

ChromeOS SWG Web-Schutz funktioniert nicht und folglich keine Web-Protokolle In der Aktivitätssuche angezeigt

Inhalt

Problem

Für ChromeOS-Benutzer wurden keine Webprotokolle generiert, obwohl der SWG-Schutz (Secure Web Gateway) für die Organisation aktiviert zu sein schien. Die betroffenen ChromeOS-Endpunkte zeigten nur Schutz auf DNS-Ebene, ohne dass in der Oberfläche für die Aktivitätssuche Aktivitäten für die SWG-/Web-Protokollierung sichtbar waren. Bei Benutzern traten vollständige Abwesenheit von Web-Datenverkehrsprotokollen auf, während der SWG-Schutzstatus anzeigte, dass diese aktiviert waren.

Während der Untersuchung deckten die Diagnoseprotokolle wiederholt fehlgeschlagene Synchronisierungen mit dem Endpunkt `http://407.checkumbrella.com` mit HTTP 407-Fehlerantworten (Proxy-Authentifizierung erforderlich) auf. Der ChromeOS-Client/die ChromeOS-Erweiterung konnte sich nicht ordnungsgemäß mit dem Proxydienst authentifizieren, was eine ordnungsgemäße Aktivierung des SWG-Schutzes und die anschließende Generierung von Webprotokollen verhinderte.

Umwelt

- Sicherer Zugriff von Cisco
- ChromeOS-Endgeräte mit Cisco Secure Access-Client/Erweiterung
- Google Admin-Konsole für ChromeOS-Management

Auflösung

Das Problem wurde behoben, indem das Authentifizierungsschema der grundlegenden Authentifizierung für die Google-Verwaltungseinheit (OU) aktiviert wurde, die die betroffenen ChromeOS-Benutzer enthält, und indem ein Policy-Neuladen durchgeführt wurde, um den SWG-Schutz zu aktivieren.

Schritt 1: Protokollierung und Analyse

Erfassung der HAR-Daten (Überprüfung der Netzwerk- und Konsolenprotokolle) zur Ermittlung der Ursache des Synchronisierungsfehlers. Bei der Synchronisierung mit dem Cisco Secure Access-Service traten in den Protokollen wiederholt Authentifizierungsfehler auf.

Phase 2: Grundlegende Auth. für Google Admin-OU aktivieren

Navigieren Sie in der Google Admin-Konsole zur Organisationseinheit, die die betroffenen ChromeOS-Benutzer enthält, und aktivieren Sie das Authentifizierungsschema für Standardauthentifizierung. Dadurch kann sich der ChromeOS-Client bzw. die ChromeOS-Erweiterung mithilfe des Cisco Secure Access-Proxydiensts ordnungsgemäß authentifizieren.

Schritt 3: Neuladen und Überprüfen von Richtlinien

Führen Sie nach der Aktivierung von Basic Auth ein Richtlinien-Neuladen auf den betroffenen ChromeOS-Geräten durch. Überprüfen Sie den Schutzstatus, um sicherzustellen, dass der SWG-Schutz aktiviert wird. Der SWG-Schutz muss jetzt als aktiv und nicht nur als Schutz auf DNS-Ebene angezeigt werden.

Schritt 4: Validierung

Testen Sie die Aktivitäten beim Surfen im Internet von den betroffenen ChromeOS-Benutzern, und stellen Sie sicher, dass jetzt Webprotokolle generiert werden und in der Oberfläche für die Aktivitätssuche angezeigt werden. Die Protokolle müssen eine ordnungsgemäße Prüfung des Web-Datenverkehrs und die Protokollierung über den SWG-Service enthalten.

Ursache

Für den ChromeOS-Client bzw. die ChromeOS-Erweiterung wurde das Authentifizierungsschema für die grundlegende Authentifizierung für die Google Admin-Organisationseinheit mit den betroffenen Benutzern deaktiviert. Ohne Aktivierung der grundlegenden Authentifizierung konnten die ChromeOS-Geräte sich nicht ordnungsgemäß mit dem Cisco Secure Access-Proxydienst authentifizieren, was zu HTTP 407-Fehlern (Proxy-Authentifizierung erforderlich) während der Synchronisierungsversuche führte. Dadurch wurde verhindert, dass der SWG-Schutz ordnungsgemäß aktiviert wurde. Die Geräte wurden auf den reinen DNS-Schutz zurückgesetzt, und die Erstellung von Webprotokollen wurde verhindert.

Verwandte Inhalte

- [Fehlerbehebung und Erfassung grundlegender Informationen für Cisco Secure Access](#)
- [Cisco Secure Access ChromeBook-Client](#)
- [Technischer Support und Downloads von Cisco](#)

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.