

ChromeOS SWG Web Protection not Working and Consecutively no Web Logs Show up in Activity Search

Contents

Issue

Web logs were not being generated for ChromeOS users despite Secure Web Gateway (SWG) protection appearing to be enabled for the organization. The affected ChromeOS endpoints were only showing DNS-level protection with no SWG/web logging activity visible in the Activity Search interface. Users were experiencing a complete absence of web traffic logs while the SWG protection status indicated it was enabled.

During investigation, diagnostic logs revealed repeated sync failures to the endpoint <http://407.checkumbrella.com> with HTTP 407 (proxy authentication required) error responses. The ChromeOS client/extension was unable to properly authenticate with the proxy service, preventing proper SWG protection activation and subsequent web log generation.

Environment

- Cisco Secure Access
- ChromeOS endpoints with Cisco Secure Access client/extension
- Google Admin console for ChromeOS management

Resolution

The issue was resolved by enabling the Basic Auth authentication scheme for the Google Admin Organizational Unit (OU) containing the affected ChromeOS users and performing a policy reload to activate SWG protection.

Step 1: Log Collection and Analysis

Collected HAR capture (review Network and Console logs) to identify the root cause of the sync failure. The logs showed repeated authentication failures when attempting to sync with the Cisco Secure Access service.

Step 2: Enable Basic Auth for Google Admin OU

In the Google Admin console, navigate to the Organizational Unit containing the affected ChromeOS users and enable the Basic Auth authentication scheme. This allows the ChromeOS client/extension to properly authenticate with the Cisco Secure Access proxy service.

Step 3: Policy Reload and Verification

After enabling Basic Auth, perform a policy reload on the affected ChromeOS devices. Verify that SWG protection becomes active by checking the protection status. The SWG protection must now show as active instead of only DNS-level protection.

Step 4: Validation

Test web browsing activity from the affected ChromeOS users and confirm that web logs are now being generated and visible in the Activity Search interface. The logs must show proper web traffic inspection and logging through the SWG service.

Cause

The ChromeOS client/extension had the Basic Auth authentication scheme disabled for the Google Admin Organizational Unit containing the affected users. Without Basic Auth enabled, the ChromeOS devices could not properly authenticate with the Cisco Secure Access proxy service, resulting in HTTP 407 (proxy authentication required) errors during sync attempts. This prevented the SWG protection from activating properly, causing the devices to fall back to DNS-only protection and preventing web log generation.

Related Content

- [Troubleshoot and Collect Basic Information for Cisco Secure Access](#)
- [Cisco Secure Access Chromebook Client](#)
- [Cisco Technical Support & Downloads](#)