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.

Revision #2
Created 2026-01-25 19:40:10 UTC by Val Redman
Updated 2026-01-25 19:42:36 UTC by Val Redman