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.

Revision #2
Created 2026-01-25 18:58:50 UTC by Val Redman
Updated 2026-01-25 19:06:04 UTC by Val Redman