

Cisco Umbrella WLAN (OpenDNS)

- Cisco Umbrella WLAN (OpenDNS), on page 1
- Configuring Cisco Umbrella WLAN (GUI), on page 2
- Configuring Cisco Umbrella WLAN (CLI), on page 3
- Configuring Local Policies for Cisco Umbrella (GUI), on page 4

Cisco Umbrella WLAN (OpenDNS)

The Cisco Umbrella WLAN (OpenDNS) provides a cloud-delivered network security service at the Domain Name System (DNS) level, with automatic detection of both known and emergent threats.

This feature allows you to block sites that host malware, bot networks, and phishing before they actually become malicious.

Cisco Umbrella WLAN provides:

- Policy configuration per user group at a single point.
- Policy configuration per network, group, user, device, or IP address.

  The following is policy priority order:

  1. Local policy
  2. AP group
  3. WLAN

- Visual security activity dashboard in real time with aggregated reports.
- Schedule and send reports through email.
- Support up to 60 content categories, with a provision to add custom allowed list and blocked list entries.

This feature does not work in the following scenarios:

- If an application or host use an IP address directly, instead of using DNS to query domain names.
- If a client is connected to a web proxy and does not send a DNS query to resolve the server address.

Note For more information about integrating this feature, see the *Cisco Umbrella WLAN Integration Guide* at

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_cisco_umbrella_wlan_integration_guide.html

.

Configuring Cisco Umbrella WLAN (GUI)

Before you begin

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

Procedure

Step 1 Choose **Security** > **Umbrella** > **General**.

The **Umbrella General Configuration** window is displayed.

Step 2 Check the **Umbrella Global Status** check box to enable Umbrella configuration.

Step 3 In the **Umbrella-ApiToken** field, enter the API-token obtained from the Umbrella Server account.

Step 4 In the **Profile Name** field, enter the profile name that is to be used in the Umbrella configuration.

Step 5 Click **Add**.

Step 6 Map the profile to the corresponding WLAN or AP group.

a) To map the profile to a WLAN, choose **WLAN** > **WLAN ID** > **Advanced**, and from the **Umbrella Profile**, select the desired profile.

Note
An administrator can configure Umbrella in a WLAN in the following modes under the WLAN advanced tab:

- **DHCP Proxy for DNS override** - This is the interface-level configuration, which forms part of the DHCP process to propagate Umbrella IP address to all WLANs associated to the interface.
- **Umbrella Mode Force (default)** - This mode is enforced per WLAN, which blocks intentional client activity after client is associated to aWLAN.
- **Umbrella Mode Ignore (default)** - The controller honors the DNS server used by the client, which could be Umbrella server or enterprise/external DNS.

b) To map the profile to an AP group, choose **WLANs** > **Advanced** > **AP Groups**, select the corresponding AP group, click the **WLAN** tab, and mouse over the blue button and select **Umbrella Profile**.

To view Umbrella mapping, choose **Security** > **Umbrella** > **General** and click the **Profile Mapped Summary** hyperlink.

Note
Each Cisco Umbrella profile will have a unique Umbrella-Identity generated on the controller (in the format *Controller name _profile name*). This will be pushed to the associated Cisco Umbrella account in the cloud.

Step 7 Click **Apply**.

What to do next

1. From the Cisco Umbrella dashboard, verify that your controller shows up under **Device Name**, along with their identities controller.
2. Create classification rules for the user roles, for example, rules for employees and nonemployees.
3. Configure policies on the Cisco Umbrella server.

Configuring Cisco Umbrella WLAN (CLI)

This section describes the procedure to configure Cisco Umbrella for a wireless LAN (WLAN) or an access point (AP) group in a WLAN.

Before you begin

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

Procedure

Step 1 **config network dns serverip** *server-ip*

Example:

```
(Cisco Controller) > config network dns serverip 208.67.222.222
```

Configures the DNS server IP address of the network.

Step 2 **config opendns enable**

Example:

```
(Cisco Controller) > config opendns enable
```

Enables the Cisco Umbrella global configuration.

Step 3 **config opendns api-token** *api-token*

Example:

```
(Cisco Controller) > config opendns api-token
D72996C18DC334FB2E3AA46148D600A4001E5997
```

Registers the Cisco Umbrella API token on the network.

Step 4 **config opendns profile create** *profilename*

Example:

```
(Cisco Controller) > config opendns profile create profile1
```

Creates an Cisco Umbrella profile that can be applied over a WLAN.

Step 5 **config wlan opendns-profile** *wlan-id profile-name* **enable**

Example:

```
(Cisco Controller) > config wlan opendns-profile wlan1 profile1 enable
```

Applies the Cisco Umbrella profile to a WLAN.

Step 6 **config wlan apgroup opendns-profile** *wlan-id site-name profile-name* **enable**

Example:

```
(Cisco Controller) >config wlan apgroup opendns-profile wlan1 apgrp1 profile1
```

(Optional) Applies the Cisco Umbrella profile to an AP group with the WLAN.

Step 7 **config policy** *policy-name* **create**

Example:

```
(Cisco Controller) > config policy ipad create
```

Creates a policy name.

In controller, policy is generic term that specifies a rule and the associated action when that rule criterion is met for given client.

You can create policy and have rule on that by saying if the rolename from AAA server comes as *employee* take an action to apply Cisco Umbrella profile associated to that policy. Cisco Umbrella profile is applied to the client if the WLAN of that client is mapped for this policy.

Step 8 **config policy** *policy-name* **action opendns-profile-name enable**

Example:

```
(Cisco Controller) > config policy ipad action opendns-profile-name enable
```

Attaches the policy name to the Cisco Umbrella profile.

What to do next

Configure policies in opendns.com.

- Configure granular policies to block sites based on the category of each profile (profiles are listed as identities).
- Add allowed list and blocked list rules for each profile.

Configuring Local Policies for Cisco Umbrella (GUI)

When mapped to local policy, the Cisco Umbrella allows for a granular differentiated user browsing experience based on dynamic evaluation of attributes (user role, device type, and so on).

Use this procedure to configure user role based local policy and tie the corresponding Cisco Umbrella profile to it. This procedure also provides information about how to map a local policy to a WLAN.

Procedure

Step 1 Choose **Security** > **Local Policies** > **New**.

This opens the new policy creation page.

a) In the **Policy Name** field, enter the local policy name.
b) Click **Apply**.

Step 2 From the policies listed under **Policy List**, choose a **Policy Name** to configure the Cisco Umbrella profile.

a) From the **Match Criteria** sub-section, enter the Match Role String.
b) From the **Action** sub-section, select the required option from the Umbrella Profile drop-down list.
c) Click **Apply**.

Step 3 Choose **WLAN** > **WLAN ID** > **Policy Mapping**.

a) In the **Priority Index** field, enter the priority index number.
b) From the **Local Policy** drop-down list, choose a value.
c) Click **Add**.

What to do next

Verify whether the policies you created are working, by connecting a client to the WLAN.