

使用Umbrella篩選時，疑難排解瀏覽器憑證撤銷錯誤

目錄

[簡介](#)

[問題](#)

[原因](#)

[解析](#)

簡介

本文檔介紹在使用Umbrella篩選時如何解決瀏覽器證書吊銷錯誤。

問題

使用僅允許模式或限制類別設定時，通常必須向允許清單中新增多個域，以便站點能夠正確載入。

一個特定問題是，HTTPS/SSL網站的證書吊銷清單(CRL)可能被阻止，這反過來會在某些瀏覽器中生成錯誤。有時，阻止這些CRL也會在瀏覽器嘗試進行驗證時產生延遲。

原因

CRL (證書撤銷清單) 和更新的OCSP (線上證書狀態協定) 用於詢問證書頒發機構是否由於任何原因撤銷了SSL證書。 當您連線到HTTPS網站時，這通常在後台透明地發生。

其思想是，如果證書已吊銷，則在證書/CA受到危害時，瀏覽器會阻止使用者訪問網站。 允許訪問CRL是一個好主意。

在僅允許模式下，除非特意取消阻止，否則大多數CRL都會被阻止。 此問題的影響取決於所使用的Web瀏覽器.....

- Internet Explorer 7顯示一個彈出警告，顯示如下所示的錯誤。 此網站的安全證書的吊銷資訊不可用。
- Internet Explorer的較新版本不顯示任何錯誤，[除非已設定特定的登錄檔項標誌。](#)
- Google Chrome在位址列旁邊顯示一個警告。 按一下警告將顯示以下錯誤： 無法檢查證書是否已吊銷
- 除非在about:config中設定了security.OCSP.require設定，否則Firefox不會顯示錯誤

解析

1. 在Web瀏覽器中檢視證書，以查詢證書的CRL (步驟因瀏覽器而異)。
2. 使用「詳細資訊」頁籤並查詢以下資訊：

- CRL分佈點
- 授權訪問資訊

3. 記下URL資訊（ 下面的示例 ） ，並將其新增到Umbrella控制面板上的允許清單：

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）。