# WLAN ごとのワイヤレス設定



# DTIM 周期

## DTIM 期間について

802.11 ネットワークでは、Lightweight アクセス ポイントは、Delivery Traffic Indication Map (DTIM) と一致するビーコンを定期的に送信します。アクセス ポイントでビーコンがブロードキャストされると、DTIM 期間で設定した値に基づいて、バッファされたブロードキャスト フレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャスト データやマルチキャストデータが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 5 回送信します。これらの設定はいずれも、ブロードキャスト フレームおよびマルチキャスト フレームの頻度を想定する、Voice over IP（VoIP）を含むアプリケーションに適しています。

ただし、DTIM 値は、802.11 のすべてのクライアントで省電力モードがイネーブルである場合、255 まで設定できます（255 回のビーコンごとにブロードキャスト フレームおよびマルチキャスト フレームを送信します）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100 ms、DTIM 値を 100 に設定すると、アクセス ポイントは、バッファされたブロードキャスト フレームお

よびマルチキャスト フレームを 10 秒ごとに 1 回送信します。このレートにより省電力クライアントで、ブロードキャストとマルチキャストをリッスンし、ウェイク アップするまでのスリープ状態が長くなり、バッテリ寿命を長くできます。

（注） ビーコン期間は、コントローラ でミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位（TU）（1 TU = 1.024 ミリ秒）に、内部的に変換されます。Cisco の 802.11n アクセス ポイントでは、この値は直近の 17 TU の倍数に丸められます。たとえば、100 ミリ秒に設定されたビーコン間隔は 104 ミリ秒の実際のビーコン間隔の結果です。

多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。このようなクライアントをサポートする 802.11 ネットワークでは、低い DTIM 値を推奨します。

特定の WLAN で 802.11 無線ネットワークの DTIM 期間を設定できます。たとえば、音声 WLAN とデータ WLAN に異なる DTIM 値を設定できます。

# DTIM period の設定（GUI）

手順

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ 2** DTIM period を設定する WLAN の ID 番号をクリックします。

**ステップ 3** [Status] チェックボックスをオフにしてこの WLAN を無効にします。

**ステップ 4** [Apply] をクリックします。

**ステップ 5** [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

**ステップ 6** [DTIM Period] で [802.11a/n/ac] テキスト ボックスと [802.11b/g/n] テキスト ボックスに 1 ～ 255 までの値を入力します。デフォルト値は1（ブロードキャストフレームおよびマルチキャストフレームはビーコンのたびに送信）です。

**ステップ 7** [Apply] をクリックします。

**ステップ 8** [General] タブを選択して、[WLANs > Edit]（[General]）ページを開きます。

**ステップ 9** [Status] チェックボックスをオンにして、この WLAN を再び有効にします。

**ステップ 10** [Save Configuration] をクリックします。

# DTIM period の設定（CLI）

手順

**ステップ 1** 次のコマンドを入力して、WLAN を無効にします。

**config wlan disable** *wlan_id*

**ステップ 2** 次のコマンドを入力して、特定の WLAN の 802.11 無線ネットワークの DTIM period を設定します。

**config wlan dtim {802.11a |802.11b** *dtim wlan_id*

*dtim* の値は、1 ～ 255（両端の値を含む）です。デフォルト値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）です。

**ステップ 3** 次のコマンドを入力して、WLAN を再び有効にします。

**config wlan enable** *wlan_id*

**ステップ 4** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 5** 次のコマンドを入力して、DTIM period を確認します。

**show wlan** *wlan_id*

# Cisco Client Extensions

## Cisco Client Extensions を実装するための前提条件

- ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。これによって、controllersとそのアクセス ポイントは、CCX をサポートするサードパーティ製クライアント デバイスと無線で通信できます。CCX サポートは、コントローラ 上の各 WLAN に対して自動的に有効になり、無効にすることはできません。ただし、Aironet Information Element（IE）を設定できます。
- Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの数などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、コントローラ は、Aironet IEs 0x85 および 0x95（コントローラ の管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション応答に格納して送信します。

# Cisco Client Extensions について

Cisco Client Extensions（CCX）ソフトウェアは、サードパーティ製クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードパーティ製クライアント デバイスは、シスコ製のアクセス ポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、高速ローミング、電源管理などの、他のクライアントデバイスがサポートしていないシスコの機能もサポートできるようになります。

# Cisco Client Extensions の設定に関する制約事項

- CCX は、Cisco OEAP 600 アクセス ポイントではサポートされず、CCX に関連する要素もすべてがサポートされるわけではありません。
- Cisco OEAP 600 では、Cisco Aeronet IE をサポートしていません。
- 7.2 リリースでは、CCX Lite と呼ばれる新規バージョンの CCX を使用できます。CCX Lite の詳細については、http://www.cisco.com/c/en/us/products/wireless/compatible-extensions.html [英語] を参照してください。

# CCX Aironet IE の設定（GUI）

**手順**

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ 2** 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

**ステップ 3** [Advanced] タブを選択して、[WLANs > Edit]（[Advanced] タブ）ページを開きます。

**ステップ 4** この WLAN で Aironet IE のサポートを有効にする場合は、[Aironet IE] チェックボックスをオンにします。有効にしない場合には、このチェックボックスをオフにします。デフォルト値が有効（オン）になっています。

**ステップ 5** [Apply] をクリックして、変更を確定します。

**ステップ 6** [Save Configuration] をクリックして、変更を保存します。

# クライアントの CCX バージョンの表示（GUI）

クライアント デバイスは、アソシエーション要求パケットに CCX バージョンを格納してアクセス ポイントに送信します。コントローラは、クライアントの CCX バージョンをデータベースに格納し、これを使用してこのクライアントの機能を制限します。たとえば、クライアントが CCX バージョン 2 をサポートしている場合、コントローラは、CCX バージョン 4 の機能を使用することをクライアントに許可しません。

手順

ステップ 1 [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。

ステップ 2 目的のクライアント デバイスの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。

[CCX Version] テキスト ボックスに、このクライアント デバイスでサポートされる CCX バージョンが表示されます。クライアントで CCX がサポートされていない場合は、*Not Supported* が表示されます。

ステップ 3 前の画面に戻るには、[Back] をクリックします。

ステップ 4 他のクライアント デバイスでサポートされる CCX バージョンを表示するには、この手順を繰り返します。

## CCX Aironet IE の設定（CLI）

CCX Aironet IE を設定するには、次のコマンドを使用します。

**config wlan ccx aironet-ie** {**enable** | **disable**} *wlan_id*

デフォルト値はイネーブルです。

## クライアントの CCX バージョンの表示（CLI）

コントローラの CLI を使用して、特定のクライアント デバイスでサポートされる CCX バージョンを表示するには、次のコマンドを入力します。

**show client detail** *client_mac*

# クライアント プロファイル

## クライアント プロファイルについて

クライアントが WLAN にアソシエートしようとする場合、プロセスで受信した情報からクライアントタイプを決定することができます。コントローラは情報のコレクタとして機能し、必要なデータとともに最適な形式で ISE を送信します。ローカル クライアント プロファイリング（DHCP と HTTP）は WLAN レベルで有効になります。WLAN 上のクライアントはプロファイリングが有効になると、ただちにプロファイリングされます。

ワイヤレス LAN コントローラを、以下のいくつかの機能で強化しました。

- WLC は HTTP や DHCP などのプロトコルに基づいてデバイスをプロファイリングし、ネットワーク上のエンド デバイスを識別します。

- また、デバイスベースのポリシーを設定して、ユーザまたはデバイスのエンドポイント単位で適用することもできます。また、デバイス単位で適用できるポリシーも設定できます。
- WLC は、ユーザ単位またはデバイス エンド ポイント単位の統計情報と、デバイスごとに適用可能なポリシーを表示します。

プロファイリングは、以下の項目に基づいて実行できます。

- ユーザ タイプまたはユーザが所属するユーザ グループを定義したロール。
- Windows マシン、スマート フォン、iPad、iPhone、Android などのデバイス タイプ。
- ユーザ名とパスワードのペア。
- エンドポイントが接続されている AP グループを基準としたロケーション。
- ネットワークでエンドポイントが許容された時刻。
- クライアントが接続に使用する EAP 方式を確認するための EAP タイプ。

ポリシングは、以下のプロファイルに基づいて決定します。

- VLAN
- QoS レベル
- ACL
- セッション タイムアウト値

### カスタム HTTP ポートのプロファイリングに関する情報

この機能により、WLC は HTTP ポート 80 以外のポートから接続してきたクライアントを識別し、プロファイリングを有効にすることができます。

ハイ アベイラビリティ（HA ）などのカスタム HTTP ポート プロファイリング機能は 8.2 リリースのすべての WLC プラットフォームとアクセス ポイント プラットフォームでサポートしています。プロファイリング ポート設定は WLC で設定して維持管理します。AP が現在の WLC に参加すると設定更新時に値が反映されます。

## クライアント プロファイルを設定するための前提条件

- デフォルトで、クライアントのプロファイルはすべての WLAN 上で無効です。
- クライアント プロファイルは、ローカル モードと FlexConnect モードのアクセス ポイントでサポートされます。
- コントローラでは DHCP プロキシと DHCP ブリッジ モードの両方がサポートされます。

- WLAN のアカウンティング サーバの設定は、1.1 MnR 以降のリリースを実行する ISE を指している必要があります。Cisco の ACS では、クライアントプロファイルはサポートされていません。
- 使用されている DHCP サーバのタイプは、クライアントのプロファイルに影響しません。
- DHCP_REQUEST のパケットに ISE プロファイル済みデバイス リストで見つかった文字列が含まれている場合、クライアントは自動的にプロファイルされます。
- クライアントは、Accounting request パケットで送信される MAC アドレスに基づいて識別されます。
- プロファイルが有効になると MAC アドレスだけがアカウンティング パケットの発信側ステーション ID として送信されます。
- クライアント プロファイルを有効にするには、DHCP Required フラグを有効にし、ローカル認証フラグを無効にする必要があります。
- クライアント プロファイルではコントローラの既存のプロファイルが使用されます。
- ワイヤレス クライアントのプロファイルは MAC OUI、DHCP、HTTP ユーザ エージェントに基づいて行われます。

（注） DHCP は HTTP ユーザ エージェントの DHCP プロファイルおよび Webauth に必要です。

# クライアント プロファイルの設定に関する制約事項

- プロファイルは、次のシナリオのクライアントではサポートされません。
  - スタンドアロン モードで FlexConnect モード AP とアソシエートしているクライアント。
  - ローカル スイッチングが有効な状態でローカル認証が行われる場合に FlexConnect モード AP とアソシエートしているクライアント。
  - WGB 背後の有線クライアントはプロファイリングされず、ポリシー アクションは実行されません。
- ローカル スイッチングの FlexConnect モードの AP でプロファイルが有効である場合、VLAN オーバーライドだけが AAA Override 属性としてサポートされます。
- コントローラによる DHCP プロファイル情報の解析中にクライアントが要求を送信する度に、プロファイル情報は一度だけ ISE に送信されます。
- 今回のリリースではカスタム プロファイルは作成できません。

- 今回のリリースには、ユーザがポリシーを作成しなければ CLI がチェックされる、88 の既存のポリシーが含まれます。
- ローカル プロファイリングを有効にすると、個々の WLAN では RADIUS プロファイルができなくなります。
- 一致した最初のポリシー ルールのみが適用されます。
- WLAN ごとに設定できるのは 16 ポリシーであり、グローバルにも 16 ポリシーを割り当てることができます。
- ポリシー アクションは、L2/L3 認証が完了するか、またはデバイスから HTTP トラフィックが送信され、デバイスがプロファイリングされないと実行されません。プロファイリング アクションとポリシング アクションはクライアントごとに複数回実行されます。
- AAA オーバーライドが有効で、ロール タイプ以外の AAA サーバから AAA 属性を取得すると、AAA オーバーライド属性の方に優先権があるため設定されたポリシーは適用されません。
- Apple デバイスの場合、バージョンとオペレーティング システムの情報は、iPhone 7 以降のバージョンおよび iPad 6.11 以降の世代でのみ表示されます（WLAN がオープンしていない場合）。古いデバイスのバージョンとオペレーティング システムの情報は表示されません。

## カスタム HTTP ポートのプロファイリングの設定制限

- この機能はカスタム HTTP ポートに基づいて HTTP プロファイリングをサポートしています。設定できるのは、カスタム HTTP ポート 1 つだけです。
- Cisco Aironet 1850 シリーズ AP の場合、DHCP プロファイリングが適用され、HTTP ポート プロファイリングは適用されません。
- HTTP プロファイリングは Apple デバイスには機能しません。

# クライアント プロファイルの設定（GUI）

**手順**

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ 2** [WLAN ID] をクリックします。[WLANs > Edit] ページが表示されます。

**ステップ 3** [Advanced] タブをクリックします。

**ステップ 4** RADIUS およびローカルのクライアント プロファイル領域で、次を行います。

a) HTTP に基づいてクライアントをプロファイルするには、[HTTP Profiling] チェックボックスをオンにします。

WLAN では、RADIUS モードとローカル モードの両方でクライアント プロファイルを設定できます。

**ステップ 5** [Apply] をクリックします。

**ステップ 6** [Save Configuration] をクリックします。

# クライアント プロファイルの設定（CLI）

- 次のコマンドを入力して、HTTP、DHCP、またはそれらの両方に基づいて、WLAN に対して RADIUS モードでクライアント プロファイルを有効または無効にします。

  **config wlan profiling radius** {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

  （注） DHCP と HTTP の両方に基づいたクライアント プロファイルを設定するには、**all** パラメータを使用します。

- 次のコマンドを入力して、HTTP、DHCP、またはそれらの両方に基づいて、WLAN に対してローカル モードでクライアント プロファイルを有効または無効にします。

  **config wlan profiling local** {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

- WLAN でクライアント プロファイルのステータスを表示するには、次のコマンドを入力します。

  **show wlan** *wlan-id*

- クライアントプロファイルのデバッグを有効または無効にするには、次のコマンドを入力します。

  **debug profiling** {**enable** | **disable**}

# プロファイルのカスタム HTTP ポート

## プロファイルのカスタム HTTP ポートの設定（GUI）

（注） HTTP ポート 80 は、カスタム HTTP ポート設定に関係なく、HTTP プロファイリング データを取得するために常にオープンです。

手順

**ステップ 1** **[Controller]** > **[General]** を選択して [General] ページを開きます。

**ステップ 2** [HTTP Profiling Port] フィールドにポート値を入力します

## プロファイルのカスタム HTTP ポートの設定（CLI）

**手順**

**ステップ 1** カスタム HTTP ポートを設定するには、次のコマンドを入力します。

**config network profiling http-port** ポート番号

デフォルトのポート値は 80 です。

**ステップ 2** 次のコマンドを入力して、設定された HTTP プロファル ポートおよび他のインバンド接続設定を表示します。

**show network summary**

ネットワーク設定が表示されます。

# WLAN ごとのクライアント カウント

## WLAN ごとのクライアント カウントの設定について

WLAN に接続できるクライアントの数に制限を設定できます。これは、コントローラ に接続できるクライアントの数に制限があるシナリオで役立ちます。たとえば、コントローラ が WLAN 上の最大 256 個のクライアントに対応でき、これらのクライアントが企業ユーザ（従業員）およびゲスト ユーザ間で共有される場合について考えます。特定の WLAN にアクセス可能なゲスト クライアントの数に制限を設定できます。WLAN ごとに設定できるクライアントの数は、使用しているプラットフォームによって異なります。

## WLAN ごとのクライアント カウントの設定に関する制約事項

- FlexConnect ローカル認証が使用されている場合は、WLAN ごとのクライアントの最大数の機能がサポートされません。
- WLAN ごとのクライアントの最大数機能は、接続モードのアクセス ポイントでのみサポートされます。
- WLAN が接続クライアントの最大数の制限に達しているか、AP 無線および新しいクライアントが WLAN に参加しようとしている場合、クライアントは既存のクライアントが切断されるまで WLAN に接続できません。

- ローミングクライアントは新しいクライアントと見なされます。クライアントの接続数の最大制限に到達している WLAN に対して新しいクライアントは、既存のクライアントが切断されたときにのみ接続できます。

（注） サポートされているクライアント数の詳細については、コントローラ の製品データ シートを参照してください。

# WLAN ごとのクライアント カウントの設定（GUI）

手順

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ 2** クライアント数を制限する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

**ステップ 3** [Advanced] タブをクリックします。

**ステップ 4** [Maximum Allowed Clients] テキスト ボックスに許可されるクライアントの最大数を入力します。

**ステップ 5** [Apply] をクリックします。

**ステップ 6** [Save Configuration] をクリックします。

# WLAN ごとの最大クライアント数の設定（CLI）

手順

**ステップ 1** 次のコマンドを入力して、最大クライアント数を設定する WLAN ID を確認します。

**show wlan summary**

リストから WLAN ID を取得します。

**ステップ 2** 次のコマンドを入力して、WLAN ごとの最大クライアント数を設定します。

**config wlan max-associated-clients** *max-clients wlan-id*

# WLAN ごとの各 AP 無線に対する最大クライアント数の設定（GUI）

手順

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ 2** クライアント数を制限する **WLAN** の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

**ステップ 3** [Advanced] タブで、アクセス ポイント無線あたり使用できるクライアントの最大数を [Maximum Allowed Clients Per AP Radio] テキスト ボックスに入力します。最大 200 のクライアントを設定できます。

**ステップ 4** [Apply] をクリックします。

# WLAN ごとの各 AP 無線に対する最大クライアント数の設定（CLI）

手順

**ステップ 1** 次のコマンドを入力して、無線ごとの最大クライアント数を設定する WLAN ID を確認します。

**show wlan summary**

リストから WLAN ID を取得します。

**ステップ 2** 次のコマンドを入力して、WLAN ごとの最大クライアント数を設定します。

**config wlan max-radio-clients** *client_count*

最大 200 のクライアントを設定できます。

**ステップ 3** **show 802.11a** コマンドを入力して、設定済みの関連クライアントの最大数を確認します。

# クライアントの認証解除（CLI）

コントローラを使用して、ユーザ名、IP アドレス、または MAC アドレスに基づいてクライアントを認証解除できます。同じユーザ名を持つ複数のクライアント セッションがある場合、ユーザ名に基づいてすべてのクライアント セッションを認証解除できます。異なるインターフェイスにわたって重複した IP アドレスがある場合、MAC アドレスを使用してクライアントを認証解除できます。

（注） コントローラ GUI を使用してクライアントを認証解除することはできません。

手順

- **config client deauthenticate** {*mac-addr* | *ipv4-addr* | *ipv6-addr* | *user-name*}