Deploying SafeDNS Endpoint Lite for macOS via MDM

This guide explains how to deploy **SafeDNS Endpoint Lite for macOS** to multiple macOS devices using an MDM solution.

The deployment consists of the following stages:

- Create the **Config.plist script file** on the target devices.
- Create and install the required configuration profiles on the target devices using the script and .mobileconfig files.
- Install the SafeDNS daemon on the target devices using the **safedns-daemon-20260515-1335-signed.pkg** package.
- Install the SafeDNS Endpoint Lite host and filtering module using the **SafeDNSMacProxy_2026-05-14_1744.pkg** package. (Provided from SafeDNS)

1. Installing the agent on client devices

Before deploying the agent at scale, complete the preparation steps below.

- Ask SafeDNS technical support (support@safedns.com) to enable the required features for your account.
- Obtain your **Base64-encoded AuthKey** from SafeDNS.
- Deploy the **create-conf.sh** script to the target devices according to **these instructions**.
- Create and install the two required configuration profiles on the target devices according to **this guide.**
- Deploy the SafeDNS daemon to the target devices according to the **SafeDNSDaemon installation guide**.

After these steps are complete, you can deploy the **SafeDNS Endpoint Lite agent**.

Install the agent package, which includes the host and filtering module, in the same way as the SafeDNS daemon package, using the attached installer package.

2. Uninstalling the agent

To remove SafeDNS Endpoint Lite from target devices:

- Add the **SafeDNS Uninstaller** script to **Scripts** in SimpleMDM according to the Running the SafeDNS Uninstaller script guide.
- Deploy the uninstaller script to the target devices in the same way as the **create-conf.sh** script.
- Remove the **SafeDNS configuration profiles**, the **SafeDNS Endpoint Lite agent**, and the **SafeDNS daemon** from the target devices.

> **IMPORTANT**
> After removing the agent and the daemon, **RESTART** each target device.
> The agent operates at the kernel level. After removal, some runtime records remain in the kernel until the device is restarted. If the device is not restarted, reinstalling the agent on the same device may cause errors or unstable behavior.

3. Additional information

Preventing DNS-over-HTTPS bypass in browsers

Advanced users **may try to bypass** system DNS filtering by configuring a custom DNS-over-HTTPS (DoH) resolver in Chromium-based browsers. The SafeDNS agent works with system DNS, so additional protection is required to reduce this risk.

> SafeDNS provides two layers of protection against this scenario:

1. Browser DNS policy configuration profile

Create and deploy the **Safedns_browser_dns_policy** custom configuration profile using the Safedns_browser_dns_policy.mobileconfig file.

This profile is deployed in the same way as the **SafeDNS_DNS_Proxy** custom configuration profile.

The profile restricts access to DNS-related settings in major browsers.
However, it does not cover all browsers. **Firefox is not included** in this policy.

2. Built-in DoH bypass detection

The SafeDNS filtering module includes a mechanism that detects attempts to bypass filtering through third-party DoH services and blocks those connections.

Known limitation

If an advanced user manually configures a **self-hosted DoH resolver** or another non-standard **custom DoH solution** in the browser, DNS filtering may not work as expected.

Revision #7
Created 22 May 2026 09:56:39 by Mickaël Gauthier
Updated 22 May 2026 19:22:23 by Mickaël Gauthier