Cisco Umbrella WLAN

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: • **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

	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.
	`-----BEGIN CERTIFICATE-----`
	MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
	EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
	HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
	MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
	Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
	CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
	EVbbHp9YwlHnLQNtK3A1b8X1fs7uHyiUe5pSQWNQE9XE0nw6Dhg9/n0OtrCRpt8OnRt
	VlF0JuJ9x8piIhMbfyOIJVNwIRYAIE//i+p1hJnuWraKmxW8oHzf6VGolbDtN+I2tIJYrVU
	muHZ9bjRXj1hJeRG/cJ9WLQDgIGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWhgXjkkD
	Ka7SU+kEbnO8lwZ2lreacroicqE7XQPUDTTAHk+q9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
	FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
	A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
	BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
	LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
	YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
	RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
	RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
	BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
	3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oW8Z
	u2XHFfq8iVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
	50gG66sSnvKhMNbgOzZgjOrAKHCjxMoiWKikipPMtFUMhoCkw+dj20tlQj7l9rxkTgi4Zxu
	YRiHas6xuwAwapu39rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
	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* **Example:** `Device(config-profile)# pattern www.google.com`	Configures the regex pattern to match. **Note** The following patterns are supported: • 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.

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 5XXXXXXXXCXXXXXXXAXXXXXXXFXXXXCXXXXXXXX`	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:**	Creates an umbrella global parameter map.

	Command or Action	Purpose
	`Device(config)# parameter-map type umbrella global`	
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. **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.

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

Configuring the Umbrella Flex Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. Enters the flex profile configuration mode. The *flex-profile-name* is the flex profile name.
Step 3	**umbrella-profile** *umbrella-profile-name* **Example:** `Device(config-wireless-flex-profile)# umbrella-profile global`	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:** `Device(config-wireless-policy)# end`	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# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile. Enters the wireless policy profile configuration mode. The *policy-profile-name* is the WLAN policy profile name.
Step 3	**flex umbrella dhcp-dns-option** **Example:** `Device(config-wireless-policy-profile)# [no] flex umbrella dhcp-dns-option`	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)# [no] flex umbrella mode force`	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)# end`	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: 5XXXXXXABXXXXXFXXXXXXXXXXDXXXXXXXXXXXXABXX
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 device registration details, use the following command:

```
Device# show umbrella deviceid
Device registration details
Param-Map Name                  Status          Device-id
global                          200 SUCCESS     010aa4eXXXXXXX8d
vj-1                            200 SUCCESS     01XXXXXXXf4541e1
GUEST                           200 SUCCESS     010a4f6XXXXXXX42
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         : 010aa4eXXXXXXX8d
      Description       : Device Id recieved successfully
      WAN interface     : None
 2.vj-1
      Tag               : vj-1
      Device-id         : 01XXXXXXXf4541e1
      Description       : Device Id recieved successfully
      WAN interface     : None
```

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 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#
```