Getting started

General Questions and Service Basics

What are SafeDNS cloud solutions?

SafeDNS cloud solutions comprise a comprehensive suite of web filtering and security services designed for deployment across a wide range of infrastructures. These solutions include dedicated documentation for all existing cloud-based filtering tools, covering everything from individual device agents to complex enterprise-level network configurations.

The service is adaptable for home users, businesses, and educational institutions, offering specific configurations for routers, mobile devices, and desktop operating systems. By operating in the cloud, SafeDNS allows for centralized management of web access policies without the need for on-site hardware maintenance.

What is the SafeDNS Global Anycast Network?

The SafeDNS Global Anycast Network is a distributed infrastructure consisting of servers located throughout the world. This architecture is specifically designed to ensure fast service and high availability for users, regardless of their geographic location.

By using Anycast technology, the network routes DNS queries to the nearest available server, reducing latency and providing a seamless filtering experience. This global reach ensures that the cloud filtering solutions remain responsive and reliable on a worldwide scale.

How do I check what filtering category a specific domain belongs to?

SafeDNS provides a dedicated tool that allows users to check the category of any specific domain. This is useful for understanding why a site might be blocked or for verifying that a site is correctly classified under your existing filtering rules.

Where can I find a complete List of SafeDNS Categories for filtering?

A detailed List of SafeDNS Categories is provided within the documentation, which includes the ID, category name, and a description of what each category covers. For example, the list includes categories such as "NRD" for Newly Registered Domains, allowing users to make informed decisions when setting up their filtering policies.

The documentation also includes a List of AppBlocker apps, which provides descriptions for specific service-level blocking, such as "Facebook" under the Social networks category. This comprehensive categorization ensures that administrators can precisely control web access based on content and security risk.

Installation and Setup Compatibility

How do I install SafeDNS on my router?

To install SafeDNS on your router, you need to log into your SafeDNS Dashboard and add the public IP address or DynDNS to the IP/DynDNS table. After that, you can proceed with the router setup. For most standard routers like Asus, Unifi, Mikrotik, and Meraki, the setup involves a Static IP address configuration where you copy your IP into the dashboard settings.

Specific brands may have unique integration methods. For instance, Keenetic routers include SafeDNS as a built-in operating system component. Conversely, some routers like Comcast Xfinity have firmware that may intercept DNS, requiring specific instructions, while OpenWRT users can utilize a dedicated filtering module for more advanced control.

What are the typical setup steps for the router configuration?

The typical setup for the router is:

1. Adding an IP address or DynDNS in the SafeDNS Dashboard.
2. Setting up the router.
3. Checking if the filtering is working.
4. Setting up the filtering rules.

How do I install the SafeDNS Agent on my specific device (Windows, Mac OS, Linux)?

Each operating system has a dedicated installation path. For Windows, SafeDNS provides both a standard setup and an unattended installation option for mass deployment in enterprise environments. macOS users require version 14 (Sonoma) or newer to run the Agent.

For Linux, the Agent is compatible with several distributions, including **Debian, Ubuntu, PopOS, and CentOS**. Installation guides for all these platforms include step-by-step instructions, and some

platforms, such as Windows, offer video tutorials to assist with the deployment and setting configuration.

Which plans support the SafeDNS Agent?

The SafeDNS Agent is not available on all tiers. It is supported on the **Safe Family, Pro, and Pro Plus** billing plans. It is also available for those on archived Safe Home and Business plans.

My device does not support the SafeDNS Agent; can I still filter content?

Yes, if your device is incompatible with the SafeDNS Agent, you can use General Setup via OpenVPN. This method utilizes a third-party app to route your traffic through SafeDNS and is available for Windows, macOS, Linux, and mobile devices.

Alternatively, you can manually configure the DNS settings on your device or router. By changing the DNS server addresses directly in the network settings of your operating system (such as Chromebook OS or Android), you can achieve content filtering without the need for an installed agent.

How do I set up filtering for Android or iOS/iPad mobile devices?

For **Android**, users can install the SafeDNS App, which is a dedicated application that enables filtering on mobile devices. If you prefer not to use an app, you can manually change the DNS server settings on the device to point to SafeDNS.

For **iOS and iPad** devices in an enterprise setting, SafeDNS supports mass deployment through **MDM (Mobile Device Management) integrators**. This allows administrators to obtain an AuthKey from support and deploy the filtering application across many devices simultaneously.

What if I have a Dynamic IP address, like with Starlink or certain routers?

If your ISP provides a **Dynamic IP address**, you can still use the service by setting up DynDNS in the router or by using the ddclient software, which helps keep your IP updated with SafeDNS.

Users on the Starlink network, which has unique networking characteristics and dynamic IPs, have a dedicated setup guide to ensure compatibility. For those on basic plans where certain advanced features like NAT DNS are unavailable, using a Dynamic DNS service is the recommended way to maintain consistent filtering.

Policy Management and Filtering Features

How can I block all subdomains of a specific domain?

To block all subdomains of a certain domain, you should add the specific record to your **Denylist**. You must add the domain without the leading WWW to ensure the block is effective. For instance, if your goal is to block subdomains of the https://www.google.com domain, you would simply enter google.com into the Denylist.

What is NAT DNS, and is it included in my plan?

Network Address Translation over DNS (NAT DNS) is a specialized feature used for identifying and filtering traffic in specific network environments. However, this feature is not included in all service tiers; it is **not available for the Safe Home and Basic plans**.

How can I create a custom schedule for blocking content?

SafeDNS provides a Schedule feature that offers more granular control than standard filtering systems. While many systems utilize simple schedules that completely block internet access during set times, the SafeDNS system allows for **content filtering schedules**. This allows administrators to adjust what types of content are blocked at different times of the day without cutting off internet access entirely.

How do I configure the block page that users see when a website is filtered?

The **block page** is the landing page displayed to a user whenever they attempt to access a website that is restricted by your active filtering rules. The documentation includes a dedicated Block Page Setup guide to assist administrators in configuring this interface.

How can I use the same list of domains across multiple policies?

To avoid manually entering the same information multiple times, you can use the Allow/Denylists and Named Lists feature. This feature is specifically designed for situations where you need to **apply the same list of domains to different policies** across your network, streamlining the management of multiple user groups or filtering levels.

How can I prevent users from bypassing web filtering?

To maintain the integrity of your network policies, SafeDNS offers several Web Filtering Bypass Prevention recommendations. A primary recommendation is to **block the "Proxies & Anonymizers" category**, which prevents users from accessing external services designed to circumvent DNS-based filters.

Additionally, administrators should **block specific browser settings or "flags"** in Google Chrome and Mozilla Firefox that enable DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) directly within the browser. Because these browser-level settings can sometimes bypass system-wide DNS configurations, disabling them is a critical step in ensuring all traffic remains filtered.

Security and Advanced Configurations

How can I set up Encrypted DNS (DNS-over-HTTPS or DNS-over-TLS)?

SafeDNS provides a dedicated guide for configuring Encrypted DNS, specifically covering **DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT)**. This setup allows users to establish secure links using the Encrypted DNS feature provided by the service.

By using these encrypted protocols, users can significantly increase their **privacy and security** by preventing unauthorized third parties from eavesdropping on their DNS queries. However, administrators should also be aware that some browser-level DoH or DoT settings can be used to bypass filtering, and the documentation recommends blocking these settings in browsers like Firefox and Chrome to ensure network policies remain effective.

Why do I need the SafeDNS Root Certificate for HTTPS pages?

A Root certificate or SSL certificate is a fundamental component of modern website security. SafeDNS provides a root certificate specifically for use with **HTTPS pages** to ensure that encrypted web traffic is handled correctly within the filtering environment.

Troubleshooting and Diagnostics

How can I determine the filtering status of my device or network?

The most effective way to verify the filtering status is through the nslookup command. Because the SafeDNS service is DNS-based, using this diagnostic command allows you to see which DNS server is resolving your requests and whether the filtering is active on your specific device or network.

For users on mobile platforms, we suggest using the Network Analyzer Guide to troubleshoot internet and filtering issues on iOS and Android devices. If a domain is loading partially or failing to block as expected, additional network tools like **Wireshark** or **DNSQuerySniffer** can be used to perform a more granular analysis of the traffic.

How do I clear the DNS cache on my router or device?

The **DNS cache** refers to the temporary storage of information regarding previous DNS lookups that is maintained on a router, operating system, or web browser. When you make changes to your filtering settings or if a domain's IP address changes, your device might still use the old information stored in this cache, leading to inconsistent filtering results.

Clearing the DNS cache is a standard troubleshooting step that forces your device to request fresh information from the SafeDNS servers. This ensures that any updated policies, such as newly blocked or allowed categories, are applied immediately across your network and devices.

How can I contact SafeDNS Support?

SafeDNS provides **24/7 Support** to assist with any issues regarding the setup or management of your filtering services. You can reach the support team through a live chat available on any page of the safedns.com website and Dashboard, or by sending feedback directly from your **Personal Account** by navigating through the Dashboard to Help and then Feedback.

For more in-depth technical assistance, you can send an email to support@safedns.com. While you can also reach the team via phone, please be aware that complex troubleshooting often requires

running several diagnostic commands - such as nslookup to check filtering status - and sharing those results with a technician, which is more efficiently handled via text-based communication.

Enterprise and Business Setup

How do I deploy SafeDNS within an Active Directory environment?

Administrators must complete the SafeDNS AD Agent environment configuration, which involves preparing and installing the agent within the network. This setup is designed to work alongside **local resources**, ensuring that internal network traffic and external web filtering are managed effectively.

How do I deploy the SafeDNS Agent on multiple devices using MDM?

SafeDNS provides specialized packages for Windows and macOS devices designed for MDM integration.

When deploying to **iOS or iPad devices** in an enterprise setting, administrators must first **obtain a personal AuthKey**. This key is used during the **mass deployment** of the application via MDM integrators, followed by an initial setup process to enable the filtering on all managed devices.

Additionally, Windows users can utilize an unattended installation method to streamline mass deployment.

How do I migrate my existing content filtering settings from OpenDNS or Cisco Umbrella?

SafeDNS provides dedicated migration guides for businesses currently using OpenDNS or Cisco Umbrella. These guides provide step-by-step instructions on how to transition to SafeDNS while **keeping all of your existing settings and policies intact**. This ensures that your network remains protected according to your established rules during the switch to the new cloud filtering solution.

Can I white-label the SafeDNS service for my customers?

Yes, SafeDNS offers a White-Labeling edition for resellers who wish to provide the filtering service to their own customers under their own branding. To access this feature, you must first sign up for a **Reseller account** by contacting the SafeDNS Sales team at sales@safedns.com. Once your account is established, you can follow the provided documentation to deploy and manage the white-labeled service.