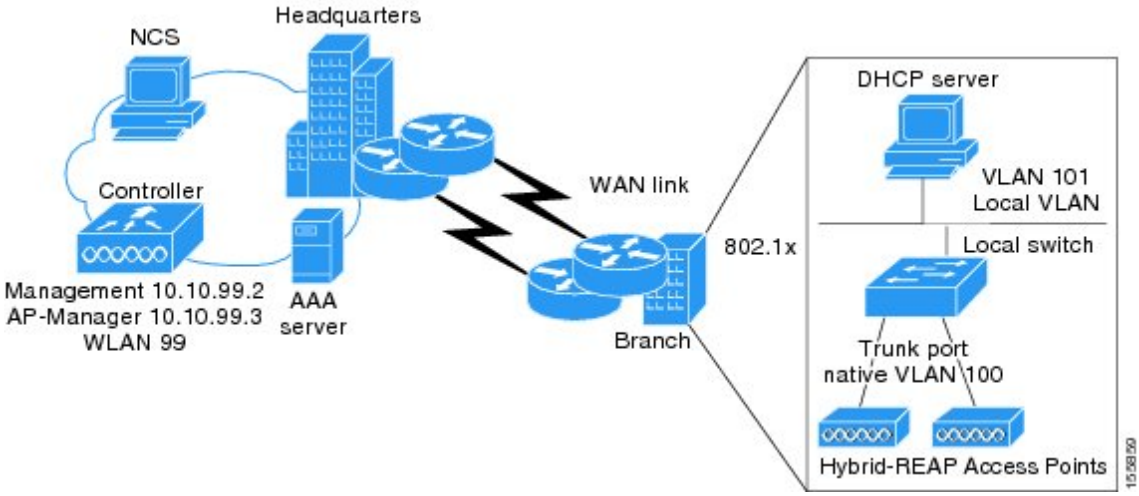
FlexConnect

FlexConnect について

FlexConnect（以前は、ハイブリッドリモートエッジアクセス ポイントまたはH-REAP と呼ばれていました）は、ブランチオフィスとリモートオフィスに導入されるワイヤレスソリューションです。これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスからワイドエリアネットワーク（WAN）経由で、支社またはリモートオフィスのアクセスポイント（AP）を設定および制御できるようになります。FlexConnect アクセスポイントは、コントローラへの接続を失ったとき、クライアント データ トラフィックをローカルにスイッチングし、クライアント認証をローカルで実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。接続モードで、FlexConnect アクセスポイントは、ローカル認証も実行できます。

図 *1 : FlexConnect* の導入

次の図に、FlexConnect の一般的な導入を示します。



コントローラソフトウェアでは、FlexConnect アクセスポイントに対する耐障害性をより強化した方法が提供されています。以前のリリースでは、コントローラから解除されるたびに、FlexConnect アクセスポイントはスタンドアロンモードに移行します。中央でスイッチされるクライアントのアソシエーションは解除されます。ただし、FlexConnect アクセス ポイントはローカルにスイッチされたクライアントに引き続き対応します。FlexConnect アクセスポイントがコントローラ（またはスタンバイコントローラ）に再joinすると、すべてのクライアントが接続解除され、再度認証されます。この機能は強化されており、クライアントと FlexConnect アクセスポイント間の接続はそのまま保持され、クライアントによるシームレスな接続が実現します。アクセスポイントとコントローラの両方の設定が同じ場合は、クライアントと AP 間の接続が維持されます。

クライアント接続が確立された後に、コントローラはクライアントの元の属性を復元しません。クライアントのユーザ名、現在のレートとサポートされているレート、およびリッスン間隔値は、セッションタイマーが切れた後でのみデフォルト値にリセットされます。

FlexConnect アクセスポイントは、1 ロケーションにつき何台でも展開できます。複数の FlexConnect グループを 1 つのロケーションで定義できます。

コントローラは、ユニキャストパケットまたはマルチキャストパケットの形式でアクセスポイントにマルチキャストパケットを送信できます。FlexConnect モードでは、アクセスポイントはユニキャスト形式でのみマルチキャストパケットを受信できます。

FlexConnect アクセスポイントは、1 対 1 のネットワークアドレス変換（NAT）設定をサポートします。また、真のマルチキャストを除くすべての機能に対して、ポートアドレス変換（PAT）をサポートします。NAT 境界を越えるマルチキャストもサポートされます（ユニキャストオプションを使用して設定されている場合）。FlexConnect アクセスポイントは、中央でスイッチされるすべての WLAN に対して真のマルチキャストが動作するときを除き、多対 1 の NAT または PAT境界もサポートします。

（注） NAT と PAT は FlexConnect アクセスポイントではサポートされていますが、対応するコントローラではサポートされていません。シスコは、NAT/PAT 境界の背後にコントローラを置く構成はサポートしません。

アクセスポイントで、これらのセキュリティタイプがローカルにアクセス可能である場合、VPN および Point-to-Point Tunnel Protocol（PPTP）は、ローカルにスイッチされるトラフィックに対してサポートされます。

FlexConnect アクセスポイントは複数の SSID をサポートします。

ワークグループブリッジおよびユニバーサル ワークグループ ブリッジは、ローカルにスイッチされるクライアントの FlexConnect アクセスポイントでサポートされます。

FlexConnect は、IPv4 の動作と同様にトラフィックをローカル VLAN にブリッジすることによって、IPv6 クライアントをサポートしています。FlexConnect は、最大 100 のアクセスポイントのグループに対するクライアントモビリティをサポートしています。

ローカルモードから FlexConnect モードに移行しても、アクセスポイントをリブートする必要はありません。

FlexConnect 認証プロセス

アクセスポイントは、ブート時にコントローラを検索します。コントローラが見つかると、そのコントローラに join し、最新のソフトウェアイメージと設定をコントローラからダウンロードして、無線を初期化します。ダウンロードした設定は不揮発性メモリに保存されて、スタンドアロンモードで使用されます。

（注） 最新のコントローラソフトウェアのダウンロード後に、アクセスポイントをリブートしたら、アクセスポイントを FlexConnect モードへ変換する必要があります。

（注） 802.1X は、Cisco 2700 シリーズの AP の AUX ポートではサポートされていません。

FlexConnect アクセスポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- アクセスポイントの IP アドレスが DHCP サーバから割り当て済みの場合は、通常の CAPWAP または LWAPP ディスカバリプロセスを介してコントローラを検出します。

  （注） OTAP はサポートされていません。

- アクセスポイントに固定 IP アドレスが割り当てられている場合は、DHCP オプション 43 以外の方法のディスカバリプロセスを使用してコントローラを検出します。アクセスポイントがレイヤ3ブロードキャストでコントローラを検出できない場合は、DNS解決を使用することをお勧めします。DNS を使用すれば、固定 IP アドレスを持ち DNS サーバを認識しているアクセスポイントは、最低 1 つのコントローラを見つけることができます。
- CAPWAP と LWAPP のどちらのディスカバリメカニズムも使用できないリモートネットワークにあるコントローラを検出できるようにするには、プライミングを使用してください。この方法を使用すると、アクセスポイントの接続先のコントローラを（アクセスポイントの CLI により）指定できます。

FlexConnectアクセスポイントがコントローラに到達できるとき（接続モードと呼ばれます）、コントローラはクライアント認証を支援します。FlexConnect アクセスポイントがコントローラにアクセスできないとき、アクセスポイントはスタンドアロンモードに入り、独自にクライアントを認証します。

（注） アクセスポイント上の LED は、デバイスが異なる FlexConnect モードに入るときに変化します。LED パターンの情報については、アクセスポイントのハードウェア インストール ガイドを参照してください。

クライアントが FlexConnect アクセスポイントにアソシエートするとき、アクセスポイントではすべての認証メッセージをコントローラに送信し、WLAN設定に応じて、クライアントデータパケットをローカルにスイッチする（ローカルスイッチング）か、コントローラに送信（中央スイッチング）します。クライアント認証（オープン、共有、EAP、Web 認証、および NAC）とデータパケットに関して、WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- 中央認証、中央スイッチング：コントローラがクライアント認証を処理し、すべてのクライアントデータはコントローラにトンネルを通じて戻されます。この状態は、接続済みモードの場合にだけ有効です。
- 中央認証、ローカルスイッチング：コントローラがクライアント認証を処理し、FlexConnect アクセスポイントがデータパケットをローカルにスイッチします。クライアントが認証に成功した後、コントローラは新しいペイロードと共にコンフィギュレーションコマンドを送信し、FlexConnect アクセスポイントに対して、ローカルにデータパケットのスイッチを始めるように指示します。このメッセージはクライアントごとに送信されます。この状態は接続モードにのみ適用されます。

（注） FlexConnect ローカルスイッチング、中央認証導入では、静的 IP アドレスを持つパッシブクライアントが存在する場合は、[WLAN] > [Advanced] タブで [Learn Client IP Address] 機能を無効にすることをお勧めします。

- ローカル認証、ローカルスイッチング：FlexConnect アクセスポイントがクライアント認証を処理し、クライアントデータパケットをローカルにスイッチします。この状態はスタンドアロンモードおよび接続済みモードの場合に有効です。

  接続済みモードでは、アクセスポイントは、ローカルで認証されたクライアントに関する最小限の情報をコントローラに提供します。次の情報はコントローラでは使用できません。

  - ポリシータイプ
  - アクセス VLAN
  - VLAN 名
  - サポートされるレート
  - 暗号化の暗号

    ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位（MTU）が 576 バイトを下回らない、最小帯域幅が 128 kbps のリモートオフィス設定を維持できない場合に役立ちます。ローカル認証で、認証機能はアクセスポイント自体に存在します。ローカル認証は、ブランチ オフィスの遅延要件を短縮できます。

    （注） ローカル認証は、ローカルスイッチングモードの FlexConnect アクセスポイントの WLAN 上のみで有効にできます。

    ローカル認証に関する注意事項は、次のとおりです。

  - ゲスト認証は、FlexConnect ローカル認証を有効にした WLAN で実行できません。
  - コントローラ上でのローカル RADIUS はサポートされていません。
  - クライアントが認証されたら、ローミングはグループ内のコントローラおよび他の FlexConnect アクセスポイントがクライアント情報に更新された後でのみサポートされます。
  - 接続モードのローカル認証には、WLAN 設定が必要です。

    （注） FlexConnectアクセスポイントに接続している、ローカルにスイッチされたクライアントがIPアドレスを更新し、またjoinする場合に、クライアントは実行状態のまま残ります。これらのクライアントはコントローラによって再認証されません。

- 認証ダウン、スイッチダウン：この状態になると、WLAN は既存クライアントのアソシエーションを解除し、ビーコン要求とプローブ要求の送信を停止します。この状態はスタンドアロンモードおよび接続済みモードの両方の場合に有効です。

- 認証ダウン、ローカルスイッチング：WLANは新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。この状態はスタンドアロンモードでのみ有効です。

FlexConnectアクセスポイントがスタンドアロンモードになると、オープン、共通、WPA-PSK、またはWPA2-PSKの認証用に設定されたWLANは、「ローカル認証、ローカルスイッチング」状態になり、新しいクライアント認証を続行します。コントローラ ソフトウェア リリース4.2以降のリリースでは、これは802.1X、WPA-802.1X、WPA2-802.1X、またはCCKM用に設定されたWLANでも正しい設定です。ただし、これらの認証タイプでは外部のRADIUSサーバが設定されている必要があります。FlexConnectアクセスポイントでローカルRADIUSサーバを設定して、スタンドアロンモードで、またはローカル認証との組み合わせで802.1Xをサポートすることもできます。

その他のWLANは、「認証停止、スイッチング停止」状態（WLANが中央スイッチング用に設定されている場合）または「認証停止、ローカルスイッチング」状態（WLANがローカルスイッチング用に設定されている場合）のいずれかになります。

FlexConnectアクセスポイントがスタンドアロンモードではなく、コントローラに接続されている場合、コントローラはプライマリRADIUSサーバを使用します。コントローラがプライマリRADIUSサーバにアクセスする順序は、[RADIUS Authentication Servers]ページまたは**config radius auth add** CLIコマンドで指定された順序になります（特定のWLANのサーバ順序がオーバーライドされている場合を除く）。ただし、802.1X EAP認証を使用する場合は、クライアントを認証するために、スタンドアロンモードのFlexConnectアクセスポイント用のバックアップRADIUSサーバが必要となります。

（注） コントローラはバックアップRADIUSサーバを使用しません。コントローラはローカル認証モードでバックアップRADIUSサーバを使用します。

バックアップRADIUSサーバは、個々のスタンドアロンモードFlexConnectアクセスポイントに対して設定することも（コントローラのCLIを使用）、スタンドアロンモードFlexConnectアクセスポイントのグループに対して設定することも（GUIまたはCLIを使用）できます。個々のアクセスポイントに対して設定されたバックアップサーバは、FlexConnectに対するバックアップRADIUSサーバ設定よりも優先されます。

Web認証がリモートサイトでFlexConnectのアクセスポイントに使用されると、クライアントはリモートローカルサブネットからIPアドレスを取得します。最初のURL要求を解決するため、DNSがサブネットのデフォルトゲートウェイを介してアクセスできます。コントローラがDNSクエリーの応答パケットを代行受信およびリダイレクトするには、これらのパケットはCAPWAP接続を介してデータセンターでコントローラにアクセスする必要があります。Web認証プロセス中、FlexConnectのアクセスポイントはDNSとDHCPメッセージのみを許可します。つまり、アクセスポイントは、クライアントのWeb認証が完了するまでDNS応答メッセージをコントローラに転送します。クライアントのWeb認証が完了すると、すべてのトラフィックがローカルでスイッチされます。

（注） コントローラが NAC に対して設定されている場合、クライアントはアクセスポイントが接続モードにある場合にのみアソシエートできます。NACが有効の場合、WLANがローカルスイッチングに設定されている場合でも、有害な（または検疫された）VLANを作成して、このVLANに割り当てられているクライアントのデータトラフィックがコントローラを通過できるようにする必要があります。クライアントが検疫 VLAN に割り当てられると、そのクライアントのデータパケットはすべて中央でスイッチングされます。隔離VLANの作成の詳細については、「動的インターフェイスの設定」の項を参照してください。NAC アウトオブバンドサポートの設定の詳細については、「NAC アウトオブバンド統合の設定」の項を参照してください。

FlexConnect アクセスポイントがスタンドアロンモードになると、次のようになります。

- アクセスポイントは、ARP経由でデフォルトゲートウェイに到達できるかどうかを確認します。その場合、アクセスポイントはコントローラへの到達を試行し続けます。

アクセスポイントが ARP を確立できない場合は、次のことが起こります。

- アクセスポイントは5回の検出を試行し、それでもコントローラを検出できない場合は、新しい DHCP IP を取得するために、イーサネットインターフェイス上で DHCP を更新しようとします。
- アクセスポイントが、5回再試行して失敗した場合、インターフェイスのIPアドレスを再度更新します。これは 3 回試行されます。
- 3回の試行が失敗した場合、アクセスポイントは固定IPに戻ってリブートします（アクセス ポイントが固定 IP を使用して設定されている場合のみ）。
- リブートの実行により、アクセス ポイントの不明なエラーの可能性が排除されます。

アクセスポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエート解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

FlexConnect の制約事項

- 固定 IP アドレスまたはDHCPアドレスを持つFlexConnectアクセスポイントを展開することができます。DHCP の状況では、DHCP サーバはローカルに使用可能であり、ブート時にアクセスポイントの IP アドレスを提供できる必要があります。
- FlexConnect は最大で 4 つの断片化されたパケット、または最低 576 バイトの最大伝送単位（MTU）WAN リンクをサポートします。
- アクセスポイントとコントローラの間のラウンドトリップ遅延が300ミリ秒（ms）を超えてはなりません。また、CAPWAP コントロールパケットは他のすべてのトラフィックよりも優先される必要があります。300 ミリ秒のラウンドトリップ遅延を実現できないシナリオでは、ローカル認証を実行するようにアクセスポイントを設定します。

- クライアント接続は、アクセスポイントがスタンドアロンモードから接続モードに移行するときに RUN 状態になっている、ローカルにスイッチされたクライアントに対してのみ復元されます。アクセスポイントのモードが移行すると、アクセスポイントの無線もリセットされます。
- コントローラの設定は、アクセスポイントがスタンドアロンモードになった時点と、アクセスポイントが接続済みモードに戻った時点の間で同じである必要があります。同様に、アクセスポイントがセカンダリコントローラまたはバックアップコントローラにフォールバックする場合、プライマリコントローラとセカンダリコントローラまたはバックアップコントローラの設定は同じである必要があります。
- 新規に接続したアクセスポイントは、FlexConnect モードでブートできません。
- 802.11r Fast Transition ローミングは、ローカル認証で運用中は Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP ではサポートされません。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカルスイッチングを行うように設定されている WLAN での使用はサポートされていません。
- FlexConnect アクセスポイントのプライマリコントローラとセカンダリコントローラの設定が同一であることが必要です。設定が異なると、アクセスポイントはその設定を失い、特定の機能（WLAN の無効化、VLAN、静的チャネル番号など）が正しく動作しないことがあります。さらに、FlexConnect アクセスポイントの SSID とそのインデックス番号を両方のコントローラで同じにしてください。
- アクセスポイントで設定された syslog サーバと組み合わせて、FlexConnect アクセス ポイントを設定する場合、アクセスポイントがリロードされ、1 以外のネイティブ VLAN になった後、初期化時に、アクセスポイントからの syslog パケットで VLAN ID 1 のタグが付けられているものはほとんどありません。
- MAC フィルタリングは、スタンドアロンモードの FlexConnect アクセスポイントではサポートされていません。ただし、MAC フィルタリングは、接続モードの FlexConnect アクセスポイントでのローカルスイッチングと中央認証はサポートされています。また、FlexConnect アクセスポイントを持つローカルにスイッチされる WLAN の Open SSID、MAC フィルタリングおよび RADIUS NAC は、MAC が Cisco ISE でチェックされる有効な設定です。
- FlexConnect で、IPv6 ACL、ネイバー ディスカバリ キャッシュ、および IPv6 NDP パケットの DHCPv6 スヌーピングはサポートされていません。
- FlexConnect では、[Client Detail] ウィンドウに IPv6 クライアントのアドレスは表示されません。
- ローカルにスイッチされた WLAN を使用した FlexConnect アクセスポイントでは、IP ソースガードを実行したり、ARP スプーフィングを防止したりすることができません。中央でスイッチングされる WLAN では、ワイヤレスコントローラが IP ソースガードおよび ARP スプーフィングを実行します。

- ローカルスイッチングを使用する FlexConnect AP における ARP スプーフィング攻撃を防ぐために、ARP インスペクションを使用することを推奨します。
- FlexConnect AP の WLAN でローカルスイッチングを有効にすると、AP はローカルスイッチングを実行します。ただし、ローカルモードの AP に対しては、中央スイッチングが実行されます。

  FlexConnect モードの AP とローカルモードの AP 間におけるクライアントのローミングがサポートされていないシナリオでは、移動後の VLAN の違いが原因で、クライアントが正しい IP アドレスを取得できない場合があります。また、FlexConnect モード AP とローカルモード AP 間の L2 および L3 のローミングはサポートされていません。
- FlexConnect スタンドアロンモードの Wi-Fi Protected Access バージョン 2（WPA2）、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Advanced Encryption Standard（AES）のみがサポートされます。
- FlexConnect スタンドアロンモードの Wi-Fi Protected Access（WPA）、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Temporal Key Integrity Protocol（TKIP）のみがサポートされます。
- TKIP による WPA2 および AES による WPA は、スタンドアロンモード、接続モードのローカル認証、および接続モードの CCKM 高速ローミングではサポートされません。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズの AP では、オープンな WPA（PSK および 802.1x）認証のみサポートされています。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP では、802.11r Fast Transition ローミングのみサポートされています。
- ローカルにスイッチングされた WLAN の AVC は、第 2 世代の AP でサポートされています。
- 外部 RADIUS サーバでユーザが利用できない場合は、ローカル認証のフォールバックはサポートされません。
- ローカルスイッチングおよびローカル認証で FlexConnect AP 用に設定された WLAN については、dot11 クライアント情報の同期がサポートされます。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP では、DNS Override はサポートされていません。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP は、IIPv6 をサポートしていません。ただし、ワイヤレス クライアントはこれらの AP 全体に IPv6 トラフィックを渡すことができます。
- flex プロファイルでは、Flex モードで VLAN グループはサポートされていません。
- 個々のクライアントまたは無線で許可されるメディアストリームの最大数の設定は、FlexConnect モードではサポートされていません。

- APがFlexConnectモード（接続されているかスタンドアロン）であり、ローカルスイッチングとローカル認証を実行している場合、WLANクライアントアソシエーションの制限は機能しません。
- FlexConnect モードのローカル スイッチング クライアントは、Cisco Aironet 1810 シリーズ AP の RLAN プロファイルの IP アドレスを取得しません。
- IPv6 RADIUS サーバは FlexConnect AP 用に設定できません。IPv4 設定のみがサポートされます。

サイトタグの設定

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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site rr-xyz-site`	サイトタグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**flex-profile** *flex-profile-name* 例： `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	flexプロファイルをサイトタグにマッピングします。
ステップ 4	**ap-profile** *ap-profile* 例： `Device(config-site-tag)# ap-profile xyz-ap-profile`	AP プロファイルをワイヤレスサイトに割り当てます。
ステップ 5	**description** *site-tag-name* 例： `Device(config-site-tag)# description "default site tag"`	サイトタグの説明を追加します。
ステップ 6	**no local-site** 例： `Device(config-site-tag)# no local-site`	アクセスポイントを FlexConnect モードに移行します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-site-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**show wireless tag site summary** 例： `Device# show wireless tag site summary`	（任意）サイトタグのサマリーを表示します。

ポリシー タグの設定（CLI）

ポリシー タグを設定するには、次の手順に従います。

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	**wireless tag policy** *policy-tag-name* 例： `Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 5	**show wireless tag policy summary** 例： `Device# show wireless tag policy summary`	（任意）設定済みのポリシー タグを表示します。 （注） ポリシー タグに関する詳細情報を表示するには、**show wireless tag policy detailed** *policy-tag-name* コマンドを使用します。

AP へのポリシータグとサイトタグの付加（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] の順に選択します。

[All Access Points] セクションに、ネットワーク内のすべての AP の詳細が表示されます。

ステップ 2 AP の設定の詳細を編集するには、その AP の行を選択します。

[Edit AP] ウィンドウが表示されます。

ステップ 3 [General] タブの [Tags] セクションで、[Configuration] > [Tags & Profiles] > [Tags] ページで作成した、該当するポリシータグ、サイトタグ、および RF タグを指定します。

ステップ 4 [Update & Apply to Device] をクリックします。

AP へのポリシー タグとサイト タグの付加（CLI）

ポリシー タグとサイト タグを AP に付加するには、次の手順に従います。

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	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、AP プロファイル コンフィギュレーション モードを開始します。 （注） *mac-address* 有線 mac アドレスである必要があります。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	ポリシー タグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例：	サイトタグを AP にマッピングします。

	コマンドまたはアクション	目的
	`Device(config-ap-tag)# site-tag rr-xyz-site`	
ステップ 5	**rf-tag** *rf-tag-name* 例： `Device(config-ap-tag)# rf-tag rf-tag1`	RF タグを関連付けます。
ステップ 6	**end** 例： `Device(config-ap-tag)# end`	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**show ap tag summary** 例： `Device# show ap tag summary`	（任意）AP の詳細と AP に関連付けられているタグを表示します。
ステップ 8	**show ap name** <*ap-name*> **tag info** 例： `Device# show ap name ap-name tag info`	（任意）AP 名とタグ情報を表示します。
ステップ 9	**show ap name** <*ap-name*> **tag detail** 例： `Device# show ap name ap-name tag detail`	（任意）AP 名とタグの詳細を表示します。

FlexConnect の設定

（注） 設定作業は、ここにリストされている順序で実行する必要があります。

リモートサイトでのスイッチの設定

手順

ステップ 1 FlexConnect を有効にするアクセスポイントを、スイッチ上のトランクまたはアクセスポートに接続します。

（注） この手順に示す設定例では、FlexConnect アクセスポイントはスイッチ上のトランクポートに接続されます。

ステップ 2 次の設定例は、FlexConnect アクセスポイントをサポートするようにスイッチを設定する方法を示しています。

この設定例では、FlexConnect アクセスポイントは、トランクインターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。このアクセスポイントは、このネイティブ VLAN 上での IP 接続を必要とします。リモートサイトのローカルサーバとリソースは、VLAN 101 上にあります。DHCP プールがスイッチの両方の VLAN のローカルスイッチ内に作成されます。最初の DHCP プール（ネイティブ）は FlexConnect アクセスポイントにより使用され、2 つ目の DHCP プール（ローカルスイッチング）は、クライアントがローカルでスイッチングされる WLAN にアソシエートする場合、クライアントにより使用されます。

```
.
.
.
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 209.165.202.225 255.255.255.224
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 101
 switchport mode trunk
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.225 255.255.255.224
end
!
.
.
.
```

FlexConnect に対するコントローラの設定

次の 2 つの環境で FlexConnect のコントローラを設定できます。

- 中央でスイッチされる WLAN
- ローカルでスイッチされる WLAN

FlexConnect のコントローラの設定には、中央でスイッチされる WLAN とローカルにスイッチされる WLAN を作成する操作が含まれます。次の表に、3 つの WLAN の例を示します。

表 *1 : WLAN* のシナリオ

WLAN	セキュリティ	認証	スイッチング	インターフェイスマッピング（VLAN）
Employee	WPA1+WPA2	中央	中央	Management（中央でスイッチされる VLAN）
Employee-local	WPA1+WPA2（PSK）	ローカル	ローカル	101（ローカルにスイッチされる VLAN）
Guest-central	Web 認証	中央	中央	Management（中央でスイッチされる VLAN）
Employee-local-auth	WPA1+WPA2	ローカル	ローカル	101（ローカルにスイッチされる VLAN）

FlexConnect モードでのローカルスイッチングの設定（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] ページで、ポリシープロファイルの名前をクリックして編集するか、[Add] をクリックして新しいポリシープロファイルを作成します。

ステップ 3 表示される [Add/Edit Policy Profile] ウィンドウで、[Central Switching] チェックボックスをオフにします。

ステップ 4 [Update & Apply to Device] をクリックします。

FlexConnect モードでのローカルスイッチングの設定（CLI）

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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**no central switching** 例： `Device(config-wireless-policy)# no central switching`	WLAN をローカルスイッチング用に設定します。
ステップ 4	**end** 例： `Device(config)# 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。

FlexConnect モードでの中央スイッチングの設定（GUI）

始める前に

ポリシープロファイルが設定されていることを確認します。ポリシープロファイルが設定されていない場合は、「ポリシープロファイルの設定（GUI）」の項を参照してください。

手順

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

ステップ 2 [Policy Profile] ページで、ポリシーを選択します。

ステップ 3 [Edit Policy Profile] ウィンドウの [General] タブで、スライダを使用して [Central Switching] を有効または無効にします。

ステップ 4 [Update & Apply to Device] をクリックします。

FlexConnect モードでの中央スイッチングの設定

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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**central switching** 例： `Device(config-wireless-policy)# central switching`	WLAN を中央スイッチング用に設定します。
ステップ 4	**end** 例： `Device(config)# 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。

FlexConnect のアクセスポイントの設定

詳細については、サイト タグの設定（CLI）を参照してください。

WLAN 上のローカル認証用のアクセスポイントの設定（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] ページで、ポリシープロファイル名を選択します。[Edit Policy Profile] ウィンドウが表示されます。

ステップ 3 [General] タブで、[Central Authentication] チェックボックスをオフにします。

ステップ 4 [Update & Apply to Device] をクリックします。

WLAN 上のローカル認証用のアクセスポイントの設定（CLI）

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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**no central authentication** 例： `Device(config-wireless-policy)# no central authentication`	WLAN を ローカル認証用に設定します。
ステップ 4	**end** 例： `Device(config)# 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。

クライアントデバイスの WLAN への接続

FlexConnect に対するコントローラの設定 （14 ページ）で作成した WLAN にクライアントデバイスを接続するためのプロファイルを作成するには、次の手順に従ってください。

シナリオ例（FlexConnect に対するコントローラの設定 （14 ページ）を参照）では、クライアントに 3 つのプロファイルがあります。

1. 「employee」WLAN に接続するには、WPA または WPA2 と PEAP-MSCHAPV2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、コントローラの管理 VLAN によってクライアントに IP アドレスが割り当てられます。
2. 「local-employee」WLAN に接続するには、WPA または WPA2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、ローカルスイッチのVLAN 101 によってクライアントに IP アドレスが割り当てられます。
3. 「guest-central」WLAN に接続するには、オープンの認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、アクセスポイントへのネットワークローカルのVLAN 101によってクライアントにIPアドレスが割り当てられます。クライアントが接続すると、ローカルユーザはWebブラウザに任意のHTTPアドレスを入力できます。ユーザは、Web認証プロセスを完了するために、自動的にコントローラに誘導されます。Webログインウィンドウが表示されたら、ユーザはユーザ名とパスワードを入力します。

FlexConnect イーサネットフォールバックの設定

FlexConnect イーサネットフォールバックについて

イーサネットリンクが機能しないときに無線をシャットダウンするように AP を設定できます。イーサネットリンクが使用可能状態に戻った場合、無線を使用可能状態に戻すように AP を設定できます。この機能は、接続されている AP に依存しない、またはスタンドアロンモードです。無線がシャットダウンすると、AP は WLAN をブロードキャストしないため、クライアントは最初のアソシエーションおよびローミングで AP に接続することができません。

FlexConnect イーサネットフォールバックの制約事項

- FlexConnectイーサネットフォールバックの設定はグローバルレベルで、すべてFlexConnect AP に適用できます。ただし、この機能は Cisco AP1130、AP1240、および AP1150 には適用されません。
- FlexConnect イーサネットフォールバック機能は、Cisco AP1520 や AP1550 などの複数のポートが使用されている AP には適用されません。
- イーサネットインターフェイスで設定するキャリア遅延は、ヒステリシスに基づいてインターフェイスをシャットダウンおよびリロードします。したがって、設定する遅延が、イーサネットおよび802.11インターフェイスがシャットダウンおよびリロードされる前の実際の遅延とは異なる場合があります。

FlexConnect イーサネットフォールバックの設定

始める前に

この機能は、複数のポートを持つ AP には適用されません。

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	**wireless profile flex** *flex-profile-name* 例： `Device(config)# wireless profile flex test`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**fallback-radio-shut** 例： `Device(config-wireless-flex-profile)# fallback-radio-shut`	無線インターフェイスのシャットダウンを有効にします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show wireless profile flex detailed** *flex-profile-name* 例： `Device# show wireless profile flex detailed test`	（任意）選択したプロファイルに関する詳細情報を表示します。

AP での flex AP ローカル認証（GUI）

手順

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

ステップ 2 [Flex] ページで、 flex プロファイルの名前をクリックするか、[Add] をクリックして新規に作成します。

ステップ 3 表示される [Add/Edit Flex Profle] ウィンドウで、[Local Authentication] タブをクリックします。

ステップ 4 [RADIUS Server Group] ドロップダウンリストからサーバグループを選択します。

ステップ 5 [AP Fast Profile] ドロップダウンリストからプロファイルを選択します。

ステップ 6 次を有効にするか無効にするかを選択します。

- [LEAP]：Lightweight Extensible Authentication Protocol（LEAP）は、ワイヤレス LAN 向けの 802.1X 認証タイプであり、クライアントと RADIUS サーバ間で、共有秘密としてログオンパスワードを使用した強力な相互認証をサポートします。LEAP では、ユーザ単位、セッション単位の動的な暗号化キーが提供されます。
- [PEAP]：Protected Extensible Authentication Protocol（PEAP）は、暗号化および認証された Transport Layer Security（TLS）トンネル内でExtensible Authentication Protocol（EAP）をカプセル化するプロトコルです。
- [TLS]：Transport Layer Security（TLS）は、コンピュータネットワーク経由での通信のセキュリティを提供する暗号化プロトコルです。
- [RADIUS]：Remote Authentication Dial-In User Service（RADIUS）は、ネットワークサービスに接続して使用するユーザに対して、一元化された認証、許可、およびアカウンティング（AAA またはトリプル A）の管理を提供するネットワーキングプロトコルです。

ステップ 7 [Users] セクションで、[Add] をクリックします。

ステップ 8 ユーザ名とパスワードの詳細を入力し、[Save] をクリックします。

ステップ 9 [Save & Apply to Device] をクリックします。

AP での flex AP ローカル認証（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 2	**aaa session-id common** 例： `Device(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。
ステップ 3	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御を有効にします。
ステップ 4	**eap profile** *name* 例： `Device(config)# eap profile aplocal-test`	EAP プロファイルを作成します。
ステップ 5	**method fast** 例： `Device(config-eap-profile)# method fast`	プロファイルで FAST 方式を設定します。
ステップ 6	**exit** 例： `Device(config-radius-server)# exit`	コンフィギュレーションモードに戻ります。
ステップ 7	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex default-flex-profile`	flex ポリシーを設定します。
ステップ 8	**local-auth ap eap-fast** *name* 例：	EAP-FAST プロファイルの詳細を設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-flex-profile)# local-auth ap eap-fast aplocal-test`	
ステップ 9	**local-auth ap leap** 例： `Device(config-wireless-flex-profile)# local-auth ap leap`	LEAP 方式を設定します。
ステップ 10	**local-auth ap peap** 例： `Device(config-wireless-flex-profile)# local-auth ap peap`	PEAP 方式を設定します。
ステップ 11	**local-auth ap username** *username* 例： `Device(config-wireless-flex-profile)# local-auth ap username test1 test1`	ユーザ名とパスワードを設定します。
ステップ 12	**local-auth ap username** *username password* 例： `Device(config-wireless-flex-profile)# local-auth ap username test2 test2`	別のユーザ名とパスワードを設定します。
ステップ 13	**exit** 例： `Device(config-wireless-flex-profile)# exit`	コンフィギュレーションモードに戻ります。
ステップ 14	**wireless profile policy** *policy-profile* 例： `Device(config)# wireless profile policy default-policy-profile`	プロファイルポリシーを設定します。
ステップ 15	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	ポリシープロファイルを無効にします。
ステップ 16	**no central authentication** 例： `Device(config)# no central authentication`	中央（コントローラ）認証を無効にします。
ステップ 17	**vlan-id** *vlan-id* 例： `Device(config)# vlan-id 54`	VLAN 名または VLAN ID を設定します。

	コマンドまたはアクション	目的
ステップ 18	**no shutdown** 例： `Device(config)# no shutdown`	設定をイネーブルにします。

外部 Radius サーバを使用した Flex AP ローカル認証

このモードでは、アクセスポイントがクライアント認証を処理し、クライアントデータパケットをローカルにスイッチングします。この状態はスタンドアロンモードおよび接続済みモードの場合に有効です。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 2	**aaa session-id common** 例： `Device(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。
ステップ 3	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御を有効にします。
ステップ 4	**radius server** *server-name* 例： `Device(config)# radius server Test-SERVER1`	RADIUS サーバ名を指定します。 （注） FreeRADIUS over RADSEC でクライアントを認証するには、1024 ビットよりも長い RSA キーを生成する必要があります。これを行うには、**crypto key generate rsa general-keys exportable label** *name* コマンドを使用します。
ステップ 5	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* } 例：	RADIUS サーバのプライマリパラメータを指定します。

	コマンドまたはアクション	目的
	`Device(config-radius-server)# address ipv4 124.3.50.62 auth-port 1112 acct-port 1113`	
ステップ 6	**key** *string* 例： `Device(config-radius-server)# key test123`	deviceと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 7	**radius server** *server-name* 例： `Device(config)# radius server Test-SERVER2`	RADIUS サーバ名を指定します。
ステップ 8	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* } 例： `Device(config-radius-server)# address ipv4 124.3.52.62 auth-port 1112 acct-port 1113`	RADIUS サーバのセカンダリパラメータを指定します。
ステップ 9	**key** *string* 例： `Device(config-radius-server)# key test113`	deviceと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 10	**exit** 例： `Device(config-radius-server)# exit`	コンフィギュレーションモードに戻ります。
ステップ 11	**aaa group server radius** *server-group* 例： `Device(config)# aaa group server radius aaa_group_name`	RADIUS サーバグループの識別を作成します。
ステップ 12	**exit** 例： `Device(config-sg-radius)# exit`	RADIUS サーバグループ コンフィギュレーション モードを終了します。
ステップ 13	**radius server** *server-name* 例： `Device(config)# radius server Test-SERVER1`	RADIUS サーバ名を指定します。
ステップ 14	**radius server** *server-name* 例：	RADIUS サーバ名を指定します。

	コマンドまたはアクション	目的
	`Device(config-radius-server)# radius server Test-SERVER2`	
ステップ 15	**exit** 例： `Device(config-radius-server)# exit`	RADIUS サーバ コンフィギュレーション モードを終了します。
ステップ 16	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex default-flex-profile`	新しい flex ポリシーを作成します。
ステップ 17	**local-auth radius-server-group** *server-group* 例： `Device(config-wireless-flex-profile)# local-auth radius-server-group aaa_group_name`	認証サーバグループ名を設定します。
ステップ 18	**exit** 例： `Device(config-wireless-flex-profile)# exit`	コンフィギュレーションモードに戻ります。
ステップ 19	**wireless profile policy** *policy-profile* 例： `Device(config)# wireless profile policy default-policy-profile`	WLANポリシープロファイルを設定します。
ステップ 20	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	ポリシープロファイルを無効にします。
ステップ 21	**no central authentication** 例： `Device(config-wireless-policy)# no central authentication`	中央（コントローラ）認証を無効にします。
ステップ 22	**vlan-id** *vlan-id* 例： `Device(config-wireless-policy)# vlan-id 54`	VLAN 名または VLAN ID を設定します。
ステップ 23	**no shutdown** 例：	設定をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# no shutdown`	

FlexConnect のための NAT-PAT

中央の DHCP サーバを使用してリモートサイト間でクライアントにサービスを提供する場合は、NAT-PAT を有効にする必要があります。

AP は、クライアントから着信するトラフィックを変換し、クライアントの IP アドレスを自身の IP アドレスに置き換えます。

（注） NAT と PAT を有効にするには、（**ipv4 dhcp required**）コマンドを使用して、ローカルスイッチング、中央の DHCP、および DHCP Required を有効にする必要があります。

WLAN またはリモート LAN 用の NAT-PAT の設定

WLAN の作成

WLAN を作成するには、ここに記載されている手順に従います。

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	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-demo 1 ssid-demo`	WLAN コンフィギュレーション サブモードを開始します。 • *wlan-name*：プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*：WLAN ID を入力します。範囲は 1 ～ 512 です。 • *SSID-name*：この WLAN に対する Service Set Identifier（SSID）を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。

	コマンドまたはアクション	目的
		（注） すでにWLANを設定している場合は、*wlan wlan-name* コマンドを入力します。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をシャットダウンします。
ステップ 4	**end** 例： `Device(config-wlan)# 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。

ワイヤレス プロファイル ポリシーと NAT-PAT の設定

ワイヤレス プロファイル ポリシーと NAT-PAT を設定するには、次の手順に従います。

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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy nat-enabled-policy`	NAT のポリシープロファイルを設定します。
ステップ 3	**no central switching** 例： `Device(config-wireless-policy)# no central switching`	WLAN をローカルスイッチング用に設定します。
ステップ 4	**ipv4 dhcp required** 例： `Device(config-wireless-policy)# ipv4 dhcp required`	WLAN の DHCP パラメータを設定します。
ステップ 5	**central dhcp** 例： `Device(config-wireless-policy)# central dhcp`	ローカルにスイッチされるクライアントの中央 DHCP を設定します。

	コマンドまたはアクション	目的
ステップ 6	**flex nat-pat** 例： `Device(config-wireless-policy)# flex nat-pat`	NAT-PAT を有効にします。
ステップ 7	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。
ステップ 8	**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。

ポリシープロファイルへの WLAN のマッピング

WLAN をポリシープロファイルにマッピングするには、次の手順に従います。

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	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy demo-tag`	ポリシータグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan wlan-demo policy nat-enabled-policy`	ポリシープロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# 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。

サイトタグの設定

サイトタグを設定するには、次の手順に従います。

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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site flex-site`	サイトタグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**no local-site** 例： `Device(config-site-tag)# no local-site`	アクセスポイントを FlexConnect モードに移行します。
ステップ 4	**end** 例： `Device(config-site-tag)# 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。

アクセスポイントへのポリシータグとサイトタグの付加

ポリシータグとサイトタグをアクセスポイントに付加するには、次の手順に従います。

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	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、ap-tag コンフィギュレーション モードを開始します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag demo-tag`	ポリシータグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag flex-site`	サイトタグを AP にマッピングします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-ap-tag)# 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。

FlexConnect のスプリットトンネリング

中央でスイッチされる WLAN に関連付けられた WAN リンクに接続するクライアントが、ローカルサイトに存在するデバイスにトラフィックを送信する必要がある場合は、そのトラフィックを CAPWAP 経由でコントローラに送信する必要があります。すると、同じトラフィックが CAPWAP 経由で、または何らかの帯域外の接続を利用してローカルサイトに送り返されます。

このプロセスでは WAN リンクの帯域幅が無駄に消費されます。この問題を回避するため、スプリットトンネリング機能を使用できます。これは、クライアントから送信されるトラフィックをパケットの内容に基づいて分類できるようにする機能です。一致するパケットはローカルでスイッチされ、残りのトラフィックは中央でスイッチされます。ローカルサイトに存在するデバイスの IP アドレスと一致するクライアントによって送信されるトラフィックを、ローカルでスイッチされるトラフィックとして分類し、残りのトラフィックを中央でスイッチされるトラフィックとして分類できます。

AP でローカルのスプリットトンネリングを設定するには、（**ipv4 dhcp required**）コマンドを使用して、WLAN で DCHP Required が有効になっていることを確認します。これにより、スプリット WLAN に関連付けられているクライアントが DHCP を使用できるようになります。

WLAN またはリモート LAN 用のスプリットトンネリングの設定

スプリットトンネリング用のアクセス コントロール リストの定義

スプリットトンネリング用のアクセス コントロール リスト（ACL）を定義するには、次の手順に従います。

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	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended split_mac_acl`	名前を使用して拡張 IPv4 アクセスリストを定義し、アクセス リスト コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**deny ip any host** *hostname* 例： `Device(config-ext-nacl)# deny ip any host 9.9.2.21`	トラフィックを中央でスイッチングできるようにします。
ステップ 4	**permit ip any any** 例： `Device(config-ext-nacl)# permit ip any any`	トラフィックをローカルでスイッチングできるようにします。
ステップ 5	**end** 例： `Device(config-ext-nacl)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

定義済み ACL への ACL ポリシーのリンク

定義した ACL に ACL ポリシーをリンクするには、次の手順に従います。

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	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex flex-profile`	flex プロファイルを設定し、flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**acl-policy** *acl policy name* 例： `Device(config-wireless-flex-profile)# acl-policy split_mac_acl`	ACL ポリシーを、定義した ACL 用に設定します。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

WLAN の作成

WLAN を作成するには、次の手順に従います。

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	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-demo 1 ssid-demo`	WLAN の名前と ID を指定します。 • *wlan-name*：プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*：WLAN ID を入力します。範囲は 1 ～ 512 です。 • *SSID-name*：この WLAN に対する Service Set Identifier（SSID）を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 4	**end** 例： `Device(config-wlan)# 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。

ワイヤレス プロファイル ポリシーとスプリット MAC ACL 名の設定

ワイヤレス プロファイル ポリシーとスプリット MAC ACL 名を設定するには、次の手順に従います。

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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy split-tunnel-enabled-policy`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**flex split-mac-acl** *split-mac-acl-name* 例： `Device(config-wireless-policy)# flex split-mac-acl split_mac_acl`	スプリットMAC ACL名を設定します。 （注） flex とポリシープロファイルのリンクには、同じACL名を使用する必要があります。
ステップ 4	**central switching** 例： `Device(config-wireless-policy)# central switching`	WLAN を中央スイッチング用に設定します。
ステップ 5	**central dhcp** 例： `Device(config-wireless-policy)# central dhcp`	中央でスイッチされるクライアント用に中央の DHCP を有効にします。
ステップ 6	**ipv4 dhcp required** 例： `Device(config-wireless-policy)# ipv4 dhcp required`	WLAN の DHCP パラメータを設定します。
ステップ 7	**ipv4 dhcp server** *ip_address* 例： `Device(config-wireless-policy)# ipv4 dhcp server 9.1.0.100`	DHCP サーバのオーバーライド IP アドレスを設定します。
ステップ 8	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。

ポリシープロファイルへの WLAN のマッピング

WLAN をポリシープロファイルにマッピングするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy split-tunnel-enabled-tag`	ポリシータグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan wlan-demo policy split-tunnel-enabled-policy`	ポリシープロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# 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。

サイト タグの設定

サイトタグを設定するには、次の手順に従います。

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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site flex-site`	サイトタグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**no local-site** 例： `Device(config-site-tag)# no local-site`	**Local site** はサイトタグでは設定しません。
ステップ 4	**flex-profile** *flex-profile-name* 例： `Device(config-site-tag)# flex-profile flex-profile`	flex プロファイルを設定します。
ステップ 5	**end** 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-site-tag)# end`	ンフィギュレーション モードを終了できます。

アクセスポイントへのポリシータグとサイトタグの付加

ポリシータグとサイトタグをアクセスポイントに付加するには、次の手順に従います。

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	**ap** *ethernet-mac-address* 例： `Device(config)# ap 188b.9dbe.6eac`	APを設定し、APタグ コンフィギュレーション モードを開始します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag split-tunnel-enabled-tag`	ポリシータグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag flex-site`	サイトタグをAPにマッピングします。
ステップ 5	**end** 例： `Device(config-ap-tag)# 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。

VLAN ベースの FlexConnect 用中央スイッチング

FlexConnectローカルスイッチングでは、VLAN定義がアクセスポイントで使用できない場合、対応するクライアントはトラフィックを通過させません。このシナリオは、AAA サーバがクライアント認証の一部として VLAN を返す場合に適用されます。

WLAN が flex でローカルにスイッチングされ、AP 側で VLAN が設定されている場合、トラフィックはローカルにスイッチングされます。AP で VLAN が定義されていない場合、VLAN はパケットをドロップします。

VLAN0 ベースの中央スイッチングが有効になっている場合、対応する AP はトンネリングを通じてトラフィックをコントローラに送り返します。その後、コントローラはトラフィックを対応する VLAN に転送します。

VLAN ベースの中央スイッチングの設定（GUI）

手順

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

ステップ 2 ポリシープロファイルの名前をクリックします。

ステップ 3 [Edit Policy Profile] ウィンドウで、次のタスクを実行します。

a) [Central Switching] を [Disabled] 状態に設定します。

b) [Central DHCP] を [Disabled] 状態に設定します。

c) [Central Authentication] を [Enabled] 状態に設定します。

ステップ 4 [Advanced] タブをクリックします。

ステップ 5 [AAA Policy] で、[Allow AAA Override] チェックボックスをオンにして、AAA オーバーライドを有効にします。

ステップ 6 [WLAN Flex Policy] で、[VLAN Central Switching] チェックボックスをオンにして、ポリシープロファイルで VLAN ベースの中央スイッチングを有効にします。

ステップ 7 [Update & Apply to Device] をクリックします。

VLAN ベースの中央スイッチングの設定（CLI）

VLAN ベースの中央スイッチングを設定するには、次の手順に従います。

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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	ワイヤレス ポリシー プロファイルを設定します。
ステップ 3	**no central switching** 例：	WLAN をローカルスイッチング用に設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# no central switching`	
ステップ 4	**no central dhcp** 例： `Device(config-wireless-policy)# no central dhcp`	ローカル DHCP モードを設定します。このモードでは、DHCP が AP で実行されます。
ステップ 5	**central authentication** 例： `Device(config-wireless-policy)# central authentication`	WLAN を中央認証用に設定します。
ステップ 6	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA ポリシーのオーバーライドを設定します。
ステップ 7	**flex vlan-central-switching** 例： `Device(config-wireless-policy)# flex vlan-central-switching`	VLANベースの中央スイッチングを設定します。
ステップ 8	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show wireless profile policy detailed** *default-policy-profile* 例： `Device# show wireless profile policy detailed default-policy-profile`	（任意）ポリシープロファイルの詳細情報を表示します。

FlexConnect の OfficeExtend アクセスポイント

Cisco OfficeExtend アクセス ポイント（OEAP）は、コントローラからリモートロケーションの Cisco AP へのセキュア通信を提供して、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。ホームオフィスにおけるユーザの使用感は、会社のオフィスとまったく同じです。アクセスポイントとコントローラの間の Datagram Transport Layer Security（DTLS）による暗号化は、すべての通信のセキュリティを最高レベルにします。

（注） コントローラ IP を、OEAP を使用したゼロタッチ展開用に事前に構成してください。他のすべてのホームユーザは、AP からローカル SSID を設定することで、同じアクセスポイントを使用して自宅用に接続できます。

OfficeExtend アクセスポイントの設定

OfficeExtend アクセスポイントを設定するには、次の手順に従います。

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	**wireless profile flex** *flex-profile-name* 例： `Device(config)# wireless profile flex test`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**office-extend** 例： `Device(config-wireless-flex-profile)# office-extend`	Flexconnect AP の OfficeExtend AP モードを有効にします。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 （注） flex プロファイルを作成した後、OEAP が flex connect モードであり、対応するサイトタグにマッピングされていることを確認します。 OfficeExtend は、デフォルトでは無効になっています。アクセスポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、コマンド Device# **clear ap config** *cisco-ap* を入力します。

OfficeExtend アクセスポイントの無効化

OfficeExtend アクセスポイントを無効にするには、次の手順に従います。

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	**wireless profile flex** *flex-profile-name* 例： `Device(config)# wireless profile flex test`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**no office-extend** 例： `Device(config-wireless-flex-profile)# no office-extend`	Flexconnect AP の OfficeExtend AP モードを無効にします。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

OfficeExtend アクセスポイントからの個人用 SSID のクリア

アクセスポイントから個人用 SSID をクリアするには、次のコマンドを実行します。

ap name *Cisco_AP* **clear-personal-ssid**

例：OfficeExtend 設定の表示

次に、OfficeExtend 設定を表示する例を示します。

```
Device# show ap config general

Cisco AP Name   : ap_name
================================================

Cisco AP Identifier                             : 70db.986d.a860
Country Code                                    : Multiple Countries : US,IN
Regulatory Domain Allowed by Country            : 802.11bg:-A   802.11a:-ABDN
AP Country Code                                 : US  - United States
AP Regulatory Domain
  Slot 0                                        : -A
  Slot 1                                        : -D
MAC Address                                     : 002c.c899.7b84
```

```
IP Address Configuration                        : DHCP
IP Address                                      : 9.9.48.51
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 9.9.48.1
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Disabled
SSH State                                       : Disabled
Jumbo MTU Status                                : Disabled
Cisco AP Location                               : default location
Site Tag Name                                   : flex-site
RF Tag Name                                     : default-rf-tag
Policy Tag Name                                 : split-tunnel-enabled-tag
AP join Profile                                 : default-ap-profile
Primary Cisco Controller Name                   : uname-controller
Primary Cisco Controller IP Address             : 9.9.48.34
Secondary Cisco Controller Name                 : uname-controller1
Secondary Cisco Controller IP Address           : 0.0.0.0
Tertiary Cisco Controller Name                  : uname-ewlc2
Tertiary Cisco Controller IP Address            : 0.0.0.0
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : FlexConnect
AP Submode                                      : Not Configured
Office Extend Mode                              : Enabled
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Software Version                                : 16.8.1.1
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 0
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power (normal mode)
```

プロシキ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネットホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカルイーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。Deviceが送信元と異なるネットワーク上にあるホストに宛てたARP要求を受信した場合、Deviceはそのホストへの最適なルートがあるかどうかを調べます。最適なルートがある場合、デバイスは自身のイーサネットMACアドレスが格納されたARP応答パケットを送信します。要求の送信元ホストはパケットをDeviceに送信し、スイッチは目的のホストにパケットを転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 要求を実行します。

AP は ARP プロキシとして動作し、ワイヤレスクライアントの代わりに ARP 要求に応答します。

FlexConnect AP 用のプロキシ ARP の有効化

FlexConnect AP 用にプロキシ ARP を設定するには、次の手順に従います。

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	**wireless profile flex** *flex-policy* 例： `Device(config)# wireless profile flex flex-test`	WLANポリシープロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**arp-caching** 例： `Device(config-wireless-flex-profile)# arp-caching`	ARP キャッシングを有効にします。 （注） ARP キャッシングを無効にするには、**no arp-caching** コマンドを使用します。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config | section wireless profile flex** 例： `Device# show running-config | section wireless profile flex`	ARP 設定情報を表示します。
ステップ 6	**show wireless profile flex detailed** *flex-profile-name* 例： `Device# show wireless profile flex detailed flex-test`	（任意）flexプロファイルの詳細情報を表示します。
ステップ 7	**show arp summary** 例： `Device# show arp summary`	（任意）ARPのサマリーを表示します。

合法的傍受

トラフィックの合法的傍受

シスコのワイヤレス ソリューションを使用すると、モニタリングを目的としてトラフィックの流れを合法的に傍受することが可能です。

シスコの AP がトラフィックに関する syslog レコードを作成し、そのレコードをコントローラに送信します。IPv4プロトコルとIPv6プロトコルの両方からのトラフィックが記録されます。AP は、設定された間隔で syslog レコードをコントローラに送信し、コントローラはそれらのレコードを AP から受信するとすぐに syslog サーバに転送します。

トラフィックの合法的傍受の制限

- IPv6 プロトコルをサポートするには、コントローラで IPv6 を有効にします。
- この機能は、Flex + Bridge モードで動作している Cisco Wave 2 AP と、Flex モードで動作している Cisco Wave 2 AP でサポートされます。
- Cisco Wave 2 AP をサポートします。

合法的傍受の設定

デフォルトでは、**lawful-interception** コマンドは無効になっています。コマンドを有効にするには、次の手順に従います。

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	**wireless lawful-interception host** {*ipv4 addr* | *ipv6 addr*} 例： `Device(config)# wireless lawful-interception host X:X:X:X::X`	コントローラで lawful-interception を有効にし、LI サーバの IP アドレスを設定します（IPv4 および IPv6 ホスト）。
ステップ 3	**ap profile** <*ap-profile-name*> 例： `Device(config)# ap profile ap-profile-name`	AP プロファイルを設定します。

	コマンドまたはアクション	目的
ステップ 4	**[no] lawful-interception** 例： `Device(config-ap-profile)# [no] lawful-interception`	合法的傍受機能を有効にします。この機能を無効にするには、このコマンドの**no**形式を使用します。デフォルトでは、合法的傍受機能は無効になっています。
ステップ 5	**lawful-interception timer** *timer-value* 例： `Device(config-ap-profile)#lawful-interception timer 70`	合法的傍受のレポート間隔を秒単位で設定します。デフォルトでは、タイマーは 60 秒です。

合法的傍受のステータスの確認

合法的傍受のステータスを確認するには、次の **show** コマンドを使用します。

```
Device#show wireless lawful-interception status
-------------------------------------------
Number AP profiles with LI enabled:     1
-------------------------------------------
Last Nexthop MAC address resolution state: Resolved
SRC IP address:             9.9.71.51
LI host IP address:         9.9.71.98
Ingress SRC MAC address:    0000.0002.0001
Egress SRC MAC address:     001e.7a9a.e9ff
Nexthop MAC address:        0050.56a0.80f4

--------------------------
LI Internal Data
--------------------------
Egress Vlan:     9
Plumb Ifid:      4026531841
Recent LI history (most recent on top):
Timestamp                          Event                          Context
-------------------------   -------------------------
---------------------------------06/21/2018 12:47:05.594163     NH_MAC_ADDR_RESULT
    next_hop mac:0050.56a0.80f4
06/21/2018 12:47:05.594081     CPP_PLUMB                  egress src
mac:001e.7a9a.e9ff,vlan:9
06/21/2018 12:47:05.593739     NH_MAC_ADDR_RESULT         next_hop mac:0050.56a0.80f4
06/21/2018 12:47:05.590337     CPP_UNPLUMB                egress src
mac:001e.7a9a.e9ff,vlan:9
06/21/2018 12:47:01.561553     NH_MAC_ADDR_RESULT         next_hop mac:0050.56a0.80f4
06/21/2018 12:47:01.555291     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:47:01.555060     MGMT_IF_CHANGE

06/21/2018 12:47:00.618530     CPP_PLUMB                  egress src
mac:001e.7a9a.e9ff,vlan:9
06/21/2018 12:47:00.607985     MAGIC_MAC_RESOLVED         0000.0002.0001
06/21/2018 12:47:00.607290     MAGIC_MAC_REQ

06/21/2018 12:47:00.606344     NH_MAC_ADDR_RESULT         next_hop mac:0050.56a0.80f4
06/21/2018 12:47:00.601806     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:47:00.600603     MGMT_IF_CHANGE

06/21/2018 12:46:55.847387     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
```

```
9.9.71.98
06/21/2018 12:46:55.847094     MGMT_IF_CHANGE

06/21/2018 12:46:54.937173     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:46:54.936310     MGMT_IF_CHANGE

06/21/2018 12:46:53.186883     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:46:53.134721     MGMT_IF_CHANGE

06/21/2018 12:46:52.965403     MGMT_IF_CHANGE
```

特定の AP で合法的傍受が有効になっているかどうかを確認するには、次の **show** コマンドを使用します。

```
show ap name <ap_name> config general | include Lawful-Interception
Lawful-Interception Admin status               : Enabled
Lawful-Interception Oper status                : Enabled
```