



Cisco Umbrella WLAN

- [Cisco Umbrella WLAN について \(1 ページ\)](#)
- [Cisco Umbrella アカウントへの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 \(8 ページ\)](#)

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、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ホワイトリストエントリとブラ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。

ここでは、Cisco Umbrella アカウントにコントローラを登録するプロセスについて説明します。コントローラは、Umbrella パラメータ マップを使用して Cisco Umbrella サーバに登録します。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、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。

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 コントローラで適用する必要があります。

Cisco Umbrella WLAN の設定

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 登録サーバとの HTTPS 接続を確立するために、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](http://www.digicert.com) から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	configure terminal 例： 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	crypto pki trustpool import url <i>http://www.cisco.com/security/pki/trs/ios.p7b</i> 例： Device(config)# crypto pki trustpool import url <i>http://www.cisco.com/security/pki/trs/ios.p7b</i>	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。 (または) ステップ 3、4、5 を実行します。
ステップ 3	crypto pki trustpool import terminal 例： Device(config)# crypto pki trustpool import terminal	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。

	コマンドまたはアクション	目的
ステップ 4	<p>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。</p> <p>例 :</p> <pre>-----BEGIN CERTIFICATE----- MIIE1DCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kT ! . . . j6tJLp07kzQoH3j01OrHvdPJbRzeXDLz -----END CERTIFICATE-----</pre>	<p>digicert.com 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 5	<p>quit</p> <p>例 :</p> <pre>Device(config)# quit</pre>	<p>quit 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> <p>(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。</p>

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	<p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 2	<p>parameter-map type regex <i>parameter-map-name</i></p> <p>例 :</p> <pre>Device(config)# parameter-map type regex dns_wl</pre>	<p>正規表現パラメータ マップを作成します。</p>
ステップ 3	<p>pattern <i>regex-pattern</i></p> <p>例 :</p> <pre>Device(config-profile)# pattern www.google.com</pre>	<p>照合する正規表現パターンを設定します。</p>
ステップ 4	<p>end</p> <p>例 :</p>	<p>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</p>

	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] > [Security] > [Web Auth] を選択します。
- ステップ 2 [Add] ボタンをクリックします。[Create WebAuth Parameter] ダイアログボックスが表示されます。
- ステップ 3 [Parameter-map name] フィールドにパラメータ マップの名前を入力します。
- ステップ 4 [Maximum HTTP connections] フィールドに値を入力します。1 ~ 200 の範囲で値を入力する必要があります。
- ステップ 5 [Init-State Timeout(secs)] フィールドに値を入力します。60 ~ 3932100 の範囲で値を入力する必要があります。
- ステップ 6 [Type] ドロップダウンリストから必要なオプションを選択します。
- ステップ 7 [Apply to Device] ボタンをクリックします。

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	configure terminal 例 : 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	parameter-map type umbrella global 例 : Device(config)# parameter-map type umbrella global	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	token token-value 例 : Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166	Umbrella トークンを設定します。

	コマンドまたはアクション	目的
ステップ 4	local-domain regex-parameter-map-name 例： Device(config-profile)# local-domain dns_w1	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。
ステップ 5	end 例： Device(config-profile)# end	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。

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	configure terminal 例： 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	parameter-map type umbrella global 例： Device(config)# parameter-map type umbrella global	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	token token-value 例： Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166	Umbrella トークンを設定します。
ステップ 4	local-domain regex-parameter-map-name 例： Device(config-profile)# local-domain dns_w1	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。
ステップ 5	[no] dnscrypt 例： Device(config-profile)# no dnscrypt	DNSCrypt を有効または無効にします。デフォルトでは、DNSCrypt オプションは有効です。
ステップ 6	end 例： Device(config-profile)# end	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。

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	configure terminal 例： 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	parameter-map type umbrella global 例： Device(config)# <code>parameter-map type umbrella global</code>	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	token token-value 例： Device(config-profile)# <code>token 57CC80106C087FB1B2A7BAB4F2F4373C00247166</code>	Umbrella トークンを設定します。
ステップ 4	local-domain regex-parameter-map-name 例： Device(config-profile)# <code>local-domain dns_w1</code>	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。
ステップ 5	udp-timeout timeout_value 例： Device(config-profile)# <code>udp-timeout 2</code>	UDP セッションのタイムアウト値を設定します。 <i>timeout_value</i> の範囲は 1 ~ 30 秒です。 (注) public-key および resolver 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 6	end 例： Device(config-profile)# <code>end</code>	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。

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	configure terminal 例： 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	wireless profile policy <i>profile-name</i> 例： Device (config)# wireless profile policy <i>profile-name</i> default-policy-profile	WLAN のポリシー プロファイルを作成します。 <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	umbrella-param-map <i>umbrella-name</i> 例： Device (config-wireless-policy)# umbrella-param-map global	WLAN の Umbrella OpenDNS 機能を設定します。
ステップ 4	end 例： Device (config-wireless-policy)# end	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
```

デバイス登録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 <deviceid>
```

Umbrella デバイス ID の詳細な説明を表示するには、次のコマンドを使用します。

```
Device# show umbrella <deviceid> detailed
```

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
```

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>
```

Umbrella の統計情報を表示するには、次のコマンドを使用します。


```
Device# show platform hardware chassis active qfp feature umbrella datapath stats
```

