Configure Cisco Umbrella on Cisco Business Wireless Access Point

Objective

The objective of this document is to show you how to configure Cisco Umbrella on a Cisco Business Wireless (CBW) Access Point (AP).

Applicable Devices | Firmware Version

- 140AC (Data Sheet) | 10.4.1.0 (Download latest)
- 141ACM (Data Sheet) | 10.4.1.0 (Download latest)
- 142ACM (Data Sheet) | 10.4.1.0 (Download latest)
- 143ACM (Data Sheet) | 10.4.1.0 (Download latest)
- 145AC (Data Sheet) | 10.4.1.0 (Download latest)
- 240AC (Data Sheet) | 10.4.1.0 (Download latest)

Introduction

If you are looking to configure Cisco Umbrella on your CBW AP, you have come to the right place! The CBW APs support the latest 802.11ac Wave 2 standard for higher performance, greater access, and higher-density networks. They deliver industry-leading performance with highly secure and reliable wireless connections, for a robust, mobile end-user experience.

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 policy 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

If you are ready to configure Cisco Umbrella on your CBW AP, let’s get started!

Configure Cisco Umbrella on the Primary AP

Beginner Help

This toggled section highlights tips for beginners.

Logging In

Log into the Web User Interface (UI) of the Primary AP. To do this, open a web browser and enter https://ciscobusiness.cisco. You may receive a warning before proceeding. Enter your credentials.You can also access the Primary AP by entering https://[ipaddress] (of the Primary AP) into a web browser.

Tool Tips

If you have questions about a field in the user interface, check for a tool tip that looks like the following:

Trouble locating the Expand Main Menu icon?

Navigate to the menu on the left-hand side of the screen, if you don’t see the menu button, click this icon to open the side-bar menu.



Cisco Business App

These devices have companion apps that share some management features with the web user interface. Not all features in the Web user interface will be available in the App.

Download iOS App Download Android App

Frequently Asked Questions

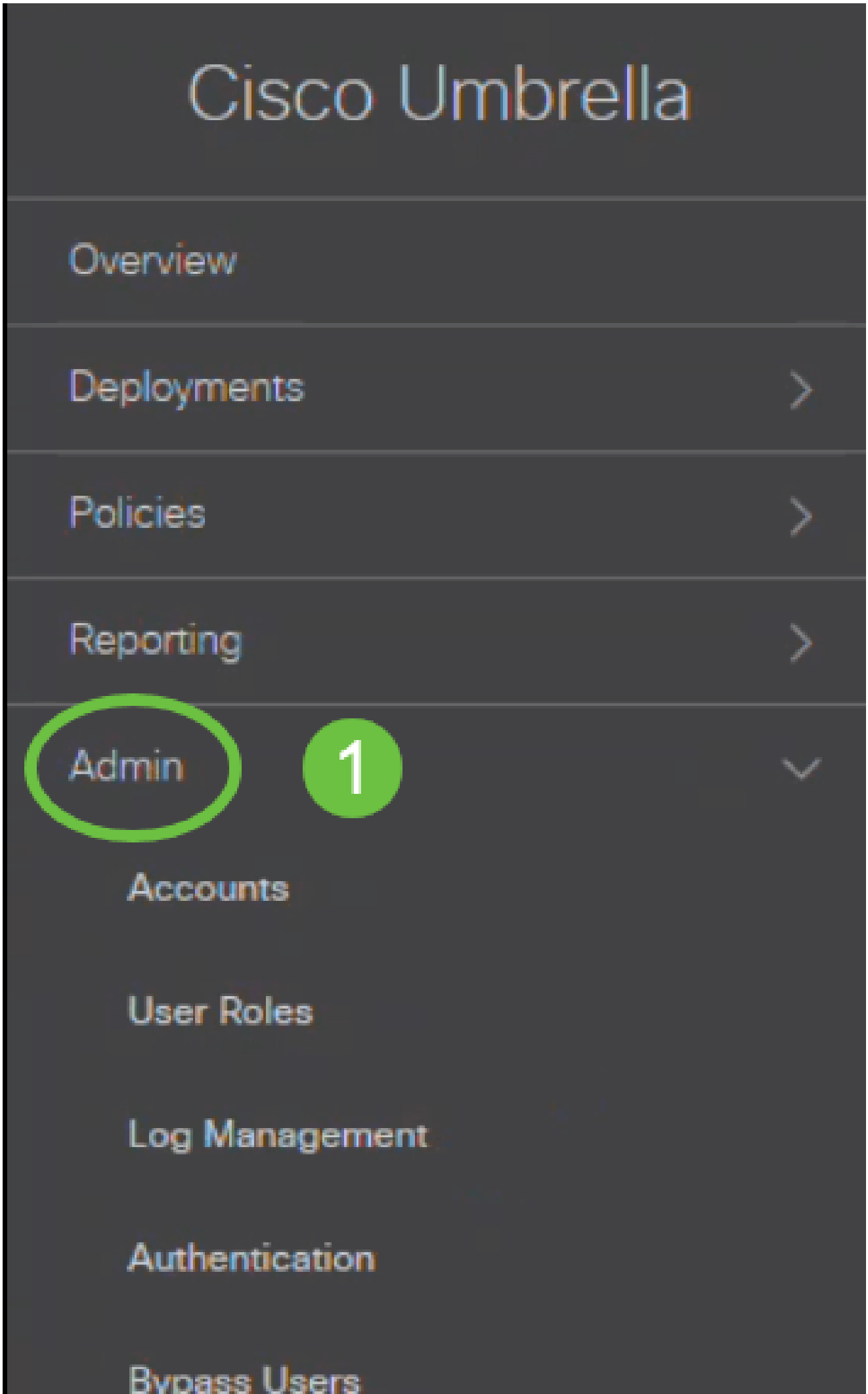
If you still have unanswered questions, you can check our frequently asked questions document. FAQ

To configure Cisco Umbrella on the Primary AP, ensure the following:

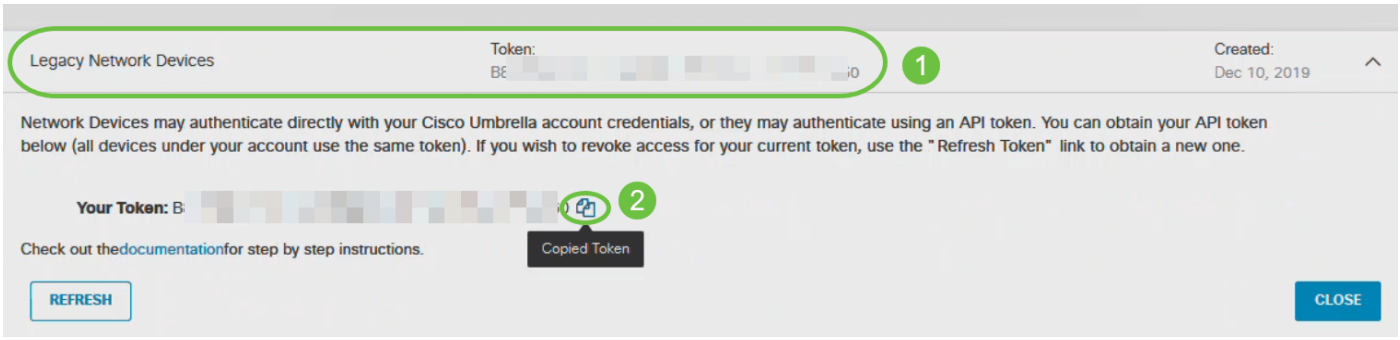
- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

To generate the API token, do the following:

1. Login into your Cisco Umbrella Account.
2. In the Umbrella dashboard, navigate to **Admin > API Keys** and click Create.


Cisco Umbrella
Overview
Deployments
Policies
Reporting
Admin
1
Accounts
User Roles
Log Management
Authentication
Bypass Users

3. Select *Legacy Network Devices* and click *Create* if you have not created one previously.
4. Expand *Legacy Network Devices* and *copy* the API token. The API token is a lengthy string of alpha numeric characters.

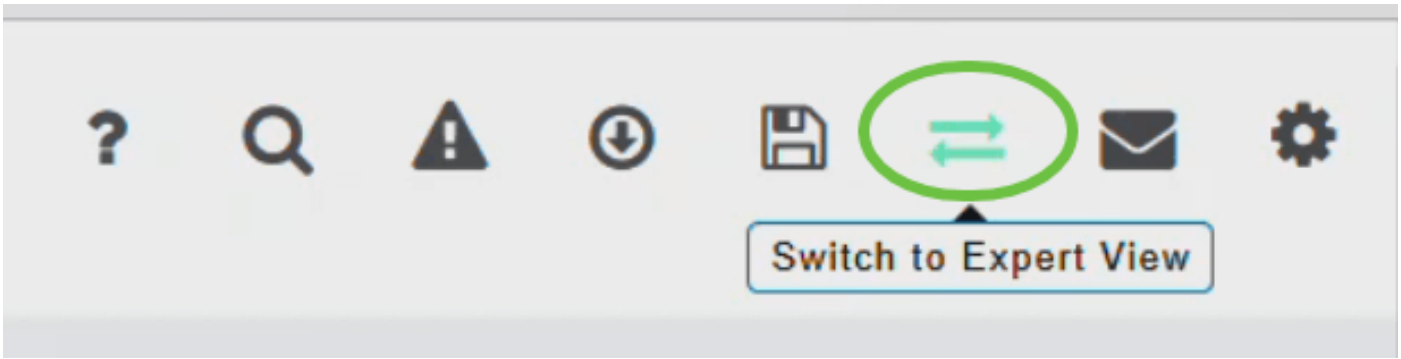


Navigate to the Web-UI of the access point and perform the following steps:

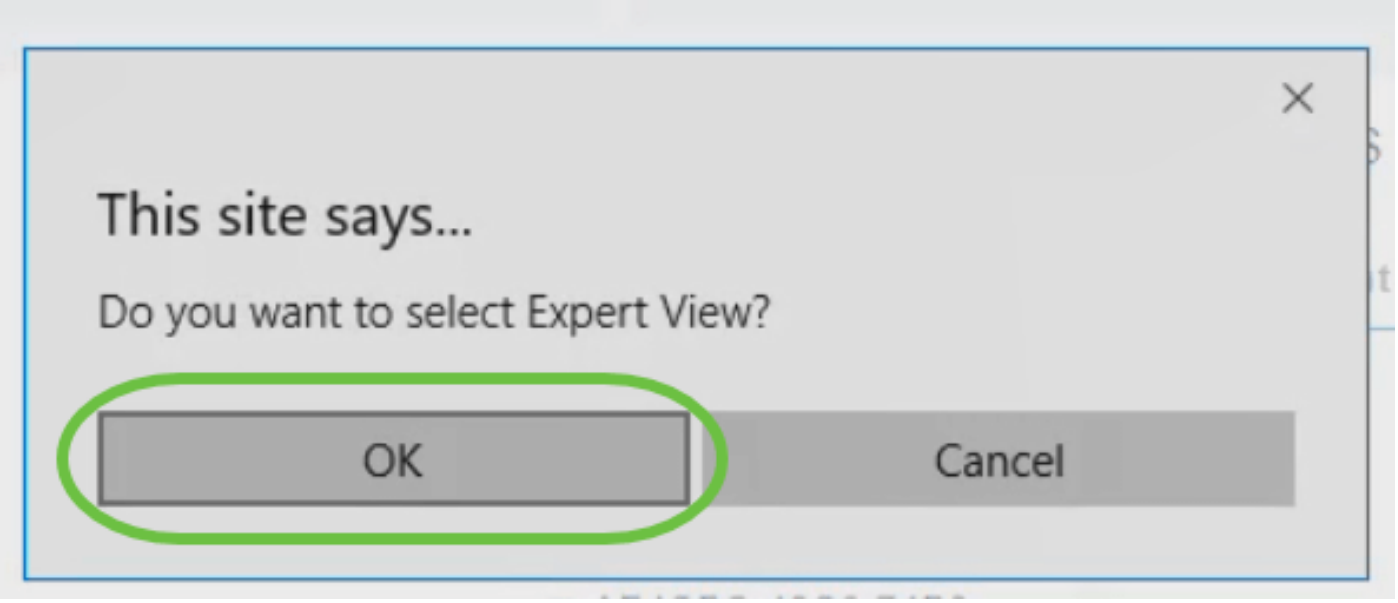
Step 1

Switch to Expert View by clicking **the bidirectional arrow icon** on the top right of the home screen in the Web-UI of the Primary AP.

If you are unfamiliar with the terms used, check out Cisco Business: Glossary of New Terms.

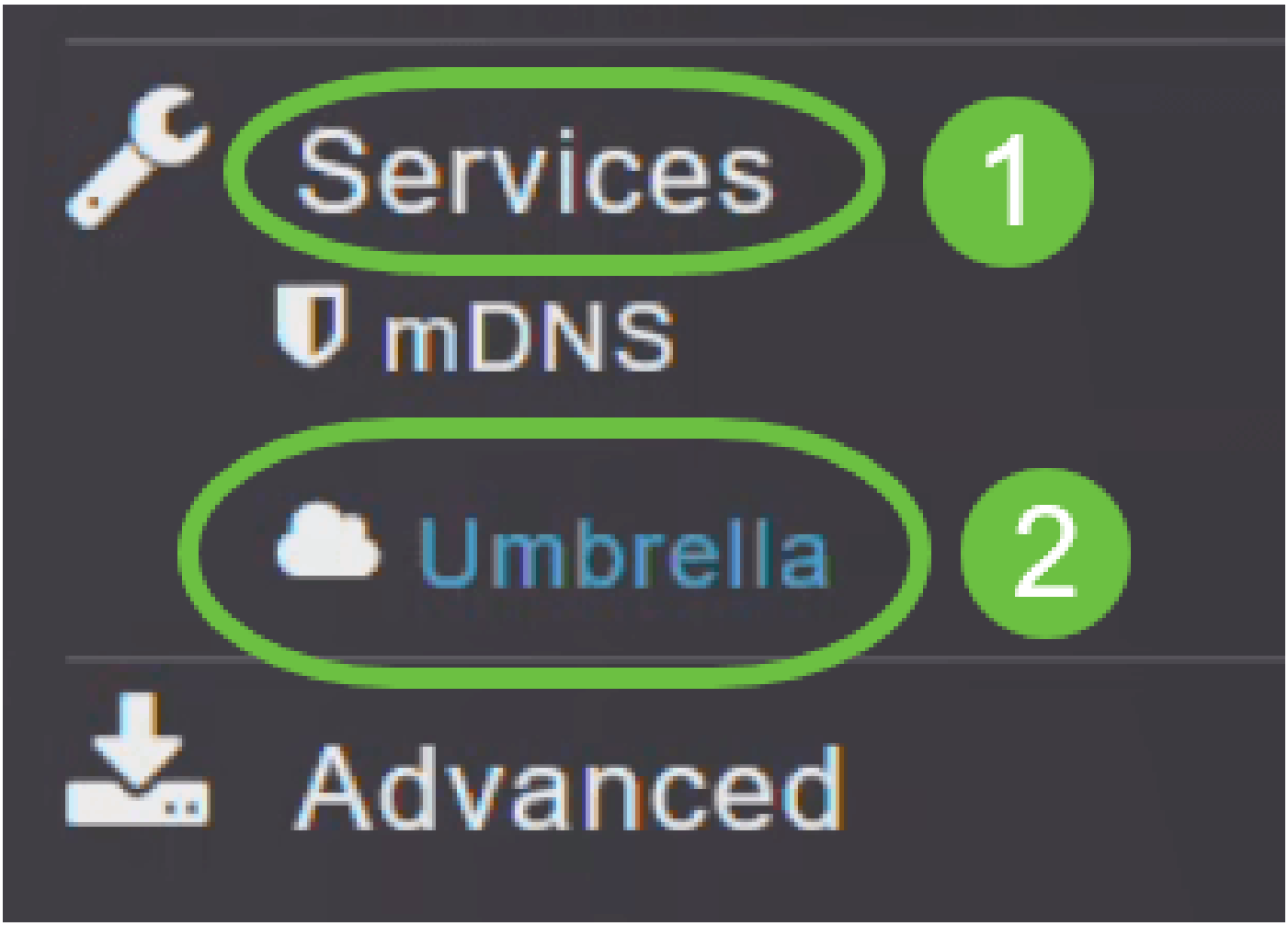


A message is displayed to confirm if you want to switch to the expert view. Click **OK**.



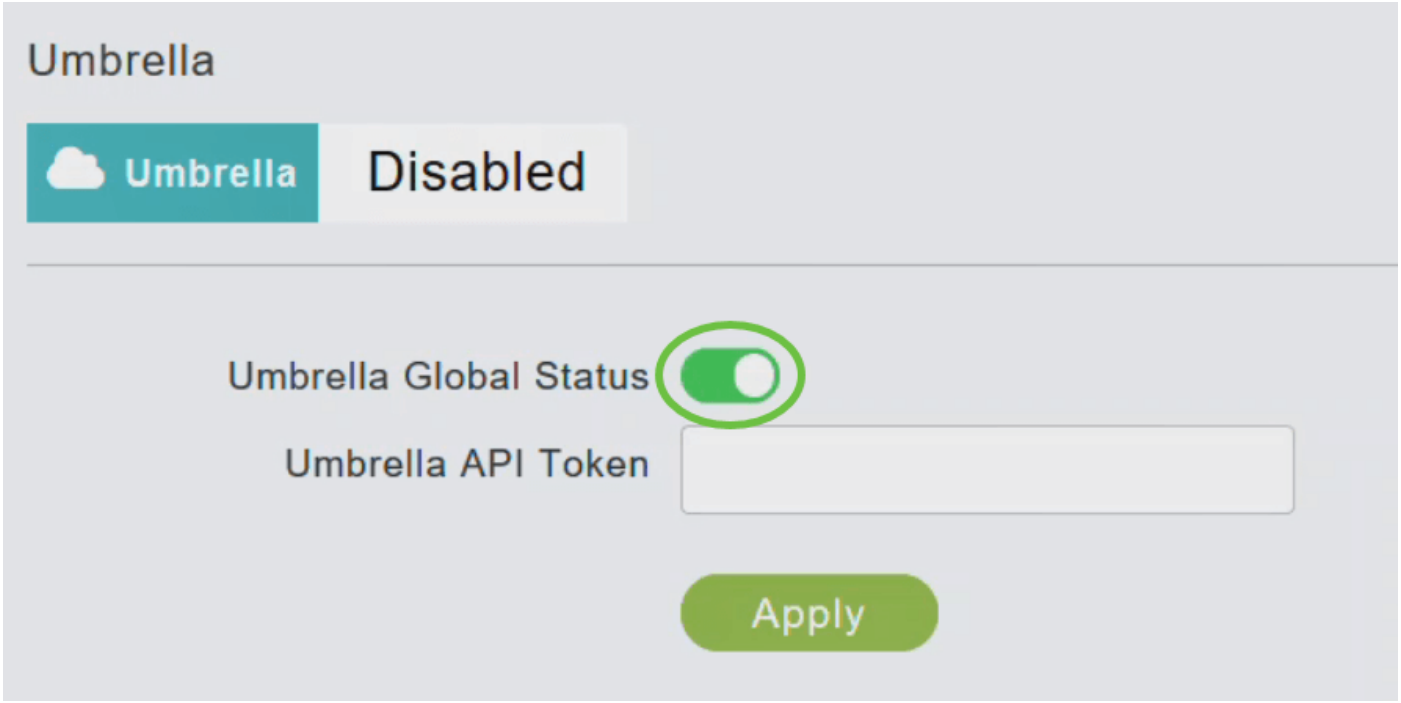
Step 2

Choose **Services** > **Umbrella**.



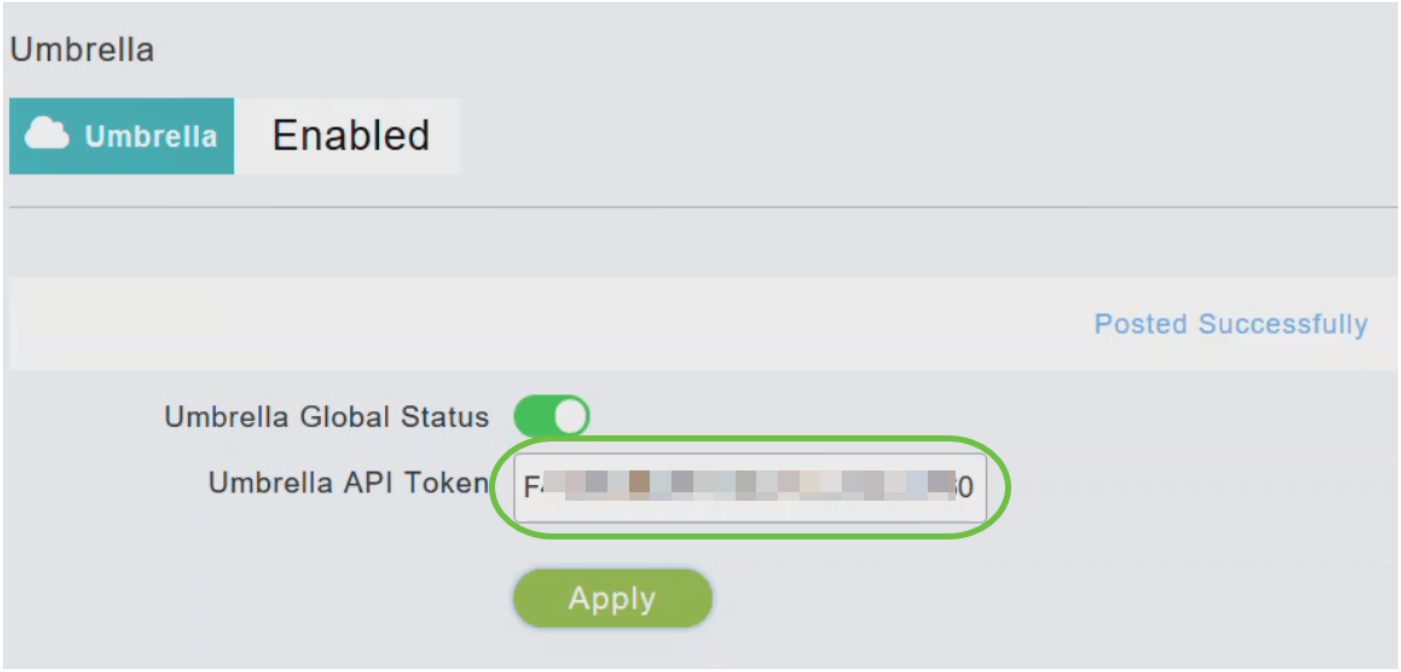
Step 3

Click the *Umbrella Global Status* toggle button to **enable** Umbrella status. This is disabled by default.



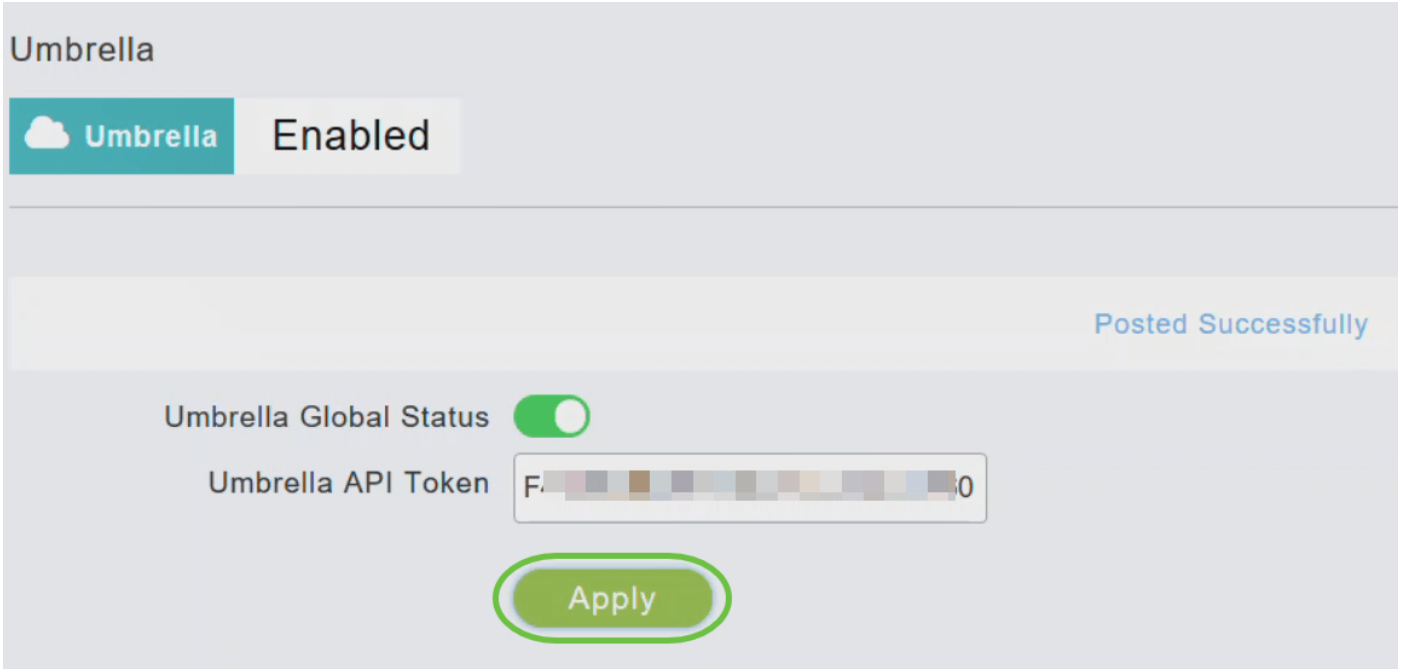
Step 4

Paste the *Umbrella API Token* that you copied.



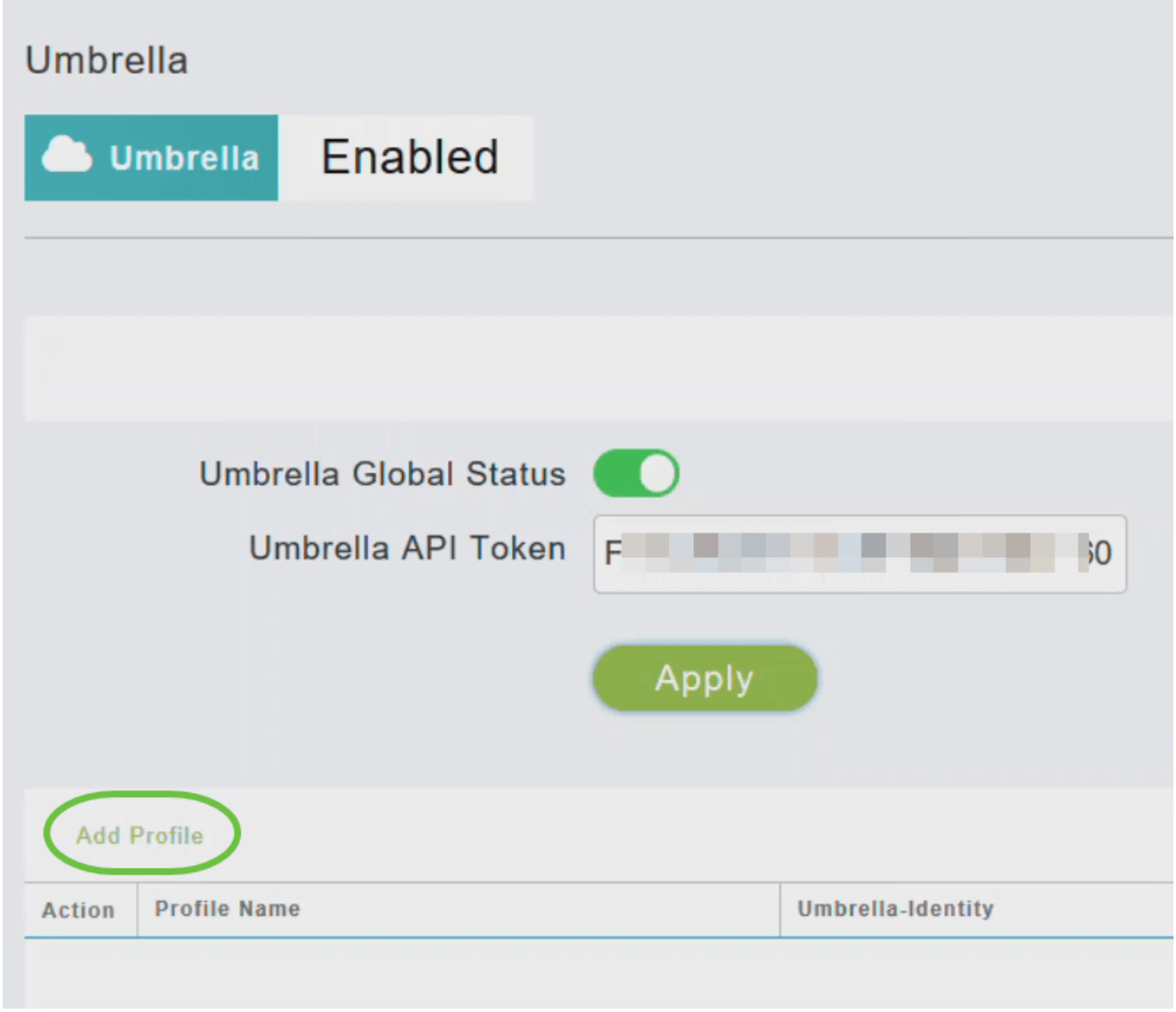
Step 5

Click **Apply** to enable Cisco Umbrella.



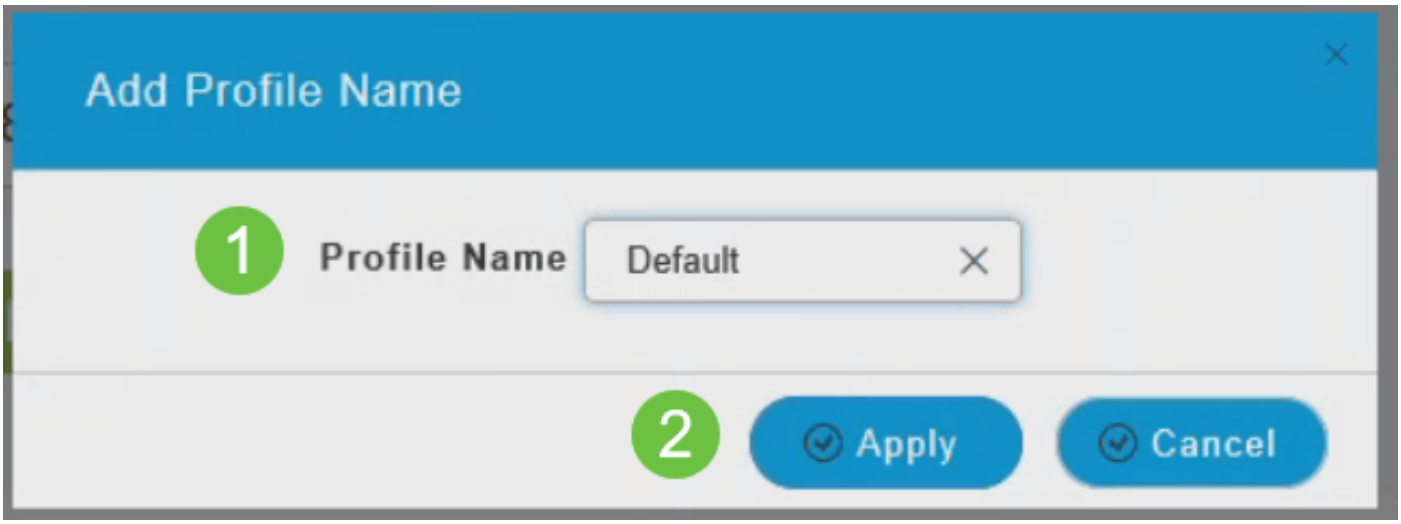
Step 6

To create a new profile, click **Add Profile**.



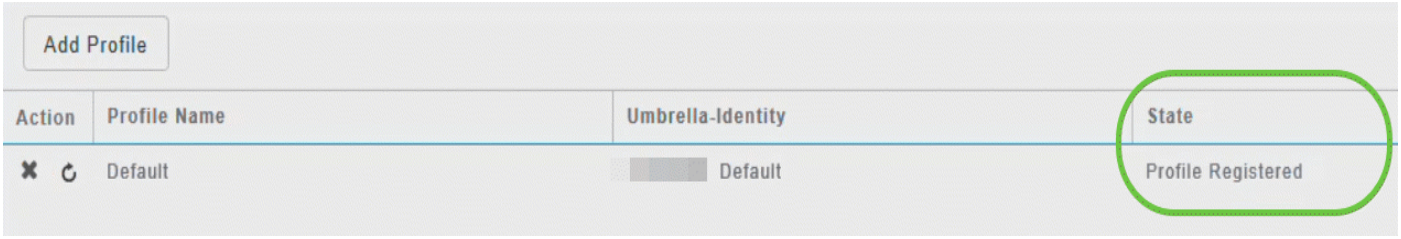
Step 7

In the *Add Profile Name* window, enter the **Profile Name** and click **Apply**. A new profile is created.



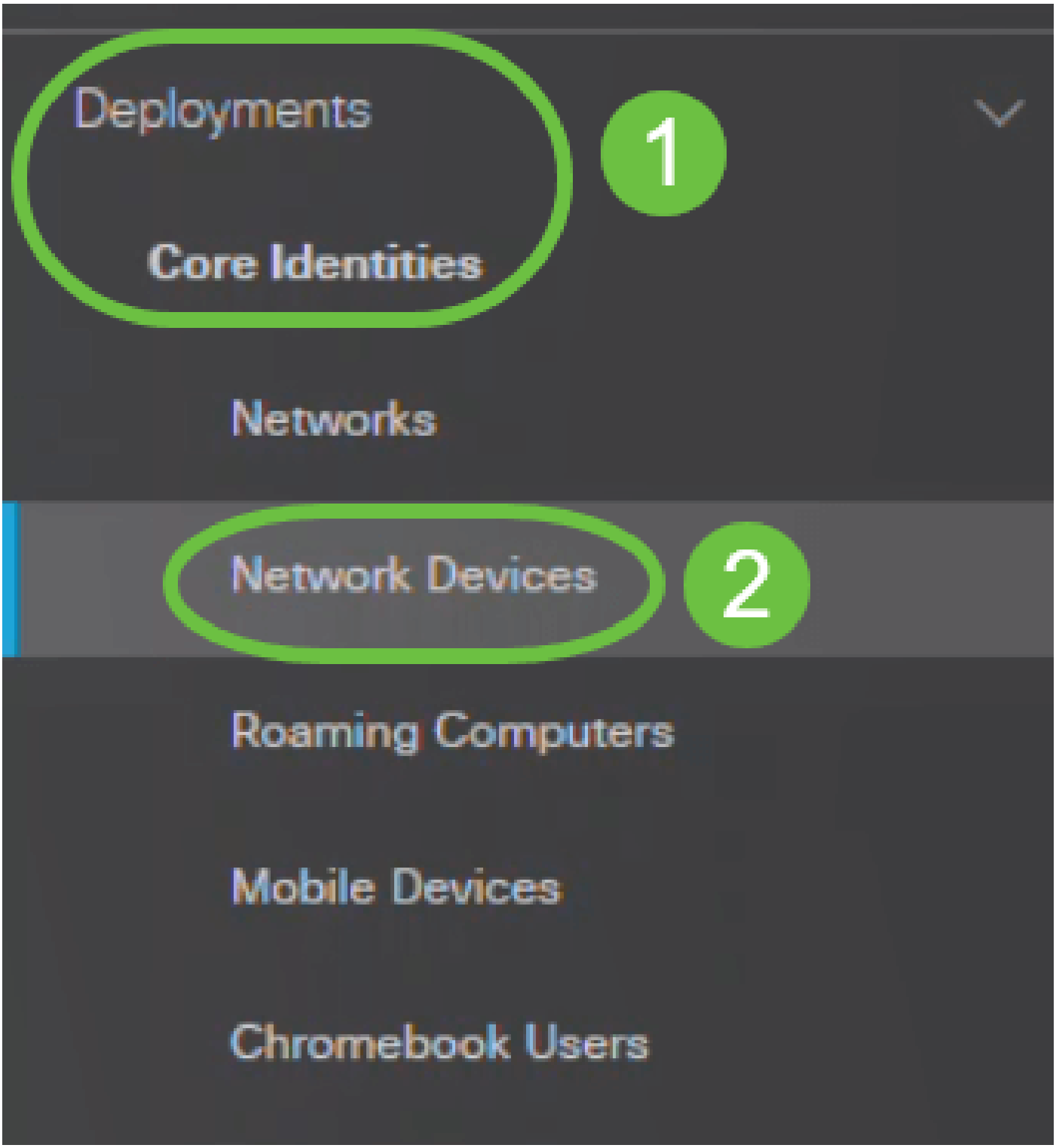
Step 8

Verify that the *State* displays as **Profile Registered**.

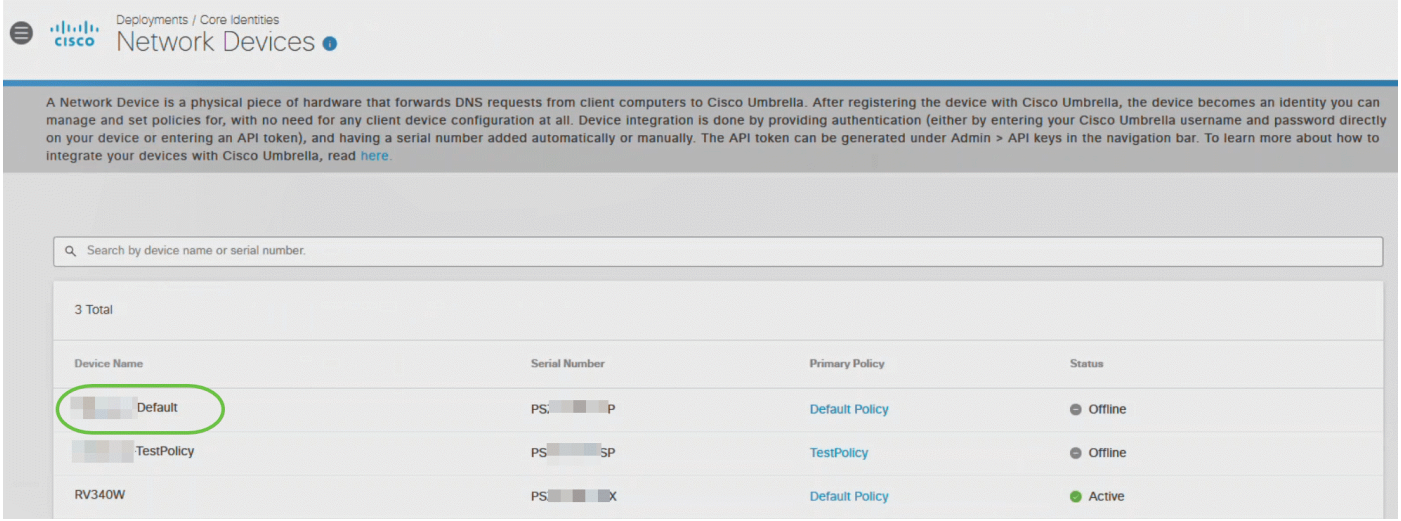


Step 9

In the Umbrella dashboard, navigate to **Deployments > Core Identities > Network Devices**.



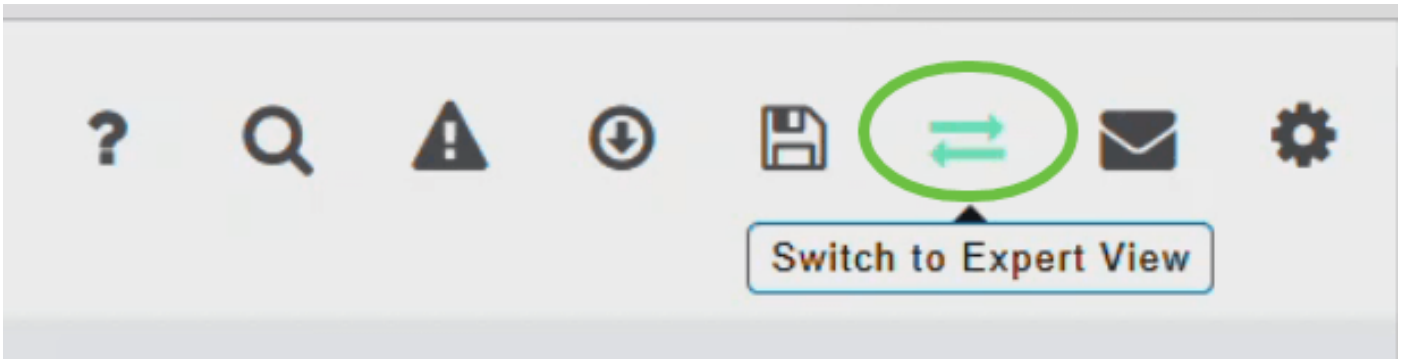
You can check if your device is listed in this window. This might take a few minutes.



Applying Cisco Umbrella Profile to WLAN

Step 1

Switch to *Expert View* by clicking the **bidirectional arrow** icon on the top right of the home screen in the Web-UI of the Primary AP.



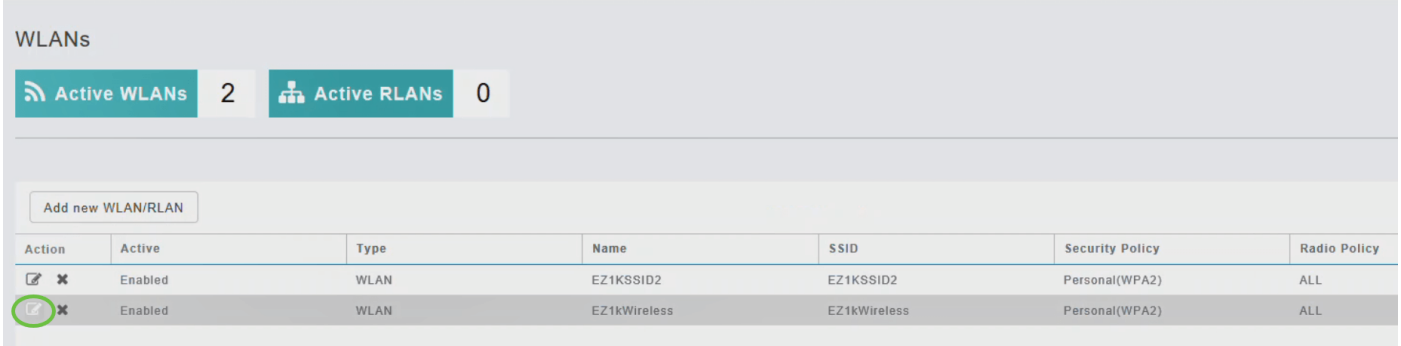
Step 2

Choose **Wireless Settings > WLANs**.

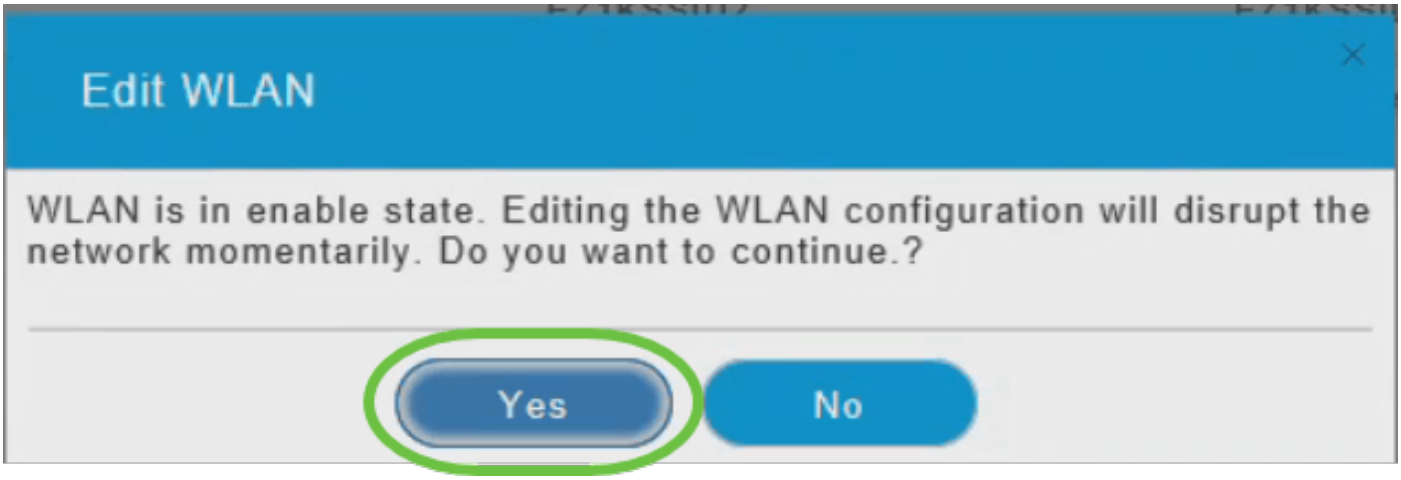


Step 3

Click *Add* to add a new WLAN or click *edit* icon to edit an existing WLAN. In this example, the edit icon is selected.

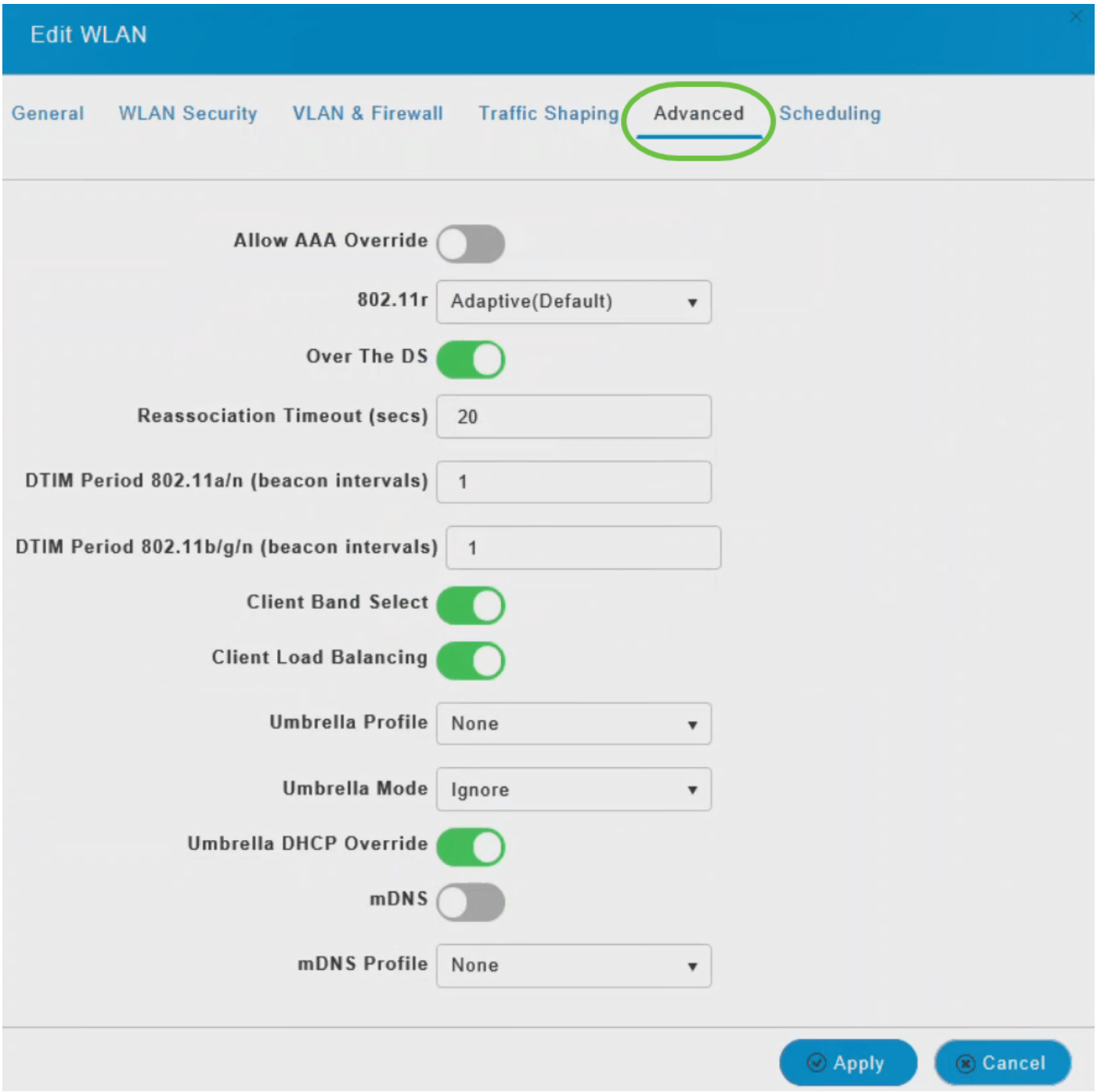


You will see the following window. Click **Yes**.



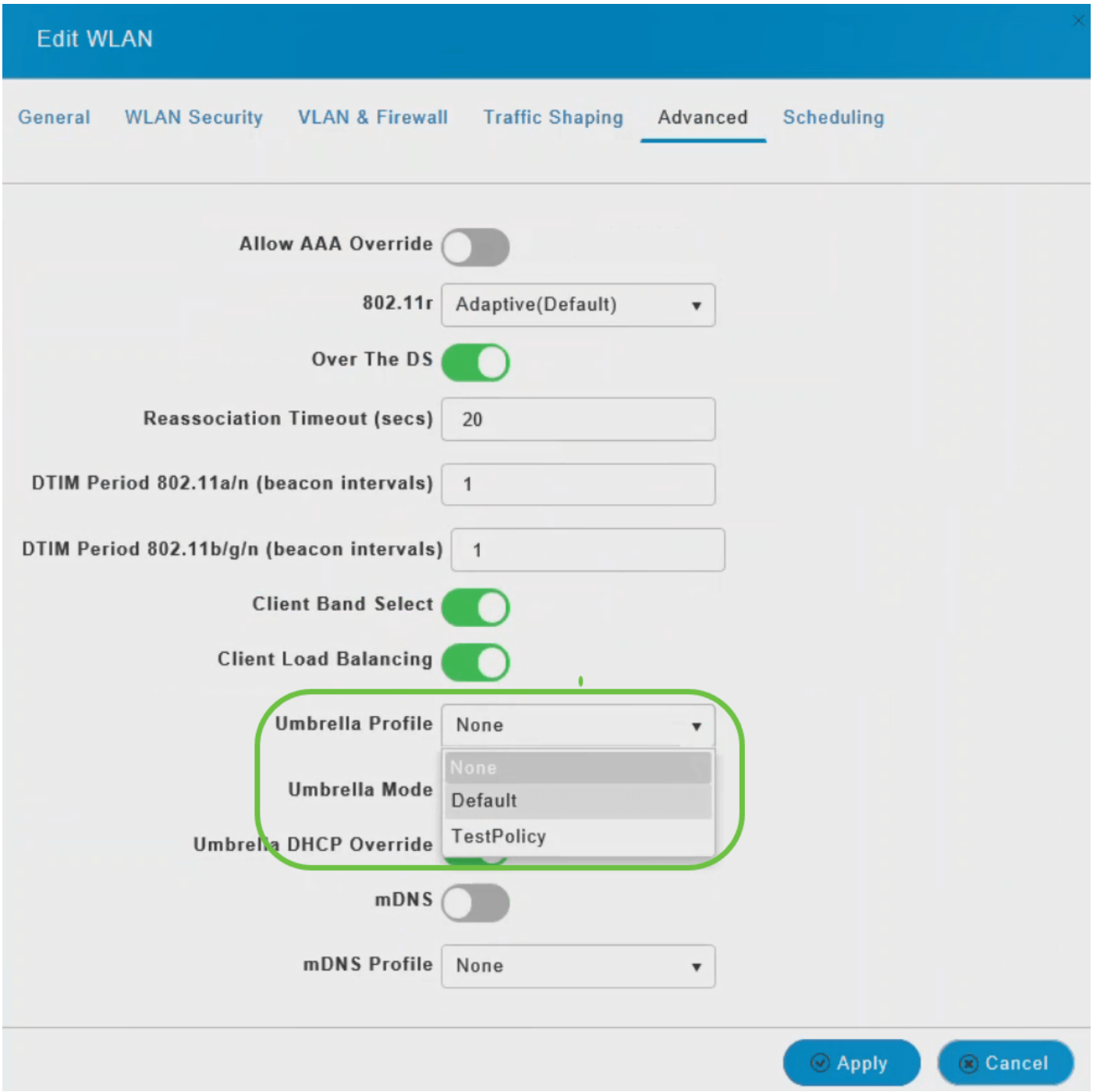
Step 4

In the *Edit WLAN* window, select **Advanced** tab.



Step 5

From the *Umbrella Profile* drop-down list, choose a profile that was created for the WLAN.

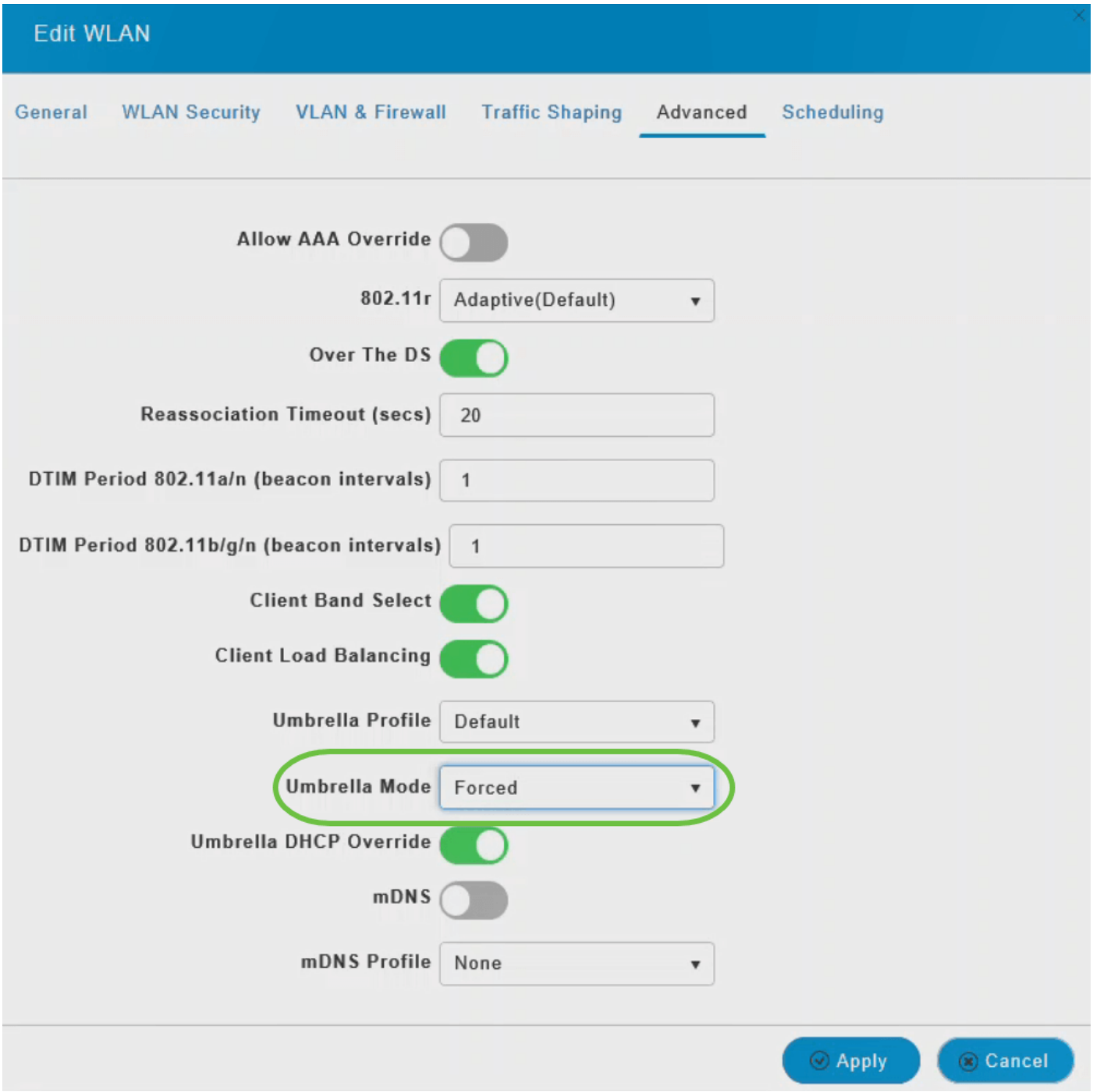


Each WLAN can have a different profile associated with it. For more information on how to add a policy to Umbrella Profile, refer to the CBW AP administration guide.

Step 6

From the *Umbrella Mode* drop-down list, choose either *Ignore* or *Forced*.

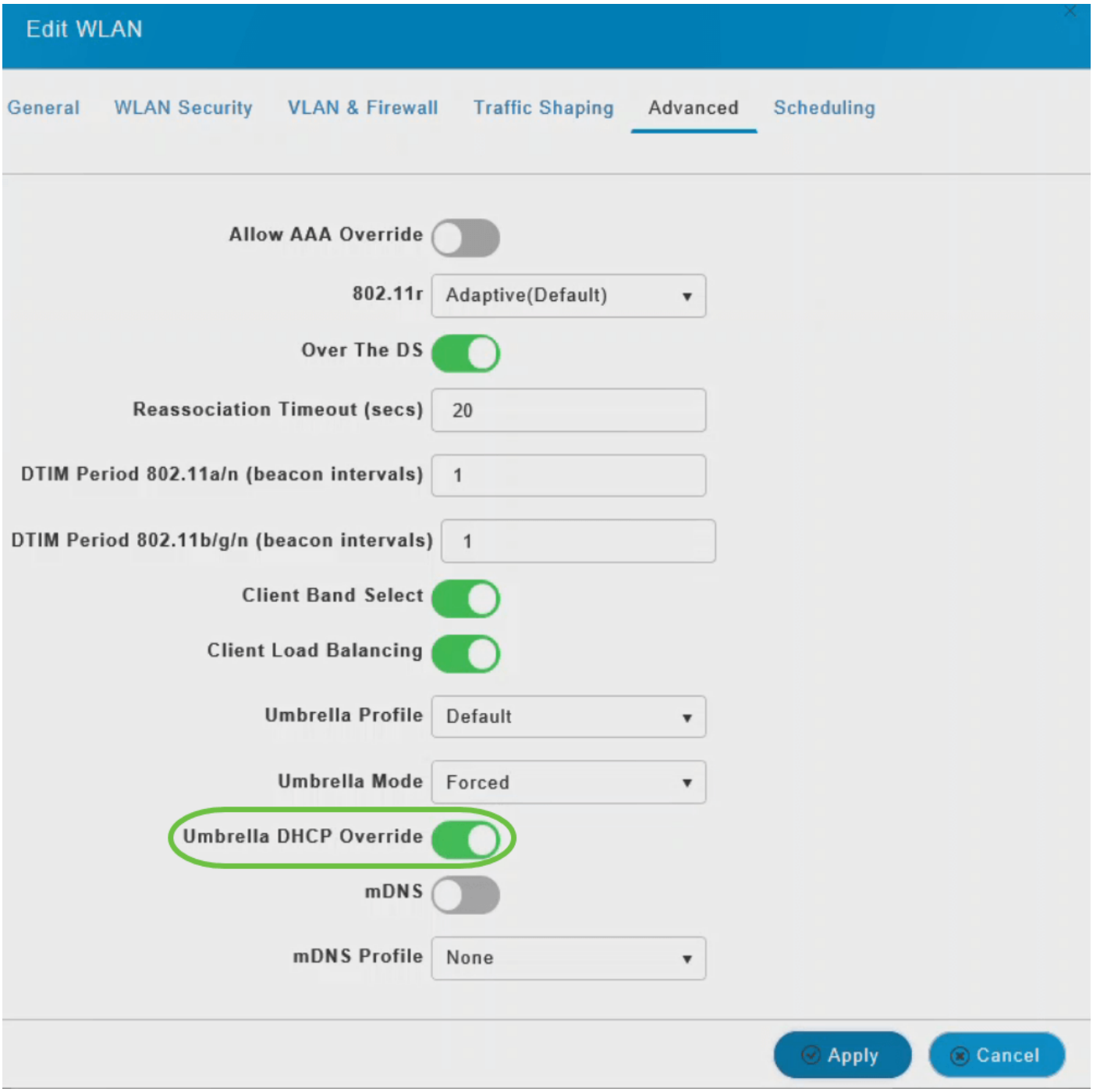
When a client obtains DNS IPs, users can manually change them on the client device, thus bypassing Umbrella policy enforcement. To prevent this security compromise, configure *Umbrella Mode* to **Forced**. This ensures that Umbrella policy enforcement cannot be overridden on the client device.



Step 7

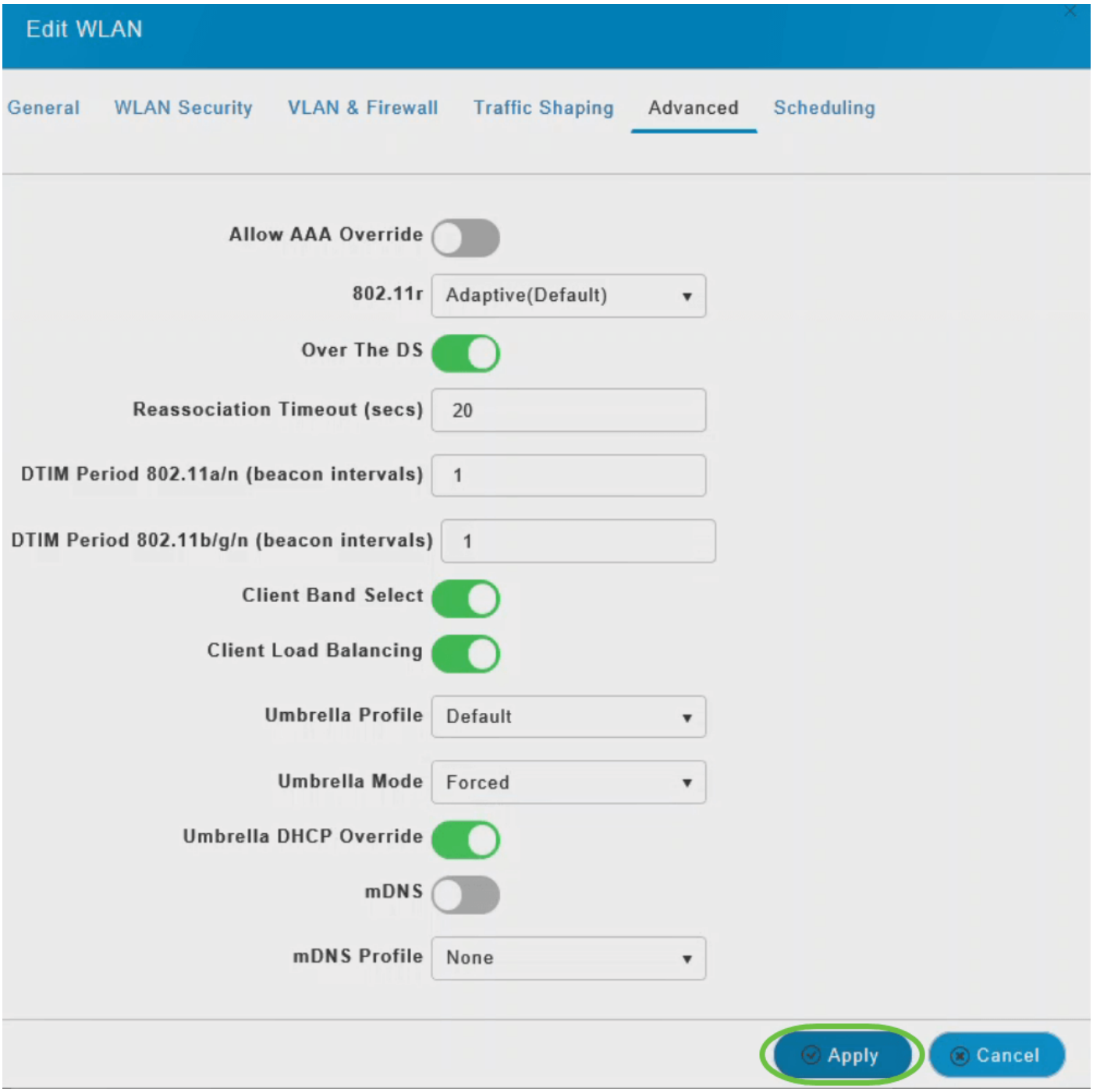
Optionally, use *the Umbrella DHCP Override* toggle button to **enable** the Cisco *Umbrella DHCP override*.

The DNS IP addresses that a client obtains when connecting to the SSID are configured on the DHCP server. For Umbrella enforcement to work, clients must send out DNS requests to Umbrella IP addresses (208.67.222.222, 208.67.220.220). Umbrella DHCP Override ignores the DNS IPs configured via DHCP and forces the Umbrella DNS IPs on the client device.



Step 8

Click **Apply** and save your configuration.



Conclusion

There you have it! You have now successfully completed configuring Cisco Umbrella on your CBW APs.

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

Frequently Asked Questions Radius Firmware Upgrade RLANs Application Profiling Client Profiling Primary AP Tools Umbrella WLAN Users Logging Traffic Shaping Rogues Interferers Configuration Management Port Configuration Mesh Mode Welcome to CBW Mesh Networking Guest Network using Email Authentication and RADIUS Accounting Troubleshooting Using a Draytek Router with CBW