

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?

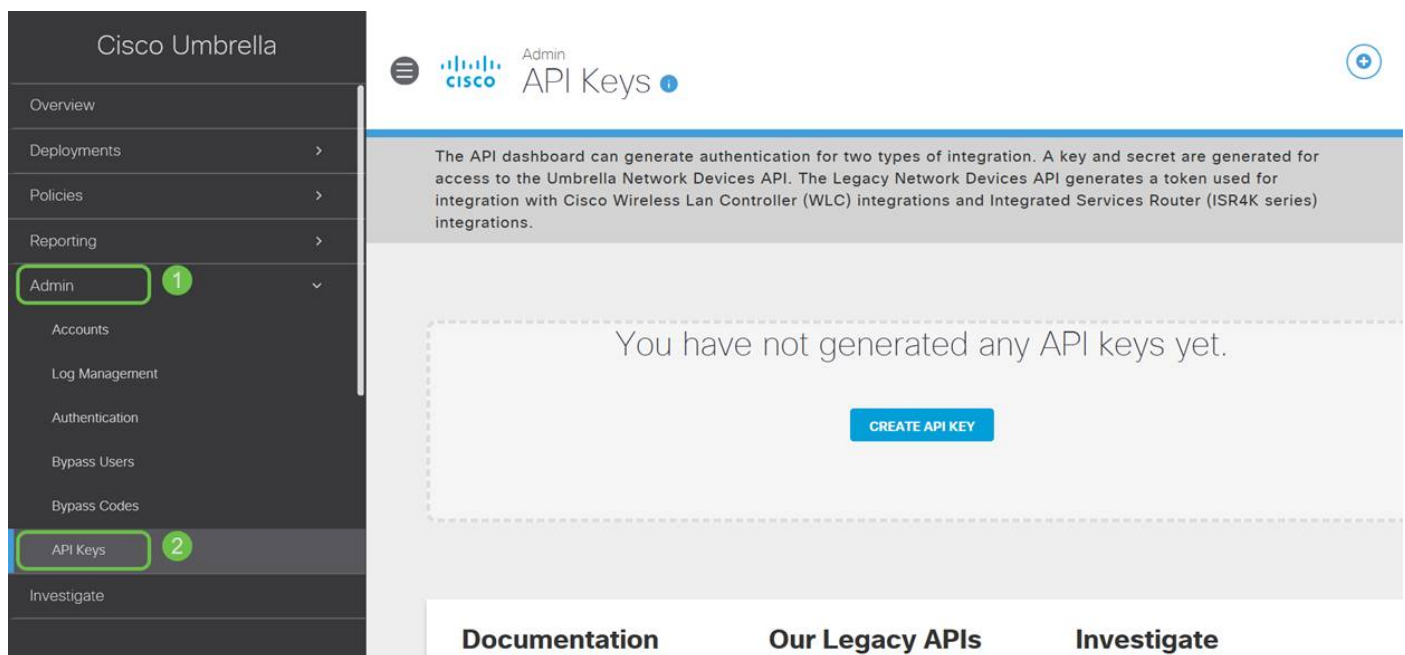
Umbrella uses DNS as its main vector for defense. When users enter a URL in their browser bar and hit Enter, Umbrella participates in the transfer. That URL passes to Umbrella's DNS resolver, and if a security warning associates with the domain, the request is blocked. This telemetry data transfers and 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**.



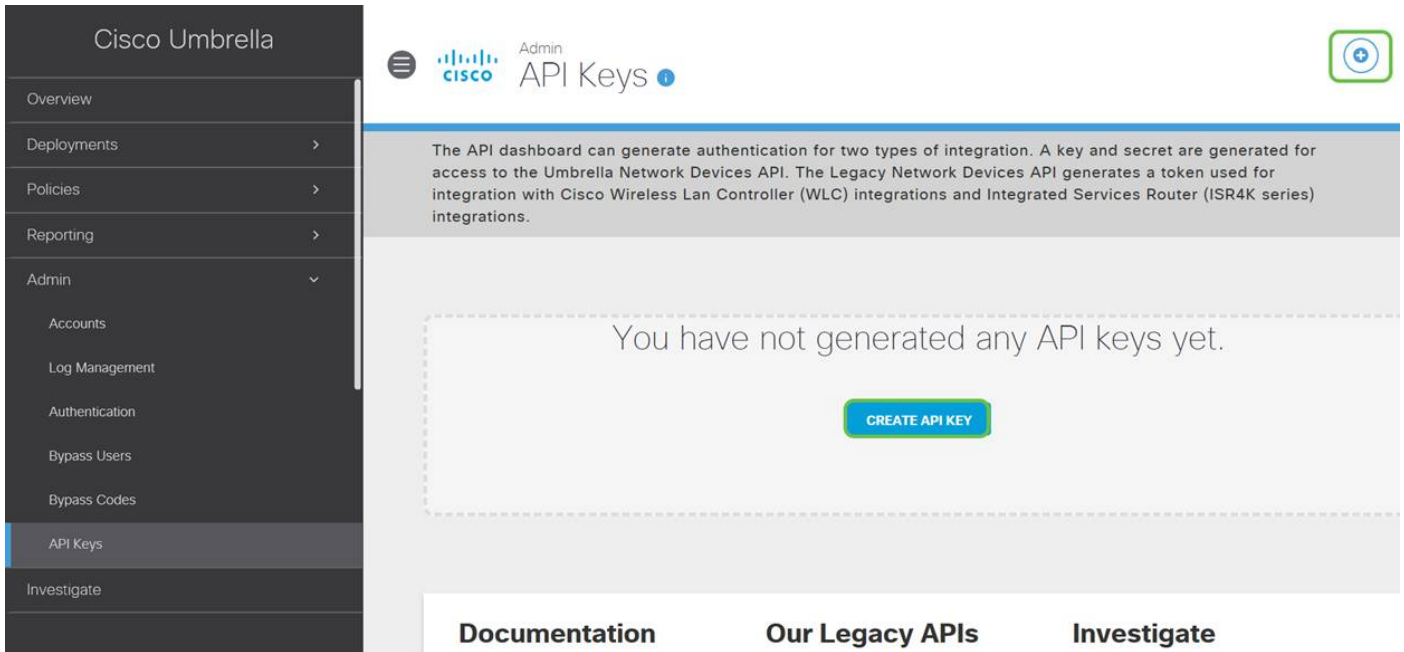
The screenshot shows the Cisco Umbrella Admin interface for API Keys. On the left is a dark sidebar menu with 'Admin' (1) expanded to show 'API Keys' (2). The main content area has a header 'Admin API Keys' and a blue bar with text explaining that the dashboard generates authentication for two types of integration: the Umbrella Network Devices API and the Legacy Network Devices API. Below this is a large dashed box containing the message 'You have not generated any API keys yet.' and a blue 'CREATE API KEY' button. At the bottom are three links: 'Documentation', 'Our Legacy APIs', and 'Investigate'.

Anatomy of the API Keys Screen -

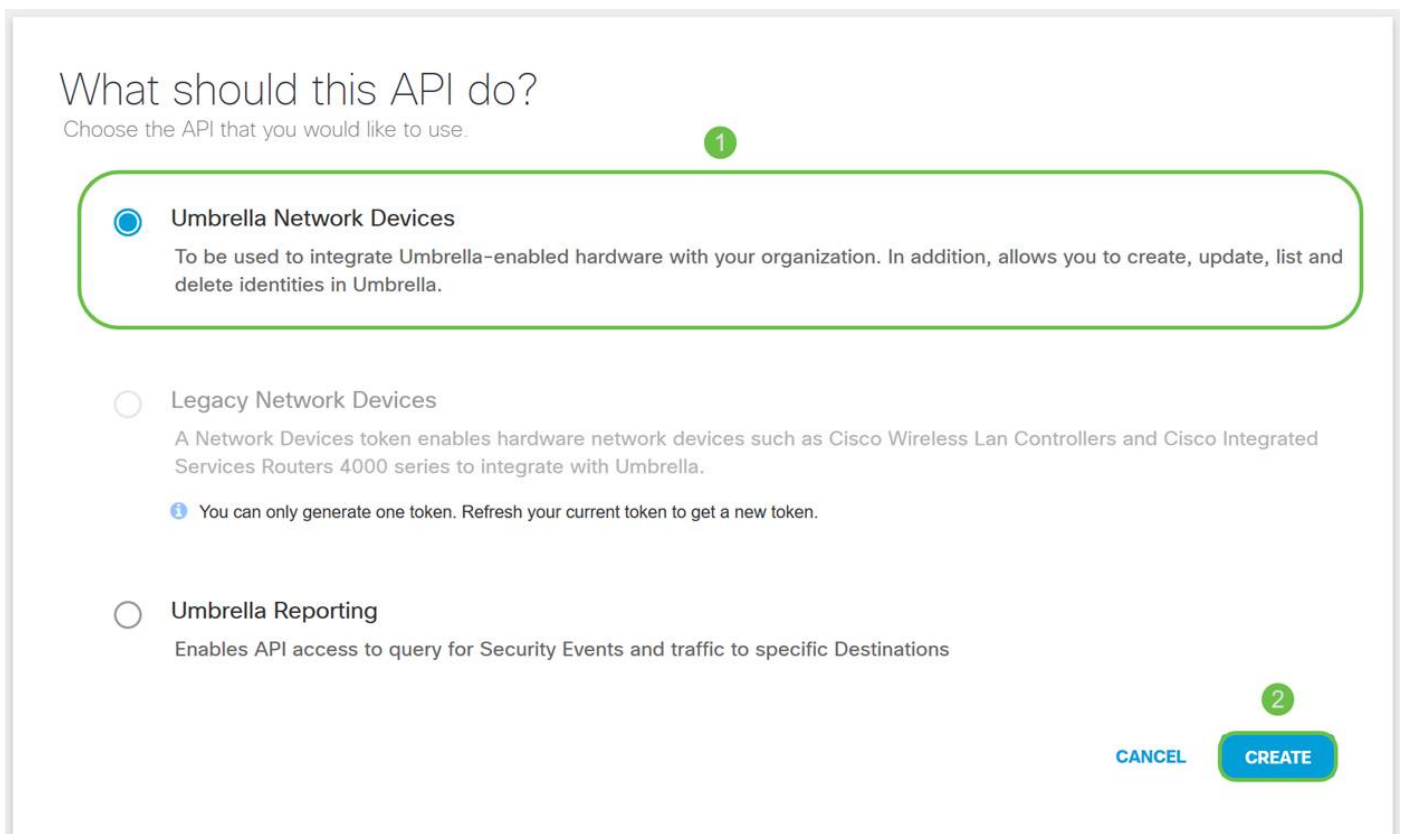
1. *Add API Key* - Initiates the creation of a new key for use with the Umbrella API.
2. *Additional Info* - Slides down/up with an explanation for this screen.
3. *Token Well* - Contains the all keys and tokens created by this account. (Populates once a key has been created)
4. *Support Documents* -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

The screenshot displays the Cisco Umbrella Admin Keys API interface. At the top left, the Cisco logo and 'Admin Keys API' are visible, with a green circle containing the number '2' next to an information icon. In the top right corner, there is a green circle with the number '1' and a blue plus icon. The main content area features a table with one row: 'Legacy Network Devices', 'Tokens: A56C3ECCF6A245D0B83ACA2A0EEE8629002...', and 'created: Apr 18, 2018'. A green circle with the number '3' is positioned above the table. Below the table is a section with three columns: 'Documentation', 'Our Legacy APIs', and 'investigate'. Each column contains a short paragraph and a 'VIEW DOCS' button. A green circle with the number '4' is positioned above the 'Documentation' column.

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.

Umbrella Network Devices Key: [redacted] Created: Jul 26, 2018

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: aae [redacted] 

Your Secret: 352 [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](#)

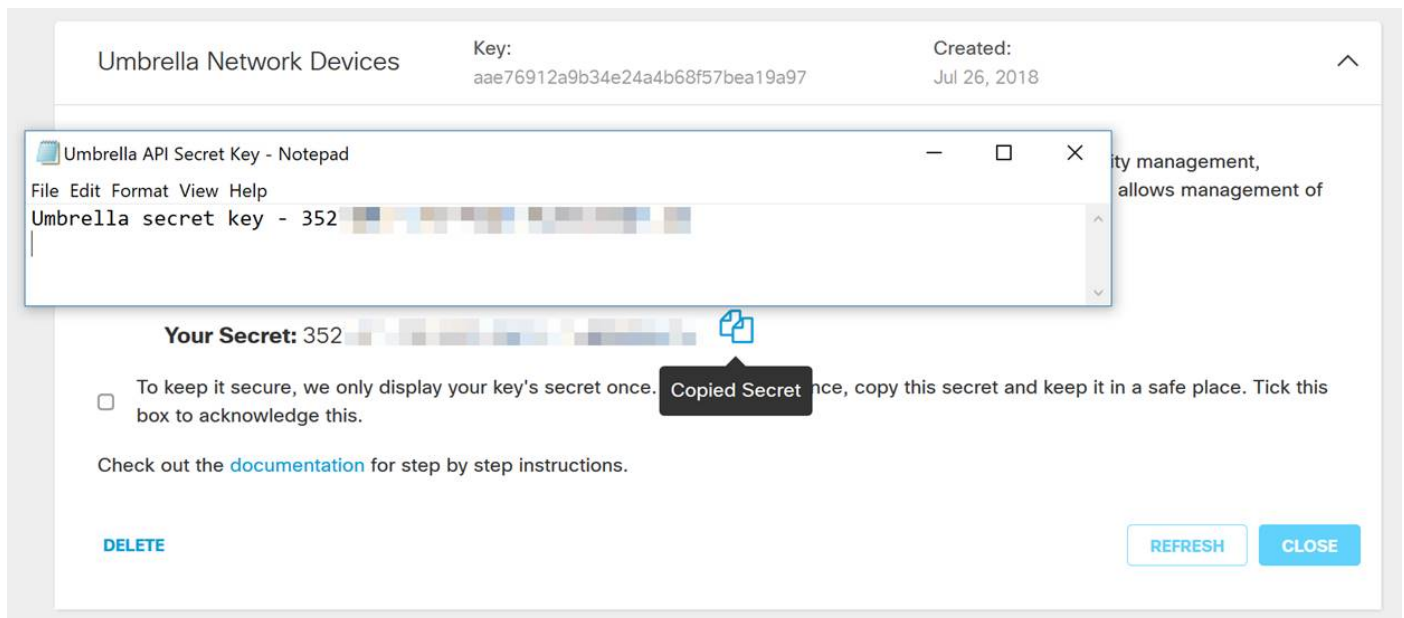
After you've copied the key and secret key to a safe location, click the **checkbox** to confirm to complete acknowledgement then click the **Close** button.

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](#)

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.



Getting Started



System Configuration



Wireless



Wireless Bridge



Fast Roaming



Single Point Setup



Access Control



Umbrella



Monitor



Administration

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.
- *DNSEncrypt* - 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.

The screenshot shows the Cisco Umbrella configuration interface for a device named WAP581-WAP581. The page title is "Umbrella" and it includes "Save" and "Cancel" buttons. The main content area contains the following fields and options:

- Enable:** An unchecked checkbox.
- API Key:** A text input field with a help icon.
- Secret:** A text input field with a help icon.
- 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".
- DNSEncrypt:** An unchecked checkbox with the label "Enable".
- Registration Status:** A label with no associated input field.

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

This screenshot is identical to the previous one, but with a green rectangular box highlighting the "API Key" and "Secret" input fields. The "Enable" checkbox is still unchecked, and the "DNSEncrypt" checkbox is checked.

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

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):

DNSEncrypt: Enable

Registration Status:

Note: DNSEncrypt 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.

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):

DNSEncrypt: Enable

Registration Status:

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.

cisco

English



Save

Cancel

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

Enable:



API Key: 

aae

Secret: 

352

Local Domains to Bypass (optional):

Multiple inputs separated by comma

Device Tag (optional):

WAP581

DNSEncrypt:



Enable

Registration Status:

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!

SECURITY THREAT DETECTED AND B... 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

View a video related to this article...

[Click here to view other Tech Talks from Cisco](#)