

Comprendre la purge des données DNS dans les journaux

Table des matières

[Introduction](#)

[Puis-je purger les données DNS dans les journaux ?](#)

[Solution de contournement](#)

Introduction

Ce document décrit si vous pouvez purger les données DNS dans les journaux dans Cisco Umbrella.

Puis-je purger les données DNS dans les journaux ?

La purge ou la suppression des données DNS n'est actuellement pas possible dans Umbrella. La journalisation est activée ou non, mais il n'y a aucun moyen de purger les données du tableau de bord une fois qu'elles ont été collectées.

Solution de contournement

Vous pouvez choisir de désactiver complètement la journalisation ou de désactiver la journalisation du contenu, qui affiche uniquement les informations relatives à la sécurité et le nombre total de demandes. Cela se fait au cas par cas, selon les politiques.

What should this policy do?

Choose the policy components that you'd like to enable.

- ☒ **Enforce Security at the DNS Layer**
Ensure domains are blocked when they host malware, command and control, phishing, and more.
- ☒ **Inspect Files**
Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.
- ☒ **Limit Content Access**
Block or allow sites based on their content, such as file sharing, gambling, or blogging.
- ☒ **Apply Destination Lists**
Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.

ADVANCED SETTINGS

- ☒ **Enable Intelligent Proxy**
Gain visibility into threats, content, or apps by proxying web connections for risky domains.
 - ☐ **SSL Decryption**
Enabling SSL decryption allows the intelligent proxy to inspect traffic over HTTPS and block custom URLs in destination lists. Turning on SSL decryption allows HTTPS URL blocking.
 - ☐ **Enable IP-Layer Enforcement**
Gain visibility into threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for Roaming Computer identities.

ALLOW-ONLY MODE

- ☐ **Allow-Only Mode**
In this mode, access to sites needs to be specifically granted; otherwise connections will be blocked by default.

LOGGING

- ☐ **Log All Requests**
- ☐ **Log Only Security Events**
Log and report on only those requests that match a security filter or integration, with no reporting on other requests.
- ☒ **Don't Log Any Requests**

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.