

Información sobre la depuración de datos DNS en los registros

Contenido

[Introducción](#)

[¿Puedo purgar los datos DNS en los registros?](#)

[Solución Alternativa](#)

Introducción

Este documento describe si puede purgar los datos DNS en los registros de Cisco Umbrella.

¿Puedo purgar los datos DNS en los registros?

Actualmente no es posible purgar o borrar datos DNS en Umbrella. El registro está habilitado o no, pero no hay forma de purgar datos del Panel una vez que se han recopilado.

Solución Alternativa

Puede optar por desactivar completamente el registro o por desactivar el registro de contenido, que sólo muestra la información relacionada con la seguridad y Total de solicitudes. Esto se lleva a cabo política por política.

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**

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).