

Grundlegendes zum Löschen von DNS-Daten in den Protokollen

Inhalt

[Einleitung](#)

[Kann ich die DNS-Daten in den Protokollen löschen?](#)

[Problemumgehung](#)

Einleitung

In diesem Dokument wird beschrieben, ob Sie DNS-Daten in Protokollen in Cisco Umbrella löschen können.

Kann ich die DNS-Daten in den Protokollen löschen?

Das Löschen oder Löschen von DNS-Daten ist derzeit in Umbrella nicht möglich. Die Protokollierung ist entweder aktiviert oder nicht aktiviert, es ist jedoch nicht möglich, Daten aus dem Dashboard zu löschen, nachdem sie erfasst wurden.

Problemumgehung

Sie können die Protokollierung vollständig deaktivieren oder die Inhaltsprotokollierung deaktivieren, in der nur sicherheitsrelevante Informationen und Gesamtanforderungen angezeigt werden. Dies erfolgt auf der Basis einzelner Richtlinien.

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**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.