FlexConnect グループの設定

- FlexConnect グループについて，1 ページ
- FlexConnect グループの設定，5 ページ
- FlexConnect グループの VLAN-ACL マッピングの設定，10 ページ
- FlexConnect グループの WLAN-VLAN マッピングの設定，11 ページ

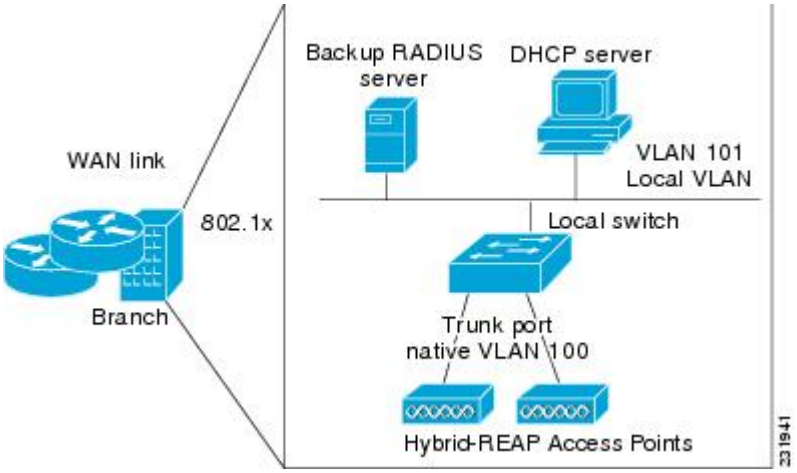
FlexConnect グループについて

お使いの FlexConnect アクセス ポイントをまとめて管理するために、FlexConnect グループを作成して、特定のアクセス ポイントをそれらのグループに割り当てることができます。

グループ内のすべての FlexConnect アクセス ポイントは、同じバックアップ RADIUS サーバ、CCKM、およびローカル認証の設定情報を共有します。 この機能は、リモート オフィス内や建物のフロア上に複数の FlexConnect アクセス ポイントがあり、それらすべてを一度に設定する場合に役立ちます。 たとえば、FlexConnect に対してバックアップ RADIUS サーバを 1 つ設定しておけば、個々のアクセス ポイント上で同じサーバを設定する必要はありません。

次の図は、ブランチ オフィスでのバックアップ RADIUS サーバを使用した FlexConnect の一般的な導入です。

図 *1*：*FlexConnect* グループの導入



FlexConnect グループおよびバックアップ RADIUS サーバ

スタンドアロン モードの FlexConnect アクセス ポイントがバックアップ RADIUS サーバに対して完全な 802.1X 認証を実行できるように、コントローラを設定することができます。 プライマリ バックアップ RADIUS サーバを設定することも、プライマリとセカンダリの両方のバックアップ RADIUS サーバを設定することもできます。 FlexConnect アクセス ポイントが 2 つのモード、スタンドアロンまたは接続の場合に、これらのサーバを使用することができます。

FlexConnect グループおよび CCKM

FlexConnect グループは、FlexConnect アクセス ポイントと共に使用する CCKM 高速ローミングで必要となります。 CCKM 高速ローミングは、ワイヤレス クライアントを別のアクセス ポイントにローミングする際に簡単かつ安全にキー交換できるように、完全な EAP 認証が実行されたマスターキーの派生キーをキャッシュすることにより実現します。 この機能により、クライアントをあるアクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。 FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM キャッシュ情報を取得する必要があります。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。 たとえば、300 台のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対して CCKM キャッシュを送信することは現実的ではありません。 少数のアクセス ポイントから成る FlexConnect を作成すれば（たとえば、同じリモート オフィス内の 4 つのアクセス ポイントのグループを作成）、クライアントはその 4 つのアクセス ポイント間でのみローミングします。CCKM キャッシュがその 4 つのアクセス ポイント間で配布されるのは、クライアントがアクセス ポイントの 1 つにアソシエートするときだけとなります。

（注） FlexConnect アクセス ポイントと FlexConnect 以外のアクセス ポイントとの間の CCKM 高速ローミングはサポートされていません。

FlexConnect グループおよび Opportunistic Key Caching

7.0.116.0 リリースから、FlexConnect グループによって、Opportunistic Key Caching（OKC）はクライアントの高速ローミングを可能にします。 OKC は、同じ FlexConnect グループにあるアクセスポイントの PMK キャッシングを使用して高速ローミングを容易にします。

この機能により、クライアントをあるアクセスポイントから別のアクセスポイントへローミングする際に、完全な認証を実行する必要がなくなります。 クライアントが 1 つの FlexConnect アクセス ポイントから別のアクセス ポイントにローミングするたびに、FlexConnect グループ アクセス ポイントはキャッシュされた PMK を使用して PMKID を計算します。

FlexConnect アクセス ポイントで PMK キャッシュ エントリを参照するには、**show capwap reap pmk** コマンドを使用します。 この機能は、Cisco FlexConnect アクセス ポイントでサポートされています。

（注） WPA2/802.1x 認証中に PMK が生成される場合、FlexConnect アクセス ポイントは接続モードになっている必要があります。

OKC または CCKM に対して FlexConnect グループを使用する場合、PMK キャッシュは、同じ FlexConnect グループの一部で同じコントローラにアソシエートされているアクセス ポイント間でのみ共有されます。 アクセス ポイントが同じ FlexConnect グループにあっても、同じモビリティ グループの一部である別のコントローラにアソシエートされている場合、PMK キャッシュは更新されず、CCKM ローミングは失敗します。

FlexConnect グループおよびローカル認証

スタンドアロン モードの FlexConnect アクセス ポイントが最大 100 人の静的に設定されたユーザに対して LEAP、EAP-FAST、PEAP、または EAP-TLS 認証を実行できるように、コントローラを設定できます。 コントローラは、各 FlexConnect アクセス ポイントがコントローラに join したときに、ユーザ名とパスワードの静的リストをその FlexConnect アクセス ポイントに送信します。 グループ内の各アクセスポイントは、そのアクセスポイントにアソシエートされたクライアントのみを認証します。

この機能が適しているのは、企業が自律アクセス ポイント ネットワークから Lightweight FlexConnect アクセス ポイント ネットワークに移行するときに、大きなユーザ データベースを保持したくない場合、または自律アクセス ポイントの持つ RADIUS サーバ機能の代わりとなる別のハードウェア デバイスを追加したくない場合です。

（注） AP ローカル認証が有効な場合、LEAP、EAP-FAST、PEAP、または EAP-TLS 認証を設定できます。

AP がクライアントに証明書を送信しなければならないため、AP に証明書をプロビジョニングする必要があります。 コントローラにベンダー デバイス証明書およびベンダー CA 証明書をダウンロードします。 コントローラは AP にこれらの証明書を送ります。 コントローラにベンダー デバイス証明書およびベンダー CA 証明書を設定しない場合、FlexConnect グループに関連する AP は、多くの無線クライアントが認識しない可能性のあるコントローラの自己署名証明書をダウンロードします。

EAP-TLS を使用すると、クライアントのルート CA が AP のルート CA と異なる場合、AP はクライアント証明書を認識および受理しません。 企業の公開キー インフラストラクチャ（PKI）を使用する場合、コントローラが FlexConnect グループの AP に証明書を渡せるように、コントローラにベンダー デバイス証明書およびベンダー CA 証明書をダウンロードする必要があります。 クライアントと AP の共通ルート CA を使用しないと、EAP-TLS はローカル AP で失敗します。 AP は外部 CA を検査することができず、クライアントの証明書検証のために自身の CA チェーンを利用します。

ローカル証明書および CA 証明書のための AP のスペースは約 7 KB です。つまり短いチェーンのみが適応します。 長いチェーンまたは複数のチェーンはサポートされません。

（注） この機能は、FlexConnect バックアップ RADIUS サーバ機能とともに使用できます。 FlexConnect がバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect アクセス ポイントは、まずプライマリ バックアップ RADIUS サーバの認証を試行します。その後、セカンダリ バックアップ RADIUS サーバを試行し（プライマリに接続できない場合）、最後に FlexConnect アクセス ポイント自身の認証を試行します（プライマリとセカンダリの両方に接続できない場合）。

FlexConnect グループの数およびアクセス ポイントのサポートは、使用しているプラットフォームによって異なります。 次の設定を行えます。

- Cisco 5500 シリーズ コントローラに対して、グループごとに最大 100 の FlexConnect グループおよび最大 25 台のアクセス ポイント。
- 7.2 リリースの Cisco Flex 7500 シリーズ コントローラに対して、グループごとに最大 1000 の FlexConnect グループおよび最大 50 台のアクセス ポイント。
- 7.3 リリースの Cisco Flex 7500 および Cisco 8500 シリーズ コントローラに対して、グループごとに最大 2000 の FlexConnect グループおよび最大 100 台のアクセス ポイント。
- 残りのプラットフォームに対して、グループごとに最大 20 の FlexConnect グループおよび最大 25 台のアクセス ポイント。

FlexConnect グループの設定

FlexConnect グループの設定（GUI）

ステップ 1 [Wireless] > [FlexConnect Groups] を選択して、[FlexConnect Groups] ページを開きます。
このページでは、これまでに作成されたすべての FlexConnect グループが表示されます。

（注） 既存のグループを削除するには、そのグループの青いドロップダウンの矢印の上にカーソルを置いて [Remove] を選択します。

ステップ 2 [New] をクリックして、新しい FlexConnect グループを作成します。

ステップ 3 [FlexConnect Groups > New] ページで、[Group Name] テキスト ボックスに新しいグループの名前を入力します。 最大 32 文字の英数字を入力できます。

ステップ 4 [Apply] をクリックします。 新しいグループが [FlexConnect Groups] ページに表示されます。

ステップ 5 グループのプロパティを編集するには、目的のグループの名前をクリックします。 [FlexConnect Groups > Edit] ページが表示されます。

ステップ 6 プライマリ RADIUS サーバをこのグループに対して設定する場合（たとえば、アクセス ポイントが 802.1X 認証を使用する場合）は、[Primary RADIUS Server] ドロップダウン リストから目的のサーバを選択します。 それ以外の場合は、そのテキスト ボックスの設定をデフォルト値の [None] のままにします。

ステップ 7 セカンダリ RADIUS サーバをこのグループに対して設定する場合は、[Secondary RADIUS Server] ドロップダウン リストからサーバを選択します。 それ以外の場合は、そのフィールドの設定をデフォルト値の [None] のままにします。

ステップ 8 次の手順に従って、FlexConnect グループに RADIUS サーバを設定します。

a) RADIUS サーバの IP アドレスを入力します。
b) プライマリまたはセカンダリとしてサーバ タイプを選択します。
c) 共有の秘密を入力して、RADIUS サーバにログインし、確認用の入力をします。
d) ポート番号を入力します。
e) [Add] をクリックします。

ステップ 9 アクセス ポイントをグループに追加するには、[Add AP] をクリックします。 追加のフィールドが、ページの [Add AP] の下に表示されます。

ステップ 10 次のいずれかの作業を実行します。

- このコントローラに接続されているアクセス ポイントを選択するには、[Select APs from Current Controller] チェックボックスをオンにして、[AP Name] ドロップダウン リストからアクセス ポイントの名前を選択します。

  （注） このコントローラ上のアクセス ポイントを選択すると、不一致が起こらないように、アクセス ポイントの MAC アドレスが自動的に [Ethernet MAC] テキスト ボックスに入力されます。

- 別のコントローラに接続されているアクセス ポイントを選択するには、[Select APs from Current Controller] チェックボックスをオフのままにして、そのアクセス ポイントの MAC アドレスを [Ethernet MAC] テキスト ボックスに入力します。

（注） 同じグループ内の FlexConnect アクセス ポイントがそれぞれ別のコントローラに接続されている場合は、すべてのコントローラが同じモビリティ グループに属している必要があります。

ステップ 11 [Add] をクリックして、アクセス ポイントをこの FlexConnect グループに追加します。 アクセス ポイントの MAC アドレス、名前、およびステータスがページ下部に表示されます。

（注） アクセス ポイントを削除するには、そのアクセス ポイントの青いドロップダウンの矢印の上にカーソルを置いて [Remove] を選択します。

ステップ 12 [Apply] をクリックします。

ステップ 13 次のように、FlexConnect グループのローカル認証を有効にします。

a) [Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。

b) [Enable AP Local Authentication] チェックボックスをオンにして、この FlexConnect グループに対してローカル認証を有効にします。 デフォルト値はオフです。

c) [Apply] をクリックします。

d) [Local Authentication] タブを選択して、[FlexConnect > Edit (Local Authentication > Local Users)] ページを開きます。

e) LEAP、EAP-FAST、PEAP、または EAP-TLS を使用して認証できるクライアントを追加するには、次のいずれかを実行します。

f) [Upload CSV File] チェックボックスをオンにして、カンマ区切り値（CSV）ファイルをアップロードします。[Browse] ボタンをクリックすると、ユーザ名とパスワードを含む CSV ファイル（ファイルの各行は、username, password の形式になっている必要があります）を参照し、[Add] をクリックすると、CSV ファイルをアップロードします。 クライアントの名前が、ページ左側の「User Name」という見出しの下に表示されます。

g) クライアントを個別に追加するには、クライアントのユーザ名を [User Name] テキスト ボックスに入力し、クライアントのパスワードを [Password] テキスト ボックスと [Confirm Password] テキスト ボックスに入力します。[Add] をクリックすると、サポートされるローカル ユーザのリストにこのクライアントが追加されます。 クライアントの名前が、ページ左側の「User Name」という見出しの下に表示されます。

（注） 最大 100 個のクライアントを追加できます。

h) [Apply] をクリックします。

i) [Protocols] タブを選択して、[FlexConnect > Edit (Local Authentication > Protocols)] ページを開きます。

j) FlexConnect アクセス ポイントが LEAP を使用してクライアントを認証できるようにするには、[Enable LEAP Authentication] チェックボックスをオンにします。

k) EAP-FAST を使用しているクライアントを FlexConnect アクセス ポイントで認証できるようにするには、[Enable EAP-FAST Authentication] チェックボックスをオンにします。 デフォルト値はオフです。

l) FlexConnect アクセス ポイントが PEAP 認証を使用してクライアントを認証できるようにするには、[Enable PEAP Authentication] チェックボックスをオンにします。

AP ローカル認証が有効な場合にのみ、PEAP 認証を設定できます。

m) EAP-TLS を使用しているクライアントを FlexConnect アクセス ポイントで認証できるようにするには、[Enable EAP TLS Authentication] チェックボックスをオンにします。
AP ローカル認証が有効な場合にのみ、EAP-TLS 認証を設定できます。

EAP-TLS 認証を有効にすると、アクセス ポイントに EAP ルートとデバイスの証明書をダウンロードできるようになります。 ダウンロードしない場合は、[EAP TLS Certificate download] チェックボックスを選択解除することができます。

n) Protected Access Credential（PAC）をプロビジョニングする方法に応じて、次のいずれかを実行します。

- 手動の PAC プロビジョニングを使用するには、[Server Key] テキスト ボックスと [Confirm Server Key] テキスト ボックスに、PAC の暗号化と復号化に使用するサーバ キーを入力します。 キーは 32 桁の 16 進数文字である必要があります。
- PAC プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようにするには、[Enable Auto Key Generation] チェックボックスをオンにします。

o) [Authority ID] テキスト ボックスに、EAP-FAST サーバの Authority ID を入力します。 識別子は 32 桁の 16 進数文字である必要があります。

p) [Authority Info] テキスト ボックスに、EAP-FAST サーバの Authority ID をテキスト形式で入力します。 32 桁までの 16 進数文字を入力できます。

q) PAC タイムアウト値を指定するには、[PAC Timeout] チェックボックスをオンにして、PAC がテキスト ボックスに表示される秒数を入力します。 デフォルトではオフになっています。入力できる有効な範囲は 2 ～ 4095 秒です。

r) [Apply] をクリックします。

ステップ 14 [WLAN-ACL mapping] タブでは、次のことを実行できます。

a) [Web Auth ACL Mapping] の下で、WLAN ID を入力し、[WebAuth ACL] を選択し、[Add] をクリックして、Web 認証 ACL と WLAN をマッピングします。

b) [Local Split ACL Mapping] の下で、WLAN ID を入力し、[Local Split ACL] を選択し、[Add] をクリックして、ローカル スプリット ACL を WLAN にマッピングします。

（注） ローカル スプリット トンネリングには、最大 16 の WLAN と ACL の組み合わせを設定できます。 ローカル スプリット トンネリングは、静的 IP アドレス使用するクライアントには機能しません。

ステップ 15 [Central DHCP] タブでは、次のことを実行できます。

a) [WLAN Id] ボックスに、中央 DHCP をマッピングする WLAN ID を入力します。

b) [Central DHCP] チェックボックスをオンまたはオフにして、マッピングに対する中央 DHCP を有効または無効にします。

c) [Override DNS] チェックボックスをオンまたはオフにして、マッピングに対する DNS のオーバーライドを有効または無効にします。

d) [NAT-PAT] チェックボックスをオンまたはオフにして、マッピングに対するネットワーク アドレス変換およびポートアドレス変換を有効または無効にします。

e) [Add] をクリックして、中央 DHCP と WLAN のマッピングを追加します。

ステップ 16 [Save Configuration] をクリックします。

ステップ 17 さらに FlexConnect を追加する場合は、この手順を繰り返します。

（注） 個々のアクセス ポイントが FlexConnect グループに属しているかどうかを確認するには、次の順に選択します。[FlexConnect] タブで [Wireless] > [Access Points] > [All APs] > 目的のアクセス ポイントの名前。アクセス ポイントが FlexConnect に属する場合、グループの名前は [FlexConnect Name] テキスト ボックスに表示されます。

FlexConnect グループの設定（CLI）

ステップ 1 次のコマンドを入力して、FlexConnect グループを追加または削除します。
config flexconnect group *group_name* {**add** | **delete**}

ステップ 2 次のコマンドを入力して、FlexConnect グループのプライマリ RADIUS サーバまたはセカンダリ RADIUS サーバを設定します。
config flexconnect group *group_name* **radius server auth**{**add** | **delete**} {**primary** | **secondary**} *server_index*

ステップ 3 次のコマンドを入力して、FlexConnect グループのプライマリ RADIUS サーバまたはセカンダリ RADIUS サーバを設定します。
config flexconect group *group-name* **radius server auth** {{**add** {**primary** | **secondary**} *ip-addr auth-port secret*} | {**delete** {**primary** | **secondary**}}}

ステップ 4 次のコマンドを入力して、FlexConnect グループにアクセス ポイントを追加します。
config flexconnect *group_name* **ap** {**add** | **delete**} *ap_mac*

ステップ 5 次のように、FlexConnect のローカル認証を設定します。

a) FlexConnect グループにプライマリおよびセカンダリの RADIUS サーバが設定されていないことを確認します。

b) この FlexConnect グループのローカル認証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。
config flexconnect group *group_name* **radius ap** {**enable** | **disable**}

c) 次のコマンドを入力して、LEAP、EAP-FAST、PEAP、または EAP-TLS を使用して認証するクライアントのユーザ名とパスワードを入力します。
config flexconnect group *group_name* **radius ap user add** *username* **password** *password*
（注） 最大 100 個のクライアントを追加できます。

d) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが LEAP を使用して認証できるかどうかを指定します。
config flexconnect group *group_name* **radius ap leap** {**enable** | **disable**}

e) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが EAP-FAST を使用して認証できるかどうかを指定します。

config flexconnect group *group_name* **radius ap eap-fast** {**enable** | **disable**}

f) AP に EAP ルートおよびデバイス証明書をダウンロードするには、次のコマンドを入力します。
config flexconnect group *group_name* **radius ap eap-cert download**

g) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが EAP-TLS を使用してクライアントを認証できるかどうかを指定します。
config flexconnect group *group_name* **radius ap eap-tls** {**enable** | **disable**}

h) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが PEAP を使用してクライアントを認証できるかどうかを指定します。
config flexconnect group *group_name* **radius ap peap** {**enable** | **disable**}

i) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが PEAP を使用して認証できるかどうかを指定します。
config flexconnect group *group_name* **radius ap peap** {**enable** | **disable**}

j) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが EAP-TLS を使用して認証できるかどうかを指定します。
config flexconnect group *group_name* **radius ap eap-tls** {**enable** | **disable**}

k) 次のコマンドを入力して、EAP ルートおよびデバイス証明書をダウンロードします。
config flexconnect group *group_name* **radius ap eap-cert download**

l) PAC をプロビジョニングする方法に応じて、次のいずれかのコマンドを入力します。

- **config flexconnect group** *group_name* **radius ap server-key** *key*：PAC の暗号化と暗号化解除に使用するサーバ キーを指定します。 キーは 32 桁の 16 進数文字である必要があります。
- **config flexconnect group** *group_name* **radius ap server-key auto**：PAC プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようにします。

m) EAP-FAST サーバの Authority ID を指定するには、次のコマンドを入力します。
config flexconnect group *group_name* **radius ap authority id** *id*
id は 32 桁の 16 進数文字です。

n) EAP-FAST サーバの Authority ID をテキスト形式で指定するには、次のコマンドを入力します。
config flexconnect group *group_name* **radius ap authority info** *info*
info は 32 桁までの 16 進数文字です。

o) PAC が表示される秒数を指定するには、次のコマンドを入力します。
config flexconnect group *group_name* **radius ap pac-timeout** *timeout*
timeout に指定できるのは、*2* ～ 4095 秒の範囲内の値または 0 です。 0 がデフォルト値です。この値を指定すると、PAC はタイムアウトしなくなります。

ステップ 6 次のコマンドを入力して、FlexConnect グループ 上に ポリシー ACL を設定します。
config flexconnect group *group-name* **policy acl** {**add** | **delete**} *acl-name*

ステップ 7 次のコマンドを入力して、FlexConnect グループごとにローカル スプリット トンネリングを設定します。
config flexconnect group *group_name* **local-split wlan** *wlan-id* **acl** *acl-name flexconnect-group-name* {**enable** | **disable**}

ステップ 8 ローカルにスイッチされるクライアントに対して、上書きされたインターフェイスの L2 ブロードキャスト ドメイン間のマルチキャスト/ブロードキャストを設定するには、次のコマンドを入力します。
config flexconnect group *group_name* **multicast overridden-interface** {**enable** | **disable**}

ステップ 9 次のコマンドを入力して、WLAN ごとに中央 DHCP を設定します。
config flexconnect group *group-name* **central-dhcp** *wlan-id* {**enable override dns** | **disable** | **delete**}

ステップ 10 次のコマンドを入力して、FlexConnect グループにポリシー ACL を設定します。
config flexconnect group *group_name* **policy acl** {**add** | **delete**} *acl-name*

ステップ 11 次のコマンドを入力して、FlexConnect グループに Web 認証 ACL を設定します。
config flexconnect group *group_name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable** | **disable**}

ステップ 12 次のコマンドを入力して、FlexConnect グループに WLAN-VLAN マッピングを設定します。
config flexconnect group *group_name* **wlan-vlan wlan** *wlan-id*{**add** | **delete**}**vlan** *vlan-id*

ステップ 13 グループの効率的なアップグレードを設定するには、次のコマンドを入力します。
config flexconnect group *group_name* **predownload** {**enable** | **disable** | **master** | **slave**} *ap-name* **retry-count** *maximum retry count* **ap-name** *ap-name*

ステップ 14 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 15 次のコマンドを入力して、FlexConnect グループの最新のリストを表示します。
show flexconnect group summary

ステップ 16 次のコマンドを入力して、特定の FlexConnect グループの詳細を表示します。
show flexconnect group detail *group_name*

FlexConnect グループの VLAN-ACL マッピングの設定

FlexConnect グループの VLAN-ACL マッピングの設定（GUI）

ステップ 1 [Wireless] > [FlexConnect Groups] を選択します。
[FlexConnect Groups] ページが表示されます。 このページに、コントローラにアソシエータされているアクセス ポイントが一覧表示されます。

ステップ 2 VLAN-ACL マッピングを設定する FlexConnect グループの [Group Name] リンクをクリックします。

ステップ 3 [VLAN-ACL Mapping] タブをクリックします。
その FlexConnect グループの [VLAN-ACL Mapping] ページが表示されます。

ステップ 4 [VLAN ID] テキスト ボックスにネイティブ VLAN ID を入力します。

ステップ 5 [Ingress ACL] ドロップダウン リストから、[Ingress ACL] を選択します。

ステップ 6 [Egress ACL] ドロップダウン リストから、出力 ACL を選択します。

ステップ 7 [Add] をクリックして、FlexConnect グループにこのマッピングを追加します。
VLAN ID は、必要な ACL とともにマッピングされます。 マッピングを削除するには、青のドロップダウン矢印の上にカーソルを移動し、[Remove] を選択します。

FlexConnect グループの VLAN-ACL マッピングの設定（CLI）

- 次のコマンドを入力して、VLAN を FlexConnect グループに追加し、入力 ACL と出力 ACL をマッピングします。
  config flexconnect group *group-name* **vlan add** *vlan-id* **acl** *ingress-acl egress acl*

VLAN-ACL マッピングの表示（CLI）

- 次のコマンドを入力して、FlexConnect グループの詳細を表示します。
  show flexconnect group detail *group-name*
- 次のコマンドを入力して、アクセス ポイントの VLAN-ACL マッピングを表示します。
  show ap config general *ap-name*

FlexConnect グループの WLAN-VLAN マッピングの設定

FlexConnect グループの WLAN-VLAN マッピングの設定（GUI）

次に注意事項を示します。

- 個々の AP 設定は、FlexConnect グループおよびグローバル WLAN の設定よりも優先されます。 FlexConnect グループ設定は、グローバル WLAN 設定よりも優先されます。
- AP レベル設定はフラッシュに保存され、WLAN および FlexConnect グループの設定は RAM に保存されます。
- AP は、異なるコントローラ間を移動する場合に、個々の VLAN マッピングを保持することができます。 ただし、FlexConnect グループおよびグローバルのマッピングは新しいコントローラの設定になります。 WLAN SSID が 2 台のコントローラ間で異なる場合、WLAN-VLAN マッピングは適用されません。

- ダウンストリーム トラフィックでは、VLAN ACL が最初に適用されてからクライアント ACL が適用されます。 アップストリーム トラフィックでは、クライアント ACL が最初に適用されてから VLAN ACL が適用されます。
- 802.1X 認証時に ACL が AP に存在する必要があります。 ACL が AP にない場合、クライアントは、802.1X 認証に成功しても AP によって認証を拒否される場合があります。

AP 上の ACL の有無	AAA から送信された ACL 名	802.1X 認証の結果
No	No	認証済み、ACL 適用なし
No	Yes	認証拒否
Yes	No	認証済み、ACL 適用なし
Yes	Yes	認証済み、クライアント ACL 適用

- クライアント認証後に、ACL 名が RADIUS サーバ上で変更された場合、クライアントは、再び最初から認証を実行して正しいクライアント ACL を取得する必要があります。
- FlexConnect グループの WLAN-VLAN マッピングは Cisco AP の 1131 および 1242 でサポートされません。

はじめる前に

WLAN がローカルにスイッチされることを確認します。 設定は、WLAN が AP でブロードキャストされる場合にのみ AP に適用されます。

ステップ 1 [Wireless] > [FlexConnect Groups] を選択します。

ステップ 2 グループ名をクリックします。
[FlexConnect Groups > Edit] ページが表示されます。

ステップ 3 [WLAN VLAN Mapping] タブをクリックします。

ステップ 4 WLAN ID と VLAN ID を入力し、[Add] をクリックします。
マッピングは同じタブに表示されます。

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。

FlexConnect グループの WLAN-VLAN マッピングの設定（CLI）

はじめる前に

WLAN がローカルにスイッチされることを確認します。 設定は、WLAN が AP でブロードキャストされる場合にのみ AP に適用されます。

- 次のコマンドを入力して、FlexConnect グループに WLAN-VLAN マッピングを設定します。
  config flexconnect group *group-name* **wlan-vlan wlan** *wlan-id* {**add** | **delete**} **vlan** *vlan-id*