將檔案檢查器配置為允許受密碼保護的檔案和其他非惡意檔案

目錄

簡介

本文檔介紹如何防止非惡意檔案被檔案檢查阻止。

問題

在某些情況下，啟用「檔案檢查」會阻止非惡意檔案。這些檔案型別包括：

- 受密碼保護的檔案
- 可能有害的應用程式（已損壞）檔案

這些檔案被Umbrella阻止，因為防病毒工具無法對其進行解壓縮和掃描。受密碼保護的檔案可能在「Protected File」（受保護檔案）類別下被阻止。損壞的檔案可能包括包含加密內容、無法提取的存檔內容、無效的壓縮資料或無效的存檔標頭，或者只是以不受支援的格式壓縮或存檔的檔案。雖然這些檔案可能是非惡意的，但出於預防考慮，Umbrella預設會阻止這些檔案，因為無法掃描這些檔案。

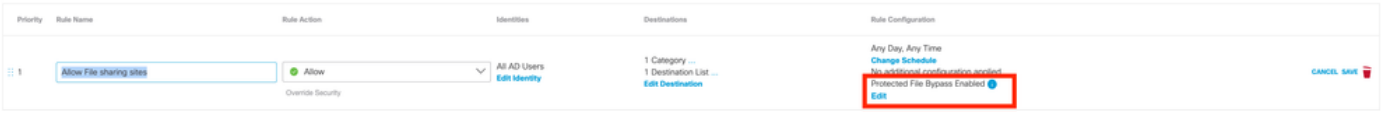
解決方案

如果您知道某個非惡意檔案由於上述原因之一而被阻止，可以通過允許受保護檔案來解決此問題。現在可以在全域性級別或在單個Web規則中更改阻止受保護檔案的行為。

- Rule(Recommended)- Allow protected files for an identity and/or destination。 如果要信任來自特定目標的受保護檔案，或希望覆蓋單個使用者/組的行為，請執行此操作。
- 全域性 — 允許所有規則/規則集中的所有使用者使用受保護檔案。 如果您接受下載受保護檔案的風險，並寧願選擇此選項，而不願承擔進行更精細的例外處理的管理負擔，請執行此操作。

Rule

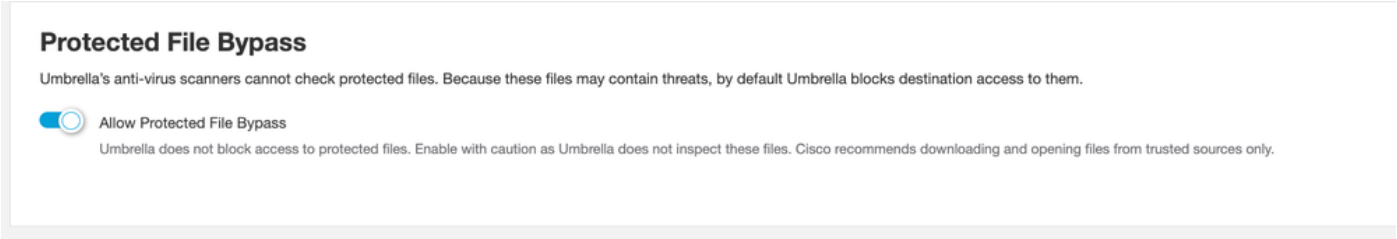
通過在Policies > Web Policies頁面上編輯Web規則可以更改此功能。



10588971481748

全域性

可在Policies > Web Policies > Global Settings中更改此功能。

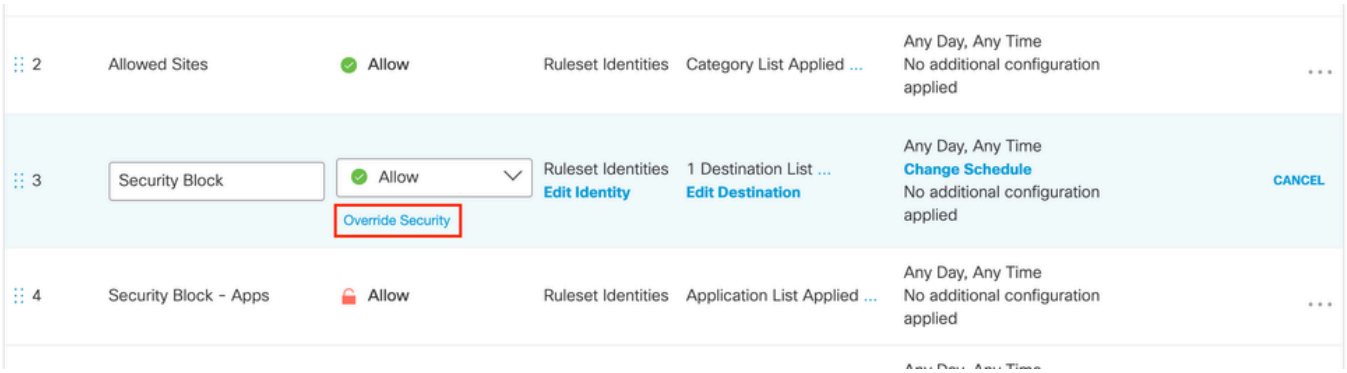


10589018672020

替代解決方案

還可以使用任何Web策略中的Override Security選項繞過檔案檢查問題。此選項必須謹慎使用，因為它禁用了所有其他安全設定，包括阻止惡意檔案。

- 對於受保護的檔案，請改用本文檔中介紹的解決方案之一。
- 只有在您完全信任目標且沒有其他解決問題選項的情況下，才使用此選項。
- 對於防病毒誤報，在實施任何變通方法之前，先從Cisco Talos中確認檔案是乾淨的。



Screen_Shot_2021-10-07_at_2.59.04_PM.png

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）。