

# 如何：擴展Cisco Umbrella以保護您的無線網路

## 簡介

資料安全是每個組織的集體工作。員工至少要承擔部分責任，確保自己不會成為騙局的犧牲品。在實踐中，安全是很困難的，這不足為奇。隨著科技工具的擴張，駭客的進步也發生了同樣的變化，可以說，所有的船都會隨著潮水而上漲。請繼續閱讀，瞭解如何在LAN上整合Umbrella保護。

## 目標

本指南將向您展示將Umbrella的安全平台整合到無線網路所涉及的步驟。在詳細瞭解細節之前，我們將回答您就Umbrella問自己的一些問題。

## 適用裝置

- WAP125
- WAP581

## 軟體版本

- 1.0.1

## 需求

有效的Umbrella帳戶(沒有帳戶？[請求報價](#)或開始免費試用)

## 什麼是Umbrella？

Umbrella是思科提供的簡單但非常有效的雲安全平台。Umbrella在雲中運行並執行許多與安全相關的服務。從突發性威脅到事後調查。Umbrella可發現並阻止所有埠和協定上的攻擊。

## 如何運作？

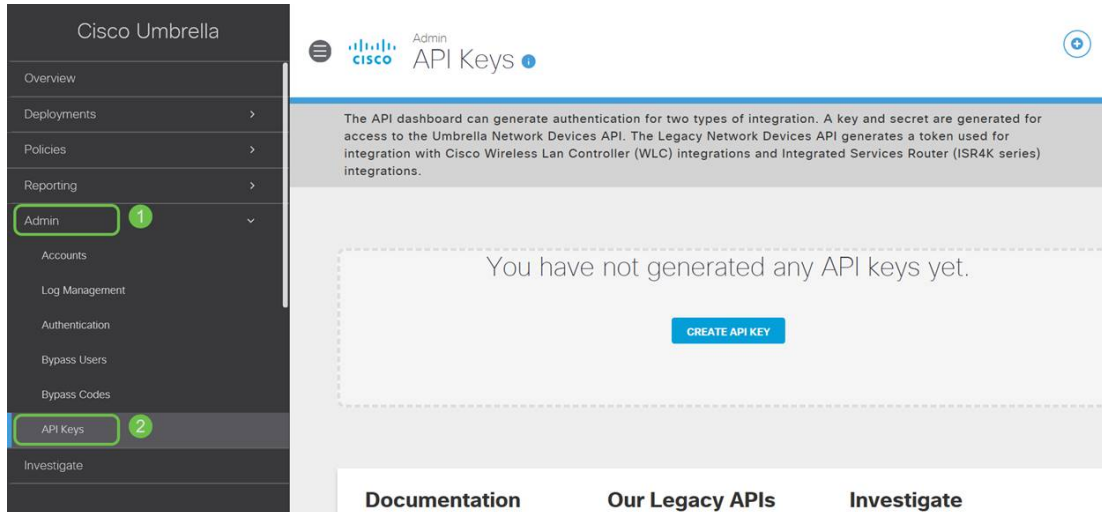
Umbrella使用DNS作為其防禦的主要載體。當使用者在其瀏覽器欄中輸入URL並點選Enter時，Umbrella會參與傳輸。該URL會傳遞到Umbrella的DNS解析程式，如果安全警告與域關聯，則請求會被阻止。此遙測資料傳輸和分析在微秒內完成，幾乎不會增加延遲。遙測資料使用日誌和儀器來跟蹤全世界數十億個DNS請求。當這些資料普遍存在時，將其關聯到全球各地便能夠在攻擊開始時快速做出響應。有關詳細資訊，請參閱思科的隱私政策 — [完整策略](#)，[摘要版本](#)。將遙測資料視為源自工具和日誌的資料。

用比喻來概括一下，假設你在一個派對上。在派對上，每個人都在手機上瀏覽網頁。在安靜的集體沈默中，參加派對的人不時輕敲他們的螢幕。[這並不是一個很棒的派對](#)，但在你自己的手機上，你可以看到一個超級連結，指向一個看起來讓人無法抗拒的小貓GIF。但是您不確定是否應該點選，因為URL看起來有問題。因此，在點選超連結之前，你要向派對的其他人喊道「這個連結不好嗎？」如果派對上還有個人去過連結，發現連結是騙局，他們會大喊，「是的，我做到了，但連結是騙局！」你感謝那個人救了你，繼續你尋找可愛的動物在安靜中的照片。當然，在思科的規模下，這種型別的請求和回撥安全檢查每秒進行數百萬次。

# 聽起來很棒，我們怎麼開始呢？

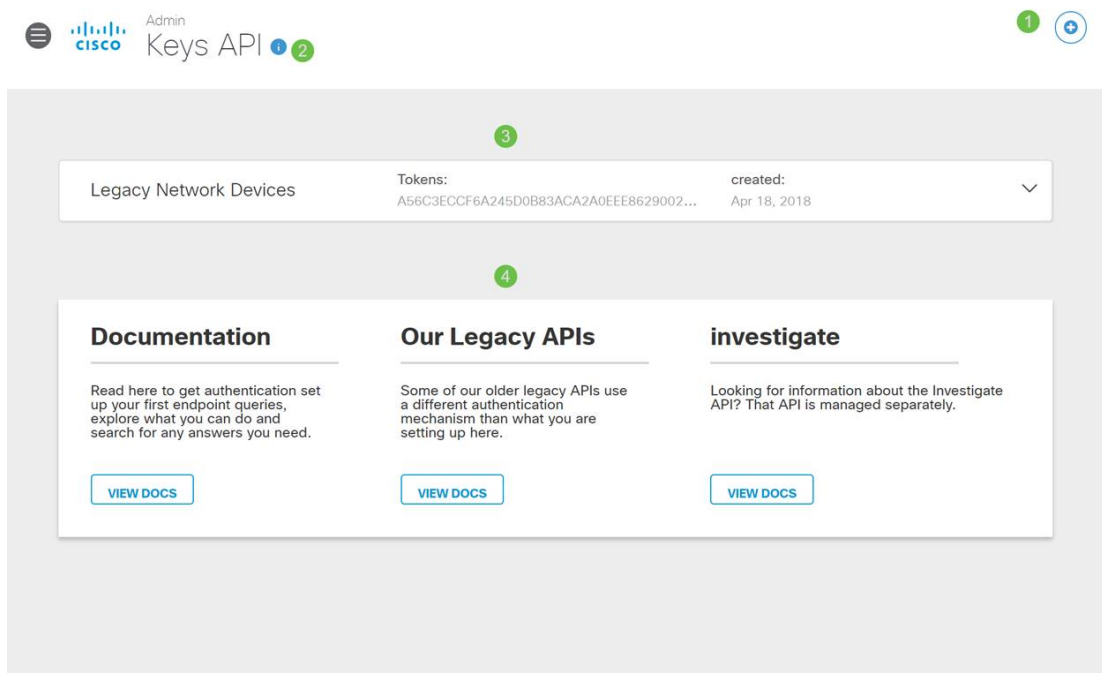
本指南導航的位置，首先從您的Umbrella帳戶控制面板中獲取API金鑰和金鑰。之後，我們將登入您的WAP裝置以新增API和金鑰。如果遇到任何問題，請查看[此處獲取文檔](#)，並查看[Umbrella支援選項](#)。

步驟1. 登入到您的Umbrella帳戶後，從Dashboard螢幕按一下Admin > API Keys。

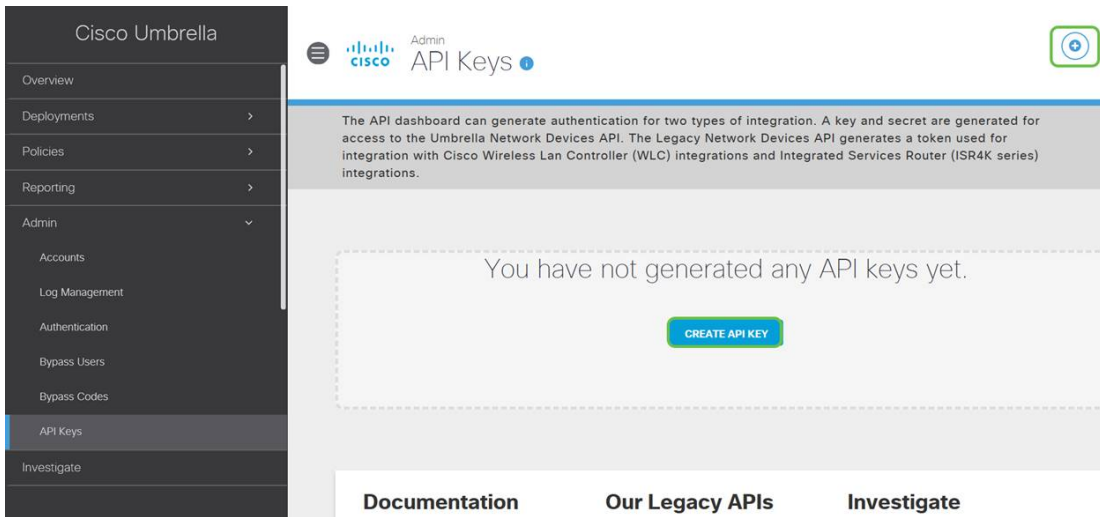


## API金鑰螢幕剖析 —

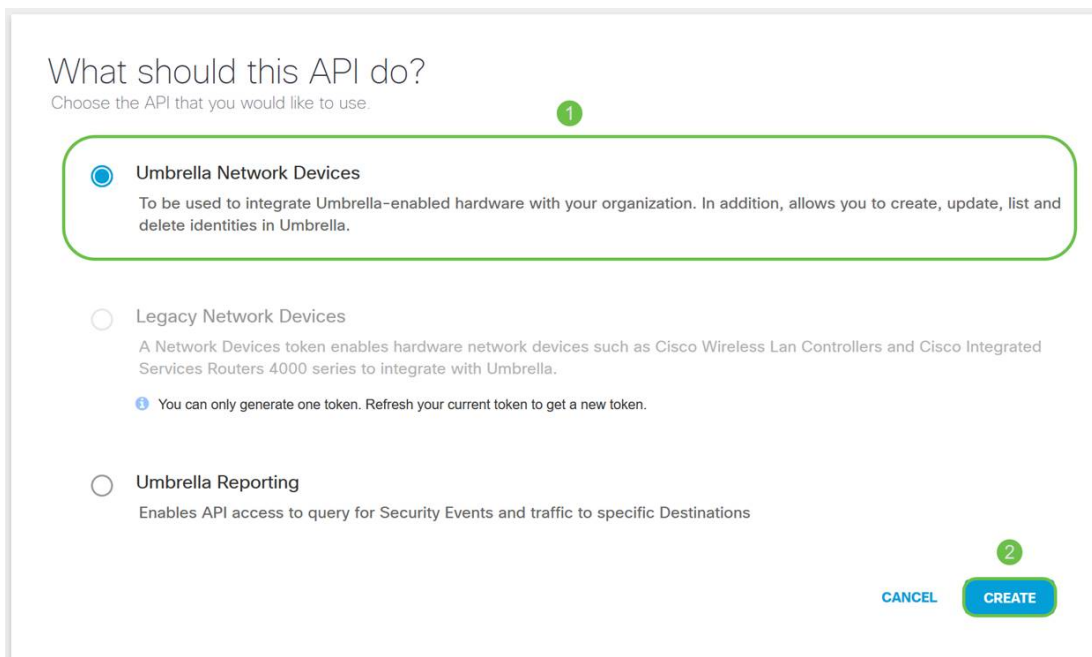
1. 新增API密鑰 — 啟動建立新金鑰以與Umbrella API一起使用。
2. Additional Info — 向下/向上滑動，提供此螢幕的說明。
3. Token Well — 包含此帳戶建立的所有金鑰和令牌。（在建立金鑰後填充）
4. 支援文件 — 指向Umbrella站點上與每個部分中的主題有關的文檔的連結。



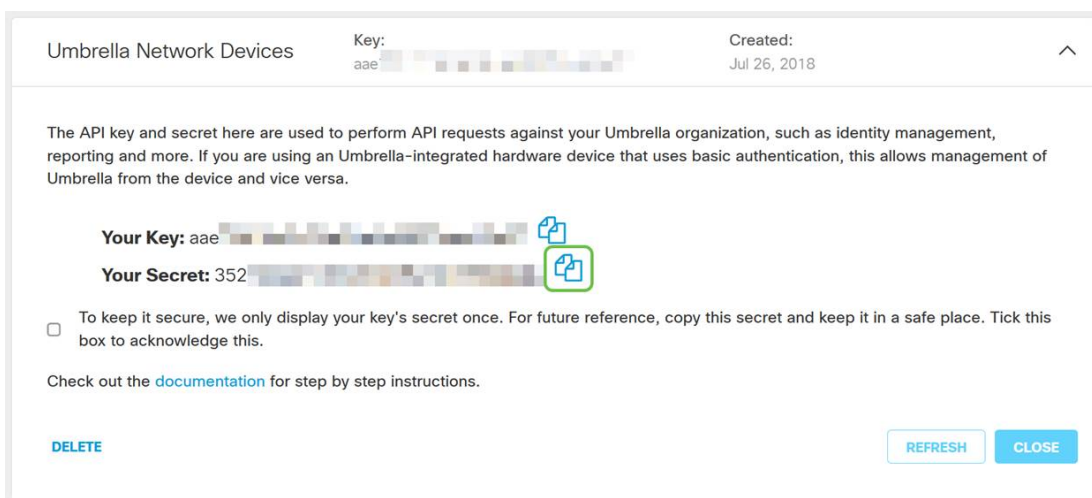
步驟2. 按一下右上角的Add API Key按鈕，或按一下Create API Key按鈕。兩者功能相同。



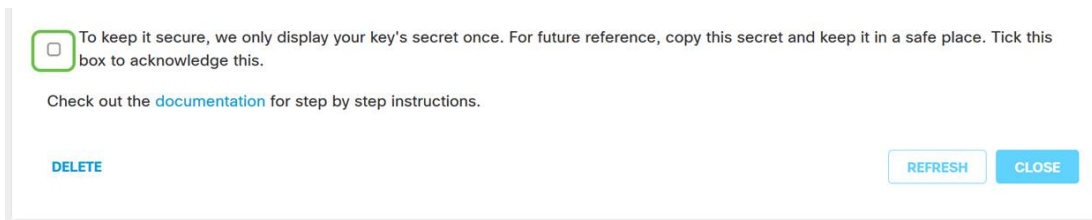
步驟3.選擇Umbrella Network Devices，然後按一下Create按鈕。



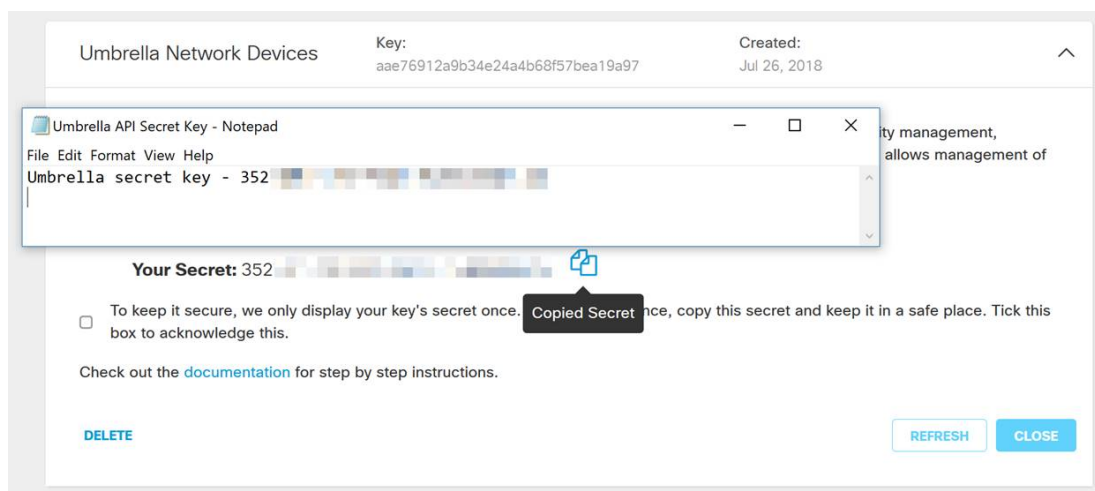
步驟4.按一下Secret Key右側的Copy按鈕，彈出通知將確認金鑰已複製到剪貼簿。



將金鑰和金鑰複製到安全位置後，按一下**覈取方塊**確認完成確認，然後按一下**關閉**按鈕。



步驟5. 開啟文字編輯器（例如記事本），並將您的密碼和API金鑰貼上到檔案內，然後貼上標籤以備日後參考。在本例中，其標籤為「Umbrella secret key」。包括API金鑰和您的金鑰，並簡要說明在同一個文本檔案中如何使用它。然後，將文本檔案儲存到安全位置，以便以後需要時輕鬆訪問。



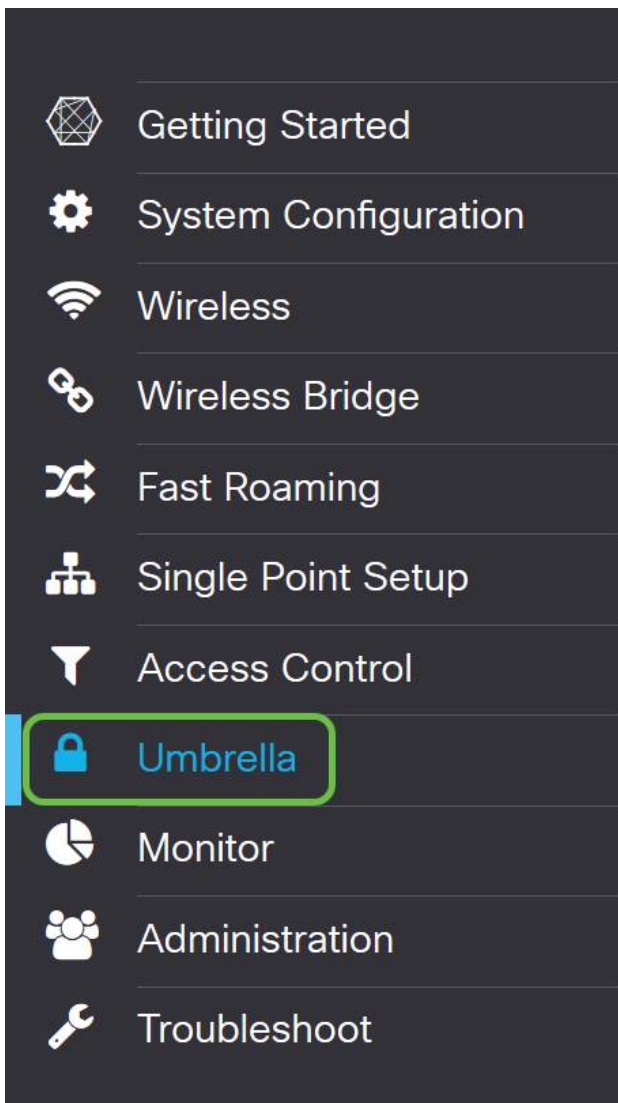
**重要附註：** 如果丟失或意外刪除了金鑰，則沒有函式或支援號碼可供呼叫以檢索此金鑰。[保守秘密](#)，[保持安全](#)。如果丟失，您將需要刪除金鑰並重新授權API金鑰以及您要使用Umbrella保護的每個WAP裝置。

**最佳實踐：** 僅將此檔案的單個副本放在任何網路無法訪問的裝置（如USB閃盤）上。

## 在WAP裝置上配置Umbrella

現在，我們已經在Umbrella內建立了API金鑰，接下來我們將使用這些金鑰並將其安裝到WAP裝置上。在本例中，我們使用WAP581。

步驟1. 登入到WAP裝置後，按一下邊欄選單中的Umbrella。



步驟2. Umbrella螢幕很簡單，但此處有兩個欄位值得定義：

- **要繞過的本地域** — 此欄位包含希望從Umbrella服務中排除的內部域。
- **DNSCrypt** — 保護DNS客戶端和DNS解析程式之間的資料包傳輸。此功能預設處於啟用狀態，禁用此功能將降低網路的安全性。

The image shows the Cisco Umbrella configuration page for a device named WAP581-WAP581. The page has a light gray background and a dark header with the Cisco logo and language settings (English). The main content area is titled "Umbrella" and contains the following fields:

- Enable:** A checkbox that is currently unchecked.
- API Key:** A text input field.
- Secret:** A text input field.
- Local Domains to Bypass (optional):** A text input field with the placeholder text "Multiple inputs separated by comma".
- Device Tag (optional):** A text input field containing the value "WAP581".
- DNSCrypt:** A checkbox labeled "Enable" that is currently unchecked.
- Registration Status:** A label with no associated input field.

At the top right of the configuration area, there are "Save" and "Cancel" buttons.

步驟3.將API和金鑰貼上到相應的欄位中

WAP581-WAP581

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.

With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

步驟4.確保Enable和DNSCrypt的覈取方塊已切換為選中狀態。

WAP581-WAP581

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.

With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

附註：DNSCrypt可保護DNS客戶端和DNS解析器之間的DNS通訊。預設啟用。

步驟5. ( 可選 ) 輸入您希望Umbrella通過DNS解析過程允許的本地域。

WAP581-WAP581

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.

With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

附註：這是所有Intranet域和拆分DNS域所必需的。如果您的網路需要使用本地域進行路由，則需要聯絡Umbrella支援以啟動和運行該功能。大多數使用者不需要使用此選項。

步驟6.對更改感到滿意或者新增了自己的Local Domains to Bypass後，請按一下右上角的Save按鈕

。



cisco





English



Save

Cancel

步驟7.完成更改後，*Registration Status*欄位將為「Successful」。

Enable:	<input checked="" type="checkbox"/>
API Key: 	aae 
Secret: 	352 
Local Domains to Bypass (optional):	Multiple inputs separated by comma
Device Tag (optional):	WAP581
DNSEncrypt:	<input checked="" type="checkbox"/> Enable
Registration Status:	Successful


## 確認一切都在正確的位置

祝賀您，您現在受到思科的Umbrella保護。還是你？可以肯定，思科已建立了一個網站，專用於在載入頁面時快速確定問題。[點選此處](#)或在瀏覽器欄中鍵入<https://InternetBadGuys.com>。

如果Umbrella配置正確，您會看到類似此的螢幕！

SECURITY THREAT DETECTED AND BLO... X

sinkhole-umbrella.cisco.com/?client\_ip=...&type=phish&url=uggc...



### SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco Umbrella security threat information, access to the web site **Not\_Found** has been blocked to prevent an attack on your browser.

Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this page should not be blocked, [open a case](#) providing the following information:

- Text or screenshot of the corresponding debug information below
- Business justification for use of the website

**Block Reason: Umbrella DNS Block**

Date: July 26, 2018  
Time: 22:58:17  
Host Requested: Not\_Found  
URL Requested: Not\_Found  
Client IP address: ...  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0  
Request Method: GET

檢視與本文相關的影片.....

[按一下此處檢視思科的其他技術對話](#)