

Begrijp het opschonen van DNS-gegevens in de logs

Inhoud

[Inleiding](#)

[Kan ik de DNS-gegevens in de logboeken opschonen?](#)

[Tijdelijke oplossing](#)

Inleiding

In dit document wordt beschreven of u DNS-gegevens kunt opschonen in logs in Cisco Umbrella.

Kan ik de DNS-gegevens in de logboeken opschonen?

Het opschonen of wissen van DNS-gegevens is momenteel niet mogelijk binnen Umbrella. Logboekregistratie is ingeschakeld of niet, maar er is geen manier om gegevens van het Dashboard te verwijderen nadat deze zijn verzameld.

Tijdelijke oplossing

U kunt ervoor kiezen om de registratie volledig uit te schakelen of de inhoudsregistratie uit te schakelen, die alleen beveiligingsgerelateerde informatie en totale verzoeken toont. Dit gebeurt op beleidswijze basis.

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**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.