Secure Access File Event Logs Missing from SIEM After License Change

Contents

Issue

File Event logs stopped being received by the SIEM from AWS S3 storage while DNS logs continued to be delivered successfully. The File Event data connectors displayed a "disconnected" icon in the SIEM interface. The logs that stopped appearing were identified as DLP/IPS-related File Event records. DNS-layer logs remained functional throughout the issue period.

The environment was using both Umbrella and Secure Access during migration, with logs sent to the same AWS bucket. Keys had been rotated and were confirmed to be working properly. The schema version was noted to be at version 10 while version 16 was available.

Environment

- Cisco Secure Access organization with both Umbrella and Secure Access configurations
- AWS S3 storage integration for log export
- Microsoft Sentinel SIEM platform
- Schema version 10 in use (version 16 available)
- Secure Access license changed from Advantage to Essentials on June 23, 2026
- File Event logs last observed on June 24, 2026

Resolution

The investigation revealed that the File Event logs were related to DLP/IPS functionality, which requires specific licensing features. The root cause was identified through the next analysis.

Step 1: Traffic Analysis

Check the **Activity Search** in **Secure Access** to confirm traffic patterns:

1.- Navigate to **Activity Search** and filter for web traffic or malicious disposition events. The analysis showed DNS traffic was present but no web traffic events were visible for the last 30 days, and no rules with File Inspection enabled were identified.
2.- **Traffic Flow > Logs on the CSA report > S3 bucket - SIEM**.

Step 2: License History Review

1.- Review the license history in Secure Access to identify any changes that align with the timing of the File Event log stoppage.

2.- Navigate to **Secure Access > Admin > Subscription** to view the current license level and features summary.

The investigation showed that the Secure Access license changed from Secure Access Advantage to Secure Access Essentials on June 23, 2026, which aligned with the timing when File Event logs stopped appearing.

Step 3: Feature Verification

Verify which features are included in the current license level. DLP and IPS functionality, which generates File Event logs, is not included in the Secure Access Essentials license tier.

Step 4: Confirmation and Root Cause

The timing of the license change perfectly matched when File Event logs stopped appearing. Since DNS-layer logging remained functional and was the primary requirement, the case was resolved with the understanding that File Event logs would not be available under the current Essentials license.

Cause

The File Event logs stopped being generated due to a license change from Secure Access Advantage to Secure Access Essentials on June 23, 2026. File Event logs are associated with DLP and IPS functionality, which are not included in the Essentials license tier. The license downgrade removed access to file inspection capabilities that generate these specific log types.

Related Content

- Cisco Technical Support & Downloads