

# Webcontentfiltering configureren met behulp van Cisco Umbrella in WAP571 of WAP571E

## Doel

Het doel van dit artikel is om u te tonen hoe u web content filtering met behulp van Cisco Umbrella op een WAP571 of WAP571E kunt configureren.

## Inleiding

U hebt hard gewerkt om uw netwerk op en uit te bouwen. Natuurlijk wil je dat het zo blijft, maar hackers zijn meedogenloos. Wat kan worden gedaan om uw netwerk veilig te houden? Eén oplossing is het instellen van webcontentfiltering. Met de functie voor webcontentfiltering kunt u beheerste toegang tot het internet bieden door beleid en filters te configureren. Het helpt het netwerk te beveiligen door kwaadaardige of ongewenste websites te blokkeren.

Cisco Umbrella is een cloudbeveiligingsplatform dat de eerste verdedigingslinie tegen bedreigingen op het internet biedt. Het fungeert als gateway tussen het internet en uw systemen en gegevens om malware, botnetten en phishing via elke poort, protocol of toepassing te blokkeren.

Gebruik van een Cisco Umbrella-account, zal de integratie op transparante wijze (via de URL-standaard) vragen onderscheppen en doorsturen naar Umbrella. Uw apparaat zal in het dashboard van Umbrella verschijnen als netwerkapparaat voor het toepassen van beleid en het bekijken van rapporten.

Wilt u meer weten over Cisco Umbrella? controleer dan de volgende koppelingen:

[Cisco Umbrella in één oogopslag](#)

[Cisco Umbrella-gebruikershandleiding](#)

[Hoe: Uitbreiding van Cisco Umbrella om uw draadloze netwerk te beschermen](#)

## Toepasselijke apparaten

WAP571

WAP571E router

## Softwareversie

- 1.1.0.3

# Cisco Umbrella op uw WAP configureren

Stap 1. Meld u aan bij het web configuratie hulpprogramma van de WAP door de gebruikersnaam en het wachtwoord in te voeren. De standaardwaarden voor gebruikersnaam en wachtwoord zijn cisco/cisco. Als u een nieuwe gebruikersnaam of wachtwoord hebt ingesteld, voert u die aanmeldingsgegevens in. Klik op **Aanmelden**.



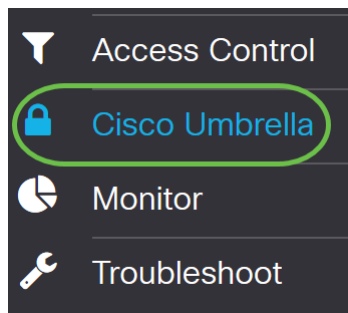
## Wireless Access Point

A login form with three numbered steps: 1. A text input field containing "cisco". 2. A password input field with ten black dots. 3. A blue "Login" button.

Below the password field is a language selection dropdown menu showing "English".

Opmerking: In dit artikel, wordt WAP571E gebruikt om de configuratie van Cisco Umbrella aan te tonen. De menuopties kunnen licht variëren afhankelijk van het model van het apparaat.

Stap 2. Kies **Cisco Umbrella**.



Stap 3. *Schakel* Cisco Umbrella in door op het aankruisvakje te klikken.

# 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):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

Stap 4. U kunt de *API*-sleutel en *het* geheim verkrijgen door op uw [Cisco Umbrella](#)-account te loggen met *e-mail of gebruikersnaam* en *Wachtwoord*. Klik op **INloggen**.



## Cisco Umbrella

**Email or Username**

**Password**

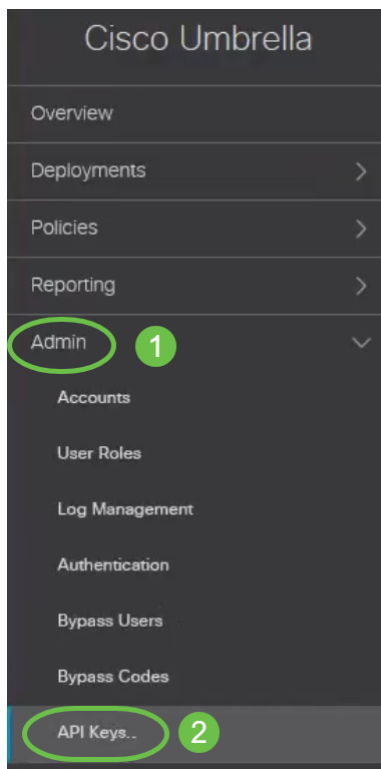
[Forgot password?](#) | [Single sign on](#)



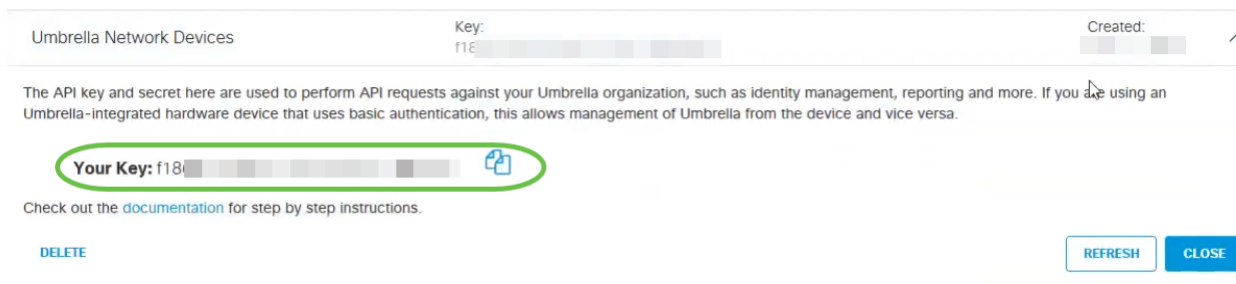
[Sign Up for a Free Trial](#)

Stap 5. Navigeer naar **Admin** en verzoek om een API-toets door **API-toetsen** te kiezen... van het

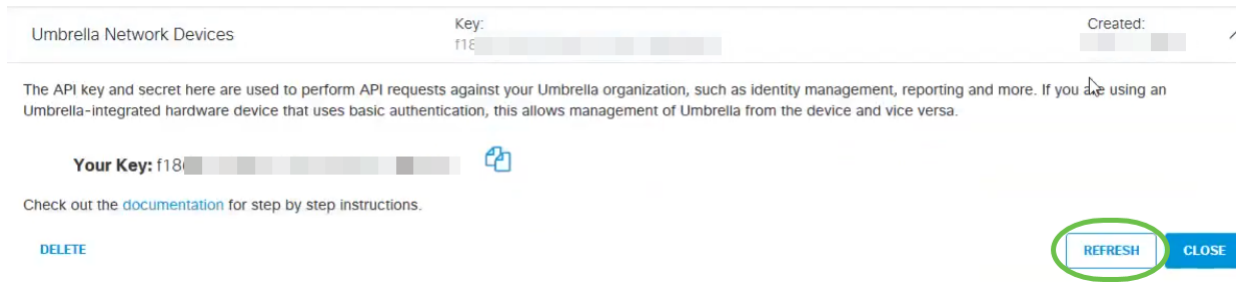
menu.



Opmerking: De eerste keer dat u een API-toets vraagt, wordt alleen de toets weergegeven zoals hieronder wordt weergegeven.



Stap 6. Klik op **Vernieuwen** om zowel de API-toets als het Geheime te verkrijgen.



Opmerking: Wanneer u op *Vernieuwen* klikt, wordt de API-toets gewijzigd.

Stap 7. Kopieer de *sleutel* en het *geheim* die worden gegenereerd.

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](#)

Stap 8. Plakt de gekopieerde *sleutel* en het *geheim* van Stap 7 in naar de velden die onder *Cisco Umbrella*-configuratie van de WAP zijn meegeleverd.

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):

DNSEncrypt:  Enable

Registration Status:

Stap 9. (Optioneel) Voer de domeinnaam in die u op het veld **Local Domain to Bypass (optioneel)** vertrouwt en de pakketten komen op de bestemming zonder Cisco Umbrella. Items in de lijst moeten worden gescheiden door een komma, terwijl de domeinen wildkaarten kunnen bevatten in de vorm van een sterretje (\*). Bijvoorbeeld: \*.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):

DNSEncrypt:  Enable

Registration Status:

Opmerking: Dit is vereist voor alle Intranet domeinen en gesplitste DNS-domeinen waar afzonderlijke servers bestaan voor interne en externe netwerken.

Stap 10. (Optioneel) Voer een tagnaam in in het veld **Apparaatmarkering (optioneel)** om het

apparaat te markeren. De *apparaattag* beschrijft het apparaat of een bepaalde oorsprong die aan het apparaat is toegewezen. Zorg ervoor dat dit uniek is voor uw organisatie.

### 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:

Opmerking: Elke wijziging in de *Secret*, *API Key* en de *Devices* zullen opnieuw registreren om een netwerkkapparaat te maken.

Stap 1. **DNSCrypt** wordt gebruikt om de DNS-communicatie tussen een DNS-client en een DNS-resolutie te beveiligen (via encryptie). Het voorkomt verschillende typen DNS-aanvallen en snoeping. Deze functie is standaard ingeschakeld.

### 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:

Stap 12. Klik op **Toepassen** om deze configuraties toe te passen.

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):

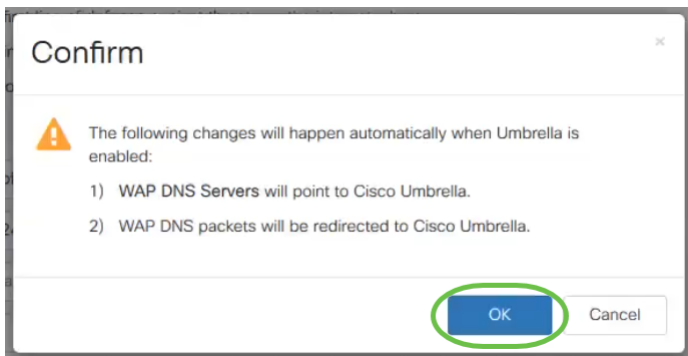
Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

Opmerking: De status van de registratie wordt in het veld *Registratiestatus* aangegeven. De status kan *succesvol* zijn, *zich registreren* of *mislukken*.

Stap 13. U ziet een pop-upscherf zoals hieronder wordt weergegeven. Klik op **OK** om dit te bevestigen.



## Verificatie

Er is een leuke manier om te controleren of het filteren van de website is ingeschakeld. Open gewoon een webbrowser en voer de volgende URL in: [www.internetbadguys.com](http://www.internetbadguys.com). Wees niet bang voor deze website. Deze is eigendom van Cisco voor test- en verificatiedoeleinden.



Aangezien webfiltering in de WAP via Cisco Umbrella is ingeschakeld, ontvangt u het volgende bericht. Het draadloze netwerk zal de DNS-query opnieuw richten op Cisco Umbrella. Cisco Umbrella werkt op zijn beurt als de DNS-server, waardoor het netwerk en de gebruikers worden beschermd.



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](http://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](http://browsercheck.qualys.com). The UID at the end of the [browsercheck.qualys.com](http://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](#)

## Conclusie

U hebt nu internetfiltering op een WAP571 of WAP571E access point ingesteld en ingeschakeld met behulp van Cisco Umbrella.

Wil je meer leren? Bekijk deze video's over Cisco Umbrella:

[Cisco Tech Talk: Een bedrijfsnetwerk beveiligen met Umbrella en Cisco Small Business Access Point](#)

[Cisco Tech Talk: Een Umbrella-account verkrijgen](#)

[Cisco Tech Talk: Een Umbrella-beleid](#)