

排除HSTS和固定證書錯誤

目錄

[簡介](#)

[證書錯誤](#)

[可能的解決方案](#)

[策略管理和漫遊客戶端](#)

[忽略證書異常錯誤（僅適用於Windows的Chrome）](#)

[適用於Mac OS X的Firefox、Safari和Chrome](#)

[Internet Explorer](#)

簡介

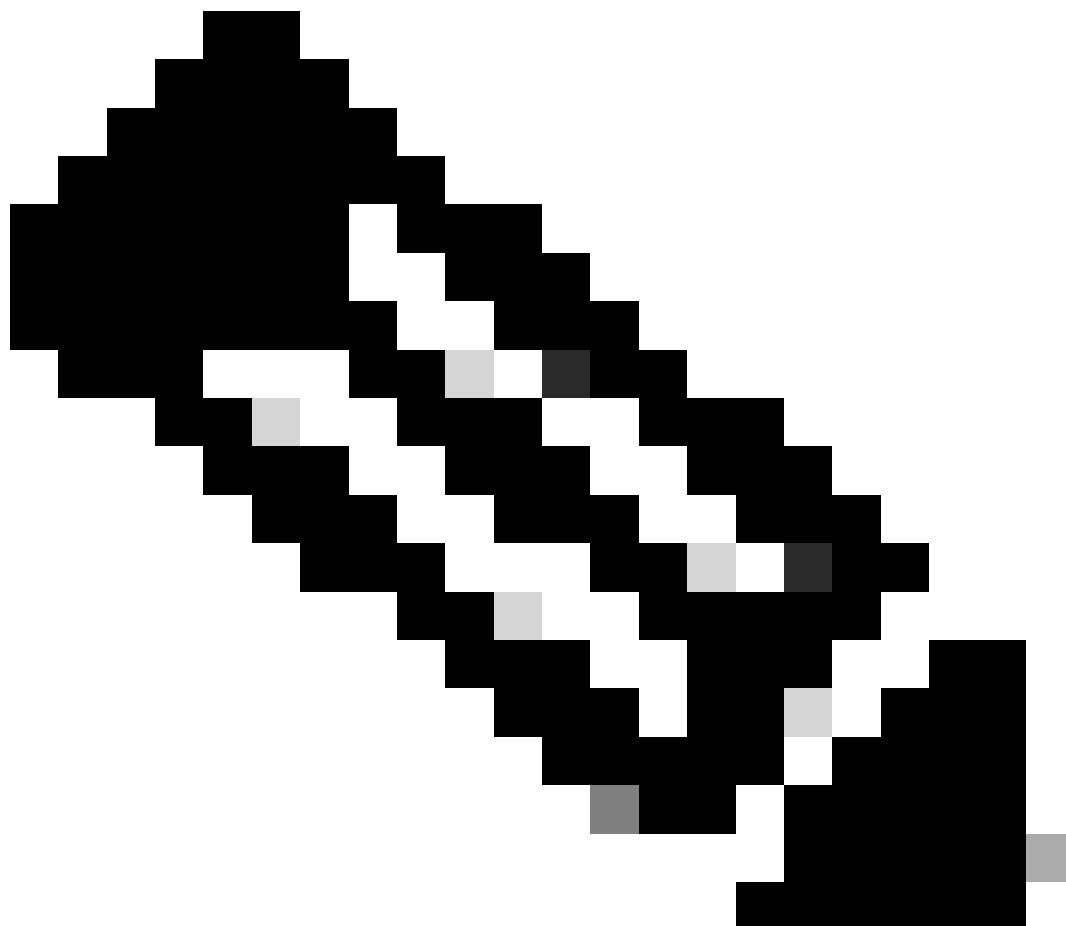
本文描述如何清除無法繞過的「您的連線不受信任/非私有」證書錯誤。

證書錯誤

當出現*.opendns.com或*.cisco.com的憑證錯誤時，但無法根據Cisco Umbrella檔案[管理Cisco Umbrella根憑證](#)中所述新增憑證例外來繞過，請使用以下步驟允許清除憑證錯誤。

如果無法通過新增例外來繞過憑證錯誤，則這是因為在現代瀏覽器中實作HTTP嚴格傳輸安全(HSTS)或預先載入憑證固定功能所致。某些瀏覽器和某些網站之間的通訊方式包括使用HTTPS的要求，並且不可能出現旁路或異常。當HSTS對網站處於活動狀態時，針對HTTPS頁面的這種額外安全性會阻止Umbrella阻止頁面和繞過阻止頁面機制工作。

因此，無法通過[Block Page Bypass](#)(BPB)訪問相關頁面（事實上，Bypass螢幕可能甚至不會顯示）。這些方法可能允許訪問BPB登入，但在登入後，證書錯誤會重新顯示並拒絕訪問。如果您在Google Chrome、Mozilla Firefox、Safari中看到無法繞過的證書錯誤，並且您正在嘗試訪問繞行登入，請檢視本文的其餘部分。



附註：針對此問題的解決方案現已面世，該解決方案易於管理，且適用於所有站點。

因此，此資訊仍然適用，但是現在可通過永久解決方案來解決。嘗試通過Cisco Umbrella文檔安裝思科根CA：[管理思科Umbrella根證書](#)

重要事項：如果域在HSTS固定清單上，則無法新增異常，因為如果您正在運行Chrome、Safari或Firefox(Internet Explorer(IE)不受影響)，則清單實際上是不可繞行的。「阻止頁面繞行」不適用於此類站點。有關這三種瀏覽器使用HSTS的服務的完整清單，請檢視[Google Chromium Code Search](#)。此清單中值得注意的服務包括：

- Google (以及Google資源，例如Gmail、Youtube或Google Docs)
- 收存箱
- 推特
- 臉書

如果這為您或您的使用者造成了問題，並且您希望看到對Block Page Bypass的更改以幫助緩解此問題，請傳送電子郵件至umbrella-support@cisco.com或您的客戶經理提交功能請求。我們的產品

管理和工程團隊意識到證書和阻止頁面繞行存在困難，正在測試此功能的替代重新設計。

可能的解決方案

有幾種方法可以解決這些問題。首先，這些部分演示如何使用更精細的策略來解決此問題。其次，您可以使用瀏覽器配置，但這些配置與受此問題影響的瀏覽器的子集無關。

策略管理和漫遊客戶端

您的網路配置或可接受的使用率(HR)策略可能存在問題，會阻止此解決方案的實施。如果僅允許使用者在特定時間（例如在午休期間）訪問這些域，策略管理不是有效的解決方案。Umbrella不能為我們的服務提供一個基於時間的策略應用程式，因此僅允許使用者始終訪問站點可能會出現問題。在共用電腦（如公共終端）上，Umbrella漫遊客戶端無法區分使用者，也不能輕鬆允許正確的人員使用正確的域。

在考慮非粒度標識（如站點或網路）時，策略管理效果不佳，除非管理員願意為該網路的所有使用者授予相同的訪問許可權。如果策略管理應用於允許訪問站點的使用者子集，而網路的其他部分則無法訪問，並且通過在他們的電腦上安裝漫遊客戶端並應用正確的策略層次結構來挑出這些使用者，則策略管理效果最佳。



附註：思科於2024年4月2日宣佈Umbrella漫遊客戶端壽命終止。Umbrella漫遊客戶端的上次支援日期為2025年4月2日。思科安全客戶端中目前提供所有Umbrella漫遊客戶端功能。思科僅提供思科安全客戶端的未來創新。我們建議客戶立即開始計畫和安排遷移。有關如何從Umbrella漫遊客戶端遷移到Cisco安全客戶端的指導，請參閱[此知識庫文章](#)。

正確的策略管理是此問題的最佳解決方案，因為瀏覽器首先不會收到失敗的驗證響應。如果允許某些使用者訪問他們通常需要使用阻止頁面繞過來訪問的站點，則可以改為為這些使用者配置單獨的策略，並將允許他們使用的域新增到「允許清單」中。由於使用者的請求從未被阻止，因此瀏覽器從未收到來自證書不匹配的域的請求。您可以使用[Umbrella Roaming Client](#)傳遞這些特定策略。這表示您正在將特定域放入允許清單中，以便特定使用者在一天中的任何時候可以解決這些錯誤。



附註：Umbrella漫遊客戶端是將特定策略分發到多個使用者的有效方法，但是如果您已啟用Active Directory(AD)整合，則您也可以將這些允許的策略應用到特定AD使用者。

忽略證書異常錯誤 (僅適用於Windows的Chrome)

只能將Chrome for Windows配置為忽略證書異常錯誤，這將緩解此錯誤。瀏覽器被告知忽略該錯誤，但會看到正常的Umbrella阻止頁面。

重要事項：此方法比調整策略管理更具風險，因為瀏覽器配置為忽略證書錯誤。因此，瀏覽器可能會受到中間人(MiTM)攻擊。因此，我們無法建議將此方法作為處理此錯誤的安全方法，但它是解決方法。

這些配置更改必須針對每台電腦進行，這使得大型環境很難進行，但確實可行。

適用於Mac OS X的Firefox、Safari和Chrome

無法將Firefox、Safari和Chrome for Mac OS X 配置為忽略固定域的證書例外錯誤，並且始終遵守

HSTS清單。沒有針對這些錯誤的已知解決方法。

Internet Explorer

Internet Explorer(IE)不實施HSTS限制。因此，不需要配置IE，也不會顯示此錯誤。如果Microsoft選擇在瀏覽器中實施HSTS，這將會在IE的未來版本中發生更改。

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）。