



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](#)
- [Configuring the Umbrella Flex Profile, on page 9](#)
- [Configuring the Umbrella Flex Profile \(GUI\), on page 9](#)
- [Configuring Umbrella Flex Parameters, on page 10](#)
- [Configuring the Umbrella Flex Policy Profile \(GUI\), on page 10](#)
- [Verifying the Cisco Umbrella Configuration, on page 11](#)

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.
 - Supports custom parameter-type Umbrella profiles. One Global profile and 15 custom profiles are supported.

- Although IPv6 is supported, device registration will always be over IPv4. There is no support of device registration over IPv6.
- The communication from device to the Umbrella Cloud can be done over IPv6 also.
- In the Flexconnect mode, DNS handling takes place in the AP instead of the controller. Multiple profiles are supported in the Flex mode.

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# configure terminal	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)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b Imports the root certificate directly from the Cisco website.	

	Command or Action	Purpose
	<p>Note The Trustpool bundle contains the root certificate of <i>digicert.com</i> together with other CA certificates.</p> <ul style="list-style-type: none"> • crypto pki trustpool import terminal <pre>Device (config) # crypto pki trustpool import terminal</pre> <p>Imports the root certificate by executing the import terminal command.</p> <ul style="list-style-type: none"> • Enter PEM-formatted CA certificate from the following location: See the Related Information section to download the CA certificate. <pre>-----BEGIN CERTIFICATE----- MIIECAIBAgEQAQJLIMKwEKLVA/3DNEjchk9OABFHMbcQDQCE EwUeRMMGALKMRCraNcrQ5fHrWMDQEBBnZGanLrQJ29Mw HjDQDEcdavq2VdBI62Wgjr9dBI7a5QMD8JOMAMB50MD8Mj MhNLAwSCABN5VAMTR6EMDQEBFavq2VdBI6MKA6jNEMTEp Z2IXOIH8UjBj0BjZ2LW9Q0EMIEFNEjchk9OABFROAQMIB CjCAQAVLZGwNIPNsCZULMNUjBj0BjZ2LW9Q0EMIEFavq2V EhH9AWiHIQHEGATB1S5HjLd55NQE9K0w0ng/0hTCTR80ND VfQIu9qJhMbfQUNwRPAIE/1pLhJhWakTn65z6C6DhE2LDy7 mzH9jRk5ThER6U9TQjG55j7K74hyER3Uq83Nco06VW9j5k0 K6/3H3b0Eh2hEacicq7KPRITTHk4c9JDA9B4BjCa0MDR0BB Eldcupp8eeq2y55W0rMBALhQMzFA8LDWJ7dC48b69PTM4C AllDEE/QAwBjR6NFBFjUBgRjHq2QIKW8QhAwRjDR0RQH3y EjE7eEAE8gRjE8QQR6yFVKW8QhAGG8QhA9192N68Z2J2X0 TnK5E8gRjE8QQR6yFVKW8QhAGG8QhA9192N68Z2J2X0R2v Y8B9dBNjDEBjNFR6EMjBj0BjZ2LW9Q0EMIEFavq2Vd5j20v RCraNcrH62W829Q0B13BMA6jHj0R0813BC5aQ2y4d5j20v RCraNcrH62W829Q0B13BMA6jHj0R0813BC5aQ2y4d5j20v EeBACjUBj0BjZ2LW9Q0EMIEFavq2Vd5j20vYRhs6uWp89wZfngq0JozXk05f2UACh8VUzwd0E2B51E8 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	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	parameter-map type regex <i>parameter-map-name</i> Example: Device(config)# <code>parameter-map type regex</code> <code>dns_wl</code>	Creates a regex parameter map.
Step 3	pattern <i>regex-pattern</i> Example: Device(config-profile)# <code>pattern</code> <code>www.google.com</code>	Configures the regex pattern to match. 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: Device(config-profile)# <code>end</code>	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: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	parameter-map type umbrella global / parameter-map-name Example: Device(config)# <code>parameter-map type umbrella custom_pmap</code>	Creates an umbrella global or customized parameter map.
Step 3	token token-value Example: Device(config-profile)# <code>token 5XX</code>	Configures an umbrella token.
Step 4	local-domain regex-parameter-map-name Example: Device(config-profile)# <code>local-domain dns_w1</code>	Configures local domain RegEx parameter map.
Step 5	resolver {IPv4 X.X.X.X IPv6 X:X:X:X::X} Example: Device(config-profile)# <code>resolver IPv6 10:1:1:1::10</code>	Configures the Anycast address. The default address is applied when there is no specific address configured.
Step 6	end Example: Device(config-profile)# <code>end</code>	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# <code>configure terminal</code>	Enters global configuration mode.
Step 2	parameter-map type umbrella global Example: Device(config)# <code>parameter-map type umbrella global</code>	Creates an umbrella global parameter map.
Step 3	[no] dnsencrypt Example: Device(config-profile)# <code>no dnsencrypt</code>	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)# <code>end</code>	Returns to privileged EXEC mode.

Configuring Timeout for UDP Sessions

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	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	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# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-name</i> Example:	Creates policy profile for the WLAN.

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

Configuring the Umbrella Flex Profile

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>Device# configure terminal</code>	Enters global configuration mode.
Step 2	wireless profile flex <i>flex-profile-name</i> Example: <code>Device(config)# wireless profile flex default-flex-profile</code>	Creates a new flex policy. Enters the flex profile configuration mode. The <i>flex-profile-name</i> is the flex profile name.
Step 3	umbrella-profile <i>umbrella-profile-name</i> Example: <code>Device(config-wireless-flex-profile)# umbrella-profile global</code>	Configures the Umbrella flex feature. Use the no form of this command to negate the command or to set the command to its default.
Step 4	end Example: <code>Device(config-wireless-policy)# end</code>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring the Umbrella Flex Profile (GUI)

Procedure

- Step 1** Choose **Configuration > Tags & Profiles > Flex**.

- Step 2** Click a **Flex Profile Name**. The **Edit Flex Profile** dialog box appears.
- Step 3** Under the **Umbrella** tab, click the **Add** button.
- Step 4** Select a name for the parameter map from the **Parameter Map Name** drop-down list and click **Save**.
- Step 5** Click the **Update & Apply to Device** button. The configuration changes are successfully applied.

Configuring Umbrella Flex Parameters

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-policy-name</i> Example: Device(config)# <code>wireless profile policy default-policy-profile</code>	Configures the WLAN policy profile. Enters the wireless policy profile configuration mode. The <i>policy-profile-name</i> is the WLAN policy profile name.
Step 3	flex umbrella dhcp-dns-option Example: Device(config-wireless-policy-profile)# <code>[no] flex umbrella dhcp-dns-option</code>	Configures the Umbrella DHCP option for DNS. By default the option is enabled.
Step 4	flex umbrella mode {force ignore} Example: Device(config-wireless-policy-profile)# <code>[no] flex umbrella mode force</code>	Configures the DNS traffic to be redirected to Umbrella. You can either forcefully redirect the traffic or choose to ignore the redirected traffic to Umbrella. The default mode is ignore .
Step 5	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.

Configuring the Umbrella Flex Policy Profile (GUI)

Procedure

- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** Click the **Add** button. The **Add Policy Profile** dialog box appears.
- Step 3** In the **Advanced** tab, and under the **Umbrella** section, complete the following:

- a) Select the parameter map from the **Umbrella Parameter Map** drop-down list. Click the **Clear** hyperlink to clear the selection.
- b) Click the field adjacent to **Flex DHCP Option for DNS** to **Disable** the option. By default it is **Enabled**.
- c) Click the field adjacent to **DNS Traffic Redirect** to set the option to **Force**. By default it is set to **Ignore**.

Step 4 Click the **Apply to Device** button.

Verifying the Cisco Umbrella Configuration

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

```
Device# show umbrella config
Umbrella Configuration
=====
Token: 5XXXXXXXXABXXXXFXXXXXXXXXDXXXXXXXXXXXABXX
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 device registration details, use the following command:

```
Device# show umbrella deviceid
Device registration details
Param-Map Name          Status      Device-id
global                  200 SUCCESS 010aa4eXXXXXXXX8d
vj-1                    200 SUCCESS 01XXXXXXXXf4541e1
GUEST                   200 SUCCESS 010a4f6XXXXXXXX42
EMP                     200 SUCCESS 0XXXXXXXXd106ecd
```

To view the detailed description for the Umbrella device ID, use the following command:

```
Device# show umbrella deviceid detailed
Device registration details

1.global
  Tag           : global
  Device-id     : 010aa4eXXXXXXXX8d
  Description   : Device Id recieved successfully
  WAN interface : None
2.vj-1
  Tag           : vj-1
  Device-id     : 01XXXXXXXXf4541e1
  Description   : Device Id recieved successfully
  WAN interface : None
```

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 wireless policy profile Umbrella configuration, use the following command:

```
Device#show wireless profile policy detailed vj-pol-profile | s Umbrella
Umbrella information
Cisco Umbrella Parameter Map : vj-2
DHCP DNS Option : ENABLED
Mode : force
```

To view the wireless flex profile Umbrella configuration, use the following command:

```
Device#show wireless profile flex detailed vj-flex-profile | s Umbrella
Umbrella Profiles :
vj-1
vj-2
global
```

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#
```