

Informazioni sulla rimozione dei dati DNS nei registri

Sommario

[Introduzione](#)

[È possibile eliminare i dati DNS nei registri?](#)

[Soluzione alternativa](#)

Introduzione

In questo documento viene descritto se è possibile eliminare i dati DNS nei registri in Cisco Umbrella.

È possibile eliminare i dati DNS nei registri?

Attualmente non è possibile eliminare o cancellare i dati DNS in Umbrella. La registrazione è abilitata o no, ma non è possibile eliminare i dati dal dashboard dopo la raccolta.

Soluzione alternativa

È possibile scegliere di disattivare completamente la registrazione o di disattivare la registrazione del contenuto, che mostra solo le informazioni relative alla protezione e le richieste totali. Ciò avviene sulla base di politiche specifiche.

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**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).