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. 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
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	Perform either of the following tasks:
	
	• **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.
	
	Note The Trustpool bundle contains the root certificate of *digicert.com* together with other CA certificates.
	
	• **crypto pki trustpool import terminal**
	
	`Device(config)# `**`crypto pki trustpool`**
	`import terminal`
	
	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
-----BEGIN CERTIFICATE----- MIIE6jCCA9KgAwIBAgIQCjUI1MwgKvKF9KL1A/3IABjkkkjki9k0BAQsFADBvMQsWQJDWQQG EwJUEWBGALKMMRGraNlcrQgB5jMRwFMWDWQJEE8BuJGraNlcrQu29MSAw HjNWQJDEdEWqQ2yJdBnH9lWvgn9vdBQJAeKWJMAEMjQMMAMBEEWQMA5MMy MiiFNlaMBCABNEYAYAMMRJUEMWQJKWEWqQ2ydEDbMMKAENVAMTIRb ZIDXUEWUjBUEjjUBmfj2IIwfAQDEMIIEFJAEjkjki9k0BAEJFAWQA9MIIB CjKCAJAWLzUbWNlENUsC8XuiFRNifjpRB8ULWKB9UiNJ5CID3FKUfaqQsbpj EWbjp9wJHIIQNiKS4U8X1fSUkjLUEbjSLQWQE9NEhw6brtg9/r00rTCRt8bMRDi VIFUiu9&piIhMbfyUUNwIRALE//i+plhJInWaKroW8vzf5/GldNH2tIYVJ muH9vJRXjIhaERG/tU9NQDjjUGBfi5yjK7iI4hyfFK3ItqkKA3Nk+c06JWHjKjk0 Kfi7SU*KBv08bvAZhearcicgFXQRUIIAk+c79JIJQAJRr4Ir-jCAoHQDROIBHE Hdcuqpp9Mwf2yf'ssWdnUMBGAUIiQMBaFARitUNW0jj7ZtC/4nbv5ejRFVMG AUIJdWBK/QAwBjAdBgNVEHFjARggEJEBQIAQYKWHEQJAAiWEjUVR0ALH/Bgw BJE/wErAUJEBggReJEHEQJBAQKWGgwAYIKWHEQJHAMJGGUuHAGLy9V3WJuRg2IjjZXU0 InNUERgqReJHEQwA0UQHRutcuJ2hY2yJdMMZJGraNlcrQu29iU0Rg7ZIDXUBzxv YnESu9v0RENinNyJEBRJNHREIBWMmgNaAjrJcuRHcJ8X3BM/5eWQb2Vyd5jz0v RGraNlcrHU0lYWjJ82900EYJ3BMrmgNaAjrJcuRHcJ8X3BN5eWQb2Vyd5jz0v RGraNlcrHU0lYWjJ82900EYJ3BMAGALdAQMoBWEZBMQEWQAGZAMQBWagG BmEHAKCaAJRgJngqBAQMEQJK7ZhvQNAQJEQJQqgBAeE3nR6/9h/jnIuJKiWEX 3SJH/EGf7UIRaAlro+JES3H90urfjKUR3GQNJC0IShckIHEHiqphirIQEBtcH4ZG*6WEZ u2XHcgJVtIRcrpjft223Sc0HMIiwKXq/EKZHr6avEWtrIwCJRjU7/Whc0KK24fSihe 5Uqy66sSnvKiHWNtqfqzjjQAHCjvMnWiNKiKrpJFWIIRMIrcUwdj2UU1QjT19cXCrjI4Zqu YRihs6uvAwqnB9cxxZJFingkjqcqfzjJozX9XRJpfZiUAA/dfK9VtzhwGUU2I3xSTIRC SaZMkE4f97Q= -----END CERTIFICATE----- Imports the root certificate by pasting the CA certificate from the **digicert.com**.	
Step 3	**quit** **Example:** Device(config)# **quit**	Imports the root certificate by entering the **quit** command. **Note** You will receive a message after the certificate has been imported.

Creating a Local Domain RegEx Parameter Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 2	**parameter-map type regex** *parameter-map-name* **Example:** Device(config)# **parameter-map type regex dns_wl**	Creates a regex parameter map.
Step 3	**pattern** *regex-pattern*	Configures the regex pattern to match.

	Command or Action	Purpose	
	Example: Device(config-profile)# pattern www.google.com	**Note**	The following patterns are supported: • Begins with .*. For example: **.*facebook.com** • Begins with .* and ends with *. For example: **.*google*** • Begins with *. For example: ***facebook.com** • Begins with * and ends with *. For example: ***google*** • Ends with *. For example: **www.facebook*** • No special character. For example: **www.facebook.com**
Step 4	**end** **Example:** Device(config-profile)# end	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration 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# 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	**token** *token-value* **Example:** Device(config-profile)# **token 5XXXXXXXCXXXXXXXAXXXXXXXFXXXXCXXXXXXXX**	Configures an umbrella token.
Step 4	**local-domain** *regex-parameter-map-name* **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.
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** *timeout_value* **Example:** `Device(config-profile)# `**`udp-timeout 2`**	Configures timeout value for UDP sessions. The *timeout_value* ranges from 1 to 30 seconds.

	Command or Action	Purpose
		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** *profile-name* **Example:** Device(config)# **wireless profile policy default-policy-profile**	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**umbrella-param-map** *umbrella-name* **Example:** Device(config-wireless-policy)# **umbrella-param-map global**	Configures the Umbrella OpenDNS feature for the WLAN.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	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: 5XXXXXXABXXXXXFXXXXXXXXXDXXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxx
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: 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 DNSCrypt details, use the following command:

```
Device# show umbrella dnscrypt
DNSCrypt: 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#
```