

Linux OS

- [SafeDNS Agent for Linux Setup](#)
- [Linux Filtering Setup via OpenVPN](#)
- [Linux DNS Setup](#)

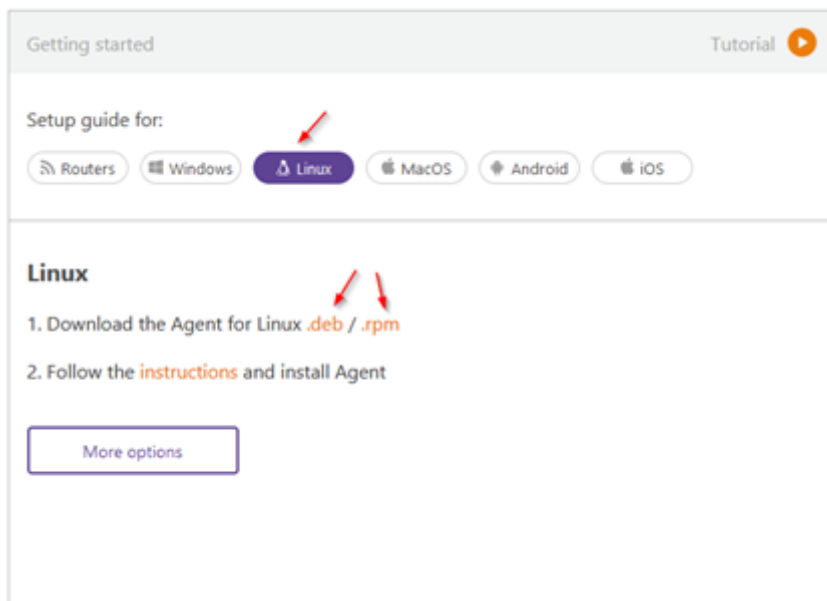
SafeDNS Agent for Linux Setup

Installation requirements: Debian 9, Ubuntu 18-22, PopOS, CentOS 7.

Requires the following billing plans: **Safe@Home**, **Safe@Office**, **Family**, **Pro**, **Pro+**

Getting Started

1. Log in to your SafeDNS account with your registration email and password.
2. Navigate to the **Getting Started** tab on the main page of the **Dashboard** and select the Linux button. Choose and download the needed package: **.rpm** or **.deb**.



.rpm package

Use the following command for the installation from the Terminal app:

```
sudo rpm -Uvh /home/user/Downloads/safedns-agent-1.3.1-x86_64.rpm
```

Please note, that the path to the file and/or package name might be different.

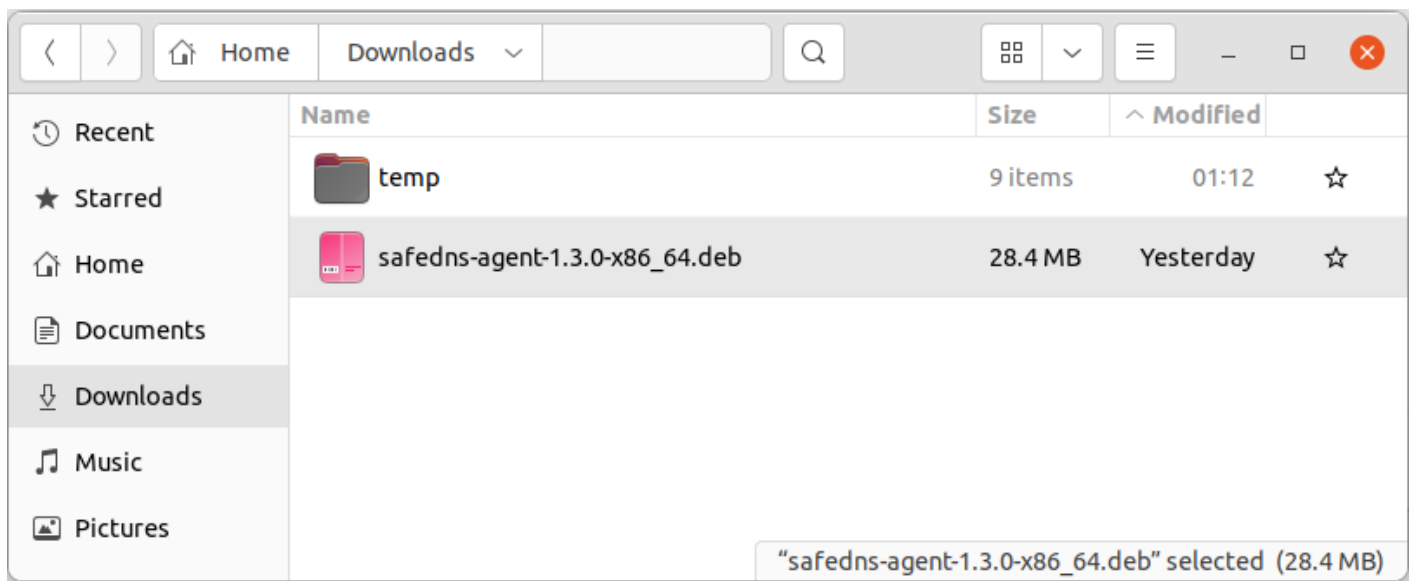
.deb package

For experienced users. You can use this command to install from the Terminal app:

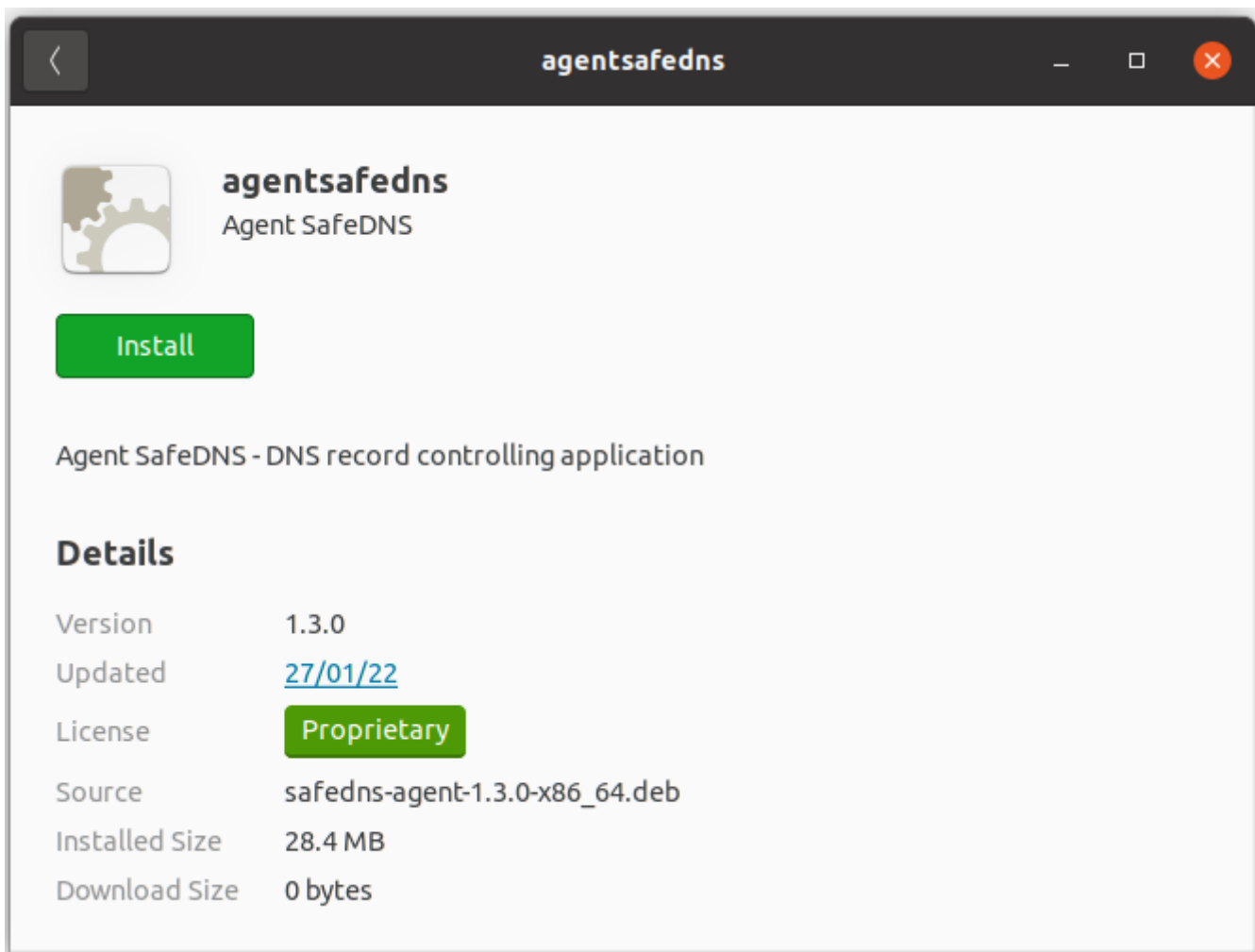
```
sudo dpkg -i /home/user/Downloads/safedns-agent-1.3.1-x86_64.deb
```

Please note, that the path to the file and/or package name might be different.

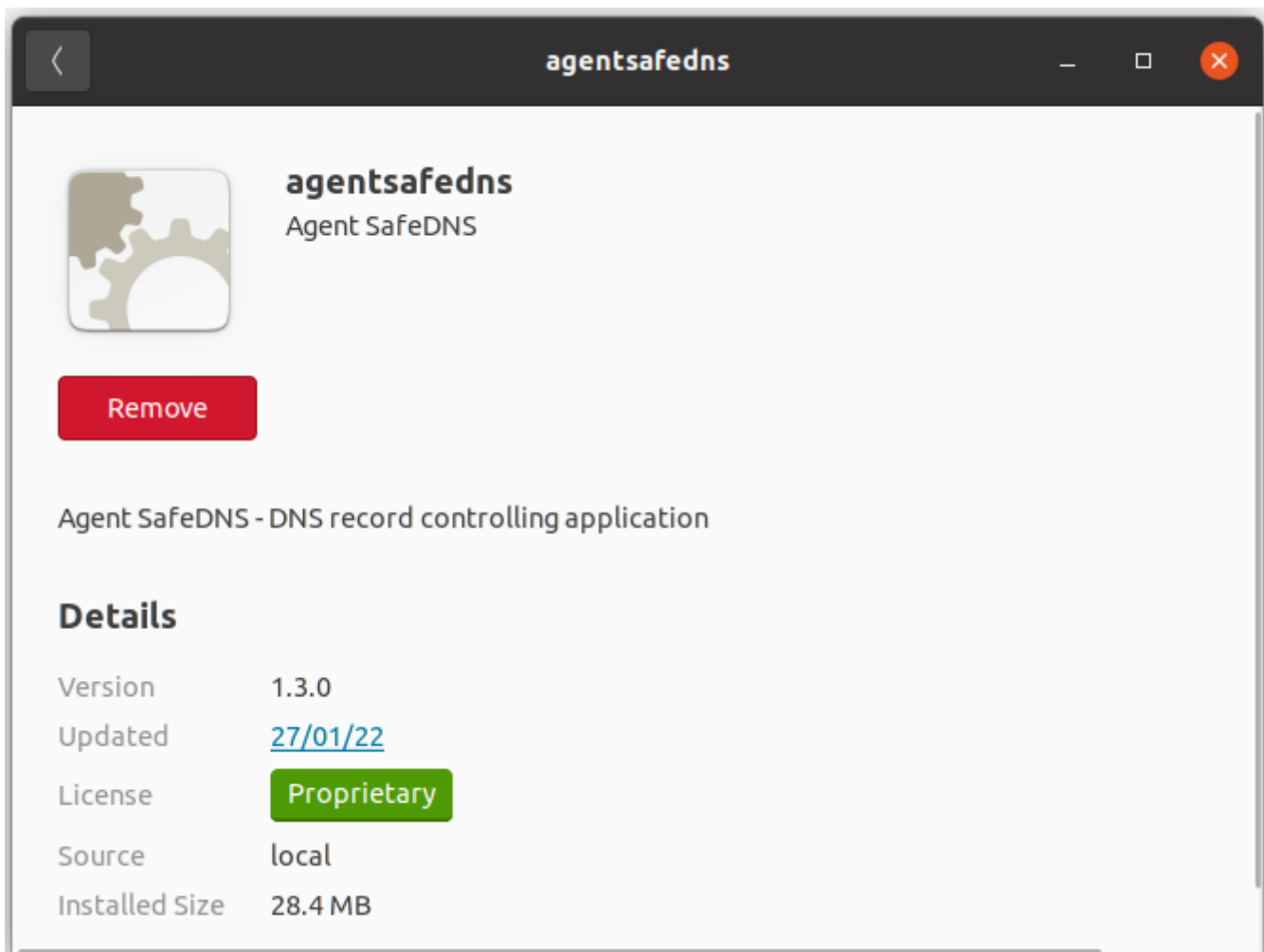
1. Open the “Downloads” folder:



2. Run the downloaded file and install the Agent. Enter the Admin password if prompted.

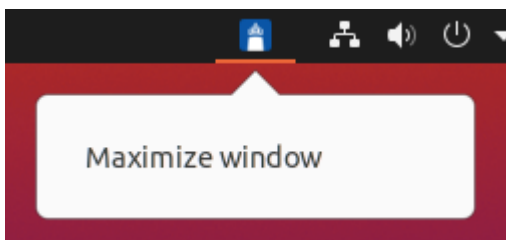


3. You will see the following window once the installation finishes:

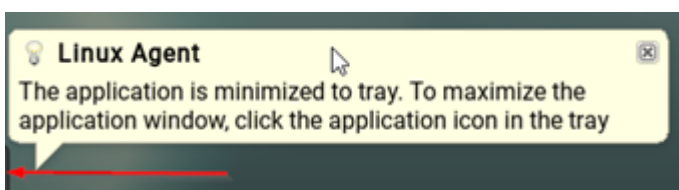


Agent Setup

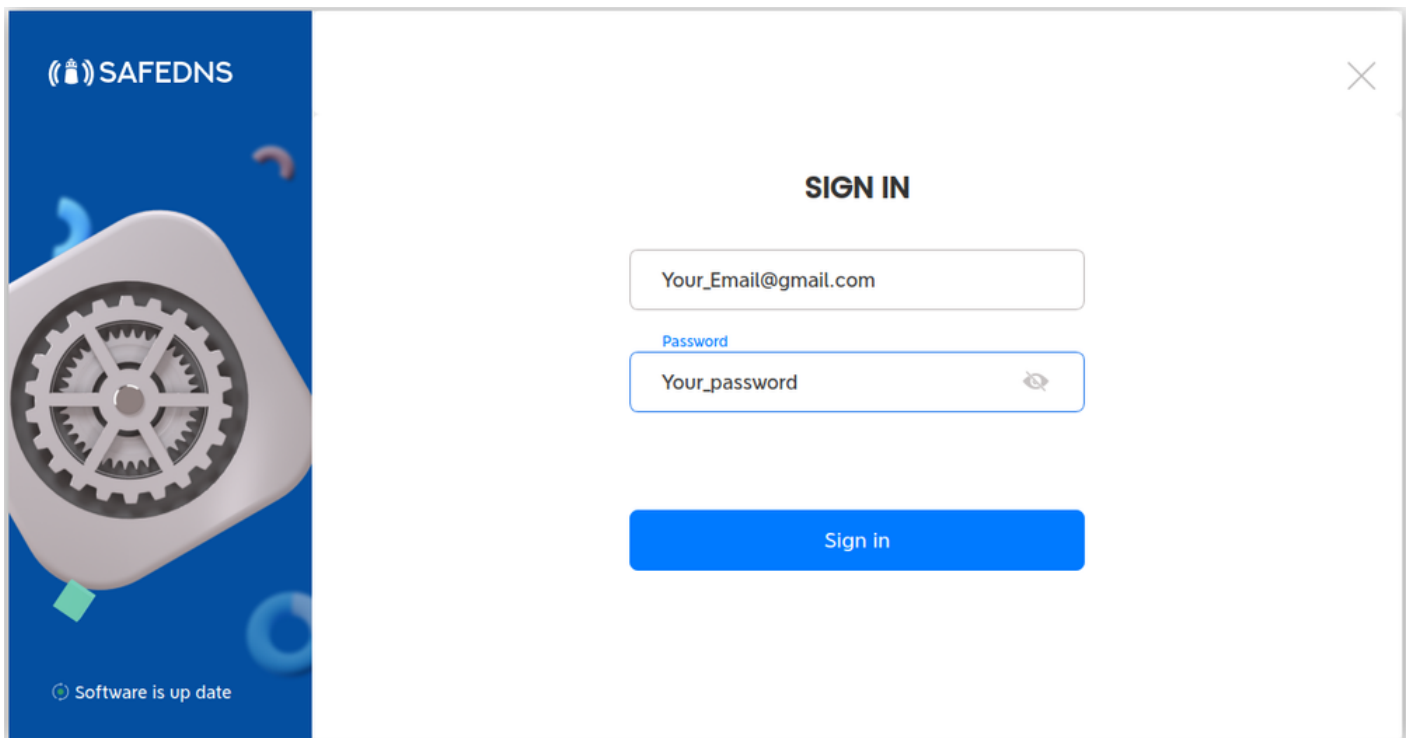
1. **Restart your system.** The Agent icon will appear in the system tray.
2. Open the Agent by clicking on the icon in the system tray.



!On **Debian 9**, click on the black line in the bottom right corner, if the tray icon is hidden.

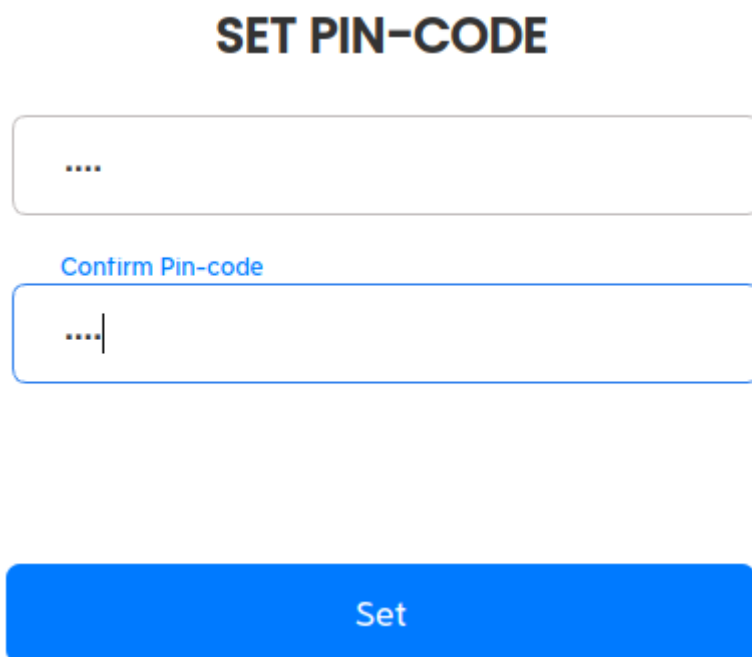


3. Enter your SafeDNS account credentials in the opened window.



The image shows a 'SIGN IN' window for SafeDNS. On the left is a blue sidebar with the SafeDNS logo, a gear icon, and the text 'Software is up date'. The main area is white and contains the title 'SIGN IN', a text input for 'Your_Email@gmail.com', a password input labeled 'Password' with the text 'Your_password' and an eye icon, and a blue 'Sign in' button.

4. Set up the security PIN that will be used later to restrict access to the Agent:



The image shows a 'SET PIN-CODE' form. It has a title 'SET PIN-CODE', a text input for the PIN (containing four dots), a label 'Confirm Pin-code', a text input for the confirmation (containing four dots and a cursor), and a blue 'Set' button.

5. Enter the PIN once again to sign in to the Agent:

PIN-CODE


Pin-code

Sign in

Agent Overview

The main window of the Agent. Here you can view your account information, current IP address, your Billing Plan, and Subscription expiration date.

Use the Policy menu to view and change the current filtering Policy.



Policy

System information

Debug

Software is up date

Account

Your IP adress
58.181.128.28

Billing Plan

Safe@Off...

Next payment

31 Dec. 2022

☒ DEFAULT


☐ MOBILE-PHONE

☐ KIDS

☒ Filtering enabled

The system information menu shows brief information about the Agent, current filtering policies, and the network interfaces. The information in this menu can be copied to the clipboard by clicking the "Copy to clipboard" button.



PolicySystem informationDebug

Software is up date

AccountYour IP address58.181.128.28


Billing PlanSafe@Off...Next payment31 Dec. 2022

Agent: SafeDNS Agent
Version: 1.3.0
Token: 50857813
UID: ffd80a34-97e1-4508-aaef-c956dcb9944c
DNS: 127.0.0.1
Protection is turned on: yes

Profiles:


Id	Active	Name
10303	*	Default
17356		MOBILE-PHONE
17357		KIDS

Network Interfaces:
1) lo
- Host Address | NetMask:
- 127.0.0.1 | 255.0.0.0
- ::1 | ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
- Hardware Address: 00:00:00:00:00:00
- Flags: IsUp IsRunning IsLoopBack
2) enp0s3



Copy to clipboard

The Debug menu displays the results of the diagnostic commands that are required in case of troubleshooting. To send the debug information to SafeDNS, click the "Send report" button.



PolicySystem informationDebug

Software is up date

AccountYour IP address58.181.128.28

Billing PlanSafe@Off...Next payment31 Dec. 2022


--- NSLOOKUP---
Server: 127.0.0.1
Address: 127.0.0.1#53

Non-authoritative answer:
black.safedns.com text = "{\"ip\": \"58.181.128.28\", \"t\": 650857813, \"p\": 10303}"

Authoritative answers can be found from:

--- DIG---

; <<>> DiG 9.16.15-Ubuntu <<>> txt black.safedns.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 20212
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0



Send report

Additional settings

To ensure the Agent was installed correctly, please navigate to the "**Settings**" tab in the [SafeDNS Dashboard](#) and scroll down to the bottom.

If you see the record with the Device name and your IP address, it means that the filtering is working.

DD Client				
<div>DD Client</div>				
DD Client	Policy	Since last update		
Default	Default			
95.95.114.171				

Agents				
<div>Agent</div>				
Device	OS	Policy	Last seen	
Default 11	(10.0.2.15)	debian 11	Default	18 hours ago

After that, you can adjust the filtering Policy according to your needs. You can select categories to block [here](#).

Don't forget to click the "Save changes" button.

SAFEDNS

English

Main

Settings

Categories

Allowlist

Denylist

Stats

Help

Categories

Default

Use the Allowlist only

Save changes

Recommended

Allow all

Block all

Close All

Security

Botnets

Parked Domains

Phishing

Virus Propagation

Illegal Activity

Academic Fraud

Child Sexual Abuse (Arachnid)

Child Sexual Abuse (IWF)

Crypto Mining

Drugs

German Youth Protection

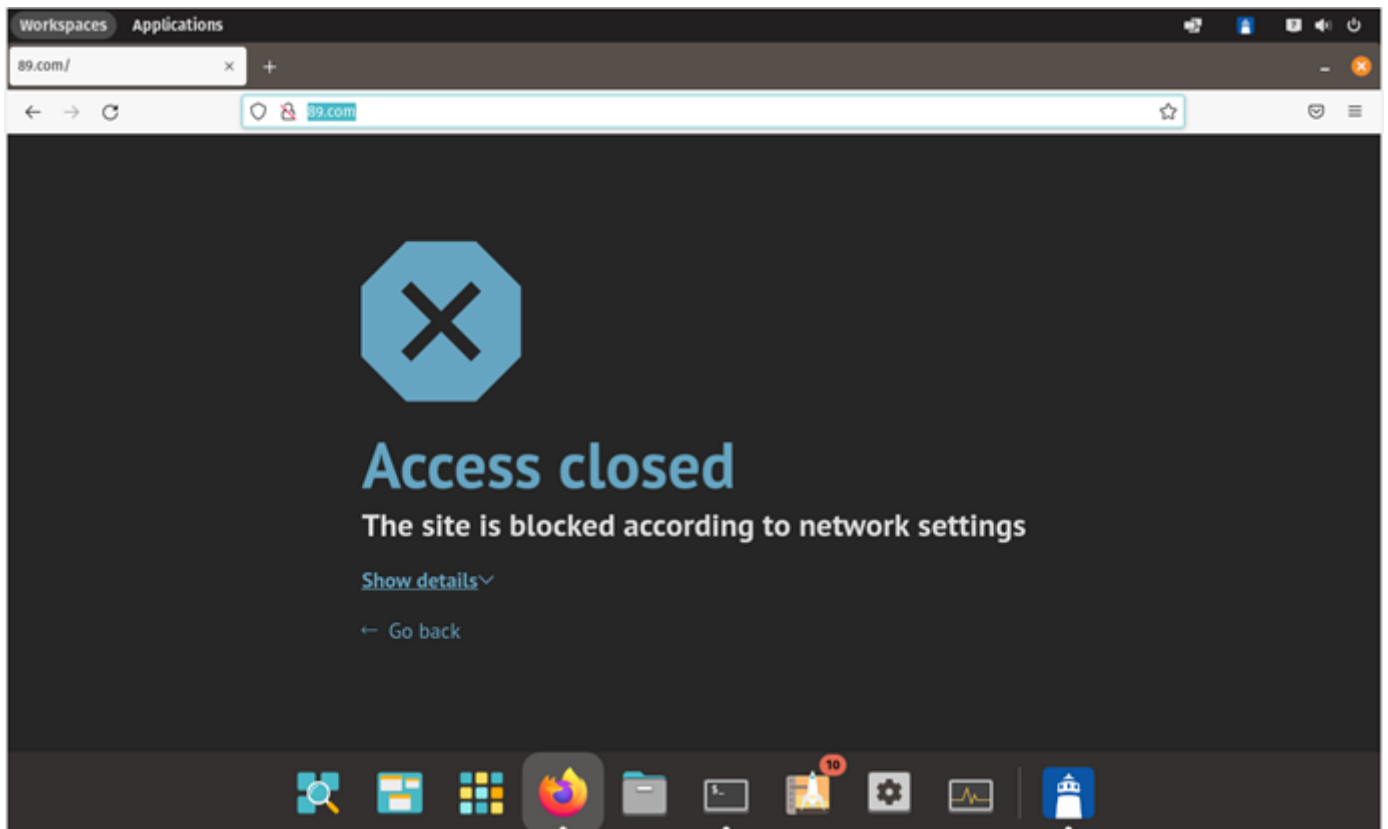
Hate & Discrimination

Proxies & Anonymizers

Tasteless

The setup is complete!

A blocked website will display an error message that the Access is closed:



If the filtering doesn't work according to your policy settings, [clear the cache of your browser](#).

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

Uninstallation

For the **.rpm** package, use the following command:

```
sudo rpm -e agentsafedns
```

For the **.deb** package, use the following command:

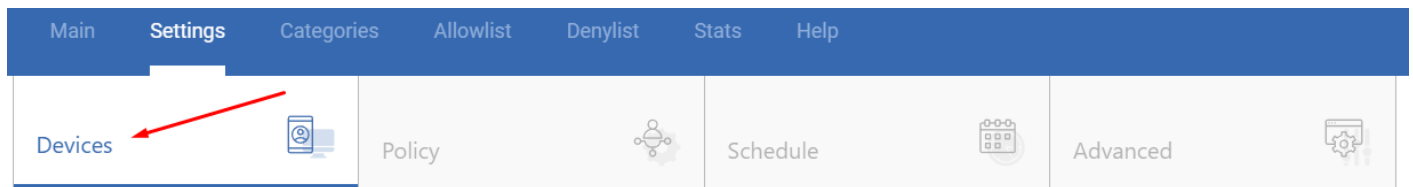
```
sudo apt-get remove agentsafedns
```

Enter **"y"** if prompted to confirm the Agent removal.

Linux Filtering Setup via OpenVPN

Please note, that this filtering option works via the third-party app OpenVPN. If you encounter any issues, please contact our Technical Support.

1. Open the SafeDNS Dashboard and navigate to **Settings > Devices**.



2. Scroll down to the VPN section, enter any name for a new VPN connection, and click Add.

Choose a filtering policy before adding a VPN connection, if needed.

A screenshot of the 'Add VPN' form in the SafeDNS dashboard. The form is titled 'VPN 0/5' in the top left corner. It has a light blue header bar. Below the header, there is a section titled 'Add VPN'. This section contains a text input field with the value 'Home Network', a dropdown menu with the value 'Default', and a purple 'Add' button. Below this section, there is a search bar with the text 'VPN' and a magnifying glass icon. At the bottom, there is a table with three columns: 'Name', 'Policy', and 'Certificate'. The 'Name' column contains the text 'List is empty'.

3. Upon creating the connection, two icons will appear in the "Certificate" column. One is for downloading the Certificate, and the other is for sending it by email. Press the "Cloud download" icon.

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

You can also change the filtering policy of the created VPN connection by clicking on the pencil icon to the right. Please note, that you don't need to redownload your VPN certificate on your mobile

device if you change its filtering policy.

Name	Policy	Certificate	
Home Network	Default		

Some Linux distributions have the OpenVPN application pre-installed. In this case, skip to **Step 5**.

4. Install the OpenVPN application on your device with the following command:

```
sudo apt install openvpn
```

5. Enter the administrator account password and approve the installation if prompted.

6. Copy the downloaded Certificate to `/etc/openvpn`

7. Start OpenVPN with the following command:

```
sudo openvpn --config /etc/openvpn/safedns-123456.ovpn
```

8. Enter the administrator account password if prompted. If the connection is established correctly, you will see the following notification:

Initialization Sequence Completed

Your Linux device is now filtered with the SafeDNS filtering policy.

You can check the OpenVPN connection with the ***ifconfig*** command. OpenVPN interface has the name ***tun***:

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.91.34.241 netmask 255.255.255.255 destination 10.91.34.242
    inet6 fe80::de1b:da21:5398:4ea4 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100
```

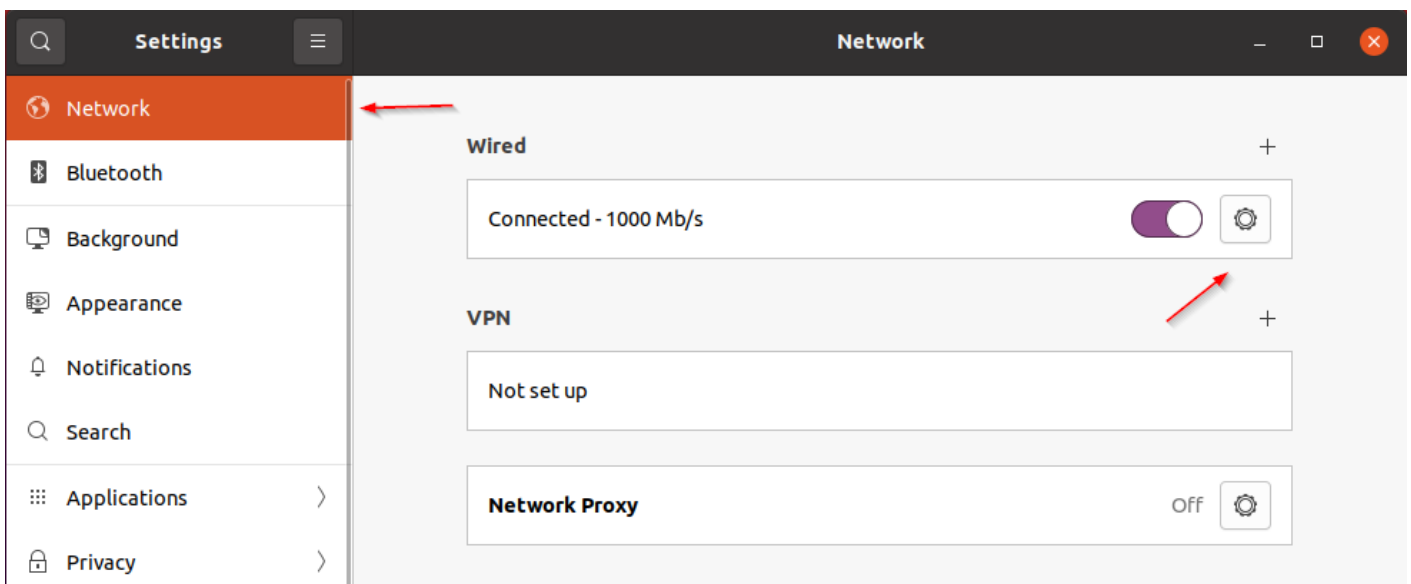
Please note that settings take 5-7 minutes to apply.
Stats and filtering status update every 10 minutes.

Linux DNS Setup

The first step is the same for both Static and Dynamic IP address configurations: change your system's DNS servers to SafeDNS addresses - **195.46.39.39** and **195.46.39.40**

If you configure the network through NetworkManager, it will be sufficient to add SafeDNS servers there.

1. Open the settings of the current Network Interface.



2. Add SafeDNS servers: **195.46.39.39** and **195.46.39.40**.

Please note, that servers should be separated by a comma.

Cancel

Wired

Apply

Details

Identity

IPv4

IPv6

Security

IPv4 Method

☒ Automatic (DHCP)

☐ Link-Local Only

☐ Manual

☐ Disable

☐ Shared to other computers

DNS

Automatic

195.46.39.39,195.46.39.40

Separate IP addresses with commas

Routes

Automatic

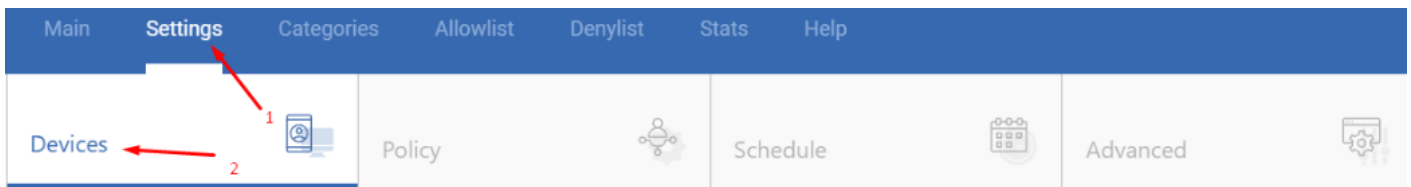
Address	Netmask	Gateway	Metric	

☐ Use this connection only for resources on its network

Otherwise, you need to find out which application is used for the network settings and add SafeDNS servers there.

Static IP address

Navigate to the SafeDNS **Dashboard > Settings** and copy your IP address in the "**Enter an IP address or DynDNS**" box. Click "**Add**".



Devices

Your IP address Copy IP address
[Redacted IP address]

IPv4 DNS-servers addresses
195.46.39.39 195.46.39.40

IPv6 DNS-servers addresses
2001:67c:2778::3939 2001:67c:2778::3940

IP addresses/DynDNS 0/3

Add IP address or DynDNS

Enter an IP-address or DynDNS Default Comment Add

Paste IP address Select filtering policy

IP address or DynDNS X Q

IP address/DynDNS Policy Comment

List is empty

Your Linux device is now filtered with the SafeDNS filtering policy.

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

Dynamic IP address

Install and configure **ddclient**.

ddclient package is shipped with most Linux distributions.

If your Linux distribution doesn't have ddclient, you can download it from [GitHub](#).

After ddclient is installed, you need to insert the next configuration in its config file (/etc/ddclient.conf or /etc/ddclient/ddclient.conf):

```
daemon=300
syslog=yes
ssl=yes
```

```
protocol=dyndns2  
server=www.safedns.com
```

```
use=web  
web=http://www.safedns.com/nic/myip
```

```
# Replace with your email and password for www.safedns.com  
login=you@yourmail.com  
password=your_password
```

```
# Enter any name for your device.  
# If you have several computers with dynamic IPs their names must differ.  
laptop
```

Reboot your device and start ddclient.

If the similar string is shown in the system logs (/var/log/syslog, /var/log/daemon.log or /var/log/messages), ddclient is successfully configured:

```
Aug 14 12:49:13 laptop ddclient[4105]: SUCCESS: updating laptop: good: IP address set to  
18.26.28.10
```

Your Linux device is now filtered with the SafeDNS filtering policy.

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