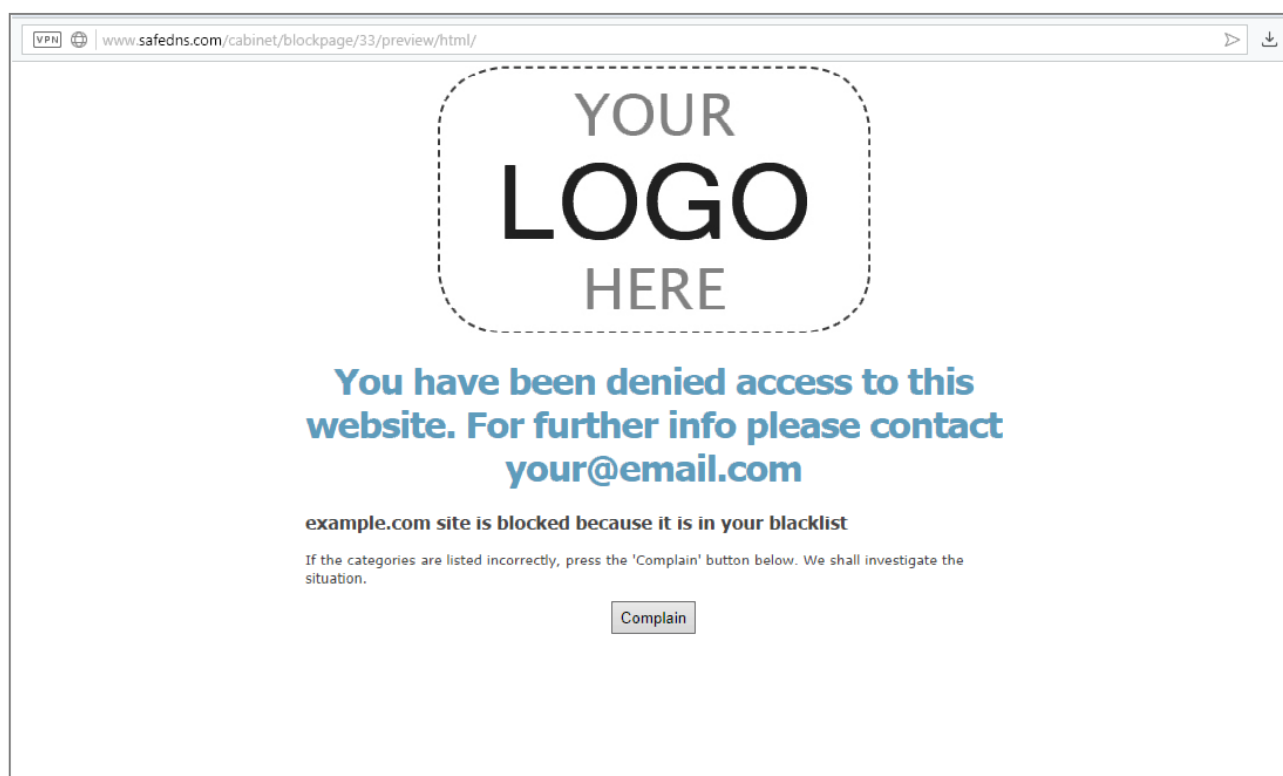
```

```

        </form>
    </div>
    </td>
</tr>
</tbody>
</table>
</body>
</html>

```

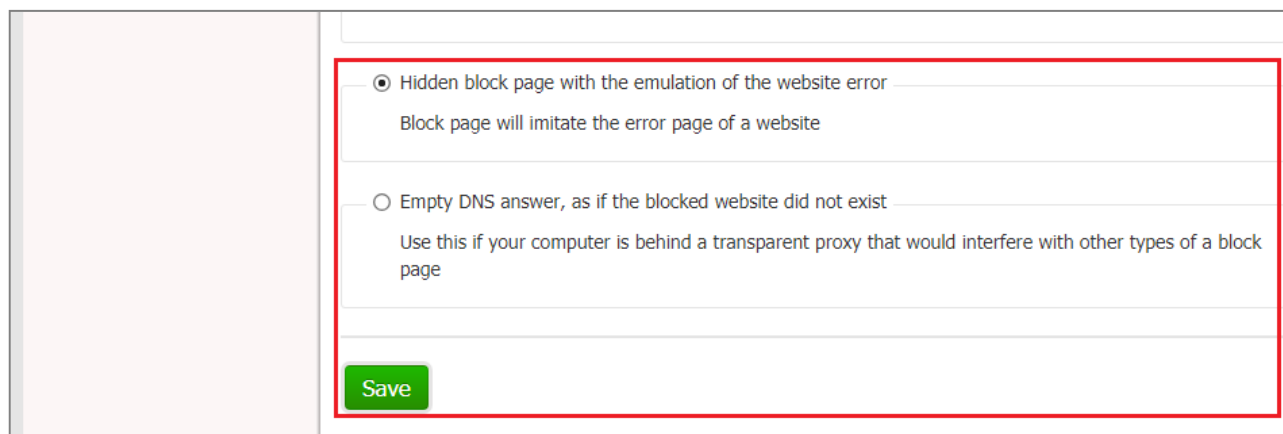
Cited above HTML example will be shown that way:



With the custom HTML block page, you can use links, pictures from the web, inline styles.

9.3. How to conceal that blocking is in effect

In **Dashboard** go to the **Block Page tab** (left menu), select **Hidden block page with the emulation of the website error** or **Empty DNS answer, as if blocked website did not exist**. Click **Save**.



The screenshot shows a web interface with a left sidebar and a main content area. The main content area contains two radio button options for blocking a page. The first option is selected and is enclosed in a red rectangular box. Below the options is a green 'Save' button, also within the red box.

☒ Hidden block page with the emulation of the website error
Block page will imitate the error page of a website

☐ Empty DNS answer, as if the blocked website did not exist
Use this if your computer is behind a transparent proxy that would interfere with other types of a block page

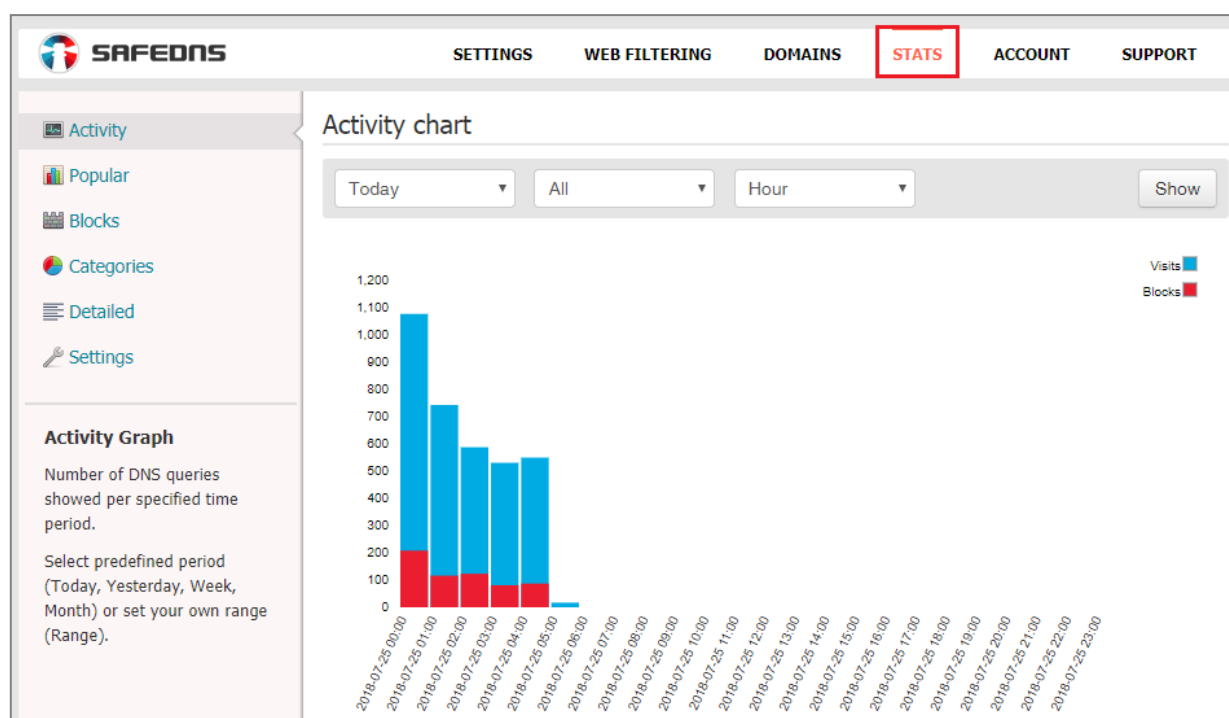
Save

[Back to the Contents](#)

10. Statistics

10.1. How do I view statistics in my account queries

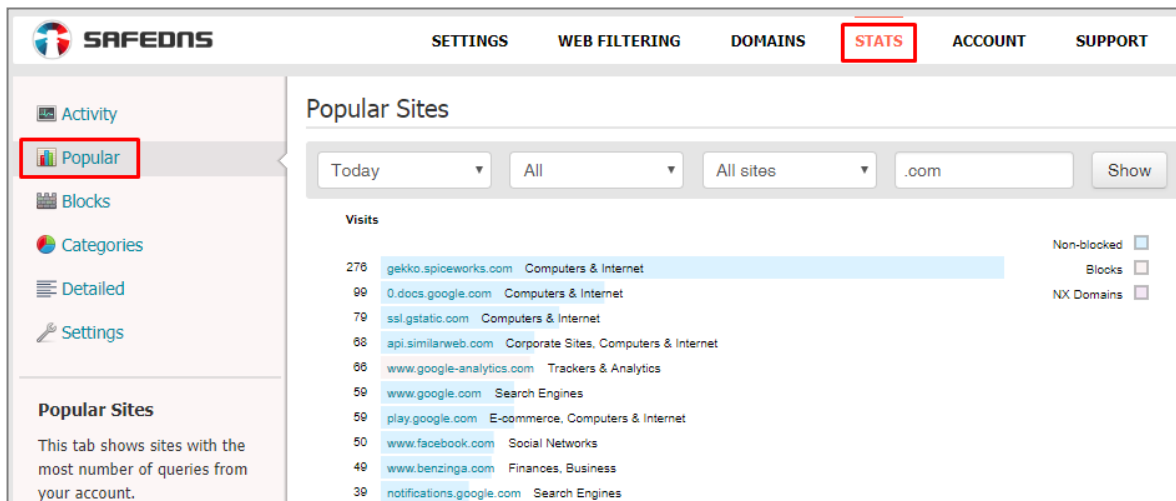
To view statistics of DNS requests from the SafeDNS protected networks and devices go to **Dashboard -> Stats**. The statistics can be sorted by predefined time frames – today, yesterday, week, month, or by a specific time frame. The statistics can be shown by hours or days. You can apply the filter just for one profile or for all profiles at once. The statistics are updated hourly.



10.2. How to see list of the most popular sites

To see the most popular sites (frequently visited sites) you have to go to **Stats** -> **Popular** and click **Show**.

Statistics of popular sites are available for today, yesterday, week, month, or for a specific time frame. Also, you can sort this list by domain. For example, you can check how popular the domain google.com is, typing it in the **Domain** box.



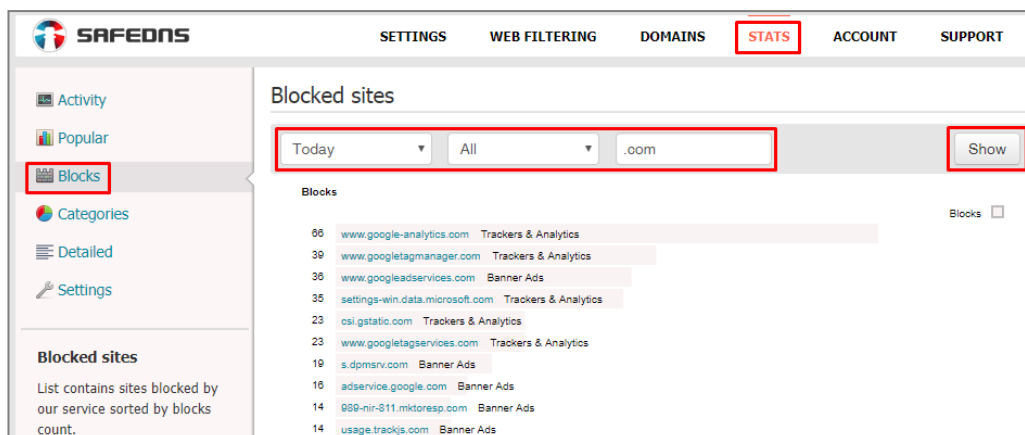
The screenshot shows the SAFEDNS web interface. The top navigation bar includes 'SETTINGS', 'WEB FILTERING', 'DOMAINS', 'STATS' (highlighted with a red box), 'ACCOUNT', and 'SUPPORT'. On the left sidebar, 'Popular' is highlighted with a red box. The main content area is titled 'Popular Sites' and features a filter bar with dropdowns for 'Today', 'All', 'All sites', and a text input for '.com', followed by a 'Show' button. Below the filter bar, a table lists popular sites with their visit counts and categories. On the right side of the table, there are checkboxes for 'Non-blocked', 'Blocks', and 'NX Domains'.

| Visits | Domain | Category |
|--------|--------------------------|---------------------------------------|
| 276 | gekko.spiceworks.com | Computers & Internet |
| 99 | 0.docs.google.com | Computers & Internet |
| 79 | ssl.gstatic.com | Computers & Internet |
| 68 | api.similarweb.com | Corporate Sites, Computers & Internet |
| 66 | www.google-analytics.com | Trackers & Analytics |
| 59 | www.google.com | Search Engines |
| 59 | play.google.com | E-commerce, Computers & Internet |
| 50 | www.facebook.com | Social Networks |
| 49 | www.benzinga.com | Finances, Business |
| 39 | notifications.google.com | Search Engines |

Non-blocked ☐
 Blocks ☐
 NX Domains ☐

10.3. How to view list of blocked sites

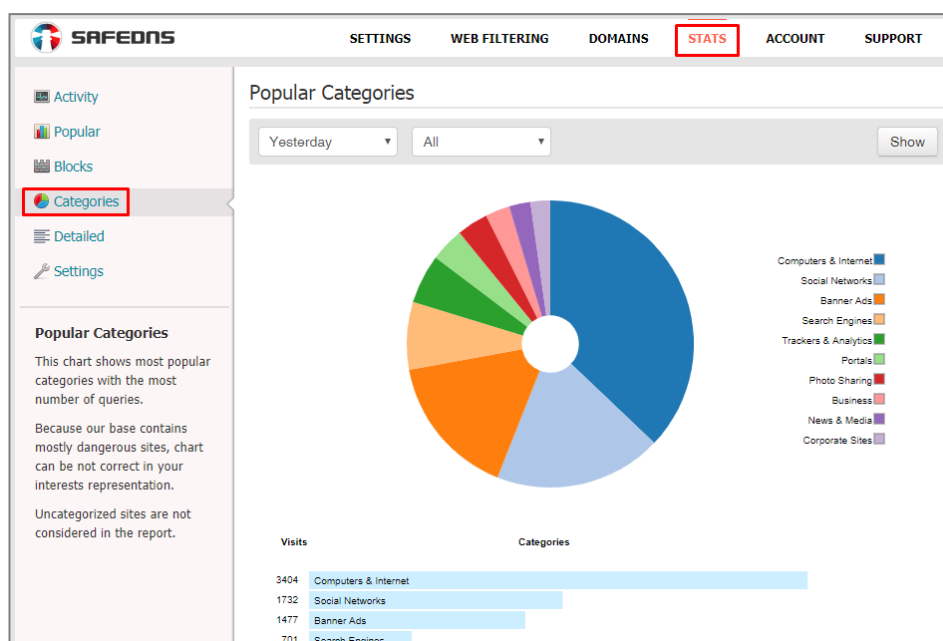
Go to **Dashboard -> Stats -> Blocks**, then chose a range, profile and click the **Show** button.



10.4. How to see a list of the most popular website categories

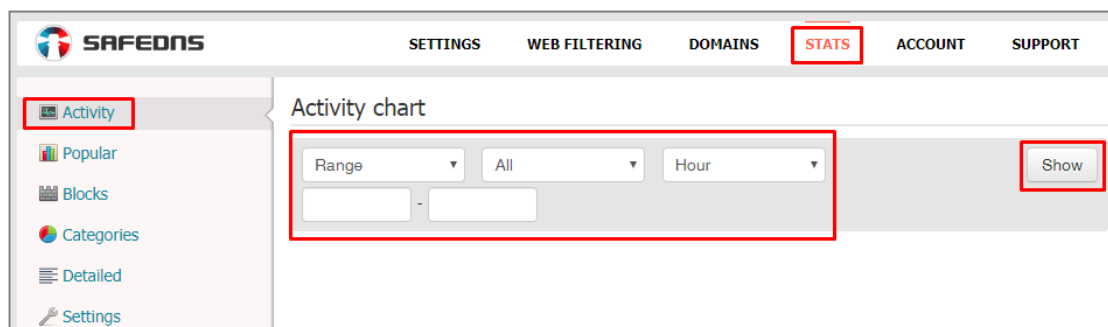
To see stats of the most popular categories go to **Dashboard -> Stats -> Categories**, then click **Show**.

Statistics of popular categories are available for today, yesterday, week, month, or for a specific time frame. You can see the statistics just for one profile or for all profiles at once.



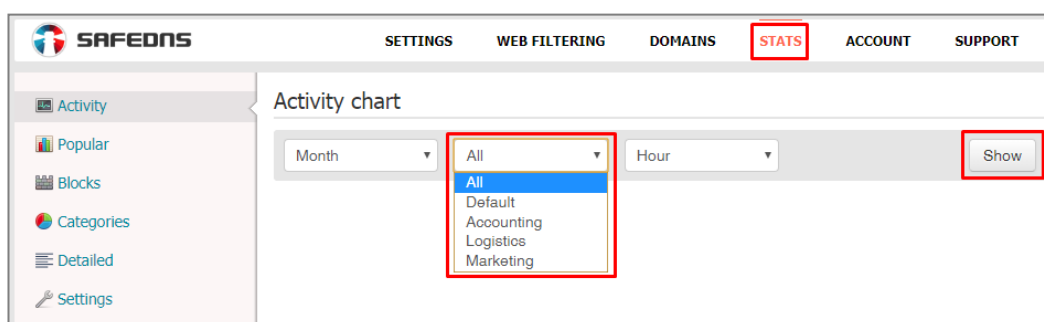
10.5. How to view statistics for a selected period

To get statistics for a selected range go to **Dashboard -> Stats**, then select one of the sections in the left menu (**Activity, Popular, Blocks, Categories, Detailed**), then select the range and click **Show**.



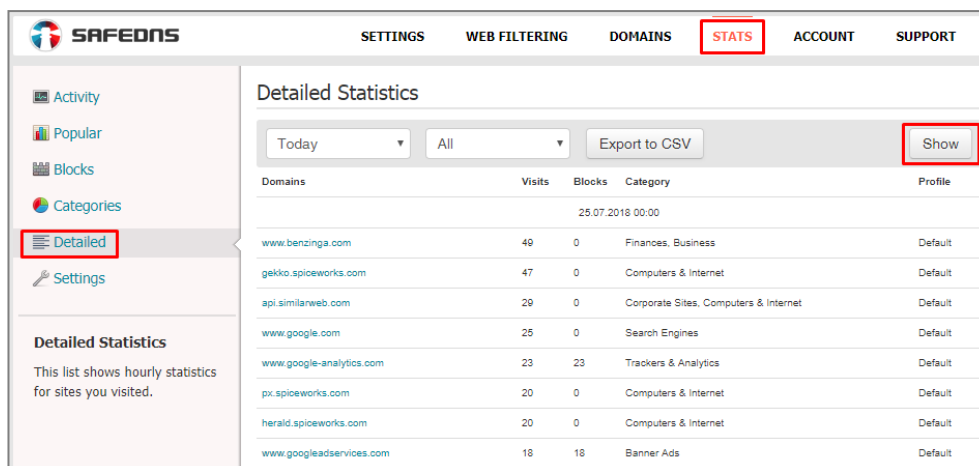
10.6. How to view statistics for a specific profile

To see statistics for a specific profile, go to **Dashboard -> Stats**, select one of the sections in the left menu (**Activity, Popular, Blocks, Categories, Detailed**), then select the entire profile and click **Show**.



10.7. How to view detailed statistics

To see detailed statistics of DNS requests, go to **Dashboard -> Stats -> Detailed**, then select a range and click **Show**.



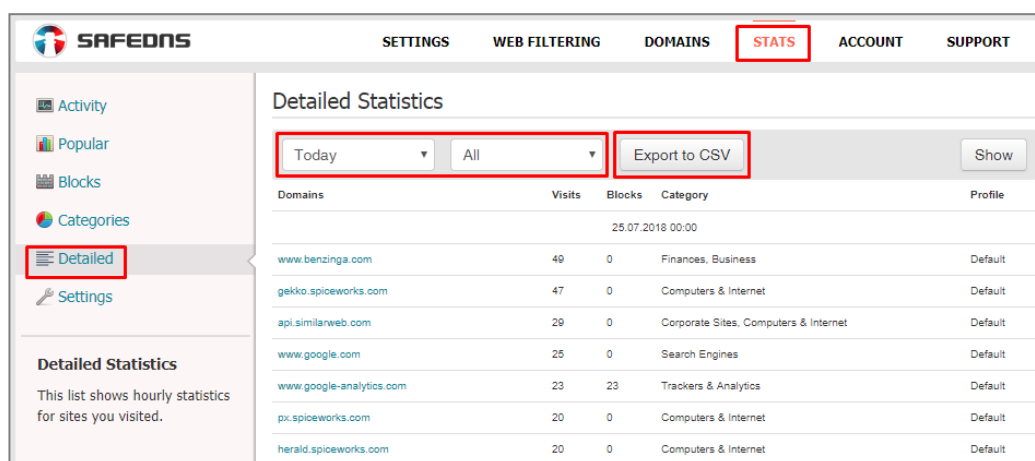
Detailed Statistics

Today All Export to CSV Show

| Domains | Visits | Blocks | Category | Profile |
|--------------------------|--------|--------|---------------------------------------|---------|
| 25.07.2018 00:00 | | | | |
| www.benzinga.com | 49 | 0 | Finances, Business | Default |
| gekko.spiceworks.com | 47 | 0 | Computers & Internet | Default |
| api.similarweb.com | 29 | 0 | Corporate Sites, Computers & Internet | Default |
| www.google.com | 25 | 0 | Search Engines | Default |
| www.google-analytics.com | 23 | 23 | Trackers & Analytics | Default |
| px.spiceworks.com | 20 | 0 | Computers & Internet | Default |
| herald.spiceworks.com | 20 | 0 | Computers & Internet | Default |
| www.googleadservices.com | 18 | 18 | Banner Ads | Default |

10.8. How to export statistics

To export statistics, go to **Dashboard -> Stats -> Detailed**, select a range and click **Export to CSV**. The statistics can be displayed (and exported) by hours or days. You can see the statistics just for one profile or for all profiles at once.



Detailed Statistics

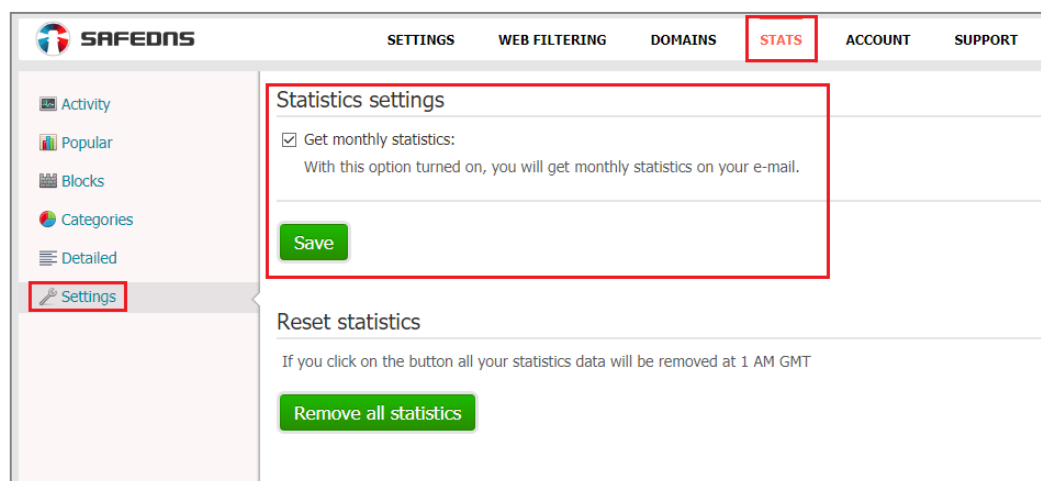
Today All Export to CSV Show

| Domains | Visits | Blocks | Category | Profile |
|--------------------------|--------|--------|---------------------------------------|---------|
| 25.07.2018 00:00 | | | | |
| www.benzinga.com | 49 | 0 | Finances, Business | Default |
| gekko.spiceworks.com | 47 | 0 | Computers & Internet | Default |
| api.similarweb.com | 29 | 0 | Corporate Sites, Computers & Internet | Default |
| www.google.com | 25 | 0 | Search Engines | Default |
| www.google-analytics.com | 23 | 23 | Trackers & Analytics | Default |
| px.spiceworks.com | 20 | 0 | Computers & Internet | Default |
| herald.spiceworks.com | 20 | 0 | Computers & Internet | Default |

Once you press **Export to CSV**, a SafeDNS server will automatically generate a CSV file and send it to your email. CSV is a text format for presenting tabular data. In order to change a file to the CSV format, open your file in any tabular editor and change the coding.

10.9. How to get automatic statistic reports by email

This option makes it possible to receive detailed statistics monthly in the CSV format. To turn this option on go to **Dashboard -> Stats -> Settings** and tick **Get monthly statistics**. Then click **Save**.



10.10. How to view statistics for different computers, devices and networks

To view statistics for individual devices, you should have different filtering profiles configured.

Follow the steps in the NAT DNS setup below to create different filtering profiles.

NAT DNS setup

1. Enter **Dashboard** and assign Public IP of a NAT device to one of the existing filtering profiles (to use NAT DNS you should have more than 2 profiles).
2. Manually or via DHCP set up target DNSes on the end devices (routers or gateways behind NAT).

A list of target DNSes:

- **195.46.39.101**
 - **195.46.39.102**
 - **195.46.39.103**
 - **195.46.39.104**
 - **195.46.39.105**
1. Then go to **Dashboard -> Settings -> NAT DNS**, choose the profile you want to assign to the target IP (one IP – one profile). Click **Save** to apply the settings.
 2. After that, all devices behind NAT will be filtered by the chosen rules.
 3. All Stats data can be shown in the **Stats** tab of a specific profile.

SafeDNS Agent

You can use SafeDNS Agent for configuring different computers in the LAN. More information about the agent can be found here:

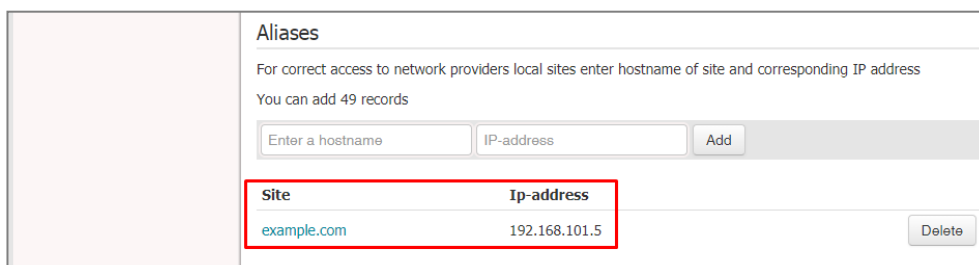
<https://www.safedns.com/en/safedns-agent-how-to-guide/>

[Back to the Contents](#)

11. Local resources

11.1. How to make local resource easily available. Use aliases

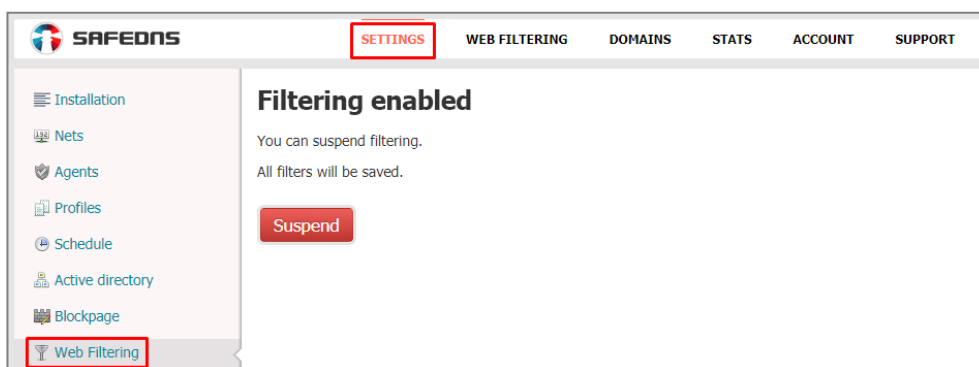
To get access to your LAN resources you should specify the IP (in the local network) of the web server which you want to access from your network and register the IP address and its domain name in **Aliases** (go to the **Domains tab** and scroll all the way down).



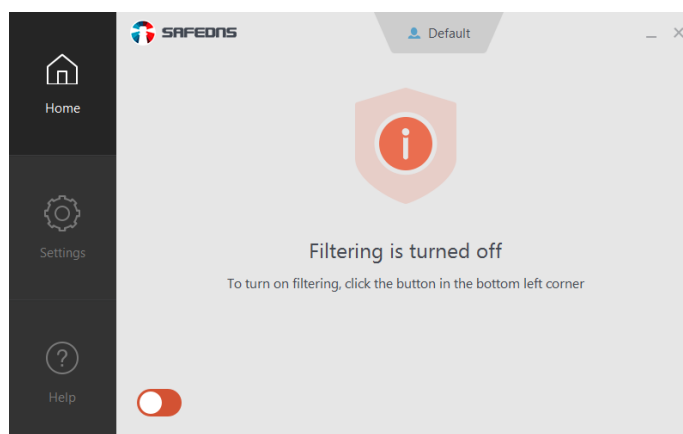
| Site | Ip-address |
|-------------|---------------|
| example.com | 192.168.101.5 |

11.2. How to temporarily suspend filtering

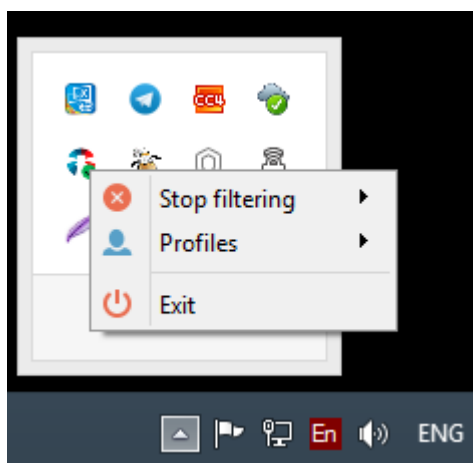
To pause the filtering enter **Dashboard**, go to **Settings -> Web Filtering** (left menu), and click **Suspend**.



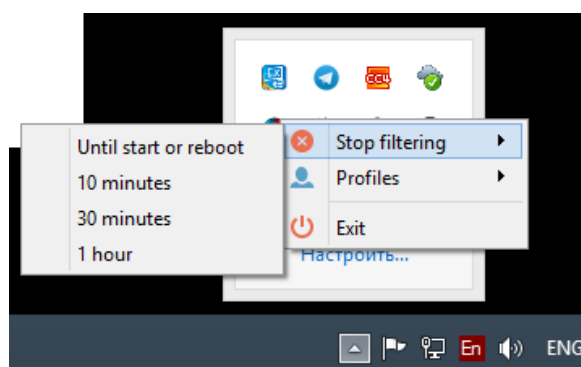
To suspend filtering via SafeDNS Agent click on the **Slider button** at the bottom of the Agent's home page. Your password is required if the settings are protected by password.



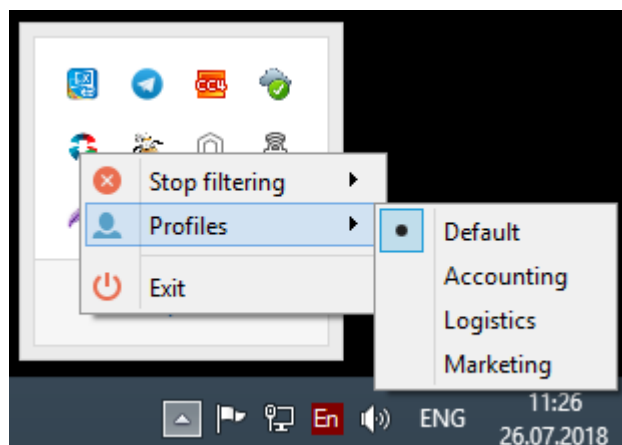
Also, you can stop filtering the internet or change the active profile in the Agent's tray icon. Just right-click on it and choose the necessary option.



You can also switch the filtering off for 10 minutes, 30 minutes, 1 hour or until switching off/ reboot.



Furthermore, you can change the active filtering profile from the tray icon.



If your settings are password protected, you will be asked for your password.

11.3. Does SafeDNS work with proxy servers?

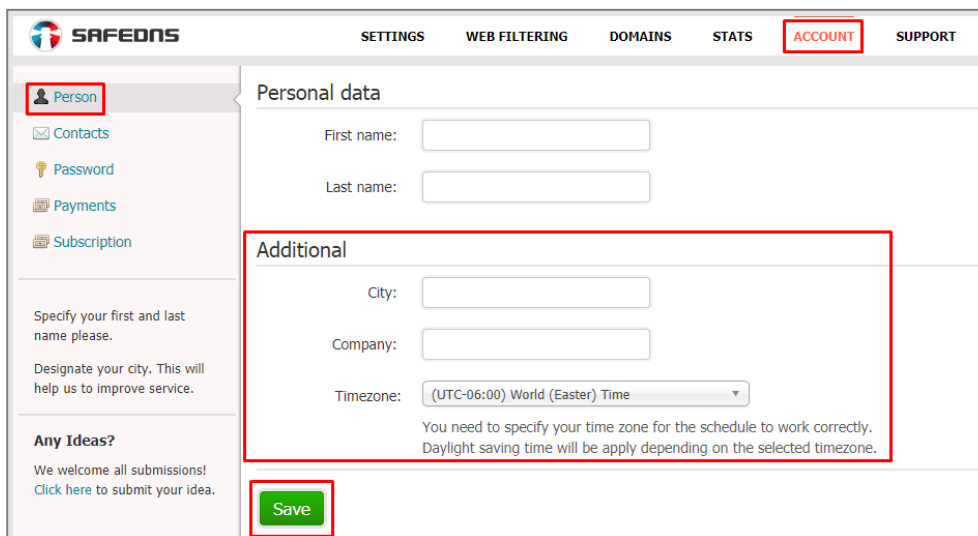
Yes, SafeDNS does work with proxy servers. You should configure a proxy server to use SafeDNS DNS addresses. Set these DNS addresses in the settings of your proxy server. If the proxy server uses the settings of the operating system, you should set our DNS in your system. After this, you should fix your external IP address in **Dashboard**.

If you use Squid, input our DNS servers in the system settings of a set parameter **dns_nameservers** in the Squid configuration.

If you use a Windows-based proxy server, you can install SafeDNS Agent and a proxy server on the same host. In such configuration, configure a proxy server to use DNS **127.0.0.1**.

11.4. How to change time zone for schedule and statistics

You can change a time zone in **Dashboard** by going to **Account -> Person** and selecting an appropriate time zone in the **Additional** section. Never forget to save your change, click **Save**.



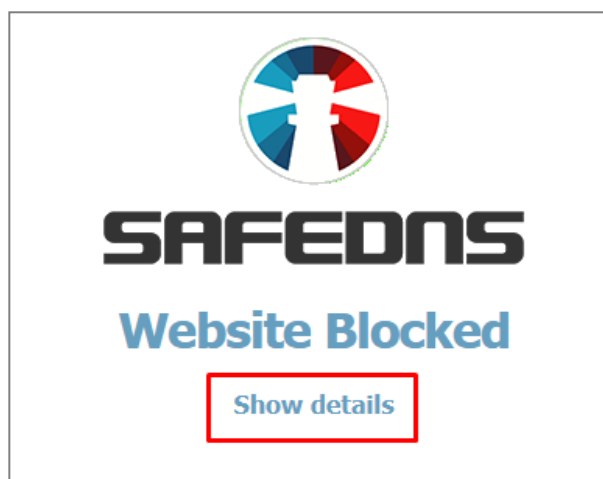
The screenshot shows the SafeDNS dashboard with the 'ACCOUNT' tab selected in the top navigation bar. On the left sidebar, the 'Person' tab is highlighted. The main content area is titled 'Personal data' and contains two sections: 'Personal data' and 'Additional'. The 'Additional' section is highlighted with a red box and contains the following fields:

- City:
- Company:
- Timezone:

Below the 'Timezone' field, there is a note: "You need to specify your time zone for the schedule to work correctly. Daylight saving time will be apply depending on the selected timezone." At the bottom of the 'Additional' section, there is a green 'Save' button, which is also highlighted with a red box.

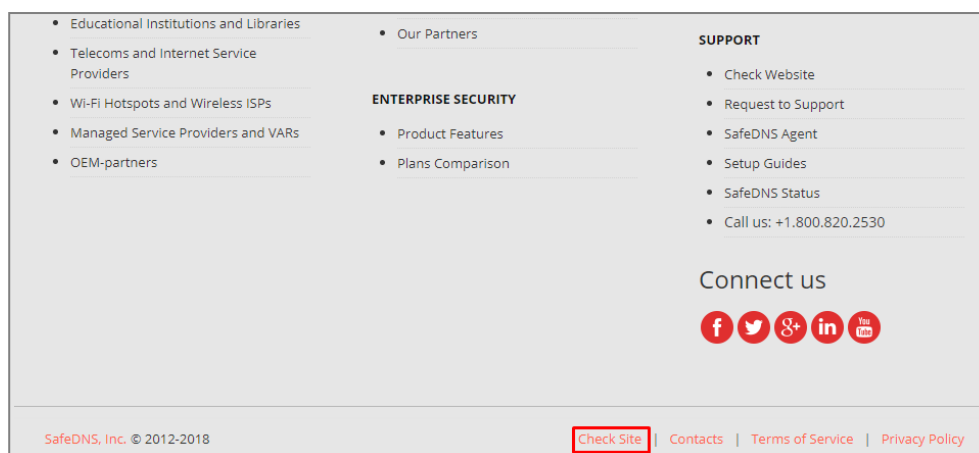
11.5. How to see reason for blocking a website on block page

Go to **Show details** on the **Block page**. If you have concealed the block page (**Hidden block page with the emulation of the website error** or **Empty DNS answer, as if the blocked website did not exist**) the reason for blocking will not be shown.

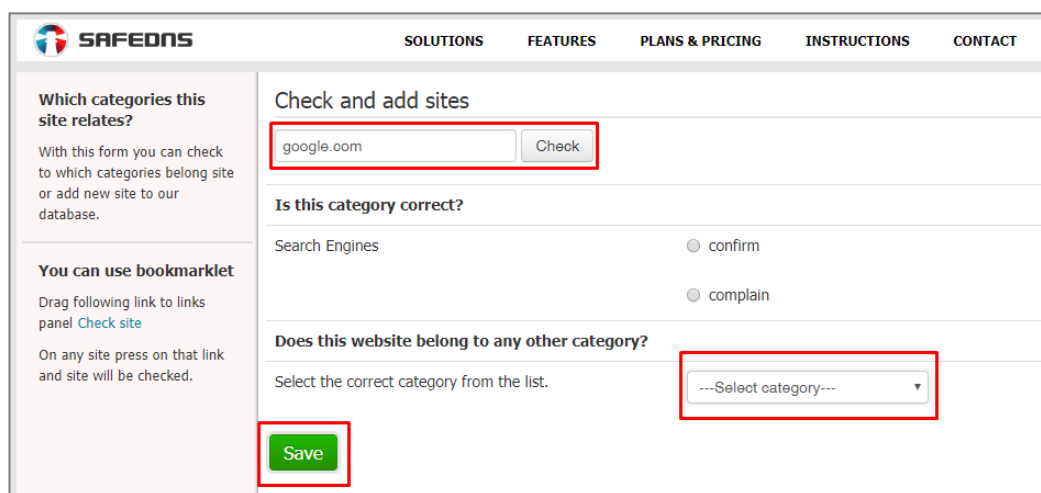


11.6. How to check website category

You can check a category of any website with our service by using the link: <https://www.safedns.com/check/> or by clicking the **Check site** link at the foot of a webpage of the SafeDNS site.



If you think a site is categorized incorrectly, you can make a review request, and advise on the category to which, in your opinion, this site belongs. After that, click the **Save** button.



The screenshot shows the 'Check and add sites' form. It includes a text input field for the website URL (containing 'google.com') and a 'Check' button. Below this, there are radio buttons for 'confirm' and 'complain'. A dropdown menu is labeled '---Select category---'. A green 'Save' button is at the bottom left of the form.

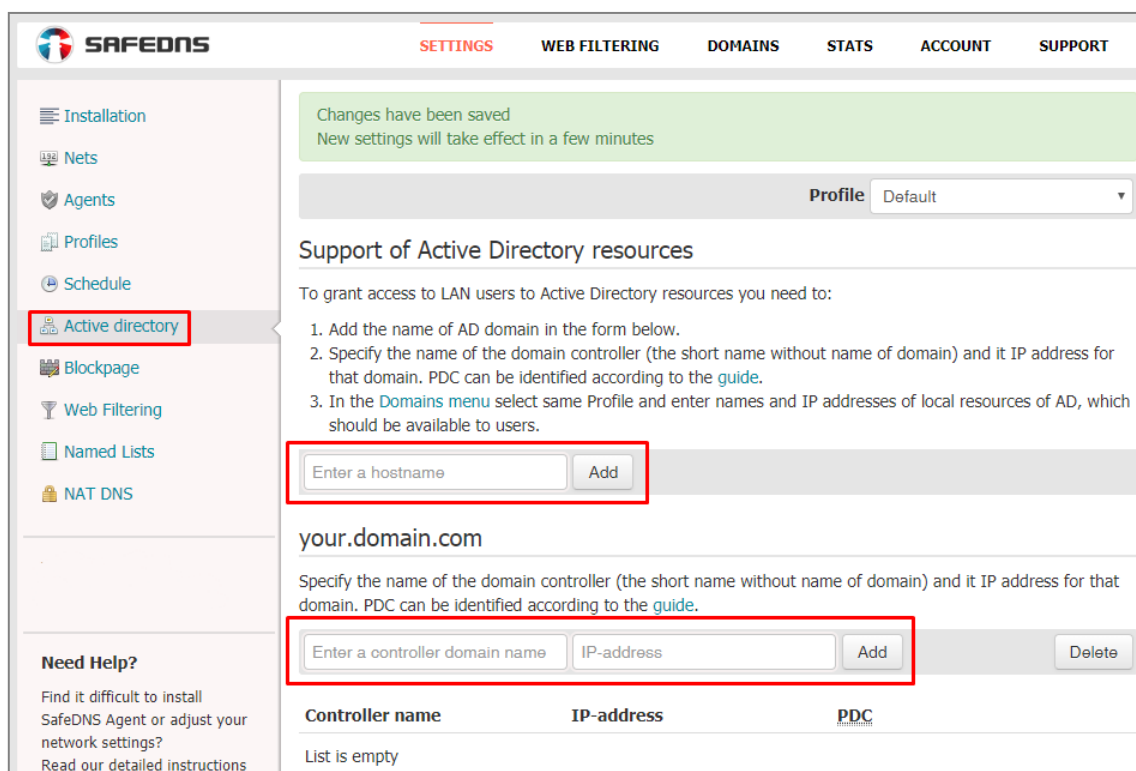
Also, you can use a SafeDNS bookmarklet (a bookmarklet is a small JavaScript program, designed as JavaScript: URL and saved as a browser bookmark). While on any site, click this link in the bookmarks bar and request site re-categorization.

[Back to the Contents](#)

12. Active Directory and Administrators

12.1. Service settings in Active Directory network through the cloud

For Active Directory service settings, go to **Dashboard -> Settings -> Active Directory**. Add a name of an AD domain in the field and click **Add**. Specify a name of a domain controller (the short name without the domain name) and its IP address.



The screenshot shows the SafeDNS web interface. The left sidebar contains a menu with items: Installation, Nets, Agents, Profiles, Schedule, **Active directory** (highlighted with a red box), Blockpage, Web Filtering, Named Lists, and NAT DNS. The main content area is titled 'SETTINGS' and shows a 'Profile' dropdown set to 'Default'. A green notification bar at the top states 'Changes have been saved. New settings will take effect in a few minutes.' Below this, the section 'Support of Active Directory resources' provides instructions: 'To grant access to LAN users to Active Directory resources you need to: 1. Add the name of AD domain in the form below. 2. Specify the name of the domain controller (the short name without name of domain) and it IP address for that domain. PDC can be identified according to the [guide](#). 3. In the Domains menu select same Profile and enter names and IP addresses of local resources of AD, which should be available to users.' There are two input fields with 'Add' buttons, both highlighted with red boxes. The first field is labeled 'Enter a hostname' and the second is labeled 'Enter a controller domain name' and 'IP-address'. Below these fields, there is a table with columns 'Controller name', 'IP-address', and 'PDC'. The table is currently empty, with the text 'List is empty' below it.

SAFEDNS

SETTINGS WEB FILTERING DOMAINS STATS ACCOUNT SUPPORT

Installation
Nets
Agents
Profiles
Schedule
Active directory
Blockpage
Web Filtering
Named Lists
NAT DNS

Changes have been saved
New settings will take effect in a few minutes

Profile: Default

Support of Active Directory resources

To grant access to LAN users to Active Directory resources you need to:

1. Add the name of AD domain in the form below.
2. Specify the name of the domain controller (the short name without name of domain) and it IP address for that domain. PDC can be identified according to the [guide](#).
3. In the Domains menu select same Profile and enter names and IP addresses of local resources of AD, which should be available to users.

Enter a hostname

your.domain.com

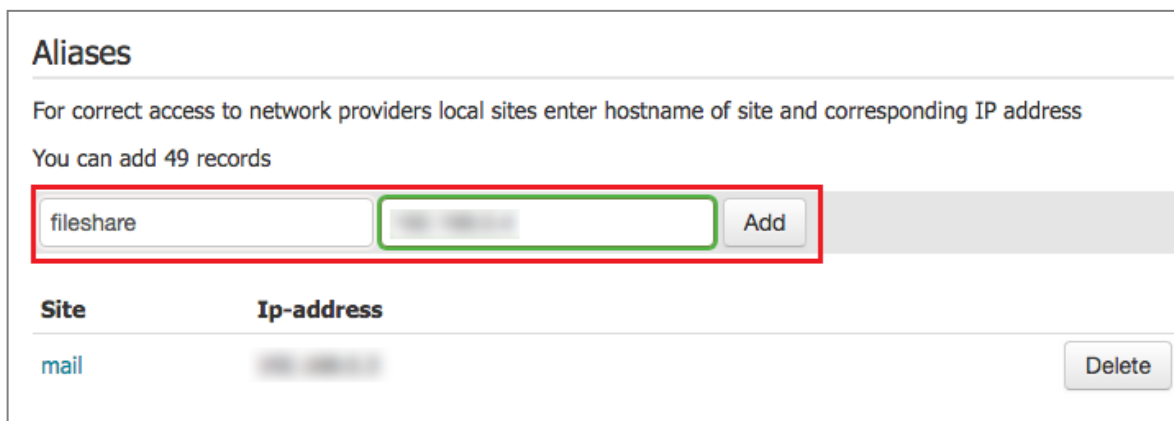
Specify the name of the domain controller (the short name without name of domain) and it IP address for that domain. PDC can be identified according to the [guide](#).

Enter a controller domain name IP-address

| Controller name | IP-address | PDC |
|-----------------|------------|-----|
| List is empty | | |

Need Help?
Find it difficult to install SafeDNS Agent or adjust your network settings?
Read our detailed instructions

Then go to **Domains -> Aliases** and enter domains of AD local resources, which should be available to users.




Aliases

For correct access to network providers local sites enter hostname of site and corresponding IP address

You can add 49 records

fileshare

| Site | Ip-address |
|------|---|
| mail |  |

12.2. Working with Active Directory through a special version of the agent

To work with Active Directory via SafeDNS Agent, you should **download a special server version of Agent**. You can get a SafeDNS Catserver Agent by [contacting our technical support](#).

12.3. Working with Active Directory for single filtering settings

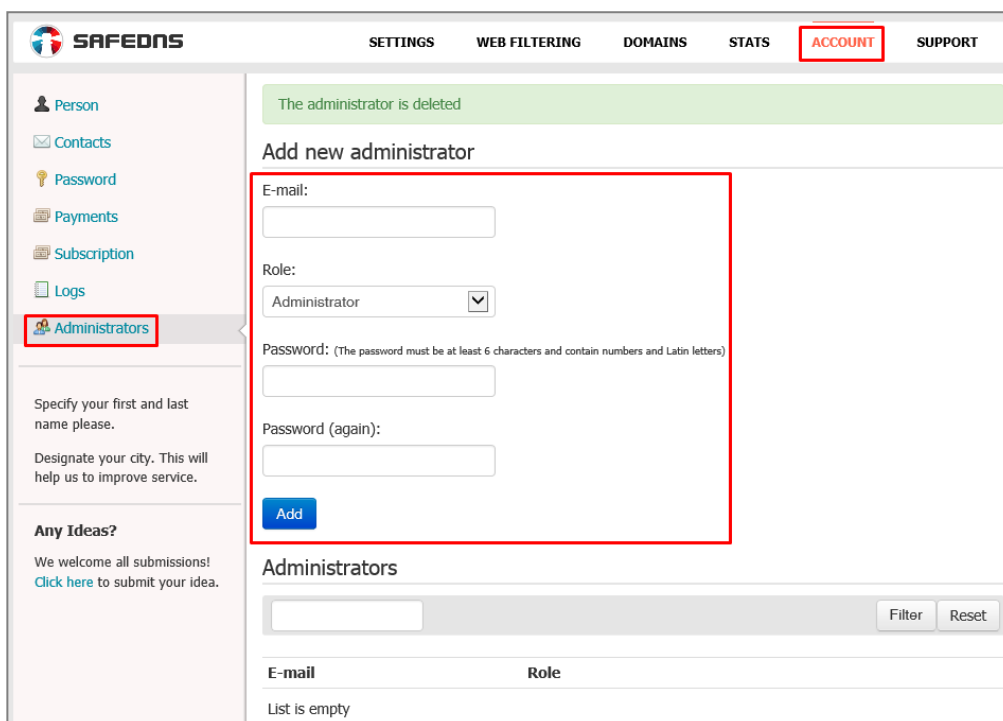
To work with Active Directory for filtering settings go to a **domain controller**, then **Start -> Administrative Tools -> DNS** and select the server that hosts a DNS server (server name). Next, open **Settings -> Redirect Server** and add the IP address of the SafeDNS DNS server, and click **OK**.

12.4. How to enable multiple account administrators

Attention! This feature is only available on the Enterprise plan. If you are a user on this plan, do the following:

1. Go to **Dashboard -> Account -> Administrators**.
2. Then you can add account administrators
3. Enter email and password for each administrator.

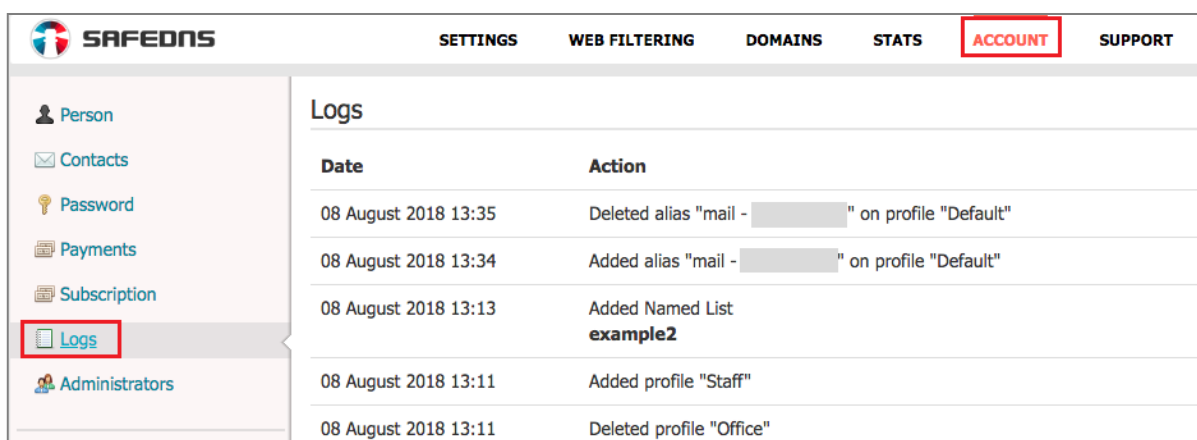
After that, all the added administrators will be displayed in the list below. The added administrators have the same rights as you, except for the ability to create other administrators.



The screenshot shows the SAFEDNS web interface. The top navigation bar includes 'SETTINGS', 'WEB FILTERING', 'DOMAINS', 'STATS', 'ACCOUNT' (highlighted with a red box), and 'SUPPORT'. The left sidebar contains links for 'Person', 'Contacts', 'Password', 'Payments', 'Subscription', 'Logs', and 'Administrators' (highlighted with a red box). The main content area has a green banner stating 'The administrator is deleted'. Below this is the 'Add new administrator' section, which is enclosed in a red box. This section contains fields for 'E-mail:', 'Role:' (a dropdown menu with 'Administrator' selected), 'Password:' (with a note: '(The password must be at least 6 characters and contain numbers and Latin letters)'), and 'Password (again):'. An 'Add' button is at the bottom of this section. Below the form is the 'Administrators' section, which includes a search bar, 'Filter' and 'Reset' buttons, and a table with columns 'E-mail' and 'Role'. The table currently shows 'List is empty'.

12.5. How to see Administrator activity log

You can monitor administrator activity logs in **Dashboard -> Account -> Logs**.



| Date | Action |
|----------------------|--|
| 08 August 2018 13:35 | Deleted alias "mail - [redacted]" on profile "Default" |
| 08 August 2018 13:34 | Added alias "mail - [redacted]" on profile "Default" |
| 08 August 2018 13:13 | Added Named List example2 |
| 08 August 2018 13:11 | Added profile "Staff" |
| 08 August 2018 13:11 | Deleted profile "Office" |

12.6. How to install Agent on a corporate network

For unattended installation of SafeDNS Agent run the installer with **/S switch** in the command line ("S" upper-case only). This functionality is supported by SafeDNS Agent starting from version 2.6.

The following keys are acceptable in the command line:

- **/login=< login > option** allows you to specify your login (for example, safedns-agent-setup /S /login=email@email.com /pass=qwerty).
- **/pass=< password > option** allows you to specify your password (for example, safedns-agent-setup /S /login=email@email.com /pass=qwerty). It is mandatory to use the /login and /pass options together. If only one of the options is used, then firstly launch the login, and the password will be requested via GUI.
- **/prof=< profile > option** allows you to specify the necessary profile (for example, safedns-agent-setup /S /login=email@email.com /pass=qwerty /prof=My profile). If the option is not used or a wrong profile is specified, then the Default profile will be used.
- **/conn=< interface > option** allows you to specify network interface that should be protected (for example, safedns-agent-setup /S /login=email@email.com/pass=qwerty /conn=Wi-Fi).
- **/pall** switch should be used if all network interfaces are to be protected. If both /conn option and /pall switch are used, then only the latter takes action. If neither /conn option nor /pall switch is used, then default network interface will be protected.
- **/dupd** switch turns off automatic checks for new versions of Agent.
- **/darun** switch disables automatic startup of SafeDNS Agent GUI when Windows starts (no Agent icon will be shown in the system tray). This switch does not affect the functionality of the SafeDNS Agent system service.
- **/D=< path > option** allows you to specify the installation directory ("D" upper-case only). It must be the last option used in the command line and must not contain any quotes, even if the path contains whitespace characters (for example, safedns-agent-setup /S /login=email@email.com /pass=qwerty /D=c:\program files(x86)\SafeDNS Agent). Only absolute paths are supported.

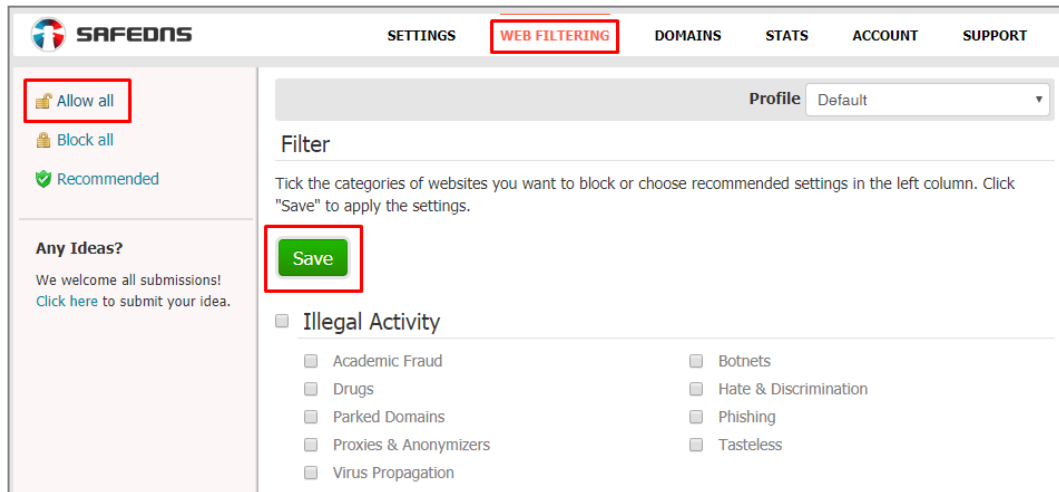
Don't quote options containing whitespace characters (for example, /prof=My profile).

[Back to the Contents](#)

13. Other modes of service

13.1. How to turn on monitor mode

To activate the monitoring mode without the web filtering go to **Dashboard -> Web Filtering** and click **Allow all** and **Save**.



13.2. How to completely block access to the internet

To completely block the internet, you have to turn on **Use the White List only** mode and leave the whitelist empty.

Additional settings


☒ Use the White List only
 With this feature enabled, you will only have access to the sites in your [White list](#).

☐ Force Safe Search
 With this option turned on all requests to Google Search and Bing Search will be forced to use Safe Search filter.
 This will filter sexually explicit video and images from Search result pages.

☐ Force Restricted Mode for Youtube
 With this option enabled, Youtube will be forced to use Restricted Mode. Restricted Mode hides videos that may contain inappropriate content flagged by users and other signals. No filter is 100% accurate, but it should help you avoid most inappropriate content. With option enabled, Youtube will be accessible even if category Movies & Video is blocked.

☐ Get botnet activity warnings
 With this option enabled you will get an email notification if our servers detect any requests from your devices to a botnet control server.

Save


SAFEDNS

[SETTINGS](#)
[WEB FILTERING](#)
[DOMAINS](#)
[STATS](#)
[ACCOUNT](#)
[SUPPORT](#)

Need Help?

Find it difficult to install SafeDNS Agent or adjust your network settings?
 Read our detailed instructions on how to customize SafeDNS for the popular operating systems.
[Getting Started Guide](#)
[FAQ - Basic Questions](#)

Profile

Default

▼

White list

Never Block

Site

List is empty

[Back to the Contents](#)

57

14. Pricing policy

14.1. SafeDNS billing plans

Safe@Home

With our internet security and parental control system your entire family is shielded from online threats and unwanted websites.

The SafeDNS service allows you to manage your kids' internet access even when you are away from home. Make internet surfing safer for them at any time.

Safe@Office

The SafeDNS filtering service for SMBs allows you to manage and control how employees use the corporate network. The SafeDNS web filter helps employers to limit personnel's irrelevant internet activity keeping employees on task and saving work time as well as significantly cutting corporate expenses. In short, it is perfect for you and your staff.

Any of the host of Safe@Office plans provides:

- Protection of all internet-connected devices and computers with any OS
- Protection from botnets, phishing and malware sites
- Support for static and dynamic IPs and third-party dynamic DNS services
- Protection for off-network computers with SafeDNS Agent
- Support for Active Directory resources
- Fully customizable block page
- Detailed reports and stats archived for one year
- Stats export in CSV
- Admin activity log

Safe@Enterprise

We offer a special protection for large corporations and enterprises. The SafeDNS cloud-based filtering service fully meets their demand in securing web connection for any number of offices and networks. Contact our Sales to learn more about the Safe@Enterprise plan with almost unlimited features.

14.2. How to calculate the number of licenses required

Being a Safe@Home user, you get a license for protection of all devices on your home network.

Attention! Usage of the Safe@Home plan is prohibited in commercial organizations and educational institutions.

Licensing fees on Safe@Office are based on a number of protected end-user computers.

Safe@Enterprise is also licensed by the number of connected networks and the number of computers (the minimum purchase amount is 100 licenses).

Licenses for the HotSpot Edition plan to protect public Wi-Fi access points are calculated by a number of access points.

All prices are shown on the SafeDNS website and all of them are for 1 year of service.

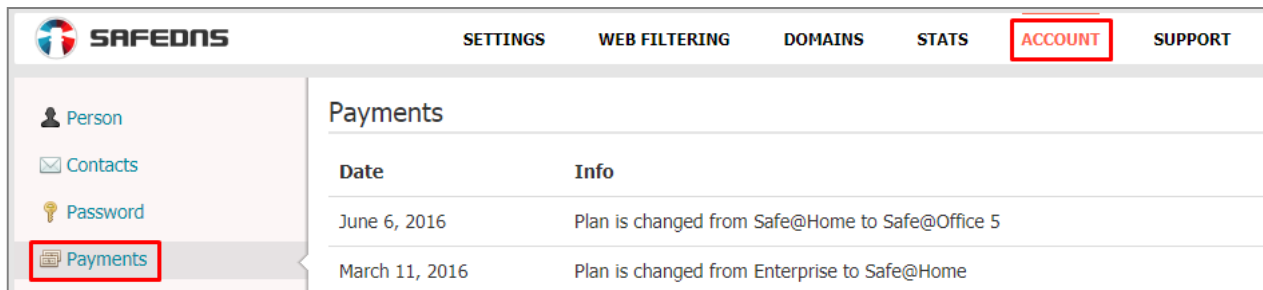
14.3. How to buy premium services

To purchase a plan, follow this link <https://www.safedns.com/en/order-safedns-online/> and select an appropriate plan. For more options you can contact our managers at +1.800.820.2530.

| Safe@Office Plans | | |
|---|---|---|
| For 5 users | 5 filtering profiles 50 white/blacklist domains per each profile | \$80 per year Buy now |
| For 10 users | 10 filtering profiles 100 white/blacklist domains per each profile | \$150 per year Buy now |
| For 25 users | 25 filtering profiles 250 white/blacklist domains per each profile | \$350 per year Buy now |
| For 50 users | 50 filtering profiles 500 white/blacklist domains per each profile | \$600 per year Buy now |
| For 75 users | 75 filtering profiles 750 white/blacklist domains per each profile | \$785 per year Buy now |
| For 100 users | 100 filtering profiles 1000 white/blacklist domains per each profile | \$970 per year Buy now |
| <p>Need plan for more than 100 users? Call us for custom pricing. We offer custom plans and discounts for educational institutions, libraries, child centers & churches. Contact us with your needs to get the quote.</p> | | |

14.4. How to extend premium services

To extend your subscription, go to **Dashboard -> Account -> Subscription**. In the upper line, you will see the option of renewal.



The screenshot shows the SAFEDNS dashboard with the 'ACCOUNT' menu item highlighted in red. On the left sidebar, the 'Payments' option is also highlighted in red. The main content area displays a table titled 'Payments' with two columns: 'Date' and 'Info'.

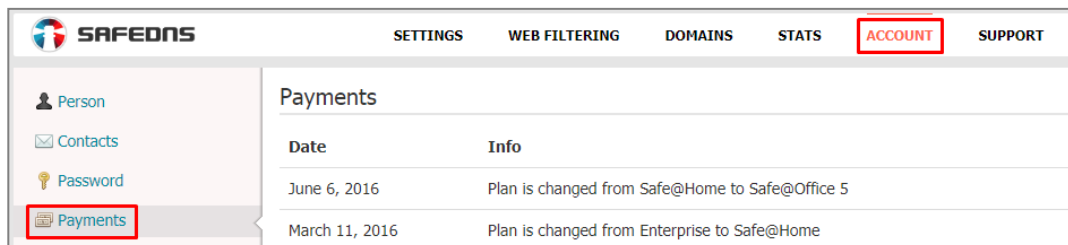
| Date | Info |
|----------------|---|
| June 6, 2016 | Plan is changed from Safe@Home to Safe@Office 5 |
| March 11, 2016 | Plan is changed from Enterprise to Safe@Home |

Clicking this link will transfer you to <https://www.safedns.com/en/order-safedns-online/>. On this page, you can extend your billing plan (for example, Safe@Home) or purchase a different plan.

You can also contact our account managers at +1.800.820.2530 or by email: accounts@safedns.com.

14.5. How to see list of fees and plan switching

You have to go to **Dashboard -> Account -> Payments** and see a list of payments and switching of billing plans.



This screenshot is identical to the one in section 14.4, showing the SAFEDNS dashboard with the 'ACCOUNT' menu item highlighted in red. On the left sidebar, the 'Payments' option is also highlighted in red. The main content area displays a table titled 'Payments' with two columns: 'Date' and 'Info'.

| Date | Info |
|----------------|---|
| June 6, 2016 | Plan is changed from Safe@Home to Safe@Office 5 |
| March 11, 2016 | Plan is changed from Enterprise to Safe@Home |

14.6. How to change paid billing plan to another

To change from one plan to another, please, contact the sales department at +1.800.820.2530. You can also request a plan change on the SafeDNS website. To do this click the link <https://www.safedns.com/en/order-safedns-online/>. After the transfer, you will need to choose a plan.

The balance of your previous plan will be taken into account and the price for your new plan will be recalculated. Transition to the Safe@Home plan can be carried out without SafeDNS manager participation, for the other plans it is necessary to leave a request on the SafeDNS site.

14.7. What happens when paid period ends of plan

After the end of a paid period, your plan will automatically change to **'Paid period ended'**. At this point access to the internet will be blocked. When your Safe@Home plan expires, your subscription will automatically switch to Free plan.

[Back to the Contents](#)

15. Technical support

15.1. How to get support

For technical support you can call +1.800.820.2530 ext. 2 or send an email at support@safedns.com.

You can also contact our technical support team using our website. Just go to **Dashboard -> Support**, and describe the problem.

15.2. What is SafeDNS Help Desk portal

On **SafeDNS Help Desk portal** (<https://help.safedns.com/support/home>) you can find:

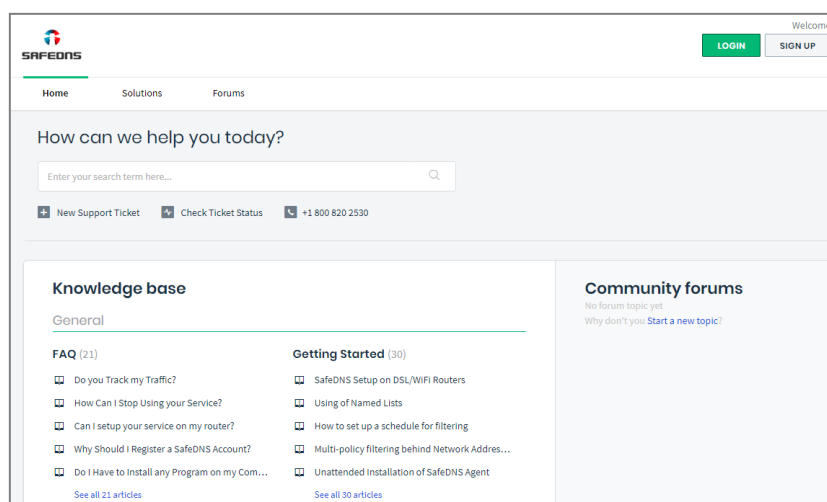
- FAQs and answers to them
- All SafeDNS technical guides on getting started with SafeDNS, setting up the content filtering service on different devices and OSes.

To find the necessary guide quicker you can search for a particular term – enter it in the search bar.

Have an online chat with Support - just click the **Need help** button.

If you are experiencing a technical issue with the SafeDNS service or have a query to SafeDNS Support, just click the **New Support Ticket** button and create a ticket. You can always check your ticket status in the **Ticket** section of the portal. Sysadmins of large organizations can now check status of all tickets created by employees of the organization.

Use the **Forums** section of the portal to start a discussion on a topic related to SafeDNS.



15.3. How to completely disable content filtering

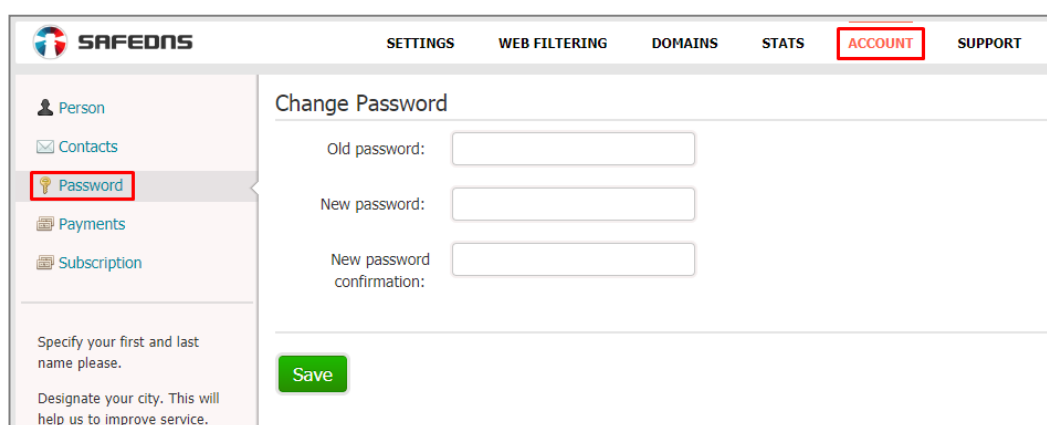
To completely disable the internet filtering, you need to delete SafeDNS Agent, delete the IP address in **Dashboard -> Settings -> Nets**, reset your router's settings, remove the preferred DNS server (network settings), remove VPN clients from a computer and mobile device.

15.4. How to change email account

To change your email, you can contact our technical support team at +1.800.820.2530 ext. 2 or send an email to support@safedns.com, or contact us via the form on the SafeDNS site.

15.5. How do I change my account password

To change your password, you can use a special form. Just go to **Dashboard -> Account -> Password**, then enter your old password and new one. If you, for some reason, cannot remember or have lost your password, you can use a password recovery form.



The screenshot shows the SafeDNS web interface. At the top, there is a navigation bar with the SafeDNS logo and several menu items: SETTINGS, WEB FILTERING, DOMAINS, STATS, ACCOUNT (highlighted with a red box), and SUPPORT. On the left side, there is a sidebar menu with options: Person, Contacts, Password (highlighted with a red box), Payments, and Subscription. Below the sidebar, there is a section for user information with the text: 'Specify your first and last name please.' and 'Designate your city. This will help us to improve service.' The main content area is titled 'Change Password' and contains three input fields: 'Old password:', 'New password:', and 'New password confirmation:'. A green 'Save' button is located at the bottom of the form.

15.6. My IP address is already used by someone else

You need to [contact technical support](#). This situation can occur if your ISP gave you the IP address of a person who used to be a SafeDNS client.

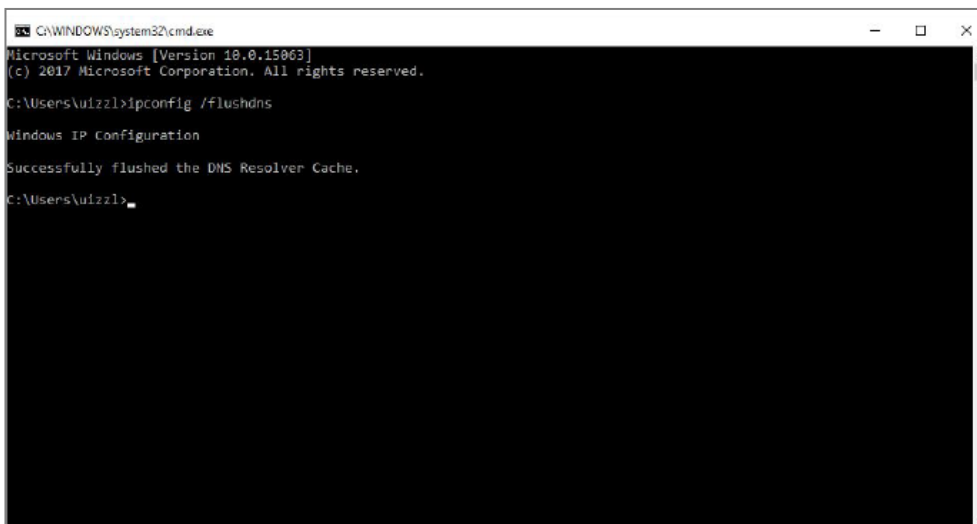
[Back to the Contents](#)

16. Clearing cache

16.1. Windows

Clear DNS cache via the command line:

```
ipconfig /flushdns
```



```
CA\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\ui221>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\ui221>
```

16.2. OS X

In the terminal mode, you need to be an administrator to execute a command corresponding to your system version:

- **10.4 TIGER:**

```
lookupd -flushcache
```

- **10.5 and 10.6 LEOPARD:**

```
dscacheutil -flushcache
```


- **10.7 and 10.8 Lion:**

```
sudo killall -HUP mDNSResponder
```

- **10.9 and 10.10.4 Yosemite:**

```
dscacheutil -flushcache  
sudo killall -HUP mDNSResponder
```

- **10.10 Yosemite (not a 10.10.4):**

```
sudo discoveryutil mdnsflushcachesudo discoveryutil  
udnsflushcaches; say flushed
```

16.3. Linux (major distributions)

Open a terminal and run the following command:

```
sudo restart /etc/init.d/nscd  
or  
sudo restart /etc/init.d/nscd
```

16.4. Debian

```
service nscd restart
```

```
root@debian:~# service nscd restart  
[ OK ] Restarting Name Service Cache Daemon: nscd.  
root@debian:~# _
```

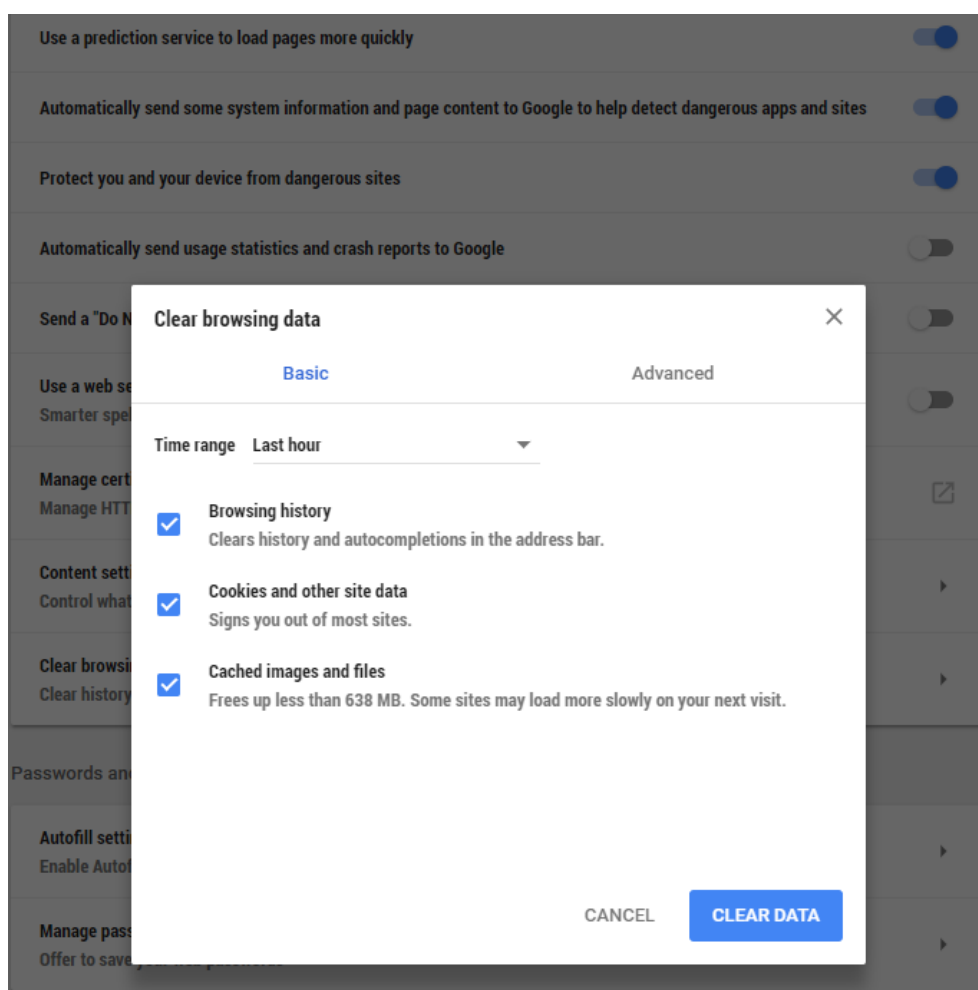
16.5. Ubuntu Linux

Open a terminal and run the following command:

```
sudo service network-manager restart
```

16.6. Clearing your cache in Google Chrome

Go to the three-dot menu at the upper-right of Chrome and select **Settings -> Show advanced settings -> Clear browsing data** (or type **'chrome://settings/clearBrowserData'** without the quotation marks in the omnibar). This will take you directly to the dialog box and delete not only your browsing history, but also your download history (it won't delete actually the downloaded files), all your cookies, cached images and files (which help load pages faster when you revisit), saved passwords and more. Moreover, you can delete only the data from the last hour, day, week, month, or all of it up to 'the beginning of time'.



Unfortunately, Google Chrome has no option of not collecting your browsing history.

What's more, if you have a Google account and are signed into it with Chrome, your history is likely to be synched with **Google My Activity**. Even though it should be secured to your Google account (use a password manager and a two-factor authentication for the best protection), if you truly wish to get rid of the history, select

the **three-dot menu at the top** -> **Activity Controls** to turn off the inclusion of Chrome activity (from desktops and handhelds), as well as delete any activity synched with the service.

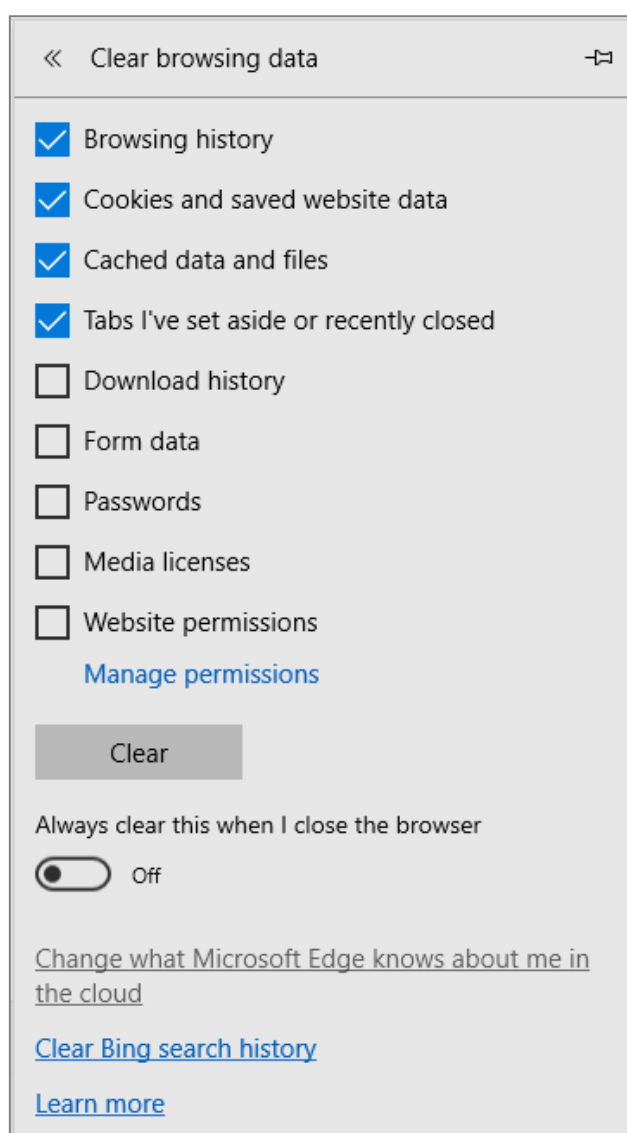
16.7. Clearing your cache in Opera

In the **main menu** in Opera, go to **Settings -> Privacy & Security**. You'll see the **Clear browsing data** button that offers almost identical settings as Chrome, right down to the "beginning of time" option. (You can also type **'opera://settings/clearBrowserData'** into the address bar.) It is similar to Chrome due to the similar platform. Opera offers a little extra to those who want to surf the Web safely. However, a built-in VPN option, a courtesy of SurfEasy, is found in the **Privacy & Security** settings.

16.8. Clearing your cache in Microsoft Edge and Internet Explorer

Go to the three-dot menu in Microsoft Edge and select settings; in the fly-out menu click the **Choose what to clear** button. Get rid of browsing and download history, cookies, cached data, stored form data, and stored passwords; click **Show more** if you want to delete things like sites that are allowed to show pop-ups.

You cannot delete just one chunk of data from a time period like a day or week, but there is the option to **Always clear this [data] when I close the browser**. That ensures you have no browser history stored, as long as you close the browser regularly.



Like Google, Microsoft keeps some of your history online. **Click Change what Microsoft Edge knows about me in the cloud** to visit a page for your Microsoft account where you can delete that synched browsing history. You can also delete search history on Bing.com, stored location data showing where you've logged in, and stuff you've stored in Cortana notebook.

Still using Internet Explorer (IE)? You're not alone. To wipe the history in IE11 and 10, go to the **Gear icon** at the upper left and select **Internet Options**. On the **General** tab, you can tick a box next to **Delete browsing history on exit** or click the **Delete** button to instantly get rid of history, passwords, cookies, cached data (called **'Temporary Internet files and website files'**), and more. If you instead click **Settings**, you go to the **History** tab and ensure your history is only collected for a specific number of days, automatically deleting anything older.

You have an option to get rid of your browsing history using the **Favorites Menu**. Click the **star** at the top-right -> **History tab**. There, you can see websites you visited on specific dates (Today, Last Week, 3 Weeks Ago, etc.) Right-click to delete everything from a specific time period, or click to view and delete specific websites. If you're using an older version of IE, there are online instructions for deleting the history.

16.9. Clearing your cache in Safari

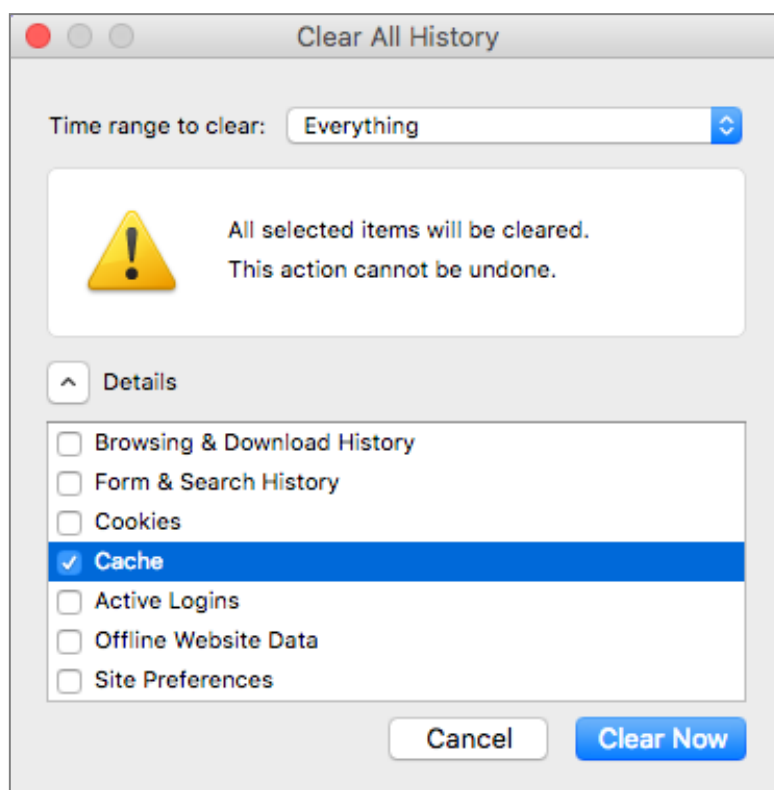
On MacOS, Safari rules. Clearing your website visit history is simple: click **Clear History** in the main menu. Then in the pop-up, pick a time frame for how far back you want to erase.



You can instead click **History -> Show History** to get a pop-up displaying every site you have visited, then take out sites individually, without losing the cookies and cache. You can zap cookies by going into **Preferences -> Privacy**; delete your cache by going to the **Develop** menu and picking **Empty Caches**. If you have no **Develop** menu in Safari, go to **Preferences -> Advanced** and tick **Show Develop** Menu in the **Menu Bar** at the bottom.

16.10. Clearing your cache in Mozilla Firefox

The latest version of Firefox uses sidebars for accessing preferences, much like Microsoft Edge. Access them at the **hamburger menu** (at upper right) and you can go right to **History**. It'll show all your visited sites and the **Clear Recent History** option (or hit **Ctrl+Shift+Del** for the same effect). If you select **Options** in that sidebar, you can go to preferences to either remember history, never remember, or do some custom settings, such as always go into private browsing mode, or never store history or cookies, or to clear the history when closing Firefox.



Check the **Sync** tab while you're there – if you are signed in with a Mozilla Firefox account – your history (as well as bookmarks, tabs, passwords, and preferences) may be synced with your other PCs and devices using Firefox, even on smartphones.

[Back to the Contents](#)

About SafeDNS

SafeDNS is founded by a team of IT and security experts for developing high quality web filtering solutions for a wide range of markets and consumers. We are creating the next generation of safer and affordable web filtering products. In July, 2016, to further improve our users' online protection SafeDNS launched an innovative system for detecting botnets and malicious internet resources (malware) which is based on continuous machine learning and user behavior analysis.

Our content and web filtering solutions are used by more than 4000 organizations and tens of thousands of private users across US, UK, the Middle East, Eastern Europe and the Far East.

We offer products for home use, business, educational institutions, telecom operators, ISPs, MSPs, and VARs. Our special filtering products comply with specific government regulations in countries where such regulations exist. We can protect individual telecom operators and therefore our solutions can be used for nationwide filtering of regulated content and websites.

Try our service for free! Get your free trial:

For Business: <https://www.safedns.com/trial/business-5>

For Home: <https://www.safedns.com/trial/premium>

Follow us:



**Also you can find some video guides
on our YouTube channel:**

