# Cisco Umbrella WLAN


- Cisco Umbrella WLAN, on page 1
- Register Embedded Wireless Controller to Cisco Umbrella account , on page 2
- Restrictions for Umbrella WLAN, on page 3
- Configure Cisco Umbrella WLAN, on page 4
- Verify the Cisco Umbrella configuration, on page 11


# Cisco Umbrella WLAN

A Cisco Umbrella WLAN is a cloud-based security solution for wireless networks that

- provides DNS-level protection by detecting and blocking both known and emergent threats
- enables granular policy configuration per user group, network, device, and IP address, and
- offers real-time security dashboards and scheduled reporting.

### Additional features and policy configuration

- Allows policy configuration at a single point for each user group and supports local policy, AP group, and WLAN priority order.
- Publishes visual, real-time activity dashboards with aggregated reports.
- Supports up to 60 content categories and lets administrators add custom allowed and blocked list entries.
- Enables scheduled email reporting.

### Policy priority order

When you configure multiple policies in Cisco Umbrella WLAN, you enforce them in order of priority:

1. **Local policy** – This is the most specific policy and is applied first. Local policies override any broader group or network rules for individual devices or users.
2. **AP group policy** – If no local policy exists, the rules defined for the AP group are applied next.
3. **WLAN policy** – If there are no local or AP group policies, the general policy for the entire wireless network (WLAN) is applied.

To summarize, the most specific rules take priority over broader ones. If a local rule exists, it is enforced first. If not, the system checks for an AP group rule. If neither exists, the general WLAN policy is used.

# Register Embedded Wireless Controller to Cisco Umbrella account

This section describes the process followed to register the Embedded Wireless Controller to the Cisco Umbrella account. Here are the prerequisites:

- Have an account with Cisco Umbrella.
- Have an API token from Cisco Umbrella.

### Summary

Registering Embedded Wireless Controller to Cisco Umbrella accounts enables centralized DNS security management and policy enforcement for wireless devices. This integration requires account access, API tokens, and specific parameter mappings.

The key components involved in the process are:

- embedded wireless controllercontroller: Wireless network devices that will be registered with Cisco Umbrella for DNS query management.
- **Cisco Umbrella account**: The cloud-based platform providing DNS security services and device identity management.
- **API token**: A credential generated from Cisco Umbrella and used for authenticating and mapping devices during registration.
- **Umbrella parameter map**: Controller-side configuration map that links API tokens to device profiles.
- **DHCP servers and DNS servers**: Network services facilitating IP assignment and DNS query redirection for WLAN clients.

This process involves obtaining an API token, applying it to the controller, and verifying device registration in Cisco Umbrella.

### Workflow

These stages describe the registration of the Embedded Wireless Controller to Cisco Umbrella Account.

1. **Obtain prerequisites:** Ensure you have a Cisco Umbrella account and generate an API token from the Umbrella dashboard.
2. **Configure umbrella parameter map on the controller:** Create an Umbrella parameter map on the controller embedded wireless controller, assigning the API token.
3. **Register the device:** Register the controller to the Cisco Umbrella server using the configured parameter map. Cisco Umbrella responds with a device ID, mapped in a one-to-one relationship with the parameter map name.
4. **Verify device registration:** In the Cisco Umbrella dashboard, confirm that the controller embedded wireless controller appears under Device Name with its identity information.

5. **Apply the API token configuration:** Register the Cisco Umbrella API token on the network through controller configuration.
6. **Redirect DNS queries:** Once registration and parameter mapping are complete, DNS queries from WLAN clients not matching local RegEx domain settings are redirected to the Umbrella DNS resolver, with encryption applied based on DNScrypt options in the parameter map.
7. **Apply profiles and handle mobility:** Apply wireless Cisco Umbrella profiles to WLAN or AP groups if device registration is successful. For Layer 3 mobility, always apply Cisco Umbrella on the anchor controller.
8. **Distribute Umbrella server IPs through DHCP:** When two DNS servers are configured under DHCP, two Cisco Umbrella server IPs are sent to clients using DHCP option 6; only one IP is sent if a single DNS server is configured.

**Result**

Embedded Wireless Controller are successfully registered with Cisco Umbrella accounts. Wireless entities can be managed with Umbrella profiles, and DNS queries are securely redirected according to policy. Device identity, profile application, and DNS traffic handling are centrally managed.

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

# Restrictions for Umbrella WLAN

- Wireless Cisco Umbrella profiles can be applied only to WLAN or AP groups after successful device registration.
- In Layer 3 mobility environments, Cisco Umbrella must be enabled on the anchor .
- DHCP configuration determines how many Cisco Umbrella DNS server IPs are distributed to clients.

## DNS dependency restrictions

Cisco Umbrella WLAN protections are only effective when client devices perform DNS queries through the network. If DNS is bypassed, Umbrella protection does not apply.

- If an application or host connects directly using an IP address, bypassing DNS resolution, Umbrella WLAN protections are not enforced.

These restrictions apply to all deployments of Cisco Umbrella WLAN where DNS traffic is required for policy enforcement.

Umbrella WLAN leverages DNS queries to monitor and enforce security policies. Direct IP or proxy-based connections circumvent DNS-based protections.

Clients that bypass DNS, or use web proxies that resolve server addresses without DNS queries, may not be protected by Umbrella WLAN security policies.

Ensure all client devices perform DNS queries through the WLAN and avoid proxy configurations that bypass DNS to maintain optimal Umbrella protection.

# Configure Cisco Umbrella WLAN

To configure Cisco Umbrella on the Embedded Wireless Controller, you need to meet these prerequisites:

- Obtain the API token from the Cisco Umbrella dashboard.
- You must have the root certificate to establish an HTTPS connection with the Cisco Umbrella registration server: api.opendns.com. Import the root certificate from digicert.com to the Embedded Wireless Controller using the command **crypto pki trustpool import terminal** .

## Import CA certificate to the trust pool

**Before you begin**

Ensure you have the root certificate and an established HTTPS connection with the Cisco Umbrella registration server.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Perform either of these steps:

- Import the root certificate directly from the Cisco website. The Trustpool bundle contains the root certificate of *digicert.com* together with other CA certificates.

```
Device(config)# crypto pki trustpool import url
http://www.cisco.com/security/pki/trs/ios.p7b
```

- Import the root certificate by executing the **import terminal** command.

```
Device(config)# crypto pki trustpool import terminal
```

- Import the root certificate by pasting the CA certificate from the digicert.com. Enter the PEM-formatted CA certificate from these location. See the Related Information section to download the CA certificate.

```
-----BEGIN CERTIFICATE-----
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
```

```
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
SaZMkE4f97Q=
-----END CERTIFICATE-----
```

**Step 3** (Optional) Import the root certificate by entering the quit command.

**Example:**

```
Device(config)# quit
```

**Note**
You will receive a message after the certificate has been imported.

# Create a local domain RegEx parameter map

To create a regex parameter map for matching specific domain patterns.

This procedure is used in network configurations where domain name filtering is required based on regex patterns.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Create a regex parameter map.

**Example:**

```
Device(config)# parameter-map type regex parameter-map-name
```

**Step 3** Configure the regex pattern to match.

**Example:**

```
Device(config-profile)# pattern regex-pattern
```

**Example:**

```
Device(config-profile)# pattern www.google.com
```

**Note**
These 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** Return to privileged EXEC mode.

**Example:**

```
Device(config-profile)# end
```

The local domain RegEx parameter map is created and configured successfully.

# Configure parameter map name in WLAN (GUI)

Assign a parameter map to a WLAN, enabling custom policy enforcement for DNS traffic and access restrictions.

This procedure ensures that your WLAN profile enforces the intended policies for DNS and wireless client access using Cisco Umbrella integration.

**Before you begin**

Confirm that required parameter maps are defined

**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.

The WLAN profile is updated with the selected parameter map, and the associated DNS and access policies are enforced for connected wireless clients.

# Configure the Umbrella parameter map

To configure the Umbrella Parameter Map for network security and management.

This configuration is used to manage and secure network traffic through the Umbrella service, which provides DNS-layer security.

**Before you begin**

Ensure you have the necessary permissions and access to the device for configuration.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Create an Umbrella global or customized parameter map.

**Example:**

```
Device(config)# parameter-map type umbrella global parameter-map-name
```

**Example:**

```
Device(config)# parameter-map type umbrella global
```

Creates an umbrella global parameter map.

**Step 3** Configure an Umbrella token.

**Example:**

```
Device(config-profile)# token token-value
```

**Example:**

```
Device(config-profile)# token 5XXXXXXXXCXXXXXXXAXXXXXXXFXXXXCXXXXXXXX
```

**Step 4** Configure local domain RegEx parameter maps.

**Example:**

```
Device(config-profile)# local-domain regex-parameter-map-name
```

**Example:**

```
Device(config-profile)# local-domain dns_wl
```

Configures local domain RegEx parameter map.

**Step 5** Configure the Anycast address.

**Example:**

```
Device(config-profile)# resolver IPv6 10:1:1:1::10
```

The default address is applied when there is no specific address configured.

**Step 6** Return to privileged EXEC mode.

**Example:**

```
Device(config-profile)# end
```

The Umbrella parameter map is now configured and ready for use in managing network security.

## Enable or disable DNScrypt using GUI

Use this task when you need to control whether DNS queries are encrypted, or to specify exceptions and update your Umbrella settings.

Configure DNScrypt to enhance or relax DNS traffic encryption as needed to adapt your organization's security requirements.

**Before you begin**

- Obtain the registration token from Cisco Umbrella.
- Determine domains to whitelist if needed.

**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** .

The DNScrypt setting is updated. DNS packets is now be encrypted or unencrypted based on your selection, and any specified domains will be excluded from filtering.

## Enable or disable DNScrypt

To configure DNScrypt settings for enhanced DNS security.

This procedure is used to enable or disable DNScrypt, which provides encryption for DNS queries, enhancing privacy and security.

**Before you begin**

Ensure you have access to the device's global configuration mode.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Create an umbrella global parameter map.

**Example:**

```
Device(config)# parameter-map type umbrella global
```

**Step 3** Enable DNScrypt

**Example:**

```
Device(config-profile)# no 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** (Optional) Return to privileged EXEC mode.

**Example:**

```
Device(config-profile)# end
```

The DNScrypt settings have been successfully configured.

## Configure timeout for UDP sessions.

To set a timeout value for UDP sessions to manage session persistence and resource allocation.

This configuration is useful in environments where UDP sessions need to be managed effectively to prevent resource exhaustion.

**Before you begin**

Ensure you have access to the device and the necessary privileges to enter global configuration mode.

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Create an umbrella global parameter map.

**Example:**

```
Device(config)# parameter-map type umbrella global
```

**Step 3** Configure timeout value for UDP sessions.

**Example:**

```
Device(config-profile)# udp-timeout timeout_value
```

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** (Optional) Return to privileged EXEC mode.

**Example:**

```
Device(config-profile)# end
```

The UDP session timeout is configured successfully, allowing for better management of UDP resources.

# 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**.

# Configure parameter map name in WLAN

Configure a parameter map name to enable Cisco Umbrella OpenDNS integration on a WLAN.

This procedure is used when secure DNS filtering and policy enforcement are required on WLANs. The parameter map defines the Umbrella integration settings for the profile.

**Before you begin**

Ensure that the WLAN profile has been created and the network device is running the appropriate software version for Umbrella OpenDNS support.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

Enters global configuration mode.

**Step 2** Create a policy profile for the WLAN.

**Example:**

```
Device(config)# wireless profile policy policy-profile-name
```

The *default-policy-profile* is the profile name of the policy profile.

**Step 3** Configure the Umbrella parameter map in the policy profile.

**Example:**

```
Device(config-wireless-policy)# umbrella-param-map umbrella-name
```

Configures the Cisco Umbrella OpenDNS feature for the WLAN using the specified parameter map.

The *global* parameter map contains policy and key settings for Umbrella integration.

**Step 4** Exit wireless policy configuration and return to privileged EXEC mode.

**Example:**

```
Device(config-wireless-policy)# end
```

Alternatively, you can press Ctrl-Z.

The Umbrella parameter map name is now configured for the WLAN. DNS protection policies will be applied to wireless clients associating with this profile.

# Verify the Cisco Umbrella configuration

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

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

To view the regex parameter map details, use the 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#
```