



Cisco Umbrella WLAN

- [Information About Cisco Umbrella WLAN, on page 1](#)
- [Registering 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 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.

This section describes the process followed to register the controller to the Cisco Umbrella account.

The 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 controller. The device ID has a 1:1 mapping with the Umbrella parameter map name.

Fetching API token for Controller from Cisco Umbrella Dashboard

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

Applying the API Token on 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 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 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. You must import the root certificate from **digicert.com** to the 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
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	Perform either of the following tasks: <ul style="list-style-type: none"> • crypto pki trustpool import url url 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. Note The Trustpool bundle contains the root certificate of <i>digicert.com</i> together with other CA certificates. • crypto pki trustpool import terminal Device(config)# <code>crypto pki trustpool import terminal</code> Imports the root certificate by executing the import terminal command. • Enter PEM-formatted CA certificate from the following location: See the Related Information section to download the CA certificate. 	

	Command or Action	Purpose
	<pre>-----BEGIN CERTIFICATE----- MIIEGjCCAgAwgCqjUIMwK9K1wA3NBjchc9MBA3BHMbCQDQg EwUUEMBAIKHMKGraNcrQ85jRkEVMQJES8BzGraNcrQ129MAw HjDQDEdchq2VcHhG9Vvgj9dEQA6QMD9jQMDAMIEB0MD9Mjy MELN1M3CAIBjNBA1MFR6EADQ8E8AVQ2VcHhMKAIBjNEMIEB Z2DZC0IHRUyB8Dg10BjZ2DZM9Q0EMIEF7NBjchc9MBA3BHMb CjCQAA1Z1hWNBNS0BZ1UMN1jR851hEUI8YD3HE07aqtqjL E85j2W1HIQNHCA7B5157Hj1E55VQE9K7w6atp910rTCR80R0 Vf01u9qj1h65QUNwRAIE/1h1h1h1h1h1h1h1h1h1h1h1h1h1h1 nuh9j85j1h8R3QUNQj8E55j7C4hyR3Q83Nec016W8Qj40 K67S9h3081vZ1heocicq7QPI114kz7QDA84Bj7CAoHQDROBE Eldcupp8eepQ2j85W0MBAL1h1QMA7ARLDV0j7ZC4h305jEPM4G A1hDEB/QAIBj7d3jVBEF7A8gE8E8Q2Q1KWEQ1HAW8jDF014h30y RjE7EAE8gRjE8Q8Q6y7KWEQ1HAGG0HPQ302W1h3Z1j7C0 1hN5E8gE8E8Q6y7KWEQ1HAGG0HPQ302W1h3Z1j7C0 Y8519d8H1jDEBjV8E1BME8j7dR0C813B45d02y15j20v RCraNcrH68Y829Q813BME8j7dR0C813B45d02y15j20v RCraNcrH68Y829Q813BME8j7dR0C813B45d02y15j20v B8E8C7j8E8j0E8Q40KZ1h1h1h1h1h1h1h1h1h1h1h1h1h1h1 35H8E71h8A70E8810r7KUR8Q8j851d3E8q1h1h1h1h1h1h1h1 U2K8V1h8E8j82330HMLk8C7h8E8W1w8E8j7/1h1h1h1h1h1h1 5g8888K1h1 YR1h6uA8p838x2E8j8q8j8z8E8j8E8UAC881h1h1h1h1h1h1h1 SaZMkE4f97Q= -----END CERTIFICATE-----</pre> <p>Imports the root certificate by pasting the CA certificate from the digicert.com.</p>	
Step 3	<p>quit</p> <p>Example:</p> <pre>Device(config)# quit</pre>	<p>Imports the root certificate by entering the quit command.</p> <p>Note You will receive a message after the certificate has been imported.</p>

Creating a Local Domain RegEx Parameter Map

Procedure

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

	Command or Action	Purpose
	Example: <pre>Device(config-profile)# pattern www.google.com</pre>	Note The following patterns are supported: <ul style="list-style-type: none"> • Begins with <code>.*</code>. For example: <code>.*facebook.com</code> • Begins with <code>.*</code> and ends with <code>*</code>. For example: <code>.*google*</code> • Ends with <code>*</code>. For example: <code>www.facebook*</code> • No special character. For example: <code>www.facebook.com</code>
Step 4	end Example: <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
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 2	parameter-map type umbrella global Example:	Creates an umbrella global parameter map.

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

	Command or Action	Purpose
Step 2	parameter-map type umbrella global Example: Device(config)# parameter-map type umbrella global	Creates an umbrella global parameter map.
Step 3	[no] dnscrypt Example: Device(config-profile)# no dnscrypt	Enables or disables DNScrypt. By default, the DNScrypt option is enabled. Note 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).
Step 4	end Example: Device(config-profile)# end	Returns to privileged EXEC mode.

Configuring Timeout for UDP Sessions

Procedure

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

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-name</i> Example: 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.
Step 3	umbrella-param-map <i>umbrella-name</i> Example: Device(config-wireless-policy)# <code>umbrella-param-map global</code>	Configures the Umbrella OpenDNS feature for the WLAN.
Step 4	end Example: Device(config-wireless-policy)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z 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: 5XXXXXXXXABXXXXXFXXXXXXXXDXXXXXXXXXXABXX
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 statistical information, use the following command:

```
Device# show platform hardware chassis active qfp feature umbrella datapath stats
```

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#
```

