

Umbrella控制面板：新功能和檔案檢測

目錄

[簡介](#)

[太好了，我該如何利用檔案檢查呢？](#)

[啟用檔案檢查](#)

[測試檔案檢查](#)

[檔案檢查報告](#)

[我怎麼能告訴你我的想法？](#)

簡介

本文檔介紹新的Umbrella控制面板。

注意到您的Umbrella控制面板有任何不同之處嗎？我們很高興地宣佈，我們正在啟動將人員轉移到一組新的很棒的Umbrella功能的過程。我們介紹的第一個功能是檔案檢測。檔案檢查會掃描您的身份下載的檔案，以檢視它們是否包含惡意代碼，如果包含惡意代碼，則會將其阻止。

為了幫助您利用此新功能，我們還發佈了新的和更新的安全報告和新的策略建立體驗。這是我們為未來版本設計的幾項功能之一，這些版本旨在提升我們的智慧代理基礎設施，以便為我們的使用者提供更多基於雲的安全性。

這些功能正在逐步向我們的客戶推出。如果您在儀表板中收到有關這些功能的警報，則表明您已擁有這些功能！如果您希望率先採用這些功能，請聯絡umbrella-support@cisco.com。

檔案檢查功能僅適用於具有Umbrella Insights或Umbrella Platform程式包的客戶機。按一下此處閱讀有關程式包的詳細資訊，如有問題，請聯絡您的思科客戶代表。

太好了，我該如何利用檔案檢查呢？

策略嚮導允許您在摘要頁面中或在建立新策略時啟用「檔案檢查」。

在報告端，Umbrella控制板的「報告」導航部分已更新，以便您可以輕鬆找到我們的新報告和更新報告。讓我們詳細介紹如何啟用該功能並檢視一些報告。

啟用檔案檢查

檔案檢查是智慧代理的一項功能，它通過新增掃描檔案以查詢可疑域上託管的惡意內容來擴展其範圍和功能。可疑域既不可信，也不知道是惡意的，它被列在我們的「灰色清單」中。

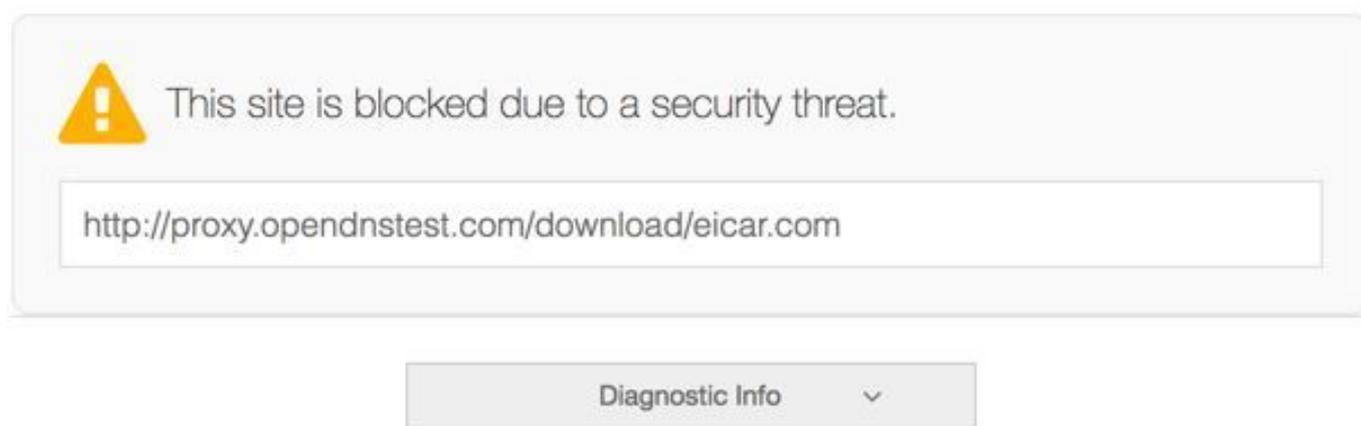
使用Umbrella策略嚮導，檔案檢查易於實施。只需導航到Policies > Policy List，然後展開策略或點選+(Add)圖示建立新策略。在策略嚮導中，確保在摘要頁面上啟用檔案檢查，或在啟用智慧代理後（在「高級設定」下），從新策略中確保選中「檢查檔案」。有關此功能的完整文檔，請訪問以下網址：<https://docs.umbrella.com/deployment-umbrella/docs/file-inspection>

我們建議啟用SSL解密以充分利用此功能。

測試檔案檢查

從已在啟用了檔案檢查的策略中註冊的裝置：

1. 瀏覽至<http://proxy.opendnstest.com/download/eicar.com>。
2. 出現一個類似此的阻止頁面：



檔案檢查報告

為了幫助更好地瞭解被阻止的內容（以及何時、為何和如何），我們更新了Umbrella中的某些報告，包括修改後的安全活動報告：

- **安全概述報告**
通過圖表和圖表可以輕鬆讀取網路活動的快照。您可以快速檢視您的身份資訊及其流量發生的情況，說明問題可能發生在何處。在此處瞭解更多[資訊](#)。
- **安全活動報告**
突出顯示由Umbrella威脅情報標籤（但不必阻止）的安全事件。其中包括通過智慧代理過濾的安全事件和檔案檢查。此報告在顯示被阻止的內容、原因和方式方面尤為重要。在此處瞭解更多[資訊](#)。
- **活動搜尋報表**
幫助您從各種身份中查詢每個DNS、URL和IP請求的結果，按降序日期和時間排序。此報告列出選定時間段Umbrella內的所有活動，使用過濾器，您可以縮小搜尋範圍，只檢視希望檢視的內容。在此處瞭解更多[資訊](#)。

而且，通過我們最新更新的導航，這些報告也很易於訪問！只需展開左側選單窗格，然後從儀表板中的任何其他位置直接跳轉到任何報表。

我怎麼能告訴你我的想法？

我們很想聽聽您對這些新功能的想法。如有任何問題或意見，我們想聽聽您的意見！將您的反饋傳送至umbrella-support@cisco.com，並包含儘可能多的詳細資訊。例如，螢幕截圖、您使用的瀏覽器、您的作業系統以及您使用這些功能的場景。

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）。