



## Cisco Umbrella WLAN

- [Cisco Umbrella WLAN について \(1 ページ\)](#)
- [Cisco Umbrella アカウントへの 組み込みワイヤレスコントローラの登録 \(2 ページ\)](#)
- [Cisco Umbrella WLAN の設定 \(3 ページ\)](#)
- [Cisco Umbrella 設定の確認 \(9 ページ\)](#)

### Cisco Umbrella WLAN について

Cisco Umbrella WLAN は、既知と緊急の両方の脅威を自動検出する、クラウド提供のネットワークセキュリティサービスをドメインネームシステム (DNS) レベルで提供します。

この機能により、マルウェア、ボットネットワーク、およびフィッシングが実際に悪意のある脅威になる前に、それらをホストしているサイトをブロックできます。

Cisco Umbrella WLAN を使用すると、次のことが可能です。

- シングルポイントでのユーザーグループごとのポリシーの設定。
- ネットワーク、グループ、ユーザー、デバイス、または IP アドレスごとのポリシーの設定。

ポリシーの優先順位は次のとおりです。

1. ローカルポリシー
2. AP グループ
3. WLAN

- リアルタイムのビジュアルセキュリティアクティビティダッシュボードと集約レポート。
- スケジュール設定と電子メールによるレポートの送信。
- 最大 60 のコンテンツカテゴリのサポートとカスタム許可リストエントリとブロックリストエントリを追加するためのプロビジョニング。

この機能は、次のシナリオでは機能しません。

- アプリケーションまたはホストが、DNS を使用する代わりに IP アドレスを直接使用してドメイン名をクエリしている場合。
- クライアントが Web プロキシに接続されていて、サーバー アドレスを解決するための DNS クエリを送信しない場合。

## Cisco Umbrella アカウントへの組み込みワイヤレスコントローラの登録

### はじめる前に

- Cisco Umbrella のアカウントが必要です。
- Cisco Umbrella からの API トークンが必要です。

組み込みワイヤレスコントローラは、Umbrella パラメータマップを使用して Cisco Umbrella サーバーに登録されます。Umbrella パラメータ マップごとに API トークンが必要です。Cisco Umbrella は、組み込みワイヤレスコントローラのデバイス ID を使用して応答します。デバイス ID は、Umbrella パラメータ マップ名と 1 対 1 でマッピングされています。

### Cisco Umbrella ダッシュボードを使用した組み込みワイヤレスコントローラの API トークンの取得

Cisco Umbrella ダッシュボードで、[Device Name] に組み込みワイヤレスコントローラとその ID が表示されていることを確認します。

### 組み込みワイヤレスコントローラでの API トークンの適用

ネットワークに Cisco Umbrella の API トークンを登録します。

### DNS クエリと応答

WLAN にデバイスを登録して Umbrella パラメータ マップを設定すると、WLAN に接続しているクライアントからの DNS クエリが Umbrella DNS リゾルバにリダイレクトされるようになります。



(注) これは、ローカル ドメインの正規表現パラメータ マップに設定されていないすべてのドメインに適用されます。

クエリと応答は、Umbrella パラメータ マップの DNSCrypt オプションに基づいて暗号化されます。

Cisco Umbrella の設定の詳細については、『[Integration for ISR 4K and ISR 1100 – Security Configuration Guide](#)』を参照してください。

### 制限事項と考慮事項

この機能の制限事項と考慮事項は次のとおりです。

- デバイス登録が成功すると、ワイヤレス Cisco Umbrella プロファイルを WLAN や AP グループなどのワイヤレス エンティティに適用できます。
- L3 モビリティの場合、Cisco Umbrella は常にアンカー 組み込みワイヤレスコントローラで適用する必要があります。
- DHCP 配下に 2 つの DNS サーバーが設定されている場合は、2 つの Cisco Umbrella サーバー IP が DHCP オプション 6 からクライアントに送信されます。DHCP 配下に 1 つの DNS サーバーだけが存在する場合は、DHCP オプション 6 の一部として 1 つの Cisco Umbrella サーバー IP のみが送信されます。

## Cisco Umbrella WLAN の設定

組み込みワイヤレスコントローラで Cisco Umbrella を設定するには、次の作業を行います。

- Cisco Umbrella ダッシュボードから API トークンを取得する必要があります。
- Cisco Umbrella 登録サーバー ([api.opendns.com](https://api.opendns.com)) との HTTPS 接続を確立するためには、ルート証明書が必要です。 **crypto pki trustpool import terminal** コマンドを使用して、**digicert.com** から 組み込みワイヤレスコントローラにルート証明書をインポートする必要があります。

## トラスト プールへの CA 証明書のインポート

### 始める前に

ここでは、ルート証明書を取得して Cisco Umbrella 登録サーバとの HTTPS 接続を確立する方法について詳しく説明します。

### 手順

|        | コマンドまたはアクション   | 目的                           |
|--------|--|------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br>Device# configure terminal   | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | 次のいずれかの作業を実行します。 <ul style="list-style-type: none"> <li>• <b>crypto pki trustpool import url url</b><br/>               Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b</li> </ul> |                              |

|        | コマンドまたはアクション  | 目的  |
|--------|---|---|
|        | <p>シスコの Web サイトからルート証明書を直接インポートします。</p> <p>(注) Trustpool バンドルには、他の CA 証明書とともに <i>digicert.com</i> のルート証明書が含まれています。</p> <ul style="list-style-type: none"> <li>• <b>crypto pki trustpool import terminal</b></li> </ul> <pre>Device(config)# crypto pki trustpool import terminal</pre> <p>import terminal コマンドを実行して、ルート証明書をインポートします。</p> <ul style="list-style-type: none"> <li>• 次の場所で入手できる PEM 形式の CA 証明書を入力します。「関連情報」の項を参照して、CA 証明書をダウンロードしてください。</li> </ul> <pre>-----BEGIN CERTIFICATE----- MIIEjDCCAQEgCjImvK9K1A/3ARjic90A8AEMQDQ0G EwEVBGALEMKCrMcQ9fjRkVWQESRuzZrAnLQZ9MA HjYQESdcaq2ydh69Vw9edHQvav0A9YQDMREv0MAY MUNLMBCAENBZAMTRVWQESRuzZrAnLQZ9MAHjY ZIXOIRBjS0Ej0BjZLW4pQEMIEjRjic90A8AEMQ CQAENLz0wNPNc3ZUFRNtP8K8K8K8K8K8K8K8K8 R0j9%lHlQNE6A7B15HjL8q5YQESRuzZrAnLQZ9 V0U99ilab6QVWVFALE/hjLnInk8K8K8K8K8K8K8 m4H9jRjLhE9/09N0CE65y704hyR3Uj8K8K8K8 R6/8hRy08vZheanc92QDIT7Hk79UJAg80EjCao Hdnop94eeQy55Vh0MBAAL0QMAFA8DW0jZC4h Alde9/0A8jy8jN8E7yR8E8QYK6E8HAAEgDRTA E8E/8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E InNtE8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8 Y8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8 RGrANcRk6Y98290Ry3BMAAL0QMAFA8DW0jZC4 E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8 35H8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8 u2E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8 58E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8 Y8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8E8 SaZMkE4f97Q= -----END CERTIFICATE-----</pre> <p><b>digicert.com</b> から CA 証明書を貼り付けて、ルート証明書をインポートします。</p> |   |
| ステップ 3 | <p><b>quit</b></p> <p>例 :</p>   | <p><b>quit</b> コマンドを入力して、ルート証明書をインポートします。</p> |

|  | コマンドまたはアクション                | 目的                              |
|--|-----------------------------|---------------------------------|
|  | Device(config)# <b>quit</b> | (注) 証明書のインポートが完了すると、メッセージが届きます。 |

## ローカルドメインの正規表現パラメータマップの作成

### 手順

|        | コマンドまたはアクション   | 目的   |
|--------|--|--|
| ステップ 1 | <b>configure terminal</b><br>例：<br>Device# configure terminal  | グローバル設定モードを開始します。  |
| ステップ 2 | <b>parameter-map type regex</b><br><i>parameter-map-name</i><br>例：<br>Device(config)# <b>parameter-map type</b><br><b>regex dns_wl</b> | 正規表現パラメータマップを作成します。  |
| ステップ 3 | <b>pattern regex-pattern</b><br>例：<br>Device(config-profile)# pattern<br>www.google.com  | 照合する正規表現パターンを設定します。<br><br>(注) 次のパターンがサポートされています。<br><ul style="list-style-type: none"><li>• .* で始まる。<br/>例： <b>.*facebook.com</b></li><li>• .* で始まり、* で終わる。<br/>例： <b>.*google*</b></li><li>• * で始まる。例：<br/><b>*facebook.com</b></li><li>• * で始まり、* で終わる。<br/>例： <b>*google*</b></li><li>• * で終わる。例：<br/><b>www.facebook*</b></li><li>• 特殊文字なし。例：<br/><b>www.facebook.com</b></li></ul> |
| ステップ 4 | <b>end</b><br>例：   | 特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコ  |

|  | コマンドまたはアクション                | 目的                     |
|--|-----------------------------|------------------------|
|  | Device(config-profile)# end | ンフィギュレーション モードを終了できます。 |

## WLAN でのパラメータ マップ名の設定 (GUI)

### 手順

- 
- ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] を選択します。
- ステップ 2 [Policy Profile Name] をクリックします。[Edit Policy Profile] ウィンドウが表示されます。
- ステップ 3 [Advanced] タブを選択します。
- ステップ 4 [Umbrella] 設定で、[Umbrella Parameter Map] ドロップダウンリストからパラメータマップを選択します。
- ステップ 5 [Flex DHCP Option for DNS] および [DNS Traffic Redirect] トグルボタンを有効または無効にします。
- ステップ 6 [Update & Apply to Device] をクリックします。
- 

## Umbrella パラメータ マップの設定

### 手順

|        | コマンドまたはアクション  | 目的                                   |
|--------|---|--------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例：<br>Device# configure terminal   | グローバル コンフィギュレーション モードを開始します。         |
| ステップ 2 | <b>parameter-map type umbrella global</b><br>例：<br>Device(config)# parameter-map type umbrella global               | Cisco Umbrella グローバルパラメータ マップを作成します。 |
| ステップ 3 | <b>token token-value</b><br>例：<br>Device(config-profile)# token<br>5XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXFXXXXXXXXXXXXXXXX | Umbrella トークンを設定します。                 |
| ステップ 4 | <b>local-domain regex-parameter-map-name</b><br>例：  | ローカル ドメインの正規表現パラメータ マップを設定します。       |

|        | コマンドまたはアクション   | 目的  |
|--------|--|---|
|        | Device(config-profile)# <b>local-domain dns_wl</b>   |   |
| ステップ 5 | <b>resolver {IPv4 X.X.X.X IPv6 X:X:X:X::X}</b><br>例 :<br>Device(config-profile)# <b>resolver IPv6 10:1:1:1::10</b> | エニーキャストアドレスを設定します。特定のアドレスが設定されていない場合はデフォルトのアドレスが適用されます。 |
| ステップ 6 | <b>end</b><br>例 :<br>Device(config-profile)# <b>end</b>  | 特権 EXEC モードに戻ります。                                       |

## DNSCrypt の有効化または無効化 (GUI)

### 手順

- ステップ 1 [Configuration] > [Security] > [Threat Defence] > [Umbrella] を選択します。
- ステップ 2 Cisco Umbrella から受け取った [Registration Token] を入力します。または [Click here to get your Token] をクリックして、Cisco Umbrella からトークンを取得することもできます。
- ステップ 3 フィルタリングから除外する [Whitelist Domains] を入力します。
- ステップ 4 [Enable DNS Packets Encryption] チェックボックスをオンまたはオフにして、DNS パケットを暗号化または復号します。
- ステップ 5 [Apply] をクリックします。

## DNSCrypt の有効化または無効化

### 手順

|        | コマンドまたはアクション  | 目的                             |
|--------|---|--------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br>Device# <b>configure terminal</b>   | グローバル コンフィギュレーション モードを開始します。   |
| ステップ 2 | <b>parameter-map type umbrella global</b><br>例 :<br>Device(config)# <b>parameter-map type umbrella global</b> | Umbrella グローバルパラメータ マップを作成します。 |
| ステップ 3 | <b>[no] dnsencrypt</b><br>例 :   | DNSCrypt を有効または無効にします。         |

|        | コマンドまたはアクション   | 目的                           |
|--------|--|------------------------------|
|        | Device(config-profile)# <b>no dnscrypt</b>             | デフォルトでは、DNSCrypt オプションは有効です。 |
| ステップ 4 | <b>end</b><br>例：<br>Device(config-profile)# <b>end</b> | 特権 EXEC モードに戻ります。            |

## UDP セッションのタイムアウトの設定

### 手順

|        | コマンドまたはアクション   | 目的  |
|--------|--|---|
| ステップ 1 | <b>configure terminal</b><br>例：<br>Device# configure terminal  | グローバル コンフィギュレーション モードを開始します。  |
| ステップ 2 | <b>parameter-map type umbrella global</b><br>例：<br>Device(config)# <b>parameter-map type umbrella global</b> | Umbrella グローバル パラメータ マップを作成します。   |
| ステップ 3 | <b>udp-timeout timeout_value</b><br>例：<br>Device(config-profile)# <b>udp-timeout 2</b>                       | UDP セッションのタイムアウト値を設定します。<br><i>timeout_value</i> の範囲は 1 ～ 30 秒です。<br>(注) <b>public-key</b> および <b>resolver</b> パラメータマップ オプションには、デフォルト値が自動的に入力されます。したがって、変更する必要はありません。 |
| ステップ 4 | <b>end</b><br>例：<br>Device(config-profile)# <b>end</b>   | 特権 EXEC モードに戻ります。   |

## WLAN でのパラメータ マップ名の設定 (GUI)

### 手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] を選択します。



- ステップ 2 [Policy Profile Name] をクリックします。[Edit Policy Profile] ウィンドウが表示されます。
- ステップ 3 [Advanced] タブを選択します。
- ステップ 4 [Umbrella] 設定で、[Umbrella Parameter Map] ドロップダウンリストからパラメータマップを選択します。
- ステップ 5 [Flex DHCP Option for DNS] および [DNS Traffic Redirect] トグルボタンを有効または無効にします。
- ステップ 6 [Update & Apply to Device] をクリックします。

## WLAN でのパラメータ マップ名の設定

### 手順

|        | コマンドまたはアクション   | 目的  |
|--------|--|---|
| ステップ 1 | <b>configure terminal</b><br>例：<br>Device# <code>configure terminal</code>   | グローバル コンフィギュレーション モードを開始します。  |
| ステップ 2 | <b>wireless profile policy <i>profile-name</i></b><br>例：<br>Device (config)# <b>wireless profile policy <i>profile-name</i></b><br><b>default-policy-profile</b> | WLAN のポリシー プロファイルを作成します。<br><i>profile-name</i> はポリシー プロファイルのプロファイル名です。 |
| ステップ 3 | <b>umbrella-param-map <i>umbrella-name</i></b><br>例：<br>Device (config-wireless-policy)#<br><b>umbrella-param-map global</b>                                     | WLAN の Umbrella OpenDNS 機能を設定します。                                       |
| ステップ 4 | <b>end</b><br>例：<br>Device (config-wireless-policy)# <b>end</b>  | 特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。        |

## Cisco Umbrella 設定の確認

Umbrella 設定の詳細を表示するには、次のコマンドを使用します。

```
Device# show umbrella config
Umbrella Configuration
=====
Token: 5XXXXXXXXABXXXXFXXXXXXXXXXXXXXXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxxx
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

```

Umbrella DNSCrypt の詳細を表示するには、次のコマンドを使用します。

```

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

```

Umbrella グローバル パラメータ マップの詳細を表示するには、次のコマンドを使用します。

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

正規表現パラメータ マップの詳細を表示するには、次のコマンドを使用します。

```
Device# show parameter-map type regex <parameter-map-name>
```

AP の Umbrella の詳細を表示するには、次のコマンドを使用します。

```

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#

```