

升級終端以支援適用於Umbrella服務的TLS 1.2

目錄

[簡介](#)

[TLS 1.2要求概述](#)

[TLS 1.0/1.1支援的更新](#)

[保護AnyConnect或漫遊客戶端裝置](#)

[安全Web閘道支援](#)

[Umbrella Active Directory聯結器要求](#)

[Umbrella代理：最低版本要求](#)

[Windows漫遊客戶端或AnyConnect模組](#)

[macOS漫遊客戶端或AnyConnect模組](#)

[其他常見問題](#)

[如果終端沒有在截止日期前更新，會發生什麼情況？](#)

[登錄檔項是否適用於舊版本？](#)

[是否可以僅測試TLS 1.2？](#)

[為什麼要棄用TLS 1.0和1.1？](#)

[為什麼選擇2020年3月31日？](#)

[這是否會影響擁有最新裝置的使用者？](#)

[更新TLS 1.2的終結點後，是否需要執行進一步的操作以重新啟用Umbrella支援？](#)

[如何確認終端對TLS 1.2的支援？](#)

[Windows Web瀏覽器支援](#)

[Windows .NET Framework支援](#)

[適用於Apple Mac和其他系統](#)

簡介

本文檔介紹如何為需要TLS 1.2的Umbrella服務準備端點和應用程式。

TLS 1.2要求概述

截至2020年3月31日，Umbrella伺服器和服务已不再支援傳輸層安全(TLS)1.0和1.1。所有端點必須支援TLS 1.2才能與Umbrella一起正常工作。

TLS 1.0/1.1支援的更新

- 除AnyConnect、Umbrella漫遊客戶端和AD聯結器外，Umbrella在2020年3月終止了對TLS 1.0/1.1的支援。
- 由於後端依賴性，某些儀表板和API服務繼續接受TLS 1.0/1.1連線，直到2021年1月27日。在此日期之後，這些服務不再接受TLS 1.0/1.1連線。
- 必須檢查無法訪問儀表板或API的裝置以獲取TLS 1.2支援。

保護AnyConnect或漫遊客戶端裝置

Umbrella將最後期限延長至2021年1月27日，以便完成對TLS 1.2的升級。不再有進一步的擴展。2021年1月27日之後不符合TLS 1.2要求的AnyConnect和漫遊客戶端裝置不再受Umbrella的保護。

安全Web閘道支援

- Umbrella不支援在安全網關產品中使用TLS 1.0或1.1的HTTPS流量。
- 在2021年1月27日之前，只有當禁用HTTPS解密時，安全Web網關才會為這些協定提供有限的支援。
- [配置所有客戶端作業系統以支援TLS 1.2](#)。
- 根據需要升級或修改非瀏覽器應用程式，以確保TLS 1.2相容性。聯絡應用程式供應商以獲取指導。

Umbrella Active Directory聯結器要求

Umbrella不支援在已停用的Windows作業系統上部署的Active Directory聯結器。運行在不支援的Windows版本（Windows Server 2008、2008 R2或Windows 7）上的AD聯結器停止與Umbrella同步，並於2021年1月27日進入錯誤狀態。

Umbrella代理：最低版本要求

Windows漫遊客戶端或AnyConnect模組

- Cisco Umbrella漫遊客戶端：版本2.2.356或更高版本
- 帶Umbrella漫遊模組的Cisco AnyConnect：[版本4.8.02042或更高版本](#)
- 要使用較舊的客戶端版本，請通過Windows登錄檔更改配置TLS 1.2（請參見下面的步驟）。
- Microsoft .NET Framework：[版本4.6.2或更新版本，或使用.NET 3.5.1修補的Windows 7](#)（AnyConnect需要.NET 4.x或更高版本）
- 支援的Windows版本：7、8、8.1、10

macOS漫遊客戶端或AnyConnect模組

- 任何版本的Umbrella漫遊客戶端或AnyConnect漫遊模組均支援TLS 1.2
- 支援的macOS版本：10.9或更高版本

其他常見問題

如果終端沒有在截止日期前更新，會發生什麼情況？

無法協商TLS 1.2連線的終端無法訪問Umbrella系統，包括儀表板、智慧代理服務和阻止頁面。對於在AnyConnect、Umbrella Enterprise Roaming Client或Umbrella AD Connector中運行Umbrella漫遊模組的客戶，客戶端無法連線到任何Umbrella服務。這會導致客戶端無法與Umbrella控制面板同步配置和狀態。

現有漫遊客戶端停止啟用並在下一次服務啟動時保持未保護狀態。不支援TLS 1.2的新客戶端無法向Umbrella註冊。這些客戶端失效開放；DNS繼續通過本地網路堆疊進行解析，但漫遊客戶端安全服務未啟用。

嘗試訪問被阻止的站點或通過智慧代理路由的站點的裝置無法連線。使用漫遊客戶端的裝置無法訪問Umbrella網站、阻止頁面或代理服務。

登錄檔項是否適用於舊版本？

是，適用於AnyConnect。應用登錄檔編輯後繼續使用舊版本以優先使用強加密。在列出的最低版本之前，漫遊客戶端在沒有明確指定TLS 1.2強加密的情況下啟動了HTTPS連線。如果.NET支援TLS 1.2，則預設使用它。登錄檔項強制使用.NET使用強加密，將更新複製到新客戶端版本中。不支援低於最新版本的獨立漫遊客戶端。

是否可以僅測試TLS 1.2？

會。[在Windows登錄檔中禁用TLS 1.0和TLS 1.1](#)，以驗證裝置是否僅使用TLS 1.2完全運行。

為什麼要棄用TLS 1.0和1.1？

TLS 1.0和1.1已經過時，缺乏對現代加密演算法的支援。它們包含攻擊者可以利用的漏洞。[Internet工程任務組正在棄用這兩種協定](#)。大多數加密的網際網路流量使用[TLS 1.2](#)，它是在十年前推出的。

為什麼選擇2020年3月31日？

在這個時間範圍內，業界正在棄用TLS 1.0和1.1。[Google](#)、[Microsoft](#)、[Apple](#)和[Mozilla](#)都宣佈其瀏覽器在2020年3月不再支援TLS 1.0和1.1。

這是否會影響擁有最新裝置的使用者？

否。大多數網站支援TLS 1.2。根據[Qualys SSL Labs](#)的資料，95.2%的網站支援TLS 1.2。預計這一數字將在2020年3月增加。少數網站無法運行，但總體使用者影響極小。確保最新裝置包含用於Windows電腦的.NET的正確版本。

更新TLS 1.2的終結點後，是否需要執行進一步的操作以重新啟用Umbrella支援？

在大多數情況下，不需要採取進一步的行動。客戶端使用安全TLS 1.2協定與Umbrella系統重新建立通訊。對於Umbrella Enterprise漫遊客戶端或Umbrella Roaming Client for AnyConnect，如果系統在客戶端軟體更新期間處於離線狀態，則恢復可能會延遲。客戶端需要在服務完全還原之前下載更新。

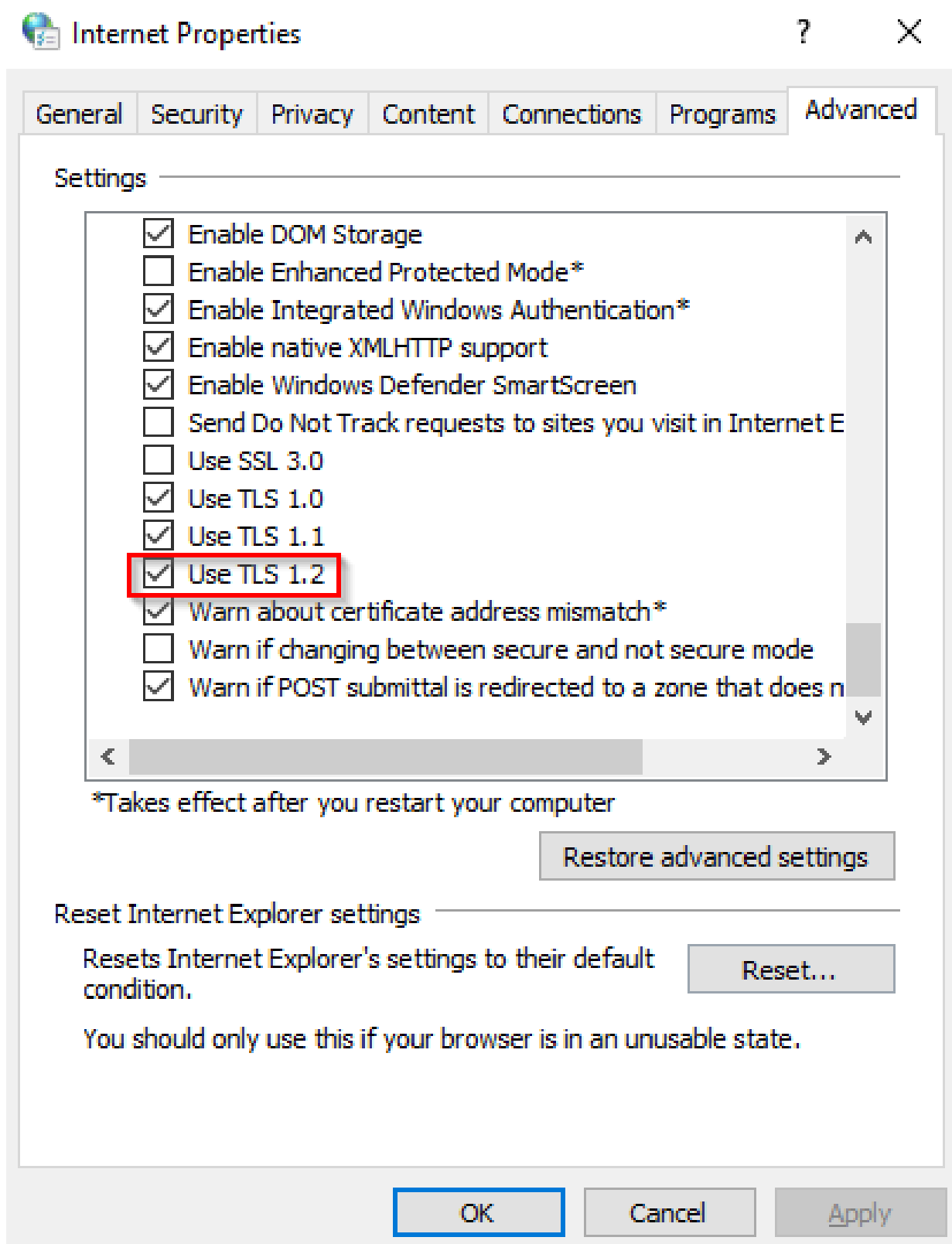
如何確認終端對TLS 1.2的支援？

- Windows Web瀏覽器支援
 - 訪問Umbrella控制面板和相關網站。

- [運行SSL Labs Browser Test](#)。「Protocols」部分的TLS 1.2旁邊顯示「Yes」（確認）。

- Windows .NET Framework支援

- 適用於企業漫遊客戶端、AnyConnect漫遊模組或AD聯結器。
- .NET 4.6.2或更高版本提供本地TLS 1.2支援。
- 以前的版本需要登錄檔編輯(4.x)或登錄檔編輯和手動修補程式補丁(3.5)。
- 此資訊適用於在.NET framework上運行的Umbrella軟體，包括AD聯結器和漫遊客戶端。
- 通過完成Microsoft提供的說明，在作業系統級別禁用SSL、TLS 1.0和[TLS 1.1](#)。



blobid0.png

- 適用於Apple Mac和其他系統
- 執行[SSL Labs Browser Test](#)。確認Protocols部分中的TLS 1.2旁邊顯示「Yes」（是）。

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）。