Configure DLP Fail-Closed Behavior Blocking User Actions During Cloud Connectivity Loss

Contents

Issue

A user with the Endpoint DLP (EDLP) module installed was experiencing blocking from printing and copying to network file shares, despite not being included in any configured EDLP rules. All existing EDLP rules were configured in MONITOR mode with only 3 specific users included in those rules. The affected user was encountering unexpected block actions for print operations and file share copy operations even though they were not intended to be subject to EDLP enforcement.

During troubleshooting, it was determined the blocking occurred when EDLP cloud connectivity was unavailable, causing the system to apply fail-closed behavior as a fallback mechanism. The user experienced denial of printing and network share access during periods when the EDLP client did not establish connectivity to the cloud service for policy verdicts.

Environment

- Cisco Endpoint DLP module version 1.5.0.292
- Cisco Secure Access/Secure/Data Loss Prevention portal management
- Multiple EDLP rules configured in MONITOR mode
- Network share channel configured with fail-closed behavior
- DNS resolution changes affecting client network connectivity

Resolution

The resolution involved understanding and explaining the EDLP fail-closed behavior and its application during cloud connectivity loss:

Root Cause Analysis

Analysis of the DART bundle and EDLP logs revealed that EDLP applied a deny fallback because the network share channel was configured as fail-closed. At the time of the blocking incidents, EDLP cloud connectivity was unavailable due to DNS resolution changes on the client network, preventing the system from obtaining policy verdicts from the cloud service.

Fail-Closed Behavior Explanation

The fail-closed policy was applied to the user's system because the EDLP module was installed, regardless of whether the user's identity was included in any specific EDLP rule. The fail-open/fail-closed state is a global setting provisioned in the DLP Policy configuration, and the channel configuration is applied based on that global setting.

Connectivity Recovery

The issue resolved automatically once DNS stability was restored on the client network, allowing the EDLP client to re-establish connectivity to the cloud service. No manual intervention was required once the underlying network connectivity issue was resolved.

Conditions Causing Fail-Closed Behavior

These conditions can trigger EDLP fail-closed behavior:

- DNS resolution issues
- Network outages
- Switching between networks
- Any condition that prevents end-to-end connection between the client and cloud service

Cause

The blocking behavior was caused by EDLP's fail-closed configuration for the network share channel. When

the EDLP client lost connectivity to the cloud service due to DNS resolution changes, it cannot obtain policy verdicts and therefore enforced the configured fail-closed behavior as a security fallback mechanism. This occurred regardless of whether the user was explicitly included in any EDLP rules, as the fail-closed setting applies globally to all systems with the EDLP module installed when cloud connectivity is unavailable.

Related Content

- Cisco Technical Support & Downloads