

瞭解Umbrella LA版本的阻止密碼保護檔案上傳DLP功能

目錄

[簡介](#)

[背景資訊](#)

[如何阻止受密碼保護的檔案上傳？](#)

[如何打包阻止密碼保護檔案上傳？](#)

[如何訪問此功能？](#)

[是否可在Umbrella控制面板中啟用或禁用此功能？](#)

[在哪裡可以找到支援的檔案型別清單？](#)

簡介

本檔案介紹封鎖密碼保護檔案上傳DLP功能的有限可用性(LA)。

背景資訊

阻止受密碼保護的檔案上傳是防止資料丟失的重要措施，因為DLP解決方案無法檢查受密碼保護的檔案。

如何阻止受密碼保護的檔案上傳？

啟用此功能後，阻止密碼保護檔案上傳將應用於使用即時DLP（如內聯）規則配置的任何目標。

如果要阻止所有受密碼保護的檔案上傳，必須至少有一個在Destination規則條件中設定「All Destinations」的Realtime DLP規則。

反之，如果只想阻止受密碼保護的檔案上傳到特定目標，則必須確保它們沒有在「目標」規則條件中設定「所有目標」的「即時DLP規則」。



附註：即時DLP規則中的目標排除不適用於阻止密碼保護檔案上傳，並且仍然適用於所有目標。

如何打包阻止密碼保護檔案上傳？

包括DLP (即SIG-A和DLP-addon) 的所有Umbrella軟體包均提供此功能。

如何訪問此功能？

請開啟支援票證，考慮將其註冊到此有限可用性功能。

是否可在Umbrella控制面板中啟用或禁用此功能？

現在不行。一旦我們將您註冊到LA計畫，我們將代表您啟用它。

在哪裡可以找到支援的檔案型別清單？

此處提供了[阻止密碼保護檔案上載所支援的檔案型別清單](#)，並且可與LA客戶共用。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。