How To: Extending Cisco Umbrella to protect your wireless Network

Introduction

Data security is a group effort at every organization. Employees are at least partly responsible for ensuring they do not fall prey to scams. In practice, security is tough and it's no wonder why. As technology's tools expand the same goes for hacker's advances, all boats rise with the tide so to speak. Read on to learn how to integrate Umbrella protection on your LAN.

Objective

This how to guide will show you the steps involved in integrating Umbrella's security platform into your wireless network. Before we get into the nitty gritty details we'll answer a few questions you may be asking yourself about Umbrella.

Applicable Devices

- WAP125
- WAP581

Software Version

- 1.0.1

Requirements

An active Umbrella account (Don't have one? Request a quote or start a free trial)

What is Umbrella?

Umbrella is a simple yet very effective cloud security platform from Cisco. Umbrella operates in the cloud and performs many security related services. From emergent threat to post event investigation. Umbrella discovers and prevents attacks across all ports and protocols.

How does it work?

Umbrella uses DNS as its main vector for defense. When users enter a URL in their browser bar and hit Enter, Umbrella participates in the transfer. That URL passes to Umbrella's DNS resolver, and if a security warning associates with the domain, the request is blocked. This telemetry data transfers and is analyzed in microseconds, adding nearly no latency. Telemetry data uses logs and instruments tracking billions of DNS requests throughout the world. When this data is pervasive, correlating it across the globe enables rapid response to attacks as they begin. See Cisco's privacy policy here for more information - full policy, summary version. Think of telemetry data as data derived from tools and logs.

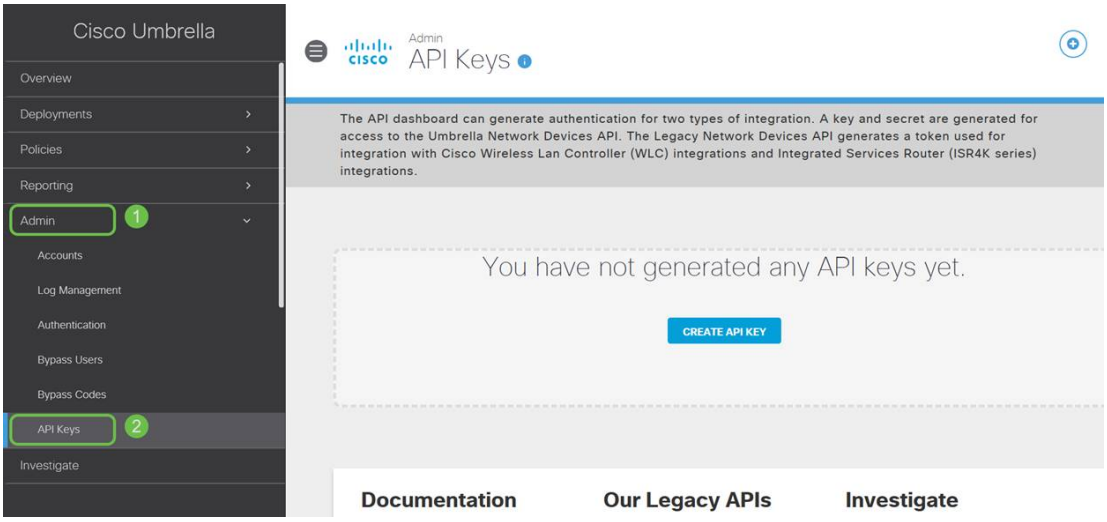
To summarize in a metaphor, imagine you're at a party. At this party everyone is on their phone

surfing the web. The quiet group-silence is punctuated by the party-goers tapping away on their screens. It's not a great party, but while on your own phone you see a hyperlink to a kitten GIF that seems irresistible. However you're unsure of if you should tap or not, because the URL appears questionable. So before you tap the hyperlink, you shout out to the rest of the party "Is this link bad?" If another person at the party has been to the link and discovered it was a scam, they would shout back "Yeah, I did and it's a scam!" You thank that person for saving you, continuing your quest for pictures of cute animals in silence. Of course, at the scale of Cisco this type of request and callback security checks are occurring millions of times a second.

Sounds great, how do we kick this off?

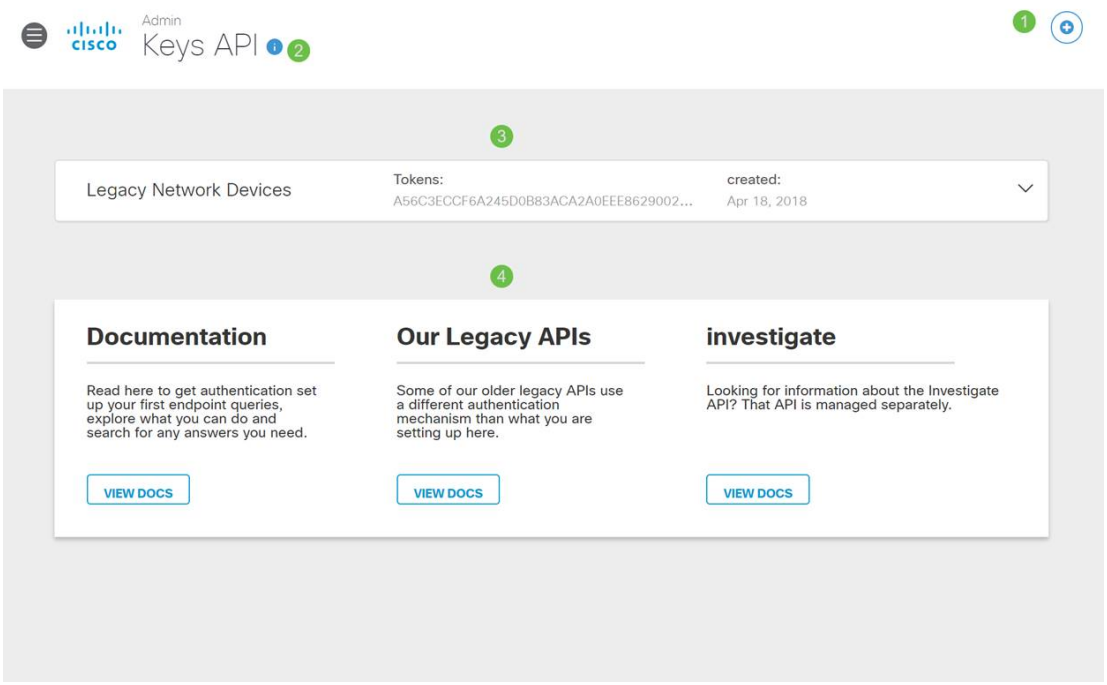
Where this guide is navigating, starts by grabbing the API key and Secret key from your Umbrella account dashboard. After, we'll log into your WAP device to add the API and Secret key. If you run into any issues, check here for documentation, and here for Umbrella Support options.

Step 1. After logging into your Umbrella Account, from the *Dashboard* screen click on **Admin** > **API Keys**.

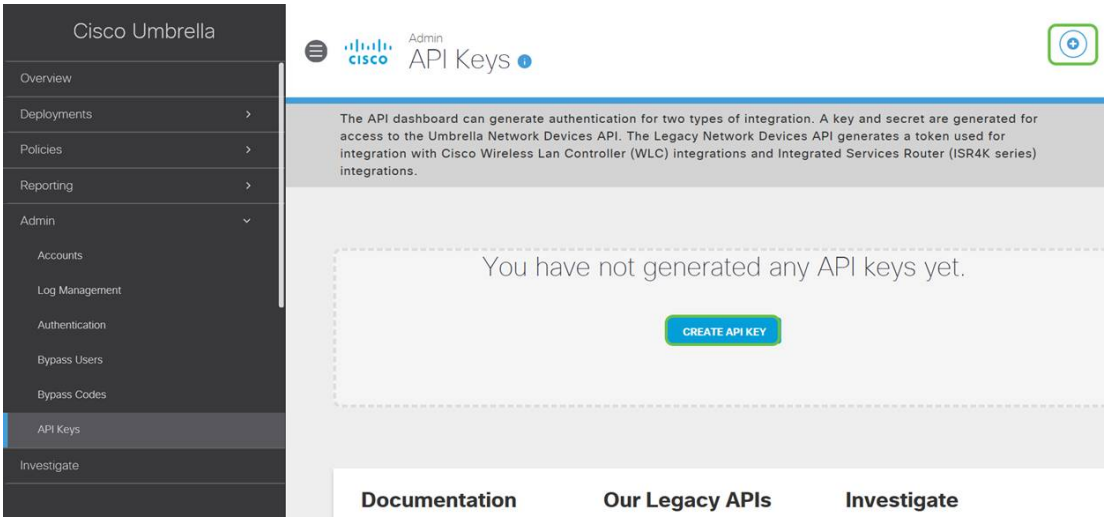


Anatomy of the API Keys Screen -

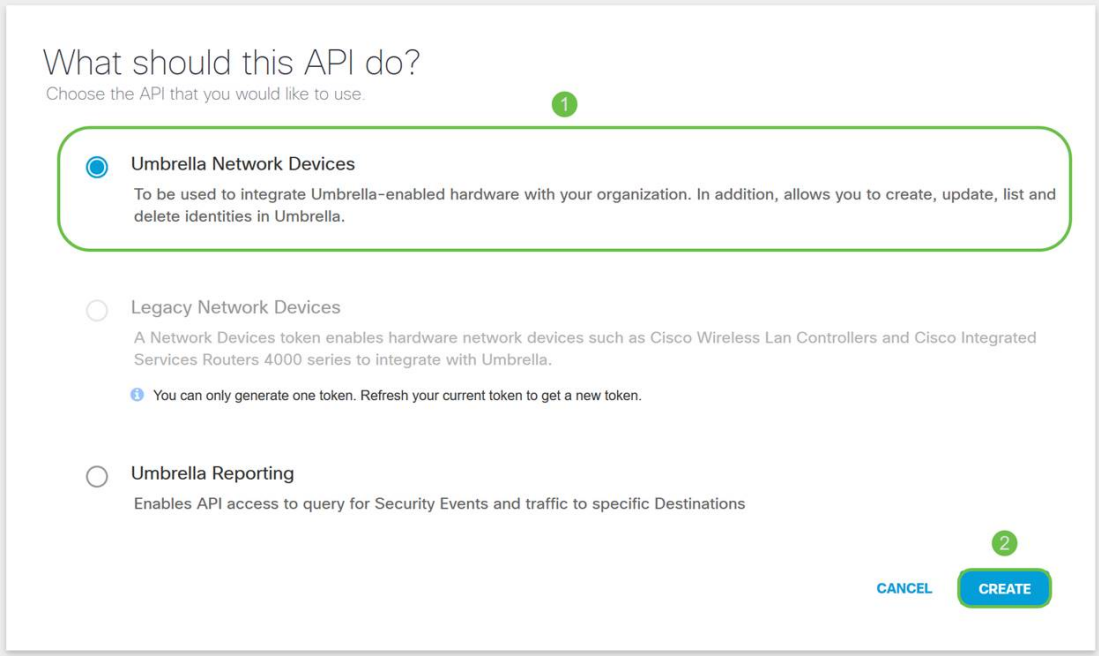
1. *Add API Key* - Initiates the creation of a new key for use with the Umbrella API.
2. *Additional Info* - Slides down/up with an explaination for this screen.
3. *Token Well* - Contains the all keys and tokens created by this account. (Populates once a key has been created)
4. *Support Documents* - Links to documentation on the Umbrella site pertaining to the topics in the each section.



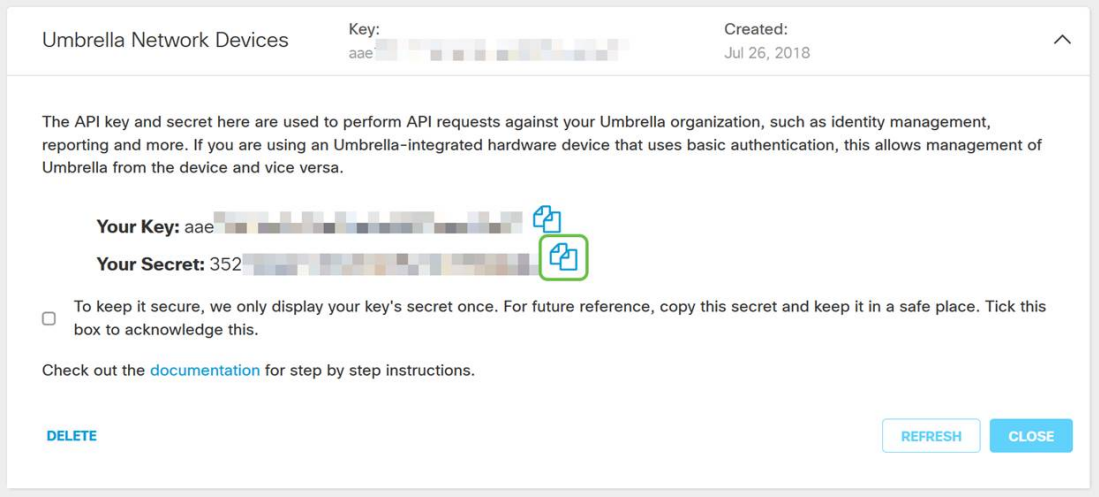
Step 2. Click on the **Add API Key** button in the upper-right hand corner, or click the **Create API Key** button. They both function the same.



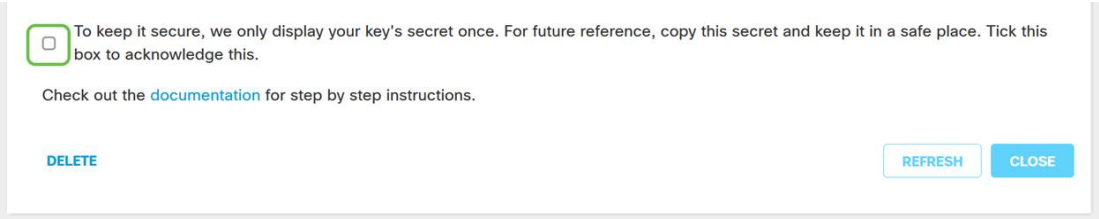
Step 3. Select **Umbrella Network Devices** and then click the **Create** button.



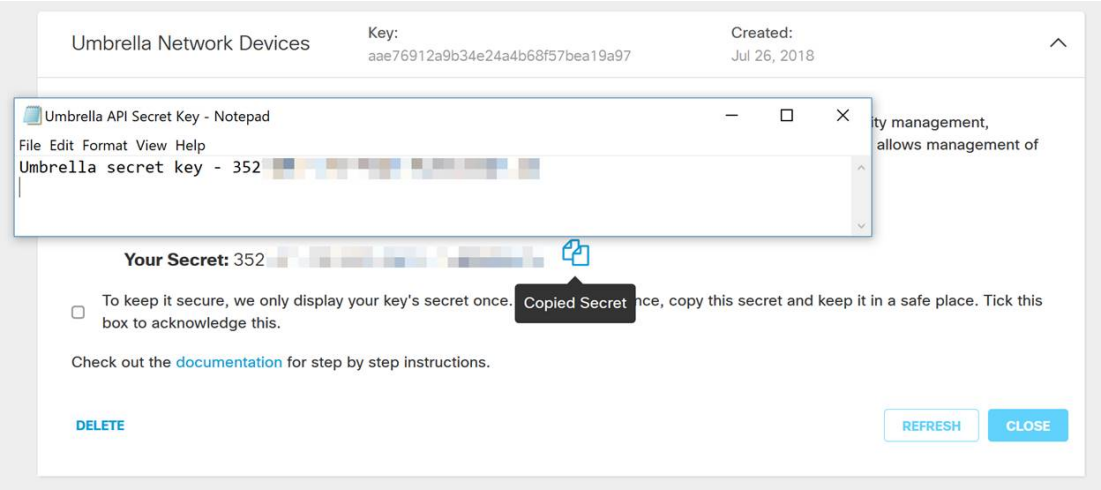
Step 4. Click the **Copy** button to the right of your *Secret Key,* a pop-up notification will confirm the key is copied to your clipboard.



After you've copied the key and secret key to a safe location, click the ***checkbox*** to confirm to complete acknowledgement then click the **Close** button.



Step 5. Open a text editor such as notepad and paste your secret and API key into the document, label them for future reference. In this case its label is "Umbrella secret key". Include the API key with your secret key along with a short description of its use in this same text file. Then save the text file to a secure location that's easy to access later should you need.



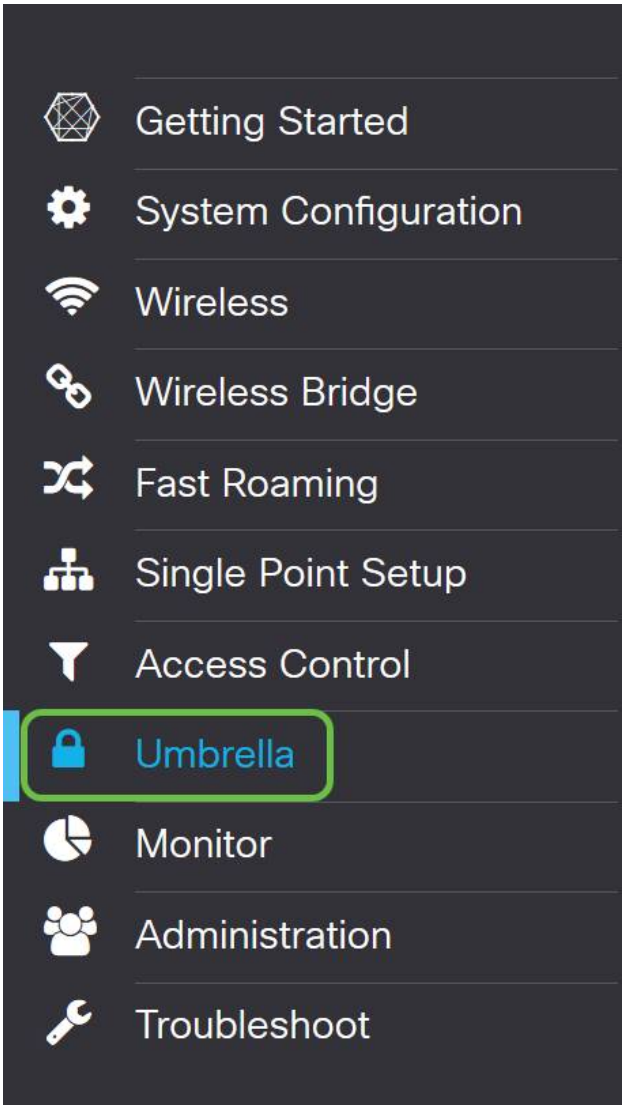
Important Note: If you lose or accidentally delete the secret key there is no function or support number to call to retrieve this key. Keep it secret, keep it safe. If lost, you will need to delete the key and re-authorize the API key with each WAP device you wish to protect with Umbrella.

Best Practice: Keep just a *single* copy of this document on a device, like a USB thumb drive, inaccessible from any network.

Configuring Umbrella on your WAP Device

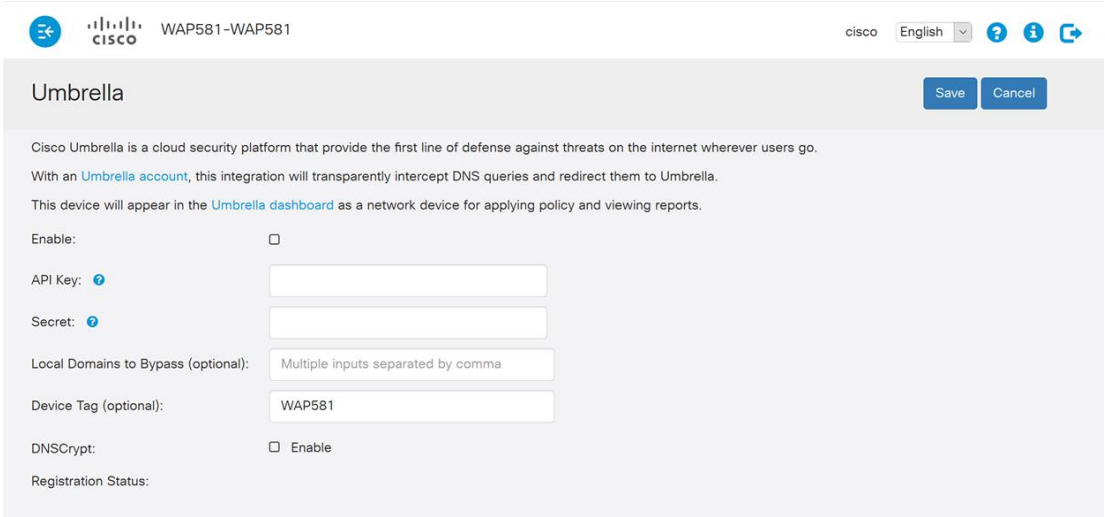
Now that we've created API keys within Umbrella, we'll take those keys and install them on our WAP Devices. In our case we are using a WAP581.

Step 1. After logging into your WAP Device, click on **Umbrella** in the sidebar menu.

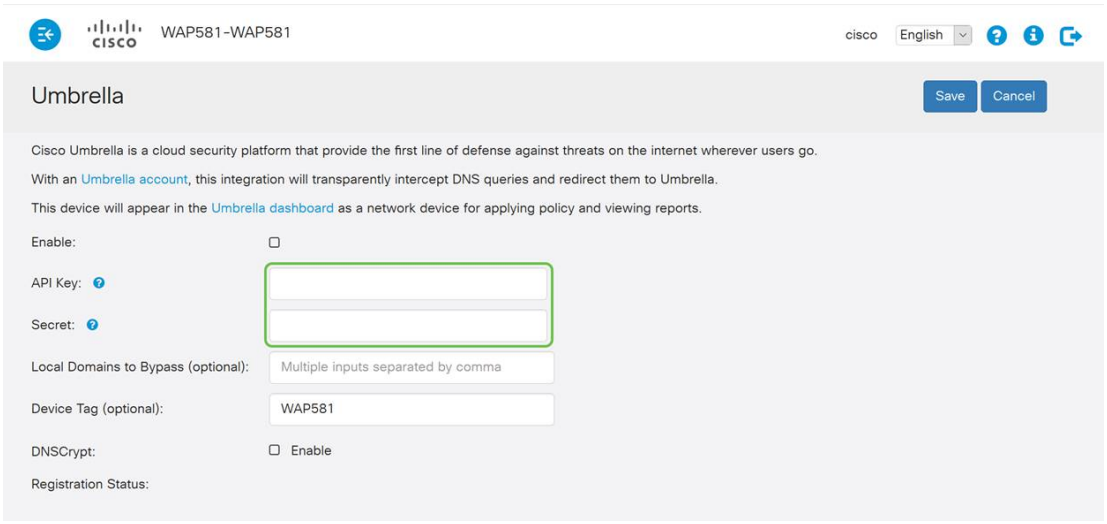


Step 2. The Umbrella screen is straightforward, but there are two fields worth defining here:

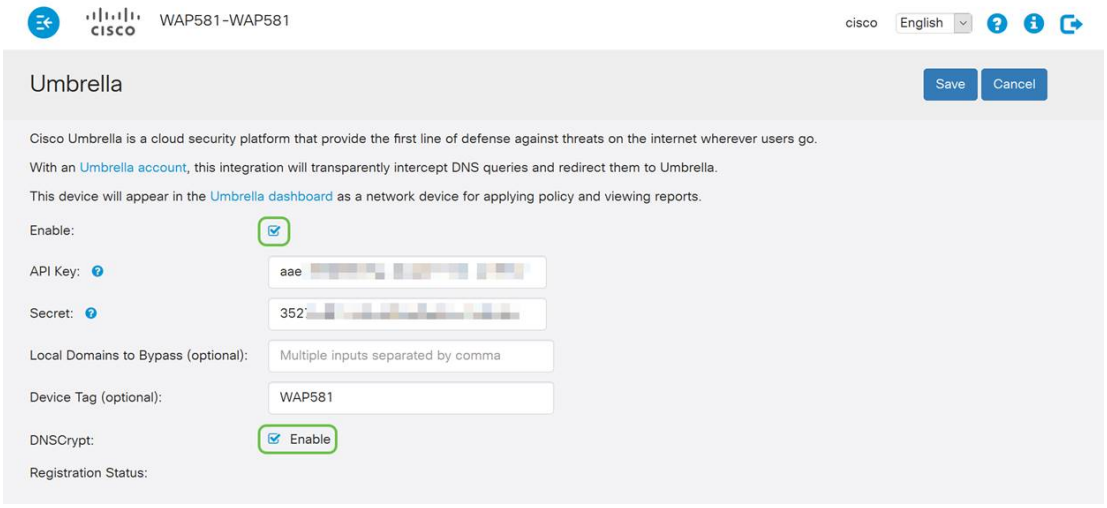
- *Local Domains to Bypass* - This field contains your internal domains that you would like to be excluded from the Umbrella service.
- *DNSCrypt* - Secures the transfer of packets between the DNS client and the DNS Resolver. This feature is on by default, disabling this feature will make your network less secure.



Step 3. Paste your API and Secret Key into the corresponding fields

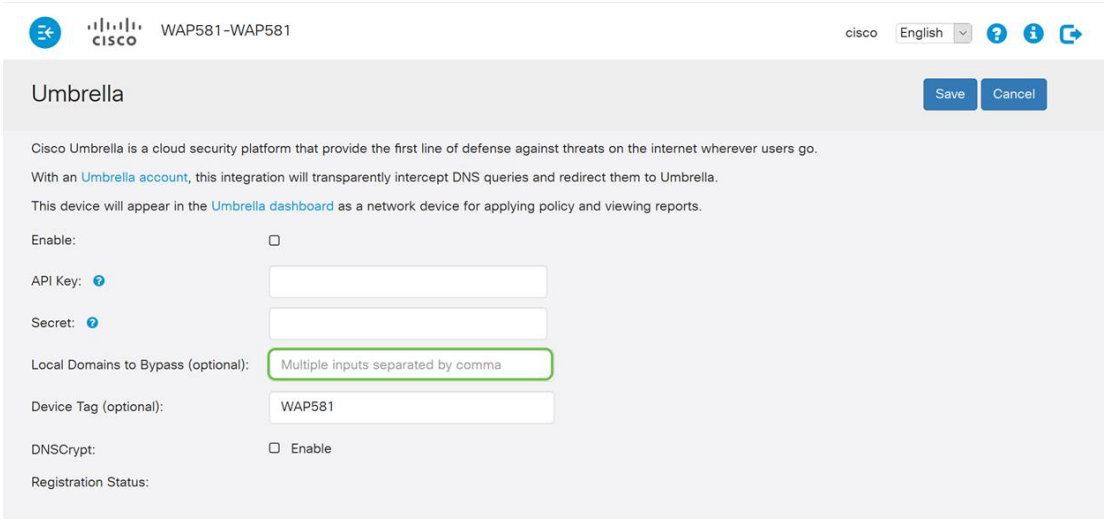


Step 4. Ensure the checkboxes for **Enable** and **DNSCrypt** are toggled the check state.



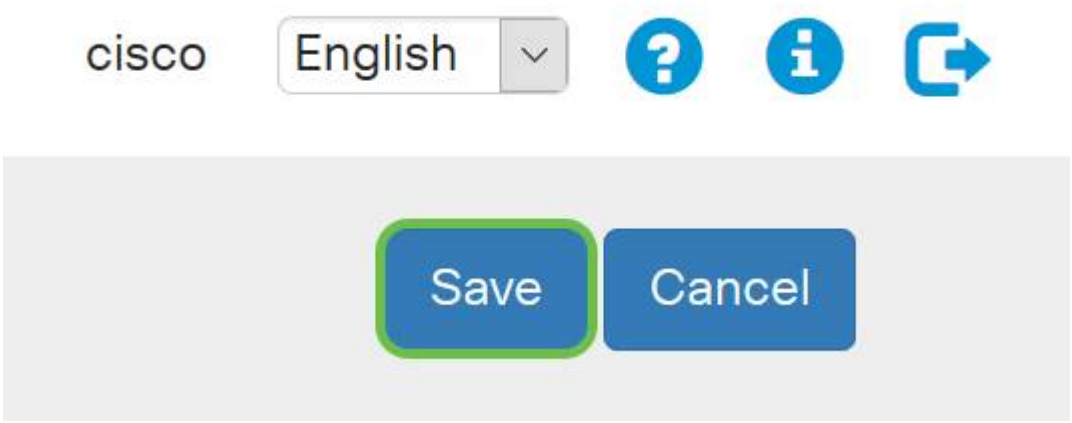
Note: DNSCrypt secures DNS communication between a DNS client and a DNS resolver. Default is enabled.

Step 5. (Optional) Enter the local domains you would like Umbrella to allow through the DNS resolution process.

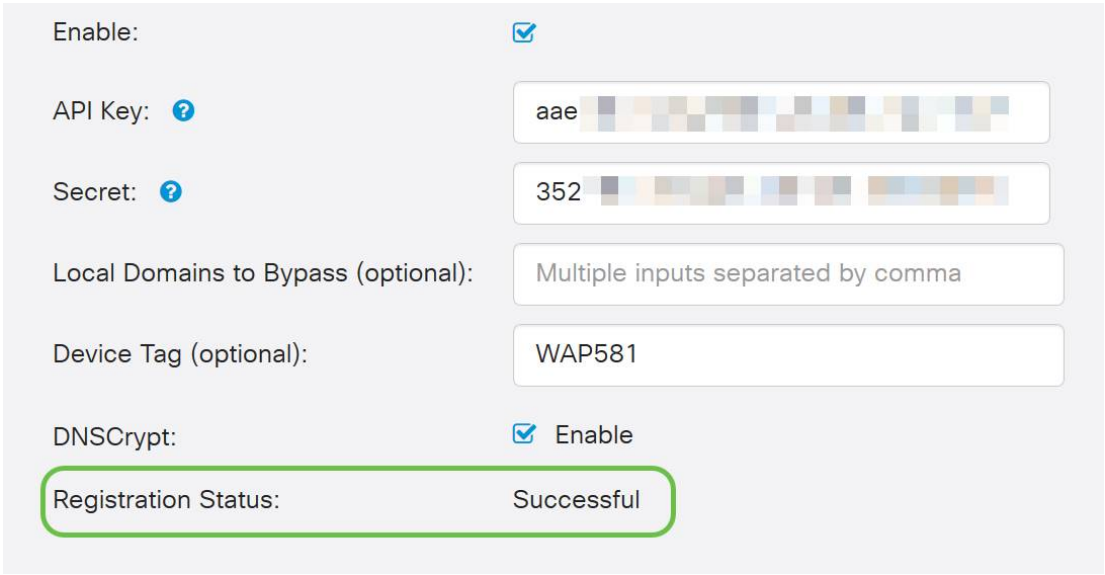


Note: This is required for all intranet domains and split DNS domains. If your network requires the use of local area domains for routing, you will need to contact Umbrella support to get this feature up and running. Most users will not need to use this option.

Step 6. After you are satisfied with the changes or have added your own *Local Domains to Bypass* , click the **Save** button in the upper-right hand corner.



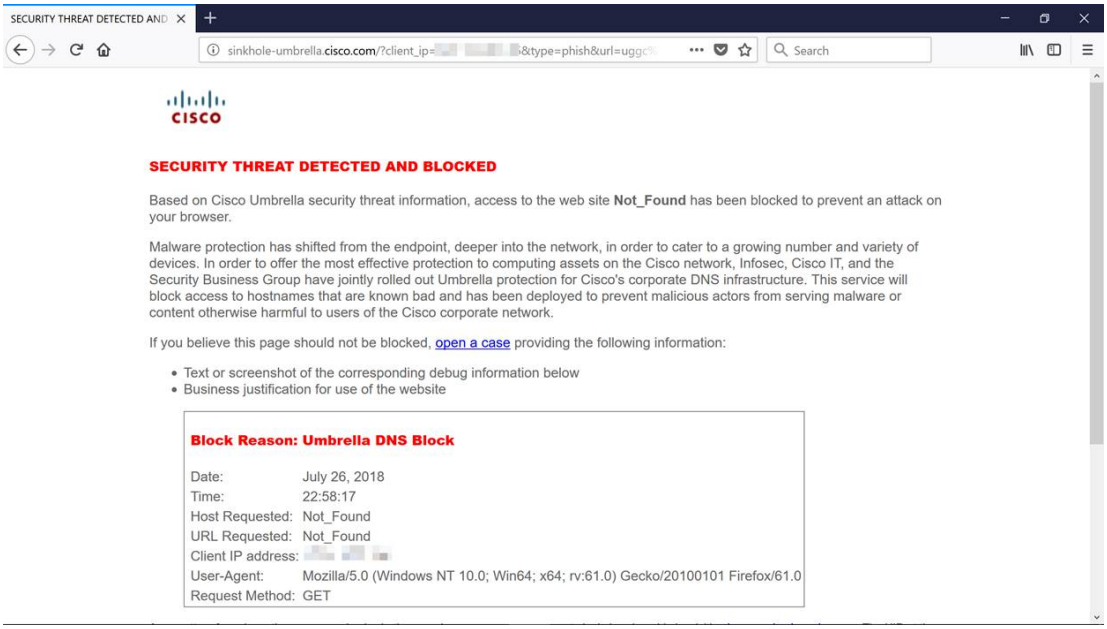
Step 7. When the changes are complete, the field *Registration Status* will read "Successful".



Confirming everything is in its right place

Congratulations, you are now protected Cisco's Umbrella. Or are you? Let's be sure, Cisco has created a website dedicated to determining this as quickly as the page loads. Click here or type https://InternetBadGuys.com into the browser bar.

If Umbrella is configured correctly you will be greeted by a screen similar to this!



View a video related to this article...

[Click here to view other Tech Talks from Cisco]