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.

Revision #2
Created 25 January 2026 19:20:26 by Val Redman
Updated 25 January 2026 19:22:17 by Val Redman