

Secure Access DLP File Size Rules without Data Classification Do Not Generate Monitor Events for Text Files

Contents

Issue

A Cisco Secure Access Web DLP policy configured with file size criteria only (no Data Classification) does not generate DLP monitor events for .txt file uploads, while the same policy correctly triggers monitor events for other file types such as .xlsx, .png, and .pdf files. The affected policy **Senior Management Policy - Web** is configured with:

- File Control with custom file size between 1KB and 49MB
- No Data Classification criteria
- Action set to Monitor

Testing revealed that:

- TXT file uploads do not appear in DLP events when **Action = Monitor**.
- The same TXT files generate DLP events correctly when **Action = Block**.
- Activity logs show all file uploads including TXT files.
- Other file formats (PNG, PDF, XLSX) generate DLP events as expected with Monitor action.

Additionally, when no Data Classification is configured in DLP rules, the logged DLP events always show **Medium** severity regardless of the configured rule severity setting.

Environment

- Cisco Secure Access (formerly Cisco Umbrella)
- DLP (Data Loss Prevention) Web policies

- Internet Access policies with HTTPS decryption enabled
- File upload testing performed via web applications

Resolution

This behavior is undocumented but expected by design. MIME types like text/plain are bypassed from DLP monitoring when using file size-only criteria with Monitor action to prevent log overload. The development team confirmed this is intentional behavior that is not externally documented.

Workaround Options

Option 1 (Recommended): Add Data Classification

Add any broad Data Classification criteria to the DLP rule while keeping **Action = Monitor**.

This restores:

- TXT file DLP event generation
- Correct severity handling based on rule configuration

Option 2: Change Action to Block

Change the rule action from Monitor to Block. This generates DLP events for TXT files, but also enforces blocking which can not be desired for monitoring-only use cases.

Lab Testing Results

Comprehensive lab testing confirmed the behavior patterns.

Test Scenario 1: DLP rule with Data Classification and File Size (1KB-49MB), Action = Block

- TXT file with PII: Blocked and logged
- PDF file: Blocked and logged
- TXT file without PII: Allowed (expected)
- PNG with PII: Allowed (expected based on classification)

Test Scenario 2: DLP rule with File Size only (no Data Classification), Action = Block

- All file types (TXT, PDF, PNG): Blocked and logged
- Severity shows as **Medium** despite rule configured as **Low**

Test Scenario 3: DLP rule with File Size only (no Data Classification), Action = Monitor

- TXT files: Allowed but NOT logged in DLP events
- PDF and PNG files: Allowed and logged in DLP events
- Activity logs show all uploads including TXT files

Cause

This is intentional but undocumented behavior in Cisco Secure Access DLP. The system bypasses DLP event logging for text/plain MIME types when using file size-only rules with Monitor action to prevent excessive log generation. The behavior is action-dependent and MIME-type specific:

- Monitor action with file size-only criteria: TXT files bypassed from logging
- Block action with file size-only criteria: TXT files logged normally
- Any action with Data Classification present: TXT files logged normally

The severity issue occurs because DLP events derive severity from Data Classification metadata rather than

rule settings when operating in content-aware mode. Without Data Classification, the system defaults to "Medium" severity regardless of the configured rule severity.

Related Content

- [Cisco Secure Access DLP File Size Configuration](#)