How To: Recover a lost Umbrella Secret Key

Objective

If you've ever lost an irretrievable key, you know how quickly blood can begin pumping through your body. This article will show you how to recover from losing your secret Application Programming Interface (API) key. This secret key displays only once when generated, and is not displayed again. If you navigate the browser away from the API key screen then you may lose that information.

Applicable Devices

- WAP125
- WAP581

Software Version

- 1.0.1

Requirements

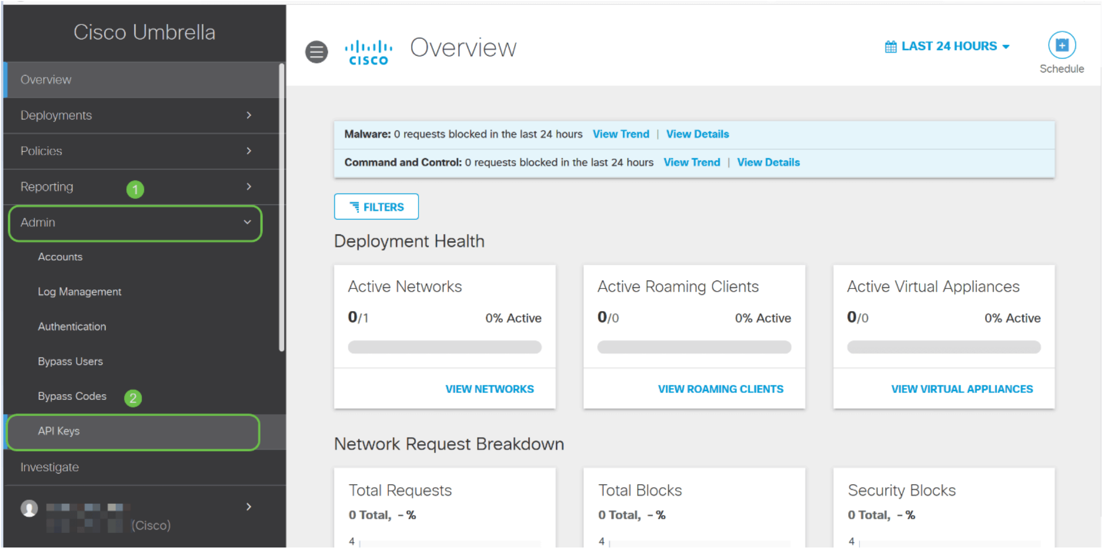
- An active Umbrella account (Don't have one? Request a quote or start a free trial)

Help, I've lost my Secret Key!

Here's the tough news, your secret key, it's lost to the ether-net, gone. Where this turns into better news, is that the recovery process isn't all that painful. By generating a new API key, you generate a new secret key. So the recovery process involves deleting the API key associated with the lost key and generating the new API key set.

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**.



Malware: 0 requests blocked in the last 24 hours View Trend | View Details

Command and Control: 0 requests blocked in the last 24 hours View Trend | View Details

Deployment Health

Active Networks 0/1 0% Active

Active Roaming Clients 0/0 0% Active

Active Virtual Appliances 0/0 0% Active

Network Request Breakdown

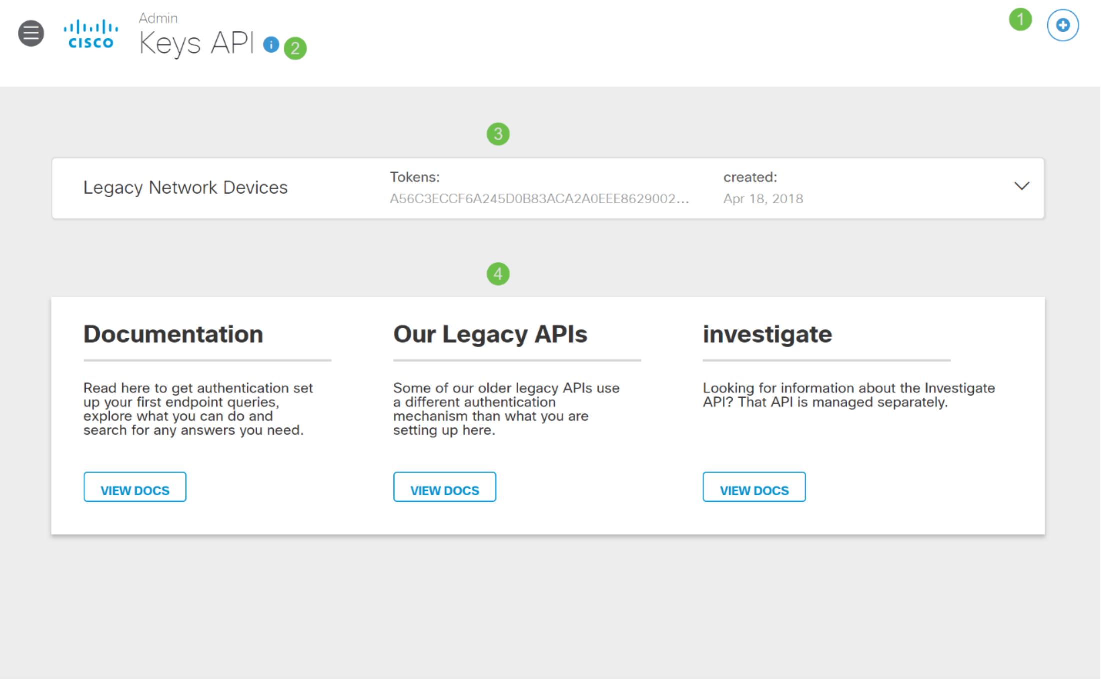
Total Requests 0 Total, - %

Total Blocks 0 Total, - %

Security Blocks 0 Total, - %

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 explainer 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.



Legacy Network Devices Tokens: A56C3ECCF6A245D0B83ACA2A0EEE8629002... created: Apr 18, 2018

Documentation

Read here to get authentication set up your first endpoint queries, explore what you can do and search for any answers you need.

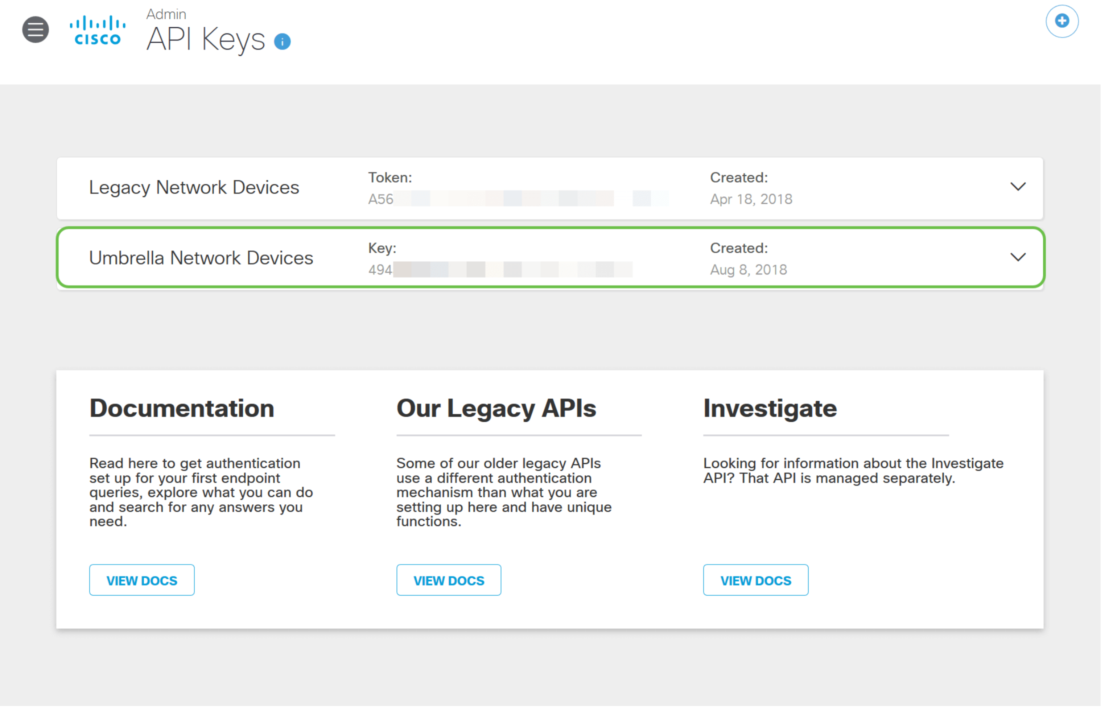
Our Legacy APIs

Some of our older legacy APIs use a different authentication mechanism than what you are setting up here.

investigate

Looking for information about the Investigate API? That API is managed separately.

Step 2. Click on the **Umbrella Network Devices** button in the *Token well*.



Legacy Network Devices | Token: A56[redacted] | Created: Apr 18, 2018

Umbrella Network Devices | Key: 494[redacted] | Created: Aug 8, 2018

Documentation

Read here to get authentication set up for your first endpoint queries, explore what you can do and search for any answers you need.

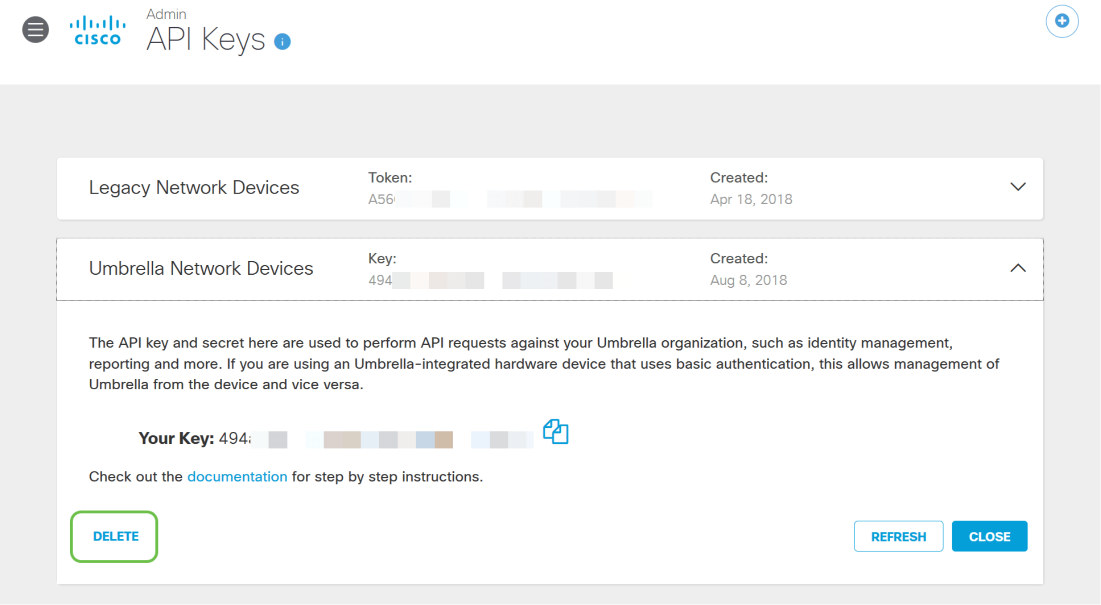
Our Legacy APIs

Some of our older legacy APIs use a different authentication mechanism than what you are setting up here and have unique functions.

Investigate

Looking for information about the Investigate API? That API is managed separately.

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



Legacy Network Devices | Token: A56[redacted] | Created: Apr 18, 2018

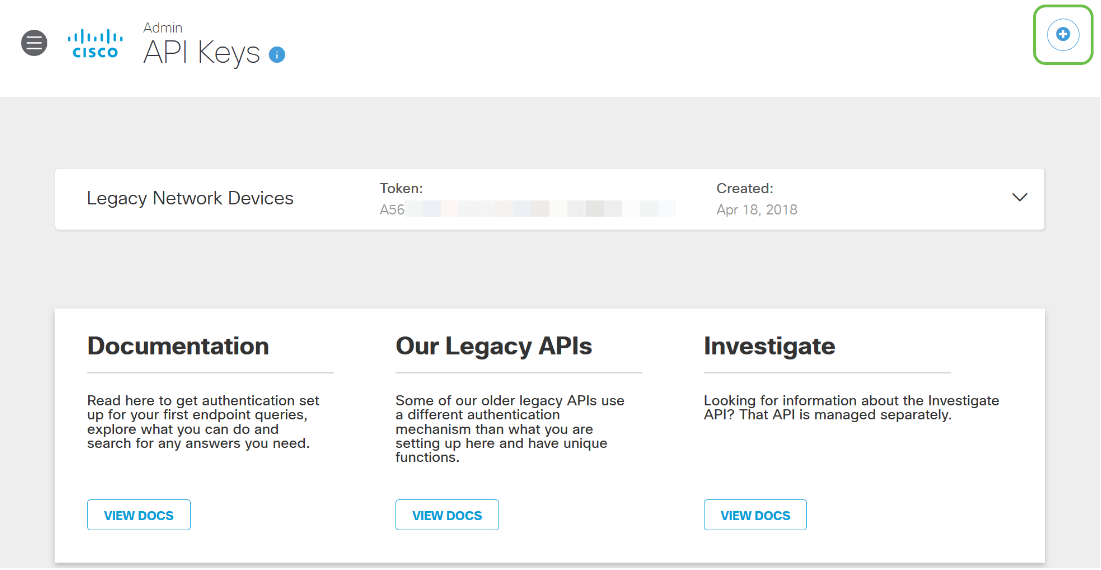
Umbrella Network Devices | Key: 494[redacted] | Created: Aug 8, 2018

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: 494[redacted]

Check out the documentation for step by step instructions.

Step 4. The key will be instantly deleted. 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.



API Keys

Legacy Network Devices — Token: A56[redacted] — Created: Apr 18, 2018

Documentation

Read here to get authentication set up for your first endpoint queries, explore what you can do and search for any answers you need.

VIEW DOCS

Our Legacy APIs

Some of our older legacy APIs use a different authentication mechanism than what you are setting up here and have unique functions.

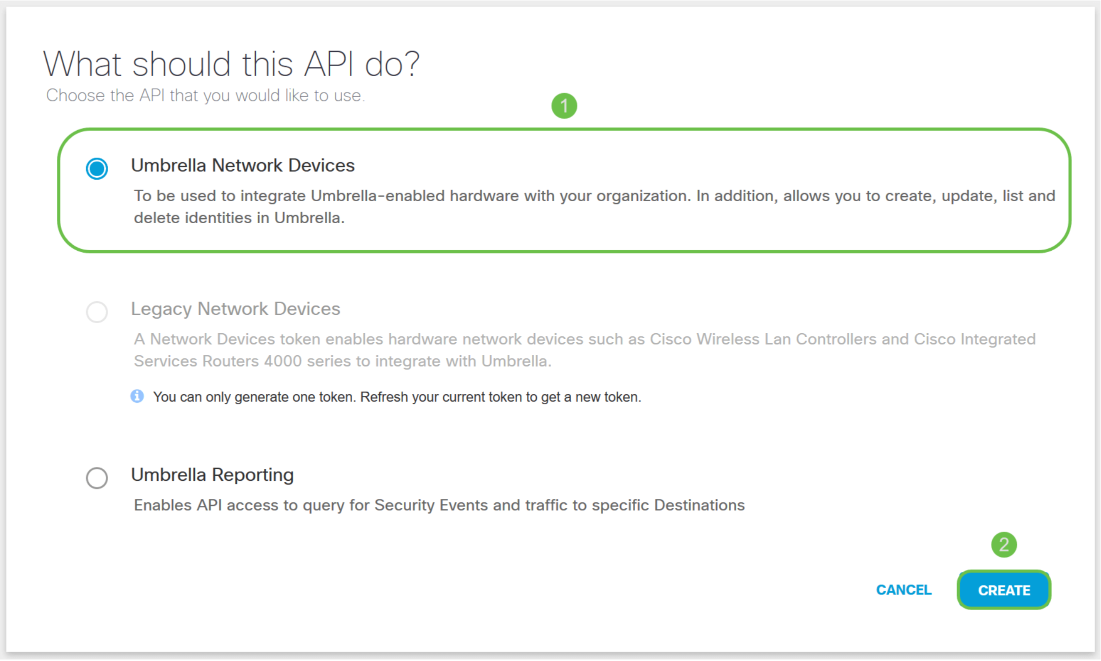
VIEW DOCS

Investigate

Looking for information about the Investigate API? That API is managed separately.

VIEW DOCS

Step 5. Select **Umbrella Network Devices** and then click the **Create** button.



What should this API do?

Choose the API that you would like to use.

● Umbrella Network Devices

To be used to integrate Umbrella-enabled hardware with your organization. In addition, allows you to create, update, list and delete identities in Umbrella.

○ Legacy Network Devices

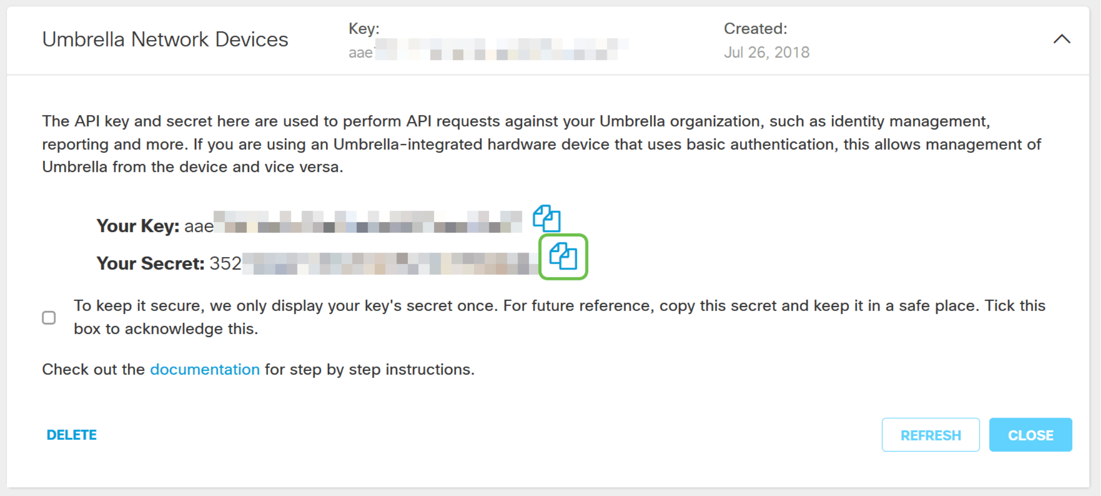
A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.

You can only generate one token. Refresh your current token to get a new token.

○ Umbrella Reporting

Enables API access to query for Security Events and traffic to specific Destinations

Step 6. 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: aae[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.

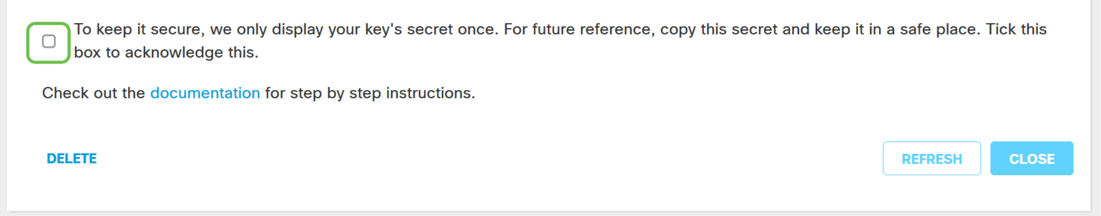
Your Key: aae[redacted]

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.

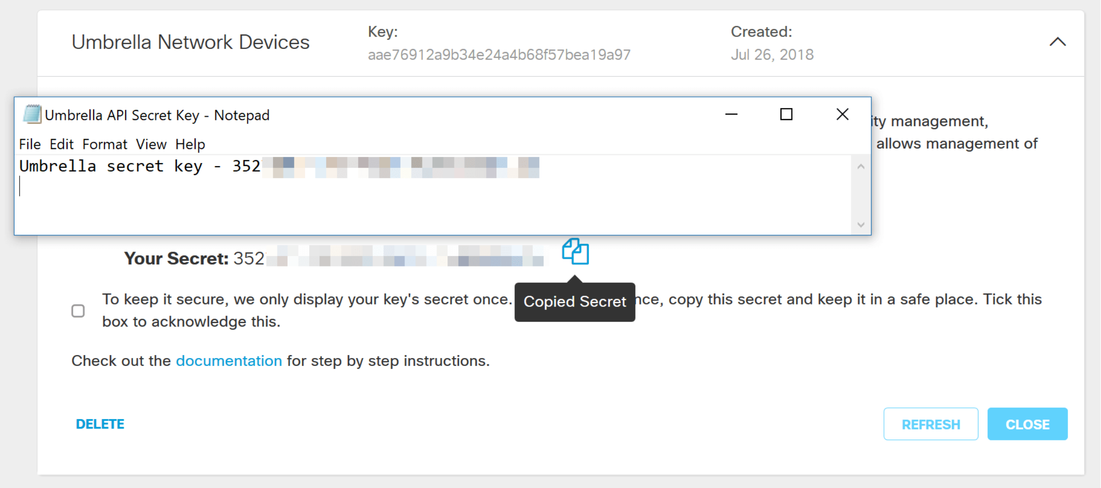
After you've copied the key and secret key to a safe location, click the ***checkbox*** to confirm to complete acknowledgement then click the **Close** button.



☐ 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.

Step 7. 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.



Umbrella Network Devices

Key: aae76912a9b34e24a4b68f57bea19a97

Created: Jul 26, 2018

Umbrella API Secret Key - Notepad

```
Umbrella secret key - 352[redacted]
```

ity management, allows management of

Your Secret: 352[redacted]

☐ To keep it secure, we only display your key's secret once. Copied Secret nce, 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.

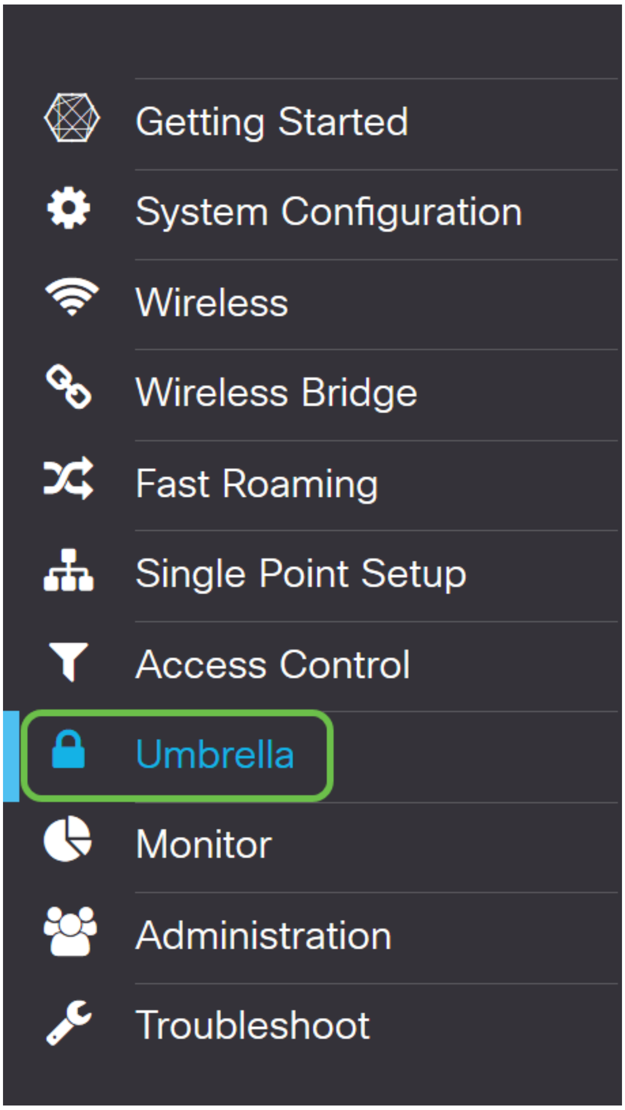
Important Note: If you lose or accidentally delete the secret key there is no function or support number to call to retrieve this key. Keep it secret, keep it safe. If lost, you will need to delete the key and re-authorize the API key with each WAP device you wish to protect with Umbrella.

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

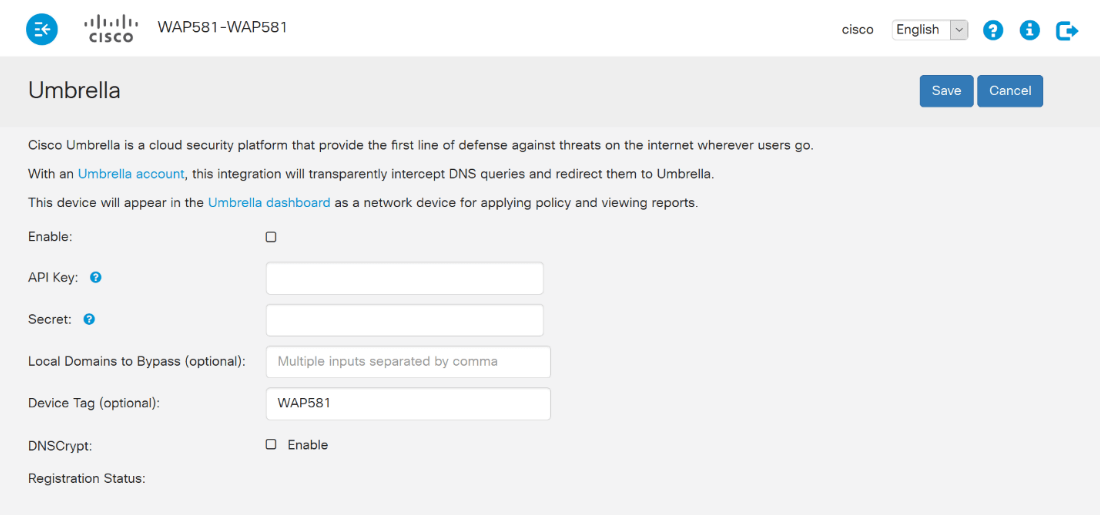
Now that we've created API keys within Umbrella, we'll take those keys and install them on our WAP Devices. In our case we are using a WAP581.

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.



Umbrella

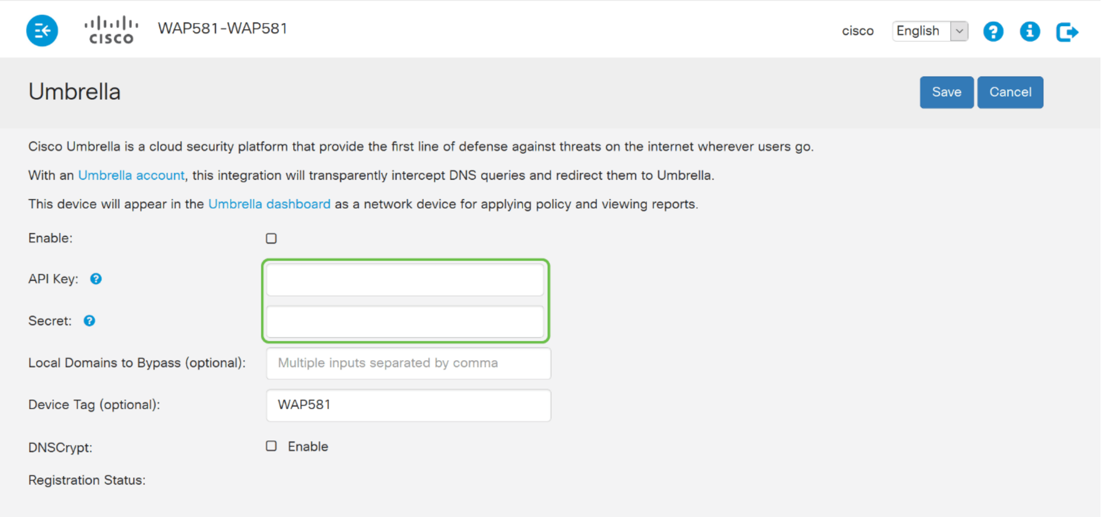
Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.

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):	Multiple inputs separated by comma
Device Tag (optional):	WAP581
DNSCrypt:	□ Enable
Registration Status:	

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



Umbrella

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:

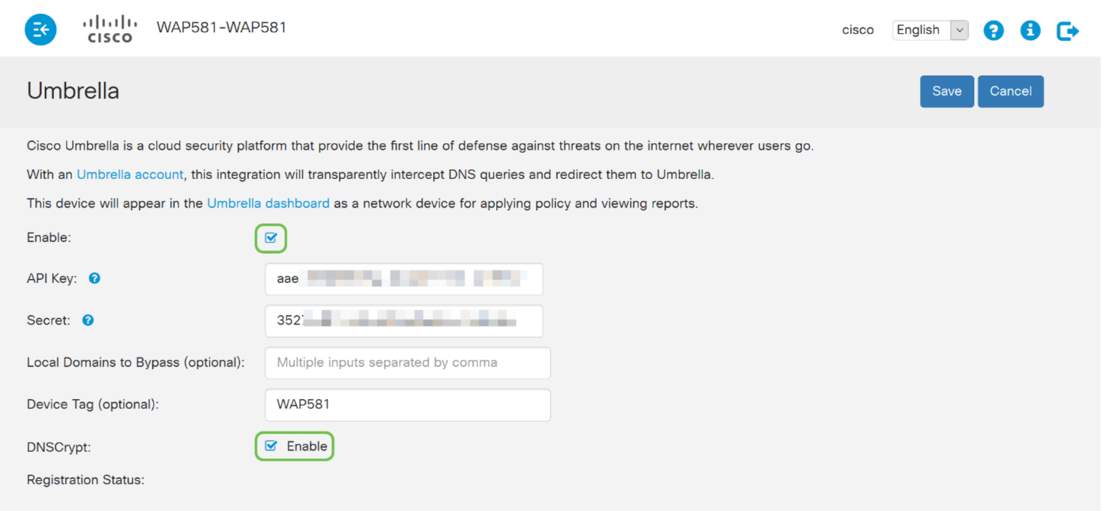
Local Domains to Bypass (optional): Multiple inputs separated by comma

Device Tag (optional): WAP581

DNSCrypt: □ Enable

Registration Status:

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



Umbrella

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: aae[redacted]

Secret: 352[redacted]

Local Domains to Bypass (optional): Multiple inputs separated by comma

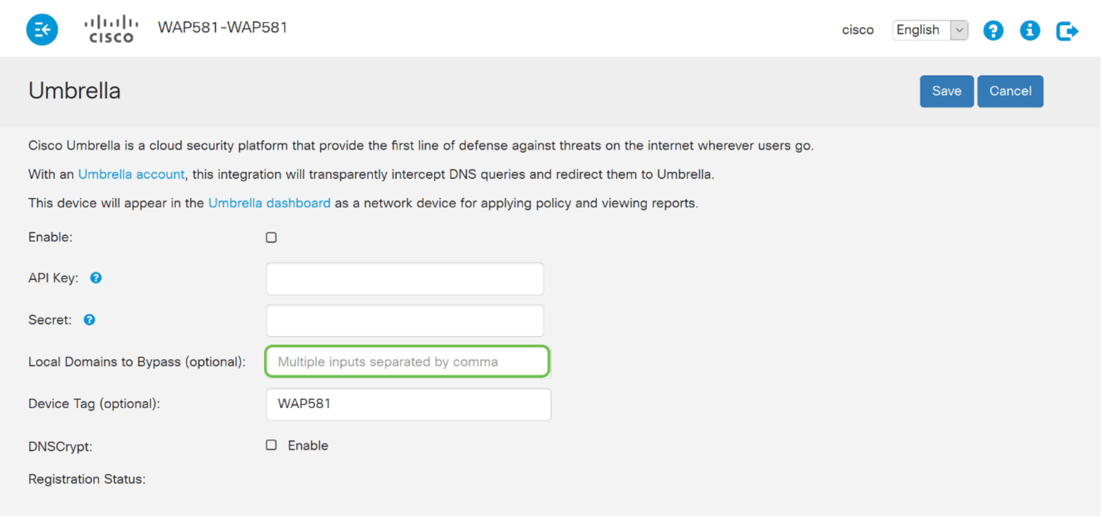
Device Tag (optional): WAP581

DNSCrypt: ☑ Enable

Registration Status:

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.



Umbrella

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): Multiple inputs separated by comma

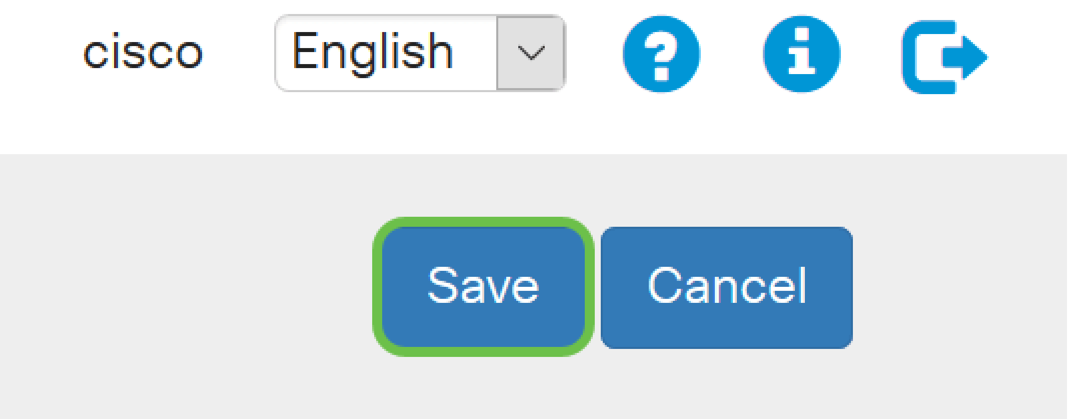
Device Tag (optional): WAP581

DNSCrypt: □ Enable

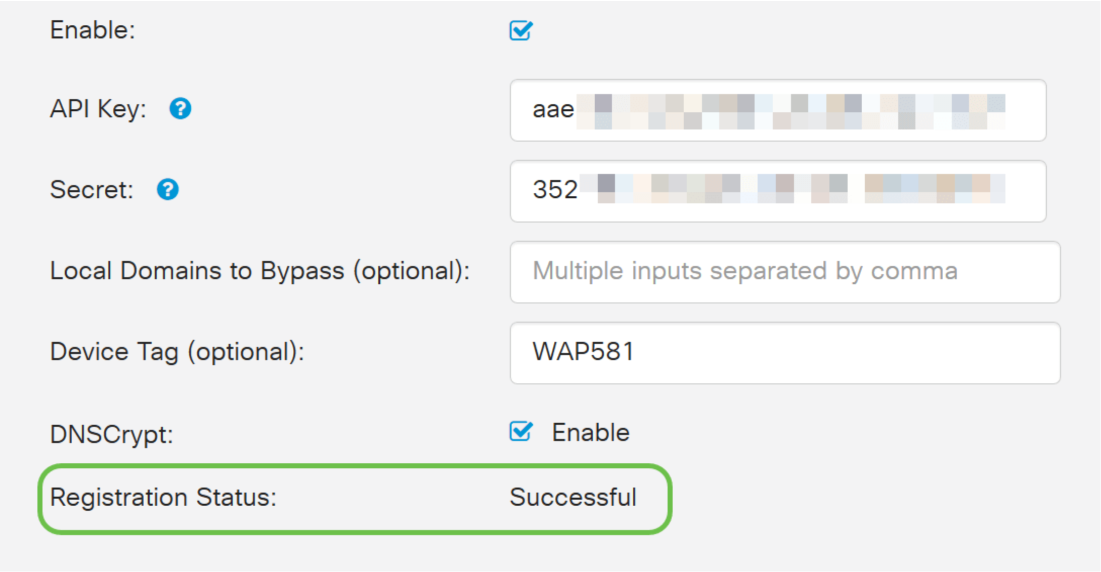
Registration Status:

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.



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



Enable: ☑

API Key: aae [redacted]

Secret: 352 [redacted]

Local Domains to Bypass (optional): Multiple inputs separated by comma

Device Tag (optional): WAP581

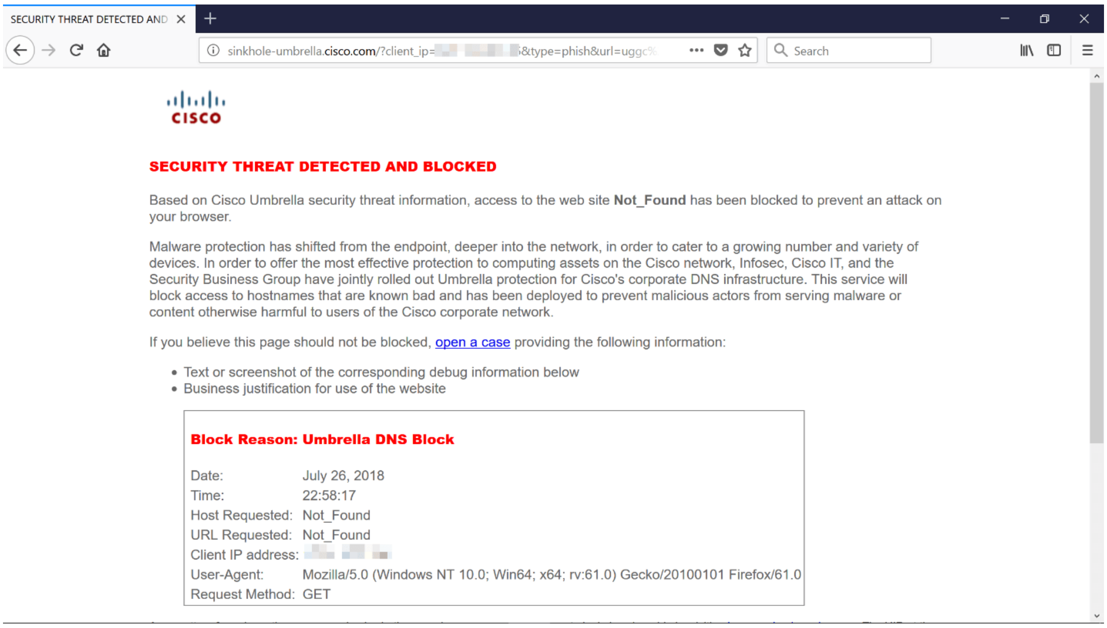
DNSCrypt: ☑ Enable

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!



sinkhole-umbrella.cisco.com/?client_ip=[redacted]&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:	[redacted]
User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Request Method:	GET