Configuring Cisco Umbrella on your Network via RV34x series routers

Introduction

As of firmware version 1.0.0.2.16 the RV34x series routers now support Cisco Umbrella. Umbrella uses DNS as a defense vector or shield in defense against malware and data intrusions.

Applicable Devices

- RV34x series router

Software Version

- 1.0.02.16

Requirements

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

Objective

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

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?

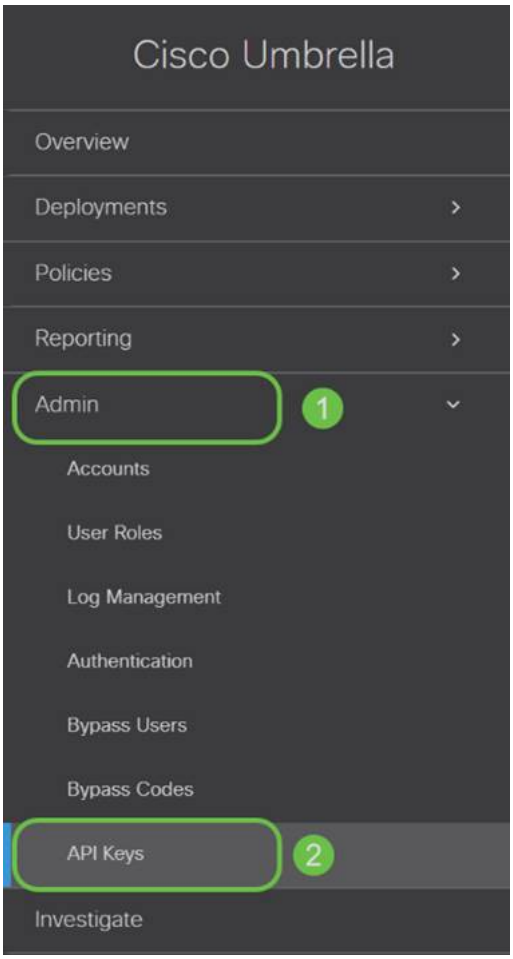
Umbrella uses DNS as its main vector for defense. When users enter a URL in their browser bar and hit Enter, Umbrella participates in the transfer. That URL passes to Umbrella's DNS resolver, and if a security warning associates with the domain, the request is blocked. This telemetry data transfers and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

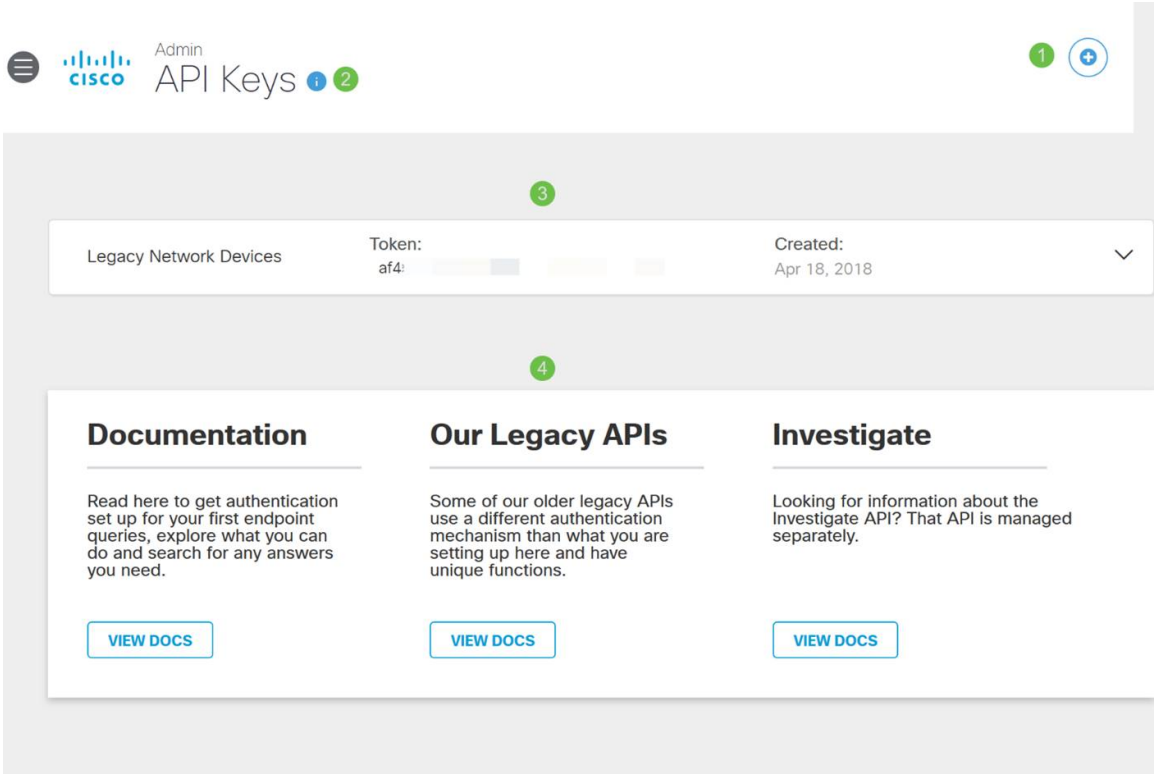
To summarize in a metaphor, imagine you're at a party. At this party everyone is on their phone surfing the web. The quiet group-silence is punctuated by the party-goers tapping away on their screens. It's not a great party, but while on your own phone you see a hyperlink to a kitten GIF that seems irresistible. However the URL appears questionable so you're unsure of if you should tap or not. 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 noble quest for pictures of cute animals. Of course, at the scale of Cisco this type of request and callback security checks are occurring millions of times a second, and that's to the benefit of security on your network.

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 router 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**.

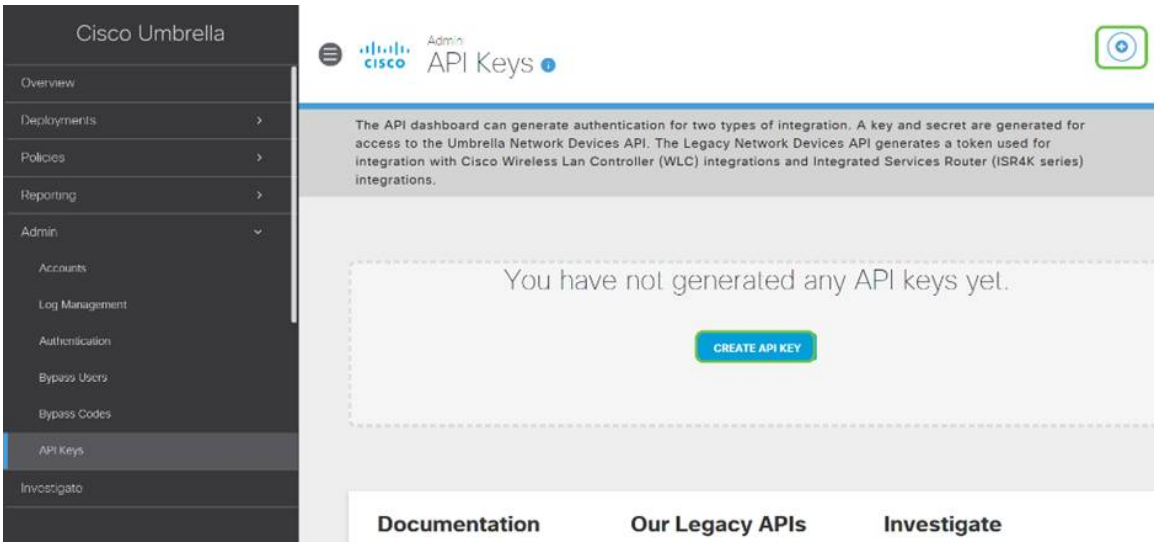




Anatomy of the API Keys Screen (with pre-existing API key) –

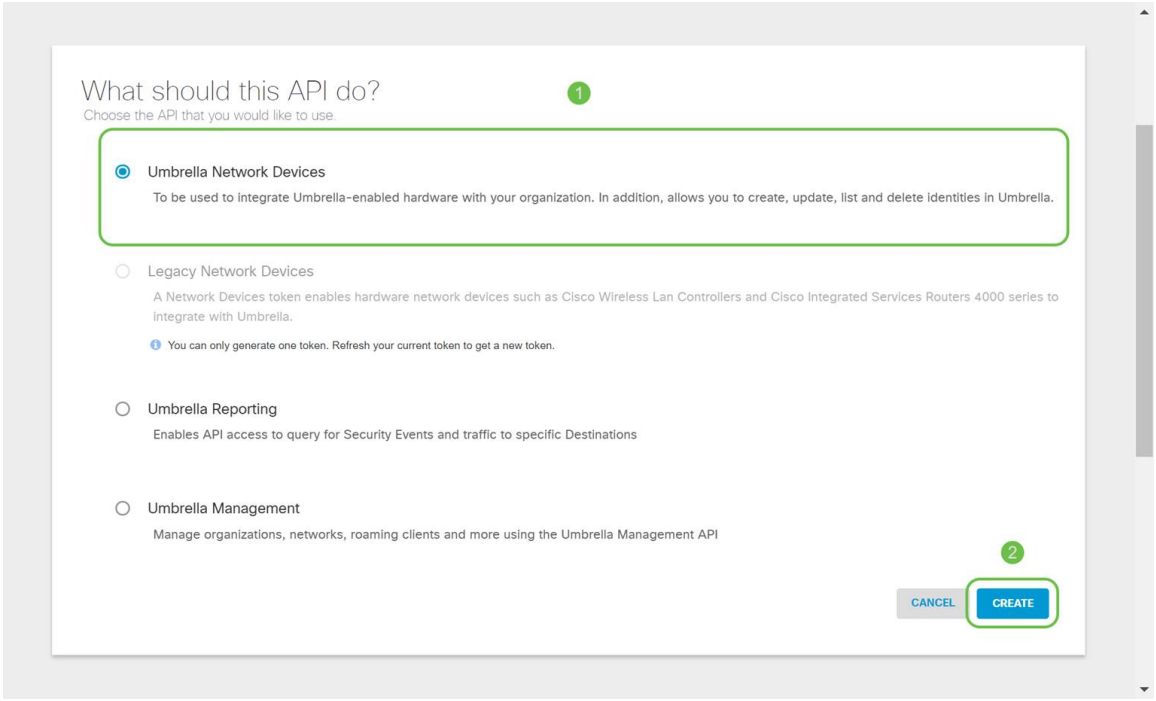
1. Add API Key – Initiates the creation of a new key for use with the Umbrella API.
2. Additional Info – Slides down/up with an explainer for this screen.
3. Token Well – Contains the all keys and tokens created by this account. (Populates once a key has been created)
4. Support Documents – Links to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

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.

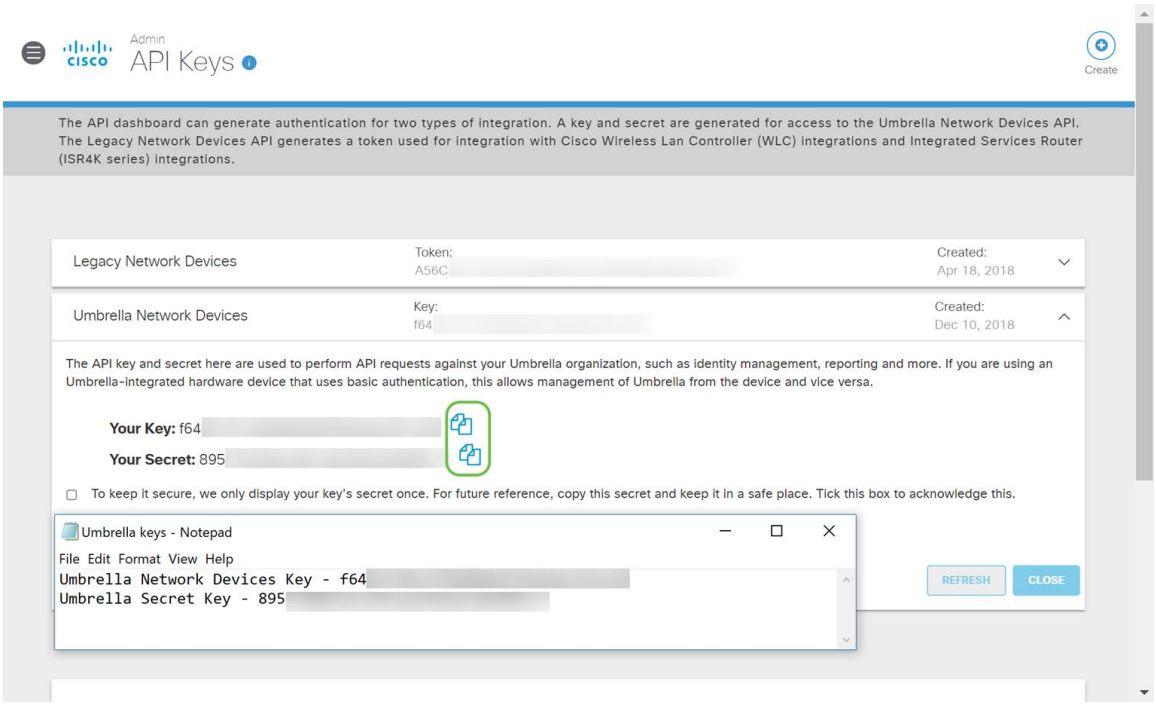


Note: the above screenshot would be similar to what you would see opening this menu for the first time.

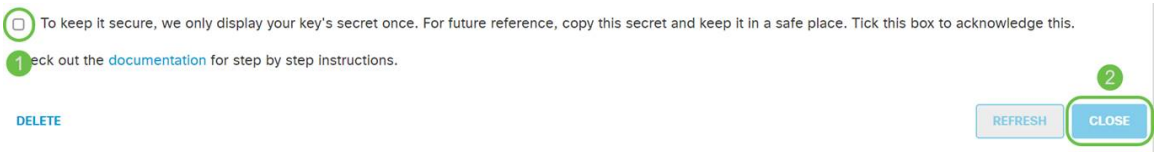
Step 3. Select **Umbrella Network Devices** and then click the **Create** button.



Step 4. Open a text editor such as notepad then click the **Copy** button to the right of your API and API *Secret Key,* a pop-up notification will confirm the key is copied to your clipboard. One at a time, paste your secret and API key into the document, labelling them for future reference. In this case its label is “Umbrella network devices key”. Then save the text file to a secure location that's easy to access later.



Step 5. After you’ve copied the key and secret key to a safe location, from the *Umbrella API screen* click the **checkbox** to confirm to complete acknowledgement of the temporary viewing of the secret key, then click the **Close** button.



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 new API key with each device you wish to protect with

Umbrella.

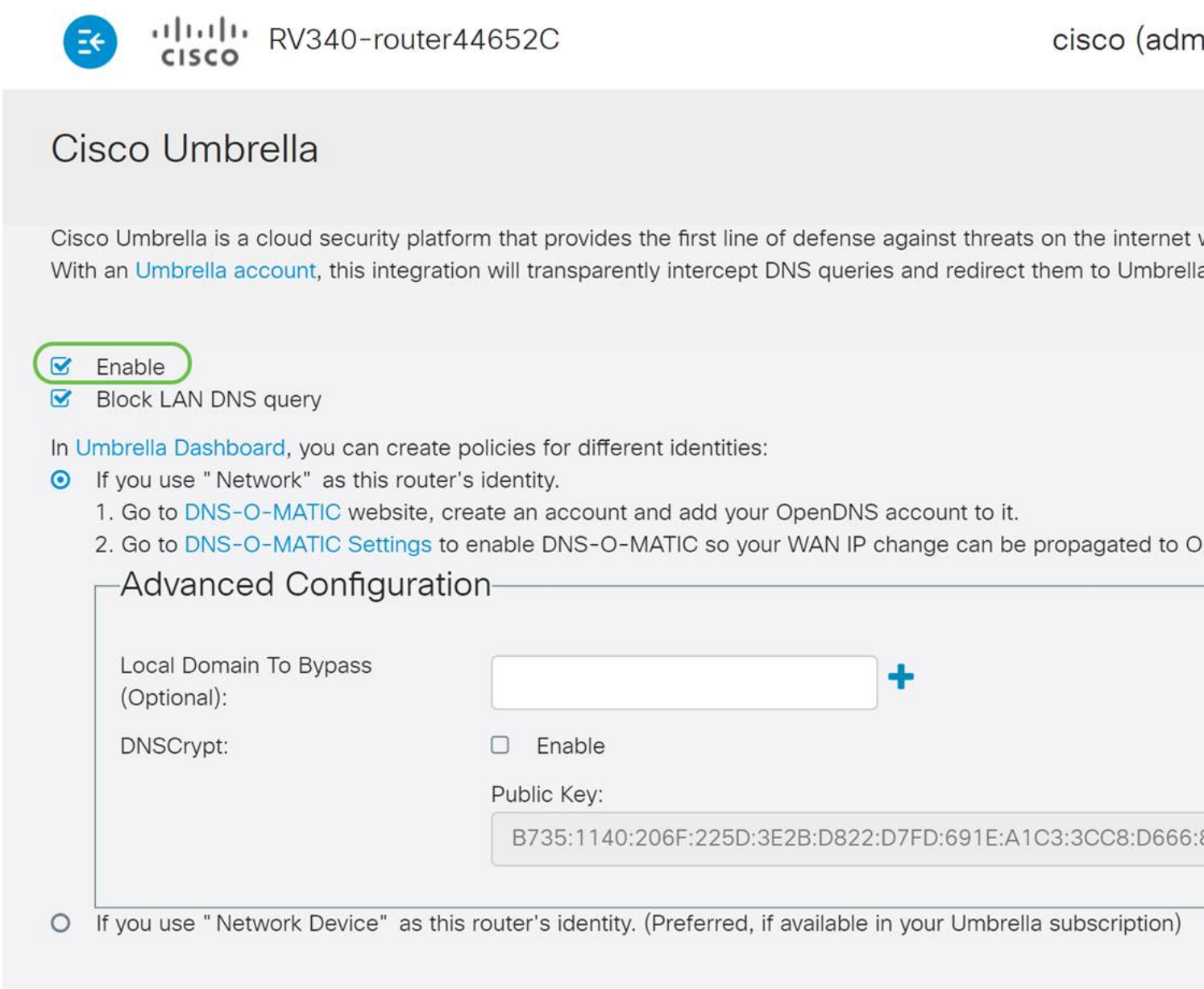
Best Practice: Keep just a *single* copy of this document on a device, like a USB thumb drive, inaccessible from any network.

Configuring Umbrella on your RV34x Device

Now that we've created API keys within Umbrella, we'll take those keys and install them on our RV34x Devices. In our case we are using a RV340.

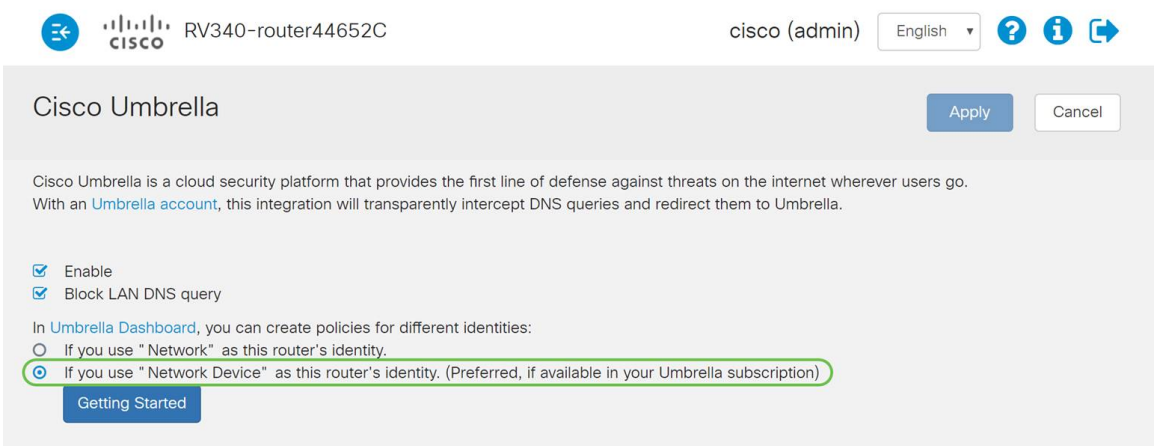
Step 1. After logging into your RV34x Device, click on **Security > Umbrella** in the sidebar menu.

Step 2. The Umbrella API screen has a range of options, begin enabling Umbrella by clicking the **Enable** checkbox.

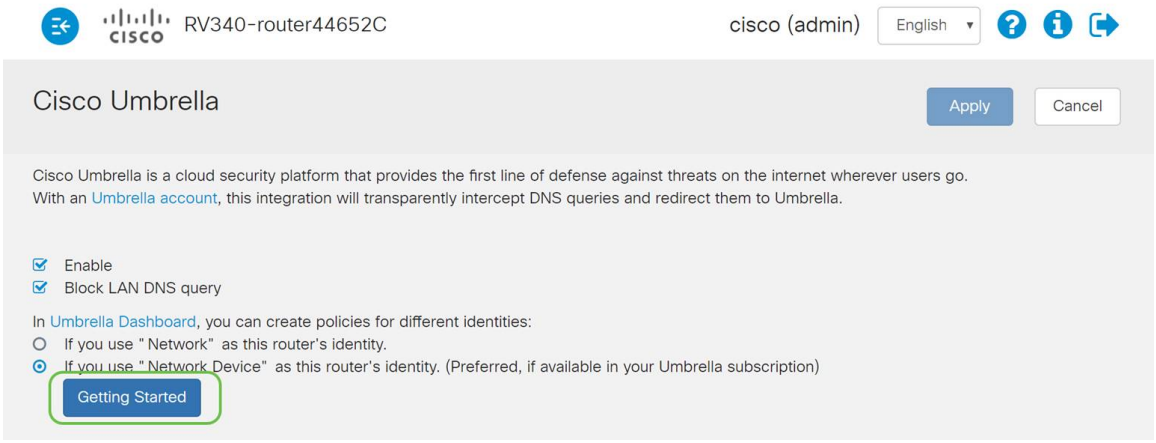


Step 3. (Optional) On by default the box Block LAN DNS Queries is selected, this neat feature automatically creates access control lists on your router which will prevent DNS traffic from going out to the internet. This feature forces all domain translation requests to be directed through the RV34x and is a good idea for most users.

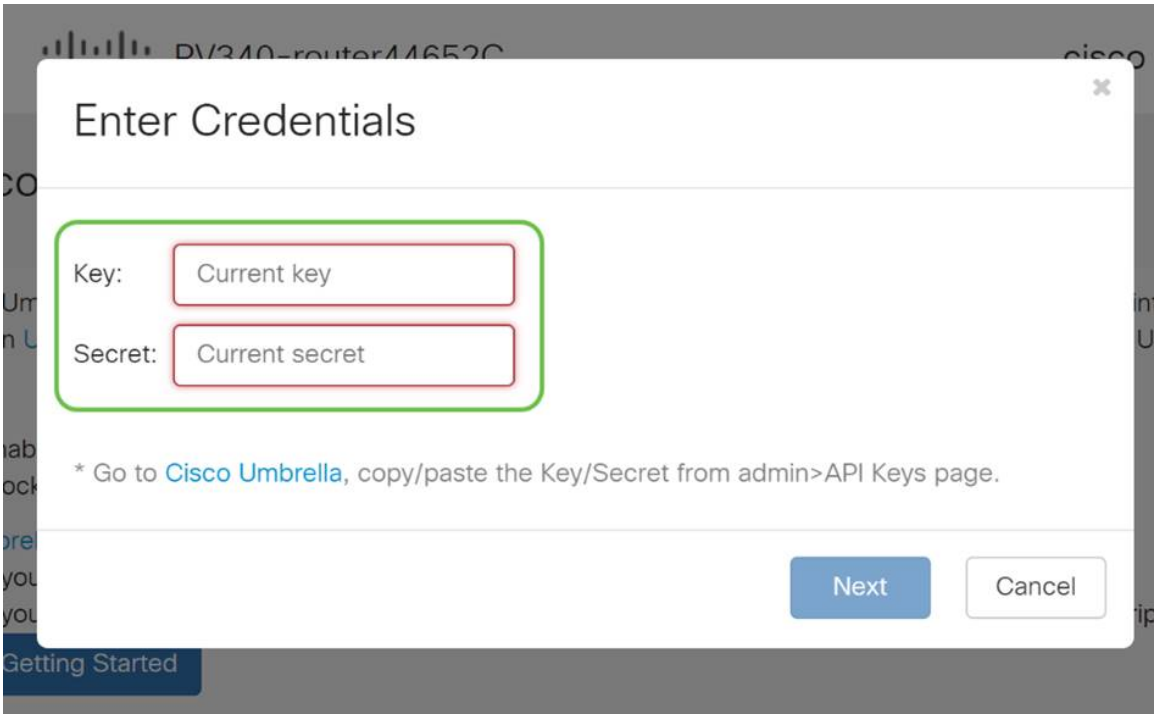
Step 4. The next step plays out in two different way. They both depend on the setup of your network. If you use a service like DynDNS or NoIP, you would leave the default naming scheme of “Network”. Then you will need to login to those account to ensure Umbrella interfaces with those services as it provides protection. For our purposes we’re relying on “Network Device”, click on the bottom radial button.



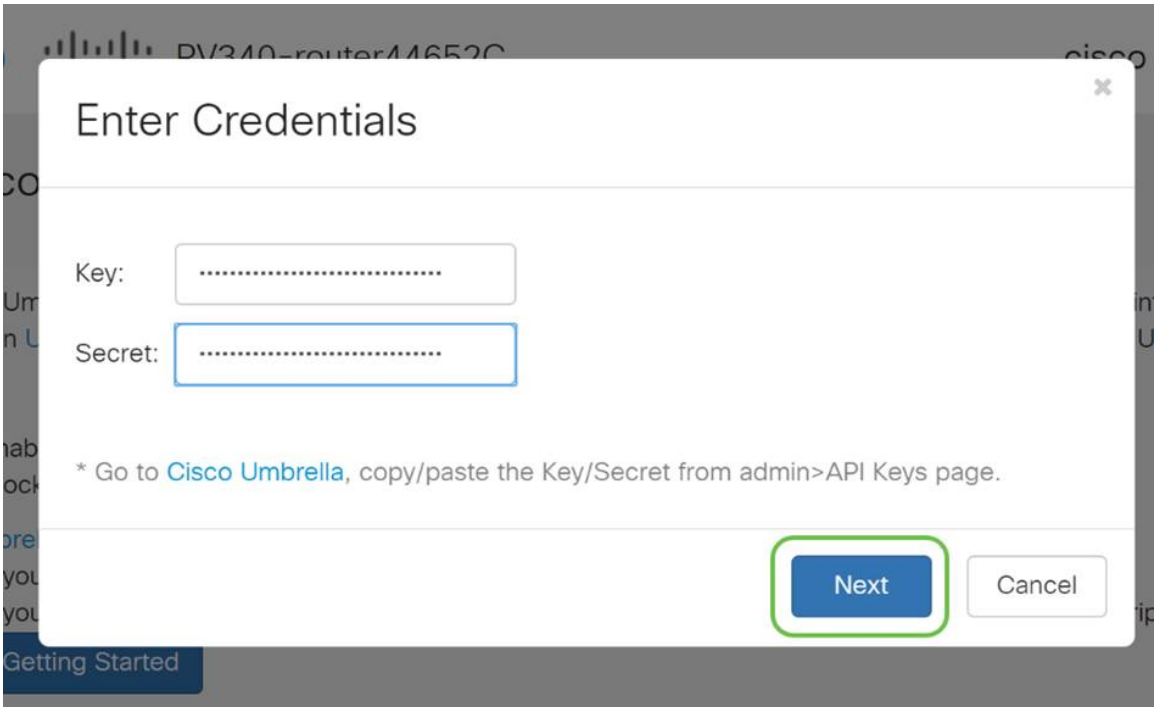
Step 5. Now click **Getting Started** to initiate the mini-wizard.



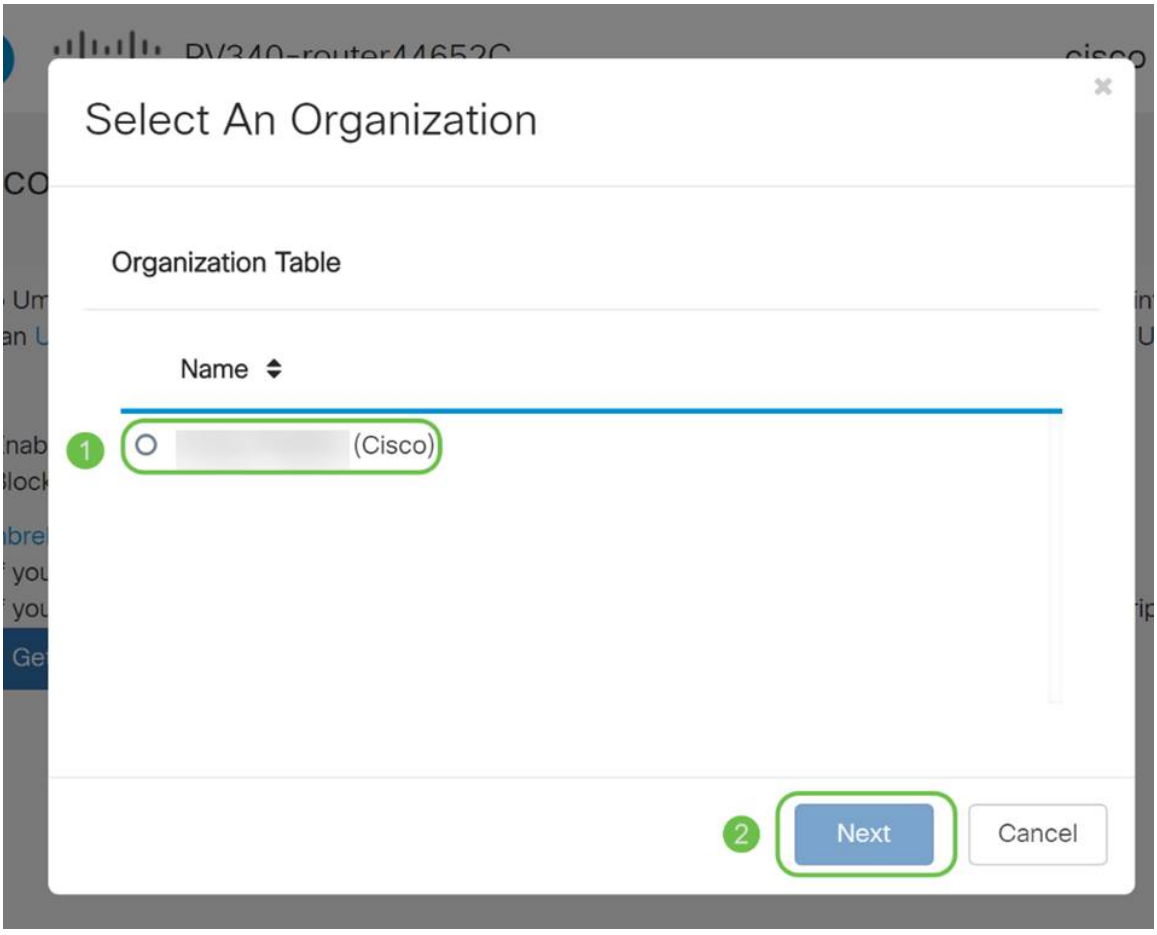
Step 6. Now enter the **API Key** and **Secret Key** to the text boxes.



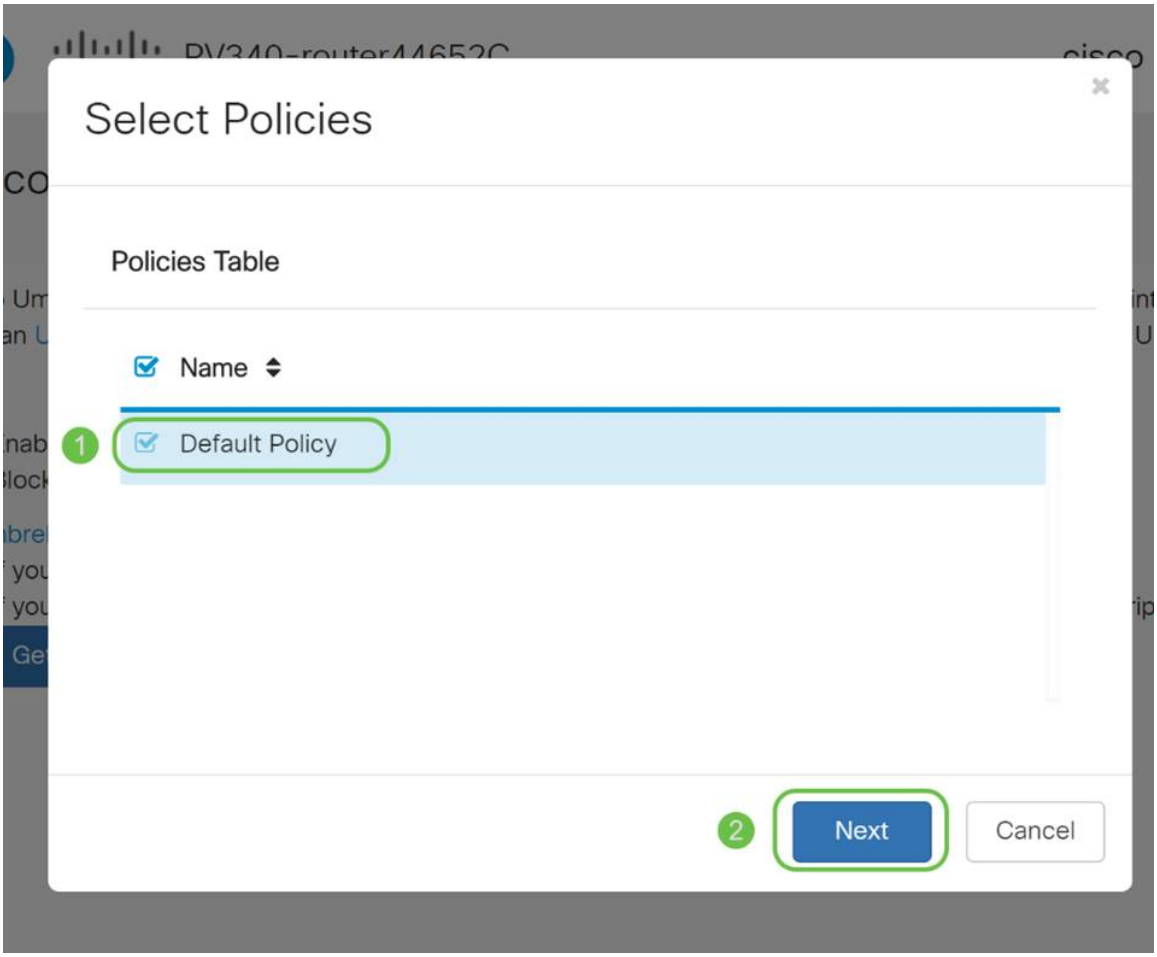
Step 7. After entering your API and Secret Key click the **Next** button.



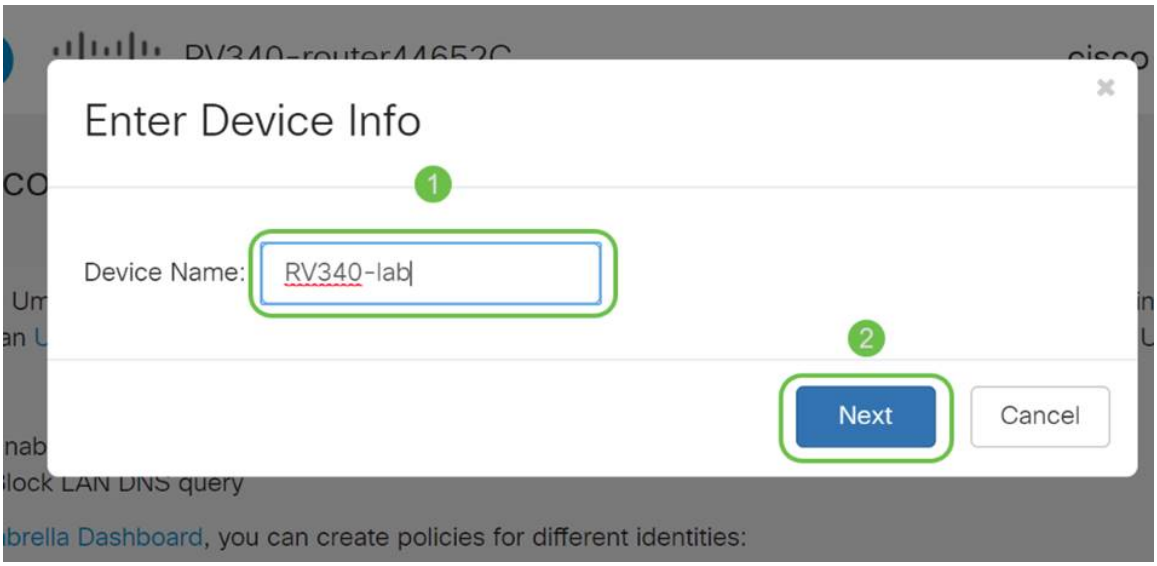
Step 8. In the next screen select the **organization** you wish to associate with the router, then click **Next**.



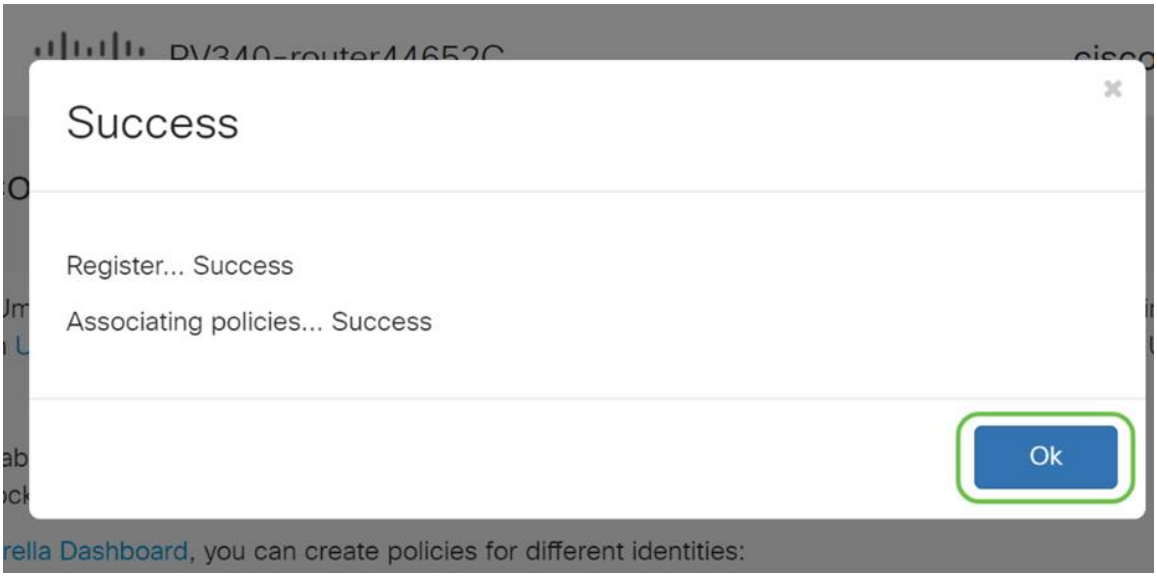
Step 9. Now select the policy to apply to traffic routed by the RV34x. For most users the default policy will provide enough coverage.



Step 10. **Assign a name** to the device so it may be designated in Umbrella reporting. In our setup we have assigned “RV340-lab”.



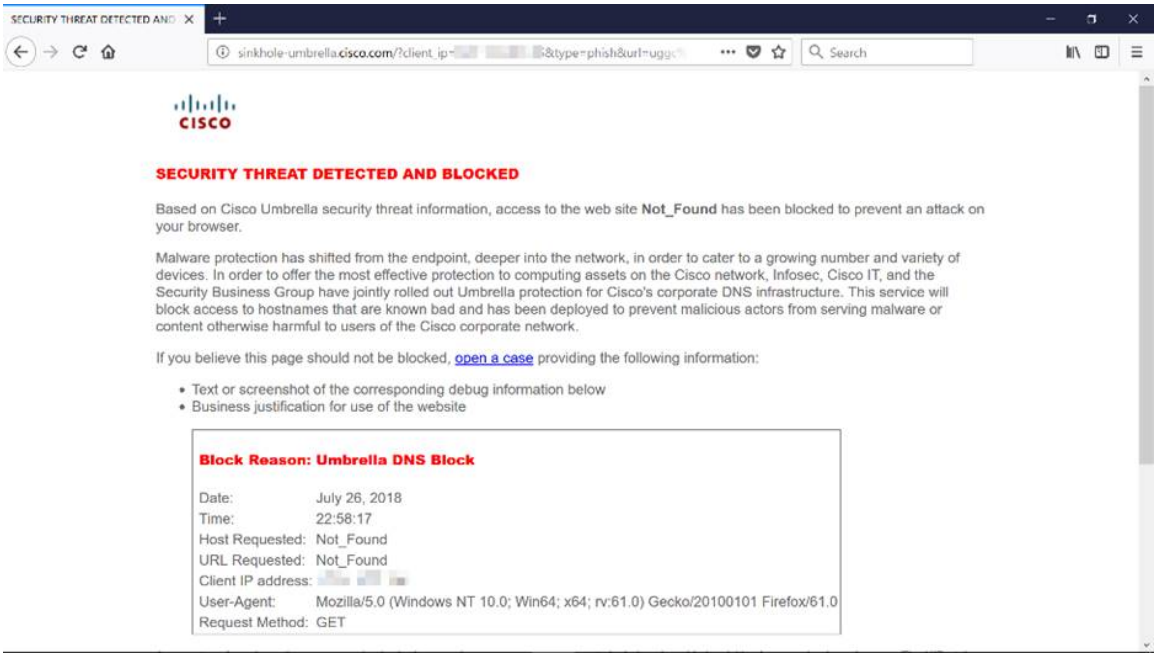
Step 11. The next screen will validate your chosen settings and provide an update, when associated successfully click **OK**.



Confirming everything is in its right place

Congratulations, you are now protected Cisco's Umbrella. Or are you? Let's be sure by double-checking with a live example, 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