Configure Web Content Filtering using Cisco Umbrella in WAP571 or WAP571E

Objective

The objective of this article is to show you how to configure web content filtering using Cisco Umbrella on a WAP571 or WAP571E.

Introduction

You have worked hard to get your network up and running. Of course, you want it to stay that way, but hackers are relentless. What can be done to keep your network safe? One solution is to set up web content filtering. The web content filtering feature allows you to provide controlled access to the Internet by configuring policies and filters. It helps to secure the network by blocking malicious or unwanted websites.

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the Internet. It acts as a gateway between the Internet and your systems and data to block malware, botnets, and phishing over any port, protocol, or application.

Using a Cisco Umbrella account, the integration will transparently (reporting at the URL level) intercept Domain Name System (DNS) queries and redirect them to Umbrella. Your device will appear in the Umbrella dashboard as a network device for applying policies and viewing reports.

To learn more about Cisco Umbrella check out the following links:

Cisco Umbrella at a Glance

Cisco Umbrella User Guide

How To: Extending Cisco Umbrella to protect your wireless Network

Applicable Devices

WAP571

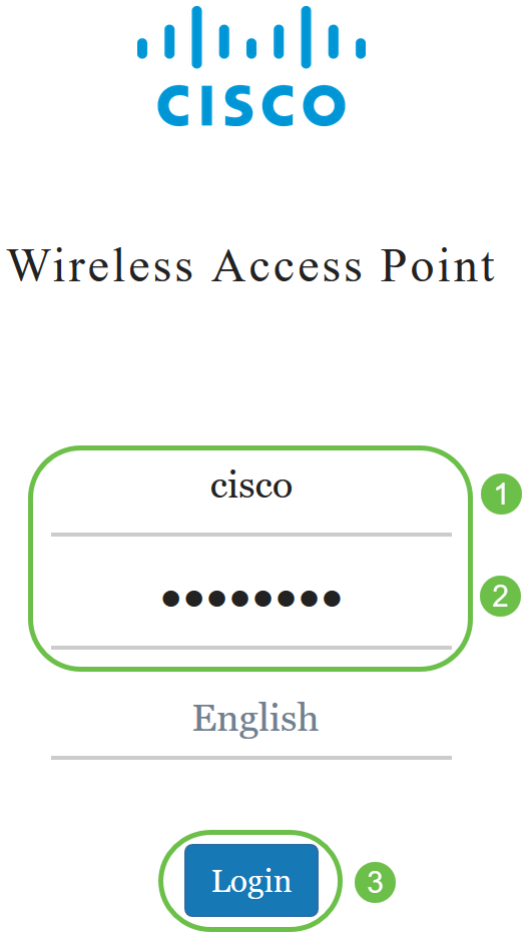
WAP571E

Software Version

- 1.1.0.3

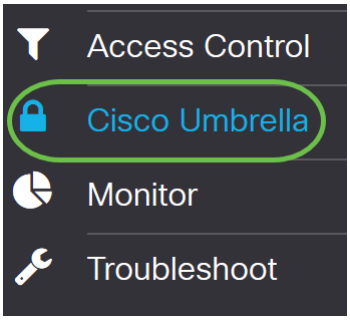
Configure Cisco Umbrella on your WAP

Step 1. Log in to the web configuration utility of the WAP by entering the username and password. The default username and password is *cisco/cisco.* If you have configured a new username or password, enter those credentials instead. Click **Login.**

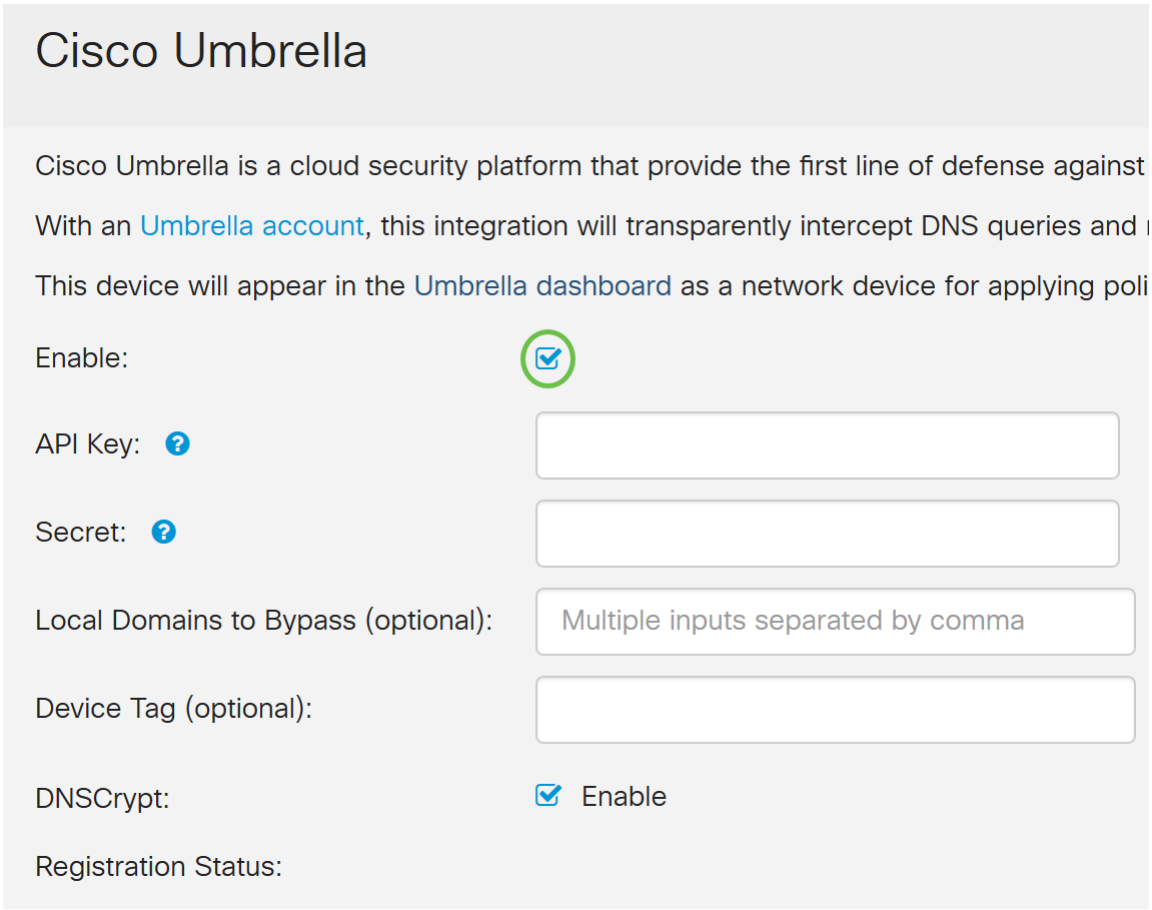


Note: In this article, the WAP571E is used to demonstrate the configuration of Cisco Umbrella. Menu options may slightly vary depending on the model of your device.

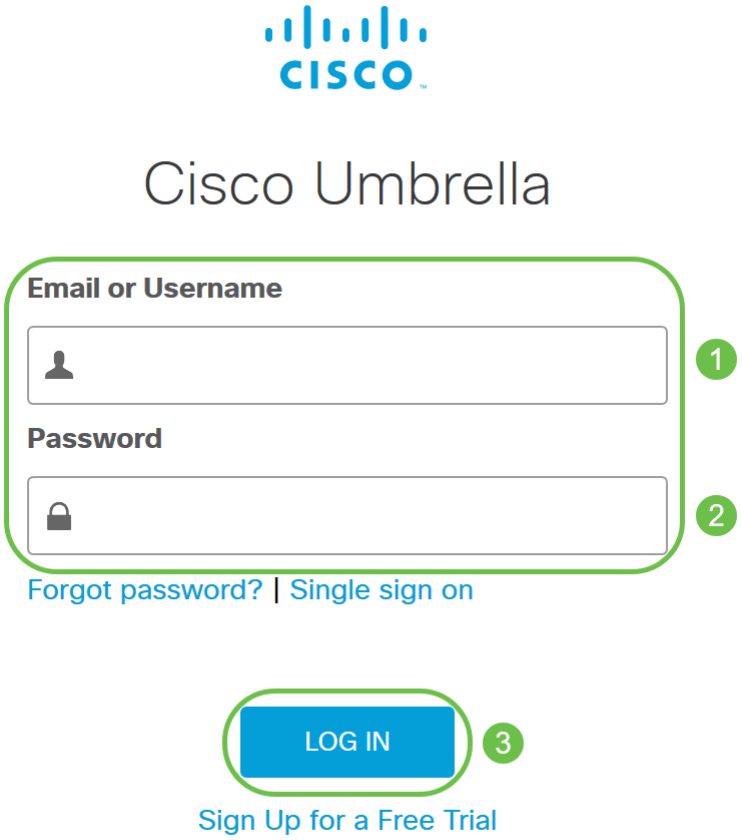
Step 2. Choose **Cisco Umbrella**.



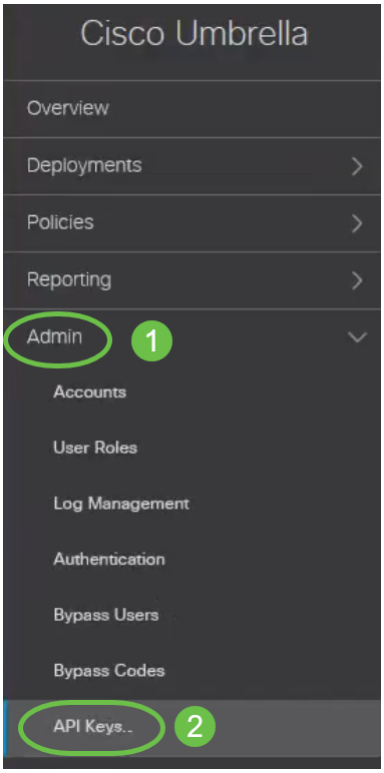
Step 3. *Enable* Cisco Umbrella by clicking on the check box.



Step 4. To obtain the *API Key* and *Secret*, log into your Cisco Umbrella account using *Email or Username* and *Password*. Click **LOG IN**.



Step 5. Navigate to **Admin** and request an API Key by choosing **API Keys…**from the menu.

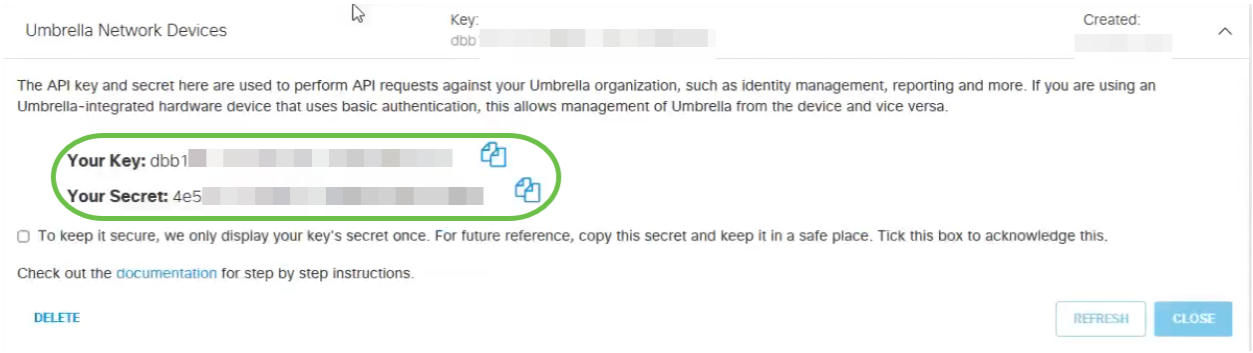


Note: The first time you request an API key, only the key gets displayed as shown below.

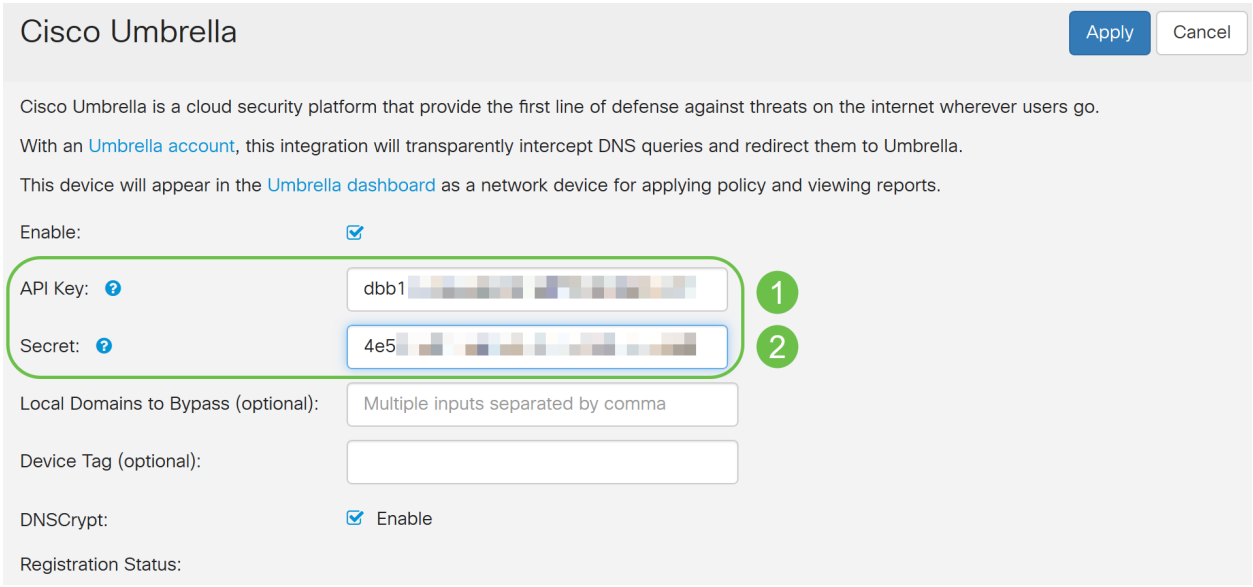
Step 6. Click **Refresh** to obtain both the API key and Secret.

Note: When you click *Refresh*, the API key will change.

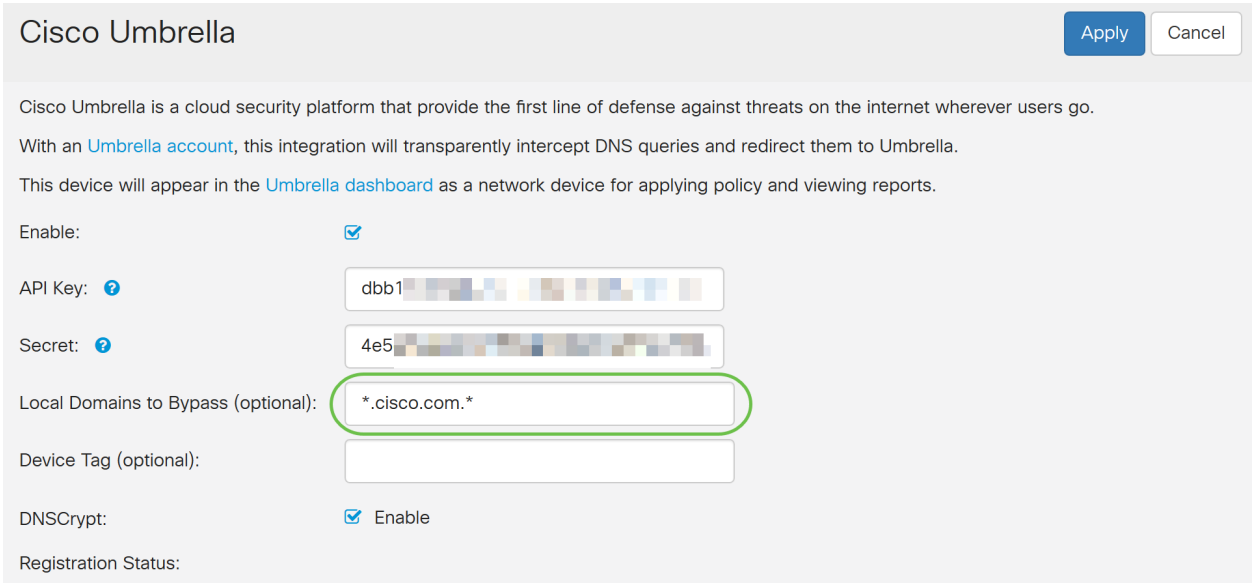
Step 7. Copy the *Key* and *Secret* that is generated.



Step 8. Paste the copied *Key* and *Secret* from Step 7 in to the fields provided under *Cisco Umbrella* configuration of the WAP.



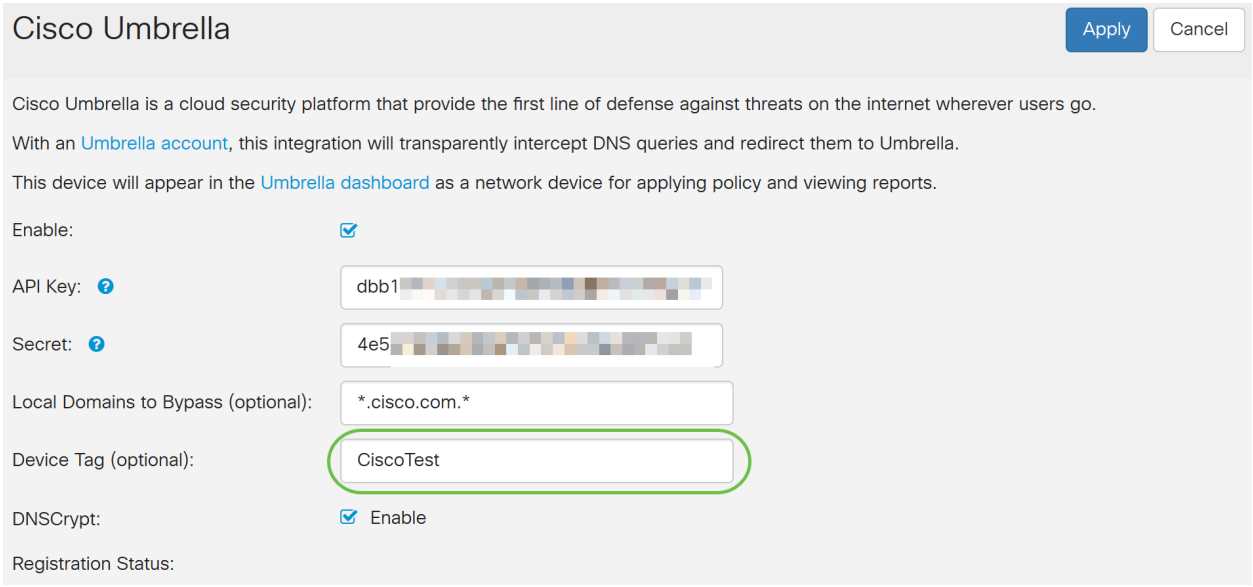
Step 9. (Optional) Enter the domain name you trust in the **Local Domains to Bypass (optional)** field and the packets will reach the destination without going through Cisco Umbrella. Items in the list should be separated by a comma, while the domains can include wildcards in the form of an asterisk (*). For example: *.cisco.com.*.



Note: This is required for all Intranet domains and split DNS domains where separate servers exist for internal and external networks.

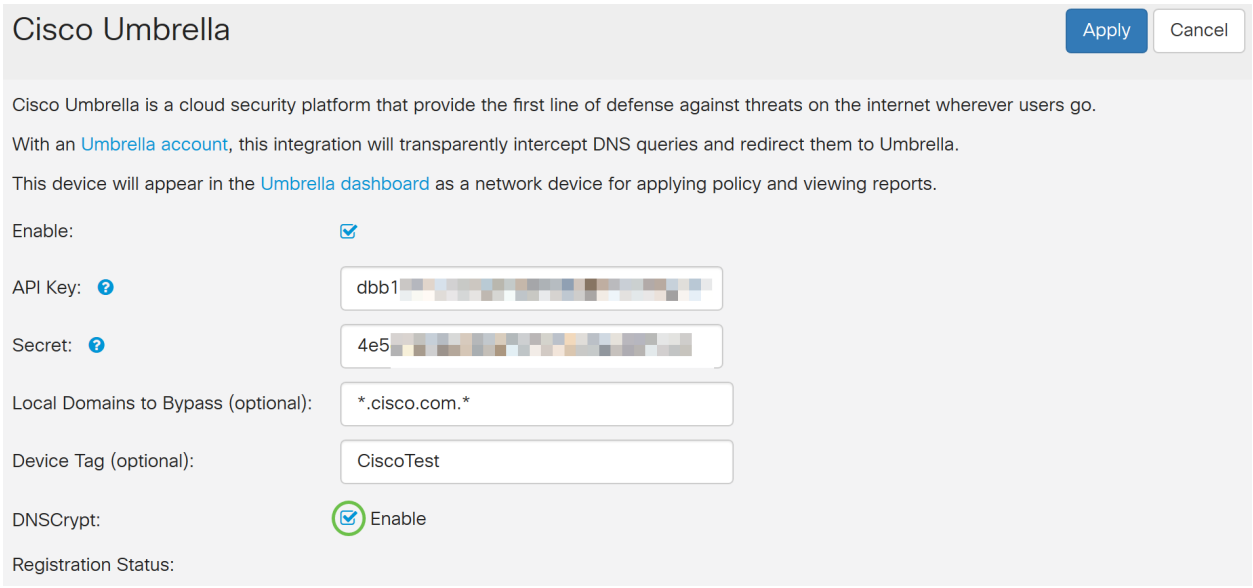
Step 10. (Optional) Enter a tag name in the **Device Tag (optional)** field to tag the device. The

Device Tag describes the device or a particular origin assigned to the device. Ensure it is unique to your organization.

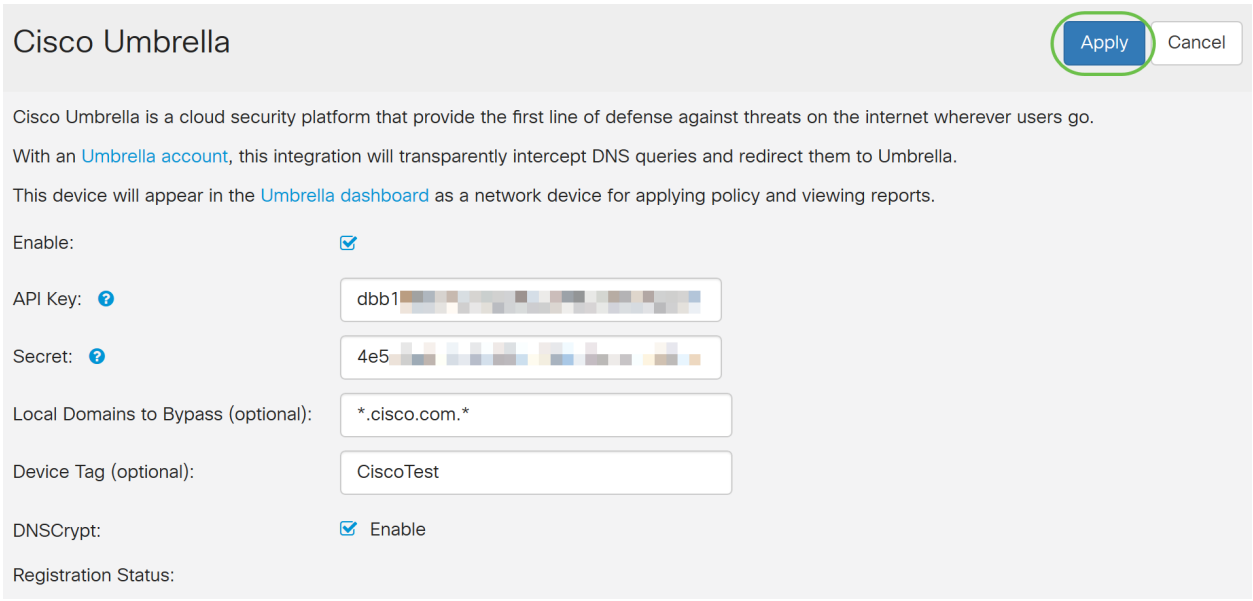


Note: Any change in the *Secret*, *API Key* and the *Device Tag* will trigger re-registration to create a network device.

Step 11. **DNSCrypt** is used to secure (via encryption) the DNS communication between a DNS client and a DNS resolver. It prevents several types of DNS attacks, and snooping. It is enabled by default.

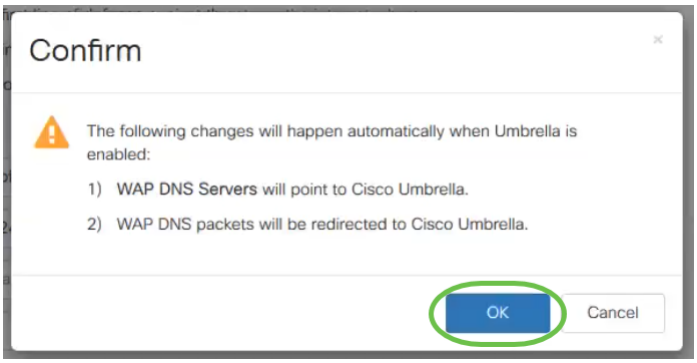


Step 12. Click **Apply** to apply these configurations.



Note: The status of the registration is indicated in the *Registration Status* field. The status can be *Successful*, *Registering* or *Failed*.

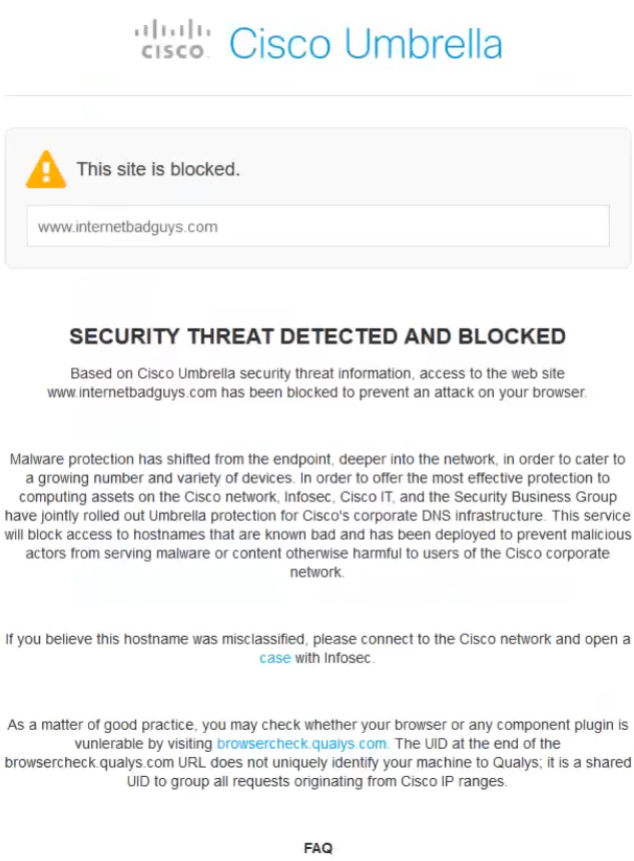
Step 13. You will see a pop-up screen as shown below. Click **OK** to confirm.



Verification

There is a fun way to check if website filtering is enabled. Simply open a web-browser and enter the following url: www.internetbadguys.com. Have no fear, this is a site owned by Cisco for testing and verification purposes.

Since website filtering is enabled in the WAP through Cisco Umbrella, you will receive the following notification. The wireless network will redirect the DNS query to Cisco Umbrella. In turn, Cisco Umbrella acts as the DNS server, protecting the network and its users.



Conclusion

You have now configured and enabled website filtering on a WAP571 or WAP571E access point using Cisco Umbrella.

Want to learn more? Check out these videos related to Cisco Umbrella:

Cisco Tech Talk: Securing a Business Network Using Umbrella and Cisco Small Business Access Points

Cisco Tech Talk: How to Get an Umbrella Account

Cisco Tech Talk: Setting Up an Umbrella Policy