

在WAP571或WAP571E中使用Cisco Umbrella配置網路內容過濾

目標

本文的目的是向您展示如何在WAP571或WAP571E上使用Cisco Umbrella配置網路內容過濾。

簡介

您一直努力使網路啟動並運行。當然，你希望它保持這種狀態，但駭客們是無情的。如何保證網路安全？一種解決方案是設定網路內容過濾。Web內容過濾功能允許您通過配置策略和過濾器提供對Internet的受控訪問。它通過阻止惡意網站或不需要的網站，幫助保護網路。

Cisco Umbrella是一個雲安全平台，提供抵禦網際網路威脅的第一道防線。它充當Internet與您的系統和資料之間的網關，用於阻止惡意軟體、殭屍網路和通過任何埠、協定或應用的網路釣魚。

使用Cisco Umbrella帳戶，該整合將以透明方式（在URL級別報告）攔截域名系統(DNS)查詢，並將其重定向到Umbrella。您的裝置將作為網路裝置顯示在Umbrella控制面板中，以便應用策略和檢視報告。

要瞭解有關Cisco Umbrella的更多資訊，請訪問以下連結：

[Cisco Umbrella概覽](#)

[Cisco Umbrella使用手冊](#)

[如何：擴展Cisco Umbrella以保護您的無線網路](#)

適用裝置

WAP571

WAP571E

軟體版本

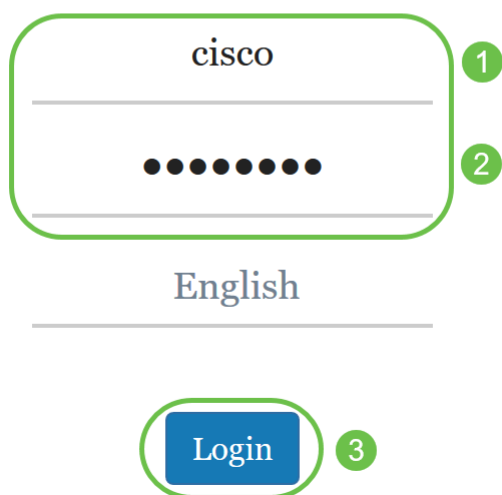
- 1.1.0.3

在WAP上配置Cisco Umbrella

步驟1.通過輸入使用者名稱和密碼登入到WAP的Web配置實用程式。預設使用者名稱和密碼為 *cisco/cisco*。如果已配置新的使用者名稱或密碼，請輸入這些憑據。按一下「Login」。

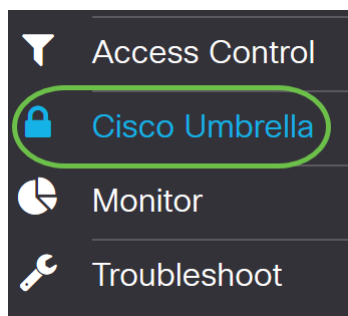


Wireless Access Point



附註：本文使用WAP571E來演示Cisco Umbrella的配置。選單選項可能會略有不同，具體取決於裝置的型號。

步驟2.選擇Cisco Umbrella。



步驟3. 單擊覈取方塊啟用Cisco Umbrella。

Cisco Umbrella

Cisco Umbrella is a cloud security platform that provide the first line of defense against
With an [Umbrella account](#), this integration will transparently intercept DNS queries and
This device will appear in the [Umbrella dashboard](#) as a network device for applying poli

Enable:



API Key: [?](#)

Secret: [?](#)

Local Domains to Bypass (optional):

Multiple inputs separated by comma

Device Tag (optional):

DNSCrypt:

Enable

Registration Status:

步驟4.要獲取API金鑰和密碼，請使用*Email or Username* and *Password*登入[Cisco Umbrella帳戶](#)。
按一下「LOG IN」。



Cisco Umbrella

Email or Username

1

Password

2

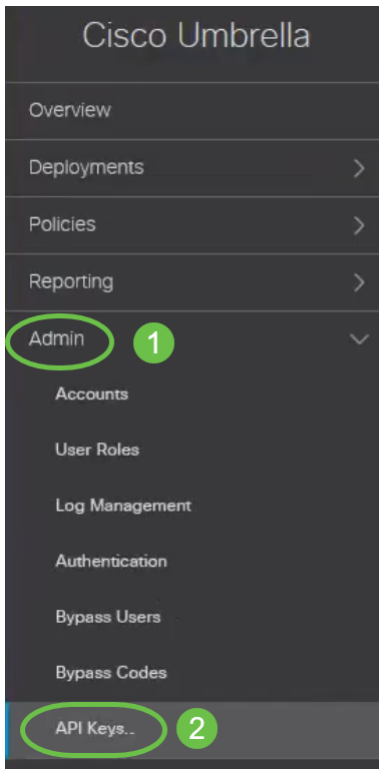
[Forgot password?](#) | [Single sign on](#)

LOG IN

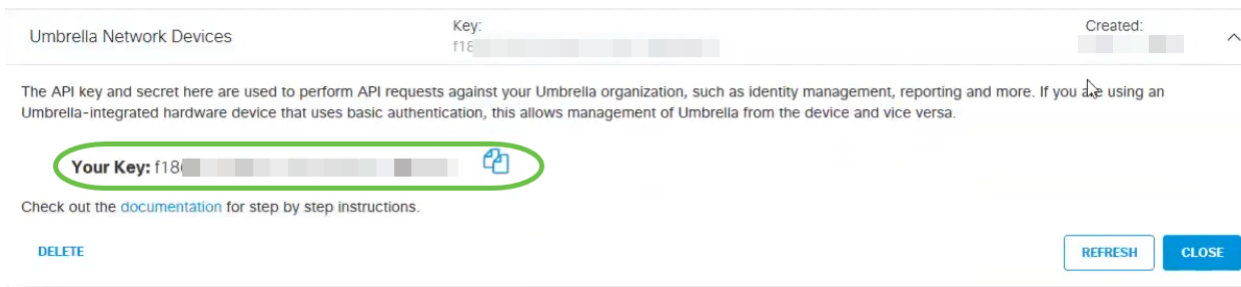
3

[Sign Up for a Free Trial](#)

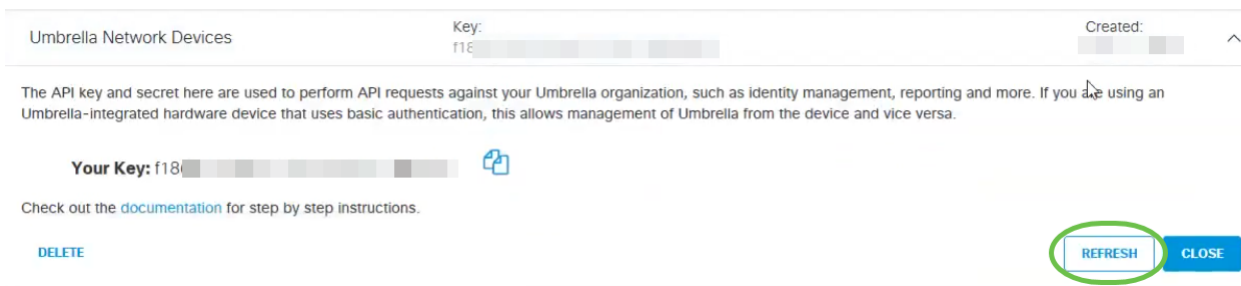
步驟5.導航至Admin，並通過從選單中選擇API Keys...來請求API金鑰。



附註：第一次請求API金鑰時，僅顯示如下所示的金鑰。



步驟6.按一下Refresh以取得API金鑰和密碼。



附註：按一下Refresh時，API金鑰將更改。

步驟7.複製產生的Key和Secret。

Umbrella Network Devices

Key: dbb1 [REDACTED]

Created: [REDACTED]

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

Your Key: dbb1 [REDACTED]

Your Secret: 4e5 [REDACTED]

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

[DELETE](#) [REFRESH](#) [CLOSE](#)

步驟8. 將步驟7中複製的Key和Secret貼到WAP的Cisco Umbrella配置下提供的欄位中。

Cisco Umbrella [Apply](#) [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: 1

Secret: 2

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt: Enable

Registration Status:

步驟9. (可選) 在「Local Domains to Bypass (可選)」欄位中輸入您信任的域名，資料包將無需通過Cisco Umbrella即可到達目標。清單中的專案應以逗號分隔，而域可以包含星號(*)形式的萬用字元。例如：*.cisco.com.*。

Cisco Umbrella [Apply](#) [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：對於內部和外部網路中存在獨立伺服器的所有Intranet域和拆分DNS域，這是必需的。

步驟10. (可選) 在Device Tag(可選)欄位中輸入標籤名稱以對裝置進行標籤。Device Tag描述裝置或分配給裝置的特定原點。確保它對於您的組織是唯一的。

Cisco Umbrella Apply 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):

DNSEncrypt: Enable

Registration Status:

附註： *Secret*、*API Key*和*Device Tag*的任何更改都將觸發重新註冊以建立網路裝置。

步驟11. **DNSEncrypt**用於保護（通過加密）DNS客戶端與DNS解析器之間的DNS通訊。它可以防止多種型別的DNS攻擊和監聽。預設情況下啟用。

Cisco Umbrella Apply 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):

DNSEncrypt: Enable

Registration Status:

步驟12. 按一下**Apply**以應用這些設定。

Cisco Umbrella

Apply 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):

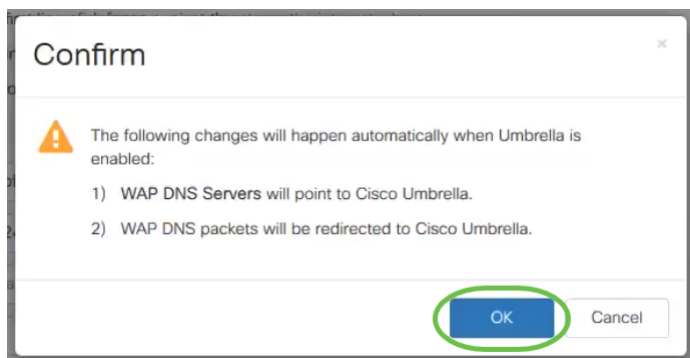
Device Tag (optional):

DNSCrypt: Enable

Registration Status:

附註：註冊的狀態在註冊狀態欄位中指示。狀態可以是 *Successful*、*Registering* 或 *Failed*。

步驟13. 您將看到一個彈出螢幕，如下所示。按一下「OK」以確認。



驗證

檢查是否已啟用網站篩選是一個有趣的方法。只需開啟Web瀏覽器並輸入以下url: www.internetbadguys.com。不必擔心，此站點為思科所有，用於測試和驗證目的。



由於通過Cisco Umbrella在WAP中啟用了網站過濾，您將收到以下通知。無線網路會將DNS查詢重定向到Cisco Umbrella。反過來，Cisco Umbrella充當DNS伺服器，保護網路及其使用者。



This site is blocked.

www.internetbadguys.com

SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco Umbrella security threat information, access to the web site www.internetbadguys.com 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 hostname was misclassified, please connect to the Cisco network and open a [case](#) with Infosec.

As a matter of good practice, you may check whether your browser or any component plugin is vulnerable by visiting browsercheck.qualys.com. The UID at the end of the browsercheck.qualys.com URL does not uniquely identify your machine to Qualys; it is a shared UID to group all requests originating from Cisco IP ranges.

[FAQ](#)

結論

現在，您已使用Cisco Umbrella在WAP571或WAP571E接入點上配置和啟用網站過濾。

想要瞭解更多資訊？檢視以下與Cisco Umbrella相關的影片：

[思科技術演講：使用Umbrella和思科S系列接入點保護企業網路](#)

[思科技術演講：如何獲取Umbrella帳戶](#)

[思科技術演講：設定保護傘策略](#)