



## Cisco Umbrella WLAN

---

- [Information About Cisco Umbrella WLAN, on page 1](#)
- [Registering Embedded Wireless Controller to Cisco Umbrella Account, on page 2](#)
- [Configuring Cisco Umbrella WLAN, on page 3](#)
- [Verifying the Cisco Umbrella Configuration, on page 8](#)

## Information About Cisco Umbrella WLAN

The Cisco Umbrella WLAN 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 the following:

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

The following is the 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.

# Registering Embedded Wireless Controller to Cisco Umbrella Account

## Before you Begin

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

The embedded wireless controller is registered to Cisco Umbrella server using the Umbrella parameter map. Each of the Umbrella parameter map must have an API token. The Cisco Umbrella responds with the device ID for the embedded wireless controller. The device ID has a 1:1 mapping with the Umbrella parameter map name.

## Fetching API token for Embedded Wireless Controller from Cisco Umbrella Dashboard

From Cisco Umbrella dashboard, verify that your embedded wireless controller shows up under Device Name, along with their identities.

## Applying the API Token on Embedded Wireless Controller

Registers the Cisco Umbrella API token on the network.

## DNS Query and Response

Once the device is registered and Umbrella parameter map is configured on WLAN, the DNS queries from clients joining the WLAN are redirected to the Umbrella DNS resolver.



---

**Note** This is applicable for all domains not configured in the local domain RegEx parameter map.

---

The queries and responses are encrypted based on the DNSCrypt option in the Umbrella parameter map.

For more information on the Cisco Umbrella configurations, see the [Integration for ISR 4K and ISR 1100 – Security Configuration Guide](#).

## Limitations and Considerations

The limitations and considerations for this feature are as follows:

- You will be able to apply the wireless Cisco Umbrella profiles to wireless entities, such as, WLAN or AP groups, if the device registration is successful.
- In case of L3 mobility, the Cisco Umbrella must be applied on the anchor embedded wireless controller always.
- When two DNS servers are configured under DHCP, two Cisco Umbrella server IPs are sent to the client from DHCP option 6. If only one DNS server is present under DHCP, only one Cisco Umbrella server IP is sent as part of DHCP option 6.

# Configuring Cisco Umbrella WLAN

To configure Cisco Umbrella on the embedded wireless controller, perform the following:

- You must have the API token from the Cisco Umbrella dashboard.
- You must have the root certificate to establish HTTPS connection with the Cisco Umbrella registration server: [api.opendns.com](https://api.opendns.com). You must import the root certificate from **digicert.com** to the embedded wireless controller using the **crypto pki trustpool import terminal** command.

## Importing CA Certificate to the Trust Pool

### Before you begin

The following section covers details about how to fetch the root certificate and establish HTTPS connection with the Cisco Umbrella registration server:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	Perform either of the following tasks: <ul style="list-style-type: none"> <li>• <b>crypto pki trustpool import url url</b>                 Device(config)# <code>crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b</code>                 Imports the root certificate directly from the Cisco website.   <b>Note</b> The Trustpool bundle contains the root certificate of <i>digicert.com</i> together with other CA certificates.</li> <li>• <b>crypto pki trustpool import terminal</b>                 Device(config)# <code>crypto pki trustpool import terminal</code>                 Imports the root certificate by executing the import terminal command.</li> <li>• Enter PEM-formatted CA certificate from the following location: See the Related Information section to download the CA certificate.</li> </ul>	

	Command or Action	Purpose
	<pre>-----BEGIN CERTIFICATE----- MIIEGjCCAgAwgCqCJULMqK9K1wA3NBjchc9MBA3BHMbCQDQ EoUEBMAIKHMKGraNcrQ86jRkEVMQEESSRzGraNcrQ129MA HjDQDEdchq2VcHhG9Vgjn9dEQA6QMD9jOMAMIEB0MD9Mj MELNMA3CAIBjNBAVAMRGEADQBE6aVQ2VcHhMKAIBjNEMIEB Z2DZC0IHRUyBjDg10BjZ2DWA9QEMIEFjNbjchc9MBA3BHMb CjCAEALZLhWNBNS0BZLUMNijR6S1hBEU1BjD3HE0TajcbjL E8Hj2WihHjQHEGAE5Mf5HjLIE5SjVQE9KhwGnc9f0rTCR60R0 Vf0L99qj1h66QUNwRAIE/hjLhJhWkGr6Bz6GEdN4Z2LY8V muf9bjk5j1hBR3LUNQjG655jK04hyR3LQ83Nec0L6WfGj40 K67S9h308Lz2heocicq7QPIU4kz7QDA64BjCAoHQDROBE Eldcupp8eeQ2j959W0MBALicQMazFARLW0j7ZCj4sb5e2FMMG ALdEB/cQABjAcjNBEFjAegEjRQ2QIKWHEjHAEjDFOUqH/B9y RjEjwEABEgRjEgRjEgRjEgRjEgRjEgRjEgRjEgRjEgRjEgRjE jN5EABegRjEgRjEgRjEgRjEgRjEgRjEgRjEgRjEgRjEgRjEgR YB5j9dBNhjdEBjNBEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjE RGrANcrH68Yw829QBE3BMEjEjEjEjEjEjEjEjEjEjEjEjEjE RGrANcrH68Yw829QBE3BMEjEjEjEjEjEjEjEjEjEjEjEjEjE BEHKAjYBjE 35H5E7U8A70wESB0rCj9UR3GQjE5rkd3EhqmTCEBchL4Gw0E2 UKEPvUjE 5qf66snKHMEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjE YRhs6wAep89xzEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjEjE SaZMkE4f97Q= -----END CERTIFICATE-----</pre> <p>Imports the root certificate by pasting the CA certificate from the <b>digicert.com</b>.</p>	
<b>Step 3</b>	<p><b>quit</b></p> <p><b>Example:</b></p> <pre>Device (config) # quit</pre>	<p>Imports the root certificate by entering the <b>quit</b> command.</p> <p><b>Note</b> You will receive a message after the certificate has been imported.</p>

## Creating a Local Domain RegEx Parameter Map

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>parameter-map type regex</b> <i>parameter-map-name</i></p> <p><b>Example:</b></p> <pre>Device (config) # parameter-map type regex dns_w1</pre>	Creates a regex parameter map.
<b>Step 3</b>	<p><b>pattern</b> <i>regex-pattern</i></p>	Configures the regex pattern to match.

	Command or Action	Purpose
	<b>Example:</b> <pre>Device(config-profile)# pattern www.google.com</pre>	<b>Note</b> The following patterns are supported: <ul style="list-style-type: none"> <li>• Begins with .*. For example: <b>. *facebook. com</b></li> <li>• Begins with .* and ends with *. For example: <b>. *google*</b></li> <li>• Ends with *. For example: <b>www. facebook*</b></li> <li>• No special character. For example: <b>www. facebook. com</b></li> </ul>
<b>Step 4</b>	<b>end</b>  <b>Example:</b> <pre>Device(config-profile)# end</pre>	Returns to privileged EXEC mode.

## Configuring Parameter Map Name in WLAN (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.
- Step 3** Choose the **Advanced** tab.
- Step 4** In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.
- Step 5** Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.
- Step 6** Click **Update & Apply to Device**.
- 

## Configuring the Umbrella Parameter Map

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>parameter-map type umbrella global</b>  <b>Example:</b> Device(config)# <b>parameter-map type umbrella global</b>	Creates an umbrella global parameter map.
<b>Step 3</b>	<b>token token-value</b>  <b>Example:</b> Device(config-profile)# <b>token 5XX</b>	Configures an umbrella token.
<b>Step 4</b>	<b>local-domain regex-parameter-map-name</b>  <b>Example:</b> Device(config-profile)# <b>local-domain dns_w1</b>	Configures local domain RegEx parameter map.
<b>Step 5</b>	<b>resolver {IPv4 X.X.X.X   IPv6 X:X:X:X::X}</b>  <b>Example:</b> Device(config-profile)# <b>resolver IPv6 10:1:1:1::10</b>	Configures the Anycast address. The default address is applied when there is no specific address configured.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Device(config-profile)# <b>end</b>	Returns to privileged EXEC mode.

## Enabling or Disabling DNScrypt (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Threat Defence > Umbrella**.
  - Step 2** Enter the **Registration Token** received from Umbrella. Alternatively, you can click on **Click here to get your Token** to get the token from Umbrella.
  - Step 3** Enter the **Whitelist Domains** that you want to exclude from filtering.
  - Step 4** Check or uncheck the **Enable DNS Packets Encryption** check box to encrypt or decrypt the DNS packets.
  - Step 5** Click **Apply**.
- 

## Enabling or Disabling DNScrypt

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 2</b>	<b>parameter-map type umbrella global</b> <b>Example:</b> Device(config)# <code>parameter-map type umbrella global</code>	Creates an umbrella global parameter map.
<b>Step 3</b>	<b>[no] dnscrypt</b> <b>Example:</b> Device(config-profile)# <code>no dnscrypt</code>	Enables or disables DNSCrypt. By default, the DNSCrypt option is enabled. <b>Note</b> Cisco Umbrella DNSCrypt is not supported when DNS-encrypted responses are sent in the data-DTLS encrypted tunnel (either mobility tunnel or AP CAPWAP tunnel).
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-profile)# <code>end</code>	Returns to privileged EXEC mode.

## Configuring Timeout for UDP Sessions

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>parameter-map type umbrella global</b> <b>Example:</b> Device(config)# <code>parameter-map type umbrella global</code>	Creates an umbrella global parameter map.
<b>Step 3</b>	<b>udp-timeout <i>timeout_value</i></b> <b>Example:</b> Device(config-profile)# <code>udp-timeout 2</code>	Configures timeout value for UDP sessions. The <i>timeout_value</i> ranges from 1 to 30 seconds. <b>Note</b> The <b>public-key</b> and <b>resolver</b> parameter-map options are automatically populated with the default values. So, you need not change them.
<b>Step 4</b>	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device (config-profile) # <b>end</b>	

## Configuring Parameter Map Name in WLAN (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
  - Step 2** Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.
  - Step 3** Choose the **Advanced** tab.
  - Step 4** In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.
  - Step 5** Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.
  - Step 6** Click **Update & Apply to Device**.
- 

## Configuring Parameter Map Name in WLAN

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-name</i></b>  <b>Example:</b> Device (config)# <code>wireless profile policy default-policy-profile</code>	Creates policy profile for the WLAN. The <i>profile-name</i> is the profile name of the policy profile.
<b>Step 3</b>	<b>umbrella-param-map <i>umbrella-name</i></b>  <b>Example:</b> Device (config-wireless-policy)# <code>umbrella-param-map global</code>	Configures the Umbrella OpenDNS feature for the WLAN.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Device (config-wireless-policy) # <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying the Cisco Umbrella Configuration

To view the Umbrella configuration details, use the following command:



```

Device# show umbrella config
Umbrella Configuration
=====
Token: 5XXXXXXXXABXXXXXXFXXXXXXXXXDXXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxxx
Local Domain Regex parameter-map name: dns_bypass
DNSEncrypt: Not enabled
Public-key: NONE
UDP Timeout: 5 seconds
Resolver address:
1. 10.1.1.1
2. 5.5.5.5
3. XXXX:120:50::50
4. XXXX:120:30::30

```

To view the Umbrella DNSEncrypt details, use the following command:

```

Device# show umbrella dnscrypt
DNSEncrypt: Enabled
    Public-key: B111:XXXX:XXXX:XXXX:3E2B:XXXX:XXXX:XXxE:XXX3:3XXX:DXXX:XXXX:BXXX:XXxB:XXXX:FXXX

    Certificate Update Status: In Progress

```

To view the Umbrella global parameter map details, use the following command:

```
Device# show parameter-map type umbrella global
```

To view the regex parameter map details, use the following command:

```
Device# show parameter-map type regex <parameter-map-name>
```

To view the Umbrella details on the AP, use the following command:

```

AP#show client.opendns summary
Server-IP role
208.67.220.220 Primary
208.67.222.222 Secondary

Server-IP role
2620:119:53::53 Primary
2620:119:35::35 Secondary

Wlan Id DHCP OpenDNS Override Force Mode
0 true false
1 false false
...

15 false false
Profile-name Profile-id
vj-1 010a29b176b34108
global 010a57bf502c85d4
vj-2 010ae385ce6c1256
AP0010.10A7.1000#

Client to profile command

AP#show client.opendns address 50:3e:aa:ce:50:17
Client-mac Profile-name
50:3E:AA:CE:50:17 vj-1
AP0010.10A7.1000#

```

