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.

Revision #3
Created 25 January 2026 19:06:16 by Val Redman
Updated 25 January 2026 19:49:51 by Val Redman