



システム設定

- [新しい設定モデルについて](#) (1 ページ)
- [ワイヤレス プロファイル ポリシーの設定 \(GUI\)](#) (4 ページ)
- [ワイヤレス プロファイル ポリシーの設定 \(CLI\)](#) (5 ページ)
- [flex プロファイルの設定](#) (6 ページ)
- [AP プロファイルの設定 \(GUI\)](#) (7 ページ)
- [AP プロファイルの設定 \(CLI\)](#) (12 ページ)
- [RF プロファイルの設定 \(GUI\)](#) (13 ページ)
- [RF プロファイルの設定 \(CLI\)](#) (14 ページ)
- [サイト タグの設定 \(GUI\)](#) (15 ページ)
- [サイト タグの設定 \(CLI\)](#) (15 ページ)
- [ポリシー タグの設定 \(GUI\)](#) (16 ページ)
- [ポリシー タグの設定 \(CLI\)](#) (17 ページ)
- [ワイヤレス RF タグの設定 \(GUI\)](#) (18 ページ)
- [ワイヤレス RF タグの設定 \(CLI\)](#) (18 ページ)
- [AP へのポリシー タグとサイト タグの付加 \(GUI\)](#) (19 ページ)
- [AP へのポリシー タグとサイト タグの付加 \(CLI\)](#) (19 ページ)
- [AP フィルタ](#) (21 ページ)
- [ロケーション設定でのアクセスポイントの設定](#) (24 ページ)

新しい設定モデルについて

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、さまざまなタグ (rf タグ、ポリシー タグ、サイト タグ) を使用して、ワイヤレス コントローラ の設定を簡素化します。アクセス ポイントでは、タグ内に含まれているプロファイルから設定が導出されます。

プロファイルは、特定のターゲットに適用される機能固有の属性とパラメータの集まりです。設定のターゲットとなるのは、AP、無線、および WLAN です。rf タグには無線プロファイル、サイトタグには flex-profile と ap-join-profile、ポリシータグには WLAN プロファイルとポリシープロファイルがそれぞれ含まれています。

新しい設定モデル（flexconnectモード）は、たとえば小売店舗やキャンパスなど、WLANが同じである地理的に分散したサイトを中央のコントローラで管理するのに役に立ちます。ローカルの展開またはトポロジに基づいてネットワークと無線のプロファイルに多少の変更が生じるだけです。

ポリシータグ

ポリシータグは、WLANプロファイルからポリシープロファイルへのマッピングを構成します。WLANプロファイルは、WLANの無線特性を定義します。ポリシープロファイルは、クライアントのネットワークポリシーとスイッチングポリシーを定義します（APポリシーも構成するQuality of Service（QoS）は除きます）。

ポリシータグにはWLANポリシープロファイルのマッピングが含まれています。ポリシータグごとに、このようなエントリが最大16個存在するマップエントリの変更は、WLANプロファイルとポリシープロファイルのステータスに基づいて影響を受けます。たとえば、マップ（WLAN1およびPolicy1）がポリシータグに追加された場合、WLANプロファイルとポリシープロファイルの両方が有効になっていると、その定義がポリシータグを使用してAPにプッシュされます。ただし、これらのいずれかが無効状態になっている場合には、定義はAPにプッシュされません。同様に、WLANプロファイルがすでにAPによってブロードキャストされている場合は、ポリシータグでコマンドのno形式を使用して削除できます。

サイトタグ

サイトタグはサイトのプロパティを定義するもので、flexプロファイルとAP joinプロファイルが含まれています。対応するflexまたはリモートサイトに固有の属性は、flexプロファイルの一部となります。flexプロファイルとは別に、サイトタグは物理サイトに固有の属性も構成します（そのため、再利用可能なエンティティであるプロファイルの一部にすることはできません）。たとえば、効率的なアップグレードのためのマスターAPのリストは、flexプロファイルの一部ではなくサイトタグの一部となります。

flexプロファイル名またはAPプロファイル名がサイトタグで変更された場合、APは、Datagram Transport Layer Security（DTLS）セッションを切断することによってコントローラへの再参加を強制されます。サイトタグが作成されると、APプロファイルとflexプロファイルはデフォルト値（default-ap-profileとdefault-flex-profile）に設定されます。

RFタグ

RFタグにはIEEE 802.11aおよびIEEE 802.11bのRFプロファイルが含まれています。デフォルトのRFタグにはグローバル設定が含まれています。どちらのプロファイルにも、それぞれの無線についてグローバルRFプロファイルの同じデフォルト値が含まれています。

プロファイル

プロファイルは、特定のターゲットに適用される機能固有の属性とパラメータの集まりです。設定のターゲットとなるのは、AP、無線、およびWLANです。プロファイルは、タグ全体で使用できる再利用可能なエンティティです。プロファイル（タグで使用されます）は、APまたはそれに関連付けられているクライアントのプロパティを定義します。

WLAN プロファイル

WLAN プロファイルは、同じまたは異なるサービスセット識別子 (SSID) で設定されます。SSIDは、コントローラがアクセスするための特定の無線ネットワークを識別します。同じ SSID で WLAN を作成すると、同じ無線 LAN 内で異なるレイヤ 2 セキュリティ ポリシーを割り当てることができます。

同じ SSID を持つ WLAN を区別するには、各 WLAN に対して一意のプロファイル名を作成します。同じ SSID を持つ WLAN には、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーが設定されている必要があります。スイッチング ポリシーとネットワーク ポリシーは WLAN 定義の一部ではありません。

ポリシー プロファイル

ポリシー プロファイルは、広義にはネットワーク ポリシーとスイッチング ポリシーで構成されます。ポリシー プロファイルはタグ全体にわたって再利用可能なエンティティです。AP またはコントローラに適用されるクライアントのポリシーとなっているものはすべて、ポリシー プロファイルに移動されます。たとえば、VLAN、ACL、QoS、セッションタイムアウト、アイドルタイムアウト、AVC プロファイル、bonjour プロファイル、ローカルプロファイリング、デバイス分類、BSSID QoS などが該当します。ただし、WLAN のワイヤレス関連のセキュリティ属性と機能はすべて、WLAN プロファイルの配下にグループ化されます。

flex プロファイル

flex プロファイルには、flex グループの一部となっている属性が含まれています。ただし、ポリシー属性はポリシープロファイルとともにグループ化されます。flex プロファイルにはリモートサイト固有のパラメータも含まれています。たとえば、EAP プロファイル (AP がローカル RADIUS サーバ情報の認証サーバとして機能する場合に使用可能)、VLAN と ACL のマッピング、VLAN 名と ID のマッピングなどです。

AP join プロファイル

デフォルトの AP join プロファイルの値には、グローバル AP パラメータと AP グループ パラメータが設定されます。AP join プロファイルには、CAPWAP、IPv4 および IPv6、UDP Lite、ハイ アベイラビリティ、再送信設定パラメータ、グローバル AP フェールオーバー、HyperLocation 設定パラメータ、Telnet および SSH、11u パラメータなどのパラメータが含まれています。



(注) Telnet は次の Cisco AP モデルではサポートされていません。1542D、1542I、1562D、1562E、1562I、1562PS、1800S、1800T、1810T、1810W、1815M、1815STAR、1815TSN、1815T、1815T、1815W、1832I、1840I、1852E、1852I、2802E、2802I、2802H、3700C、3800、3802E、3802I、3802P、4800、9115AXI、9115AXE、9117I、APVIRTUAL、9120AXE、および 9120AXI。

RF プロファイル

RF プロファイルには、AP の共通の無線設定が含まれています。RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。

AP の静的な関連付け

AP を静的に設定できるのは、ポリシータグ、サイトタグ、および RF タグを使用した場合のみです。AP はイーサネット MAC アドレスによって識別され、AP およびタグへの関連付けは設定としてコントローラに保存されます。

AP タグの変更

AP タグを変更すると、DTLS 接続がリセットされ、AP が強制的にコントローラに再参加します。設定でタグが1つだけ指定されている場合は、他のタイプにデフォルトタグが使用されます。たとえば、ポリシータグのみが指定されている場合は、サイトタグと RF タグに対して default-site-tag と default-rf-tag が使用されます。

ワイヤレス プロファイル ポリシーの設定 (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、[Add] をクリックします。
- ステップ 3 [Add Policy Profile] ウィンドウの [General] タブで、ポリシー プロファイルの名前と説明を入力します。
- ステップ 4 ポリシー プロファイルを有効にするには、[Status] を [Enabled] に設定します。
- ステップ 5 スライダを使用して、[Passive Client] と [Encrypted Traffic Analytics] を有効または無効にします。
- ステップ 6 [CTS Policy] セクションで、次について適切なステータスを選択します。
 - [Inline Tagging] : コントローラまたはアクセスポイントが送信元 SGT を認識するために使用するトランスポートメカニズム。
 - [SGACL Enforcement]
- ステップ 7 デフォルトの SGT を指定します。有効な範囲は 2 ~ 65519 です。
- ステップ 8 [WLAN Switching Policy] セクションで、必要に応じて次を選択します。
 - [No Central Switching]
 - [Central Authentication]
 - [No Central DHCP]

- [Central Association Enable]
- [Flex NAT/PAT]

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

ワイヤレス プロファイル ポリシーの設定 (CLI)

ワイヤレス プロファイル ポリシーを設定するには、次の手順に従います。



- (注) クライアントが古いコントローラから新しいコントローラ (Prime Infrastructure により管理されている) に移動すると、IP アドレスが ARP またはデータ グリーニングによって学習されている場合は、クライアントの古い IP アドレスが保持されます。このシナリオを回避するには、ポリシープロファイルで **ipv4 dhcp required** コマンドを有効にします。そうしない場合は、24 時間後にならないと IP アドレスが更新されません。

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 policy <i>profile-policy</i> 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	idle-timeout <i>timeout</i> 例 : Device (config-wireless-policy)# idle-timeout 1000	(任意) アイドル タイムアウト時間を秒単位で設定します。
ステップ 4	vlan <i>vlan-id</i> 例 : Device (config-wireless-policy)# vlan 24	VLAN 名または VLAN ID を設定します。
ステップ 5	accounting-list <i>list-name</i> 例 : Device (config-wireless-policy)# accounting-list user1-list	IEEE 802.1x のアカウントリングリストを設定します。

	コマンドまたはアクション	目的
ステップ 6	no shutdown 例： Device(config-wireless-policy)# no shutdown	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 wireless profile policy summary 例： Device# show wireless profile policy summary	設定されたポリシー プロファイルを表示します。 (注) (任意) ポリシー プロファイルに関する詳細情報を表示するには、 show wireless profile policy detailed <i>policy-profile-name</i> コマンドを使用します。

flex プロファイルの設定

Flex プロファイルを設定するには、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 <i>flex-profile</i> 例： Device(config)# wireless profile flex rr-xyz-flex-profile	RFプロファイルを設定し、RF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	description 例： Device(config-wireless-flex-profile)# description xyz-default-flex-profile	(任意) RF プロファイルのデフォルトパラメータを有効にします。
ステップ 4	arp-caching 例： Device(config-wireless-flex-profile)# arp-caching	(任意) ARP キャッシングを有効にします。

	コマンドまたはアクション	目的
ステップ 5	end 例 : Device(config-wireless-flex-profile)# 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 6	show wireless profile flex summary 例 : Device# show wireless profile flex summary	(任意) flex プロファイルパラメータを表示します。 (注) flex プロファイルに関する詳細なパラメータを表示するには、 show wireless profile flex detailed flex-profile-name コマンドを使用します。

AP プロファイルの設定 (GUI)

始める前に

デフォルトの AP join プロファイルの値には、グローバル AP パラメータと AP グループパラメータが設定されます。AP join プロファイルには、CAPWAP IPv4/IPv6、UDP Lite、ハイアベイラビリティ、再送信設定パラメータ、グローバル AP フェールオーバー、HyperLocation 設定パラメータ、Telnet/SSH、11u パラメータなどのパラメータが含まれています。

手順

-
- ステップ 1** [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。
- ステップ 2** [AP Join Profile] ページで、[Add] をクリックします。
[Add AP Join Profile] ページが表示されます。
- ステップ 3** [General] タブで、AP join プロファイルの名前と説明を入力します。
- ステップ 4** AP を簡単に探せるように、デバイスに接続されているすべての AP の LED 状態を点滅に設定するには、[LED State] チェックボックスをオンにします。
- ステップ 5** [Client] タブの [Statistics Timer] セクションに、AP が自身の 802.11 統計情報をコントローラに送信する時間を秒単位で入力します。
- ステップ 6** [TCP MSS Configuration] セクションで、[Adjust MSS Enable] チェックボックスをオンにして、[Adjust MSS] の値を入力します。ルータを通過する一時的なパケットの最大セグメントサイズ (MSS) を入力または更新できます。TCP MSS の調整により、ルータを通過する一時的なパケット (特に SYN ビットが設定された TCP セグメント) の最大セグメントサイズ (MSS) を設定できます。

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP ディスカバリ メカニズムを使用してデバイスを検知してから、デバイスに CAPWAP join 要求を送信します。デバイスは、アクセス ポイントがデバイスに join することを許可する CAPWAP join 応答をアクセス ポイントに送信します。

アクセス ポイントがデバイスに参加すると、デバイスによってアクセス ポイントの設定、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。

ステップ 7 [CAPWAP] タブでは次の設定が行えます。

- ハイ アベイラビリティ

すべてのアクセスポイントのプライマリおよびセカンダリバックアップコントローラを、プライマリ、セカンダリ、ターシャリ、プライマリバックアップ、セカンダリバックアップの順序で設定できます (プライマリ、セカンダリ、またはターシャリコントローラが応答しない場合に使用されます)。また、ハートビート タイマーやディスカバリ要求タイマーなどのさまざまなタイマーを設定できます。コントローラの障害検出時間を短縮するには、高速ハートビート間隔 (コントローラとアクセスポイントの間) に設定するタイムアウト値をより小さくします。高速ハートビートタイマーの期限 (ハートビート間隔ごとの) を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラへ送信します。

- [High Availability] タブで、[Fast Heartbeat Timeout] フィールドに時間 (秒単位) を入力して、すべてのアクセスポイントのハートビートタイマーを設定します。ハートビート間隔の値を小さく指定すると、デバイスの障害検出にかかる時間が短縮されます。
- [Heartbeat Timeout] フィールドに時間 (秒単位) を入力して、すべてのアクセスポイントのハートビートタイマーを設定します。ハートビート間隔の値を小さく指定すると、デバイスの障害検出にかかる時間が短縮されます。
- [Discovery Timeout] フィールドに 1 ~ 10 秒の範囲 (両端を含む) の値を入力して、AP ディスカバリ要求タイマーを設定します。
- [Primary Discovery Timeout] フィールドに 30 ~ 3000 秒の範囲 (両端を含む) の値を入力して、アクセスポイントのプライマリ ディスカバリ要求タイマーを設定します。
- [Primed Join Timeout] フィールドに 120 ~ 43200 秒の範囲 (両端を含む) の値を入力して、アクセスポイントのプライマリ join タイムアウトを設定します。
- [Retransmit Timers Count] フィールドに、AP からデバイスに (またはその逆に) 要求を再送信する回数を入力します。有効な範囲は、3 ~ 8 です。
- [Retransmit Timers Interval] フィールドに、要求の再送信から次の再送信までの時間を入力します。有効な範囲は、2 ~ 5 です。
- フォールバックを有効にするには、[Enable Fallback] チェックボックスをオンにします。
- [Primary Controller] の名前と IP アドレスを入力します。
- [Secondary Controller] の名前と IP アドレスを入力します。
- [Save & Apply to Device] をクリックします。

- 高度

- a) [Advanced] タブで、[Enable VLAN Tagging] チェックボックスをオンにして、VLAN のタグ付けを有効にします。
- b) [Enable Data Encryption] チェックボックスをオンにして、データグラム トランスポート層セキュリティ (DTLS) データ暗号化を有効にします。
- c) [Enable Jumbo MTU] をオンにして、大きい最大伝送ユニット (MTU) を有効にします。MTU とは、ネットワークが送信できる最大の物理パケット サイズのことで、バイト単位で測定されます。MTU よりも大きなメッセージは送信前に小さなパケットに分割されます。ジャンボフレームとは、標準のイーサネットフレーム サイズである 1518 バイト (レイヤ 2 (L2) ヘッダーと FCS を含む) より大きいフレームのことです。フレームサイズの定義は IEEE 標準の一部ではないため、ベンダーによって異なります。
- d) [Link Latency] ドロップダウン リストを使用して、リンク遅延を選択します。リンク遅延は、AP からコントローラ、およびコントローラから AP における CAPWAP ハートビートパケット (エコー要求および応答) のラウンドトリップ時間をモニタします。
- e) [Preferred Mode] ドロップダウン リストからモードを選択します。
- f) [Save & Apply to Device] をクリックします。

ステップ 8 [AP] タブでは次の設定が行えます。

- 一般

- a) [General] タブで、[Switch Flag] チェックボックスをオンにしてスイッチを有効にします。
- b) パワーインジェクタが使用されている場合は、[Power Injector State] チェックボックスをオンにします。パワーインジェクタにより、ローカル電源、インラインパワー対応のマルチポートスイッチ、およびマルチポート電源パッチパネルに代替電源のオプションが提供され、AP の無線 LAN 配置の柔軟性が向上します。
- c) [Power Injector Type] ドロップダウン リストで、次のオプションからパワー インジェクタタイプを選択します。
 - [Installed] : 現在接続されているスイッチ ポートの MAC アドレスを AP に調べさせ記憶させる場合に使用します (この選択は、パワーインジェクタが接続されていることを前提としています) 。
 - [Override] : 最初に MAC アドレスの一致を検証せずに、AP が高電力モードで稼働できるようにします。
- d) [Injector Switch MAC] フィールドに、スイッチの MAC アドレスを入力します。
- e) 関連する国コードを入力します。特定の運用国を国コードで指定できます (フランスは FR、スペインは ES など) 。
- f) [EAP Type] ドロップダウン リストから、EAP タイプとして [EAP-FAST]、[EAP-TLS]、または [EAP-PEAP] を選択します。
- g) [AP Authorization Type] ドロップダウン リストから、タイプとして [CAPWAP DTLS +] または [CAPWAP DTLS] のいずれかを選択します。
- h) [Client Statistics Reporting Interval] セクションに、5 GHz および 2.4 GHz の無線の間隔を秒単位で入力します。
- i) 拡張モジュールを有効にするには [Enable] チェックボックスをオンにします。
- j) [Profile Name] ドロップダウン リストから、メッシュのプロファイル名を選択します。

- k) [Save & Apply to Device] をクリックします。
- HyperLocation : Cisco Hyperlocation は、ワイヤレス クライアントの場所を 1 メートルの精度で追跡できるロケーション ソリューションです。このオプションを選択すると、NTP サーバを除く画面内の他のすべてのフィールドが無効になります。
- a) [Hyperlocation] タブで、[Enable Hyperlocation] チェックボックスをオンにします。
- b) 低い RSSI を持つパケットを除外するには、[Detection Threshold] の値を入力します。有効な範囲は -100 ~ -50 dBm です。
- c) BAR をクライアントに送信する前のスキャン サイクルの数を設定するには、[Trigger Threshold] の値を入力します。有効な範囲は 0 ~ 99 です。
- d) トリガー後にスキャン サイクルの値をリセットするには、[Reset Threshold] の値を入力します。有効な範囲は 0 ~ 99 です。
- e) [NTP Server] の IP アドレスを入力します。
- f) [Save & Apply to Device] をクリックします。
- BLE : AP が Bluetooth Low Energy (BLE) 対応の場合はビーコンメッセージを送信できます。ビーコンメッセージは、低電力リンクを介して送信されるデータまたは属性のパケットです。これらの BLE ビーコンは、ヘルス モニタリング、プロキシミティ検出、アセット トラッキング、およびストア内ナビゲーションに頻繁に使用されます。AP ごとに、すべての AP に対してグローバルに設定される BLE ビーコン設定をカスタマイズできます。
- a) [BLE] タブで、[Beacon Interval] フィールドに値を入力して、AP が近くにあるデバイスにビーコンアダプタイズメントを送出する頻度を指定します。範囲は 1 ~ 10 です。デフォルトは 1 です。
- b) [Advertised Attenuation Level] フィールドに、減衰レベルを入力します。範囲は 40 ~ 100 で、デフォルトは 59 です。
- c) [Save & Apply to Device] をクリックします。
- パケット キャプチャ : パケット キャプチャ機能では、ワイヤレス クライアントのトラブルシューティングを行うために AP 上のパケットをキャプチャできます。パケットキャプチャ操作は、指定されたパケットキャプチャフィルタに基づいて、AP が動作している現在のチャンネルの無線ドライバによって、AP 上で実行されます。
- a) [Packet Capture] タブで、ドロップダウン リストから [AP Packet Capture Profile] を選択します。
- b) または、[+] 記号をクリックして新しいプロファイルを作成することもできます。
- c) AP パケット キャプチャ プロファイルの名前および説明を入力します。
- d) [Buffer Size] を入力します。
- e) [Duration] を入力します。
- f) [Truncate Length] の情報を入力します。
- g) [Server IP] フィールドに、TFTP サーバの IP アドレスを入力します。
- h) [File Path] フィールドに、ディレクトリパスを入力します。
- i) ユーザ名とパスワードの詳細を入力します。
- j) [Password Type] ドロップダウン リストから、タイプを選択します。

- k) [Packet Classifiers] セクションで、オプションを使用して、キャプチャするパケットを選択または入力します。
- l) [Save] をクリックします。
- m) [Save & Apply to Device] をクリックします。

ステップ 9 [Management] タブでは次の設定が行えます。

- デバイス

- a) [Device] タブで、TFTP サーバの [TFTP Downgrade] セクションの [IPv4/IPv6 Address] を入力します。
- b) [Image File Name] フィールドに、ソフトウェア イメージファイルの名前を入力します。
- c) [Facility Value] ドロップダウン リストから、適切な機能を選択します。
- d) ホストの IPv4 または IPv6 アドレスを入力します。
- e) 適切な [Log Trap Value] を選択します。
- f) 必要に応じて、Telnet か SSH またはその両方の設定を有効にします。
- g) 必要に応じて、コア ダンプを有効にします。
- h) [Save & Apply to Device] をクリックします。

- ユーザ

- a) [User] タブで、ユーザ名とパスワードの詳細を入力します。
- b) 適切なパスワード タイプを選択します。
- c) [Secret] フィールドに、カスタムのシークレット コードを入力します。
- d) 適切なシークレット タイプを選択します。
- e) 適切な暗号化タイプを選択します。
- f) [Save & Apply to Device] をクリックします。

- クレデンシャル

- a) [Credentials] タブで、ローカルのユーザ名とパスワードの詳細を入力します。
- b) 適切なローカルパスワードタイプを選択します。
- c) 802.1x ユーザ名とパスワードの詳細を入力します。
- d) 適切な 802.1x パスワードタイプを選択します。
- e) セッションが期限切れになるまでの時間を秒単位で入力します。
- f) 必要に応じて、ローカルクレデンシャルや 802.1 x クレデンシャルを有効にします。
- g) [Save & Apply to Device] をクリックします。

- CDP インターフェイス

- a) [CDP Interface] タブで、必要に応じて CDP の状態を有効にします。
- b) [Save & Apply to Device] をクリックします。

ステップ 10 不正検出を有効にするには、[Rogue AP] タブで [Rogue Detection] チェックボックスをオンにします。

ステップ 11 [Rogue Detection Minimum RSSI] フィールドに、RSSI 値を入力します。

- ステップ 12 [Rogue Detection Transient Interval] フィールドに、一時的な間隔の値を入力します。
- ステップ 13 [Rogue Detection Report Interval] フィールドに、レポート間隔の値を入力します。
- ステップ 14 不正な封じ込めの自動レート選択を有効にするには、[Rogue Containment Automatic Rate Selection] チェックボックスをオンにします。
- ステップ 15 [Auto Containment on FlexConnect Standalone] チェックボックスをオンにして、この機能を有効にします。
- ステップ 16 [Save & Apply to Device] をクリックします。

AP プロファイルの設定 (CLI)

AP プロファイルを設定するには、次の手順に従います。

始める前に



- (注) コントローラの AP join プロファイルを変更した場合、NTP サーバの IP は AP にプッシュされません。これは、HyperLocation 機能の時間感度に対応するために AP プロファイル固有の NTP サーバ IP が導入され、HyperLocation の動作ステータスが Up の場合にのみ AP にプッシュされるためです。この動作は、すべての HyperLocation 関連の TLV (トリガーしきい値、リセットしきい値、および検出しきい値) に適用されます。

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 profile ap-profile 例： Device(config)# ap profile xyz-ap-profile	AP プロファイルを設定し、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) 名前付きプロファイルを削除した場合、そのプロファイルに関連付けられていた AP はデフォルトプロファイルに戻らなくなります。
ステップ 3	description ap-profile-name 例：	AP プロファイルの説明を追加します。

	コマンドまたはアクション	目的
	Device(config-ap-profile)# description "xyz ap profile"	
ステップ 4	cdp 例： Device(config-ap-profile)# cdp	すべての Cisco AP について CDP を有効にします。
ステップ 5	end 例： Device(config-ap-profile)# 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 6	show ap profile profile-namesummary 例： Device# show ap profile xyz-ap-profile summary	(任意) AP join プロファイルの数を表示します。 (注) AP join プロファイルに関する詳細情報を表示するには、 show ap profile profile-namedetailed コマンドを使用します。

RF プロファイルの設定 (GUI)

始める前に

プライマリコントローラとバックアップコントローラを設定する前に、AP Join プロファイルがすでに設定済みであることを確認します。

手順

-
- ステップ 1 [Configuration] > [Tags & Profiles] > [RF] を選択します。
 - ステップ 2 [RF Profile] ページで、[Add] をクリックします。
 - ステップ 3 [General] タブで、RF プロファイルの名前を入力します。
 - ステップ 4 適切な [Radio Band] を選択します。
 - ステップ 5 プロファイルを有効にするには、ステータスを [Enable] に設定します。
 - ステップ 6 RF プロファイルの [Description] を入力します。
 - ステップ 7 [Save & Apply to Device] をクリックします。
-

RF プロファイルの設定 (CLI)

RF プロファイルを設定するには、次の手順に従います。

始める前に

ワイヤレス RF タグを同時に設定する場合は、ここで作成したものと同一 RF プロファイル名を使用してください。RF プロファイル名に不一致がある場合（たとえば、RF タグに存在しない RF プロファイルが含まれている場合など）、対応する無線は起動しません。

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	ap dot11 24ghz rf-profile rf-profile 例： Device(config)# ap dot11 24ghz rf-profile rfprof24_1	RF プロファイルを設定し、RF 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	default 例： Device(config-rf-profile)# default	(任意) RF プロファイルのデフォルト パラメータを有効にします。
ステップ 4	no shutdown 例： Device(config-rf-profile)# no shutdown	デバイスで RF プロファイルを有効にします。
ステップ 5	end 例： Device(config-rf-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 6	show ap rf-profile summary 例： Device# show ap rf-profile summary	(任意) 使用可能な RF プロファイルのサマリーを表示します。
ステップ 7	show ap rf-profile name rf-profile detail 例： Device# show ap rf-profile name rfprof24_1 detail	(任意) 特定の RF プロファイルに関する詳細情報を表示します。

サイトタグの設定 (GUI)

手順

- ステップ1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。
- ステップ2 [Manage Tags] ページで、[Site] タブをクリックします。
- ステップ3 [Add] をクリックして、[Add Site Tag] ウィンドウを表示します。
- ステップ4 サイトタグの名前と説明を入力します。
- ステップ5 サイトタグに付加する必要がある [AP Join Profile] を選択します。
- ステップ6 必要に応じて、必要な [Control Plane Name] を選択します。
- ステップ7 必要に応じて、[Local Site] を有効にします。
- ステップ8 [Save & Apply to Device] をクリックします。

サイトタグの設定 (CLI)

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 <i>site-name</i> 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 <i>flex-profile-name</i> 例： Device(config-site-tag)# flex-profile rr-xyz-flex-profile	flex プロファイルを設定します。 (注) サイトタグでローカルサイトが設定されている場合、flex プロファイル設定をサイトタグから削除することはできません。

	コマンドまたはアクション	目的
		(注) サイトタグを Flexconnect として設定するには、 no local-site コマンドを使用する必要があります。そうしないと flex プロファイル設定が有効になりません。
ステップ 4	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 5	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 6	show wireless tag site summary 例： Device# show wireless tag site summary	(任意) サイトタグの数を表示します。 (注) タグに関する詳細情報を表示するには、 show wireless tag site detailed site-tag-name コマンドを使用します。 (注) サイトタグとポリシータグの両方が設定されていない場合、 show wireless loadbalance tag affinity wncd wncd-instance-number コマンドの出力にはデフォルトタグ (サイトタグ) タイプが表示されます。

ポリシー タグの設定 (GUI)

手順

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

ステップ 2 [Add] をクリックして、[Add Policy Tag] ウィンドウを表示します。

ステップ 3 ポリシー タグの名前と説明を入力します。

ステップ 4 [Add] をクリックして、WLAN とポリシーをマッピングします。

ステップ5 適切なポリシープロファイルを使用してマッピングする WLAN プロファイルを選択し、チェックアイコンをクリックします。

ステップ6 [Save & Apply to Device] をクリックします。

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 default-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。

ワイヤレス RF タグの設定 (GUI)

手順

- ステップ 1 a) [Configuration] > [Tags & Profiles] > [RF] > > > を選択します。
- ステップ 2 [Add] をクリックして、[Add RF Tag] ウィンドウを表示します。
- ステップ 3 RF タグの名前と説明を入力します。
- ステップ 4 RF タグに関連付ける、必要な [5 GHz Band RF Profile] および [2.4 GHz Band RF Profile] を選択します。
- ステップ 5 [Update & Apply to Device] をクリックします。

ワイヤレス RF タグの設定 (CLI)

ワイヤレス RF タグを設定するには、次の手順に従います。

始める前に

- RF タグでは 2 つのプロファイル (IEEE 802.11a および IEEE 802.11b) のみを使用できます。
- AP タグ タスクを設定するときに作成したものと同一 AP タグ名を使用してください。

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 rf rf-tag 例： Device(config)# wireless tag rf rftag1	RF タグを作成し、ワイヤレス RF 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	24ghz-rf-policy rf-policy 例： Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1	RF タグに IEEE 802.11b RF ポリシーを付加します。 dot11a ポリシーを設定するには、 5ghz-rf-policy コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	description <i>policy-description</i> 例 : Device (config-wireless-rf-tag) # description Test	RF タグの説明を追加します。
ステップ 5	end 例 : Device (config-wireless-rf-tag) # 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 6	show wireless tag rf summary 例 : Device# show wireless tag rf summary	使用可能な RF タグを表示します。
ステップ 7	show wireless tag rf detailed <i>rf-tag</i> 例 : Device# show wireless tag rf detailed rftag1	特定の RF タグの詳細情報を表示します。

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、ネットワーク上にあるすべての 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) <i>mac-address</i> 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： Device(config-ap-tag)# site-tag rr-xyz-site	サイトタグを AP にマッピングします。
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。

AP フィルタ

AP フィルタの概要

Cisco Catalyst 9800 シリーズワイヤレスコントローラの新しい設定モデルでタグが導入され、タグをアクセスポイント（AP）に関連付けるための複数のソースが作成されました。タグソースは、スタティック設定、AP フィルタエンジン、AP 単位の PNP、またはデフォルトのタグソースにすることができます。これに加えて、タグの優先順位も重要な役割を果たします。AP フィルタ機能は、シームレスで直感的な方法でこれらの課題に対処します。

AP フィルタ機能では、設定に基づいて、タグソースが正しい優先順位で整理されます。

AP フィルタ機能が無効にすることはできません。ただし、**ap filter-priority priority filter-name** コマンドを使用してタグソースの相対的な優先順位を設定できます。

タグの優先順位の設定

複数のタグソースがあるとネットワーク管理者にとってあいまいになる可能性があります。これに対処するため、タグの優先順位を定義できます。AP がコントローラに参加すると、優先順位に基づいてタグが選択されます。優先順位が設定されていない場合は、デフォルトが使用されます。

タグの優先順位を設定するには、次の手順を使用します。

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	ap tag-source-priority source-priority source {filter pnp} 例： Device(config)# ap tag-source-priority 2 source pnp	AP タグソースの優先順位を設定します。 (注) AP フィルタの設定は必須ではありません。静的、フィルタ、および PnP については、デフォルトの優先順位があります。
ステップ 3	end 例： Device(config)# 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。

	コマンドまたはアクション	目的
ステップ 4	ap tag-sources revalidate 例： Device# ap tag-sources revalidate	Revalidates AP タグ ソースを再検証します。優先順位は、このコマンドの実行後にのみアクティブになります。 (注) フィルタと PnP の優先順位を変更した場合、それらを評価するには revalidate コマンドを実行します。

AP フィルタの作成

AP フィルタは、コントローラで使用されるアクセス コントロール リスト (ACL) に似ており、グローバル レベルで適用されます。AP 名はフィルタとして追加できます。また、必要に応じて他の属性を追加することもできます。フィルタ条件はディスカバリ要求の一部として追加します。



(注) PnP サーバでタグ名を設定できます (flex グループや AP グループと同様)。また、AP はタグ名を、ディスカバリ要求と join 要求の一部として保存し送信します。

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	ap filter name filter_name 例： Device(config)# ap filter filter-1	AP フィルタを設定します。
ステップ 3	ap name-regex regular-expression 例： Device(config-ap-filter)# ap name-regex testany	正規表現に基づいて AP フィルタを設定します。
ステップ 4	tag policy policy-tag 例： Device(config-ap-filter)# tag policy pol-tag1	このフィルタのポリシー タグを設定します。

	コマンドまたはアクション	目的
ステップ 5	tag rf rf-tag 例： Device(config-ap-filter)# tag rf rf-tag1	このフィルタの RF タグを設定します。
ステップ 6	tag site site-tag 例： Device(config-ap-filter)# tag site site1	このフィルタのサイト タグを設定します。
ステップ 7	end 例： Device(config-ap-filter)# 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。

フィルタの優先順位の設定と更新

フィルタの優先順位を設定および更新するには、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 filter priority priority filter-name filter-name 例： Device(config)# ap filter priority 10 filter-name test1	AP フィルタの優先順位を設定します。 (注) 優先順位のないフィルタはアクティブではありません。同様に、フィルタを使用せずにフィルタの優先順位を設定することはできません。
ステップ 3	end 例： Device(config-ap)# 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。

AP フィルタの設定の確認

タグソースとフィルタ、およびそれらの優先順位を表示するには、次の **show** コマンドを使用します。

タグソースの優先順位を表示するには、次のコマンドを使用します。

```
Device# show ap tag sources
```

```
Priority Tag source
-----
0 Static
1 Filter
2 AP
3 Default
```

使用可能なフィルタを表示するには、次のコマンドを使用します。

```
Device# show ap filter all
```

Filter Name	RF Tag	regex	Site Tag	Policy Tag
first		abcd		pol-tag1
	rf-tag1		site-tag1	
test1		testany		
			site1	
filter1		testany		

アクティブなフィルタのリストを表示するには、次のコマンドを使用します。

```
Device# show ap filters active
```

Priority Tag	Filter Name	RF Tag	regex	Site Tag	Policy
10	test1		testany	site1	

AP タグのソースを表示するには、次のコマンドを使用します。

```
Device# show ap tag summary
```

```
Number of APs: 4
```

AP Name	AP Mac	Site Tag Name	Policy Tag Name	RF Tag Name	Misconfigured	Tag Source
AP002A.1034.CA78	002a.1034.ca78	named-site-tag	named-policy-tag	named-rf-tag	No Filter	
AP00A2.891C.2480	00a2.891c.2480	named-site-tag	named-policy-tag	named-rf-tag	No Filter	
AP58AC.78DE.9946	58ac.78de.9946	default-site-tag	default-policy-tag	default-rf-tag	No AP	
AP0081.C4F4.1F34	0081.c4f4.1f34	default-site-tag	default-policy-tag	default-rf-tag	No Default	

ロケーション設定でのアクセスポイントの設定

ロケーションの設定について

ロケーションの設定時には次の操作を実行できます。

- AP のサイトまたはロケーションを設定する。
- このロケーションのタグ セットを設定する。
- このロケーションに AP を追加する。

どのロケーションも、次のコンポーネントで構成されます。

- 一意のタグのセット。各タイプ（ポリシー、RF、サイト）に1つずつ。
- タグに適用されるイーサネット MAC アドレスのセット。

この機能は、既存のタグ解決スキームと連携して機能します。ロケーションは、既存のシステムに対する新しいタグ ソースと見なされます。静的なタグ ソースに対しても同様です。

ロケーションの設定の前提条件

アクセス ポイントを1つのロケーションで設定する場合、同じアクセス ポイントを別の場所に設定することはできません。

アクセス ポイントのロケーションの設定（GUI）

手順

- ステップ 1 [Configuration] > [Wireless Setup] > [Basic] を選択します。
- ステップ 2 [Basic Wireless Setup] ページで、[Add] をクリックします。
- ステップ 3 [General] タブで、ロケーションの名前と説明を入力します。
- ステップ 4 [Location Type] を [Local] または [Flex] のいずれかに設定します。
- ステップ 5 スライダーを使用して、[Client Density] を [Low]、[Typical]、または [High] に設定します。このプラグインにより、AP の RF 特性が設定されます。
- ステップ 6 [Apply] をクリックします。

アクセス ポイントのロケーションの設定（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	ap location name <i>location_name</i> 例： Device(config)# ap location name location1	アクセスポイントのロケーションを設定します。 アクセスポイントのロケーションを削除するには、このコマンドの no 形式を実行します。
ステップ 3	tag { policy <i>policy_name</i> rf <i>rf_name</i> site <i>site_name</i> } 例： Device(config-ap-location)# tag policy policy_tag Device(config-ap-location)# tag rf rf_tag Device(config-ap-location)# tag site site_tag	ロケーションのタグを設定します。
ステップ 4	location description 例： Device(config-ap-location)# location description	ロケーションに説明を追加します。
ステップ 5	end 例： Device(config-ap-location)# 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。

ロケーションへのアクセスポイントの追加 (GUI)

手順

ステップ 1 [Configuration] > [Wireless Setup] > [Basic] を選択します。

ステップ 2 [Basic Wireless Setup] ページで、[Add] をクリックし、次を設定します。

- 一般
- 無線ネットワーク
- AP プロビジョニング

ステップ 3 [AP Provisioning] タブの [Add/Select APs] セクションで、AP の MAC アドレスを入力し、右矢印をクリックして、関連付けられているリストに AP を追加します。

ステップ 4 [Available AP List] の検索オプションを使用して、選択した AP リストから AP を選択し、右矢印をクリックして、関連付けられているリストに AP を追加します。

ステップ5 [Apply] をクリックします。

ロケーションへのアクセスポイントの追加 (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# <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	ap location name <i>location_name</i> 例： Device(config)# ap location name location1	アクセスポイントのロケーションを設定します。
ステップ3	ap-eth-mac <i>ap_ethernet_mac</i> 例： Device(config-ap-location)# ap-eth-mac 188b.9dbe.6eac	アクセスポイントをロケーションに追加します。
ステップ4	end 例： Device(config-ap-location)# 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。 (注) APをロケーションに追加した後、APが自動的にリセットされて新しい設定が取得される場合があります。

ロケーション設定での SNMP の設定

ロケーションの設定における SNMP の前提条件

- 管理ポートが稼働している必要があります。
- SNMP コマンドをクエリする場合、管理ポートには 10x のネットワーク IP アドレスが必要です。これは、SNMP の **getmany** を発行する IP アドレスが **10.x.x.x** ネットワークにあるためです。

SNMP MIB

SNMP MIBは、論理エンティティと物理エンティティを表す一連の管理対象オブジェクトと、それらの間の関係に関する情報を提供します。

表 1: MIB オブジェクトと注記

MIB オブジェクト	注
cLApLocationName	AP ロケーションの名前を提供します。
cLApLocationPolicyTag	ロケーションに設定されているポリシータグを提供します。
cLApLocationSitetag	ロケーションに設定されているサイト タグを提供します。
cLApLocationRfTag	ロケーションに設定されている RF タグを提供します。
cLAssociatedApsApMac	ロケーションに設定されている AP を提供します。

ロケーション設定の確認

AP ロケーション設定のサマリーを表示するには、次のコマンドを使用します。

```
Device# show ap location summary
```

```
Location Name      Description      Policy Tag      RF Tag
Site Tag
-----
first              first floor     default-policy-tag  default-rf-tag
default-site-tag
second             second floor     default-policy-tag  default-rf-tag
default-site-tag
```

特定のロケーションについて AP ロケーション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 ap location details first
Location Name.....: first
Location description.....: first floor
Policy tag.....: default-policy-tag
Site tag.....: default-site-tag
RF tag.....: default-rf-tag
```

```
Configured list of APs
005b.3400.0af0
005b.3400.0bf0
```

AP タグのサマリーを表示するには、次のコマンドを使用します。

```
Device# show ap tag summary
Number of APs: 4
AP Name      AP Mac      Site Tag Name      Policy Tag Name      RF Tag Name
Misconfigured  Tag Source
-----
Asim_5-1     005b.3400.02f0  default-site-tag  default-policy-tag  default-rf-tag
  Yes
  Filter
Asim_5-2     005b.3400.03f0  default-site-tag  default-policy-tag  default-rf-tag
  No
  Default
```

```
Asim_5-9      005b.3400.0af0  default-site-tag  default-policy-tag  default-rf-tag
  No          Location
Asim_5-10    005b.3400.0bf0  default-site-tag  default-policy-tag  default-rf-tag
  No          Location
```

ロケーションの統計情報の確認

AP ロケーション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 ap location stats
```

```
Location name    APs joined    Clients joined  Clients on 11a  Clients on 11b
-----
first            2             0               3               4
second          0             0               0               0
```

