Catalyst アクセスポイント、IOS XE Bengaluru 17.7.x 上の Cisco 組み込みワイヤレスコントローラのコンフィギュレーションガイド

初版：2021 年 12 月 7 日

最終更新：2023 年 4 月 3 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

ここでは、このマニュアルの表記法、および他資料の入手方法について説明します。また、シスコ製品のマニュアルの最新情報についても説明します。

表記法

このマニュアルでは、以下の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
italic フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`Courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	**`太字の Courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3 つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス　時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　安全上の重要な注意事項

装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。使用、設置、電源への接続を行う前にインストール手順を読んでください。各警告の最後に記載されているステートメント番号を基に、装置の安全についての警告を参照してください。ステートメント 1071

SAVE THESE INSTRUCTIONS

関連資料

（注）　deviceCisco 組み込みワイヤレスコントローラをインストールまたはアップグレードする前に、のリリースノートを参照してください。

（注）　この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager [英語] でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。

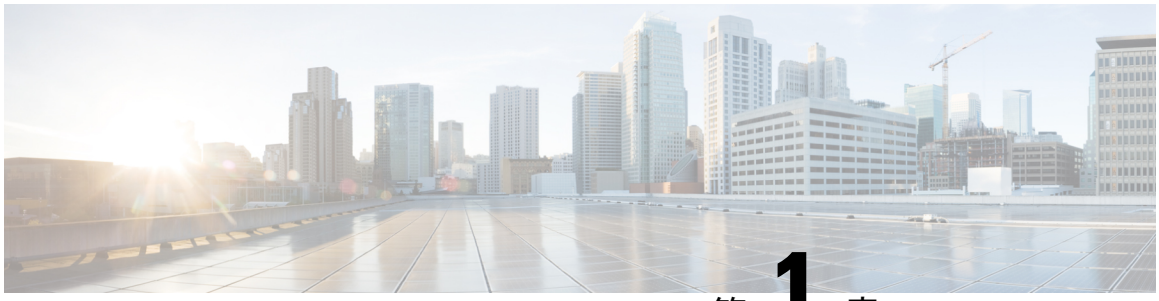
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder [英語] にアクセスしてください。

シスコバグ検索ツール

シスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 1 章

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの概要

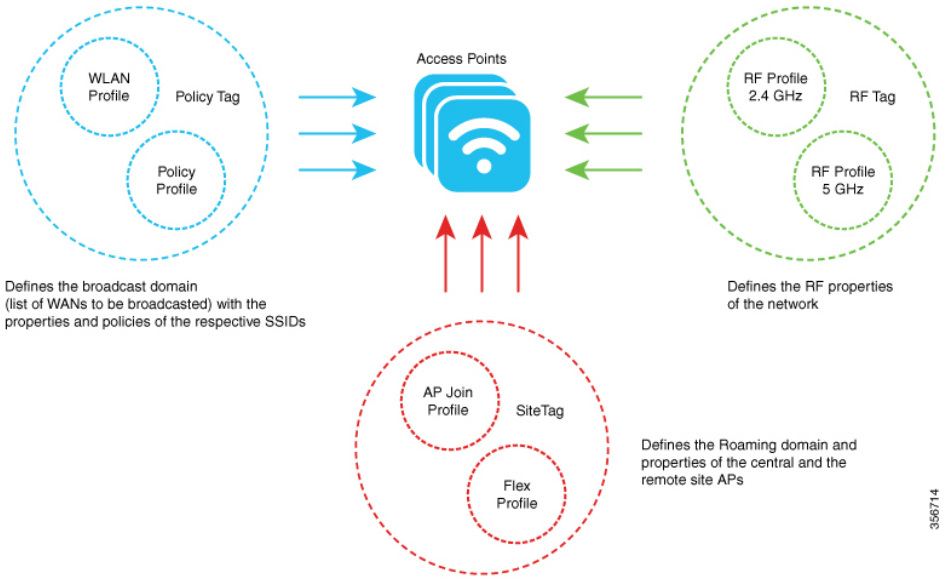
Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラは、インテントベースのネットワーキング向けに設計された次世代ワイヤレスコントローラです。Cisco コントローラは IOS XE ベースであり、Aironet の優れた RF 性能と IOS XE のインテントベースのネットワーキング機能を統合して、進化と成長を続ける組織にクラス最高水準のワイヤレスエクスペリエンスを提供します。

コントローラは、物理フォームファクタで展開可能であり、Cisco DNA Center、Netconf/YANG、Web ベース GUI、または CLI を使用して管理できます。

設定データ モデルは、再利用可能性、簡略化されたプロビジョニング、柔軟性とモジュール化の向上を基盤とし、拡張に応じたネットワークの管理を支援し、動的に変化し続けるビジネスと IT の要件の管理を簡略にします。

新しい設定モデルの要素

次の図は、新しい設定モデルの要素を示しています。



タグ

タグのプロパティは、タグに関連付けられているポリシーのプロパティによって定義されます。プロパティはさらに、関連付けられているクライアントまたは AP によって継承されます。タグにはさまざまなタイプがあり、それぞれが異なるプロファイルに関連付けられています。タグにはすべて、システムのブートアップ時に作成されたデフォルトが備わっています。

プロファイル

プロファイルは、AP に関連付けられているクライアントまたは AP 自身に適用される属性のセットを表します。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。

設定ワークフロー

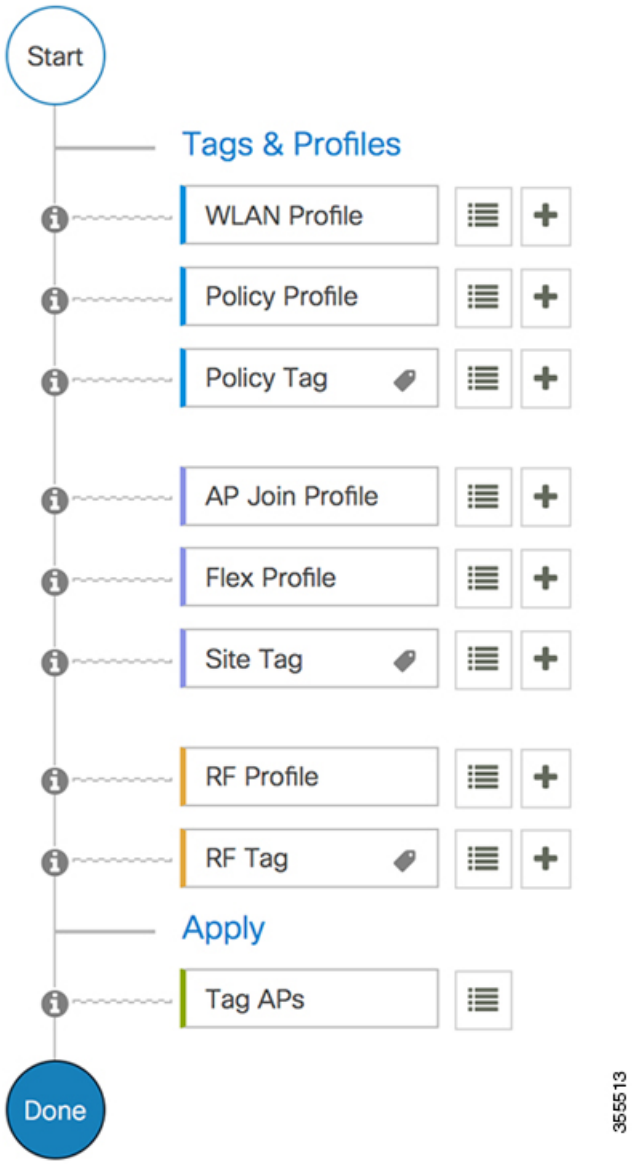
次の一連のステップで、設定の論理的順序を定義します。WLANプロファイル以外のすべてのプロファイルとタグにはデフォルトのオブジェクトが割り当てられています。

1. 次のプロファイルを作成します。
   - WLAN
   - ポリシー
   - AP 接続
   - Flex
   - RF
2. 次のタグを作成します。

- ポリシー
- サイト
- RF

3. タグを AP に関連付けます。

図 *1* : 設定ワークフロー



初期設定

コントローラの設定

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの初期設定ウィザードは簡素化されていて、コントローラのインストールおよび設定用のインターフェイスとしてすぐに利用できます。ここでは、コントローラを小規模から大規模までのあらゆるネットワークワイヤレス環境で動作するようにセットアップする手順について説明します。このような環境では、アクセスポイントをシンプルなソリューションとしてまとめることにより、社員ワイヤレス アクセスやゲスト ワイヤレス アクセスなどのさまざまなサービスをネットワーク上で提供できます。

（注） Cisco IOS XE Amsterdam 17.1.x 以降、Network Time Protocol（NTP）と同期しない限り、日付と時刻は Web UI に反映されません。

（注） **wireless ewc-ap factory-reset** コマンドを使用して、EWC デバイスを Day 0 状態にリセットすることをお勧めします（構成ウィザードを使用）。また、このコマンドは、ネットワーク内のすべての AP および EWC-AP を Day 0 状態にリセットします。**erase startup-config** コマンドを使用して、デバイスから設定を削除できますが、ネットワーク内の他のデバイスには同期されません。

（注） Day 0 ウィザードを完了すると、内部 AP が切断され、1 分後に再接続します。

（注） ワイヤレス管理は AP ギガビットポートで行う必要があり、IOS-XE で複数の SVI を設定することはできません。

（注） 新しい TAR ファイルをコピーした後に **write memory** コマンドを実行する必要があります。

Day 0 ウィザードを使用したコントローラの設定（GUI）

Day 0 ウィザードを使用してコントローラを設定するには、次の手順を実行します。

始める前に

AP が EWC モードで再起動すると、MAC アドレスの最後の数字で終わるプロビジョニング SSID がブロードキャストされます。PSK パスワードを使用してプロビジョニング SSID に接続できます。

次に、ブラウザを開いて mywifi.cisco.com にリダイレクトすると、AP Web UI に移動します。ユーザー名に **webui**、パスワードに **cisco** と入力します。

注：EWC 構成ポータルへの Web リダイレクションは、プロビジョニング SSID に接続している場合にのみ機能します。ラップトップが別の Wi-Fi ネットワークまたは有線ネットワークに接続されている場合は機能しません。Day 0 ウィザードプロビジョニングモードのときに EWC IP アドレスを入力しても、有線ネットワークからは AP を設定できません。

手順

ステップ 1 コントローラにログオンし、[Configuration Setup Wizard] で [General Settings] ページに移動します。

ステップ 2 [Configuration Mode] オプションで、次のいずれかを選択します。

a) [Non Mesh]：次のフィールドに入力します。

1. [Host Name]：ホスト名を入力します。
2. [Country]：ドロップダウンリストから適切な国番号を選択します。

   （注） エンドユーザーライセンス契約で要求されているように、適切な国番号を選択して、解放されたネットワークが地域および国の規制に違反しないようにしてください。国番号の割り当てが不適切な場合、ワイヤレス通信を妨害する可能性があり、不適切な国番号に設定されたデバイスを使用するワイヤレスネットワークのオペレーターに対して、政府から罰則や制裁が課される可能性があります。

3. [Management User Settings] セクションで、ユーザー名とパスワードを入力します。
4. [Wireless Management Settings] セクションで、[DHCP] チェックボックスをオンにして、DHCP サーバーの IP アドレスを表示します。
5. [Wireless Network] セクションで、[Add] をクリックして、少なくとも 1 つの WLAN を作成します。

b) [Mesh]：次のフィールドに入力します。

1. [Host Name]：ホスト名を入力します。
2. [Country]：[+] アイコンをクリックして、適切な国番号を入力します。
3. [Management User Settings] セクションで、ユーザー名とパスワードを入力します。
4. [Wireless Management Settings] セクションで、[DHCP] チェックボックスをオンにして、DHCP サーバーの IP アドレスを表示します。

5. [Wireless Mesh Settings] セクションで、次のフィールドに入力します。
   - [Enable Wireless Bridge] 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。
   - [Mesh AP MAC Address] フィールドに MAC アドレスを入力するか、[+] アイコンをクリックして、表示されるメッシュ AP の MAC アドレスのリストから MAC アドレスを選択します。
6. [Wireless Network] セクションで、[Add] をクリックして、少なくとも 1 つの WLAN を作成します。

ステップ 3 [Finish] をクリックします。

Day 0 ウィザードを使用したコントローラの設定（CLI）

Day 0 ウィザードを使用してコントローラを設定するには、以下の手順を実行します。次の手順は、メッシュ AP と非メッシュ AP の設定に共通です。既存の Day 0 ワークフローでは、**factory-reset** コマンドによる設定が可能です。

始める前に

- 利用可能なオプションは、各設定パラメータの後の括弧内に示されます。デフォルト値は、すべて大文字で示されます。
- 入力した応答が正しくない場合は、「Invalid Response」などのエラーメッセージがコントローラに表示され、ウィザードのプロンプトが再び表示されます。
- 前のコマンドラインに戻るには、ハイフンキーを押します。

手順

ステップ 1 **wireless ewc-ap factory-reset** コマンドを入力して、Day 0 ワークフローを開始します。このコマンドは、ユーザーがアクションを確認するとデバイスを再起動します。

ステップ 2 デバイスが再起動し、初期設定ダイアログでプロンプトが表示されたら、**Yes** と入力してダイアログを開始します。

例：

```
Would you like to enter the initial configuration dialog? [yes/no]: Yes
```

ステップ 3 以下の質問に対して、有効な入力を入力します（それぞれ、メッシュ AP と非メッシュ AP のプロンプトが表示されます）。

a) 操作する国番号を入力します。

（注） 使用可能な国コードの一覧を表示するには、「help」と入力します。

複数の国の AP を 1 つのコントローラで管理する場合は、複数の国番号を入力できます。複数の Country Code を入力するには、Country Code をカンマで区切ります（「US,CA,MX」など）。構成ウィザードの実行後、コントローラに接続している各 AP を特定の国を割り当てる必要があります。

例：

```
Configure country code(s) for wireless operation in ISO format [US]: US,CH,CN,GB
```

b) 国番号を入力して AP プロファイルを設定します。

例：

```
Configure default wireless AP profile country code in ISO format [US]:
```

c) ホスト名を入力します。

例：

```
Enter the hostname [EWC]: EWC
```

d) 詳細を入力して、AP の管理アクセスのログイン情報を設定します。

例：

```
Configure credentials for management access on Access Points? [yes]: yes
 [AP] Enter the management username: EWC_User
 [AP] Enter the management password: ********
 [AP] Reenter the password: ********
 [AP] Enter the privileged mode access password: ********
 [AP] Reenter the password: ********
```

e) 管理ログイン情報入力します。

例：

```
Enter the management username: EWC_User
Enter the password: ********
Reenter the password: ********
```

f) DHCP インターフェイスを設定します。

例：

```
Configure interface as DHCP [yes/no]? [no]: yes
```

g) ワイヤレスネットワークの設定を設定します。

例：

```
Configure Wireless network settings? [yes]: yes
 Enter the network name or service set identifier (SSID): test
 Choose the network type
   1. Employee
   2. Guest
 Enter your selection [1]: 1
 Choose the security type
   1. WPA Personal
   2. WPA Enterprise
 Enter your selection [2]: 1
 Enter the pre-shared key: ****
```

非メッシュ AP の場合、設定はこれで終了です。設定を保存または廃棄します。

ステップ 4 メッシュ対応 AP を設定するには、以下の手順に従ってください。

a) AP でメッシュモードを設定します。

例：

```
Set Internal AP in mesh mode [yes/no]? [no]: yes
```

b) 追加のメッシュアクセスポイント（MAP）を設定します。

例：

```
Configure additional MAPs [yes/no]? [no]: yes
Enter a comma separated list of max 20 Mesh AP ethernet macs (format: 'aabbccddeeff'
 or 'aabb.ccdd.eeff'): aabbccddeeff, 1122.3344.5566
```

c) ワイヤレスブリッジングを有効にします。

例：

```
Enable wireless bridging [yes/no]? [no]: yes
```

例

メッシュ AP の設定が完了すると、入力した選択肢から、次の構成スクリプトが生成されます。

```
!

ap profile default-ap-profile
country US

!
hostname EWC
!
ap profile default-ap-profile
mgmtuser username EWC_User password 0 test secret 0 test

!
username EWC_User privilege 15 secret 9
$x$xxxxxxxxxx9xxxxxxxxxxjxxxxxxxxxxzxxxxxxxxxxOxxxxxxxxxxxxxxx

!
wireless management interface GigabitEthernet0

!

interface GigabitEthernet0
ip address dhcp

!
wlan test 1 test
security wpa psk set-key ascii 0 test
no security wpa akm dot1x
security wpa akm psk
no shut

!
```

```
wireless tag policy default-policy-tag
wlan test policy default-policy-profile

!
end
wireless country US
wireless country CH
wireless country CN
wireless country GB
aaa new-model
aaa authentication login default local
aaa authorization credential-download default local
username 3C5731C58478 mac


!
ap profile default-ap-profile
ssid broadcast persistent
username aabbccddeeff mac
username 112233445566 mac


wireless mesh security psk provisioning
wireless mesh security psk provisioning default_psk

!
wireless profile mesh default-mesh-profile
security psk
ethernet-bridging
ethernet-vlan-transparent
```

次のタスク

設定を保存または廃棄します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection:

Example:
Enter your selection: 2
```

インタラクティブヘルプ

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ の GUI には、GUI 全体を順を追って説明し、複雑な設定をガイドするインタラクティブヘルプがあります。

次の方法でインタラクティブヘルプを開始できます。

- GUI のウィンドウの右隅にある青いフラップの上にカーソルを置き、[Interactive Help] をクリックします。
- GUI のウィンドウの左ペインで [Walk-me Thru] をクリックします。

- GUI のさまざまな場所に表示される [Show me How] をクリックします。[Show me How] をクリックすると、現在のコンテキストに関連する具体的なインタラクティブヘルプが表示されます。

  たとえば、[Configure] > [AAA] の [Show me How] をクリックすると、RADIUS サーバーを設定するための各手順の説明が表示されます。[Configuration] > [Wireless Setup] > [Advanced] の順に選択し、[Show me How] をクリックすると、さまざまな種類の認証に関連する手順を説明するインタラクティブヘルプがトリガーされます。

次の機能には、インタラクティブヘルプが関連付けられています。

- AAA の設定
- FlexConnect 認証の設定
- 802.1X 認証の設定
- ローカル Web 認証の設定
- OpenRoaming の設定
- メッシュ AP の設定

（注） Safari で WalkMe ランチャーが使用できない場合は、次のように設定を変更します。

1. [Preferences] > [Privacy] の順に選択します。
2. [Website tracking] セクションで、[Prevent cross-site tracking] チェックボックスをオフにしてこのアクションを無効にします。
3. [Cookies and website data] セクションで、[Block all cookies] チェックボックスをオフにしてこのアクションを無効にします。

Catalyst アクセスポイント上の Cisco 組み込みワイヤレスコントローラのリセット

Catalyst AP のコントローラを工場出荷時のデフォルトにリセットするには、次の手順に従います。

手順

ステップ 1 アクセスポイントを電源から外します。

ステップ 2 コンソールケーブルを接続し、コンピュータまたはラップトップでシリアルセッションを開きます。

ステップ 3 AP の [Mode/Reset] ボタンを押したままにします。

ステップ 4 [Mode/Reset] ボタンを押したまま、AP を電源に接続し直します。

ステップ 5 コンピュータまたはラップトップのシリアルセッションにプロンプトが表示されるまで、ボタンを押し続けます。

（注） コンソールセッションには、ボタンが押されている時間も表示されます。完全に再起動するまで、ボタンを 20 秒以上押す必要があります。

次のタスク

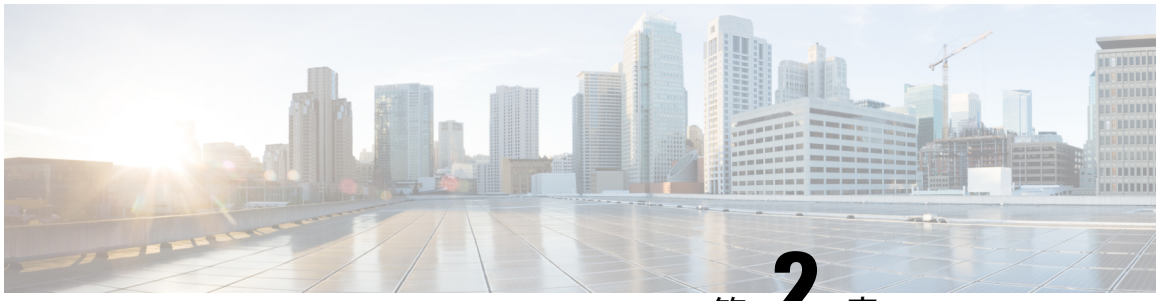
AP が再起動したら、デフォルトのログイン情報 Cisco/Cisco を使用してログインします。

パスワードの回復

パスワードを回復するには、AP を工場出荷時設定にリセットする必要があります。工場出荷時のデフォルトにリセットする方法の詳細については、「Catalyst アクセスポイント上の Cisco 組み込みワイヤレスコントローラのリセット」を参照してください。

第 I 部

システム設定



第 2 章

システム設定

新しい設定モデルについて

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの設定は、さまざまなタグ（RF タグ、ポリシータグ、サイトタグ）を使用して簡素化されます。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、タグ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。rfタグには無線プロファイル、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、サイトタグにはフレックスプロファイルと ap-join プロファイルがそれぞれ含まれています。

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プが含まれています。ポリシータグごとに、このようなエントリが最大 可能性があります。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プライマリ 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になります。

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、2.4 GHz および 5 GHz 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、タグ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。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、ポリシー属性とリモートサイト固有のパラメータが含まれています。たとえば、EAP プロファイル（AP がローカル RADIUS サーバー情報の認証サーバー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 接続プロファイルには、CAPWAP、IPv4 と IPv6、UDP Lite、高可用性、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 と SSH、11u パラメータなどの AP に固有の属性が含まれています。

（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、IW6300、ESW6300、9105AXI、9105AXW、9115AXI、9115AXE、9117I、APVIRTUAL、9120AXI、9120AXE、 9130AXI、および 9130AXE。

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 の関連付け

AP は、さまざまな方法を使用して関連付けることができます。デフォルトのオプションは、MAC がポリシータグ、サイトタグ、および RF タグに関連付けられているイーサネット MAC アドレスによって使用されます。

フィルタベースの関連付けでは、AP は正規表現を使用してマッピングされます。正規表現（regex）は、入力文字列とのマッチングを行うためのパターンです。その正規表現に一致する任意の数の AP には、ポリシータグ、サイトタグ、および RF タグがマッピングされ、AP フィルタの一部として作成されます。

AP ベースの関連付けでは、タグ名は PnP サーバーで設定され、AP はそれらのタグを保存し、検出プロセスの一部としてタグ名を送信します。

ロケーションベースの関連付けでは、タグはロケーションごとにマッピングされ、そのロケーションにマッピングされている AP イーサネット MAC アドレスにプッシュされます。

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。名前には、32 ～ 126 文字の ASCII 文字を使用できます（先頭と末尾のスペースはなし）。システムが不安定になるため、スペースは使用しないでください。

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 [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]：ワイヤレス ユーザー トラフィックとすべての制御トラフィックが、CAPWAP 経由で中央集中型コントローラにトンネリングされます。ユーザートラフィックはコントローラ上のダイナミック インターフェイスまたは VLAN にマッピングされます。これは、CAPWAP モードの通常の動作です。
- [Central Authentication]：コントローラがクライアント認証を処理するため、クライアントデータはコントローラにトンネリングされます。
- [No Central DHCP]：AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。

- [Central Association Enable]：中央アソシエーションが有効になっている場合、すべてのスイッチングはコントローラで実行されます。
- [Flex NAT/PAT]：ネットワークアドレス変換（NAT）およびポートアドレス変換（PAT）モードを有効にします。

ステップ 6 [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（Cisco 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** *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	**idle-timeout** *timeout* 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** *vlan-id* 例： `Device(config-wireless-policy)# vlan 24`	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 5	**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 6	**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** *policy-profile-name* 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** *flex-profile* 例： `Device(config)# wireless profile flex rr-xyz-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	**description** 例： `Device(config-wireless-flex-profile)# description xyz-default-flex-profile`	（任意）Flex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 接続プロファイルには、CAPWAP、IPv4/IPv6、UDP Lite、高可用性、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 AP に固有の属性が含まれています。

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 [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) [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。
f) [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。
g) [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。
h) 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。
i) [Profile Name] ドロップダウン リストから、プロファイル名を選択します。
j) [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 サーバー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 モニターリング、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 アドバ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。

ステップ 8 [Management] タブでは次の設定が行えます。

- デバイス

a) [Device] タブで、TFTP サーバーの [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、ローカルのユーザー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 ユーザー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。
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 9 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 10 [Rogue Detection Minimum RSSI] フィールドに、RSSI 値を入力します。

このフィールドは、不正 AP が報告される最小 RSSI 値を指定します。設定されている値よりも RSSI が低いすべての不正 AP は、コントローラに報告されません。

ステップ 11 [Rogue Detection Transient Interval] フィールドに、一時的な間隔の値を入力します。

このフィールドは、コントローラに報告する前に不正 AP が表示される時間を示します。

ステップ 12 [Rogue Detection Report Interval] フィールドに、レポート間隔の値を入力します。

このフィールドは、AP からコントローラに送信される不正レポートの頻度（秒単位）を示します。

ステップ 13 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。

ここで、AP は、RSSI に基づいて、ターゲットの不正に最適なレートを選択します。

ステップ 14 [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。

ここで、AP は、FlexConnect スタンドアロンモードに移行した場合に封じ込めを継続します。

ステップ 15 [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。

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 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） AP プロファイルでは、**EAP-FAST** がデフォルトの EAP タイプです。 （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： `Device(config-ap-profile)# description "xyz ap profile"`	AP プロファイルの説明を追加します。
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 name** *profile-name***detailed** 例： `Device# show ap profile name xyz-ap-profile detailed`	（任意）AP 接続プロファイルに関する詳細情報を表示します。

RF プロファイルの設定（GUI）

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。名前には、32 ～ 126 文字の ASCII 文字を使用できます（先頭と末尾のスペースはなし）。

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じ 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。 （注） **24ghz** コマンドを使用して、802.11b パラメータを設定します。**5ghz** コマンドを使用して、802.11a パラメータを設定します。
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。

	コマンドまたはアクション	目的
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。

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。名前には、32 ～ 126 文字の ASCII 文字を使用できます（先頭と末尾のスペースはなし）。

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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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。 （注） LWA を実行すると、コントローラに接続されているクライアントが、セッション タイムアウトの前に断続的に切断されます。 回避策として、特定のポリシータグの下に、中央アソシエーションを持つ、または中央アソシエーションを持たないすべてのポリシー プロファイルを含めることをお勧めします。
ステップ 4	**description** *description* 例： `Device(config-policy-tag)# description "default-policy-tag"`	ポリシータグに説明を追加します。
ステップ 5	**remote-lan** *name* **policy** *profile-policy-name* {**ext-module**| **port-id** } 例： `Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2`	リモート LAN プロファイルをポリシー プロファイルにマッピングします。
ステップ 6	**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 7	**end** 例： `Device(config-policy-tag)# end`	ポリシー タグ 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 8	**show wireless tag policy summary** 例：	（任意）設定済みのポリシー タグを表示します。

	コマンドまたはアクション	目的
	`Device# show wireless tag policy summary`	（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。名前には、32 ～ 126 文字の ASCII 文字を使用できます（先頭と末尾のスペースはなし）。

ステップ 4 RF タグに関連付ける、必要な **[5 GHz Band RF Profile]**、**[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 タグで使用できるプロファイルは 2 つ（2.4 GHz および 5 GHz 帯域の RF プロファイル）のみです。
- AP タグ タスクを設定するときに作成したものと同じ 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。

	コマンドまたはアクション	目的
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。6GHz 無線 dot11 ポリシーを設定するには、6ghz-rf-policy コマンドを使用します。
ステップ 4	**description** *policy-description* 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** *rf-tag* 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） *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： `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：	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。

	コマンドまたはアクション	目的
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。

時間管理

Wireless Express セットアップウィザードの初回実行時には、EWC のシステム日時を設定します。[Administration] > [Time] を選択することで、GUI メニューから時刻を変更または設定できます。

Wireless Express のセットアップ時に日時を設定しなかった場合、日時を同期するように Network Time Protocol（NTP）サーバーを設定できます。コントローラ上の時間帯は、Greenwich Mean Time（GMT; グリニッジ標準時）を基準として設定します。特定の NTP サーバーを EWC に追加または更新することもできます。

（注） EWC AP は、電源がオフになっている場合は時間を追跡しないため、EWC での再起動後も適切な時間が維持されるように NTP を設定することをお勧めします。

AP フィルタ

AP フィルタの概要

Catalyst アクセスポイント上のシスコ組み込み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。

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 フィルタ機能を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。

（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。

タグの優先順位の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[Tags]** > **[AP]** > **[Tag Source]** を選択します。

ステップ 2 タグソースをドラッグアンドドロップして優先順位を変更します。

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。

	コマンドまたはアクション	目的
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。
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（GUI）

手順

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

ステップ 2 [Add] をクリックします。

ステップ 3 表示される [Associate Tags to AP] ダイアログボックスで、[Rule Name]、[AP name regex]、および [Priority] を入力します。必要に応じて、[Policy Tag Name] ドロップダウンリストからポリシータグ、[Site Tag Name] ドロップダウンリストからサイトタグ、[RF Tag Name] ドロップダウンリストから RF タグを選択することもできます。

ステップ 4 [Apply to Device] をクリックします。

AP フィルタの作成（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。
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。

	コマンドまたはアクション	目的
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。 たとえば、APに **ap-lab-12** という名前を付けた場合、AP名に一致するように、**ap-lab-\d+** などの正規表現を使用してフィルタを設定できます。
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。
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（GUI）

手順

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

ステップ 2
a) 新しい AP フィルタを設定する場合は、[Add] をクリックします。表示される [Associate Tags to AP] ダイアログボックスで、[Rule Name]、[AP name regex]、および [Priority] を入力します。オプションで、[Policy Tag Name]、[Site Tag Name]、および [RF Tag Name] を選択することもできます。[Apply to Device] をクリックします。
b) 既存の AP フィルタの優先順位を更新する場合は、[Filter] をクリックし、[Edit Tags] ダイアログボックスで [Priority] を変更します。[Filter] が非アクティブの場合、優先順位は設定できません。[Update and Apply to Device] をクリックします。

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             regex             Policy Tag               RF Tag
Site 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   Filter Name       regex          Policy Tag              RF Tag
 Site Tag
------------------------------------------------------------------------------------------------------------
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）

始める前に

（注） 基本的なセットアップワークフローでローカルおよびリモートサイトを作成すると、対応するポリシーとタグがバックエンドで作成されます。基本的なセットアップで作成されたこれらのタグとポリシーは、高度なワークフローを使用して変更することはできません。その逆も同様です。

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 スライダを使用して、[Client Density] を [Low]、[Typical]、または [High] に設定します。
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。
ステップ 2	**ap location name** *location_name* 例： `デバイス(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。

	コマンドまたはアクション	目的

ステップ 3	**tag** { **policy** *policy_name*| **rf** *rf_name* | **site** **site_name**}
	例：
	`デバイス(config-ap-location)# tag policy policy_tag`
	`デバイス(config-ap-location)# tag rf rf_tag`
	`デバイス(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： `デバイス(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： `デバイス(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）

（注） タグソースがロケーションに設定されていない場合、AP カウントと AP ロケーションのタグ付けが Web UI に正しく反映されません。AP の静的タグソースを変更するには、コントローラで **no ap** *ap-mac* コマンドを実行して、AP タグソースをデフォルト（ロケーション）に変更します。

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。MAC アドレスは、

xx:xx:xx:xx:xx:xx、xx-xx-xx-xx-xx-xx、または xxxx.xxxx.xxxx のいずれかの形式で指定できます。

システムから CSV ファイルを追加することもできます。CSV に MAC アドレス列が含まれていることを確認します。

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# 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 location name** *location_name* 例： `デバイス(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** *ap_ethernet_mac* 例： `デバイス(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： `デバイス(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

SNMP

EWC は SNMP をサポートしておらず、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SNMP MIB を実装していませんが、EWC は一部のオブジェクト識別子（OID）に応答する場合があります。

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
```

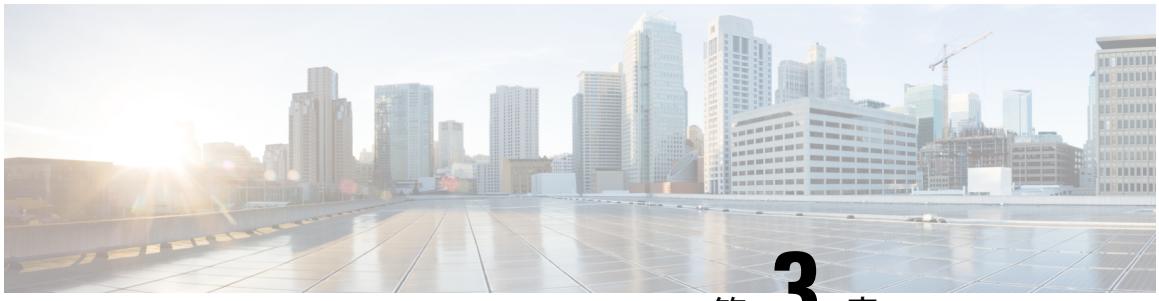
AP タグのサマリーを表示するには、次のコマンドを使用します。

```
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
```



第 3 章

ポリシーを使用したスマートライセンス

ポリシーを使用したスマートライセンシングの概要

ポリシーを使用したスマートライセンシングは、スマートライセンシングの拡張バージョンであり、ネットワークの運用を中断させないライセンスソリューションを提供するという主目的がありますが、むしろ、購入および使用しているハードウェアおよびソフトウェアライセンスを考慮してコンプライアンス関係を実現するライセンスソリューションを提供するという目的もあります。

Smart Licensing Using Policy は、Cisco IOS XE Amsterdam 17.3.2a 以降でサポートされます。

この拡張ライセンスモデルの主な利点は次のとおりです。

- シームレスな初日運用

  ライセンスを注文した後は、輸出規制または適用ライセンスを使用しない限り、キーの登録や生成などの準備手順は必要ありません。Cisco Catalyst ワイヤレスコントローラには、輸出規制ライセンスや適用ライセンスがなく、製品機能をデバイスですぐに設定できます。

- Cisco IOS XE の一貫性

  Cisco IOS XE ソフトウェアを実行するキャンパスおよび産業用イーサネットスイッチング、ルーティング、およびワイヤレスデバイスには、均一なライセンスエクスペリエンスがあります。

- 可視性と管理性

  使用中の情報を把握するためのツール、テレメトリ、製品タギング。

- コンプライアンスを維持するための柔軟な時系列レポート

  Cisco Smart Software Manager（CSSM）に直接または間接的に接続しているか、外部との接続性のないネットワークに接続しているかにかかわらず、簡単なレポートオプションを使用できます。

このドキュメントでは、Cisco Catalyst ワイヤレスコントローラにおけるポリシーを使用したスマートライセンシングの概念、設定、およびトラブルシューティング情報について説明します。

シスコ ライセンスの詳細については、cisco.com/go/licensingguide [英語] を参照してください。

ポリシーを使用したスマートライセンシングに関する情報

このセクションでは、ポリシーを使用したスマートライセンシングの概念、サポートされる製品、サポートされる各トポロジの概要、およびポリシーを使用したスマートライセンシングと他の機能との連携について説明します。

概要

ポリシーを使用したスマートライセンシングは、ライセンスのさまざまな側面をシームレスに体験できるソフトウェアライセンス管理ソリューションです。

- ライセンスの購入：既存のチャネルからライセンスを購入し、Cisco Smart Software Manager（CSSM）ポータルを使用して製品インスタンスとライセンスを表示します。

（注） 新しいハードウェアまたはソフトウェアの注文の場合、シスコは、次のアイテムを工場でインストールすることで、Smart Licensing Using Policy の実装を簡素化します（用語については、以下の「概念 （49 ページ）」の項で説明します）。

- カスタムポリシー（使用可能な場合）
- CSSM に送信されるデータの信頼性を保証する信頼コード。これは、Cisco IOS XE Cupertino 17.7.1 以降でインストールされます。この信頼コードは、CSSMとの通信には使用できません。

- 使用：Cisco Catalyst ワイヤレスコントローラのライセンスはすべて適用されません。つまり、ソフトウェアとそれに関連付けられているライセンスの使用を開始する前に、キーの登録や生成などのライセンス固有の操作を完了する必要はありません。ライセンスの使用状況はタイムスタンプとともにデバイスに記録され、必要なワークフローは後日完了できます。
- ライセンスの使用状況をCSSMにレポート：ライセンス使用状況レポートには複数のオプションを使用できます。Cisco Smart Licensing Utility（CSLU）を使用したり、使用状況情報をCSSMに直接レポートしたりできます。エアギャップネットワークの場合、使用状況情報をダウンロードしてCSSMにアップロードする、オフラインレポートのプロビジョニングも使用できます。使用状況レポートはプレーンテキストの XML 形式です。リソース使用率測定レポートの例 （162 ページ）を参照してください。
- 調整：差分請求が適用される状況用（購入と消費を比較して差分がある場合）。

サポート対象製品

このセクションでは、ポリシーを使用したスマートライセンシングをサポートするCisco IOS-XE製品インスタンスについて説明します。特に指定のない限り、製品シリーズのすべてのモデル（製品 ID または PID）がサポートされます。

表 *1 :* サポート対象製品インスタンス：*Cisco Catalyst* ワイヤレスコントローラ

Cisco Catalyst ワイヤレスコントローラ	**ポリシーを使用したスマートライセンシングのサポート導入時点**
Cisco Catalyst 9800-40 ワイヤレスコントローラ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800-L ワイヤレス コントローラ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800-CL ワイヤレス コントローラ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800 組み込みワイヤレスコントローラ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9100 アクセスポイント上の Cisco 組み込みワイヤレスコントローラ（EWC-AP）	Cisco IOS XE Amsterdam 17.3.2a

アーキテクチャ

ここでは、ポリシーを使用したスマートライセンシングの実装に含めることができるさまざまなコンポーネントについて説明します。1つ以上のコンポーネントでトポロジが構成されます。

製品インスタンス

製品インスタンスとは、Unique Device Identifier（UDI）によって識別されるシスコ製品の単一インスタンスです。

製品インスタンスは、ライセンス使用状況（RUM レポート）を記録および報告し、期限切れのレポートや通信障害などに関するアラートとシステムメッセージを提供します。RUM レポートおよび使用状況データは、製品インスタンスに安全に保存されます。

このドキュメントでは、「製品インスタンス」という用語は、特に明記しない限り、サポートされているすべての物理および仮想製品インスタンスを指します。このドキュメントの範囲内にある製品インスタンスについては、サポート対象製品 （45 ページ）を参照してください。

CSLU

Cisco Smart License Utility（CSLU）は、集約ライセンスワークフローを提供する Windows ベースのレポートユーティリティです。このユーティリティが実行する主な機能は次のとおりです。

- ワークフローのトリガー方法に関するオプションを提供します。ワークフローは、CSLU や製品インスタンスによってトリガーできます。
- 1 つ以上の製品インスタンスから使用状況レポートを収集し、それらの使用状況レポートを対応するスマートアカウントやバーチャルアカウントに、オンラインかオフラインで、またはファイルを使用してアップロードします。同様に、RUM レポート ACK をオンラインまたはオフラインで収集し、製品インスタンスに返送します。
- 承認コード要求を CSSM に送信し、CSSM から承認コードを受信します（該当する場合）。

CSLU は、次の方法で実装に含めることができます。

- CSSM に接続されているスタンドアロンツールとして CSLU を使用するための Windows アプリケーションをインストールします。
- CSSM から切断されているスタンドアロンツールとして CSLU を使用するための Windows アプリケーションをインストールします。このオプションを使用すると、必要な使用状況情報がファイルにダウンロードされ、CSSM にアップロードされます。これは、外部と接続していないネットワークに適しています。
- Cisco DNA Center などのコントローラに（シスコが）組み込みます。
- Linux を実行しているマシン（ラップトップまたはデスクトップ）に CSLU を導入します。

CSLU は、Windows 10 および Linux オペレーティングシステムをサポートします。リリースノートおよび最新バージョンをダウンロードするには、[Software Download] ページの [Smart Licensing Utility] をクリックします。https://software.cisco.com/download/home/286285506/type

CSSM

Cisco Smart Software Manager（CSSM）は、一元化された場所からすべてのシスコ ソフトウェア ライセンスを管理できるポータルです。CSSM は、現在の要件を管理し、将来のライセンス要件を計画するための使用傾向を確認するのに役立ちます。

CSSM Web UI には https://software.cisco.com でアクセスできます。[License] タブで、[Smart Software Licensing] のリンクをクリックします。

CSSM に接続できるさまざまな方法については、サポートされるトポロジ （55 ページ） のセクションを参照してください

CSSM では、次のことができます。

- バーチャルアカウントを作成、管理、または表示する。
- 製品インスタンスの登録トークンを作成および管理する。
- バーチャルアカウント間または表示ライセンス間でライセンスを転送する。
- 製品インスタンスを転送、削除、または表示する。
- バーチャルアカウントに関するレポートを実行する。
- 電子メール通知の設定を変更する。
- 仮想アカウント情報を表示する。

コントローラ

複数の製品インスタンスを管理する管理アプリケーションまたはサービス。

（注） この章における、ポリシーを使用したスマートライセンシングのコンテキストでは、「コントローラ」という用語は、常に製品インスタンスを管理する管理アプリケーションまたはサービスを意味します。「コントローラ」という用語は、製品インスタンスである Cisco Catalyst ワイヤレスコントローラを指すためには使用されません。

Cisco Catalyst ワイヤレスコントローラでは、Cisco DNA Center がサポートされているコントローラです。コントローラ、コントローラをサポートする製品インスタンス、およびコントローラと製品インスタンスで必要な最小ソフトウェアバージョンに関する情報を次に示します。

表 *2:* コントローラのサポート情報：*Cisco DNA Center*

Smart Licensing Using Policy へ移行するために必要な **Cisco DNA Center** の最小バージョン[1]	**Cisco IOS XE** に必要な最小バージョン[2]	サポート対象製品インスタンス
Cisco DNA Center リリース 2.2.2	Cisco IOS XE Amsterdam 17.3.2a	• Cisco Catalyst 9800-40 ワイヤレス コントローラ • Cisco Catalyst 9800-80 ワイヤレス コントローラ • Cisco Catalyst 9800-L ワイヤレス コントローラ • Cisco Catalyst 9800-CL ワイヤレス コントローラ • Cisco Catalyst 9800 組み込みワイヤレスコントローラ • Cisco Catalyst 9100 アクセスポイント上の Cisco 組み込みワイヤレスコントローラ（EWC-AP）

1 コントローラに必要な最小ソフトウェアバージョン。これは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

2 製品インスタンスに必要な最小ソフトウェアバージョン。これは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

Cisco DNA Center の詳細については、https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html [英語] でサポートページを参照してください。

SSM オンプレミス

Smart Software Manager オンプレミス（SSM オンプレミス）は、CSSM と連動するアセットマネージャです。これにより、CSSMに直接接続する代わりに、オンプレミスで製品とライセンスを管理できます。

SSM オンプレミスで Smart Licensing Using Policy を実装するために必要なソフトウェアバージョンについては、次を参照してください。

Smart Licensing Using Policy に必要な SSM オンプレミスの最小バージョン[3]	Cisco IOS XE に必要な最小バージョン[4]	サポート対象製品インスタンス
バージョン 8、リリース 202102	Cisco IOS XE Amsterdam 17.3.3	• Cisco Catalyst 9800-40 ワイヤレス コントローラ • Cisco Catalyst 9800-80 ワイヤレス コントローラ • Cisco Catalyst 9800-L ワイヤレス コントローラ • Cisco Catalyst 9800-CL ワイヤレス コントローラ • Cisco Catalyst 9800 組み込みワイヤレスコントローラ • Cisco Catalyst 9100 アクセスポイント上の Cisco 組み込みワイヤレスコントローラ（EWC-AP）

[3] 必要な SSM オンプレミスの最小バージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

[4] 製品インスタンスに必要な最小ソフトウェアバージョン。これは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

SSM オンプレミスの詳細については、ソフトウェアダウンロードページの Smart Software Manager On-Prem [英語] を参照してください。ドキュメントリンクを表示するには、.iso イメージにカーソルを合わせます。

概念

ここでは、ポリシーを使用したスマートライセンシングの主要な概念について説明します。

ライセンス執行（エンフォースメント）タイプ

所与のライセンスは、3 つの適用タイプのいずれかに属します。適用タイプは、ライセンスを使用する前に承認が必要かどうかを示します。

- 不適用または非適用

  不適用ライセンスは、外部との接続がないネットワークで使用する前、または接続されたネットワークでの登録前に承認を必要としません。このようなライセンスの使用条件は、エンドユーザライセンス契約（EULA）に基づきます。

Cisco Catalyst ワイヤレスコントローラで使用可能なライセンスはすべて、不適用ライセンスです。

- 適用

  この適用タイプに属するライセンスは、使用前に承認が必要です。必要な承認は承認コードの形式で行われ、対応する製品インスタンスにインストールする必要があります。

  適用ライセンスの例としては、シスコの産業用イーサネットスイッチで利用可能な Media Redundancy Protocol（MRP）クライアントライセンスがあります。

- 輸出規制

  この適用タイプに属するライセンスは米国の取引規制法によって輸出が制限されていて、これらのライセンスは使用前に承認が必要です。これらのライセンスの場合も、必要な承認コードは、対応する製品インスタンスにインストールする必要があります。シスコは、ハードウェア購入の際に発注がある場合、輸出規制ライセンスをプリインストールすることがあります。

  輸出規制ライセンスの例としては、シスコの特定のルータで使用可能な高速暗号化（HSECK9）ライセンスがあります。

ライセンス継続期間

これは、購入したライセンスが有効な期間を指します。所与のライセンスは、上記のいずれかの適用タイプに属し、次の期間有効です。

- 永久：このライセンスには使用期限日はありません。

  AIR Network Essentials および AIR Network Advantage ライセンスは、Cisco Catalyst ワイヤレスコントローラで使用可能な不適用の永続的ライセンスの例です。

- サブスクリプション：ライセンスは特定の日付まで有効です。

  AIR Digital Network Architecture（DNA）Essentials および AIR DNA Advantage ライセンスは、Cisco Catalyst ワイヤレスコントローラで使用可能な不適用のサブスクリプション ライセンスの例です。

承認コード

スマートライセンシング承認コード（SLAC）は、輸出規制または適用（エンフォース）ライセンスの有効化および継続使用を可能にします。

SLAC は、Cisco Catalyst ワイヤレスコントローラで使用可能なライセンスには必要ありませんが、以前のライセンスモデルからポリシーを使用したスマートライセンシングにアップグレードする場合は、独自の承認コードを含む特定のライセンス予約（SLR）を持つことができます。SLR 承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後にサポートされるようになります。

（注） 既存の SLR はアップグレード後に引き継がれますが、「予約」の概念が適用されないため、ポリシーを使用したスマートライセンシング環境で新しい SLR を要求することはできません。エアギャップネットワークの場合は、代わりに CSSM への接続なし、CSLU なしのトポロジが適用されます。

SLR 承認コードの処理方法の詳細については、アップグレード （69 ページ） を参照してください。SLR 承認コードを返す場合は、承認コードの削除と返却 （146 ページ） を参照してください。

ポリシー

ポリシーは、製品インスタンスに次のレポート手順を提供します。

- License usage report acknowledgement requirement (Reporting ACK required)：ライセンス使用状況レポートは RUM レポートと呼ばれ、確認応答は ACK と呼ばれます（「RUM レポートおよびレポート確認応答」を参照）。これは、この製品インスタンスのレポートに CSSM 確認応答が必要かどうかを指定する yes または no の値です。デフォルトポリシーは常に「yes」に設定されます。
- First report requirement (days)：最初のレポートは、ここで指定した期間内に送信される必要があります。

  この値がゼロの場合、最初のレポートは必要ありません。
- Reporting frequency (days)：後続のレポートは、ここで指定した期間内に送信される必要があります。

  ここの値がゼロの場合、使用状況が変更されない限り、以降のレポートは必要ありません。
- Report on change (days)：ライセンスの使用状況が変更された場合は、ここで指定した期間内にレポートが送信される必要があります。

  ここの値がゼロの場合、使用状況の変更時のレポートは必要ありません。

  ここの値がゼロでない場合は、変更を加えた後にレポートが必要です。次に示すすべてのシナリオは、製品インスタンスのライセンス使用状況における変更としてカウントされます。
  - 消費されたライセンスの変更（別のライセンスへの変更やライセンスの追加または削除を含む）。
  - ライセンスの消費なしから 1 つ以上のライセンスの消費への移行。
  - 1 つ以上のライセンスの消費からライセンスの消費なしへの移行。

（注） 製品インスタンスがライセンスを使用していない場合、ポリシーのレポート要件（最初のレポート要件、レポート頻度、変更に関するレポート）のいずれかにゼロ以外の値が設定されていても、レポートは必要ありません。

ポリシー選択について

CSSMは、製品インスタンスに適用されるポリシーを決定します。特定の時点で使用されているポリシーは1つだけです。ポリシーとその値は、使用されているライセンスなど、さまざまな要因に基づいています。

`Cisco default`は、製品インスタンスで常に使用可能なデフォルトポリシーです。他のポリシーが適用されていない場合、製品インスタンスはこのデフォルトポリシーを適用します。次の表（表 3 : ポリシー：Cisco default （52 ページ））に、`Cisco default` ポリシー値を示します。

お客様はポリシーを設定することはできませんが、Cisco Global Licensing Operations チームに連絡して、カスタマイズされたポリシーを要求することができます。Support Case Manager に移動します。[OPEN NEW CASE] をクリックして、[Software Licensing] を選択します。ライセンスチームから、プロセスの開始や追加情報について連絡があります。カスタマイズされたポリシーは、CSSM のスマートアカウントを介して使用することもできます。

（注） 適用されているポリシー（使用中のポリシー）とそのレポート要件を確認するには、特権EXECモードで **show license all** コマンドを入力します。

表 *3 :* ポリシー：*Cisco default*

ポリシー：`Cisco default`	デフォルトポリシー値
Export (Perpetual/Subscription) （注） 適用タイプが「輸出規制」のライセンスにのみ適用されます。	Reporting ACK required：Yes First report requirement (days)：0 Reporting frequency (days)：0 Report on change (days)：0
Enforced (Perpetual/Subscription) （注） 適用タイプが「適用（エンフォース）」のライセンスにのみ適用されます。	Reporting ACK required：Yes First report requirement (days)：0 Reporting frequency (days)：0 Report on change (days)：0

ポリシー：`Cisco default`	デフォルトポリシー値
Unenforced/Non-Export Perpetual[5]	Reporting ACK required：Yes First report requirement (days)：365 Reporting frequency (days)：0 Report on change (days)：90
Unenforced/Non-Export Subscription	Reporting ACK required：Yes First report requirement (days)：90 Reporting frequency (days)：90 Report on change (days)：90

[5] Unenforced/Non-Export Perpetual の場合：デフォルトポリシーの最初のレポート要件（365日以内）は、ディストリビュータやパートナーからハードウェアやソフトウェアを購入した場合にのみ適用されます。

RUM レポートおよびレポート確認応答

リソース使用率測定レポート（RUM レポート）は、ポリシーで指定されたレポート要件を満たすためのライセンス使用状況レポートです。RUM レポートは製品インスタンスによって生成され、CSSMによって使用されます。製品インスタンスは、ライセンス使用状況情報とすべてのライセンス使用状況の変更を、開いている RUM レポートに記録します。システムが決定した間隔で、開いている RUM レポートが閉じられ、新しい RUM レポートが開かれて、ライセンスの使用状況の記録が継続されます。閉じられた RUM レポートは、いつでも CSSM に送信できます。

RUM確認応答（RUM ACK またはACK）はCSSMからの応答であり、RUM レポートのステータスに関する情報を提供します。レポートの ACK が製品インスタンスで使用可能になると、対応する RUM レポートが不要になり、削除できることが示されます。

レポート方式、つまり CSSM への RUM レポートの送信方法は、実装するトポロジによって異なります。

CSSM は、最後に受信した RUM レポートに従ってライセンス使用状況情報を表示します。

RUM レポートには、信頼コード要求や SLAC 要求などの他の要求が伴う場合があります。そのため、受信した RUM レポート ID に加えて、CSSM からの ACK には承認コード、信頼コード、およびポリシーファイルが含まれることがあります。

製品インスタンスに適用されるポリシーによって、レポート要件の次の側面が決まります。

- RUM レポートが CSSM に送信されるかどうか、およびこの要件を満たすために提供される最大日数。
- RUM レポートに CSSM からの確認応答（ACK）が必要かどうか。
- ライセンス消費の変化を報告するために提供される最大日数。

RUM レポートの生成、保存、管理

Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートの生成と関連プロセスが次のように最適化および強化されました。

- 製品インスタンスで使用可能なすべての RUM レポートのリストを表示できます（レポートの数、それぞれの処理状態、エラーがあるかどうかなど）。この情報は、**show license rum**、**show license all**、**show license tech** 特権 EXEC コマンドで使用できます。出力に表示されるフィールドの詳細については、対応するリリースのコマンドリファレンスを参照してください。
- RUM レポートは、処理時間を短縮し、メモリ使用量を削減する新しい形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、次の状況では、トポロジに適用される方法で RUM レポートを送信することをお勧めします。

  ポリシーを使用したスマートライセンシングをサポートする以前のリリースから、Cisco IOS XE Cupertino 17.7.1 以降のリリースにアップグレードする場合。

  Cisco IOS XE Cupertino 17.7.1 以降のリリースから、ポリシーを使用したスマートライセンシングをサポートする以前のリリースにダウングレードする場合。
- 継続的なディスク領域とメモリの可用性を確保するために、製品インスタンスは、対象と見なされる RUM レポートの削除を検出してトリガーします。

信頼コード

製品インスタンスが使用する *UDI* に関連付けられた公開キー

- RUM レポートに署名します。これにより、改ざんが防止され、データの真正性が確保されます。
- CSSM でセキュア通信を有効化します。

信頼コードを取得する方法は複数あります。

- Cisco IOS XE Cupertino 17.7.1 以降、すべての新規注文の信頼コードは出荷時にインストールされています。

（注） 出荷時にインストールされた信頼コードは、CSSM との通信には使用できません。

- 信頼コードは、IDMトークンを使用して CSSM から取得できます。

  ここでは SSM Web UI で *ID* トークンを生成して信頼コードを入手して製品インスタンスにインストールする必要があります。出荷時にインストールされた信頼コードがある場合は、上書きする必要があります。製品インスタンスが CSSM に直接接続されている場合は、この方法を使用して、製品インスタンスがCSSMと安全に通信できるようにします。

信頼コードを取得するこの方法は、CSSMに直接接続するすべてのオプションに適用できます。詳細については、CSSM に直接接続 （57 ページ）を参照してください。

- Cisco IOS XE Cupertino 17.7.1 以降では、信頼コードは、製品インスタンスが CSLU へのデータ送信を開始するトポロジと、製品インスタンスがエアギャップネットワーク内にあるトポロジで自動的に取得されます。

  出荷時にインストールされた信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM とのセキュアな通信に使用できます。

  トポロジの説明と対応するワークフローを参照して、各シナリオにおける信頼コードの要求およびインストール方法を確認してください（サポートされるトポロジ （55ページ））。

信頼コードが製品インスタンスにインストールされている場合、**show license status** コマンドの出力の [Trust Code Installed:] フィールドにタイムスタンプが表示されます。

サポートされるトポロジ

このセクションでは、ポリシーを使用したスマートライセンシングを実装するさまざまな方法について説明します。各トポロジについて、付属の概要を参照してセットアップの動作設計を確認し、考慮事項と推奨事項（ある場合）を参照してください。

トポロジを選択した後

トポロジを選択した後、ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （75 ページ） を参照してください。これらのワークフローは、新規展開のみに該当します。これらのワークフローにより、トポロジを実装する最も簡単で迅速な方法が実現します。

既存のライセンシングモデルから移行する場合は、ポリシーを使用したスマートライセンシングへの移行 （90 ページ） を参照してください。

初期実装後、追加の設定タスクを実行する必要がある場合（AIR ライセンスを変更する、RUM レポートを同期する場合など）は、「ポリシーを使用したスマートライセンシングのタスクライブラリ」を参照してください。

（注） 続行する前に、必ず「サポートされるトポロジ」を確認してください。

CSLU を介して CSSM に接続

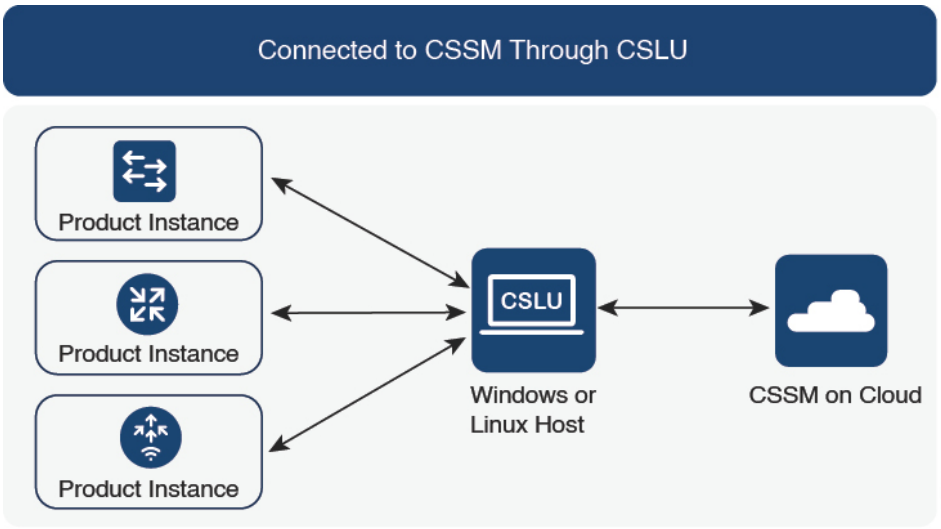
概要：

ここでは、ネットワーク内の製品インスタンスは CSLU に接続され、CSLU は CSSM との単一のインターフェイスポイントになります。製品インスタンスは、必要な情報を CSLU にプッシュするように設定できます。または、構成可能な頻度で製品インスタンスから必要な情報を取得するように CSLU を設定することもできます。

製品インスタンス開始型通信（プッシュ）：製品インスタンスは、CSLU の REST エンドポイントに接続することで、CSLU との通信を開始します。送信されるデータには、RUM レポート、および承認コード、UDI に関連付けられた信頼コード、ポリシーの要求が含まれます。必要な間隔で自動的に RUM レポートを CSLU に送信するように製品インスタンスを設定できます。これは、製品インスタンスのデフォルトの方法です。

CSLU 開始型通信（pull 型）：製品インスタンスからの情報の取得を開始するために、CSLU は YANG を使用した NETCONF、RESTCONF、gRPC のモデル、またはネイティブ REST API を使用して製品インスタンスに接続します。サポートされるワークフローには、RUM レポートの製品インスタンスからの受信と CSSM への送信、承認コードのインストール、UDI に関連付けられた信頼コードのインストール、およびポリシーの適用が含まれます。

図 *2:* トポロジ：***CSLU*** を介して ***CSSM*** に接続



考慮事項または推奨事項：

ネットワークのセキュリティポリシーに応じて通信方法を選択します。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1 以降：

- 信頼コードの要求とインストール

  信頼コードが製品インスタンスで使用できない場合、製品インスタンスは RUM レポートの一部として、信頼コードの要求を検出し、自動的に要求を含めます。CSSM からの対応する ACK には信頼コードが含まれています。出荷時にインストールされた既存の信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM との通信に使用できます。

これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないすべての接続製品インスタンスの信頼コードを要求します。

このリリースでは、この拡張は、製品インスタンス開始モードにのみ適用されます。

- RUM レポートスロットリング

  製品インスタンス開始モードでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

  特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

  RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリースおよび 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースに適用されます。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSLU を介して CSSM に接続 （75 ページ）を参照してください。

CSSM に直接接続

概要：

このトポロジは、スマートライセンシングの以前のバージョンで使用でき、ポリシーを使用したスマートライセンシングで引き続きサポートされます。

ここでは、製品インスタンスから CSSM への直接かつ信頼できる接続を確立します。直接接続には、CSSM へのネットワーク到達可能性が要求されます。その後、製品インスタンスがメッセージを交換し、CSSM と通信するには、このトポロジで使用可能な転送オプションのいずれかを設定します（以下を参照）。最後に、信頼を確立するには、CSSM の対応するスマートアカウントとバーチャルアカウントからトークンを生成し、製品インスタンスにインストールする必要があります。

（注） 出荷時にインストールされた信頼コードは、CSSM との通信には使用できません。つまり、このトポロジでは、出荷時にインストールされた信頼コードが存在する場合でも、CSSM で ID トークンを生成して信頼コードを取得し、出荷時にインストールされた既存の信頼コードを上書きする必要があります。信頼コード （54 ページ）も参照してください。

次の方法で CSSM と通信するように製品インスタンスを設定できます。

- スマート転送を使用して CSSM と通信する。

  スマート転送は、スマートライセンシング（JSON）メッセージが HTTPS メッセージ内に含まれ、製品インスタンスと CSSM の間で交換されることにより通信する転送方法です。次のスマート転送設定オプションを使用できます。

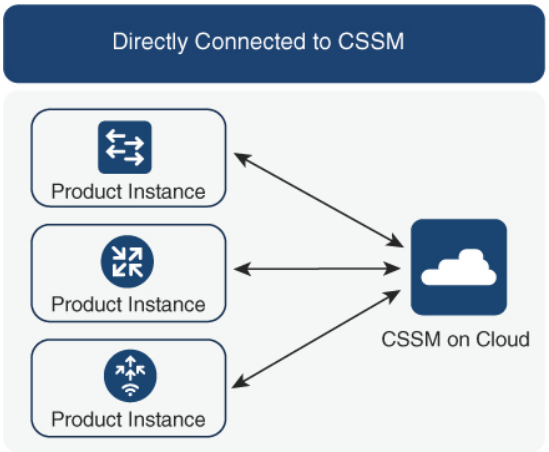
  - スマート転送：この方法では、製品インスタンスは特定のスマート転送ライセンスサーバ URL を使用します。これは、ワークフローのセクションに示すとおりに設定する必要があります。
  - HTTPS プロキシを介したスマート転送：この方法では、製品インスタンスはプロキシサーバを使用してライセンスサーバと通信し、最終的には CSSM と通信します。

- Call Home を使用して CSSM と通信する。

  Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。CSSM へのこの接続方法は、以前のスマートライセンシング環境で使用でき、ポリシーを使用したスマートライセンシングで引き続き使用できます。次の Call Home 設定オプションを使用できます。

  - ダイレクトクラウドアクセス：この方法では、製品インスタンスはインターネット経由で CSSM に使用状況情報を直接送信します。接続に追加のコンポーネントは必要ありません。
  - HTTPS プロキシを介したダイレクトクラウドアクセス：この方法では、製品インスタンスはインターネット経由でプロキシサーバ（Call Home Transport Gateway または市販のプロキシ（Apache など）のいずれか）を介して CSSM に使用状況情報を送信します。

図 *3*：トポロジ：*CSSM* に直接接続



考慮事項または推奨事項：

CSSM に直接接続する場合は、スマート転送が推奨される転送方法です。この推奨事項は以下に適用されます。

- 新規展開。
- 以前のライセンスモデル。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。
- 現在 Call Home 転送方法を使用している登録済みライセンス。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。
- 以前のライセンスモデルの評価ライセンスや期限切れのライセンス。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。

移行後に設定を変更するには、トポロジのワークフロー：CSSM に直接接続 （78 ページ）の「製品インスタンスの設定」にある「接続方法と転送タイプの設定」のオプション1を参照してください。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

- RUM レポートスロットリング

  このトポロジでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

  特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

  RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリースおよび 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースに適用されます。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSSM に直接接続 （78 ページ）を参照してください。

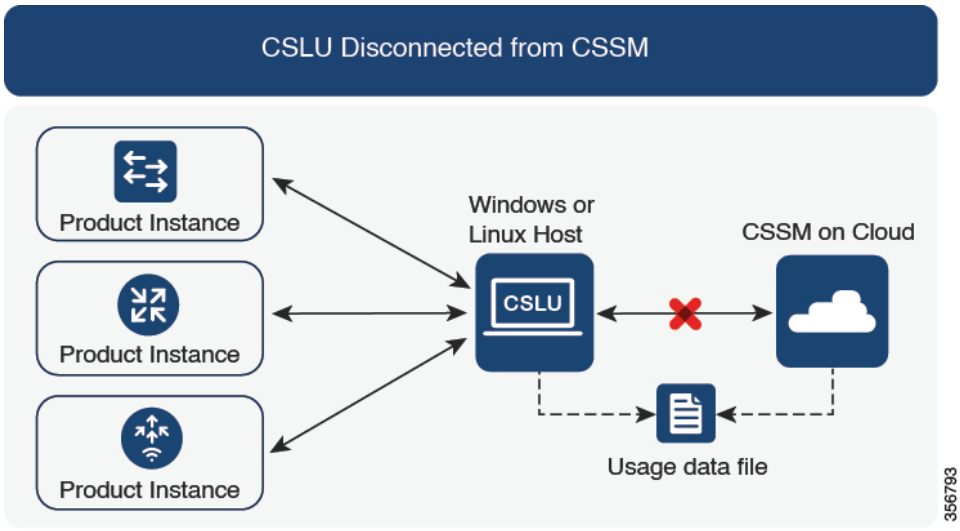
CSLU は CSSM から切断

概要：

ここでは、製品インスタンスが CSLU と通信し、製品インスタンス開始の通信または CSLU 開始の通信を実装するオプションがあります（CSLU を介して CSSM に接続のトポロジと同様）。CSLU と CSSM 間の通信のもう一方はオフラインです。CSLU には、CSSM から切断されたモードで動作するオプションがあります。

CSLU と CSSM 間の通信は、署名済みファイルの形式で送受信され、オフラインで保存された後、場合によっては CSLU または CSSM にアップロードまたはダウンロードされます。

図 *4:* トポロジ：*CSLU* は *CSSM* から切断



考慮事項または推奨事項：

ネットワークのセキュリティポリシーに応じて通信方法を選択します。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1 以降：

- 信頼コードの要求とインストール

  信頼コードが製品インスタンスで使用できない場合、製品インスタンスは、CSLU に送信される RUM レポートの一部として要求を検出し、自動的にその要求を含めます。この要求は、CSSM にアップロードされます。CSSM からダウンロードする ACK には信頼コードが含まれています。出荷時にインストールされた既存の信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM との通信に使用できます。

  これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないメンバーやスタンバイの信頼コードを要求します。

  このリリースでは、この拡張は、製品インスタンス開始モードにのみ適用されます。

- RUM レポートスロットリング

  製品インスタンス開始モードでは、レポートの最小頻度は 1 日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これに

より、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリースおよび 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースに適用されます。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSLU は CSSM から切断 （79 ページ）を参照してください。

コントローラを介して CSSM に接続

コントローラを使用して製品インスタンスを管理する場合、コントローラはCSSMに接続してCSSM とのすべての通信のインターフェイスとなります。Cisco Catalyst ワイヤレスコントローラでサポートされているコントローラは、Cisco DNA Center です。

概要：

Cisco DNA Center がコントローラとして製品インスタンスを管理している場合、製品インスタンスはライセンスの使用状況を記録し、保存しますが、Cisco DNA Center が RUM レポートを取得し、CSSM に報告し、製品インスタンスにインストールするために ACK を返すために製品インスタンスとの通信を開始します。

Cisco DNA Center で管理する必要があるすべての製品インスタンスは、そのインベントリの一部である必要があり、サイトに割り当てる必要があります。Cisco DNA Center は NETCONF プロトコルを使用して設定をプロビジョニングし、製品インスタンスから必要な情報を取得します。したがって、これを容易にするために製品インスタンスでNETCONF を有効にする必要があります。

レポートの要件を満たすために、Cisco DNA Center は CSSM から該当するポリシーを取得し、次のレポートオプションを提供します。

- Ad hoc reporting：必要に応じてアドホックレポートをトリガーできます。
- Scheduled reporting：ポリシーで指定されたレポート頻度に対応し、Cisco DNA Center によって自動的に処理されます。

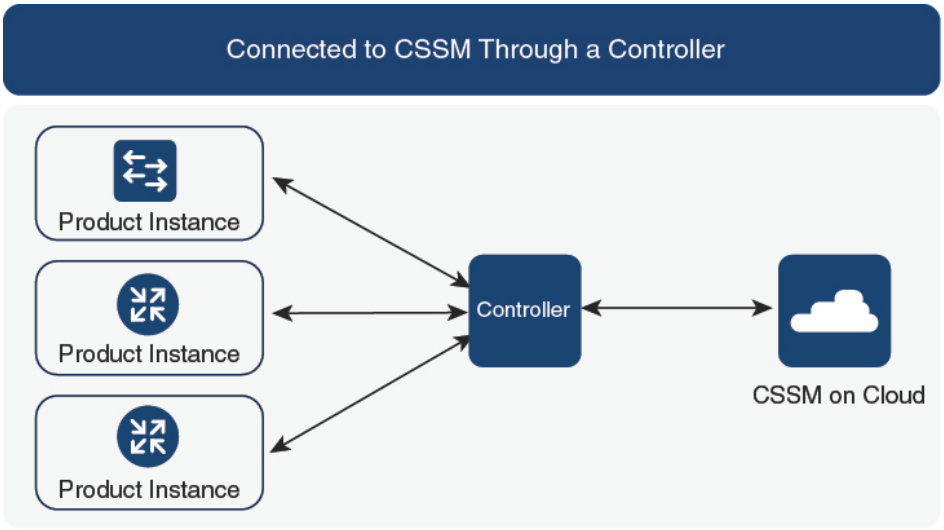
（注） 製品インスタンスが定期レポートの対象となる前に、アドホックレポートを少なくとも 1 回実行する必要があります。

最初のアドホックレポートにより、Cisco DNA Center は、後続の RUM レポートをアップロードする必要があるスマートアカウントとバーチャルアカウントを決定できます。製品インスタンスのアドホックレポートが一度も実行されていない場合は、通知されます。

Cisco DNA Center では、輸出規制ライセンス用の SLAC のインストールと削除ができます。Cisco Catalyst ワイヤレスコントローラで使用可能なライセンスはすべて不適用ライセンスであるため、SLAC のインストールと削除は適用されません。

信頼コードは必要ありません。

図 *5:* トポロジ：コントローラを介して *CSSM* に接続



考慮事項または推奨事項：

これは、Cisco DNA Center を使用している場合に推奨されるトポロジです。

次の手順：

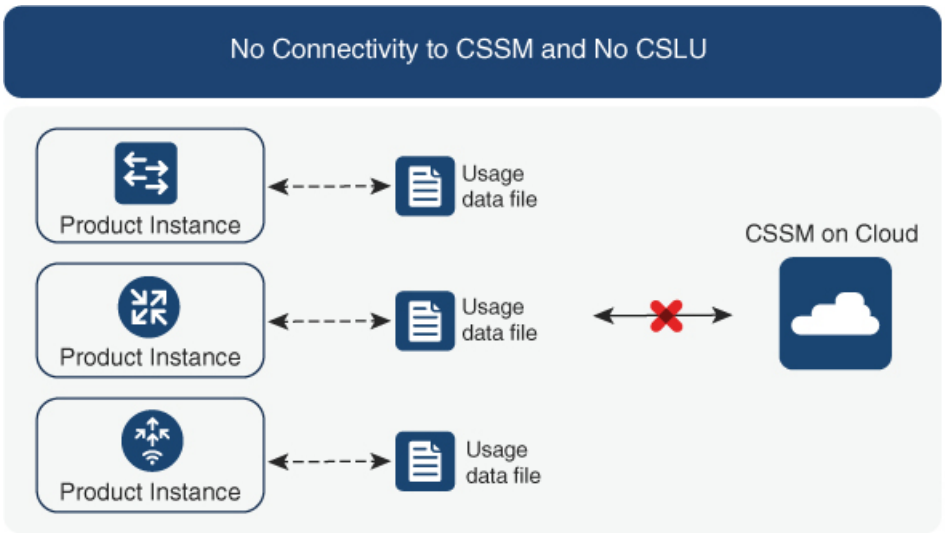
このトポロジを実装するには、トポロジのワークフロー：コントローラを介して CSSM に接続（83 ページ）を参照してください。

CSSM への接続なし、CSLU なし

概要：

ここでは、製品インスタンスと CSSM は相互に切断され、他の中間ユーティリティまたはコンポーネントはありません。すべての通信は、ファイルのアップロードとダウンロードという形式です。これらのファイルは、RUM レポート UDI に関連付けられた信頼コードの要求です。

図 *6 :* トポロジ：*CSSM* への接続なし、*CSLU* なし



考慮事項または推奨事項：

このトポロジは、製品インスタンスがネットワークの外部とオンラインで通信できない高セキュリティ展開に適しています。

リリースごとの変更と拡張

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1 以降：

- 信頼コードの要求とインストール

  製品インスタンスで信頼コードが使用できない場合、製品インスタンスは、ユーザーが保存し、CSSM にアップロードする RUM レポートに信頼コードの要求を自動的に含めます。CSSM からダウンロードする ACK には信頼コードが含まれています。

  出荷時にインストールされた信頼コードがある場合、ACK をインストールすると自動的に上書きされます。この方法で取得した信頼コードは、CSSM とのセキュアな通信に使用できます。

  これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないすべての接続製品インスタンスの信頼コードを要求します。

- よりシンプルな承認コードの返却

  承認コードの返却ファイルをアップロードする簡単な方法を CSSM Web UI で使用できます。CSSM Web UI で正しいバーチャルアカウントの製品インスタンスを見つける必要がなくなりました。RUM レポートと同様に、返却ファイルをアップロードできます。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSSM への接続なし、CSLU なし（84 ページ）を参照してください。

SSM オンプレミス展開

概要：

SSM オンプレミスは、オンプレミスに展開される CSSM の拡張として機能するように設計されています。

ここでは、製品インスタンスが SSM オンプレミスに接続され、SSM オンプレミスが CSSM との単一のインターフェイスポイントになります。SSM オンプレミスの各インスタンスは、SSM オンプレミスのローカルアカウントに必須の登録と同期を通じて、CSSM 内のバーチャルアカウントを使用して CSSM に通知する必要があります。

製品インスタンスを管理するために SSM オンプレミスを展開する場合、SSM オンプレミスに必要な情報をプッシュするように製品インスタンスを設定できます。または、設定可能な頻度で製品インスタンスから必要な情報をプルするように SSM オンプレミスを設定することもできます。

- 製品インスタンス開始型通信（プッシュ）：製品インスタンスは SSM オンプレミスの REST エンドポイントを接続することで SSM オンプレミスの通信を開始します。送信されるデータには、RUM レポート、および承認コード、信頼コード、ポリシーの要求が含まれます。

  このモードでの製品インスタンスと SSM オンプレミス間の通信のオプション：

  - 必要に応じて、CLI コマンドを使用して SSM オンプレミスに情報をプッシュします。
  - スケジュールされた頻度で RUM レポートを SSM オンプレミスに自動的に送信するには、CLI コマンドを使用し、レポート間隔を設定します。

- SSM オンプレミス開始型通信（プル）：製品インスタンスからの情報の取得を開始するには、SSM オンプレミスで NETCONF、RESTCONF、およびネイティブの REST API オプションを使用して製品インスタンスを接続します。サポートされるワークフローには、RUM レポートの製品インスタンスからの受信と CSSM への送信、承認コードのインストール、信頼コードのインストール、およびポリシーの適用が含まれます。

  このモードでの製品インスタンスと SSM オンプレミス間の通信のオプション：

  - 必要に応じて（オンデマンドで）、1 つ以上の製品インスタンスから使用状況情報を収集します。
  - スケジュールされた頻度で 1 つ以上の製品インスタンスから使用状況情報を収集します。

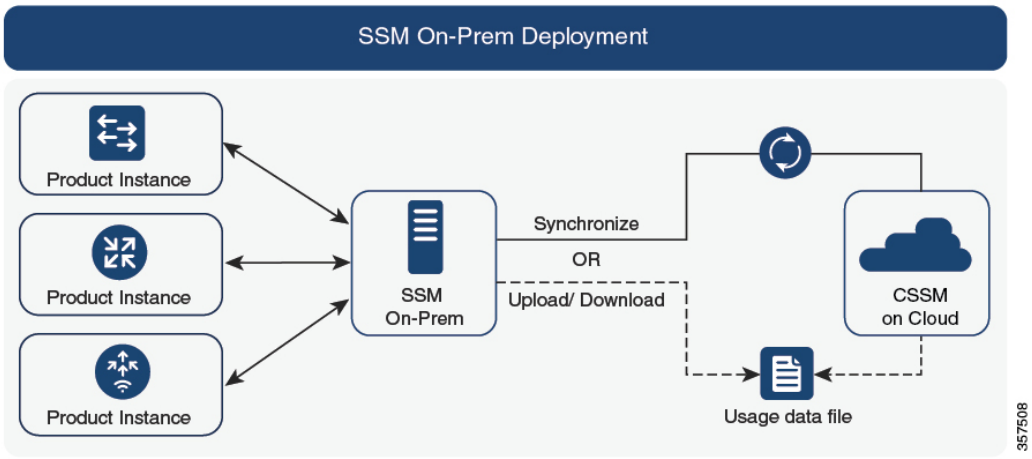
SSMオンプレミスでは、レポート間隔が製品インスタンスのデフォルトポリシーに設定されます。これは変更できますが、より頻繁に（より短い間隔で）レポートを作成するか、または使用可能な場合はカスタムポリシーをインストールできます。

SSM オンプレミスで使用状況が使用できるようになったら、同じ間隔で CSSM と同期して、製品インスタンス数、ライセンス数、およびライセンス使用状況情報が CSSM と SSM オンプレミスの両方と同じであることを確認します。SSM オンプレミスと CSSM 間の使用状況の同期オプション：プッシュとプルモードの場合：

- CSSM でアドホック同期を実行します（Cisco と同期されました）。
- 指定した時刻で CSSMとの同期をスケジュールします。
- オフラインで保存されている指名済みファイルを通じて CSSM と通信し、場合によって SSM オンプレミスまたは CSSM からアップロードするか、またはダウンロードします。

（注） このトポロジでは、SSM オンプレミスと CSSM 間で 2 つの異なる同期が行われます。1 つは、ローカルアカウントと CSSM との同期です。この同期は、SSM オンプレミスインスタンスに CSSM を認識させるためであり、SSM オンプレミスの [Synchronization] ウィジェットを使用して実行します。2 番目は、CSSM に接続するか、またはファイルをダウンロードおよびアップロードすることのいずれかによるライセンスの使用状況の CSSM との同期です。ライセンスの使用状況を同期する前に、ローカルアカウントを同期する必要があります。

図 *7:* トポロジ：***SSM*** オンプレミス展開



考慮事項または推奨事項：

このトポロジは、次の状況に適しています。

- CSSM と直接通信せずにオンプレミスで製品インスタンスを管理する場合。
- 会社のポリシーにより、製品インスタンスでライセンスの使用状況をシスコ（CSSM）に直接報告できない場合。

- 製品インスタンスがエアギャップネットワーク内にあり、ネットワーク外にあるものとオンラインで通信できない場合。

Smart Licensing Using Policy のサポートとは別に、SSM オンプレミスのバージョン 8 の主な利点は次のとおりです。

- マルチテナント：1 つのテナントが 1 つのスマートアカウントとバーチャルアカウントのペアを構成します。SSM オンプレミスでは複数のペアを管理できます。ここでは、SSM オンプレミスに存在するローカルアカウントを作成します。CSSM のスマートアカウントとバーチャルアカウントのペアへの複数のローカルアカウントのロールアップ。詳細については、『Cisco Smart Software Manager On-Prem User Guide』[英語] の「About Accounts and Local Virtual Accounts」を参照してください。

（注） CSSM と SSM オンプレミスのインスタンス間の関係は、まだ 1 対 1 です。

- スケール：合計 300,000 の製品インスタンスをサポートします。
- 高可用性：2 台の SSM オンプレミスサーバをアクティブ/スタンバイクラスタの形式で実行できます。詳細については、『Cisco Smart Software On-Prem Installation Guide』[英語] の「Appendix 4 Managing a High Availability (HA) Cluster in Your System」を参照してください。

  高可用性展開は SSM オンプレミスのコンソールでサポートされています。必要なコマンドの詳細については、『Cisco Smart Software On-Prem Console Guide』[英語] を参照してください。
- CSSM へのオンライン接続とオフライン接続のオプション。

SSM オンプレミスの制限：

- ライセンス使用の同期を目的とした CSSM との通信のプロキシサポートが利用できるのは、バージョン 8 202108 以降のみです。ローカルアカウントの同期を目的とするプロキシの使用はサポートされています。これは [Synchronization] ウィジェットを使用して実行され、Smart Licensing Using Policy がサポートされている SSM オンプレミス導入リリースから利用可能です。
- SSM オンプレミス開始型通信は、ネットワークアドレス変換（NAT）設定の製品インスタンスではサポートされていません。製品インスタンス開始型通信を使用する必要があります。さらに、NAT 設定の製品インスタンスをサポートするために SSM オンプレミスを有効にする必要があります。詳細は、このトポロジのワークフローで提供されます。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.9.1 以降：

- RUM レポートスロットリング

  製品インスタンス開始モードでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

  特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

  RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリースおよび 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースに適用されます。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：SSM オンプレミス展開 （85 ページ）を参照してください。

SSM オンプレミスの既存のバージョンから移行する場合は、アップグレード関連のさまざまなアクティビティを実行する順序が重要です。Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行 （112 ページ） を参照してください

他の機能との相互作用

ハイ アベイラビリティ

このセクションでは、ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンを実行するときに、高可用性設定に適用される考慮事項について説明します。次の高可用性セットアップは、このドキュメントの範囲内です。

デュアルシャーシのセットアップ（固定またはモジュラ）。一方のシャーシにアクティブ、もう一方のシャーシにスタンバイがあります。

ワイヤレス N+1 トポロジでは、「n」個のワイヤレスコントローラがプライマリとして機能し、「+1」のワイヤレスコントローラがアクセスポイント（AP）のセカンダリまたはフォールバック ワイヤレス コントローラとして機能します。各アクセスポイントには、プライマリ ワイヤレス コントローラとセカンダリ ワイヤレス コントローラが設定されています。プライマリで障害が発生した場合、プライマリに接続されていたすべてのアクセスポイントがセカンダリ ワイヤレス コントローラにフォールバックするようになりました。

高可用性セットアップでの信頼コード要件

必要な信頼コードの数は、UDI の数によって異なります。アクティブな製品インスタンスは、高可用性セットアップのすべてのデバイスに対する要求を送信し、ACK で返されるすべての信頼コードをインストールできます。

高可用性セットアップでのポリシー要件

高可用性セットアップにのみ適用されるポリシー要件はありません。スタンドアロン製品インスタンスの場合と同様に、高可用性セットアップにも1つのポリシーのみが存在し、これがアクティブになります。アクティブのポリシーは、セットアップのすべてのスタンバイに適用されます。

高可用性セットアップでの製品インスタンス機能

ここでは、高可用性設定での一般的な製品インスタンス機能と、新しいスタンバイまたはセカンダリが既存の高可用性設定に追加された場合の製品インスタンスの動作について説明します。

承認コードと信頼コードの場合：アクティブな製品インスタンスは、スタンバイの承認コードと信頼コードを要求し（必要な場合）、インストールできます。

ポリシーの場合：アクティブな製品インスタンスがスタンバイと同期します。

レポートの場合：アクティブな製品インスタンスのみが使用状況を報告します。アクティブな場合、高可用性設定のすべてのデバイスの使用状況情報を報告します。スケジュールされたレポートに加えて、次のイベントがレポートをトリガーします。

- スタンバイの追加または削除。RUM レポートには、追加または削除されたスタンバイに関する情報が含まれます。
- スイッチオーバー。
- リロード。

上記のいずれかのイベントが発生すると、**show license status** 特権EXECコマンドの [Next report push] の日付が更新されます。ただし、レポートが製品インスタンスによって送信されるかどうかは、実装されたトポロジと関連するレポート方法で決まります。たとえば、製品インスタンスが切断されているトポロジ（[Transport Type] が [Off]）を実装した場合は、[Next report push] の日付が更新されても、製品インスタンスは RUM レポートを送信しません。

新しいスタンバイの追加または削除の場合：

- CSLU に接続されている製品インスタンスは、それ以上のアクションを実行しません。
- CSSMに直接接続されている製品インスタンスは、信頼の同期を実行します。信頼の同期には、次のものが含まれます。

  スタンバイでの信頼コードのインストール（まだインストールされていない場合）。

  信頼コードがすでにインストールされている場合は、信頼の同期プロセスにより、新しいスタンバイがアクティブと同じスマートアカウントおよびバーチャルアカウントにあることが保証されます。そうでない場合、新しいスタンバイは、アクティブと同じスマートアカウントとバーチャルアカウントに移動されます。

  承認コード、ポリシー、および購入情報のインストール（該当する場合）

  現在の使用状況情報を含む RUM レポートの送信。

セカンダリの追加または削除の場合：

セカンダリ製品インスタンスの追加または削除にのみ適用される製品インスタンス機能はありません。さらに、すべてのセカンダリ製品インスタンスは、プライマリ製品インスタンスと同じスマートアカウントおよびバーチャルアカウントにあります。

アップグレード

このセクションでは、次の点について説明します。

以前のライセンスモデルから Smart Licensing Using Policy への移行以前のライセンスモデルから移行する場合は、Cisco Catalyst ワイヤレスコントローラに適用される移行シナリオの例について、ポリシーを使用したスマートライセンシングへの移行 （90 ページ）セクションも参照してください。

Smart Licensing Using Policy 環境でのアップグレード：アップグレード元のソフトウェアバージョンとアップグレード先のソフトウェアバージョンの両方で、Smart Licensing Using Policy がサポートされます。

アップグレード前に現在のライセンシングモデルを識別する

ポリシーを使用したスマートライセンシングにアップグレードする前に、製品インスタンスで有効な現在のライセンシングモデルを確認するには、特権 EXEC モードで **show license all** コマンドを入力します。

アップグレードが既存ライセンスの適用タイプに与える影響

ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードする場合、既存ライセンスの処理方法は、主に適用タイプによって決まります。

- アップグレード前に使用されていた不適用ライセンスは、アップグレード後も引き続き使用できます。Cisco Catalyst ワイヤレスコントローラのすべてのライセンスは、不適用ライセンスです。これには、以前のすべてのライセンシングモデルのライセンスが含まれます。
  - スマートライセンス
  - 特定のライセンス予約（SLR）。承認コードが付属しています。承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後も引き続き有効であり、既存のライセンスの使用を承認します。
  - 上記のライセンシングモデルのいずれかの評価ライセンスまたは期限切れライセンス。
- アップグレード前に使用されていた適用ライセンスや輸出規制ライセンスは、必要な承認が存在する場合、アップグレード後も引き続き使用できます。

  サポートされている Cisco Catalyst ワイヤレスコントローラのいずれにも、輸出規制ライセンスや適用ライセンスがないため、これらの適用タイプと必要な SLAC は適用されません。

アップグレードが既存ライセンスのレポートに与える影響

既存ライセンス	ポリシーを使用したスマートライセンシングへの移行後のレポート要件
特定のライセンス予約（SLR）	ライセンス消費に変更がある場合にのみ必要です。 既存の SLR 承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後に既存のライセンス消費を承認します。
スマートライセンシング（登録および承認済みライセンス）	ポリシーによって異なります。
評価ライセンスまたは期限切れライセンス	シスコのデフォルトポリシーのレポート要件に基づいています。

アップグレードが既存ライセンスの転送タイプに与える影響

既存の設定で転送タイプが設定されている場合、ポリシーを使用したスマートライセンシングへのアップグレード後も転送タイプが保持されます。

スマートライセンシングの以前のバージョンと比較した場合、ポリシーを使用したスマートライセンシングでは追加の転送タイプを使用できます。デフォルトの転送モードにも変更があります。次の表に、これがアップグレードに与える影響を示します。

アップグレード前の転送タイプ	アップグレード前のライセンスまたはライセンスの状態	アップグレード後の転送タイプ
デフォルト（callhome）	評価	cslu（ポリシーを使用したスマートライセンシングのデフォルト）
	SLR	off
	登録	callhome
smart	評価	off
	SLR	off
	登録	smart

アップグレードがトークン登録プロセスに与える影響

以前のバージョンのスマートライセンシングでは、CSSMへの登録と接続にトークンが使用されていました。ID トークンの登録は、ポリシーを使用したスマートライセンシングでは必要ありません。トークン生成機能はCSSMでも引き続き使用でき、製品インスタンスがCSSMに直接接続されている場合に信頼を確立するために使用されます。「CSSMに直接接続」を参照してください。

Smart Licensing Using Policy 環境内のアップグレード

この項では、Smart Licensing Using Policy がサポートされているリリースから Smart Licensing Using Policy がサポートされているリリースに製品インスタンスをアップグレードする場合に適用される、リリース固有の考慮事項またはアクションについて説明します。

Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートは処理時間を短縮する形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、ポリシーを使用したスマートライセンシングをサポートする以前のリリースから Cisco IOS XE Cupertino 17.7.1 以降のリリースにアップグレードする場合は、標準的な方法として 1 回の使用状況レポートを完了することをお勧めします。

ダウングレード

ここでは、新規展開と既存の展開に関する以前のライセンスモデルへのダウングレードについて説明します。また、ポリシーを使用したスマートライセンシング環境内のダウングレードに関連する情報についても説明します。

新規展開のダウングレード

このセクションでは、Smart Licensing Using Policy がデフォルトで有効になっているソフトウェアバージョンで新しく購入した製品インスタンスが、Smart Licensing Using Policy がサポートされていないソフトウェアバージョンにダウングレードされた場合に適用される考慮事項とアクションについて説明します。

ダウングレードの結果は、ポリシーを使用したスマートライセンシング環境での操作中に信頼コードがインストールされたかどうかによって異なります。ダウングレード先のリリースによっては、追加のアクションが必要になる場合があります。

ポリシーを使用したスマートライセンシング環境で実装したトポロジが「CSSMに直接接続」である場合、トポロジ実装の一部として信頼コードが必要であるため、信頼コードのインストールが想定または仮定されます。他のトポロジでは、信頼の確立は必須ではありません。そのため、他のトポロジのいずれかを使用する製品インスタンスをダウングレードすると、スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元する必要が生じます。以下の表（スマートライセンシングへの新規展開のダウングレードの結果とアクション）を参照してください。

表 *4:* スマートライセンシングへの新規展開のダウングレードの結果とアクション

ポリシーを使用したスマートライセンシング環境で	以下にダウングレードした場合…	結果と追加のアクション
CSSM に直接接続され、信頼が確立されたスタンドアロン製品インスタンス。	Cisco IOS XE Amsterdam 17.3.1 または Cisco IOS XE Gibraltar 16.12.x の Cisco IOS XE Gibraltar 16.12.4 以降のリリース	これ以上の操作は不要です。 製品インスタンスは、ダウングレード後に CSSM からの信頼を更新しようとします。 更新が正常に完了すると、ライセンスは登録済みの状態になり、以前のバージョンのスマートライセンシングが製品インスタンスで有効になります。
	スマートライセンシングをサポートするその他のリリース（上の行に記載されているものを除く）	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken** *idtoken* コマンドを設定します。
CSSM に直接接続され、信頼が確立された高可用性セットアップ。	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken** *idtoken* **all** コマンドを設定します。
その他のトポロジ。（CSLU を介した CSSM への接続、CSLU は CSSM から切断、CSSM への接続なし、CSLU なし）	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。 スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元します。

アップグレード後のダウングレード

ここでは、ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンに製品インスタンスをアップグレードしてから、以前のライセンスモデルにダウングレードする場合に適用される、考慮事項とアクションについて説明します。

そのような製品インスタンスをダウングレードしても、ライセンスの使用は変更されず、製品インスタンスで設定した製品機能は維持されます。ポリシーを使用したスマートライセンシングで使用可能な機能のみが使用できなくなります。以前のライセンシングモデルへの復帰の詳細については、以下の対応するセクションを参照してください。

ポリシーを使用したスマートライセンシングへのアップグレード後のスマートライセンシングへのダウングレード

ダウングレードの結果は、ポリシーを使用したスマートライセンシング環境での操作中に信頼コードがインストールされたかどうかによって異なります。ダウングレード先のリリースによっては、さらにアクションが必要になる場合があります。次の表を参照してください。

表 *5:* ポリシーを使用したスマートライセンシングへのアップグレード後のスマートライセンシングへのダウングレードの結果とアクション

ポリシーを使用したスマートライセンシング環境で	以下にダウングレードした場合…	結果と追加のアクション
CSSM に直接接続され、信頼が確立されたスタンドアロン製品インスタンス。	Cisco IOS XE Amsterdam 17.3.1 または Cisco IOS XE Gibraltar 16.12.x の Cisco IOS XE Gibraltar 16.12.4 以降のリリース	これ以上の操作は不要です。 システムは信頼コードを認識し、元の登録済みID トークンに変換します。これにより、ライセンスは AUTHORIZED および REGISTERED の状態に戻ります。
	スマートライセンシングをサポートするその他のリリース（上の行に記載されているものを除く）	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken***idtoken* コマンドを設定します。

ポリシーを使用したスマートライセンシング環境で	以下にダウングレードした場合...	結果と追加のアクション
CSSM に直接接続され、信頼が確立された高可用性セットアップ。	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken** *idtoken* **all** コマンドを設定します。
その他のトポロジ（CSLU を介した CSSM への接続、CSLU は CSSM から切断、CSSM への接続なし、CSLU なし）	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。 スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元します。

（注） スマートライセンシング環境で評価状態または期限切れ状態になっていたライセンスは、ダウングレード後に同じ状態に戻ります。

ポリシーを使用したスマートライセンシングへのアップグレード後の SLR へのダウングレード

SLR に戻すのに必要な操作は、イメージのダウングレードのみです。ライセンスは予約済みおよび承認済みのままになります。これ以上の操作は必要ありません。

ただし、ポリシーを使用したスマートライセンシング環境で SLR に戻した場合は、サポートされているリリースで、必要に応じて SLR を取得するプロセスを繰り返す必要があります。

Smart Licensing Using Policy 環境内のダウングレード

この項では、Smart Licensing Using Policy がサポートされているリリースから Smart Licensing Using Policy がサポートされている別のリリースに製品インスタンスをダウングレードする場合に適用される、リリース固有の考慮事項またはアクションについて説明します。

Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートは処理時間を短縮する形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、Cisco IOS XE Cupertino 17.7.1 以降のリリースからポリシーを使用したスマートライセンシングをサポートする以前のリリースにダウングレードする際に、使用状況レポートを 1 回完了することをお勧めします。

ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー

このセクションでは、トポロジを実装する最も簡単で迅速な方法について説明します。

（注） これらのワークフローは、新規展開のみに該当します。既存のライセンシングモデルから移行する場合は、ポリシーを使用したスマートライセンシングへの移行 （90 ページ） を参照してください。

トポロジのワークフロー：CSLU を介して CSSM に接続

製品インスタンス開始型通信とCSLU開始型通信のどちらを実装するかに応じて、対応する一連のタスクを実行します。

- 製品インスタンス開始型通信の場合のタスク
- CSLU 開始型通信の場合のタスク

製品インスタンス開始型通信の場合のタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定

1. ***CSLU* のインストール**

   タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン（VM）。

   [Smart Software Manager]https://software.cisco.com/download/home/286285506/type> [Smart Licensing Utility] からファイルをダウンロードします。

   インストールとセットアップの詳細については、『Cisco Smart License Utility クイック スタート セットアップ ガイド』および『Cisco Smart License Utility ユーザーガイド』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU

   1. シスコへのログイン（CSLU インターフェイス） （114 ページ）
   2. スマートアカウントとバーチャルアカウントの設定（CSLUインターフェイス） （115 ページ）
   3. CSLU での製品開始型製品インスタンスの追加（CSLUインターフェイス） （116 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   1. 製品インスタンス開始型通信のネットワーク到達可能性の確認 （116 ページ）
   2. 転送タイプが **cslu** に設定されていることを確認します。

      CSLU がデフォルトの転送タイプです。別のオプションを設定した場合は、グローバル コンフィギュレーション モードで **license smart transport cslu** コマンドを入力します。構成ファイルへの変更を保存します。

      ```
      Device(config)# license smart transport cslu
      Device(config)# exit
      Device# copy running-config startup-config
      ```

   3. CSLU の検出方法を指定します（1 つ選択）

      - オプション 1：

        No action required.`cslu-local` のゼロタッチ DNS ディスカバリ用に設定されたネームサーバ

        ここでは、DNS を設定してあり（ネームサーバーの IP アドレスが製品インスタンスで設定されている）、ホスト名 `cslu-local` が CSLU IP アドレスにマッピングされているエントリが DNS サーバーにある場合、追加のアクションは不要です。製品インスタンスは、ホスト名 `cslu-local` を自動的に検出します。

      - オプション 2：

        No action required.`cslu-local.<domain>` のゼロタッチ DNS ディスカバリ用に設定されたネームサーバとドメイン

        ここでは、DNS を設定してあり（ネームサーバーの IP アドレスとドメインが製品インスタンスで設定されている）、`cslu-local.<domain>` が CSLU IP アドレスにマッピングされているエントリが DNS サーバーにある場合、追加のアクションは不要です。製品インスタンスは、ホスト名 `cslu-local` を自動的に検出します。

      - オプション 3：

        CSLU に特定の URL を設定します。

        グローバル コンフィギュレーション モードで **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* コマンドを入力します。`<cslu_ip_or_host>` には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

        ```
        Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
        Device(config)# exit
        Device# copy running-config startup-config
        ```

結果：

製品インスタンスは通信を開始すると、ポリシーに従って、スケジュールされた時刻に最初の RUM レポートを自動的に送信します。この最初のレポートとともに、必要に応じて、UDI に

関連付けられた信頼コード要求を送信します。CSLU は RUM レポートを CSSM に転送し、信頼コードも含む ACK を取得します。ACK は、製品インスタンスが次回 CSLU に接続したときに製品インスタンスに適用されます。

17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースでは、製品インスタンスは 1 日に複数の RUM レポートを送信しません。特権 EXEC モードで **license smart sync** コマンドを入力すると、製品インスタンスと CSSM 間のオンデマンド同期のためにこれをオーバーライドできます。

製品インスタンスが次にいつ RUM レポートを送信するかを確認するには、特権 EXEC モードで **show license all** コマンドを入力し、出力の [Next report push] フィールドの日付を確認します。

信頼コードがインストールされていることを確認するには、特権 EXEC モードで **show license status** コマンドを入力します。[Trust Code Installed] フィールドで更新されたタイムスタンプを確認します。

ライセンスの使用状況が変更された場合は、AIR ライセンスの設定（158 ページ）を参照しレポートへの影響を確認してください。

CSLU 開始型通信の場合のタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定→使用状況の同期

1. ***CSLU* のインストール**

   タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン（VM）。

   [Smart Software Manager]https://software.cisco.com/download/home/286285506/type> [Smart Licensing Utility] からファイルをダウンロードします。

   インストールとセットアップの詳細については、『Cisco Smart License Utility クイック スタート セットアップ ガイド』および『Cisco Smart License Utility ユーザーガイド』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU

   1. シスコへのログイン（CSLU インターフェイス）（114 ページ）
   2. スマートアカウントとバーチャルアカウントの設定（CSLUインターフェイス）（115 ページ）
   3. CSLU での CSLU 開始型製品インスタンスの追加（CSLU インターフェイス）（118 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   CSLU 開始型通信のネットワーク到達可能性の確認（121 ページ）

4. **使用状況の同期**

   タスクが実行される場所：製品インスタンス

   使用状況レポートの収集：CSLU 開始（CSLU インターフェイス） （118 ページ）

結果：

CSLU が現在シスコにログインしているため、レポートは CSSM の関連するスマートアカウントとバーチャルアカウントに自動的に送信され、CSSM は CSLU と製品インスタンスに確認応答を送信します。CSSM から ACK を取得し、インストールのために製品インスタンスに送り返します。CSSM からの ACK には信頼コードと SLAC が含まれます（要求した場合）。

ライセンスの使用状況が変更された場合は、AIR ライセンスの設定 （158 ページ） を参照しレポートへの影響を確認してください。

トポロジのワークフロー：CSSM に直接接続

[Smart Account Set-Up] → [Product Instance Configuration] → [Trust Establishment with CSSM]

1. **スマートアカウントのセットアップ**

   タスクが実行される場所：CSSM Web UI、 https://software.cisco.com/

   スマートアカウントと必要なバーチャルアカウントへの適切なアクセス権を持つユーザロールがあることを確認します。

2. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   1. CSSM への製品インスタンス接続の設定： CSSM への接続の設定 （138 ページ）
   2. 接続方法と転送タイプの設定（1 つ選択）

      - オプション 1：

        スマート転送：転送タイプを **smart** に設定し、対応する URL を設定します。

        転送モードが **license smart transport smart** に設定されている場合は、**license smart url default** を設定すると、スマート URL（https://smartreceiver.cisco.com/licservice/license）が自動的に設定されます。構成ファイルへの変更を保存します。

        ```
        Device(config)# license smart transport smart
        Device(config)# license smart url default
        Device(config)# exit
        Device# copy running-config startup-config
        ```

      - オプション 2：

        HTTPS プロキシを介してスマートトランスポートを設定します。HTTPS プロキシを介したスマート転送の設定 （141 ページ） を参照してください

      - オプション 3：

ダイレクトクラウドアクセス用に Call Home サービスを設定します。「ダイレクトクラウドアクセス用の Call Home サービスの設定 （142 ページ）」を参照してください。

- オプション 4：

  HTTPS プロキシを介したダイレクトクラウドアクセス用に Call Home サービスを設定します。「HTTPS プロキシサーバを介したダイレクトクラウドアクセス用の Call Home サービスの設定 （145 ページ）」を参照してください。

3. ***CSSM* との信頼の確立**

   タスクが実行される場所：CSSM Web UI、次に製品インスタンス

   1. 所有するバーチャルアカウントごとに 1 つのトークンを生成します。1 つのバーチャルアカウントに属するすべての製品インスタンスに同じトークンを使用できます。CSSM からの信頼コード用新規トークンの生成 （150 ページ）
   2. トークンをダウンロードしたら、製品インスタンスに信頼コードをインストールできます。 信頼コードのインストール （151 ページ）

結果：

信頼を確立した後、CSSMはポリシーを返します。ポリシーは、そのバーチャルアカウントのすべての製品インスタンスに自動的にインストールされます。ポリシーは、製品インスタンスが使用状況をレポートするかどうか、およびその頻度を指定します。

17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースでは、製品インスタンスは 1 日に複数の RUM レポートを送信しません。特権 EXEC モードで **license smart sync** コマンドを入力すると、製品インスタンスと CSSM 間のオンデマンド同期のためにこれをオーバーライドできます。

レポート間隔を変更するには、グローバル コンフィギュレーション モードで **license smart usage interval** コマンドを設定します。シンタックスの詳細については、対応するリリースのコマンドリファレンスで *license smart (privileged EXEC)* コマンドを参照してください。

ライセンスの使用状況が変更された場合は、AIR ライセンスの設定 （158 ページ） を参照しレポートへの影響を確認してください。

トポロジのワークフロー：CSLU は CSSM から切断

製品インスタンス開始型通信またはCSLU開始型通信のどちらの方法を実装するかによって異なります。以下の対応するタスク一覧を実行します。

- 製品インスタンス開始型通信の場合のタスク
- CSLU 開始型通信の場合のタスク

製品インスタンス開始型通信の場合のタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定→使用状況の同期

1. ***CSLU* のインストール**

   タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン（VM）。

   [Smart Software Manager]https://software.cisco.com/download/home/286285506/type> [Smart Licensing Utility] からファイルをダウンロードします。

   インストールとセットアップの詳細については、『Cisco Smart License Utility クイック スタート セットアップ ガイド』および『Cisco Smart License Utility ユーザーガイド』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU

   1. CSLU の [Preferences] タブで、[Cisco Connectivity] トグルスイッチを**オフ**にします。フィールドが「Cisco Is Not Available」に切り替わります。
   2. スマートアカウントとバーチャルアカウントの設定（CSLU インターフェイス）（115 ページ）
   3. CSLU での製品開始型製品インスタンスの追加（CSLU インターフェイス）（116 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   1. 製品インスタンス開始型通信のネットワーク到達可能性の確認（116 ページ）
   2. 転送タイプが **cslu** に設定されていることを確認します。

      CSLU がデフォルトの転送タイプです。別のオプションを設定した場合は、グローバル コンフィギュレーション モードで **license smart transport cslu** コマンドを入力します。構成ファイルへの変更を保存します。

      ```
      Device(config)# license smart transport cslu
      Device(config)# exit
      Device# copy running-config startup-config
      ```

   3. CSLU の検出方法を指定します（1 つ選択）

      - オプション 1：

        No action required.`cslu-local` のゼロタッチ DNS ディスカバリ用に設定されたネームサーバ

        ここでは、DNS を設定してあり（ネームサーバーの IP アドレスが製品インスタンスで設定されている）、ホスト名 `cslu-local` が CSLU IP アドレスにマッピングされているエントリが DNS サーバーにある場合、追加のアクションは不要です。製品インスタンスは、ホスト名 `cslu-local` を自動的に検出します。

- オプション 2：

  No action required.`cslu-local.<domain>` のゼロタッチ DNS ディスカバリ用に設定されたネームサーバとドメイン

  ここでは、DNS を設定してあり（ネームサーバーの IP アドレスとドメインが製品インスタンスで設定されている）、`cslu-local.<domain>` が CSLU IP アドレスにマッピングされているエントリが DNS サーバーにある場合、追加のアクションは不要です。製品インスタンスは、ホスト名 `cslu-local` を自動的に検出します。

- オプション 3：

  CSLU に特定の URL を設定します。

  グローバル コンフィギュレーション モードで **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* コマンドを入力します。`<cslu_ip_or_host>` には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

```
Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
Device(config)# exit
Device# copy running-config startup-config
```

4. 使用状況の同期

タスクの実行場所：CSLU と CSSM

製品インスタンスは通信を開始すると、ポリシーに従って、スケジュールされた時刻に最初の RUM レポートを自動的に送信します。これをトリガーする **license smart sync** 特権 EXECコマンドを入力することもできます。この最初のレポートとともに、必要に応じて、UDI に関連付けられた信頼コード要求を送信します。CSLU は CSSM から切断されているため、次のタスクを実行して RUM レポートを CSSM に送信します。

1. CSSM へのエクスポート（CSLU インターフェイス）（120 ページ）
2. CSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ）
3. CSSM からのインポート（CSLU インターフェイス）（120 ページ）

結果：

CSSM からインポートした ACK に信頼コードが含まれます（要求した場合）。ACK は、製品インスタンスが次回 CSLU に接続したときに製品インスタンスに適用されます。

17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースでは、製品インスタンスは 1 日に複数の RUM レポートを送信しません。特権 EXEC モードで **license smart sync** コマンドを入力すると、製品インスタンスと CSSM 間のオンデマンド同期のためにこれをオーバーライドできます。

製品インスタンスが次にいつ RUM レポートを送信するかを確認するには、特権 EXEC モードで **show license all** コマンドを入力し、出力の [Next report push] フィールドの日付を確認します。

信頼コードがインストールされていることを確認するには、特権 EXEC モードで `show license status` コマンドを入力します。[Trust Code Installed] フィールドで更新されたタイムスタンプを確認します。

ライセンスの使用状況が変更された場合は、AIR ライセンスの設定（158 ページ）を参照しレポートへの影響を確認してください。

CSLU 開始型通信の場合のタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定→使用状況の同期

1. ***CSLU* のインストール**

   タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン（VM）。

   [Smart Software Manager]https://software.cisco.com/download/home/286285506/type> [Smart Licensing Utility] からファイルをダウンロードします。

   インストールとセットアップの詳細については、『Cisco Smart License Utility クイック スタート セットアップ ガイド』および『Cisco Smart License Utility ユーザーガイド』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU

   1. CSLU の [Preferences] タブで、[Cisco Connectivity] トグルスイッチを**オフ**にします。フィールドが「Cisco Is Not Available」に切り替わります。
   2. スマートアカウントとバーチャルアカウントの設定（CSLU インターフェイス）（115 ページ）
   3. CSLU での CSLU 開始型製品インスタンスの追加（CSLU インターフェイス）（118 ページ）
   4. 使用状況レポートの収集：CSLU 開始（CSLU インターフェイス）（118 ページ）

3. **製品インスタンスの設定**

   タスクの実行場所：製品インスタンス

   CSLU 開始型通信のネットワーク到達可能性の確認（121 ページ）

4. **使用状況の同期**

   タスクの実行場所：CSLU と CSSM

   製品インスタンスから使用状況データを収集します。CSLU は CSSM から切断されるため、後で CSLU が製品インスタンスから収集した使用状況データをファイルに保存します。該当する場合、この最初のレポートに加えて、承認コードと UDI に関連付けられた信頼コード要求が RUM レポートに含まれます。次に、シスコに接続されているワークステーションからファイルを CSSM にアップロードします。この後、CSSM から ACK をダウン

ロードします。CSLU がインストールされて製品インスタンスに接続されているワークステーションで、ファイルを CSLU にアップロードします。

1. CSSM へのエクスポート（CSLU インターフェイス）（120 ページ）
2. CSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ）
3. CSSM からのインポート（CSLU インターフェイス）（120 ページ）

結果：

CSSM からインポートした ACK に信頼コードと SLAC が含まれます（要求した場合）。CSLU が次に更新を実行するときに、アップロードされた ACK が製品インスタンスに適用されます。

ライセンスの使用状況が変更された場合は、AIR ライセンスの設定（158 ページ）を参照しレポートへの影響を確認してください。

トポロジのワークフロー：コントローラを介して CSSM に接続

コントローラとして Cisco DNA Center を展開するには、次のワークフローを実行します。

製品インスタンスの設定 → Cisco DNA Center の設定

1. **製品インスタンスの設定**

   タスクの実行場所：製品インスタンス

   NETCONF を有効にします。Cisco DNA Center は NETCONF プロトコルを使用して設定をプロビジョニングし、製品インスタンスから必要な情報を取得します。したがって、これを容易にするために製品インスタンスで NETCONF を有効にする必要があります。

   詳細については、『Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.3.x』を参照してください。このガイドの「Model-Driven Programmability」の「NETCONF Protocol」を確認します。

2. **Cisco DNA Center の設定**

   タスクの実行場所：Cisco DNA Center GUI

   次に、実行する必要のあるタスクの概要と、付属のドキュメントリファレンスを示します。このドキュメントには、Cisco DNA Center GUI で実行する必要がある詳細な手順が示されています。

   1. スマートアカウントとバーチャルアカウントを設定します。

      CSSM Web UI へのログインに使用するのと同じログインクレデンシャルを入力します。これにより、Cisco DNA Center は CSSM との接続を確立できます。

      必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center Administrator Guide』[英語] の「Manage Licenses」の「Set Up License Manager」を参照してください。

   2. 必要な製品インスタンスを Cisco DNA Center インベントリに追加してサイトに割り当てます。

これにより、Cisco DNA Center は、要求されている証明書を含む必要な設定をプッシュして、Smart Licensing Using Policy が予想どおりに機能するようにします。

必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center User Guide』[英語] の「Display Your Network Topology」の「Assign Devices to a Site」を参照してください。

結果：

トポロジを実装したら、Cisco DNA Center で最初のアドホックレポートをトリガーし、スマートアカウントとバーチャルアカウント、および製品インスタンス間のマッピングを確立する必要があります。必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center Administrator Guide』[英語] で「Manage Licenses」の「Upload Resource Utilization Details to CSSM」を参照してください。これが完了すると、Cisco DNA Center はレポートポリシーに基づいて後続のレポートを処理します。

複数のポリシーが使用可能な場合、Cisco DNA Centerは 最も短いレポート間隔を維持します。この間隔はより頻繁に（より短い間隔で）報告するようにのみ変更できます。必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center Administrator Guide』[英語] の「Manage Licenses」の「Modify License Policy」を参照してください。

この後にライセンスレベルを変更する場合は、必要なリリース（リリース2.2.2以降）の『Cisco DNA Center Administrator Guide』[英語] の「Manage Licenses」の「Change License Level」を参照してください。

トポロジのワークフロー：CSSM への接続なし、CSLU なし

他のコンポーネントへの接続を設定する必要がないため、トポロジの設定に必要なタスクのリストは短くなります。このトポロジを実装した後に必要な使用状況レポートを作成する方法については、ワークフローの最後にある「結果」セクションを参照してください。

製品インスタンスの設定

タスクの実行場所：製品インスタンス

転送タイプを**オフ**に設定します。

グローバル コンフィギュレーション モードで **license smart transport off** コマンドを入力します。構成ファイルへの変更を保存します。

```
Device(config)# license smart transport off
Device(config)# exit
Device# copy running-config startup-config
```

結果：

製品インスタンスからのすべての通信を無効にします。ライセンスの使用状況を報告するには、RUM レポートを製品インスタンスのファイルに保存する必要があります。インターネットおよびシスコに接続できるワークステーションからファイルを CSSM にアップロードします。

1. RUM レポートの生成と保存

license smart save usage コマンドを特権 EXEC モードで入力します。次の例では、すべての RUM レポートがファイル `all_rum.txt` で製品インスタンスのフラッシュメモリに保存されます。

Cisco IOS XE Cupertino 17.7.1 以降では、信頼コードが製品インスタンスにまだ存在しない場合、このコマンドを設定すると、RUM レポートに自動的に信頼コードの要求が含まれます。これは、スタンドアロンおよび高可用性設定でサポートされます。

下記の例では、ファイルはまずブートフラッシュに保存されてから、TFTP の場所にコピーされます。

```
Device# license smart save usage all file bootflash:all_rum.txt
Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
```

2. 使用状況データを CSSM にアップロード：CSSM へのデータまたは要求のアップロードとファイルのダウンロード （153 ページ）
3. ACK を製品インスタンスにインストール：製品インスタンスへのファイルのインストール （154 ページ）

ライセンスの使用方法を変更する場合は、AIR ライセンスの設定 （158 ページ）を参照してください。

SLR 承認コードを返す場合は、承認コードの削除と返却 （146 ページ） を参照してください。

トポロジのワークフロー：SSM オンプレミス展開

製品インスタンス開始型通信（プッシュ）方式を実装するか、または SSM オンプレミス開始型通信（プル）方式を実装するかによって、対応する一連のタスクを実行します。

製品インスタンス開始型通信の場合のタスク

SSM オンプレミスのインストール → 製品インスタンスの追加と検証（該当する場合のみ） → 製品インスタンスの設定 → 使用状況の最初の同期

1. ***SSM* オンプレミスのインストール**

   タスクの実行場所：Cisco UCS C220 M3 ラックサーバなどの物理サーバ、または必要な要件を満たしているハードウェアベースのサーバ。

   Smart Software Manager の [Smart Software Manager On-Prem] からファイルをダウンロードします。

   インストールのヘルプについては、『*Cisco Smart Software On-Prem Installation Guide*』と『*Cisco Smart Software On-Prem User Guide*』を参照してください。

   SSM オンプレミスを展開し、SSM オンプレミスで共通名を設定し（[Security Widgets] > [Certificates]）、NTP サーバを同期し（[Settings] ウィジェット > [Time Settings]）、SSM オンプレミスアカウントを作成して登録し、CSSM のスマートアカウントとバーチャルアカウントと同期（[Synchronization] ウィジェット）したら、インストールが完了します。

（注） [On-Prem Licensing Workspace] のライセンス機能は、ローカルアカウントを作成し、登録し、CSSM のスマートアカウントと同期するまではグレー表示になります。CSSM とのローカルアカウントの同期は、SSM オンプレミスインスタンスを CSSM に認識させるためであり、次に示す**「4. 使用状況の最初の同期」で実行する使用状況の同期とは異なります。**

2. 製品インスタンスの追加と検証

タスクの実行場所：SSM オンプレミス UI

この手順により、製品インスタンスが検証され、CSSM の該当するスマートアカウントとバーチャルアカウントにマッピングされます。この手順は、次の場合にのみ必要です。

- 製品インスタンスを CSSM で報告する前に、SSM オンプレミスで追加および検証する場合（セキュリティを強化するため）。
- （デフォルトのローカル バーチャル アカウントに加えて）ローカル バーチャル アカウントを SSM オンプレミスで作成した場合。この場合は、SSM オンプレミスが CSSM の正しいライセンスプールに使用状況を報告できるように、SSM オンプレミスにこれらのローカル バーチャル アカウントの製品インスタンスのスマートアカウント情報とバーチャルアカウント情報を提供する必要があります。

1. スマートアカウントとバーチャルアカウントの割り当て（SSM オンプレミス UI）（125 ページ）
2. デバイスの検証（SSM オンプレミス UI）（126 ページ）

（注） 製品インスタンスが NAT 設定にある場合は、デバイス検証を有効にするときに NAT 設定のサポートも有効にします。両方のトグルスイッチが同じウィンドウにあります。

3. 製品インスタンスの設定

タスクの実行場所：製品インスタンスと SSM オンプレミス UI

特権 EXEC モードで **copy running-config startup-config** コマンドを入力して、製品インスタンスの設定変更を必ず保存してください。

1. 製品インスタンス開始型通信のネットワーク到達可能性の確認（127 ページ）
2. トランスポート URL の取得（SSM オンプレミス UI）（129 ページ）
3. 転送タイプ、URL、およびレポート間隔の設定（155 ページ）

   CSLU と SSM オンプレミスのトランスポートタイプ設定は同じですが（グローバル コンフィギュレーション モードの **license smart transport cslu** コマンド）、URL が異なります。

4. 使用状況の最初の同期

タスクの実行場所：製品インスタンス、SSM オンプレミス、CSSM

1. 製品インスタンスを SSM オンプレミスと同期します。

   製品インスタンスに **license smart sync** {**all**｜ **local**} コマンドを特権 EXEC モードで入力します。これにより、SSM オンプレミスと製品インスタンスが同期され、保留中のデータが送受信されます。次に例を示します。

   ```
   Device# license smart sync local
   ```

   これは、SSM オンプレミス UI で確認できます。ログインして、[Smart Licensing] ワークスペースを選択します。[Inventory] > [SL Using Policy] タブに移動します。対応する製品インスタンスの [Alerts] 列に、「Usage report from product instance」というメッセージが表示されます。

（注） 上記の手順 2（製品インスタンスの追加と検証）を実行していない場合、このサブ手順を実行すると、製品インスタンスが SSM オンプレミスのデータベースに追加されます。

2. 使用状況情報を CSSM と同期します（いずれかを選択）。

   - オプション 1：

     SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。

   - オプション 2：

     SSM オンプレミスが CSSM に接続されていません。使用状況データのエクスポートとインポート（SSM オンプレミス UI） （130 ページ）を参照してください。

結果：

使用状況の最初の同期が完了しました。製品インスタンスとライセンス使用状況情報が SSM オンプレミスに表示されるようになりました。

後続のレポートには、次のオプションが含まれています。

- 製品インスタンスと SSM オンプレミスとの間でデータを同期するには、次の手順を実行します。

  レポート間隔を設定して、製品インスタンスと SSM オンプレミスとの間の定期的な同期をスケジュールします。グローバル コンフィギュレーション モードで **license smart usage interval** *interval_in_days* コマンドを入力します。

  17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースでは、製品インスタンスは 1 日に複数の RUM レポートを送信しません。特権 EXEC モードで **license smart sync** コマンドを入力すると、製品インスタンスと CSSM 間のオンデマンド同期のためにこれをオーバーライドできます。

製品インスタンスが次にいつ RUM レポートを送信するかを確認するには、特権 EXEC モードで **show license all** コマンドを入力し、出力の [Next report push:] フィールドを確認します。

- 使用状況情報を CSSM と同期するには、次のように、定期的な同期をスケジュールするか、必要なファイルをアップロードおよびダウンロードします。
  - CSSM との定期的な同期をスケジュールします。SSM オンプレミス UI で、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。次の頻度情報を入力し、保存します。
    - [Days]：同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
    - [Time of Day]：24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes を入力すると、ローカルタイムゾーンの午後 2 時（1400）に同期が行われます。
  - レポートに必要なファイルのアップロードとダウンロードを実行します（使用状況データのエクスポートとインポート（SSM オンプレミス UI）（130 ページ））。

SSM オンプレミスインスタンス開始型通信の場合のタスク

SSM オンプレミスのインストール → 製品インスタンスの追加 → 製品インスタンスの設定 → 使用状況の最初の同期

1. ***SSM* オンプレミスのインストール**

   タスクの実行場所：Cisco UCS C220 M3 ラックサーバなどの物理サーバ、または必要な要件を満たしているハードウェアベースのサーバ。

   Smart Software Manager の [Smart Software Manager On-Prem] からファイルをダウンロードします。

   インストールのヘルプについては、『*Cisco Smart Software On-Prem Installation Guide*』と『*Cisco Smart Software On-Prem User Guide*』を参照してください。

   SSM オンプレミスを展開し、SSM オンプレミスで共通名を設定し（[Security Widgets] > [Certificates]）、NTP サーバを同期し（[Settings] ウィジェット > [Time Settings]）、SSM オンプレミスアカウントを作成して登録し、CSSM のスマートアカウントとバーチャルアカウントと同期（[Synchronization] ウィジェット）したら、インストールが完了します。

（注） [On-Prem Licensing Workspace] のライセンス機能は、ローカルアカウントを作成し、登録し、CSSM のスマートアカウントと同期するまではグレー表示になります。CSSM とのローカルアカウントの同期は、SSM オンプレミスインスタンスを CSSM に認識させるためであり、次に示す「4. **使用状況の最初の同期」で実行する使用状況の同期とは異なります。**

2. **製品インスタンスの追加**

タスクの実行場所：SSM オンプレミス UI

単一の製品インスタンスを追加するか、または複数の製品インスタンスを追加するかに応じて、対応するサブ手順（1 つ以上の製品インスタンスの追加（SSM オンプレミス UI）（131 ページ））を実行します。

3. **製品インスタンスの設定**

   タスクの実行場所：製品インスタンスと SSM オンプレミス UI

   特権 EXEC モードで **copy running-config startup-config** コマンドを入力して、製品インスタンスの設定変更を必ず保存してください。SSM オンプレミス開始型通信のネットワーク到達可能性の確保 （132 ページ）

4. **使用状況の最初の同期**

   タスクの実行場所：SSM オンプレミス UI と CSSM

   1. 製品インスタンスから使用状況情報を取得します。

      SSM オンプレミス UI で、[Reports] > [Synchronization pull schedule] > [Synchronize now with the device] に移動します。

      [Alerts] 列に、「Usage report from product instance」というメッセージが表示されます。

ヒント　同期がトリガーされるまでに 60 秒かかります。進行状況を表示するには、[On-Prem Admin Workspace] に移動し、[Support Center] ウィジェットをクリックします。このウィジェットにシステムログに進行状況が表示されます。

   2. 使用状況情報を CSSM と同期します（いずれかを選択）。

      - オプション 1：

        SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。

      - オプション 2：

        SSM オンプレミスが CSSM に接続されていません。使用状況データのエクスポートとインポート（SSM オンプレミス UI） （130 ページ）を参照してください。

結果：

使用状況の最初の同期が完了しました。製品インスタンスとライセンス使用状況情報が SSM オンプレミスに表示されるようになりました。SSM オンプレミスは ACK を製品インスタンスに自動的に返します。製品インスタンスが ACK を受信していることを確認するには、特権 EXEC モードで **show license status** コマンドを入力し、出力で [Last ACK received] フィールドの日付を確認します。

後続のレポートには、次のオプションが含まれています。

- 製品インスタンスから使用状況情報を取得するには、次の手順を実行します。
  - SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco）]に移動します。
  - 頻度を設定して、製品インスタンスから情報を定期的に取得するようにスケジュールします。SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronisation pull schedule with the devices] に移動します。次のフィールドに値を入力します。
    - [Days]：同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
    - [Time of Day]：24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes と入力すると、午後 2 時（1400）に同期が行われます。
  - CSSM に接続せずに製品インスタンスから使用状況データを収集します。SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Inventory] > [SL Using Policy] タブに移動します。対応するチェックボックスを有効にして、1 つ以上の製品インスタンスを選択します。[Actions for Selected...] > [Collect Usage] をクリックします。選択した製品インスタンスにオンプレミスが接続し、使用状況レポートを収集します。その後、これらの使用状況レポートはオンプレミスのローカルライブラリに保存されます。これらのレポートは、オンプレミスがシスコに接続されている場合はシスコに転送できます。また、（シスコに接続されていない場合は）[Export/Import All..] > [Export Usage to Cisco] を選択することで、使用状況の収集を手動でトリガーできます。
- 使用状況情報を CSSM と同期するには、次の手順を実行します。
  - CSSM との定期的な同期をスケジュールします。SSM オンプレミス UI で、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。次の頻度情報を入力し、保存します。
    - [Days]：同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
    - [Time of Day]：24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes と入力すると、午後 2 時（1400）に同期が行われます。
  - レポートに必要なファイルのアップロードとダウンロードを実行します（使用状況データのエクスポートとインポート（SSM オンプレミス UI）（130 ページ））。

ポリシーを使用したスマートライセンシングへの移行

ポリシーを使用したスマートライセンシングにアップグレードするには、製品インスタンスのソフトウェアバージョン（イメージ）をサポートされているバージョンにアップグレードする必要があります。

はじめる前に

「アップグレード （69 ページ）」の項を必ず読み、ポリシーを使用したスマートライセンシングによる以前の全ライセンスモデルの処理方法を理解してください。

ポリシーを使用したスマートライセンシングは、Cisco IOS XE Amsterdam 17.3.2a で導入されました。そのため、これがポリシーを使用したスマートライセンシングに最低限必要なバージョンになります。

移行前に使用していたすべてのライセンスは、アップグレード後も使用できることに注意してください。つまり、登録済みライセンスと承認済みライセンス（予約済みライセンスを含む）だけでなく、評価ライセンスもすべて移行されます。登録済みライセンスと承認済みライセンスを移行する利点は、アップグレード後も設定（トランスポートタイプの設定と、CSSM への接続の設定、すべての証人コード）が保持されるため、移行後に実行する設定手順が少なくなります。これにより、Smart Licensing Using Policy 環境への移行がよりスムーズになります。

デバイス先行の変換は、ポリシーを使用したスマートライセンシングへの移行ではサポートされていません。

ワイヤレス コントローラ ソフトウェアのアップグレード

アップグレード手順の詳細については、以下を参照してください。

- Cisco Catalyst 9100 アクセスポイントの Cisco 組み込みワイヤレスコントローラ については、Catalyst アクセスポイントのオンラインヘルプの Cisco 組み込みワイヤレスコントローラ の「Software Upgrade」の項を参照してください。
- その他のサポートされるワイヤレスコントローラについては、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのソフトウェア設定ガイドの「System Upgrade」の「Upgrading the Cisco Catalyst 9800 Wireless Controller Software」の項を参照してください。

この手順を使用して、インストールモードまたは ISSU でアップグレードできます（ISSU はサポートされているプラットフォームおよびリリースでのみ）。

ソフトウェアバージョンのアップグレード後

- トポロジを実装します。

  アップグレード前の設定でトランスポートモードを使用できる場合は、アップグレード後も保持されます。評価ライセンスや、トランスポートタイプの概念が存在しないライセンスモデルの場合など、一部の場合にのみ、デフォルト（cslu）が適用されます。このような場合は、Smart Licensing Using Policy 環境で動作するように設定する前に実行する必要がある手順がいくつかある場合があります。

  アップグレード元のライセンスモデルに関係なく、アップグレード後にトポロジを変更できます。

- ライセンスの使用状況と CSSM の同期

  どのライセンスモデルからアップグレードするか、どのトポロジを実装するかに関係なく、使用状況情報を CSSM と同期します。そのためには、実装するトポロジに適用されるレポート方式に従う必要があります。この最初の同期により、使用状況の最新の情報が

CSSMに反映され、カスタムポリシー（使用可能な場合）が適用されます。この同期後に適用されるポリシーは、後続のレポート要件も示します。これらのルールをアップグレードが既存ライセンスのレポートに与える影響 （70 ページ）の表にも示します。

（注） 使用状況の最初の同期が完了した後、ポリシー、またはシステムメッセージに示されている場合にのみ、レポートが必要です。

移行シナリオの例

さまざまな既存のライセンスモデルとライセンスを考慮した移行シナリオの例を示します。すべてのシナリオで、移行前と後の出力例と注意すべき CSSM Web UI の変更を（移行の成功または追加アクションのインジケータとして）示し、また、必要な移行後の手順を特定して実行する方法も示します。

（注） SSMオンプレミスでは、アップグレード関連のさまざまなアクティビティを実行する順序が重要です。したがって、このシナリオでのみ、例ではなく、移行の順序が示されています。

例：スマートライセンシングからポリシーを使用したスマートライセンシングへ

次に、スマートライセンシングからポリシーを使用したスマートライセンシングに移行する Cisco Catalyst 9800-CL ワイヤレスコントローラの例を示します。

- 表 6 : スマートライセンシングからポリシーを使用したスマートライセンシングへ：show コマンド （92 ページ）
- 移行後の CSSM Web UI （96 ページ）
- 移行後のレポート （99 ページ）

show コマンドは、移行の前後に確認すべき以下の重要なフィールドを抽出して出力します。

表 *6 :* スマートライセンシングからポリシーを使用したスマートライセンシングへ：*show* コマンド

アップグレード前（スマートライセンシング）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license summary `Status`フィールドと `License Authorization` フィールドに、ライセンスについて `REGISTERED` および `AUTHORIZED` と表示されます。	**show license summary** `Status` フィールドに、ライセンスについて、登録済みおよび承認済みではなく `IN USE` と表示されます。

アップグレード前（スマートライセンシング）	アップグレード後（ポリシーを使用したスマートライセンシング）
Device# **show license summary** Smart Licensing is ENABLED Registration: **Status: REGISTERED** Smart Account: SA-Eg-Company-02 Virtual Account: Dept-02 Export-Controlled Functionality: ALLOWED Last Renewal Attempt: None Next Renewal Attempt: May 01 08:19:02 2021 IST License Authorization: Status: AUTHORIZED Last Communication Attempt: SUCCEEDED Next Communication Attempt: Dec 02 08:19:09 2020 IST License Usage: License Entitlement tag Count Status --- AP Perpetual Network... (DNA_NWSTACK_E) 1 **AUTHORIZED** Aironet DNA Essentia... (AIR-DNA-E) 1 **AUTHORIZED**	Device# **show license summary** License Usage: License Entitlement Tag Count Status --- air-network-essentials (DNA_NWSTACK_E) 1 **IN USE** air-dna-essentials (AIR-DNA-E) 1 **IN USE**

アップグレード前（スマートライセンシング）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license usage アップグレード前に1つの永続的ライセンスと1つのサブスクリプション ライセンスが使用されています。	**show license usage** すべてのライセンスが移行され、[Enforcement Type] フィールドに NOT ENFORCED と表示されます。 Cisco Catalyst ワイヤレスコントローラには、輸出規制ライセンスや適用ライセンスはありません。

アップグレード前（スマートライセンシング）	アップグレード後（ポリシーを使用したスマートライセンシング）

Device# **show license usage**
 	
License Authorization:
  Status: AUTHORIZED on Nov 02 08:21:29 2020 IST
 	
AP Perpetual Networkstack Essentials (DNA_NWSTACK_E):
  Description: AP Perpetual Network Stack entitled with DNA-E
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
 	
Aironet DNA Essentials Term Licenses (AIR-DNA-E):
  Description: DNA Essentials for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
	Device# **show license usage**
	
	License Authorization:
	  Status: Not Applicable
	
	air-network-essentials (DNA_NWSTACK_E):
	  Description: air-network-essentials
	  Count: 1
	  Version: 1.0
	  Status: IN USE
	  Export status: NOT RESTRICTED
	  Feature Name: air-network-essentials
	  Feature Description: air-network-essentials
	  Enforcement type: NOT ENFORCED
	  License type: Perpetual
	
	air-dna-essentials (AIR-DNA-E):
	  Description: air-dna-essentials
	  Count: 1
	  Version: 1.0
	  Status: IN USE
	  Export status: NOT RESTRICTED
	  Feature Name: air-dna-essentials
	  Feature Description: air-dna-essentials
	  Enforcement type: NOT ENFORCED
	  License type: Perpetual

アップグレード前（スマートライセンシング）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license status	**show license status** `Transport:` フィールドには、更新前に設定され、アップグレード後も保持される転送タイプが表示されます。 `Policy:` ヘッダーと詳細には、スマートアカウントまたはバーチャルアカウントで使用可能なカスタムポリシーが表示されます。このポリシーは製品インスタンスにも自動的にインストールされています。（信頼を確立した後、CSSM はポリシーを返します。その後、このポリシーが自動的にインストールされます）。 `Usage Reporting:` ヘッダー：`Next report push:` フィールドには、製品インスタンスが次の RUM レポートを CSSM に送信するタイミングについての情報が表示されます。 `Trust Code Installed:` フィールド：ID トークンが正常に変換され、信頼できる接続が CSSM で確立されたことを示します。

アップグレード前（スマートライセンシング）	アップグレード後（ポリシーを使用したスマートライセンシング）

Device# **show license status**
 	
Smart Licensing is ENABLED
 	
Utility:
  Status: DISABLED
 	
Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
 	
Transport:
  Type: Callhome
 	
Registration:
  Status: REGISTERED
  Smart Account: SA-Eg-Company-02
  Virtual Account: Dept-02
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 02 08:19:02 2020 IST
  Last Renewal Attempt: None
  Next Renewal Attempt: May 01 08:19:01 2021 IST
  Registration Expires: Nov 02 08:14:06 2021 IST
 	
License Authorization:
  Status: AUTHORIZED on Nov 02 08:21:29 2020 IST
  Last Communication Attempt: SUCCEEDED on Nov 02 08:21:29 2020 IST
  Next Communication Attempt: Dec 02 08:19:09 2020 IST
  Communication Deadline: Jan 31 08:14:15 2021 IST
 	
Export Authorization Key:
  Features Authorized:
  <none>
	Device# **show license status**
	Utility:
	  Status: DISABLED
	
	Smart Licensing Using Policy:
	  Status: ENABLED
	
	Data Privacy:
	  Sending Hostname: yes
	  Callhome hostname privacy: DISABLED
	  Smart Licensing hostname privacy: DISABLED
	  Version privacy: DISABLED
	
	Transport:
	  Type: Callhome
	
	Policy:
	  Policy in use: Installed On Nov 02 09:09:47 2020 IST
	  Policy name: **SLE Policy**
	  Reporting ACK required: yes (Customer Policy)
	  Unenforced/Non-Export Perpetual Attributes:
	  First report requirement (days): 60 (Customer Policy)
	  Reporting frequency (days): 60 (Customer Policy)
	  Report on change (days): 60 (Customer Policy)
	  Unenforced/Non-Export Subscription Attributes:
	  First report requirement (days): 30 (Customer Policy)
	  Reporting frequency (days): 30 (Customer Policy)
	  Report on change (days): 30 (Customer Policy)
	  Enforced (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 90 (Customer Policy)
	  Report on change (days): 90 (Customer Policy)
	  Export (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 90 (Customer Policy)
	  Report on change (days): 90 (Customer Policy)
	
	Miscellaneous:
	  Custom Id: <empty>
	
	Usage Reporting:
	  Last ACK received: Nov 02 09:09:47 2020 IST
	  Next ACK deadline: Jan 01 09:09:47 2021 IST
	  Reporting push interval: 30 days
	  Next ACK push check: Nov 02 09:13:54 2020 IST
	  Next report push: Dec 02 09:05:45 2020 IST
	  Last report push: Nov 02 09:05:45 2020 IST
	  Last report file write: <none>
	
	Trust Code Installed:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  INSTALLED on Nov 02 08:59:26 2020 IST
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  INSTALLED on Nov 02 09:00:45 2020 IST

アップグレード前（スマートライセンシング）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license udi	**show license udi** これは高可用性セットアップであり、このコマンドによってセットアップ内のすべての UDI が表示されます。 移行前と移行後のサンプル出力に変化はありません。

`Device# show license udi`
`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
 	
`HA UDI List:`
`Active:PID:C9800-CL-K9,SN:93BBAH93MGS`
`Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`Device# show license udi`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	
	`HA UDI List:`
	`Active:PID:C9800-CL-K9,SN:93BBAH93MGS`
	`Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN`

移行後の CSSM Web UI

https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。[Inventory] > [Product Instances] の順に選択します。

以前はホスト名で表示されていた製品インスタンス（この例では Catalyst 9800-CL Cloud ワイヤレスコントローラ）が、代わりに UDI で表示されるようになりました。移行されたすべての UDI、つまり、PID:C9800-CL-K9、SN:93BBAH93MGS、および PID:C9800-CL-K9、SN:9XECPSUU4XN が表示されます。

アクティブな製品インスタンスの使用状況のみが報告されるため、PID:C9800-CL-K9、SN:93BBAH93MGS の [License Usage] にはライセンス使用情報が表示されます。スタンバイの使用状況は報告されず、スタンバイの [License Usage] には [No Records Found] と表示されます。

図 *8 :* スマートライセンシングからポリシーを使用したスマートライセンシングへ：移行前の ***CSSM Web UI*** の製品インスタンスのホスト名

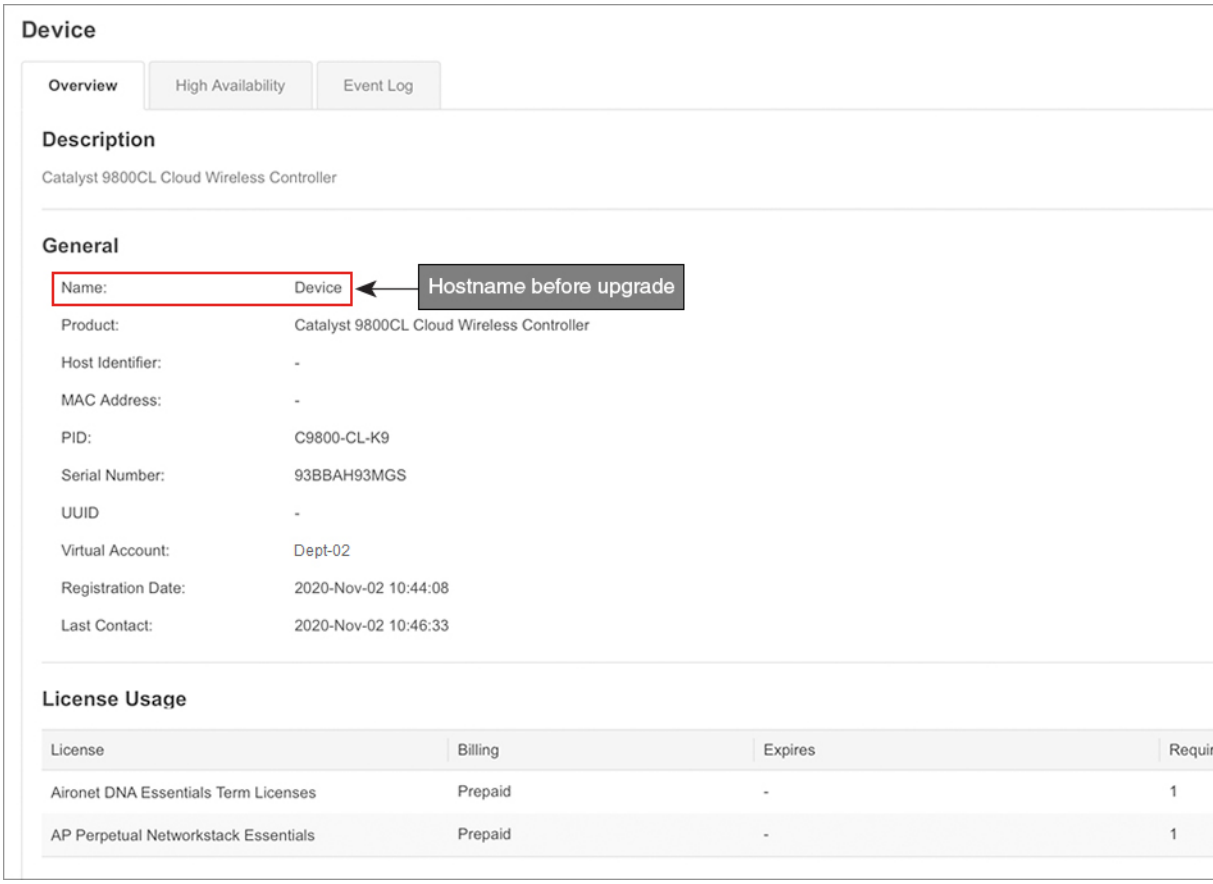


図 *9:* スマートライセンシングからポリシーを使用したスマートライセンシングへ：移行後のアクティブな製品インスタンスでの *UDI* とライセンス使用状況

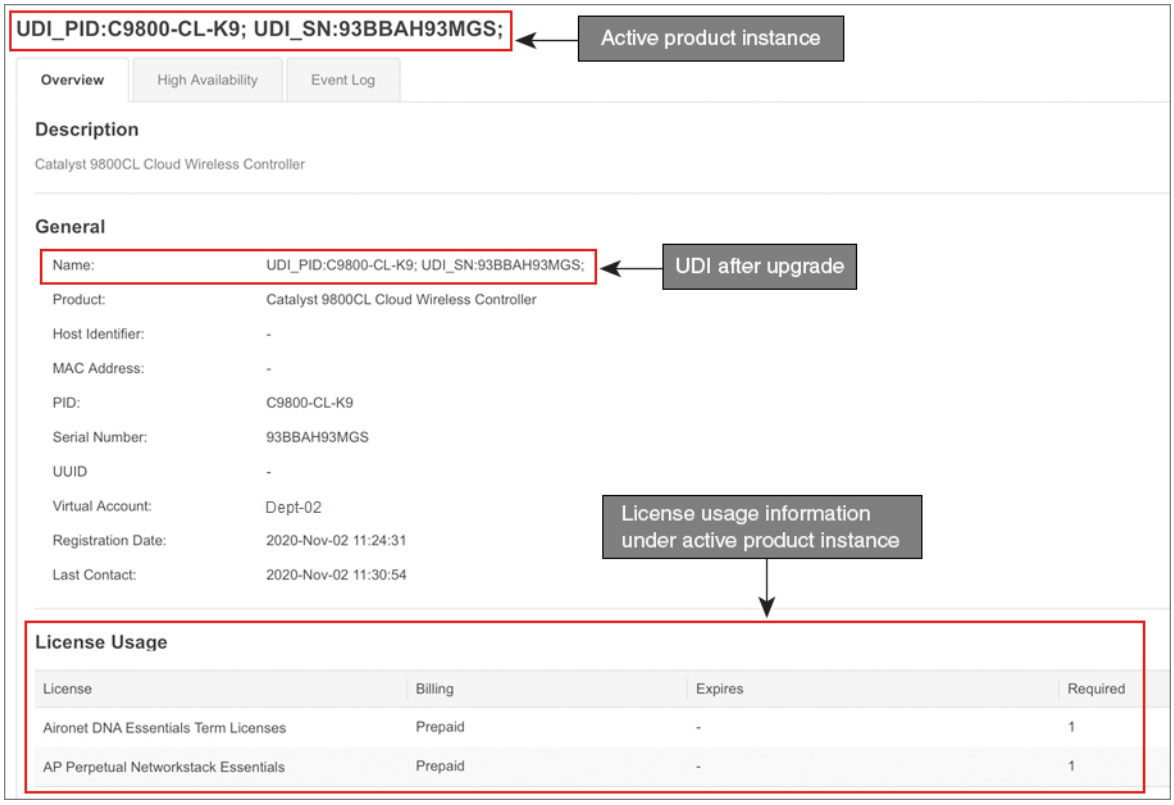
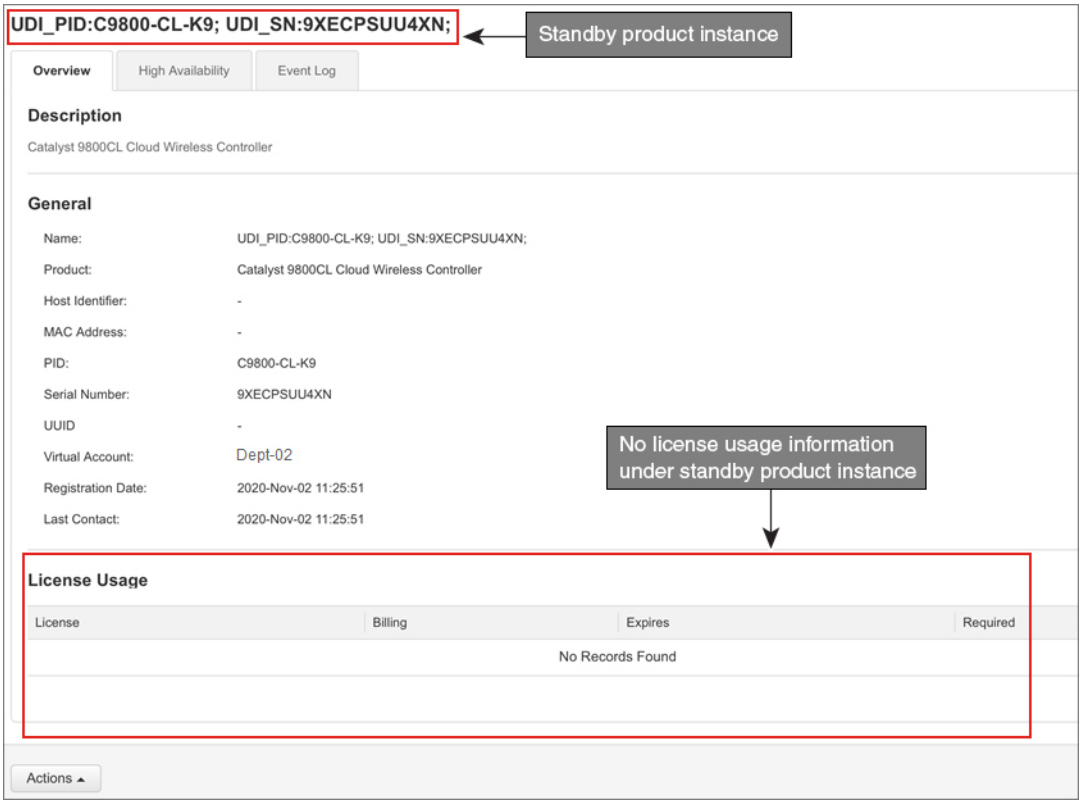


図 *10* : スマートライセンシングからポリシーを使用したスマートライセンシングへ：移行後のスタンバイ製品インスタンス



常にアクティブの使用状況が報告されるため、この高可用性セットアップのアクティブが変更されると、新しいアクティブな製品インスタンスのライセンス使用情報が表示され、使用状況が報告されるようになります。

移行後のレポート

製品インスタンスは、ポリシーに基づいて次の RUM レポートを CSSM に送信します。

より頻繁にレポートを作成するようにレポート間隔を変更する場合は、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart usage interval** コマンドを設定します。シンタックスの詳細については、対応するリリースのコマンドリファレンスで *license smart (global config)* コマンドを参照してください。

例：SLR からポリシーを使用したスマートライセンシングへ

次に、特定のライセンス予約（SLR）からポリシーを使用したスマートライセンシングに移行する Cisco Catalyst 9800-CL ワイヤレスコントローラの例を示します。これはアクティブとスタンバイを含む高可用性セットアップの例です。

ライセンス転換は自動的に行われ、承認コードが移行されます。移行を完了するためにこれ以上の操作は必要ありません。移行後は CSSM への接続なし、CSLU なし （62 ページ） トポロ

ジが有効になります。ポリシーを使用したスマートライセンシング環境の SLR 承認コードについては、承認コード （50 ページ） を参照してください。

- 表 7 : SLR からポリシーを使用したスマートライセンシングへ：show コマンド （100 ページ）
- 移行後の CSSM Web UI （106 ページ）
- 移行後のレポート （107 ページ）

show コマンドは、移行の前後に確認すべき以下の重要なフィールドを抽出して出力します。

表 *7: SLR* からポリシーを使用したスマートライセンシングへ：*show* コマンド

アップグレード前（SLR）	アップグレード後（ポリシーを使用したスマートライセンシング）

show license summary
 	
Registration ステータスフィールドと License Authorization ステータスフィールドに、ライセンスについて REGISTERED - SPECIFIC LICENSE RESERVATION および AUTHORIZED - RESERVED と表示されます。
 	
`Device# show license summary`
 	
`Smart Licensing is ENABLED`
`License Reservation is ENABLED`
 	
`Registration:`
 	
`  Status: REGISTERED - SPECIFIC LICENSE RESERVATION`
`  Export-Controlled Functionality: ALLOWED`
 	
`License Authorization:`
`  Status: AUTHORIZED - RESERVED`
 	
`License Usage:`
`  License  Entitlement tag  Count Status`
 	
`---`
 	
`  AP Perpetual Network... (DNA_NWStack)`
`1 AUTHORIZED`
`  Aironet DNA Advantag... (AIR-DNA-A)`
`1 AUTHORIZED`
	show license summary
	
	ライセンスは移行されますが、いずれの AP もコントローラに接続していないため、現在の使用数（カウント）はゼロであり、[Status] フィールドにはライセンスが [NOT IN USE] であると表示されます。
	
	`Device# show license summary`
	`License Reservation is ENABLED`
	
	`License Usage:`
	`  License  Entitlement Tag  Count Status`
	
	`---`
	
	`  Aironet DNA Advantag... (AIR-DNA-A)  0 NOT IN USE`
	`  AP Perpetual Network... (DNA_NWStack)  0 NOT IN USE`

アップグレード前（SLR）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license reservation	**show license authorization** `Last Confirmation code:` フィールド：高可用性設定のアクティブおよびスタンバイ製品インスタンスの SLR 承認コードが正常に移行されたことを示します。 `Specified license reservations:` ヘッダーは、永続的ライセンス（AP Perpetual Networkstack Advantage）とサブスクリプション ライセンス（Aironet DNA Advantage 期間ライセンス）が移行された SLR ライセンスであることを示しています。

アップグレード前（SLR）	アップグレード後（ポリシーを使用したスマートライセンシング）

Device# **show license reservation**
License reservation: ENABLED
 	
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
  Reservation status: SPECIFIC INSTALLED on Nov 02
03:16:01 2020 IST
  Export-Controlled Functionality: ALLOWED
  Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
  Reservation status: SPECIFIC INSTALLED on Nov 02
03:15:45 2020 IST
  Export-Controlled Functionality: ALLOWED
  Last Confirmation code: ad4382fe
 	
Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
  Description: DNA Advantage for Wireless
  Total reserved count: 20
  Term information:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
  License type: TERM
  Start Date: 2020-OCT-14 UTC
  End Date: 2021-APR-12 UTC
  Term Count: 5
  License type: TERM
  Start Date: 2020-JUN-18 UTC
  End Date: 2020-DEC-15 UTC
  Term Count: 5
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
  License type: TERM
  Start Date: 2020-OCT-14 UTC
  End Date: 2021-APR-12 UTC
  Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
  Description: AP Perpetual Network Stack entitled
with DNA-A
  Total reserved count: 20
  Term information:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
  License type: TERM
  Start Date: 2020-OCT-14 UTC
  End Date: 2021-APR-12 UTC
  Term Count: 5
  License type: TERM
  Start Date: 2020-JUN-18 UTC
  End Date: 2020-DEC-15 UTC
  Term Count: 5
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
  License type: TERM
  Start Date: 2020-OCT-14 UTC
  End Date: 2021-APR-12 UTC
  Term Count: 10	

アップグレード前（SLR）	アップグレード後（ポリシーを使用したスマートライセンシング）

	Device# **show license authorization**
	Overall status:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
	  Last Confirmation code: 102fc949
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  Last Confirmation code: ad4382fe
	
	Specified license reservations:
	  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
	  Description: DNA Advantage for Wireless
	  Total reserved count: 20
	  Enforcement type: NOT ENFORCED
	  Term information:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-OCT-14 UTC
	  End Date: 2021-APR-12 UTC
	  Term Count: 5
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-JUN-18 UTC
	  End Date: 2020-DEC-15 UTC
	  Term Count: 5
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-OCT-14 UTC
	  End Date: 2021-APR-12 UTC
	  Term Count: 10
	  AP Perpetual Networkstack Advantage (DNA_NWStack):
	  Description: AP Perpetual Network Stack entitled with DNA-A
	  Total reserved count: 20
	  Enforcement type: NOT ENFORCED
	  Term information:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-OCT-14 UTC
	  End Date: 2021-APR-12 UTC
	  Term Count: 5
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-JUN-18 UTC
	  End Date: 2020-DEC-15 UTC
	  Term Count: 5
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM

アップグレード前（SLR）	アップグレード後（ポリシーを使用したスマートライセンシング）
	Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 10 Purchased Licenses: No Purchase Information Available

アップグレード前（SLR）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license status	**show license status** Transport: ヘッダーの下にある Type: フィールドは、転送タイプがオフに設定されていることを示します。 Usage Reporting: ヘッダーの下にある Next report push: フィールドは、次の RUM レポートを CSSM にアップロードする必要性の有無とタイミングを示します。

アップグレード前（SLR）	アップグレード後（ポリシーを使用したスマートライセンシング）

-	Device# **show license status**
	
	Utility:
	  Status: DISABLED
	
	Smart Licensing Using Policy:
	  Status: ENABLED
	
	Data Privacy:
	  Sending Hostname: yes
	  Callhome hostname privacy: DISABLED
	  Smart Licensing hostname privacy: DISABLED
	  Version privacy: DISABLED
	
	Transport:
	  Type: Transport Off
	
	Policy:
	  Policy in use: Merged from multiple sources.
	  Reporting ACK required: yes (CISCO default)
	  Unenforced/Non-Export Perpetual Attributes:
	  First report requirement (days): 365 (CISCO default)
	
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Unenforced/Non-Export Subscription Attributes:
	  First report requirement (days): 90 (CISCO default)
	
	  Reporting frequency (days): 90 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Enforced (Perpetual/Subscription) License Attributes:
	
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	  Export (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	
	Miscellaneous:
	  Custom Id: <empty>
	
	Usage Reporting:
	  Last ACK received: <none>
	  Next ACK deadline: <none>
	  Reporting push interval: 0 (no reporting)
	  Next ACK push check: Nov 01 20:31:46 2020 IST
	  Next report push: <none>
	  Last report push: <none>
	  Last report file write: <none>
	
	Trust Code Installed: <none>

移行後の CSSM Web UI

https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。[Inventory] > [Product Instances] の順に選択します。

[Product Instances] タブに変更はありません。使用状況レポートがまだないため、[Last Contact] 列には「Reserved Licenses」と表示されます。必要な RUM レポートがアップロードされ、「Reserved Licenses」が表示されていないことが確認されると、ライセンスの使用状況はアクティブな製品インスタンスのみで表示されます。

図 *11 : SLR* からポリシーを使用したスマートライセンシング：アップグレード前のアクティブな製品インスタンス

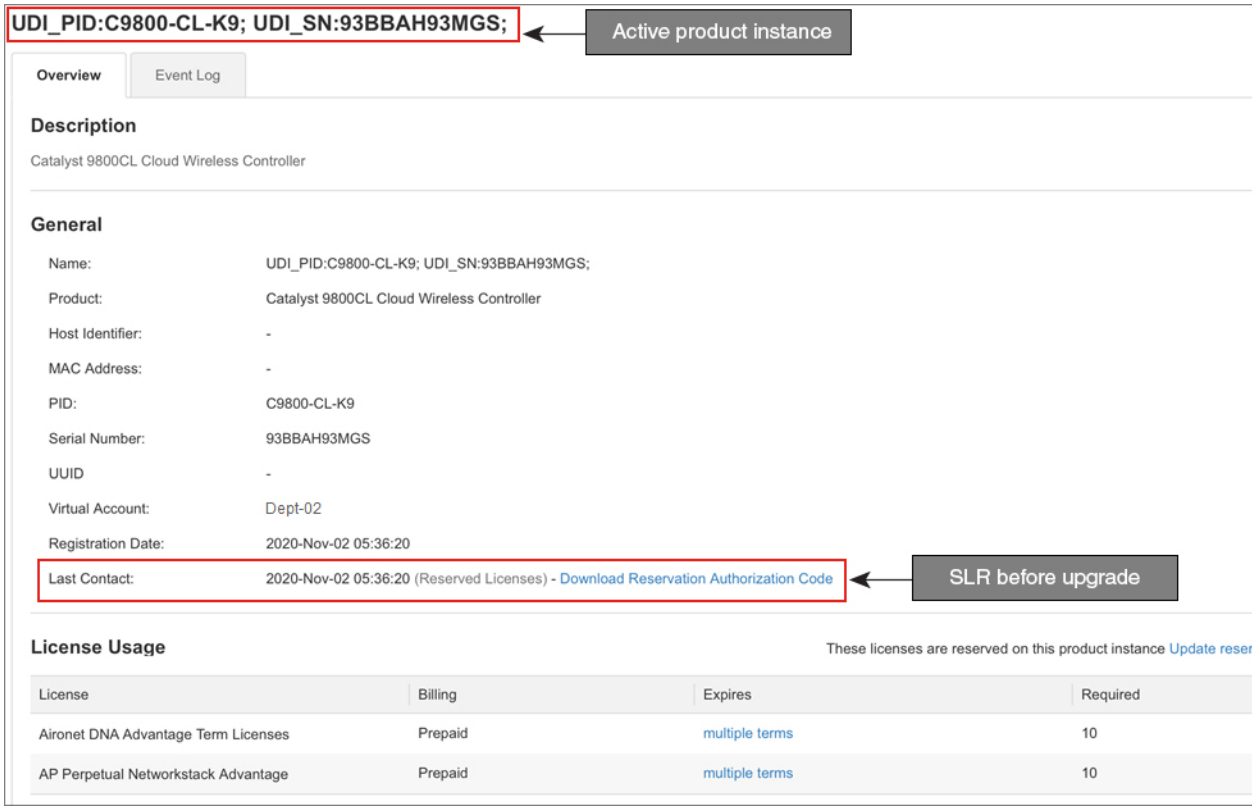
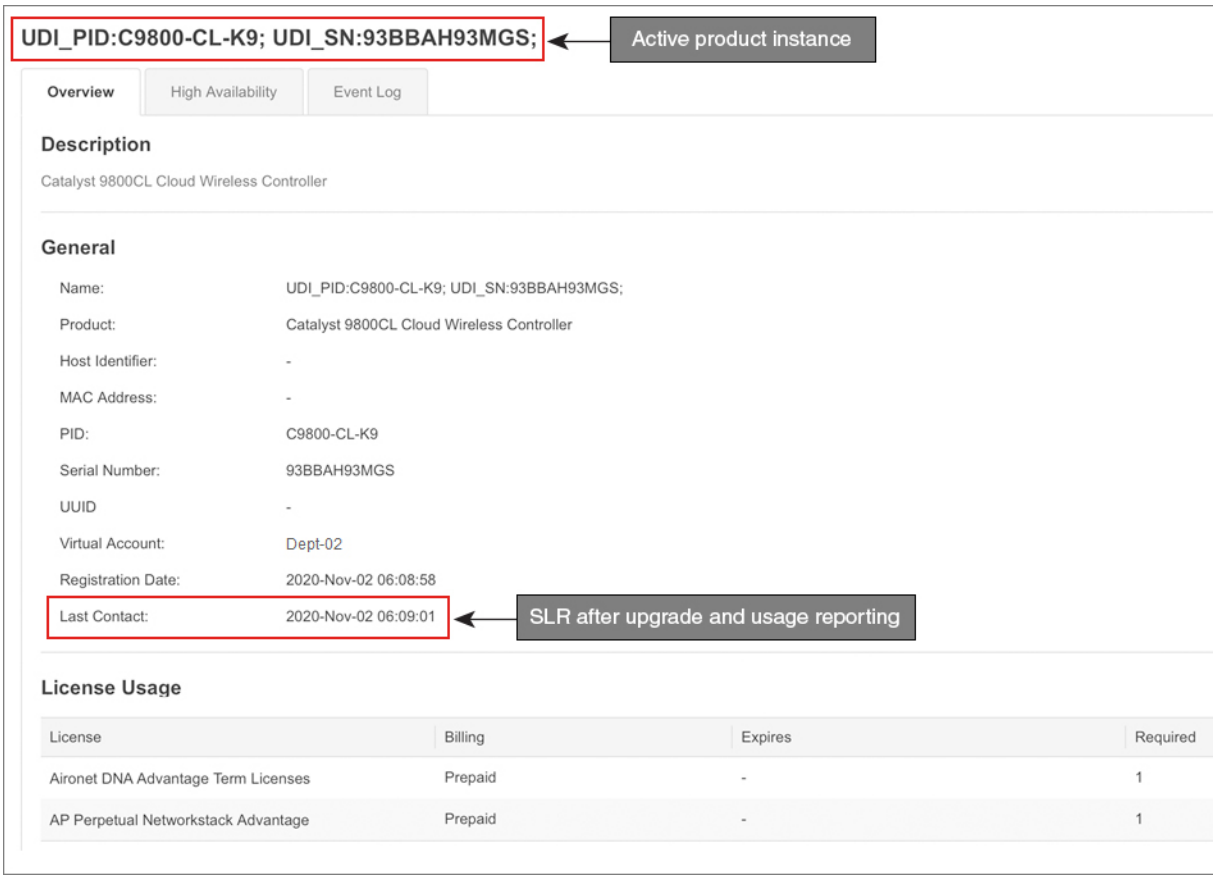


図 *12 : SLR* からポリシーを使用したスマートライセンシング：アップグレード後のアクティブな製品インスタンス



移行後のレポート

SLR ライセンスは、ライセンスの使用に変化した場合にのみレポートを必要とします（たとえば、サブスクリプション ライセンスを指定された期間使用する場合）。

エアギャップネットワークでは、**show license status** の出力の `Next report push:` の日付を使用して、次の使用状況レポートの送信タイミングを確認することで、製品インスタンスと CSSM が同期されます。

製品インスタンスとのすべての通信を無効にしているため、ライセンスの使用状況をレポートするには、RUM レポートをファイルに保存してから、CSSM にアップロードする必要があります（インターネットとシスコに接続されているワークステーションからアップロード）。

1. RUM レポートの生成と保存

   license smart save usage コマンドを特権 EXEC モードで入力します。次の例では、すべての RUM レポートがファイル `all_rum.txt` で製品インスタンスのフラッシュメモリに保存されます。シンタックスの詳細については、コマンドリファレンスで license smart（特権 EXEC）コマンドを参照してください。この例では、ファイルはまずブートフラッシュに保存され、次に TFTP の場所にコピーされます。

```
Device# license smart save usage all bootflash:all_rum.txt
Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
```

2. 使用状況データをCSSMにアップロード：CSSMへのデータまたは要求のアップロードとファイルのダウンロード （153 ページ）
3. ACKを製品インスタンスにインストール：製品インスタンスへのファイルのインストール （154 ページ）

例：評価ライセンスまたは期限切れライセンスからポリシーを使用したスマートライセンシングへ

以下は、評価期限切れライセンス（スマートライセンシング）を、ポリシーを使用したスマートライセンシングに移行したCisco Catalyst 9800-CL ワイヤレスコントローラの例です。

評価ライセンスの概念は、ポリシーを使用したスマートライセンスには適用されません。ソフトウェアバージョンを、ポリシーを使用したスマートライセンシングをサポートするバージョンにアップグレードすると、すべてのライセンスがIN USEとして表示され、シスコのデフォルトポリシーが製品インスタンスに適用されます。Cisco Catalystワイヤレスコントローラのライセンスはすべて適用されない（適用タイプ）であるため、機能は失われません。

- 表 8 : 評価ライセンスまたは期限切れライセンスからポリシーを使用したスマートライセンシングへ：show コマンド （108 ページ）
- 移行後の CSSM Web UI （112 ページ）
- 移行後のレポート （112 ページ）

次の表に、ポリシーを使用したスマートライセンシングへのアップグレード後に、**show** コマンドの出力でチェックすべき主な変更点または新しいフィールドを示します。

表 *8 :* 評価ライセンスまたは期限切れライセンスからポリシーを使用したスマートライセンシングへ：***show*** コマンド

アップグレード前（スマートライセンシング、評価モード）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license summary ライセンスはUNREGISTEREDで、EVAL MODEになっています。	**show license summary** すべてのライセンスが移行され、IN USEになっています。評価モードライセンスがありません。

アップグレード前（スマートライセンシング、評価モード）	アップグレード後（ポリシーを使用したスマートライセンシング）
Device# **show license summary** Smart Licensing is ENABLED Registration: **Status: UNREGISTERED** Export-Controlled Functionality: NOT ALLOWED License Authorization: Status: EVAL EXPIRED License Usage: License Entitlement tag Count Status --- (DNA_NWStack) 1 **EVAL EXPIRED** (AIR-DNA-A) 1 **EVAL EXPIRED**	Device# **show license summary** License Usage: License Entitlement Tag Count Status --- air-network-advantage (DNA_NWStack) 1 IN USE air-dna-advantage (AIR-DNA-A) 1 IN USE

アップグレード前（スマートライセンシング、評価モード）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license usage Device# **show license usage** License Authorization: Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC (DNA_NWStack): Description: Count: 1 Version: 1.0 Status: EVAL EXPIRED Export status: NOT RESTRICTED (AIR-DNA-A): Description: Count: 1 Version: 1.0 Status: EVAL EXPIRED Export status: NOT RESTRICTED	**show license usage** Enforcement Type フィールドに NOT ENFORCED と表示されます。（Cisco Catalyst ワイヤレスコントローラには、輸出規制ライセンスや適用ライセンスはありません）。 Device# **show license usage** License Authorization: Status: Not Applicable air-network-advantage (DNA_NWStack): Description: air-network-advantage Count: 1 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: air-network-advantage Feature Description: air-network-advantage **Enforcement type: NOT ENFORCED** License type: Perpetual air-dna-advantage (AIR-DNA-A): Description: air-dna-advantage Count: 1 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: air-dna-advantage Feature Description: air-dna-advantage **Enforcement type: NOT ENFORCED** License type: Perpetual

アップグレード前（スマートライセンシング、評価モード）	アップグレード後（ポリシーを使用したスマートライセンシング）
show license status	**show license status** `Transport:` フィールドには、デフォルトのタイプが設定されていて、製品インスタンスが CSLU を検出するための URL またはメソッドが指定されていないことが表示されます。 `Trust Code Installed:` フィールドには、信頼コードがインストールされていないことが表示されます。 `Policy:` ヘッダーと詳細には、`Cisco default` ポリシーが適用されていることが示されます。 `Usage Reporting:` ヘッダーの `Next report push:` フィールドには、次の RUM レポートを CSSM に送信するタイミングに関する情報が表示されます。

アップグレード前（スマートライセンシング、評価モード）	アップグレード後（ポリシーを使用したスマートライセンシング）

Device# **show license status**
 	
Smart Licensing is ENABLED
 	
Utility:
  Status: DISABLED
 	
Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
 	
Transport:
  Type: Callhome
 	
Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED
 	
License Authorization:
  Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC
 	
Export Authorization Key:
  Features Authorized:
  <none>
	Device# **show license status**
	Utility:
	  Status: DISABLED
	
	Smart Licensing Using Policy:
	  Status: ENABLED
	
	Data Privacy:
	  Sending Hostname: yes
	  Callhome hostname privacy: DISABLED
	  Smart Licensing hostname privacy: DISABLED
	  Version privacy: DISABLED
	
	Transport:
	  Type: cslu
	  Cslu address: <empty>
	  Proxy:
	  Not Configured
	
	Policy:
	  Policy in use: Merged from multiple sources.
	  Reporting ACK required: yes (CISCO default)
	  Unenforced/Non-Export Perpetual Attributes:
	  First report requirement (days): 365 (CISCO default)
	
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Unenforced/Non-Export Subscription Attributes:
	  First report requirement (days): 90 (CISCO default)
	
	  Reporting frequency (days): 90 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Enforced (Perpetual/Subscription) License Attributes:
	
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	  Export (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	
	Miscellaneous:
	  Custom Id: <empty>
	
	Usage Reporting:
	  Last ACK received: <none>
	  Next ACK deadline: <none>
	  Reporting push interval: 0 (no reporting)
	  Next ACK push check: <none>
	  Next report push: <none>
	  Last report push: <none>
	  Last report file write: <none>
	
	Trust Code Installed: <none>

移行後の CSSM Web UI

https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。[Inventory] > [Product Instances] で、移行された製品インスタンスの [Last Contact] フィールドに、移行後に更新されたタイムスタンプが表示されます。

移行後のレポート

サポートされているトポロジのいずれかを実装し、レポート要件に適合するようにします。サポートされるトポロジ （55 ページ）およびポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （75 ページ）を参照してください。使用可能なレポートメソッドは、実装するトポロジによって異なります。

Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行

必要な最小バージョンよりも前の SSM オンプレミスのバージョンを使用している場合（SSM オンプレミス （48 ページ）を参照）、SSM オンプレミスのバージョンおよび製品インスタンスを移行するために従う必要があるプロセスや手順の概要としてこの項を使用できます。

1. SSM オンプレミスをアップグレードします。

   必要な最小バージョンであるバージョン 8、リリース 202102 以降にアップグレードします。

   『Cisco Smart Software Manager On-Prem Migration Guide』を参照してください。

2. 製品インスタンスをアップグレードします。

   必要な最小ソフトウェアバージョンについては、SSM オンプレミス （48 ページ）を参照してください。

   アップグレード手順については、ワイヤレス コントローラ ソフトウェアのアップグレード （91 ページ）を参照してください。

3. CSSM へのローカルアカウントの再登録

   オンラインとオフラインのオプションを使用できます。『Cisco Smart Software Manager On-Prem Migration Guide』[英語] の「*Re-Registering a local Account (Online Mode)*」または「*Manually Re-Registering a Local Account (Offline Mode)*」を参照してください。

   再登録が完了すると、次のイベントが自動的に発生します。

   - SSM オンプレミスは、SSM オンプレミスのテナントを指す新しいトランスポート URL で応答します。
   - 製品インスタンスのトランスポートタイプ設定が **call-home** または **smart** から **cslu** に変更されます。トランスポート URL も自動的に更新されます。

4. 特権 EXEC モードで **copy running-config startup-config** コマンドを入力して、製品インスタンスの設定変更を保存します。

5. 製品インスタンスの古いオンプレミス スマート ライセンス証明書をクリアし、製品インスタンスをリロードします。この後は設定変更を保存しないでください。

（注） この手順は、製品インスタンスで実行されているソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.x または Cisco IOS XE Bengaluru 17.4.x の場合にのみ必要です。

特権 EXEC モードで **licence smart factory reset** コマンドと **reload** コマンドを入力します。

```
Device# licence smart factory reset
Device# reload
```

6. 使用状況の同期の実行

   1. 製品インスタンスに特権 EXEC モードで **license smart sync** {**all**|**local**} コマンドを入力します。これにより、SSM オンプレミスと製品インスタンスが同期され、保留中のデータが送受信されます。

      ```
      Device(config)# license smart sync local
      ```

      これは、SSM オンプレミス UI で確認できます。[Inventory] > [SL Using Policy] に移動します。[Alerts] 列に、「Usage report from product instance」というメッセージが表示されます。

   2. 使用状況情報を CSSM と同期します（いずれかを選択）。

      - オプション 1：

        SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。

      - オプション 2：

        SSM オンプレミスが CSSM に接続されていません。使用状況データのエクスポートとインポート（SSM オンプレミス UI） （130 ページ）を参照してください。

結果：

移行および使用状況の最初の同期が完了しました。製品インスタンスとライセンス使用状況情報が SSM オンプレミスに表示されるようになりました。

後続のレポートには、次のオプションが含まれています。

- 製品インスタンスと SSM オンプレミスとの間でデータを同期するには、次の手順を実行します。
  - レポート間隔を設定して、製品スタンスと SSM オンプレミスとの間の定期的な同期をスケジュールします。グローバル コンフィギュレーション モードで **license smart usage interval** *interval_in_days* コマンドを入力します。

製品インスタンスが次にいつRUMレポートを送信するかを確認するには、特権EXECモードで **show license all** コマンドを入力し、出力の [Next report push:] フィールドを確認します。

- 製品インスタンスとSSMオンプレミスとの間でアドホックまたはオンデマンドの同期を行うには、**license smart sync** 特権EXECコマンドを入力します。

- 使用状況情報をCSSMと同期するには、次の手順を実行します。
  - CSSMとの定期的な同期をスケジュールします。SSMオンプレミスUIで、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。次の頻度情報を入力し、保存します。
    - [Days]：同期が実行される頻度を示します。たとえば、2を入力すると、同期は2日に1回行われます。
    - [Time of Day]：24時間表記法で、同期が実行される時刻を示します。たとえば、14 hoursと0 minutesを入力すると、ローカルタイムゾーンの午後2時（1400）に同期が行われます。
  - レポートに必要なファイルをアップロードおよびダウンロードします。使用状況データのエクスポートとインポート（SSMオンプレミスUI）（130ページ）を参照してください。

ポリシーを使用したスマートライセンシングのタスクライブラリ

このセクションでは、ポリシーを使用したスマートライセンシングに適用されるタスクのグループ化について説明します。製品インスタンス、CSLUインターフェイス、およびCSSM Web UIで実行されるタスクが含まれます。

特定のトポロジを実装するには、対応するワークフローを参照して、適用されるタスクの順序を確認します。ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー（75ページ）を参照してください。

追加の設定タスクを実行する場合（たとえば別のライセンスの設定、アドオンライセンスの使用、またはより短いレポート間隔の設定）は、対応するタスクを参照してください。続行する前に、入手可能な場合には「サポートされるトポロジ」を確認してください。

シスコへのログイン（CSLUインターフェイス）

必要に応じて、CSLUで作業するときに接続モードまたは切断モードのいずれかにすることができます。接続モードで作業するには、次の手順を実行してシスコに接続します。

手順

ステップ 1 CSLU のメイン画面で、[Login to Cisco]（画面の右上隅）をクリックします。

ステップ 2 [CCO User Name] と [CCO Password] を入力します。

ステップ 3 CSLU の [Preferences] タブで、シスコ接続トグルに「Cisco Is Available」と表示されていることを確認します。

スマートアカウントとバーチャルアカウントの設定（CSLU インターフェイス）

スマートアカウントとバーチャルアカウントはどちらも [Preferences] タブで設定します。シスコに接続するためのスマートアカウントとバーチャルアカウントの両方を設定するには、次の手順を実行します。

手順

ステップ 1 CSLU のホーム画面から [Preferences] タブを選択します。

ステップ 2 スマートアカウントとバーチャルアカウントの両方を追加するには、次の手順を実行します。

a) [Preferences] 画面で、[Smart Account] フィールドに移動し、[Smart Account Name] を追加します。

b) 次に、[Virtual Account] フィールドに移動し、[Virtual Account Name] を追加します。

CSSM に接続している場合（[Preferences] タブに「Cisco is Available」）、使用可能な SA/VA のリストから選択できます。

CSSM に接続していない場合（[Preferences] タブに「Cisco Is Not Available」）、SA/VA を手動で入力します。

（注） SA/VA 名では大文字と小文字が区別されます。

ステップ 3 [Save] をクリックします。SA/VA アカウントがシステムに保存されます。

一度に 1 つの SA/VA ペアのみが CSLU に存在できます。複数のアカウントを追加することはできません。別の SA/VA ペアに変更するには、ステップ 2a および 2b を繰り返してから [Save] をクリックします。新しい SA/VA アカウントペアは、以前に保存されたペアを置き換えます。

CSLU での製品開始型製品インスタンスの追加（CSLU インターフェイス）

[Preferences] タブを使用してデバイス作成の製品インスタンスを追加するには、次の手順を実行します。

手順

ステップ 1 [Preferences] タブを選択します。

ステップ 2 [Preferences] 画面で、[Validate Instance] チェックボックスをオフにします。

ステップ 3 [Default Instance Method] を [Product Instance Initiated] に設定し、[Save] をクリックします。

製品インスタンス開始型通信のネットワーク到達可能性の確認

このタスクでは、製品インスタンス開始型通信のネットワーク到達可能性を確認するために必要になる可能性のある設定を提供します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

始める前に

サポートされるトポロジ：CSLU を介して CSSM に接続（製品インスタンス開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 4	**vrf forwarding** *vrf-name* 例：	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、イン

	コマンドまたはアクション	目的
	`Device(config-if)# vrf forwarding Mgmt-vrf`	ターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 6	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。 （注） Cisco Catalyst 9800-L-F ワイヤレスコントローラ 10G ポートは、自動ネゴシエーション操作をサポートしていません。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーションモードを終了し、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 8	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface gigabitethernet0/0`	HTTP クライアントのソース インターフェイスを設定します。
ステップ 9	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	（必須）製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# Device(config)# ip name-server vrf mgmt-vrf 173.37.137.85`	VRF インターフェイスでドメインネームシステム（DNS）を設定します。
ステップ 11	**ip domain lookup source-interface** *interface-type-number* 例：	DNS ドメインルックアップ用のソースインターフェイスを設定します。

	コマンドまたはアクション	目的
	`Device(config)# ip domain lookup source-interface gigabitethernet0/0`	
ステップ 12	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメインの DNS ディスカバリを設定します。ここの例では、ネームサーバはエントリ `cslu-local.example.com` を作成します。

CSLU での CSLU 開始型製品インスタンスの追加（CSLU インターフェイス）

CSLU インターフェイスを使用して、接続方法を CSLU 開始型に設定できます。この接続方法（モード）により、CSLU は製品インスタンスから製品インスタンス情報を取得できます。

（注） デフォルトの接続方法は、[Preferences] タブで設定されます。

[Inventory] タブから製品インスタンスを追加するには、次の手順を実行します。

手順

ステップ 1 [Inventory] タブに移動し、[Product Instances] テーブルから [Add Single Product] を選択します。

ステップ 2 [Host] に入力します（ホストの IP アドレス）。

ステップ 3 [Connect Method] を選択し、CSLU 開始の接続方法を 1 つを選択します。

ステップ 4 右側のパネルで、[Product Instance Login Credentials] をクリックします。画面の左側のパネルが変化して [User Name] フィールドと [Password] フィールドに変わります。

ステップ 5 製品インスタンスの [User Name] と [Password] を入力します。

ステップ 6 [保存（**Save**）] をクリックします。

情報がシステムに保存され、デバイスが [Product Instances] テーブルにリストされて、[Last Contact] には [never] と表示されます。

使用状況レポートの収集：CSLU 開始（CSLU インターフェイス）

CSLU では、デバイスからの使用状況レポートの収集を手動でトリガーすることもできます。

製品インスタンスを設定して選択した後（[Add Single Product] を選択し、[Host] に名前を入力して [CSLU Initiated] 接続メソッドを選択）、[Actions for Selected] > [Collect Usage] を選択します。CSLU は選択した製品インスタンスに接続し、使用状況レポートを収集します。収集された使用状況レポートは、CSLU のローカルライブラリに保存されます。これらのレポートは、

CSLU がシスコに接続されている場合はシスコに転送できます。または（シスコに接続されていない場合は）[Data] > [Export to CSSM] の順に選択して、手動で使用状況の収集をトリガーできます。

CSLU 開始モードで作業している場合は、次の手順を実行して、製品インスタンスから RUM レポートを収集するように CSLU を設定します。

手順

ステップ 1 [Preferences] タブをクリックし、有効な [Smart Account] と [Virtual Account] を入力して、適切な CSLU 開始型収集メソッドを選択します。（[Preferences] に変更があった場合は、[Save] をクリックします）。

ステップ 2 [Inventory] タブをクリックし、1 つまたは複数の製品インスタンスを選択します。

ステップ 3 [Actions for Selected] > [Collect Usage] をクリックします。

RUM レポートは、選択した各デバイスから取得され、CSLU ローカルライブラリに保存されます。[Last Contacted] 列が更新され、レポートが受信された時刻が表示されます。[Alerts] 列にはステータスが表示されます。

CSLU が現在シスコにログインしている場合、レポートはシスコの関連するスマートアカウントとバーチャルアカウントに自動的に送信され、シスコはCSLU と製品インスタンスに確認応答を送信します。確認応答は、[Product Instance] テーブルの [Alerts] 列に表示されます。シスコに手動で使用状況レポートを転送するには、CSLU のメイン画面から [Data] > [Export to CSSM] を選択します。

ステップ 4 [Export to Cisco] モーダルから、レポートを保存するローカルディレクトリを選択します。（<CSLU_WORKING_Directory>/data/default/rum/unsent）

この時点で、使用状況レポートがローカルディレクトリ（ライブラリ）に保存されます。使用状況レポートをシスコにアップロードするには、CSSMへのデータまたは要求のアップロードとファイルのダウンロード （153 ページ） の手順に従ってください。

（注） Windows オペレーティングシステムでは、ファイルの名前が変更されたときに拡張子をドロップすることで、使用状況レポートファイルのプロパティの動作を変更できます。動作の変更は、ダウンロードしたファイルの名前を変更し、名前を変更したファイルが拡張子をドロップすると発生します。たとえば、`UD_xxx.tar` という名前のダウンロード済みデフォルトファイルの名前が `UD_yyy` に変更されたとします。ファイルは tar 拡張子を失い、機能しなくなります。使用状況ファイルを正常に機能させるには、使用状況レポートファイルの名前を変更した後、`UD_yyy.tar` のように、ファイル名に tar 拡張子を追加する必要があります。

CSSM へのエクスポート（CSLU インターフェイス）

[Download All for Cisco] メニューオプションは、オフラインの目的で使用される手動プロセスです。[Download For Cisco] メニューオプションを使用するには、次の手順を実行します。

手順

ステップ 1 [Preferences] タブに移動し、[Cisco Connectivity] トグルスイッチをオフにします。

フィールドが「Cisco Is Not Available」に切り替わります。

ステップ 2 ホーム画面から、[Data] > [Export to CSSM] の順に移動します。

ステップ 3 開いたウィンドウからファイルを選択し、[Save] をクリックします。これでファイルが保存されました。

（注） この時点で、DLC ファイル、RUM ファイル、またはその両方があります。

ステップ 4 シスコに接続できる端末に移動し、次の手順を実行します。CSSM へのデータまたは要求のアップロードとファイルのダウンロード （153 ページ）

ファイルがダウンロードされたら、CSLU にインポートできます。CSSM からのインポート（CSLU インターフェイス） （120 ページ）を参照してください。

CSSM からのインポート（CSLU インターフェイス）

シスコから ACK またはその他のファイル（承認コードなど）を受信すると、そのファイルをシステムにアップロードできます。この手順は、オフラインのワークステーションに使用できます。シスコからファイルを選択してアップロードするには、次の手順を実行します。

手順

ステップ 1 CSLU にアクセス可能な場所にファイルがダウンロードされていることを確認します。

ステップ 2 CSU のホーム画面から、[Data] > [Import from CSSM] の順に移動します。

ステップ 3 [Import from CSSM] モーダルが開き、次のいずれかを実行できます。

- ローカルドライブにあるファイルをドラッグアンドドロップします。または、
- 適切な *.xml ファイルを参照し、ファイルを選択して [Open] をクリックします。

アップロードが成功すると、ファイルがサーバーに正常に送信されたことを示すメッセージが表示されます。アップロードが成功しない場合は、インポートエラーが発生します。

ステップ 4 アップロードが完了したら、ウィンドウの右上隅にある [x] をクリックして閉じます。

CSLU 開始型通信のネットワーク到達可能性の確認

このタスクでは、CSLU 開始型通信のネットワーク到達可能性を確認するために必要になる可能性のある設定を提供します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

始める前に

サポートされるトポロジ：CSLU を介して CSSM に接続（CSLU 開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**aaa new model** 例： `Device(config)# aaa new model`	（必須）認証、許可、アカウンティング（AAA）アクセスコントロールモデルをイネーブルにします。
ステップ 4	**aaa authentication login default local** 例： `Device(config)# aaa authentication login default local`	（必須）認証時にローカルのユーザ名データベースを使用するように、AAA 認証を設定します。
ステップ 5	**aaa authorization exec default local** 例： `Device(config)# aaa authorization exec default local`	ネットワークへのユーザアクセスを制限するパラメータを設定します。ユーザは EXEC シェルの実行が許可されます。
ステップ 6	ip routing 例： `Device(config)# ip routing`	IP ルーティングを有効にします。
ステップ 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server vrf Mgmt-vrf`	（任意）名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区

	コマンドまたはアクション	目的
	192.168.1.100 192.168.1.200 192.168.1.300	切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNSクエリを最初に送信します。そのクエリが失敗した場合は、バックアップサーバにクエリが送信されます。
ステップ 8	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	デバイス上で、DNSに基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 9	**ip domain name** *name* 例： `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	非完全修飾ホスト名（ドット付き10進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。
ステップ 10	**no username** *name* 例： `Device(config)# no username admin`	（必須）指定されたユーザ名が存在する場合はクリアします。*name*には、次のステップで作成するユーザ名と同じものを入力します。これにより、次のステップで作成するユーザ名が重複していないことが保証されます。 CSLU 開始型の RUM レポート取得に REST API を使用する場合は、CSLUにログインする必要があります。ここでユーザ名が重複していると、システムにユーザ名が重複している場合にこの機能が正しく動作しないことがあります。
ステップ 11	**username** *name* **privilege** *level* **password** *password* 例：	（必須）ユーザ名をベースとした認証システムを構築します。

	コマンドまたはアクション	目的
	`Device(config)# username admin privilege 15 password 0 lab`	**privilege** キーワードにより、ユーザの権限レベルを設定します。ユーザの権限レベルを指定する 0 ～ 15 の数字です。 password を使用すると、name 引数にアクセスできます。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 これにより、CSLU が製品インスタンスのネイティブ REST を使用できるようになります。 （注） このユーザ名とパスワードを CSLU で入力します（使用状況レポートの収集：CSLU 開始（CSLU インターフェイス）（118 ページ）→ステップ 4.f）。その後、CSLU は製品インスタンスから RUM レポートを収集できます。
ステップ 12	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 13	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。

	コマンドまたはアクション	目的
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	無効にされたインターフェイスを再起動します。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、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 18	**ip http server** 例： `Device(config)# ip http server`	（必須）シスコの Web ブラウザ ユーザ インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。HTTP サーバは、デフォルトにより標準のポート 80 を使用します。

ステップ 19	**ip http authentication local**
	例：
	`ip http authentication local`
	`Device(config)#`
		（必須）HTTP サーバユーザに対して特定の認証方法を指定します。
		local キーワードは、認証および許可に、ローカルシステム設定で（username グローバル コンフィギュレーション コマンドによって）指定したログイン ユーザ名、パスワード、権限レベル アクセスの組み合わせを使用することを示します。

ステップ 20	**ip http secure-server** 例： `Device(config)# ip http server`	（必須）セキュア HTTP（HTTPS）サーバを有効にします。HTTPS サーバは、セキュア ソケット レイヤ（SSL）バージョン 3.0 プロトコルを使用します。
ステップ 21	**ip http max-connections** 例： `Device(config)# ip http max-connections 16`	（必須）HTTP サーバへの同時最大接続数を設定します。1 ～ 16 の範囲の整数を入力します。デフォルトは 5 です。
ステップ 22	**ip tftp source-interface** *interface-type-number* 例： `Device(config)# ip tftp source-interface GigabitEthernet0/0`	TFTP 接続用の送信元アドレスとして、インターフェイスの IP アドレスを指定します。
ステップ 23	**ip route** *ip-address ip-mask subnet mask* 例：	製品インスタンスにルートとゲートウェイを設定します。スタティック

	コマンドまたはアクション	目的
	`Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	ルートまたはダイナミックルートのいずれかを設定できます。
ステップ 24	**logging host** 例： `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	リモートホストへのシステムメッセージおよびデバッグ出力を記録します。
ステップ 25	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 26	**show ip http server session-module** 例： `Device# show ip http server session-module`	（必須）HTTP 接続を確認します。出力で、`SL_HTTP` がアクティブであることを確認します。また、次のチェックも実行できます。 • CSLU がインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます • CSLU がインストールされているデバイスの Web ブラウザで、`https://<product-instance-ip>/` を確認します。これにより、CSLU から製品インスタンスへの REST API が期待どおりに動作することが保証されます。

スマートアカウントとバーチャルアカウントの割り当て（SSMオンプレミス UI）

この手順を使用して、1 つ以上の製品インスタンスを対応するスマートアカウントおよびバーチャルアカウント情報とともに SSM オンプレミスのデータベースにインポートできます。これにより、SSM オンプレミスは、ローカルバーチャルアカウント（デフォルトのローカルバーチャル アカウント以外）の一部である製品インスタンスを CSSM の正しいライセンスプールにマッピングできます。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

ステップ 1 SSM オンプレミスにログインし、[Smart Licensing] ワークスペースを選択します。

ステップ 2 [Inventory] > [SL Using Policy] > [Export/Import All] > [Import Product Instances List] に移動します。

[Upload Product Instances] ウィンドウが表示されます。

ステップ 3 [Download] をクリックして .csv テンプレートファイルをダウンロードし、テンプレート内のすべての製品インスタンスに必要な情報を入力します。

ステップ 4 テンプレートに入力したら、[Inventory] > [SL Using Policy] > [Export/Import All] > [Import Product Instances List] をクリックします。

[Upload Product Instances] ウィンドウが表示されます。

ステップ 5 [Browse] をクリックし、入力した .csv テンプレートをアップロードします。

アップロードしたすべての製品インスタンスのスマートアカウント情報とバーチャルアカウント情報が SSM オンプレミスで使用できるようになりました。

デバイスの検証（SSM オンプレミス UI）

デバイス検証が有効になっている場合、不明な製品インスタンス（SSM オンプレミスデータベース内にない）からの RUM レポートは拒否されます。

デフォルトでは、デバイスは検証されません。検証を有効にするには、次の手順を実行します。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

ステップ 1 [On-Prem License Workspace] ウィンドウで、[Admin Workspace] をクリックし、プロンプトが表示されたらログインします。

[On-Prem Admin Workspace] ウィンドウが表示されます。

ステップ 2 [Settings] ウィジェットをクリックします。

[Settings] ウィンドウが表示されます。

ステップ 3 [CSLU] タブに移動し、[Validate Device] トグルスイッチをオンにします。

不明な製品インスタンスからの RUM レポートが拒否されるようになりました。必要な製品インスタンスを SSM オンプレミスデータベースにまだ追加していない場合は、RUM レポートを送信する前に追加する必要があります。スマートアカウントとバーチャルアカウントの割り当て（SSM オンプレミス UI） （125 ページ） を参照してください

製品インスタンス開始型通信のネットワーク到達可能性の確認

このタスクでは、製品インスタンス開始型通信のネットワーク到達可能性を確認するために必要になる可能性のある設定を提供します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

（注） 手順 13、14、および 15 では、必ず次のように設定してください。これらのコマンドは、正しいトラストポイントが使用され、ネットワーク到達可能性に必要な証明書が受け入れられるように設定する必要があります。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 6	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーションモードを終了し、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 8	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface gigabitethernet0/0`	HTTP クライアントのソース インターフェイスを設定します。
ステップ 9	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	（必須）製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# Device(config)# ip name-server vrf mgmt-vrf 198.51.100.1`	VRF インターフェイスでドメインネームシステム（DNS）を設定します。
ステップ 11	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	DNS ドメインルックアップ用のソースインターフェイスを設定します。
ステップ 12	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメインの DNS ディスカバリを設定します。この例では、ネームサーバがエントリ `cslu-local.example.com` を作成します。

	コマンドまたはアクション	目的

ステップ 13	**crypto pki trustpoint SLA-TrustPoint**
	例：
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		（必須）製品インスタンスがトランスポイント「SLA-TrustPoint」を使用する必要があることを宣言し、CA トランスポイント コンフィギュレーション モードを開始します。このコマンドを使用してトラストポイントを宣言するまで、製品インスタンスはトラストポイントを認識しません。

ステップ 14	enrollment terminal 例： `Device(ca-trustpoint)# enrollment terminal`	（必須）証明書登録方式を指定します。
ステップ 15	**revocation-check none** 例： `Device(ca-trustpoint)# revocation-check none`	（必須）ピアの証明書が失効していないことを確認するために使用する方法を指定します。SSM オンプレミス展開トポロジの場合は、**none** キーワードを入力します。つまり、失効チェックは実行されず、証明書は常に受け入れられます。

ステップ 16	**exit**
	例：
	`Device(ca-trustpoint)# exit`
	`Device(config)# exit`
		CA トランスポイント コンフィギュレーション モードを終了し、次にグローバル コンフィギュレーション モードを終了してから、特権 EXEC モードに戻ります。

ステップ 17	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

トランスポート URL の取得（SSM オンプレミス UI）

製品インスタンス開始型通信を SSM オンプレミス展開で展開するときに、製品インスタンスでトランスポート URL を設定する必要があります。このタスクでは、テナント ID を含む完全な URL を SSM オンプレミスから簡単にコピーする方法を示します。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

ステップ 1 SSM オンプレミスにログインし、[Smart Licensing] ワークスペースを選択します。

ステップ 2 [Inventory] タブに移動し、ローカルバーチャルアカウントのドロップダウンリスト（右上隅）から、デフォルトのローカルバーチャルアカウントを選択します。この場合、[Inventory] タブの下の領域に [Local Virtual Account: Default] が表示されます。

ステップ 3 [General] タブに移動します。

[Product Instance Registration Tokens] 領域が表示されます。

ステップ 4 [Product Instance Registration Tokens] 領域で、[CSLU Transport URL] をクリックします。

[Product Registration URL] ポップアップウィンドウが表示されます。

ステップ 5 URL 全体をコピーし、アクセス可能な場所に保存します。

製品インスタンスでトランスポートタイプと URL を設定するときに、この URL が必要になります。

ステップ 6 トランスポートタイプと URL を設定します。転送タイプ、URL、およびレポート間隔の設定（155 ページ）を参照してください。

使用状況データのエクスポートとインポート（SSMオンプレミスUI）

SSM オンプレミスが CSSM から切断されている場合は、この手順を使用して SSMオンプレミスと CSSM との間で使用状況の同期を実行できます。

始める前に

サポートされているトポロジ：

- SSM オンプレミス展開（SSM オンプレミス開始型通信）
- SSM オンプレミス展開（製品インスタンス開始型通信）。

レポートデータは、SSMオンプレミスで使用できる必要があります。必要なレポートデータを製品インスタンスからSSMオンプレミスにプッシュする（製品インスタンス開始型通信）か、または必要なレポートデータを製品インスタンスから取得する（SSM オンプレミス開始型通信）必要があります。

手順

ステップ 1 SSM オンプレミスにログインし、[Smart Licensing] を選択します。

ステップ 2 [Inventory] > [SL Using Policy] タブに移動します。

ステップ 3 [SL Using Policy] タブ領域で、[Export/Import All ...] > [Export Usage to Cisco] をクリックします。

これにより、SSM オンプレミスサーバで使用可能なすべての使用状況レポートを含む .tar ファイルが 1 つ生成されます。

ステップ 4 CSSM でCSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ）のタスクを実行します。

このタスクの最後に、SSM オンプレミスにインポートする ACK ファイルを取得します。

ステップ 5 再度、[Inventory] > [SL Using Policy] タブに移動します。

ステップ 6 [SL Using Policy] タブ領域で、[Export/Import All ...] > [Import From Cisco] をクリックします。.tar ACK ファイルをアップロードします。

ACK インポートを確認するには、[SL Using Policy] タブ領域で、対応する製品インスタンスの [Alerts] 列を確認します。「Acknowledgmentreceived from CSSM」というメッセージが表示されます。

1 つ以上の製品インスタンスの追加（SSM オンプレミス UI）

次の手順を使用して、1 つの製品インスタンスを追加したり、複数の製品インスタンスをインポートして追加したりできます。これにより、SSM オンプレミスは製品インスタンスから情報を取得できるようになります。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（SSM オンプレミス開始型通信）。

手順

ステップ 1 SSM オンプレミス UI にログインし、[Smart Licensing] をクリックします。

ステップ 2 [Inventory] タブに移動します。右上隅にあるドロップダウンリストからローカル バーチャル アカウントを選択します。

ステップ 3 [SL Using Policy] に移動します。

ステップ 4 単一の製品インスタンスを追加するか、または複数の製品インスタンスをインポートします（いずれかを選択します）。

- **単一の製品インスタンスを追加**するには、次の手順を実行します。
  1. [SL Using Policy] タブ領域で、[Add Single Product] をクリックします。
  2. [Host] フィールドにホストの IP アドレスを入力します（製品インスタンス）。
  3. [Connect Method] ドロップダウンリストから、適切な SSM オンプレミス開始型の接続方式を選択します。

     SSM オンプレミス開始型通信に使用できる接続方法は、NETCONF、RESTCONF、および REST API です。

4. 右側のパネルで、[Product Instance Login Credentials] をクリックします。

   [Product Instance Login Credentials] ウィンドウが表示されます。

   （注） 製品インスタンスに SLAC が必要な場合は、ログインクレデンシャルのみが必要です。

5. [User ID] と [Password] に入力し、[Save] をクリックします。

   これは、ネットワーク到達可能性を確立するために必要なコマンドの一部として設定したものと同じユーザ ID とパスワードです（SSM オンプレミス開始型通信のネットワーク到達可能性の確保 （132 ページ））。

   検証が完了すると、製品インスタンスが [SL Using Policy] タブ領域のリストに表示されます。

- **複数の製品インスタンスをインポート**するには、次の手順を実行します。

1. [SL Using Policy] タブで、[Export/Import All ...] > [Import Product Instances List] をクリックします。

   [Upload Product Instances] ウィンドウが表示されます。

2. [Download] をクリックし、事前に定義した .csv テンプレートをダウンロードします。

3. .csv テンプレートのすべての製品インスタンスに必要な情報を入力します。

   テンプレートで、すべての製品インスタンスの [Host]、[Connect Method]、および [Login Credentials] を必ず指定してください。

   SSM オンプレミス開始型通信に使用できる接続方法は、NETCONF、RESTCONF、および REST API です。

   ログインクレデンシャルは、ネットワーク到達可能性を確立するために必要なコマンドの一部として設定したユーザ ID とパスワードを参照します（SSM オンプレミス開始型通信のネットワーク到達可能性の確保 （132 ページ））。

4. 再度、[Inventory] > [SL Using Policy] タブに移動します。[Export/Import All....] > [Import Product Instances List] をクリックします。

   [Upload Product Instances] ウィンドウが表示されます。

5. 次に、入力した .csv テンプレートをアップロードします。

   検証されると、製品インスタンスが [SL Using Policy] タブのリストに表示されます。

SSM オンプレミス開始型通信のネットワーク到達可能性の確保

このタスクでは、SSM オンプレミス開始型通信のネットワーク到達可能性を確保するために必要になる可能性のある設定を実行します。「（必須）」と付いている手順は、すべての製品イ

ンスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

（注） 手順 25、26、および 27 では、必ず次のように設定してください。これらのコマンドは、正しいトラストポイントが使用され、ネットワーク到達可能性に必要な証明書が受け入れられるように設定する必要があります。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（SSM オンプレミス開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**aaa new model** 例： `Device(config)# aaa new model`	（必須）認証、許可、アカウンティング（AAA）アクセスコントロールモデルをイネーブルにします。
ステップ 4	**aaa authentication login default local** 例： `Device(config)# aaa authentication login default local`	（必須）認証時にローカルのユーザ名データベースを使用するように、AAA 認証を設定します。
ステップ 5	**aaa authorization exec default local** 例： `Device(config)# aaa authorization exec default local`	ネットワークへのユーザアクセスを制限するパラメータを設定します。ユーザは EXEC シェルの実行が許可されます。
ステップ 6	ip routing 例： `Device(config)# ip routing`	IP ルーティングを有効にします。
ステップ 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例：	（任意）名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。

	コマンドまたはアクション	目的
	`Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNSクエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 8	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	デバイス上で、DNSに基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 9	**ip domain name** *name* 例： `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	非完全修飾ホスト名（ドット付き10進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。
ステップ 10	**no username** *name* 例： `Device(config)# no username admin`	（必須）指定されたユーザ名が存在する場合はクリアします。*name* には、次のステップで作成するユーザ名と同じものを入力します。これにより、次のステップで作成するユーザ名が重複していないことが保証されます。 SSM オンプレミス開始型の RUM レポートを取得に REST API を使用する場合は、SSMオンプレミスにログインする必要があります。ユーザ名が重複していると、システムにそのユーザ名がある場合はこの機能が正しく動作しない場合があります。

	コマンドまたはアクション	目的
ステップ 11	**username** *name* **privilege** *level* **password** *password* 例： `Device(config)# username admin privilege 15 password 0 lab`	（必須）ユーザ名をベースとした認証システムを構築します。 **privilege** キーワードにより、ユーザの権限レベルを設定します。ユーザの権限レベルを指定する 0 ～ 15 の数字です。 password を使用すると、name 引数にアクセスできます。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 これにより、SSM オンプレミスが製品インスタンスのネイティブ REST を使用できるようになります。 （注） このユーザ名とパスワードを SSM オンプレミスに入力します（1 つ以上の製品インスタンスの追加（SSM オンプレミス UI）（131 ページ））。これにより、SSM オンプレミスは製品インスタンスから RUM レポートを収集できるようになります。
ステップ 12	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネット インターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 13	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。

	コマンドまたはアクション	目的
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	無効にされたインターフェイスを再起動します。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーションモードを終了し、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 18	**ip http server** 例： `Device(config)# ip http server`	（必須）シスコの Web ブラウザ ユーザ インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。HTTP サーバは、デフォルトにより標準のポート 80 を使用します。

ステップ 19	**ip http authentication local**
	例：
	`ip http authentication local`
	`Device(config)#`
		（必須）HTTP サーバユーザに対して特定の認証方法を指定します。
		local キーワードは、認証および許可に、ローカルシステム設定で（username グローバル コンフィギュレーション コマンドによって）指定したログイン ユーザ名、パスワード、権限レベル アクセスの組み合わせを使用することを示します。

ステップ 20	**ip http secure-server** 例： `Device(config)# ip http server`	（必須）セキュア HTTP（HTTPS）サーバを有効にします。HTTPS サーバは、セキュア ソケット レイヤ（SSL）バージョン 3.0 プロトコルを使用します。
ステップ 21	**ip http max-connections** 例： `Device(config)# ip http max-connections 16`	（必須）HTTP サーバへの同時最大接続数を設定します。1 ～ 16 の範囲の整数を入力します。デフォルトは 5 です。
ステップ 22	**ip tftp source-interface** *interface-type-number* 例： `Device(config)# ip tftp source-interface GigabitEthernet0/0`	TFTP 接続用の送信元アドレスとして、インターフェイスの IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 23	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 24	**logging host** 例： `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	リモートホストへのシステムメッセージおよびデバッグ出力を記録します。

ステップ 25	**crypto pki trustpoint SLA-TrustPoint**
	例：
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		（必須）製品インスタンスがトランスポイント「SLA-TrustPoint」を使用する必要があることを宣言し、CA トランスポイント コンフィギュレーション モードを開始します。このコマンドを使用してトラストポイントを宣言するまで、製品インスタンスはトラストポイントを認識しません。

ステップ 26	enrollment terminal 例： `Device(ca-trustpoint)# enrollment terminal`	（必須）証明書登録方式を指定します。
ステップ 27	**revocation-check none** 例： `Device(ca-trustpoint)# revocation-check none`	（必須）ピアの証明書が失効していないことを確認するために使用する方法を指定します。SSM オンプレミス展開トポロジの場合は、**none** キーワードを入力します。つまり、失効チェックは実行されず、証明書は常に受け入れられます。

ステップ 28	**end**
	例：
	`Device(ca-trustpoint)# exit`
	`Device(config)# end`
		CA トランスポイント コンフィギュレーション モードを終了し、次にグローバル コンフィギュレーション モードを終了してから、特権 EXEC モードに戻ります。

ステップ 29	**show ip http server session-module** 例： `Device# show ip http server session-module`	（必須）HTTP 接続を確認します。出力で、`SL_HTTP` がアクティブであることを確認します。また、次のチェックも実行できます。

	コマンドまたはアクション	目的
		• SSM オンプレミスがインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます • SSM オンプレミスがインストールされているデバイスの Web ブラウザで、`https://<product-instance-ip>/` を確認します。これにより、SSM オンプレミスから製品インスタンスへの REST API が期待どおりに動作することが保証されます。
ステップ 30	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルに設定を保存します。

CSSM への接続の設定

次の手順では、CSSM へのレイヤ 3 接続を設定してネットワーク到達可能性を確認する方法を説明します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例：	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。

	コマンドまたはアクション	目的
	Device(config)# **ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230**	最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* 例： Device(config)# **ip name-server vrf Mgmt-vrf 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230**	（任意）VRF インターフェイスで DNS を設定します。最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。 （注） このコマンドは、**ip name-server** コマンドの代わりです。
ステップ 5	**ip domain lookup source-interface** *interface-type interface-number* 例： Device(config)# **ip domain lookup source-interface Vlan100**	DNS ドメインルックアップ用のソース インターフェイスを設定します。
ステップ 6	**ip domain name** *domain-name* 例： Device(config)# **ip domain name example.com**	ドメイン名を設定します。
ステップ 7	**ip host tools.cisco.com** *ip-address* 例： Device(config)# **ip host tools.cisco.com 209.165.201.30**	自動 DNS マッピングが使用できない場合は、DNS ホスト名キャッシュ内のホスト名/アドレス静的マッピングを設定します。
ステップ 8	**interface** *interface-type-number* 例： Device(config)# **interface Vlan100** Device(config-if)# **ip address 192.0.2.10 255.255.255.0** Device(config-if)# **exit**	レイヤ 3 インターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。
ステップ 9	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] 例： Device(config)# **ntp server 198.51.100.100 version 2 prefer**	（必須）NTP サービスをアクティブにし（まだアクティブになっていない場合）、システムがシステム ソフトウェア クロックを指定された NTP サーバと同期できるようにします。これによ

	コマンドまたはアクション	目的
		り、デバイスの時刻が CSSM と同期されます。 このコマンドを複数回使用する必要があるために優先サーバを設定する場合は、**prefer** キーワードを使用します。このキーワードを使用すると、サーバ間の切り換え回数が減少します。

ステップ 10	**switchport access vlan** *vlan_id*
	例：
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)# switchport access vlan 100`
	`Device(config-if)# switchport mode access`
	`Device(config-if)# exit`
	`OR`
	`Device(config)#`
		このアクセスポートがトラフィックを伝送する VLAN を有効にし、非トランキングで非タグ付きのシングル VLAN イーサネットインターフェイスとしてインターフェイスを設定します。
		（注） このステップは、スイッチポート アクセス モードが必要な場合にのみ設定します。**switchport access vlan** コマンドは、たとえば Catalyst スイッチング製品インスタンスに適用できます。ルーティング製品インスタンスの場合は、代わりに **ip address** *ip-address mask* コマンドを設定できます。

ステップ 11	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1`	デバイスにルートを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 12	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface Vlan100`	（必須）HTTP クライアントのソースインターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。
ステップ 13	**exit** 例： `Device(config)# exit`	グローバル 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 14	**copy running-config startup-config** 例：	コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

HTTPS プロキシを介したスマート転送の設定

スマート転送モードを使用している場合にプロキシサーバを使用してCSSMと通信するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**license smart transport smart** 例： `Device(config)# license smart transport smart`	スマート転送モードを有効にします。
ステップ 4	**license smart url default** 例： `Device(config)# license smart transport default`	スマート URL を自動的に設定します（https://smartreceiver.cisco.com/licservice/license）。このオプションを想定どおりに動作させるには、前の手順の転送モードを smart に設定する必要があります。

ステップ 5	**license smart proxy** {**address** *address_hostname* | **port** *port_num*}
	例：
	`Device(config)# license smart proxy address 192.168.0.1`
	`Device(config)# license smart proxy port 3128`
		スマート転送モードのプロキシを設定します。プロキシが設定されている場合、ライセンスメッセージは最終宛先 URL（CSSM）に加えてプロキシにも送信されます。プロキシはメッセージをCSSMに送信します。プロキシアドレスとポート番号を個別に設定します。
		• **address** *address_hostname*：プロキシアドレスを指定します。プロキシサーバの IP アドレスまたはホスト名を入力します。

	コマンドまたはアクション	目的
		• **port** *port_num*：プロキシポートを指定します。プロキシ ポートポート番号を入力します。 Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` です。ステータス行の詳細については、RFC 7230 のセクション 3.1.2 を参照してください。

ダイレクトクラウドアクセス用の Call Home サービスの設定

Call Home サービスは、CSSM に対してクリティカルなシステムイベントを電子メールおよび Web 上で通知します。転送モードを設定するには、Call Home サービスを有効にし、宛先プロファイルを設定して（宛先プロファイルには、アラート通知に必要な配信情報が含まれます。少なくとも 1 つの宛先プロファイルが必要です）、次の手順を実行します。

（注） 「（任意）」と特に明記されていない限り、すべての手順を実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**license smart transport callhome** 例： `Device(config)# license smart transport callhome`	転送モードとして Call Home 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	**license smart url** *url* 例： `Device(config)# license smart url https://tools.cisco.com/its/service/oddce/services/DDCService`	**callhome** 転送モードの場合は、例に示すように CSSM URL を設定します。
ステップ 5	**service call-home** 例： `Device(config)# service call-home`	Call Home 機能をイネーブルにします。
ステップ 6	**call-home** 例： `Device(config)# call-home`	Call Home コンフィギュレーション モードを開始します。
ステップ 7	**no http secure server-identity-check** 例： `Device(config-call-home)# no http secure server-identity-check`	HTTP 接続の確立時のサーバー ID チェックを無効にします。
ステップ 8	**contact-email-address** *email-address* 例： `Device(config-call-home)# contact-email-addr username@example.com`	お客様の電子メールアドレスを割り当て、Smart Call Home サービスのフルレポート機能を有効にし、フルインベントリメッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。電子メールアドレスフォーマットには、スペースなしで最大 200 文字まで入力できます。

ステップ 9	**profile** *name*
	例：
	`Device(config-call-home)# profile CiscoTAC-1`
	`Device(config-call-home-profile)#`
		指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。
		デフォルトは次のとおりです。
		• CiscoTAC-1 プロファイルは非アクティブです。このプロファイルを Call Home サービスで使用するには、プロファイルを有効にする必要があります。
		• CiscoTAC-1 プロファイルは、プロファイルに登録されているすべてのイベントタイプが記載された完全なレポートを送信します。または、

	コマンドまたはアクション	目的
		`Device(cfg-call-home-profile)# anonymous-reporting-only` anonymous-reporting-only を追加で設定します。これが設定されている場合は、クラッシュ、インベントリ、およびテストメッセージのみが送信されます。 プロファイルのステータスを確認するには、**show call-home profile all** コマンドを使用します。
ステップ 10	**active** 例： `Device(config-call-home-profile)# active`	宛先プロファイルをイネーブルにします。

ステップ 11	**destination transport-method http**{**email**|**http**}
	例：
	`Device(config-call-home-profile)# destination transport-method http`
	AND
	`Device(config-call-home-profile)# no destination transport-method email`
		メッセージの転送形式をイネーブルにします。この例では、HTTP経由でCall Homeサービスが有効になり、電子メールによる転送が無効になります。
		
		このコマンドのno形式を使用すると、メソッドが無効になります。

ステップ 12	**destination address** { **email** *email_address*|**http** *url*}
	例：
	`Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
	AND
	`Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
		Call Home メッセージを送信する宛先 E メール アドレスまたは URL を設定します。宛先URLを入力する場合は、サーバがセキュアサーバであるかどうかに応じて http://（デフォルト）または https:// を指定します。
		
		ここに示す例では、http:// の形式で宛先URLが設定されています。コマンドの **no** 形式ではhttps://に設定されます。

ステップ 13	**exit** 例： `Device(config-call-home-profile)# exit`	Call Home 宛先プロファイル コンフィギュレーションモードを終了して、Call Home コンフィギュレーション モードに戻ります。
ステップ 14	**exit** 例： `Device(config-call-home)# end`	Call Home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。

	コマンドまたはアクション	目的
ステップ 15	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルに設定を保存します。
ステップ 16	**show call-home profile** {*name* |**all**}	指定されたプロファイル、または設定済みのすべてのプロファイルに関する宛先プロファイル設定を表示します。

HTTPS プロキシサーバを介したダイレクトクラウドアクセス用の Call Home サービスの設定

Call Home サービスは、HTTPS プロキシサーバを介して設定できます。この設定では、CSSM への接続にユーザ認証は必要ありません。

（注） 認証された HTTPS プロキシ設定はサポートされていません。

HTTPS プロキシを介して Call Home サービスを設定して有効にするには、次の手順を実行します。

（注） 「（任意）」と特に明記されていない限り、すべての手順を実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**license smart transport callhome** 例： `Device(config)# license smart transport callhome`	転送モードとして Call Home 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	**service call-home** 例： `Device(config)# service call-home`	Call Home 機能をイネーブルにします。
ステップ 5	**call-home** 例： `Device(config)# call-home`	Call Home コンフィギュレーション モードを開始します。
ステップ 6	**http-proxy** *proxy-address* **proxy-port** *port-number* 例： `Device(config-call-home)# http-proxy 198.51.100.10 port 5000`	Call Home サービスへのプロキシサーバ情報を設定します。 Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` です。ステータス行の詳細については、RFC 7230 のセクション 3.1.2 を参照してください。
ステップ 7	**exit** 例： `Device(config-call-home)# exit`	Call Home コンフィギュレーション モードを終了し、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 8	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

承認コードの削除と返却

SLR 承認コードを削除して返却するには、次の手順を実行します。

始める前に

サポートされるトポロジ：すべて

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**show license summary** 例： `Device# show license summary`	削除して返却するライセンスが使用中でないことを確認します。使用中の場合は、まず機能を無効にする必要があります。

ステップ 3	**license smart authorization return** {**all** | **local**} {**offline** [*path*] | **online**}
	例：
	`Device# license smart authorization return all online`
	
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	`Return code:`
	`CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h`
	`UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`Return code:`
	`CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA`
	
	`OR`
	
	`Device# license smart authorization return local offline`
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	`Return code:`
	`CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h`
	`UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`Return code:`
	`CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA`
	
	`OR`
	
	`Device# license smart authorization return local offline bootflash:return-code.txt`
		CSSM のライセンスプールに承認コードを返却します。このコマンドを入力すると、戻りコードが表示されます。
		製品インスタンスを指定します。
		• all：高可用性セットアップで接続されたすべての製品インスタンスに対してアクションを実行します。
		• local：アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。
		CSSM に接続しているかどうかを指定します。
		• CSSM に接続している場合は、**online** を入力します。コードは自動的に CSSM に返却され、確認が返されて製品インスタンスにインストールされます。このオプションを選択すると、戻りコードが自動的に CSSM に送信されます。
		• CSSM に接続していない場合は、**offline**[*path*] を入力します。
		offline キーワードのみを入力する場合は、CLI に表示されるリターンコードをコピーして、CSSM に入力する必要があります。
		ファイル名とパスを指定すると、リターンコードは指定した場所に保存されます。ファイル形式は、読み取

	コマンドまたはアクション	目的
		り可能な任意の形式にすることができます。例：`Device# license smart authorization return local offline bootflash:return-code.txt`. ソフトウェアバージョン Cisco IOS XE Cupertino 17.7.1 以降では、返却要求をファイルに保存した後、RUM レポートをアップロードする場合と同じ場所に、同じ方法でファイルを CSSM にアップロードできます。CSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ） CSSM にリターンコードを入力するには、次のタスクを実行します。CSSM からの製品インスタンスの削除（149 ページ）この手順を完了してから、次の手順に進みます。
ステップ 4	**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 5	**no license smart reservation** 例： `Device(config)# no license smart reservation`	製品インスタンスの SLR 設定を無効にします。 この手順で no license smart reservation コマンドを入力する前に、上記の手順 3 で（オンラインまたはオフラインで）承認コードの返却プロセスを完了する必要があります。そうしないと、返却が CSSM または show コマンドに反映されない場合があります。問題を修正するには、シスコのテクニカルサポート担当者に連絡する必要があります。
ステップ 6	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

ステップ 7	**show license all**
	
	例：
	`Device# show license all`
	`<output truncated>`
		ライセンス情報を表示します。出力の `License Authorizations` ヘッダーを確認します。返却プロセスが正常に完了する

	コマンドまたはアクション	目的

	License Authorizations
	=====================
	Overall status:
	  Active:
	PID:C9800-CL-K9,SN:93BBAH93MGS
	  Status: NOT INSTALLED
	  Last return code:
	CCpUPW-WSPYiq-ZNU2ci-SnWyoS-hBCXHP-MuyPqy-PJ1GiG-tPTQQj-S2h
	
	  Standby:
	PID:C9800-CL-K9,SN:9XECPSUU4XN
	  Status: NOT INSTALLED
	  Last return code:
	CNLwxR-eWiAEJ-XsIIEQg-j4nrWW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
	<output truncated>
		と、Last return code: フィールドに戻りコードが表示されます。

CSSM からの製品インスタンスの削除

製品インスタンスを削除し、すべてのライセンスをライセンスプールに戻すには、次のタスクを実行します。

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

予約済みライセンス（SLR）を使用している製品インスタンスを削除する場合は、承認コードの削除と返却（146ページ）に示されているとおり、リターンコードが生成されていることを確認します。（このタスクの手順 7 で入力します）。

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 [Inventory] タブをクリックします。

ステップ 3 [Virtual Account] ドロップダウンリストから、バーチャルアカウントを選択します。

ステップ 4 [Product Instances] タブをクリックします。

使用可能な製品インスタンスのリストが表示されます。

ステップ 5 製品インスタンスリストから必要な製品インスタンスを見つけます。オプションで、検索タブに名前または製品タイプの文字列を入力して、製品インスタンスを検索できます。

ステップ 6 削除する製品インスタンスの [Actions] 列で、[Remove] リンクをクリックします。

- 製品インスタンスが SLR 承認コードを含むライセンスを使用していない場合は、[Confirm Remove Product Instance] ウィンドウが表示されます。

- 製品インスタンスが SLR 承認コードを含むライセンスを使用している場合は、リターンコードを入力するためのフィールドのある [Remove Product Instance] ウィンドウが表示されます。

ステップ 7 [Reservation Return Code] フィールドに、作成したリターンコードを入力します。

（注） この手順は、製品インスタンスが SLR 承認コードを含むライセンスを使用している場合にのみ適用されます。

ステップ 8 [Remove Product Instance] をクリックします。

ライセンスがライセンスプールに返され、製品インスタンスが削除されます。

CSSM からの信頼コード用新規トークンの生成

信頼コードを要求するトークンを生成するには、次の手順を実行します。

所有するバーチャルアカウントごとに 1 つのトークンを生成します。1 つのバーチャルアカウントに属するすべての製品インスタンスに同じトークンを使用できます。

始める前に

サポートされるトポロジ：CSSM に直接接続

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 [Inventory] タブをクリックします。

ステップ 3 [Virtual Account] ドロップダウンリストから、必要なバーチャルアカウントを選択します。

ステップ 4 [General] タブをクリックします。

ステップ 5 [New Token] をクリックします。[Create Registration Token] ウィンドウが表示されます。

ステップ 6 [Description] フィールドに、トークンの説明を入力します。

ステップ 7 [Expire After] フィールドに、トークンをアクティブにする必要がある日数を入力します。

ステップ 8 （オプション）[Max. Number of Uses] フィールドに、トークンの有効期限が切れるまでの最大使用回数を入力します。

ステップ 9 [Create Token] をクリックします。

ステップ 10 リストに新しいトークンが表示されます。[Actions] をクリックし、トークンを `.txt` ファイルとしてダウンロードします。

信頼コードのインストール

信頼コードを手動でインストールするには、次の手順を実行します。

始める前に

サポートされるトポロジ：

- CSSM に直接接続

手順

	コマンドまたはアクション	目的
ステップ 1	CSSM からの信頼コード用新規トークンの生成 （150 ページ）	まだ CSSM から信頼コードファイルを生成してダウンロードしていない場合は、生成とダウンロードを実行します。
ステップ 2	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 3	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] 例： `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	CSSM との信頼できる接続を確立できます。*id_token_value* には、CSSM で生成したトークンを入力します。 次のいずれかのオプションを入力します。 • **local**：高可用性セットアップのアクティブデバイスに対してのみ信頼要求を送信します。これがデフォルトのオプションです。 • **all**：高可用性セットアップのすべてのデバイスに対して信頼要求を送信します。 製品インスタンスに既存の信頼コードがあるにもかかわらず、信頼コード要求を送信するには、**force** キーワードを入力します。 信頼コードは、製品インスタンスの UDI にノードロックされます。UDI がすでに登録されている場合、CSSM は同じ UDI の新規登録を許可しません。**force** キーワードを入力すると、CSSM に送信されるメッセージに強制フラグが設定され、

	コマンドまたはアクション	目的
		すでに存在する場合でも新しい信頼コードが作成されます。

ステップ 4	**show license status**
	例：
	`<output truncated>`
	`Trust Code Installed:`
	`  Active:`
	`PID:C9800-CL-K9,SN:93BBAH93MGS`
	`    INSTALLED on Nov 02 08:59:26 2020`
	`IST`
	`  Standby:`
	`PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`    INSTALLED on Nov 02 09:00:45 2020`
	`IST`
		信頼コードがインストールされている場合は、日時が表示されます。日時はローカルタイムゾーンで表示されます。`Trust Code Installed:` フィールドを参照してください。

CSSM からのポリシーファイルのダウンロード

カスタムポリシーを要求した場合、または製品インスタンスに適用されるデフォルトとは異なるポリシーを適用する場合は、次のタスクを実行します。

始める前に

サポートされるトポロジ：

- CSSM への接続なし、CSLU なし
- CSLU は CSSM から切断

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 次のディレクトリパス、[Reports] > [Reporting Policy] を移動します。

ステップ 3 [Download] をクリックして、`.xml` ポリシーファイルを保存します。

これで、ファイルを製品インスタンスにインストールできます。製品インスタンスへのファイルのインストール （154 ページ） を参照してください

CSSM へのデータまたは要求のアップロードとファイルのダウンロード

このタスクは、次の目的で使用できます。

- RUM レポートを CSSM にアップロードし、ACK をダウンロードします。
- SLAC または SLR 承認コードの返却要求をアップロードします。

  これは、*CSSM* への接続なし、*CSLU* なしのトポロジにのみ適用され、Cisco IOS XE cupertino 17.7.1 以降でサポートされています。

製品インスタンスが CSSM や CSLU に接続されていない場合に RUM レポートを CSSM にアップロードして ACK をダウンロードするには、次のタスクを実行します。

始める前に

サポートされるトポロジ：

- CSSM への接続なし、CSLU なし
- CSLU は CSSM から切断
- SSM オンプレミス展開（製品インスタンス開始型通信と SSM オンプレミス開始型通信）

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインします。

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 レポートを受信する**スマートアカウント**（画面の左上隅）を選択します。

ステップ 3 [Smart Software Licensing] → [Reports] → [Usage Data Files] を選択します。

ステップ 4 [Upload Usage Data] をクリックします。ファイルの場所（tar 形式の RUM レポート）を参照して選択し、[Upload Data] をクリックします。

RUM レポート（`.tar` 形式）、または SLAC 返却要求ファイル（`.txt` 形式）をアップロードします。

使用状況レポートは、アップロード後に CSSM で削除できません。

ステップ 5 [Select Virtual Accounts] ポップアップから、アップロードされたファイルを受信する**バーチャルアカウント**を選択します。ファイルがシスコにアップロードされ、[Reports] 画面の [Usage Data Files] テーブルにファイル名、レポートの時刻、アップロード先のバーチャルアカウント、レポートステータス、レポートされた製品インスタンス数、確認ステータスが表示されます。

ステップ 6 [Acknowledgment] 列で [Download] をクリックして、アップロードしたレポートの `.txt` ACK ファイルを保存します。

[Acknowledgment] 列に「ACK」が表示されるまで待ちます。処理する RUM レポートまたは要求が多数ある場合、CSSM では数分かかることがあります。

実装したトポロジに応じて、ファイルを製品インスタンスにインストールするか、またはCSLUに転送する、あるいは SSM オンプレミスにインポートすることができます。

製品インスタンスへのファイルのインストール

製品インスタンスが CSSM や CSLU に接続されていない場合に、製品インスタンスに SLAC、ポリシー、または ACK をインストールするには、次のタスクを実行します。

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

製品インスタンスにアクセスできる場所に、対応するファイルを保存しておく必要があります。

- ポリシーの場合の参照： CSSM からのポリシーファイルのダウンロード （152 ページ）
- ACK の場合の参照： CSSM へのデータまたは要求のアップロードとファイルのダウンロード （153 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**copy** *source* **bootflash:***file-name* 例： `Device# copy tftp://10.8.0.6/example.txt bootflash:`	ファイルをソースの場所またはディレクトリから製品インスタンスのフラッシュメモリにコピーします。 • *source*：これは、コピー元となるファイルまたはディレクトリの場所です。コピー元は、ローカルまたはリモートのいずれかです。 • **bootflash:**：これはブートフラッシュメモリの場合の宛先です。
ステップ 3	**license smart import bootflash:** *file-name* 例： `Device# license smart import bootflash:example.txt`	ファイルを製品インスタンスにインポートしてインストールします。インストール後、インストールしたファイルのタイ

	コマンドまたはアクション	目的
		プを示すシステムメッセージが表示されます。
ステップ 4	**show license all** 例： `Device# show license all`	製品インスタンスのライセンス承認、ポリシー、およびレポート情報を表示します。

転送タイプ、URL、およびレポート間隔の設定

製品インスタンスの転送モードを設定するには、次のタスクを実行します。

始める前に

サポートされるトポロジ：すべて

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	
ステップ 3	**license smart transport** {**automatic** | **callhome** | **cslu** | **off** | **smart**} 例： `Device(config)# license smart transport cslu`	使用する製品インスタンスの転送モードを設定します。次のオプションから選択します。 • **automatic**：転送モード **cslu** を設定します。 • **callhome**：転送モードとして Call Home を有効にします。 • **cslu**：これがデフォルトのトランスポートモードです。製品インスタンス開始型通信で CSLU または SSM オンプレミスを使用している場合は、このキーワードを入力します。 トランスポート モード キーワードは CSLU と SSM オンプレミスで同じですが、トランスポート URL は

	コマンドまたはアクション	目的
		異なります。次の手順の **license smart url cslu** *cslu_or_on-prem_url* を参照してください。 • **off**：製品インスタンスからのすべての通信を無効にします。 • **smart**：スマート転送を有効にします。

ステップ 4	**license smart url** {*url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *smart_url*}
	例：
	`Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi`
		設定された転送モードの URL を設定します。前のステップで選択した転送モードに応じて、対応する URL をここで設定します。
		• *url*：転送モードとして **callhome** を設定している場合は、このオプションを設定します。CSSM URL を次のように正確に入力します。
		`https://software.cisco.com/#module/SmartLicensing`
		no license smart url*url* コマンドは、デフォルトの URL に戻ります。
		• **cslu** *cslu_or_on-prem_url*：トランスポートモードを **cslu** として設定している場合は、必要に応じてCSLUまたはSSMオンプレミスのURLを使用してこのオプションを設定します。
		• CSLUを使用している場合は、次のようにURLを入力します。
		`http://<cslu_ip_or_host>:8182/cslu/v1/pi`
		`<cslu_ip_or_host>`には、CSLUをインストールしたWindowsホストのホスト名やIPアドレスを入力します。8182はポート番号であり、CSLUが使用する唯一のポート番号です。
		no license smart url cslu *cslu_url* コマンドは `http://cslu-local:8182/cslu/v1/pi` に戻ります

	コマンドまたはアクション	目的
		• SSM オンプレミスを使用している場合は、次のように URL を入力します。 `http://<ip>/cslu/v1/pi/<tenant ID>` <ip> には、SSM オンプレミスをインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID> はデフォルトのローカル バーチャル アカウント ID にする必要があります。 ヒント SSM オンプレミスから URL 全体を取得できます。「トランスポート URL の取得（SSM オンプレミス UI）（129ページ）」を参照してください **no license smart url cslu** *cslu_url* コマンドは `http://cslu-local:8182/cslu/v1/pi` に戻ります • **default**：設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。 転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます（`https://cslu-local:8182/cslu/v1/pi`）。 転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます（`https://smartreceiver.cisco.com/licservice/license`）。 • **smart** *smart_url*：転送タイプとして **smart** を設定している場合は、この

	コマンドまたはアクション	目的
		オプションを設定します。URL を次のように正確に入力します。 https://smartreceiver.cisco.com/licservice/license このオプションを設定すると、システムは **license smart url** *url* で自動的に URL の複製を作成します。重複するエントリは無視できます。これ以上の操作は必要ありません。 **no license smart url smart***smart_url* コマンドは、デフォルトの URL に戻ります。 • **utility** *smart_url*：このオプションは CLI では使用できますがサポートされていません。
ステップ 5	**license smart usage interval** *interval_in_days* 例： `Device(config)# license smart usage interval 40`	（任意）レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ～ 3650 です。 間隔を設定しない場合、レポート間隔はポリシーの値のみで決まります。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル 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 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

AIR ライセンスの設定

ポリシーを使用したスマートライセンシング環境では、このタスクを使用して、ライセンスを変更したり、製品インスタンスで使用されているライセンスを変更したり、製品インスタンスでアドオンライセンスを追加設定したりできます。たとえば、現在 AIR Network Advantage を使用しており、対応する Digital Networking Architecture（DNA）Advantage ライセンスで使用可能な機能も使用する場合は、このタスクを使用して同じ機能を設定できます。また、アドオンライセンスを使用しない場合などは、AIR Network Advantage ライセンスのみを使用するようにこのコマンドを再設定します。

使用可能なライセンスに関する情報は、スマートアカウントまたはバーチャルアカウントで確認できます。使用可能なライセンスは、次のいずれかです。

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

Cisco IOS XE Bengaluru 17.4.1 以降、EWC-AP の場合のみ、AIR DNA ライセンスの購入をオプトアウトできます。AIR DNA ライセンスをオプトアウトするオプションは、Cisco Commerce ポータルからのみ利用できます。オプトアウトすると、ポリシーを使用したスマートライセンシング機能が無効になります。

新しい製品インスタンスの場合、次のことを意味します。

条件	必須のアクション	結果
AIR DNA ライセンスをオプトアウトする	なし。	AIR Network Essentials のみを使用します。 ポリシーを使用したスマートライセンシング機能は、製品インスタンス、および CSSM のスマートアカウントとバーチャルアカウントで無効になっています。ライセンスの使用状況は記録されず、レポート要件も適用されません。
AIR DNA ライセンスを購入する	グローバル コンフィギュレーション モードで license air level コマンドを入力し、対応する AIR DNA ライセンスを設定します。対応するライセンスを使用するには、リロードします。 サポートされているトポロジのいずれかを実装し、レポート要件を満たします。トポロジの実装については、このドキュメントの「サポートされるトポロジ」セクションを参照してください。	購入した AIR DNA および AIR Network ライセンスを使用します。 ポリシーを使用したスマートライセンシング機能は、製品インスタンス、および CSSM のスマートアカウントとバーチャルアカウントで有効になっています。

既存の製品インスタンスの場合、次のことを意味します。

条件	必須のアクション	結果
AIR DNA ライセンスを使用している	なし。	変化なし すでにポリシーを使用したスマートライセンシング環境にいます。
期間満了時に DNA ライセンスを更新したくない	期限満了時に、グローバル コンフィギュレーション モードで **license air level** コマンドを入力し、AIR Network Essentials または AIR Network Advantage を設定します。対応するライセンスを使用するには、リロードします。	AIR DNA Essentials を使用していた場合は、AIR Network Essentials を使用します。 AIR DNA Advantage を使用していた場合は、AIR Network Advantage を使用します。 ポリシーを使用したスマートライセンシング機能は、製品インスタンス、および CSSM のスマートアカウントとバーチャルアカウントで無効になっています。ライセンスの使用状況は記録されず、レポート要件も適用されません。

使用中ライセンスを設定または変更するには、次の手順に従います。

始める前に

サポートされるトポロジ：すべて

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**license air level** {**air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] } 例： `Device(config)# license air level air-network-essentials addon air-dna-essentials`	製品インスタンスで設定されたライセンスをアクティブにします。この例では、製品インスタンスにより、リロード後に AIR DNA Essentials（および AIR Network Essentials）ライセンスがアクティブ化されます。

	コマンドまたはアクション	目的
		（注） Cisco IOS XE Bengaluru 17.4.1 より前では、EWC-AP のデフォルトは AIR DNA Essentials でした。17.4.1 以降のデフォルトは AIR Network Essentials です。
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	設定変更を保存します。
ステップ 6	**reload** 例： `Device# reload`	デバイスがリロードされます。

ステップ 7	**show version**
	例：
	`Device# show version`
	`Cisco IOS XE Software, Version 17.03.02`
	`Cisco IOS Software [Amsterdam],`
	`C9800-CL Software (C9800-CL-K9_IOSXE),`
	`Version 17.3.2, RELEASE SOFTWARE`
	`<output truncated>`
	`AIR License Level: AIR DNA Essentials`
	`Next reload AIR license Level: AIR DNA Essentials`
	
	`Smart Licensing Status: Registration Not Applicable/Not Applicable`
	`<output truncated>`
		現在使用しているライセンスと次回のリロード時に有効なライセンス情報を表示します。

次のタスク

ライセンスレベルを設定すると、変更はリロード後に有効になります。レポートが必要かどうかを確認するには、**show license status** 特権EXECコマンドの出力を参照し、`Next ACK deadline:` フィールドと `Next report push:` フィールドを確認します。

（注） ライセンスの使用状況の変更は、製品インスタンスに記録されます。レポートに関連した次の手順は、必要に応じて実行しますが、現在のトポロジによって異なります。

- CSLU を介して CSSM に接続

- 製品インスタンス開始型通信：製品インスタンスがレポートをトリガーし、返されるACK をインストールします。CSLU は RUM レポートを CSSM に送信し、CSSM からACK を収集します。
- CSLU開始型通信：CSLUインターフェイスから使用状況を収集する必要があります。使用状況レポートの収集：CSLU開始（CSLUインターフェイス）（118ページ）CSLU は RUM レポートを CSSM に送信し、CSSM から ACK を収集します。

- CSSM に直接接続：製品インスタンスがレポートをトリガーし、返される ACK をインストールします。
- CSLU は CSSM から切断：
  - 製品インスタンス開始型通信：製品インスタンスがレポートをトリガーします。次に、切断モードでの使用状況を報告する必要があります。CSSM へのエクスポート（CSLU インターフェイス）（120 ページ）＞CSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ）＞CSSM からのインポート（CSLU インターフェイス）（120 ページ）
  - CSLU 開始型通信：CSLU インターフェイスから使用状況を収集し、非接続モードで使用状況を報告する必要があります。使用状況レポートの収集：CSLU 開始（CSLU インターフェイス）（118 ページ）＞CSSM へのエクスポート（CSLU インターフェイス）（120 ページ）＞CSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ）＞CSSM からのインポート（CSLU インターフェイス）（120 ページ）
- CSSM への接続なし、CSLU なし：ライセンスの使用状況は製品インスタンスに記録されます。RUM レポートを製品インスタンスのファイルに保存し、インターネットとシスコに接続しているワークステーションからCSSMにアップロードする必要があります。**license smart save usage** 特権 EXEC コマンドを入力して使用状況を保存します。＞CSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ）＞製品インスタンスへのファイルのインストール（154 ページ）

リソース使用率測定レポートの例

次に、リソース使用率測定（RUM）レポートの例を XML 形式で示します（RUM レポートおよびレポート確認応答（53 ページ）を参照）。このような複数のレポートを連結して 1 つのレポートを形成できます。

```
<?xml version="1.0" encoding="UTF-8"?>
  <smartLicense>
```

[redacted]

```
  </smartLicense>
```

ポリシーを使用したスマートライセンシングのトラブルシューティング

このセクションでは、発生する可能性のあるポリシーを使用したスマートライセンシングに関連するシステムメッセージ、考えられる失敗の理由、および推奨するアクションを示します。

システム メッセージの概要

システムメッセージは、システムソフトウェアからコンソール（および任意で別のシステムのロギングサーバー）に送信されます。すべてのシステム メッセージがシステムの問題を示すわけではありません。通知目的のメッセージもあれば、通信回線、内蔵ハードウェア、またはシステム ソフトウェアの問題を診断するうえで役立つメッセージもあります。

システム メッセージの読み方

システムログメッセージには最大 80 文字を含めることができます。各システム メッセージはパーセント記号（%）から始まります。構成は次のとおりです。

```
%FACILITY-SEVERITY-MNEMONIC: Message-text
```

%FACILITY

メッセージが参照するファシリティを示す2 文字以上の大文字です。ファシリティは、ハードウェアデバイス、プロトコル、またはシステムソフトウェアのモジュールなどです。

SEVERITY

0 ～ 7 の 1 桁のコードで、状態のシビラティ（重大度）を表します。この値が小さいほど、重大な状況を意味します。

表 *9:* メッセージのシビラティ（重大度）

シビラティ（重大度）	説明
0：緊急	システムが使用不可能な状態。
1：アラート	ただちに対応が必要な状態。
2：クリティカル	危険な状態。
3：エラー	エラー条件。
4：警告	警告条件。
5：通知	正常だが注意を要する状態。
6：情報	情報メッセージのみ。

シビラティ（重大度）	説明
7：デバッグ	デバッグ時に限り表示されるメッセージのみ。

MNEMONIC

メッセージを一意に識別するコード。

Message-text

メッセージテキストは、状態を説明したテキスト文字列です。メッセージのこの部分には、端末ポート番号、ネットワーク アドレス、またはシステム メモリ アドレス空間の位置に対応するアドレスなど、イベントの詳細情報が含まれることがあります。この可変フィールドの情報はメッセージごとに異なるので、ここでは角カッコ（[]）で囲んだ短い文字列で示します。たとえば 10 進数は [dec] で表します。

表 *10*：メッセージの変数フィールド

シビラティ（重大度）	説明
[char]	1 文字
[chars]	文字列
[dec]	10 進数
[enet]	イーサネット アドレス（たとえば 0000.FEED.00C0）
[hex]	16 進数
[inet]	インターネット アドレス（10.0.2.16）
[int]	整数
[node]	アドレス名またはノード名
[t-line]	8 進数のターミナルライン番号（10 進数 TTY サービスが有効な場合は 10 進数）
[clock]	クロック（例：01:20:08 UTC Tue Mar 2 1993）

システム メッセージ

このセクションでは、発生する可能性のあるポリシーを使用したスマートライセンシングに関連するシステムメッセージ、考えられる失敗の理由（失敗メッセージの場合）、および推奨するアクション（アクションが必要な場合）を示します。

すべてのエラーメッセージについて、問題を解決できない場合は、シスコのテクニカルサポート担当者に次の情報をお知らせください。

コンソールまたはシステムログに出力されたとおりのメッセージ。

show license tech support、**show license history message**、および **show platform software sl-infra** 特権 EXEC コマンドの出力。

- %SMART_LIC-3-POLICY_INSTALL_FAILED
- %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED
- %SMART_LIC-3-COMM_FAILED
- %SMART_LIC-3-COMM_RESTORED
- %SMART_LIC-3-POLICY_REMOVED
- %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED
- %SMART_LIC-4-REPORTING_NOT_SUPPORTED
- %SMART_LIC-6-POLICY_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_REMOVED
- %SMART_LIC-6-REPORTING_REQUIRED
- %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS
- %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG
- %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED

```
Error Message %SMART_LIC-3-POLICY_INSTALL_FAILED: The installation of a new
licensing policy has failed: [chars].
```

説明：ポリシーがインストールされましたが、ポリシーコードの解析中にエラーが検出され、インストールに失敗しました。[chars] はエラーの詳細を示すエラー文字列です。

失敗の理由として次が考えられます。

- 署名の不一致：これは、システムクロックが正確でないことを意味します。
- タイムスタンプの不一致：製品インスタンスのシステムクロックが CSSM と同期していないことを意味します。

（注） デバイスには、有効なクロックと NTP 設定が必要です。

推奨するアクション：

考えられる両方の失敗の理由に関しては、システムクロックが正確で、CSSM と同期していることを確認します。**ntp server** コマンドをグローバル コンフィギュレーション モードで設定します。次に例を示します。

```
Device(config)# ntp server 198.51.100.100 version 2 prefer
```

前述の手順を実行しても、ポリシーのインストールが失敗する場合は、シスコのテクニカルサポート担当者にお問い合わせください。

```
Error Message %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED: The install of a new
licensing authorization code has failed on [chars]: [chars].
```

このメッセージは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチには該当しません。これらの製品インスタンスには輸出規制ライセンスや適用ライセンスがないためです。

```
Error Message %SMART_LIC-3-COMM_FAILED: Communications failure with the [chars] :
[chars]
```

説明：CSSM、CSLU、または SSM オンプレミスのいずれかとのスマートライセンシング通信が失敗しました。最初の [chars] は現在設定されている転送タイプで、2 番めの [chars] はエラーの詳細を示すエラー文字列です。このメッセージは、失敗した通信の試行ごとに表示されます。

失敗の理由として次が考えられます。

- CSSM、CSLU、または SSM オンプレミスに到達できない：これは、ネットワーク到達可能性に問題があることを意味します。
- 404 ホストが見つからない：これは CSSM サーバがダウンしていることを意味します。

正インスタンスが RUM レポートの送信を開始するトポロジ（CSLU を介して CSSM に接続：製品インスタンス開始型通信、CSSM から切断されているCSSM、CSLU への直接接続：製品スタンス開始型通信、および SSM オンプレミス展開：製品インスタンス開始型通信）では、この通信障害メッセージがスケジュールされたレポート（**license smart usage interval** *interval_in_days* グローバル コンフィギュレーション コマンド）と一致している場合は、製品インスタンスはスケジュールされた時間が経過した後、最大 4 時間にわたって RUM レポートを送信しようとします。（通信障害が続くために）それでもレポートを送信できない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔は最後に設定された値に戻ります。

推奨するアクション：

CSSM に到達できない場合、および CSLU に到達できない場合のトラブルシューティング手順を説明します。

CSSM が到達不能で、設定されている転送タイプが smart の場合：

1. スマート URL が正しく設定されているかどうかを確認します。特権 EXEC モードで **show license status** コマンドを使用して、URL が次のようになっているかどうかを確認します。https://smartreceiver.cisco.com/licservice/licenseそうでない場合は、グローバル コンフィギュレーション モードで **license smart url smart** *smar_URL* コマンドを再設定します。

2. DNS 解決を確認します。製品インスタンスが `smartreceiver.cisco.com` または nslookup で変換された IP に対して ping を実行できることを確認します。次の例は、変換された IP に対して ping を実行する方法を示しています。

```
Device# ping 171.70.168.183
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 171.70.168.183, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

CSSM が到達不能で、設定されている転送タイプが callhome の場合：

1. URL が正しく入力されているかどうかを確認します。特権 EXEC モードで **show license status** コマンドを使用して、URL が次のようになっているかどうかを確認します。https://tools.cisco.com/its/service/oddce/services/DDCEService

2. Call Home プロファイル `CiscoTAC-1` がアクティブで、接続先 URL が正しいことを確認します。**show call-home profile all** コマンドは特権 EXEC モードで使用してください。

```
Current smart-licensing transport settings:
 Smart-license messages: enabled
 Profile: CiscoTAC-1 (status: ACTIVE)
 Destination  URL(s):  https://tools.cisco.com/its/service/oddce/services/DDCEService
```

3. DNS 解決を確認します。製品インスタンスが `tools.cisco.com` または nslookup で変換された IP に対して ping を実行できることを確認します。

```
Device# ping tools.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
```

上記の方法で解決しない場合は、製品インスタンスが設定されているかどうか、製品インスタンスの IP ネットワークが稼働しているかどうかを確認します。ネットワークが稼働していることを確認するには、インターフェイス コンフィギュレーション モードで **no shutdown** コマンドを設定します。

デバイスがサブネット IP でサブネットマスクされているかどうか、および DNS IP が設定されているかどうかを確認します。

4. HTTPS クライアントの送信元インターフェイスが正しいことを確認します。

現在の設定を表示するには、特権 EXEC モードで **show ip http client** コマンドを使用します。グローバル コンフィギュレーション モードで **ip http client source-interface** コマンドを使用して、再設定します。

上記の方法で解決しない場合は、ルーティングルール、およびファイアウォール設定を再確認します。

CSLU に到達できない場合：

1. CSLU 検出が機能するかどうかを確認します。

   - `cslu-local` のゼロタッチ DNS 検出またはドメインの DNS 検出。

show license all コマンドの出力で、`Last ACK received:` フィールドを確認します。このフィールドに最新のタイムスタンプがある場合は、製品インスタンスが CSLU と接続されていることを意味します。ない場合は、次のチェックに進みます。

製品インスタンスが `cslu-local` に対して ping を実行できるかどうかを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます。

上記の方法で解決しない場合は、ホスト名 `cslu-local` が CSLU の IP アドレス（CSLU をインストールした Windows ホスト）にマッピングされているエントリを使用してネームサーバを設定します。グローバル コンフィギュレーション モードで **ip domain name** *domain-name* コマンドと **ip name-server** *server-address* コマンドを設定します。この例では、CSLU IP は 192.168.0.1 で、name-server によってエントリ `cslu-local.example.com` が作成されます。

```
Device(config)# ip domain name example.com
Device(config)# ip name-server 192.168.0.1
```

- CSLU URL が設定されています。

  show license all コマンド出力の `Transport:` ヘッダーで、次の点を確認します。 `Type:` は `cslu` で、`Cslu address:` は CSLU をインストールした Windows ホストのホスト名または IP アドレスになっている必要があります。残りのアドレスが下記のように設定されているかどうかを確認するとともに、ポート番号が 8182 であるかどうかを確認します。

  ```
  Transport:
    Type: cslu
    Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  ```

  そうでない場合は、グローバル コンフィギュレーション モードで **license smart transport cslu** および **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* コマンドを設定します。

2. CSLU 開始型通信の場合、上記の CSLU 検出チェックに加えて、次の点を確認します。

   HTTP 接続を確認します。特権 EXEC モードで **show ip http server session-module** コマンドを使用します。出力の `HTTP server current connections:` ヘッダーで、`SL_HTTP` がアクティブになっていることを確認します。CSLU 開始型通信のネットワーク到達可能性の確認（121 ページ） で説明されているとおりに **ip http** が再設定されていない場合：

   CSLU がインストールされているデバイスの Web ブラウザで、`https://<product-instance-ip>/` を確認します。これにより、CSLU から製品インスタンスへの REST API が期待どおりに動作することが保証されます。

SSM オンプレミスに到達できない場合：

1. 製品インスタンス開始型通信の場合は、SSM オンプレミスのトランスポートタイプと URL が正しく設定されているかどうかを確認します。

   show license all コマンドの出力の `Transport:` ヘッダーの下で、`Type:` が `cslu` であり、`Cslu address:` には、SSM オンプレミスにインストールしたサーバのホスト名または IP アドレスと、デフォルトのローカル バーチャル アカウントの <tenantID> があることを確認します。次の例を参照してください。

```
Transport:
  Type: cslu
  Cslu address: https://192.168.0.1/cslu/v1/pi/on-prem-default
```

SSM オンプレミスの正しい URL があることを確認し（トランスポート URL の取得（SSM オンプレミス UI）（129 ページ））、グローバル コンフィギュレーション モードで **license smart transport cslu** コマンドと **license smart url cslu** *http://<ip>/cslu/v1/pi/<tenant ID>* コマンドを設定します。

製品インスタンス開始型通信のネットワーク到達可能性の確認（127 ページ）で説明されているよおりに、ネットワークに必要な他のコマンドが設定されていることを確認します。

2. SSM オンプレミス開始型通信の場合は、HTTPS 接続を確認します。

   特権 EXEC モードで **show ip http server session-module** コマンドを使用します。出力の `HTTP server current connections:` ヘッダーで、`SL_HTTP` がアクティブになっていることを確認します。SSM オンプレミス開始型通信のネットワーク到達可能性の確保（132 ページ）で説明されているとおりに **ip http** コマンドが再設定されていない場合は、次の手順を実行します。

3. トラストポイントと証明書が受け入れられることを確認します。

   SSM オンプレミス展開の両方の通信形式で、正しいトラストポイントが使用され、必要な証明書が受け入れられることを確認します。

```
Device(config)# crypto pki trustpoint SLA-TrustPoint
Device(ca-trustpoint)#
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device# copy running-config startup-config
```

前述の手順を実行しても、ポリシーのインストールが失敗する場合は、シスコのテクニカルサポート担当者にお問い合わせください。

```
Error Message  %SMART_LIC-3-COMM_RESTORED: Communications with the [chars] restored.
[chars] - depends on the transport type
        - Cisco Smart Software Manager (CSSM)
        - Cisco Smart License utility (CSLU)
Smart Agent communication with either the Cisco Smart Software Manager (CSSM) or the
Cisco Smart License
utility (CSLU) has been restored. No action required.
```

説明：CSSM、CSLU、または SSM オンプレミスのいずれかとの製品インスタンス通信が復元されます。

推奨するアクション：アクションは必要ありません。

`Error Message %SMART_LIC-3-POLICY_REMOVED: The licensing policy has been removed.`

説明：以前にインストールしたカスタムライセンスポリシーが削除されました。`Cisco default` ポリシーが自動的に有効になります。これにより、スマートライセンシングの動作が変更される可能性があります。

失敗の理由として次が考えられます。

特権 EXEC モードで **license smart factory reset** コマンドを入力すると、ポリシーを含むすべてのライセンス情報が削除されます。

推奨するアクション：

ポリシーが意図的に削除された場合、それ以上のアクションは不要です。

ポリシーが誤って削除された場合は、ポリシーを再適用できます。実装したトポロジに応じて、該当するメソッドに従ってポリシーを取得します。

- CSSM に直接接続：

  show license status を入力し、`Trust Code Installed:` フィールドを確認します。信頼が確立されると、CSSMは再度ポリシーを自動的に返します。ポリシーは、対応するバーチャルアカウントのすべての製品インスタンスに自動的に再インストールされます。

  信頼が確立されていない場合は、次のタスクを実行します。CSSMからの信頼コード用新規トークンの生成（150ページ）および信頼コードのインストール（151ページ）これらのタスクを完了すると、CSSMは再度ポリシーを自動的に返します。その後、バーチャルアカウントのすべての製品インスタンスにポリシーが自動的にインストールされます。

- CSLU を介して CSSM に接続：

  - 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。同期要求により、CSLU は欠落している情報（ポリシーまたは承認コード）を製品インスタンスにプッシュします。
  - CSLU 開始型通信の場合は、次のタスクを実行します。使用状況レポートの収集：CSLU開始（CSLUインターフェイス）（118ページ）タスクを実行すると、CSLUはACK 応答で欠落しているポリシーを検出して再提供します。

- CSLU は CSSM から切断：

  - 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。同期要求により、CSLU は欠落している情報（ポリシーまたは承認コード）を製品インスタンスにプッシュします。次に、次のタスクを指定された順序で実行します。CSSMへのエクスポート（CSLUインターフェイス）（120ページ）>CSSM へのデータまたは要求のアップロードとファイルのダウンロード（153 ページ）>CSSM からのインポート（CSLU インターフェイス）（120 ページ）
  - CSLU 開始型通信の場合は、次のタスクを実行します。使用状況レポートの収集：CSLU開始（CSLUインターフェイス）（118ページ）タスクを実行すると、CSLUはACK 応答で欠落しているポリシーを検出して再提供します。次に、次のタスクを指定された順序で実行します。CSSM へのエクスポート（CSLU インターフェイス）（120ページ）>CSSMへのデータまたは要求のアップロードとファイルのダウンロー

ド （153 ページ） > CSSM からのインポート（CSLU インターフェイス） （120 ページ）

- CSSM への接続なし、CSLU なし

  完全に外部との接続性がないネットワークにいる場合は、インターネットと CSSM に接続できるワークステーションから次のタスクを実行します。CSSM からのポリシーファイルのダウンロード （152 ページ）

  次に、製品インスタンスで次のタスクを実行します。製品インスタンスへのファイルのインストール （154 ページ）

- SSM オンプレミス展開

  - 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。製品インスタンスを SSM オンプレミスと同期させ、必要な情報または欠落している情報を復元する原因です。必要に応じて、SSM オンプレミスと CSSM を同期します。
  - SSM オンプレミス開始型通信の場合：SSM オンプレミス UI で、[Reports] > [Synchronization pull schedule] > [Synchronize now with the device] に移動します。

  SSM オンプレミス展開の両方の通信形式で、次のいずれかのオプションを使用して CSSM と同期します。

  - SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。
  - SSM オンプレミスが CSSM に接続されていません。使用状況データのエクスポートとインポート（SSM オンプレミス UI） （130 ページ）

```
Error Message %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED: The install of a new licensing
trust code has failed on [chars]: [chars].
```

説明：信頼コードのインストールに失敗しました。最初の [chars] は、信頼コードのインストールが試行された UDI です。2 番目の [chars] は、エラーの詳細を示すエラー文字列です。

失敗の理由として次が考えられます。

- 信頼コードがすでにインストールされています。信頼コードは製品インスタンスの UDI にノードロックされています。UDI がすでに登録されている場合に別の UDI をインストールしようとすると、インストールは失敗します。
- スマートアカウントとバーチャルアカウントの不一致：これは、（トークン ID が生成された）スマートアカウントまたはバーチャルアカウントに、信頼コードをインストールした製品インスタンスが含まれていないことを意味します。CSSM で生成されたトークン

は、スマートアカウントまたはバーチャルアカウントレベルで適用され、そのアカウントのすべての製品インスタンスにのみ適用されます。

- 署名の不一致：これは、システムクロックが正確でないことを意味します。
- タイムスタンプの不一致：製品インスタンスの時刻がCSSMと同期していないため、インストールが失敗する可能性があります。

推奨するアクション：

- 信頼コードはすでにインストールされています。製品インスタンスに信頼コードがすでに存在する状況で信頼コードをインストールする場合は、特権EXECモードで **license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] コマンドを再設定します。再設定の際、**force** キーワードを必ず含めてください。**force** キーワードを入力すると、CSSMに送信されるメッセージに強制フラグが設定され、すでに存在する場合でも新しい信頼コードが作成されます。
- スマートアカウントとバーチャルアカウントの不一致：

  https://software.cisco.com でCSSM Web UIにログインし、[Smart Software Licensing] > [Inventory] > [Product Instances] をクリックします。

  トークンを生成する製品インスタンスが、選択したバーチャルアカウントにリストされているかどうかを確認します。リストされている場合は、次のステップに進みます。リストされていない場合は、正しいスマートアカウントとバーチャルアカウントを確認して選択します。その後、次のタスクを再度実行します。CSSMからの信頼コード用新規トークンの生成 （150 ページ） および 信頼コードのインストール （151 ページ）
- タイムスタンプの不一致と署名の不一致：グローバル コンフィギュレーション モードで **ntp server** コマンドを設定します。次に例を示します。

  ```
  Device(config)# ntp server 198.51.100.100 version 2 prefer
  ```

```
Error Message    %SMART_LIC-4-REPORTING_NOT_SUPPORTED: The CSSM OnPrem that this
product instance is connected to is down rev and does not support the enhanced policy
and usage
reporting mode.
```

説明：Cisco Smart Software Managerオンプレミス（旧称Cisco Smart Software Managerサテライト）は、Cisco IOS XE Amsterdam 17.3.3以降でのみSmart Licensing Using Policy環境でサポートされています（SSM オンプレミス （48 ページ）を参照）。サポートされていないリリースでは、製品インスタンスは次のように動作します。

- 登録の更新と承認の更新の送信を停止します。
- 使用状況の記録を開始し、RUMレポートをローカルに保存します。

推奨するアクション：

次の選択肢があります。

- 代わりに、サポートされているトポロジを参照し、いずれかを実装します。サポートされるトポロジ （55 ページ）を参照してください。
- Smart Licensing Using Policy で SSM オンプレミスがサポートされているリリースにアップグレードします。Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行 （112 ページ）を参照してください。

```
Error Message %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed.
```

説明：次のいずれかの方法でポリシーがインストールされました。

- Cisco IOS コマンドの使用
- CSLU 開始型通信
- ACK 応答の一部として

推奨するアクション：アクションは必要ありません。適用されているポリシー（使用中のポリシー）とそのレポート要件を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。

```
Error Message %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was successfully installed on: [chars].
```

このメッセージは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチには該当しません。これらの製品インスタンスには輸出規制ライセンスや適用ライセンスがないためです。

```
Error Message %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has
 been removed from [chars]
```

説明：[chars] は、承認コードがインストールされた UDI です。承認コードが削除されました。これにより、製品インスタンスからライセンスが削除され、スマートライセンシングとライセンスを使用する機能の動作が変更される可能性があります。

推奨するアクション：アクションは必要ありません。ライセンスの現在の状態を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。

```
Error Message %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in [dec] days.
```

説明：これは、シスコへの RUM レポートが必要であることを意味するアラートです。[dec] は、このレポート要件を満たすために残された時間（日数）です。

推奨するアクション：要求された時間内に RUM レポートが送信されるようにします。実装したトポロジによって、レポート方式が決まります。

- CSLU を介して CSSM に接続
  - 製品インスタンス開始型通信の場合：特権 EXEC モードで **license smart sync** コマンドを入力します。CSLU が現在 CSSM にログインしている場合、CSSM 内の関連付けられているスマートアカウントとバーチャルアカウントに自動的に送信されます。
  - CSLU 開始型通信の場合は、次のタスクを実行します。使用状況レポートの収集：CSLU 開始（CSLU インターフェイス） （118 ページ）
- CSSM への直接接続：特権 EXEC モードで **license smart sync** コマンドを入力します。
- コントローラを介して CSSM に接続：製品インスタンスがコントローラによって管理されている場合、コントローラはスケジュールされた時間に RUM レポートを送信します。

  Cisco DNA Center をコントローラとして使用している場合は、アドホックレポートのオプションがあります。必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center Administrator Guide』[英語] で「Manage Licenses」の「Upload Resource Utilization Details to CSSM」を参照してください。
- CSSM からの CSLU の切断：製品スタンスが CSLU に接続されている場合は、上記の「CSLU を介した CSSM への接続」に示したように製品インスタンスと同期してから、タスクCSSM へのエクスポート（CSLU インターフェイス） （120 ページ）、CSSM へのデータまたは要求のアップロードとファイルのダウンロード （153 ページ）、CSSM からのインポート（CSLU インターフェイス） （120 ページ）を実行します。
- CSSM への接続なしで CSLU なし：特権 EXEC モードで **license smart save usage** コマンドを入力し、使用状況の必要な情報をファイルに保存します。次に、CSSM に接続しているワークステーションから、次のタスクを実行します。CSSM へのデータまたは要求のアップロードとファイルのダウンロード （153 ページ）＞製品インスタンスへのファイルのインストール （154 ページ）
- SSM オンプレミス展開：

  製品インスタンスを SSM オンプレミスと同期します。
  - 製品インスタンス開始型通信の場合：特権 EXEC モードで **license smart sync** コマンドを入力します。CSLU が現在 CSSM にログインしている場合、CSSM 内の関連付けられているスマートアカウントとバーチャルアカウントに自動的に送信されます。
  - SSM オンプレミス開始型通信の場合は、次の手順を実行します。SSM オンプレミス UI で、[Reports] > [Synchronization pull schedule] > [Synchronize now with the device] に移動します。

使用状況情報を CSSM と同期します（いずれかを選択）。

- SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。
- SSM オンプレミスが CSSM に接続されていません。使用状況データのエクスポートとインポート（SSM オンプレミス UI） （130 ページ）

```
Error Message %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS: A new licensing trust code
 was successfully installed on [chars].
```

説明：[chars] は、信頼コードが正常にインストールされた UDI です。

推奨するアクション：アクションは必要ありません。信頼コードがインストールされていることを確認するには、特権 EXEC モードで **show license status** コマンドを入力します。出力のヘッダー `Trust Code Installed:` で更新されたタイムスタンプを探します。

```
Error Message %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG: Unregistered 9800-CL can only
be used in lab. For production usage, please register this device in [int] days. Failure
 to do so
will result in a limited number [50] of Access Points being allowed post this.
```

説明：この製品インスタンスには ACK が必要です。[int] は、製品インスタンスに ACK をインストールするための残り時間です。

このシステムメッセージは、製品インスタンスで最初の ACK が使用可能になるまで、1 日 1 回表示されます。

推奨するアクション：

サポートされているトポロジの 1 つを実装し、完全な使用状況レポートを作成します。RUM レポートを CSSM と ACK のインストールに送信するために使用できる方法は、実装するトポロジによって異なります。サポートされるトポロジ （55 ページ）およびポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （75 ページ）を参照してください。

```
Error Message %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED: Chassis 1 R0/0:
wncmgrd: Ap MAC: [enet] is not allowed to join. Please start reporting licensing to Cisco
 to get the
 ACK for resumption of usual operation.
```

説明：この製品インスタンスの ACK の期限は過ぎましたが、ACK はまだインストールされていません。[enet] は、Cisco Catalyst 9800-CL ワイヤレスコントローラに接続しようとしている AP の MAC アドレスですが、必要な ACK がインストールされていないため許可されません。

推奨するアクション：

サポートされているトポロジの 1 つを実装し、完全な使用状況レポートを作成します。RUM レポートを CSSM と ACK のインストールに送信するために使用できる方法は、実装するトポロジによって異なります。サポートされるトポロジ （55 ページ）およびポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （75 ページ）を参照してください。

ポリシーを使用したスマートライセンシングのその他の参考資料

トピック	マニュアル タイトル
この章で使用するコマンドの構文および使用方法の詳細については、対応するリリースのコマンドリファレンスを参照してください。	Cisco Catalyst 9800 Series Wireless Controller Command Reference
Cisco Smart Software Manager のヘルプ	Smart Software Manager Help
Cisco Smart License Utility（CSLU）のインストールおよびユーザガイド	Cisco Smart License Utility Quick Start Setup Guide Cisco Smart License Utility User Guide

ポリシーを使用したスマートライセンシングの機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

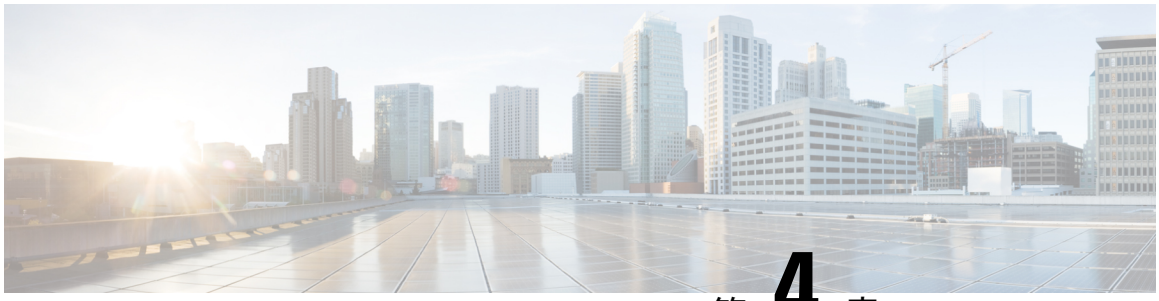
リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.10.1	スマートライセンス	クラウドベースのソフトウェアライセンス管理ソリューションであり、ライセンス、ハードウェア、およびソフトウェアの使用状況の傾向を管理および追跡できます。
Cisco IOS XE Amsterdam 17.3.2a	ポリシーを使用したスマートライセンス	スマートライセンシングの拡張バージョンには、ネットワークの運用を中断させないライセンスソリューションを提供するという主目的がありますが、むしろ、購入および使用しているハードウェアおよびソフトウェアライセンスを考慮して、コンプライアンス関係を実現するライセンスソリューションを提供するという目的もあります。 このリリース以降、ポリシーを使用したスマートライセンスがデバイスで自動的に有効になります。これは、このリリースにアップグレードする場合にも当てはまります。 デフォルトでは、CSSM のスマートアカウントとバーチャルアカウントは、ポリシーを使用したスマートライセンスで有効になっています。
	Smart Licensing Using Policy への Cisco DNA Center のサポート	Cisco DNA Center は、Cisco DNA Center リリース 2.2.2 以降、Smart Licensing Using Policy 機能をサポートしています。Cisco DNA Center を使用して製品インスタンスを管理する場合、Cisco DNA Center は CSSM に接続し、CSSM とのすべての通信のインターフェイスとなります。 互換性のあるコントローラと製品インスタンスバージョンについては、コントローラ （47 ページ）を参照してください。 このトポロジについては、コントローラを介して CSSM に接続 （61 ページ）とトポロジのワークフロー：コントローラを介して CSSM に接続 （83 ページ）を参照してください。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.3.3	Smart Licensing Using Policy 用の Smart Software Manager オンプレミス（SSMオンプレミス）サポート	SSMオンプレミスは、CSSMと連動するアセットマネージャです。これにより、CSSMに直接接続する代わりに、オンプレミスで製品とライセンスを管理できます。 互換性のあるSSMオンプレミスと製品インスタンスバージョンについては、SSM オンプレミス （48 ページ）を参照してください。 このトポロジの概要と実装方法については、SSM オンプレミス展開 （64 ページ）とトポロジのワークフロー：SSM オンプレミス展開（85 ページ）を参照してください。 既存のバージョンの SSMオンプレミスから、Smart Licensing Using Policy への移行をサポートするバージョンへの移行については、Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行 （112 ページ）を参照してください。
Cisco IOS XE Bengaluru 17.4.1	AIR DNA ライセンスをオプトアウトし、EWC-APのデフォルトのライセンスレベルを変更するオプション。	AIR DNA ライセンスの購入をオプトアウトするオプションが導入されました。このオプションは、Cisco Commerce ポータルからのみ利用できます。オプトアウトすると、AIR Network Essentialsライセンスのみが使用され、ポリシーを使用したスマートライセンシング機能が製品インスタンスで無効になります。詳細については、本ガイドの「AIRライセンスの設定」の項を参照してください。 このリリース以降、EWC-AP のデフォルトライセンスも AIR Network Essentials に変更されました。

リリース	機能	機能情報
Cisco IOS XE Cupertino 17.7.1	Cisco Catalyst 9800-CL ワイヤレスコントローラの RUM レポートと確認応答の要件	Cisco Catalyst 9800-CL ワイヤレスコントローラを使用している場合は、RUM レポートを完了し、製品インスタンスで確認応答（ACK）が少なくとも 1 回利用できるようにする必要があります。これは、正しい最新の使用状況情報が CSSM に反映されるようにするためです。
	工場でインストールされた信頼コード	新しいハードウェアの注文では、信頼コードは製造時にインストールされるようになりました。注：出荷時にインストールされた信頼コードを使用して CSSM と通信することはできません。 概要 （44 ページ）および信頼コード （54 ページ）を参照してください。
	追加のトポロジでの信頼コードのサポート	信頼コードは、製品インスタンスが *CSLU* へのデータ送信を開始するトポロジと、製品インスタンスがエアギャップネットワーク内にあるトポロジで自動的に取得されます。 次を参照してください。 • 信頼コード （54 ページ） • CSLU を介して CSSM に接続 （55 ページ）、製品インスタンス開始型通信の場合のタスク （75 ページ）を次に示します。 • CSLU は CSSM から切断 （59 ページ）、製品インスタンス開始型通信の場合のタスク （80 ページ）を次に示します。 • CSSM への接続なし、CSLU なし （62 ページ）、トポロジのワークフロー：CSSM への接続なし、CSLU なし （84 ページ）を次に示します。
	RUM レポートの最適化と統計情報の可用性	

リリース	機能	機能情報
		RUM レポートの生成と関連プロセスが最適化されました。これには、RUM レポートの処理にかかる時間の短縮、メモリとディスク領域の使用率の向上、および製品インスタンス上の RUM レポートの可視性（エラーがある場合、エラーの数、各プロセスの処理状態など）が含まれます。 RUM レポートおよびレポート確認応答 （53 ページ）を参照してください。 該当するリリースのコマンドリファレンスにある **show license rum**、**show license all**、および **show license tech** コマンドも参照してください。
	RUM レポートでソフトウェアバージョンを収集するためのサポート	バージョンプライバシーが無効になっている場合（**no license smart privacy version** グローバル コンフィギュレーション コマンド）、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンと Smart Agent バージョン情報が RUM レポートに含まれます。 該当するリリースのコマンドリファレンスで **license smart** グローバル コンフィギュレーション コマンドを参照してください。
	ACK および show コマンドの出力に含まれるアカウント情報	RUM 確認応答（ACK）には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれます。次に、さまざまな show コマンドを使用してアカウント情報を表示できます。このアカウント情報は、製品インスタンスで使用可能な最新の ACK に基づいて常に表示されます。 該当するリリースのコマンドリファレンスにある **show license all**、**show license summary**、**show license status**、および **show license tech** コマンドを参照してください。
	Linux の CSLU サポート	

リリース	機能	機能情報
		Linux を実行しているマシン（ラップトップまたはデスクトップ）に CSLU を導入できるようになりました。 CSLU （46 ページ）、トポロジのワークフロー：CSLU を介して CSSM に接続 （75 ページ）、およびCSLU は CSSM から切断 （59 ページ）を参照してください。



第 4 章

変換と移行

組み込みワイヤレスコントローラ 対応 AP での変換と移行

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ は、非 802.11ax（非 11ax）ベースのアクセスポイント（AP）ではサポートされていません。802.11ax（11ax）ベースの AP でのみサポートされています。組み込みワイヤレスコントローラ は、11ax ベースの AP でサポートされている Cisco Mobility Express の唯一の形式です。

この変換により、CAPWAP を実行している 11ax AP を 組み込みワイヤレスコントローラ に、またはその逆に変換できます。

変換のタイプ

サポートされている変換シナリオのタイプは次のとおりです。

- AP 変換：次の AP 変換がサポートされています。
  - CAPWAP AP から 組み込みワイヤレスコントローラ への変換：この変換は、CAPWAP イメージがある AP があり、その AP を 組み込みワイヤレスコントローラ ベースのネットワークに展開する場合に必要です。この変換を実行するには、CAPWAP AP を組み込みワイヤレスコントローラに変換する必要があります。

- 組み込みワイヤレスコントローラ AP から CAPWAP AP への変換：この変換は、AP を組み込みワイヤレスコントローラ ネットワークから非組み込みワイヤレスコントローラ ネットワークに移行する場合、または AP をプライマリ AP 選択プロセスに参加させたくない場合に必要です。

- ネットワーク変換
- SKU の変換

（注） EWC 非対応 AP（たとえば、Cisco Aironet 1830 シリーズ アクセスポイント）の EWC モードへの変換要求は、検証されて拒否されました（AP を変換できないため）。

アクセスポイントの変換

ここでは、CAPWAP アクセスポイントから組み込みワイヤレスコントローラへの変換の詳細について説明します。

CAPWAP AP から 組み込みワイヤレスコントローラ 対応 AP への変換

（注） CAPWAP から組み込みワイヤレスコントローラ（EWC）に変換する前に、対応する AP を Cisco AireOS リリース 8.10.105.0 の CAPWAP イメージでアップグレードしてください。このアップグレードを実行しないと、変換は失敗します。

CAPWAP イメージを持つ 802.11ax AP を 組み込みワイヤレスコントローラ 対応イメージに変換するには、自動のイメージのダウンロードプロセスに基づいてコントローライメージをダウンロードするか、変換コマンドを使用するか、WebUI を介して変換します。

（注） AP が 組み込みワイヤレスコントローラ 対応の場合、その AP はプライマリ AP 選択プロセスに参加できます。AP はプライマリとして選択された場合のみ、コントローラの機能を実行できます。

組み込みワイヤレスコントローラ 対応 AP から CAPWAP AP への変換

802.11ax AP を組み込みワイヤレスコントローラ ネットワークから非組み込みワイヤレスコントローラ ネットワークに変換するには、変換コマンドまたは WebUI をそれぞれ使用して AP タイプを CAPWAP に設定し、コントローラネットワークに接続してコントローラに接続され

るようにします。そのコントローラのイメージが AP のイメージと異なる場合は、新しい CAPWAP イメージがコントローラから要求されます。

単一 AP から CAPWAP または組み込みワイヤレスコントローラ対応 AP への変換（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `>enable`	特権 EXEC モードを開始します。
ステップ 2	**wireless ewc ap ap-type***ap-name* {**capwap** | **ewc**} 例： `Device#wireless ewc-ap ap ap-type ap-name capwap`	AP を CAPWAP タイプまたは組み込みコントローラタイプに変更します。

例

```
wireless ewc-ap ap ap-type ap-name {capwap | ewc}
```

AP 変換の展開シナリオ

1. 組み込みワイヤレス コントローラ ネットワークを開始するスタンドアロン 802.11ax CAPWAP AP：

802.11ax AP	組み込みワイヤレスコントローラ対応 AP	ユースケース	自動変換
スタンドアロン 802.11ax CAPWAP AP	ネットワークが存在しません。	組み込みワイヤレスコントローラ ネットワークを設定するための最初の AP としてスタンドアロン 802.11ax CAPWAP AP を使用する場合。	自動変換はできません。 AP コマンドでサポートされている画像転送プロトコルを使用して、コントローラと AP の両方のイメージをダウンロードする必要があります。 `ap-type {capwap | ewc-ap} [<sftp/tftp>://<server ip>/<AP imagepath> <sftp/tftp>://<server ip> Controller ImagePath>]`

2. 既存の 組み込みワイヤレスコントローラ ネットワークに接続する非 802.11ax CAPWAP AP：

CAPWAP AP	組み込みワイヤレスコントローラ対応 AP	ユースケース	自動変換
CAPWAP AP：AireOS Mobility Express 対応、組み込みワイヤレスコントローラ 対応 AP、または AireOS Mobility Express 対応 Wave 2 AP のいずれでもありません。	既存のネットワーク	組み込みワイヤレスコントローラ 対応ではない CAPWAP AP を既存の 組み込みワイヤレスコントローラ ネットワークに導入し、既存のネットワークに AP を 1 つ追加する場合。	対応。自動変換可能です。 変換は、AP 接続イメージのダウンロードプロセスによって自動的に行われます。

3. 既存の 組み込みワイヤレスコントローラ ネットワークに接続する 802.11ax AP：

組み込みワイヤレスコントローラ対応 AP	組み込みワイヤレスコントローラ Network	ユースケース	自動変換

802.11ax AireOS CAPWAP AP または 802.11ax Catalyst CAPWAP AP または 802.11ax 対応 AP組み込みワイヤレスコントローラ	既存のネットワーク	AireOS CAPWAP ネットワークまたは CAPWAP ネットワークから、あるいは別の 組み込みワイヤレスコントローラ ネットワークから既存の組み込みワイヤレスコントローラ ネットワークに 802.11ax AP を導入し、既存のネットワークに AP を 1 つ追加する場合。	対応。自動変換が行われます。
			変換は、AP 接続イメージのダウンロードプロセスによって自動的に行われます。
			AP タイプが明示的に CAPWAP に設定されている場合、AP コマンド、コントローラコマンド、または WebUI を使用して組み込みワイヤレスコントローラ AP に再度変換されない限り、AP は引き続き CAPWAP AP として機能します。
			次のコマンドは、変換、および AP イメージのダウンロードに使用されます。
			`ap-type {capwap | ewc-ap} [<sftp/tftp>://<server ip>/<AP imagepath> <sftp/tftp>://<server ip>Controller ImagePath>]`
			特定の AP を CAPWAP または組み込みワイヤレスコントローラに変換するには、次のコマンドを使用します。
			`wireless ewc-ap ap ap-type` *`ap-name`* `{capwap | ewc-ap}`

4. AireOS CAPWAP ネットワークまたは CAPWAP ネットワークに接続する 802.11ax 組み込みワイヤレスコントローラ AP：

802.11 AX 組み込みワイヤレスコントローラ対応 AP	組み込みワイヤレスコントローラ Network	ユースケース	自動変換

以前は組み込みワイヤレスコントローラ AP だった 802.11ax AP	既存のネットワーク	既存の 802.11ax 組み込みワイヤレスコントローラ AP を導入し、CAPWAP ネットワークまたは AireOS CAPWAP ネットワークに追加して、既存のネットワークに AP を 1 つ追加する場合。	AP を CAPWAP ネットワークに導入する前に、AP を CAPWAP タイプに変換することをお勧めします。この変換は、AP コマンド、コントローラコマンド、コントローラ WebUI、または DHCP オプションを使用して手動で実行できます。
			変換後は、通常のイメージのダウンロードプロセスに従う必要があります。
			`ap-type {capwap | ewc-ap} [<sftp/tftp>://<server ip>/<AP imagepath> <sftp/tftp>://<server ip>Controller ImagePath>]`
			`wireless ewc-ap ap ap-type` *`ap-name`* `{capwap | ewc-ap}`

ネットワーク変換

ここでは、変換コマンドとネットワーク変換の展開シナリオを通じて、ネットワーク変換について説明します。

ネットワークの変換（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `>enable`	特権 EXEC モードを開始します。
ステップ 2	**Wireless ewc-ap ap capwap***primary-controller-name* {**A:B:C:D** | **X:X:X:X::X**} 例： `Device#wireless ewc-ap ap capwap wlc-name 10.0.0.0`	現在組み込みワイヤレスコントローラネットワークに接続されているすべての AP が接続する必要があるワイヤレスコントローラ名と IP アドレスを指定します。

ネットワーク変換の展開シナリオ

1. 既存の集中型 CAPWAP ネットワークまたは AireOS CAPWAP ネットワークを組み込みワイヤレスコントローラ ネットワークに変換する

既存のネットワーク	組み込みワイヤレスコントローラ Network	ユースケース	自動変換
CAPWAP ネットワーク：少なくとも 1 つの 802.11ax AP を備えた集中型 CAPWAP ネットワークまたは AireOS CAPWAP ネットワーク。	ネットワークが存在しません。	既存の集中型 CAPWAP ネットワークまたは AireOS CAPWAP ネットワークを組み込みワイヤレスコントローラ ネットワークに変換する場合。	なし。自動変換は行われません。 AP コマンドでサポートされている画像転送プロトコルを使用して、コントローラと AP の両方のイメージをダウンロードするには、1 つの 802.11ax AP を選択する必要があります。 `ap-type {capwap | ewc-ap} <sftp/tftp>://<server ip>/<AP imagepath> <sftp/tftp>://<server ip> Controller ImagePath>]`

2. 既存の組み込みワイヤレスコントローラ ネットワークを AireOS CAPWAP ネットワークまたは集中型 CAPWAP ネットワークに変換する

既存のネットワーク	組み込みワイヤレスコントローラ Network	ユースケース	自動変換
多くの AP を備えた組み込みワイヤレス コントローラ ネットワーク。	既存のネットワーク	既存の組み込みワイヤレスコントローラ ネットワークを AireOS CAPWAP ネットワークまたは集中型 CAPWAP ネットワークに変換する場合。	自動変換なし。 すべての AP または 1 つの AP を一度に変換するには、コントローラコマンドを使用して、AP が接続する必要があるコントローラの IP アドレスを指定する必要があります。 WebUI を使用して、AP が接続する必要があるコントローラの IP アドレスを指定することで、選択した AP またはすべての AP を変換することもできます。

SKU 変換シナリオ

1. 802.11ax 組み込みワイヤレスコントローラ SKU（CAPWAP SKU の代わり）

SKU	Network	ユースケース	自動変換
802.11ax 組み込みワイヤレスコントローラ SKU（CAPWAP SKU の代わり）	ネットワークが存在しません。	CAPWAP SKU ではなく 802.11ax 組み込みワイヤレスコントローラ SKU を注文した場合は、CAPWAP SKU に変換する必要があります。	自動変換は利用できません。 AP が CAPWAP AP として Catalyst 9800 コントローラに接続するように、DHCP オプション 43 を使用して Catalyst 9800 コントローラを指すことができます。

	SKU	Network	ユースケース	自動変換
2.	802.11ax CAPWAP SKU（組み込みワイヤレスコントローラ SKU の代わり）	ネットワークが存在しません。	組み込みワイヤレスコントローラ SKU ではなく 802.11ax CAPWAP SKU を注文したが、組み込みワイヤレスコントローラ SKU に変換したい場合。	自動変換は利用できません。 AP コマンドでサポートされている画像転送プロトコルを使用して、コントローラと AP の両方のイメージをダウンロードするには、1 つの 802.11ax AP を選択する必要があります。 `ap-type ewc-ap <sftp/tftp>://<server ip>/<AP imagepath> <sftp/tftp>://<server ip> Controller ImagePath>`

AireOS Mobility Express ネットワークから組み込みワイヤレスコントローラ ネットワークへの変換

手順

ステップ 1 [Next Preferred Master] 設定を既存の AireOS Mobility Express ネットワークから削除し、設定を保存します。

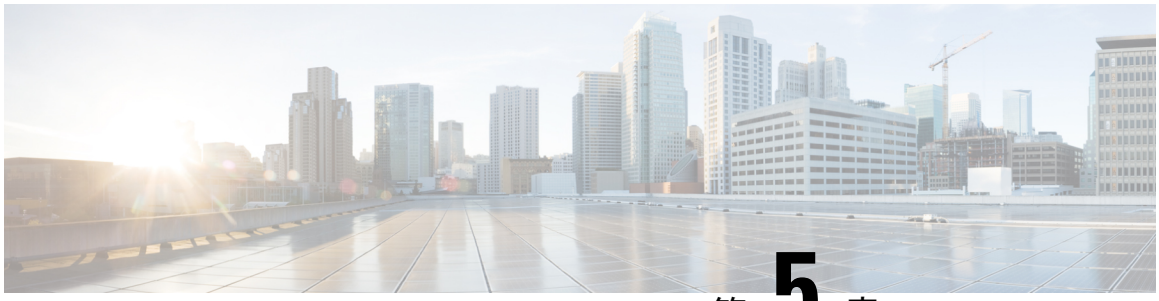
ステップ 2 プライマリ AP を含む AireOS Mobility Express ネットワーク内のすべての AP の電源を切ります。

ステップ 3 組み込みワイヤレスコントローラ SKU を使用して 11 AX AP の電源をオンにして、コントローラを起動します。

ステップ 4 必要な構成で 11 AX AP をプロビジョニングします（ボックスが Day-0 にある場合は、Day-1 に到達するための必須構成をプロビジョニングします）。

ステップ 5 すべての AireOS Mobility Express 設定をコピー、変換、および 11 AX 組み込みワイヤレスコントローラ AP に適用し、イメージのダウンロード設定を追加します。

ステップ 6 AireOS Mobility Express ネットワーク内のすべての AP の電源をオンにします。以前の AireOS Mobility Express ネットワークからの AP はすべて、組み込みワイヤレスコントローラ ネットワーク内の通常の AP として接続します。



第 5 章

ベスト プラクティス

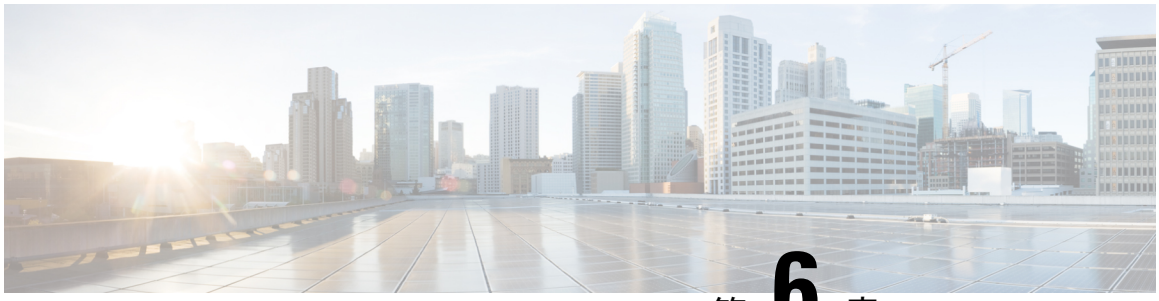
はじめに

この章では、一般的な Cisco Catalyst 9800 シリーズ ワイヤレス インフラストラクチャの設定に推奨されるベストプラクティスについて説明します。この章の目的は、大部分のワイヤレスネットワークの実装に適用できる共通設定を示すことにあります。ただし、すべてのネットワークが同じではないため、一部のヒントはインストール時に適用できない場合があります。適用できない内容については、稼働中のネットワークに変更を加える前に必ず確認してください。

詳細については、Cisco Catalyst 9800 シリーズのコンフィギュレーション ベスト プラクティスを参照してください。

第 II 部

Lightweight アクセスポイント



第 6 章

国コード

国番号について

コントローラおよびアクセスポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセスポイント内の無線は、製造時に特定の規制ドメインに割り当てられています（ヨーロッパの場合はEなど）が、国コードを使用すると、規制ドメイン内で稼働する特定の国を指定できます（フランスの場合はFR、スペインの場合はESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

日本の国番号について

国番号は、各国で合法的に使用できるチャネルを定義します。日本で使用できる国番号は、次のとおりです。

- JP：コントローラに接続できるのは、-J 無線のみです。
- J2：コントローラに接続できるのは、-P 無線のみです。
- J3：コントローラに接続できるのは、- U、- P、および - Qの無線ですが、- U の周波数を使用します。
- J4：コントローラに接続できるのは、2.4G JPQU および 5G PQU です。

日本の規制区域のアクセスポイントでサポートされているチャネルと電力レベルの一覧については、『Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points』[英語]を参照してください。

国番号の設定の前提条件

- 通常、deviceごとに1つの国番号を設定します。deviceの物理的な場所とそのアクセスポイントが一致しているコードを 1 つ設定します。device ごとに最大 20 の国番号を設定できます。これによって複数の国がサポートされ、1 台のdeviceからさまざまな国にあるアクセスポイントを管理できます。
- multiple-country 機能を使用している場合、同じ RF グループに join する予定のすべてのdeviceは、同じ国のセットを同じ順序で設定する必要があります。
- アクセスポイントは、使用可能なすべての法定周波数を使用できます。ただし、アクセスポイントは関連するドメインでサポートされる周波数に割り当てられます。
- RF グループリーダーに設定されている国リストによって、メンバーが動作するチャネルが決定します。このリストは、RF グループメンバーに設定されている国とは無関係です。
- 日本の規制ドメインにあるdeviceの場合は、deviceに join された - J 規制ドメインのアクセスポイントを少なくとも 1 つ持っている必要があります。
- 指定した国が ap country list コマンドを使用して設定されている場合、wireless country country-code コンフィギュレーション コマンドを使用して国番号を削除することはできません。その逆も同様です。

国番号の設定（GUI）

手順

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

ステップ 2 [Country] ページで、アクセスポイントがインストールされている各国のチェックボックスをオンにします。複数のチェックボックスをオンにした場合、RRM チャネルと電力レベルが共通のチャネルと電力レベルに制限されることを記載したメッセージが表示されます。

ステップ 3 [Apply] をクリックします。

国番号の設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス# enable`	特権 EXEC モードを開始します。
ステップ 2	**show wireless country supported** 例： `デバイス# show wireless country supported`	使用可能なすべての国番号のリストを表示します。
ステップ 3	**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 4	**ap dot11 24ghz shutdown** 例： `デバイス(config)# ap dot11 24ghz shutdown`	802.11b/g ネットワークをディセーブルにします。
ステップ 5	**ap dot11 5ghz shutdown** 例： `デバイス(config)# ap dot11 5ghz shutdown`	802.11a ネットワークをディセーブルにします。
ステップ 6	**ap dot11 6ghz shutdown** 例： `デバイス(config)# ap dot11 6ghz shutdown`	802.11 6 GHz ネットワークを無効にします。
ステップ 7	**ap country** *country_code* 例： `デバイス(config)# ap country IN`	
ステップ 8	**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。

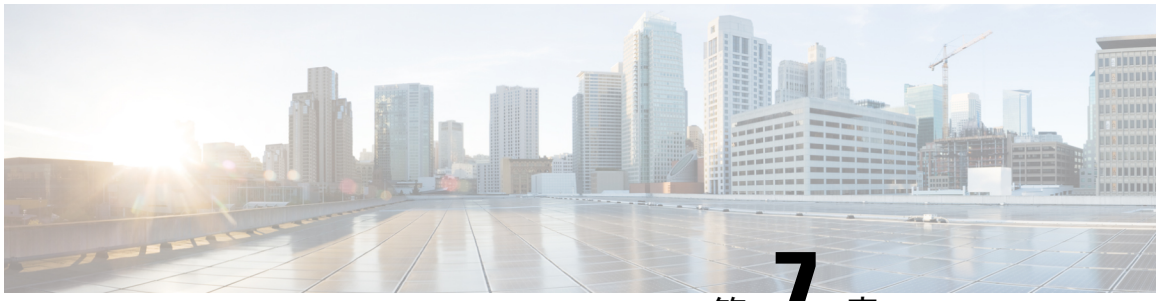
	コマンドまたはアクション	目的
ステップ 9	**show wireless country channels** 例： `デバイス# show wireless country channels`	deviceに設定された国番号の使用可能なチャネルのリストを表示します。 （注） ステップ 6 で複数の国番号を設定した場合にのみ、ステップ 9 ～ 17 を実行します。
ステップ 10	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**no ap dot11 5ghz shutdown** 例： `デバイス(config)# no ap dot11 5ghz shutdown`	802.11a ネットワークをイネーブルにします。
ステップ 12	**no ap dot11 24ghz shutdown** 例： `デバイス(config)# no ap dot11 24ghz shutdown`	802.11b/g ネットワークをイネーブルにします。
ステップ 13	**no ap dot11 6ghz shutdown** 例： `デバイス(config)# no ap dot11 6ghz shutdown`	802.11 6 GHz ネットワークを有効にします。
ステップ 14	**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。
ステップ 15	**ap name** *cisco-ap* **shutdown** 例： `デバイス# ap name AP02 shutdown`	アクセスポイントをディセーブルにします。 （注） 国番号を設定しているアクセスポイントのみをディセーブルにすることを確認します。
ステップ 16	**ap name** *cisco-ap* **no shutdown** 例： `デバイス# ap name AP02 no shutdown`	アクセスポイントを有効にします。

国番号の設定例

国番号のチャネルリストの表示

次に、deviceの国番号に使用可能なチャネルの一覧を表示する例を示します。

```
デバイス# show wireless country channels

Configured Country........................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
     A = Channel is the Auto-RF default in this country.
     . = Channel is not legal in this country.
     C = Channel has been configured for use by Auto-RF.
     x = Channel is available to be configured for use by Auto-RF.
  (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11bg         :
Channels         :                   1 1 1 1 1
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : A * * * * A * * * * A . . .
Auto-RF          : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11a          :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels         :3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                  4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : . A . A . A . A A A A A * * * * * . . . * * * A A A A*
Auto-RF          : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
4.9GHz 802.11a   :
Channels         :                   1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
US (-A ,-AB )    : * * * * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF          : . . . . . . . . . . . . . . . . . . . . . . . . . .

デバイス# show wireless country configured

Configured Country......................... US - United States
Configured Country Codes
US - United States 802.11a Indoor,Outdoor/ 802.11b Indoor,Outdoor/ 802.11g Indoor,Outdoor
```



第 7 章

ドメイン削減のための規制コンプライアンス（その他の地域）

規制コンプライアンスドメインについて

コントローラおよびアクセスポイント（AP）は、規制基準の異なるさまざまな国で使用できるように設計されています。国番号で特定の運用国を指定できます（フランスは FR、スペインは ES など）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

この機能により、既存の事前プロビジョニング ドメイン ワークフローを変更して、実行時に国番号ごとに規制ドメインを決定することで、規制ドメインの数を削減できます。新しいその他の地域（RoW）ドメインが導入され、既存の9つのドメインを含むように統合されました。すべての AP は、規制電力テーブルと許可された無線チャネルを持つドメインのいずれかから、独自の規制ドメインを決定できます。

（注） ビーコンの TPC IE の送信電力値は、**show controllers dot11radio** コマンドに表示される AP の送信電力値と最大 2 dB の差があります。ビーコンの TPC IE で許容される最大偏差は 2 dB です。

グローバルな国レベルのドメイン

表 *11 :* グローバルドメインの各国の電源テーブルとサポートされるチャネル（*2.4 GHz* および *5 GHz*）

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
アルバニア：AL	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
オーストラリア：AU	2G-A	5G-Z	1-2-3-4-5- 6-7-8-9-10-11	100-104-108- 112-116-132-136 -140-149-153-161-165
オーストリア：AT	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-S36-140
ベルギー：BE	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
ブルガリア：BG	2G-E	5G-E	1-2-3-4-5-6、 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
カナダ：CA	2G-A	5G-A	1-2-3-4-5-6 7-8-9-10-11	56-60-64-100-104-108-112-116 -132-136-140-149-153-157- 161-165
クロアチア：HR	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
キプロス：CY	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
チェコ共和国：CZ	2G-E	5G-E	1-2-3-4-5- 6-7-8-10-11-12-13	100-104-108- 112-116-132-136-140
デンマーク：DK	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
エストニア：EE	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
フィンランド：FI	2G-E	5G-E	1-2、-3-4-5 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-S36-140
フランス：FR	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
ドイツ：DE	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
ギリシャ：GR	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
ハンガリー：HU	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-S36-140
アイスランド：IS	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
インドネシア：ID	2G-F	5G-F	1-2-3-4-5-6 7-8-9-10-11-12-13	149-153-157-161
イタリア：IT	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-S36-140
日本：JP	2G-Q	5G-Q	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-120-124-128-132- 136-140-144
ラトビア：LV	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-S36-140
リヒテンシュタイン：LI	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
リトアニア：LT	2G-E	5G-E	1、2、3、4、5、6、7、8、9、10、11、12、および 13	100-104-108-112-116-132-136-140
ルクセンブルク：LU	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
マルタ：MT	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
オランダ：NL	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
ニュージーランド：NZ	2G-A	5G-E	1-2-3-4-5- 6-7-8-9-10-11	100-104-108-112-116-132-136-140- 149-153-161-165
ノルウェー：NO	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
ポーランド：PL	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
ポルトガル：PT	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
プエルトリコ：PR	2G-A	5G-B	1-2-3-4-5- 6-7-8-9-10-11	36-40-44-48-52-56-60-64-100-104-108-112-116-120-128-132-140-144-149-153- 157-161-165
ルーマニア：RO	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
ロシア連邦：RU	2G-R	5G-R	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-136-140-144-149-153-157-161-165
スロバキア共和国：SK	2G-E	5G-E	1-2、-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
スロベニア：SI	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
スペイン：ES	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
スウェーデン：SE	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
スイス：CH	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
アメリカ合衆国：US	2G-A	5G-B	1-2-3-4-5- 6-7-8-9-10-11	36-40-44-48-52-56-60-64-100-104-108-112-116-120-128-132-140-144-149-153 157-161-165

その他の地域ドメイン

次の AP は、RoW ドメインをサポートします。

- Cisco Catalyst 9124AX 屋外用アクセスポイント
- Cisco Catalyst 9136 アクセスポイント

- Cisco Catalyst 9164 シリーズ アクセスポイント
- Cisco Catalyst 9166 シリーズ アクセスポイント

表 *12 : RoW* ドメインの各国の電源テーブルとサポートされるチャネル

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
アルジェリア：DZ	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10-11-12-13	52-56-60-64-100-104-108-112-116-132
アルゼンチン：AR	2G-Z	5G-A1	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140 149-153-157-161-165
バハマ：BS	2G-A	5G-B1	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60-64-149-153-157-161-165
バーレーン：BH	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10 11-12-13	149-153-157-161-165
バングラデシュ：BD	2G-A	5G-A2	1-2-3-4-5-6-7-8-9-10- 11	149-153-157-161-165
バルバドス：BB	2G-A	5G-B1	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64 149-153-157-161-165
ボリビア：BO	2G-A	5G-A10	1-2-3-4-5-6-7-8-9-10- 11	149-153-157-161-165
ボスニア：BA	2G-E	5G-E	1-2-3-4-5-6-7-8-9-0-11-12-13	100-104-108-112-116-132-136-140
ブラジル：BR	2G-Z	5G-Z1	1-2-3-4-5-6-7-8-9-10-11-12-13	100- 104-112-116-120 124-128-132-136-140-149-153-157- 161-165
ブルネイ：BN	2G-V1	5G-M3	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64-116-120-124-128-132-136-140-149-153-157-161-165
カメルーン：CM	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116-132-136-140

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
チリ：CL	2G-A	5G-A3	1-2-3-4-5-6-7-8-9-10- 11	52-56-60-64-100-104-108-112-116-120-124-128-132-136 140-149-153-157-161-165
中国：CN	2G-E	5G-H1	1-2-3-4-5-6-7-8-9-10 11-12-13	149-153-157-161-165
コロンビア：CO	2G-A	5G-B2	1-2-3- 4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132 136-140-149-153-157-161-165
コスタリカ：CR	2G-A	5G-A4	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165
ドミニカ共和国：DO	2G-A	5G-A5	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-58-60-64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165
エクアドル：EC	2G-A	5G-A4	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165
エジプト：EG	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64
エルサルバドル：SV	2G-A	5G-A	1-2-3-4-5-6-7-8-9-10- 11	52-56-60-64-149-153-157-161-165
ガーナ：GH	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
ジブラルタル：GI	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-S36-140
香港：HK	2G-Z	5G-Z1	1-2-3-4-5-6-7-8-9-10- 11	100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
インド：IN	2G-Z	5G-D1	1-2-3-4-5-6-8-9-10-11	36-40-44-48-52-56-60- 100-104-108-112- 116-124-128-132 136-140-144-153-157-161-165-169
イスラエル：IL	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	—
ジャマイカ：JM	2G-E	5G-Z	1-2-3-4-5-6-7-8-9-10- 11	52-56-60-64-100-104- 108-112-116-120-124-128- 132-136-140-153-161-165
ヨルダン：JO	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
ケニア：KE	2G-E	5G-E	1、2、3、4、5、6、7、8、9、10、11、12、および 13	100-104-108-112-116-132-136-140
韓国：KR	2G-E	5G-K1	1-2-3-4-5-6-7-8-9-10- 11-12-13	36-40-44-48-52-56-60 64- 100-104-108-112-116-120- 124-128-132-136-140-149- 153-157-161-165
レバノン：LB	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
マケドニア：MK	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
マカオ：MO	2G-V1	5G-M3	1- 2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64 116-120-124-128- 132-140-149-153 157-161-165
マレーシア：MY	2G-F	5G-C2	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116- 120-124-128-149-153- 157-161-165
メキシコ：MX	2G-A1	5G-A6	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60- 64-149-153-157-161-165

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
モンゴル：MN	2G-E1	5G-E6	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64 116-120-124-128- 132-140-149-153 157-161-165
モナコ：MC	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-S36-140
モンテネグロ：ME	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108- 112-116-132-S36-140
オマーン：OM	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
パキスタン：PK	2G-A1	5G-E7	1-2-3-4-5-6-7-8-9-10- 11	149-153-157-161
パナマ：PA	2G-A	5G-B2	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60- 64-100-104-108-112- 116-120-124-128 132-136-140-149-153-157-161-165
パラグアイ：PY	2G-A	5G-Z1	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60- 64-100-104-108-112- 116-120-124-128- 132-136-140-149-153-157-161-165
ペルー：PE	2G-A	5G-A	1-2-3-4-5-6-7-8-9-10- 11	56-60-64-100-104-108 112-116-132-136-140- 149-153-157 161-165
フィリピン：PH	2G-E	5G-A7	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64 100-104-108-112-116-120-128-136 140-149-153-157-161-165
その他の地域（デフォルト）	2G-RW	5G-RW	1-2-3-4-5-6-7-8-9-10 11-12-13	—
サウジアラビア：SA	2G-E	5G-M1	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116 120-124-128-132-136-140
セルビア：RS	2G-E	5G-E	1-2-3-4-5- 6-7- 8-9-10-11-12-13	100-104-108- 112-116-132-136-140

国およびコード	屋外電源テーブル **2.4 GHz**	屋外電源テーブル **5 GHz**	サポートされるチャネル **2.4 GHz**	サポートされるチャネル **5 GHz**
シンガポール：SG	2G-V1	5G-M3	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64 116-120-124-128- 132-136-140-144 149-153-157-161-165
スロバキア共和国：SK	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116-132-136-140
南アフリカ：ZA	2G-E	5G-Z	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140-149-153- 157-161-165
台湾：TW	2G-Z	5G-B	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-100-104-108-112- 116-120-128-132 140-144-149-153-157-161-165
タイ：TH	2G-E	5G-M3	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60- 64- 116-120-124-128-132-136- 140-149-153-157-161-165
トリニダード：TI	2G-A1	5G-M2	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116 124-128-132-136-140
チュニジア：TN	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
トルコ：TR	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
アラブ首長国連邦：AE	2G-E	5G-E	1-2-3-4-5- 6-7-8 9-10-11-12-13	100-104-108-112-116-132-136-140
英国：GB	2G-E	5G-E1	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
ベネズエラ：VE	2G-A	5G-A8	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64- 149-153-157-161-165
ベトナム：VN	2G-V1	5G-M2	1-2-3-4-5-6-7-8-9-10-11-12-13	52-56-60-64-100-104- 112-116-124-128-132-136- 140-153-157-161-165

その他の地域に関する国番号の設定（CLI）

これは、RoW には必須の構成です。

以下の手順で国番号を設定してください。

始める前に

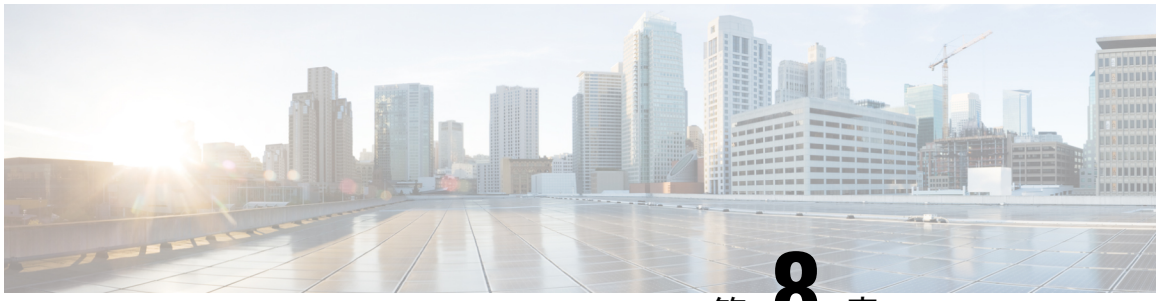
- AP プロファイルで国番号を設定する前に、その国がグローバル国リストに存在することを確認してください。設定された国番号がグローバルリストに存在しない場合、AP では以前の国番号構成が保持されます。さらに、操作が正しく設定されていないと、デフォルトフラグがトリガーされ、無線操作が停止します。
- 設定された国番号が 1 つ以上の無線スロットの規制ドメインと一致しない場合、AP では以前の国番号設定が保持されます。さらに、操作が正しく設定されていないと、デフォルトフラグがトリガーされ、無線操作が停止します。

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 profile** *ap-profile* 例： `Device(config)# ap profile default-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） Cisco組み込みワイヤレスコントローラ（EWC）は、デフォルトの AP プロファイルのみをサポートします。
ステップ 3	**country** *code* 例： `Device(config-ap-profile)# country IN`	国番号を設定します。国番号を削除するには、このコマンドの **no** 形式を使用します。 （注） Cisco IOS XE Bengaluru 17.6.1 から、**ap country** *code* コマンドが変更されました。**ap** キーワードが削除されました。変更後のコマンドは **country** *code* です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-ap-profile)# end`	特権 EXEC モードに戻ります。

ステップ 5	**show ap profile name default-ap-profile detailed**
	例：
	`Device# show ap profile name default-ap-profile detailed`
	
	`AP Profile Name : default-ap-profile`
	`Description : default ap profile`
	`.`
	`.`
	`.`
	`Country code : IN`
		AP 参加プロファイルの AP 国番号を表示します。
		AP 参加プロファイルで国が設定されていない場合、国番号は「Not configured」として表示されます。
		RoW AP の規制ドメインは、ROW として表示されます。



第 8 章

AP 優先度

アクセスポイントのフェールオーバー優先順位

各コントローラには、定義された数のアクセスポイント用通信ポートが装備されています。未使用のアクセスポイントポートがある複数のコントローラが同じネットワーク上に展開されている場合、1 つのコントローラが故障すると、ドロップしたアクセスポイントは、自動的に未使用のコントローラポートをポーリングして、そのポートにアソシエートします。

次に、アクセスポイントのフェールオーバープライオリティを設定する際の注意事項を示します。

- バックアップコントローラがプライオリティレベルの高いアクセスポイントからの join 要求を認識できるよう、また、プライオリティレベルの低いアクセスポイントを必要に応じて関連付け解除してポートを使用可能にできるようにワイヤレスネットワークを設定できます。
- フェールオーバーのプライオリティレベルは、通常の無線ネットワークの運用中は無効です。これは、コントローラで使用可能な AP キャパシティを超えるアソシエーション要求がコントローラに対して発生する場合のみ有効となります。
- コントローラがフルスケールになっている、またはプライマリコントローラで障害が発生し、APがセカンダリコントローラにフォールバックする場合、APのプライオリティはコントローラへの接続中にチェックされます。
- ネットワークのフェールオーバープライオリティを有効にして、個別のアクセスポイントにプライオリティを割り当てることができます。
- デフォルトでは、すべてのアクセスポイントはプライオリティレベル 1 に設定されています。これは、最も低いプライオリティレベルです。このため、これよりも高いプライオリティレベルを必要とするアクセスポイントにのみ、プライオリティレベルを割り当てる必要があります。

AP の優先順位の設定（GUI）

手順

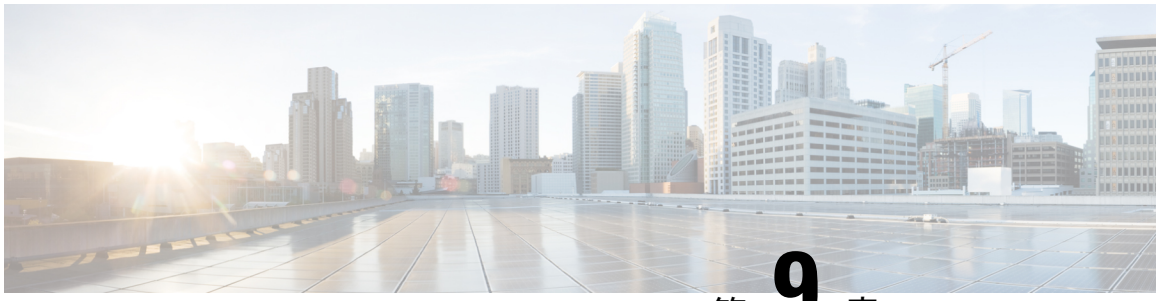
ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ 2 [Access Point] をクリックします。
ステップ 3 [Edit AP] ダイアログボックスの [High Availability] タブに移動します。
ステップ 4 [AP failover priority] ドロップダウンリストから優先順位を選択します。
ステップ 5 [Update and Apply to Device] をクリックします。

AP プライオリティの設定

（注） アクセスポイントのプライオリティの範囲は 1 ～ 4 で、4 が最高です。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* **priority** *priority* 例： `Device# ap name AP44d3.ca52.48b5 priority 1`	アクセス ポイントのプライオリティを指定します。
ステップ 2	**show ap config general** 例： `Device# show ap config general`	すべてのアクセスポイントに共通の情報を表示します。
ステップ 3	**show ap name** *ap-name* **config general** 例： `Device# show ap name AP44d3.ca52.48b5 config general`	特定のアクセスポイントの設定を表示します。



第 9 章

シスコ アクセスポイントの 802.11 パラメータ

2.4 GHz 無線サポート

指定したスロット番号に対する 2.4 GHz 無線サポートの設定

始める前に

（注） ここでは用語「802.11b 無線」または「2.4 GHz 無線」を同じ意味で使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC 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 name** *ap-name* **dot11 24ghz slot 0 SI** 例： `デバイス# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI`	特定のアクセス ポイントのスロット 0 でホストされている専用の 2.4 GHz 無線のスペクトル インテリジェンス（SI）を有効にします。詳細については、本ガイドの「スペクトルインテリジェンス」の項を参照してください。 ここで、**0** はスロット ID を示しています。
ステップ 3	**ap name** *ap-name* **dot11 24ghz slot 0 antenna** { **ext-ant-gain** *antenna_gain_value* | **selection** [**internal** | **external**]} 例： `デバイス# ap name AP-SIDD-A06 dot11 24ghz slot 0 antenna selection internal`	特定のアクセス ポイントのスロット 0 でホストされている 802.11b アンテナを設定します。 • **ext-ant-gain**：802.11b 外部アンテナゲインを設定します。*antenna_gain_value*：外部アンテナゲイン値を .5 dBi の倍数単位で参照します。有効な範囲は 0 ～ 4294967295 です。 • **selection**：802.11b アンテナの選択を設定します（内部または外部）。
ステップ 4	**ap name** *ap-name* **dot11 24ghz slot 0 beamforming** 例： `デバイス# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming`	特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線のビームフォーミングを設定します。
ステップ 5	**ap name** *ap-name* **dot11 24ghz slot 0 channel** {*channel_number* | **auto**} 例： `デバイス# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto`	特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線の高度な 802.11 チャネル割り当てパラメータを設定します。
ステップ 6	**ap name** *ap-name* **dot11 24ghz slot 0 cleanair** 例： `デバイス# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair`	特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線の CleanAir を有効にします。
ステップ 7	**ap name** *ap-name* **dot11 24ghz slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} 例：	特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線の 802.11n アンテナを設定します。

	コマンドまたはアクション	目的
	デバイス# **ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A**	ここで、各変数は次のように定義されます。 **A**：アンテナポート A。 **B**：アンテナポート B。 **C**：アンテナポート C。 **D**：アンテナポート D。
ステップ 8	**ap name** *ap-name* **dot11 24ghz slot 0 shutdown** 例： デバイス# **ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown**	特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線を無効にします。
ステップ 9	**ap name** *ap-name* **dot11 24ghz slot 0 txpower** {*tx_power_level* | **auto**} 例： デバイス# **ap name AP-SIDD-A06 dot11 24ghz slot 0 txpower auto**	特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線の送信電力レベルを無効にします。 • *tx_power_level*：送信電力レベル（dBm 単位）。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。

5 GHz 無線サポート

指定したスロット番号に対する 5 GHz 無線サポートの設定

始める前に

（注） このドキュメントでは、用語「802.11a 無線」または「5 GHz 無線」を同じ意味で使用されています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
	`Device# enable`	
ステップ 2	**ap name** *ap-name* **dot11 5ghz slot 1 SI** 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 SI`	特定のアクセス ポイントのスロット 1 でホストされている専用の 5 GHz 無線のスペクトル インテリジェンス（SI）を有効にします。 ここで、**1** はスロット ID を示しています。
ステップ 3	**ap name** *ap-name* **dot11 5ghz slot 1 antenna ext-ant-gain** *antenna_gain_value* 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna ext-ant-gain`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線の外部アンテナ ゲインを設定します。 *antenna_gain_value*：外部アンテナ ゲイン値を .5 dBi の倍数単位で参照します。有効な範囲は 0 ～ 4294967295 です。
ステップ 4	**ap name** *ap-name* **dot11 5ghz slot 1 antenna mode** [**omni** | **sectorA** | **sectorB**] 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna mode sectorA`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線のアンテナ モードを設定します。
ステップ 5	**ap name** *ap-name* **dot11 5ghz slot 1 antenna selection** [**internal** | **external**] 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna selection internal`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線のアンテナ選択を設定します。
ステップ 6	**ap name** *ap-name* **dot11 5ghz slot 1 beamforming** 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 beamforming`	特定のアクセス ポイントのスロット 1 でホストされている 5 GHz 無線のビームフォーミングを設定します。
ステップ 7	**ap name** *ap-name* **dot11 5ghz slot 1 channel** {*channel_number* | **auto** | **width** [**20** | **40** | **80** | **160**]} 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 channel auto`	特定のアクセス ポイントのスロット 1 でホストされている 5 GHz 無線の高度な 802.11 チャネル割り当てパラメータを設定します。 ここで、各変数は次のように定義されます。 *channel_number*：チャネル番号を指します。有効な範囲は 1 ～ 173 です。

	コマンドまたはアクション	目的
ステップ 8	**ap name** *ap-name* **dot11 5ghz slot 1 cleanair** 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 cleanair`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線の CleanAir を有効にします。
ステップ 9	**ap name** *ap-name* **dot11 5ghz slot 1 dot11n antenna** {**A** | **B** | **C** | **D**} 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 dot11n antenna A`	特定のアクセス ポイントのスロット 1 でホストされている 5 GHz 無線の 802.11n アンテナを設定します。 ここで、各変数は次のように定義されます。 **A**：アンテナ ポート A。 **B**：アンテナ ポート B。 **C**：アンテナ ポート C。 **D**：アンテナ ポート D。
ステップ 10	**ap name** *ap-name* **dot11 5ghz slot 1 rrm channel** *channel* 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 rrm channel 2`	特定のアクセス ポイントのスロット 1 でホストされているチャネルを変更するもう 1 つの方法です。 ここで、各変数は次のように定義されます。 *channel*：802.11h チャネル アナウンスを使用して作成された新しいチャネルを指します。有効な範囲は 1 ～ 173 で、173 は、アクセス ポイントを展開している国の有効なチャネルです。
ステップ 11	**ap name** *ap-name* **dot11 5ghz slot 1 shutdown** 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 shutdown`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線を無効にします。
ステップ 12	**ap name** *ap-name* **dot11 5ghz slot 1 txpower** {*tx_power_level* | **auto**} 例： `デバイス# ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線を設定します。 • *tx_power_level*：送信電力レベルを dBm 単位で示します。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。

デュアルバンド無線サポートについて

Cisco 2800、3800、4800、および 9120 シリーズの AP モデルのデュアルバンド（XOR）無線は、2.4 GHz または 5 GHz 帯域を利用、または同一 AP 上での両帯域を受動的に監視する機能を提供します。これらの AP は、クライアントに 2.4 GHz および 5 GHz 帯域でサービスを提供するように設定できます。または、メインの 5 GHz 無線がクライアントにサービスを提供しながら、フレキシブル無線で 2.4 GHz 帯と 5 GHz 帯の両方を順次スキャンします。

Cisco 9120 AP までの Cisco AP はデュアル 5 GHz 帯域の動作に対応できるように設計されており、専用のマクロ/マイクロアーキテクチャをサポートする i モデルと、マクロ/マクロをサポートする e および p モデルがあります。Cisco 9130AXI AP および Cisco 9136 AP はデュアル 5 GHz 動作をマイクロ/Messo セルとしてサポートします。

無線が帯域間を移動する場合（2.4 GHz から 5 GHz へ、またはその逆）、無線間で最適な分散を実現するには、クライアントをステアリングする必要があります。AP に 5 GHz 帯域の無線が 2 つある場合、フレキシブル ラジオ アサインメント（FRA）アルゴリズムに含まれるクライアント ステアリング アルゴリズムを使用して、同じ帯域の共存無線間でクライアントをステアリングします。

XOR 無線のサポートのステアリングは、手動または自動で行うことができます。

- 無線での帯域の手動ステアリング：XOR 無線の帯域は手動でのみ変更できます。
- 無線でのクライアントおよび帯域の自動ステアリングは、サイトの要件に従って帯域構成を監視および変更する FRA 機能によって管理されます。

（注） スロット 1 で静的チャネルが設定されている場合、RF 測定は実行されないため、デュアルバンド無線スロット 0 は 5 GHz 無線でのみ移動し、モニターモードには移動しません。

スロット 1 の無線が無効になっている場合、RF 測定は実行されず、デュアルバンド無線のスロット 0 は 2.4 GHz 無線のみになります。

デフォルトの XOR 無線サポートの設定

始める前に

（注） デフォルトの無線とは、スロット 0 でホストされている XOR 無線を指します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* 例： `デバイス# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	特定のシスコ アクセス ポイントの 802.11 デュアルバンド アンテナを設定します。 *antenna_gain_value*：有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** 例： `デバイス# ap name ap-name dot11 dual-band shutdown`	特定のシスコ アクセス ポイントでデフォルトのデュアルバンド無線をシャットダウンします。 無線を有効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band role manual client-serving** 例： `デバイス# ap name ap-name dot11 dual-band role manual client-serving`	シスコアクセスポイントでクライアントサービングモードに切り替えます。
ステップ 5	**ap name** *ap-name* **dot11 dual-band band 24ghz** 例： `デバイス# ap name ap-name dot11 dual-band band 24ghz`	2.4 GHz 無線帯域に切り替えます。
ステップ 6	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} 例：	特定のシスコ アクセス ポイントにおける無線の送信電力を設定します。

	コマンドまたはアクション	目的
	デバイス# ap name *ap-name* dot11 dual-band txpower 2	（注） FRA 対応無線（たとえば、9120 AP のスロット 0）が Auto に設定されている場合、この無線で静的チャネルと送信電力を設定することはできません。 この無線で静的チャネルと送信電力を設定する場合は、無線のロールを手動クライアントサービスモードに変更する必要があります。
ステップ 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* 例： デバイス# ap name *ap-name* dot11 dual-band channel 2	デュアルバンドのチャネルを入力します。 *channel-number*：有効な範囲は 1 ～ 173 です。
ステップ 8	**ap name** *ap-name* **dot11 dual-band channel auto** 例： デバイス# ap name *ap-name* dot11 dual-band channel auto	デュアルバンドの自動チャネル割り当てを有効にします。
ステップ 9	**ap name** *ap-name* **dot11 dual-band channel width**{**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} 例： デバイス# ap name *ap-name* dot11 dual-band channel width 20 MHz	デュアルバンドのチャネル幅を選択します。
ステップ 10	**ap name** *ap-name* **dot11 dual-band cleanair** 例： デバイス# ap name *ap-name* dot11 dual-band cleanair	デュアルバンド無線の Cisco CleanAir 機能を有効にします。
ステップ 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz** | **5 GMHz**} 例： デバイス# ap name *ap-name* dot11 dual-band cleanair band 5 GHz	Cisco CleanAir 機能の帯域を選択します。 Cisco CleanAir 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。

	コマンドまたはアクション	目的
	デバイス# ap name *ap-name* [no] dot11 dual-band cleanair band 5 GHz	
ステップ 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A** | **B** | **C** | **D**} 例： デバイス# ap name *ap-name* dot11 dual-band dot11n antenna A	特定のアクセス ポイントの 802.11n デュアルバンドパラメータを設定します。
ステップ 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** 例： デバイス# show ap name *ap-name* auto-rf dot11 dual-band	シスコ アクセス ポイントの自動 RF 情報を表示します。
ステップ 14	**show ap name** *ap-name* **wlan dot11 dual-band** 例： デバイス# show ap name *ap-name* wlan dot11 dual-band	シスコ アクセスポイントの BSSID のリストを表示します。

指定したスロット番号に対する XOR 無線サポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Access Points]** の順にクリックします。

ステップ 2 [Dual-Band Radios] セクションで、デュアルバンド無線を設定する AP を選択します。

AP の AP 名、MAC アドレス、CleanAir 機能、およびスロット情報が表示されます。HyperLocation 方式が HALO の場合は、アンテナの PID とアンテナの設計情報も表示されます。

ステップ 3 [Configure] をクリックします。

ステップ 4 [General] タブで、必要に応じて [Admin Status] を設定します。

ステップ 5 [CleanAir Admin Status] フィールドを [Enable] または [Disable] に設定します。

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

指定したスロット番号に対する XOR 無線サポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド アンテナを設定します。 *external_antenna_gain_value*：外部アンテナ ゲイン値（.5 dBi の倍数単位）。有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線の現在の帯域を設定します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド チャネルを設定します。 *channel_number*：有効な範囲は 1 ～ 165 です。
ステップ 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線の CleanAir 機能を有効にします。
ステップ 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	特定のアクセス ポイントのスロット 0 でホストされている 802.11n デュアルバンド パラメータを設定します。 ここで、各変数は次のように定義されます。 **A**：アンテナ ポート A を有効にします。 **B**：アンテナ ポート B を有効にします。

	コマンドまたはアクション	目的
		C：アンテナポートCを有効にします。 **D**：アンテナポートDを有効にします。
ステップ 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンドの役割を設定します。 デュアルバンドの役割は次のとおりです。 • **auto**：無線の役割を自動で選択することを指します。 • **manual**：無線の役割を手動で選択することを指します。

ステップ 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown**
	例：
	`デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown`
	`デバイス# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`
		特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線を無効にします。
		デュアルバンド無線を有効にするには、このコマンドの **no** 形式を使用します。

ステップ 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	特定のアクセスポイントのスロット 0 でホストされている XOR 無線のデュアルバンド送信電力を設定します。 • *tx_power_level*：送信電力レベルを dBm 単位で示します。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。

受信専用デュアルバンド無線サポート

受信専用デュアルバンド無線のサポートについて

この機能では、デュアルバンド無線を備えたアクセスポイントのデュアルバンド受信専用無線機能を設定します。

このデュアルバンド受信専用無線は、分析、HyperLocation、ワイヤレスセキュリティモニターリング、および BLE AoA* の専用となります。

この無線は常にモニターモードでの機能を継続するため、3番目の無線でチャネル設定や*tx-rx*設定を行うことはできません。

アクセスポイントの受信専用デュアルバンドパラメータの設定

シスコアクセスポイントでの受信専用デュアルバンド無線によるCleanAirの有効化（GUI）

手順

ステップ1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ2 [Dual-Band Radios] の設定で、デュアルバンド無線を設定する AP をクリックします。
ステップ3 [General] タブで、[CleanAir] トグルボタンを有効にします。
ステップ4 [Update & Apply to Device] をクリックします。

シスコ アクセス ポイントでの受信専用デュアルバンド無線による CleanAir の有効化

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 cleanair band** {**24Ghz** | **5Ghz**} 例： デバイス# **ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 cleanair band 24Ghz** デバイス# **ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 cleanair band 24Ghz**	特定のアクセスポイントで受信専用（Rx専用）デュアルバンド無線による CleanAir を有効にします。 ここで、2 はスロット ID を示しています。 CleanAir を無効にするには、このコマンドの **no** 形式を使用します。

シスコアクセスポイントでの受信専用デュアルバンド無線の無効化（GUI）

手順

ステップ1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ2 [Dual-Band Radios] の設定で、デュアルバンド無線を設定する AP をクリックします。
ステップ3 [General] タブで、[CleanAir Status] トグルボタンを無効にします。

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

シスコ アクセス ポイントでの受信専用デュアルバンド無線の無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 shutdown** 例： デバイス# **ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 shutdown** デバイス# **ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 shutdown**	特定のシスコ アクセス ポイントで受信専用デュアルバンド無線を無効にします。 ここで、2 はスロット ID を示しています。 受信専用デュアルバンド無線を有効にするには、このコマンドの **no** 形式を使用します。

クライアント ステアリングの設定（CLI）

始める前に

対応するデュアルバンド無線で Cisco CleanAir を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス# **enable**	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： デバイス# **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。

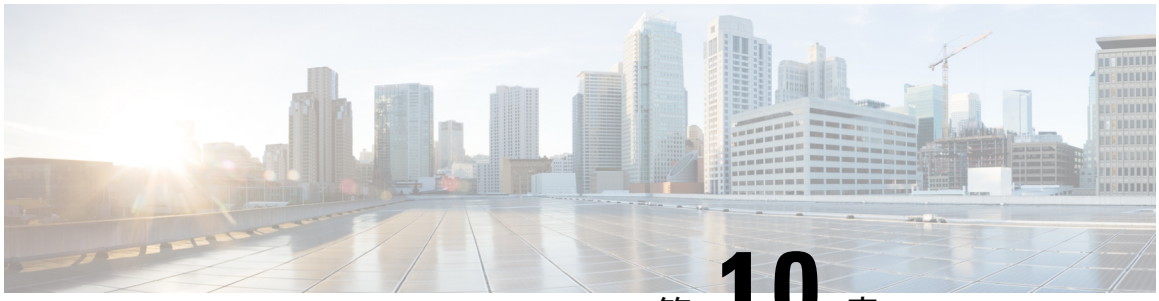
	コマンドまたはアクション	目的
ステップ 3	**wireless macro-micro steering transition-threshold balancing-window** *number-of-clients(0-65535)* 例： `デバイス(config)# wireless macro-micro steering transition-threshold balancing-window 10`	設定した数のクライアントのマイクロマクロ クライアント ロードバランシング ウィンドウを設定します。
ステップ 4	**wireless macro-micro steering transition-threshold client count** *number-of-clients(0-65535)* 例： `デバイス(config)# wireless macro-micro steering transition-threshold client count 10`	移行する最小クライアント数のマクロマイクロ クライアント パラメータを設定します。
ステップ 5	**wireless macro-micro steering transition-threshold macro-to-micro** *RSSI-in-dBm(–128—0)* 例： `デバイス(config)# wireless macro-micro steering transition-threshold macro-to-micro -100`	マクロからマイクロへの移行の RSSI を設定します。
ステップ 6	**wireless macro-micro steering transition-threshold micro-to-macro** *RSSI-in-dBm(–128—0)* 例： `デバイス(config)# wireless macro-micro steering transition-threshold micro-to-macro -110`	マイクロからマクロへの移行の RSSI を設定します。
ステップ 7	**wireless macro-micro steering probe-suppression aggressiveness** *number-of-cycles(–128—0)* 例： `デバイス(config)# wireless macro-micro steering probe-suppression aggressiveness -110`	抑制するプローブ サイクル数を設定します。
ステップ 8	**wireless macro-micro steering probe-suppression hysteresis** *RSSI-in-dBm* 例： `デバイス(config)# wireless macro-micro steering probe-suppression hysteresis -5`	RSSI でのマクロからマイクロへのプローブを設定します。範囲は -6 ～ -3 です。

	コマンドまたはアクション	目的
ステップ 9	**wireless macro-micro steering probe-suppression probe-only** 例： `デバイス(config)# wireless macro-micro steering probe-suppression probe-only`	プローブ抑制モードを有効にします。
ステップ 10	**wireless macro-micro steering probe-suppression probe-auth** 例： `デバイス(config)# wireless macro-micro steering probe-suppression probe-auth`	プローブおよびシングル認証抑制モードを有効にします。
ステップ 11	**show wireless client steering** 例： `デバイス# show wireless client steering`	ワイヤレス クライアント ステアリング情報を表示します。

デュアルバンド無線を備えたシスコ アクセスポイントの確認

デュアルバンド無線によるアクセス ポイントを確認するには、次のコマンドを使用します。

```
Device# show ap dot11 dual-band summary

AP Name Subband Radio      Mac   Status Channel Power Level Slot ID Mode
------------------------------------------------------------------------------
4800   All 3890.a5e6.f360 Enabled (40)* *1/8     (22 dBm)      0   Sensor
4800   All 3890.a5e6.f360 Enabled N/A    N/A       2               Monitor
```



第 10 章

802.1x サポート

802.1X 認証の概要

IEEE 802.1X ポートベースの認証は、不正なデバイスによるネットワークアクセスを防止するためにデバイスに設定されます。デバイスでは、固定された構成に基づいて、ルータ、スイッチ、およびアクセスポイントの機能を組み合わせることができます。802.1X認証が有効になっているスイッチポートに接続しているデバイスはすべて、トラフィックの交換を開始する場合に、関連する EAP 認証モデルを実行する必要があります。

現在、Cisco Wave 2 AP および Wi-Fi 6（802.11AX）APは、EAP-FAST、EAP-TLS、および EAP-PEAP 方式のスイッチポートを使用した 802.1X 認証をサポートしています。そのため、設定を有効にして組み込みコントローラから AP にクレデンシャルを提供できます。

EAP-FAST プロトコル

シスコが開発した EAP-FAST プロトコルでは、RADIUS を使用したセキュアな TLS トンネルを確立するために、AP では、インバンドプロビジョニング（セキュア チャネル内）またはアウトバンドプロビジョニング（手動）を介して提供される強力な共有キー（PAC）を必要とします。

（注） AP では MSCHAP バージョン 2 方式の EAP-FAST が使用されるため、EAP-FAST タイプの設定では AP に対して Dot1x クレデンシャルの設定が必要です。

（注） ローカル EAP は、Cisco 7925 電話ではサポートされていません。

EAP-TLS/EAP-PEAP プロトコル

EAP-TLS プロトコルまたは EAP-PEAP プロトコルは、証明書ベースの相互 EAP 認証を提供します。

EAP-TLS では、サーバー側証明書とクライアント側証明書の両方が必要であり、特定のセッションに対してデータを暗号化または復号化するために、セキュリティ保護された共有キーが導出されます。一方、EAP-PEAP ではサーバー側証明書のみ必要であり、クライアントはセキュリティ保護されたチャネルでパスワードベースのプロトコルを使用して認証を行います。

（注） EAP-PEAP タイプの設定では AP に対して Dot1x クレデンシャルの設定が必要です。また、AP では LSC のプロビジョニングを実行する必要もあります。AP では MSCHAP バージョン 2 方式の PEAP プロトコルが使用されます。

802.1X 認証の制限事項

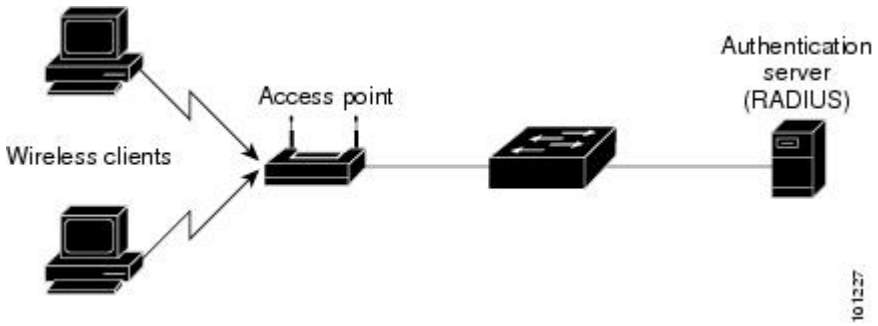
- 802.1Xはダイナミックポートまたはイーサネットチャネルポートではサポートされていません。
- 802.1X はメッシュ AP のシナリオではサポートされていません。
- クレデンシャルの不一致、またはAP上の証明書の期限切れ/無効が生じた場合、組み込みコントローラから回復することはありません。構成を修正するために再び AP に接続するには、スイッチポートで 802.1X 認証を無効にする必要があります。
- AP にインストールされた証明書では証明書失効チェックは実装されません。
- AP ではローカルで有効な証明書（LSC）を 1 つだけプロビジョニングでき、組み込みコントローラによる CAPWAP DTLS セッションの確立と、スイッチによる 802.1X 認証では、これと同じ証明書を使用する必要があります。組み込みコントローラのグローバル LSC 設定が無効になった場合、AP では、すでにプロビジョニングされている LSC が削除されます。
- AP に構成のクリアが適用された場合、AP では 802.1X EAP タイプの構成と LSC 証明書が失われます。802.1X が必要な場合、AP では再度ステージングプロセスを実行する必要があります。
- マルチホスト認証モードのトランクポート AP の 802.1X がサポートされています。Network Edge Authentication Topology（NEAT）は COS AP ではサポートされていません。

トポロジ - 概要

802.1X 認証のイベントは次のとおりです。

1. AP は 802.1X サプリカントとして機能し、RADIUS サーバーに対してスイッチによって認証されます。RADIUS サーバーは、EAP-FAST とともに EAP-TLS と EAP-PEAP もサポートします。dot1x 認証がスイッチポートで有効になっている場合、そのポートに接続しているデバイスは、802.1X トラフィック以外のデータを受信して転送するために自分自身を認証します。
2. EAP-FAST 方式による認証を行うには、AP で RADIUS サーバーのクレデンシャルが必要になります。クレデンシャルは組み込みコントローラで設定でき、そこから設定更新要求を介して AP に渡されます。EAP-TLS または EAP-PEAP の場合、AP では、ローカル CA サーバーによって重要扱いにされた証明書（デバイス/ID および CA）が使用されます。

図 *13 :* 図 *1* : *802.1X* 認証のトポロジ



802.1X 認証タイプと LSC AP 認証タイプの設定（GUI）

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 **[AP]** > **[General]** タブで、[AP EAP Auth Configuration] セクションに移動します。

ステップ 4 [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] を選択して、dot1x 認証タイプを設定します。

ステップ 5 [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。

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

802.1X 認証タイプと LSC AP 認証タイプの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**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 3	**ap profile** *profile-name* 例： `Device(config)# ap profile new-profile`	プロファイル名を指定します。
ステップ 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプを設定します。 **max-sessions**：AP ごとに開始される 802.1X セッションの最大数を設定します。 **username**：すべての AP の 802.1X ユーザー名を設定します。 **eap-type**：スイッチ ポートを使用した dot1x 認証タイプを設定します。 **lsc-ap-auth-state**：AP での LSC 認証状態を設定します。
ステップ 5	**dot1x eap-type {EAP-FAST | EAP-TLS | EAP-PEAP}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプ（EAP-FAST、EAP-TLS、または EAP-PEAP）を設定します。
ステップ 6	**dot1x lsc-ap-auth-state {CAPWAP-DTLS | Dot1x-port-auth | Both}** 例： `Device(config-ap-profile)#dot1x lsc-ap-auth-state Dot1x-port-auth`	AP での LSC 認証状態を設定します。 **CAPWAP-DTLS**：CAPWAP DTLS にのみ LSC を使用します。

	コマンドまたはアクション	目的
		Dot1x-port-auth：ポートでの dot1x 認証にのみ LSC を使用します。 **Both**：CAPWAP-DTLS とポートでの Dot1x 認証の両方に LSC を使用します。
ステップ 7	**end** 例： `Device(config-ap-profile)# end`	AP プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

802.1X ユーザー名とパスワードの設定（GUI）

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] ページで、 AP Join 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 [Management] タブをクリックし、[Credentials] タブをクリックします。

ステップ 4 ローカルのユーザ名とパスワードの詳細を入力します。

ステップ 5 適切なローカル パスワード タイプを選択します。

ステップ 6 802.1X ユーザー名とパスワードの詳細を入力します。

ステップ 7 適切な 802.1X パスワードタイプを選択します。

ステップ 8 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。

ステップ 9 必要に応じて、ローカルログイン情報や 802.1X ログイン情報を有効にします。

ステップ 10 [Update & Apply to Device] をクリックします。

802.1X ユーザー名とパスワードの設定（CLI）

次の手順では、すべての AP の 802.1X パスワードを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
ステップ 2	**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 3	**ap profile** *profile-name* 例： `Device(config)# ap profile new-profile`	プロファイル名を指定します。
ステップ 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプを設定します。 **max-sessions**：AP ごとに開始される 802.1X セッションの最大数を設定します。 **username**：すべての AP の 802.1X ユーザー名を設定します。 **eap-type**：スイッチ ポートを使用した dot1x 認証タイプを設定します。 **lsc-ap-auth-state**：AP での LSC 認証状態を設定します。
ステップ 5	**dot1x username** <username> **password {0 | 8}** <password> 例： `Device(config-ap-profile)#dot1x username username password 0 password`	すべての AP の dot1x パスワードを設定します。 0：暗号化されていないパスワードに従うことを指定します。 8：AES で暗号化されたパスワードに従うことを指定します。

スイッチポートでの 802.1X の有効化

次の手順では、スイッチポートで 802.1X を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**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 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authentication dot1x {default | listname} method1[method2...]** 例： `Device(config)# aaa authentication dot1x default group radius`	デバイスが AAA サーバーと通信できるように、特権コマンドレベルにアクセスするユーザー権限の決定に使用される一連の認証方式を作成します。
ステップ 5	**aaa authourization network group** 例： `aaa authourization network group`	802.1X でのネットワークサービスの AAA 認証を有効にします。
ステップ 6	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 7	**interface type slot/port** 例： `Device(config)# interface fastethernet2/1`	インターフェイス コンフィギュレーション モードを開始し、802.1X認証をイネーブルにするインターフェイスを指定します。
ステップ 8	**authentication port-control {auto | force-authorized | force-unauthorized}** 例： `Device(config-if)# authentication port-control auto`	インターフェイス上で 802.1x ポートベースの認証をイネーブルにします。 [auto]：IEEE 802.1X 認証を有効にし、ポートを無許可ステートで開始します。ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。デバイスはサプリカントの識別を要求し、サプリカントと認証サーバ間で認証メッセージのリレーを開始します。デバイスはサプリカントの MAC アドレスを使用して、ネットワーク アクセスを試みる各サプリカントを一意に識別します。 [force-authorized]：IEEE 802.1X 認証を無効にし、その結果、認証の交換を必

	コマンドまたはアクション	目的
		要とせずにポートが許可済みステートに変更されます。ポートは、クライアントの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。 [force unauthorized]：ポートが無許可ステートのままになり、サプリカントからの認証の試みをすべて無視します。デバイスは、このポートを介してサプリカントに認証サービスを提供することはできません。
ステップ 9	**dot1x pae [supplicant | authenticator | both]** 例： `Device(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードを開始します。

スイッチポートでの 802.1X の確認

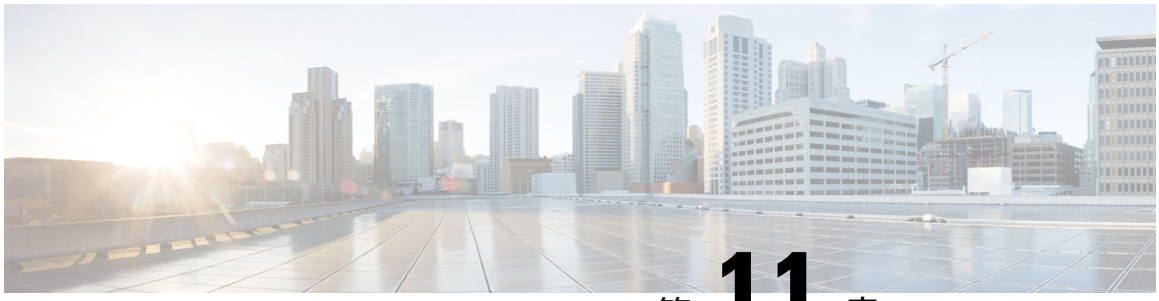
次の show コマンドは、スイッチポートでの 802.1X の認証状態を表示します。

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version      2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Device#
```

認証タイプの確認

次の show コマンドは、AP プロファイルの認証状態を表示します。

```
Device#show ap profile <profile-name> detailed ?
  chassis  Chassis
  |        Output modifiers
  <cr>

Device#show ap profile <profile-name> detailed

  AP Profile Name        : default-ap-profile
  Description            : default ap profile
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port
auth
```



第 11 章

リアルタイム アクセスポイント統計

アクセスポイントのリアルタイム統計に関する情報

Cisco IOS XE Bengaluru 17.5.1 以降では、AP のリアルタイム統計を生成することにより、AP の CPU 使用率とメモリ使用率を追跡し、AP の正常性を監視できます。

SNMP トラップは、AP とコントローラの CPU およびメモリ使用率に対して定義されます。SNMP トラップは、しきい値を超えたときに送信されます。サンプリング期間および統計間隔は、SNMP、YANG、および CLI を使用して設定できます。

統計間隔は、AP からのデータを処理するために使用され、平均 CPU 使用率とメモリ使用率が経時的に計算されます。これらの統計の上限しきい値を設定することもできます。統計値が上限しきい値を超えると、アラームが有効になり、SNMP トラップがトリガーされます。

Cisco IOS XE Cupertino 17.7.1 リリース以降では、無線モニタリングのために、サンプリング期間中に AP から送信された統計に基づいて無線をリセットできます。コントローラで無線を設定するときに、無線が稼働しているときに Tx または Rx の統計に増分がない場合、無線のリセットがトリガーされます。

リアルタイム アクセスポイント統計の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

表 *13 :* リアルタイム アクセスポイント統計の機能履歴

リリース	機能	機能情報
Cisco IOS XE Cupertino 17.7.1	リアルタイム アクセスポイント統計	この機能は、アラームをトリガーする AP しきい値（0 ～ 50）の実装により強化されています。

AP 無線モニタリング統計の制約事項

コントローラから無線ファームウェアをリセットすることはできません。指定された期間に無線スロットの Rx または Tx カウントが増分されない場合、コントローラは無線を遮断および遮断解除します。

アクセスポイントのリアルタイム統計の設定（GUI）

手順

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

ステップ 2 [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 [AP] タブの下にある [AP Statistics] タブをクリックします。

ステップ 4 [System Monitoring] セクションで、以下の手順を実行します。

a) [Monitor Real Time Statistics] を有効にして、AP の計算された統計とアラームを取得します。

b) CPU使用率やメモリなどのパラメータの上限しきい値を超えたときにアラームを受信するには、[Trigger Alarm for AP] を有効にします。

c) [CPU Threshold to Trigger Alarm] フィールドと [Memory Threshold to Trigger Alarm] フィールドに、それぞれ CPU とメモリ使用量のしきい値の割合を入力します。有効な範囲は 0 ～ 50 です。SNMP トラップは、このしきい値を超えたときに送信されます。

d) [Interval to Hold Alarm] フィールドに、アラームがトリガーされる前に保持される時間を入力します。有効な範囲は 0 ～ 3600 秒です。

e) [Trap Retransmission Time] フィールドに、アラームの再送信間隔を入力します。有効な範囲は 0 ～ 65535 秒です。

f) AP からデータを収集する頻度を定義するには、[Sampling Interval] フィールドに値を入力します。有効な範囲は 720 ～ 3600 秒です。

g) AP統計の計算間隔を定義するには、[Statistics Interval] フィールドに値を入力します。有効な範囲は 2 ～ 900 秒です。

h) 定義されたサンプリング間隔における CPU とメモリ使用量が高い場合に AP を自動的にリロードするには、[Reload the AP] チェックボックスをオンにします。

ステップ 5 [Radio Monitoring] セクションで、以下の手順を実行します。

a) [Monitoring of AP Radio Stuck] チェックボックスをオンにして、ペイロードが AP からコントローラに着信するたびに AP の Tx および Rx 統計が更新されることを確認します。

b) ペイロードの Tx および RX 統計に増分がない場合に AP の無線のアラームを生成するには、[Alarms for AP Radio Stuck] チェックボックスをオンにします。

c) [Reset the stuck AP Radio] チェックボックスをオンにして、無線を不良状態から回復します。無線を切り替えるために無線管理状態ペイロードがコントローラから送信されます。Tx および Rx 統計に増分がない場合、無線はシャットダウンされます。

d) 無線からデータを収集する頻度を定義するには、[Sampling Interval] フィールドに値を入力します。有効な範囲は 720 ～ 3600 秒です。

ステップ 6 [Apply to Device] をクリックして、設定を保存します。

リアルタイム アクセスポイント統計の設定（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。
ステップ 2	**ap profile** *ap-profile-name* 例： `Device(config)# ap profile doc-test`	APプロファイルを設定します。デフォルトの AP 接続プロファイル名は default-ap-profile です。
ステップ 3	**stats-timer** *frequency* 例： `Device(config-ap-profile)# stats-timer 60`	（任意）統計タイマーを設定します。このコマンドは、APから統計レポートを取得する頻度を変更するために使用されます。有効な値の範囲は0～65535秒です。
ステップ 4	**statistics ap-system-monitoring enable** 例： `Device(config-ap-profile)# statistics ap-system-monitoring enable`	（任意）APのリアルタイム統計（CPUとメモリ）の監視を有効にします。
ステップ 5	**statistics ap-system-monitoring alarm-enable** 例： `Device(config-ap-profile)# statistics ap-system-monitoring alarm-enable`	AP のリアルタイム統計（CPU とメモリ）のアラームを有効にします。

	コマンドまたはアクション	目的
ステップ 6	**statistics ap-system-monitoring alarm-hold-time** *duration* 例： `Device(config-ap-profile)# statistics ap-system-monitoring alarm-hold-time 400`	AP のリアルタイム統計（CPU とメモリ）のアラームを定義します。有効な値の範囲は 0 ～ 3600 秒です。
ステップ 7	**ap-system-monitoring alarm-retransmit-time** *duration* 例： `Device(config-ap-profile)# ap-system-monitoring alarm-retransmit-time 100`	トラップアラームの再送信間隔を定義します。有効な値の範囲は 0 ～ 65535 秒です。
ステップ 8	**statistics ap-system-monitoring cpu-threshold** *percentage* 例： `Device(config-ap-profile)# statistics ap-system-monitoring cpu-threshold 30`	アラームをトリガーする AP の CPU 使用率のしきい値（パーセンテージ）を定義します。 （注） Cisco IOS XE Cupertino 17.7.1 リリース以降、アラームをトリガーする AP の CPU の有効なしきい値は 0 ～ 50 です。
ステップ 9	**ap-system-monitoring mem-threshold** *percentage* 例： `Device(config-ap-profile)# ap-system-monitoring mem-threshold 40`	アラームをトリガーする AP のメモリ使用量のしきい値を定義します。トリガーする AP のメモリ使用量のしきい値のパーセンテージは 0 ～ 100 です。 （注） Cisco IOS XE Cupertino 17.7.1 リリース以降、アラームをトリガーする AP のメモリ使用量の有効なしきい値は 0 ～ 50 です。
ステップ 10	**ap-system-monitoring sampling-interval** *duration* 例： `Device(config-ap-profile)# statistics ap-system-monitoring sampling-interval 600`	（任意）サンプリング間隔を定義します。有効な値の範囲は 2 ～ 900 秒です。
ステップ 11	**exit** 例： `Device(config-ap-profile)# exit`	APプロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション 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 12	**trapflags ap ap-stats** 例： `Device(config)# trapflags ap ap-stats`	AP関連トラップの送信をイネーブルにします。統計値が設定されたしきい値を超えると、トラップが送信されます。

例

```
Device(config)# ap profile default-policy-profile
Device(config-ap-profile)# statistics ap-system-monitoring enable
Device(config-ap-profile)#statistics ap-system-monitoring sampling-interval 90
Device(config-ap-profile)#statistics ap-system-monitoring stats-interval 120
Device(config-ap-profile)#statistics ap-system-monitoring alarm-enable
Device(config-ap-profile)#statistics ap-system-monitoring alarm-hold-time 3
Device(config-ap-profile)#statistics ap-system-monitoring alarm-retransmit-time 10
Device(config-ap-profile)#statistics ap-system-monitoring cpu-threshold 90
Device(config-ap-profile)#statistics ap-system-monitoring mem-threshold 90
Device(config)# trapflags ap ap-stats
```

AP 無線モニタリング統計の設定

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	**ap profile** *profile-name* 例： `Device(config)# ap profile test1`	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。
ステップ 3	**statistic ap-radio-monitoring enable** 例： `(config-ap-profile)#statistic ap-radio-monitoring enable`	AP 無線スタック統計のモニタリングを有効にします。
ステップ 4	**statistic ap-radio-monitoring alarm-enable** 例： `(config-ap-profile)#statistic ap-radio-monitoring alarm-enable`	（任意）AP 無線スタック統計のアラームを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**statistic ap-system-monitoring action reload-ap interval** *duration* 例： `(config-ap-profile)# statistic ap-radio-monitoring action reload-ap interval850`	（任意）サンプリング間隔を秒単位で指定します。有効な値の範囲は720～3600秒です。
ステップ 6	**statistic ap-radio-monitoring action radio-reset** 例： `(config-ap-profile)# statistic ap-radio-monitoring action radio-reset`	（任意）無線がスタックしている場合、アラームを生成し、無線をリセットします。
ステップ 7	**statistic ap-system-monitoring action reload-ap** 例： `(config-ap-profile)# statistic ap-system-monitoring action reload-ap`	AP をリロードします。

例

```
Device(config)# ap profile test1
Device(config-ap-profile)# statistics ap-radio-monitoring enable
Device(config-ap-profile)#statistic ap-radio-monitoring alarm-enable
Device(config-ap-profile)#statistic ap-radio-monitoring sampling-interval 750
Device(config-ap-profile)# statistic ap-radio-monitoring action radio-reset
Device(config-ap-profile)#statistic ap-system-monitoring action reload-ap
```

アクセスポイントのリアルタイム統計の監視（GUI）

手順

ステップ 1 [Monitoring] > [Wireless] > [AP Statistics] を選択します。

ステップ 2 [General] タブをクリックします。

ステップ 3 AP 名をクリックします。[General] ウィンドウが表示されます。

ステップ 4 AP 統計データを表示するには、[AP Statistics] タブをクリックします。

次の情報が表示されます。

- [Memory alarm last send time]：最後にメモリートラップを送信した時刻を表示します。

- [Memory Alarm Status]：メモリーアラームの状態を表示します。アラームには、ACTIVE、INACTIVE、INACTIVE_SOAKING、ACTIVE_SOAKING があります。設定されたホールド時間が経過するまで、アラームはソークされます。
- [Memory alarm raise time]：メモリーアラームが最後に作動した時刻を表示します。
- [Memory alarm clear time]：最後にメモリーアラームが解除された時刻を表示します。
- [Last statistics received]：AP から最後に統計レポートを受信した時刻を表示します。
- [Current CPU Usage]：報告された最新の CPU 使用率を表示します。
- [Average CPU Usage]：計算された平均 CPU 使用率を表示します。
- [Current Memory Usage]：報告された最新のメモリ使用量の割合を表示します。
- [Average Memory Usage]：計算された平均メモリ使用量を表示します。
- [Current window size]：ウィンドウサイズを表示します。ウィンドウサイズは、統計間隔をサンプリング間隔で割って計算されます。平均 CPU およびメモリ使用量は、ウィンドウサイズによって計算されます。
- [CPU alarm last send time]：CPU トラップが最後に送信された時刻を表示します。
- [CPU Alarm Status]：CPU アラームの状態を表示します。アラームには、ACTIVE、INACTIVE、INACTIVE_SOAKING、ACTIVE_SOAKING があります。設定されたホールド時間が経過するまで、アラームはソークされます。
- [CPU alarm raise time]：CPU アラームが最後に発生した時刻を表示します。
- [CPU alarm clear time]：CPU アラームが最後に解除された時刻を表示します。

ステップ 5 [OK] をクリックします。

アクセスポイントのリアルタイム統計の確認

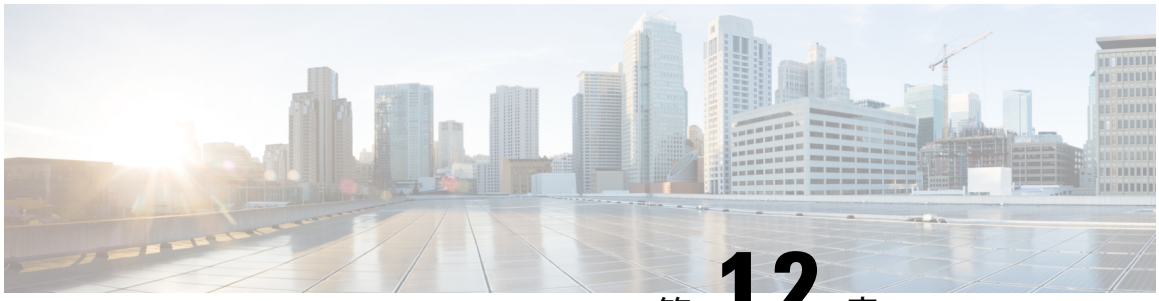
AP のリアルタイム統計を確認するには、**show ap config general | section AP statistics** コマンドを実行します。

```
Device# show ap config general | section AP statistics
!Last Statistics
AP statistics : Enabled
Current CPU usage : 4
Average CPU usage : 49
Current memory usage : 35
Average memory usage : 35
Last statistics received : 03/09/2021 15:25:08
!Statistics Configuration
Current window size : 1
Sampling interval : 30
Statistics interval : 300
AP statistics alarms : Enabled
!Alarm State - Active, Inactive, Inactive_Soaking, Inactive_Soaking
```

```
Memory alarm status : Active
Memory alarm raise time : 03/09/2021 15:24:29
Memory alarm clear time : NA
Memory alarm last send time : 03/09/2021 15:24:59
CPU alarm status : Inactive
CPU alarm raise time : 03/09/2021 15:24:25
CPU alarm clear time : 03/09/2021 15:25:05
CPU alarm last send time : 03/09/2021 15:25:05
!Alarm Configuration
Alarm hold time : 6
Alarm retransmission time : 30
Alarm threshold cpu : 30
Alarm threshold memory : 32
```

統計レポート期間を確認するには、**show ap config general | i Stats Reporting Period** コマンドを実行します。

```
Device# show ap config general | i Stats Reporting Period
Stats Reporting Period : 10
```



第 12 章

アクセスポイントタグの永続性

アクセスポイントタグの永続性に関する情報

Cisco IOS XE Bengaluru 17.6.1 以降では、AP タグの永続性がコントローラでグローバルに有効になります。タグの永続性が有効になっているコントローラに AP が接続すると、マッピングされたタグが AP に保存され、各 AP にタグの設定が個別に書き込まれることはありません。

AP タグの永続性の設定（GUI）

手順

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

ステップ 2 [AP] タブをクリックします。

ステップ 3 [Tag Source] タブで、[Enable AP Tag Persistency] チェックボックスをオンにして、AP タグの永続性をグローバルに設定します。

タグの永続性が有効になっているコントローラに AP が接続すると、マッピングされたタグが AP に保存され、タグの設定は各 AP に個別に書き込まれません。

ステップ 4 [Apply to Device] をクリックします。

次のタスク

AP にタグを保存します。

アクセスポイントでのタグの保存（GUI）

手順

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

ステップ 2 リストから AP をクリックします。
[Edit AP] ページが表示されます。

ステップ 3 [General] タブをクリックします。

ステップ 4 [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 5 [Policy] ドロップダウンリストから値を選択します。

ステップ 6 [Site] ドロップダウンリストから値を選択します。

ステップ 7 [RF] ドロップダウンリストから値を選択します。

ステップ 8 [Write Tag Config to AP] チェックボックスをオンにしてタグを AP にプッシュし、AP がコントローラ間で移動した場合でも、この情報を保存して記憶できるようにします。

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

アクセスポイントに保存されているタグの削除

手順

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

ステップ 2 AP のリストから AP をクリックします。
[Edit AP] ウィンドウが表示されます。

ステップ 3 [Edit AP] ウィンドウで、[Advanced] タブを選択します。

ステップ 4 [Set to Factory Default] セクションで、[Clear Resolved Tag Config] チェックボックスをオンにして、AP に保存されているタグをクリアします。

ステップ 5 [Update & Apply to Device] をクリックします。

AP タグの永続性の設定（CLI）

始める前に

プライマリコントローラから設定されたポリシータグ、サイトタグ、および RF タグを AP で保持するためには、それらのタグがその AP が接続する他のコントローラにも存在する必要が

あります。3 つのタグがすべて存在しない場合、AP はデフォルトのポリシータグ、サイトタグ、および RF タグを適用します。同様に、タグポリシーは、1 つまたは 2 つのタグが存在する場合でも適用されます。AP タグの永続性は、N+1 冗長性シナリオで AP をプライミングするのに役立ちます。タグの設定の詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_config_model.html を参照してください。

（注） 有効にすると、AP 接続中に AP タグの永続性が実行されるため、コントローラにすでに接続している AP がある場合、それらの AP はコントローラに再接続する必要があります。

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 persistency enable** **例：** `Device(config)# ap tag persistency enable`	AP タグの永続性を設定します。
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。

AP タグの永続性の確認

プライマリコントローラで AP タグの永続性を確認するには、次のコマンドを使用します。

```
Device# show ap tag summary
Number of APs: 1

AP Name          AP Mac           Site Tag Name          Policy Tag Name        RF Tag
Name             Misconfigured    Tag Source
-----------------------------------------------------------------------------------
Cisco01_AP       xxxx.xxxx.xxxx   default-site-tag       OpenRoaming
default-rf-tag          No               Static
```

（注） [Tag Source] に [Static] または [Filter] が表示されている場合は、AP タグマッピングがプライマリコントローラで設定されていることを意味します。ソースに [Default] が表示されている場合は、AP がコントローラに接続するときにデフォルトのタグを受信したことを意味します。

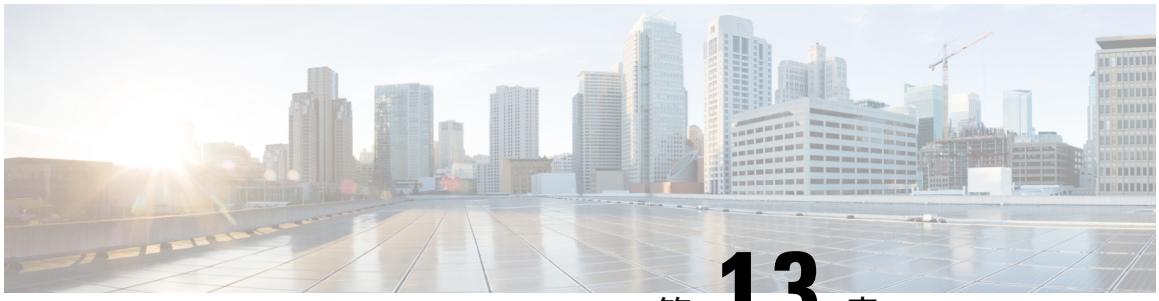
セカンダリコントローラで AP タグの永続性を確認するには、次のコマンドを使用します。

```
Device# show ap tag summary
Number of APs: 1

AP Name        AP Mac           Site Tag Name        Policy Tag Name     RF Tag Name
   Misconfigured   Tag Source
-------------------------------------------------------------------------------------------------
Cisco01_AP   xxxx.xxxx.xxxx    default-site-tag     OpenRoaming         default-rf-tag
    No              AP
```

（注） [Tag Source] に [AP] が表示されている場合は、ポリシータグ、サイトタグ、および RF タグがプライマリコントローラで設定されたものと一致しており、AP タグがコントローラ間で保持されていることを意味します。

第 III 部

Radio Resource Management



第 13 章

Radio Resource Management

Radio Resource Management について

Radio Resource Management（RRM）ソフトウェアはdeviceに組み込まれており、ワイヤレスネットワークのリアルタイムでの無線周波数（RF）管理を一貫して行えるようにする組み込みのRFエンジニアとして機能します。RRMを使用すると、devicesは次の情報について、アソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- トラフィックの負荷：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- 干渉：他の 802.11 発信元から送られてくるトラフィック量。
- ノイズ：現在割り当てられているチャネルに干渉している 802.11 以外のトラフィック量。
- カバレッジ：接続されているすべてのクライアントの受信信号強度インジケータ（RSSI）と信号対雑音比（SNR）。
- その他：近くにあるアクセス ポイントの数。

RRM は次の機能を実行します。

- 無線リソースの監視
- 電力制御の送信
- チャネルの動的割り当て
- カバレッジ ホールの検出と修正

- RF グループ化

（注） AP が DCA チャネルのリストにないスタティック チャネルで動作している場合、RRM のグループ化は行われません。ネイバー探索プロトコル（NDP）は DCA チャネルでのみ送信されます。したがって、無線が DCA 以外のチャネルで動作している場合は、チャネルで NDP を受信しません。

無線リソースの監視

RRM は、ネットワークに追加された新しいdevicesや Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントでは、使用国で有効なすべての チャネルをスキャンできます。また、他の地域で使用可能なチャネルも同様です。ローカル モードのアクセス ポイントは、これらのチャネルのノイズと干渉を監視するために、最大で 70 ミリ秒の間「オフチャネル」になります。 不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

（注） 音声トラフィックやその他の重要なトラフィックがある場合（過去 100 ミリ秒内）、アクセス ポイントはオフチャネル測定を延期できます。また、アクセス ポイントは、WLAN スキャン プライオリティの設定に基づいてオフチャネルの測定を延期します。

各アクセス ポイントがオフチャネルになるのはすべての時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。

送信電力の制御

デバイスは、リアルタイムのワイヤレス LAN 状況に基づいて、アクセスポイントの送信電力を動的に制御します。

伝送パワー コントロール（TPC）アルゴリズムによって、RF 環境での変化に応じて、アクセス ポイントの電力が増減します。多くの場合、TPC は干渉を低減させるため、アクセス ポイントの電力を下げようとします。しかし、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になったりして、RF カバレッジに急激な変化が発生すると、TPC は周囲のアクセスポイントで電力を上げることもあります。この機能は、主にクライアントと関係があるカバレッジ ホールの検出とは異なります。TPC はアクセス ポイント間におけるチャネルの干渉を回避しながら、必要なカバレッジ レベルを達成するために、十分な RF 電力を提供します。TPCv1 を選択することをお勧めします。 TPCv2 オプションは廃止されます。TPCv1 では、チャネル認識モードを選択できます。5 GHz の場合はこのオプションを選択し、2.4 GHz の場合はオフのままにすることをお勧めします。

最小/最大送信電力の設定による TPC アルゴリズムの無効化

TPC アルゴリズムは、数多くのさまざまな RF 環境で RF 電力を分散させます。ただし、自動電力制御では、アーキテクチャの制限事項やサイトの制限事項のため、適切な RF 設計を実装できなかった一部のシナリオは解決できない可能性があります。たとえば、すべてのアクセスポイントを互いに近づけて中央の廊下に設置する必要があるが、建物の端までカバレッジが必要とされる場合などです。

このようなケースでは、最大および最小の送信電力制限を設定し、TPCの推奨を無効化することができます。最大および最小の TPC 電力設定は、RF ネットワークの RF プロファイルを通じてすべてのアクセス ポイントに適用されます。

[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定するには、[Tx Power Control] ウィンドウのフィールドに、RRM で使用される最大および最小の送信電力を入力します。これらのパラメータの範囲は -10 ～ 30 dBm です。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRM では、コントローラに接続されているすべてのアクセスポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC またはカバレッジホールの検出のどちらで設定されるかは関係ありません）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限り、アクセス ポイントが 11 dBm を上回って伝送を行うことはありません。

チャネルの動的割り当て

同じチャネル上の2つの隣接するアクセスポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突の場合、アクセス ポイントではデータが受信されません。この機能は問題になることがあります。たとえば、誰かがカフェで電子メールを読むことで、近隣の会社のアクセスポイントのパフォーマンスに影響が及ぶような場合です。これらがまったく別のネットワークであっても、チャネル1を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。Devicesはアクセス ポイント チャネル割り当てを動的に割り当てて、衝突を回避し、キャパシティとパフォーマンスを改善することができます。チャネルは、希少な RF リソースの浪費を防ぐために再利用されます。つまり、チャネル1はカフェから離れた別のアクセスポイントに割り当てられます。これは、チャネル1をまったく使用しない場合に比べてより効率的です。

deviceの動的チャネル割り当て（DCA）機能は、アクセス ポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、チャネル 1 とチャネル 2 など、802.11b/g 帯域でオーバーラップする 2 つのチャネルは、同時に 11 または 54 Mbps を使用できません。deviceは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離します。

（注） 非オーバーラップ チャネル（1、6、11 など）だけを使用することをお勧めします。

（注） チャネルの変更時に、無線をシャットダウンする必要はありません。

deviceは、さまざまなリアルタイムの RF 特性を検証して、次のようにチャネルの割り当てを効率的に処理します。

- アクセスポイントの受信エネルギー：各アクセスポイントとその近隣のアクセスポイント間で測定された受信信号強度。チャネルを最適化して、ネットワーク キャパシティを最大にします。
- ノイズ：ノイズによって、クライアントおよびアクセスポイントの信号の品質が制限されます。ノイズが増加すると、有効なセル サイズが小さくなり、ユーザー エクスペリエンスが低下します。deviceでは、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- 802.11 干渉：干渉とは、不正アクセスポイントや隣接するワイヤレスネットワークなど、ワイヤレス LAN に含まれない 802.11 トラフィックのことです。Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。802.11 干渉の量が定義済みの設定可能なしきい値（デフォルトは 10 %）を超えると、アクセス ポイントからdeviceにアラートが送信されます。その場合、deviceでは、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステムパフォーマンスを向上させることができます。このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセス ポイントが原因で使用できないチャネルにアクセス ポイントを割り当てたままにしておくよりも効果的です。

  また、他のワイヤレス ネットワークがある場合、deviceは、他のネットワークを補足するようにチャネルの使用を変更します。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャネル 1 または 11 に割り当てられます。この調整によって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルにキャパシティがほとんど残っていない場合、deviceはそのチャネルを回避できます。すべての非オーバーラップ チャネルが使用される非常に大規模な展開では、deviceでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。
- 負荷および利用率：利用率の監視が有効な場合、たとえば、ロビーとエンジニアリングエリアを比較して、一部のアクセスポイントが他のアクセスポイントよりも多くのトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。deviceは、パフォーマンスが最も低いアクセスポイントを改善するようにチャネルを割り当てることができます。チャネル構造を変更する際には、負荷を考慮して、現在ワイヤレス LAN に存在するクライアントへの影響を最小限に抑えるようにします。このメトリックによって、すべてのアクセスポイントの送信パケットおよび受信パケットの数が追跡されて、アクセス ポイントのビジー状態が測定されます。新しいクライアントは過負荷のアクセスポイントを回避し、別のアクセス ポイントにアソシエートします。*Load and utilization* パラメータはデフォルトでは無効になっています。

deviceは、このRF特性情報をRRMアルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、軟判定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。最終的には、3次元空間における最適なチャネル設定が実現します。この場合、上下のフロアにあるアクセスポイントが全体的な無線LAN設定において主要な役割を果たします。

（注） 動的周波数選択（DFS）が有効なAP環境では、DCAチャネルでUNII2チャネルオプションを有効にして、デュアル5 GHz無線で100 MHzの分離を許可していることを確認します。

RRMスタートアップ モードは、次のような状況で起動されます

- シングルdevice環境では、deviceをアップグレードしてリブートすると、RRMスタートアップ モードが起動します。
- マルチdevice環境では、RRMスタートアップ モードは、RFグループ リーダーが選定されてから起動されます。
- RRMスタートアップ モードはCLIからトリガーできます。

RRMスタートアップ モードは、100分間（10分間隔で10回繰り返し）実行されます。RRMスタートアップ モードの持続時間は、DCA間隔、感度、およびネットワーク サイズとは関係ありません。スタートアップ モードは、定常状態のチャネル計画に収束するための高感度な（環境に対するチャネルを容易かつ敏感にする）10回のDCAの実行で構成されます。スタートアップ モードが終了した後、DCAは指定した間隔と感度で実行を継続します。

（注） DCAアルゴリズム間隔は1時間に設定されますが、DCAアルゴリズムは常に10分間隔（デフォルト）で実行されます。最初の10サイクルでは10分ごとにチャネル割り当てが行われ、チャネルの変更は、DCAアルゴリズムに従って10分ごとに行われます。その後、DCAアルゴリズムは設定された時間間隔に戻ります。DCAアルゴリズム間隔は定常状態に従うため、DCA間隔とアンカー時間の両方に共通です。

（注） RFグループ メンバーで動的チャネル割り当て（DCA）/伝送パワーコントロール（TPC）がオフになっていて、RFグループ リーダーが自動に設定されている場合、メンバーのチャネルまたは送信パワーは、RFグループ リーダーで実行されるアルゴリズムに従って変更されます。

カバレッジ ホールの検出と修正

RRMカバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線LANの無線カバレッジの領域を検出することができます。この機能によって、Lightweightアクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）で Lightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントからdeviceに「カバレッジ ホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセスポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。device では、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジホールの場合、deviceでは、その特定のアクセスポイントの送信電力レベルを上げることによってカバレッジホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジホールがdeviceによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

無線リソース管理の制約事項

- AP の最大数をすでに保持している RF グループに AP が join しようとすると、デバイスはアプリケーションを拒否し、エラーをスローします。

RRM の設定方法

ネイバー探索タイプの設定（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。

ステップ 2	**ap dot11 {24ghz | 5ghz} rrm ndp-type {protected | transparent}**
	例：
	`デバイス(config)#ap dot11 24ghz rrm ndp-type protected`
	`デバイス(config)#ap dot11 24ghz rrm ndp-type transparent`
		ネイバー探索タイプを設定します。デフォルトでは、モードは「transparent」に設定されます。
		• [protected]：ネイバー探索タイプを「protected」に設定します。パケットが暗号化されます。
		• [transparent]：ネイバー探索タイプを「transparent」に設定します。パケットはそのまま送信されます。

	コマンドまたはアクション	目的
ステップ 3	**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。

送信電力制御の設定

送信電力制御のしきい値の設定（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。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm tpc-threshold** *threshold_value* 例： `デバイス(config)#ap dot11 24ghz rrm tpc-threshold -60`	自動電力割り当てのために RRM が使用する送信電力制御のしきい値を設定します。範囲は -80 ～ -50 です。
ステップ 3	**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。

送信電力レベルの設定（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。
ステップ 2	**ap dot11 {24ghz | 5ghz} rrm txpower**{*trans_power_level* | **auto** | **max** | **min** | **once**} 例：	802.11 の送信電力レベルを設定します。 • [trans_power_level]：送信電力レベルを設定します。

	コマンドまたはアクション	目的
	`Device(config)#ap dot11 24ghz rrm txpower auto`	• [auto]：自動 RF をイネーブルにします。 • [max]：最大自動 RF 送信電力を設定します。 • [min]：最小自動RF送信電力を設定します。 • [once]：自動 RF を一度だけイネーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

802.11 RRM パラメータの設定

高度な 802.11 チャネル割り当てパラメータの設定（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。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} 例： `デバイス(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	CleanAir のイベント駆動型 RRM パラメータを設定します。 • [High]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。 • [Low]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。 • [Medium]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。

	コマンドまたはアクション	目的

ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** { | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
	例：
	デバイス(config)#**ap dot11 24ghz rrm channel**
	dca interval 2
		802.11 帯域の動的チャネル割り当て（DCA）アルゴリズム パラメータを設定します。
		• ：DCA リストに追加するチャネル番号を入力します。
		• [anchor-time]：DCA のアンカー時間を設定します。範囲は 0 ～ 23 時間です。
		• [global]：すべての 802.11 Cisco AP の DCA モードを設定します。
		  • [auto]：自動 RF をイネーブルにします。
		  • [once]：自動 RF を一度だけイネーブルにします。
		• [interval]：DCA のインターバル値を設定します。値は 1、2、3、4、6、8、12、24 時間です。デフォルト値 0 は 10 分を意味します。
		• [min-metric]：DCA の最小 RSSI エネルギーメトリックを設定します。範囲は -100 ～ -60 です。
		• [sensitivity]：環境の変化に対する DCA 感度レベルを設定します。
		  • [high]：最高の感度を指定します。
		  • [low]：最低の感度を指定します。
		  • [medium]：中間の感度を指定します。

ステップ 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80**} 例： デバイス(config)#**ap dot11 5ghz rrm channel**	5 GHz 帯域のすべての 802.11 無線に対する DCA チャネル幅を設定します。チャネル幅を [20 MHz]、[40 MHz]、[80 MHz]、または [Best] に設定します。チャネル幅のデフォルト値は 20 MHz です。[Best] のデフォルト値は 80 MHz です。

	コマンドまたはアクション	目的
	dca chan-width best	制約を設定する場合は、事前にチャネル帯域幅を [Best] に設定します。
ステップ 5	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** 例： デバイス(config)#**ap dot11 24ghz rrm channel device**	802.11 チャネル割り当てで、非 Wi-Fi デバイスの継続的な回避を設定します。
ステップ 6	**ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign** 例： デバイス(config)#**ap dot11 24ghz rrm channel foreign**	チャネル割り当てで、外部 AP の 802.11 干渉の回避を設定します。
ステップ 7	**ap dot11** {**24ghz** | **5ghz**} **rrm channel load** 例： デバイス(config)#**ap dot11 24ghz rrm channel load**	チャネル割り当てで、Cisco AP の 802.11 負荷の回避を設定します。
ステップ 8	**ap dot11** {**24ghz** | **5ghz**} **rrm channel noise** 例： デバイス(config)#**ap dot11 24ghz rrm channel noise**	チャネル割り当てで、802.11 ノイズの回避を設定します。
ステップ 9	**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。

802.11 カバレッジ ホール検出の設定（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 dot11 {24ghz | 5ghz} rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **data fail-percentage 60**	データ パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンクデータパケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100% の範囲で設定します。 • [packet-count]：アップリンクデータパケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：データパケットの 802.11 最小受信カバレッジレベルを、-90 ～ -60 dBm の範囲で設定します。
ステップ 3	**ap dot11 {24ghz | 5ghz} rrm coverage exception global** 例外レベル 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **exception global 50**	802.11 Cisco AP のカバレッジ例外レベルを、0 ～ 100 % の範囲で設定します。
ステップ 4	**ap dot11 {24ghz | 5ghz} rrm coverage level global** *cli_min* 例外レベル 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **level global 10**	802.11 Cisco AP クライアントの最小例外を、1 ～ 75 の範囲で指定します。
ステップ 5	**ap dot11 {24ghz | 5ghz} rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **voice packet-count 10**	音声パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100% の範囲で設定します。 • [packet-count]：アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。

	コマンドまたはアクション	目的
		• [rssi-threshold]：音声パケットの 802.11 最小受信カバレッジレベルを、-90 ～ -60 dBm の範囲で設定します。
ステップ 6	**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。

802.11 イベント ロギングの設定（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。

ステップ 2	**ap dot11 24ghz | 5ghz rrm logging {channel | coverage | foreign | load | noise | performance | txpower}**
	例：
	`デバイス(config)#ap dot11 24ghz rrm logging channel`
	`デバイス(config)#ap dot11 24ghz rrm logging coverage`
	`デバイス(config)#ap dot11 24ghz rrm logging foreign`
	`デバイス(config)#ap dot11 24ghz rrm logging load`
	`デバイス(config)#ap dot11 24ghz rrm logging noise`
	`デバイス(config)#ap dot11 24ghz rrm logging performance`
	`デバイス(config)#ap dot11 24ghz rrm logging txpower`
		各種パラメータに対するイベント ロギングを設定します。
		• [channel]：802.11 チャネル変更ロギング モードを設定します。
		• [coverage]：802.11 のカバレッジ プロファイル ロギング モードを設定します。
		• [foreign]：802.11 外部干渉プロファイル ロギング モードを設定します。
		• [load]：802.11 負荷プロファイル ロギング モードを設定します。
		• [noise]：802.11 ノイズ プロファイル ロギング モードを設定します。
		• [performance]：802.11 パフォーマンス プロファイル ロギング モードを設定します。
		• [txpower]：802.11 送信電力変更ロギング モードを設定します。

	コマンドまたはアクション	目的
ステップ 3	**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。

802.11 統計情報の監視の設定（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。
ステップ 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} 例： `デバイス(config)#ap dot11 24ghz rrm monitor channel-list all`	noise/interference/rogue などのパラメータに 802.11 監視チャネル リストを設定します。 • [all]：すべてのチャネルを監視します。 • [country]：設定された国コードで使用するチャネルを監視します。 • [dca]：動的なチャネル割り当てで使用されるチャネルを監視します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* 例： `デバイス(config)#ap dot11 24ghz rrm monitor coverage 600`	802.11 のカバレッジ測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* 例： `デバイス(config)#ap dot11 24ghz rrm monitor load 180`	802.11 負荷測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* 例：	802.11 のノイズ測定間隔（チャネル スキャン間隔）を、60 ～ 3600 秒の範囲で設定します。

	コマンドまたはアクション	目的
	デバイス(config)#**ap dot11 24ghz rrm monitor noise 360**	
ステップ 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* 例： デバイス(config)#**ap dot11 24ghz rrm monitor signal 480**	802.11 の信号測定間隔（ネイバーパケットの頻度）を、60 ～ 3600 秒の範囲で設定します。
ステップ 7	**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。

802.11 パフォーマンス プロファイルの設定（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。
ステップ 2	**ap dot11** {**24ghz | 5ghz**} **rrm profile clients** *cli_threshold_value* 例： Device(config)#**ap dot11 24ghz rrm profile clients 20**	802.11 Cisco AP クライアント数のしきい値を、1 ～ 75 の範囲で設定します。
ステップ 3	**ap dot11** {**24ghz | 5ghz**}**rrm profile foreign** *int_threshold_value* 例： Device(config)#**ap dot11 24ghz rrm profile foreign 50**	802.11 外部干渉のしきい値を、0 ～ 100 % の範囲で設定します。
ステップ 4	**ap dot11** {**24ghz | 5ghz**} **rrm profile noise** *for_noise_threshold_value* 例： Device(config)#**ap dot11 24ghz rrm profile noise -65**	802.11 外部ノイズのしきい値を、-127 ～ 0 dBm の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 5	**ap dot11** {**24ghz** | **5ghz**} **rrm profile throughput** *throughput_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	802.11 Cisco AP スループットのしきい値を、1000 ～ 10000000 バイト/秒の範囲で設定します。
ステップ 6	**ap dot11** {**24ghz** | **5ghz**} **rrm profile utilization** *rf_util_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile utilization 75`	802.11 RF 使用率のしきい値を、0 ～ 100% の範囲で設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

高度な 802.11 RRM の設定

チャネル割り当ての有効化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel-update** 例： `デバイス# ap dot11 24ghz rrm channel-update`	シスコ アクセス ポイントごとに 802.11 チャネル選択の更新を有効にします。 （注） **ap dot11 {24ghz | 5ghz} rrm channel-update** を有効にすると、DCA アルゴリズムのチャネル割り当てに対してトークンが割り当てられます。

DCA 動作の再開

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm dca restart** 例： `デバイス# ap dot11 24ghz rrm dca restart`	802.11 無線の DCA サイクルを再開します。

電力割り当てパラメータの更新（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm txpower update** 例： `デバイス# ap dot11 24ghz rrm txpower update`	各シスコ アクセス ポイントの 802.11 送信電力を更新します。

RF グループ内の不正アクセス ポイント検出の設定

RF グループ内の不正アクセス ポイント検出の設定（CLI）

始める前に

RF グループ内の各組み込みコントローラに同じ RF グループ名が設定されていることを確認します。

（注） この名前は、すべてのビーコン フレーム内の認証 IE を確認するために使用されます。組み込みコントローラに異なる名前が設定されている場合は、誤アラームが生成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	例： デバイス#	組み込みコントローラに接続されたすべてのアクセスポイントについて、次の手順を実行します。 • [monitor]：AP モードをモニターモードに設定します。 • [clear]：AP モードをサイトに基づいてローカルまたはリモートにリセットします。 • [sensor]：AP モードをセンサーモードに設定します。 • [sniffer]：AP モードをワイヤレススニファモードに設定します。
ステップ 2	**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。
ステップ 3	**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 4	**wireless wps ap-authentication** 例： `デバイス (config)# wireless wps ap-authentication`	不正なアクセスポイントの検出をイネーブルにします。
ステップ 5	**wireless wps ap-authentication threshold** *value* 例： `デバイス (config)# wireless wps ap-authentication threshold 50`	不正アクセス ポイント アラームが生成されるタイミングを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

	コマンドまたはアクション	目的
		しきい値の有効範囲は 1 ～ 255 で、デフォルトのしきい値は1です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。 （注） RF グループ内のすべての組み込みコントローラで、不正アクセスポイントの検出としきい値を有効にします。 （注） 不正アクセスポイントの検出が有効になっていない組み込みコントローラが RF グループ内にある場合、この機能が無効になっている組み込みコントローラ上のアクセスポイントは不正アクセスポイントとして報告されます。

RRM パラメータと RF グループ ステータスの監視

RRM パラメータの監視

表 *14 :* 無線リソース管理を監視するためのコマンド

コマンド	説明
show ap dot11 24ghz channel	802.11b チャネル割り当ての設定および統計情報を表示します。
show ap dot11 24ghz coverage	802.11b カバレッジの設定と統計情報を表示します。
show ap dot11 24ghz group	802.11b グループ化の設定と統計情報を表示します。
show ap dot11 24ghz logging	802.11b イベント ロギングの設定と統計情報を表示します。
show ap dot11 24ghz monitor	802.11b モニタリングの設定および統計情報を表示します。
show ap dot11 24ghz profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
show ap dot11 24ghz summary	802.11b Cisco AP の設定と統計情報を表示します。
show ap dot11 24ghz txpower	802.11b 送信電力制御の設定と統計情報を表示します。

コマンド	説明
show ap dot11 5ghz channel	802.11a チャネル割り当ての設定および統計情報を表示します。
show ap dot11 5ghz coverage	802.11a カバレッジの設定と統計情報を表示します。
show ap dot11 5ghz group	802.11a グループ化の設定と統計情報を表示します。
show ap dot11 5ghz logging	802.11a イベント ロギングの設定と統計情報を表示します。
show ap dot11 5ghz monitor	802.11a モニターリングの設定および統計情報を表示します。
show ap dot11 5ghz profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
show ap dot11 5ghz summary	802.11a Cisco AP の設定と統計情報を表示します。
show ap dot11 5ghz txpower	802.11a 送信電力制御の設定と統計情報を表示します。

RF グループ ステータスの確認（CLI）

ここでは、RF グループ ステータスの新しいコマンドについて説明します。

次のコマンドを使用して、 の RF グループ ステータスを確認できます。

表 *15*：アグレッシブ ロード バランシング コマンドの確認

コマンド	目的
show ap dot11 5ghz group	802.11a RF ネットワークの RF グループ リーダーであるコントローラの名前が表示されます。
show ap dot11 24ghz group	802.11b/g RF ネットワークの RF グループ リーダーであるコントローラの名前が表示されます。

例：RF グループの設定

次に、RF グループ名を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless rf-network test1
デバイス(config)# ap dot11 24ghz shutdown
デバイス(config)# end
デバイス # show network profile 5
```

次に、RF グループ内の不正アクセス ポイントの検出を設定する例を示します。

```
デバイス#
```

```
デバイス# end
デバイス# configure terminal
デバイス(config)# wireless wps ap-authentication
デバイス(config)# wireless wps ap-authentication threshold 50
デバイス(config)# end
```

ED-RRM について

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir のイベント駆動型 RRM 機能を使用すると、電波品質（AQ）に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセス ポイントに対してチャネル変更がただちに行われます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。

Cisco ワイヤレス LAN コントローラでの ED-RRM の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、イベント駆動型無線リソース管理（RRM）の実行がトリガーされるよう設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** ：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM パラメータを設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM 感度を設定します。デフォルトの選択は、Medium です。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**：不正な寄与を有効にします。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution duty-cycle** *thresholdvalue*：不正な寄与のしきい値を設定します。値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

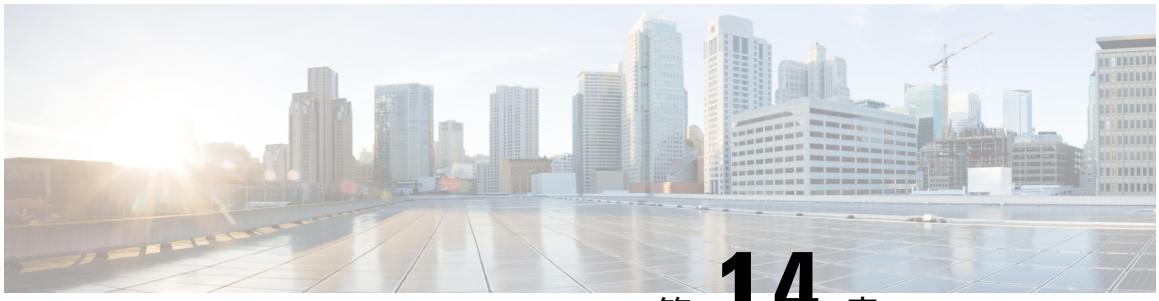
ステップ 2 次のコマンドを入力して、変更を保存します。

write memory

ステップ 3 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークに対する CleanAir の設定を確認します。

show ap dot11 {**24ghz** | **5ghz**} **cleanair config**

以下に類似した情報が表示されます。



第 14 章

カバレッジ ホール検出

カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線 LAN の無線カバレッジの領域を検出することができます。この機能によって、Lightweight アクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）で Lightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントからdeviceに「カバレッジ ホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセス ポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。device では、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジ ホールの場合、deviceでは、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジ ホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジ ホールがdeviceによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

カバレッジ ホールの検出の設定（GUI）

クライアント アカウンティングを設定するには、次の手順に従います。

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** をクリックします。

このページでは、802.11 a/n/ac（5 GHz）および 802.11 b/g/n（2.4 GHz）無線の無線リソース管理パラメータと、フレキシブル ラジオ アサインメントのパラメータを設定できます。

ステップ 2 [Enable Coverage Hole Detection] チェックボックスをオンにします。

カバレッジ ホール検出を有効にします。

カバレッジ ホール検出の設定（CLI）

カバレッジホール検出（CHD）は、APによって監視されるアップストリームのRSSIメトリックに基づきます。

CHD を設定するには、次の手順に従います。

始める前に

設定を適用する前に、802.11 ネットワークを無効にしてください。

手順

	コマンドまたはアクション	目的

ステップ 1	**ap dot11 {24ghz | 5ghz} rrm coverage data** {**fail-percentage | packet-count | rssi-threshold**}
	例：
	`Device(config)# ap dot11 24ghz rrm coverage`
	`data fail-percentage 60`
		データ パケットの 802.11 カバレッジ レベルを設定します。
		• [fail-percentage]：アップリンクデータパケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100% の範囲で設定します。
		• [packet-count]：アップリンクデータパケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。
		• [rssi-threshold]：データパケットの 802.11 最小受信カバレッジレベルを、-90 ～ -60 dBm の範囲で設定します。

ステップ 2	**ap dot11 {24ghz | 5ghz} rrm coverage exception global** 例外レベル
	例：
	`Device(config)# ap dot11 24ghz rrm coverage`
	`exception global 50`
		802.11 Cisco AP のカバレッジ例外レベルを、0 ～ 100 % の範囲で設定します。

	コマンドまたはアクション	目的

ステップ 3	**ap dot11{24ghz | 5ghz}rrm coverage level global** *cli_min* 例外レベル
	例：
	`Device(config)# ap dot11 24ghz rrm coverage`
	`level global 10`
		802.11 Cisco AP クライアントの最小例外を、1 ～ 75 の範囲で指定します。

ステップ 4	**ap dot11 {24ghz | 5ghz} rrm coverage voice** {**fail-percentage | packet-count | rssi-threshold**}
	例：
	`Device(config)# ap dot11 24ghz rrm coverage`
	`voice packet-count 10`
		音声パケットの 802.11 カバレッジ ホール検出を設定します。
		• [fail-percentage]：アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100% の範囲で設定します。
		• [packet-count]：アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。
		• [rssi-threshold]：音声パケットの 802.11 最小受信カバレッジレベルを、-90 ～ -60 dBm の範囲で設定します。

ステップ 5	**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。
ステップ 6	**show ap dot11 {24ghz | 5ghz} coverage** 例： `Device# show ap dot11 5ghz coverage`	CHD の詳細を表示します。

（注） 5 秒間で失敗したパケットの数と割合の両方が、**packet-count** および **fail-rate** コマンドに入力された値を超える場合、クライアントは事前アラーム状態にあると判断されます。コントローラでは、この情報を使用して、真のカバレッジ ホールと偽のカバレッジ ホールが区別されます。false positive は通常、大部分のクライアントに実装されているローミング ロジックが不適切であることが原因です。90 秒間で失敗したクライアントの数と割合の両方が、**coverage level global** および **coverage exception global** コマンドで入力された値を満たすか、これを超えている場合、カバレッジ ホールが検出されます。コントローラでは、カバレッジ ホールが修正可能かどうかが判断され、適切な場合は、その特定のアクセス ポイントの送信電力 レベルを上げることによってカバレッジ ホールが解消されます。

RF タグ プロファイルの CHD の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2 [Coverage] タブで、[Enable Coverage Hole Detection] チェックボックスをオンにします。

ステップ 3 [Data Packet Count] フィールドに、データ パケットの数を入力します。

ステップ 4 [Data Packet Percentage] フィールドに、データ パケットの割合を入力します。

ステップ 5 [Data RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm です。デフォルト値は -80 dBm です。

ステップ 6 [Voice Packet Count] フィールドに、音声データ パケットの数を入力します。

ステップ 7 [Voice Packet Percentage] フィールドに、音声データ パケットの割合を入力します。

ステップ 8 [Voice RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm です。デフォルト値は -80 dBm です。

ステップ 9 [Minimum Failed Client per AP] フィールドに、信号対雑音比（SNR）がカバレッジしきい値より低い AP 上の最小クライアント数を入力します。値の範囲は 1 ～ 75 で、デフォルト値は 3 です。

ステップ 10 [Percent Coverage Exception Level per AP] フィールドに、目的のカバレッジしきい値未満で動作しているアクセス ポイントの無線上におけるクライアントの最大必要割合を入力し、[Apply] をクリックします。値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

ステップ 11 [Apply] をクリックします。

RF プロファイルの CHD の設定（CLI）

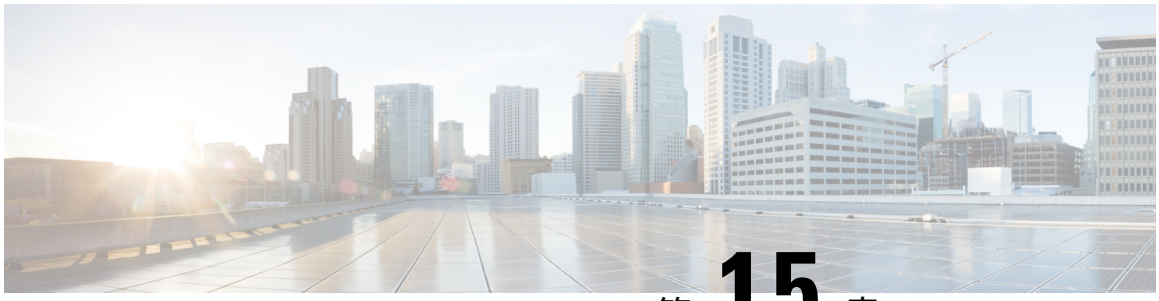
RF プロファイルのカバレッジホール検出（CHD）を設定するには、次の手順を実行します。

始める前に

RF プロファイルがすでに作成されていることを確認します。

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 dot11** {**24ghz** | **5ghz** } **rf-profile** *rf-profile-tag* 例： `Device(config)# ap dot11 24ghz rf-profile alpha-rfprofile-24ghz`	データ パケットの 802.11 カバレッジ ホール検出を設定します。
ステップ 3	**coverage data rssi threshold** *threshold-value* 例： `Device(config-rf-profile)# coverage data rssi threshold -80`	アクセス ポイントが受信したデータ パケットの最小 RSSI 値を設定します。有効な値の範囲は -90 ～ -60 dBm です。
ステップ 4	**end** 例： `Device(config-rf-profile)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ap dot11 24ghz rf-profile summary** 例： `Device# show ap dot11 24ghz rf-profile summary`	使用可能な RF プロファイルのサマリーを表示します。



第 15 章

シスコ フレキシブル ラジオ アサインメント

フレキシブル ラジオ アサインメントについて

フレキシブル ラジオ アサインメント（FRA）は、AP に含まれるデュアルバンド無線を利用します。FRA は、ネイバー探索プロトコル（NDP）の測定値を分析するために RRM に追加された新機能で、ネットワークにおける新しいフレキシブルラジオ（2.4 GHz、5 GHz、またはモニター）の役割を決定するために使用されるハードウェアを管理します。

従来のレガシーデュアルバンド AP では、常に無線スロットが 2 つあり（帯域ごとに 1 スロットずつ）、サービスを提供している帯域別に整理されていました（スロット 0 = 802.11b/g/n、スロット 1 = 802.11a/n/ac）。

2.4 GHz または 5 GHz 帯域での XOR サポート

フレキシブル ラジオ（XOR）は、2.4 GHz または 5 GHz 帯域の利用、もしくは同一 AP 上での両帯域の受動的な監視機能を提供します。提供される AP モデルはデュアル 5 GHz 帯の動作に対応できるように設計されており、専用のマクロ/マイクロ アーキテクチャをサポートする Cisco AP「i」モデルと、マクロ/マクロ アーキテクチャをサポートする「e」および「p」モデルがあります。

内部アンテナ（「i」シリーズ モデル）で FRA を使用すると、2 つの 5 GHz 無線をマイクロ/マクロ セル モードで使用できます。外部アンテナ（「e」モデルと「p」モデル）で FRA を使用すると、2 つの完全に分離したマクロ セル（ワイド エリア セル）または 2 つのマイクロ セル（スモール セル）を作成できるようにアンテナを配置し、HDX または任意の組み合わせを実現できます。

FRA は、2.4 Ghz 無線の冗長性の測定値の計算や維持を行い、COF（Coverage Overlap Factor）と呼ばれる新しい測定メトリックとして示します。

この機能は既存の RRM に統合され、レガシー AP との混在環境で動作します。「AP モード」の選択では、AP 全体（スロット 0 およびスロット 1）が、以下を含む複数の動作モードのいずれかに設定されます。

- ローカルモード
- モニターモード
- FlexConnect モード
- スニファモード
- Spectrum Connect モード

XOR が導入される前は、AP のモードを変更すると、 AP 全体、つまり両方の無線スロット 0 およびスロット 1 に変更が伝達されていました。スロット 0 の位置に XOR 無線を追加することで、1 つの無線インターフェイスを以前のモードの多くで動作させることができ、AP 全体を 1 つのモードに配置する必要がなくなりました。この概念を 1 つの無線レベルに適用する場合、「ロール」と呼ばれます。現在は次の 3 つのロールを割り当てることができます。

- クライアント サービス モード
- 2.4 GHz（1）または 5 GHz（2）
- Monitor-Monitor モード（3）

（注）
- 「モード」：AP 全体（スロット 0 とスロット 1）に割り当てられます。
- 「ロール」：単一の無線インターフェイス（スロット 0）に割り当てられます。

FRA の利点

- 2.4 GHz 過剰カバレッジの問題を解決。
- 2 つの異なる 5-GHz セルを作成して使用可能な通信時間を倍増。
- 1 つのイーサネット ドロップを持つ 1 つの AP が 2 つの 5 GHz AP のように機能可能。
- 通信時間を効率化させるためのマクロ/マイクロセルの概念の導入。
- より大きなカバレッジ セル内の 1 つのエリアにより多くの帯域幅を適用可能。
- 非線形トラフィックの処理に使用可能。
- 1 つの AP での High Density Experience（HDX）の向上。
- 対応するユーザーが XOR 無線をバンドサービスクライアントモードまたはモニターモードで選択可能。

FRA 無線の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `デバイス# 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 3	**[no] ap fra** 例： `デバイス(config)# [no] ap fra`	AP 上で FRA を有効または無効にします。
ステップ 4	**ap fra interval** 例： `デバイス(config)# ap fra interval 3`	FRA の間隔を時間単位で設定します。範囲は 1 ～ 24 時間です。 （注） FRA 間隔は、設定済みの RRM 間隔よりも長くする必要があります。
ステップ 5	**ap fra sensitivity** {**high** | **medium** | **low**} 例： `デバイス(config)# ap fra sensitivity high`	FRA 感度を設定します。 • **high**：FRA カバレッジのオーバーラップ感度を **high** に設定します。 • **medium**：FRA カバレッジのオーバーラップ感度を **medium** に設定します。 • **low**：FRA カバレッジのオーバーラップ感度を **low** に設定します。
ステップ 6	**end** 例： `デバイス(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。
ステップ 7	**ap fra revert** {**all** | **auto-only**}{**auto** | **static**} 例： `デバイス# ap fra revert all auto`	XOR 無線状態をロールバックします。 • **all**: すべての XOR 無線を元に戻します。

	コマンドまたはアクション	目的
		• **auto-only**：現在自動バンド選択になっているXOR無線のみを元に戻します。 • **auto**：XOR無線を自動バンド選択モードに設定します。 • **static**：XOR無線を静的2.4 GHz帯域に設定します。
ステップ 8	**show ap dot11** {**24ghz** | **5ghz**} **summary** 例： デバイス# **show ap dot11 5ghz summary**	802.11 Cisco APの構成と統計を表示します。
ステップ 9	デバイス# **show ap fra** 例： デバイス# **show ap fra** FRA State : Disabled FRA Sensitivity : medium (95%) FRA Interval : 1 Hour(s) AP Name MAC Address Slot ID Current-Band COF % Suggested Mode AP00A6.CA36.295A 006b.f09c.8290 0 2.4GHz None 2.4GHz COF : Coverage Overlap Factor test_machine#	現在のFRA構成を表示します。
ステップ 10	**show ap name** *ap-name* **config dot11 dual-band** 例： デバイス# **show ap name config dot11 dual-band**	特定のAPにおける現在の802.11デュアルバンドパラメータを表示します。

FRA 無線の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** > **[FRA]** を選択します。

ステップ 2 [Flexible Radio Assignment] ウィンドウで、FRA ステータスを有効にし、各 AP の重複する 2.4 GHz または 5 GHz カバレッジを確認し、[FRA Status] フィールドで [Enabled] を選択します。デフォルトでは、FRA ステータスは無効になっています。

ステップ 3 [FRA Interval]ドロップダウンリストで、[FRA run interval] を選択します。間隔の値の範囲は 1 ～ 24 時間です。FRA ステータスを有効にした後でのみ、[FRA run interval] の値を選択できます。

ステップ 4 [FRA Sensitivity]ドロップダウン リストで、無線を冗長と見なすために必要なカバレッジ オーバーラップ係数（COF）のパーセンテージを選択します。FRA ステータスを有効にした後にのみ、サポートされている値を選択できます。

次の値がサポートされています。

- [Low]：100%
- [Medium]（デフォルト）：95%
- [High]：90%

[Last Run] フィールドと [Last Run Time] フィールドには、FRA が最後に実行された時刻と、FRA が実行された時刻が表示されます。

ステップ 5 [Client Aware] チェックボックスをオンにして、冗長性に関する決定をします。

有効になっている場合、[Client Aware] 機能により、5 GHz の専用無線がモニターされ、クライアントの負荷が事前に設定されたしきい値を超えると、フレキシブル ラジオ アサインメントがモニターロールから 5 GHz のロールに自動的に変わり、オンデマンドでセルのキャパシティが効率的に倍増されます。容量の心配がなくなり、Wi-Fi の負荷が正常に戻ると、無線で前のロールが再開されます。

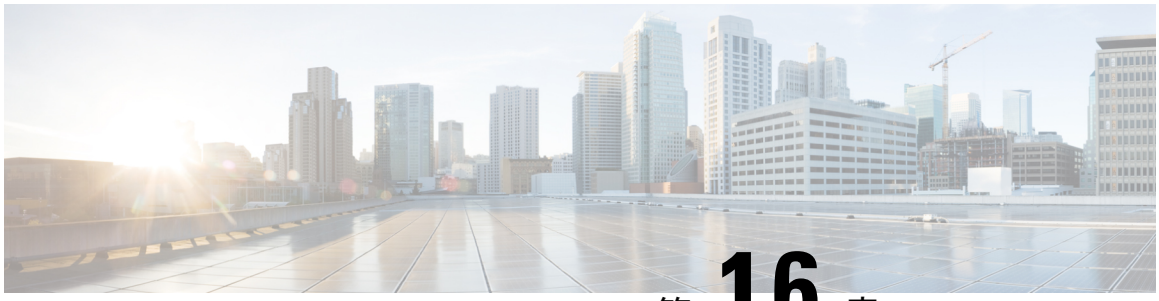
ステップ 6 [Client Select] フィールドに、クライアント選択の値を入力します。有効な値の範囲は 0 ～ 100% です。デフォルト値は 50% です。

つまり、専用の 5 GHz インターフェイスのチャネル使用率が 50% に達すると、モニターロールのデュアルバンド インターフェイスから 5 GHz クライアントサービスロールへの移行がトリガーされます。

ステップ 7 [Client Reset] フィールドに、クライアントのリセット値を入力します。有効な値の範囲は 0 ～ 100% です。デフォルト値は 5 パーセントです。

AP がデュアル 5 GHz AP として動作し始めると、この設定により、デュアルバンド無線をモニターロールにリセットするために必要な無線の合計チャネル使用率が減少します。

ステップ 8 [Apply] をクリックして、設定を保存します



第 16 章

XOR 無線サポート

デュアルバンド無線サポートについて

Cisco 2800、3800、4800、および 9120 シリーズの AP モデルのデュアルバンド（XOR）無線は、2.4 GHz または 5 GHz 帯域を利用、または同一 AP 上での両帯域を受動的に監視する機能を提供します。これらの AP は、クライアントに 2.4 GHz および 5 GHz 帯域でサービスを提供するように設定できます。または、メインの 5 GHz 無線がクライアントにサービスを提供しながら、フレキシブル無線で 2.4 GHz 帯と 5 GHz 帯の両方を順次スキャンします。

Cisco 9120 AP までの Cisco AP はデュアル 5 GHz 帯域の動作に対応できるように設計されており、専用のマクロ/マイクロアーキテクチャをサポートする i モデルと、マクロ/マクロをサポートする e および p モデルがあります。Cisco 9130AXI AP および Cisco 9136 AP はデュアル 5 GHz 動作をマイクロ/Messo セルとしてサポートします。

無線が帯域間を移動する場合（2.4 GHz から 5 GHz へ、またはその逆）、無線間で最適な分散を実現するには、クライアントをステアリングする必要があります。AP に 5 GHz 帯域の無線が 2 つある場合、フレキシブル ラジオ アサインメント（FRA）アルゴリズムに含まれるクライアント ステアリング アルゴリズムを使用して、同じ帯域の共存無線間でクライアントをステアリングします。

XOR 無線のサポートのステアリングは、手動または自動で行うことができます。

- 無線での帯域の手動ステアリング：XOR 無線の帯域は手動でのみ変更できます。
- 無線でのクライアントおよび帯域の自動ステアリングは、サイトの要件に従って帯域構成を監視および変更する FRA 機能によって管理されます。

（注） スロット 1 で静的チャネルが設定されている場合、RF 測定は実行されないため、デュアルバンド無線スロット 0 は 5 GHz 無線でのみ移動し、モニターモードには移動しません。

スロット 1 の無線が無効になっている場合、RF 測定は実行されず、デュアルバンド無線のスロット 0 は 2.4 GHz 無線のみになります。

デフォルトの XOR 無線サポートの設定

始める前に

（注） デフォルトの無線とは、スロット 0 でホストされている XOR 無線を指します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* 例： `デバイス# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	特定のシスコ アクセス ポイントの 802.11 デュアルバンド アンテナを設定します。 *antenna_gain_value*：有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** 例： `デバイス# ap name ap-name dot11 dual-band shutdown`	特定のシスコ アクセス ポイントでデフォルトのデュアルバンド無線をシャットダウンします。 無線を有効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band role manual client-serving** 例： `デバイス# ap name ap-name dot11 dual-band role manual client-serving`	シスコ アクセス ポイントでクライアント サービング モードに切り替えます。
ステップ 5	**ap name** *ap-name* **dot11 dual-band band 24ghz**	2.4 GHz 無線帯域に切り替えます。

	コマンドまたはアクション	目的
	例： `デバイス# ap name ap-name dot11 dual-band band 24ghz`	
ステップ 6	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} 例： `デバイス# ap name ap-name dot11 dual-band txpower 2`	特定のシスコアクセスポイントにおける無線の送信電力を設定します。 （注） FRA 対応無線（たとえば、9120 AP のスロット 0）が Auto に設定されている場合、この無線で静的チャネルと送信電力を設定することはできません。 この無線で静的チャネルと送信電力を設定する場合は、無線のロールを手動クライアントサービスモードに変更する必要があります。
ステップ 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* 例： `デバイス# ap name ap-name dot11 dual-band channel 2`	デュアルバンドのチャネルを入力します。 *channel-number*：有効な範囲は 1 ～ 173 です。
ステップ 8	**ap name** *ap-name* **dot11 dual-band channel auto** 例： `デバイス# ap name ap-name dot11 dual-band channel auto`	デュアルバンドの自動チャネル割り当てを有効にします。
ステップ 9	**ap name** *ap-name* **dot11 dual-band channel width**{**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} 例： `デバイス# ap name ap-name dot11 dual-band channel width 20 MHz`	デュアルバンドのチャネル幅を選択します。
ステップ 10	**ap name** *ap-name* **dot11 dual-band cleanair** 例： `デバイス# ap name ap-name dot11 dual-band cleanair`	デュアルバンド無線の Cisco CleanAir 機能を有効にします。

	コマンドまたはアクション	目的

ステップ 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz | 5 GMHz**}
	例：
	`デバイス# ap name ap-name dot11 dual-band cleanair band 5 GHz`
	`デバイス# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`
		Cisco CleanAir 機能の帯域を選択します。
		Cisco CleanAir 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。

ステップ 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A | B | C | D**} 例： `デバイス# ap name ap-name dot11 dual-band dot11n antenna A`	特定のアクセス ポイントの 802.11n デュアルバンドパラメータを設定します。
ステップ 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** 例： `デバイス# show ap name ap-name auto-rf dot11 dual-band`	シスコ アクセス ポイントの自動 RF 情報を表示します。
ステップ 14	**show ap name** *ap-name* **wlan dot11 dual-band** 例： `デバイス# show ap name ap-name wlan dot11 dual-band`	シスコアクセスポイントの BSSID のリストを表示します。

指定したスロット番号に対する XOR 無線サポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Access Points]** の順にクリックします。

ステップ 2 [Dual-Band Radios] セクションで、デュアルバンド無線を設定する AP を選択します。

AP の AP 名、MAC アドレス、CleanAir 機能、およびスロット情報が表示されます。HyperLocation 方式が HALO の場合は、アンテナの PID とアンテナの設計情報も表示されます。

ステップ 3 [Configure] をクリックします。

ステップ 4 [General] タブで、必要に応じて [Admin Status] を設定します。

ステップ 5 [CleanAir Admin Status] フィールドを [Enable] または [Disable] に設定します。

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

指定したスロット番号に対する XOR 無線サポートの設定

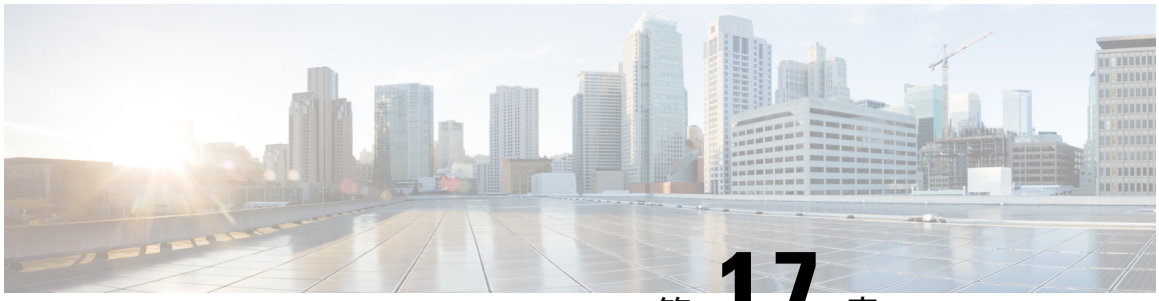
手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド アンテナを設定します。 *external_antenna_gain_value*：外部アンテナ ゲイン値（.5 dBi の倍数単位）。有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線の現在の帯域を設定します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド チャネルを設定します。 *channel_number*：有効な範囲は 1 ～ 165 です。
ステップ 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線の CleanAir 機能を有効にします。
ステップ 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	特定のアクセス ポイントのスロット 0 でホストされている 802.11n デュアルバンド パラメータを設定します。 ここで、各変数は次のように定義されます。

	コマンドまたはアクション	目的
		A：アンテナ ポート A を有効にします。 **B**：アンテナ ポート B を有効にします。 **C**：アンテナ ポート C を有効にします。 **D**：アンテナ ポート D を有効にします。
ステップ 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンドの役割を設定します。 デュアルバンドの役割は次のとおりです。 • **auto**：無線の役割を自動で選択することを指します。 • **manual**：無線の役割を手動で選択することを指します。

ステップ 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown**
	例：
	`デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown`
	`デバイス# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`
		特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線を無効にします。
		デュアルバンド無線を有効にするには、このコマンドの **no** 形式を使用します。

ステップ 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} 例： `デバイス# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	特定のアクセスポイントのスロット 0 でホストされている XOR 無線のデュアルバンド送信電力を設定します。 • *tx_power_level*：送信電力レベルを dBm 単位で示します。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。



第 17 章

シスコ レシーバのパケット開始

レシーバのパケット検出開始しきい値について

レシーバのパケット検出開始（Rx SOP）しきい値機能は、アクセス ポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。Wi-Fi レベルが上がると、無線の受信感度が下がり、レシーバのセル サイズが小さくなります。セル サイズの減少は、ネットワークのクライアントの分散に影響します。

RF リンクが脆弱なクライアント、つなぎっぱなしのクライアント、およびアクセス ポイント全体で負荷分散しているクライアントに対処するために Rx SOP が使用されます。Rx SOP は、アクセス ポイントが最も近くにある最も強力なクライアントを最適化する必要のあるスタジアムやホールなどの高密度展開でネットワーク性能を最大限引き出すのに役立ちます。

Rx SOP の制約事項

- Rx SOP 設定は Cisco Aironet シリーズ AP でプラグ着脱可能なサードパーティの無線モジュールには適用できません。
- Rx SOP 設定は、ローカル、FlexConnect、ブリッジ、および Flex + ブリッジモードでのみサポートされます。
- Rx SOP 設定は、FlexConnect + PPPoE、FlexConnect + PPPoE-wIPS、および FlexConnect + OEAP サブモードではサポートされていません。

次の表に、Rx SOP しきい値で許容される範囲を示します。

表 *16 : Rx SOP* しきい値

無線帯域	しきい値高	しきい値中	しきい値低
2.4 GHz	-79 dBm	-82 dBm	-85 dBm
5 GHz	-76 dBm	-78 dBm	-80 dBm

Rx SOP の設定（CLI）

手順

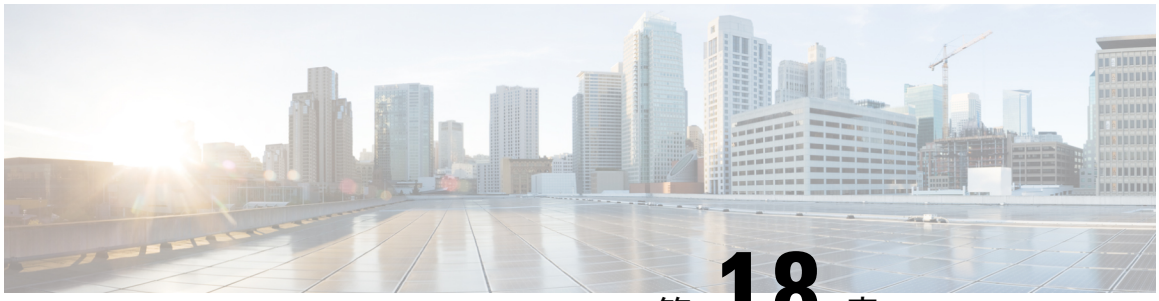
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {24ghz | 5ghz} rx-sop threshold {auto | custom | high | low | medium}** 例： デバイス(config)# **ap dot11 5ghz rx-sop threshold high**	802.11bg/802.11a 無線 Rx SOP しきい値を設定します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	**show ap dot11 {24ghz | 5ghz} high-density** 例： デバイス# **show ap dot11 5ghz high-density**	802.11bg/802.11a 高密度パラメータを表示します。
ステップ 5	**show ap summary** 例： デバイス# **show ap summary**	接続されたすべての Cisco AP のサマリーを表示します。

RF プロファイルのカスタマイズ（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： デバイス# **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** | **5ghz** } **rf-profile** *profile-name* 例： デバイス(config)# **ap dot11 24ghz rf-profile AHS_2.4ghz**	802.11a および 11b パラメータを設定します。
ステップ 3	**high-density rx-sop threshold {auto | custom | high | low | medium}** 例： デバイス(config-rf-profile)# **high-density rx-sop threshold high**	802.11bg、802.11a 高密度パラメータを設定します。
ステップ 4	**show ap summary** 例： デバイス# **show ap summary**	接続されたすべての Cisco AP のサマリーを表示します。
ステップ 5	end	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
		（注） • 無線モードに関係なく、コントローラは設定された RX-SOP 値で無線を設定します。AP により、設定された RX-SOP 値の使用の有無が決まります。 • XOR 無線（スロット 0）の場合、AP がモニターモードの場合、AP にプッシュされる RX-SOP 値は、モニターモードに移行する前に動作していた帯域に依存します（基本的に、無線動作帯域が24gの場合、RX-SOP パラメータは 24GHz RF プロファイル（またはデフォルトのRFプロファイル）から選択されます）。5gの場合は、AP 用に設定された 5GHz RFプロファイル（またはデフォルトのRFプロファイル）から選択された RX-SOP パラメータです。



第 18 章

クライアント リミット

クライアント リミットについて

この機能により、AP に関連付けることができるクライアントの数に制限が適用されます。さらに、各 AP 無線に関連付けることができるクライアントの数を設定できます。

WLAN ごとのクライアントリミットの設定（GUI）

手順

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

ステップ 2 WLAN のリストから WLAN をクリックします。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [Max Client Connections] 設定で、[Per WLAN]、[Per AP Per WLAN]、および [Per AP Radio Per WLAN] のクライアントリミットを入力します。

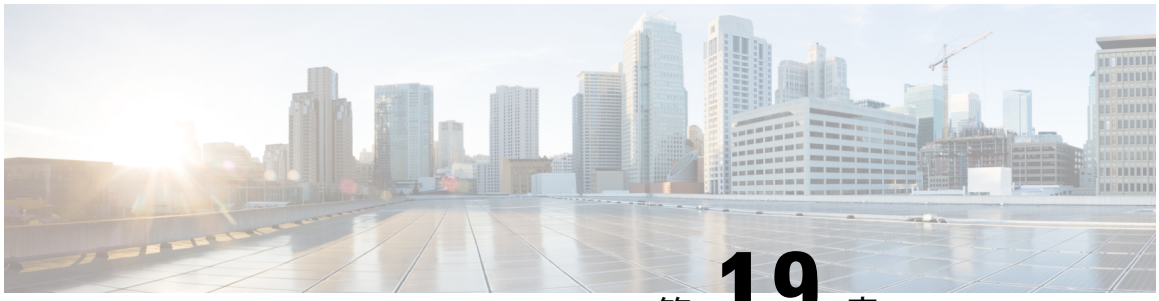
ステップ 5 [Update & Apply to Device] をクリックします。

WLAN あたりのクライアントリミットの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**wlan** *wlan-name* 例： `Device(config)# wlan ramban`	WLAN 名を指定します。
ステップ 4	**client association limit** *maximum-clients-per-WLAN* 例： `Device(config-wlan)# client association limit 110`	特定の WLAN に関連付けることができるクライアントの最大数を設定します。 （注） Cisco 組み込みワイヤレスコントローラ ネットワーク内のプライマリ AP によって、サポートされるクライアントの最大数が異なります。Cisco 組み込みワイヤレスコントローラ ネットワーク内における WLAN ごとのクライアント数制限の詳細については、表 17 : Cisco 組み込みワイヤレスコントローラ ネットワークでサポートされるスケール（302 ページ）を参照してください。 **表 *17 : Cisco* 組み込みワイヤレスコントローラ ネットワークでサポートされるスケール**
ステップ 5	**client association limit ap** *max-clients-per-AP-per-WLAN* 例： `Device(config-wlan)# client association limit ap 120`	WLAN 内の AP に関連付けることができるクライアントの最大数を設定します。

	コマンドまたはアクション	目的
ステップ 6	**client association limit radio** *max-clients-per-AP-radio-per-WLAN* 例： `Device(config-wlan)# client association limit radio 100`	WLAN 内の AP 無線に関連付けることができるクライアントの最大数を設定します。
ステップ 7	**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。
ステップ 8	**show wlan id** *wlan-id* 例： `Device#  show wlan id 2`	WLAN の現在の設定と、対応するクライアント関連付け制限を表示します。



第 19 章

IP 盗難

IP 盗難の概要

IP 盗難機能は、すでに別のデバイスに割り当てられている IP アドレスが使用されないようにします。2 つのワイヤレス クライアントが同じ IP アドレスを使用していることがコントローラによって検出された場合、コントローラは、優先順位が低い方のクライアントを IP 盗難者であると宣言し、他方のクライアントが継続できるようにします。ブロックリストが有効になっている場合、そのクライアントが除外リストに登録され、追放されます。

コントローラでは、IP 盗難機能がデフォルトで有効になっています。クライアント（データベース内の新規および既存のクライアント）の優先順位レベルも IP 盗難の報告に使用されます。優先順位レベルは、Dynamic Host Configuration Protocol（DHCP）、Address Resolution Protocol（ARP）、データ収集（クライアントがどの IP アドレスを使用しているかを示す IP データ パケットを調べる）などの学習タイプまたは学習ソースです。有線クライアントは、常に他よりも高い優先順位レベルになります。ワイヤレス クライアントが有線 IP の盗難を試みると、そのクライアントは盗難者であると宣言されます。

IPv4 クライアントの優先順位は次のとおりです。

1. DHCPv4
2. ARP
3. データ パケット

IPv6 クライアントの優先順位は次のとおりです。

1. DHCPv6
2. NDP

3. データ パケット

（注） 静的な有線クライアントは、DHCP よりも優先順位が高くなります。

IP 盗難の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** > **[Client Exclusion Policies]** を選択します。

ステップ 2 [IP Theft or IP Reuse] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックします。

IP 盗難の設定

IP 盗難機能を設定するには、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 wps client-exclusion ip-theft** 例： `Device(config)# wireless wps client-exclusion ip-theft`	クライアント除外ポリシーを設定します。

IP 盗難除外タイマーの設定

IP 盗難除外タイマーを設定するには、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`	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	**exclusionlist timeout** *time-in-seconds* 例： `Device(config-wireless-policy)# exclusionlist timeout 5`	タイムアウトを秒単位で指定します。有効な範囲は 0 ～ 2147483647 です。タイムアウトなしの場合は0を入力します。

IP 盗難設定の確認

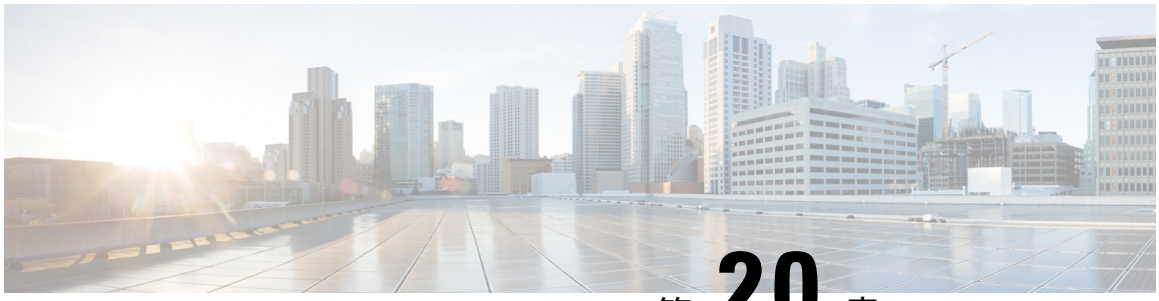
IP 盗難機能が有効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : Enabled
  Excessive 802.11-authentication failures: Enabled
  Excessive 802.1x-authentication         : Enabled
  IP-theft                                : Enabled
  Excessive Web authentication failure    : Enabled
  Cids Shun failure                       : Enabled
  Misconfiguration failure                : Enabled
  Failed Qos Policy                       : Enabled
  Failed Epm                              : Enabled
```

IP 盗難機能に関するその他の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method     Role
-------------------------------------------------------------------------------------
000b.bbb1.0001 SimAP-1                2    Run                11a      None       Local


Number of Excluded Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method
-------------------------------------------------------------------------------------
10da.4320.cce9 charlie2               2    Excluded           11ac     None
```

```
Device# show wireless device-tracking database ip

IP                              VLAN  STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------
  20.20.20.2                     20    Reachable   Local       001e.14cc.cbff
  20.20.20.6                     20    Reachable   IPv4 DHCP   000b.bbb1.0001


Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason               Time Remaining
-------------------------------------------------------------------------------------
10da.4320.cce9                         IP address theft                   59


Device# show wireless exclusionlist client mac 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : IP address theft
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```



第 20 章

不定期自動省電力配信

不定期自動省電力配信について

不定期自動省電力配信（U-APSD）は、モバイルクライアントのバッテリ寿命を延ばすQoS機能で、IEEE 802.11e で定義されています。この機能により、バッテリ寿命が延びるだけでなく、無線メディアで配信されるトラフィック フローの遅延時間が短縮されます。U-APSD では、クライアントはアクセスポイントでバッファされる個々のパケットをポーリングする必要がないため、単一のアップリンク トリガー パケットを送信して複数のダウンリンク パケットを配信することが可能になります。

WMM が有効化されると、U-APSD は自動的に有効化されます。

不定期自動省電力配信の確認（CLI）

手順

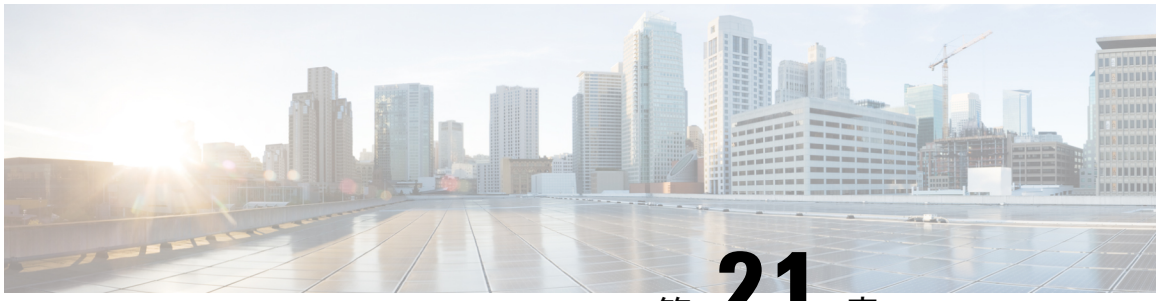
show wireless client mac-address *client_mac***detail**

例：

```
Device# show wireless client mac-address 2B:5B:B3:18:56:E9 detail
Output Policy State : Unknown
Output Policy Source : Unknown
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 15
  APSD ACs    : BK(T/D), BE, VI(T/D), VO(T/D)
Power Save : OFF
Current Rate :

--------------------------
BK : Background
BE : Best Effort
```

```
VI : Video
VO : Voice.

T: UAPSD Trigger Enabled
D: UAPSD Delivery Enabled
T/D : UAPSD Trigger and Delivery Enabled
```

クライアントの詳細情報を MAC アドレス別に表示します。



第 21 章

ターゲット起動時間

ターゲット起動時間

既存の Wi-Fi クライアントの省電力メカニズムは 802.11b 以降使用されており、クライアントデバイスは AP ビーコンまたは複数のビーコン間でスリープ状態になり、送信するデータがある場合にのみ起動します（AP はスリープ状態でないため、いつでも送信できます）。ビットマップである Delivery Traffic Indication Map（DTIM）を含むビーコンは、特定のクライアントに送信するためにバッファリングされたダウンリンクトラフィックが AP にあることを示します。

クライアントは、DTIM ビットが設定されている場合、省電力ポーリング（PS-Poll）フレームを AP に送信することにより、AP からデータを取得できます。この省電力スキームは効果的ですが、クライアントは短いビーコン間隔でしか休止できません。クライアントは AP のビーコンフレームから DTIM を読み取るために、1 秒間に数回起動する必要があります。

音声パケットは短い時間間隔（通常は 20 ミリ秒/秒）で送信されるため、802.11e では、音声対応 Wi-Fi デバイスを支援する新しい省電力メカニズムが導入されました。不定期自動省電力配信（U-APSD）により、省電力モードのクライアントはビーコン期間内に周期的にスリープ状態になることができます。AP は、クライアントが起動して配信を要求するまで、ダウンリンクトラフィックをバッファリングします。

（注） デフォルトでは、ターゲット起動時間（TWT）はコントローラで無効になっています。TWT を有効にするには、**ap dot11 {24ghz | 5ghz} dot11ax twt-broadcast** コマンドを実行します。

ターゲット起動時間を使用した省電力の拡張

ターゲット起動時間（TWT）により、APはWi-Fiネットワーク内のアクティビティを管理して、ステーション（STA）間の中程度の競合を最小限に抑え、省電力モードのSTAが起動するために必要な時間を短縮できます。これは、重複しない時間および周波数で動作するようにSTAを割り当て、事前定義されたサービス期間にフレーム交換を集中させることで実現されます。

TWT対応STAは、TWTスケジューリングAPと個別のTWTアグリーメントをネゴシエートするか、AP上に存在するブロードキャストTWTアグリーメントの一部またはメンバーになることを選択できます。STAは、TWTサービス期間（SP）を使用して他のSTAとフレームを交換できることを認識する必要はありません。TWT SP中に送信されるフレームは、そのTWT SPに対応するTWTアグリーメントを確立したSTAのペアによってサポートされる任意のPPDUフォーマットで伝送できます。これには、高効率マルチユーザー物理プロトコルデータユニット（HE MU PPDU）、高効率トリガーベース物理プロトコルデータユニット（HE TB PPDU）などが含まれます。

TWTアグリーメントの種類は次のとおりです。

個別 TWT

APとSTAの間で単一のTWTセッションがネゴシエートされます。これにより、APとSTA間のDLおよびULの特定のサービス期間が保証され、予想されるトラフィックは精度99%のネゴシエートされたSP内に限定されます。サービス期間は、ターゲットビーコンの送信時間（TBTT）からの特定のオフセットで始まり、SP期間中継続し、SP間隔ごとに繰り返されます。

TWT要求側STAは起動スケジュール情報をTWT応答側APに通信します。次に、APはスケジュールを作成し、両者の間でTWTアグリーメントが確立されたときにTWT値をTWT要求側STAに配信します。

要請 TWT

STAはAPとのTWTセッションを開始します。

未要請 TWT

APはSTAとのTWTセットアップを開始します。APは、STAによって受け入れられるサービス期間でTWT応答を送信します。

ブロードキャスト TWT

高効率APは、進行中のブロードキャストSPまたは新しいSPのいずれかでブロードキャストTWT操作に参加するようにSTAに要求します。

無線レベルでのターゲット起動時間の設定（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。
ステップ 2	**ap dot11** {**24ghz** | **5ghz** } **shutdown** 例： `Device(config)#ap dot11 24ghz shutdown`	802.11a または 802.11b ネットワークを無効にします。
ステップ 3	**ap dot11** {**24ghz** | **5ghz** } **dot11ax** 例： `Device(conf)#ap dot11 24ghz dot11ax`	802.11ax パラメータを設定します。
ステップ 4	**[no] ap dot11** {**24ghz** | **5ghz** } **dot11ax target-wakeup-time** 例： `Device(config)#ap dot11 24ghz dot11ax target-wakeup-time`	802.11ax ターゲット起動時間を設定します。
ステップ 5	**[no] ap dot11** {**24ghz** | **5ghz**} **dot11ax target-waste-time** 例： `Device(config)#ap dot11 24ghz dot11ax target waste-time`	802.11ax ターゲット消費時間を設定します。
ステップ 6	**no ap dot11** {**24ghz** | **5ghz** } **shutdown** 例： `Device(config)#no ap dot11 24ghz shutdown`	802.11a または 802.11b ネットワークを有効にします。
ステップ 7	**show ap dot11** {**24ghz** | **5ghz** } **network** 例： `Device(config)#show ap dot11 24ghz network`	ターゲット起動時間とターゲット起動時間ブロードキャストに関する情報を含む、802.11ax ネットワーク構成の詳細を表示します。

WLAN でのターゲット起動時間の設定

WLAN でのターゲット起動時間の有効化（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。
ステップ 2	**wlan** *wlan-profile* 例： `Device(config)# wlan wlan-profile`	WLAN コンフィギュレーション サブモードを開始します。wlan-profile は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device(conf-wlan)#shutdown`	WLAN ネットワークを無効にします。
ステップ 4	**dot11ax target-waketime** 例： `Device(conf-wlan)#dot11ax target-waketime`	WLAN のターゲット起動時間モードを設定します。
ステップ 5	**dot11ax twt-broadcast-support** 例： `Device(conf-wlan)#dot11ax twt-broadcast-support`	WLAN の TWT ブロードキャストのサポートを設定します。
ステップ 6	**no shutdown** 例： `Device(conf-wlan)#no shutdown`	WLAN を有効にします。

ステップ 7	**show wlan** {**all** | **id** | **name** | **summary**}
	例：
	`Device# show wlan all`
	`Device# show wlan id`
	`Device# show wlan name`
		ターゲット起動時間やターゲット起動時間ブロードキャストなど、設定された WLAN の詳細を表示します。

WLAN でのターゲット起動時間の無効化（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。
ステップ 2	**wlan** *profile-name* 例： `Device(config)# wlan wlan-profile`	WLAN コンフィギュレーション サブモードを開始します。wlan-profile は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device(conf-wlan)#shutdown`	WLAN ネットワークを無効にします。
ステップ 4	**no dot11ax target-waketime** 例： `Device(conf-wlan)#no dot11ax target-waketime`	WLAN のターゲット起動時間モードを無効にします。
ステップ 5	**no dot11ax twt-broadcast-support** 例： `Device(conf-wlan)#no dot11ax twt-broadcast-support`	WLAN の TWT ブロードキャストのサポートを無効にします。
ステップ 6	**no shutdown** 例： `Device(conf-wlan)#no shutdown`	WLAN を有効にします。

ターゲット起動時間の設定（GUI）

手順

ステップ 1 [Configuration] > [Radio Configuration] > [Parameters] の順に選択します。

パラメータページが表示され、5 GHz および 2.4 GHz 帯域無線のグローバルパラメータを設定できます。

ステップ 2 [11ax Parameters] セクションで、[Target Wakeup Time] チェックボックスと [Target Wakeup Time Broadcast] チェックボックスをオンにして、ターゲット起動時間とターゲット起動時間ブロードキャストを設定します。

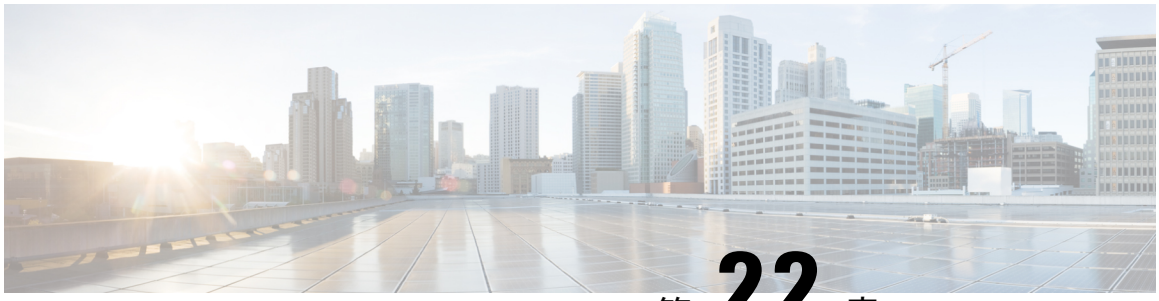
ターゲット起動時間の確認

ターゲット起動時間とターゲット起動時間ブロードキャストを確認するには、次のコマンドを使用します。

show ap dot11 24ghz network

次に、出力例を示します。

```
Device#show ap dot11 24ghz network
.
.
.
802.11ax                                : Enabled
Target Wakeup Time                      : Enabled
Target Wakeup Time Broadcast            : Enabled
.
.
.
```



第 22 章

アクセスポイントの USB ポートの有効化

アクセスポイントの電源としての USB ポート

一部の Cisco AP には、一部の USB デバイスの電源として機能する USB ポートがあります。最大電力は 2.5 W です。USB デバイスが 2.5 W を超える電力を取り出すと、USB ポートは自動的にシャットダウンにします。消費電力が 2.5 W 以下の場合、ポートは有効になっています。AP のデータシートを参照して、AP に電源として機能できる USB ポートがあるかどうかを確認してください。

（注） コントローラは、最後の 5 つの電力の超過引き出しインシデントをそのログに記録します。

⚠

注意 サポートされていない USB デバイスが Cisco AP に接続されている場合、次のメッセージが表示されます。

挿入された USB モジュールはサポート対象デバイスではありません。この USB デバイスの動作およびアクセス ポイントへの影響は保証されていません。シスコは、障害または欠陥が、顧客または再販業者が取り付けたサードパーティ製 USB モジュールを使用したことによるものと判断される場合、保証に基づくサポートまたは契約に基づくサポート プログラムの提供を差し控える場合があります。シスコのネットワーキング製品のサポートを提供する過程で、トラブルシューティングの目的で根本原因を診断する上でサードパーティ製の部品を取り外すことがシスコに役立つと判断した場合に、エンド ユーザーはシスコがサポートする USB モジュールを取り付けるように求められることがあります。また、シスコは、当該サービスを提供した後に、製品の欠陥の根本原因はサポート対象外のデバイスによるものだったとシスコが判断したときに、シスコは、お客様に提供されるサービスのその時点で最新の実費請求レートをお客様に請求する権利を留保します。

AP プロファイルの設定（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。
ステップ 2	**ap profile** *ap-profile* **例：** `デバイス(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	**usb-enable** **例：** `デバイス(config-ap-profile)# usb-enable`	各 AP プロファイルの USB を有効にします。 （注） デフォルトでは、各 AP プロファイルのUSBは有効になっています。

	コマンドまたはアクション	目的
		no usb-enable コマンドを使用して、各 AP プロファイルの USB を無効にします。
ステップ 4	**end** 例： デバイス(config-ap-profile)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

アクセスポイントの USB 設定の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス# **enable**	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **usb-module** 例： デバイス# **ap name AP44d3.xy45.69a1 usb-module**	AP の USB ポートを有効にします。 AP の USB ポートを無効にするには、**ap name** *ap-name* **no usb-module** コマンドを使用します。
ステップ 3	**ap name** *ap-name* **usb-module override** 例： デバイス# **ap name AP44d3.xy45.69a1 usb-module override**	AP プロファイルの USB ステータスをオーバーライドし、ローカル AP 設定を考慮します。 **ap name** *ap-name* **no usb-module override** コマンドを使用して AP の USB ステータスをオーバーライドし、AP プロファイルの設定を考慮します。 （注） USB オーバーライドを有効にした場合にのみ、対応する AP の USB ステータスを設定できます。

アクセスポイントの USB 構成の監視（CLI）

• AP のインベントリの詳細を表示するには、次のコマンドを使用します。

show ap name *ap-name* **inventory**

次に、出力例を示します。

```
Device# show ap name AP500F.8059.1620  inventory
NAME: AP2800    , DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP2802I-D-K9  ,  VID: 01,  SN: XXX1111Y2ZZZZ2800
NAME: SanDisk    , DESCR: Cruzer Blade
PID: SanDisk  ,  SN: XXXX1110010, MaxPower: 224
```

- AP モジュールのサマリーを表示するには、次のコマンドを使用します。

show ap module summary

次に、出力例を示します。

```
Device# show ap module summary
AP Name               External Module       External Module PID   External Module
Description
-----------------------------------------------------------------------------------------
AP500F.1111.2222      Enable                SanDisk               Cruzer Blade
```

- 各 AP の USB 設定の詳細を表示するには、次のコマンドを使用します。

show ap name *ap-name* **config general**

次に、出力例を示します。

```
Device# show ap name AP500F.111.2222 config general

.
.
.
USB Module Type.................................. USB Module
USB Module Status................................ Disabled
USB Module Operational State..................... Enabled
USB Override ……..... Enabled
```

- USB モジュールのステータスを表示するには、次のコマンドを使用します。

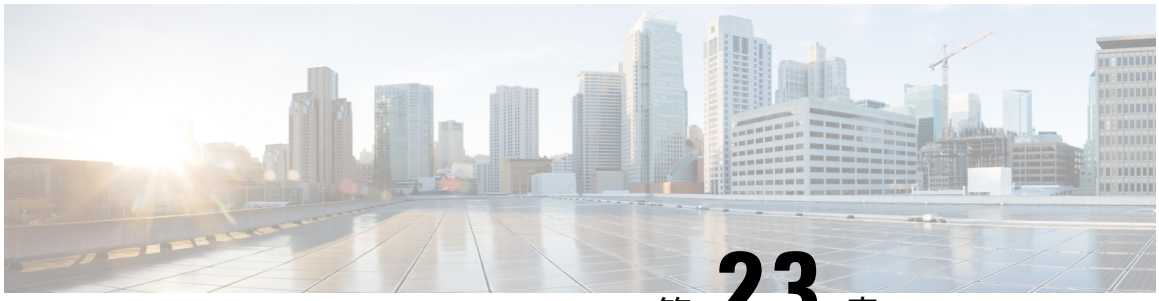
show ap profile name *xyz* **detailed**

次に、出力例を示します。

```
Device# show ap profile name xyz detailed
USB Module               : ENABLED
```

第 IV 部

ネットワーク管理



第 23 章

DHCP オプション 82

DHCP オプション 82 について

クライアントからの DHCP 要求にオプション 82 の情報を追加してからその要求を DHCP サーバーに転送するように、 組み込みワイヤレスコントローラを設定することができます。その後、DHCP オプション 82 に含まれている情報に基づいてワイヤレス クライアントに IP アドレスを割り当てるように、DHCP サーバーを設定できます。

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータやその他の制御情報は、DHCP メッセージのオプション フィールドに格納されたタグ付きデータ項目で伝送されます。これらのデータ項目自体もオプションと呼ばれます。オプション 82 には、リレー エージェントが認識する情報が含まれています。

リレー エージェント情報オプションは、1 つまたは複数のサブオプションを含む単一の DHCP オプションとして構成されています。このサブオプションによってリレーエージェントが認識する情報が伝達されます。オプション 82 は、DHCP リレー エージェントが DHCP サーバーに転送中の要求に回線固有の情報を挿入できるようにすることを目的として設計されました。このオプションは、次の 2 つのサブオプションを設定することで機能します。

- 回線 ID
- リモート ID

回線 ID サブオプションには、要求が送信された回線に固有の情報が含まれます。このサブオプションはリレー エージェントに固有の識別子です。したがって、記述される回線はリレー エージェントによって異なります。

リモート ID サブオプションには、回線のリモート ホスト側の情報が含まれます。通常、このサブオプションには、リレー エージェントを識別する情報が含まれます。ワイヤレス ネットワークであれば、これはワイヤレス アクセス ポイントの固有識別子になります。

組み込みワイヤレスコントローラでは、DHCP オプション 82 の次のオプションを設定できます。

- DHCP 有効
- DHCP Opt82 有効
- DHCP Opt82 Ascii
- DHCP Opt82 RID
- DHCP Opt82 形式
- DHCP AP MAC
- DHCP SSID
- DHCP AP ETH MAC
- DHCP AP NAME
- DHCP サイトタグ
- DHCP AP ロケーション
- DHCP VLAN ID

（注） Cisco Catalyst 9800 シリーズのコンフィギュレーション ベスト プラクティスについては、次のリンクを参照してください。 https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html

DHCP オプション 82 グローバル インターフェイスの設定

サーバーオーバーライドによる DHCP オプション 82 のグローバル設定（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： `デバイス# 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	**ip dhcp-relay information option server-override** 例： デバイス(config)# **ip dhcp-relay information option server-override**	グローバル サーバー オーバーライドおよびリンク選択サブオプションを挿入します。

各種 SVI による DHCP オプション 82 のグローバル設定（GUI）

手順

ステップ 1 [Configuration] > [VLAN] を選択します。

ステップ 2 ドロップダウンリストから VLAN を選択します。

[Edit SVI] ウィンドウが表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [IPv4 Inbound ACL] ドロップダウンリストからオプションを選択します。

ステップ 5 [IPv4 Outbound ACL] ドロップダウンリストからオプションを選択します。

ステップ 6 [IPv6 Inbound ACL] ドロップダウンリストからオプションを選択します。

ステップ 7 [IPv6 Outbound ACL] ドロップダウンリストからオプションを選択します。

ステップ 8 [IPv4 Helper Address] フィールドに IP アドレスを入力します。

ステップ 9 [Relay Information Option] 設定を有効にする場合は、ステータスを [Enabled] に設定します。

ステップ 10 [Subscriber ID] を入力します。

ステップ 11 [Server ID Override] 設定を有効にする場合は、ステータスを [Enabled] に設定します。

ステップ 12 [Option Insert] 設定を有効にする場合は、ステータスを [Enabled] に設定します。

ステップ 13 [Source-Interface Vlan] ドロップダウンリストからオプションを選択します。

ステップ 14 [Update & Apply to Device] をクリックします。

各種 SVI による DHCP オプション 82 のグローバル設定（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：	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
	デバイス# **configure terminal**	
ステップ 2	**ip dhcp-relay source-interface vlan** *vlan-id* 例： デバイス(config)# **ip dhcp-relay source-interface vlan 74**	リレーされるメッセージのグローバル送信元インターフェイスを設定します。

DHCP オプション 82 の形式の設定

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 profile policy** *policy-name* 例： Device(config)# **wireless profile policy *pp3***	指定したプロファイルポリシーの設定を有効にします。
ステップ 3	**shutdown** 例： Device(config-wireless-policy)# **shutdown**	プロファイルポリシーをシャットダウンします。
ステップ 4	**vlan** *vlan-name* 例： Device(config-wireless-policy)# **vlan 72**	プロファイルポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： Device(config-wireless-policy)# **session-timeout 300**	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： Device(config-wireless-policy)# **idle-timeout 15**	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。

	コマンドまたはアクション	目的
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format** {**ap_ethmac**|**ap_location**|**apmac**|**apname**|**policy_tag**|**ssid**|**vlan_id**} 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format apmac`	対応する AP で DHCP オプション 82 を有効にします。 このコマンドで使用可能な各種オプションの詳細については、『Cisco Catalyst 9800 Series Wireless Controller Command Reference』[英語] を参照してください。
ステップ 12	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

VLAN インターフェイスによる DHCP オプション 82 の設定

option-insert コマンドを使用した DHCP オプション 82 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： デバイス# **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	**interface vlan** *vlan-id* 例： デバイス(config)# **interface vlan 72**	VLAN ID を設定します。
ステップ 3	**ip dhcp relay information option-insert** 例： デバイス(config-if)# **ip dhcp relay information option-insert**	BOOTREQUEST にリレー情報を挿入します。
ステップ 4	**ip address** *ip-address* 例： デバイス(config-if)# **ip address 9.3.72.38 255.255.255.0**	インターフェイスの IP アドレスを設定します。
ステップ 5	**ip helper-address** *ip-address* 例： デバイス(config-if)# **ip helper-address 9.3.72.1**	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 6	**[no] mop enabled** 例： デバイス(config-if)# **no mop enabled**	インターフェイスの MOP を無効にします。
ステップ 7	**[no] mop sysid** 例： デバイス(config-apgroup)# **[no] mop sysid**	MOP 定期システム ID メッセージを送信するタスクを無効にします。

server-id-overrideコマンドを使用したDHCPオプション82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。
ステップ 2	**ip dhcp compatibility suboption server-override cisco** 例： `Device(config)# ip dhcp compatibility suboption server-override cisco`	server-id オーバーライド サブオプションを RFC またはシスコ固有の値に設定します。
ステップ 3	**ip dhcp compatibility suboption link-selection cisco** 例： `Device(config)# ip dhcp compatibility suboption link-selection cisco`	link-selection サブオプションを RFC またはシスコ固有の値に設定します。
ステップ 4	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 72`	VLAN ID を設定します。
ステップ 5	**ip dhcp relay information option server-id-override** 例： `Device(config-if)# ip dhcp relay information option server-id-override`	サーバー ID オーバーライドおよびリンク選択サブオプションを挿入します。
ステップ 6	**ip address** *ip-address* 例： `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 7	**ip helper-address** *ip-address* 例： `Device(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 8	**[no] mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。

	コマンドまたはアクション	目的
ステップ 9	**[no] mop sysid** 例： `Device(config-if)# [no] mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。

サブスクライバ ID による DHCP オプション 82 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： `デバイス# 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	**interface vlan** *vlan-id* 例： `デバイス(config)# interface vlan 72`	VLAN ID を設定します。
ステップ 3	**ip dhcp relay information option subscriber-id** *subscriber-id* 例： `デバイス(config-if)# ip dhcp relay information option subscriber-id test10`	サブスクライバ ID サブオプションを挿入します。
ステップ 4	**ip address** *ip-address* 例： `デバイス(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**ip helper-address** *ip-address* 例： `デバイス(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 6	**[no] mop enabled** 例： `デバイス(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。
ステップ 7	**[no] mop sysid** 例： `デバイス(config-apgroup)# [no] mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。

server-ID-override および subscriber-id コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

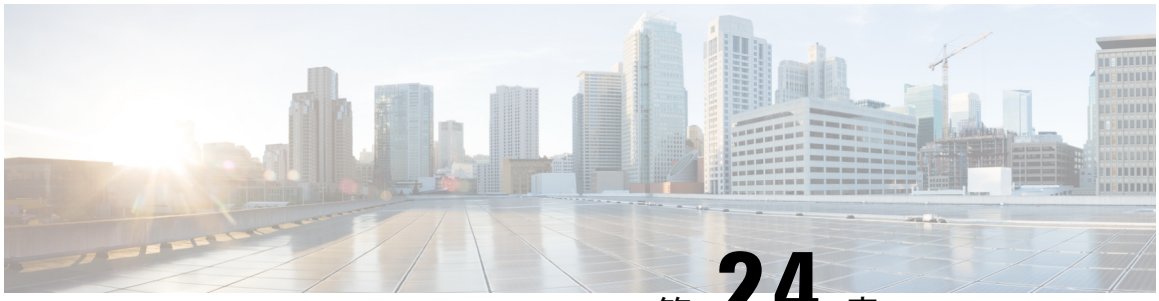
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id* 例： `デバイス(config)# interface vlan 72`	VLAN ID を設定します。
ステップ 3	**ip dhcp relay information option server-id-override** 例： `デバイス(config-if)# ip dhcp relay information option server-id-override`	サーバー ID オーバーライドおよびリンク選択サブオプションを挿入します。
ステップ 4	**ip dhcp relay information option subscriber-id** *subscriber-id* 例： `デバイス(config-if)# ip dhcp relay information option subscriber-id test10`	サブスクライバ ID サブオプションを挿入します。
ステップ 5	**ip address** *ip-address* 例： `デバイス(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 6	**ip helper-address** *ip-address* 例： `デバイス(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 7	**[no] mop enabled** 例： `デバイス(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。
ステップ 8	**[no] mop sysid** 例：	MOP 定期システム ID メッセージを送信するタスクを無効にします。

	コマンドまたはアクション	目的
	デバイス(config-apgroup)# **[no] mop sysid**	

各種 SVI による DHCP オプション 82 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： デバイス# **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	**interface vlan** *vlan-id* 例： デバイス(config)# **interface vlan 72**	VLAN ID を設定します。
ステップ 3	**ip dhcp relay source-interface vlan** *vlan-id* 例： デバイス(config-if)# **ip dhcp relay source-interface vlan 74**	VLAN ID でリレーされるメッセージの送信元インターフェイスを設定します。
ステップ 4	**ip address** *ip-address* 例： デバイス(config-if)# **ip address 9.3.72.38 255.255.255.0**	インターフェイスの IP アドレスを設定します。
ステップ 5	**ip helper-address** *ip-address* 例： デバイス(config-if)# **ip helper-address 9.3.72.1**	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 6	**[no] mop enabled** 例： デバイス(config-if)# **no mop enabled**	インターフェイスの MOP を無効にします。
ステップ 7	**[no] mop sysid** 例： デバイス(config-apgroup)# **[no] mop sysid**	MOP 定期システム ID メッセージを送信するタスクを無効にします。



第 24 章

RADIUS レルム

RADIUS レルムについて

RADIUS レルム機能は、ユーザーのドメインに関連付けられています。クライアントはこの機能を使用して、認証とアカウンティングの処理に使用する RADIUS サーバーを選択できます。

モバイル クライアントが WLAN に関連付けられている場合、Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement（EAP-AKA）の ID 応答要求の一部として、認証要求パケット内で RADIUS レルムを受信します。WLAN のネットワーク アクセス ID（NAI）形式（EAP-AKA）は、*username@domain.com* として指定できます。NAI 形式のレルムは @ 記号の後ろに示され、domain.com として指定されます。ベンダー固有の属性が *test* として追加された場合は、NAI 形式は test@domain.com として表されます。

RADIUS レルム機能は、WLAN で有効または無効にすることができます。レルムが WLAN で有効になっている場合、対応するユーザーはユーザー名を NAI 形式で送信する必要があります。 組み込みワイヤレスコントローラは、クライアントから受信した NAI 形式のレルムが定められた標準に従っている場合にのみ、AAA サーバーに認証要求を送信します。認証とは別に、アカウンティング要求もレルム フィルタリングに基づいて AAA サーバーに送信する必要があります。

WLAN 上のレルム サポート

各 WLAN は NAI レルムをサポートするように設定されます。レルムが特定の SSID に対して有効になると、RADIUS サーバー上で設定されたレルムに対して EAP ID 応答で受信したレルムを照合するためのルックアップが実行されます。クライアントがレルムとともにユーザー名を送信しない場合は、WLAN で設定されているデフォルトの RADIUS サーバーが認証に使用

されます。クライアントから受信したレルムが、WLAN上で設定されているレルムと一致しない場合、クライアントは認証解除され、ドロップされます。

RADIUS レルム機能が WLAN で有効になっていない場合は、EAP ID 要求の一部として受信したユーザー名がユーザー名として直接使用され、設定されているRADIUSサーバーが認証およびアカウンティングに使用されます。デフォルトでは、RADIUS レルム機能は WLAN で無効になっています。

- **認証用のレルム照合**：EAP方式を使用したdot1x（EAP AKAと同様）では、ユーザー名がEAP ID 応答の一部として受信されます。レルムはユーザー名から抽出され、対応するRADIUS認証サーバーですでに設定されているレルムと照合されます。一致した場合は、認証要求がRADIUSサーバーに転送されます。一致しなかった場合は、クライアントが認証解除されます。
- **アカウンティング用のレルム照合**：クライアントのユーザ名がaccess-acceptメッセージを通じて受信されます。アカウンティングメッセージがトリガーされると、対応するクライアントのユーザー名からレルムが抽出され、RADIUSアカウンティング サーバー上で設定されたアカウンティング レルムと比較されます。一致した場合は、アカウンティング要求がRADIUSサーバーに転送されます。一致しなかった場合は、アカウンティング要求が破棄されます。

RADIUS レルムの有効化

RADIUS レルムを有効にするには、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 aaa policy** *aaa-policy* **例**： `Device(config)# wireless aaa policy policy-1`	新しい AAA ポリシーを作成します。
ステップ 3	**aaa-realm enable** **例**： `Device(config-aaa-policy)# aaa-realm enable`	AAA RADIUS レルムの選択を有効にします。 （注） RADIUS レルムを無効にするには、**no aaa-realm enable** または **default aaa-realm enable** コマンドを使用します。

認証およびアカウンティング用に RADIUS サーバーと照合するためのレルムの設定

認証およびアカウンティング用にRADIUSサーバーと照合するようにレルムを設定するには、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	**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 3	**aaa authorization network default group** *radius-server-group* 例： `Device(config)# aaa authorization network default group aaa_group_name`	許可の方法を設定します。
ステップ 4	**aaa authentication dot1x** *realm* **group** *radius-server-group* 例： `Device(config)# aaa authentication dot1x cisco.com group cisco1`	dot1x がレルム グループ RADIUS サーバーを使用する必要があることを示します。
ステップ 5	**aaa authentication login** *realm* **group** *radius-server-group* 例： `Device(config)# aaa authentication login cisco.com group cisco1`	ログイン時の認証方法を定義します。
ステップ 6	**aaa accounting identity** *realm* **start-stop group** *radius-server-group* 例： `Device(config)# aaa accounting identity cisco.com start-stop group cisco1`	アカウンティングを有効にして、クライアントが承認されたときに start-record アカウンティング通知を送信し、最後に stop-record を送信できるようにします。

WLAN の AAA ポリシーの設定

WLAN の AAA ポリシーを設定するには、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 aaa policy** *aaa-policy-name* 例： `Device(config)# wireless aaa policy aaa-policy-1`	ワイヤレスの新しい AAA ポリシーを作成します。
ステップ 3	**aaa-realm enable** 例： `Device(config-aaa-policy)# aaa-realm enable`	レルム別の AAA RADIUS サーバーの選択を有効にします。
ステップ 4	**exit** 例： `Device(config-aaa-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**wireless profile policy** *wlan-policy-profile* 例： `Device(config)# wireless profile policy wlan-policy-a`	WLAN ポリシープロファイルを設定します。
ステップ 6	**aaa-policy** *aaa-policy* 例： `Device(config-wireless-policy)# aaa-policy aaa-policy-1`	AAA ポリシーをマッピングします。
ステップ 7	**accounting-list** *acct-config-realm* 例： `Device(config-wireless-policy)# accounting-list cisco.com`	アカウンティング リストを設定します。
ステップ 8	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション 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 9	**wlan** *wlan-name wlan-id ssid* 例： `Device(config)# wlan wlan2 14 wlan-aaa`	WLAN を設定します。
ステップ 10	**security dot1x authentication-list** *auth-list-realm* 例： `Device(config-wlan)# security dot1x authentication-list cisco.com`	IEEE 802.1x のセキュリティ認証リストを有効にします。
ステップ 11	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**wireless tag policy** *policy* 例： `Device(config)# wireless tag policy tag-policy-1`	ポリシー タグを設定します。
ステップ 13	**wlan** *wlan-name* **policy** *policy-profile* 例： `Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a`	ポリシープロファイルを WLAN にマッピングします。
ステップ 14	**exit** 例： `Device(config-policy-tag)# exit`	グローバル コンフィギュレーション モードに戻ります。

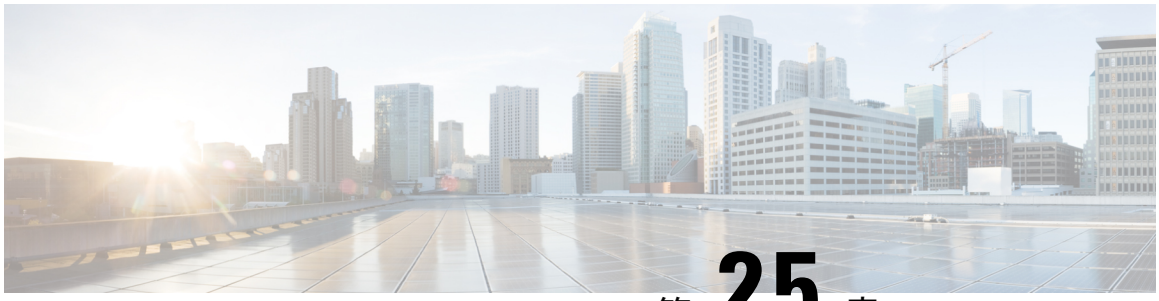
RADIUS レルム設定の確認

RADIUS レルム設定を確認するには、次のコマンドを使用します。

```
Device# show wireless client mac-address 14bd.61f3.6a24 detail


Client MAC Address : 14bd.61f3.6a24
Client IPv4 Address : 9.4.113.103
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : sacthoma@cisco.com
AP MAC Address : 4c77.6d79.5a00
AP Name: AP4c77.6d53.20ec
AP slot : 1
Client State : Associated
Policy Profile : name-policy-profile
Flex Profile : N/A
Wireless LAN Id : 3
Wireless LAN Name: ha_realm_WLAN_WPA2_AES_DOT1X
BSSID : 4c77.6d79.5a0f
```

```
Connected For : 26 seconds
Protocol : 802.11ac
Channel : 44
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Re-Authentication Timeout : 1800 sec (Remaining time: 1775 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 06/12/2018 19:52:35 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 25 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN : 113
Multicast VLAN : 0
Access VLAN : 113
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_9040000f
  IIF ID           : 0x9040000F
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 097704090000000DF4607B3B
  Acct Session ID  : 0x00000fa2
  Aaa Server Details
  Server IP        : 9.4.23.50
  Auth Method Status List
       Method : Dot1x
              SM State         : AUTHENTICATED
              SM Bend State    : IDLE
  Local Policies:
       Service Template : wlan_svc_name-policy-profile_local (priority 254)
              Absolute-Timer   : 1800
              VLAN             : 113
  Server Policies:
  Resultant Policies:
```

```
              VLAN             : 113
              Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
.
.
.
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```



第 25 章

永続的 SSID ブロードキャスト

永続的 SSID ブロードキャスト

メッシュ ネットワーク内のアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）として動作します。RAP は 組み込みワイヤレスコントローラへ有線で接続され、MAP は 組み込みワイヤレスコントローラへ無線で接続されます。この機能は、Flex + ブリッジ モードの Cisco Aironet 1542 アクセス ポイントにのみ適用されます。

この機能により、WAN 接続がダウンしている場合でも、ルート アクセス ポイント（RAP）とメッシュ アクセス ポイント（MAP）が SSID をブロードキャストします。このことは、障害の原因がバックホールにあるのかアクセス ワイヤレス ネットワークにあるのかにかかわらず、責任を分離するために必要です。なぜなら、ネットワークの各部分はさまざまな通信事業者が所有している可能性があるためです。

デフォルト ゲートウェイが到達可能である限り、RAP および MAP はスタンドアロン モード時は SSID をブロードキャストします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのメッシュ導入ガイドも参照してください。

永続的 SSID ブロードキャストの設定

手順

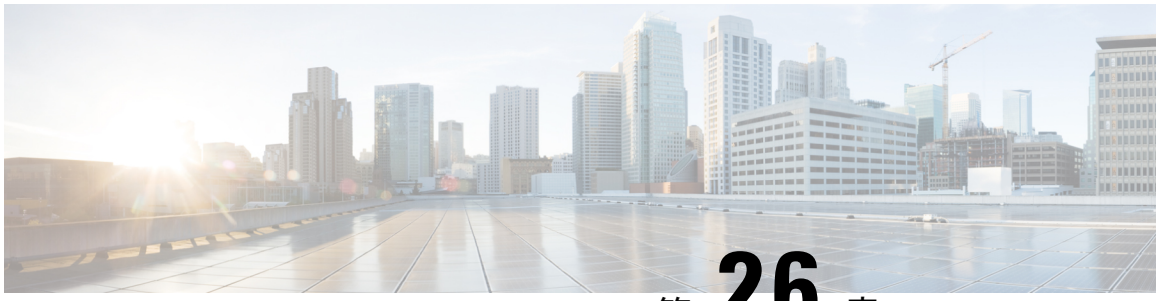
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**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。
ステップ 3	**[no]ssid broadcast persistent** 例： `Device(config-ap-profile)# [no] ssid broadcast persistent`	**ssid broadcast** コマンドを実行すると、SSID ブロードキャスト モードが設定されます。**persistent** キーワードを指定すると、永続的 SSID ブロードキャストが有効になり、関連付けられた AP が再参加します。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。 （注） この機能を有効または無効にすると、AP が再参加します。

永続的 SSID ブロードキャストの確認

すべてのシスコ AP の設定を表示するには、次の **show** コマンドを使用します。

```
Device#show ap config general
Cisco AP Name   : AP4C77.6DF2.D598
================================================
Office Extend Mode                              : Disabled
Persistent SSID Broadcast                       : Enabled
Remote AP Debug                                 : Disabled
```



第 26 章

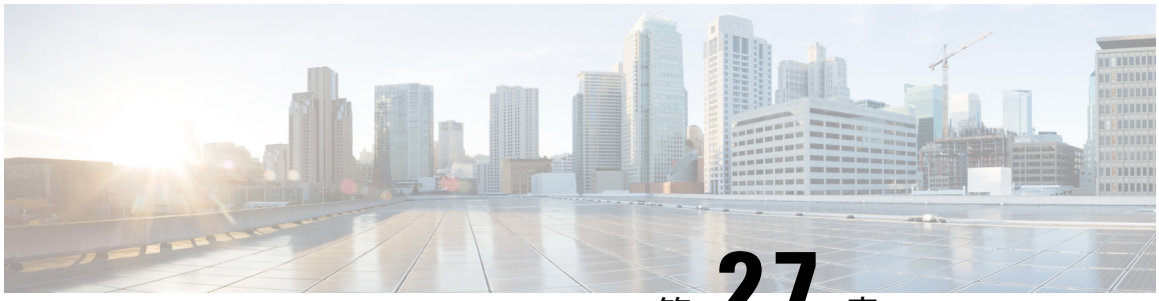
ネットワーク モニターリング

ネットワーク モニターリング

組み込みワイヤレスコントローラでサポートされる唯一のネットワークモニタリングは、Cisco Digital Network Architecture（DNA）Center を介したものです。このモニタリングは、設定またはステータス情報のプッシュおよびプルに独自のプロトコルを使用しNETCONF を介して行われます。

第 V 部

システム管理



第 27 章

Network Mobility Services Protocol（ネットワーク モビリティ サービス プロトコル）

Network Mobility Services Protocol について

Cisco Network Mobility Services Protocol（NMSP）は、コネクション型（TLS）またはコネクションレス型（DTLS）の転送を介して実行できる、セキュアな双方向プロトコルです。ワイヤレスインフラストラクチャで NMSP サーバーを実行し、Cisco Connected Mobile Experiences（Cisco CMX）が NMSP クライアントとして機能します。 組み込みワイヤレスコントローラは複数のサービスをサポートし、複数の Cisco CMX が NMSP サーバーに接続して、NMSP セッションを介して各種サービスのデータを取得できます（ワイヤレスデバイスの場所、プローブ RSSI、HyperLocation、wIPS など）。

NMSP は、Cisco CMX と 組み込みワイヤレスコントローラ間の相互通信を定義します。Cisco CMX は、ルーテッド IP ネットワークを介して 組み込みワイヤレスコントローラと通信します。publish-subscribe と request-reply の両方の通信モデルがサポートされています。通常、Cisco CMX は、 組み込みワイヤレスコントローラから定期的な更新の形式でサービスデータを受信するためのサブスクリプションを確立します。組み込みワイヤレスコントローラはデータパブ

リッシャとして機能し、複数のCMXにサービスデータをブロードキャストします。CiscoCMXは、サブスクリプションに加えて、組み込みワイヤレスコントローラが応答を送り返すように組み込みワイヤレスコントローラに要求を送信することもできます。

NMSPは基本的に、外部との通信手段を組み込みワイヤレスコントローラのアプリケーションに提供します。組み込みワイヤレスコントローラのNMSPは、外部と通信するようにプロトコルを変更する柔軟性も備えています。

Network Mobility Services Protocol の機能の一覧を次に示します。

- NMSP はデフォルトで無効になっています。
- NMSP は TCP を使用して Cisco CMX と通信し、暗号化に TLS を使用します。

（注） HTTPS は、組み込みワイヤレスコントローラと Cisco CMX 間のデータ転送ではサポートされていません。

NMSP オンプレミスサービスの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**nmsp enable** 例： `デバイス(config)# nmsp enable`	NMSP オンプレミス サービスを有効にします。 （注） デフォルトでは、NMSP は組み込みワイヤレスコントローラで有効になっています。
ステップ 3	**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、RFID タグ、および不正デバイスの NMSP 通知間隔の変更

NMSP は、Cisco Connected Mobile Experiences（Cisco CMX）と 組み込みワイヤレスコントローラ間の発着信トラフィックに関する通信を管理します。高い頻度でのロケーション更新を必要とするアプリケーションがある場合は、クライアント、アクティブな RFID タグ、および不正なアクセス ポイント/クライアントの NMSP 通知間隔を 1 ～ 180 秒の範囲内で変更できます。

（注） 組み込みワイヤレスコントローラと Cisco CMX との通信には、TCP ポート（16113）が使用されます。組み込みワイヤレスコントローラと Cisco CMX の間にファイアウォールがある場合、Cisco CMX for NMSP が機能するにはこのポートが開いている（ブロックされていない）必要があります。

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	**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。

クライアントおよびタグの NMSP 通知しきい値の変更

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	**location notify-threshold** {**clients** | **tags** } *threshold* 例：	クライアントおよびタグの NMSP 通知しきい値の設定

	コマンドまたはアクション	目的
	デバイス(config)# **location notify-threshold clients 5**	*threshold*：RSSI しきい値（db 単位）。有効な範囲は 0 ～ 10 です。
ステップ 3	**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。

NMSP の強力な暗号の設定

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	**nmsp strong-cipher** 例： デバイス(config)# **nmsp strong-cipher**	「ECDHE-RSA-AES128-GCM-SHA256:、ECDHE-ECDSA-AES128-GCM-SHA256:、AES256-SHA256:AES256-SHA:、および AES128-SHA256:AES128-SHA」を含む NMSP サーバーの強力な暗号を有効にします。 通常の暗号スイートには、「ECDHE-RSA-AES128-GCM-SHA256:、ECDHE-ECDSA-AES128-GCM-SHA256:、および AES128-SHA」が含まれます。
ステップ 3	**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。

NMSP 設定の表示

組み込みワイヤレスコントローラの NMSP 機能を表示するには、次のコマンドを使用します。

```
Device# show nmsp capability
Service            Subservice
----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum           Aggregate Interferer, Air Quality, Interferer,
```

```
Info                Rogue, Mobile Station,
Statistics          Rogue, Tags, Mobile Station,
AP Monitor          Subscription
On Demand Services Device Info
AP Info             Subscription
```

NMSP 通知間隔を表示するには、次のコマンドを使用します。

```
Device# show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```

すべての CMX 接続における接続固有の統計カウンタを表示するには、次のコマンドを使用します。

```
Device# show nmsp statistics connection
NMSP Connection Counters
------------------------
 CMX IP Address: 10.22.244.31, Status: Active
 State:
      Connections : 1
      Disconnections : 0
      Rx Data Frames : 13
      Tx Data Frames : 99244
      Unsupported messages : 0
  Rx Message Counters:
     ID  Name                                  Count
    ------------------------------------------------
      1  Echo Request                          6076
      7  Capability Notification                  2
     13  Measurement Request                      5
     16  Information Request                      3
     20  Statistics Request                       2
     30  Service Subscribe Request                1

  Tx Message Counters:
     ID  Name                                  Count
    ------------------------------------------------
      2  Echo Response                         6076
      7  Capability Notification                  1
     14  Measurement Response                    13
     15  Measurement Notification             91120
     17  Information Response                     6
     18  Information Notification              7492
     21  Statistics Response                      2
     22  Statistics Notification                305
     31  Service Subscribe Response               1
     67  AP Info Notification                   304
```

組み込みワイヤレスコントローラの NMSP サービスにおける共通の統計カウンタを表示するには、次のコマンドを使用します。

```
Device# show nmsp statistics summary
NMSP Global Counters
--------------------
Number of restarts                :
```

```
SSL Statistics
--------------------
Total amount of verifications      : 6
Verification failures              : 6
Verification success               : 0
Amount of connections created      : 8
Amount of connections closed       : 7
Total amount of accept attempts    : 8
Failures in accept                 : 0
Amount of successful accepts       : 8
Amount of failed registrations     : 0

AAA Statistics
--------------------
Total amount of AAA requests       : 7
Failed to send requests            : 0
Requests sent to AAA               : 7
Responses from AAA                 : 7
Responses from AAA to validate     : 7
Responses validate error           : 6
Responses validate success         : 1
```

NMSP の全体的な接続を表示するには、次のコマンドを使用します。

```
Device# show nmsp status
NMSP Status
-----------

CMX IP Address   Active    Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data     Transport
------------------------------------------------------------------------------------------
127.0.0.1        Active    6             6             1           2           TLS
```

すべてのCMXによってサブスクライブされているすべてのモビリティ サービスを表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription detail
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

特定の CMX によってサブスクライブされているすべてのモビリティ サービスを表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription detail <ip_addr>
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

すべてのCMXによってサブスクライブされているモビリティ サービス全体を表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription summary
Service            Subservice
```

```
-----------------------------
RSSI                Rogue, Tags, Mobile Station,
Spectrum
Info                Rogue, Mobile Station,
Statistics          Tags, Mobile Station,
AP Info             Subscription
```

例：NMSP の設定

次に、RFID タグの NMSP 通知間隔を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# nmsp notification interval rssi rfid 50
デバイス(config)# end
デバイス# show nmsp notification interval
```

次に、クライアントの NMSP 通知間隔を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# nmsp notification interval rssi clients 180
デバイス(config)# end
デバイス# show nmsp notification interval
```

プローブ RSSI ロケーション

プローブ RSSI ロケーション機能を使用すると、ワイヤレス 組み込みワイヤレスコントローラと Cisco CMX で次の動作をサポートできます。

- ロード バランシング
- カバレッジ ホールの検出
- CMX へのロケーションの更新

ワイヤレス クライアントが有効な場合、ワイヤレス クライアントから、近くにあるワイヤレス ネットワークを識別すると同時に、識別されたサービス セット識別子（SSID）に関連付けられた受信信号強度表示（RSSI）を検出するための、プローブ要求が送信されます。

ワイヤレス クライアントは、アクセス ポイントに接続した後も、定期的にバックグラウンドでアクティブ スキャンを実行します。これにより、ワイヤレス クライアントは、接続に最も適した信号強度を持つアクセス ポイントのリストを更新できるようになります。アクセス ポイントに接続できなくなると、ワイヤレス クライアントは、保存されているアクセス ポイント リストを使用して、最適な信号強度を提供する別のアクセスポイントに接続します。WLAN のアクセスポイントは、これらのプローブ要求、RSSI、およびワイヤレスクライアントの MAC アドレスを収集して、それらをワイヤレス 組み込みワイヤレスコントローラに転送します。Cisco CMX は、ワイヤレス 組み込みワイヤレスコントローラからこのデータを収集し、それ

らのデータを使用して、ネットワークでのローミング時にワイヤレスクライアントの更新された場所を計算します。

プローブ RSSI 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 probe filter** 例： `Device(config)# wireless probe filter`	AP から受け取る未応答のプローブ要求のフィルタリングを有効にして、ロケーションの精度を向上させます。 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。これで、応答済みと未応答の両方のプローブ要求が組み込みワイヤレスコントローラに転送されます。
ステップ 3	**wireless probe limit** *limit-value interval* 例： `Device(config)# wireless probe limit 10 100`	同じクライアントに対して、指定した間隔で AP から組み込みワイヤレスコントローラに報告されるプローブ要求の数を設定します。 デフォルトの制限（500 ミリ秒の間隔で 2 つのプローブ）に戻すには、このコマンドの **no** 形式を使用します。
ステップ 4	**wireless probe locally-administered-mac** 例： `Device(config)# wireless probe locally-administered-mac`	ローカルに管理された MAC アドレスを持つクライアントからのプローブの報告を有効にします。
ステップ 5	**location algorithm rssi-average** 例： `Device(config)# location algorithm rssi-average`	プローブ RSSI 測定の更新を、より正確なアルゴリズムに設定します。ただし、CPU のオーバーヘッドは高くなります。
ステップ 6	**location algorithm simple** 例： `Device(config)# location algorithm simple`	（任意）プローブ RSSI 測定の更新を、より高速なアルゴリズムに設定します。CPU のオーバーヘッドは小さくなりますが、精度は低くなります。

	コマンドまたはアクション	目的
		アルゴリズム タイプをデフォルト（*rssi-average*）に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**location expiry client** *interval* 例： `Device(config)# location expiry client 300`	RSSI 値のタイムアウトを設定します。 このコマンドの **no** 形式を指定すると、デフォルト値の 15 に設定されます。
ステップ 8	**location notify-threshold client** *threshold-db* 例： `Device(config)# location notify-threshold client 5`	クライアントの通知しきい値を設定します。 このコマンドの **no** 形式を指定すると、デフォルト値の 0 に設定されます。
ステップ 9	**location rssi-half-life client** *time-in-seconds* 例： `Device(config)# location rssi-half-life client 20`	2 つの RSSI 測定値を平均するときの半減期を設定します。 このオプションを無効にするには、値を 0 に設定します。

次のタスク

各プローブ クライアント（関連付けられていて、プローブのみ）を 10 個の MAC アドレスの集まりで表示するには、**show wireless client probing** コマンドを使用します。

プローブ RSSI の確認

関連付けられたクライアントが検出された AP の詳細と、使用している RSSI を表示するには、次の手順を実行します。

```
Device# show wireless client mac-address 4.4.4 detail
****snippet of the output****
Nearby AP Statistics:
TEST_AP-1 (slot 0)
antenna 0: 0 s ago ........ -77 dBm
antenna 1: 0 s ago ........ -88 dBm
TEST_AP-5 (slot 0)
antenna 0: 0 s ago ........ -64 dBm
antenna 1: 0 s ago ........ -36 dBm
TEST_AP-6 (slot 0)
antenna 0: 0 s ago ........ -69 dBm
antenna 1: 0 s ago ........ -79 dBm
```

RFID タグのサポート

組み込みワイヤレスコントローラでは、無線周波数 ID（RFID）タグの追跡を設定できます。RFID タグは、独自の信号を継続的にブロードキャストし、リアルタイムのロケーション トラッキングのためにアセットに付加される小型のワイヤレスバッテリ電源タグです。これらのタグは、専用の 802.11 パケットを使用してその位置をアドバタイズします。アドバタイズされたパケットは、アクセスポイント、 組み込みワイヤレスコントローラ、および Cisco CMX によって処理されます。アクティブな RFID のみがサポートされています。アクティブな RFID タグとワイヤレス組み込みワイヤレスコントローラの組み合わせにより、機器の現在の場所を追跡できます。「アクティブ」なタグは、一般には「クローズドループ」システム（タグがタグの所有者または発信者が管理する施設から物理的に離れることを前提としないシステム）での高価値資産のリアルタイム追跡に使用されます。

RFID タグの詳細については、『Wi-Fi Location-Based Services 4.1 Design Guide』[英語] の「Active RFID tags」の項を参照してください。

一般的な注意事項

- シスコ準拠の「アクティブ RFID タグ」のみがサポートされています。
- 組み込みワイヤレスコントローラで RFID タグを確認できます。
- RFID タグのハイ アベイラビリティがサポートされています。

RFID タグのサポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 rfid** 例： `Device(config)# wireless rfid`	RFID タグ追跡をイネーブルにします。 デフォルト値はイネーブルです。 RFID タグ追跡をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**wireless rfid timeout** *timeout-value* 例： `Device(config)# wireless rfid timeout 90`	テーブルをクリーンアップするための RFID タグ データ タイムアウト値を設定します。

	コマンドまたはアクション	目的
		タイムアウト値は、タグを失効させるまで 組み込みワイヤレスコントローラが保持する時間の長さです。たとえば、タグが 30 秒ごとにビーコンするよう設定されている場合は、タイムアウト値を 90 秒（ビーコン値の約 3 倍）に設定することをお勧めします。デフォルト値は 1200 秒です。

RFID タグのサポートの確認

クライアントである RFID 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 wireless rfid client
```

RFID タグの詳細情報を表示するには、次のコマンドを使用します。

```
Device# show wireless rfid detail <rfid-mac-address>

RFID address  000c.cc96.0001
Vendor Cisco
Last Heard 6 seconds  ago
Packets Received 187
Bytes Received 226

Content Header
==============
  CCX Tag Version 0
  Tx power: 12
  Channel: 11
  Reg Class: 4
CCX Payload
==============
  Last Sequence Control 2735
  Payload length 221
  Payload Data Hex Dump:
  00000000  00 02 00 00 01 09 00 00  00 00 0c b8 ff ff ff 02  |................|
  00000010  07 42 03 20 00 00 0b b8  03 4b 00 00 00 00 00 00  |.B. .....K......|
  00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

既知のすべての RFID タグについてそれらのサマリー情報を表示するには、次のコマンドを使用します。

```
Device# show wireless rfid summary

Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 3 minutes 30 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 4 minutes 5 seconds ago
0012.b80b.806c Cisco 7069.5a63.0520 -46 15 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 4 minutes 28 seconds ago
```

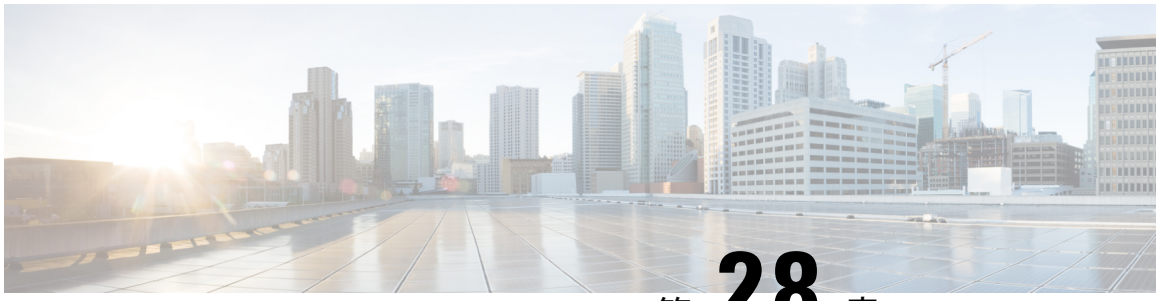
```
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 4 minutes 29 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 4 minutes 26 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 3 minutes 21 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 4 minutes 28 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 4 minutes 7 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 minute 52 seconds ago
```

ロケーションベースのシステム RFID 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 wireless rfid stats

RFID stats :
==============
RFID error db full : 0
RFID error invalid paylod : 0
RFID error invalid tag : 0
RFID error dot11 hdr : 0
RFID error pkt len : 0
RFID error state drop : 0
RFID total pkt received : 369
RFID populated error value : 0
RFID error insert records : 0
RFID error update records : 0
RFID total insert record : 16
RFID ccx payload error : 0
RFID total delete record : 0
RFID error exceeded ap count : 0
RFID error record remove : 0
RFID old rssi expired count: 0
RFId smallest rssi expireed count : 0
RFID total query insert : 0
RFID error invalid rssi count : 0
```

NMSP 通知間隔を表示するには、次のコマンドを使用します。

```
Device# show nmsp notification interval

NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```



第 28 章

Application Visibility and Control（アプリケーションの可視化と制御）

Application Visibility and Control について

Application Visibility and Control（AVC）は、トラフィック情報を提供できる Flexible NetFlow（FNF）パッケージ全体のサブセットです。AVC 機能では、アクセスポイント（AP）または組み込みワイヤレスコントローラで実行される NBAR のメリットをもたらす分散型アプローチが利用されており、ディープパケットインスペクション（DPI）を実行してその結果を FNF メッセージで報告することを目的としています。

AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストのかかるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成できます。トラフィック フローが NBAR2 エンジンを使用して分析および認識され、認識されたプロトコルまたはアプリケーションと一緒に、特定のフローがマークされます。このフロー単位の情報を、FNF によるアプリケーションの可視化に使用できます。アプリケーションの可視化が確立されると、ユーザーはクライアントのポリシング メカニズムを使用してコントロール ルールを定義できます。

AVC ルールを使用すると、WLAN 上で join しているすべてのクライアントに対して、特定アプリケーションの帯域幅を制限できます。これらの帯域幅コントラクトは、アプリケーション単位のレート制限より優先されるクライアント単位のダウンストリーム レート制限と共存します。

FNF はワイヤレスでサポートされる機能であり、フレックスモードの 組み込みワイヤレスコントローラで NetFlow が有効になっている必要があります。

AVC ソリューションの動作は、ワイヤレスの展開に基づいて変わります。ここでは、すべてのシナリオにおける共通点と相違点について説明します。

フレックス モード

- NBAR は AP で有効になっています。
- AVC は、FNF 設定を AP にプッシュします。
- AVC-FNF で、ローミングのコンテキスト転送をサポートします。
- NetFlow エクスポータをサポートします。

Application Visibility and Control の前提条件

- アクセスポイントは、AVC 対応である必要があります
- AVC（QoS）の制御部分を機能させるには、FNF 付きのアプリケーションの可視化機能を設定する必要があります。

Application Visibility and Control の制限

- レイヤ 2 ローミングは、 組み込みワイヤレスコントローラでサポートされていません。
- マルチキャスト トラフィックはサポートされていません。
- AVC は次のアクセス ポイントでのみサポートされます。
  - Cisco Aironet 1800 シリーズ アクセス ポイント
  - Cisco Aironet 2700 シリーズ アクセス ポイント
  - Cisco Aironet 2800 シリーズ アクセス ポイント
  - Cisco Aironet 3700 シリーズ アクセス ポイント

- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント

- AVC は、Cisco Aironet 702W、702I（128 M メモリ）、および 1530 シリーズ アクセス ポイントではサポートされません。
- App の可視性と認識されているアプリケーションのみ、QoS 制御の適用に使用できます。
- データリンクは AVC の NetFlow フィールドではサポートされません。
- AVC 非対応ポリシープロファイルと AVC 対応ポリシープロファイルの両方に同じ WLAN プロファイルをマッピングすることはできません。
- NBAR 対応 QoS ポリシー設定は有線物理ポートでポリシープロファイルで設定された、クライアントレベルおよび BSSID レベルの VLAN、ポートチャネル、および他の論理インターフェイスなどの仮想インターフェイスではサポートされていません。

AVC が有効になっている場合、AVC プロファイルは、デフォルトの DSCP ルールを含む最大 23 個のルールのみをサポートします。ルールが 23 個を超えている場合、AVC ポリシーは AP までプッシュされません。

AVC の設定の概要

AVC を設定するには、次の手順に従います。

1. **record wireless avc basic** コマンドを使用してフロー モニターを作成します。
2. ワイヤレス ポリシー プロファイルを作成します。
3. フロー モニターをワイヤレス ポリシー プロファイルに適用します。
4. ワイヤレス ポリシー タグを作成します。
5. WLAN をポリシー プロファイルにマッピングします。
6. ポリシー タグを AP に接続します。

フロー モニターの作成

NetFlow の設定には、フロー レコード、フロー モニター、およびフロー エクスポータが必要です。この設定は、AVC 全体の設定における最初のステップとして行ってください。

（注） Flex モードでは、**cache timeout active** および **cache timeout inactive** コマンドのデフォルト値は AVC に最適ではありません。フロー モニターでは、両方の値を 60 に設定することを推奨します。

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	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor fm_avc`	フロー モニターを作成します。
ステップ 3	**record wireless avc basic** 例： `Device(config-flow-monitor)# record wireless avc basic`	基本のワイヤレス AVC フローテンプレートを指定します。 （注） **record wireless avc basic** コマンドは **record wireless avc ipv4 basic** コマンドと同じです。ただし、Flex またはファブリックモードでは **record wireless avc ipv4 basic** コマンドはサポートされていません。このようなシナリオでは **record wireless avc basic** コマンドを使用します。

フローモニターの設定（GUI）

始める前に

フローモニターからデータをエクスポートするには、フローエクスポータを作成しておく必要があります。

手順

ステップ 1 **[Configuration]** > **[Services]** > **[Application Visibility]** の順に選択し、[Flow Monitor] タブに移動します。

ステップ 2 [Monitor] エリアで、[Add] をクリックしてフローモニターを追加します。

ステップ 3 [Flow Monitor] ウィンドウで、フローモニターと説明を追加します。

ステップ 4 ドロップダウンリストからフローエクスポータを選択して、フローモニターからコレクタにデータをエクスポートします。

（注） Wireless NetFlow データをエクスポートするには、以下のテンプレートを使用します。

- ETA（暗号化トラフィック分析）
- ワイヤレス AVC の基本
- ワイヤレス AVC の基本 IPv6

ステップ 5 [Apply to Device] をクリックして、設定を保存します。

フロー エクスポータの作成

フロー エクスポータを作成すると、フローのエクスポート パラメータを定義できます。これは、フローのエクスポート パラメータを設定するためのオプションの手順です。

（注） AVC 統計情報が 組み込みワイヤレスコントローラに表示されるようにするには、次のコマンドを使用してローカルのフローエクスポータを設定する必要があります。

- **flow exporter** *my_local*
- **destination local wlc**

また、フローモニターでは、統計情報を組み込みワイヤレスコントローラに表示するためにこのローカルのエクスポータを使用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**flow exporter** *flow-export-name* **例**： `Device(config)# flow exporter export-test`	フロー モニターを作成します。
ステップ 2	**description** *string* **例**： `Device(config-flow-exporter)# description IPv4flow`	最大 63 文字で、フロー レコードの説明を示します。
ステップ 3	**例**： `Device(config-flow-exporter) # destination local wlc`	エクスポータがデータを送信する宛先のローカル WLC を指定します。

	コマンドまたはアクション	目的
ステップ 4	**show flow exporter** 例： `Device # show flow exporter`	（任意）設定を確認します。

フローエクスポータの確認

フローエクスポータの説明を確認するには、次のコマンドを使用します。

たとえば、my-flow-exporter という名前のフローエクスポータに関するフローエクスポータの説明を確認するには、次の例を参照してください。

```
Device# show flow exporter
Flow Exporter my-flow-exporter:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination type:       Local (1)
    Destination IP address: 0.0.0.0
    Source IP address:      10.0.0.1
    Transport Protocol:     UDP
    Destination Port:       9XXX
    Source Port:            5XXXX
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Not Used
```

（注） 宛先のないフローエクスポータは、UNKNOWN タイプとしてマークされます。エクスポータが UNKNOWN としてマークされる 2 つの方法は次のとおりです。

1. 宛先を指定しないで CLI コマンドを使用してフローエクスポータを設定する場合。
2. EWC は、最大 1 つの外部フローエクスポータと 1 つの内部フローエクスポータをサポートします。タイプごとに複数のフローエクスポータを設定しようとすると、宛先が拒否され、フローエクスポータは UNKNOWN と見なされます。

AVC の WLAN の設定

AVC の WLAN 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	**wlan** *wlan-avc* **1** *ssid-avc* 例：	WLAN を設定します。

	コマンドまたはアクション	目的
	`Device(config)# wlan wlan1 1 ssid1`	
ステップ 2	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をシャット ダウンします。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を無効にします。

ポリシー 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 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	**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。

WLAN インターフェイスへのポリシー プロファイルのアタッチ（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、[Policy] タブをクリックします。

ステップ 3 [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 4 ポリシー タグの名前と説明を入力します。

ステップ 5 [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 6 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 7 [Save & Apply to Device] をクリックします。

WLAN インターフェイスへのポリシー プロファイルのアタッチ（CLI）

始める前に

- 異なるポリシー タグ間で同じ WLAN に異なる AVC ポリシー プロファイルを適用しないでください。

  次に、正しくない設定例を示します。

```
wireless profile policy avc_pol1
   ipv4 flow monitor fm-avc1 input
   ipv4 flow monitor fm-avc1 output
   no shutdown
  wireless profile policy avc_pol2
   ipv4 flow monitor fm-avc2 input
   ipv4 flow monitor fm-avc2 output
   no shutdown
  wireless tag policy avc-tag1
   wlan wlan1 policy avc_pol1
  wireless tag policy avc-tag2
   wlan wlan1 policy avc_pol2
```

  この例は前述の制限に反しています。つまり、WLAN *wlan1* を 2 つのポリシープロファイル（*avc_pol1* と *avc_pol2*）にマッピングしています。したがって、WLAN *wlan1* をすべての場所で *avc_pol1* または *avc_pol2* にマッピングする必要があるため、この設定は正しくありません。

- 同じ WLAN でのポリシー プロファイルの競合はサポートされていません。たとえば、ポリシー プロファイルを（AVC の有無にかかわらず）異なるポリシー タグ内の同じ WLAN に適用する場合などです。

  次に、正しくない設定例を示します。

```
wireless profile policy avc_pol1
   no shutdown
  wireless profile policy avc_pol2
   ipv4 flow monitor fm-avc2 input
   ipv4 flow monitor fm-avc2 output
   no shutdown
  wireless tag policy avc-tag1
   wlan wlan1 policy avc_pol1
  wireless tag policy avc-tag2
   wlan wlan1 policy avc_pol2
```

  この例では、AVC の有無にかかわらずポリシープロファイルを異なるタグ内の同じ WLAN に適用しています。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless tag policy** *avc-tag* 例： `Device(config)# wireless tag policy avc-tag`	ポリシー タグを作成します。
ステップ 2	**wlan** *wlan-avc* **policy** *avc-policy* 例： `Device(config-policy-tag)# wlan wlan_avc policy avc_pol`	WLAN プロファイルにポリシー プロファイルをアタッチします。

次のタスク

- 設定が完了したら、WLAN で **no shutdown** コマンドを実行します。
- WLAN がすでに **no shutdown** モードになっている場合は、 **shutdown** コマンドを実行し、その後に **no shutdown** コマンドを実行します。

AP へのポリシー プロファイルのアタッチ

手順

	コマンドまたはアクション	目的
ステップ 1	**ap** *ap-ether-mac* 例： `Device(config)# ap 34a8.2ec7.4cf0`	AP 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	**policy-tag** *policy-tag* 例： `Device(config)# policy-tag avc-tag`	アクセス ポイントにアタッチするポリシー タグを指定します。

AVC の設定の確認

手順

	コマンドまたはアクション	目的
ステップ 1	**show avc wlan** *wlan-name* **top** *num-of-applications* **applications {aggregate | downstream | upstream}** 例： `Device# show avc wlan wlan_avc top 2 applications aggregate`	これらのアプリケーションを使用している上位のアプリケーションとユーザーに関する情報を表示します。 （注） ワイヤレス クライアントが WLAN に関連付けられていて、トラフィックが生成されていることを確認し、その後 90 秒間待ってからコマンドを実行してください（統計情報を確実に参照できるようにするため）。
ステップ 2	**show avc client** *mac* **top** *num-of-applications* **applications {aggregate | downstream | upstream}**	上位の数のアプリケーションに関する情報を表示します。

	コマンドまたはアクション	目的
	例： `Device# show avc client 9.3.4 top 3 applications aggregate`	（注） ワイヤレス クライアントが WLAN に関連付けられていて、トラフィックが生成されていることを確認し、その後 90 秒間待ってからコマンドを実行してください（統計情報を確実に参照できるようにするため）。
ステップ 3	**show avc wlan** *wlan-name* **application** *app-name* **top** *num-of-clients* **aggregate** 例： `Device# show avc wlan wlan_avc application app top 4 aggregate`	これらのアプリケーションを使用している上位のアプリケーションとユーザーに関する情報を表示します。
ステップ 4	**show ap summary** 例： `Device# show ap summary`	組み込みワイヤレスコントローラに接続しているすべてのアクセスポイントのサマリーを表示します。
ステップ 5	**show ap tag summary** 例： `Device# show ap tag summary`	ポリシー タグを持つすべてのアクセスポイントのサマリーを表示します。

AVC ベースの選択的リアンカー

AVC ベースの選択的リアンカー機能は、クライアントが一方の組み込みワイヤレスコントローラから他方のコントローラにローミングするときにクライアントをリアンカーすることを目的としています。クライアントをリアンカーすることで、Cisco WLC の新しいクライアントで使用可能な IP アドレスが枯渇するのを防ぎます。クライアントをリアンカーするか保留するかを決めるために、AVC プロファイル ベースの統計情報が使用されます。この機能は、AVC ルールで定義されている音声またはビデオアプリケーションをクライアントが積極的に実行している場合に便利です。

リアンカーのプロセスでは、アンカーされたクライアントの認証解除も伴います。クライアントは、WLC 間をローミングしている時に、AVC ルールにリストされているアプリケーションのトラフィックを送信していない場合に、認証解除されます。

AVC ベースの選択的リアンカーの制限事項

- この機能はローカル モードでのみサポートされています。FlexConnect モードおよびファブリック モードはサポートされていません。

- この機能は、ゲスト トンネリングおよびエクスポート アンカーのシナリオではサポートされていません。
- 古い IP アドレスは、IP アドレスのリース期間が終了するまで、リアンカー後も解放されません。

フロー エクスポータの設定

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	**flow exporter** *name* 例： `Device(config)# flow exporter avc-reanchor`	フロー エクスポータを作成し、フロー エクスポータ コンフィギュレーション モードを開始します。 （注） このコマンドを使用して既存のフロー エクスポータを変更することもできます。
ステップ 3	**destination local wlc** 例： `Device(config-flow-exporter)# destination local wlc`	エクスポータをローカルとして設定します。

フロー モニターの設定

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	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor fm_avc`	フロー モニターを作成し、Flexible NetFlow フロー モニター 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
		（注） このコマンドを使用して既存のフロー モニターを変更することもできます。
ステップ 3	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter avc-reanchor`	フロー エクスポータの名前を指定します。
ステップ 4	**record wireless avc basic** 例： `Device(config-flow-monitor)# record wireless avc basic`	キャッシュの定義に使用するフロー レコードを指定します。
ステップ 5	**cache timeout active** *value* 例： `Device(config-flow-monitor)# cache timeout active 60`	アクティブ フロー タイムアウトを秒単位で設定します。
ステップ 6	**cache timeout inactive** *value* 例： `Device(config-flow-monitor)# cache timeout inactive 60`	非アクティブ フロー タイムアウトを秒単位で設定します。

AVC リアンカー プロファイルの設定

始める前に

- AVC-Reanchor-Class クラス マップを使用していることを確認します。それ以外のクラス マップ名はすべて、選択的リアンカーでは無視されます。
- システムの起動中に、AVC-Reanchor-Class クラスマップが存在するかどうかがチェックされます。見つからなかった場合は、デフォルトのプロトコル（jabber-video、wifi-calling など）が作成されます。AVC-Reanchor-Class クラスマップが見つかった場合、設定の変更は行われず、スタートアップ コンフィギュレーションに保存されているプロトコルの更新はリブート後も維持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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	**class-map** *cmap-name* 例： `Device(config)# class-map AVC-Reanchor-Class`	クラス マップを設定します。
ステップ 3	**match any** 例： `Device(config-cmap)# match any`	デバイスを通過するいずれかのプロトコルと照合するようにデバイスに指示します。
ステップ 4	**match protocol jabber-audio** 例： `Device(config-cmap)# match protocol jabber-audio`	アプリケーション名との一致を指定します。 必要に応じて、後でクラスマップ設定を編集し、jabber-video や wifi-calling などのプロトコルを追加または削除することができます。

ワイヤレス WLAN プロファイル ポリシーの設定

WLAN 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。

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** *policy-name* 例： `Device(config)# wireless profile policy default-policy-profile`	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	**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 4	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチ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	**ipv4 flow monitor** *monitor-name***input** 例： `Device(config-wireless-policy)# ipv4 flow monitor fm_avc input`	IPv4 入力フローモニターの名前を指定します。
ステップ 6	**ipv4 flow monitor** *monitor-name* **output** 例： `Device(config-wireless-policy)# ipv4 flow monitor fm_avc output`	IPv4 出力フローモニターの名前を指定します。
ステップ 7	**reanchor class** *class-name* 例： `Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class`	選択的リアンカー機能のプロトコルを使用してクラス マップを設定します。
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。

AVC リアンカーの確認

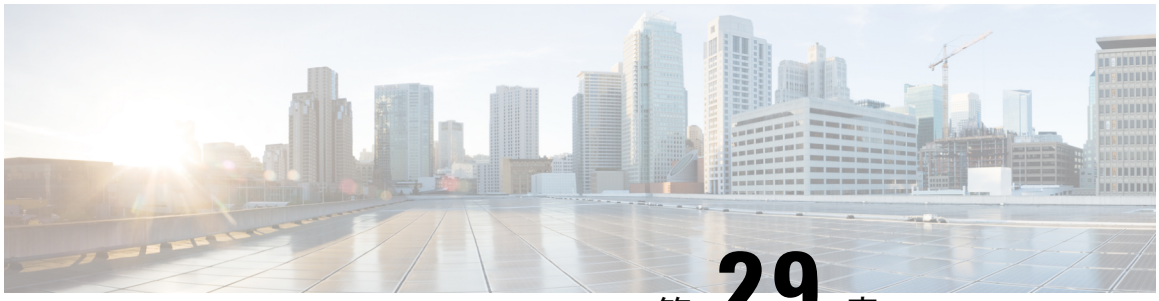
AVC リアンカーの設定を確認するには、次のコマンドを使用します。

```
Device# show wireless profile policy detailed avc_reanchor_policy

Policy Profile Name           : avc_reanchor_policy
Description                   :
Status                        : ENABLED
VLAN                          : 1
Wireless management interface VLAN        : 34
!
.
.
.
AVC VISIBILITY                : Enabled
Flow Monitor IPv4
  Flow Monitor Ingress Name   : fm_avc
  Flow Monitor Egress Name    : fm_avc
Flow Monitor IPv6
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
NBAR Protocol Discovery       : Disabled
Reanchoring                   : Enabled
Classmap name for Reanchoring
  Reanchoring Classmap Name   : AVC-Reanchor-Class
!
.
.
.
```

```
  ---------------------------------------------------


Device# show platform software trace counter tag wstatsd chassis active R0 avc-stats
debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
Reanch_deassociated_clients 28340 1
Reanch_tracked_clients 28340 4
Reanch_deleted_clients 28340 3

Device# show platform software trace counter tag wncd chassis active R0 avc-afc debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
Reanch_co_ignored_clients 30063 1
Reanch_co_anchored_clients 30063 5
Reanch_co_deauthed_clients 30063 4


Device# show platform software wlavc status wncd

Event history of WNCD DB:

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.630342 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822780 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822672 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172073 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738367 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738261 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.162689 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757643 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757542 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.468749 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18857 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18717 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164304 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163877 2 :READY 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593257 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593152 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.664772 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
```

```
06/12/2018 16:45:28.822499 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822222 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.207605 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738105 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.737997 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164225 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757266 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757181 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472778 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.15413 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.15263 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164254 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163209 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163189 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------ ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.630764 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822621 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822574 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172357 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738212 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738167 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164048 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757403 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757361 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472561 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18660 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18588 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164293 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163799 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163773 1 :INIT 24:CREATE_FSM 0 0


Device# show platform software wlavc status wncmgrd

Event history of WNCMgr DB:

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------ ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.629278 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629223 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629179 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510867 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510411 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510371 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
```

```
06/12/2018 16:45:28.886377 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------ ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.664032 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.663958 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.663921 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.511151 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510624 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510608 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.810867 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807239 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807205 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806734 4 :READY 3 :FSM_WLAN_DOWN 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------ ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.629414 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629392 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629380 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510954 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510572 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510532 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886293 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807844 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807795 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806990 4 :READY 3 :FSM_WLAN_DOWN 0 0
!
```



第 29 章

組み込みワイヤレスコントローラの Flexible NetFlow エクスポータ

組み込みワイヤレスコントローラの Flexible NetFlow エクスポータ

組み込みワイヤレスコントローラ（EWC）上の Flexible NetFlow（FnF）エクスポータは、Cisco IOS XE Amsterdam 17.2.1 以降でサポートされています。

NetFlow は、ネットワークを通過するパケットの統計情報を得られる Cisco IOS テクノロジーです。NetFlow は、IP ネットワークから実際の IP データを取得するための標準規格です。NetFlow は、ネットワークとセキュリティの監視、ネットワーク計画、トラフィック分析、および IP アカウンティングをサポートするためのデータを提供します。

Flexible NetFlow は、実際の要件に合わせてトラフィック分析パラメータをカスタマイズする機能を追加することで、以前の NetFlow よりも改善されています。Flexible NetFlow では、トラフィック分析のための非常に複雑な構成を作成したり、再利用可能な構成コンポーネントを使用してデータをエクスポートすることが容易になります。

EWC の FnF エクスポータは、Flex モードでのみサポートされます。

この機能は、EWC の AVC ソリューションの一部です。AVC の詳細については、「Application Visibility and Control」の章を参照してください。

EWC での AVC 設定の制限事項

- 1 つのローカルエクスポータのみ（EWC の統計コレクタ）サポートされています。

- FnF は、Flex モードの IP タイプおよび方向ごとに 1 つフローモニターのみサポートします。
- UDP トランスポートプロトコルのみサポートしています。
- AVC キャッシュはサポートされていません。
- option コマンドおよび DP 統計に関するコマンドは EWC ではサポートされていません。
- ワイヤレス AVC Basic テンプレートのみサポートしています。
- NetFlow バージョン 9 のみサポートしています。
- IP アドレス 0.0.0.0 は有効な宛先アドレスですが、使用すると、Flexible NetFlow データは破棄され、コレクタによって収集されません。

フロー エクスポータの作成

次に、EWC でフローエクスポータを作成する手順を示します。

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	**flow exporter** *flow-export-name* 例： `Device(config)# flow exporter export-test`	フロー エクスポータを作成します。
ステップ 3	**description** *string* 例： `Device(config-flow-exporter)# description IPv4flow`	（任意）最大 63 文字で、このフローエクスポータの説明を指定します。
ステップ 4	例： `Device(config-flow-exporter)# destination 10.0.1.0`	

フロー モニターの作成

NetFlow の設定には、フロー レコード、フロー モニター、およびフロー エクスポータが必要です。この設定は、AVC 全体の設定における最初のステップとして行ってください。

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	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor monitor-test`	フロー モニターを作成します。
ステップ 3	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter export-test`	このフローモニターを、定義済みのフローエクスポータにバインドします。
ステップ 4	**record wireless avc basic** 例： `Device(config-flow-monitor)# record wireless avc basic`	基本のワイヤレス AVC フローテンプレートを指定します。

ワイヤレス WLAN プロファイル ポリシーの設定

この設定では、フローモニターまたはエクスポータの構造をワイヤレス WLAN にマッピングすることで、AP が FnF 測定値を収集するようにします。

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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy default-policy-profile`	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	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	ポリシープロファイルを無効にします。

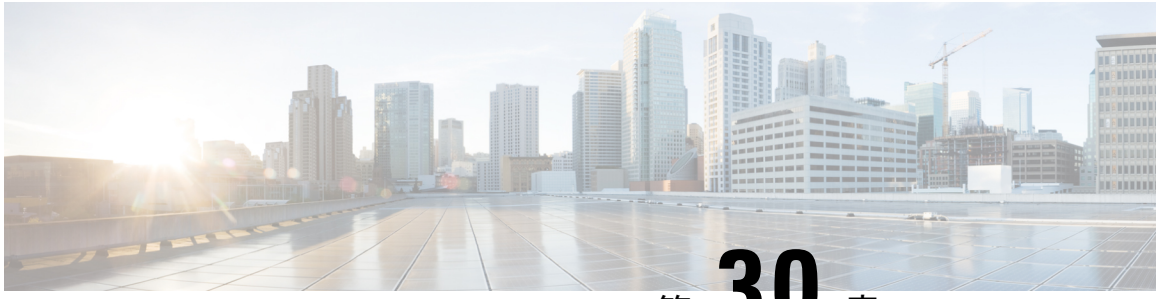
	コマンドまたはアクション	目的
ステップ 4	{**ipv4** | **ipv6**} **flow monitor** *monitor-name* **input** 例： `Device(config-wireless-policy)# ipv4 flow monitor monitor-test input`	IPv4 または IPv6 入力フローモニターの名前を指定します。
ステップ 5	{**ipv4** | **ipv6**} **flow monitor** *monitor-name* **output** 例： `Device(config-wireless-policy)# ipv4 flow monitor monitor-test output`	IPv4 または IPv6 出力フローモニターの名前を指定します。
ステップ 6	**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。

組み込みワイヤレスコントローラでのフローエクスポータの確認

組み込みワイヤレスコントローラでフローエクスポータの詳細を表示するには、次のコマンドを使用します。

show platform software wlavc status cp-exporter

```
show platform software wlavc status cp-exporter
AVC FNF Exporter status
IP: 10.10.1.1
connection statistics
        Sent bytes : 5672
        Sent packets : 569
        Sent records : 240
        Received packets : 800
        Received records : 564
Socket statistics
        New sockets : 3
        Closed sockets : 0
Library statistics  AVC
        cache errors : 0
        Unexpected Flow Monitor ID : 0
        Socket creation error : 0
```



第 30 章

Cisco Connected Mobile Experiences クラウド

Cisco Connected Mobile Experiences（CMX）は、コネクション型（TLS）トランスポート経由で動作するネットワーク モビリティ サービス プロトコル（NMSP）を使用して、シスコ ワイヤレス組み込みワイヤレスコントローラと通信します。このトランスポートではセキュアな双方向接続が提供されます。 組み込みワイヤレスコントローラと CMX の両方がオンプレミスで、それらの間に直接 IP 接続がある場合に便利です。

Cisco CMX クラウドは、オンプレミス CMX のクラウドによって提供されるバージョンです。Cisco CMX クラウドサービスにアクセスする場合、HTTPS がトランスポートプロトコルとして使用されます。

Cisco CMX クラウドの設定

CMX クラウドを設定するには、次の手順に従います。

始める前に

- **DNS の設定**：NMSP クラウドサービスで使用される完全修飾ドメイン名を解決するには、ステップ 2 に示すように、**ip name-server** *server_address* コンフィギュレーション コマンドを使用して **DNS** を設定します。
- **サード パーティのルート CA のインポート**：コントローラは、接続確立時に CMX から送信される証明書に基づいてピアとホストを確認します。ただし、ルート CA はコントローラに事前にインストールされていません。ステップ 3 に示すように、**crypto pki trustpool import url <url>** コンフィギュレーション コマンドを使用して、シスコが信頼するルート CA のセットを crypto PKI の trustpool にインポートする必要があります。
- この設定の完了に必要な **server url** および **server token** パラメータの構成を有効にするには、Cisco Spaces への登録が成功している必要があります。

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 name-server** *namesvr-ip-addr* 例： `Device(config)#ip name-server 10.10.10.205`	NMSP クラウドサービスで使用される FQDN名を解決するようにコントローラの DNS を設定します。
ステップ 3	**crypto pki trustpool import url** *url* 例： `Device(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	サードパーティのルート CA をインポートします。コントローラは、インポートされた証明書を使用してピアを確認します。
ステップ 4	**[no] nmsp cloud-services server url** *url* 例： `Device(config)# nmsp cloud-services server url https://cisco.com`	クラウド サービスに使用する URL を設定します。コンフィギュレーションからサーバー URL を削除するには、このコマンドの **no** 形式を使用します。
ステップ 5	**[no] nmsp cloud-services server token** *token* 例： `Device(config)# nmsp cloud-services server token test`	NMSP クラウド サービスの認証トークンを設定します。コンフィギュレーションからサーバー トークンを削除するには、このコマンドの **no** 形式を使用します。
ステップ 6	**[no] nmsp cloud-services http-proxy** *proxy-server port* 例： `Device(config)# nmsp cloud-services http-proxy 10.0.0.1 10`	（任意）NMSP クラウド サービスの HTTP プロキシの詳細を設定します。HTTP プロキシの使用を無効にするには、このコマンドの **no** 形式を使用します。
ステップ 7	**[no] nmsp cloud-services enable** 例： `Device(config)# nmsp cloud-services enable`	NMSP クラウド サービスを有効にします。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。

Cisco CMX クラウド構成の確認

CMX クラウドの構成を確認するには、次のコマンドを使用します。

アクティブな NMSP 接続のステータスを表示するには、、次のコマンドを使用します。

```
Device# show nmsp status

MSE IP Address   Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data   Transport
------------------------------------------------------------------------------
9.9.71.78        0             0             1           1         TLS
64.103.36.133    0             0             1230        2391      HTTPs
```

NMSP クラウド サービスのステータスを表示するには、次のコマンドを使用します。

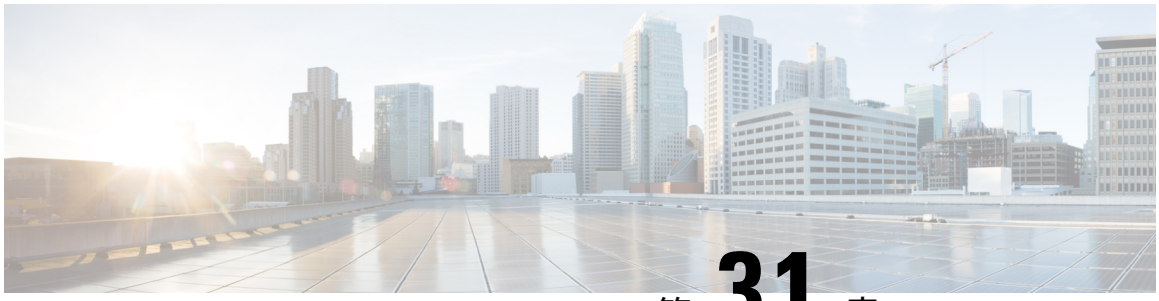
```
Device# show nmsp cloud-services summary

CMX Cloud-Services Status
-------------------------

   Server:                                 https://yenth8.cmxcisco.com
   IP Address:                             64.103.36.133
   Cmx Service:                            Enabled
   Connectivity:                           https: UP
   Service Status:                         Active
   Last Request Status:                    HTTP/1.1 200 OK
   Heartbeat Status:                       OK
```

NMSP クラウド サービス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 nmsp cloud-services statistics

CMX Cloud-Services Statistics
-----------------------------

   Tx DataFrames:                           3213
   Rx DataFrames:                           1606
   Tx HeartBeat Req:                       31785
   Heartbeat Timeout:                          0
   Rx Subscr Req:                           2868
   Tx DataBytes:                           10069
   Rx DataBytes:                           37752
   Tx HeartBeat Fail:                          2
   Tx Data Fail:                               0
   Tx Conn Fail:                               0
```

モビリティ サービス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 nmsp subscription summary

Mobility Services Subscribed:
Index Server IP Services
----- --------- --------
1 209.165.200.225 RSSI, Info, Statistics, AP Monitor, AP Info
2 209.165.200.225 RSSI, Statistics, AP Info
```



第 31 章

EDCA パラメータ

Enhanced Distributed Channel Access パラメータ

Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータは、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。

ここでは、次の内容について説明します。

EDCA パラメータの設定（GUI）

手順

ステップ 1 [Configuration] > [Radio Configuration] > [Parameters] を選択します。このページを使用して、802.11a/n/ac（5 GHz）および 802.11b/g/n（2.4 GHz）無線のグローバルパラメータを設定できます。

（注） 無線ネットワークが有効になっている場合、パラメータを設定または変更することはできません。続行する前に、[Configuration] > [Radio Configuration] > [Network] ページでネットワーク ステータスを無効にしてください。

ステップ 2 [EDCA Parameters] セクションで、[EDCA Profile] ドロップダウン リストから EDCA プロファイルを選択します。Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータは、音声、ビデオ、およびその他の Quality-of-Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。

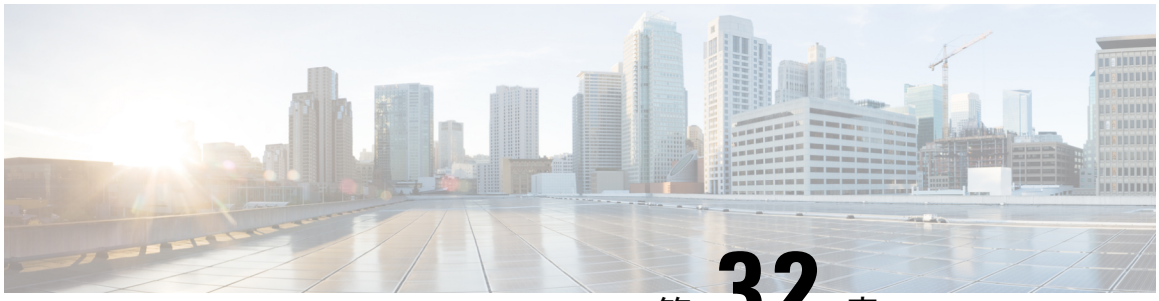
ステップ 3 [Apply] をクリックします。

EDCA パラメータの設定（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。
ステップ 2	**ap dot11 {5ghz | 24ghz } shutdown** 例： `デバイス(config)# ap dot11 5ghz shutdown`	無線ネットワークをディセーブルにします。
ステップ 3	**ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | fastlane | optimized-video-voice | optimized-voice | svp-voice | wmm-default}** 例： `デバイス(config)# ap dot11 5ghz edca-parameters optimized-voice`	802.11a または 802.11b/g ネットワークに対する特定の EDCA パラメータを有効にします。 • custom-voice：802.11a または 802.11b/g ネットワークのカスタム音声パラメータを有効にします。 • fastlane：802.11a または 802.11b/g ネットワークの fastlane パラメータを有効にします。 • optimized-video-voice：802.11a または 802.11b/g ネットワークの EDCA 音声およびビデオ最適化パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。 • optimized-voice：802.11a または 802.11b/g ネットワークで、SpectraLink 以外の音声用に最適化されたプロファイルパラメータを有効にします。ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。

	コマンドまたはアクション	目的
		• svp-voice：802.11a または 802.11b/g ネットワークの SpectraLink 音声優先パラメータを有効にします。コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。 • wmm-default：802.11a または 802.11b/g ネットワークの Wi-Fi マルチメディア（WMM）デフォルトパラメータを有効にします。これがデフォルトのオプションです。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
ステップ 4	**no ap dot11 {5ghz | 24ghz} shutdown** 例： `デバイス(config)# no ap dot11 5ghz shutdown`	無線ネットワークを再度イネーブルにします。
ステップ 5	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ap dot11 {5ghz | 24ghz} network** 例： `デバイス# show ap dot11 5ghz network`	音声用の MAC 最適化の現在のステータスを表示します。



第 32 章

802.11 パラメータおよび帯域選択

帯域選択、802.11 帯域およびパラメータについて

帯域選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、輻輳の少ない 5 GHz アクセスポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetoothデバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセスポイントからの同一チャネル干渉も受けます。これは、802.11b/g では、重複しないチャネルの数が 3 つに制限されているためです。このような干渉源を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、deviceで帯域選択を設定します。

クライアントに対するプローブ応答を調整すると帯域選択が機能し、WLAN単位で有効にできます。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。アクセス ポイントでは、**show dot11 band-select** コマンドを実行して帯域選択表を表示できます。show cont d0/d1 | begin Lru コマンドを実行して表示することもできます。

帯域選択アルゴリズム

帯域選択アルゴリズムは 2.4 GHz 帯域を使用するクライアントに影響を与えます。最初に、クライアントがアクセス ポイントにプローブ要求を送信すると、対応するクライアント プローブのアクティブ値とカウント値（帯域選択表に表示）が 1 になります。以下のシナリオによるアルゴリズム機能を示します。

- シナリオ1：クライアントRSSI（**show cont d0/d1 | begin RSSI** コマンドの出力に表示）が、中間 RSSI と受け入れ可能クライアント RSSI のどちらよりも強い場合。
  - デュアルバンドクライアント：2.4 GHz プローブ応答は常に表示されず、すべての 5 GHz プローブ要求に 5 GHz プローブ応答が表示されます。
  - シングルバンド（2.4 GHz）クライアント：プローブ抑制サイクル後にのみ 2.4 GHz プローブ応答が表示されます。
  - 設定したプローブサイクルカウントにクライアントのプローブカウントが達すると、アルゴリズムはエージング アウト抑止時間を待ち、プローブのアクティブ値を 0 にマークします。そして、アルゴリズムが再起動します。
- シナリオ2：クライアント RSSI（**show cont d0/d1 | begin RSSI** で表示）が、中間 RSSI と受け入れ可能クライアント RSSI の間の場合。
  - 2.4 GHz プローブ要求と 5 GHz プローブ要求はすべて制限なしで応答します。
  - このシナリオは、帯域選択無効時と似ています。

（注） クライアントの RSSI 値（**sh cont d0 | begin RSSI** コマンドの出力で表示）は、受信したクライアント パケットの平均値であり、中間 RSSI 機能はプローブ パケットの RSSI の瞬時値です。結果として、クライアント RSSI は設定した中間 RSSI 値（7 dB デルタ）より弱くなります。クライアントからのプローブ 802.11b は、802.11a バンドに関連付けるためクライアントをプッシュするように抑制されます。

802.11 帯域

自国の法的な規制基準を遵守するために、コントローラの 802.11b/g/n（2.4 GHz）帯域と 802.11a/n（5 GHz）帯域を設定できます。デフォルトでは、802.11b/g/n と 802.11a/n の両方が有効になっています。

ここでは、次の内容について説明します。

802.11n パラメータ

ここでは、ネットワーク上の 802.11n アクセス ポイントの管理手順について説明します。802.11n デバイスは、2.4 GHz 帯域と 5 GHz 帯域をサポートしており、高スループット データ レートを提供します。

802.11n の高スループット レートは、WMM を使用している WLAN のすべての 802.11n アクセス ポイントで使用できます。この場合、レイヤ 2 暗号化を使用していないか、WPA2/AES 暗号化が有効になっている必要があります。

（注） Cisco 802.11n AP は、偽の wIPS アラームをトリガーする可能性がある誤ったビーコン フレームを断続的に送信する場合があります。これらのアラームを無視することをお勧めします。

802.11h パラメータ

802.11h では、チャネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。

帯域選択、802.11 帯域、およびパラメータの制約事項

- 帯域選択が有効になっている WLAN では、ローミングの遅延が発生するため、音声やビデオなどの時間的に制約があるアプリケーションはサポートされません。
- 帯域選択は、Cisco Wave 2 および 802.11ax AP でのみサポートされています。

  特定の AP のサポートに関する詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html [英語] を参照してください。
- 帯域選択が動作するのは、コントローラに接続された AP に対してのみです。コントローラに接続しない FlexConnect AP では、再起動後の帯域選択は実行されません。
- 帯域選択アルゴリズムによるデュアルバンドクライアントの誘導は、同じ AP の 2.4 GHz 無線から 5 GHz 無線に限られます。このアルゴリズムが機能するのは、AP で 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。
- コントローラ GUI またはコントローラ CLI を使用して、帯域選択とクライアント ロード バランシングをグローバルで有効または無効にすることはできません。ただし、特定の WLAN の帯域選択とクライアント ロード バランシングを有効または無効にできます。帯域選択とクライアント ロード バランシングは、デフォルトではグローバルで有効になっています。

802.11 帯域とそのパラメータを設定する方法

帯域選択の設定（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 参加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]** > **[Wireless Advanced]** > **[Band Select]** を選択します。

ステップ 2 [Cycle Count] フィールドに、1 ～ 10 の値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。

ステップ 3 [Cycle Threshold (milliseconds)] フィールドに、スキャン サイクル期間しきい値を 1 ～ 1000 ミリ秒の値で入力します。この設定は、クライアントからの新しいプルーブ要求が新しいスキャンサイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は 200 ミリ秒です。

ステップ 4 [Age Out Suppression (seconds)] フィールドに、10 ～ 200 秒の値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g/n クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 5 [Age Out Dual Band (seconds)] フィールドに、10 ～ 300 秒の値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンドクライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 50 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 6 [Client RSSI (dbm)] フィールドに、-90 ～ -20 の値を入力します。これは、受信するクライアント パケットの平均です。

ステップ 7 [Client Mid RSSI (dbm)] フィールドに、-90 ～ -20 の値を入力します。これは、プローブパ ケットの瞬間 RSSI 値です。

ステップ 8 [AP Join Profile] ページで、AP 参加プロファイル名をクリックします。

ステップ 9 [Apply] をクリックします。

帯域選択の設定（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。
ステップ 2	**wireless client band-select cycle-count** *cycle_count* 例： `Device(config)# wireless client band-select cycle-count 3`	帯域選択のプローブ サイクル カウントを設定します。有効な範囲は 1 ～ 10 です。

	コマンドまたはアクション	目的
ステップ 3	**wireless client band-select cycle-threshold** *milliseconds* 例： `Device(config)# wireless client band-select cycle-threshold 5000`	新規スキャン周期の時間のしきい値を設定します。有効な範囲は 1 ～ 1000 です。
ステップ 4	**wireless client band-select expire suppression** *seconds* 例： `Device(config)# wireless client band-select expire suppression 100`	抑制の期限切れを帯域幅選択に設定します。有効な範囲は 10 ～ 200 です。
ステップ 5	**wireless client band-select expire dual-band** *seconds* 例： `Device(config)# wireless client band-select expire dual-band 100`	デュアル バンドの期限を設定します。有効な範囲は 10 ～ 300 です。
ステップ 6	**wireless client band-select client-rssi** *client_rssi* 例： `Device(config)# wireless client band-select client-rssi 40`	クライアント RSSI しきい値を設定します。有効な範囲は 20 ー 90 です。

ステップ 7	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select**
	例：
	`Device(config)# wlan wlan1 25 ssid12`
	`Device(config-wlan)# band-select`
		特定の WLAN で帯域選択を設定します。有効な範囲は 1 ～ 512 です。*SSID_network_name* パラメータには、最大 32 文字の英数字を入力できます。

802.11 帯域の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[Network]** を選択します。

ステップ 2 [5 GHz Band] または [2.4 GHz Band] のいずれかをクリックします。

ステップ 3 ネットワーク パラメータを設定できるようにするには、[Network Status] チェックボックスをオフにしてネットワークを無効にします。

ステップ 4 [Beacon Interval] フィールドに、AP による SSID のブロードキャスト レートを 100 ～ 600 ミリ秒の範囲で入力します。デフォルトは 100 ミリ秒です。

ステップ 5 802.11b/g/n（2.4 GHz）無線の場合、無線でショート プリアンブルを有効にするには、[Short Preamble] チェックボックスをオンにします。ショート プリアンブルを使用するとスループットのパフォーマンスが向上します。

ステップ 6 [Fragmentation Threshold (in bytes)] フィールドに、256 ～ 2346 バイトの値を入力します。ここで指定したサイズよりも大きいパケットはフラグメント化されます。

ステップ 7 ビーコンおよびプローブ応答で無線の送信電力レベルをアドバタイズするには、[DTPC Support] チェックボックスをオンにします。Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を使用するクライアント デバイスは、アクセス ポイントからチャネルおよび電力レベル情報を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアントデバイスをイタリアに移送し、そこのネットワークに追加した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。[DTPC Support] チェックボックスをオンにした場合、802.11a/n/ac（5 GHz）無線ネットワークで電力制限値を設定することはできません。

ステップ 8 [Apply] をクリックします。

ステップ 9 ネットワークの CCX 無線管理をグローバルに有効にするには、[CCX Location Measurement] セクションで、[Mode] チェックボックスをオンにします。このパラメータによって、このデバイスに接続されている AP から、CCX v2 以降のリリースを実行しているクライアントに対してブロードキャスト無線測定要求が発行されます。

ステップ 10 [Interval] フィールドに値を入力して、AP がブロードキャスト無線測定要求を発行する頻度を指定します。

ステップ 11 [Apply] をクリックします。

ステップ 12 アクセス ポイントとクライアントとの間で可能なデータ送信レートを指定するには、[Data Rates] セクションでその値を選択します。

- [Mandatory]：クライアントは、このコントローラ 組み込みワイヤレスコントローラ上のアクセスポイントにアソシエートするにはこのデータレートをサポートしている必要があります。
- [Supported]：アソシエートしたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信することができます。
- [Disabled]：通信に使用するデータ レートは、クライアントが指定します。

ステップ 13 [Apply] をクリックします。

ステップ 14 設定を保存します。

802.11 帯域の設定（CLI）

802.11 の帯域とパラメータを設定するには、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	**ap dot11 5ghz shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	802.11a 帯域をディセーブルにします。 （注） 802.11a ネットワーク パラメータを設定する前に、802.11a 帯域をディセーブルにする必要があります。
ステップ 3	**ap dot11 24ghz shutdown** 例： `Device(config)# ap dot11 24ghz shutdown`	802.11b 帯域をディセーブルにします。 （注） 802.11b ネットワーク パラメータを設定する前に、802.11b 帯域をディセーブルにする必要があります。
ステップ 4	**ap dot11** {**5ghz** | **24ghz** } **beaconperiod** *time_unit* 例： `Device(config)# ap dot11 5ghz beaconperiod 500`	対応するアクセス ポイントによる SSID のブロードキャスト レートを指定します。 ビーコン間隔は時間単位（TU）で測定されます。1 TU は 1024 マイクロ秒です。20 ～ 1000 ミリ秒ごとにビーコンを送信するように、アクセス ポイントを設定できます。
ステップ 5	**ap dot11** {**5ghz** | **24ghz** } **fragmentation** *threshold* 例： `Device(config)# ap dot11 5ghz fragmentation 300`	パケットを断片化するサイズを指定します。 しきい値は、256 ～ 2346 バイト（両端の値を含む）です。接続不良や多くの無線干渉が発生している領域では、この値を小さくします。

ステップ 6	**[no] ap dot11** {**5ghz** | **24ghz** } **dtpc**
	例：
	`Device(config)# ap dot11 5ghz dtpc`
	`Device(config)# no ap dot11 24ghz dtpc`
		アクセス ポイントによる、チャネルのアドバタイズ、ビーコンの電力レベル送信、応答プローブを有効にします。
		デフォルト値はイネーブルです。Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を使用するクライアント デバイスは、アクセス ポイントからチャネル レベルおよび電力レベ

	コマンドまたはアクション	目的
		ルの情報を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアントデバイスをイタリアに移送し、その場所のネットワークに参加させた場合、チャネルと電力の設定の自動調整を DTPC に任せることができます。 このコマンドの no 形式は、DTPC 設定を無効にします。
ステップ 7	**wireless client association limit** *number* **interval** *milliseconds* 例： `Device(config)# wireless client association limit 50 interval 1000`	設定できるクライアントの最大数を指定します。 単一アクセスポイントスロットの、所定の間隔内におけるアソシエーション要求の最大数を設定できます。設定できるアソシエーション制限の範囲は 1 ～ 100 です。 アソシエーション要求制限間隔は 100 ～ 10000 ミリ秒です。
ステップ 8	**ap dot11 {5ghz | 24ghz} rate** *rate* {**disable** | **mandatory** | **supported**} 例： `Device(config)# ap dot11 5ghz rate 36 mandatory`	データをコントローラ組み込みワイヤレスコントローラとクライアント間で送信できる速度を指定します。 • disable：クライアントが通信に使用するデータレートを指定するように定義します。 • mandatory：クライアントがコントローラ組み込みワイヤレスコントローラのアクセスポイントにアソシエートするには、このデータレートをサポートする必要があることを定義します。 • supported：このデータレートをサポートしているアソシエートしたクライアントはこのレートを使用してアクセスポイントと通信できます。ただし、クライアントがこのレートを使用できなくても、アソシエートは可能です。 • rate：データの送信レートを指定します。802.11a、802.11b 帯域では、

	コマンドまたはアクション	目的
		データは 1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps のレートで送信されます。
ステップ 9	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 10	**no ap dot11 24ghz shutdown** 例： `Device(config)# no ap dot11 24ghz shutdown`	802.11b 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 11	**ap dot11 24ghz dot11g** 例： `Device(config)# ap dot11 24ghz dot11g`	802.11g ネットワークのサポートをイネーブルまたはディセーブルにします。 デフォルト値はイネーブルです。このコマンドは、802.11b 帯域が有効になっている場合のみ使用できます。この機能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

帯域選択 RF プロファイルの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Advanced]** を選択します。

ステップ 2 [Band Select] タブで、[Cycle Count] フィールドに 1 ～ 10 の値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。

ステップ 3 [Cycle Threshold] フィールドに、スキャン サイクル期間しきい値を 1 ～ 1000 ミリ秒の値で入力します。この設定は、クライアントからの新しいプローブ要求が新しいスキャン サイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は200 ミリ秒です。

ステップ 4 [Age Out Suppression] フィールドに、10 ～ 200 秒の値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g/n クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 5 [Age Out Dual Band] フィールドに、10 ～ 300 秒の値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンドクライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 50 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 6 [Client RSSI] フィールドに、-90 ～ -20 dBm の値を入力します。クライアントがプローブに応答するための最大 RSSI です。

ステップ 7 [Client Mid RSSI] フィールドに、-20 ～ -90 dBm の値を入力します。このパラメータは mid-RSSI を設定します。この値を使用して RSSI 値に基づき 2.4 GHz プローブの抑制をトグルできます。

ステップ 8 [Apply] をクリックします。

802.11n のパラメータの設定（GUI）

手順

ステップ 1 [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 Profile] ウィンドウを表示します。

ステップ 3 [802.11] タブで、次の手順を実行します。

a) 必要な動作レートを選択します。

b) 対応するチェックボックスをオンにして、必要な [802.11n MCS Rates] を選択します。

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

802.11n のパラメータの設定（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。
ステップ 2	**ap dot11 {5ghz | 24ghz} dot11n** 例：	ネットワークで 802.11n サポートを有効にします。

	コマンドまたはアクション	目的
	デバイス(config)# **ap dot11 5ghz dot11n**	このコマンドの **no** 形式は、ネットワークでの 802.11n サポートを無効にします。
ステップ 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* 例： デバイス(config)# **ap dot11 5ghz dot11n mcs tx 20**	データをアクセスポイントとクライアント間で送信できる変調および符号化方式（MCS）レートを指定します。 *rtu*：有効な範囲は 0 ～ 23 です。 このコマンドの **no** 形式は、設定された MCS レートを無効にします。
ステップ 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require** 例： デバイス(config)# **wlan wlan1 25 ssid12** デバイス(config-wlan)# **wmm require**	WLAN で WMM をイネーブルにし、設定した 802.11n データ レートを使用します。 **require** キーワードは、クライアントデバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に接続できません。
ステップ 5	**ap dot11 {5ghz | 24ghz} shutdown** 例： デバイス(config)# **ap dot11 5ghz shutdown**	ネットワークをディセーブルにします。
ステップ 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** 例： デバイス(config)# **ap dot11 5ghz dot11n a-mpdu tx priority all**	802.11n パケットに使用する集約方法を指定します。 集約は、パケットデータ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。A-MPDU と A-MSDU は、両方ともソフトウェアで実行されます。 集約方法は、アクセスポイントからクライアントへのトラフィックのタイプごとに指定できます。 リストでは、トラフィック タイプごとに割り当てられる優先レベル（0～7）を定義します。 • 0：ベスト エフォート

	コマンドまたはアクション	目的
		• 1：バックグラウンド • 2：スペア • 3：エクセレント エフォート • 4：制御ロード • 5：ビデオ（100 ms 未満の遅延およびジッタ） • 6：音声（100 ms 未満の遅延およびジッタ） • 7：ネットワーク コントロール 各優先レベルを個別に設定するか、all パラメータを使用して一度にすべての優先レベルを設定できます。トラフィックが A-MPDU 送信または A-MSDU 伝送を使用するよう、プライオリティ レベルを設定できます。 • 他のオプションとともに **ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられたトラフィックは、A-MPDU 送信に関連付けらます。 • 他のオプションとともに **no ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられたトラフィックは、A-MSDU 送信に関連付けられます。 クライアントが使用する集約方法に合わせて優先度を設定します。デフォルトでは、A-MPDU は、優先レベル 0、4、および 5 に対して有効になっており、それ以外は無効になっています。デフォルトでは、A-MPDU は、6 と 7 以外のすべての優先度に対して有効になっています。
ステップ 7	**no ap dot11 {5ghz | 24ghz} shutdown** 例：	ネットワークを再度イネーブルにします。

	コマンドまたはアクション	目的
	デバイス(config)# **no ap dot11 5ghz shutdown**	
ステップ 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** 例： デバイス(config)# **ap dot11 5ghz dot11n guard-interval long**	ネットワークのガード間隔を設定します。
ステップ 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** 例： デバイス(config)# **ap dot11 5ghz dot11n rifs rx**	ネットワークの Reduced Interframe Space（RIFS）を設定します。
ステップ 10	**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。

802.11h のパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ap dot11 5ghz shutdown** 例： Device(config)# **ap dot11 5ghz shutdown**	802.11 ネットワークを無効にします。
ステップ 2	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* 例： Device(config)# **ap dot11 5ghz channelswitch mode 0**	アクセス ポイントの、新しいチャネルに切り替わった際のアナウンス機能をイネーブルまたはディセーブルにします。 *switch_mode*：0 または 1 を入力して、チャネルが実際に切り替えられるまで送信を制限する（0）か、制限しない（1）かを指定します。デフォルト値は [disabled] です。
ステップ 3	**ap dot11 5ghz power-constraint** *value* 例： Device(config)# **ap dot11 5ghz power-constraint 200**	802.11h の電力制限値を dB 単位で設定します。有効範囲は 0 ～ 255 です。 デフォルト値は 3 です。

	コマンドまたはアクション	目的
ステップ 4	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a ネットワークを再度イネーブルします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

帯域選択、802.11 帯域およびパラメータの設定のモニターリング

帯域選択と 802.11 帯域を使用した設定の確認コマンド

次のコマンドは、組み込みワイヤレスコントローラの帯域選択と 802.11 帯域、およびパラメータの確認に使用できます。

表 *18 :* 帯域選択と *802.11* 帯域を使用した設定のモニターリング コマンド

コマンド	目的
show ap dot11 5ghz network	802.11a 帯域ネットワーク パラメータ、802.11a 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。
show ap dot11 24ghz network	802.11b 帯域ネットワーク パラメータ、802.11b/g 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。
show wireless dot11h	802.11h 設定パラメータを表示します。
show wireless band-select	帯域選択の設定を表示します。

例：5 GHz 帯域の設定の確認

```
デバイス# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
```

```
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
```

```
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：2.4 GHz 帯域の設定の確認

```
デバイス# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

  802.11b/g Operational Rates
  802.11b 1M : Mandatory
  802.11b 2M : Mandatory
  802.11b 5.5M : Mandatory
  802.11g 6M : Supported
  802.11g 9M : Supported
  802.11b 11M : Mandatory
  802.11g 12M : Supported
  802.11g 18M : Supported
  802.11g 24M : Supported
  802.11g 36M : Supported
  802.11g 48M : Supported
  802.11g 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
```

```
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
  Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable Mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
```

```
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：802.11h パラメータの状態の確認

```
Device# show wireless dot11
Power Constraint: 0
Channel Switch : Enabled
Channel Switch Mode : Quiet
Smart DFS : Enabled
```

例: 帯域選択の設定の確認

次に、帯域選択の設定を表示する例を示します。

```
デバイス# show wireless band-select

Band Select Probe Response   : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : -80
Client Mid RSSI (dBm)        : -80
```

帯域選択、802.11 帯域およびパラメータの設定例

例：帯域選択の設定

次に、帯域選択の新規スキャン周期のプローブ サイクル カウントおよび時間しきい値を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select cycle-count 3
デバイス(config)# wireless client band-select cycle-threshold 5000
デバイス(config)# end
```

次に、抑制の期限を帯域選択に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select expire suppression 100
デバイス(config)# end
```

次に、デュアル バンドの期限を帯域選択に設定する例を示します。

```
デバイス# configure terminal
```

```
デバイス(config)# wireless client band-select expire dual-band 100
デバイス(config)# end
```

次に、クライアント RSSI しきい値を帯域選択に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select client-rssi 40
デバイス(config)# end
```

次に、特定の WLAN 上で帯域選択を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wlan wlan1 25 ssid12
デバイス(config-wlan)# band-select
デバイス(config)# end
```

例：802.11 帯域設定

次に、ビーコン間隔、フラグメンテーション、および動的な送信電力コントロールを使用して 802.11 帯域を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ap dot11 5ghz shutdown
デバイス(config)# ap dot11 24ghz shutdown
デバイス(config)# ap dot11 5ghz beaconperiod 500
デバイス(config)# ap dot11 5ghz fragmentation 300
デバイス(config)# ap dot11 5ghz dtpc
デバイス(config)# wireless client association limit 50 interval 1000
デバイス(config)# ap dot11 5ghz rate 36 mandatory
デバイス(config)# no ap dot11 5ghz shutdown
デバイス(config)# no ap dot11 24ghz shutdown
デバイス(config)# ap dot11 24ghz dot11g
デバイス(config)#end
```

例：802.11n 設定

次に、集約方法を使って 5 GHz 帯域の802.11n パラメータを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ap dot11 5ghz dot11n
デバイス(config)# ap dot11 5ghz dot11n mcs tx 20
デバイス(config)# wlan wlan1 25 ssid12
デバイス(config-wlan)# wmm require\
デバイス(config-wlan)# exit
デバイス(config)# ap dot11 5ghz shutdown
デバイス(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
デバイス(config)# no ap dot11 5ghz shutdown
デバイス(config)#exit
```

次に、5 GHz 帯域でガード インターバルを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ap dot11 5ghz dot11n
デバイス(config)# ap dot11 5ghz dot11n mcs tx 20
デバイス(config)# wlan wlan1 25 ssid12
デバイス(config-wlan)# wmm require\
デバイス(config-wlan)# exit
デバイス(config)# no ap dot11 5ghz shutdown
デバイス(config)# ap dot11 5ghz dot11n guard-interval long
デバイス(config)#end
```

次に、5 GHz 帯域で RIFS を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ap dot11 5ghz dot11n
デバイス(config)# ap dot11 5ghz dot11n mcs tx 20
デバイス(config)# wlan wlan1 25 ssid12
デバイス(config-wlan)# wmm require\
デバイス(config-wlan)# exit
デバイス(config)# ap dot11 5ghz shutdown
デバイス(config)# ap dot11 5ghz dot11n rifs rx
デバイス(config)#end
```

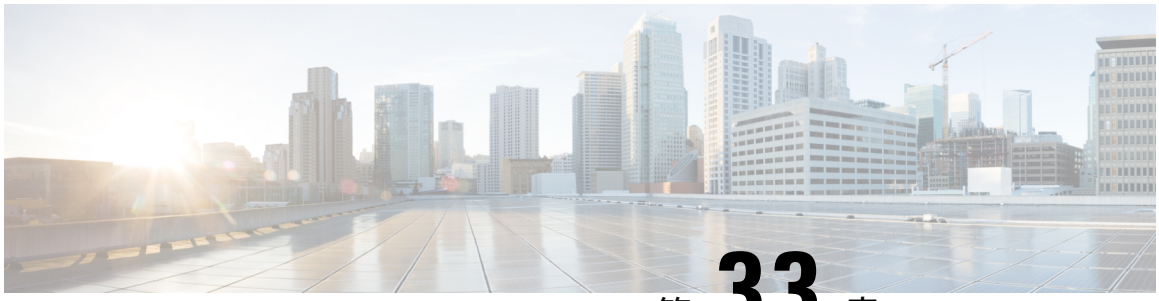
例：802.11h 設定

次に、制限伝送を使用して、アクセス ポイントをいつ新しいチャネルに切り替えるかをアナウンスするために、そのアクセスポイントを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ap dot11 5ghz shutdown
デバイス(config)# ap dot11 5ghz channelswitch mode 0
デバイス(config)# no ap dot11 5ghz shutdown
デバイス(config)#end
```

次に、5 GHz 帯域で 802.11h 電力制限を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ap dot11 5ghz shutdown
デバイス(config)# ap dot11 5ghz power-constraint 200
デバイス(config)# no ap dot11 5ghz shutdown
デバイス(config)#end
```



第 33 章

イメージのダウンロード

イメージのダウンロードに関する情報

ソフトウェアアップデートにより、Cisco 組み込みワイヤレスコントローラ ネットワーク内のすべての アクセスポイント が最新のソフトウェアを実行していることを確認できます。ソフトウェアアップデートまたはイメージのダウンロードは、GUI と CLI の両方を使用して実行できます。

一般的な Cisco 組み込みワイヤレスコントローラ ネットワークには、次のコンポーネントが含まれています。

- コントローラ（組み込みワイヤレスコントローラ）として機能する Cisco Catalyst AP
- Cisco 組み込みワイヤレスコントローラ 対応 AP（Virtual Router Redundancy Protocol（VRRP）ベースの選択プロセスに参加する他の Cisco Catalyst シリーズ AP）
- 下位 AP（Cisco Catalyst シリーズ または Cisco Aironet シリーズ Wave 2 AP）
- 外部 TFTP および SFTP サーバー。

（注） GUI の使用時に最適なユーザーエクスペリエンスを得るには、ブラウザを 100% の解像度で表示します。解像度が 100% を超えると、線が途切れることがあります。

AP イメージ事前ダウンロードステータスの更新（GUI）

Cisco IOS XE Amsterdam リリース 17.3.1 以降、アクセスポイント（AP）イメージのダウンロード中に、Catalyst アクセスポイントの Cisco 組み込みワイヤレスコントローラにより、ダウンロードの現在の割合とダウンロードの推定完了時間が計算されます（計算された値は、**show wireless ewc-ap ap image predownload status** コマンドを実行して、CLI 出力で確認できます）。

[Software Upgrage] ウィンドウにアクセスするには、Catalyst アクセスポイントのホームページの Cisco 組み込みワイヤレスコントローラ から、[Administration] > [Software Management] > [Software Upgrade] を選択します。

GUI の [Software Update Status] セクションには、[Initiate]、[Controller Image Download]、[AP Image Download]、[Network Upgrade]、[Activate, and Reload] などのソフトウェアアップデートの進行状況を示すアップデートステータスバーが表示されます。

ログを表示するには、[Show Install Logs] リンクをクリックします。

[Status] フィールドには、アップグレードの現在のステータスが表示され、実行する必要がある追加アクション示されます（ある場合）。

ウィンドウに表示されるその他の詳細は、[Total Number of APs]、[Initiated]、[Predownloading AP Image]、[Predownloading Controller Image]、[Completed Predownloading AP Image]、[Completed Predownloading Controller Image]、[Failed to Predownload AP Image]、[Failed to Predownload Controller Image] です。

現在アクティブな AP、スタンバイ状態の AP、および優先されるアクティブな AP も表示されます。

イメージのダウンロードシナリオ

Cisco 組み込みワイヤレスコントローラ ネットワークでは、組み込みワイヤレスコントローラから下位 AP へのイメージのダウンロードは、次のシナリオで実行されます。

- AP 接続中
- ネットワーク ソフトウェア アップグレード中（事前ダウンロード）

（注） EWC の展開の推奨事項は次のとおりです。

通常の EWC（AP 上の EWC）ネットワークでは、コントローライメージはすべての EWC 対応 AP に転送されます。ただし、メッシュトポロジでは、EWC 対応 MAP がある場合、ワイヤレスバックホールに追加のトラフィックフローが追加されるため、イメージのダウンロード手順が遅くなり、エラーが発生しやすくなります。この問題を改善するために、CAPWAP モードのときにコントローライメージが EWC 対応 MAP にコピーされないオプションが追加されました。MAP はコントローラを生成しないため、EWC 対応 MAP を CAPWAP AP に変更しても、EWC ネットワークの冗長設計には影響しません。

AP 接続中のイメージのダウンロード

古いソフトウェアを搭載した AP が Cisco 組み込みワイヤレスコントローラ ネットワークに接続しようとしている場合は、組み込みワイヤレスコントローラ最新のソフトウェアバージョンに一致するように自動的にアップグレードされます。組み込みワイヤレスコントローラは、新しい AP のソフトウェアバージョンをコントローラのソフトウェアバージョンと比較します。不一致がある場合、AP はコントローラにソフトウェアアップグレードを要求し、イメージのダウンロードがトリガーされます。組み込みワイヤレスコントローラにより、外部 TFTP サーバー、SFTP サーバーから新しい AP への最新ソフトウェアの転送が容易になります。

ネットワークに接続する新しい AP に応じて、次の 2 つのイメージのダウンロードが行われます。

- AP ソフトウェアイメージのダウンロード：Cisco 組み込みワイヤレスコントローラに接続するすべての新しい AP に適用されます。
- コントローラ ソフトウェア イメージのダウンロード：コントローラになることができ、Cisco 組み込みワイヤレスコントローラ ネットワークに接続しようとする Cisco Catalyst シリーズ APにのみ適用されます。

AP ソフトウェアイメージのダウンロード

Cisco Catalyst シリーズ AP または Cisco Aironet シリーズ Wave 2 AP は、その AP ソフトウェアイメージ バージョンがコントローラのバージョンと一致する場合にのみ 組み込みワイヤレスコントローラ に接続できます。

AP 接続プロセス中、組み込みワイヤレスコントローラにより最初に新しい AP の AP ソフトウェアイメージのバージョンがチェックされ、コントローラのバージョンと一致しない場合は、最新の AP ソフトウェアがコントローラから新しい AP にダウンロードされます。新しい AP の AP ソフトウェアイメージがネットワーク内の組み込みワイヤレスコントローラのバージョンと一致するようにアップグレードされると、新しいAPがリロードされます。新しいAPはアップグレードされた AP ソフトウェアイメージでバックアップされると、組み込みワイヤレスコントローラに接続します。

コントローラ ソフトウェア イメージのダウンロード

ネットワークに接続する新しい AP が組み込みワイヤレスコントローラになることが可能な Cisco Catalyst シリーズ AP 場合、コントローラはまず新しい AP の AP ソフトウェアイメージをチェックし、古い場合は、コントローラの AP ソフトウェアバージョンと一致するようにアップグレードします。その後、AP は新しい AP ソフトウェアイメージをリロードし、組み込みワイヤレスコントローラをネットワークに接続させます。

次に、組み込みワイヤレスコントローラは同様のチェックを実行して、組み込みワイヤレスコントローラ対応 AP のコントローラ ソフトウェア バージョンを比較します。AP ソフトウェアアップグレードと同様に、不一致がある場合、この Cisco Catalyst シリーズ AP のコントローラ ソフトウェアも組み込みワイヤレスコントローラの最新バージョンにアップグレードされます。AP が再びリロードされ、今度は、アップグレードされたコントローラ ソフトウェア イメージが使用されます。

効率的な AP 接続

Cisco 組み込みワイヤレスコントローラ ネットワークに、新たに接続した AP と同じイメージタイプの AP が含まれている場合、新しい AP はこの AP から AP ソフトウェアイメージをダウンロードします。たとえば、Cisco Catalyst 9130AX シリーズ AP が新たに Cisco 組み込みワイヤレスコントローラ ネットワークに接続し、別の Cisco Catalyst 9130AX シリーズ AP がネットワークにすでに存在している場合、新しい AP は、すでに接続している AP から AP ソフトウェアイメージを取得します。

効率的な AP 接続と呼ばれるこの方法により、同種の AP は、外部サーバーからソフトウェアをダウンロードするのではなく、ローカル（Cisco 組み込みワイヤレスコントローラ ネットワーク内）でソフトウェアを取得できるため、ソフトウェアのダウンロード効率が向上します。

ネットワークに接続して 組み込みワイヤレスコントローラ からソフトウェアをダウンロードするシリーズの最初の AP は、プライマリイメージと呼ばれます。同じシリーズの他の AP は、下位イメージとして知られています。

ネットワーク ソフトウェア アップグレード（事前ダウンロード）

事前ダウンロードのシナリオでは、Cisco 組み込みワイヤレスコントローラネットワークでイメージのダウンロードが発生し、すべての AP 上のソフトウェアがあるソフトウェアバージョンから別のバージョンにアップグレードされます。ただし、それらの AP は引き続き既存のクライアントと新しいクライアントにサービスを提供するため、ネットワークの中断はありません。

事前ダウンロードでは、すべての AP が安定した接続状態で組み込みワイヤレスコントローラに接続されている必要があります。事前ダウンロード中にイメージのダウンロードが開始されると、新しい AP は組み込みワイヤレスコントローラに接続できなくなります。

効率的な AP アップグレード

この方法では、組み込みワイヤレスコントローラからイメージを取得する AP シリーズの最初の AP がプライマリイメージになります。同じ AP シリーズの残りの AP は、下位のイメージであり、このプライマリイメージからローカルにソフトウェアイメージをダウンロードします。この方法は、効率的な AP アップグレードとも呼ばれます。

イメージのダウンロードでサポートされるメソッド

Cisco 組み込みワイヤレスコントローラ ネットワークでは、ソフトウェアイメージを 4 つの方法で組み込みワイヤレスコントローラからダウンロードできます。これらの方法は、コントローラがソフトウェアイメージを下位 AP に転送する場所に基づいています。

- 外部 TFTP サーバーから
- 外部 SFTP サーバーから
- デスクトップから（HTTP 経由）

TFTP イメージのダウンロードメソッド

TFTP メソッドでは、AP およびコントローラ ソフトウェア イメージは TFTP サーバーに保存されます。TFTP サーバーからソフトウェアイメージをダウンロードするには、TFTP サーバーの IP アドレスと、TFTP サーバー上のソフトウェア イメージ バンドルへのパスを指定する必要があります。

TFTP イメージのダウンロードメソッドは、GUI と CLI の両方を使用してトリガーできます。

SFTP イメージのダウンロードメソッド

SFTP メソッドでは、AP およびコントローラ ソフトウェア イメージは SFTP サーバーに保存されます。SFTP サーバーからソフトウェアイメージをダウンロードするには、SFTP サーバーの IP アドレスとソフトウェア イメージ バンドル パスに加えて、SFTP サーバーのログイン情報を指定する必要があります。

SFTP イメージのダウンロードメソッドは、GUI と CLI の両方を使用してトリガーすることもできます。

デスクトップ（HTTP）イメージのダウンロードメソッド

デスクトップ（HTTP）を介したイメージのダウンロードは、ネットワーク ソフトウェア アップグレード（事前ダウンロード）のシナリオにのみ適用されます。

デスクトップ（HTTP）方式の場合、Cisco 組み込みワイヤレスコントローラのソフトウェア イメージバンドルをコンピュータまたはラップトップデスクトップにダウンロードします。このダウンロードされたバンドルには、組み込みワイヤレスコントローラにアップロードする前にコンピュータまたはラップトップデスクトップに展開する必要がある AP およびコントローラ ソフトウェア イメージが含まれています。

デスクトップ（HTTP）方式は、同種のネットワークでのみ機能することに注意してください。同種の Cisco 組み込みワイヤレスコントローラ ネットワークは、同じ AP ソフトウェアイメージタイプを持つ AP を含むネットワークです。たとえば、Cisco Catalyst 9115AX シリーズ AP および Cisco Catalyst 9120AX シリーズ AP では、ap1g7 AP ソフトウェア イメージ ファイルが使用されるため、Cisco Catalyst 9115AX シリーズ および 9120AX シリーズ AP を含むこの例の Cisco 組み込みワイヤレスコントローラ ネットワークは、同種のネットワークです。

組み込みワイヤレスコントローラ CLI は、イメージのダウンロードのモードをデスクトップ（HTTP）として設定する場合にのみ使用できます。デスクトップ（HTTP）イメージのダウンロードメソッドを使用してネットワーク ソフトウェア アップグレード（事前ダウンロード）を設定およびトリガーするには、Cisco 組み込みワイヤレスコントローラ GUI を使用する必要があります。

イメージの並行ダウンロード

ソフトウェアとネットワークの更新により、Cisco 組み込みワイヤレス コントローラ ネットワーク内のすべてのアクセスポイントで最新のソフトウェアが実行されます。イメージのダウ

ンロードでサポートされるメソッドは、外部TFTPサーバー、外部SFTPサーバー、デスクトップ（HTTP 経由）、またはCCO 経由のメソッドです。

Cisco IOS XE Bengaluru 17.6.1 リリースでは、メッシュネットワークのイメージのダウンロード手順（サブツリー レベルごとのダウンロード）が適用され、Flex EWC ネットワークの全体的なプロセスがTFTPおよびSFTP用に機能強化されています。このイメージの新しいダウンロードメソッドは、並行ダウンロードと呼ばれます。この機能強化により、得られるメリットは大きくなります。

イメージのダウンロードプロセスには、通常、次の手順が含まれます。

1. アクティブ AP とスタンバイ AP のコントローライメージを取得します。
2. 外部のイメージサーバーから AP タイプごとに AP イメージを 1 回取得します。
3. 前述の AP から、同じタイプの他の AP にイメージを配布します。

新しいイメージのダウンロード手順は次のとおりです。

1. アクティブ AP とスタンバイ AP のコントローライメージを取得します。
2. TFTP や SFTP などの外部イメージサーバーからすべての AP イメージを並行して取得します。

（注） Cisco IOS XE Bengaluru 17.5.x 以前のリリースでは、イメージは最初にアクティブな EWC にコピーされてから、CAPWAP 経由でイメージマスターに送信されました。並行ダウンロードメソッドでは、イメージマスターがイメージを直接受け取ります。

TFTP の場合、AP はイメージサーバーに直接接続できる必要があります。SFTP には直接接続は必要ありません。

並行ダウンロードメソッドの導入により、ステップ 2 は迅速に終了し、ステップ 3 は以前よりも早く開始されます。

（注） EWC メッシュトポロジにおけるイメージの並行ダウンロードのコマンドでは、トポロジ階層が考慮され、RAPから始まるレベルごとにイメージが配布または事前ダウンロードされます。これにより、メッシュリンクを介してイメージを事前ダウンロードしている AP が、1 ホップ先の AP を見つけてイメージを提供できる可能性が高くなります。

3. 前述の AP から、同じタイプの他の AP にイメージを配布します。

イメージのダウンロードの前提条件

- AP が Cisco 組み込みワイヤレスコントローラ ネットワークに接続しているときにイメージをダウンロードするには、外部（TFTP または SFTP）サーバーへの接続が必要です。

- Cisco 組み込みワイヤレスコントローラ ネットワークでのネットワーク ソフトウェア アップグレード中にイメージをダウンロードするには、PC またはラップトップへの接続が必要です。
- すべての AP は、ネットワーク ソフトウェア アップグレード（事前ダウンロード）シナリオでのイメージのダウンロード用に 組み込みワイヤレスコントローラ に接続する必要があります。
- イメージのアップグレードの場合は、優先マスターを設定しないでください。優先マスターを設定する場合は、**show wireless ewc-ap redundancy summary** コマンドで表示される現在アクティブな AP を優先マスターが指していることを確認してください。

  別の AP が優先マスターとして設定されている場合、**install activate** ステップではアップグレードプロセスは実行されません。アップグレードが実行されない場合は、優先マスターの設定を削除するか、現在アクティブな AP に一致するように優先マスターを再設定してから、**install activate** コマンドを再度実行する必要があります。
-

イメージのダウンロードプロファイルの設定

AP 接続イメージのダウンロードと事前ダウンロードの両シナリオに対して、イメージのダウンロードプロファイルを設定する必要があります。サポートされている唯一のプロファイルは default です。Cisco 組み込みワイヤレスコントローラネットワークでは、default-site-tag の 1 つのサイトタグのみがサポートされています。default イメージのダウンロードプロファイルは、default-site-tag に添付されます。

（注） 異なるタイプの AP が、イメージのアップグレードのために以前 HTTP モードを使用していた同種のネットワークに接続しようとすると、AP の接続に失敗します。この失敗を回避するには、**wireless profile image-download default** 設定手順で **image-download-mode** を **tftp**に更新する必要があります。

TFTP イメージのダウンロードの設定（GUI）

手順

ステップ 1 **[Administration]** > **[Software Management]** を選択します。

ステップ 2 [Software Management] ページの [Software Upgrade] タブで、[Mode] として [TFTP] を選択します。

ステップ 3 [Image Server] フィールドに、TFTP サーバーの IP アドレスを入力します。

ステップ 4 [Image Path] フィールドに、ソフトウェア イメージ バンドルへの絶対パスまたは相対パスを入力します。

ステップ 5 次のいずれかを選択します。

- [Save]：イメージのダウンロードプロファイルを保存し、Cisco 組み込みワイヤレスコントローラ ネットワークに接続する新しい AP のイメージのダウンロードを有効にするには、このオプションを選択します。
- [Save & Download]：設定を保存し、ネットワーク ソフトウェア アップグレード（事前ダウンロード）を有効にするには、このオプションを選択します。イメージのダウンロードプロファイルは保存され（設定が変更されていない場合も保存）、最新のイメージがバックグラウンドでダウンロードされるため、AP は引き続きクライアントにサービスを提供できます。
- [Activate]：ネットワーク内の AP が最新のイメージにスワップして再起動できるようにするには、このオプションを選択します。APが新しいイメージファイルで起動すると、Cisco 組み込みワイヤレスコントローラ ネットワークがアクティブになります。
- [Cancel]：イメージのダウンロードプロファイルに加えられた変更をキャンセルするには、このオプションを選択します。

オプション	説明
Save	イメージのダウンロードプロファイルを保存し、Cisco 組み込みワイヤレスコントローラ ネットワークに接続する新しい AP のイメージのダウンロードを有効にするには、このオプションを選択します。
Save & Download	設定を保存し、ネットワーク ソフトウェア アップグレード（事前ダウンロード）を有効にするには、このオプションを選択します。イメージのダウンロードプロファイルは保存され（設定が変更されていない場合も保存）、最新のイメージがバックグラウンドでダウンロードされるため、AP は引き続きクライアントにサービスを提供できます。
アクティブ化	ネットワーク内の AP が最新のイメージにスワップして再起動できるようにするには、このオプションを選択します。AP が新しいイメージファイルで起動すると、Cisco 組み込みワイヤレスコントローラ ネットワークがアクティブになります。
キャンセル	イメージのダウンロードプロファイルに加えられた変更をキャンセルするには、このオプションを選択します。

TFTP イメージのダウンロードの設定（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。
ステップ 2	（任意） **wireless ewc-ap image-download parallel** 例： `Device (config)# wireless ewc-ap image-download parallel`	ネットワークのアップグレード中に、AP イメージの並行ダウンロードを有効にします。このコマンドは、メッシュ ネットワークにおけるレベルごとのイメージのダウンロードに必要です。
ステップ 3	**wireless profile image-download default** 例： `Device (config)# wireless profile image-download default`	デフォルトの AP プロファイルを設定します。
ステップ 4	**image-download-mode tftp** 例： `Device(config-wireless-image-download-profile)# image-download-mode tftp`	TFTP を使用してイメージのダウンロードを設定します。
ステップ 5	**tftp-image-server** *server-ip* 例： `Device(config-wireless-image-download-profile-tftp)# tftp-image-server 10.1.1.1`	IPv4 または IPv6 *server-ip* アドレスを指定して、イメージのダウンロード用の TFTP サーバーを構成します。
ステップ 6	**tftp-image-path** *server-path* 例： `Device(config-wireless-image-download-profile-tftp)# tftp-image-path /download/object/stream/images/ap-images`	TFTP サーバー上のソフトウェアイメージへの絶対パスまたは相対パスを設定します。
ステップ 7	**end** 例： `Device(config-wireless-image-download-profile-tftp)# 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。

SFTP イメージのダウンロードの設定（GUI）

手順

ステップ 1 **[Administration]** > **[Software Management]** を選択します。

ステップ 2 [Software Management] ページの [Software Upgrade] タブで、[Mode] として [SFTP] を選択します。

SFTP ポートは設定できず、22 に固定されています。

ステップ 3 [Image Server] フィールドに、SFTP サーバーの IP アドレスを入力します。

ステップ 4 [Image Path] フィールドに、ソフトウェア イメージ バンドルへのパスを入力します。

ステップ 5 [User Name] フィールドに、SFTP サーバーのユーザー名を入力します。

ステップ 6 適切な [Password Type]（[Unencrypted] または [AES Encrypted]）を選択します。

ステップ 7 [Password] フィールドに、SFTP サーバーのパスワードを入力します。

ステップ 8 次のいずれかを選択します。

オプション	説明
Save	イメージのダウンロードプロファイルを保存し、Cisco 組み込みワイヤレスコントローラ ネットワークに接続する新しい AP のイメージのダウンロードを有効にするには、このオプションを選択します。
Save & Download	設定を保存し、ネットワーク ソフトウェア アップグレード（事前ダウンロード）を有効にするには、このオプションを選択します。イメージのダウンロードプロファイルは保存され（設定が変更されていない場合も保存）、最新のイメージがバックグラウンドでダウンロードされるため、AP は引き続きクライアントにサービスを提供できます。
アクティブ化	ネットワーク内の AP が最新のイメージにスワップして再起動できるようにするには、このオプションを選択します。AP が新しいイメージファイルで起動すると、Cisco 組み込みワイヤレスコントローラ ネットワークがアクティブになります。
キャンセル	イメージのダウンロードプロファイルに加えられた変更をキャンセルするには、このオプションを選択します。

SFTP イメージのダウンロードの設定（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。
ステップ 2	（任意） **wireless ewc-ap image-download parallel** 例： `Device (config)# wireless ewc-ap image-download parallel`	ネットワークのアップグレード中に、AP イメージの並行ダウンロードを有効にします。このコマンドは、メッシュ ネットワークにおけるレベルごとのイメージのダウンロードに必要です。
ステップ 3	**wireless profile image-download default** 例： `Device (config)# wireless profile image-download default`	デフォルトの AP プロファイルを設定します。
ステップ 4	**image-download-mode sftp** 例： `Device(config-wireless-image-download-profile)# image-download-mode sftp`	SFTP を使用してイメージのダウンロードを設定します。
ステップ 5	**sftp-image-server** *server-ip* 例： `Device(config-wireless-image-download-profile-sftp)# sftp-image-server 10.1.1.1`	IPv4 または IPv6 *server-ip* アドレスを指定して、イメージのダウンロード用の SFTP サーバーを設定します。
ステップ 6	**sftp-image-path** *server-path* 例： `Device(config-wireless-image-download-profile-sftp)# sftp-image-path /download/object/stream/images/ap-images`	SFTP サーバー上のソフトウェアイメージへのパスを設定します。
ステップ 7	**sftp-username** *username* 例： `Device(config-wireless-image-download-profile-sftp)# sftp-username test`	イメージのダウンロードのために SFTP サーバーにログインするためのユーザー名を指定します。
ステップ 8	**sftp-password** {**0** | **8**} *password* 例：	前述のユーザー名に関連付けられたパスワードを指定して、SFTP サーバーからイメージをダウンロードします。エント

	コマンドまたはアクション	目的
	Device(config-wireless-image-download-profile-sftp)# **sftp-password 0** *password1*	リの確認のためにパスワードを再入力する必要があります。 AES 暗号化パスワードを設定する場合は 8 を指定し、暗号化されていないパスワードを設定する場合は 0 を指定します。
ステップ 9	**end** 例： Device(config-wireless-image-download-profile-tftp)# **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。

ソフトウェアアップグレード用の CCO モードの設定（GUI）

始める前に

CCO アカウントには、CCO プロファイルマネージャで入力した物理アドレスが設定されている必要があり、EULA と K9 が承認されている必要があります。CCO アカウントの作成の詳細については、https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html [英語] を参照してください。

手順

ステップ 1 **[Administration]** > **[Software Management]** を選択します。

ステップ 2 [Software Management] ページの [Software Upgrade] タブで、[Mode] として [CCO] を選択します。

ステップ 3 [User Name] フィールドに、CCO ユーザー名を入力します。

ステップ 4 [Password] フィールドに、CCO サーバーにアクセスするためのパスワードを入力します。

ステップ 5 適切な [Password Type]（[Unencrypted] または [AES Encrypted]）を選択します。

ステップ 6 [Automatically Check for Updates] フィールドから [Enabled] または [Disabled] を選択します。このオプションを有効にすると、ソフトウェアアップデートが自動的にチェックされます。

間隔は 30 日間です。間隔が経過すると、コントローラにより、コントローラ設定内の最新または推奨ソフトウェアバージョン情報が自動的にチェックされて更新されます。

ステップ 7 [Software Check] フィールドで、[Check now] ボタンをクリックして、最新のソフトウェアリリース（CCO の Web サイトで入手可能な最新バージョン）のバージョン番号および推奨ソフトウェアリリース（現在実行中のソフトウェアの推奨ソフトウェアバージョン）のバージョン番号に関する最新情報を取得します。

ステップ 8 [Last CCO Response] フィールドには、CCO イメージのダウンロードメソッドを設定するときに発生したエラーメッセージが表示されます。たとえば、間違ったユーザー名とパスワードを

入力した場合、エラーメッセージ「HTTP 400 Error: 400 Client Error: Bad Request for url: https://cloudsso.cisco.com/as/token.oauth2 Please check your username/password and try again」が表示されます。https://cloudsso.cisco.com/as/token.oauth2[Last CCO Response] エラーメッセージの詳細については、トラブルシューティング：CCOイメージのダウンロードエラーメッセージ（424ページ）を参照してください。

ステップ 9 [Version] ドロップダウンリストから、[Version] または [Latest] を選択します。最新の推奨ソフトウェアバージョンを取得したら、アップグレードするバージョンを選択できます。

ステップ 10 次のいずれかを選択します。

オプション	説明
Save	イメージのダウンロードプロファイルを保存し、Cisco 組み込みワイヤレスコントローラ ネットワークに接続する新しい AP のイメージのダウンロードを有効にするには、このオプションを選択します。
Save & Download	設定を保存し、ネットワーク ソフトウェア アップグレード（事前ダウンロード）を有効にするには、このオプションを選択します。イメージのダウンロードプロファイルは保存され（設定が変更されていない場合も保存）、最新のイメージがバックグラウンドでダウンロードされるため、AP は引き続きクライアントにサービスを提供できます。
アクティブ化	ネットワーク内の AP が最新のイメージにスワップして再起動できるようにするには、このオプションを選択します。AP が新しいイメージファイルで起動すると、Cisco 組み込みワイヤレスコントローラ ネットワークがアクティブになります。
キャンセル	イメージのダウンロードプロファイルに加えられた変更をキャンセルするには、このオプションを選択します。

CCO イメージのダウンロードの設定（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。
ステップ 2	**wireless profile image-download default** 例： `Device (config)# wireless profile image-download default`	デフォルトの 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 3	**image-download-mode cco** 例： `Device(config-wireless-image-download-profile)# image-download-mode cco`	CCO を使用してイメージのダウンロードを設定します。
ステップ 4	**cco-username** *username* 例： `Device(config-wireless-image-download-profile-cco)# cco-username username`	イメージのダウンロードのために CCO サーバーにログインするためのユーザー名を指定します。
ステップ 5	**cco-password** {**0** | **8**} *password* 例： `Device(config-wireless-image-download-profile-cco)# cco-password 0 password1`	前述のユーザー名に関連付けられたパスワードを指定して、CCO サーバーからイメージをダウンロードします。エントリの確認のためにパスワードを再入力する必要があります。 AES 暗号化パスワードを設定する場合は 8 を指定し、暗号化されていないパスワードを設定する場合は 0 を指定します。
ステップ 6	**cco-version** {**latest** | **suggested**} 例： `Device(config-wireless-image-download-profile-cco)# cco-version latest`	CCO サーバーからダウンロードする最新または推奨バージョンを指定します。デフォルトでは、推奨バージョンがダウンロードされます。
ステップ 7	**cco-auto-check** 例： `Device(config-wireless-image-download-profile-cco)# cco-auto-check`	CCO での 30 日ごとの新しいソフトウェアバージョンの自動チェックを有効または無効にします。これは、イメージのアップグレードまたは事前ダウンロードにのみ適用されます。デフォルトでは、 **cco-auto-check** が有効になっています。このコマンドを無効にするには、コマンドの **no** 形式を使用します。
ステップ 8	**end** 例： `Device(config-wireless-image-download-profile-cco)# 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。
ステップ 9	**wireless ewc-ap predownload poll-cco** 例： `Device# wireless ewc-ap predownload poll-cco`	CCO サーバーをポーリングして、最新のソフトウェアバージョンを確認します。

	コマンドまたはアクション	目的
ステップ 10	**clear ap predownload statistics** 例： `Device# clear ap predownload statistics`	AP事前ダウンロードの統計情報をクリアします。
ステップ 11	**install remove profile default** 例： `Device# install remove profile default`	イメージのダウンロードプロファイルを削除します。 [Y] を選択してプロファイルを削除するか、[N] を選択してキャンセルします。
ステップ 12	**install add profile default** 例： `Device# clear ap predownload statistics`	組み込みワイヤレスコントローラからコントローラと AP ソフトウェアのイメージをダウンロードします。 コントローライメージは、すべてのCisco組み込みワイヤレスコントローラ対応 AP に送信されます。APイメージは、同じイメージタイプを共有するすべての AP にダウンロードされます
ステップ 13	**install activate** 例： `Device# install activate`	アップグレード後にネットワークをアクティブにします。 すべての下位APが新しいAPイメージを取得して再起動します。すべてのAPが再起動すると、組み込みワイヤレスコントローラも再起動します。 （注） コントローライメージがダウンロードされたが、すべての AP が事前ダウンロード経由で AP イメージを受信していない場合にも、ネットワークをアクティブにできます。

	コマンドまたはアクション	目的
		重要 部分的な事前ダウンロードが成功している間にネットワークがアクティブになり、古いコントローラソフトウェアを搭載した Cisco 組み込みワイヤレスコントローラ 対応の AP がコントローラになる場合、ネットワークは新しいイメージにアップグレードされません。
ステップ 14	**install commit** 例： `Device# install commit`	再起動後に組み込みワイヤレスコントローラ が起動したら、現在のソフトウェアイメージをコミットします。 （注） アップグレード中は、アクティベーションプロセスが失敗するため、単一のコマンドで **add**、**active**、**commit** キーワードを使用しないでください。

トラブルシューティング：CCO イメージのダウンロード エラー メッセージ

次に、予期されるエラーメッセージと原因を示します。これらは、[Last CCO Response] フィールドに表示されます。

DNS 解決または接続の問題

接続エラー：HTTPSConnectionPool(host='cloudsso.cisco.com', port=443)：URL での最大再試行回数を超えました：/as/token.oauth2 (Caused by NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object at 0xf6170250>：新しい接続の確立に失敗しました：[Errno -3] 名前解決の一時的な失敗',))

CCO ユーザー名/パスワードエラー

HTTP 400 Error: 400 Client Error: Bad Request for url: https://cloudsso.cisco.com/as/token.oauth2 ユーザー名/パスワードを確認して、再試行してください。

アドレスの欠落例外

Cisco.com にご登録いただきありがとうございます。ソフトウェアまたはサービスを使用するためには、完全な住所を入力していただく必要があります。このリンクをたどってプロファイルマネージャに戻り、プロファイルを完成させてください。

EULA フォームの欠落例外

EULA フォームが受け入れられなかったか、またはダウンロードを続行することを拒否されました。https://software.cisco.com/download/eula にアクセスしてください。

K9 フォームの欠落例外

K9 フォームが受け入れられなかったか、またはダウンロードを続行することを拒否されました。https://software.cisco.com/download/k9 にアクセスしてください。

デスクトップ（HTTP）イメージのダウンロードの設定（GUI）

- デスクトップ（HTTP）を使用したイメージのダウンロードは、同種ネットワーク、つまり同じイメージタイプの AP を含むネットワークでのみ有効です。
- デスクトップ（HTTP）を使用したイメージのダウンロードは、GUI からのみ設定できます。
- CLI は、イメージのダウンロードモードをデスクトップ（HTTP）に設定する場合にのみ使用できます。

手順

ステップ 1 **[Administration]** > **[Software Management]** を選択します。

ステップ 2 [Software Management] ページの [Software Upgrade] タブで、[Mode] として [Desktop (HTTP)] を選択します。

ステップ 3 [Controller Image] フィールドで、コンピュータまたはラップトップデスクトップの 組み込みワイヤレスコントローラ ソフトウェアイメージに移動します。

ステップ 4 [AP Image] フィールドで、コンピュータまたはラップトップデスクトップの AP ソフトウェアイメージに移動します。

GUI には、使用する AP イメージの名前が表示されます。AP モデルによって、AP イメージの名前は異なります。

ステップ 5 次のいずれかを選択します。

オプション	説明
Save	イメージのダウンロードプロファイルを保存し、Cisco 組み込みワイヤレスコントローラ ネットワークに接続する新しい AP のイメージのダウンロードを有効にするには、このオプションを選択します。
Save & Download	設定を保存し、ネットワーク ソフトウェア アップグレード（事前ダウンロード）を有効にするには、このオプションを選択します。イメージのダウンロードプロファイルは保存され（設定が変更されていない場合も保存）、最新のイメージがバックグラウンドでダウンロードされるため、AP は引き続きクライアントにサービスを提供できます。
アクティブ化	ネットワーク内の AP が最新のイメージにスワップして再起動できるようにするには、このオプションを選択します。AP が新しいイメージファイルで起動すると、Cisco 組み込みワイヤレスコントローラ ネットワークがアクティブになります。
キャンセル	イメージのダウンロードプロファイルに加えられた変更をキャンセルするには、このオプションを選択します。

事前ダウンロードの開始（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless ewc-ap predownload poll-cco**	イメージのアップグレードについては、最新の推奨バージョンを確認してください。
ステップ 2	**clear ap predownload statistics**	AP 事前ダウンロードの統計情報をクリアします。
ステップ 3	**install remove profile default**	イメージのダウンロードプロファイルを削除します。 [Y] を選択してプロファイルを削除するか、[N] を選択してキャンセルします。
ステップ 4	**install add profile default**	組み込みワイヤレスコントローラからコントローラと AP ソフトウェアのイメージをダウンロードします。 コントローライメージは、すべての Cisco 組み込みワイヤレスコントローラ対応 AP に送信されます。AP イメージ

	コマンドまたはアクション	目的
		は、同じイメージタイプを共有するすべての AP にダウンロードされます。
ステップ 5	**show wireless ewc-ap predownload status**	ソフトウェアのダウンロードステータス全体を監視します。 ステータスメッセージが `Controller Image Predownload to EWC Capable APs Complete` の場合、ダウンロードは成功しています。
ステップ 6	**install activate**	アップグレード後にネットワークをアクティブにします。 すべての下位 AP が新しい AP イメージを取得して再起動します。すべての AP が再起動すると、 組み込みワイヤレスコントローラも再起動します。 （注） コントローライメージがダウンロードされたが、すべての AP が事前ダウンロード経由で AP イメージを受信していない場合にも、ネットワークをアクティブにできます。 **重要** 部分的な事前ダウンロードが成功している間にネットワークがアクティブになり、古いコントローラソフトウェアを搭載した Cisco 組み込みワイヤレスコントローラ 対応の AP がコントローラになる場合、ネットワークは新しいイメージにアップグレードされません。
ステップ 7	**show install summary**	再起動後に現在のイメージステータスを確認します。 ステータスが `Activated and Uncommitted` の場合は、ステップ 7 に進み、それ以外の場合は待機します。

	コマンドまたはアクション	目的
ステップ 8	**install commit**	再起動後に 組み込みワイヤレスコントローラが起動したら、現在のソフトウェアイメージをコミットします。 （注） アップグレード中は、アクティベーションプロセスが失敗するため、単一のコマンドで **add**、**active**、**commit** キーワードを使用しないでください。

イメージのアップグレードプロセス中、イメージの事前ダウンロードステータスは、「コントローライメージのダウンロードが進行中」、「AP イメージの事前ダウンロードが進行中」、「EWC 対応 AP へのコントローライメージの事前ダウンロードが進行中」など、さまざまな段階で表示されます。イメージのアップグレードは、さまざまな理由で失敗することがあり、失敗した場合、各 AP の個別の事前ダウンロードステータスを表示する **show wireless ewc-ap ap image predownload status** コマンドの出力に基づいて、**install activate** 操作を続行するか、またはキャンセルできます。

イメージのダウンロードの確認

事前ダウンロード中にソフトウェアのダウンロードプロセスの全体的な進行状況を監視するには、次のコマンドを実行します。

```
Device# show wireless ewc-ap predownload status
```

次に、事前ダウンロード操作のステータスを示すさまざまなステータスメッセージを示します。各メッセージは、**show wireless ewc-ap predownload status** コマンドを実行すると表示されます。

- なし
- コントローライメージのダウンロードが開始されました
- コントローライメージのダウンロードが進行中です
- コントローライメージのダウンロードが完了しました
- コントローライメージのダウンロードが失敗しました
- AP イメージの事前ダウンロードが開始されました
- AP イメージの事前ダウンロードが進行中です
- AP イメージの事前ダウンロードが完了しました
- AP イメージの事前ダウンロードはサポートされていません

- AP イメージの事前ダウンロードが失敗しました
- EWC 対応 AP へのコントローライメージの事前ダウンロードが進行中です
- EWC 対応 AP へのコントローライメージの事前ダウンロードが完了しました
- EWC 対応 AP へのコントローライメージの事前ダウンロードに失敗しました
- イメージのアクティブ化に成功しました
- イメージのアクティブ化に失敗しました
- 無効な状態

AP イメージの事前ダウンロード統計を表示するには、次のコマンドを実行します。

```
Device# show wireless ewc-ap ap image predownload status
Total number of APs                          : 5
Total number of EWC capable APs              : 4
Number of APs
        Initiated                            : 0
        Predownloading AP image              : 0
        Predownloading Controller image      : 1
        Completed predownloading AP          : 5
        Completed predownloading Controller : 0
        Failed to Predownload AP             : 0
        Failed to Predownload Controller     : 0
AP Name               Primary Image (AP/Controller)         Backup Image (AP/Controller)
           Predownload Status          Predownload Version                     AP Image
  Role    Retries  AP image       Controller image

                                                                                  Type
                      ETA/Percent    ETA/Percent
-----------------------------------------------------------------------------------------
APXXXX.9XXX.8FXX       17.3.0.85      /17.3.01.0.XXXX         17.2.2.2
/17.2.02.0.XXXX         Complete                    17.2.2.2       /17.2.02.0.2XXX
   ap1g7       Slave   0        00:00:00/100%  00:00:00/  0%
APXXXX.5XXX.71XX       17.3.0.85      /                       17.2.2.2       /
              Complete                    17.2.2.2       /                       ap1g5
     Master  0        00:00:00/100%  00:00:00/  0%
APXXXX.8XXX.59XX       17.3.0.85      /17.3.01.0.XXXX         17.2.2.2
/17.2.02.0.XXXX         Complete                    17.2.2.2       /
   ap1g7       Slave   0        00:00:00/100%  00:00:00/  0%
APXXXX.8XXX.5AXX      17.3.0.85     /17.3.01.0.XXXX        17.2.2.2      /17.3.01.0.XXX
          Controller Predownloading  17.2.2.2       /                       ap1g7
 Master  0        00:00:00/100%  00:00:00/  0%
APXXXX.8XXX.5BXX       17.3.0.85      /17.3.01.0.XXXX         17.2.2.2       /
              Complete                    17.2.2.2       /                       ap1g7
     Slave   0        00:00:00/100%  00:00:00/  0%
```

プライマリイメージとして機能する AP の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless ewc-ap image-master
Image Master List
Image Name: ap1g7
-----------------------------------------------------------------------------------------------------
Master AP MAC                AP                          AP                 Controller
            Controller
                 Predownload In Progress   Predownload Complete     Predownload In
Progress  Predownload Complete
-----------------------------------------------------------------------------------------------------
c0XX.eXXX.90XX    No                          No                       No
```

```
      Yes
Image Name: ap1g5
-------------------------------------------------------------------------------------------------------------
Master AP MAC                AP                          AP                  Controller
           Controller
                Predownload In Progress   Predownload Complete     Predownload In
Progress  Predownload Complete
-------------------------------------------------------------------------------------------------------------
70XX.1XXX.4bXX    No                          No                       No
      Yes
```

全 AP のイメージのダウンロードステータスを確認するには、次のコマンドを実行します。

```
Device# show ap image
```

イメージのダウンロード中に AP ステータスを確認するには、次のコマンドを実行します。

```
Device# show ap summary
```

効率的な AP 接続ステータスを監視するには、次のコマンドを実行します。

```
Device# show ap master list
```

最後の AP イメージのダウンロード試行の詳細を表示するには、次のコマンドを実行します。

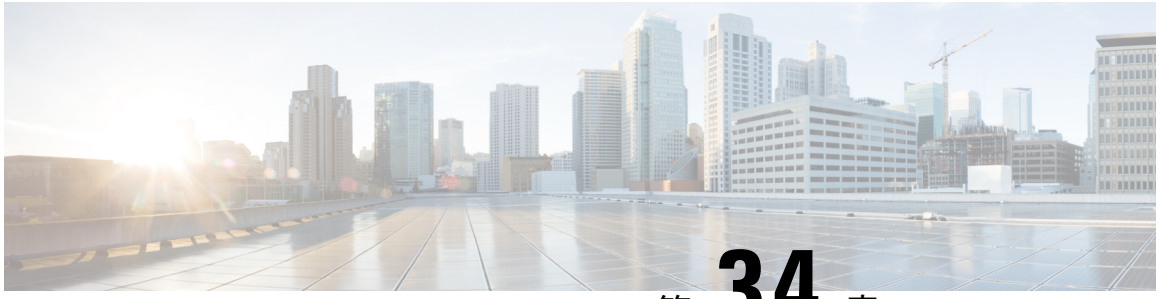
```
Device# show wireless stats ap image-download
```

アップグレードされたイメージの最新ステータスを確認するには、次のコマンドを使用します。

```
Device# show install summary
```

外部サーバー（TFTP または SFTP）からのダウンロードステータスを確認するには、次のコマンドを実行します。

```
Device# show install log
```



第 34 章

条件付きデバッグとラジオアクティブ トレース

条件付きデバッグの概要

条件付きデバッグ機能によって、定義した条件に基づき、特定の機能のデバッグおよびロギングを選択して有効にすることができます。この機能は、多くの機能がサポートされているシステムで有用です。

条件付きデバッグでは、多数の機能が導入されていて大規模に稼働しているネットワークにおけるきめ細かなデバッグが可能です。これにより、システム内の細かなインスタンスに対しても、詳細なデバッグを実行できます。これは、何千ものセッションのうちの特定のセッションのみをデバッグするような場合に、非常に有用です。条件は複数指定することもできます。

条件とは、機能またはアイデンティティをいいます。アイデンティティは、インターフェイス、IP アドレス、MAC アドレスなどです。

これは、処理する機能オブジェクトを区別せずに出力を生成する、一般的なデバッグ コマンドとは対照的です。一般的なデバッグ コマンドは、多数のシステム リソースを消費し、システム パフォーマンスに影響します。

ラジオアクティブ トレースの概要

ラジオアクティブ トレース（RA）により、冗長性のレベルを高めた状態で、システムの全体にわたって目的とする動作を連鎖的に実行できます。また、複数のスレッド、プロセス、および関数呼び出しにわたって、デバッグ情報を条件に基づいて（DEBUG レベルまで、または指定のレベルまで）出力する方法を提供します。

（注）

- ラジオアクティブ トレースではファーストホップ セキュリティ（FHS）がサポートされています。
- 証明書が有効でない場合、ラジオアクティブ トレース フィルタは機能しません。
- メッシュ機能の問題を効果的にデバッグできるようにするため、ログの収集時に、イーサネット アドレスと無線 MAC アドレスの両方を RA トレースの条件付き MAC として追加してください。
- ワイヤレス IP のデバッグを有効にするには、**debug platform condition feature wireless ip** *ip-address* コマンドを使用します。

条件付きデバッグおよび放射線トレース

条件付きデバッグと組み合わせた放射線トレースによって、条件に関連するすべての実行コンテキストをデバッグする単一のデバッグCLIを取得できます。これは、ボックス内の機能のさまざまな制御フロー プロセスを認識していなくても行うことができ、これらのプロセスでデバッグを個別に発行する必要もありません。

（注） プラットフォームに適用されているデバッグ条件を削除するには、clear platform condition all コマンドを使用します。

トレースファイルの場所

デフォルトでは、トレースファイルログは各プロセスで生成され、**/tmp/rp/trace** または **/tmp/fp/trace** ディレクトリに保存されます。この一時ディレクトリで、トレース ログがファイルに書き込まれます。各ファイルは 1 MB サイズです。これらのログ（プロセス単位）は **show platform software trace message** *process_name***chassis active R0** コマンドを使用して確認できます。このディレクトリでは、特定のプロセスのこうしたファイルを、最大 25 件保持できます。**/tmp** ディレクトリのトレースファイルがその 1 MB 制限またはブート時に設定されたサ

イズに達した場合、ローテーションから外れ、**tracelogs** ディレクトリの **/crashinfo** パーティションの下にあるアーカイブの場所に移動します。

/tmp ディレクトリが 1 つのプロセスで保持するトレースファイルは 1 つのみです。ファイルがそのファイル サイズの制限に達すると、ローテーションから外れ、**/crashinfo/tracelogs** に移動します。アーカイブ ディレクトリに蓄積されるファイルは最大 25 ファイルであり、その後は最も古いものから順に、**/tmp** から新たにローテーションされたファイルに置換されます。ファイルサイズはプロセスに依存し、一部のプロセスではより大きなファイルサイズ（最大10MB）が使用されます。同様に、tracelogsディレクトリ内のファイル数もプロセスによって決定されます。たとえば、WNCDプロセスでは、プラットフォームに応じて、インスタンスごとに400ファイルの制限が使用されます。

crashinfo ディレクトリ内のトレースファイルは次の形式で配置されます。

1. Process-name_Process-ID_running-counter.timestamp.gz

   例：IOSRP_R0-0.bin_0.14239.20151101234827.gz

2. Process-name_pmanlog_Process-ID_running-counter.timestamp.bin.gz

   例：wncmgrd_R0-0.27958_1.20180902081532.bin.gz

条件付きデバッグの設定（GUI）

手順

ステップ 1 **[Troubleshooting]** > **[Radioactive Trace]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [MAC/IP Address] を入力します。MAC アドレスは、xx:xx:xx:xx:xx:xx、xx-xx-xx-xx-xx-xx、または xxxx.xxxx.xxxx のいずれかの形式で指定できます。

ステップ 4 [Apply to Device] をクリックします。

ステップ 5 条件付きデバッグを開始する場合は [Start]、停止する場合は [Stop] をクリックしします。

ステップ 6 [Generate] をクリックして、放射線トレースログを作成します。

ステップ 7 オプションボタンをクリックして、時間間隔を設定します。

ステップ 8 トレースファイル名の横に表示される [Download Logs] アイコンをクリックして、ログをローカルフォルダにダウンロードします。

ステップ 9 トレースファイル名の横に表示される [View Logs] アイコンをクリックして、GUI ページでログファイルを表示します。[Load More] をクリックして、ログファイルの他の行を表示します。

ステップ 10 [Apply to Device] をクリックします。

条件付きデバッグの設定

条件付きデバッグを設定するには、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	**debug platform condition feature wireless mac** {*mac-address*} 例： デバイス# **debug platform condition feature wireless mac b838.61a1.5433**	指定されたMACアドレスを使用する機能の条件付きデバッグを設定します。 （注） これは、APまたはクライアントMAC/IPでサポートされ、CMXIPアドレスとモビリティピアIPでもサポートされます。
ステップ 2	**debug platform condition start** 例： デバイス# **debug platform condition start**	条件付きデバッグを開始します（上記のいずれかの条件に一致すると放射線トレースを開始します）。 （注） これは、APまたはクライアントMAC/IPでサポートされ、CMXIPアドレスとモビリティピアIPでもサポートされます。
ステップ 3	**show platform condition** または **show debug** 例： デバイス# **show platform condition** デバイス# **show debug**	現在設定されている条件を表示します。
ステップ 4	**debug platform condition stop** 例： デバイス# **debug platform condition stop**	条件付きデバッグを停止します（放射線トレースを停止します）。 （注） これは、APまたはクライアントMAC/IPでサポートされ、CMXIPアドレスとモビリティピアIPでもサポートされます。
ステップ 5	**show logging profile wireless** [**counter** | **[last]**{*x days/hours*} | **filter mac**{<*mac address*>} **[to-file]**{<*destination*>}	最新のワイヤレスプロファイルからのログを表示します。

	コマンドまたはアクション	目的
	例： デバイス# **show logging profile wireless start last 20 minutes to-file bootflash:logs.txt**	（注） ログを収集するには、show logging profile wireless コマンドまたは show logging process コマンドを使用できます。
ステップ 6	**show logging process** <*process name*> 例： デバイス# **show logging process wncd to-file flash:wncd.txt**	プロセスに固有のログコレクションを表示します。
ステップ 7	**clear platform condition all** 例： デバイス# **clear platform condition all**	すべての条件をクリアします。

次のタスク

（注） コマンド **request platform software trace filter-binary wireless** {*mac-address*} は次の 3 つのフラッシュファイルを生成します。

- *collated_log_<.date..>*
- *mac_log <..date..>*
- *mac_database .. file*

その中でも、mac_log <..date..> は最も重要なファイルで、デバッグする MAC 用のメッセージが含まれます。コマンド **show platform software trace filter-binary** も同じフラッシュ ファイルを生成し、また、画面に mac_log を出力します。

トレース ファイルの推奨ワークフロー

1. 特定の時間帯のトレースログを要求する場合。

   たとえば 1 日。

   使用するコマンドは、次のとおりです。

   デバイス#**show logging process wncd to-file flash:wncd.txt**

2. ロケーション（/flash:）にトレースログのテキストファイルが生成されます。

3. デバイスの外にファイルをコピーします。ファイルをコピーすることによって、オフラインでトレースログが使用できます。ファイルのコピーについての詳細は、次のセクションを参照してください。
4. ロケーション（/flash:）からトレースログファイル（.txt）を削除します。これにより、他の操作に十分な領域がデバイスに確保されます。

ボックス外へのトレースファイルのコピー

トレース ファイルの例を以下に示します。

```
デバイス# dir flash:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
```

トレース ファイルは、次に示すさまざまなオプションのいずれかを使用して、コピーできます。

```
デバイス# copy flash:/tracelogs ?
  crashinfo: Copy to crashinfo: file system
  flash: Copy to flash: file system
  ftp: Copy to ftp: file system
  http: Copy to http: file system
  https: Copy to https: file system
  null: Copy to null: file system
  nvram: Copy to nvram: file system
  rcp: Copy to rcp: file system
  running-config Update (merge with) current system configuration
  scp: Copy to scp: file system
  startup-config Copy to startup configuration
  syslog: Copy to syslog: file system
  system: Copy to system: file system
  tftp: Copy to tftp: file system
  tmpsys: Copy to tmpsys: file system
```

TFTP サーバーにコピーするための一般的な構文は次のとおりです。

```
デバイス# copy source: tftp:
デバイス# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```

（注） tracelogおよび他の目的に使用可能な空き容量があることを確認するために、生成されたレポート/アーカイブ ファイルをスイッチからクリアすることが重要です。

条件付きデバッグの設定例

次に、*show platform condition* コマンドの出力例を示します。

```
デバイス# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|-----------------------|--------------------------------
デバイス#
```

次に、*show debug* コマンドの出力例を示します。

```
デバイス# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|-----------------------|--------------------------------
Packet Infra debugs:
Ip Address Port
------------------------------------------------------|----------
デバイス#
```

条件付きデバッグの確認

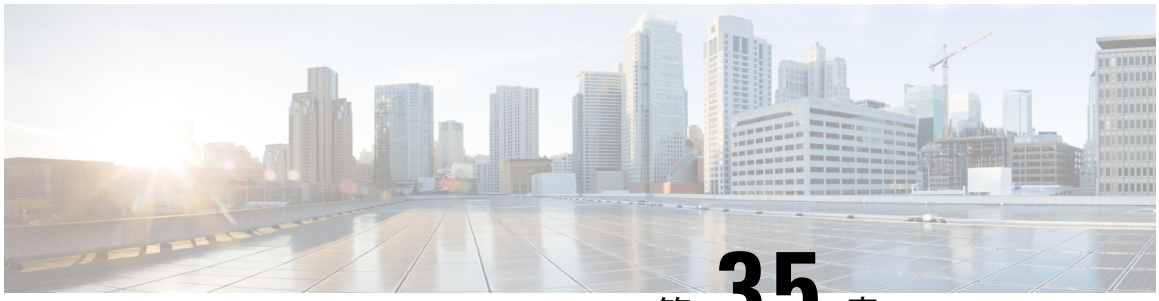
次の表に、条件付きデバッグの確認に使用できる各種コマンドを示します。

コマンド	目的
show platform condition	現在設定されている条件を表示します。
show debug	現在設定されているデバッグ条件を表示します。
show platform software trace filter-binary	最新のトレース ファイルからマージされたログを表示します。
request platform software trace filter-binary	システムにマージされたトレース ファイルの履歴ログを表示します。

例：SISF のラジオアクティブ トレース ログの確認

次に、*show platform software trace message ios chassis active R0 | inc sisf* コマンドの出力例を示します。

```
デバイス# show platform software trace message ios chassis active R0 | inc sisf

2017/10/26 13:46:22.104 {IOSRP_R0-0}{1}: [parser]: [5437]:  UUID: 0, ra: 0 (note):  CMD:
 'show platform software trace message ios switch active R0 | inc sisf' 13:46:22 UTC Thu
 Oct 26 2017
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Unlocking, count is now 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Unlocking, count is now 1
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Setting State to 2
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Start timer 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc  Timer value/granularity for 0 :299998/1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Updated Mac Timer : 299998
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Before Timer :  350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Timer 0, default value is 350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):   Allocating timer wheel for 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc No timer running
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Granularity for timer MAC_T1  is 1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Current State :MAC-STALE, Req Timer : MAC_T1
Current Timer MAC_T1
```



第 35 章

アグレッシブ クライアント ロード バランシング

アグレッシブ クライアント ロード バランシングに関する情報

アグレッシブ クライアント ロード バランシング機能を使用すると、ワイヤレスクライアントの負荷を Lightweight アクセスポイント間で分散できます。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエートされた応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。このコード 17 は AP がビジー状態であることを示します。AP のしきい値に達成しなければ、AP からは「success」を示す応答は返りません。AP 使用率のしきい値を超えると、コード 17（AP ビジー）が返り、処理能力に余裕がある別の AP がクライアント要求を受け取ります。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロード バランシング ウィンドウを上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントは、AP1 にアソシエートしようとするときに、ステータス コード 17 が含まれている 802.11 応答パケットを受け取ります。アクセス ポイントの負荷が高いことがこのステータス コードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

組み込みワイヤレスコントローラは、クライアント アソシエーションを 10 回まで拒否するように設定できます（クライアントがアソシエーションを 11 回試みた場合は、11 回目の試行時にアソシエーションが許可されます）。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指定できます。これは、特定のクライアント グループ（遅延に敏感な音声クライアントなど）に対してロード バランシングを無効にする場合に便利です。

（注） 300ミリ秒を超えて遅延を設定すると、音声クライアントは認証しません。これを避けるには、中央認証（Cisco Centralized Key Management（CCKM）による WLAN のローカルスイッチング）を設定し、AP と WLC 間に遅延 600 ms（UP と DOWN それぞれ 300 ms）の pagent ルータを設定して、音声クライアントのアソシエートを試みます。

（注） FlexConnect AP の場合は、アソシエーションがローカルに処理されます。ロードバランシングの判断は、コントローラで行われます。FlexConnect AP は、コントローラでの計算結果を確認する前に、最初の応答をクライアントに送信します。FlexConnect APがスタンドアロンモードの場合は、ロード バランシングが適用されません。

FlexConnect AP は、ローカル モードの AP と同様のロード バランシング用のステータス 17 で（再）アソシエーション応答を送信しません。代わりに、ステータス 0（成功）で（再）アソシエーションを送信してから、理由 5 で認証解除を送信します。

アグレッシブ クライアント ロード バランシングの有効化（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [WLANs] > [Wireless Networks] の順に選択します。
ステップ 2 [WLAN] を選択して、[Edit WLAN] ウィンドウを表示します。
ステップ 3 [Advanced] タブをクリックします。
ステップ 4 [Load Balance] チェックボックスをオンにして機能を有効にします。
ステップ 5 [Update & Apply to Device] をクリックします。

アグレッシブ クライアント ロード バランシングの設定（GUI）

手順

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

[Load Balancing] ウィンドウが表示されます。

ステップ 2 [Aggressive Load Balancing Window (clients)] フィールドに、アグレッシブ ロードバランシング クライアント ウィンドウのクライアント数を入力します。

ステップ 3 [Aggressive Load Balancing Denial Count] フィールドに、ロードバランシングの拒否カウントを入力します。

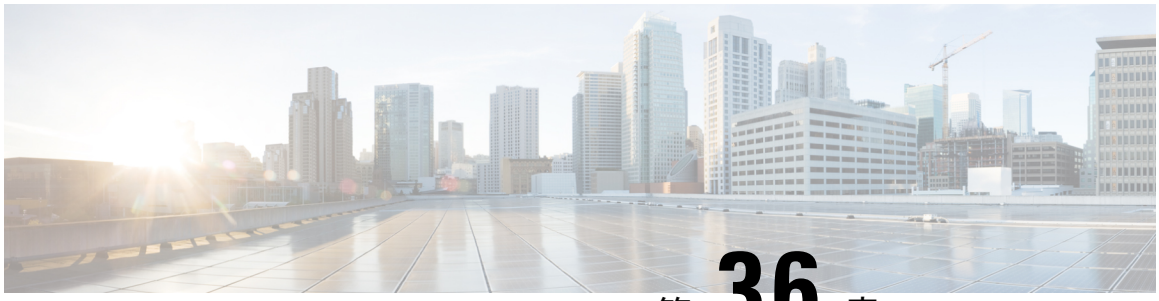
ステップ 4 [Apply] をクリックします。

アグレッシブ クライアント ロード バランシングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `デバイス# 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 3	**wlan** *wlan-name* 例： `デバイス(config)# wlan test-wlan`	WLAN 名を指定します。
ステップ 4	**shutdown** 例： `デバイス(config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 5	**load-balance** 例： `デバイス(config-wlan)# load-balance`	特定の WLAN へのクライアントロードバランスを有効にするために、ゲスト組み込みワイヤレスコントローラをモビリティコントローラとして設定します。 WLAN の要件として WLAN のセキュリティ設定を設定します。
ステップ 6	**no shutdown** 例：	WLAN を有効にします。

	コマンドまたはアクション	目的
	デバイス(config-wlan)# **no shutdown**	
ステップ 7	**end** 例： デバイス(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。
ステップ 8	**configure terminal** 例： デバイス# **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 9	**ap dot11** {**24ghz** | **5ghz**} **load-balancingdenial***count* 例： Device(config)# **ap dot11 5ghz load-balancing denial 10**	ロードバランシングの拒否数を設定します。
ステップ 10	**ap dot11** {**24ghz** | **5ghz**} **load-balancingwindow** クライアント 例： Device(config)# **ap dot11 5ghz load-balancing denial 10**	アグレッシブ ロード バランシング クライアント ウィンドウのクライアント数を設定します。
ステップ 11	**end** 例： デバイス(config-wlan)# **end**	特権 EXEC モードに戻ります。
ステップ 12	**show running-config | section** *wlan-name* 例： デバイス# **show running-config | section test-wlan**	現在の設定のフィルタリングされたセクションを表示します。



第 36 章

アカウンティング ID リスト

アカウンティング ID リストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。

ステップ 2 [AAA Method List] タブで、[Accounting] セクションに移動し、[Add] をクリックします。

ステップ 3 表示される [Quick Setup: AAA Accounting] ウィンドウに、メソッド リストの名前を入力します。

ステップ 4 [Type] ドロップダウン リストで、認証タイプとして ID を選択します。

ステップ 5 [Available Server Groups] リストで、ネットワークへのアクセスの認証に使用するサーバー グループを選択し、[>] アイコンをクリックして [Assigned Server Groups] リストに移動します。

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

アカウンティング ID リストの設定（CLI）

アカウンティングは、ユーザの操作をロギングしてユーザのネットワーク使用状況を追跡するプロセスです。ユーザーによる操作が正常に実行されるとそのたびに、RADIUS アカウンティング サーバーでは、変更された属性、変更を行ったユーザーのユーザー ID、ユーザーがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザーの認可レベル、および実行された処理と入力された値の説明が、ログに記録されます。

アカウンティング ID リストを設定するには、次の手順に従います。

始める前に

RADIUS サーバーと AAA サーバー グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* 例： `Device(config)# aaa accounting identity user1 start-stop group aaa-test`	アカウンティングを有効にして、クライアントが承認されたときに start-record アカウンティング通知を送信し、最後に stop-record を送信できるようにします。 （注） 名前付きリストの代わりにデフォルトのリストを使用することもできます。

クライアント属性が変更された場合（たとえば、IPアドレスの変更、クライアントのローミングなど）はそのたびに、アカウンティングの中間アップデートがRADIUSサーバーに送信されます。

クライアント アカウンティングの設定（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 Name]** をクリックし、[Edit Policy Profile] ウィンドウで [Advanced] タブに移動します。

ステップ 3 [Accounting List] ドロップダウンから、このポリシープロファイルの適切なアカウンティングリストを選択します。これにより、ポリシープロファイルに対して、ネットワークへのアクセスを許可する前に、必要なタイプのアカウンティングが実行されるようになります。

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

クライアント アカウンティングの設定（CLI）

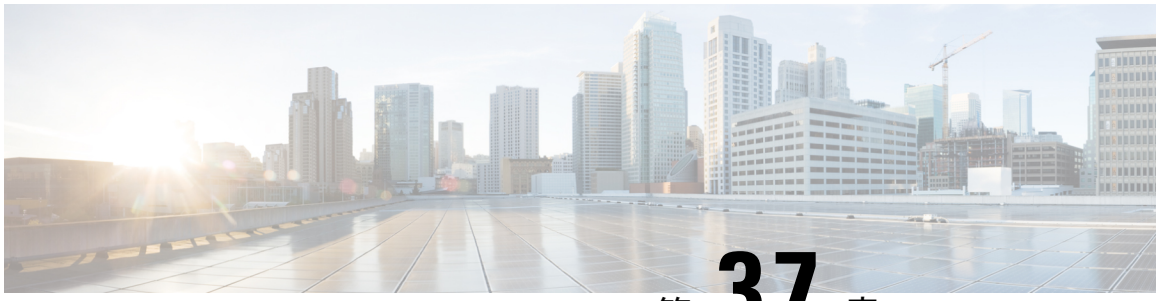
クライアント アカウンティングを設定するには、次の手順に従います。

始める前に

RADIUS アカウンティングが設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	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 2	**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 3	**accounting-list** *list-name* 例： `Device(config-wireless-policy)# accounting-list user1`	アカウンティング リストを設定します。
ステップ 4	**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。



第 37 章

ボリューム測定

ボリューム測定機能を使用すると、アクセスポイント（AP）がクライアント アカウンティング統計情報を 組み込みワイヤレスコントローラに対して更新し、さらに RADIUS サーバーに対して更新する間隔を設定できます。現在、レポートは 90 秒ごとに AP からコントローラに送信されます。この機能を使用することで、5～90秒の時間を設定できます。これにより、デバイスでのアカウンティング データの使用における遅延が削減されます。

• ボリューム測定の設定 （447 ページ）

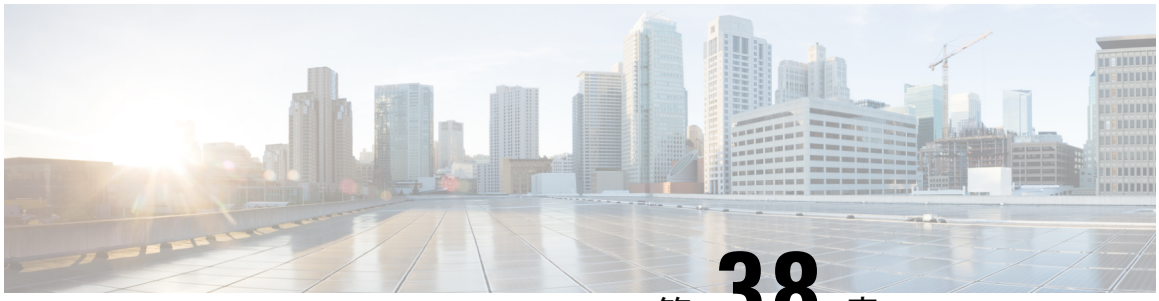
ボリューム測定の設定

ボリューム測定を設定するには、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	**ap profile** *profile-name* 例： `Device(config)# ap profile yy-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。
ステップ 3	**dot11 24ghz reporting-interval** *reporting-interval* 例： `Device(config-ap-profile)# dot11 24ghz reporting-interval 60`	dot11 パラメータを設定します。
ステップ 4	**dot11 5ghz reporting-interval** *reporting-interval* 例：	dot11 パラメータを設定します。

	コマンドまたはアクション	目的
	`Device(config-ap-profile)# dot11 5ghz reporting-interval 60`	
ステップ 5	**exit** 例： `Device(config-ap-profile)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**aaa accounting update periodic** *interval-in-minutes* 例： `Device(config)# aaa accounting update periodic 75`	組み込みワイヤレスコントローラがクライアントの中間アカウンティング更新を RADIUS サーバーに送信する時間間隔（分単位）を設定します。
ステップ 7	**exit** 例： `Device(config)# exit`	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。



第 38 章

AP グループ NTP サーバー

AP グループ NTP サーバーの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

この機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

表 *19 : AP* グループ *NTP* サーバーの機能履歴

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.1	AP グループ NTP サーバー	このリリース以降、グローバル NTP サーバーの設定は、AP グループごとの NTP サーバーの設定に置き換えられます。現在、Cisco Hyperlocation 機能を設定するには AP グループごとの NTP サーバーが必須です。

AP グループ NTP サーバーに関する情報

Cisco HyperLocation、BLE 到着角度（AoA）、インテリジェントキャプチャ（iCAP）などの機能では、高い位置精度を実現するために、AP グループ内の全 AP の時間が正確である必要があります。コントローラとコントローラのグローバル NTP サーバーは WAN 上に設定されて

いるため、AP からの同期の遅延が大きくなる可能性があり、位置精度が低下することがあります。

AP グループ内のすべての AP が同じ NTP サーバーと同期する場合、位置計算のための正確なデータを取得できます。AP グループ内のすべての AP に対して NTP サーバーをローカルに設定すると、AP 間の同期が向上します。

AP グループ NTP サーバーの設定

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	**ap profile** *profile-name* 例： `Device(config)# ap profile profile-name`	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。
ステップ 3	**[no] ntp ip** *ip-address* 例： `Device(config-ap-profile)# [no] ntp ip 9.0.0.4`	NTP サーバの IP アドレスを設定します。このコマンドの **no** 形式を使用すると NTP サーバーが削除されます。

AP タイムゾーンの設定

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	**ap profile** *profile-name* 例： `Device(config)# ap profile test`	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。
ステップ 3	**timezone** {**use-controller** | **delta hour** *offset-hour* **minute** *offset-minute*} 例：	AP のタイムゾーンオフセットを設定します。

	コマンドまたはアクション	目的
	`Device(config-ap-profile)# timezone delta hour -12 minute 2`	AP タイムゾーンは、AP プロファイルごとにのみ設定できます。AP ごとにタイムゾーンを設定することはできません。 タイムゾーンを設定するには、現在のコントローラのタイムゾーンまたは時差を適用します。デフォルトでは、タイムゾーンは無効になっています。

Cisco Hyperlocation の確認

すべての AP プロファイルについて HyperLocation のステータス値とパラメータを表示するには、次のコマンドを使用します。

```
Device# show ap hyperlocation summary

Profile Name: custom-profile

Hyperlocation operational status: Down
Reason: Hyperlocation is administratively disabled
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Disabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8


Profile Name: default-ap-profile

Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 22
Hyperlocation reset threshold: 8
```

全体と AP ごとの両方の設定値と動作ステータスを表示するには、次のコマンドを使用します。

```
Device# show ap hyperlocation detail

Profile Name: house24

Hyperlocation operational status: Up
 Reason: NTP server is not properly configured
Hyperlocation NTP server: 198.51.100.1
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7
```

```
AP Name                 Radio MAC         Method      CMX IP            AP Profile
-------------------------------------------------------------------------------------------
APe865.49d9.bfe0        e865.49ea.a4b0    WSM2+Ant    198.51.100.2        house24

APa89d.21b9.69d0        a89d.21b9.69d0    Local       198.51.100.3        house24

APe4aa.5d3f.d750        e4aa.5d5f.3630    WSM         198.51.100.4        house24
```

特定のプロファイルについて全体（プロファイル固有）の設定値と動作ステータスを表示するには、次のコマンドを使用します。

```
Device# show ap profile profile-name hyperlocation summary

Profile Name: profile-name
Hyperlocation operational status: Up
   Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

特定のプロファイルについて全体（プロファイル固有）と AP ごとの両方の設定値と動作ステータスを表示するには、次のコマンドを使用します。リストされる AP は、指定した join プロファイルに属する AP のみです。

```
Device# show ap profile profile-name hyperlocation detail

Profile Name: profile-name
Hyperlocation operational status: Up
 Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                 Radio MAC         Method      CMX IP
-----------------------------------------------------------------
APf07f.0635.2d40        f07f.0635.2d40    WSM2+Ant    198.51.100.2
APf07f.0635.2d41        f07f.0635.2d41    Local       198.51.100.3
APf07f.0635.2d42        f07f.0635.2d42    WSM         198.51.100.4
```

AP プロファイルの設定値を表示するには、次のコマンドを使用します。

```
Device# show ap profile profile-name detailed

Hyperlocation :
  Admin State             : ENABLED
  PAK RSSI Threshold Detection: -100
  PAK RSSI Threshold Trigger  : 10
  PAK RSSI Threshold Reset    : 8
.
.
.
```

正しく接続されていて HyperLocation によって使用されている Cisco CMX を表示するには、次のコマンドを使用します。

```
Device# show ap hyperlocation cmx summary

Hyperlocation-enabled CMXs

IP            Port Dest MAC        Egress src MAC Egress VLAN Ingress src MAC Join time

-------------------------------------------------------------------------------------------
198.51.100.4  2003 aaaa.bbbb.cccc  aabb.ccdd.eeff 2           0000.0001.0001  12/14/18
09:27:14
```

HyperLocation クライアントの統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp
feature wireless wlclient cpp-client summary

Client Type Abbreviations:
  RG - REGULAR BL - BLE
  HL - HALO    LI - LWFL INT
Auth State Abbreviations:
  UK - UNKNOWN IP - LEARN IP IV - INVALID
  L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
  UK - UNKNOWN IN - INIT
  LC - LOCAL   AN - ANCHOR
  FR - FOREIGN MT - MTE
  IV - INVALID
EoGRE Abbreviations:
  N - NON EOGRE Y - EOGRE
 CPP IF_H     DPIDX      MAC Address    VLAN  CT  MCVL  AS  MS  E  WLAN POA
------------------------------------------------------------------------------
   0X32     0XF0000001  0000.0001.0001   9    HL   0    RN  LC  N       NULL
```

インターフェイスハンドル値の統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics start
```

記録されたフローを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0X32 statistics

                  Pkts               Bytes
Rx                 26                3628
```

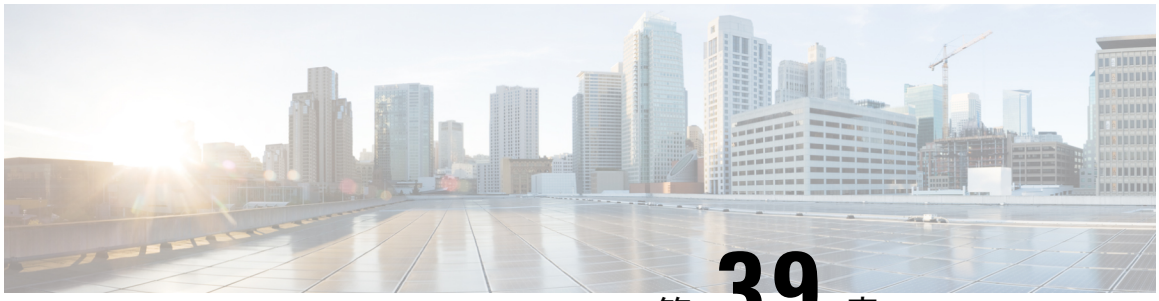
統計情報のキャプチャを停止するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics stop
```

AP グループのサポートがある Cisco CMX によって要求された AP を表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription group summary
```

```
CMX IP address: 198.51.100.4
  Groups subscribed by this CMX server:
  Group name: CMX_1198.51.100.4

Device# show nmsp subscription group detail ap-list CMX_198.51.100.1 198.51.100.1

CMX IP address: 198.51.100.1
CMX Group name: CMX_198.51.100.1
CMX Group AP MACs:
: aa:bb:cc:dd:ee:01 aa:bb:cc:dd:ee:02 aa:bb:cc:dd:ee:03 aa:bb:cc:dd:ee:03
```



第 39 章

Syslog サーバー用のアクセス ポイントとコントローラでの Syslog メッセージの有効化

Syslog サーバー用のアクセスポイントと 組み込みワイヤレスコントローラでの Syslog メッセージの有効化について

（注） AP が参加した後にのみ、Syslog サーバー メッセージを表示できるようになります。

アクセスポイントおよび 組み込みワイヤレスコントローラの Syslog サーバーには、数多くのレベルとファシリティがあります。

Syslog レベルは次のとおりです。

- Emergencies
- Alerts
- Critical
- Errors

- Warnings
- [Notifications]
- Informational
- Debugging

Syslog ファシリティでは次のオプションを使用できます。

- auth：認可システム。
- cron：Cron/at ファシリティ。
- daemon：システム デーモン。
- kern：カーネル。
- local0：ローカル用。
- local1：ローカル用。
- local2：ローカル用。
- local3：ローカル用。
- local4：ローカル用。
- local5：ローカル用。
- local6：ローカル用。
- local7：ローカル用。
- lpr：ライン プリンタ システム。
- mail：メール システム。
- news：USENET ニュース。
- sys10：システム用。
- sys11：システム用。
- sys12：システム用。
- sys13：システム用。
- sys14：システム用。
- sys9：システム用。
- syslog：Syslog それ自体。
- user：ユーザー プロセス。
- uucp：Unix-to-Unix コピー システム。

AP プロファイルの Syslog サーバーの設定

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	**ap profile** *ap-profile* 例： `デバイス(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。
ステップ 3	**syslog facility** 例： `デバイス(config-ap-profile)# syslog facility`	Syslog メッセージのファシリティ パラメータを設定します。
ステップ 4	**syslog host** *ip-address* 例： `デバイス(config-ap-profile)# syslog host 9.3.72.1`	SyslogサーバーのIPアドレスとパラメータを設定します。
ステップ 5	**syslog level** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} 例： `デバイス(config-ap-profile)# syslog level`	Syslog サーバーのロギング レベルを設定します。 Syslog サーバーのロギング レベルは次のとおりです。 • **emergencies**：シビラティ（重大度）0を示します。システムが使用できないことを意味します。 • **alerts**：シビラティ（重大度） 1 を示します。ただちに対処する必要があることを意味します。 • **critical**：シビラティ（重大度）2を示します。クリティカルな状態を意味します。 • **errors**：シビラティ（重大度） 3 を示します。エラー状態を意味します。

	コマンドまたはアクション	目的
		• **warnings**：シビラティ（重大度）4を示します。警告状態を意味します。 • **notifications**：シビラティ（重大度）5を示します。正常ですが、注意を必要とする状態であることを意味します。 • **informational**：シビラティ（重大度）6を示します。情報メッセージを意味します。 • **debugging**：シビラティ（重大度）7を示します。デバッグ メッセージを意味します。 （注） サポートされる Syslog レベルの数を確認するには、Syslog レベルを選択する必要があります。Syslog レベルを選択すると、それ以下のすべてのレベルも有効になります。 「critical」Syslog レベルを有効にすると、その下のすべてのレベルも有効になります。したがって、「critical」、「alerts」、「emergencies」の 3 つすべてが有効になります。
ステップ 6	**end** 例： `デバイス(config-ap-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

コントローラの Syslog サーバーの設定（GUI）

手順

ステップ 1 **[Troubleshooting]** > **[Logs]** を選択します。

ステップ 2 [Manage Syslog Servers] ボタンをクリックします。

ステップ 3 [Log Level Settings] の [Syslog] ドロップダウンリストから、セキュリティレベルを選択します。

ステップ 4 [Message Console] ドロップダウンリストから、ロギングレベルを選択します。

ステップ 5 [Message Buffer Configuration] の [Level] ドロップダウンリストから、サーバーのロギングレベルを選択します。

ステップ 6 [IP Configuration] 設定で、[Add] をクリックします。

ステップ 7 [IPv4/IPv6] または [FQDN] オプションからサーバータイプを選択します。

ステップ 8 サーバータイプが [IPv4/IPv6] の場合は、[IPv4/IPv6 Server Address] を入力します。サーバータイプが [FQDN] の場合は、[Host Name] を入力し、IP タイプと適切な [VRF Name] をドロップダウンリストから選択します。

Syslog サーバーを削除するには、[Remove] 列の下にある適切なサーバーエントリの横にある [x] をクリックします。

（注） ホスト名を作成する場合、スペースは使用できません。

ステップ 9 [Apply to Device] をクリックします。

（注） [Apply to Device] をクリックすると、変更内容が設定されます。[Cancel] をクリックすると、設定が破棄されます。

組み込みワイヤレスコントローラの Syslog サーバーの設定

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	**logging host** {*hostname* | *ipv6*} 例： `デバイス(config)# logging host 124.3.52.62`	Syslog サーバーの IP アドレスとパラメータを有効にします。
ステップ 3	**logging facility** {**auth** | **cron** | **daemon** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **sys10** | **sys11** | **sys12** | **sys13** | **sys14** | **sys9** | **syslog** | **user** | **uucp**} 例： `デバイス(config)# logging facility syslog`	Syslog メッセージのファシリティ パラメータを有効にします。 Syslog メッセージに対して次のファシリティ パラメータを有効にすることができます。 • **auth**：認可システム。 • **cron**：cron ファシリティ。 • **daemon**：システム デーモン。 • **kern**：カーネル。 • **local0** ～ **local7**：ローカル用。 • **lpr**：ライン プリンタ システム。 • **mail**：メール システム。 • **news**：USENET ニュース。 • **sys10** ～ **sys14** および **sys9**：システム用。 • **syslog**：Syslog それ自体。 • **user**：ユーザー プロセス。 • **uucp**：UNIX から UNIX へのコピー システム。
ステップ 4	**logging trap** {*severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} 例： `デバイス(config)# logging trap 2`	Syslog サーバーのロギング レベルを有効にします。 *severity-level*：ロギングのシビラティ（重大度）レベルを示します。有効範囲は 0 ～ 7 です。 Syslog サーバーのロギング レベルは次のとおりです。 • **emergencies**：シビラティ（重大度）0 を示します。システムが使用できないことを意味します。

	コマンドまたはアクション	目的
		• **alerts**：シビラティ（重大度） 1 を示します。ただちに対処する必要があることを意味します。 • **critical**：シビラティ（重大度）2 を示します。クリティカルな状態を意味します。 • **errors**：シビラティ（重大度） 3 を示します。エラー状態を意味します。 • **warnings**：シビラティ（重大度）4 を示します。警告状態を意味します。 • **notifications**：シビラティ（重大度）5 を示します。正常ですが、注意を必要とする状態であることを意味します。 • **informational**：シビラティ（重大度）6 を示します。情報メッセージを意味します。 • **debugging**：シビラティ（重大度）7 を示します。デバッグ メッセージを意味します。 （注） サポートされる Syslog レベルの数を確認するには、Syslog レベルを選択する必要があります。Syslog レベルを選択すると、それ以下のすべてのレベルも有効になります。 「critical」Syslog レベルを有効にすると、その下のすべてのレベルも有効になります。したがって、「critical」、「alerts」、「emergencies」の 3 つすべてが有効になります。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： デバイス(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。

Syslog サーバーの設定の確認

すべてのアクセス ポイントに対するグローバルな Syslog サーバーの設定の確認

コントローラに join しているすべてのアクセス ポイントに対するグローバルな Syslog サーバーの設定を表示するには、次のコマンドを使用します。

```
Device# show ap config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
```

```
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```

特定のアクセス ポイントに対する Syslog サーバーの設定の確認

特定のアクセス ポイントに対する Syslog サーバーの設定を表示するには、次のコマンドを使用します。

```
Device# show ap name <ap-name> config general
show ap name APA0F8.4984.5E48 config general
Cisco AP Name : APA0F8.4984.5E48
```

```
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
```

```
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```

第 40 章

ソフトウェア メンテナンス アップグレード

ソフトウェア メンテナンス アップグレードの概要

ソフトウェア メンテナンス アップグレード（SMU）は、システムにインストールしてパッチ修正やセキュリティ解決をリリースされたイメージに提供できるパッケージです。SMU パッケージはリリースごとに提供され、対応するプラットフォームに固有です。

SMU では、必要なテストの時間と範囲を削減しながら、ネットワークの問題に迅速に対応できるため、従来の Cisco IOS ソフトウェアには多大なメリットがあります。Cisco IOS XE プラットフォームでは SMU の互換性を内部的に検証し、互換性のない SMU はインストールできません。

すべて SMU が後続の Cisco IOS XE ソフトウェア メンテナンス リリースに統合されています。SMU は独立した自己完結型パッケージであり、前提条件や依存関係はありません。SMU はどのような順序でもインストールまたはアンインストールできます。

（注） SMU は拡張メンテナンスリリースでのみ、基盤となるソフトウェアリリースのライフサイクルにわたってサポートされます。

（注） **install add file** コマンドで使用するファイルは、アクティブデバイスのファイルシステムからのみアクティブ化できます。スタンバイまたはメンバーのファイルシステムからファイルを使用することはできません。このような場合、**install add file** コマンドは失敗します。

SMU インフラストラクチャは、ワイヤレスの状況における次の要件を満たすために使用できます。

- コントローラ SMU： 組み込みワイヤレスコントローラのバグ修正または Cisco Product Security Incident Response information（PSIRT）。
- AP のバグ修正、PSIRT、または組み込みワイヤレスコントローラの変更を必要としないマイナー機能。
- APDP：新しいハードウェアまたはソフトウェアの機能を導入しない新しい AP モデルのサポート。

（注） show ap image コマンドは、コントローラの AP イメージに関する累積統計を表示します。show ap image コマンドを使用する前に、clear ap predownload statistics コマンドを使用して統計情報をクリアして、正しいデータが表示されるようにすることをお勧めします。

SMU のワークフロー

SMU プロセスは、SMU Committee への要求によって開始される必要があります。カスタマーサポートに連絡し、SMU 要求を行います。SMU パッケージは、リリースの間に [Cisco Software Download] ページに掲載されるため、ダウンロードしてインストールできます。

SMU パッケージ

SMU パッケージには、SMU が要求されている報告済みの問題のメタデータと修正が含まれています。

SMU のリロード

SMUのタイプは、SMUのインストール後のシステムへの影響を説明します。SMUはトラフィックに影響を与えない場合もありますが、デバイスの再起動、リロード、スイッチオーバーを引き起こす可能性もあります。

コントローラのホットパッチのサポートにより、システムをリロードすることなく、SMU をアクティブ化の直後に実行できます。他のコントローラの SMU では、アクティブ化中にシステムをコールドリロードする必要があります。コールド リロードは、オペレーティング システムを完全にリロードします。このアクションは、リロードの間（現在は最大5分間）、トラフィック フローに影響します。このリロードにより、SMU の一部としてインストールされている正しいライブラリとファイルですべてのプロセスが起動します。

SUM がコミットされると、リロードが繰り返されてもアクティブ化の変更が持続します。

コントローラ SMU の概要

次の表に、Cisco組み込みワイヤレスコントローラ でサポートされる SMU タイプを示します。

表 *20* : 組み込みワイヤレスコントローラでサポートされる *SMU* タイプ

パッケージ タイプ	使用例	SMU タイプ	EWC でサポート
コントローラ SMU：コールドパッチ	影響を受けるバイナリ、ライブラリ、またはサブパッケージを置き換えます。	リロード	限定的なサポート（パッチサイズ＜20 MB）。IOSD のサポートはありません。
コントローラ SMU：ホットパッチ	影響を受ける機能を置き換えます。	リロードなし	対応
APSP	AP イメージの置き換えによる AP の修正（アクティブコントローラを実行している AP には影響しません）。	リロードなし	対応
APSP	AP イメージの置き換えによる AP の修正（アクティブコントローラを実行している AP に影響します）。	リロード	対応（EWC 固有のバリエーション）
APDP	コントローラをアップグレードせずに、新しい AP モデルをサポート。	リロードなし	対応

コントローラのホットまたはコールド SMU パッケージの管理

手順

	コマンドまたはアクション	目的
ステップ 1	**install add file tftp:**//<server-ip>/<path>/<smu-filename> 例： `Device# install add file tftp://<server-ip>/<path>/<smu-filename>`	`install add` コマンドは、ファイルを外部サーバーから組み込みワイヤレスコントローラの backup_image ディレクトリにコピーします。
ステップ 2	**install activate file backup_image:** *smu-filename* 例： `Device# install activate file backup_image:<smu-filename>`	このコマンドは、パッチをアクティブにするために使用されます。`install activate` により、コールドパッチの場合にのみコントローラがリロードされ

	コマンドまたはアクション	目的
		ます。ホットパッチはリロードされません。
ステップ 3	**install auto-abort-timer stop** 例： `Device# install auto-abort-timer stop`	（任意）SMUがアクティブ化または非アクティブ化された場合に自動キャンセルタイマーを停止します。
ステップ 4	**install commit** 例： `Device# install commit`	リロードが繰り返されても持続するようにアクティブ化の変更をコミットします。 アクティブ化の後で、システムがアップしている間、または最初のリロード後にコミットできます。パッチがアクティブ化されて、コミットされていない場合、自動キャンセルタイマーにより、6 時間後にパッチのアクティブ化が自動的にキャンセルされます。
ステップ 5	**show install rollback** 例： `Device# show install rollback`	使用可能なロールバック IDのリストを表示します。
ステップ 6	**install rollback to** {**base** | **committed** | **id** | **label** } *specific-rollback-point* 例： `Device# install rollback to base`	コミットされたパッチをロールバックします。コミットされたパッチは非アクティブ化でき、非アクティブ化のコミットは単一の install rollback コマンドを使用して実行できます。
ステップ 7	**install deactivate file backup_image:** *smu-filename* 例： `Device# install deactivate file backup_image:<Smu-Filename>`	コミットされたパッチを非アクティブ化します。コールドパッチの場合、`install deactivate` コマンドによりコントローラがリロードします。ホットパッチの場合、コントローラはリロードしません。
ステップ 8	**install auto-abort-timer stop** 例： `Device# install auto-abort-timer stop`	（任意）SMUがアクティブ化または非アクティブ化された場合に自動キャンセルタイマーを停止します。
ステップ 9	**install commit** 例： `Device# install commit`	リロードが繰り返されても持続するようにアクティブ化の変更をコミットします。

	コマンドまたはアクション	目的
ステップ 10	**install remove file backup_image:** *smu-filename* 例： `Device# install remove file backup_image:<smu-filename>`	非アクティブ状態のパッチを削除します。このコマンドは、backup-image: からもファイルを物理的に削除します。
ステップ 11	**install abort** 例： `Device# install abort`	ローリング方式で AP をリセットすることで、アップグレードを中止します。
ステップ 12	**show install summary** 例： `Device# show install summary`	アクティブパッケージに関する情報を表示します。 このコマンドの出力は、パッケージ、およびインストールされているパッケージの状態によって異なります。
ステップ 13	**show install package backup_image:** *smu-filename* 例： `Device# show install package backup-image: <smu_filename>`	SMUパッケージに関する情報を表示します。

SMU ファイルの作成（GUI）

以下の手順に従って、SMU ファイルを作成します。

手順

ステップ 1 [Administration] > [Software Management] > [Software Maintenance Upgrade (SMU)] を選択します。

ステップ 2 [Add] をクリックします。
ダイアログボックスが表示されます。

ステップ 3 [Transport Type] ドロップダウンリストから、以下を選択します。

- [TFTP]：[Server IP Address (IPv4/IPv6)]、[File Path]、[File Name]、および [File System] を指定します。
- [SFTP]：[Server IP Address (IPv4/IPv6)]、[Port Number]（デフォルトのポート番号は 22）、SFTP ユーザー名とパスワード、[File Path]、[File Name]、および [File System] を指定します。
- [FTP]：[Server IP Address (IPv4/IPv6)]、[Port Number]（デフォルトのポート番号は 22）、FTP ユーザー名とパスワード、[File Path]、[File Name]、および [File System] を指定します。
- [Device]：[File System] と [File path] を指定します。

- [My Desktop]：[File System] と [Source File Path] を指定します。

ステップ 4 [Add File] をクリックします。

SMU の設定例

次に、SMU の設定例を示します。

```
Device# install add file
tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-apsp1.bin
install_add: START Tue Jun 4 15:08:26 UTC 2019
Downloading file tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-smu.bin
Finished downloading file tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-smu.bin to
backup_image:ewc-smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....
install_add: ap image predownload is allowed.

--- Starting initial file syncing ---
Info: Finished copying backup_image: ewc-smu.bin to the selected chassis
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on chassis 1
MEWLC response success sync_successCumulative SMU Size: 24 KB
Cumulative size of all SMU's will not exceed 20000 KB
Available Memory in /backup_image is 251480 KB
Available memory 251480 KB is greater than available memory required 2000 KB
[1] Finished SMU_ADD on chassis 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add
```

```
Device# install activate file backup_image:ewc-apsp1.bin
install_activate: START Tue Jun 4 15:18:58 UTC 2019
install_activate: Activating SMU
Cumulative SMU Size: 24 KB
Cumulative size of all SMU's will not exceed 20000 KB
Available Memory in /backup_image is 250984 KB
Available memory 250984 KB is greater than available memory required 2000 KB
MEWLC response success sync_successExecuting pre scripts....
Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
[1] SMU_ACTIVATE package(s) on chassis 1
valid
install_activate: FP fp error skipping. Platform to fix this in Fru List
[1] Finished SMU_ACTIVATE on chassis 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

Executing post scripts....
```

```
Executing post scripts done.
Executing post scripts....
Executing post scripts done.
SUCCESS: install_activate /backup_image/ewc-apsp1.bin
```

Device#install commit

```
install_commit: START Tue Jun 4 16:15:25 UTC 2019
install_commit: Committing SMU
Executing pre scripts....
install_commit:
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
[1] SMU_COMMIT package(s) on chassis 1
valid
[1] Finished SMU_COMMIT on chassis 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

Waiting for the platform to set the SMU sync timerSMU sync status is sync_successSMU
sync to AP's success
/tmp/rp/chasfs/wireless/wlc_notify
SUCCESS: install_commit /backup_image/ewc-apsp1.bin
```

Device#install rollback to base

```
install_rollback: START Tue Jun 4 16:42:24 UTC 2019
install_rollback: Rolling back SMU
Executing pre scripts....
install_rollback:
Executing pre sripts done.

--- Starting SMU Rollback operation ---
Performing SMU_ROLLBACK on all members
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
[1] SMU_ROLLBACK package(s) on chassis 1
[1] Finished SMU_ROLLBACK on chassis 1
Checking status of SMU_ROLLBACK on [1]
SMU_ROLLBACK: Passed on [1]
Finished SMU Rollback operation

Executing post scripts....
Executing post scripts done.
Waiting for the platform to set the SMU sync timerSMU sync status is sync_successSMU
sync to AP's success
/tmp/rp/chasfs/wireless/wlc_notifyExecuting post scripts....
Executing post scripts done.
SUCCESS: install_rollback /backup_image/ewc-apsp1.bin Tue Jun 4 16:43:01 UTC 2019
```

Device# install deactivate file backup_image: ewc-apsp1.bin

install remove file backup_image:ewc-apsp1.bin

Device#show install sum

```
[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
APSP C backup_image:ewc-apsp1.bin
IMG C 17.1.1.0.69043
```

```
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

ローリング AP アップグレード

APのローリングアップグレードは、いくつかのAPをネットワーク内で常にアップ状態にし、他の AP がアップグレード対象として選択されている状態で、クライアントにシームレスなカバレッジを提供するように、段階的な方法で AP をアップグレードする方法です。

（注） ローリング アップグレードがトリガーされる前に、AP イメージがダウンロードされている必要があります。これにより、アップグレード対象のすべてのAPに新しいイメージバージョンが用意されます。

ローリング AP アップグレードのプロセス

AP のローリング アップグレードはコントローラ単位で実行されます。特定の時間にアップグレードされる AP の数は、コントローラに接続している AP の総数のパーセンテージになります。パーセンテージは、ユーザーが設定した値を上限とします。デフォルトのパーセンテージは 15 です。AP の実際のアップグレードが開始される前に、クライアント以外の AP がアップグレードされます。

アップグレード プロセスは次のようになります。

1. **候補となる AP セットの選択**

   この段階では、隣接 AP の情報に基づいて一連の AP の候補が選択されます。たとえば、ある AP をアップグレード対象として特定した場合、そのネイバーの特定の番号（N）が候補の選択から除外されます。この N の値は次の方法で生成されます。

   ユーザーが設定可能な上限値が 25% の場合、N = 6（想定される反復回数 = 5）

   ユーザーが設定可能な上限値が 15% の場合、N = 12（想定される反復回数 = 12）

   ユーザーが設定可能な上限値が 5% の場合、N = 24（想定される反復回数 = 22）

   隣接 AP の情報を使用して候補を選択できない場合は、間接のネイバーから候補を選択します。それでも候補を選択できない場合、AP は失敗せずに正常にアップグレードされます。

（注） 候補が選択された後、候補の数が設定されたパーセンテージの値を超えると、追加の候補が削除され、パーセンテージの上限が維持されます。

2. **クライアントのステアリング**

AP の候補に接続しているクライアントは、AP の候補を再起動する前に、AP の候補のリストにない AP にステアリングされます。AP は、自身に関連付けられた各クライアントに対して、最適な AP のリストを求めるための要求を送信します。これには AP の候補は含まれません。AP の候補は、ネイバー リストで使用不可としてマークされます。その後、AP の再 join とリロードのプロセスでマーキングがリセットされます。

3. **AP の再 join とリロードのプロセス**

   クライアントのステアリングの完了後もクライアントが AP の候補に接続している場合は、クライアントに認証解除が送信され、AP はリロードされて新しいイメージで起動します。AP が再 join するために 3 分間のタイマーが設定されます。このタイマーが経過すると、すべての候補は、コントローラまたはモビリティ ピアのいずれかに join したかどうかがチェックされ、マークされます。AP の候補の 90% が join を完了すると、反復が完了します。join を完了していない場合はタイマーがさらに 3 分間延長され、3分 後に同じチェックが繰り返されます。チェックが 3 回繰り返されると、反復が終了し、次の反復が開始されます。反復はそれぞれ 10 分ほど続く場合があります。

   AP のローリング アップグレードの場合、必要な設定は 1 つだけです。それは、一度にアップグレードする AP の数であり、ネットワークにある AP の総数のパーセンテージとして表されます。

   デフォルト値は 15 になります。

```
Device (config)#ap upgrade staggered <25 | 15 | 5>
```

コントローラでの AP アップグレードの確認

コントローラでの AP のアップグレードを確認するには、次の **show** コマンドを使用します。

```
Device# show ap upgrade
AP upgrade is in progress

From version: 17.1.0.6
To version: 17.1.0.99

Started at: 06/04/2019 15:19:32 UTC
Configured percentage: 15
Percentage complete: 0
Expected time of completion: 06/04/2019 16:39:32 UTC

Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-------------------------------------------------------------------------------------------------------
0 06/04/2019 15:19:33 UTC 06/04/2019 15:19:33 UTC 1
1 06/04/2019 15:19:33 UTC ONGOING 1

Upgraded
--------
Number of APs: 1
AP Name Ethernet MAC Iteration Status Site
-------------------------------------------------------------------------------------------------------
AP7069.5A74.7604 7069.5a78.5580 0 Not Impacted default-site-tag
```

```
In Progress
-----------
Number of APs: 1
AP Name Ethernet MAC
-----------------------------------------------
APB4DE.3169.7842 4c77.6dc4.a220

Remaining
---------
Number of APs: 0

AP Name Ethernet MAC
-----------------------------------------------

APs not handled by Rolling AP Upgrade
-------------------------------------
AP Name Ethernet MAC Status Reason for not handling by Rolling AP Upgrade
```

AP デバイスパック（APDP）と AP サービスパック（APSP）

APSP と APDP

AP サービスパック（APSP）：APSP は、1 つ以上の AP モデルの AP イメージに修正をロールアウトします。APイメージを事前にダウンロードし、APモデルのサブセットに対してダウンロードしたイメージを（ローリングアップグレードによって）アクティブ化します。

- パッチが適用された AP では、他の AP とは異なる CAPWAP バージョンが実行されます。例：17.1.0.100 および 17.1.0.0。
- サイトごとの APSP ロールアウトはサポートされていません。組み込みワイヤレスコントローラ APSP では、すべての AP が単一のデフォルトサイトにある必要があります。

AP デバイスパック（APDP）

現時点では、新しいAPハードウェアモデルが導入された場合、それらは対応する 組み込みワイヤレスコントローラ関連のメジャー ソフトウェア バージョンとともに出荷されます。その後、新しいAPモデルを基準とした対応する 組み込みワイヤレスコントローラバージョンがリリースされるまで待ち、ネットワーク全体をアップグレードする必要があります。

APDP を使用すると、新しい組み込みワイヤレス コントローラ バージョンにアップグレードせずに、SMUインフラストラクチャを使用して新しいAPモデルをワイヤレスネットワークに導入できます。

AP イメージの変更

新しいAPモデルが導入された場合、新しいAPイメージに対応しているかどうかは不明です。これは、APイメージがAPモデル ファミリにマッピングされることを意味します。新しいAPモデルが既存の AP モデル ファミリに属している場合は、既存の APイメージ エントリ（例：ap3g3、ap1g5 など）が存在します。たとえば、AP モデルが ap3g3 または ap1g5 に属している

場合、それぞれのイメージファイルが APDP SMU zip ファイルとともにバンドルされます。対応するメタデータファイルは、新しい AP モデルの機能情報（必要な AP イメージを含む）で更新されます。

新しい AP モデルが新しい AP モデルファミリに属している場合、新しいイメージファイルが APDP SMU zip ファイルにバンドルされます。対応するメタデータファイルは、新しい AP モデルの機能情報（必要な AP イメージを含む）で更新されます。

APSP と APDP に関する情報

SMU APイメージはSMUバイナリの一部ではなく、APイメージはコントローラの外部でホストされます。

- SMU AP イメージのダウンロードでは、SFTP および TFTP メソッドのみがサポートされています。
- HTTP、HTTP、および CCO メソッドは、APSP または APDP ではサポートされていません。

SMUパッケージには、APモデルとその機能に関連する詳細情報を伝えるためのメタデータが含まれています。

（注） アップグレードを正常に続行するには、すべてのzipファイルが必要です。zipフォルダに含まれるファイルはすべて、ダウンロードメソッドを使用してアクセスできます。

TFTP/SFTP ソフトウェアアップグレードの前提条件は次のとおりです。

- TFTP/SFTP サーバーが組み込みワイヤレスコントローラの管理 IP アドレスから到達可能である。
- Web サイトからダウンロードした AP イメージ（ap1g6、ap1g6a、ap1g7、ap3g3 など）とコントローライメージ（C9800-AP-iosxe-wlc.bin）を含むアップグレードバンドルが解凍され、TFTP/SFTP サーバーにコピーされている。

APSP と APDP の管理

AP イメージは、ワイヤレスコントローラの外部でホストされます。組み込みワイヤレスコントローラでは、SMU AP イメージのダウンロードについて TFTP または SFTP のみがサポートされています。

APSP と APDP ファイルの設定（GUI）

以下の手順に従って、APSP または APDP ファイルを追加します。

手順

ステップ 1 [Administration] > [Software Management] > [AP Service Package (APSP)] または [AP Device Package (APDP)] を選択します。
[Add an AP Device Package] または [Add an AP Service Package] ウィンドウが表示されます。

ステップ 2 [Transport Type] ドロップダウンリストから、以下を選択します。

- [TFTP]：[Server IP Address (IPv4/IPv6)]、[File Path]、[File Name]、および [File System] を指定します。
- [SFTP]：[Server IP Address (IPv4/IPv6)]、[Port Number]（デフォルトのポート番号は 22）、SFTP ユーザー名とパスワード、[File Path]、[File Name]、および [File System] を指定します。

ステップ 3 [Add File] をクリックします。

TFTP サーバーディレクトリの設定

TFTP サーバーディレクトリを設定するには、次の手順を実行します。

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`	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 image-download default** 例： `Device(config)#wireless profile image-download default`	EWC-AP イメージのダウンロードパラメータを設定します。イメージのダウンロードプロファイル名としてデフォルトのみを使用します。
ステップ 3	**image-download-mode** {**tftp** | **sftp**} 例： `Device(config-wireless-image-download-profile)#image-download-mode tftp`	TFTP を使用してイメージのダウンロードを設定します。
ステップ 4	**tftp-image-path** *tftp-image-path* 例： `Device(config-wireless-image-download-profile-tftp)#tftp-image-path /tftpboot/cisco/ewc/`	AP イメージの TFTP サーバールートディレクトリを設定します。
ステップ 5	**tftp-image-server** {**A.B.C.D** | **X:X:X:X::X**} 例：	TFTP サーバーアドレスを設定します。

	コマンドまたはアクション	目的
	Device(config-wireless-image-download-profile-tftp)#tftp-image-server 5.5.5.5	

次のタスク

- リモート サーバー ディレクトリを設定します。zip ファイルで完全なバンドルを受け取ったら、zip ファイルをルートディレクトリ（/tftpboot/user/ewc など）にコピーします。完全なバンドルの例：/tftpboot/user/ewc/17.1.zip。
- ファイルを解凍します。次は、ルートディレクトリに存在するファイルの例です。ap3g3、ap1g4、C9800-AP-iosxe-wlc.bin など。

（注） 問題があり、17.1 パッチファイル C9800_AP.17_1.22.CSCvr11111.apsp.zip に基づいて APSP SMU にパッチを適用する場合は、同じルートフォルダ、つまり /tftproot/user/ewc/C9800_AP.17_1.22.CSCvr11111.apsp.zip に貼り付けます。ファイルを解凍すると、/tftpboot/user/ewc/17_1.22.CSCvr11111/ などのサブディレクトリが自動的に作成されます。AP イメージ（ap3g3 など）と SMU バイナリ（apsp_CSCvr11111.bin）は、そのサブディレクトリに存在します。

SFTP サーバーディレクトリの設定

SFTP サーバーディレクトリを設定するには、次の手順を実行します。

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	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 image-download default** 例： Device(config)#wireless profile image-download default	EWC-AP イメージのダウンロードパラメータを設定します。イメージのダウンロードプロファイル名としてデフォルトのみを使用します。
ステップ 3	**image-download-mode** {**tftp** | **sftp**} 例： Device(config-wireless-image-download-profile)#image-download-mode sftp	SFTP を使用してイメージのダウンロードを設定します。
ステップ 4	**sftp-image-path** *sftp-image-path* 例：	AP イメージの SFTP サーバールートディレクトリを設定します。

	コマンドまたはアクション	目的
	Device(config-wireless-image-download-profile-sftp)#sftp-image-path /sftpboot/isc/ewc/	
ステップ 5	**sftp-image-server** {**A.B.C.D** | **X:X:X:X::X**} 例： Device(config-wireless-image-download-profile-sftp)#sftp-image-server 5.5.5.5	SFTP サーバーアドレスを設定します。
ステップ 6	**sftp-password** {**0** | **8**} *password re-enter password* 例： Device(config-wireless-image-download-profile-sftp)#sftp-password 0 admin	SFTP パスワードを設定します。
ステップ 7	**sftp-username** *username* 例： Device(config-wireless-image-download-profile-sftp)#sftp-username admin	SFTP ユーザー名を設定します。

次のタスク

- リモート サーバー ディレクトリを設定します。zip ファイルで完全なバンドルを受け取ったら、zip ファイルをルートディレクトリ（/sftpboot/user/ewc など）にコピーします。完全なバンドルの例：/sftpboot/user/ewc/17.1.zip。
- ファイルを解凍します。次は、ルートディレクトリに存在するファイルの例です。ap3g3、ap1g4、C9800-AP-iosxe-wlc.bin など。

（注） 問題があり、17.1 パッチファイル C9800_AP.17_1.22.CSCvr11111.apsp.zip に基づいて APSP SMU にパッチを適用する場合は、同じルートフォルダ、つまり /sftproot/user/ewc/C9800_AP.17_1.22.CSCvr11111.apsp.zip に貼り付けます。ファイルを解凍すると、サブディレクトリ、たとえば /sftpboot/user/ewc/17_1.22.CSCvr11111/ が自動的に作成されます。AP イメージ（ap3g3 など）および SMU バイナリ（apsp_CSCvr11111.bin）はサブディレクトリに存在します。

ポジティブワークフロー：APSP と APDP

手順

	コマンドまたはアクション	目的

ステップ 1	**install add file** {**tftp:** | **sftp:** | **backup_image:**} apsp.bin
	例：
	TFTP とバックアップイメージ：
	`Device# install add file tftp://server_path/atc/tftpboot/user/ewc/17_12_03vr11111/apsp_03vr11111.bin`
	`Device#install add file backup-image:apsp_CSCvr11111.bin`
		install add コマンドは、ファイルを外部サーバーから組み込みワイヤレスコントローラの backup_image ディレクトリにコピーします。

ステップ 2	**ap image predownload** 例： `Device# ap image predownload`	このコマンドはオプションです。このコマンドは、AP イメージを事前にダウンロードします。事前ダウンロードが開始されている場合は、ステップ 3 を開始する前に事前ダウンロードが完了していることを確認してください。
ステップ 3	**install activate file backup-image:** *apsp.bin* 例： `Device# install activate file backup-image:apsp.bin`	このコマンドは、ローリング AP アップグレードを開始します。 （注） APDP の場合、アクティブになると、EWC コントローラにより新しい AP モデルの AP が接続可能になり、新たにインストールされた SMU AP イメージが取得されます。
ステップ 4	**install commit** 例： `Device# install commit`	リロードが繰り返されても持続するようにアクティブ化の変更をコミットします。 アクティブ化後、システムが稼働している間、または 1 回リロードした後でコミットできます。パッチがアクティブ化されて、コミットされていない場合、自動中止タイマーにより、6 時間後にパッチのアクティブ化が自動的にキャンセルされます。

ロールバックとキャンセル

ワンショットロールバック

手順

	コマンドまたはアクション	目的
ステップ 1	**show install rollback** 例： `Device# show install rollback`	可能なロールバックポイントを表示します。
ステップ 2	**install rollback to** {**base** | **committed** | **id** | **label** } *specific-rollback-point* 例： `Device# install rollback to base`	このコマンドは、ローリング AP アップグレードをトリガーします。ローリングアップグレードは、必要なイメージがあるすべての AP で機能します。残りの AP は一緒に再起動されます。 コミットされたパッチをロールバックします。コミットされたパッチは非アクティブ化でき、非アクティブ化のコミットは単一の install rollback コマンドを使用して実行できます。

複数手順ロールバック

手順

	コマンドまたはアクション	目的
ステップ 1	**show install profile** 例： `Device# show install profile`	show install profile コマンドは、ロールバックポイントに対応するプロファイルを表示します。
ステップ 2	**install add profile** *profile-rollback-point* 例： `Device# install add profile profile-rollback-point`	このコマンドは、ロールバックポイントに対応する事前ダウンロード手順のためにワイヤレスモジュールを準備します。
ステップ 3	**install rollback to** {**base** | **committed** | **id** | **label** } *specific-rollback-point* 例： `Device# install rollback to base`	このコマンドは、ローリング AP アップグレードをトリガーします。ローリングアップグレードは、必要なイメージがあるすべての AP で機能します。残りの AP は一緒に再起動されます。 コミットされたパッチをロールバックします。コミットされたパッチは非アク

	コマンドまたはアクション	目的
		ティブ化でき、非アクティブ化のコミットは単一の install rollback コマンドを使用して実行できます。

ワンショットキャンセル

ワンショット手動キャンセルには次のコマンドを使用します。

手順

- **install abort**

  例：

  ```
  Device# install abort
  ```

  このコマンドは、ローリング AP アップグレードをトリガーします。キャンセルは、コミットがまだ完了していない場合にのみ許可されます。ワンショットキャンセルには、事前ダウンロードの手順はありません。ローリング AP アップグレードは、必要なイメージを持つすべての AP で機能し、残りの AP は一緒に再起動します。

自動タイマーによるワンショットキャンセル

アクティブ化後、デフォルトの 6 時間のキャンセルタイマーが起動します。キャンセルタイマーは、activate コマンドの発行時に、auto-abort-timer パラメーターを使用して別の値に設定できます。キャンセルタイマーが時間切れになると、手動キャンセルと同じ方法でキャンセルが実行されます。

ロールバックの設定（GUI）

以下の手順に従って、APSP および APDP のロールバックを設定します。

手順

ステップ 1 [Administration] > [Software Management] を選択します。

ステップ 2 [AP Service Pack (APSP)] または [AP Device Pack (APDP)] を選択します。

ステップ 3 [Rollback to] ドロップダウンリストから、ロールバックタイプとして [Base] または [Committed] を選択します。

ステップ 4 [Submit] をクリックします。

組み込みワイヤレスコントローラでの APDP の確認

組み込みワイヤレスコントローラでの APDP パッケージのステータスを確認するには、次のコマンドを使用します。

```
Device# show install summary

[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
APDP  I    bootflash:apdp_CSCvp12345.bin
IMG   C    17.1.0.0
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

（注） このコマンドの出力は、パッケージ、およびインストールされているパッケージの状態によって異なります。

第 VI 部

セキュリティ

- ユーザーおよびエンティティの行動分析　（775 ページ）

第 41 章

IPv4 ACL

ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト（ACL）を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL はコントローラを通過するトラフィックをフィルタリングし、特定のインターフェイスを通過するパケットを許可または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、コントローラがパケットを受け入れるか拒否するかが決定されます。コントローラは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、コントローラはパケットを拒否します。コントローラは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。コントローラは、転送されるすべてのパケットに ACL を使用します。暗黙のホスト拒否拒否ルールがあります。

ネットワークに基本的なセキュリティを導入する場合は、コントローラにアクセスリストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラ

フィックの種類を決定したりできます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。

アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

（注） 中央スイッチングのアクセスポリシー（ACL）の下で適用できる ACE の最大数は 256 ACE です。Flex モードまたはローカルスイッチングに適用できる ACE の最大数は 64 ACE です。

ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートします。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージプロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類 ACL もサポートしています。

サポートされる ACL

コントローラでは、トラフィックをフィルタ処理するために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。IPv4 と MAC どちらのアクセス リスト タイプのどの方向に対してでも、レイヤ 2 インターフェイスにポート ACL を適応できます。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向（着信または発信）に適用されます。
- FQDN ACL：FQDN ACL は、IPv6 ACL とともにエンコードされ、AP に送信されます。FQDN ACL は常にカスタム ACL です。AP は、DNS スヌーピングを行い、IPv4 および IPv6 アドレスをコントローラに送信します。

ACL 優先順位

、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、ポート ACL です。

次の例で、簡単な使用例を説明します。

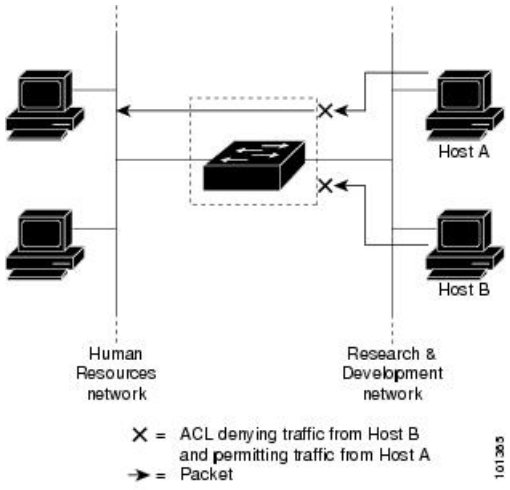
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。ポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

ポート ACL

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

図 *14 : ACL* によるネットワーク内のトラフィックの制御



次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が

同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注） レイヤ 2 インターフェイスに適用できるのは、IP アクセスリスト 1 つと MAC アクセスリスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス（SVI）、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケッ

トの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ（ACE）には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化されたIPパケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ4情報が含まれておらず、ACEが一部のレイヤ4情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。

（注） L4 Ops をともなう ACE の TCP では、フラグメント化パケットは RFC 1858 ごとにドロップします。

- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

ACEおよびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例

次のコマンドで構成され、フラグメント化された3つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
デバイス(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
デバイス(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
デバイス(config)# access-list 102 permit tcp any host 10.1.1.2
デバイス(config)# access-list 102 deny tcp any any
```

（注） 最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ3情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。

- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE（deny）と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。残りのフラグメントは 3 つめの ACE（permit）と一致します。

  最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。

ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

（注） 拡張 ACL のみがサポートされており、標準 ACL はサポートされていません。

IPv4 ACL スイッチでサポートされていない機能

このスイッチで IPv4 ACL を設定する手順は、他の Cisco スイッチやルータで IPv4 ACL を設定する手順と同じです。

以下の ACL 関連の機能はサポートされていません。

- 非 IP プロトコル ACL または
- IP アカウンティング

- 再帰 ACL およびダイナミック ACL はサポートされていません。
-
-

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

表 *21 :* アクセス リスト番号

アクセス リスト番号	タイプ	サポートあり
1 ～ 99	IP 標準アクセス リスト	あり
100 ～ 199	IP 拡張アクセス リスト	あり
200 ～ 299	プロトコル タイプコード アクセス リスト	なし
300 ～ 399	DECnet アクセス リスト	なし
400 ～ 499	XNS 標準アクセス リスト	なし
500 ～ 599	XNS 拡張アクセス リスト	なし
600 ～ 699	AppleTalk アクセス リスト	なし
700 ～ 799	48 ビット MAC アドレス アクセス リスト	なし
800 ～ 899	IPX 標準アクセス リスト	なし
900 ～ 999	IPX 拡張アクセス リスト	なし
1000 ～ 1099	IPX SAP アクセス リスト	なし
1100 ～ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	なし
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	なし
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	あり
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	あり

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACLの終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準IPv4 ACLを端末回線（仮想テレタイプ（VTY）回線）、またはインターフェイスに適用できます。

番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このスイッチは、ダイナミックまたは再帰アクセスリストをサポートしていません。また、タイプ オブ サービス（ToS）の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。また、このスイッチはこれらの IP プロトコルをサポートします。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル（**ahp**）
- カプセル化セキュリティペイロード（**esp**）
- Enhanced Interior Gateway Routing Protocol（**eigrp**）
- 総称ルーティング カプセル化（**gre**）
- インターネット制御メッセージ プロトコル（**icmp**）
- インターネット グループ管理プロトコル（**igmp**）
- すべての内部プロトコル（**ip**）
- IP-in-IP トンネリング（**ipinip**）
- KA9Q NOS 互換 IP over IP トンネリング（**nos**）

- Open Shortest Path First ルーティング（**ospf**）
- ペイロード圧縮プロトコル（**pcp**）
- プロトコル独立マルチキャスト（**pim**）
- 伝送制御プロトコル（**tcp**）
- ユーザ データグラム プロトコル（**udp**）

名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、必ずしも、IP アクセス リストを使用するすべてのコマンドで名前付きアクセスリストを利用できるわけではありません。

（注） 標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ～ 99 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。

ACL ロギング

標準 IP アクセスリストによって許可または拒否されたパケットに関するログメッセージが、コントローラのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslog メッセージを管理する **logging console** コマンドで管理されます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可（*permit*）または拒否（*deny*）ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケッ

トの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

（注） ロギング メッセージが多すぎて処理できない場合、または1秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギングパケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセスリストと一致する数の正確な情報源としてロギング設備をを使用しないでください。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。

コントローラの ACL スケールは次のとおりです。

- Cisco Catalyst 9800-40 ワイヤレスコントローラ、Cisco Catalyst 9800-L ワイヤレスコントローラ、Cisco Catalyst 9800-CL ワイヤレスコントローラ（中規模および小規模）は、128 の ACL と 128 のアクセスリストエントリ（ACE）をサポートします。
- Cisco Catalyst 9800-80 ワイヤレスコントローラおよび Cisco Catalyst 9800-CL ワイヤレスコントローラ（大規模）は、256 の ACL と 256 の ACE をサポートします。
- FlexConnect およびファブリックモード AP は、96 の ACL をサポートします。

（注） コントローラのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、コントローラに着信した該当 VLAN 内のトラフィックだけです。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチド パケットおよびルーテッド パケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、 特権 EXEC コマンドを使用します。

IPv4 ACL のインターフェイスに関する注意事項

インバウンド ACL の場合、パケットの受信後コントローラはパケットを ACL と照合します。ACL がパケットを許可する場合、コントローラはパケットの処理を継続します。ACL がパケットを拒否する場合、コントローラはパケットを廃棄します。

アウトバウンド ACL の場合、パケットを受信し制御対象インターフェイスにルーティングした後、コントローラはパケットを ACL と照合します。ACL がパケットを許可する場合、コントローラはパケットを送信します。ACL がパケットを拒否する場合、コントローラはパケットを廃棄します。

未定義の ACL に何もリストされていない場合、それは空のアクセスリストです。

IPv4アクセスコントロールリストの設定に関する制約事項

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **AppleTalk** は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アクセスリスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。
- DNS トラフィックは、Web 認証を待機しているクライアントの ACL エントリの有無にかかわらず、デフォルトで許可されます。

IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

レイヤ 2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

（注） **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合のみ有効です。このコマンドは、EtherChannel ポート チャネルでは使用できません。

IP アクセス リスト エントリ シーケンス番号

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。

ACL の設定方法

IPv4 ACL の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Add ACL Setup] ダイアログボックスで、次のパラメータを入力します。

- [ACL Name]：ACL の名前を入力します。
- [ACL Type]：[IPv4 Standard]。
- [Sequence]：シーケンス番号を入力します。
- [Action]：ドロップダウン リストからパケット フローの [Permit] または [Deny] を選択します。
- [Source Type]：パケットの送信元として [any]、[Host]、または [Network] を選択します。
- [Log]：ロギングを有効または無効にします。

ステップ 4 [Add] をクリックします。

ステップ 5 残りのルールを追加し、[Apply to Device] をクリックします。

IPv4 ACL の設定

スイッチで IP ACL を使用するには、次の手順に従います。

手順

ステップ 1 アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。

ステップ 2 ACL をインターフェイスまたは端末回線に適用します。

番号付き標準 ACL の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [ACL] ページで、[Add] をクリックします。

ステップ 3 [Add ACL Setup] ウィンドウで、次のパラメータを入力します。

- [ACL Name]：ACL の名前を入力します。
- [ACL Type]：[IPv4 Standard]。
- [Sequence]：シーケンス番号を入力します。
- [Action]：ドロップダウン リストからアクセスの [Permit] または [Deny] を選択します。
- [Source Type]：[any]、[Host]、または [Network] を選択します。
- [Log]：ロギングを有効または無効にします。これは、レイヤ 3 インターフェイスに関連付けられている ACL のみに限定されます。

ステップ 4 [Add] をクリックします。

ステップ 5 [Save & Apply to Device] をクリックします。

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# 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	**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard* [**log**] 例： デバイス(config)# **access-list 2 deny your_host**	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 *access-list-number* には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny** を指定し、許可する場合は **permit** を指定します。 *source* には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • キーワード **any** は 0.0.0.0 255.255.255.255 という *source* および *source-wildcard* の省略形です。source-wildcard を入力する必要はありません。 • キーワード **host** は送信元および *source* 0.0.0.0 の *source-wildcard* の省略形です。 （任意）*source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 （任意）**log** を指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。 （任意）**smartlog** を指定すると、拒否または許可されたパケットのコピーが NetFlow 収集装置に送信されます。 （注） ロギングは、レイヤ 3 インターフェイスに割り当てられた ACL でだけサポートされます。
ステップ 3	**end** 例：	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
	デバイス(config)# **end**	

番号付き拡張 ACL の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [ACL] ページで、[Add] をクリックします。

ステップ 3 [Add ACL Setup] ウィンドウで、次のパラメータを入力します。

- [ACL Name]：ACL の名前を入力します。
- [ACL Type]：[IPv4 Extended]。
- [Sequence]：シーケンス番号を入力します。
- [Action]：ドロップダウン リストからパケット フローの [Permit] または [Deny] を選択します。
- [Source Type]：パケットの送信元として [any]、[Host]、または [Network] を選択します。
- [Destination Type]：パケットの宛先として [any]、[Host]、または [Network] を選択します。
- [Protocol]：ドロップダウン リストからプロトコルを選択します。
- [Log]：ロギングを有効または無効にします。
- [DSCP]：パケットを DSCP 値に合わせる場合に入力します。

ステップ 4 [Add] をクリックします。

ステップ 5 [Save & Apply to Device] をクリックします。

番号付き拡張 ACL の作成（CLI）

番号付き拡張 ACL 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：	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
	デバイス# **configure terminal**	
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** tos] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： デバイス(config)# **access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log**	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 条件が一致した場合にパケットを拒否する場合は **deny** を指定し、許可する場合は **permit** を指定します。 *protocol* には、インターネット プロトコルの名前または番号を入力します。**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、**udp**、または IP プロトコル番号を表す 0 ～ 255 の整数を使用できます。一致条件としてインターネット プロトコル（ICMP、TCP、UDP など）を指定するには、キーワード **ip** を使用します。 （注） この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。 *source* には、パラメータの送信元であるネットワークまたはホストの番号を指定します。 *source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 *destination* には、パラメータの宛先であるネットワークまたはホストの番号を指定します。 *destination-wildcard* は、ワイルドカード ビットを宛先アドレスに適用します。

	コマンドまたはアクション	目的
		source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • 単一のホスト 0.0.0.0 を表すキーワード **host**。 その他のキーワードはオプションであり、次の意味を持ちます。 • **precedence**：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、**routine**（0）、**priority**（1）、**immediate**（2）、**flash**（3）、**flash-override**（4）、**critical**（5）、**internet**（6）、**network**（7）です。 • **fragments**：2 つ目以降のフラグメントをチェックする場合に入力します。 • **tos**：パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、**normal**（0）、**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）です。 • **time-range**：時間範囲の名前を指定します。 • **dscp**：パケットを 0 ～ 63 の番号で指定する DSCP 値と一致させる場合に入力します。または、指定できる値のリストを表示するには、疑問符（?）を使用します。

	コマンドまたはアクション	目的
		（注） 組み込みコントローラは次の機能をサポートしている必要があります。 • DCSP のマーク • UP のマーク • DSCP と UP のマッピング 「DSCP から UP へのマッピング」の詳細については、次を参照してください。 https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01 （注） **dscp** 値を入力する場合は、**tos** または **precedence** を入力できません。**dscp** を入力せずに **tos** と **precedence** の両方の値を入力できます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*] 例： `デバイス(config)# access-list 101 permit tcp any any eq 500`	拡張 TCP アクセス リストおよびアクセス条件を定義します。 次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。 （任意）*operator* および *port* を入力すると、送信元ポート（*source source-wildcard* の後に入力した場合）または宛先ポート（*destination destination-wildcard* の後に入力した場合）が比較されます。演算子の候補には、**eq**（次の値に等しい）、**gt**（次の値より大きい）、**lt**（次の値より小さい）、**neq**（次の値に等しくない）、および **range**（次の範囲）があります。演算子にはポート番号を指定する必要があります（range の場合は 2 つのポート番号をスペースで区切って指定する必要があります）。

	コマンドまたはアクション	目的
		port には、10 進数（0 ～ 65535）のポート番号または TCP ポート名を入力します。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。 他のオプションのキーワードの意味は次のとおりです。 • *flag*：指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、または **urg**（緊急）です。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `デバイス(config)# access-list 101 permit udp any any eq 100`	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag**は無効です。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `デバイス(config)# access-list 101 permit icmp any any 200`	拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指

	コマンドまたはアクション	目的
		定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。
ステップ 6	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `デバイス(config)# access-list 101 permit igmp any any 14`	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 *igmp-type*IGMP メッセージ タイプと比較するには、0～15 の番号またはメッセージ名（**dvmrp**、**host-query**、**host-report**、**pim**、または **trace**）を入力します。
ステップ 7	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

名前付き標準 ACL の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順にクリックします。

ステップ 2 [Add] をクリックして、新しい ACL 設定を作成します。

ステップ 3 [Add ACL Setup] ウィンドウで、次のパラメータを入力します。

- [ACL Name]：ACL の名前を入力します。
- [ACL Type]：[IPv4 Standard]。
- [Sequence]：有効な範囲は 1 ～ 99 または 1300 ～ 1999 です。
- [Action]：ドロップダウン リストからアクセスの [Permit] または [Deny] を選択します。
- [Source Type]：[any]、[Host]、または [Network] を選択します。

- [Log]：ロギングを有効または無効にします。これは、レイヤ 3 インターフェイスに関連付けられている ACL のみに限定されます。

ステップ 4 [追加（Add）] をクリックしてルールを追加します。

ステップ 5 [Save & Apply to Device] をクリックします。

名前付き標準 ACL の作成

名前を使用して標準 ACL 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	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# 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 3	**ip access-list standard** *name* 例： `デバイス(config)# ip access-list standard 20`	名前を使用して標準 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。 名前には、1 ～ 99 の番号を使用できます。
ステップ 4	次のいずれかを使用します。 • **deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] • **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] 例： `デバイス(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255` または	アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を指定します。 • **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。 • **any**：送信元および送信元ワイルドカードの値である 0.0.0.0 255.255.255.255

	コマンドまたはアクション	目的
	デバイス(config-std-nacl)# **permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0**	
ステップ 5	**end** 例： デバイス(config-std-nacl)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

名前付き拡張 ACL の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Add ACL Setup] ウィンドウで、次のパラメータを入力します。

- [ACL Name]：ACL の名前を入力します。
- [ACL Type]：[IPv4 Extended]。
- [Sequence]：シーケンス番号を入力します。
- [Action]：ドロップダウン リストからパケット フローの [Permit] または [Deny] を選択します。
- [Source Type]：パケットの送信元として [any]、[Host]、または [Network] を選択します。
- [Destination Type]：パケットの宛先として [any]、[Host]、または [Network] を選択します。
- [Protocol]：ドロップダウン リストからプロトコルを選択します。

- [Log]：ロギングを有効または無効にします。
- [DSCP]：パケットを DSCP 値に合わせる場合に入力します。

ステップ 4 [Add] をクリックします。

ステップ 5 残りのルールを追加し、[Apply to Device] をクリックします。

名前付き拡張 ACL の作成

名前を使用して拡張 ACL 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	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# 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 3	**ip access-list extended** *name* 例： `デバイス(config)# ip access-list extended 150`	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。 名前には、100 ～ 199 の番号を使用できます。
ステップ 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] 例： `デバイス(config-ext-nacl)# permit 0 any any`	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。**log** キーワードを使用すると、違反を含むアクセス リストのログ メッセージを取得できます。 • **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。 • **host** *destination*：接続先および接続先ワイルドカードの値である *destination* 0.0.0.0。

	コマンドまたはアクション	目的
		• **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 5	**end** 例： デバイス(config-ext-nacl)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

次のタスク

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

インターフェイスへの IPv4 ACL の適用（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [Associating Interfaces] をクリックします。

ステップ 3 [Available Interfaces] リストからインターフェイスを選択して、右側に ACL の詳細を表示します。必要に応じて、ACL の詳細を変更できます。

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

インターフェイスへの IPv4 ACL の適用（CLI）

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで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	**interface** *interface-id* 例： `Device(config)#`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ3インターフェイス（ルータ ACL）を指定できます。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} 例： `Device(config-if)# ip access-group 2 in`	指定されたインターフェイスへのアクセスを制御します。
ステップ 4	**end** 例：	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
	`Device(config-if)# end`	
ステップ 5	**show running-config** 例： `Device# show running-config`	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ポリシープロファイルへの ACL の適用（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] ウィンドウで、[Access Policies] タブをクリックします。
ステップ 4 [WLAN ACL] 領域で、[IPv4 ACL] ドロップダウンリストから [IPv4 ACL] を選択します。
ステップ 5 [Apply to Device] をクリックします。

ポリシープロファイルへの ACL の適用

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 profile-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。

	コマンドまたはアクション	目的
ステップ 3	**ipv4 acl** *acl-name* 例： `Device(config-wireless-policy)# ipv4 acl test-acl`	IPv4 ACL を設定します。
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ACL の設定例

例：ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。コメントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
デバイス(config)# access-list 1 remark Permit only Jones workstation through
デバイス(config)# access-list 1 permit 171.69.2.88
デバイス(config)# access-list 1 remark Do not allow Smith through
デバイス(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセスリスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
デバイス(config)# ip access-list extended telnetting
デバイス(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
```

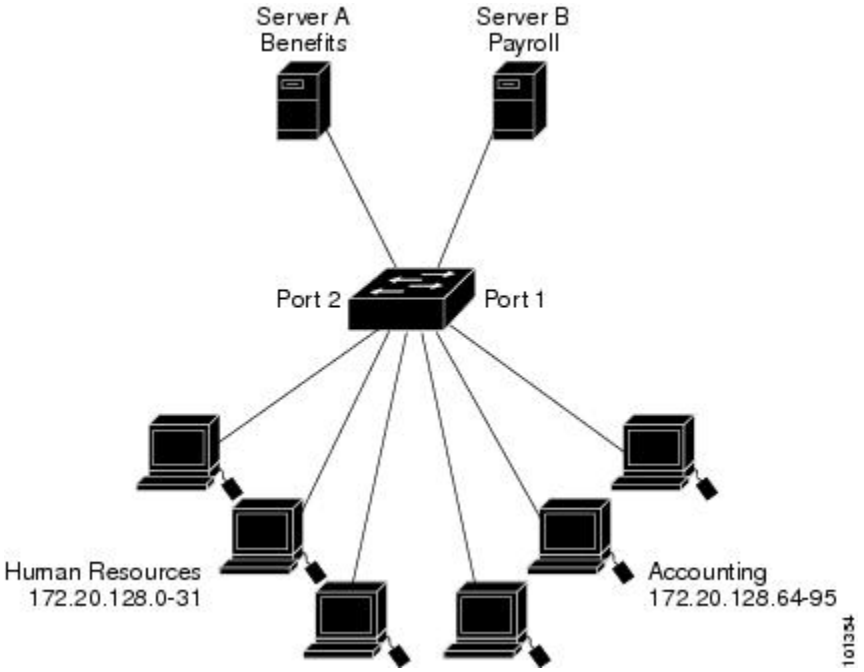
```
デバイス(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

IPv4 ACL の設定例

ここでは、IPv4 ACL を設定および適用する例を示します。ACL のコンパイルに関する詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』および『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Adderssing and Services」の章にある「Configuring IP Services」の項を参照してください。

小規模ネットワークが構築されたオフィス用の ACL

図 *15 :* ルータ *ACL* によるトラフィックの制御



次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッドポート2に接続されたサーバー A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバー B には、機密扱いの給与支払いデータが格納されています。サーバー A にはすべてのユーザーがアクセスできますが、サーバー B にアクセスできるユーザーは制限されています。

ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバーに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバーからポート 1 に着信するトラフィックをフィルタリングします。

例：小規模ネットワークが構築されたオフィスの ACL

次に、標準 ACL を使用してポートからサーバー B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
デバイス(config)# access-list 6 permit 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 6 out
```

次に、拡張 ACL を使用してサーバー B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバー B）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。この ACL は、ルーテッド ポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
デバイス(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 106 in
```

例：番号付き ACL

次の例のネットワーク 10.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク 10.0.0.0 アドレスの 3 番目および 4 番目のオクテットで特定のホストを指定します。アクセス リスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 10.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
デバイス(config)# access-list 2 permit 10.48.0.3
デバイス(config)# access-list 2 deny 10.48.0.0 0.0.255.255
デバイス(config)# access-list 2 permit 10.0.0.0 0.255.255.255
デバイス(config)#
デバイス(config-if)# ip access-group 2 in
```

例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番目の行は、ホスト 128.88.1.2 のシンプルメール転送プロトコル（SMTP）ポートへの着信 TCP 接続を許可します。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
デバイス(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
デバイス(config)# access-list 102 permit icmp any any
デバイス(config)#
デバイス(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。安全なネットワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスとを個別に制御できます。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
デバイス(config)#
デバイス(config-if)# ip access-group 102 in
```

例：名前付き ACL

名前付き標準 ACL および名前付き拡張 ACL の作成

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
デバイス(config)# ip access-list standard Internet_filter
デバイス(config-ext-nacl)# permit 1.2.3.4
デバイス(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
デバイス(config)# ip access-list extended marketing_group
デバイス(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
デバイス(config-ext-nacl)# deny tcp any any
デバイス(config-ext-nacl)# permit icmp any any
デバイス(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
デバイス(config-ext-nacl)# deny ip any any log
デバイス(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
デバイス(config)# interface gigabitethernet3/0/1

デバイス(config-if)# ip address 2.0.5.1 255.255.255.0
デバイス(config-if)# ip access-group Internet_filter out
デバイス(config-if)# ip access-group marketing_group in
```

名前付き ACL からの個別 ACE の削除

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
デバイス(config)# ip access-list extended border-list
デバイス(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

IPv4 ACL のモニタリング

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用済みの ACL を表示することで、IPv4 ACL をモニターできます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 *22*：アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
show access-lists [*number* | *name*]	最新の IP および MAC アドレス アクセス リストの全体または特定のアクセス リスト（番号付きまたは名前付き）を表示します。
show ip access-lists [*number* | *name*]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。

コマンド	目的
show ip interface *interface-id*	インターフェイスの詳細設定およびステータスを表示しま ネーブルになっているインターフェイスに、**ip access-gro** フェイス コンフィギュレーション コマンドを使用して A た場合は、アクセス グループも表示に含まれます。
show running-config [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのコンフィ ン ファイルの内容（設定されたすべての MAC および IP ストや、どのアクセス グループがインターフェイスに適用 ど）を表示します。

第 42 章

DNS ベースのアクセス コントロール リスト

DNS ベースのアクセス コントロール リストについて

DNS ベースの ACL は、ワイヤレス クライアント デバイスに使用されます。これらのデバイスを使用する場合は、許可またはブロックするデータ要求を決定するために、組み込みワイヤレスコントローラで認証前 ACL を設定できます。

組み込みワイヤレスコントローラで DNS ベースの ACL を有効にするには、ACL の許可 URL または拒否 URL を設定する必要があります。URL は、ACL で事前設定しておく必要があります。

DNS ベースの ACL によって、登録フェーズ中のクライアントは、設定された URL への接続を許可されます。 組み込みワイヤレスコントローラは ACL 名で設定され、AAA サーバーから返されます。ACL 名が AAA サーバーによって返されると、ACL は Web リダイレクト用にクライアントに適用されます。

クライアント認証フェーズで、AAA サーバーは事前認証 ACL（url-redirect-acl：AAA サーバーに与えられた属性名）を返します。DNS スヌーピングは、登録が完了してクライアントが SUPPLICANT PROVISIONING 状態になるまで、各クライアントの AP で実行されます。URL で設定された ACL が 組み込みワイヤレスコントローラで受信されると、CAPWAP ペイロードが AP に送信され、クライアントの DNS スヌーピングが有効になり、URL がスヌーピングされます。

適切な URL スヌーピングにより、AP は DNS 応答の解決済みドメイン名の IP アドレスを学習します。設定された URL にドメイン名が一致した場合は、IP アドレスを求めるために DNS 応答が解析されます。AP によって IP アドレスの許可リストに IP アドレスが追加されるため、クライアントは設定された URL にアクセスできます。

事前認証または事後認証中に、DNS ACL がアクセスポイントのクライアントに適用されます。クライアントが、ある AP から別の AP にローミングした場合、古い AP で DNS により学習された IP アドレスは新しい AP でも有効になります。

この機能は次のように URL リストをサポートします。

- 最大 32 個の URL リスト。
- URL リストごとに最大 32 個の URL。
- URL ごとに最大 30 個の IP アドレス。
- ワイルドカードを含む最大 16 個の URL リスト。
- ワイルドカードの URL ごとに最大 10 個の URL。

（注） ワイルドカードベースの URL を設定する場合、一般的なワイルドカード URL は使用できません。ドメイン名の間にワイルドカードを使用することはできません。1 つの URL に複数のワイルドカードを使用することはできません。URL でのワイルドカードの指定は、第 3 レベル以上のレベルでのみ使用できます。

（注） 競合する設定や無効な設定は使用できません。同じ URL に異なるアクションを設定することはできません。たとえば、拒否（Deny）許可（Allow）を www.yahoo.com で設定することはできません。

（注） ローカルモードの場合は、ポリシープロファイルに URL フィルタをアタッチする必要があります。フレックスモードでは、URL フィルタはフレックスプロファイルにアタッチされるため、ポリシープロファイルにアタッチする必要はありません。

（注） DNS ベースの URL は、クライアントからのアクティブな DNS クエリで機能します。したがって、URL フィルタリングでは、DNS を正しく設定する必要があります。

（注） URL フィルタは、パントまたはリダイレクト ACL、およびカスタムまたは静的事前認証 ACL よりも優先されます。

組み込みワイヤレスコントローラの FlexConnect

FlexConnect 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。このソリューションを使用することで、各ブランチオフィスで組み込みワイヤレスコントローラを展開することなく、企業オフィスからワイドエリアネットワーク（WAN）リンク経由で、ブランチまたはリモートオフィスのアクセスポイントを設定および制御できます。

FlexConnect アクセスポイントは、クライアント データ トラフィックをローカルに切り替え、認証を中央で実行できます。また、FlexConnect AP は、コントローラへの接続を失った場合にクライアント認証をローカルで実行できます。コントローラへの接続が回復した場合、認証とポリシーの詳細を組み込みワイヤレスコントローラに送り返すこともできます。

組み込みワイヤレス コントローラ ネットワークは、少なくとも 1 つの 802.11ax Wave 2 Cisco Aironet シリーズアクセスポイント（AP）と、ネットワーク内の他の AP を管理するソフトウェアベースの組み込みワイヤレスコントローラで構成されます。組み込みワイヤレスコントローラとして機能している AP をプライマリ AP といい、そのプライマリ AP によって管理されるネットワーク内の他の AP を下位 AP といいます。プライマリ AP は、組み込みワイヤレスコントローラとして機能するのに加え、下位 AP と連動してクライアントにサービスを提供する AP としても動作します。

事前認証 DNS ACL 機能は、ウォールドガーデン機能とも呼ばれます。ウォールドガーデンは、認証なしでアクセスできる Web サイトまたはドメインのリストです。DNS スヌーピングは各クライアントの AP で実行され、設定されたルールは送信元または宛先 IP と一致した後にクライアントトラフィックに適用されます。

ローミング

ローミング中、サポートクライアントは既存のローミングサポートを使用して AP 間をローミングします。DNS ACL は、ローミング後もターゲット AP で保持されます。DNS 事前認証 ACL および事後認証 ACL を使用したローミングの場合、ターゲット AP は、サービスを提供する AP からクライアントが解決した IP を学習します。

DNS ベースのアクセス コントロール リストの制約事項

DNS ベースの ACL には次の制約があります。

- 中央認証を使用した FlexConnect ローカルスイッチング AP でのみサポートされています。
- AP が FlexConnect ローカル スイッチング モードにある場合、ローカル認証を使用した FlexConnect では認証後の DNS ベースの ACL はサポートされません。
- 完全修飾ドメイン名（FQDN）または DNS ベースの ACL は、Cisco Wave 1 アクセスポイントではサポートされていません。
- URL フィルタでは最初の 20 個の URL のみ考慮されますが、追加もできます。

- URL フィルタでは通常の正規表現パターンが採用され、ワイルドカード文字は URL の先頭または末尾でのみ使用できます。
- URL ACL が定義され、WLAN に関連付けられる FlexConnect ポリシープロファイルに追加されます。URL ACL は、ローカルモードの URL ACL と同様の方法で作成されます。
- FlexConnect モードでは、URL ドメイン ACL は、FlexConnect ポリシープロファイルに接続されている場合にのみ機能します。
- ポリシープロファイルを WLAN またはローカル ポリシーに関連付けることにより、ACL を WLAN に適用できます。ただし、「url-redirect-acl」を使用してオーバーライドできます。
- ISE から受信した Cisco AV ペアの場合、特定のクライアントに適用する必要があるポリシーは、ADD MOBILE の一部としてプッシュされます。

  message.
- AP が接続するか、既存の URL ACL が変更されて FlexConnect プロファイルに適用されると、マッピングされた URL フィルタリストとともに ACL 定義が AP にプッシュされます。
- AP は、マッピングされた ACL 名を使用して URL ACL 定義を保存し、DNS パケットをスヌープして、ACL の各 URL の最初の IP アドレスを学習します。AP は、IP アドレスを学習すると、URL および IP バインディングのコントローラを更新します。コントローラは、将来使用するためにこの情報をクライアントデータベースに記録します。
- 事前認証状態の間にクライアントが別の AP にローミングすると、学習した IP アドレスが新しい AP にプッシュされます。それ以外の場合、学習した IP アドレスは、クライアントが認証後の状態に移行したとき、または学習した IP アドレスの TTL が期限切れになったときに消去されます。

フレックス モード

URL フィルタリストの設定（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。
ステップ 2	**wireless profile flex** *custom-flex-profile* **例：** `Device(config)# wireless profile flex custom-flex-profile`	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。

	コマンドまたはアクション	目的
ステップ 3	**acl-policy** *acl-policy-name* 例： `Device(config-wireless-flex-profile)#acl-policy acl-policy-name`	ACL ポリシーの説明を設定します。
ステップ 4	**urlfilter list** *url-filterlist-name* 例： `Device(config-wireless-flex-profile-acl)# urlfilter list url-filterlist-name`	URL フィルタリストの名前を設定して Flex プロファイルに適用します。 これは、ACL バインディング用の Flex URL フィルタ コンフィギュレーション コマンドです。

URL フィルタリストの設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [URL Filters] を選択します。
[URL Filters] ページが表示されます。

ステップ 2 [Add] ボタンをクリックします。
[Add URL Filters] ウィンドウが表示されます。

ステップ 3 [Type] ドロップダウンリストから、[PRE-AUTH] または [POST-AUTH] を選択します。

a) [POST-AUTH]：[IPv4] および [IPv6] の [Redirect Servers] を指定します。

ステップ 4 スライダを使用して、[Action] を [Permit] または [Deny] にします。

ステップ 5 [URLs] フィールドで URL を指定します。すべての URL を新しい行に入力します。

ステップ 6 [Apply to Device] をクリックします。

WLAN でのカスタム事前認証 DNS ACL の適用

事前認証の場合、この設定は Web 認証 WLAN 上にある必要があります。

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	**wlan***wlan-name wlan-id ssid-name* 例： `Device(config)# wlan wlan-name wlan-id ssid-name`	WLAN コンフィギュレーション サブモードを開始します。 1. 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。 2. wlan-id：WLAN ID を入力します。範囲は 1 ～ 512 です。 3. 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。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	**ip access-group web** *access-list-name* 例： `Device(config-wlan)#ip access-group web preauth-acl-wlan`	ACL を Web 認証 WLAN にマッピングします。 access-list-name は、IPv4 ACL の名前または ID です。

ポリシープロファイルでのカスタム事後認証 DNS ACL の適用

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-name* 例： `Device(config)# wireless profile policy custom-policy-profile`	WLAN のポリシー プロファイルを作成します。
ステップ 3	{**ipv4** | **ipv6**} **acl** *post-acl-name* 例： `Device(config-wireless-policy)#ipv4 acl post-acl`	ワイヤレス IPv4 または IPv6 設定の ACL 設定を作成します。

中央 Web 認証用の ISE の設定（GUI）

中央 Web 認証用に ISE を設定するには、次の手順に従います。

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 3 [Results] をクリックします。

ステップ 4 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 5 [Add] をクリックして、URL フィルタ用の新しい許可プロファイルを作成します。

ステップ 6 [Name] フィールドにプロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 7 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] オプションを選択します。

ステップ 8 または、[Common Tasks] セクションで、[Web Redirection] をオンにします。

ステップ 9 ドロップダウンリストから [Centralized Web Auth] オプションを選択します。

ステップ 10 ACL を指定し、ドロップダウンリストから ACL 値を選択します。

ステップ 11 [Advanced Attributes Setting] セクションで、ドロップダウン リストから [Cisco:cisco-av-pair] を選択します。

（注） 優先順位に基づいて、複数の ACL をコントローラに適用できます。L2 認証 + WebAuth マルチ認証のシナリオでは、ISE が L2 認証中に ACL を返す場合、ISE ACL はデフォルトの WebAuth リダイレクト ACL よりも優先されるため、ISE ACL に許可ルールがある場合、トラフィックは WebAuth 保留状態で実行されます。このシナリオを回避するには、L2 認証 ISE から返される ACL の優先順位を設定する必要があります。デフォルトの WebAuth リダイレクト ACL の優先順位は 100 です。トラフィックの問題を回避するには、ISE によって返される ACL のリダイレクト ACL 優先順位を 100 より上の値に設定する必要があります。

ステップ 12 それぞれのペアの後にある（[+]）アイコンをクリックして 1 つずつ入力します。

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

次に例を示します。

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?
sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&daysToExpiry=value&action=cwa
```

ステップ 13 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

DNS ベースのアクセス コントロール リストの表示

URL リストを表示するには、次のコマンドを使用します。

```
Device #show wireless urlacl-enhanced summary
URL-List
--------------------------------
urllist_ut
urllist_max1
urllist_max2
urllist_max3
urllist_max4
urllist_max5
```

特定の URL リストの詳細を表示するには、次のコマンドを使用します。

```
Device#show wireless urlacl-enhanced details urllist_ut
List Name..................... : urllist_ut
Configured List of URLs
URL                  Preference Action Validity Invalidated URL
-------------------------------------------------------------------------------
url1.dns.com         1                 PERMIT         VALID 0
url2.dns.com         2                 DENY           VALID 0
url3.dns.com         3                 PERMIT         VALID 0
url4.dns.com         4                 DENY           VALID 0
url11.dns.com        6                 DENY           VALID 0
url12.dns.com        7                 PERMIT         VALID 0
url13.dns.com        8                 DENY           VALID 0
www.example.com      14                PERMIT         VALID 0
```

Flex プロファイルの詳細を表示するには、次のコマンドを使用します。

```
Device# sh wireless profile flex detailed custom-flex-profile
Flex Profile Name : custom-flex-profile
Description : custom flex profile
Local Auth :
        AP:
                Radius Enable            : ENABLED
                PEAP                     : DISABLED
                LEAP                     : DISABLED
                TLS                      : DISABLED
                EAP fast profile         : Not Configured
                User List                : Not Configured
        RADIUS:
                RADIUS server group name : Not Configured
        Fallback Radio shut              : DISABLED
        ARP caching                      : ENABLED
        Efficient Image Upgrade          : ENABLED
        OfficeExtend AP                  : DISABLED
        Join min latency                 : DISABLED
        Policy ACL :
                ACL Name                          URL Filter List
        Name                 Central Webauth
        ---------------------------------------------------------------
        post-acl                urllist_ut        DISABLED
        pre_v4              urllist_pre_cwa   DISABLED
        ACL-REDIRECTTTTTTT2     urllist_ut        DISABLED
        VLAN Name - VLAN ID mapping       : Not Configured
```

クライアントの詳細を表示するには、次のコマンドを使用します。

```
Device#sh wireless client mac-address <Mac-address> detail
```

アクセスポイントの確認

AP の ACL の設定を表示するには、次のコマンドを使用します。

```
Device# show ip access-lists
Extended IP access list pre_v4
        1 permit udp any range 0 65535 any eq 53
        2 permit tcp any range 0 65535 any eq 53
        3 permit udp any dhcp_server any range 0 65535
        4 permit udp any range 0 65535 any eq 68
        5 permit udp any dhcp_client any range 0 65535
        6 deny ip any any
```

URL リストの設定を表示するには、次のコマンドを使用します。

```
Device#show flexconnect url-acl
ACL-NAME         ACTION         URL-LIST
pre_v4
                 allow          test.dns.com
                 allow          url2.dns.com
                 allow          url3.dns.com
                 allow          url10.dns.com
                 allow          url11.dns.com
                 allow          www.cwapre.com
                 allow          www.google.com
                 allow          oldconfig.dns.com
                 allow          *.cisco.com
```

事前認証クライアントの設定を表示するには、次のコマンドを使用します。

```
Device# show client access-lists pre-auth all C0:C1:C0:70:58:2F
Pre-Auth URL ACLs for Client: C0:C1:C0:70:58:2F
IPv4 ACL: pre_v4
IPv6 ACL:
ACTION         URL-LIST
allow          url1.dns.com
deny           url2.dns.com
allow          url3.dns.com
deny           url4.dns.com
allow          www.example.com
deny           url11.dns.com
allow          url12.dns.com
deny           url13.dns.com

Resolved IPs for Client: C0:C1:C0:70:58:2F
HIT-COUNT         URL         ACTION         IP-LIST
post-acl
        rule 0:   allow true
No IPv6 ACL found
```

事後認証クライアントの設定を表示するには、次のコマンドを使用します。

```
Device# show client access-lists post-auth all C0:C1:C0:70:58:2F
Post-Auth URL ACLs for Client: C0:C1:C0:70:58:2F
IPv4 ACL: post-acl
IPv6 ACL:
ACTION         URL-LIST
allow          url1.dns.com
deny           url2.dns.com
allow          url3.dns.com
deny           url4.dns.com
allow          www.example.com
deny           url11.dns.com
allow          url12.dns.com
deny           url13.dns.com
```

```
Resolved IPs for Client: C0:C1:C0:70:58:2F
HIT-COUNT         URL         ACTION         IP-LIST
post-acl
        rule 0: allow true
No IPv6 ACL found
```

事前認証で学習した IP を表示するには、次のコマンドを使用します。

```
Device#show client access-lists pre-auth all 60:14:B3:AA:C6:FB
Pre-Auth URL ACLs for Client: 60:14:B3:AA:C6:FB
IPv4 ACL: acl_1
IPv6 ACL:
ACTION         URL-LIST
allow          url1.dns.com
deny           url2.dns.com

Resolved IPs for Client: 60:14:B3:AA:C5:FB
HIT-COUNT         URL                 ACTION         IP-LIST
10                url1.dns.com        allow          9.10.8.1
```

事後認証で学習した IP を表示するには、次のコマンドを使用します。

```
Device#show client access-lists post-auth all 60:14:B3:AA:C6:FB
Post-Auth URL ACLs for Client: 60:14:B3:AA:C5:FB
IPv4 ACL: post_acl
IPv6 ACL:
ACTION         URL-LIST
deny           url1.dns.com
allow          url2.dns.com

Resolved IPs for Client: 60:14:B3:AA:C5:FB
HIT-COUNT         URL                 ACTION         IP-LIST
16                url2.dns.com        allow          9.10.9.1
postauth_acl
          rule 0: allow true
```

第 43 章

特定の URL の許可リスト

特定の URL の許可リスト

この機能は、 組み込みワイヤレスコントローラまたは AP で特定の URL を許可リストに追加するのに役立ち、インターネット接続がなくても追加した特定の URL を使用できるようになります。キャプティブポータルとウォールドガーデンの Web 認証用の URL を許可リストに登録できます。URL の許可リストにアクセスする際に認証は必要ありません。許可リストに含まれていないサイトにアクセスしようとすると、ログインページにリダイレクトされます。

許可リストへの URL の追加

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	**urlfilter list** *<urlfilter-name>* 例： `Device(config)# urlfilter list url-allowedlist-nbn`	URL フィルタプロファイルを設定します。
ステップ 3	**action** [**deny** | **permit**] 例： `Device(config-urlfilter-params)# action permit`	リストを許可リストとして設定します。permit コマンドではリストを許可リストとして設定し、deny コマンドではリストをブロックリストとして設定します。

	コマンドまたはアクション	目的
ステップ 4	{**redirect-server-ipv4** | **redirect-server-ipv6**} 例： `Device(config-urlfilter-params)# redirect-server-ipv4 X.X.X.X`	要求が拒否された場合にユーザー要求がリダイレクトされるリダイレクトサーバーの IP アドレスを設定します。
ステップ 5	**url** *url-to-be-allowed* 例： `Device(config-urlfilter-params)# url www.cisco.com`	許可する URL を設定します。

（注） コントローラでは 2 つの IP アドレスを使用し、メカニズムによって 1 つのポータル IP のみが許可されます。より多くの HTTP リソースへの事前認証アクセスを許可するには、URL フィルタを使用する必要があります。これにより、URL フィルタに入力した URL を持つ Web サイトに関連する IP の代行受信（リダイレクト）およびセキュリティ（事前認証）ACL に動的にホールが作成されます。コントローラがこれらの URL の IP アドレスを学習し、ACL に動的に追加できるように、DNS 要求が動的にスヌーピングされます。

（注） **redirect-server-ipv4** および **redirect-server-ipv6** は、ローカルモードで、特に認証後にのみ適用できます。さらに追跡したり、警告メッセージを表示したりする場合、拒否されたユーザー要求は設定されたサーバーにリダイレクトされます。

ただし、拒否されたアクセスのリダイレクトログイン URL のコントローラにリダイレクトされるため、**redirect-server-ipv4** および **redirect-server-ipv6** の設定は事前認証シナリオには適用されません。

許可された URL を Flex プロファイルの ACL ポリシーに関連付けることができます。

例

Flex プロファイルでの許可 URL と ACL ポリシーの関連付け：

```
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy user_v4_acl
Device(config-wireless-flex-profile-acl)# urlfilter list url_allowedlist_nbn
Device(config-wireless-flex-profile-acl)# exit
Device(config-wireless-flex-profile)# description "default flex profile"

Device(config)# urlfilter enhanced-list urllist_pre_cwa
Device(config-urlfilter-enhanced-params)# url url1.dns.com preference 1 action permit
Device(config-urlfilter-enhanced-params)# url url2.dns.com preference 2 action deny
Device(config-urlfilter-enhanced-params)# url url3.dns.com preference 3 action permit

Device(config)# wlan wlan5 5 wlan5
Device(config-wlan)#ip access-group web user_v4_acl
```

```
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa wpa2 ciphers aes
Device(config-wlan)#no security wpa akm dot1x
Device(config-wlan)#security web-auth
Device(config-wlan)#security web-auth authentication-list default
Device(config-wlan)#security web-auth parameter-map global
Device(config-wlan)#no shutdown
```

許可リストの URL の確認

許可リストの URL のサマリーと詳細を確認するには、次の show コマンドを使用します。

```
Device# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                          ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------
url-whitelist                     1    PRE-AUTH     PERMIT   1.1.1.1

Device#

Device# show wireless urlfilter details url-whitelist
List Name..................... : url-whitelist
Filter ID..................... : : 1
Filter Type................... : PRE-AUTH
Action........................ : PERMIT
Redirect server ipv4...... : 1.1.1.1
Redirect server ipv6...... :
Configured List of URLs
   URL........................ : www.cisco.com
```

第 44 章

Web ベース認証

この章では、デバイスで Web ベース認証を設定する方法について説明します。この章の内容は、次のとおりです。

認証の概要

Web 認証は、オープン認証または適切なレイヤ 2 セキュリティ方式を使用して、WLAN 上のホストへの簡単で安全なゲストアクセスを提供するように設計されたレイヤ 3 セキュリティソリューションです。Web 認証を使用すると、クライアント側で最小限の設定を行うだけで、ユーザーはワイヤレスクライアントの Web ブラウザを介して認証を受けることができます。これにより、ユーザーはユーザープロファイルを設定しなくても、オープン SSID に関連付けることができます。ホストは DHCP サーバーから IP アドレスと DNS 情報を受け取りますが、認証に成功するまでネットワークリソースにアクセスできません。ホストがゲストネットワークに接続すると、WLC はホストを認証 Web ページにリダイレクトします。そこで、ユーザーは有効なログイン情報を入力する必要があります。ログイン情報は WLC または外部認証サーバーによって認証され、認証に成功すると、ネットワークへのフルアクセスが許可されます。また、事前認証 ACL 機能を設定する必要がある認証の前に、特定のネットワークリソースへの制限付きアクセスをホストに許可することもできます。

次に、さまざまなタイプの Web 認証方式を示します。

- ローカル Web 認証（LWA）：コントローラ上のレイヤ 3 セキュリティとして設定され、Web 認証ページと事前認証 ACL はコントローラでローカルに設定されます。コントローラは、htttp(s) トラフィックを代行受信し、認証のためにクライアントを内部 Web ページにリダイレクトします。ログインページでクライアントが入力したログイン情報は、コントローラによってローカルに認証されるか、RADIUS サーバーまたは LDAP サーバーを介して認証されます。
- 外部 Web 認証（EWA）：コントローラ上のレイヤ 3 セキュリティとして設定され、コントローラは htttp(s) トラフィックを代行受信し、外部 Web サーバーでホストされているロ

グインページにクライアントをリダイレクトします。ログインページでクライアントが入力したログイン情報は、コントローラによってローカルに認証されるか、RADIUS サーバーまたは LDAP サーバーを介して認証されます。事前認証 ACL は、コントローラで静的に設定されます。

- 中央 Web 認証（CWA）：主にコントローラ上のレイヤ 2 セキュリティとして設定され、リダイレクト URL と事前認証 ACL は ISE 上に存在し、レイヤ 2 認証時にコントローラにプッシュされます。コントローラは、クライアントからのすべての Web トラフィックを ISE ログインページにリダイレクトします。ISE は、HTTPS を介してクライアントによって入力されたログイン情報を検証し、ユーザーを認証します。

IEEE 802.1x サプリカントが実行されていないホスト システムでエンド ユーザーを認証するには、Web 認証プロキシとして知られている 認証機能を使用します。

クライアントが HTTP セッションを開始すると、認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザーに HTML ログインページを送信します。ユーザーはクレデンシャルを入力します。このクレデンシャルは、認証機能により、認証のために認証、許可、アカウンティング（AAA）サーバーに送信されます。

認証に成功した場合、認証は、ログインの成功を示す HTML ページをホストに送信し、AAA サーバーから返されたアクセス ポリシーを適用します。

認証に失敗した場合、認証は、ログインの失敗を示す HTML ページをユーザーに転送し、ログインを再試行するように、ユーザーにプロンプトを表示します。最大試行回数を超過した場合、認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザーは。

（注） Webauth クライアントの認証試行時に受信する traceback には、パフォーマンスや行動への影響はありません。これは、ACL アプリケーションの EPM に FFM が返信したコンテキストがすでにキュー解除済み（タイマーの有効期限切れの可能性あり）で、セッションが「未承認」になった場合にまれに発生します。

（注） コマンド許可が TACACS を介した AAA 認証構成の一部として有効になっていて、対応する方式リストが HTTP 構成の一部として設定されていない場合、WebUI ページでデータが読み込まれません。ただし、一部のワイヤレス機能ページは、コマンドベースではなく権限ベースであるため、動作する場合があります。

Web ページがホストされている場所に基づいて、ローカル Web 認証は次のように分類できます。

- 内部：ローカル Web 認証時に、組み込みワイヤレスコントローラの内部デフォルト HTML ページ（ログイン、成功、失敗、および期限切れ）が使用されます。
- カスタマイズ：ローカル Web 認証時に、カスタマイズされた Web ページ（ログイン、成功、失敗、および期限切れ）が組み込みワイヤレスコントローラにダウンロードされ、使用されます。

- 外部：組み込みまたはカスタム Web ページを使用する代わりに、外部 Web サーバー上でカスタマイズされた Web ページがホストされます。

さまざまな Web 認証ページに基づき、Web 認証のタイプは次のように分類できます。

- *Webauth*：これが基本的な Web 認証です。この場合、組み込みワイヤレスコントローラはユーザー名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザーは正しいクレデンシャルを入力する必要があります。
- *Consent* または *web-passthrough*：この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンが表示されたポリシー ページを提示します。ネットワークにアクセスするには、ユーザーは [Accept] ボタンをクリックする必要があります。
- *Webconsent*：これは webauth と consent の Web 認証タイプの組み合わせです。この場合、組み込みワイヤレスコントローラは、[Accept] ボタンまたは [Deny] ボタンがあり、ユーザー名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザーは正しいクレデンシャルを入力して [Accept] ボタンをクリックする必要があります。

（注）
- webauth パラメータマップ情報は、**show running-config** コマンドの出力を使用して表示できます。
- ワイヤレス Web 認証機能は、バイパス タイプをサポートしていません。
- AP の再接続が発生するまで、Web 認証パラメータマップのリダイレクトログイン URL の変更は発生しません。新しい URL リダイレクションを適用するには、WLAN を有効または無効にする必要があります。

（注）
カスタマイズされた Web 認証ログイン ページを作成する場合は、シスコのガイドラインに従うことをお勧めします。Google Chrome または Mozilla Firefox ブラウザの最新バージョンにアップグレードした場合は、Web 認証バンドルの login.html ファイルに次の行が含まれていることを確認します。

```
<body onload="loadAction();">
```

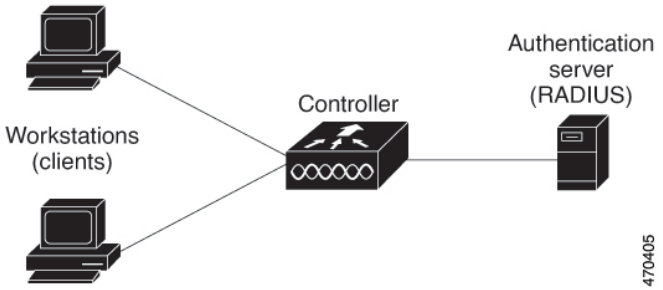
デバイスのロール

ローカル Web 認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：ネットワークおよびコントローラへのアクセスを要求し、コントローラからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script が有効な HTML ブラウザが実行されている必要があります。

- 認証サーバー：クライアントを認証します。認証サーバーはクライアントのIDを確認し、そのクライアントにネットワークおよびコントローラサービスへのアクセスを許可するか、そのクライアントを拒否するかをコントローラに通知します。
- コントローラ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。コントローラはクライアントと認証サーバーとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、識別情報を認証サーバーで確認し、クライアントに応答をリレーします。

図 *16 :* ローカル *Web* 認証のデバイスの役割



認証プロセス

ページがコントローラでホストされている場合、コントローラは仮想 IP（通常は 192.0.2.1 などのルーティング不可能なIP）を使用してリクエストを処理します。ページが外部でホストされている場合、Web リダイレクトは最初にクライアントを仮想 IP に送信します。その後、仮想 IP の場所などの引数が URL に追加されて、ユーザーが外部ログインページに再度送信されます。ページが外部でホストされている場合でも、ユーザーはそのログイン情報を仮想 IP に送信します。

ローカル Web 認証を有効にすると、次のイベントが発生します。

- ユーザーが HTTP セッションを開始します。
- HTTP トラフィックが横取りされ、認証が開始されます。コントローラは、ユーザーにログインページを送信します。ユーザーはユーザー名とパスワードを入力します。コントローラはこのエントリを認証サーバーに送信します。
- 認証に成功した場合、コントローラは、認証サーバーからこのユーザーのアクセスポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザーに送信されます
- 認証に失敗した場合は、コントローラはログインの失敗ページを送信します。ユーザーはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、コントローラは、ログイン期限切れページを送信します。このホストはウォッチリストに入れられます。ウォッチ リストのタイム アウト後、ユーザーは認証プロセスを再試行することができます。

- 認証サーバーを利用できない場合、Web認証が再試行された後、クライアントは除外状態に移行し、クライアントに [Authentication Server is Unavailable] ページが表示されます。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドルタイムアウト内にトラフィックを送信しなかった場合、コントローラはクライアントを再認証します。
- クライアントにはすでに IP アドレスが割り当てられており、VLAN が変更された場合はクライアントの IP アドレスを変更できないため、Web 認証セッションは認証ポリシーの一部として新しい VLAN を適用できません。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザバナーを作成して、コントローラにログインしたときに表示されるようにできます。

このバナーは、ログインページと認証結果ポップアップページの両方に表示されます。デフォルトのバナー メッセージは次のとおりです。

- 認証成功
- 認証失敗
- 認証期限切れ

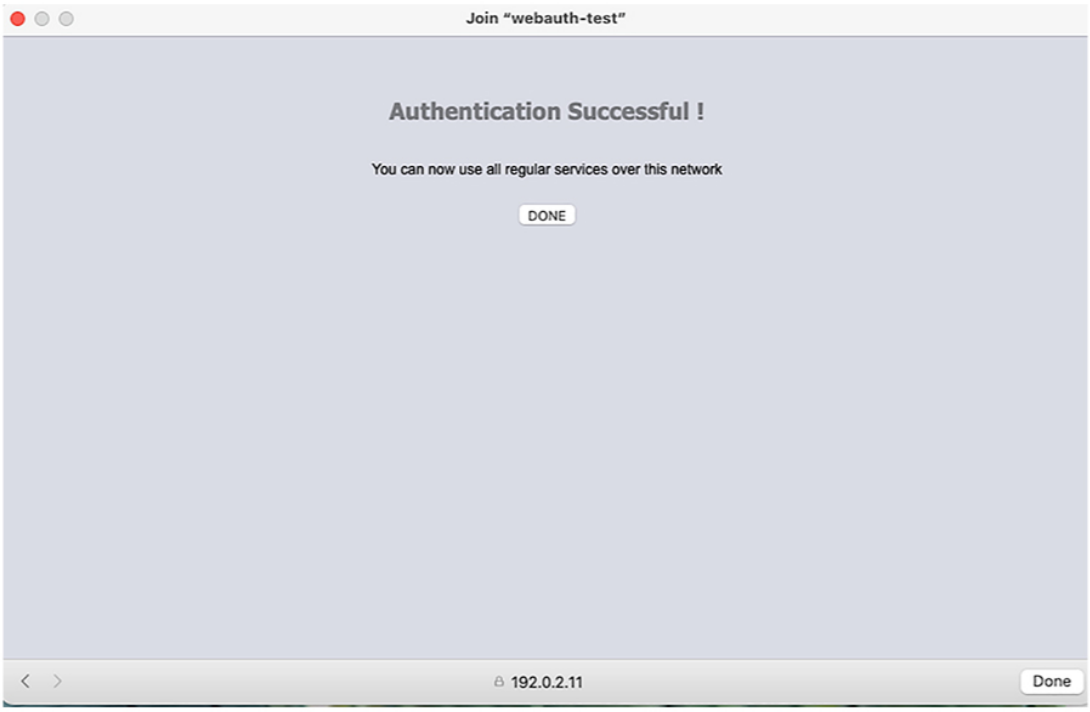
ローカル Web 認証バナーは、次のように設定できます。

- 次のグローバル コンフィギュレーション コマンドを使用します。

```
Device(config)# parameter map type webauth global
Device(config-params-parameter-map)# banner ?
file <file-name>
text <Banner text>
title <Banner title>
```

ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は認証結果ポップアップ ページに表示されます。

図 *17* : 認証成功バナー



バナーは次のようにカスタマイズ可能です。

- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
  - 新スタイルモード：次のグローバルコンフィギュレーションコマンドを使用します。

    parameter-map type webauth global

    banner text <text>

- ロゴまたはテキスト ファイルをバナーに追加する。
  - 新スタイルモード：次のグローバルコンフィギュレーションコマンドを使用します。

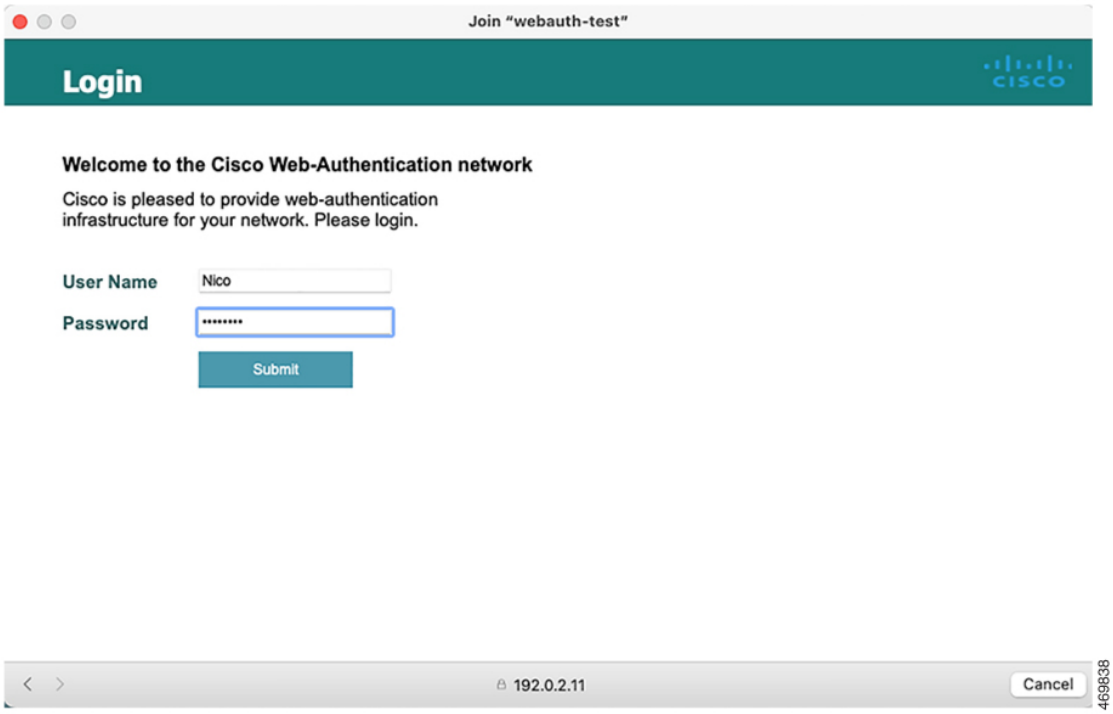
    parameter-map type webauth global

    banner file <filepath>

図 *18* : カスタマイズされた *Web* バナー

バナーが有効にされていない場合、Web認証ログイン画面にはユーザー名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 *19* : バナーが表示されていないログイン画面



カスタマイズされたローカル Web 認証

ローカル Web 認証プロセスでは、スイッチ内部の HTTP サーバーは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバーはこれらのページを使用して、ユーザーに次の 4 種類の認証プロセス ステートを通知します。

- ログイン：ログイン情報が要求されます
- 成功：ログインに成功しました
- 失敗：ログインに失敗しました
- 期限切れ：ログインの失敗回数が多すぎて、ログインセッションが期限切れになりました

（注） カスタム Web 認証を設定するには、仮想 IP アドレスが必要です。

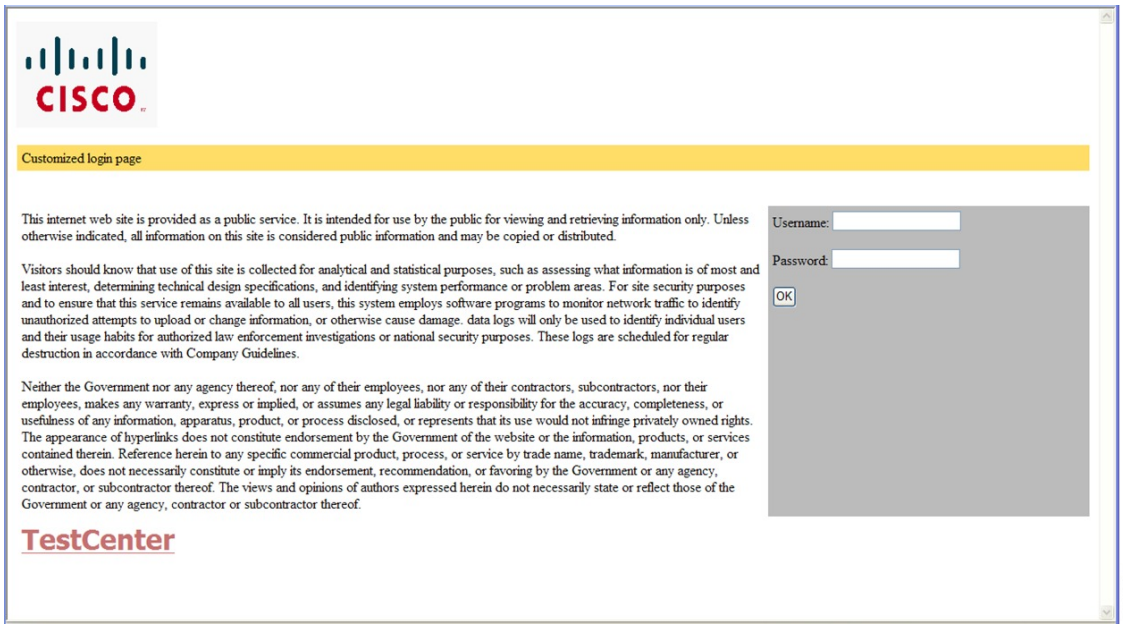
ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。

- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：http://www.cisco.com）でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイムアウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります. WebAuth バンドルのカスタムページのサンプルには、変更できるものと変更できないものに関する画像と詳細が含まれています。
- 設定されたログイン フォームが有効な場合、特定の URL にユーザーをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザーをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザーをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- ログインページを任意のフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、アクティブスイッチ、またはメンバスイッチのフラッシュ）に配置できます。
- 4 ページすべてを設定する必要があります。
- システムディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログインページに表示する必要のあるロゴファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、*web_auth_<filename>* の形式で名前を付けてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部 HTML ページの代わりに、自分の HTML ページを使用することができます。認証後のユーザーのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 *20 :* カスタマイズ可能な認証ページ



成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能が有効に設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。
- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL（たとえば http://）で開始し、その後に URL 情報が続く必要があります。http:// を含まない URL が指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。

ローカル Web 認証の設定方法

デフォルトのローカル Web 認証の設定

次の表に、ローカル Web 認証に必要なデフォルト設定を示します。

表 *23 :* デフォルトのローカル *Web* 認証の設定

機能	デフォルト設定
AAA	無効
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	• 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	ディセーブル

AAA 認証の設定（GUI）

（注） WebUI は、AAA RADIUS サーバーグループ設定における ipv6 radius source-interface をサポートしていません。

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。

ステップ 2 [Authentication] セクションで [Add] をクリックします。

ステップ 3 表示される [Quick Setup: AAA Authentication] ウィンドウに、メソッド リストの名前を入力します。

ステップ 4 ネットワークへのアクセスを許可する前に実行する認証のタイプを [Type] ドロップダウン リストから選択します。

ステップ 5 [Group Type] ドロップダウン リストから、サーバーのグループをアクセス サーバーとして割り当てるか、またはローカル サーバーを使用してアクセスを認証するかを選択します。

ステップ 6 グループ内のサーバーが使用できない場合にフォールバック方式として機能するようにローカル サーバーを設定するには、[Fallback to local] チェックボックスをオンにします。

ステップ 7 [Available Server Groups] リストで、ネットワークへのアクセスの認証に使用するサーバー グループを選択し、[>] アイコンをクリックして [Assigned Server Groups] リストに移動します。

ステップ 8 [Save & Apply to Device] をクリックします。

AAA 認証の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** 例： `デバイス(config)# aaa new-model`	AAA 機能をイネーブルにします。
ステップ 2	**aaa authentication login** {**default** | *named_authentication_list*} **group** *AAA_group_name* 例： `デバイス(config)# aaa authentication login default group group1`	ログイン時の認証方法のリストを定義します。 **named_authentication_list** は、31 文字未満の名前を示します。 **AAA_group_name** はサーバー グループ名を示します。サーバーグループ **server_name** をその先頭で定義する必要があります。
ステップ 3	**aaa authorization network** {**default** | **named**} **group** *AAA_group_name* 例： `デバイス(config)# aaa authorization network default group group1`	Web ベース許可の許可方式リストを作成します。
ステップ 4	**tacacs-server host** {*hostname* | *ip_address*} 例： `デバイス(config)# tacacs-server host 10.1.1.1`	AAA サーバーを指定します。

HTTP/HTTPS サーバーの設定（GUI）

手順

ステップ 1 **[Administration]** > **[Management]** > **[HTTP/HTTPS/Netconf]** の順に選択します。

ステップ 2 [HTTP/HTTPS Access Configuration] セクションで、[HTTP Access] を有効にして、HTTP 要求をリッスンするポートを入力します。デフォルトのポートは 80 です。有効な値は、80 または 1025 ～ 65535 の値です。

ステップ 3 デバイスで [HTTPS Access] を有効にし、HTTPS 要求をリッスンする指定ポートを入力します。デフォルトのポートは 1025 です。有効な値は、443 または 1025 ～ 65535 の値です。セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。

ステップ 4 [Personal Identity Verification] について [enabled] または [disabled] を選択します。

ステップ 5 [HTTP Trust Point Configuration] セクションで、[Enable Trust Point] を有効にして、認証局サーバーをトラストポイントとして使用します。

ステップ 6 [Trust Points] ドロップダウン リストから、トラスト ポイントを選択します。

ステップ 7 [Timeout Policy Configuration] セクションで、HTTP タイムアウト ポリシーを秒単位で入力します。有効な値の範囲は、10 ～ 600 秒です。

ステップ 8 セッションがタイムアウトするまでに許容される非アクティブな時間（分数）を入力します。有効な値の範囲は、180 ～ 1200 秒です。

ステップ 9 サーバーの有効期間を秒単位で入力します。有効値の範囲は、1 ～ 86400 秒です。

ステップ 10 デバイスが受け取ることのできる要求の最大数を入力します。有効値の範囲は、1 ～ 86400 件です。

ステップ 11 設定を保存します。

HTTP サーバーの設定（CLI）

ローカル Web 認証を使用するには、デバイス内で HTTP サーバーを有効にする必要があります。このサーバーは HTTP または HTTPS のいずれかについて有効にできます。

（注） Apple の疑似ブラウザは、**ip http secure-server** コマンドを設定するだけでは開きません。**ip http server** コマンドも設定する必要があります。

HTTP または HTTPS のいずれかについてサーバーを有効にするには、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	**ip http server** 例： `Device(config)# ip http server`	HTTP サーバーを有効にします。ローカル Web 認証機能は、HTTP サーバーを使用してホストと通信し、ユーザー認証を行います。
ステップ 3	**ip http secure-server** 例： `Device(config)# ip http secure-server`	HTTPS を有効にします。 カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。 （注） **ip http secure-server** コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザーが HTTP 要求を送信した場合でも、ログイン ページは必ず HTTPS（セキュア HTTP）形式になるようにします。
ステップ 4	**end** 例： `Device(config)# end`	設定モードを終了します。

パラメータマップの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Policy Map] をクリックします。

ステップ 4 [Parameter Name]、[Maximum HTTP connections]、[Init-State Timeout(secs)] を入力し、[Type] ドロップダウンリストで [webauth] を選択します。

ステップ 5 [Apply to Device] をクリックします。

Web 認証要求の最大再試行回数の設定

最大 Web 認証要求再試行回数を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# 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	**configure terminal** 例： `デバイス# 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 3	**wireless security web-auth retries** *number* 例： `デバイス(config)# wireless security web-auth retries 2`	*number* は Web 認証要求の最大試行回数です。有効な範囲は 0 ～ 20 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

Web 認証ページ内のローカル バナーの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [General] タブで、必要なバナー タイプを選択します。

- [Banner Text] を選択した場合は、表示するバナー テキストを入力します。
- [File Name] を選択した場合は、バナー テキストを取得する取得元のファイルのパスを指定します。

ステップ 4 [Update & Apply] をクリックします。

Web 認証ページ内のローカル バナーの設定（CLI）

Web 認証ページ内のローカル バナーを設定するには、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	**parameter-map type webauth** *param-map* 例： `Device(config)# parameter-map type webauth param-map`	Web 認証パラメータを設定します。パラメータ マップ 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	**banner** ［ *file* ｜*banner-text* ｜*title*］ 例： `Device(config-params-parameter-map)# banner http C My Switch C`	ローカル バナーを有効にします。 C banner-text C（C は区切り文字）、バナーに表示されるファイル（ロゴやテキストファイル）の file、またはバナーのタイトルを示す title を入力して、カスタムバナーを作成します。
ステップ 4	**end** 例： `Device(config-params-parameter-map)# end`	特権 EXEC モードに戻ります。

ローカル Web 認証の設定例

例：Web 認証証明書の入手

次の例は、Web 認証証明書を取得する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco

デバイス(config)# end
デバイス# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
デバイス# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
```

```
    c=US
  Validity Date:
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

例：Web 認証証明書の表示

次の例は、Web 認証証明書を表示する方法を示しています。

```
デバイス# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
    Subject:
    Name: WS-C3780-6DS-S-2037064C0E80
    Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
    cn=WS-C3780-6DS-S-2037064C0E80
    serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
    CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/cmca.crl
    Validity Date:
    start date: 15:43:22 UTC Aug 21 2011
    end   date: 15:53:22 UTC Aug 21 2021
    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
    Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
    X509v3 extensions:
    X509v3 Key Usage: F0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
      Data Encipherment
    X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
    X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
    Authority Info Access:
    Associated Trustpoints: CISCO_IDEVID_SUDI
    Key Label: CISCO_IDEVID_SUDI
```

例：デフォルトの Web 認証ログイン ページの選択

次の例は、デフォルトの Web 認証ログイン ページを選択する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their
CPL control-policy equivalents. As this conversion is irreversible and will
```

```
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
 advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
デバイス(config)# wlan wlan50
デバイス(config-wlan)# shutdown
デバイス(config-wlan)# security web-auth authentication-list test
デバイス(config-wlan)# security web-auth parameter-map test
デバイス(config-wlan)# no shutdown
デバイス(config-wlan)# end
デバイス# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

デバイス# show running-config | section parameter-map type webauth test
parameter-map type webauth test
 type webauth
```

例：IPv4 外部 Web サーバーでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、IPv4 外部 Web サーバーからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# parameter-map type webauth global
デバイス(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
デバイス(config-params-parameter-map)# parameter-map type webauth test
デバイス(config-params-parameter-map)# type webauth
デバイス(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
デバイス(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：IPv6 外部 Web サーバーでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、IPv6 外部 Web サーバーからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# parameter-map type webauth global
デバイス(config-params-parameter-map)# virtual-ip ipv6 1:1:1::1
デバイス(config-params-parameter-map)# parameter-map type webauth test
デバイス(config-params-parameter-map)# type webauth
デバイス(config-params-parameter-map)# redirect for-login http://9:1:1::100/login.html
デバイス(config-params-parameter-map)# redirect portal ipv6 9:1:1::100
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv6 1:1:1::1
parameter-map type webauth test
type webauth
redirect for-login http://9:1:1::100/login.html
redirect portal ipv6 9:1:1::100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

次の例は、WLAN ごとのログイン割り当て、ログイン失敗、およびログアウト ページを割り当てる方法を示しています。

```
デバイス# configure terminal
デバイス(config)# parameter-map type webauth test
デバイス(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
デバイス(config-params-parameter-map)# custom-page login expired device
flash:loginexpire.html
デバイス(config-params-parameter-map)# custom-page failure device flash:loginfail.html
デバイス(config-params-parameter-map)# custom-page success device flash:loginsucess.html
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

例：事前認証 ACL の設定

次の例は、事前認証 ACL を設定する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# wlan fff
デバイス(config-wlan)# shutdown
デバイス(config-wlan)# ip access-group web preauthrule
デバイス(config-wlan)# no shutdown
デバイス(config-wlan)# end
デバイス# show wlan name fff
```

例：Webpassthrough の設定

次の例は、Webpassthrough を設定する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# parameter-map type webauth webparalocal
デバイス(config-params-parameter-map)# type consent
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
```

Web 認証タイプの確認

Web 認証タイプを確認するには、次のコマンドを実行します。

```
Device# show parameter-map type webauth all
Type Name
---------------------------------
Global global
Named webauth
Named ext
Named redirect
Named abc
Named glbal
Named ewa-2

Device# show parameter-map type webauth global
Parameter Map Name : global
Banner:
Text : CisCo
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Enabled
Sleeping-Client timeout : 60 min
Virtual-ipv4 : 1.1.1.1
Virtual-ipv4 hostname :
```

```
Webauth intercept https : Disabled
Webauth Captive Bypass : Disabled
Webauth bypass intercept ACL :
Trustpoint name :
HTTP Port : 80
Watch-list:
Enabled : no
Webauth login-auth-bypass:

Device# show parameter-map type webauth name global
Parameter Map Name : global
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Disabled
Webauth login-auth-bypass:
```

スリープ状態にあるクライアントの認証

スリープ状態にあるクライアントの認証について

Web 認証に成功したゲスト アクセスを持つクライアントは、ログイン ページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効範囲は 10 ～ 43200 分、デフォルトは 720 分です。この期間は、WLAN にマッピングされている WebAuth パラメータマップでも設定できます。スリープ状態にあるクライアントのタイマーは、アイドルタイムアウト、セッションタイムアウト、WLAN の無効化、AP の停止などのインスタンスが原因で有効になることに注意してください。

この機能は FlexConnect のローカル スイッチング、中央認証のシナリオでサポートされています。

⚠

注意 スリープ モードに切り替わったクライアント MAC アドレスがスプーフィングされた場合、ラップトップなどの偽のデバイスを認証することができます。

モビリティのシナリオ

次に、モビリティ シナリオでの注意事項を示します。

- 同じサブネットの L2 ローミングがサポートされています。
- アンカー スリープ タイマーを適用できます。
- スリープ状態にあるクライアントの情報は、クライアントがアンカー間を移動する場合に、複数の自動アンカー間で共有されます。

スリープ状態にあるクライアントは、次のシナリオでは再認証が必要ありません。

- モビリティグループに2台の 組み込みワイヤレスコントローラがあるとします。1台の 組み込みワイヤレスコントローラに関連付けられているクライアントがスリープ状態になり、その後復帰して他方の 組み込みワイヤレスコントローラに関連付けられます。
- モビリティグループに3台の 組み込みワイヤレスコントローラがあるとします。1台目の組み込みワイヤレスコントローラにアンカーされた2台目のコントローラに関連付けられたクライアントは、スリープ状態から復帰して、3台目の 組み込みワイヤレスコントローラに関連付けられます。
- クライアントはスリープ状態から復帰して、エクスポートアンカーにアンカーされた同じまたは別のエクスポート外部 組み込みワイヤレスコントローラに関連付けられます。

スリープ状態にあるクライアントの認証に関する制約事項

- スリープ クライアント機能は、WebAuth セキュリティが設定された WLAN に対してのみ動作します。
- スリープ状態にあるクライアントはWebAuthパラメータマップごとにのみ設定できます。
- スリープ状態にあるクライアントの認証機能は、レイヤ 3 セキュリティが有効な WLAN でのみサポートされています。
- レイヤ 3 セキュリティでは、認証、パススルー、および On MAC Filter 失敗 Web ポリシーがサポートされています。条件付き Web リダイレクトとスプラッシュ ページ Web リダイレクト Web ポリシーはサポートされていません。
- スリープ状態にあるクライアントの中央 Web 認証はサポートされていません。
- スリープ状態にあるクライアントの認証機能は、ゲスト LAN およびリモート LAN ではサポートされていません。
- ローカル ユーザー ポリシーを持つスリープ状態のゲスト アクセス クライアントはサポートされません。この場合、WLAN 固有のタイマーが適用されます。

スリープ状態のクライアントの認証の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [Sleeping Client Status] チェックボックスをオンにします。

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

スリープ状態のクライアントの認証の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} 例： `Device(config)# parameter-map type webauth global`	パラメータ マップを作成し、parameter-map webauth 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	**sleeping-client** [**timeout** *time*] 例： `Device(config-params-parameter-map)# sleeping-client timeout 100`	スリープ状態のクライアントのタイムアウトを 100 分に設定します。有効な範囲は 10 ～ 43200 分です。 （注） タイムアウト キーワードを使用しない場合、スリープ状態のクライアントにはデフォルトのタイムアウト値である 720 分が設定されます。
ステップ 3	**end**	parameter-map webauth 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 4	（任意） **show wireless client sleeping-client** 例： `Device# show wireless client sleeping-client`	クライアントのMACアドレスと、それぞれのセッションの残り時間を表示します。
ステップ 5	（任意） **clear wireless client sleeping-client** [**mac-address** *mac-addr*] 例： `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**：スリープ状態のクライアントキャッシュからスリープ状態のクライアント エントリをすべて削除します。 • **clear wireless client sleeping-client mac-address** *mac-addr*：スリープ状態のクライアント キャッシュから特定の MAC エントリを削除します。

第 45 章

中央 Web 認証

中央 Web 認証について

中央 Web 認証では、Web ポータルとして機能する中央デバイス（この例では ISE）を配置することができます。通常のローカル Web 認証と比較した場合の主な相違点は、MAC フィルタリングまたは dot1x 認証に伴ってレイヤ 2 にシフトされることです。また、RADIUS サーバー（この例では ISE）が、スイッチに対して Web リダイレクションの必要性を指示する特別な属性を返す点も異なります。このソリューションにより、Web 認証を開始する際の遅延が解消されます。

次に、さまざまなタイプの Web 認証方式を示します。

- ローカル Web 認証（LWA）：コントローラ上のレイヤ 3 セキュリティとして設定され、Web 認証ページと事前認証 ACL はコントローラでローカルに設定されます。コントローラは、htttp(s) トラフィックを代行受信し、認証のためにクライアントを内部 Web ページにリダイレクトします。ログインページでクライアントが入力したログイン情報は、コントローラによってローカルに認証されるか、RADIUS サーバーまたは LDAP サーバーを介して認証されます。

- 外部 Web 認証（EWA）：コントローラ上のレイヤ 3 セキュリティとして設定され、コントローラは htttp(s) トラフィックを代行受信し、外部 Web サーバーでホストされているログインページにクライアントをリダイレクトします。ログインページでクライアントが入力したログイン情報は、コントローラによってローカルに認証されるか、RADIUS サーバーまたは LDAP サーバーを介して認証されます。事前認証 ACL は、コントローラで静的に設定されます。

- 中央 Web 認証（CWA）：主にコントローラ上のレイヤ 2 セキュリティとして設定され、リダイレクト URL と事前認証 ACL は ISE 上に存在し、レイヤ 2 認証時にコントローラにプッシュされます。コントローラは、クライアントからのすべての Web トラフィックを

ISE ログインページにリダイレクトします。ISE は、HTTPS を介してクライアントによって入力されたログイン情報を検証し、ユーザーを認証します。

クライアントステーションの MAC アドレスがグローバルに RADIUS サーバーに知られていない場合（ただし他の基準を使用することも可能）、サーバーはリダイレクション属性を返し、組み込みワイヤレスコントローラは（MAC フィルタリングを使用して）ステーションを認可しますが、Web トラフィックをポータルへリダイレクトするためのアクセスリストを配置します。

ユーザがゲスト ポータルへログインすると、クライアントの再認証が可能になり、認可変更（CoA）を使用する新しいレイヤ 2 MAC フィルタリングが行われます。これにより、ISE が Web 認証ユーザーだったことが ISE によって記憶され、ISE は、ネットワークにアクセスするために必要な許可属性を 組み込みワイヤレスコントローラにプッシュします。

中央 Web 認証の前提条件

- Cisco Identity Services Engine（ISE）

ISE の設定方法

ISE を設定するには、次の手順に従います。

1. 認可プロファイルを作成します。
2. 認証ルールを作成します。
3. 認可ルールを作成します。

認可プロファイルの作成

手順

ステップ 1 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 2 [Results] をクリックします。

ステップ 3 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 4 [Add] をクリックして、中央 Web 認証用の新しい認可プロファイルを作成します。

ステップ 5 [Name] フィールドに、プロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 6 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

ステップ 7 [Web Redirection (CWA, MDM, NSP, CPP)] チェックボックスをオンにし、ドロップダウン リストから [Centralized Web Auth] を選択します。

ステップ 8 [ACL] フィールドに、リダイレクトするトラフィックを定義する ACL の名前を入力します。たとえば、「redirect」などと入力します。

ステップ 9 [Value] フィールドで、デフォルト値またはカスタマイズされた値を選択します。

[Value] 属性は、ISE がデフォルトの Web ポータルを参照するか、または ISE 管理者が作成したカスタム Web ポータルを参照するかを定義します。

ステップ 10 [Save] をクリックします。

認証ルールの作成

認証プロファイルを使用して認証ルールを作成するには、次の手順に従います。

手順

ステップ 1 **[Policy]** > **[Authentication]** ページで、[Authentication] をクリックします。

ステップ 2 認証ルールの名前を入力します。たとえば、「MAB」と入力します。

ステップ 3 [If] 条件フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 4 [Compound condition] を選択し、[Wireless_MAB] を選択します

ステップ 5 [and ...] の横にある矢印をクリックして、ルールをさらに展開します。

ステップ 6 [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します。

ステップ 7 [If user not found] ドロップダウン リストから [Continue] を選択します。

このオプションを使用すると、MAC アドレスが不明な場合でもデバイスを認証できます。

ステップ 8 [Save] をクリックします。

認可ルールの作成

認可ポリシーでは多数のルールを設定できます。このセクションでは [MAC not known] ルールが設定されています。

手順

ステップ 1 [Policy] > [Authorization] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。たとえば、「Mac not known」などと入力します。

ステップ 3 [Conditions] フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 4 [Compound Conditions] を選択し、[Wireless_MAB] を選択します

ステップ 5 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

ステップ 6 [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [AuthenticationStatus] を選択します。

ステップ 7 [Equals] 演算子を選択します。

ステップ 8 右側のフィールドから、[UnknownUser] を選択します。

ステップ 9 [Permissions] フィールドで、以前に作成した認可プロファイル名を選択します。

ISE は、ユーザー（または MAC）が不明の場合でも続行されます。

これで、不明なユーザーにログイン ページが表示されるようになりました。ただし、ユーザーが自分のログイン情報を入力すると、再び ISE の認証要求が表示されます。そのため、ユーザーがゲスト ユーザーである場合に満たされる条件で別のルールを設定する必要があります。たとえば、「UseridentityGroup Equals Guest」を使用している場合に、すべてのゲストがこのグループに属すると仮定します。

ステップ 10 [Conditions] フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 11 [Compound Conditions] を選択し、新しい条件の作成を選択します。

新しいルールは「MAC not known」ルールの前に置く必要があります。

ステップ 12 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

ステップ 13 [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [UseCase] を選択します。

ステップ 14 [Equals] 演算子を選択します。

ステップ 15 右側のフィールドから、[GuestFlow] を選択します。

ステップ 16 [Permissions] フィールドで、プラス（[+]）アイコンを選択してルールの結果を選択します。

[Standard] > [PermitAccess] オプションを選択するか、または必要な属性を返すカスタム プロファイルを作成できます。

ユーザがログイン ページで承認されると、レイヤ 2 認証の再起動の結果として、ISE により COA がトリガーされます。ユーザーがゲスト ユーザーとして識別されると、ユーザーが承認されます。

コントローラでの中央 Web 認証の設定方法

コントローラで中央 Web 認証を設定するには、次の手順に従います。

1. WLAN を設定します。
2. ポリシー プロファイルを設定します。
3. リダイレクト ACL を設定します。
4. 中央 Web 認証用の AAA を設定します。

5. Flex プロファイルでリダイレクト ACL を設定します。

WLAN の設定（GUI）

始める前に

リダイレクト URL と ACL をダウンロードするには、レイヤ 2 認証の MAC フィルタリングを有効にする必要があります。

手順

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

ステップ 2 [WLANs] ウィンドウで、WLAN 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 WLAN] ウィンドウで、[General] タブをクリックして次のパラメータを設定します。

- [Profile Name]フィールドで、プロファイルの名前を入力または編集します。
- [SSID] フィールドで、SSID 名を入力または編集します。

  SSID 名には、最大 32 文字の英数字を使用できます。
- [WLAN ID] フィールドで、ID 番号を入力または編集します。有効な範囲は 1 ～ 512 です。
- [Radio Policy] ドロップダウンリストから、[802.11] 無線帯域を選択します。
- [Broadcast SSID] トグルボタンを使用して、ステータスを [Enabled] または [Disabled] に変更します。
- [Status] トグルボタンを使用して、ステータスを [Enabled] または [Disabled] に変更します。

ステップ 4 [Security] タブ、[Layer 2] タブの順にクリックして、次のパラメータを設定します。

- [Layer 2 Security Mode] ドロップダウンリストから、[None] を選択します。この設定により、レイヤ 2 セキュリティが無効になります。
- [Reassociation Timeout] の値（秒単位）を入力します。これは、高速移行の再アソシエーションがタイムアウトするまでの時間です。
- 分散システム経由の高速移行を有効にするには、[Over the DS] チェック ボックスをオンにします。
- OWE を選択すると、Opportunistic Wireless Encryption（OWE）によって、AP 無線とワイヤレスクライアント間の無線暗号化によるデータの機密性が提供されます。OWE 移行モードは、一種の下位互換性を提供することを目的としています。
- 高速移行を選択すると、高速ローミングの IEEE 標準である 802.11r によって、対応するクライアントがターゲットアクセスポイントにローミングする前でも、新しい AP との最初

のハンドシェイクが実行されるローミングの新しい概念が導入されます。この概念は高速移行と呼ばれます。

- WLAN で MAC フィルタリングを有効にするには、チェックボックスをオンにします。

ステップ 5 [Save & Apply to Device] をクリックします。

WLAN の設定（CLI）

（注） リダイレクト URL と ACL をダウンロードするには、レイヤ 2 認証の MAC フィルタリングを有効にする必要があります。

WLAN の設定を完了後、変更がすべての AP にプッシュされていない場合、次の Syslog メッセージが表示されます。

2021/01/06 16:20:00.597927186 {wncd_x_R0-4}{1}: [wlanmgr-db] [20583]: UUID: 0, ra: 0, TID: 0 (note): Unable to push WLAN config changes to all APs, cleanup required for WlanId: 2, profile: wlan1 state: Delete pending

前述の Syslog メッセージが 6 分以上表示される場合は、コントローラをリロードします。

コントローラがリロードせず、まだSyslogメッセージが表示されている場合は、アーカイブログ、wncd コアファイルを収集し、リンク（Support Case Manager）をクリックしてケースを提起します。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan wlan-name wlan-id SSID-name** **例：** `Device(config)# wlan wlanProfileName 1 ngwcSSID`	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** は、設定されている WLAN の名前です。 **wlan-id** はワイヤレス LAN の ID です。指定できる範囲は 1 ～ 512 です。 **SSID-name** は、最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンドを設定している場合は、**wlan wlan-name** コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 2	**mac-filtering** [*name*] 例： `Device(config-wlan)# mac-filtering name`	WLAN での MAC フィルタリングを有効にします。 （注） 認証リストを事前に設定していない場合は、MAC フィルタリングの設定時にデフォルトの認証リストが仮定されます。
ステップ 3	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 4	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 5	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。

例

```
Device# config terminal
Device(config)# wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)# mac-filtering default
Device(config-wlan)# no security wpa
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

ポリシー プロファイルの設定（CLI）

（注） AAA または ISE サーバーからのポリシーを適用するには、AAA オーバーライドが必要です。リダイレクト URL とリダイレクト ACL を ISE サーバーから受信すると、NAC を使用して中央 Web 認証（CWA）がトリガーされます。

クライアントが関連付けられるポリシープロファイルで、NAC と AAA オーバーライドの両方が使用可能である必要があります。

AP が他のどのポリシープロファイルにも関連付けられていない場合、デフォルトポリシープロファイルが AP に関連付けられます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless profile policy default-policy-profile** 例： `Device(config)# wireless profile policy default-policy-profile`	ポリシープロファイルを設定します。
ステップ 2	**vlan vlan-id** 例： `Device(config-wireless-policy)# vlan 41`	VLANをポリシープロファイルにマッピングします。vlan-id を指定しない場合は、デフォルトのネイティブの vlan 1 が適用されます。vlan-id の有効な範囲は 1 ～ 4096 です。 ポリシープロファイルに VLAN が設定されていない場合、管理 VLAN が適用されます。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバーまたは ISE サーバーから受信したポリシーを適用するようにAAAオーバーライドを設定します。
ステップ 4	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシープロファイルでネットワークアクセス コントロールを設定します。NAC は、中央 Web 認証（CWA）をトリガーするために使用されます。
ステップ 5	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	WLAN をイネーブルにします。
ステップ 6	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。

例

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# vlan 41
Device(config-wireless-policy)# aaa-override
Device(config-wireless-policy)# nac
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```

ポリシー プロファイルの設定（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 （任意） [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]： 組み込みワイヤレス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。

- [Central Switching]
- [Central Authentication]
- 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。

リダイレクト ACL の作成

リダイレクト ACL は、コントローラ（または FlexConnect ローカルスイッチングの場合は AP）で事前定義する必要があるパント ACL です。AAA サーバーは、定義ではなく ACL の名前を返します。リダイレクト ACL は、データプレーンの通過を許可されるトラフィック（リダイレクトを拒否する「拒否」ステートメントに一致）と、さらなる処理（この場合は Web インターセプトとリダイレクト）のためにコントロールプレーンに送信されて CPU に向かうトラフィック（「許可」ステートメントに一致）を定義します。ACL には、LWA の場合と同様に、すべての IP への DHCP および DNS トラフィックを許可する暗黙の（つまり、隠れた）ステートメントがあります。また、セキュリティ ACL が暗黙的に拒否するというステートメントで終わります。

手順

	コマンドまたはアクション	目的
ステップ 1	**ip access-list extended redirect** 例： `Device(config)# ip access-list extended redirect`	ISE がリダイレクト ACL（**redirect** という名前）を使用するように設定されているため、HTTP および HTTPS ブラウジングは（他の ACL ごとの）認証なしでは機能しません。
ステップ 2	**deny ip any host ISE-IP-add** 例： `Device(config)# deny ip any host 123.123.134.112`	ISE へのトラフィックを許可し、その他のすべてのトラフィックをブロックします。
ステップ 3	**deny ip host ISE-IP-add any** 例： `Device(config)# deny ip host 123.123.134.112 any`	ISE へのトラフィックを許可し、その他のすべてのトラフィックをブロックします。 （注） このACLは、ローカルモードと flex モードの両方に適用できます。

ステップ 4	**permit TCP any any eq web address/port-number**
	例：
	HTTP の場合：
	`Device(config)# permit TCP any any eq www`
	`Device(config)# permit TCP any any eq 80`
	例：
	HTTPS の場合：
	`Device(config)# permit TCP any any eq 443`
		ISE ログイン ページへのすべての HTTP または HTTPS アクセスをリダイレクトします。HTTP ではポート番号 80 が使用され、HTTPS では ポート番号 443 が使用されます。
		ACE が ISE へのトラフィックを許可するには、ISE を HTTP/HTTPS ACE の上に設定する必要があります。

ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

中央 Web 認証用の AAA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	組み込みワイヤレスコントローラの認可変更（CoA）を設定します。
ステップ 2	**client ISE-IP-add server-key radius-shared-secret** 例： `Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET`	RADIUS クライアントと RADIUS キーがデバイスと RADIUS クライアントの間で共有されるように指定します。 **ISE-IP-add** は RADIUS クライアントの IP アドレスです。 **server-key** は RADIUS クライアントのサーバーキーです。 radius-shared-secret の内容は以下のとおりです。 • **0**：暗号化されていないキーを指定します。 • **6**：暗号化されたキーを指定します。 • **7**：「隠し」キーを指定します。 • **Word**：暗号化されていない（クリアテキスト）サーバー キー。 GUI で WSMA データを設定する場合、RADIUS 共有秘密は 240 文字を超えることはできません。 （注） これらのステップはすべて、AAA が設定されている場合にのみ機能します。詳細については、「AAA 認証の設定」を参照してください。

例

```
Device# config terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET
Device(config-locsvr-da-radius)# end
```

Flex プロファイルでのリダイレクト ACL の設定（GUI）

リダイレクト ACL の定義を FlexConnect プロファイル内のアクセス ポイントに送信する必要があります。それには、AP に関連付けられているリダイレクト ACL を、クライアントがホストされている FlexConnect プロファイルに設定する必要があります。アクセス ポイントがどの FlexConnect プロファイルでも設定されていない場合は、デフォルトの FlexConnect プロファイルが関連付けられます。

手順

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

ステップ 2 [Flex Profile] ページで、 FlexConnect プロファイルの名前をクリックするか、[Add] をクリックして新しい FlexConnect プロファイルを作成します。

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

ステップ 4 [Add] をクリックして、ACL を FlexConnect プロファイルにマッピングします。

ステップ 5 ACL 名を選択し、中央 Web 認証を有効にして、認証 URL フィルタを指定します。

ステップ 6 [Save] をクリックします。

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

Flex プロファイルでのリダイレクト ACL の設定（CLI）

リダイレクト ACL の定義を Flex プロファイル内のアクセス ポイントに送信する必要があります。それには、AP に関連付けられているリダイレクト ACL を、クライアントがホストされている Flex プロファイルに設定する必要があります。アクセス ポイントがどの Flex プロファイルでも設定されていない場合は、デフォルトの Flex プロファイルが関連付けられます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless profile flex default-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。デフォルトの flex プロファイル名は **default-flex-profile** です。

	コマンドまたはアクション	目的
ステップ 2	**acl-policy** *acl policy name* 例： `Device(config-wireless-flex-profile)# acl-policy acl1`	ACL ポリシーを設定します。
ステップ 3	**central-webauth** 例： `Device(config-wireless-flex-profile-acl)# central-webauth`	中央 Web 認証を設定します。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile-acl)# end`	特権 EXEC モードに戻ります。

スリープ状態にあるクライアントの認証

スリープ状態にあるクライアントの認証について

Web 認証に成功したゲスト アクセスを持つクライアントは、ログイン ページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効範囲は 10 ～ 43200 分、デフォルトは 720 分です。この期間は、WLAN にマッピングされている WebAuth パラメータマップでも設定できます。スリープ状態にあるクライアントのタイマーは、アイドルタイムアウト、セッションタイムアウト、WLAN の無効化、AP の停止などのインスタンスが原因で有効になることに注意してください。

この機能は FlexConnect のローカル スイッチング、中央認証のシナリオでサポートされています。

⚠

注意 スリープ モードに切り替わったクライアント MAC アドレスがスプーフィングされた場合、ラップトップなどの偽のデバイスを認証することができます。

モビリティのシナリオ

次に、モビリティ シナリオでの注意事項を示します。

- 同じサブネットの L2 ローミングがサポートされています。
- アンカー スリープ タイマーを適用できます。

- スリープ状態にあるクライアントの情報は、クライアントがアンカー間を移動する場合に、複数の自動アンカー間で共有されます。

スリープ状態にあるクライアントは、次のシナリオでは再認証が必要ありません。

- モビリティグループに2台の 組み込みワイヤレスコントローラがあるとします。1台の 組み込みワイヤレスコントローラに関連付けられているクライアントがスリープ状態になり、その後復帰して他方の 組み込みワイヤレスコントローラに関連付けられます。
- モビリティグループに3台の 組み込みワイヤレスコントローラがあるとします。1台目の組み込みワイヤレスコントローラにアンカーされた2台目のコントローラに関連付けられたクライアントは、スリープ状態から復帰して、3台目の組み込みワイヤレスコントローラに関連付けられます。
- クライアントはスリープ状態から復帰して、エクスポートアンカーにアンカーされた同じまたは別のエクスポート外部 組み込みワイヤレスコントローラに関連付けられます。

スリープ状態にあるクライアントの認証に関する制約事項

- スリープ クライアント機能は、WebAuth セキュリティが設定された WLAN に対してのみ動作します。
- スリープ状態にあるクライアントはWebAuthパラメータマップごとにのみ設定できます。
- スリープ状態にあるクライアントの認証機能は、レイヤ 3 セキュリティが有効な WLAN でのみサポートされています。
- レイヤ 3 セキュリティでは、認証、パススルー、および On MAC Filter 失敗 Web ポリシーがサポートされています。条件付き Web リダイレクトとスプラッシュ ページ Web リダイレクト Web ポリシーはサポートされていません。
- スリープ状態にあるクライアントの中央 Web 認証はサポートされていません。
- スリープ状態にあるクライアントの認証機能は、ゲスト LAN およびリモート LAN ではサポートされていません。
- ローカル ユーザー ポリシーを持つスリープ状態のゲスト アクセス クライアントはサポートされません。この場合、WLAN 固有のタイマーが適用されます。

スリープ状態のクライアントの認証の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [Sleeping Client Status] チェックボックスをオンにします。

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

スリープ状態のクライアントの認証の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} 例： `Device(config)# parameter-map type webauth global`	パラメータ マップを作成し、parameter-map webauth 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	**sleeping-client** [**timeout** *time*] 例： `Device(config-params-parameter-map)# sleeping-client timeout 100`	スリープ状態のクライアントのタイムアウトを100分に設定します。有効な範囲は 10 ～ 43200 分です。 （注） タイムアウト キーワードを使用しない場合、スリープ状態のクライアントにはデフォルトのタイムアウト値である 720 分が設定されます。
ステップ 3	**end**	parameter-map webauth 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 4	（任意） **show wireless client sleeping-client** 例： `Device# show wireless client sleeping-client`	クライアントのMACアドレスと、それぞれのセッションの残り時間を表示します。
ステップ 5	（任意） **clear wireless client sleeping-client** [**mac-address** *mac-addr*] 例： `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**：スリープ状態のクライアントキャッシュからスリープ状態のクライアント エントリをすべて削除します。 • **clear wireless client sleeping-client mac-address** *mac-addr*：スリープ状態のクライアント キャッシュから

	コマンドまたはアクション	目的
		特定の MAC エントリを削除します。

第 46 章

ISE の簡素化と拡張

セキュリティ設定用のユーティリティ

この章では、次のコマンドを使用してすべての RADIUS サーバー側設定を行う方法について説明します。

wireless-default radius server *ip* **key** *secret*

この簡易設定オプションは次の機能を提供します。

- ネットワークサービスの AAA 認証、Web 認証および Dot1x の認証を設定します。
- デフォルトの認証を使用してローカル認証を有効にします。
- CWA のデフォルトのリダイレクト ACL を設定します。
- 仮想 IP でグローバルパラメータマップを作成し、キャプティブ バイパス ポータルを有効にします。
- RADIUS サーバーの設定時に、デフォルト ケースのすべての AAA 設定を行います。
- WLAN では、メソッドリストの設定がデフォルトで仮定されます。
- デフォルトで RADIUS アカウンティングを有効にします。
- デフォルトで RADIUS アグレッシブ フェールオーバーを無効にします。
- RADIUS 要求のタイムアウトをデフォルトで 5 秒に設定します。
- キャプティブ バイパス ポータルを有効にします。

このコマンドは、次の設定をバックグラウンドで行います。

```
aaa new-model
aaa authentication webauth default group radius
```

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
!
aaa server radius dynamic-author
 client <IP> server-key cisco123
!
radius server RAD_SRV_DEF_<IP>
 description Configured by wireless-default
 address ipv4 <IP> auth-port 1812 acct-port 1813
 key <key>
!
aaa local authentication default authorization default
aaa session-id common
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <IP>
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

このため、設定ガイドの内容をすべて調べなくても、簡易な設定要件を満たすようにワイヤレス 組み込みワイヤレスコントローラを設定することができます。

複数の RADIUS サーバーの設定

RADIUS サーバーを設定するには、次の手順を実行します。

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	**wireless-default radius server** *ip* **key** *secret* 例： `Device(config)# wireless-default radius server 9.2.58.90 key cisco123`	RADIUS サーバーを設定します。 （注） 最大 10 個の RADIUS サーバーを設定できます。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： デバイス(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。

AAA および RADIUS サーバーの設定の確認

AAA サーバーの詳細を表示するには、次のコマンドを使用します。

```
Device# show run aaa
!
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting Identity default start-stop group radius
!
aaa server radius dynamic-author
 client 9.2.58.90 server-key cisco123
!
radius server RAD_SRV_DEF_9.2.58.90
 description Configured by wireless-default
 address ipv4 9.2.58.90 auth-port 1812 acct-port 1813
 key cisco123
!
aaa local authentication default authorization default
aaa session-id common
!
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host 9.2.58.90
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

（注） このユーティリティに新しいコマンドを追加すると **show run aaa** の出力が変わる場合があります。

ローカルおよび中央 Web 認証のキャプティブ ポータル バイパスの設定

キャプティブ バイパスについて

WISPr は、ユーザーが異なるワイヤレス サービス プロバイダ間をローミングできるようにするドラフト プロトコルです。一部のデバイス（Apple iOS デバイスなど）には、指定の URL に対する HTTP WISPr 要求に基づいて、デバイスがインターネットに接続するかどうかを決定するときに使用するメカニズムが搭載されています。このメカニズムは、インターネットへの直接接続が不可能なときにデバイスが自動的に Web ブラウザを開くために使用されます。これにより、ユーザーがインターネットにアクセスするために、自身の認証情報を提供することが可能となります。実際の認証は、デバイスが新しい SSID に接続するたびにバックグラウンドで実行されます。

クライアントデバイス（Apple iOS デバイス）は、WISPr 要求を組み込みワイヤレスコントローラに送信します。コントローラはユーザーエージェントの詳細をチェックし、組み込みワイヤレスコントローラでの Web 認証代行受信により HTTP リクエストをトリガーします。ユーザーエージェントによって提供される iOS バージョンおよびブラウザの詳細の確認後、クライアントは、組み込みワイヤレスコントローラによってキャプティブポータル設定のバイパスを許可され、インターネットにアクセスできます。

この HTTP 要求は、他のページ要求がワイヤレスクライアントによって実行されると、組み込みワイヤレスコントローラでの Web 認証代行受信をトリガーします。この代行受信によって Web 認証プロセスが発生し、プロセスは正常に完了します。Web 認証がいずれかの 組み込みワイヤレスコントローラ スプラッシュページ機能で使用されている場合（設定された RADIUS サーバーが URL を指定）、WISPr 要求が非常に短い間隔で発信されるため、スプラッシュページは表示されず、いずれかのクエリが指定のサーバーに到達可能になるとただちに、バックグラウンドで実行されている Web リダイレクションまたはスプラッシュページ表示プロセスがキャンセルされます。そして、デバイスによってページ要求が処理され、スプラッシュページ機能は中断されます。

たとえば、Apple は iOS 機能を導入して、キャプティブ ポータルがある場合のネットワーク アクセスを容易にしました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を送信することにより、キャプティブ ポータルの存在を検出します。この要求は、Apple iOS バージョン 6 以前の場合は http://www.apple.com/library/test/success.html に、Apple iOS バージョン 7 以降の場合は複数の該当するターゲット URL に送信されます。応答が受信されると、インターネット アクセスが使用可能であると見なされ、それ以上の操作は必要ありません。応答が受信されない場合、インターネット アクセスはキャプティブ ポータルによってブロックされたと見なされ、Apple の Captive Network Assistant（CNA）が疑似ブラウザを自動起動して管理ウィンドウでポータル ログインを要求します。ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。 組み込みワイヤレスコントローラは、この疑似ブラウザがポップアップ表示されないようにします。

現在、WISPr検出プロセスをバイパスするように組み込みワイヤレスコントローラを設定できるようになりました。それによって、ユーザーが、ユーザーコンテキストでスプラッシュページのロードを引き起こす Web ページを要求したときに、バックグラウンドで WISPr 検出を実行せずに、Web 認証代行受信だけが行われるようにすることができます。

LWA および CWA における WLAN のキャプティブ バイパスの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [Captive Bypass Portal] チェックボックスをオンにします。

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

LWA および CWA内の WLAN におけるキャプティブ バイパスの設定（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`	グローバル設定モードを開始します。
ステップ 2	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth WLAN1_MAP`	パラメータ マップを作成します。 *parameter-map-name* は 99 文字を超えないようにする必要があります。
ステップ 3	**captive-bypass-portal** 例： `Device(config)# captive-bypass-portal`	キャプティブ バイパスを設定します。
ステップ 4	**wlan** *profile-name wlan-id ssid-name* 例：	WLAN の名前と ID を指定します。 • *profile-name* は、最大 32 文字の英数字からなる WLAN 名です。

	コマンドまたはアクション	目的
	`Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME`	• *wlan-id* はワイヤレス LAN の ID です。有効な範囲は 1 ～ 512 です。 • *ssid-name* は、最大 32 文字の英数字からなる SSID です。
ステップ 5	**security web-auth** 例： `Device(config-wlan)# security web-auth`	WLAN の Web 認証を有効にします。
ステップ 6	**security web-auth parameter-map** *parameter-map-name* 例： `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	パラメータ マップをマッピングします。 （注） パラメータ マップが WLAN に関連付けられていない場合は、グローバル パラメータ マップの設定と見なされます。
ステップ 7	**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。

DHCP オプション 55 および 77 の ISE への送信

DHCP オプション 55 および 77 について

DHCP センサーは、ネイティブおよびリモート プロファイリングのために、ISE で次の DHCP オプションを使用します。

- **オプション 12**：ホスト名
- **オプション 6**：クラス ID

これと一緒に、次のオプションをプロファイリングのために ISE に送信する必要があります。

- **オプション 55**：パラメータ要求リスト
- **オプション 77**：ユーザー クラス

DHCP オプション 55 および 77 を ISE に送信するための設定（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] をクリックして [Add Policy Profile] ウィンドウを表示します。

ステップ 3 [Access Policies] タブをクリックし、[RADIUS Profiling] チェックボックスと [DHCP TLV Caching] チェックボックスをオンにして、WLANで RADIUS プロファイリングと DHCP TLV キャッシングを設定します。

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

DHCP オプション 55 および 77 を ISE に送信するための設定（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。
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	**dhcp-tlv-caching** 例： `Device(config-wireless-policy)# dhcp-tlv-caching`	WLAN で DHCP TLV キャッシングを設定します。
ステップ 4	**radius-profiling** 例： `Device(config-wireless-policy)# radius-profiling`	WLAN でクライアント RADIUS プロファイリングを設定します。
ステップ 5	**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。

EAP 要求のタイムアウトの設定（GUI）

以下の手順に従って、GUI を使用して EAP 要求タイムアウトを設定します。

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Advanced EAP]** を選択します。

ステップ 2 [EAP-Identity-Request Timeout] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP ID 要求を送信する際の試行時間（秒単位）を指定します。

ステップ 3 [EAP-Identity-Request Max Retries] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP ID 要求を再送信する際の最大試行回数を指定します。

ステップ 4 [EAP Max-Login Ignore Identity Response] を [Enabled] 状態に設定して、同じユーザー名を使用してデバイスに接続できるクライアントの数を制限します。同じデバイス上の異なるクライアント（PDA、ラップトップ、IP フォンなど）から最大 8 台までログインできます。デフォルトの状態は [Disabled] です。

ステップ 5 [EAP-Request Timeout] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP 要求を送信する際の試行時間（秒単位）を指定します。

ステップ 6 [EAP-Request Max Retries] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP 要求を再送信する際の最大試行回数を指定します。

ステップ 7 [EAPOL-Key Timeout] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに LAN 経由で EAP キーを送信する際の試行時間（秒単位）を指定します。

ステップ 8 [EAPOL-Key Max Retries] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。

ステップ 9 [EAP-Broadcast Key Interval] フィールドで、クライアントに使用されるブロードキャスト暗号キーのローテーションの時間間隔を指定し、[Apply] をクリックします。

（注） EAP ブロードキャストキー間隔を新しい期間に設定した後、変更を有効にするには、WLAN をシャットダウンまたは再起動する必要があります。WLAN がシャットダウンまたは再起動し、設定されたタイマー値が期限切れになると、M5 および M6 パケットが交換されます。

EAP 要求のタイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 wps client-exclusion dot1x-timeout** 例： `Device(config)# wireless wps client-exclusion dot1x-timeout`	タイムアウト時および応答がない場合の除外を有効にします。 デフォルトでは、この機能は有効です。 無効にするには、コマンドの先頭に **no** を付けます。
ステップ 3	**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。

ワイヤレスセキュリティでの EAP 要求タイムアウトの設定（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。
ステップ 2	0 - 20 1 - 120 } **wireless security dot1x request** {**retries** | **timeout** 例： `Device(config)# wireless security dot1x request timeout 60`	EAP 要求の再送信タイムアウト値を秒単位で設定します。
ステップ 3	**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。

キャプティブ ポータル

キャプティブ ポータル設定

この機能を使用すると、AP に基づき同じ SSID に対して、複数の Web 認証 URL（外部のキャプティブ URL を含む）を設定できます。デフォルトの設定では、グローバル URL が認証に使用されます。オーバーライド オプションは、WLAN および AP レベルで使用できます。

優先順位は次のとおりです。

- AP
- WLAN
- グローバル コンフィギュレーション

キャプティブ ポータルの設定の制約事項

- この設定は、スタンドアロン コントローラでのみサポートされています。
- エクスポート アンカー設定はサポートされていません。

キャプティブポータルの設定（GUI）

手順

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

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、[Profile Name]、[SSID]、および [WLAN ID] を入力します。

ステップ 4 [Security] > [Layer2] タブで、[WPA Policy]、[AES]、および [802.1x] チェックボックスをオフにします。

ステップ 5 [Security] > [Layer3] タブで、[Web Auth Parameter Map] ドロップダウンリストからパラメータマップを選択し、[Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 6 [Security] > [AAA] タブの [Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 7 [Apply to Device] をクリックします。

ステップ 8 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 9 [Web Auth Parameter Map] を選択します。

ステップ 10 [General] タブで、[Maximum HTTP connections]、[Init-State Timeout(secs)] を入力し、[Type] ドロップダウンリストから [webauth] を選択します。

ステップ 11 [Advanced] タブの [Redirect to external server] 設定で、**Redirect for log-in server** と入力します。

ステップ 12 [Update & Apply] をクリックします。

キャプティブ ポータルの設定

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	**wlan** {*profile-name* | **shutdown**} *network-name* 例： `Device(config)# wlan edc6 6 edc`	WLANプロファイルを設定します。すべてのWLANを有効または無効にし、WLAN IDを作成します。プロファイル名と SSID ネットワーク名には、最大 32 文字の英数字を使用できます。
ステップ 3	**ip** {**access-group** | **verify**} **web** *IPv4-ACL-Name* 例： `Device(config-wlan)# ip access-group web CPWebauth`	WLAN の Web ACL を設定します。 （注） この操作を実行する前に、WLANを無効にしておく必要があります。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を無効にします。

ステップ 7	**security web-auth** {**authentication-list** *authentication-list-name* | **authorization-list** *authorization-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*}
	例：
	`Device(config-wlan)# security web-auth authentication-list cp-webauth`
	`Device(config-wlan)# security web-auth parameter-map parMap6`
		WLAN の Web 認証を有効にします。ここで、各変数は次のように定義されます。
		• **authentication-list**
		authentication-list-name：IEEE 802.1x の認証リストを指定します。
		• **authorization-list**

	コマンドまたはアクション	目的
		authorization-list-name：IEEE 802.1x のオーバーライド認可リストを指定します。 • **on-macfilter-failure**：MAC フィルタの失敗における Web 認証を有効にします。 • **parameter-map** *parameter-map-name*：パラメータ マップを設定します。 （注） **security web-auth** を有効にすると、デフォルトの **authentication-list** とグローバルの **parameter-map** がマッピングされます。これは、明示的に記述されていない認証リストとパラメータマップに適用されます。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**exit** 例： `Device(config-wlan)# exit`	WLAN 設定を終了します。
ステップ 10	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth parMap6`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 11	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth parMap6`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 12	**type webauth** 例： `Device(config-params-parameter-map)# type webauth`	webauth タイプ パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 13	**timeout init-state sec** <*timeout-seconds*> 例： `Device(config-params-parameter-map)# timeout inti-state sec 3600`	WEBAUTH のタイムアウトを秒単位で設定します。タイムアウト（秒単位）パラメータの有効な範囲は 60 ～ 3932100 秒です。
ステップ 14	**redirect for-login** <*URL-String*> 例： `Device(config-params-parameter-map)# redirect for-login https://172.16.100.157/portal/login.html`	ログイン時のリダイレクト用の URL 文字列を設定します。
ステップ 15	**exit** 例： `Device(config-params-parameter-map)# exit`	パラメータ設定を終了します。
ステップ 16	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy policy_tag_edc6`	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 17	**wlan** *wlan-profile-name* **policy** *policy-profile-name* 例： `Device(config-policy-tag)# wlan edc6 policy policy_profile_flex`	WLAN プロファイルにポリシー プロファイルをアタッチします。
ステップ 18	**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。

キャプティブ ポータル設定：例

次に、複数の AP を異なるロケーションに配置して同じ SSID をブロードキャストするものの、クライアントを異なるリダイレクト ポータルにリダイレクトする例を示します。

異なるリダイレクトポータルを指す複数のパラメータ マップを設定するには、次のようにします。

```
parameter-map type webauth parMap1
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.3:8080/portal/PortalSetup.action?portal=cfdbce00-2ce2-11e8-b83c-005056a06b27
redirect portal ipv4 172.16.12.3
!
```

```
!
parameter-map type webauth parMap11
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.4:8443/portal/PortalSetup.action?portal=094e7270-3808-11e8-9797-02421e4cae0c
redirect portal ipv4 172.16.12.4
!
```

これらのパラメータ マップを異なる WLAN に関連付けます。

```
wlan edc1 1 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap11
no shutdown
wlan edc2 2 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap1
no shutdown
```

（注） すべての WLAN に同じ SSID があります。

WLAN を異なるポリシー タグに関連付けます。

```
wireless tag policy policy_tag_edc1
wlan edc1 policy policy_profile_flex
wireless tag policy policy_tag_edc2
wlan edc2 policy policy_profile_flex
```

これらのポリシー タグを目的の AP に割り当てます。

```
ap E4AA.5D13.14DC
policy-tag policy_tag_edc1
site-tag site_tag_flex
ap E4AA.5D2C.3CAC
policy-tag policy_tag_edc2
site-tag site_tag_flex
```

第 47 章

複数の RADIUS サーバー間での認証および認可

複数の RADIUS サーバー間での認証および認可について

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ は、認証と認可の両方を組み合わせた単一の RADIUS サーバーと要求および応答トランザクションを行うアプローチを使用します。コントローラでの認証と認可は、複数の RADIUS サーバーに分割することができます。

RADIUS サーバーは、認証サーバー、認可サーバー、またはその両方の役割を担うことができます。認証と認可を異なる RADIUS サーバーで行う場合は、 組み込みワイヤレスコントローラ上の Session Aware Network（SANet）コンポーネントによって、クライアントが 組み込みワイヤレスコントローラに参加するときに一方のサーバーで認証を行い、別のサーバーで認可を行うことが可能になりました。

認証は、Cisco ISE、Cisco DNAC、Free RADIUS、または任意のサードパーティ製 RADIUS サーバーを使用して実行できます。認証サーバーで認証が成功すると、組み込みワイヤレスコントローラは、認証サーバーから受信した属性を、認可サーバーとして指定された別の RADIUS サーバーに中継します。

その後、認可サーバーは次の処理を実行します。

- サーバーで定義されている他のポリシーやルールを使用して、受信した属性を処理する。
- 認証応答の一部として属性を導出し、 組み込みワイヤレスコントローラに返す。

（注） 認証と認可の分割設定では、両方のサーバーを使用可能にする必要があります。また、組み込みワイヤレスコントローラがセッションを受け入れられるように、両方のサーバーで ACCESS-ACCEPT を使用して認証と認可を正常に行う必要があります。

認証および認可サーバーの分割による WLAN の 802.1X セキュリティの設定

明示的な認証および認可サーバー リストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。

ステップ 2 [Authentication Authorization and Accounting] ページで、[Servers/Groups] タブをクリックします。

ステップ 3 次のオプションから、設定する AAA サーバーのタイプをクリックします。

- RADIUS
- TACACS+
- LDAP

この手順では、RADIUS サーバーの設定について説明します。

ステップ 4 [RADIUS] オプションを選択した状態で、[Add] をクリックします。

ステップ 5 RADIUS サーバーの名前と、サーバーの IPv4 または IPV6 アドレスを入力します。

ステップ 6 デバイスと、RADIUS サーバー上で動作するキー文字列 RADIUS デーモンとの間で使用される認証および暗号キーを入力します。PAC キーまたは非 PAC キーのどちらを使用するかを選択できます。

ステップ 7 サーバーのタイムアウト値を入力します。有効な範囲は 1 ～ 1000 秒です。

ステップ 8 再試行回数を入力します。有効な範囲は 0 ～ 100 です。

ステップ 9 [Support for CoA] フィールドは [Enabled] 状態のままにしておきます。

ステップ 10 [Save & Apply to Device] をクリックします。

ステップ 11 [Authentication Authorization and Accounting] ページで、[RADIUS] オプションを選択した状態で、[Server Groups] タブをクリックします。

ステップ 12 [Add] をクリックします。

ステップ 13 表示される [Create AAA RADIUS Server Group] ウィンドウで、RADIUS サーバー グループの名前を入力します。

ステップ 14 [MAC-Delimiter] ドロップダウン リストから、RADIUS サーバーに送信される MAC アドレスで使用される区切り文字を選択します。

ステップ 15 [MAC Filtering] ドロップダウン リストから、MAC アドレスをフィルタリングするための基準値を選択します。

ステップ 16 サーバー グループのデッドタイムを設定し、稼働特性が異なる別のサーバー グループに AAA トラフィックを転送するには、[Dead-Time] フィールドに、サーバーが停止していると見なされる時間を分単位で入力します。

ステップ 17 [Available Servers] リストから、サーバー グループに含めるサーバーを選択し、それらを [Assigned Servers] リストに移動します。

ステップ 18 [Save & Apply to Device] をクリックします。

明示的な認証サーバーリストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** > **[Servers/Groups]** 選択します。

ステップ 2 [RADIUS] > [Servers] タブを選択します。

ステップ 3 [Add] をクリックして新しいサーバーを追加するか、既存のサーバーをクリックします。

ステップ 4 [Name]、[Server Address]、[Key]、[Confirm Key]、[Auth Port]、[Acct Port] を入力します。[PAC Key] チェックボックスをオンにして、[PAC key] と [Confirm PAC Key] を入力します。

ステップ 5 [Apply to Device] をクリックします。

ステップ 6 [RADIUS] > [Server Groups] を選択し、[Add] をクリックして新しいサーバーグループを追加するか、既存のサーバーグループをクリックします。

ステップ 7 サーバーグループの [Name] を入力し、そのサーバーグループに含めるサーバーを [Available Servers] リストから選択し、[Assigned Servers] リストに移動します。

ステップ 8 [Apply to Device] をクリックします。

明示的な認証サーバーリストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**radius server** *server-name* 例： デバイス(config)# **radius server free-radius-authc-server**	RADIUS サーバー名を指定します。
ステップ 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* 例： デバイス(config-radius-server)# **address ipv4 9.2.62.56 auth-port 1812 acct-port 1813**	RADIUS サーバーのパラメータを指定します。
ステップ 5	[**pac**] **key** *key* 例： デバイス(config-radius-server)# **key cisco**	デバイスと、RADIUS サーバー上で動作するキー文字列 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 6	**exit** 例： デバイス(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	**aaa group server radius** *server-group* 例： デバイス(config)# **aaa group server radius authc-server-group**	RADIUS サーバ グループの ID を作成します。 *server-group* はサーバー グループ名です。有効な範囲は 1 ～ 32 文字の英数字です。 コントローラに定義されたルートに RADIUS サーバーの IP アドレスが追加されていない場合、デフォルトルートが使用されます。AAA サーバーグループで定義された SVI からトラフィックを送信する特定のルートを定義することをお勧めします。
ステップ 8	**server name** *server-name* 例： デバイス(config)# **server name free-radius-authc-server**	サーバー名を設定します。
ステップ 9	**end** 例： デバイス(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。

	コマンドまたはアクション	目的
		詳細については、「外部認証用の AAA の設定」を参照してください。

明示的な認可サーバーリストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** > **[Servers/Groups]** 選択します。

ステップ 2 [RADIUS] > [Servers] タブを選択します。

ステップ 3 [Add] をクリックして新しいサーバーを追加するか、既存のサーバーをクリックします。

ステップ 4 [Name]、[Server Address]、[Key]、[Confirm Key]、[Auth Port]、[Acct Port] を入力します。[PAC Key] チェックボックスをオンにして、[PAC key] と [Confirm PAC Key] を入力します。

ステップ 5 [Apply to Device] をクリックします。

ステップ 6 [RADIUS] > [Server Groups] を選択し、[Add] をクリックして新しいサーバーグループを追加するか、既存のサーバーグループをクリックします。

ステップ 7 サーバーグループの [Name] を入力し、そのサーバーグループに含めるサーバーを [Available Servers] リストから選択し、[Assigned Servers] リストに移動します。

ステップ 8 [Apply to Device] をクリックします。

明示的な認可サーバーリストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**radius server** *server-name* 例： `デバイス(config)# radius server cisco-dnac-authz-server`	RADIUS サーバー名を指定します。

	コマンドまたはアクション	目的
ステップ 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* 例： `デバイス(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813`	RADIUS サーバーのパラメータを指定します。
ステップ 5	[**pac**] **key** *key* 例： `デバイス(config-radius-server)# pac key cisco`	デバイスと、RADIUS サーバー上で動作するキー文字列 RADIUS デーモンとの間で使用される認可および暗号キーを指定します。
ステップ 6	**exit** 例： `デバイス(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	**aaa group server radius** *server-group* 例： `デバイス(config)# aaa group server radius authz-server-group`	RADIUS サーバ グループの ID を作成します。
ステップ 8	**server name** *server-name* 例： `デバイス(config)# server name cisco-dnac-authz-server`	
ステップ 9	**end** 例： `デバイス(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。

802.1X セキュリティ用の認証および認可リストの設定（GUI）

手順

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

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、[Profile Name]、[SSID]、および [WLAN ID] を入力します。

ステップ 4 [Security] > [AAA] タブの [Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 5 [Apply to Device] をクリックします。

802.1X セキュリティ用の認証および認可リストの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**wlan** *wlan-name wlan-id SSID-name* 例： `デバイス(config)# wlan wlan-foo 222 foo-ssid`	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*：設定されている WLAN の名前です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID-name*：最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンド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 4	**security dot1x authentication-list** *authenticate-list-name* 例： `デバイス(config-wlan)# security dot1x authentication-list authc-server-group`	dot1x セキュリティ用の認証リストを有効にします。
ステップ 5	**security dot1x authorization-list** *authorize-list-name* 例： `デバイス(config-wlan)# security dot1x authorization-list authz-server-group`	dot1x セキュリティ用の認可リストを指定します。 **Cisco Digital Network Architecture Center**（**DNAC**）の詳細については、DNAC のマニュアルを参照してください。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `デバイス(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。

認証および認可サーバーの分割による WLAN の Web 認証の設定

Web 認証用の認証および認可リストの設定（GUI）

手順

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

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、[Profile Name]、[SSID]、および [WLAN ID] を入力します。

ステップ 4 [Security] > [Layer2] タブで、[WPA Policy]、[AES]、および [802.1x] チェックボックスをオフにします。

ステップ 5 [MAC Filtering] チェックボックスをオンにして、機能を有効にします。MAC フィルタリングを有効にした状態で、[Authorization List] ドロップダウンリストから認可リストを選択します。

ステップ 6 [Security] > [AAA] タブの [Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 7 [Apply to Device] をクリックします。

Web 認証用の認証および認可リストの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**wlan** *wlan-name wlan-id SSID-name* 例： `デバイス(config)# wlan wlan-bar 1 bar-ssid`	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*：設定されている WLAN の名前です。 • *wlan-id*：ワイヤレス LAN の ID です。 • *SSID-name*：最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンド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 4	**no security wpa** 例： `デバイス(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no security wpa akm dot1x** 例： `デバイス(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2** 例： `デバイス(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 7	**security web-auth** {**authentication-list** *authenticate-list-name* | **authorization-list** *authorize-list-name*} 例： `デバイス(config-wlan)# security web-auth authentication-list authc-server-group`	dot1x セキュリティ用の認証または認可リストを有効にします。 （注） WPA セキュリティ、dot1x の AKM、および WPA2 セキュリティを無効にしていない場合は、次のエラーが表示されます。 *% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.*

	コマンドまたはアクション	目的
ステップ 8	**end** 例： デバイス(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。

認証と認可の分割設定の確認

WLAN の詳細を表示するには、次のコマンドを使用します。

```
Device# show run wlan
wlan wlan-foo 2 foo-ssid
security dot1x authentication-list authc-server-group
security dot1x authorization-list authz-server-group

wlan wlan-bar 3 bar-ssid
security web-auth authentication-list authc-server-group
security web-auth authorization-list authz-server-group
```

AAA 認証およびサーバーの詳細を表示するには、次のコマンドを使用します。

```
Device# show run aaa
!
aaa authentication dot1x default group radius
username cisco privilege 15 password 0 cisco
!
!
radius server free-radius-authc-server
 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
 key cisco
!
radius server cisco-dnac-authz-server
 address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
 pac key cisco
!
!
aaa new-model
aaa session-id common
!
```

802.1Xセキュリティ用の認証および認可リストを表示するには、次のコマンドを使用します。

```
Device# show wlan name wlan-foo | sec 802.1x
802.1x authentication list name               : authc-server-group
802.1x authorization list name                : authz-server-group
            802.1x                            : Enabled
```

Web 認証用の認証および認可リストを表示するには、次のコマンドを使用します。

```
Device# show wlan name wlan-bar | sec Webauth
    Webauth On-mac-filter Failure             : Disabled
    Webauth Authentication List Name          : authc-server-group
    Webauth Authorization List Name           : authz-server-group
    Webauth Parameter Map                     : Disabled
```

設定例

サードパーティの RADIUS サーバーを使用した認証のための Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの設定：例

次に、サードパーティの RADIUS サーバーを使用した認証のための Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの設定例を示します。

```
Device(config)# radius server free-radius-authc-server
Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
Device(config-radius-server)# key cisco
Device(config-radius-server)# exit
Device(config)# aaa group server radius authc-server-group
Device(config)# server name free-radius-authc-server
Device(config)# end
```

Cisco ISE または DNAC を使用した認証のための Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの設定：例

次に、Cisco ISE または DNAC を使用した認証のための Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの設定例を示します。

```
Device(config)# radius server cisco-dnac-authz-server
Device (config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
Device (config-radius-server)# pac key cisco
Device (config-radius-server)# exit
Device(config)# aaa group server radius authz-server-group
Device(config)# server name cisco-dnac-authz-server
Device(config)# end
```

第 48 章

Secure LDAP

SLDAP について

Transport Layer Security（TLS）

Transport Layer Security（TLS）は、プライバシー、認証、およびデータ整合性によるデータのセキュア トランザクションを可能にするアプリケーションレベル プロトコルです。TLS は、証明書、公開キーおよび秘密キーに基づいて、クライアントの ID を証明します。

証明書は認証局（CA）によって発行されます。

各証明書には次のものが含まれています。

- 発行された権限の名前。
- 証明書の発行先エンティティの名前。
- エンティティの公開キー。
- 証明書の有効期限を示すエンティティのタイムスタンプ。

TLS による LDAP のサポートについては、LDAP プロトコルの拡張である RFC 2830 を参照してください。

LDAP 操作

バインド

バインド操作は、サーバーに対してユーザーを認証するために使用されます。LDAP サーバーとの接続を開始するために使用されます。LDAP はコネクション型プロトコルです。クライアントはプロトコル バージョンと認証情報を指定します。

LDAP は次のバインドをサポートします。

- 認証済みバインド：認証済みバインドは、ルートの認定者名（DN）とパスワードが使用できる場合に実行されます。
- 匿名バインド：ルート DN とパスワードがない場合は、匿名バインドが実行されます。

LDAP 環境では、検索操作が実行されてから、バインド操作が実行されます。これは、パスワード属性が検索操作の一部として返される場合、パスワードの確認を LDAP クライアントのローカルで実行できるためです。したがって、余計なバインド操作を実行する必要がなくなります。パスワード属性が返されない場合、バインド操作を後で実行できます。検索操作を先に実行してバインド操作を後で実行するもう 1 つの利点は、ユーザー名（cn 属性）の前にベース DN を付けることで DN を構成するのではなく、検索結果で受信した DN をユーザー DN として使用できることです。LDAP サーバーに保存されているすべてのエントリには、固有の DN があります。

DN は 2 つの部分で構成されます。

- 相対識別名（RDN）
- レコードが存在する LDAP サーバー内の場所。

LDAP サーバーに保存されているエントリのほとんどには名前があり、多くの場合、名前は Common Name（cn）属性で保存されます。すべてのオブジェクトには名前があるため、LDAP に保存されているほとんどのオブジェクトは RDN のベースとして cn 値を使用します。

検索

検索操作は、LDAP サーバーを検索するために使用されます。クライアントは検索の開始点（ベース DN）、検索範囲（オブジェクト、その子、またはそのオブジェクトをルートとするサブツリー）、およびサーチ フィルタを指定します。

認可要求の場合、検索操作はバインド操作なしで直接実行されます。検索操作を正常に実行するには、LDAP サーバを特定の特権で設定します。この特権レベルは、バインド操作で設定します。

LDAP 検索操作は、特定のユーザーについて複数のユーザー エントリを返す可能性があります。このような場合、LDAP クライアントは適切なエラー コードを AAA に返します。このようなエラーを回避するために、単一のエントリに一致させるための適切なサーチ フィルタを設定する必要があります。

比較

認証のために、比較操作を使用して、バインド要求を比較要求で置換します。比較操作によって、接続のための最初のバインド パラメータを維持できます。

LDAP ダイナミック属性マッピング

Lightweight Directory Access Protocol（LDAP）は、AAA サーバーとの通信に適した強力で柔軟性の高いプロトコルです。LDAP 属性マップには、サーバから取得した属性を、セキュリティアプライアンスによってサポートされるシスコ属性にクロスリファレンスする方式が備わっています。

ユーザがセキュリティアプライアンスを認証すると、次にセキュリティアプライアンスはサーバを認証し、LDAP プロトコルを使用してそのユーザのレコードを取得します。このレコードは、サーバにユーザ インターフェイスに表示されるフィールドに関連付けられた LDAP 属性で構成されます。取得される各属性には、ユーザー レコードを更新する管理者が入力した値が含まれます。

SLDAP の設定の前提条件

セキュア Transport Layer Security（TLS）のセキュア接続を使用している場合、 X.509 証明書を設定する必要があります。

SLDAP の設定の制約事項

- LDAP 照会はサポートされていません
- LDAP サーバからの割り込みメッセージまたは通知は処理されません。
- LDAP 認証は、インタラクティブ（端末）セッションではサポートされていません。

SLDAP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**ldap server** *name* 例：	Lightweight Directory Access Protocol（LDAP）サーバーを定義し、LDAP

	コマンドまたはアクション	目的
	デバイス(config)# **ldap server server1**	サーバー コンフィギュレーション モードを開始します。
ステップ 4	**ipv4** *ipv4-address* 例： デバイス(config-ldap-server)# **ipv4 9.4.109.20**	IPv4 を使用して LDAP サーバの IP アドレスを指定します。
ステップ 5	**timeout retransmit** *seconds* 例： デバイス(config-ldap-server)# **timeout retransmit 20**	組み込みワイヤレスコントローラが LDAP 要求を再送信する前に応答を待機する秒数を指定します。
ステップ 6	**bind authenticate root-dn password** [**0** *string* | **7** *string*] *string* 例： デバイス(config-ldap-server)# **bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345**	組み込みワイヤレスコントローラと LDAP サーバー間で使用される共有秘密テキスト ストリングを指定します。 暗号化されていない共有秘密を設定するには、**0** 回線オプションを使用します。 暗号化された共有秘密を設定するには、**7** 回線オプションを使用します。
ステップ 7	**base-dn** *string* 例： デバイス(config-ldap-server)# **base-dn CN=Users,DC=ca,DC=ssh2,DC=com**	検索のベース識別名（DN）を指定します。
ステップ 8	**mode secure** [**no- negotiation**] 例： デバイス(config-ldap-server)# **mode secure no- negotiation**	TLS 接続を開始するよう LDAP を設定し、セキュア モードを指定します。
ステップ 9	**end** 例： デバイス(config-ldap-server)# **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。

AAA サーバー グループの設定（GUI）

AAA サーバ グループを使用するようにデバイスを設定すると、既存のサーバ ホストをグループ化し、設定済みのサーバ ホストのサブセットを選択して、それらのサーバを特定のサービスに使用することが簡単にできます。サーバー グループは、グローバル サーバー ホストの一覧

と一緒に使用されます。サーバー グループには、選択したサーバー ホストの IP アドレスが一覧表示されます。

次のサーバー グループを作成できます。

手順

ステップ 1 RADIUS

a) [Services] > [Security] > [AAA] > [Server Groups] > [RADIUS] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Radius Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、RADIUS サーバー グループの名前を入力します。
d) [MAC-Delimiter] ドロップダウン リストから目的の区切り文字を選択します。コロン、ハイフン、およびシングルハイフンから選択できます。
e) [MAC-Filtering] ドロップダウン リストから目的のフィルタを選択します。[mac] および [Key] を選択できます。
f) サーバーを非稼働にするには、[Dead-Time (mins)] フィールドに値を入力します。値は 1 ～ 1440 の範囲で指定する必要があります。
g) [Available Servers] リストから使用可能なサーバーを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
h) [Save & Apply to Device] ボタンをクリックします。

ステップ 2 TACACS+

a) [Services] > [Security] > [AAA] > [Server Groups] > [TACACS+] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Tacacs Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、TACACS サーバー グループの名前を入力します。
d) [Available Servers] リストから使用可能なサーバーを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
e) [Save & Apply to Device] ボタンをクリックします。

ステップ 3 LDAP

a) [Services] > [Security] > [AAA] > [Server Groups] > [LDAP] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Ldap Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、LDAP サーバ グループの名前を入力します。
d) [Available Servers] リストから使用可能なサーバーを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
e) [Save & Apply to Device] ボタンをクリックします。

AAA サーバー グループの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**aaa new-model** 例： `デバイス(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa group server ldap** *group-name* 例： `デバイス(config)# aaa group server ldap name1`	グループ名を使用して AAA サーバ グループを定義し、LDAP サーバ グループ コンフィギュレーション モードを開始します。 グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS、LDAP、または TACACS+ です。
ステップ 5	**server** *name* 例： `デバイス(config-ldap-sg)# server server1`	特定の LDAP サーバーを定義済みのサーバー グループと関連付けます。 セキュリティ サーバーは、IP アドレスと UDP ポート番号で識別されます。
ステップ 6	**exit** 例： `デバイス(config-ldap-sg)# exit`	LDAP サーバー グループ コンフィギュレーション モードを終了します。

認証要求のための検索操作とバインド操作の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**aaa new-model** 例： `デバイス(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**ldap server** *name* 例： `デバイス(config)# ldap server server1`	Lightweight Directory Access Protocol（LDAP）サーバーを定義し、LDAP サーバー コンフィギュレーション モードを開始します。
ステップ 5	**authentication bind-first** 例： `デバイス(config-ldap-server)# authentication bind-first`	認証要求のために一連の検索操作とバインド操作を設定します。
ステップ 6	**authentication compare** 例： `デバイス(config-ldap-server)# authentication compare`	バインド要求を認証の比較要求に置き換えます。
ステップ 7	**exit** 例： `デバイス(config-ldap-server)# exit`	LDAP サーバー グループ コンフィギュレーション モードを終了します。

SLDAP サーバーでのダイナミック属性マップの設定

既存のユーザー定義属性名と値を、セキュリティアプライアンスと互換性があるシスコ属性名と値にマッピングする、LDAP 属性マップを作成する必要があります。作成した属性マップは、必要に応じて LDAP サーバーにバインドしたり削除したりできます。

（注） 属性マッピング機能を適切に使用するには、シスコ LDAP 属性の名前と値、およびユーザ定義属性の名前と値を理解する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**ldap attribute-map** *map-name* 例： `デバイス(config)# ldap attribute-map map1`	ダイナミック LDAP 属性マップを設定し、属性マップ コンフィギュレーション モードを開始します。
ステップ 4	**map type** *ldap-attr-type aaa-attr-type* 例： `デバイス(config-attr-map)# map type department supplicant-group`	属性マップを定義します。
ステップ 5	**exit** 例： `デバイス(config-attr-map)# exit`	属性マップ コンフィギュレーション モードを終了します。

SLDAP の設定の確認

デフォルトの LDAP 属性マッピングの詳細を表示するには、次のコマンドを使用します。

```
Device# show ldap attributes
```

LDAP サーバーの状態情報や、それ以外のサーバーの各種カウンタを表示するには、次のコマンドを使用します。

```
Device# show ldap server
```

第 49 章

RADIUS DTLS

RADIUS DTLS について

Remote Authentication Dial-In User Service（RADIUS）は、ネットワークへの管理アクセス権を取得しようとするユーザーに対して中央管理されたセキュリティ機能を提供する、クライアントまたはサーバープロトコルです。RADIUS プロトコルは広く導入されている認証および認可プロトコルであり、完全な認証、認可、およびアカウンティング（AAA）ソリューションを実現します。

RADIUS DTLS のポート

RADIUS のポート（DTLS サーバー）は認証とアカウンティングに使用されます。デフォルトの DTLS サーバー ポートは 2083 です。

RADIUS DTLS ポート番号は **dtls port** *port_number* を使用して変更できます。詳細については、「RADIUS DTLS ポート番号の設定」を参照してください。

共有秘密

すでに特定のサーバーに対して DTLS を有効にしている場合は、共有秘密として **radius/dtls** を使用できます。

CTS 通信のための PAC の処理

CTS 通信のために ISE から PAC をダウンロードできます。PAC をダウンロードしたら、共有秘密の代わりに PAC キーを使用してすべての CTS 属性を暗号化する必要があります。

その後、ISE は PAC を使用してそれらの属性を復号化します。

セッション管理

RADIUS クライアントは、DTLS サーバーからの応答にのみ依存します。セッションが理想的なタイムアウトに最も適している場合は、セッションを閉じる必要があります。

応答が無効の場合は、セッションを削除する必要があります。

DTLS 経由で RADIUS パケットを送信する必要がある場合は、特定のサーバーで DTLS セッションを再確立する必要があります。

ロード バランシング

複数の DTLS サーバーとロード バランシング方式が設定されています。

要求を必要とする送信先の AAA サーバーを選択する必要があります。その後、特定のサーバーの DTLS コンテキストを使用し、RADIUS パケットを暗号化して送り返します。

接続タイムアウト

暗号化された RADIUS パケットを送信した後、再送信タイマーを開始する必要があります。再送信タイマーが期限切れになる前に応答がなかった場合は、パケットが再暗号化され再送信されます。

この試行回数は、**dtls retries** の設定に従って、またはデフォルト値まで継続できます。試行回数が制限を超えると、サーバーは使用不可となり、応答は AAA クライアントに戻されます。

（注） デフォルトの接続タイムアウトは 5 秒です。

接続の再試行回数

RADIUS DTLS は UDP ベースであるため、特定の再試行回数において特定のタイムアウト間隔後に接続を再試行する必要があります。

すべての再試行を終えると、DTLS 接続では次のことが実行されます。

- 失敗としてマークされます。
- RADIUS 要求を処理するために次に使用可能なサーバーを検索します。

（注） デフォルトの接続再試行回数は 5 回です。

アイドル タイムアウト

アイドル タイマーが期限切れになり、最後のアイドル タイムアウト以降にトランザクションが存在しない場合、DTLS セッションは閉じたままになります。

DTLS セッションを確立した後、アイドル タイマーを開始できます。アイドル タイマーを 30 秒間にわたって開始し、RADIUS DTLS パケットの 1 つが送信されると、30 秒後にアイドル タイマーが期限切れになり、RADIUS DTLS トランザクションの数がチェックされます。

アイドル タイマーの値がゼロを超えると、アイドル タイマーはトランザクション カウンタをリセットし、タイマーを再開します。

（注） デフォルトのアイドル タイムアウトは 60 秒です。

サーバーおよびサーバー グループのフェールオーバーの処理

RADIUS サーバーは DTLS ありおよび DTLS なしで設定できます。DTLS 対応サーバーと非 DTLS サーバーを使用して AAA サーバー グループを作成することをお勧めします。ただし、AAA サーバー グループの設定時にはこのような制限は受けません。

DTLS サーバーを選択し、DTLS サーバーが接続を確立し、RADIUS 要求パケットが DTLS サーバーに送信されるとします。すべての RADIUS の再試行後も DTLS サーバーが応答しない場合は、同じサーバー グループ内で次に設定されているサーバーに引き継がれます。次のサーバが DTLS サーバの場合、RADIUS 要求パケットの処理は次のサーバで続行されます。次のサーバーが非 DTLS サーバーの場合、RADIUS 要求パケットの処理はそのサーバー グループでは行われません。その後、サーバー グループのフェールオーバーが発生し、次のサーバー グループが使用可能であれば、同じシーケンスが次のサーバー グループで続行されます。

（注） サーバー グループ内では、DTLS サーバーか非 DTLS サーバーのいずれかのみを使用する必要があります。

前提条件

IOS および BINOS AAA のサポート

AAA サーバーは、IOS および BINOS プラットフォームで動作します。IOS で RADIUS DTLS のサポートを完了したら、同じサポートを BINOS にも移植する必要があります。

RADIUS DTLS サーバーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**radius server** *server-name* 例： `デバイス(config)# radius server R1`	RADIUS サーバー名を指定します。
ステップ 4	**dtls** 例： `デバイス(config-radius-server)# dtls`	DTLS パラメータを設定します。
ステップ 5	**end** 例： `デバイス(config-radius-server)# 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。

RADIUS DTLS 接続タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**radius server** *server-name* 例：	RADIUS サーバー名を指定します。

	コマンドまたはアクション	目的
	デバイス(config)# **radius server R1**	
ステップ 4	**dtls connectiontimeout** *timeout* 例： デバイス(config-radius-server)# **dtls connectiontimeout 1**	RADIUS DTLS 接続タイムアウトを設定します。 ここで、各変数は次のように定義されます。 *timeout* は、DTLS 接続タイムアウト値を指します。有効な範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： デバイス(config-radius-server)# **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。

RADIUS DTLS アイドル タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Device# enable	特権 EXEC モードを開始します。
ステップ 2	**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 3	**radius server** *server-name* 例： デバイス(config)# **radius server R1**	RADIUS サーバー名を指定します。
ステップ 4	**dtls idletimeout** *idle_timeout* 例： デバイス(config-radius-server)# **dtls idletimeout 2**	RADIUS DTLS アイドル タイムアウトを設定します。 ここで、各変数は次のように定義されます。 *idle_timeout* は、DTLS アイドル タイムアウト値を指します。有効な範囲は 1 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `デバイス(config-radius-server)# 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。

RADIUS DTLS サーバー用の送信元インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**radius server** *server-name* 例： `デバイス(config)# radius server R1`	RADIUS サーバー名を指定します。
ステップ 4	**dtls ip** {**radius source-interface Ethernet-Internal** *interface_number* 例： `デバイス(config-radius-server)# dtls ip radius source-interface Ethernet-Internal 0`	RADIUS DTLS サーバーの送信元インターフェイスを設定します。 ここで、各変数は次のように定義されます。 • *interface_number* は、イーサネット内部インターフェイス番号を指します。デフォルト値は 0 です。
ステップ 5	**end** 例： `デバイス(config-radius-server)# 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。

RADIUS DTLS ポート番号の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**radius server** *server-name* 例： `デバイス(config)# radius server R1`	RADIUS サーバー名を指定します。
ステップ 4	**dtls port** *port_number* 例： `デバイス(config-radius-server)# dtls port 2`	RADIUS DTLS ポート番号を設定します。 ここで、各変数は次のように定義されます。 *port_number* は、DTLS ポート番号を指します。
ステップ 5	**end** 例： `デバイス(config-radius-server)# 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。

RADIUS DTLS 接続再試行回数の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**radius server** *server-name* 例： `デバイス(config)# radius server R1`	RADIUS サーバー名を指定します。
ステップ 4	**dtls retries** *retry_number* 例： `デバイス(config-radius-server)# dtls retries 3`	RADIUS 接続の再試行回数を設定します。 ここで、各変数は次のように定義されます。 *retry_number* は、DTLS 接続の再試行回数を指します。有効な範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `デバイス(config-radius-server)# 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。

RADIUS DTLS トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**radius server** *server-name* 例： `デバイス(config)# radius server R1`	RADIUS サーバー名を指定します。

ステップ 4	**dtls trustpoint** {**client** *LINE* **dtls** | **server** *LINE* **dtls**}
	例：
	`デバイス(config-radius-server)# dtls trustpoint client client1 dtls`
	`デバイス(config-radius-server)# dtls trustpoint server server1 dtls`
		クライアントとサーバーにトラストポイントを設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： デバイス(config-radius-server)# **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。

DTLS ダイナミック認証の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Device# enable	特権 EXEC モードを開始します。
ステップ 2	**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 3	**aaa server radius dynamic-author** 例： デバイス(config)# **aaa server radius dynamic-author**	RFC 3576 サポート用のローカル サーバー プロファイルを設定します。
ステップ 4	**dtls** 例： デバイス(config-locsvr-da-radius)# **dtls**	DTLS 送信元パラメータを設定します。
ステップ 5	**end** 例： デバイス(config-locsvr-da-radius)# **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。

クライアントの DTLS の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**aaa server radius dynamic-author** 例： `デバイス(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバー プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls** 例： `デバイス(config-locsvr-da-radius)# client 10.104.49.14 dtls`	クライアントの DTLS を有効にします。
ステップ 5	**end** 例： `デバイス(config-locsvr-da-radius)# 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。

DTLS のクライアント トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**aaa server radius dynamic-author** 例： `デバイス(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバー プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls** {**client-tp** *client-tp-name* | **server-tp** *server-tp-name*} 例： `デバイス(config-locsvr-da-radius)# client 10.104.49.14 dtls client-tp client_tp_name`	DTLS のクライアント トラストポイントを設定します。
ステップ 5	**end** 例： `デバイス(config-locsvr-da-radius)# 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。

DTLS アイドル タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**aaa server radius dynamic-author** 例： `デバイス(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバー プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls idletimeout** *timeout-interval* {**client-tp** *client_tp_name* | **server-tp** *server_tp_name*} 例： `デバイス(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 62 client-tp dtls_ise`	DTLS のアイドル時間を設定します。 ここで、各変数は次のように定義されます。 *timeout-interval* は、アイドル タイムアウト間隔を指します。有効な範囲は 60 ～ 600 です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `デバイス(config-locsvr-da-radius)# 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。

DTLS のサーバー トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**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 3	**aaa server radius dynamic-author** 例： `デバイス(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバー プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls server-tp** *server_tp_name* 例： `デバイス(config-locsvr-da-radius)# client 10.104.49.14 dtls server-tp dtls_client`	サーバー トラストポイントを設定します。
ステップ 5	**end** 例： `デバイス(config-locsvr-da-radius)# 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。

RADIUS DTLS サーバーの設定の確認

DTLS 対応サーバーに関する情報を表示するには、次のコマンドを使用します。

```
Device# show aaa servers
DTLS: Packet count since last idletimeout 1,
Send handshake count 3,
```

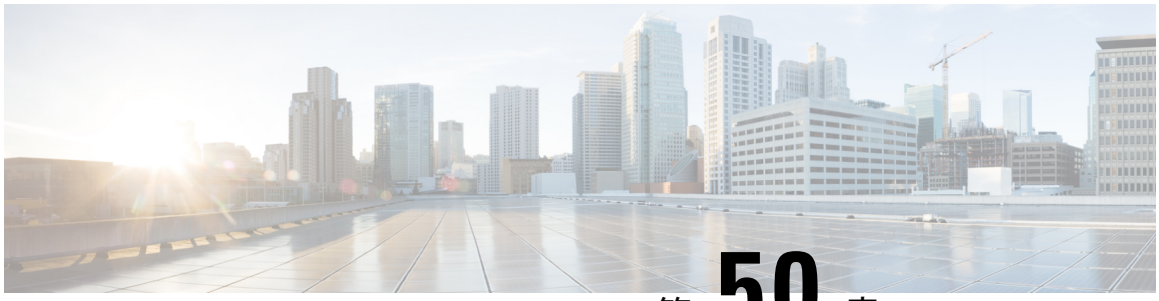
```
Handshake Success 1,
Total Packets Transmitted 1,
Total Packets Received 1,
Total Connection Resets 2,
Connection Reset due to idle timeout 0,
Connection Reset due to No Response 2,
Connection Reset due to Malformed packet 0,
```

RADIUS DTLS 固有の統計情報のクリア

Radius DTLS 固有の統計情報をクリアするには、次のコマンドを使用します。

```
Device# clear aaa counters servers radius {<server-id> | all}
```

（注） *server-id* は、**show aaa servers** によって表示されるサーバー ID を指します。0 ～ 2147483647 の範囲の値を指定できます。



第 50 章

MAC 認証バイパス

MAC 認証バイパス

MAC 認証バイパス（MAB）機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するように 組み込みワイヤレスコントローラを設定できます。

MAB を有効にすると、 組み込みワイヤレスコントローラはクライアント ID として MAC アドレスを使用します。認証サーバーには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。クライアントの検出後、組み込みワイヤレスコントローラはクライアントからのパケットを待機します。 組み込みワイヤレスコントローラは、MAC アドレスに基づくユーザー名とパスワードを含む RADIUS アクセス/要求フレームを認証サーバーに送信します。認証が成功すると、 組み込みワイヤレスコントローラはクライアントにネットワークへのアクセス権を付与します。認証が失敗した場合、ゲスト WLAN が設定されていれば、 組み込みワイヤレスコントローラはゲスト WLAN にポートを割り当てます。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、認証されたクライアントの場合と同じです。再認証の間、ポートは前に割り当てられた WLAN のままです。再認証が成功すると、 組み込みワイヤレスコントローラは同じ WLAN でポートを保持します。再認証が失敗した場合、ゲスト WLAN が設定されていれば、 組み込みワイヤレスコントローラはゲスト WLAN にポートを割り当てます。

MAB の設定に関する注意事項

- MAB の設定に関する注意事項は、802.1x 認証の注意事項と同じです。
- MAC アドレスで認可された後にポートで MAB を無効にしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバーデータベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAB によって接続されているにもかかわらず非アクティブなホストのタイムアウト時間を設定できます。有効な範囲は 1 ～ 65535 秒です。

（注） ユーザーに対して wlan-profile-name が設定されている場合、ゲストユーザー認証はその WLAN からのみ許可されます。

ユーザーに対して wlan-profile-name が設定されていない場合、すべての WLAN でゲストユーザー認証が許可されます。

クライアントを SSID1 に接続するが、MAC フィルタリングを使用して SSID2 には接続しない場合は、ポリシープロファイルで aaa-override を設定してください。

次の例では、MAC アドレスが 1122.3344.0001 のクライアントが WLAN に接続しようとすると、要求がローカル RADIUS サーバーに送信され、属性リスト（FILTER_1 および FILTER_2）にクライアントの MAC アドレスが存在するかどうかがチェックされます。クライアントの MAC アドレスが属性リスト（FILTER_1）にリストされている場合、クライアントは、RADIUS サーバーから ssid 属性として返される WLAN（WLAN_1）に接続できます。クライアントの MAC アドレスが属性リストにリストされていない場合、そのクライアントは拒否されます。

ローカル RADIUS サーバーの設定

```
!Configures an attribute list as FILTER_2
aaa attribute list FILTER_2
!Defines an attribute type that is to be added to an attribute list.
attribute type ssid "WLAN_2"

!Username with the MAC address is added to the filter
username 1122.3344.0002 mac aaa attribute list FILTER_2

!
aaa attribute list FILTER_1
attribute type ssid "WLAN_1"
username 1122.3344.0001 mac aaa attribute list FILTER_1
```

Controller Configuration

```
! Sets authorization to the local radius server
aaa authorization network MLIST_MACFILTER local
```

```
!A WLAN with the SSID WLAN_2 is created and MAC filtering is set along with security
parameters.
wlan WLAN_2 2 WLAN_2
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers

!WLAN with the SSID WLAN_1 is created and MAC filtering is set along with security
parameters.
wlan WLAN_1 1 WLAN_1
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list WEBAUTH

! Policy profile to be associated with the above WLANs
wireless profile policy MAC_FILTER_POLICY
aaa-override
vlan 504
no shutdown
```

WLAN の 802.11 セキュリティの設定（GUI）

手順

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

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 [Security] タブで次の設定を行えます。

- レイヤ 2
- Layer3
- AAA

ステップ 4 [Layer2] タブで次の設定を行えます。

a) [Layer2 Security Mode] を次のオプションから選択します。

- [None]：レイヤ 2 セキュリティなし。
- [WPA + WPA2]：Wi-Fi Protected Access。
- Static WEP：静的 WEP 暗号化パラメータ。

b) 必要に応じて、[MAC Filtering] を有効にしますMAC フィルタリングは、MAC 認証バイパス（MAB）とも呼ばれます。

c) [Protected Management Frame] セクションの [PMF] で、[Disabled]、[Optional]、または [Required] を選択します。デフォルトでは、PMF は無効になっています。
d) [WPA Parameters] セクションで、必要に応じて次のオプションを選択します。
   - WPA Policy
   - WPA2 Policy
   - WPA2 Encryption
e) [Auth Key Mgmt] のオプションを選択します。
f) AP 間の [Fast Transition] の適切なステータスを選択します。
g) 分散システム経由の高速移行を有効にするには、[Over the DS] チェック ボックスをオンにします。
h) [Reassociation Timeout] の値（秒単位）を入力します。これは、高速移行の再アソシエーションがタイムアウトするまでの時間です。
i) [Save & Apply to Device] をクリックします。

ステップ 5 [Layer3] タブで次の設定を行えます。
a) Web ポリシーを使用するには、[Web Policy] チェック ボックスをオンにします。
b) 必要な [Webauth Parameter Map] 値をドロップダウンリストから選択します。
c) 必要な [Authentication List] 値をドロップダウンリストから選択します。
d) [Show Advanced Settings] セクションで、[On Mac Filter Failure] チェック ボックスをオンにします。
e) [Conditional Web Redirect] と [Splash Web Redirect] を有効にします。
f) ドロップダウンリストから適切な IPv4 および IPv6 ACL を選択します。
g) [Save & Apply to Device] をクリックします。

ステップ 6 [AAA] タブで次の設定を行えます。
a) ドロップダウンから認証リストを選択します。
b) WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボックスをオンにします。また、必要な [EAP Profile Name] をドロップダウンリストから選択します。
c) [Save & Apply to Device] をクリックします。

WLAN の 802.11 セキュリティの設定（CLI）

WLAN の 802.11 セキュリティを設定するには、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	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan ha-wlan-dot1x-test 3 ha-wlan-dot1x-test`	WLAN プロファイルを設定します。
ステップ 2	**security dot1x authentication-list** *auth-list-name* 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

外部認証用の AAA の設定

外部認証用に AAA 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	**radius server** *server-name* 例： `Device(config)# radius server ISE`	Radius サーバーを設定します。
ステップ 2	**address** {**ipv4** | **ipv6**}*radius-server-ip-address* **auth-port** *auth-port-no* **acct-port** *acct-port-no* 例： `Device(config-radius-server)# address ipv4 9.2.58.90 auth-port 1812 acct-port 1813`	Radius サーバーのアドレスを指定します。
ステップ 3	**key** *key* 例： `Device(config-radius-server)# key any123`	サーバーごとの暗号キーを設定します。
ステップ 4	**exit** 例：	コンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-locsvr-da-radius)# exit`	
ステップ 5	**aaa local authentication default authorization default** 例： `Device(config)# aaa local authentication default authorization default`	デフォルトのローカル認証および許可を選択します。
ステップ 6	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA認証モデルを作成します。新しいアクセス制御コマンドと機能を有効にします。
ステップ 7	**aaa session-id common** 例： `Device(config)# aaa session-id common`	コモン セッション ID を作成します。
ステップ 8	**aaa authentication dot1x default group radius** 例： `Device(config)# aaa authentication dot1x default group radius`	デフォルトの dot1x 方式の認証を設定します。 .
ステップ 9	**aaa authorization network default group radius** 例： `Device(config)# aaa authorization network default group radius`	ネットワークサービスに対する認証を設定します。
ステップ 10	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	SysAuthControl を有効にします。

ローカル認証用の AAA の設定（GUI）

手順

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

ステップ 2 [Wireless Networks] ページで [Add] をクリックします。

ステップ 3 表示される [Add WLAN] ウィンドウで、**[Security]** > **[AAA]** を選択します。

ステップ 4 [Authentication List] ドロップダウンから値を選択します。

ステップ 5 WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボックスをオンにします。

ステップ 6 [EAP Profile Name] ドロップダウンから値を選択します。

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

ローカル認証用の AAA の設定（CLI）

ローカル認証用に AAA 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	**aaa authentication dot1x default local** 例： `Device(config)# aaa authentication dot1x default local`	デフォルトのローカルRADIUSサーバーを使用するように設定します。
ステップ 2	**aaa authorization network default local** 例： `Device(config)# aaa authorization network default local`	ネットワークサービスに対する認証を設定します。
ステップ 3	**aaa authorization credential-download default local** 例： `Device(config)# aaa authorization credential-download default local`	ローカル サーバーからログイン情報をダウンロードするようにデフォルトデータベースを設定します。
ステップ 4	**username** *mac-address***mac** 例： `Device(config)# username abcdabcdabcd mac`	ユーザー名を使用したMACフィルタリングには、**username** *abcdabcdabcd* **mac** コマンドを使用します。
ステップ 5	**aaa local authentication default authorization default** 例： `Device(config)# aaa local authentication default authorization default`	ローカル認証方式リストを設定します。
ステップ 6	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。新しいアクセス制御コマンドと機能を有効にします。

	コマンドまたはアクション	目的
ステップ 7	**aaa session-id common** 例： `Device(config)# aaa session-id common`	コモン セッション ID を作成します。

ローカル認証用の MAB の設定

ローカル認証用に MAB を設定するには、次の手順に従います。

始める前に

AAA ローカル認証を設定します。

username *mac-address* **mac** コマンドを使用して、WLAN 設定（ローカル認証）のユーザー名を設定します。

（注） MAC アドレスの形式は、abcdabcdabcd にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *profile-name wlan-id* 例： `wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default`	WLAN の名前と ID を指定します。
ステップ 2	**mac-filtering default** 例： `Device(config-wlan)# mac-filtering default`	WLAN の MAC フィルタリング サポートを設定します。
ステップ 3	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**no security wpa wpa2** 例：	WPA2 セキュリティを無効にします。

	コマンドまたはアクション	目的
	`Device(config-wlan)# no security wpa wpa2`	
ステップ 6	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

外部認証用の MAB の設定（GUI）

始める前に

AAA 外部認証を設定します。

手順

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

ステップ 2 [Wireless Networks] ページで WLAN の名前をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで [Security] タブをクリックします。

ステップ 4 [Layer2] タブで、[MAC Filtering] チェック ボックスをオンにして機能を有効にします。

ステップ 5 MAC フィルタリングを有効にした状態で、ドロップダウンリストから [Authorization List] を選択します。

ステップ 6 設定を保存します。

外部認証用の MAB の設定（CLI）

外部認証用に MAB を設定するには、次の手順に従います。

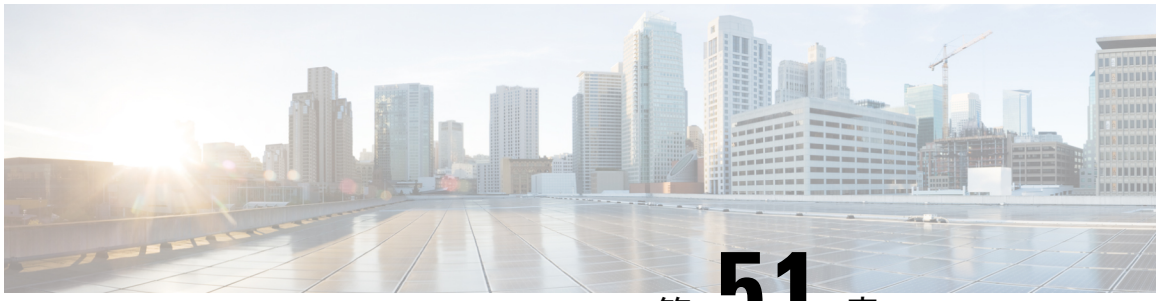
始める前に

AAA 外部認証を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *wlan-name wlan-id ssid-name* 例： `wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius`	WLAN の名前と ID を指定します。
ステップ 2	**mac-filtering** *list-name* 例： `Device(config-wlan)# mac-filtering ewlc-radius`	MAC フィルタリング パラメータを設定します。ここで、ewlc-radius は list-name の例です
ステップ 3	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 6	**mab request format attribute** {**1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** {**0** | **7** | **LINE**} **LINE** *password* | **32 vlan access-vlan**} 例： `Device(config)# mab request format attribute 1 groupsize 4 separator`	オプション。WLAN で MAC フィルタリングを使用する際のデリミタを設定します。 ここで、各変数は次のように定義されます。 **1**：MAB 要求に使用するユーザー名形式を指定します。 **groupsize** *size*：グループごとの 16 進数の桁数を指定します。有効な値の範囲は 1 ～ 12 です。 **separator** *separator*：グループを区切る方法を指定します。区切り文字は、コンマ、セミコロン、およびピリオドです。 **lowercase**：ユーザー名を小文字で指定します。

	コマンドまたはアクション	目的
		uppercase：ユーザー名を大文字で指定します。 **2**：すべてのMAB要求に使用するグローバルパスワードを指定します。 **0**：暗号化されていないパスワードを指定します。 **7**：非表示のパスワードを指定します。 **LINE**：暗号化されたパスワードまたは暗号化されていないパスワードを指定します。 *password*：回線パスワード。 **32**：NAS-Identifier 属性を指定します。 **vlan**：VLAN を指定します。 **access-vlan**：設定されたアクセス VLAN を指定します。
ステップ 7	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。



第 51 章

Dynamic Frequency Selection（動的周波数選択）

動的周波数選択について

動的周波数選択（DFS）は、レーダー信号を検出し、DFS 対応の 5.0 GHz（802.11a/h）無線の周波数を自動的に設定して、レーダー信号との干渉を回避するプロセスです。規制ドメインで使用するように設定された無線が、レーダー システムに干渉しないようにする必要があります。

通常の DFS では、レーダー信号が 40 MHz または 80 MHz 帯域幅のチャネルのいずれかで検出されると、チャネル全体がブロックされます。Flex DFS を使用すると、セカンダリ チャネルでレーダー信号が検出されていない場合は AP がセカンダリ チャネルに移動され、帯域幅が（通常は半分に）削減されます。

動的周波数選択の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 プロファイルを選択します。

ステップ 3 [General] タブで、[Full sector DFS status] チェックボックスをオンにします。

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

動的周波数選択の設定

DFS を設定するには、次の手順に従います。

始める前に

- 対応する AP が、いずれかの DFS チャネル上に存在する必要があります。
- 設定変更を適用する前に、無線をシャットダウンします。

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	**no ap dot11 5ghz dtpc** 例： `Device(config)# no ap dot11 5ghz dtpc`	802.11a ダイナミック伝送パワーコントロール（DTPC）設定を無効にします。
ステップ 3	**ap dot11 5ghz channelswitch mode** *mode-num* 例： `Device(config)# ap dot11 5ghz channelswitch mode 1`	802.11h チャネル スイッチ モードを設定します。
ステップ 4	**ap dot11 5ghz power-constraint** *value* 例： `Device(config)# ap dot11 5ghz power-constraint 12`	802.11h 電力制限値を設定します。
ステップ 5	**ap dot11 5ghz smart-dfs** 例： `Device(config)# ap dot11 5ghz smart-dfs`	レーダー干渉チャネルの非占有時間を設定します。

DFS の確認

DFS 設定を確認するには、次のコマンドを使用します。

802.11h 設定を表示するには、次のコマンドを使用します。

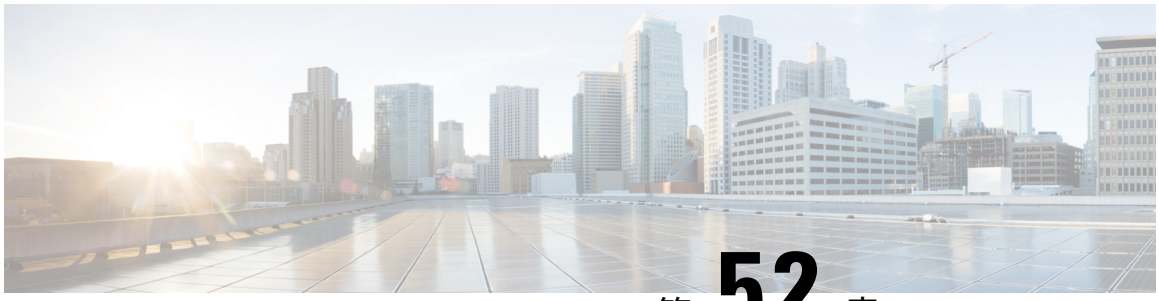
```
Device# show wireless dot11h
```

802.11h 設定の自動 RF 情報を表示するには、次のコマンドを使用します。

```
Device# show ap auto-rf dot11 5ghz
```

Cisco AP の自動 RF 情報を表示するには、次のコマンドを使用します。

```
Device# show ap name ap1 auto-rf dot11 5gh
```



第 52 章

不正なデバイスの管理

Rogue Detection

不正なデバイス

不正なアクセスポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセスポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセスポイントになりすまして、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセスポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザーがこのアクセスポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。ワイヤレス ユーザーがエンタープライズ ネットワーク内のアクセス ポイントに接続する場合、エンタープライズ セキュリティ違反が発生する可能性が高くなります。

次に、不正なデバイスの管理に関する注意事項を示します。

- アクセスポイントは、関連付けられたクライアントにサービスを提供するように設計されています。これらのアクセス ポイントは比較的短時間でオフチャネル スキャンを実行します（各チャネル約 50 ミリ秒）。大量の不正 AP とクライアントを高感度で検出する場合、モニター モード アクセス ポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 秒や 60 秒などに短縮して、無線がオフチャネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセス ポイントは引き続き各チャネル上で約 50 ミリ秒を費やします。
- 家庭環境で展開されるアクセス ポイントは多数の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出がデフォルトで無効になっています。
- クライアントカードの実装により、封じ込めの効果が低下することがあります。これは通常、「関連付け解除/認証解除」フレームを受信後、クライアントがネットワークにすぐに再接続する可能性がある場合に発生し、一部のトラフィックが引き続き通過できる可能性があります。ただし、不正なクライアントが封じ込められると、そのブラウジングエクスペリエンスに悪影響を及ぼす可能性があります。
- 不正の状態と、状態の自動的な移行を可能にするユーザー定義の分類規則を使って、不正なアクセス ポイントを分類および報告できます。
- 各コントローラは、モニターモードでの不正アクセスポイントの封じ込めを無線ごとに 3 および 6 台に制限します。
- 設定を使用して手動の阻止を実行すると、不正エントリは有効期限が切れた後でも保持されます。
- 不正エントリの有効期限が切れると、管理対象のアクセス ポイントはすべてのアクティブな封じ込めを停止するように指示されます。
- [Validate Rogue Clients Against AAA] が有効になっている場合、コントローラは一度だけ不正なクライアントの検証を AAA サーバーに要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[Validate Rogue Clients Against AAA] を有効にする前に、認証サーバーに有効なクライアント エントリを追加します。

不正検出の制約事項

- 不正な封じ込めは DFS チャネルではサポートされていません。

不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセス ポイントを選択し、そのアクセス ポイントに情報を提供します。アクセスポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、モニター モードのアクセス ポイントだけを使用するようにコントローラを設定できます。阻止動作は次の 2 つの方法で開始されます。

- コンテナ アクセス ポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセスポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。

• 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャスト アソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

17.7.1 リリース以降、Beacon DS Attack および Beacon Wrong Channel シグネチャが導入されました。

[Beacon DS Attack]：管理対象 AP と不正 AP が同じ BSSID を使用している場合、不正 AP は偽装者と呼ばれます。攻撃者は、任意のチャネル番号で Direct-Sequence パラメータ セット情報要素を追加できます。追加されたチャネル番号が管理対象 AP が使用するチャネル番号と異なる場合、その攻撃は Beacon DS Attack と呼ばれます。

[Beacon Wrong Channel]：管理対象の AP と不正 AP が同じ BSSID を使用している場合、不正 AP は AP 偽装者と呼ばれます。AP 偽装者が、同じ BSSID を持つ管理対象 AP によって使用される番号とは異なるチャネル番号を使用している場合、その攻撃は Beacon Wrong Channel と呼ばれます。そのような場合、Direct-Sequence 情報要素がビーコンフレームに存在しないこともあります。

不正な封じ込めに関する情報（保護された管理フレーム（PMF）が有効）

Cisco IOS XE Amsterdam 17.3.1 以降では、802.11w 保護された管理フレーム（PMF）が有効になっている不正デバイスは含まれていません。代わりに、不正デバイスは [Contained Pending] としてマークされ、WSA アラームが発生して Contained Pending イベントに関する通知がされます。デバイスの抑制は実行されないため、アクセスポイント（AP）リソースが不必要に消費されることはありません。

（注） この機能は Wave 2 AP でのみサポートされています。

不正デバイスで PMF が有効になっているときに、show wireless wps rogue ap detailed コマンドを実行して、デバイスの抑制を確認します。

AP 偽装検出

AP 偽装の検出方法は次のとおりです。

- 管理対象 AP が AP 自体を不正であると報告した場合の AP 偽装検出。この方法は常に有効であり、設定は不要です。
- MFP に基づく AP 偽装検出。
- AP 認証に基づく AP 偽装検出。

インフラストラクチャ MFP は、クライアントではなく、AP によって送信され、ネットワーク内の他の AP によって検証される管理フレームにメッセージ整合性チェック（MIC）情報要素を追加することによって、802.11 セッション管理機能を保護します。インフラストラクチャ MFP が有効になっている場合、管理対象 AP によって、MIC 情報要素の存在の有無、MIC 情報要素が期待どおりの内容であるかがチェックされます。いずれかの条件が満たされていない

場合、管理対象 AP は、更新された AP 認証失敗カウンタを含む不正 AP レポートを送信します。

AP認証機能を使用すると、AP偽装を検出できます。この機能を有効にすると、コントローラで AP ドメインの秘密が作成され、同じネットワーク内の他の AP と共有されます。これにより、AP が相互に認証できるようになります。

AP認証情報要素は、ビーコンおよびプローブ応答フレームに添付されます。AP認証情報要素に不正な [Signature] フィールドがある場合、タイムスタンプがオフの場合、または AP 認証情報要素が欠落している場合、そのような状態を検出した AP により [AP authentication failure count] フィールドが増分されます。[AP authentication failure count] フィールドがしきい値を超えると、偽装アラームが発生します。不正 AP は、状態が [Threat] である [Malicious] として分類されます。

show wireless wps rogue ap detail コマンドを実行して、認証エラーが原因で偽装が検出された時刻を確認します。

不正検出の設定（GUI）

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 Name] をクリックして、AP 接続プロファイルのプロパティを編集します。

ステップ 3 [Edit AP Join Profile] ウィンドウで [Rogue AP] タブをクリックします。

ステップ 4 [Rogue Detection] チェックボックスをオンにして、不正 AP 検知を有効にします。

ステップ 5 [Rogue Detection Minimum RSSI] フィールドに、RSSI 値を入力します。

ステップ 6 [Rogue Detection Transient Interval] フィールドに、間隔を秒単位で入力します。

ステップ 7 [Rogue Detection Report Interval] フィールドに、レポート間隔の値を秒単位で入力します。

ステップ 8 [Rogue Detection Client Number Threshold] フィールドに、不正なクライアント検出のしきい値を入力します。

ステップ 9 [Auto Containment on FlexConnect Standalone] チェックボックスをオンにして、自動封じ込めを有効にします。

ステップ 10 [Update & Apply to Device] をクリックします。

不正検出の設定（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。

ステップ 2	**ap profile** *profile-name* **rogue detection min-transient-time** *time in seconds*
	例：
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection min-transient-time 120`
		不正が初めてスキャンされた後、AP で不正スキャンを連続的に実行する間隔を入力します。
		time in sec パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。
		（注） この機能は、すべての AP モードに適用できます。
		一時的な間隔値を使用して、APが不正をスキャンする間隔を制御できます。APでは、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。
		この機能には次のような利点があります。
		• APからコントローラへの不正レポートが短くなる
		• 一時的な不正エントリをコントローラで回避できる
		一時的な不正への不要なメモリ割り当てを回避できる

ステップ 3	**ap profile** *profile-name* **rogue detection containment** {**auto-rate** | **flex-rate**}
	例：
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection containment flex-rate`
		不正な封じ込めオプションを指定します。auto-rate オプションを指定すると、不正を封じ込めるための自動レートが有効になります。flex-rate オプションを指定すると、スタンドアロン FlexConnect

	コマンドまたはアクション	目的
		AP の不正な封じ込めが有効になります。
ステップ 4	**ap profile** *profile-name* **rogue detection enable** 例： `Device(config)# ap profile profile1`	すべての AP で不正 AP 検知を有効にします。

ステップ 5	**ap profile** *profile-name* **rogue detection report-interval** *time in seconds*
	例：
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection report-interval 120`
		モニターモードの Cisco AP に対する不正レポートの間隔を設定します。
		報告する間隔の有効な範囲（秒単位）は、10 ～ 300 秒です。

不正 AP の RSSI 偏差通知しきい値の設定（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。
ステップ 2	**wireless wps rogue ap notify-rssi-deviation** 例： `Device(config)# wireless wps rogue ap notify-rssi-deviation`	不正 AP の RSSI 偏差通知しきい値を設定します。
ステップ 3	**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。

管理フレーム保護の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] を選択します。

ステップ 2 [Rogue Policy] タブの [MFP Configuration] セクションで、[Global MFP State] チェックボックスと [AP Impersonation Detection] チェックボックスをオンにして、グローバル MFP 状態と AP 偽装検出をそれぞれ有効にします。

ステップ 3 [MFP Key Refresh Interval] フィールドで、更新間隔を時間単位で指定します。

ステップ 4 [Apply] をクリックします。

管理フレーム保護の設定（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。
ステップ 2	**wireless wps mfp** 例： `Device(config)# wireless wps mfp`	管理フレーム保護を設定します。

ステップ 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**}
	例：
	`Device(config)# wireless wps mfp ap-impersonation`
	`Device(config)# wireless wps mfp key-refresh-interval`
		AP の偽装検出（または）MFP キーの更新間隔を時単位で設定します。
		key-refresh-interval：MFP キーの更新間隔を時単位で設定します。有効な範囲は 1 ～ 24 です。デフォルト値は 24 です。

ステップ 4	**end** 例： `Device(config)# 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。

アクセスポイント認証の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wireless wps ap-authentication** 例： `Device(config)# wireless wps ap-authentication`	ワイヤレス WPS AP 認証を設定します。
ステップ 3	**wireless wps ap-authentication threshold** *threshold* 例： `Device(config)# wireless wps ap-authentication threshold 100`	AP ネイバー認証を設定し、AP 認証エラーのしきい値を設定します。
ステップ 4	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-demo 1 ssid-demo`	WLAN を設定します。
ステップ 5	**ccx aironet-iesupport** 例： `Device(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet 情報要素のサポートを有効にします。
ステップ 6	**end** 例： `Device# end`	特権 EXEC モードに戻ります。

管理フレーム保護の確認

管理フレーム保護（MFP）機能が有効かどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

MFP の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

不正検出の検証

この項では、不正検出の新しいコマンドについて説明します。

次のコマンドを使用して、デバイスでの不正 AP 検知を確認できます。

表 *24 :* アドホック不正情報の確認

コマンド	目的
show wireless wps rogue adhoc detailed *mac_address*	アドホック不正の詳細情報を表示します。
show wireless wps rogue adhoc summary	すべてのアドホック不正のリストを表示します。

表 *25 :* 不正 *AP* 情報の確認

コマンド	目的
show wireless wps rogue ap clients *mac_address*	不正に関連付けられているすべての不正クライアントのリストを表示します。
show wireless wps rogue ap custom summary	カスタム不正 AP の情報を表示します。
show wireless wps rogue ap detailed *mac_address*	不正 AP の詳細情報を表示します。
show wireless wps rogue ap friendly summary	危険性のない不正 AP の情報を表示します。
show wireless wps rogue ap list *mac_address*	特定の AP によって検出された不正 AP のリストを表示します。
show wireless wps rogue ap malicious summary	悪意のある不正 AP の情報を表示します。
show wireless wps rogue ap summary	すべての不正 AP のリストを表示します。
show wireless wps rogue ap unclassified summary	未分類の不正 AP の情報を表示します。

表 *26 :* 不正の自動封じ込めに関する情報の確認

コマンド	目的
show wireless wps rogue auto-contain	不正の自動封じ込めに関する情報を表示します。

表 *27 :* 分類ルールの情報の確認

コマンド	目的

show wireless wps rogue rule detailed *rule_name*	分類ルールの詳細情報を表示します。
show wireless wps rogue rule summary	すべての不正ルールのリストを表示します。

表 *28 :* 不正統計情報の確認

コマンド	目的
show wireless wps rogue stats	不正統計情報を表示します。

表 *29 :* 不正クライアントの情報の確認

コマンド	目的
show wireless wps rogue client detailed *mac_address*	不正クライアントの詳細情報を表示します。
show wireless wps rogue client summary	すべての不正クライアントのリストを表示します。

表 *30 :* 不正無視リストの確認

コマンド	目的
show wireless wps rogue ignore-list	不正無視リストを表示します。

例：不正検出の設定

次に、検出された不正 AP が存在する必要がある最小 RSSI を、デバイスで作成されたエントリを持つように設定する例を示します。

```
Device# wireless wps rogue ap notify-min-rssi 100
```

次に、分類インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)#
Device(config)#
Device(config)# end
Device# show wireless wps rogue client /show wireless wps rogue ap summary
```

不正ポリシーの設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [Rogue Policies] タブで、[Rogue Detection Security Level] ドロップダウンを使用してセキュリティレベルを選択します。

ステップ 3 [Expiration timeout for Rogue APs (seconds)] フィールドに、タイムアウト値を入力します。

ステップ 4 [Validate Rogue Clients against AAA] チェック ボックスをオンにして、AAA サーバーに対して不正クライアントを検証します。

ステップ 5 [Validate Rogue APs against AAA] チェック ボックスをオンにして、AAA サーバーに対して不正アクセス ポイントを検証します。

ステップ 6 [Rogue Polling Interval (seconds)] フィールドに、不正情報について AAA サーバーにポーリングする間隔を入力します。

ステップ 7 不正アドホックネットワークの検出を有効にするには、[Detect and Report Adhoc Networks] チェックボックスをオンにします。

ステップ 8 [Rogue Detection Client Number Threshold] フィールドに、SNMP トラップを生成するしきい値を入力します。

ステップ 9 [Auto Contain] セクションで、次の詳細情報を入力します。

ステップ 10 [Auto Containment Level] ドロップダウンを使用してレベルを選択します。

ステップ 11 自動封じ込めをモニター モードの AP のみに制限するには、[Auto Containment only for Monitor Mode APs] チェック ボックスをオンにします。

ステップ 12 自動封じ込めを有線の不正 AP のみに制限するには、[Rogue on Wire] チェック ボックスをオンにします。

ステップ 13 コントローラに設定されているいずれかの SSID を使用している不正 AP のみに自動封じ込めを制限するには、[Using our SSID] チェックボックスをオンにします。

ステップ 14 自動封じ込めをアドホック不正 AP のみに制限するには、[Adhoc Rogue AP] チェック ボックスをオンにします。

ステップ 15 [Apply] をクリックします。

不正ポリシーの設定（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。
ステップ 2	**wireless wps rogue ap timeout** *number of seconds* 例： `Device(config)# wireless wps rogue ap timeout 250`	不正なエントリの有効期限を秒単位で設定します。秒単位の時間の有効な範囲は 240 ～ 3600 秒です。

	コマンドまたはアクション	目的
ステップ 3	**wireless wps rogue client notify-min-rssi** *RSSI threshold* 例： `Device(config)# wireless wps rogue client notify-min-rssi -128`	不正なクライアントの最小 RSSI 通知しきい値を設定します。RSSI しきい値（dB 単位）の有効な範囲は -128 ～ -70 dB です。
ステップ 4	**wireless wps rogue client notify-min-deviation** *RSSI threshold* 例： `Device(config)# wireless wps rogue client notify-min-deviation 4`	不正なクライアントの RSSI 偏差通知しきい値を設定します。RSSI しきい値（dB 単位）の有効な範囲は 0 ～ 10 dB です。
ステップ 5	**wireless wps rogue ap aaa polling-interval** *AP AAA Interval* 例： `Device(config)# wireless wps rogue ap aaa polling-interval 120`	不正 AP AAA 検証間隔を設定します。AP AAA 間隔の有効な範囲（秒単位）は 60 ～ 86400 秒です。
ステップ 6	**wireless wps rogue adhoc** 例： `Device(config)# wireless wps rogue adhoc`	アドホック不正（IBSS）の検出とレポートを有効にします。
ステップ 7	**wireless wps rogue client client-threshold** *threshold* 例： `Device(config)# wireless wps rogue client client-threshold 100`	不正 AP SNMP トラップしきい値ごとに不正なクライアントを設定します。しきい値の有効な範囲は 0 ～ 256 です。

Rogue Location Discovery Protocol（RLDP）

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモードは、デフォルトで無効になっており、不正チャネルに移動して、クライアントとして不正に接続するようにアクティブ AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、不正 AP が RLDP 機能を使用して有線ネットワークで検出されたことをネットワーク管

理者に通知するためのアラームが設定されます。RLDP の不正 AP の検出精度は 100% です。オープン AP と NAT AP を検出します。

RLDP を管理するためのガイドラインの一部を次に示します。

- Rogue Location Discovery Protocol（RLDP）は、オープン認証に設定されている不正なアクセス ポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier（BSSID）を使用する不正なアクセス ポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセス ポイント）を検出します。
- RLDP は、同じネットワークにある不正なアクセス ポイントのみを検出します。ネットワークのアクセスリストによって不正なアクセスポイントから組み込みワイヤレスコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。
- RLDP は 5 GHz の動的周波数選択（DFS）チャネルでは機能しません。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションは組み込みワイヤレスコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP がモニター モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。

次の手順では、RLDP の機能について説明します。

1. 信号強度値を使用して不正に最も近い統合 AP を特定します。
2. その後で、この AP が WLAN クライアントとして不正に接続します。3 回のアソシエーションを試みて、成功しない場合はタイムアウトします。
3. アソシエーションが成功すると、AP が DHCP を使用して IP アドレスを取得します。
4. IP アドレスが取得されると、AP（WLAN クライアントとして機能している）は、 組み込みワイヤレスコントローラのそれぞれの IP アドレスに UDP パケットを送信します。
5. 組み込みワイヤレスコントローラがクライアントから RLDP パケットを 1 つでも受信すると、その不正が on-wire としてマークされます。

（注） 組み込みワイヤレスコントローラのネットワークと不正デバイスが設置されたネットワークの間にフィルタリングルールが設定されている場合は、RLDPパケットが組み込みワイヤレスコントローラに到達できません。

組み込みワイヤレスコントローラは、すべての近隣のアクセスポイントを継続的に監視し、不正なアクセスポイントおよびクライアントに関する情報を自動的に検出して収集します。組み込みワイヤレスコントローラは、不正アクセスポイントを検出すると、Rogue Location Discovery

Protocol（RLDP）を使用し、その不正アクセスポイントがネットワークに接続されているかどうかを判断します。

組み込みワイヤレスコントローラは、オープンの不正デバイスで RLDP を開始します。RLDP が FlexConnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDPのサイクルが終了すると、クライアントはアクセスポイントに再接続します。不正アクセスポイントが検出された時点で、RLDPプロセスが開始されます。

すべてのアクセスポイントで、または監視（リッスン専用）モードに設定されたアクセスポイントでのみ、RLDPを使用するように、組み込みワイヤレスコントローラを設定できます。後者のオプションでは、混雑した無線周波数（RF）空間での自動不正アクセス ポイント検出が実現され、不要な干渉を生じさせたり、正規のデータ アクセス ポイント機能に影響を与えずにモニターリングを実行できます。すべてのアクセスポイントで RLDP を使用するように 組み込みワイヤレスコントローラを設定していて、モニターアクセスポイントとローカル（データ）アクセスポイントの両方が近くにある場合、 組み込みワイヤレスコントローラは常に RLDP 動作に対してモニターアクセスポイントを選択します。ネットワーク上に不正があると RLDP が判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDPは、オープン認証に設定されている不正なアクセスポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行回数は、を使用して設定できます。

3 つの方法で 組み込みワイヤレスコントローラから RLDP を開始またはトリガーできます。

1. 組み込みワイヤレスコントローラの CLI から RLDP 開始コマンドを手動で入力します。
2. 組み込みワイヤレスコントローラ CLI から RLDP をスケジュールします。
3. 自動 RLDP。 組み込みワイヤレスコントローラの CLI または GUI のどちらからでも 組み込みワイヤレスコントローラの自動 RLDP を設定できますが、次の注意事項を考慮してください。
   - 不正検出のセキュリティ レベルが custom に設定されている場合にのみ、自動 RLDP オプションを設定できます。
   - 自動 RLDP および RLDP のスケジュールを同時に有効にすることはできません。

RLDP の制約事項

- RLDP は、認証と暗号化が無効になっている SSID をブロードキャストするオープン不正 AP でのみ動作します。
- RLDP では、クライアントとして機能しているマネージド AP が不正ネットワーク上で DHCP を介して IP アドレスを取得できる必要があります。
- 手動 RLDP を使用して、不正上で RLDP トレースを複数回試すことができます。
- RLDP プロセス中は、AP がクライアントにサービスを提供できません。これがローカル モード AP のパフォーマンスと接続に悪影響を及ぼします。この問題を回避するために、RLDP はモニター モード AP に対してのみ選択的に有効にできます。

- RLDP は、5GHz DFS チャネルで動作する不正 AP への接続は試行しません。
- RLDP は、Cisco IOS AP でのみサポートされています。

アラームを生成する RLDP の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [RLDP] タブで、[Rogue Location Discovery Protocol] ドロップダウンリストを使用して、次のいずれかのオプションを選択します。

a) [Disable]：すべてのアクセスポイントで RLDP を無効にします。[Disable] がデフォルトオプションです。

b) [All APs]：すべての AP で RLDP を有効にします。

c) [Monitor Mode APs]：モニターモードの AP でのみ RLDP を有効にします。

（注） [Schedule RLDP] チェックボックスは、[Disable] オプションが選択されている場合にのみ有効になります。[All APs] オプションまたは [Monitor Mode APs] オプションを選択すると、[Schedule RLDP] チェックボックスは無効のままになります。

ステップ 3 [Retry Count] フィールドで、試行する再試行の回数を指定します。許可される範囲は 1 ～ 5 です。

ステップ 4 [Apply] をクリックします。

アラームを生成する RLDP 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。

ステップ 2	**wireless wps rogue ap rldp alarm-only <monitor-ap-only>**
	例：
	`Device(config)# wireless wps rogue ap rldp alarm-only`
	`Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only`
		RLDP でアラームを生成できるようにします。この方法では、RLDP は常に有効になります。
		monitor-ap-only キーワードはオプションです。

	コマンドまたはアクション	目的
		alarm-only キーワードのみを指定してコマンドを実行すると、AP モードの制限なしで RLDP が有効になります。 **alarm-only <monitor-ap-only>** キーワードを指定してコマンドを実行すると、モニター モードのアクセス ポイントでのみ RLDP が有効になります。
ステップ 3	**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。

RLDP のスケジュールの設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [RLDP] タブで、[Rogue Location Discovery Protocol] ドロップダウンリストから次のオプションを選択します。

- [Disable]（デフォルト）：すべてのアクセスポイントで RLDP を無効にします。

ステップ 3 [Retry Count] フィールドで、試行する再試行の回数を指定します。有効な範囲（1 ～ 5）を指定してください、

ステップ 4 [Schedule RLDP] チェックボックスをオンにして、プロセスを実行する曜日、開始時刻、終了時刻を指定します。

ステップ 5 [Apply] をクリックします。

RLDP のスケジュールの設定（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 wps rogue ap rldp schedule day** *day* **start** *start-time* **end** *end-time* 例： `Device(config)# wireless wps rogue ap rldp schedule day Monday start 10:10:01 end 12:00:00`	スケジュール設定された曜日、開始時刻、終了時刻に基づいてRLDPを有効にします。 ここで、各変数は次のように定義されます。 *day* は、RLDP のスケジューリングを実行できる曜日です。値は Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday です。 *start-time* は、RLDP のスケジューリングの開始時刻です。開始時刻は **HH:MM:SS** 形式で入力する必要があります。 *end time* は、RLDP のスケジューリングの終了時刻です。終了時刻は **HH:MM:SS** 形式で入力する必要があります。
ステップ 3	**wireless wps rogue ap rldp schedule** 例： `Device(config)# wireless wps rogue ap rldp schedule`	スケジュールを有効にします。
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。

自動封じ込め用の RLDP の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [Rogue Policies] タブの [Auto Contain] セクションで、[Rogue on Wire] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックします。

自動封じ込め用の RLDP 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。

ステップ 2	**wireless wps rogue ap rldp auto-contain** [**monitor-ap-only**]
	例：
	`デバイス(config)# wireless wps rogue ap rldp auto-contain`
	`デバイス(config)# wireless wps rogue ap rldp auto-contain monitor-ap-only`
		RLDP で自動封じ込めを実行できるようにします。この方法では、RLDP は常に有効になります。
		monitor-ap-only キーワードはオプションです。
		auto-contain キーワードのみを指定してコマンドを実行すると、AP モードの制限なしで RLDP が有効になります。
		auto-contain <monitor-ap-only> キーワードを指定してコマンドを実行すると、モニター モードのアクセス ポイントでのみ RLDP が有効になります。

ステップ 3	**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。

不正アクセス ポイントでの RLDP 再試行回数の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** を選択します。

ステップ 2 [Wireless Protection Policies] ページで [RLDP] タブをクリックします。

ステップ 3 [Retry Count] フィールドに、不正アクセス ポイントの RLDP 再試行の値を入力します。

有効な範囲は 1 ～ 5 です。

ステップ 4 設定を保存します。

不正アクセス ポイントでの RLDP 再試行回数の設定（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。
ステップ 2	**wireless wps rogue ap rldp retries** *num-entries* 例： `Device(config)# wireless wps rogue ap rldp retries 2`	不正アクセス ポイントでの RLDP 再試行回数を有効にします。 *num-entries* は、不正アクセス ポイントごとの RLDP 再試行回数です。 有効な範囲は 1 ～ 5 です。
ステップ 3	**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。

不正 AP RLDP の確認

次のコマンドを使用して、不正 AP RLDP を確認できます。

表 *31* : 不正 *AP* 情報の確認

コマンド	目的
show wireless wps rogue ap rldp detailed *mac_address*	不正 AP の RLDP の詳細を表示します。
show wireless wps rogue ap rldp in progress	進行中の RLDP のリストを表示します。
show wireless wps rogue ap rldp summary	RLDP スケジューリング情報の要約を表示します。

不正検出セキュリティ レベル

不正検出セキュリティ レベルの設定を使用して、不正検出パラメータを設定できます。

使用可能なセキュリティ レベルは次のとおりです。

- Critical：機密性の高い展開向けの基本不正検出。

- High：中規模な展開向けの基本不正検出。
- Low：小規模な展開向けの基本不正検出。
- Custom：デフォルトのセキュリティレベル（すべての検出パラメータが設定可能）。

（注） Critical、High、または Low の場合、一部の不正パラメータは固定されており、設定できません。

次の表に、事前に定義された 3 つのレベルについてパラメータの詳細を示します。

表 *32*：不正検出：事前に定義されたレベル

パラメータ	Critical	High	Low
クリーンアップ タイマー	3600	1200	240
AAA 検証クライアント	ディセーブル	ディセーブル	ディセーブル
アドホック レポート	イネーブル	イネーブル	イネーブル
モニターモードレポート間隔	10 秒	30 秒	60 秒
最小 RSSI	-128 dBm	-80 dBm	-80 dBm
一時間隔	600 秒	300 秒	120 秒
自動封じ込め モニター モードの AP でのみ動作します。	ディセーブル	ディセーブル	ディセーブル
自動封じ込めレベル	1	1	1
同じ SSID の自動封じ込め	ディセーブル	ディセーブル	ディセーブル
不正 AP 上の有効なクライアントの自動封じ込め	ディセーブル	ディセーブル	ディセーブル
アドホックの自動封じ込め	ディセーブル	ディセーブル	ディセーブル
封じ込め自動レート	イネーブル	イネーブル	イネーブル

パラメータ	Critical	High	Low
CMX によるクライアントの検証	イネーブル	イネーブル	イネーブル
封じ込め FlexConnect	イネーブル	イネーブル	イネーブル
RLDP	RLDP スケジューリングが無効になっている場合は、モニター AP。	RLDP スケジューリングが無効になっている場合は、モニター AP。	ディセーブル
RLDP の自動封じ込め	ディセーブル	ディセーブル	ディセーブル

不正検出セキュリティレベルの設定

不正検出セキュリティレベルを設定するには、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 wps rogue security-level custom** **例：** `Device(config)# wireless wps rogue security-level custom`	不正検出セキュリティ レベルを「カスタム」に設定します。
ステップ 3	**wireless wps rogue security-level low** **例：** `Device(config)# wireless wps rogue security-level low`	小規模展開向けの基本不正検出を設定するための不正検出セキュリティ レベルを設定します。
ステップ 4	**wireless wps rogue security-level high** **例：** `Device(config)# wireless wps rogue security-level high`	中規模展開向けの不正検出を設定するための不正検出セキュリティ レベルを設定します。
ステップ 5	**wireless wps rogue security-level critical** **例：** `Device(config)# wireless wps rogue security-level critical`	機密性の高い展開向けの不正検出を設定するための不正検出セキュリティ レベルを設定します。

Wireless Service Assurance 不正イベント

リリース 16.12.x 以降のリリースでサポートされている Wireless Service Assurance（WSA）不正イベントは、SNMP トラップのサブセットに対応したテレメトリ通知で構成されています。WSA 不正イベントは、対応する SNMP トラップの一部となっている同じ情報を複製します。

エクスポートされたすべてのイベントについて、次の詳細が Wireless Service Assurance（WSA）インフラストラクチャに提供されます。

- 不正 AP の MAC アドレス
- 最も強力な RSSI で不正 AP を検出した管理対象 AP と無線の詳細
- イベント固有のデータ（SSID、潜在的なハニーポットイベントのチャネル、偽装イベント用偽装 AP の MAC アドレスなど）

WSA 不正イベント機能は、サポートされる AP の最大数の 4 倍まで、およびサポートされるクライアントの最大数の半分まで拡張できます。

WSA 不正イベント機能は、Cisco DNA Center およびその他のサードパーティ インフラストラクチャでサポートされています。

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	**network-assurance enable** 例： `Device# network-assurance enable`	Wireless Service Assurance を有効にします。
ステップ 3	**wireless wps rogue network-assurance enable** 例： `Device# wireless wps rogue network-assurance enable`	不正デバイスに対する Wireless Service Assurance を有効にします。これにより、WSA 不正イベントがイベント キューに送信されます。

Wireless Service Assurance 不正イベントのモニターリング

手順

- **show wireless wps rogue stats**

  例：

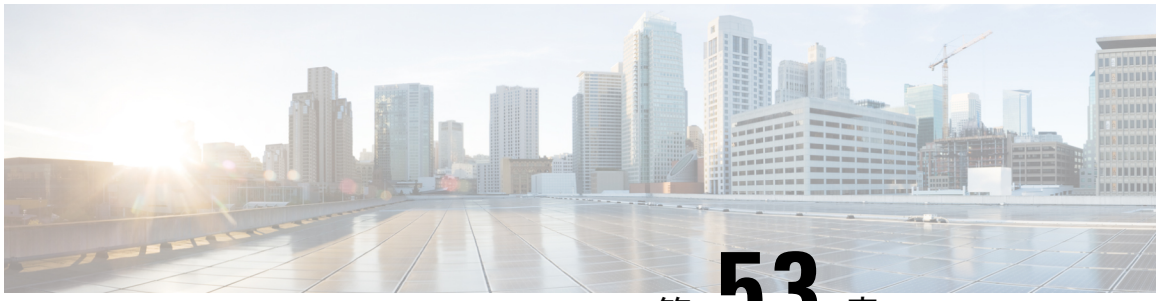
```
Device# show wireless wps rogue stats

WSA Events
  Total WSA Events Triggered            : 9
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 2
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 3
    ROGUE_AP_IMPERSONATION_DETECTED     : 4
  Total WSA Events Enqueued             : 6
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 1
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 2
    ROGUE_AP_IMPERSONATION_DETECTED     : 3
```

この例では、9 つのイベントがトリガーされていますが、そのうちの 6 つだけがキューに入れられています。これは、WSA 不正機能が有効になる前に 3 つのイベントがトリガーされたためです。

- **show wireless wps rogue stats internal**

  show wireless wps rogue ap detailed *rogue-ap-mac-addr*

  これらのコマンドは、WSA イベントに関連する情報をイベント履歴に表示します。



第 53 章

不正なアクセス ポイントの分類

不正なアクセス ポイントの分類について

組み込みワイヤレスコントローラソフトウェアでは、不正なアクセスポイントを Friendly、Malicious、または Unclassified に分類して表示するルールを作成できます。

デフォルトでは、いずれの分類ルールも使用されません。ルールを有効にする必要があります。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成または変更し、条件を設定して有効にすると、すべての不正アクセス ポイントが再分類されます。ルールを変更するたびに、すべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にルールが適用されます。

（注）

- ルールベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。
- 組み込みワイヤレスコントローラごとに最大 64 個の不正分類ルールを設定できます。

組み込みワイヤレスコントローラは、管理対象のアクセスポイントの 1 つから不正レポートを受信すると、次のように応答します。

- 不明なアクセスポイントが危険性のない MAC アドレスのリストに含まれている場合、組み込みワイヤレスコントローラはそのアクセスポイントを Friendly に分類します。
- 不明なアクセスポイントが危険性のない MAC アドレスのリストに含まれていない場合、組み込みワイヤレスコントローラはそのアクセスポイントに対して不正分類ルールの適用を開始します。

-
- 設定されているルールの条件に不正アクセスポイントが一致すると、組み込みワイヤレスコントローラはそのルールに設定された分類タイプに基づいて不正を分類します。
- 設定されたルールのいずれにも不正アクセスポイントが一致しない場合、不正はUnclassifiedのままになります。

  組み込みワイヤレスコントローラは、すべての不正アクセスポイントに対して上記の手順を繰り返します。
- 不正アクセスポイントが同じ有線ネットワーク上で検出されると、ルールが設定されていなくても、 組み込みワイヤレスコントローラは不正の状態を Threat とマークし、そのアクセスポイントを自動的に Malicious に分類します。その後は、不正を手動で封じ込めて不正の状態を Contained に変更できます。不正アクセスポイントがネットワーク上で使用不可能な場合、 組み込みワイヤレスコントローラは不正の状態を Alert としてマークします。その後は、不正を手動で封じ込めることができます。
- 必要に応じて、各アクセスポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

表 *33*：分類マッピング

ルール ベースの分類タイプ	不正の状態
Friendly	• Internal：不明なアクセス ポイントが WLAN のセキュリティに脅威を与えない場合は、手動で Friendly、Internal に設定できます。たとえば、ラボ ネットワーク内のアクセス ポイントがこれに該当します。 • External：ネットワーク内に存在する不明なアクセスポイントがWLANのセキュリティに脅威を与えない場合は、手動でFriendly、Externalに設定できます。たとえば、隣接するコーヒー ショップのアクセス ポイントがこれに該当します。 • Alert：
Malicious	• Alert： • Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
Unclassified	• Alert： • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。

前述したように、ユーザー定義のルールに基づいて、未知のアクセスポイントの分類タイプと不正の状態を組み込みワイヤレスコントローラで自動的に変更できます。または、手動で未知のアクセス ポイントを別の分類タイプや不正の状態に移行させることも可能です。

不正アクセスポイントの分類に関する注意事項と制約事項

- カスタムタイプの不正の分類は、不正ルールに関連付けられています。このため、不正を手動で Custom として分類することはできません。カスタム クラスの変更は、不正ルールが使用されている場合にのみ行われます。
- 一部の は、不正分類の変更に対して、ルールによって 30 分ごとに封じ込めのために送信されます。
- 不正ルールは、優先順位に従って、組み込みワイヤレスコントローラ内のすべての新しい着信不正レポートに適用されます。
- 不正がのルールを満たし、分類されると、同じレポートの優先順位リスト内で下位に下がることはありません。
- 不正 AP が Friendly に分類される
- コントローラが AP からのネイバーレポートを介してすべての AP を検出するまで、不正 AP は検出後から 3 分間、未設定状態に維持されます。3 分後、不正ポリシーが不正 AP に適用され、AP は、Unclassified、Friendly、Malicious、またはカスタムクラスに移動されます。未設定状態のままになっている不正 AP は、不正ポリシーがまだ適用されていないことを意味します。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの封じ込めのために不正な BSSID が送信された場合、コントローラに十分なリソースがある場合は封じ込められます。特定の封じ込まれた不正 AP を検出した AP は、DEAUTH パケットのブロードキャストを開始します。

  封じ込まれた不正な BSSID に接続されているワイヤレスクライアントは、DEAUTH パケットを受信すると切断されます。ただし、クライアントが接続状態にあると想定すると、再接続が繰り返し試行され、ワイヤレスクライアントのユーザー ブラウジング エクスペリエンスが悪影響を受けます。

  また、スタジアムのような高 RF 環境では、DEAUTH パケットがブロードキャストされますが、クライアントは RF 妨害のためにすべてのパケットを受信できません。このシナリオでは、クライアントが完全に切断されていない可能性がありますが、深刻な影響を受けます。

不正なアクセス ポイントの分類方法

不正アクセス ポイントおよびクライアントの手動による分類（GUI）

手順

ステップ 1 [Monitoring] > [Wireless] > [Rogues] の順に選択します。
ステップ 2 [Unclassified] タブで AP を選択し、下部のペインに詳細を表示します。
ステップ 3 [Class Type] ドロップダウンを使用して、ステータスを設定します。
ステップ 4 [Apply] をクリックします。

不正アクセス ポイントおよびクライアントの手動による分類（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。
ステップ 2	**wireless wps rogue adhoc** { **alert** *mac-addr* | **auto-contain** | **contain** *mac-addr containment-level* | **internal** *mac-addr* | **external** *mac-addr*} 例： `Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520`	アドホック不正を検出して報告します。 **adhoc** キーワードの後に、次のいずれかのオプションを入力します。 • **alert**：アドホック不正アクセス ポイントをアラート モードに設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。 • **auto-contain**：アドホック不正の自動的な封じ込めを自動封じ込めモードに設定します。 • **contain**：アドホック不正アクセス ポイントの封じ込めを封じ込めモードに設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力し、

	コマンドまたはアクション	目的
		containment-level パラメータに封じ込めレベルを入力します。*containment-level* の有効な範囲は 1 ～ 4 です。 • **external**：アドホック不正アクセス ポイントを **external** に設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。 • **internal**：アドホック不正アクセス ポイントを **internal** に設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。
ステップ 3	**wireless wps rogue ap** { **friendly** *mac-addr* **state** [**external** | **internal**] | **malicious** *mac-addr* **state** [**alert** | **contain** *containment-level*]} 例： `Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3`	不正アクセス ポイントを設定します。 **ap** キーワードの後に、次のいずれかのオプションを入力します。 • **friendly**：危険性のない不正アクセス ポイントを設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。その後、**state** キーワードに続けて **internal** または **external** のいずれかのオプションを入力します。**internal** オプションを選択した場合は、外部アクセス ポイントを信頼していることを示します。**external** オプションを選択した場合は、不正アクセス ポイントの存在を認識していることを示します。 • **malicious**：悪意のある不正アクセス ポイントを設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。その後、**state** キーワードに続けて **alert** または **contain** のいずれかのオプションを入力します。

	コマンドまたはアクション	目的
		• **alert**：悪意のある不正アクセス ポイントを**アラート** モードに設定します。 • **contain**：悪意のある不正アクセス ポイントを**封じ込め**モードに設定します。このオプションを選択した場合は、*containment-level* パラメータに封じ込めレベルを入力します。有効な範囲は 1 ～ 4 です。
ステップ 4	**wireless wps rogue client** { **contain** *mac-addr containment-level*} 例： `Device(config)# wireless wps rogue client contain 74a0.2f45.c520 2`	不正クライアントを設定します。 **client** キーワードの後に次のオプションを入力します。 **contain**：不正クライアントを封じ込めます。このオプションを選択した後は、*mac-addr* パラメータに MAC アドレスを入力し、*containment-level* パラメータに封じ込めレベルを入力します。*containment-level* の有効な範囲は 1 ～ 4 です。
ステップ 5	**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。

不正分類ルールの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** を選択します。

ステップ 2 [Wireless Protection Policies] ページで [Rogue AP Rules] タブを選択します。

ステップ 3 [Rogue AP Rules] ページで、**ルール**の名前をクリックするか、[Add] をクリックして新しいルールを作成します。

ステップ 4 表示される [Add/Edit Rogue AP Rule] ウィンドウで、[Rule Name] フィールドにルールの名前を入力します。

ステップ 5 次の [Rule Type] ドロップダウンリストのオプションからルール タイプを選択します。

- Friendly

- Malicious
- Unclassified
- Custom

不正分類ルールの設定（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。
ステップ 2	**wireless wps rogue rule** *rule-name* **priority** *priority* 例： `Device(config)# wireless wps rogue rule rule_3 priority 3`	ルールを作成またはイネーブルにします。ルールの作成時にルールのプライオリティを入力する必要があります。 （注） ルールの作成後に編集およびプライオリティの変更が可能なのは、無効になっている不正ルールのみです。有効になっている不正ルールのプライオリティは変更できません。編集時の不正ルールのプライオリティ変更は任意です。

ステップ 3	**classify** {**friendly state** {**alert** | **external** | **internal**} | **malicious state** {**alert** | **contained** }}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# classify friendly`
		• **friendly**：危険性のない不正アクセス ポイントを設定します。その後、**state** キーワードに続けて、**alert**、**internal**、または **external** のいずれかのオプションを入力します。**internal** オプションを選択した場合は、外部アクセスポイントを信頼していることを示します。**external** オプションを選択した場合は、不正アクセスポイントの存在を認識していることを示します。
		• **malicious**：悪意のある不正アクセス ポイントを設定します。その

	コマンドまたはアクション	目的
		後、state キーワードに続けて alert または contained のいずれかのオプションを入力します。 • alert：悪意のある不正アクセスポイントをアラートモードに設定します。 • contained：悪意のある不正アクセスポイントを封じ込めモードに設定します。

ステップ 4	**condition** {**client-count** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# condition client-count 5`
		不正アクセスポイントが満たす必要がある次の条件をルールに追加します。
		• **client-count**：不正アクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正アクセスポイントに関連付けられているクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、不正アクセスポイントに関連付けられるクライアントの最小数をパラメータに入力します。有効な範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。
		• **duration**：不正アクセス ポイントが最小期間で検出される必要があります。このオプションを選択する場合は、パラメータに最小検出期間の値を入力します。有効な範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。
		• **encryption**：アドバタイズされた WLAN で暗号化が無効になっている必要があります。任意のタイプの暗号化には any、暗号化なしの場合は off、WPA 暗号化の場合は wpa1、WPA2 暗号化の場合は wpa2、WPA3 OWE 暗号化の場合

	コマンドまたはアクション	目的
		はwpa3-owe、WPA3 SAE暗号化の場合はwpa3-saeを選択できます。 • **infrastructure**：SSIDがコントローラで認識される必要があります。 • **rssi**：有効な範囲は-95 ～ -50 dBm（両端の値を含む）です。 • **ssid**：不正アクセスポイントには、特定のSSIDが必要です。最大25個の異なるSSIDを指定できます。コントローラによって管理されていないSSIDを指定する必要があります。このオプションを選択する場合は、パラメータにSSIDを入力します。 • **wildcard-ssid**：SSID文字列に一致する可能性のある表現を指定できます。SSIDは最大25個指定できます。

ステップ5	**match** {**all** | **any**}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# match all`
		検出された不正アクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。

ステップ6	**default**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# default`
		コマンドをデフォルトに設定します。

ステップ7	**exit**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# exit`
	`Device(config)#`
		サブモードを終了します。

	コマンドまたはアクション	目的

ステップ 8	**shutdown**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# shutdown`
		特定の不正ルールを無効にします。この例では、ルール **rule_3** が無効になります。

ステップ 9	**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。
ステップ 10	**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 11	**wireless wps rogue rule shutdown** 例： `Device(config)# wireless wps rogue rule shutdown`	すべての不正ルールを無効にします。
ステップ 12	**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。

不正分類ルールのモニターリング

次のコマンドを使用して、不正分類ルールをモニタリングできます。

表 *34 :* 不正分類ルールのモニターリング用コマンド

コマンド	目的
show wireless wps rogue rule detailed	分類ルールの詳細情報を表示します。
show wireless wps rogue rule summary	分類ルールの概要を表示します。

例：不正なアクセス ポイントの分類

次に、MAC アドレスが 00:11:22:33:44:55 の不正 AP を Malicious として分類し、2 つの管理対象 AP に含まれているとマークする例を示します。

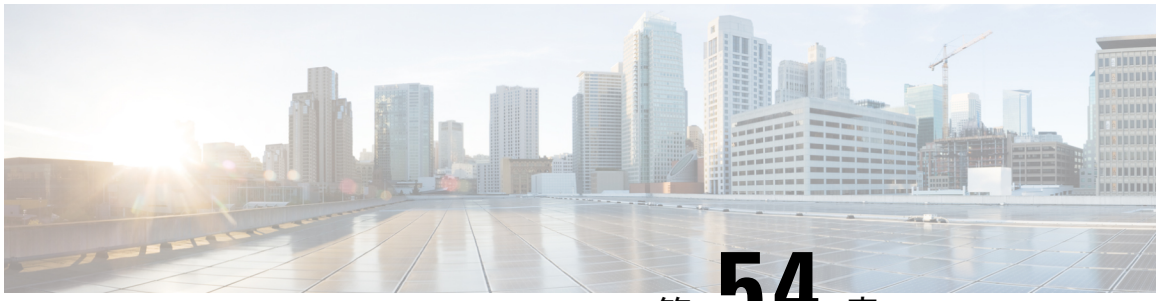
```
Device# configure terminal
Device(config)# wireless wps rogue ap malicious 0011.2233.4455 state contain 2
```

次に、SSID my-friendly-ssid を使用している不正 AP を分類できるルールを作成する方法、および少なくとも 1000 秒間、Friendly Internal として表示される例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition ssid my-friendly-ssid
Device(config-rule)# condition duration 1000
Device(config-rule)# match all
Device(config-rule)# classify friendly state internal
```

この例は、不正アクセス ポイントが満たす必要がある条件を適用する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# end
```



第 54 章

セキュア シェルの設定

セキュア シェルの設定について

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH およびデバイスアクセス

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュア シェル（SSH）統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いて Telnet のアウトバウンド接続と同様の機能を提供します。SSH クライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSHサーバおよびSSH統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSHクライアントは、市販の一般的なSSHサーバと連動します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートします。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対するTelnetセッションの認証と同様に実行されます。SSHは、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

SSH 設定時の注意事項

スイッチをSSHサーバーまたはSSHクライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバーは、SSHv1 サーバーで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- SSHサーバーがアクティブスイッチ上で動作しており、アクティブスイッチに障害が発生した場合、新しいアクティブスイッチは、以前のアクティブスイッチによって生成された RSA キーペアを使用します。
- **crypto key generate rsa**グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。
- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

Secure Copy Protocol の概要

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。SCP にはセキュア シェル（SSH）が必要です（Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです）。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 許可が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

（注） SCP を使用する場合、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

Secure Copy Protocol

セキュア コピー プロトコル（SCP）機能は、deviceの設定やスイッチ イメージ ファイルのコピーにセキュアな認証方式を提供します。SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。また、SCP では認証、許可、およびアカウンティング（AAA）の設定が必要なため、deviceはユーザーが正しい権限レベルを保有しているかどうかを特定できます。セキュア コピー機能を設定するには、SCP の概念を理解する必要があります。

SFTP のサポート

SFTP クライアントのサポートは、Cisco IOS XE Gibraltar 16.10.1 リリース以降で導入されています。SFTP クライアントはデフォルトで有効になっており、個別の設定は必要ありません。

SFTP プロシージャは、**scp** および **tftp** コマンドの場合と同様に、**copy** コマンドを使用して呼び出すことができます。**sftp** コマンドを使用した一般的なファイルダウンロード手順は、次のように実行できます。

copy sftp://*user* :*password* @*server-ip*/*file-name* **flash0://** *file-name*

copy コマンドの詳細については、次の URL を参照してください。
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html

セキュア シェルを設定するための前提条件

セキュア シェル（SSH）用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman（RSA）の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル（SCP）も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、およびアカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。
- セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェアイメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。
- グローバル コンフィギュレーション モードで **hostname** および **ip domain-name** コマンドを使用して、デバイスのホスト名とホストドメインを設定します。

セキュア シェルの設定に関する制約事項

セキュア シェル用にデバイスを設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格（DES）（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。

- device は、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。
- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。セキュア シェル バージョン 2 ではサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-l キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。
- 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。その場合は、**crypto key generate rsa general-keys exportable label** *label-name* コマンドを使用します。

SSH の設定方法

SSH を実行するためのデバイスの設定

SSH を実行するようにデバイスをセットアップするには、次の手順を実行してください。

始める前に

ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。

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# 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	**hostname** *hostname* 例： `Device(config)# hostname your_hostname`	device のホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、device を SSH サーバとして設定する場合だけです。
ステップ 3	**ip domain name** *domain_name* 例： `Device(config)# ip domain name`	device のホストドメインを設定します。

	コマンドまたはアクション	目的
	your_domain	
ステップ 4	**crypto key generate rsa** 例： `Device(config)# crypto key generate rsa`	device 上でローカルおよびリモート認証用にSSHサーバをイネーブルにし、RSA キー ペアを生成します。device の RSA キー ペアを生成すると、SSH が自動的にイネーブルになります。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。 （注） この手順を実行するのは、device を SSH サーバとして設定する場合だけです。
ステップ 5	**end** 例： `Device(config)# end`	設定モードを終了します。

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） デバイスを SSH サーバとして設定する場合にのみ、この手順を実行します。

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	**ip ssh version** [2] 例： `Device(config)# ip ssh version 2`	（任意）SSH バージョン 2 を実行するように device を設定します。

	コマンドまたはアクション	目的
ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*} 例： `Device(config)# ip ssh timeout 90 authentication-retries 2`	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は120秒）。指定できる範囲は0～120秒です。このパラメータは、SSHネゴシエーション フェーズに適用されます。接続が確立されると、デバイスは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。

ステップ 4	次のいずれかまたは両方を使用します。
	• `line vty` *line_number* [*ending_line_number*]
	• **transport input ssh**
	例：
	`Device(config)# line vty 1 10`
	または
	`Device(config-line)# transport input ssh`
		（任意）仮想端末回線設定を設定します。
		• ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。*line_number* および *ending_line_number* には、回線のペアを指定します。指定できる範囲は 0 ～ 15 です。
		• 非 SSH Telnet によるデバイスへの接続を許可しない設定です。これにより、ルータは SSH 接続に限定されます。

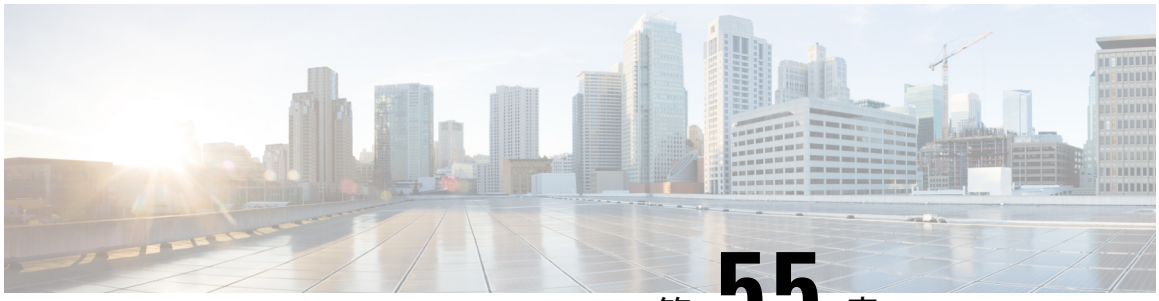
	コマンドまたはアクション	目的
		（注） 仮想端末（VTY）回線が使い果たされると、Telnet または SSH は失敗します。Telnet または SSH セッションを切断して VTY 回線を解放するか、以下の回復手順に従って VTY 回線をクリアして Telnet または SSH をリロードします。 `Device# configure terminal` `Device(config)# clear line` *`line number`*
ステップ 5	**end** 例： `Device(config-line)# end`	特権 EXEC モードに戻ります。

SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *35 : SSH* サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。



第 55 章

秘密共有キー

秘密事前共有キーについて

Internet of Things（IoT）の出現により、インターネットに接続されるデバイスの数は著しく増加しています。これらのデバイスがすべて 802.1x サプリカントをサポートしているわけではないため、インターネットに接続するための代替メカニズムが必要です。セキュリティメカニズムの 1 つである WPA-PSK が代替手段として考えられます。現在の設定では、PSK は同じ WLAN に接続するすべてのクライアントで同じです。教育機関などの一部の設置環境では、これによりキーが不正ユーザーに共有され、セキュリティ違反が生じます。このため、大規模な範囲でクライアントごとに一意の PSK をプロビジョニングすることが必要になります。

Identity PSK は、同じ SSID の個人またはユーザー グループのために作成される一意の PSK です。クライアントに複雑な設定は必要ありません。PSK と同じシンプルさで、IoT、BYOD（Bring Your Own Device）、およびゲスト展開に適しています。PSK SSID のデフォルトパスワードは password です。

Identity PSK は 802.1x 未対応のほとんどのデバイスでサポートされるため、より強力な IoT セキュリティを実現します。他に影響を与えずに 1 つのデバイスまたは個人に対するアクセスを簡単に取り消せます。何千ものキーを簡単に管理でき、AAA サーバーを介して配布することができます。

（注） 「<」や「>」などの特殊文字は、SSID 事前共有キーではサポートされていません。

（注） PSK では、二重引用符で囲まれたパスワードでのみ空白（パスワードの前後または中間）がサポートされます。空白に対する一重引用符はサポートされていません。

IPSK ソリューション

クライアントの認証時に、AAA サーバーはクライアントの MAC アドレスを認証し、Cisco-AV ペア リストの一部としてパスフレーズ（設定されている場合）を送信します。組み込みワイヤレスコントローラは RADIUS 応答の一部としてパスフレーズを受信し、さらに処理して PSK を計算します。

クライアントが、対応するアクセスポイントによる SSID ブロードキャストに対して関連付け要求を送信すると、組み込みワイヤレスコントローラは、クライアントの特定の MAC アドレスを含む RADIUS 要求パケットを形成し、RADIUS サーバーに中継します。

RADIUS サーバーは認証を実行し、クライアントが許可されているかどうか、および WLC への応答として ACCESS-ACCEPT または ACCESS-REJECT のいずれかを送信するかどうかをチェックします。

Identity PSK をサポートするために、認証サーバーは認証応答を送信するだけでなく、この特定のクライアントに AV ペア パスフレーズを提供します。これは、PMK の計算に使用されます。

RADIUS サーバーは、ユーザー名、VLAN、Quality of Service（QoS）など、このクライアントに固有の追加パラメータも応答に含めることがあります。1 人のユーザーが複数のデバイスを所有している場合は、すべてのデバイスで同じパスフレーズを使用できます。

（注） PSK の長さが連邦情報処理標準（FIPS）の 15 文字未満の場合、コントローラにより WLAN 設定は許可されますが、コンソールに次のエラーメッセージが表示されます。

「AP は接続できますが、対応する WLAN はアクセスポイントにプッシュされません（AP is allowed to join but corresponding WLAN will not be pushed to the access point）」

WLAN での PSK の設定（CLI）

WLAN で PSK を設定するには、次の手順に従います。

始める前に

- WLAN で事前共有キー（PSK）のセキュリティを設定する必要があります。
- AAA サーバーからのオーバーライドがない場合は、対応する WLAN 上の値が認証用と見なされます。

- 連邦情報処理標準（FIPS）およびコモンクライテリアモードでは、PSK WLAN に少なくとも 15 文字の ASCII 文字が含まれていることを確認します。含まれていない場合、AP はコントローラに接続しません。

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	**wlan** *wlan-name wlan-id ssid* 例： `Device(config)# wlan test-profile 4 abc`	WLAN と SSID を設定します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**security wpa akm psk** 例： `Device(config-wlan)# security wpa akm psk`	セキュリティ タイプ PSK を設定します。
ステップ 5	**security wpa akm psk set-key** *ascii/hex key* 例： `Device(config-wlan)# security wpa akm psk set-key asci 0`	PSK 認証キー管理（AKM）の共有キーを設定します。
ステップ 6	**security wpa akm psk** 例： `Device(config-wlan)# security wpa akm psk`	PSK サポートを設定します。
ステップ 7	**mac-filtering** *auth-list-name* 例： `Device(config-wlan)# mac-filtering test1`	WLAN で MAC フィルタリングを指定します。

WLAN での PSK の設定（GUI）

手順

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

ステップ 2 [Wireless Networks] ページで [Security] タブをクリックします。

ステップ 3 表示される [Layer 2] ウィンドウで、[WPA Parameters] セクションに移動します。

ステップ 4 [Auth Key Mgmt] ドロップダウンから PSK フォーマットおよびタイプを選択します。

ステップ 5 事前共有キーを 16 進数文字で入力します。

- PSK フォーマットとして HEX を選択した場合、キーの長さは 64 文字にする必要があります。
- PSK フォーマットとして ASCII を選択した場合、キーの長さは 8 ～ 63 文字にする必要があります。

キーを設定した後は、セキュリティ上の理由により、事前共有キーボックスの横にある目のアイコンをクリックしても、これらの詳細は表示されないことに注意してください。

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

WLAN へのポリシー プロファイルの適用（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、[Policy] タブをクリックします。

ステップ 3 [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 4 ポリシー タグの名前と説明を入力します。

ステップ 5 [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 6 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 7 [Save & Apply to Device] をクリックします。

WLAN へのポリシー プロファイルの適用（CLI）

WLAN にポリシー プロファイルを適用するには、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** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-iot`	デフォルト ポリシー プロファイルを設定します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバーまたは Cisco Identify Services Engine（ISE）サーバーから受信したポリシーを適用するように AAA オーバーライドを設定します。

秘密 PSK の確認

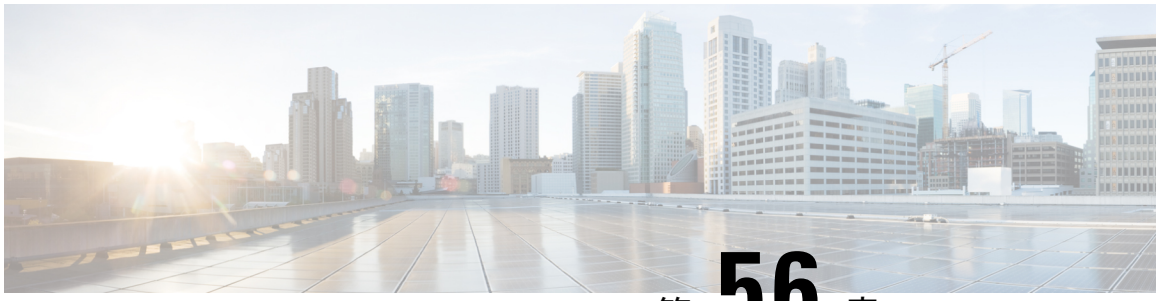
WLAN とクライアントの設定を確認するには、次の **show** コマンドを使用します。

```
Device# show wlan id 2


WLAN Profile Name     : test_ppsk
================================================
Identifier                                       : 2
Network Name (SSID)                              : test_ppsk
Status                                           : Enabled
Broadcast SSID                                   : Enabled
Universal AP Admin                               : Disabled
Max Associated Clients per WLAN                  : 0
Max Associated Clients per AP per WLAN           : 0
Max Associated Clients per AP Radio per WLAN     : 0
Number of Active Clients                         : 0
Exclusionlist Timeout                            : 60
CHD per WLAN                                     : Enabled
Interface                                        : default
Multicast Interface                              : Unconfigured
WMM                                              : Allowed
WifiDirect                                       : Invalid
Channel Scan Defer Priority:
  Priority (default)                             : 4
  Priority (default)                             : 5
  Priority (default)                             : 6
Scan Defer Time (msecs)                          : 100
```

```
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Diagnostics Channel Capability            : Disabled
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : test1
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Enabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            PMF dot1x                           : Disabled
            PMF PSK                             : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Disabled
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Disabled
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 200
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Parameter Map                       : Disabled
    Tkip MIC Countermeasure Hold-down Timer     : 60
Call Snooping                                   : Disabled
Passive Client                                  : Disabled
Non Cisco WGB                                   : Disabled
Band Select                                     : Disabled
Load Balancing                                  : Disabled
Multicast Buffer                                : Disabled
Multicast Buffer Size                           : 0
IP Source Guard                                 : Disabled
Assisted-Roaming
    Neighbor List                               : Disabled
    Prediction List                             : Disabled
    Dual Band Support                           : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                  : Disabled
    BSS Max Idle                                : Disabled
        Protected Mode                          : Disabled
    Traffic Filtering Service                   : Disabled
    BSS Transition                              : Enabled
        Disassociation Imminent                 : Disabled
            Optimised Roaming Timer             : 40
            Timer                               : 200
    WNM Sleep Mode                              : Disabled
```

```
802.11ac MU-MIMO                                : Disabled

Device# show wireless client mac-address a886.adb2.05f9 detail


Client MAC Address : a886.adb2.05f9
Client IPv4 Address : 9.9.58.246
Client Username : A8-86-AD-B2-05-F9
AP MAC Address : c025.5c55.e400
AP Name: saurabh-3600
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 6
Wireless LAN Name: SSS_PPSK
BSSID : c025.5c55.e40f
Connected For : 280 seconds
Protocol : 802.11n - 5 GHz
Channel : 60
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 320 sec (Remaining time: 40 sec)
Input Policy Name  :
Input Policy State : None
Input Policy Source : None
Output Policy Name  :
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Current Rate : m22
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 09/27/2017 16:32:25 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 280 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : PSK
AAA override passphrase: Yes
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 58
Access VLAN : 58
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
```

```
  Interface        : capwap_90000005
  IIF ID           : 0x90000005
  Device Type      : Apple-Device
  Protocol Map     : 0x000001
  Authorized       : TRUE
  Session timeout  : 320
  Common Session ID: 1F3809090000005DC30088EA
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : MAB
                 SM State        : TERMINATE
                 Authen Status   : Success
  Local Policies:
        Service Template : wlan_svc_default-policy-profile (priority 254)
                 Absolute-Timer   : 320
                 VLAN             : 58
  Server Policies:
  Resultant Policies:
                 VLAN             : 58
                 Absolute-Timer   : 320
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 59795
  Number of Bytes Sent : 21404
  Number of Packets Received : 518
  Number of Packets Sent : 274
  Number of EAP Id Request Msg Timeouts :
  Number of EAP Request Msg Timeouts :
  Number of EAP Key Msg Timeouts :
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -32 dBm
  Signal to Noise Ratio : 58 dB
Fabric status : Disabled
```



第 56 章

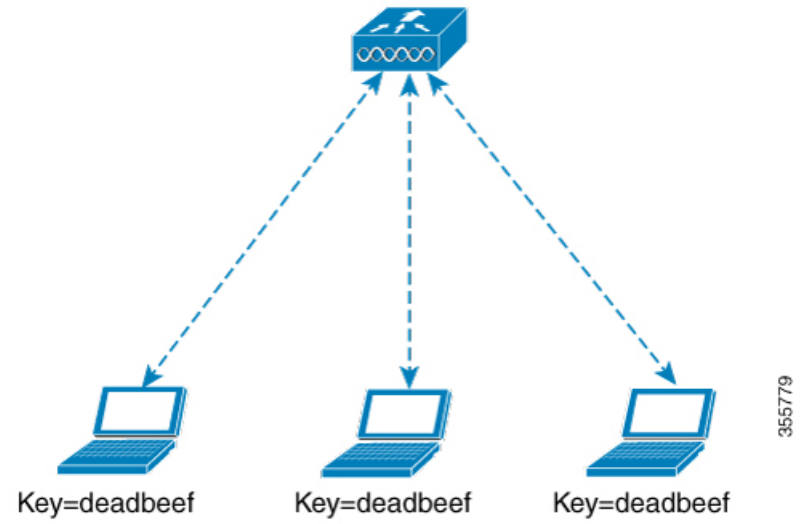
マルチ事前共有キー

マルチ事前共有キーについて

マルチ PSK 機能は、1 つの SSID で同時に複数の PSK をサポートします。設定された PSK のいずれかを使用してネットワークに接続できます。これは Identity PSK（iPSK）とは異なり、同じ SSID 上の個人またはユーザー グループに対して一意の PSK が作成されます。

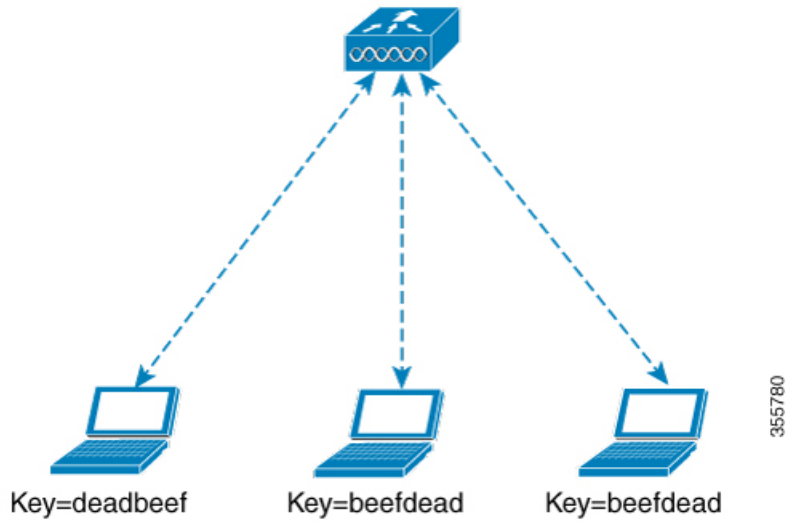
従来の PSK では、次の図に示すように、ネットワークに接続しているすべてのクライアントが同じパスワードを使用します。

図 *21* : 従来の *PSK*



ところがマルチ PSK を使用すると、クライアントは次の図に示すように設定済みの事前共有キーのいずれかを使用してネットワークに接続できます。

図 *22 : マルチ PSK*



マルチ PSK では、同じ SSID に 2 つのパスワード（deadbeef と beefdead）が設定されます。このシナリオでは、クライアントはいずれかのパスワードを使用してネットワークに接続できます。

マルチ PSK の制約事項

- 中央認証は、ローカル、フレックス、およびファブリック モードでのみサポートされています。
- 中央認証フレックス モードの場合、スタンドアロン AP は、最もプライオリティの高い PSK（*priority 0* キー）を使用するクライアントの接続を許可します。最もプライオリティの高い PSK を使用しない新しいクライアントは、スタンドアロン モードでは拒否されます。
- マルチ PSK はローカル認証をサポートしません。

マルチ事前共有キーの設定（GUI）

手順

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

ステップ 2 [Wireless Networks] ページで WLAN の名前をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで [Security] タブをクリックします。

ステップ 4 [Layer2] タブで、[Layer2 Security Mode] を次のオプションから選択します。

- [None]：レイヤ 2 セキュリティなし
- [802.1X]：WEP 802.1X データ暗号化タイプ
- [WPA + WPA2]：Wi-Fi Protected Access
- [Static WEP]：静的 WEP 暗号化パラメータ
- [Static WEP+802.1X]：静的 WEP と 802.1X の両方のパラメータ。

パラメータ	説明
802.1X	
WEP Key Size	キーサイズを選択します。使用可能な値は、[None]、[40 bits]、および [104 bits] です。
WPA + WPA2	
Protected Management Frame	次のオプションから選択します。 • ディセーブル • 任意 • 必須
WPA Policy	WPA ポリシーを有効にするには、このチェック ボックスをオンにします。
WPA Encryption	WPA 暗号化規格を選択します。WPA ポリシーを有効にしている場合は、WPA 暗号化規格を指定する必要があります。
WPA2 Policy	WPA2 ポリシーを有効にするには、このチェック ボックスをオンにします。
WPA2 Encryption	WPA2 暗号化規格を選択します。WPA ポリシーを有効にしている場合は、WPA 暗号化規格を指定する必要があります。

パラメータ	説明
Auth Key Mgmt	次のオプションからキー再生成メカニズムを選択します。 • 802.1X • [FT + 802.1X] • [PSK]：PSK 形式と事前共有キーを指定する必要があります • Cisco Centralized Key Management：Cisco Centralized Key Management のタイムスタンプの許容値を指定する必要があります。 • 802.1X + Cisco Centralized Key Management：Cisco Centralized Key Management のタイムスタンプの許容値を指定する必要があります。 • FT + 802.1X + Cisco Centralized Key Management：Cisco Centralized Key Management のタイムスタンプの許容値を指定する必要があります。
Static WEP	
Key Size	次のオプションからキーサイズを選択します。 • 40 ビット • 104 ビット
Key Index	1 ～ 4 の範囲でキー インデックスを選択します。各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。WEP キーインデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化に設定できる WLAN は 4 つのみです。
Key Format	暗号キーの形式として、ASCII または HEX のいずれかを選択します。
Encryption Key	長さが 13 文字の暗号キーを入力します。
Static WEP + 802.1X	
Key Size	次のオプションからキーサイズを選択します。 • 40 ビット • 104 ビット

パラメータ	説明
Key Index	1 ～ 4 の範囲でキー インデックスを選択します。各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。WEP キーインデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化に設定できる WLAN は 4 つのみです。
Key Format	暗号キーの形式として、ASCII または HEX のいずれかを選択します。
Encryption Key	長さが 13 文字の暗号キーを入力します。
WEP Key Size	次のオプションから選択します。 • なし • 40 ビット • 104 ビット

ステップ 5 [Save & Apply to Device] をクリックします。

マルチ事前共有キーの設定（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。
ステップ 2	**wlan** *wlan-name wlan-id ssid* 例： `デバイス(config)# wlan mywlan 1 SSID_name`	WLAN と SSID を設定します。
ステップ 3	**no security wpa akm dot1x** 例： `デバイス(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**security wpa akm psk** 例： `デバイス(config-wlan)# security wpa akm psk`	PSK を設定します。
ステップ 5	**security wpa wpa2 mpsk** 例： `デバイス(config-wlan)# security wpa wpa2 mpsk`	マルチ PSK を設定します。
ステップ 6	**priority** *priority_value* **set-key** {**ascii** [**0** | **8**] *pre-shared-key* | **hex** [**0** | **8**] *pre-shared-key*} 例： `デバイス(config-mpsk)# priority 0 set-key ascii 0 deadbeef`	PSK のプライオリティおよび関連するすべてのパスワードを設定します。 *priority_value* の範囲は 0 ～ 4 です。 （注） マルチ PSK には **priority 0** キーを設定する必要があります。
ステップ 7	**no shutdown** 例： `デバイス(config-mpsk)# no shutdown`	WLAN を有効にします。
ステップ 8	**exit** 例： `デバイス(config-wlan)# exit`	WLAN コンフィギュレーション モードを終了して、コンフィギュレーション モードに戻ります。
ステップ 9	**end** 例： `デバイス(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。

マルチ PSK 設定の確認

WLAN とクライアントの設定を確認するには、次のコマンドを使用します。

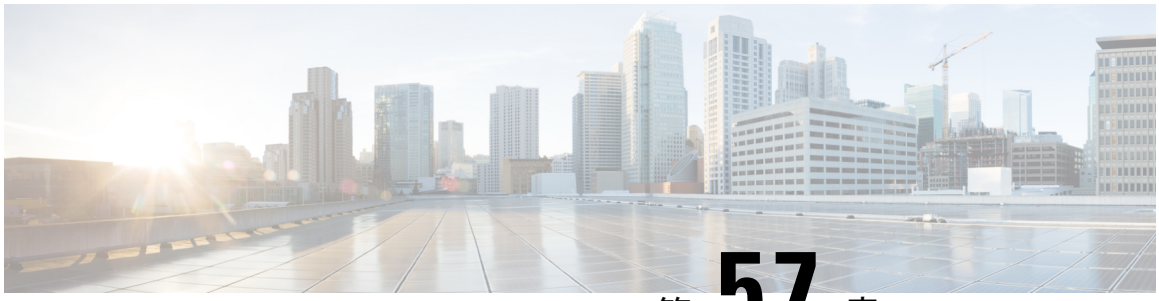
```
Device# show wlan id 8
WLAN Profile Name     : wlan_8
================================================
Identifier                                    : 8
Network Name (SSID)                           : ssid_8
Status                                        : Enabled
Broadcast SSID                                : Enabled
Universal AP Admin                            : Disabled
Max Associated Clients per WLAN               : 0
Max Associated Clients per AP per WLAN        : 0
```

```
Max Associated Clients per AP Radio per WLAN   : 200
Number of Active Clients                       : 0
CHD per WLAN                                   : Enabled
Multicast Interface                            : Unconfigured
WMM                                            : Allowed
WifiDirect                                     : Invalid
Channel Scan Defer Priority:
  Priority (default)                           : 5
  Priority (default)                           : 6
Scan Defer Time (msecs)                        : 100
Media Stream Multicast-direct                  : Disabled
CCX - AironetIe Support                        : Enabled
CCX - Diagnostics Channel Capability           : Disabled
Peer-to-Peer Blocking Action                   : Disabled
Radio Policy                                   : All
DTIM period for 802.11a radio                  : 1
DTIM period for 802.11b radio                  : 1
Local EAP Authentication                       : Disabled
Mac Filter Authorization list name             : Disabled
Mac Filter Override Authorization list name    : Disabled
Accounting list name                           :
802.1x authentication list name                : Disabled
802.1x authorization list name                 : Disabled
Security
    802.11 Authentication                      : Open System
    Static WEP Keys                            : Disabled
    802.1X                                     : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)     : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Enabled
            MPSK                               : Enabled
            AES Cipher                         : Enabled
            CCMP256 Cipher                     : Disabled
            GCMP128 Cipher                     : Disabled
            GCMP256 Cipher                     : Disabled
        WPA3 (WPA3 IE)                         : Disabled
        Auth Key Management
            802.1x                             : Disabled
            PSK                                : Enabled
            CCKM                               : Disabled
            FT dot1x                           : Disabled
            FT PSK                             : Disabled
            FT SAE                             : Disabled
            PMF dot1x                          : Disabled
            PMF PSK                            : Disabled
            SAE                                : Disabled
            OWE                                : Disabled
            SUITEB-1X                          : Disabled
            SUITEB192-1X                       : Disabled
    CCKM TSF Tolerance                         : 1000
    FT Support                                 : Adaptive
        FT Reassociation Timeout               : 20
        FT Over-The-DS mode                    : Enabled
    PMF Support                                : Disabled
        PMF Association Comeback Timeout       : 1
        PMF SA Query Time                      : 200
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      : Disabled
    Tkip MIC Countermeasure Hold-down Timer    : 60
```

```
Non Cisco WGB                                   : Disabled
Band Select                                     : Enabled
Load Balancing                                  : Disabled
Multicast Buffer                                : Disabled
Multicast Buffer Size                           : 0
IP Source Guard                                 : Disabled
Assisted-Roaming
    Neighbor List                               : Disabled
    Prediction List                             : Disabled
    Dual Band Support                           : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                  : Disabled
    BSS Max Idle                                : Disabled
        Protected Mode                          : Disabled
    Traffic Filtering Service                   : Disabled
    BSS Transition                              : Enabled
        Disassociation Imminent                 : Disabled
            Optimised Roaming Timer             : 40
            Timer                               : 200
    WNM Sleep Mode                              : Disabled
802.11ac MU-MIMO                                : Disabled
802.11ax paramters
    OFDMA Downlink                              : unknown
    OFDMA Uplink                                : unknown
    MU-MIMO Downlink                            : unknown
    MU-MIMO Uplink                              : unknown
    BSS Color                                   : unknown
    Partial BSS Color                           : unknown
    BSS Color Code                              :
```

WLAN の詳細を表示するには、次のコマンドを使用します。

```
Device# show run wlan
wlan wlan_8 8 ssid_8
 security wpa psk set-key ascii 0 deadbeef
 no security wpa akm dot1x
 security wpa akm psk
 security wpa wpa2 mpsk
  priority 0 set-key ascii 0 deadbeef
  priority 1 set-key ascii 0 deaddead
  priority 2 set-key ascii 0 d123d123
  priority 3 set-key hex 0 023456789012345678901234567890123456789012345678901234567890123456789012345678901234

  priority 4 set-key hex 0 123456789012345678901234567890123456789012345678901234567890123456789012345678901234

 no shutdown
```



第 57 章

クライアントの複数認証

クライアントの複数認証について

複数認証機能は、クライアント接続でサポートされるレイヤ2およびレイヤ3セキュリティ タイプの拡張機能です。

（注） 特定の SSID に対して L2 認証と L3 認証の両方を有効にすることができます。

（注） 複数認証機能は、通常のクライアントにのみ適用されます。

クライアントに対する認証の組み合わせのサポートに関する情報

クライアントの複数認証では、WLANプロファイルで設定された特定のクライアントに対する複数の認証の組み合わせがサポートされます。

次の表に、サポートされる認証の組み合わせの概要を示します。

レイヤ 2	レイヤ 3	サポートあり
MAB	CWA	はい
MAB のエラー	LWA	対応
802.1X	CWA	はい

PSK	CWA	はい
iPSK + MAB	CWA	はい
iPSK	LWA	非対応
MAB のエラー + PSK	LWA	非対応 対応
MAB のエラー + PSK	CWA	非対応

16.10.1 以降では、WLAN の 802.1X 設定で、WPA または WPA2 設定を使用した Web 認証設定がサポートされます。

この機能は、次の AP モードもサポートしています。

- Local
- FlexConnect
- ファブリック

クライアントの複数認証の設定

802.1X およびローカル Web 認証用の WLAN の設定（GUI）

手順

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

ステップ 2 表示された WLAN のリストから必要な WLAN を選択します。

ステップ 3 [Security] > [Layer2] タブを選択します。

ステップ 4 [Layer 2 Security Mode] ドロップダウンリストからセキュリティ方式を選択します。

ステップ 5 [Auth Key Mgmt] で、[802.1x] チェックボックスをオンにします。

ステップ 6 [MAC Filtering] チェックボックスをオンにして、機能を有効にします。

ステップ 7 MAC フィルタリングを有効にした状態で、[Authorization List] ドロップダウンリストからオプションを選択します。

ステップ 8 [Security] > [Layer3] タブを選択します。

ステップ 9 [Web Policy] チェックボックスをオンにして、Web 認証ポリシーを有効にします。

ステップ 10 [Web Auth Parameter Map] および [Authentication List] ドロップダウンリストから、オプションを選択します。

ステップ 11 [Update & Apply to Device] をクリックします。

802.1X およびローカル Web 認証用の WLAN 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。
ステップ 2	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • profile-name：設定されている WLAN のプロファイル名。 • wlan-id：ワイヤレス LAN の ID。範囲は 1 ～ 512 です。 • SSID_Name：最大 32 文字の英数字からなる SSID。 （注） すでにこのコマンドを設定している場合は、wlan profile-name コマンドを入力します。
ステップ 3	**security dot1x authentication-list** *auth-list-name* 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。 この設定は、すべての dot1x セキュリティ WLAN で類似しています。
ステップ 4	**security web-auth** 例： `Device(config-wlan)# security web-auth`	Web 認証を有効にします。
ステップ 5	**security web-auth authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security web-auth authentication-list default`	dot1x セキュリティ用の認証リストを有効にします。
ステップ 6	**security web-auth parameter-map** *parameter-map-name*	パラメータ マップをマッピングします。

	コマンドまたはアクション	目的
	例： `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	（注） パラメータマップが WLAN に関連付けられていない場合は、グローバルパラメータマップの設定と見なされます。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

例

```
wlan wlan-test 3 ssid-test
 security dot1x authentication-list default
 security web-auth
 security web-auth authentication-list default
 security web-auth parameter-map WLAN1_MAP
 no shutdown
```

事前共有キー（PSK）およびローカル Web 認証用の WLAN の設定（GUI）

手順

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

ステップ 2 必要な WLAN を選択します。

ステップ 3 [Security] > [Layer2] タブを選択します。

ステップ 4 [Layer 2 Security Mode] ドロップダウンリストからセキュリティ方式を選択します。

ステップ 5 [Auth Key Mgmt] で、[802.1x] チェックボックスをオフにします。

ステップ 6 [PSK] チェックボックスをオンにします。

ステップ 7 [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。

ステップ 8 [Security] > [Layer3] タブを選択します。

ステップ 9 [Web Policy] チェックボックスをオンにして、Web 認証ポリシーを有効にします。

ステップ 10 [Web Auth Parameter Map] ドロップダウンリストから [Web Auth Parameter Map] を選択し、[Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 11 [Update & Apply to Device] をクリックします。

事前共有キー（PSK）およびローカル Web 認証用の WLAN 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	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • *profile-name*：設定する WLAN のプロファイル名です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID_Name*：最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**security wpa psk set-key** *ascii/hex key password* 例： `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	PSK 共有キーを設定します。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**security wpa akm psk** 例： `Device(config-wlan)# security wpa akm psk`	PSK サポートを設定します。
ステップ 6	**security web-auth** 例： `Device(config-wlan)# security web-auth`	WLAN の Web 認証を有効にします。

	コマンドまたはアクション	目的
ステップ 7	**security web-auth authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security web-auth authentication-list webauth`	dot1x セキュリティ用の認証リストを有効にします。
ステップ 8	**security web-auth parameter-map** *parameter-map-name* 例： `(config-wlan)# security web-auth parameter-map WLAN1_MAP`	パラメータ マップを設定します。 （注） パラメータ マップが WLAN に関連付けられていない場合は、グローバル パラメータ マップの設定と見なされます。

例

```
wlan wlan-test 3 ssid-test
 security wpa psk set-key ascii 0 PASSWORD
 no security wpa akm dot1x
 security wpa akm psk
 security web-auth
 security web-auth authentication-list webauth
 security web-auth parameter-map WLAN1_MAP
```

PSK または iPSK（ID 事前共有キー）および中央 Web 認証用の WLAN の設定（GUI）

手順

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

ステップ 2 必要な WLAN を選択します。

ステップ 3 [Security] > [Layer2] タブを選択します。

ステップ 4 [Layer 2 Security Mode] ドロップダウンリストからセキュリティ方式を選択します。

ステップ 5 [Auth Key Mgmt] で、[802.1x] チェックボックスをオフにします。

ステップ 6 [PSK] チェックボックスをオンにします。

ステップ 7 [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。

ステップ 8 [MAC Filtering] チェックボックスをオンにして、機能を有効にします。

ステップ 9 MAC フィルタリングを有効にした状態で、[Authorization List] ドロップダウンリストから認可リストを選択します。

ステップ 10 [Security] > [Layer3] タブを選択します。

ステップ 11 [Web Policy] チェックボックスをオンにして、Web 認証ポリシーを有効にします。

ステップ 12 [Web Auth Parameter Map] ドロップダウンリストから [Web Auth Parameter Map] を選択し、[Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 13 [Update & Apply to Device] をクリックします。

PSK または iPSK（ID 事前共有キー）および中央 Web 認証用の WLAN の設定

WLAN 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	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • *profile-name*：設定する WLAN のプロファイル名です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID_Name*：最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**security wpa psk set-key** *ascii/hex key password* 例：	PSK AKM の共有キーを設定します。

	コマンドまたはアクション	目的
	`Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	
ステップ 5	**mac-filtering** *auth-list-name* 例： `Device(config-wlan)# mac-filtering test-auth-list`	MAC フィルタリング パラメータを設定します。

例

```
wlan wlan-test 3 ssid-test
 no security wpa akm dot1x
 security wpa psk set-key ascii 0 PASSWORD
 mac-filtering test-auth-list
```

WLAN へのポリシー プロファイルの適用

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** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-iot`	デフォルト ポリシー プロファイルを設定します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバーまたは ISE サーバーから受信したポリシーを適用するように AAA オーバーライドを設定します。
ステップ 4	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシー プロファイルに NAC を設定します。
ステップ 5	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	WLAN を停止します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。

例

```
wireless profile policy policy-iot
 aaa-override
 nac
 no shutdown
```

コントローラでの 802.1x および中央 Web 認証の設定（CLI）

AAA 認証の作成

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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。

外部認証用の AAA サーバーの設定

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	**radius-server attribute wireless authentication call-station-id ap-name-ssid** 例： `Device(config)# radius-server attribute wireless authentication call-station-id ap-name-ssid`	RADIUS 認証メッセージで送信される発信側ステーション識別子を設定します。
ステップ 3	**radius server** *server-name* 例： `Device(config)# radius server ISE2`	RADIUS サーバーを設定します。
ステップ 4	**address ipv4** *radius-server-ip-address* 例： `Device(config-radius-server)# address ipv4 111.111.111.111`	RADIUS サーバーのアドレスを指定します。
ステップ 5	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 10`	秒単位のタイムアウト値を指定します。範囲は 10 ～ 1000 秒です。
ステップ 6	**retransmit** *number-of-retries* 例： `Device(config-radius-server)# retransmit 10`	サーバーへの再試行回数を指定します。範囲は 0 ～ 100 です。
ステップ 7	**key** *key* 例： `Device(config-radius-server)# key cisco`	デバイスと、RADIUS サーバー上で動作するキー文字列 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。 *key* には次の値を使用できます。 • 0：暗号化されていないキーを指定します。 • 6：暗号化されたキーを指定します。 • 7：「隠し」キーを指定します。 • Word：暗号化されていない（クリアテキスト）サーバー キー。
ステップ 8	**exit** 例：	コンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-radius-server)# exit`	
ステップ 9	**aaa group server radius** *server-group* 例： `Device(config)# aaa group server radius ISE2`	RADIUS サーバーグループの ID を作成します。
ステップ 10	**server name** *server-name* 例： `Device(config)# server name ISE2`	サーバー名を設定します。
ステップ 11	**radius-server deadtime** *time-in-minutes* 例： `Device(config)# radius-server deadtime 5`	DEAD とマークされたサーバーがその状態で保持される時間を分単位で定義します。このデッドタイムが経過すると、コントローラはサーバーを UP（ALIVE）としてマークし、登録クライアントに状態の変更を通知します。状態が UP としてマークされた後もサーバーに到達できない場合、および DEAD 条件が満たされている場合、そのサーバーはデッドタイム間隔で再び DEAD としてマークされます。 *time-in-mins*：有効な値の範囲は 1 ～ 1440 分です。デフォルト値はゼロです。デフォルト値に戻すには、**no radius-server deadtime** コマンドを使用します。 **radius-server deadtime** コマンドは、グローバルに設定することも、AAA グループサーバーレベルで設定することもできます。 **show aaa dead-criteria** または **show aaa servers** コマンドを使用して、デッドサーバーの検出を確認できます。デフォルト値がゼロの場合、デッドタイムは設定されません。

認証用の AAA の設定

始める前に

RADIUS サーバーと AAA サーバー グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa authentication login** 例： `Device# aaa authentication login ISE_GROUP group ISE2 local`	ログイン時の認証方法を定義します。
ステップ 2	**aaa authentication dot1x** 例： `Device(config)# aaa authentication network ISE_GROUP group ISE2 local`	dot1x での認証方法を定義します。

アカウンティング ID リストの設定

始める前に

RADIUS サーバーと AAA サーバー グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* 例： `Device# aaa accounting identity ISE start-stop group ISE2`	アカウンティングを有効にして、クライアントが承認されたときに start-record アカウンティング通知を送信し、最後に stop-record を送信できるようにします。 （注） 名前付きリストの代わりにデフォルトのリストを使用することもできます。

中央 Web 認証用の AAA の設定

始める前に

RADIUS サーバーと AAA サーバー グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa server radius dynamic-author** 例：	コントローラの認可変更（CoA）を設定します。

	コマンドまたはアクション	目的
	`Device# aaa server radius dynamic-author`	
ステップ 2	**client** *client-ip-addr* **server-key** *key* 例： `Device(config-locsvr-da-radius)# client 111.111.111.111 server-key ciscokey`	RADIUS クライアントのサーバーキーを設定します。

Radius サーバーのアクセス制御リストの定義

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 redirect** 例： `Device(config)# ip access-list extended redirect`	ISE がリダイレクト ACL（**redirect** という名前）を使用するように設定されているため、HTTP および HTTPS ブラウジングは（他の ACL ごとの）認証なしでは機能しません。
ステップ 3	*sequence-number* **deny icmp any** 例： `Device(config-ext-nacl)# 10 deny icmp any`	シーケンス番号に従って拒否するパケットを指定します。 （注） 拒否シーケンスには、DHCP、DNS、および ISE サーバーが必要です。「Radius サーバーのアクセス制御リストを定義する構成例」を参照してください。この例で、*111.111.111.111* は ISE サーバーの IP アドレスを指します。
ステップ 4	**permit TCP any any eq** *web-address* 例： `Device(config-ext-nacl)# permit TCP any any eq www`	すべての HTTP または HTTPS アクセスを Cisco ISE のログインページにリダイレクトします。

Radius サーバーのアクセス制御リストを定義する構成例

この例では、RADIUS サーバーのアクセス制御リストを定義する方法を示します。

```
Device# configure terminal
Device(config-ext-nacl) # 10 deny icmp any
Device(config-ext-nacl) # 20 deny udp any any eq bootps
Device(config-ext-nacl) # 30 deny udp any any eq bootpc
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # 50 deny tcp any host 111.111.111.111 eq 8443
Device(config-ext-nacl) # 55 deny tcp host 111.111.111.111 eq 8443 any
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # end
```

WLAN 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	**wlan** *wlan-name* 例： `Device(config)# wlan wlan30`	WLAN 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	**security dot1x authentication-list ISE_GROUP** 例： `Device(config-wlan)# security dot1x authentication-list ISE_GROUP`	WLAN の 802.1X を設定します。
ステップ 4	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

ポリシー プロファイルの設定

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-name* 例： `Device(config)# wireless profile policy wireless-profile1`	ポリシープロファイルを設定します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバーまたは Cisco Identify Services Engine（ISE）サーバーから受信したポリシーを適用するように AAA オーバーライドを設定します。
ステップ 4	**accounting-list** *list-name* 例： `Device(config-wireless-policy)# accounting-list ISE`	IEEE 802.1x のアカウンティング リストを設定します。
ステップ 5	**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 6	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシープロファイルでネットワーク アクセス コントロール（NAC）を設定します。NAC は、中央 Web 認証（CWA）をトリガーするために使用されます。
ステップ 7	**vlan 25** 例： `Device(config-wireless-policy)# vlan 25`	ゲスト VLAN プロファイルを設定します。
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。

ポリシータグへの WLAN とポリシープロファイルのマッピング

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-policy-tag)# wireless tag policy xx-xre-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 wlan30 policy wireless-profile1`	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。

中央 Web 認証と Dot1x 用の ISE の設定（GUI）

ゲストポータルの定義

始める前に

ゲストポータルを定義するか、デフォルトのゲストポータルを使用します。

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。
ステップ 2 **[Work Centers]** > **[Guest Access]** > **[Portals & Components]** の順に選択します。
ステップ 3 [Guest Portal] をクリックします。

クライアントの認証プロファイルの定義

始める前に

要件に応じて、ゲストポータルおよびその他の追加パラメータを使用する認証プロファイルを定義できます。認証プロファイルは、クライアントを認証ポータルにリダイレクトします。Cisco ISE の最新バージョンでは、Cisco_Webauth 認証結果がすでに存在しており、これを編集して、コントローラの構成と一致するようにリダイレクト ACL の名前を変更できます。

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 3 [Add] をクリックして独自のカスタムを作成するか、Cisco_Webauth のデフォルトの結果を編集します。

認証ルールの定義

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 **[Policy]** > **[Policy Sets]** の順に選択し、適切なポリシーセットをクリックします。

ステップ 3 [Authentication] ポリシーを展開します。

ステップ 4 [Options] を展開し、適切な [User ID] を選択します。

認証ルールの定義

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 **[Policy]** > **[Policy Sets]** > **[Authorization Policy]** の順に選択します。

ステップ 3 特定の SSID で 802.1x の条件に一致するルールを作成します（Radius-Called-Station-ID を使用）。

（注） CWA リダイレクト属性が表示されます。

ステップ 4 作成済みの認証プロファイルを選択します。

ステップ 5 [Result/Profile] 列から、作成済みの認証プロファイルを選択します。

ステップ 6 [Save] をクリックします。

（注）　次の図に、機能する構成例を参考として示します。

図 *23 :* 機能する構成例

ゲストフロー条件に一致するルールの作成

始める前に

ユーザーがポータルで認証を完了したらゲストフロー条件に一致してネットワークアクセスの詳細に戻る 2 番目のルールを作成する必要があります。

手順

ステップ 1　Cisco Identity Services Engine（ISE）にログインします。

ステップ 2　**[Policy]** > **[Policy Sets]** > **[Authorization Policy]** の順に選択します。

ステップ 3　Network Access-UseCase EQUALS Guest、および特定の SSID で 802.1x の条件に一致するルールを作成します（Radius-Called-Station-ID を使用）。

（注）　アクセス許可が表示されます。

ステップ 4　[Result/Profile] 列から、作成済みの認証プロファイルを選択します。

ステップ 5　デフォルトまたはカスタマイズされたアクセス許可を選択します。

ステップ 6　[Save] をクリックします。

複数の認証設定の確認

レイヤ 2 認証

L2 認証（Dot1x）が完了すると、クライアントは Webauth Pending 状態に移行します。

L2 認証後のクライアントの状態を確認するには、次のコマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------
```

```
58ef.68b6.aa60 ewlc1_ap_1   3  Webauth Pending    11n(5)        Dot1x  Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address <mac_address> detail

Auth Method Status List

Method: Dot1x
Webauth State: Init
Webauth Method: Webauth
Local Policies:
Service Template: IP-Adm-V6-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V6-Int-ACL-global
Service Template: IP-Adm-V4-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V4-Int-ACL-global
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50
```

```
Device# show platform software wireless-client chassis active R0

        ID  MAC Address      WLAN  Client     State
------------------------------------------------------------------------------------------

  0xa0000003      58ef.68b6.aa60    3             L3          Authentication
```

```
Device# show platform software wireless-client chassis active F0

    ID     MAC Address   WLAN  Client     State  AOM ID    Status
-------------------------------------------------------------------------------------------------
0xa0000003    58ef.68b6.aa60    3           L3          Authentication.         730.
   Done
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO    LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL               AN - ANCHOR
FR - FOREIGN          MT - MTE
IV - INVALID


EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
-------------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
summary
Vlan   DP IDX         MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
-------------------------------------------------------------------------------------
0X49   0xa0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

レイヤ 3 認証

L3 認証が成功すると、クライアントは Run 状態に移行します。

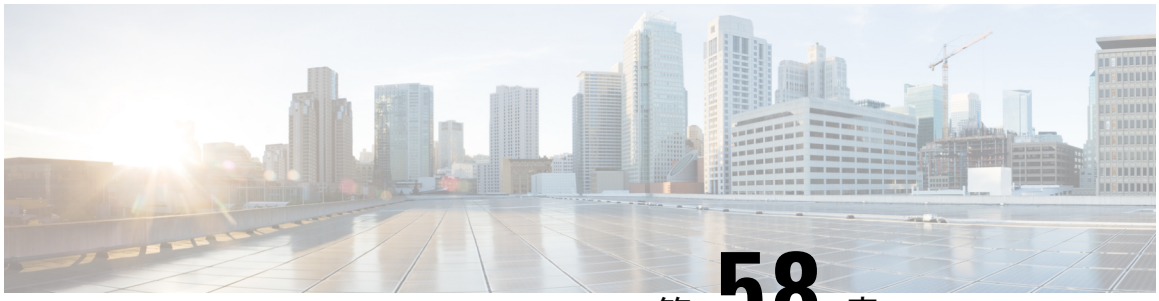
L3 認証後のクライアントの状態を確認するには、次のコマンドを使用します。

```
Device# show wireless client summary

Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------

58ef.68b6.aa60   ewlc1_ap_1  3     Run    11n(5)   Web Auth      Local
Number of Excluded Clients: 0

Device# show wireless client mac-address 58ef.68b6.aa60 detail

Auth Method Status List

Method: Web Auth
Webauth State: Authz
Webauth Method: Webauth
Local Policies:
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

Server Policies:

Resultant Policies:
VLAN: 50
Absolute-Timer: 1800

Device# show platform software wireless-client chassis active R0

ID          MAC Address     WLAN    Client State
-------------------------------------------------
0xa0000001 58ef.68b6.aa60    3          Run

Device# show platform software wireless-client chassis active f0

ID         MAC Address       WLAN    Client State   AOM ID.  Status
-----------------------------------------------------------------------
0xa0000001 58ef.68b6.aa60.   3          Run         11633    Done

Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO      LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL         AN - ANCHOR
FR - FOREIGN       MT - MTE
IV - INVALID
EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address   VLAN  CT  MCVL AS MS E   WLAN     POA
-------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60  50   RG   0   RN LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
summary

Vlan   pal_if_hd1        mac            Input Uidb     Output Uidb
------------------------------------------------------------------
50     0xa0000003    58ef.68b6.aa60     95929            95927
```

PSK + WebAuth 設定の確認

```
Device# show wlan summary

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 12:08:32.941 CEST Tue Oct 6 2020


Number of WLANs: 1

ID Profile Name SSID Status Security
-----------------------------------------------------------------------------------------------------------------------------

23 Gladius1-PSKWEBAUTH Gladius1-PSKWEBAUTH UP [WPA2][PSK][AES],[Web Auth]
```



第 58 章

SAE 認証でのパスワード要素の Hash-to-Element のサポート

Hash-to-Element（H2E）

Hash-to-Element（H2E）は、新しいSAEのパスワード要素（PWE）方式です。この方式では、SAE プロトコルで使用されるシークレット PWE がパスワードから生成されます。

H2E をサポートする STA は AP との SAE を開始するときに、AP が H2E をサポートしているかどうかを確認します。サポートしている場合、AP は H2E を使用して、SAE のコミットメッセージで新しく定義されたステータスコード値を使用して PWE を導出します。

STA で Hunting-and-Pecking を使用する場合、SAE 交換全体は変更されません。

H2E の使用中、PWE の導出は次の項目で構成されます。

- パスワードからのシークレット中間要素 PT の導出。これは、サポートされる各グループのデバイスでパスワードが最初に設定されるときに、オフラインで実行できます。
- 保存された PT からの PWE の導出。これは、ネゴシエートされたグループとピアの MAC アドレスに依存します。これは、SAE 交換時にリアルタイムで実行されます。

（注）

- H2E方式には、グループダウングレードの中間者攻撃からの保護も組み込まれています。SAE 交換時、ピアは PMK の導出にバインドされた拒否グループのリストを交換します。各ピアは、受信したリストをサポートされるグループのリストと比較し、不一致がある場合はダウングレード攻撃として検出し、認証を終了します。

YANG（RPC モデル）

SAE のパスワード要素（PWE）モードの RPC を作成するには、次の RPC モデルを使用します。

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:0a77124f-c563-469d-bd21-cc625a9691cc">
<nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<sae-pwe-mode>both-h2e-hnp</sae-pwe-mode>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>
```

（注） 現在のインフラの制限により、**delete** 操作で実行されるアクションは一度に 1 つです。つまり、YANG モジュールでは、複数ノードでの **delete** 操作はサポートされていません。

WPA3 SAE H2E 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	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan WPA3 1 WPA3`	WLAN コンフィギュレーション サブモードを開始します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**no security ft over-the-ds** 例： `Device(config-wlan)# no security ft over-the-ds`	WLAN のデータ ソース経由の高速移行を無効にします。
ステップ 5	**no security ft** 例： `Device(config-wlan)# no security ft`	WLAN の 802.11r 高速移行を無効にします。
ステップ 6	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。これで PMF は無効になります。
ステップ 7	**security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# security wpa wpa2 ciphers aes`	WPA2 暗号化を設定します。 （注） **no security wpa wpa2 ciphers aes** コマンドを使用して、暗号が設定されているかどうかを確認できます。暗号がリセットされない場合は、暗号を設定します。
ステップ 8	**security wpa psk set-key ascii** *value preshared-key* 例： `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	事前共有キーを指定します。
ステップ 9	**security wpa wpa3** 例： `Device(config-wlan)# security wpa wpa3`	WPA3 のサポートを有効にします。
ステップ 10	**security wpa akm sae** 例： `Device(config-wlan)# security wpa akm sae`	AKM SAE のサポートを有効にします。
ステップ 11	**security wpa akm sae pwe** {**h2e** | **hnp** | **both-h2e-hnp**} 例： `Device(config-wlan)# security wpa akm sae pwe`	AKM SAE PWE のサポートを有効にします。 PWE は次のオプションをサポートしています。

	コマンドまたはアクション	目的
		• h2e：Hash-to-Element のみ。 HnP を無効にします。 • hnp：Hunting and Pecking のみ。H2E を無効にします。 • Both-h2e-hnp：Hash-to-Element と Hunting and Pecking の両方のサポート（デフォルトのオプションです）。
ステップ 12	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 13	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。

WLAN での WPA3 SAE H2E サポートの確認

WLAN ID に基づいて WLAN プロパティ（PWE 方式）を表示するには、次のコマンドを使用します。

```
Device# show wlan id 1
WLAN Profile Name     : wpa3
================================================
Identifier                                       : 1
Description                                      :
Network Name (SSID)                              : wpa3
Status                                           : Enabled
Broadcast SSID                                   : Enabled
Advertise-Apname                                 : Disabled
Universal AP Admin                               : Disabled
Max Associated Clients per WLAN                  : 0
Max Associated Clients per AP per WLAN           : 0
Max Associated Clients per AP Radio per WLAN     : 200
OKC                                              : Enabled
Number of Active Clients                         : 0
CHD per WLAN                                     : Enabled
WMM                                              : Allowed
WiFi Direct Policy                               : Disabled
Channel Scan Defer Priority:
  Priority (default)                             : 5
  Priority (default)                             : 6
Scan Defer Time (msecs)                          : 100
Media Stream Multicast-direct                    : Disabled
CCX - AironetIe Support                          : Disabled
Peer-to-Peer Blocking Action                     : Disabled
DTIM period for 802.11a radio                    : 1
DTIM period for 802.11b radio                    : 1
```

```
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Mac Filter Override Authorization list name     : Disabled
Accounting list name                            :
802.1x authentication list name                 : Disabled
802.1x authorization list name                  : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Disabled
        WPA3 (WPA3 IE)                          : Enabled
            AES Cipher                          : Enabled
            CCMP256 Cipher                      : Disabled
            GCMP128 Cipher                      : Disabled
            GCMP256 Cipher                      : Disabled
        Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            Dot1x-SHA256                        : Disabled
            PSK-SHA256                          : Disabled
            SAE                                 : Enabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    SAE PWE Method                              : Hash to Element(H2E)
    Transition Disable                          : Disabled
    CCKM TSF Tolerance (msecs)                  : 1000
    OWE Transition Mode                         : Disabled
    OSEN                                        : Disabled
    FT Support                                  : Disabled
        FT Reassociation Timeout (secs)         : 20
        FT Over-The-DS mode                     : Disabled
    PMF Support                                 : Required
        PMF Association Comeback Timeout (secs): 1
        PMF SA Query Time (msecs)               : 200
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Authorization List Name             : Disabled
    Webauth Parameter Map                       : Disabled
Band Select                                     : Disabled
Load Balancing                                  : Disabled
Multicast Buffer                                : Disabled
Multicast Buffers (frames)                      : 0
IP Source Guard                                 : Disabled
Assisted-Roaming
    Neighbor List                               : Enabled
    Prediction List                             : Disabled
    Dual Band Support                           : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                  : Enabled
    BSS Max Idle                                : Enabled
        Protected Mode                          : Disabled
    Traffic Filtering Service                   : Disabled
    BSS Transition                              : Enabled
        Disassociation Imminent                 : Disabled
            Optimised Roaming Timer (TBTTS)     : 40
```

```
            Timer (TBTTS)                          : 200
        Dual Neighbor List                         : Disabled
    WNM Sleep Mode                                 : Disabled
802.11ac MU-MIMO                                   : Enabled
802.11ax parameters
    802.11ax Operation Status                      : Enabled
    OFDMA Downlink                                 : Enabled
    OFDMA Uplink                                   : Enabled
    MU-MIMO Downlink                               : Enabled
    MU-MIMO Uplink                                 : Enabled
    BSS Target Wake Up Time                        : Enabled
    BSS Target Wake Up Time Broadcast Support      : Enabled
802.11 protocols in 2.4ghz band
    Protocol                                       : dot11bg
Advanced Scheduling Requests Handling              : Enabled
mDNS Gateway Status                                : Bridge
WIFI Alliance Agile Multiband                      : Disabled
Device Analytics
    Advertise Support                              : Enabled
    Advertise Support for PC analytics             : Enabled
    Share Data with Client                         : Disabled
Client Scan Report (11k Beacon Radio Measurement)
    Request on Association                         : Disabled
    Request on Roam                                : Disabled
WiFi to Cellular Steering                          : Disabled
Advanced Scheduling Requests Handling              : Enabled
Locally Administered Address Configuration
    Deny LAA clients                               : Disabled
```

PWE 方式を H2E または HnP として使用しているクライアント関連付けを確認するには、次のコマンドを使用します。

```
Device# show wireless client mac-address e884.a52c.47a5 detail
Client MAC Address : e884.a52c.47a5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 11.11.0.65
Client IPv6 Addresses : fe80::c80f:bb8c:86f6:f71f
Client Username: N/A
AP MAC Address : d4ad.bda2.e9e0
AP Name: APA453.0E7B.E73C
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: wpa3
Wireless LAN Network Name (SSID): wpa3
BSSID : d4ad.bda2.e9ef
Connected For : 72 seconds
Protocol : 802.11ax - 5 GHz
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 2
Authentication Algorithm : Simultaneous Authentication of Equals (SAE)
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1728 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
```

```
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m6 ss2
Supported Rates : 6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 08/24/2021 04:39:47 Pacific
Client Join Time:
  Join Time Of Client : 08/24/2021 04:39:47 Pacific
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 72 seconds
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
AAA override passphrase : No
SAE PWE Method : Hash to Element(H2E)
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : Yes
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : VLAN0011
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90000006
  IIF ID              : 0x90000006
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 0000000000000000C76750C17
  Acct Session ID  : 0x00000000
  Auth Method Status List
   Method : SAE
  Local Policies:
   Service Template : wlan_svc_default-policy-profile_local (priority 254)
    VLAN             : VLAN0011
    Absolute-Timer   : 1800
  Server Policies:
  Resultant Policies:
                VLAN Name        : VLAN0011
    VLAN             : 11
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
```

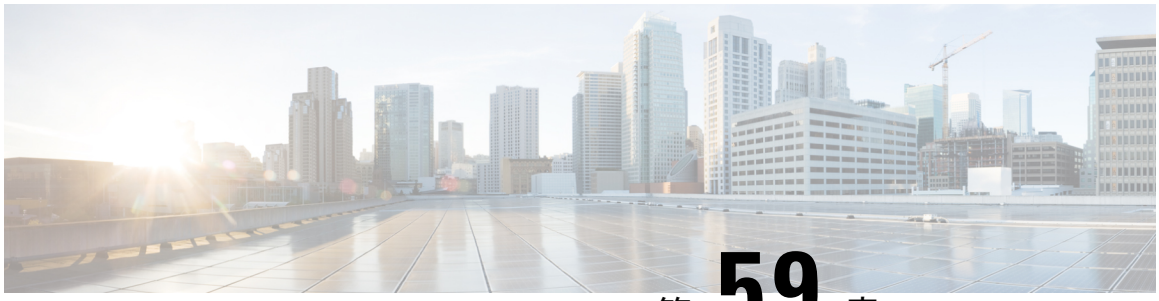
```
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Implemented
11v DMS Capable : No
QoS Map Capable : Yes
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
Client Statistics:
  Number of Bytes Received from Client : 21757
  Number of Bytes Sent to Client : 4963
  Number of Packets Received from Client : 196
  Number of Packets Sent to Client : 37
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -72 dBm
  Signal to Noise Ratio : 20 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: Neighbor Report, Passive Beacon Measurement, Active Beacon Measurement,
 Table Beacon Measurement
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
```

H2E および HnP を使用する SAE 認証の数を表示するには、次のコマンドを使用します。

```
Device# show wireless stats client detail
Total Number of Clients : 0

Protocol Statistics

--------------------------------------------------------------------------------
Protcol            Client Count
 802.11b              : 0
 802.11g              : 0
 802.11a              : 0
 802.11n-2.4GHz       : 0
 802.11n-5 GHz        : 0
 802.11ac             : 0
 802.11ax-5 GHz       : 0
 802.11ax-2.4 GHz     : 0
  802.11ax-6 GHz      : 0



Current client state statistics:
--------------------------------------------------------------------------------
  Authenticating         : 0
  Mobility               : 0
  IP Learn               : 0
  Webauth Pending        : 0
  Run                    : 0
  Delete-in-Progress     : 0


Client Summary
```

```
-----------------------------
Current Clients : 0
Excluded Clients: 0
Disabled Clients: 0
Foreign Clients : 0
Anchor Clients  : 0
Local Clients   : 0
Idle Clients    : 0
Locally Administered MAC Clients: 0

client global statistics:
--------------------------------------------------------------------------------
Total association requests received             : 0
Total association attempts                      : 0
Total FT/LocalAuth requests                     : 0
Total association failures                      : 0
Total association response accepts              : 0
Total association response rejects              : 0
Total association response errors               : 0
Total association failures due to exclusion list      : 0
Total association drops due to multicast mac    : 0
Total association drops due to random mac       : 0
Total association drops due to throttling       : 0
Total association drops due to unknown bssid    : 0
Total association drops due to parse failure    : 0
Total association drops due to other reasons    : 0
Total association requests wired clients        : 0
Total association drops wired clients           : 0
Total association success wired clients         : 0
Total peer association requests wired clients   : 0
Total peer association drops wired clients      : 0
Total peer association success wired clients    : 0
Total association success wifi direct clients   : 0
Total association rejects wifi direct clients   : 0
Total association response errors               : 0
Total 11r ft authentication requests received   : 0
Total 11r ft authentication response success    : 0
Total 11r ft authentication response failure    : 0
Total 11r ft action requests received           : 0
Total 11r ft action response success            : 0
Total 11r ft action response failure            : 0
Total 11r PMKR0-Name mismatch                   : 0
Total 11r PMKR1-Name mismatch                   : 0
Total 11r MDID mismatch                         : 0
Total AID allocation failures                   : 0
Total AID free failures                         : 0
Total Roam Across Policy Profiles               : 0
Total roam attempts                             : 0
  Total CCKM roam attempts                      : 0
  Total 11r roam attempts                       : 0
  Total 11r slow roam attempts                  : 0
  Total 11i fast roam attempts                  : 0
  Total 11i slow roam attempts                  : 0
  Total other roam type attempts                : 0
Total roam failures in dot11                    : 0

Total WPA3 SAE attempts                         : 0
Total WPA3 SAE successful authentications       : 0
Total WPA3 SAE authentication failures          : 0
  Total incomplete protocol failures            : 0
Total WPA3 SAE commit messages received         : 0
Total WPA3 SAE commit messages rejected                                    : 0
  Total unsupported group rejections                                       : 0
  Total PWE method mismatch for SAE Hash to Element commit received        : 0
```

```
  Total PWE method mismatch for SAE Hunting And Pecking commit received : 0
Total WPA3 SAE commit messages sent              : 0
Total WPA3 SAE confirm messages received         : 0
Total WPA3 SAE confirm messages rejected         : 0
  Total WPA3 SAE message confirm field mismatch  : 0
  Total WPA3 SAE confirm message invalid length  : 0
Total WPA3 SAE confirm messages sent             : 0
Total WPA3 SAE Open Sessions                     : 0
Total SAE Message drops due to throttling        : 0
Total WPA3 SAE Hash to Element commit received   : 0
Total WPA3 SAE Hunting and Pecking commit received : 0

Total Flexconnect local-auth roam attempts       : 0
  Total AP 11i fast roam attempts                : 0
  Total AP 11i slow roam attempts                : 0
  Total 11r flex roam attempts                   : 0
```



第 59 章

Cisco Umbrella WLAN

Cisco Umbrella WLAN について

Cisco Umbrella WLAN は、既知と緊急の両方の脅威を自動検出する、クラウド提供のネットワーク セキュリティ サービスをドメイン ネーム システム（DNS） レベルで提供します。

この機能により、マルウェア、ボットネットワーク、およびフィッシングが実際に悪意のある脅威になる前に、それらをホストしているサイトをブロックできます。

Cisco Umbrella WLAN を使用すると、次のことが可能です。

- シングル ポイントでのユーザー グループごとのポリシーの設定。
- ネットワーク、グループ、ユーザー、デバイス、または IP アドレスごとのポリシーの設定。

  ポリシーの優先順位は次のとおりです。

  1. ローカル ポリシー
  2. AP グループ
  3. WLAN

- リアルタイムのビジュアルセキュリティアクティビティダッシュボードと集約レポート。
- スケジュール設定と電子メールによるレポートの送信。
- 最大 60 のコンテンツカテゴリのサポートとカスタム許可リストエントリとブロックリストエントリを追加するためのプロビジョニング。

この機能は、次のシナリオでは機能しません。

- アプリケーションまたはホストが、DNS を使用する代わりに IP アドレスを直接使用してドメイン名をクエリしている場合。
- クライアントが Web プロキシに接続されていて、サーバー アドレスを解決するための DNS クエリを送信しない場合。

Cisco Umbrella アカウントへの 組み込みワイヤレスコントローラの登録

はじめる前に

- Cisco Umbrella のアカウントが必要です。
- Cisco Umbrella からの API トークンが必要です。

組み込みワイヤレスコントローラは、Umbrella パラメータマップを使用して Cisco Umbrella サーバーに登録されます。Umbrella パラメータ マップごとに API トークンが必要です。Cisco Umbrella は、 組み込みワイヤレスコントローラのデバイス ID を使用して応答します。デバイス ID は、Umbrella パラメータ マップ名と 1 対 1 でマッピングされています。

Cisco Umbrella ダッシュボードを使用した 組み込みワイヤレスコントローラの API トークンの取得

Cisco Umbrella ダッシュボードで、[Device Name] に 組み込みワイヤレスコントローラとその ID が表示されていることを確認します。

組み込みワイヤレスコントローラでの API トークンの適用

ネットワークに Cisco Umbrella の API トークンを登録します。

DNS クエリと応答

WLAN にデバイスを登録して Umbrella パラメータ マップを設定すると、WLAN に接続しているクライアントからの DNS クエリが Umbrella DNS リゾルバにリダイレクトされるようになります。

（注） これは、ローカル ドメインの正規表現パラメータ マップに設定されていないすべてのドメインに適用されます。

クエリと応答は、Umbrella パラメータ マップの DNScrypt オプションに基づいて暗号化されます。

Cisco Umbrella の設定の詳細については、『Integration for ISR 4K and ISR 1100 – Security Configuration Guide』を参照してください。

制限事項と考慮事項

この機能の制限事項と考慮事項は次のとおりです。

- デバイス登録が成功すると、ワイヤレス Cisco Umbrella プロファイルを WLAN や AP グループなどのワイヤレス エンティティに適用できます。
- L3 モビリティの場合、Cisco Umbrella は常にアンカー組み込みワイヤレスコントローラで適用する必要があります。
- DHCP 配下に 2 つの DNS サーバーが設定されている場合は、2 つの Cisco Umbrella サーバー IP が DHCP オプション 6 からクライアントに送信されます。DHCP 配下に 1 つの DNS サーバーだけが存在する場合は、DHCP オプション 6 の一部として 1 つの Cisco Umbrella サーバー IP のみが送信されます。

Cisco Umbrella WLAN の設定

組み込みワイヤレスコントローラで Cisco Umbrella を設定するには、次の作業を行います。

- Cisco Umbrella ダッシュボードから API トークンを取得する必要があります。
- Cisco Umbrella 登録サーバー（api.opendns.com）との HTTPS 接続を確立するためには、ルート証明書が必要です。**crypto pki trustpool import terminal** コマンドを使用して、**digicert.com** から 組み込みワイヤレスコントローラにルート証明書をインポートする必要があります。

トラスト プールへの CA 証明書のインポート

始める前に

ここでは、ルート証明書を取得して Cisco Umbrella 登録サーバとの HTTPS 接続を確立する方法について詳しく説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかの作業を実行します。 • **crypto pki trustpool import url** *url* `Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	

	コマンドまたはアクション	目的
	シスコの Web サイトからルート証明書を直接インポートします。 （注）　Trustpool バンドルには、他の CA 証明書とともに *digicert.com* のルート証明書が含まれています。 • **crypto pki trustpool import terminal** `Device(config)#` **`crypto pki trustpool import terminal`** import terminal コマンドを実行して、ルート証明書をインポートします。 • 次の場所で入手できる PEM 形式の CA 証明書を入力します。「関連情報」の項を参照して、CA 証明書をダウンロードしてください。 `-----BEGIN CERTIFICATE-----` [illegible] `SaZMkE4f97Q=` `-----END CERTIFICATE-----` **digicert.com** から CA 証明書を貼り付けて、ルート証明書をインポートします。	

	コマンドまたはアクション	目的
ステップ 3	**quit** 例： `Device(config)# quit`	**quit** コマンドを入力して、ルート証明書をインポートします。 （注） 証明書のインポートが完了すると、メッセージが届きます。

ローカル ドメインの正規表現パラメータ マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル設定モードを開始します。
ステップ 2	**parameter-map type regex** *parameter-map-name* 例： `Device(config)# parameter-map type regex dns_wl`	正規表現パラメータ マップを作成します。
ステップ 3	**pattern** *regex-pattern* 例： `Device(config-profile)# pattern www.google.com`	照合する正規表現パターンを設定します。 （注） 次のパターンがサポートされています。 • .* で始まる。例：**.*facebook.com** • .* で始まり、*で終わる。例：**.*google*** • * で始まる。例：***facebook.com** • * で始まり、* で終わる。例：***google*** • * で終わる。例：**www.facebook*** • 特殊文字なし。例：**www.facebook.com**

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN でのパラメータ マップ名の設定（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 Name] をクリックします。[Edit Policy Profile] ウィンドウが表示されます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [Umbrella] 設定で、[Umbrella Parameter Map] ドロップダウンリストからパラメータマップを選択します。

ステップ 5 [Flex DHCP Option for DNS] および [DNS Traffic Redirect]トグルボタンを有効または無効にします。

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

Umbrella パラメータ マップの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	Cisco Umbrella グローバルパラメータ マップを作成します。
ステップ 3	**token** *token-value* 例： `Device(config-profile)# token 5XXXXXXXXCXXXXXXXAXXXXXXXFXXXXCXXXXXXXX`	Umbrella トークンを設定します。

	コマンドまたはアクション	目的
ステップ 4	**local-domain** *regex-parameter-map-name* 例： `Device(config-profile)# local-domain dns_wl`	ローカル ドメインの正規表現パラメータ マップを設定します。
ステップ 5	**resolver** { **IPv4** *X.X.X.X* | **IPv6** *X:X:X:X::X*} 例： `Device(config-profile)# resolver IPv6 10:1:1:1::10`	エニーキャストアドレスを設定します。特定のアドレスが設定されていない場合はデフォルトのアドレスが適用されます。
ステップ 6	**end** 例： `Device(config-profile)# end`	特権 EXEC モードに戻ります。

DNScrypt の有効化または無効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Threat Defence]** > **[Umbrella]** を選択します。

ステップ 2 Cisco Umbrella から受け取った [Registration Token] を入力します。または [Click here to get your Token] をクリックして、Cisco Umbrella からトークンを取得することもできます。

ステップ 3 フィルタリングから除外する [Whitelist Domains] を入力します。

ステップ 4 [Enable DNS Packets Encryption] チェックボックスをオンまたはオフにして、DNS パケットを暗号化または復号します。

ステップ 5 [Apply] をクリックします。

DNScrypt の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	Umbrella グローバル パラメータ マップを作成します。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **dnscrypt** 例： `Device(config-profile)# no dnscrypt`	DNScrypt を有効または無効にします。 デフォルトでは、DNScrypt オプションは有効です。 （注） DNS 暗号化応答がデータ DTLS暗号化トンネル（モビリティトンネルまたは AP CAPWAP トンネル）で送信される場合、Cisco Umbrella DNScrypt はサポートされません。
ステップ 4	**end** 例： `Device(config-profile)# end`	特権 EXEC モードに戻ります。

UDP セッションのタイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	Umbrella グローバル パラメータ マップを作成します。
ステップ 3	**udp-timeout** *timeout_value* 例： `Device(config-profile)# udp-timeout 2`	UDP セッションのタイムアウト値を設定します。 *timeout_value* の範囲は 1 ～ 30 秒です。 （注） **public-key** および **resolver** パラメータマップ オプションには、デフォルト値が自動的に入力されます。したがって、変更する必要はありません。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-profile)# end`	特権 EXEC モードに戻ります。

WLAN でのパラメータ マップ名の設定（GUI）

手順

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

ステップ 2 [Policy Profile Name] をクリックします。[Edit Policy Profile] ウィンドウが表示されます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [Umbrella] 設定で、[Umbrella Parameter Map] ドロップダウンリストからパラメータマップを選択します。

ステップ 5 [Flex DHCP Option for DNS] および [DNS Traffic Redirect]トグルボタンを有効または無効にします。

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

WLAN でのパラメータ マップ名の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**umbrella-param-map** *umbrella-name* 例： `Device(config-wireless-policy)# umbrella-param-map global`	WLAN の Umbrella OpenDNS 機能を設定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Cisco Umbrella 設定の確認

Umbrella 設定の詳細を表示するには、次のコマンドを使用します。

```
Device# show umbrella config
Umbrella Configuration
=======================
Token: 5XXXXXXABXXXXXFXXXXXXXXXXDXXXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxx
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: Not enabled
Public-key: NONE
UDP Timeout: 5 seconds
Resolver address:
1. 10.1.1.1
2. 5.5.5.5
3. XXXX:120:50::50
4. XXXX:120:30::30
```

Umbrella DNSCrypt の詳細を表示するには、次のコマンドを使用します。

```
Device# show umbrella dnscrypt
DNSCrypt: Enabled
   Public-key:
B111:XXXX:XXXX:XXXX:3E2B:XXXX:XXXX:XXXE:XXX3:3XXX:DXXX:XXXX:BXXX:XXXB:XXXX:FXXX
   Certificate Update Status: In Progress
```

Umbrella グローバル パラメータ マップの詳細を表示するには、次のコマンドを使用します。

```
Device# show parameter-map type umbrella global
```

正規表現パラメータ マップの詳細を表示するには、次のコマンドを使用します。

```
Device# show parameter-map type regex <parameter-map-name>
```

AP の Umbrella の詳細を表示するには、次のコマンドを使用します。

```
AP#show client opendns summary
Server-IP role
208.67.220.220 Primary
208.67.222.222 Secondary

Server-IP role
2620:119:53::53 Primary
2620:119:35::35 Secondary

Wlan Id DHCP OpenDNS Override Force Mode
0 true false
1 false false
...

15 false false
```

```
Profile-name Profile-id
vj-1 010a29b176b34108
global 010a57bf502c85d4
vj-2 010ae385ce6c1256
AP0010.10A7.1000#

Client to profile command

AP#show client opendns address 50:3e:aa:ce:50:17
Client-mac Profile-name
50:3E:AA:CE:50:17 vj-1
AP0010.10A7.1000#
```

第 60 章

ローカルで有効な証明書

ローカルで有効な証明書について

このモジュールでは、ローカルで有効な証明書（LSC）を使用するように Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラおよびLightweightアクセスポイント（LAP）を設定する方法について説明します。LSC を使用する公開キーインフラストラクチャ（PKI）を選択した場合は、AP と組み込みワイヤレスコントローラで LSC を生成でき、証明書を使用して組み込みワイヤレスコントローラと AP を手動で認証できます。

シスコ 組み込みワイヤレスコントローラでは、LSC を使用するように組み込みワイヤレスコントローラを設定できます。独自の PKI でセキュリティを強化して認証局（CA）を管理し、生成された証明書でポリシー、制約事項、および使用方法を定義する場合は、LSC を使用します。

組み込みワイヤレスコントローラで新しい LSC 証明書をプロビジョニングし、CA サーバーから Lightweight アクセスポイント（LAP）をプロビジョニングする必要があります。

LAP は、CAPWAP プロトコルを使用して組み込みワイヤレスコントローラと通信します。証明書への署名と、LAP および組み込みワイヤレスコントローラ自体の CA 証明書の発行についての要求は、組み込みワイヤレスコントローラから開始する必要があります。LAP は CA サーバーと直接通信しません。CA サーバーの詳細が組み込みワイヤレスコントローラで設定されていて、アクセス可能である必要があります。

組み込みワイヤレスコントローラは、デバイス上で生成された certReqs を CA に転送するために Simple Certificate Enrollment Protocol（SCEP）を使用し、CA から署名済み証明書を取得するために SCEP を再度使用します。

SCEP は、証明書の登録と失効をサポートするために PKI クライアントと CA サーバーで使用される証明書管理プロトコルです。SCEP はシスコで広く使用され、多くの CA サーバーでサポートされています。SCEP では、HTTP は PKI メッセージのトランスポートプロトコルとして使用されます。SCEP の主な目的は、ネットワーク デバイスに証明書を安全に発行することです。SCEP は多くの操作に対応していますが、このリリースでは次の操作に使用されています。

- CA およびルータアドバタイズメント（RA）公開キーの配布
- 認証登録

コントローラでの証明書プロビジョニング

新しい LSC 証明書（CA 証明書とデバイス証明書の両方）をコントローラにインストールする必要があります。

SCEP を使用する場合、CA 証明書は CA サーバーから受け取ります。この時点では、コントローラに証明書は存在しません。CA 証明書は get 操作で取得後、コントローラにインストールされます。AP が LSC でプロビジョニングされるときに、同じ CA 証明書が AP にもプッシュされます。

デバイスの証明書の登録操作

CA 署名付き証明書を要求する LAP とコントローラの両方に対して、certRequest が PKCS#10 メッセージとして送信されます。certRequest には、X.509 証明書に含まれる件名、公開キー、およびその他の属性が含まれています。また、要求者の秘密キーでデジタル署名される必要があります。これらは CA に送信され、そこで certRequest が X.509 証明書に変換されます。

PKCS#10 certRequest を受け取る CA には、要求者の ID を認証し、要求が変更されていないことを確認するための追加情報が必要です（証明書の要求や応答を送受信するために、PKCS#10 は PKCS#7 などの他のアプローチと組み合わされることがあります）。

PKCS#10 は PKCS#7 Signed Data メッセージタイプでラップされます。これは SCEP クライアント機能の一部としてサポートされ、PKCSReq メッセージがコントローラに送信されます。登録操作が成功すると、CA 証明書とデバイス証明書の両方がコントローラで使用可能になります。

Lightweight アクセス ポイントでの証明書プロビジョニング

LAP で新しい証明書をプロビジョニングするには、CAPWAP モードの間に LAP が新しい署名付き X.509 証明書を取得できる必要があります。そのために、LAP はコントローラに certRequest を送信します。コントローラは CA プロキシとして機能し、CA により署名された LAP 用の certRequest を取得を支援します。

certReq および certResponse は LWAPP ペイロードを使用して LAP に送信されます。

LSC CA 証明書と LAP デバイス証明書の両方が LAP にインストールされ、システムが自動的に再起動します。システムは、次回起動時には LSC を使用するように設定されているため、AP は join 要求の一部として LSC デバイス証明書をコントローラに送信します。join 応答の一部として、コントローラは新しいデバイス証明書を送信し、新しい CA ルート証明書を使用して受信 LAP 証明書も検証します。

次の作業

コントローラおよび AP の既存の PKI インフラストラクチャを使用して証明書の登録を設定、許可、および管理するには、LSC プロビジョニング機能を使用する必要があります。

ローカルで有効な証明書の制約事項

- LSC ワークフローは、FIPS + WLANCC モードでは異なります。CA サーバーは Enrollment over Secure Transport（EST）プロトコルをサポートし、FIPS + WLANCC モードで EC 証明書を発行できる必要があります。
- 楕円曲線デジタル署名アルゴリズム（ECDSA）暗号は、AP とコントローラの両方に LSC でプロビジョニングされた EC 証明書がある場合にのみ機能します。
- EC 証明書（LSC-EC）は、CA サーバーが（SCEP ではなく）EST をサポートしている場合にのみプロビジョニングできます。
- EC 証明書をプロビジョニングするには、FIPS + CC セキュリティモードを設定する必要があります。

ローカルで有効な証明書のプロビジョニング

PKI トラストポイントの RSA キーの設定

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	**crypto key generate rsa** [**exportable**] **general-keys modulus** *key_size* **label** *RSA_key* 例：	PKI トラストポイントの RSA キーを設定します。 **exportable** はオプションのキーワードです。エクスポート可能なキーの設定は任

	コマンドまたはアクション	目的
	`Device(config)# crypto key generate rsa exportable general-keys modulus 2048 label lsc-tp`	意です。選択すると、必要に応じて、ボックスから出してキーをエクスポートできます。 • key_size：キー係数のサイズ。有効な範囲は 2048 ～ 4096 です。 • *RSA_key*：RSA キーペアのラベル。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

PKI トラストポイントパラメータの設定

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	**crypto pki trustpoint** *trustpoint_name* 例： `Device(config)# crypto pki trustpoint microsoft-ca`	外部 CA サーバーの新しいトラストポイントを作成します。*trustpoint_name* はトラストポイント名を指します。
ステップ 3	**enrollment url** *HTTP_URL* 例： `Device(ca-trustpoint)# enrollment url http://CA_server/certsrv/mscep/mscep.dll`	ルータが証明書要求を送信する CA の URL を指定します。 url url：ルータが証明書要求を送信するファイルシステムの URL。URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。登録方式オプションの詳細については、「enrollment url (ca-trustpoint)」コマンド ページを参照してください。
ステップ 4	**subject-name** *subject_name* 例： `Device(ca-trustpoint)# subject-name C=IN,`	トラストポイントの件名パラメータを作成します。

	コマンドまたはアクション	目的
	ST=KA, L=Bengaluru, O=Cisco, CN=eagle-eye/emailAddress=support@abc.com	
ステップ 5	**rsakeypair** *RSA_key key_size* 例： `Device(ca-trustpoint)# rsakeypair ewlc-tp1`	RSA キーをトラストポイントの RSA キーにマッピングします。 • *RSA_key*：RSA キーペアのラベル。 • *key_size*：署名キーの長さ。範囲は 360 ～ 4096 です。
ステップ 6	**revocation** {**crl** | **none** | **ocsp**} 例： `Device(ca-trustpoint)# revocation none`	失効を確認します。
ステップ 7	**end** 例： `Device(ca-trustpoint)# end`	特権 EXEC モードに戻ります。

PKI トラストポイントの認証と登録（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoints] タブをクリックします。

ステップ 3 [Add Trustpoint] ダイアログボックスで、次の情報を入力します。

a) [Label] フィールドに、RSA キーラベルを入力します。
b) [Enrollment URL] フィールドに、登録 URL を入力します。
c) [Authenticate] チェックボックスをオンにして、登録 URL の公開証明書を認証します。
d) [Subject Name] セクションで、[Country Code]、[State]、[Location]、[Organisation]、[Domain Name]、および [Email Address] を入力します。
e) [Key Generated] チェックボックスをオンにして、使用可能な RSA キーペアを表示します。[Available RSA Keypairs] ドロップダウンリストからオプションを選択します。
f) [Enroll Trustpoint] チェックボックスをオンにします。
g) [Password] フィールドにパスワードを入力します。
h) [Re-Enter Password] フィールドで、パスワードを確認します。
i) [Apply to Device] をクリックします。

新しいトラストポイントがトラストポイント名リストに追加されます。

CA サーバーを使用した PKI トラストポイントの認証と登録（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。
ステップ 2	**crypto pki authenticate** *trustpoint_name* 例： `Device(config)# crypto pki authenticate microsoft-ca`	CA 証明書を取得します。

ステップ 3	**yes**
	例：
	`Device(config)# % Do you accept this certificate? [yes/no]:`
	`yes Trustpoint CA certificate accepted.`	

ステップ 4	**crypto pki enroll** *trustpoint_name*
	例：
	`Device(config)# crypto pki enroll microsoft-ca`
	`% Start certificate enrollment ..`
	`% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it.`
		クライアント証明書を登録します。

ステップ 5	**password** 例： `Device(config)# abcd123`	CA サーバーへのチャレンジパスワードを入力します。
ステップ 6	**password** 例： `Device(config)# abcd123`	CA サーバーへのチャレンジパスワードを再入力します。
ステップ 7	**yes** 例：	

	コマンドまたはアクション	目的
	Device(config)# **% Include the router serial number in the subject name? [yes/no]: yes**	
ステップ 8	**no** 例： Device(config)# **% Include an IP address in the subject name? [no]: no**	
ステップ 9	**yes** 例： Device(config)# **Request certificate from CA? [yes/no]: yes** **% Certificate request sent to Certificate Authority** **% The 'show crypto pki certificate verbose client' command will show the fingerprint.**	
ステップ 10	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。

LSC 証明書による AP の接続試行回数の設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ 2 [All Access Points] ウィンドウで LSC プロビジョンの名前をクリックします。
ステップ 3 [Status] ドロップダウンリストから、LSC を有効にするステータスを選択します。
ステップ 4 [Trustpoint Name] ドロップダウンリストからトラストポイントを選択します。
ステップ 5 [Number of Join Attempts] フィールドに、許可される再試行回数を入力します。
ステップ 6 [Apply] をクリックします。

LSC 証明書による AP の接続試行回数の設定（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。
ステップ 2	**ap lsc-provision join-attempt** *number_of_attempts* 例： `デバイス(config)# ap lsc-provision join-attempt 10`	新たにプロビジョニングされた LSC 証明書を使用した AP の接続失敗の最大試行回数を指定します。 AP の接続回数が指定の制限を超えると、AP は製造元でインストールされる証明書（MIC）を使用して再接続します。
ステップ 3	**end** 例： `デバイス(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。

LSC 証明書の件名パラメータの設定

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	**ap lsc-provision subject-name-parameter country** *country-str* **state** *state-str* **city** *city-str* **domain** *domain-str* **org** *org-str* **email-address** *email-addr-str* 例： `Device(config)# ap lsc-provision subject-name-parameter country India state Karnataka city Bangalore domain domain1 org Right email-address adc@gfe.com`	AP によって生成された証明書要求の件名パラメータに含める属性を指定します。
ステップ 3	**end** 例：	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
	`Device(config)# end`	

LSC 証明書のキー サイズの設定

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	**ap lsc-provision key-size**{ **2048** | **3072** | **4096}**} 例： `デバイス(config)# ap lsc-provision key-size 2048`	AP 上の LSC に対して生成されるキーのサイズを指定します。
ステップ 3	**end** 例： `デバイス(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。

アクセスポイントでの LSC プロビジョニング用トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 lsc-provision trustpoint** *tp-name* 例： `Device(config)# ap lsc-provision trustpoint microsoft-ca`	LCS を AP にプロビジョニングする際に使用するトラストポイントを指定します。 tp-name：トラストポイント名。
ステップ 3	**end** 例：	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
	`Device(config)# end`	

AP LSC プロビジョンリストの設定（GUI）

手順

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

ステップ 2 [All Access Points] ウィンドウで、対応する LSC プロビジョンの名前をクリックします。

ステップ 3 [Status] ドロップダウンリストから、LSC を有効にするステータスを選択します。

ステップ 4 [Trustpoint Name] ドロップダウンリストからトラストポイントを選択します。

ステップ 5 [Number of Join Attempts] フィールドに、許可される再試行回数を入力します。

ステップ 6 [Key Size] ドロップダウンリストから、キーを選択します。

ステップ 7 [Edit AP Join Profile] ウィンドウで [CAPWAP] タブをクリックします。

ステップ 8 [Add APs to LSC Provision List] セクションで [Select File] をクリックして、AP の詳細を含む CSV ファイルをアップロードします。

ステップ 9 [**Upload File**（ファイルのアップロード）] をクリックします。

ステップ 10 [AP MAC Address] フィールドに、AP の MAC アドレスを入力して、追加します（プロビジョンリストに追加された AP は、[APs in Provision List] に表示されます）。

ステップ 11 [Subject Name Parameters] セクションに、次の詳細情報を入力します。

- **国**
- **State**
- **市区町村郡（City）**
- **Organisation**
- **部署名（Department）**
- **電子メール アドレス（Email Address）**

ステップ 12 [Apply] をクリックします。

AP LSC プロビジョンリストの設定（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。
ステップ 2	[**no**] **ap lsc-provision mac-address** *mac-addr* 例： `Device(config)# no ap lsc-provision mac-address 001b.3400.02f0`	LSC プロビジョンリストに AP を追加します。 （注） **ap lsc-provision provision-list** コマンドを使用して AP のリストをプロビジョニングできます。 （または） **ap lsc-provision** コマンドを使用してすべての AP をプロビジョニングできます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

すべての AP に対する LSC プロビジョニングの設定（GUI）

手順

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

ステップ 2 [Access Points] ウィンドウで [LSC Provision] セクションを展開します。

ステップ 3 [Status] を [Enabled] 状態に設定します。

（注） [Status] を [Provision List] に設定すると、そのプロビジョンリストに含まれている AP に対してのみ LSC プロビジョニングが設定されます。

ステップ 4 [Trustpoint Name] ドロップダウンリストから、すべての AP に対して適切なトラストポイントを選択します。

ステップ 5 [Number of Join Attempts] フィールドに、AP が組み込みワイヤレスコントローラへの参加を再試行できる回数を入力します。

ステップ 6 [Key Size] ドロップダウンリストから、証明書のキーサイズを選択します。

- **2048**
- **3072**
- **4096**

ステップ 7 [Add APs to LSC Provision List] セクションで [Select File] をクリックして、AP の詳細を含む CSV ファイルをアップロードします。

ステップ 8 [**Upload File**（ファイルのアップロード）] をクリックします。

ステップ 9 [AP MAC Address] フィールドに、AP の MAC アドレスを入力します（プロビジョンリストに追加された AP は、[APs in Provision List] セクションに表示されます）。

ステップ 10 [Subject Name Parameters] セクションに、次の詳細情報を入力します。

1. 国
2. **State**
3. 市区町村郡（**City**）
4. **Organization**
5. 部署名（**Department**）
6. 電子メール アドレス（**Email Address**）

ステップ 11 [Apply] をクリックします。

すべての AP に対する LSC プロビジョニングの設定（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。
ステップ 2	[**no**] **ap lsc-provision** 例： `デバイス(config)# no ap lsc-provision`	すべての AP に対して LSC プロビジョニングを有効にします。 デフォルトでは、LSC プロビジョニングはすべての AP に対して無効になっています。
ステップ 3	**end** 例： `デバイス(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。

プロビジョンリストに含まれる AP に対する LSC プロビジョニングの設定

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。
ステップ 2	**ap lsc-provision provision-list** 例： `デバイス(config)# ap lsc-provision provision-list`	プロビジョンリストに設定されている一連の AP に対して LSC プロビジョニングを有効にします。
ステップ 3	**end** 例： `デバイス(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。

ローカルで有効な証明書のプロビジョニング解除

ローカルで有効な証明書（LSC）のプロビジョニングを解除するには、次の手順を実行します。

1. シャーシを WLAN コモンクライテリア（WLANCC）モードに移行します。
2. LSC とワイヤレス管理トラストポイントをプロビジョニングして、AP をリロードします。詳細については、LSC プロビジョニングおよび管理トラストポイントの設定（754 ページ）を参照してください。
3. 連邦情報処理標準（FIPS）と WLANCC を削除します。詳細については、FIPS および WLAN コモンクライテリアの削除（754 ページ）を参照してください。
4. LSC プロビジョニングを削除します。詳細については、LSC プロビジョニングの削除（755 ページ）を参照してください。

LSC プロビジョニングおよび管理トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 lsc-provision** 例： `Device(config)# ap lsc-provision`	AP LSC プロビジョニングパラメータを設定します。
ステップ 3	**wireless management trustpoint** *trustpoint_name* 例： `Device(config)# wireless management trustpoint trustpoint-name`	LSC の管理トラストポイントを設定します。
ステップ 4	**do write** 例： `Device(config)# do write`	実行コンフィギュレーションをメモリ、ネットワーク、または端末に書き込みます。

FIPS および WLAN コモンクライテリアの削除

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 dtls-version dtls_1_2** 例： `Device(config)# ap dtls-version dtls_1_2`	AP DTLS バージョンを設定します。
ステップ 3	**ap dtls-cipher** *ECDHE-ECDSA-AES256-GCM-SHA384* 例： `Device(config)# ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	AP DTLS 暗号スイートを設定します。

	コマンドまたはアクション	目的
ステップ 4	**no wireless wlancc** 例： `Device(config)# no wireless wlancc`	コントローラの WLAN CC を無効にします。
ステップ 5	**no fips authorization-key** 例： `Device(config)# no fips authorization-key`	FIPS の認証キーを無効にします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**write memory** 例： `Device# write memory`	設定を保存します。
ステップ 8	**reload** 例： `Device# reload`	内部 AP をリロードして、非 FIPS および非 CC モードに移行します。

LSC プロビジョニングの削除

始める前に

スタンバイ AP が起動するのを待ちます。

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	**no ap lsc-provisioning** 例： `Device(config)# no ap lsc-provisioning`	AP LSC プロビジョニングパラメータを無効にします。
ステップ 3	**shutdown** 例： `Device(config)# shutdown`	スタンバイ AP をリロードします。 （注） マスター AP の次のリロードも待ちます。

	コマンドまたはアクション	目的
ステップ 4	**no ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384** 例： `Device(config)# no ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	AP DTLS 暗号スイートを無効にします。
ステップ 5	**no ap dtls-version dtls_1_2** 例： `Device(config)# no ap dtls-version dtls_1_2`	DTLS バージョンを無効にします。
ステップ 6	**no wireless management trustpoint** 例： `Device(config)# no wireless management trustpoint`	ワイヤレス管理トラストポイントを無効にします。
ステップ 7	**reload** 例： `Device# reload`	内部 AP をリロードします。

Trustpool への CA 証明書のインポート（GUI）

PKI Trustpool Management は、コントローラ上のさまざまなサービスによって使用される信頼できる証明書（ダウンロードまたは組み込み）のリストを保存するために使用されます。また、マルチレベル CA 証明書の認証にも使用されます。PKI Trustpool 内の組み込み CA 証明書バンドルが最新のものではない、破損している、または特定の証明書を更新する必要がある場合、シスコから自動更新を受信します。

PKI Trustpool の CA 証明書を手動で更新するには、このタスクを実行します。

（注） LSC が中間 CA によって発行されている場合は、CA 証明書の完全なチェーンを Trustpool にインポートする必要があります。インポートせず、コントローラに完全なチェーンが存在しない状態では AP をプロビジョニングできません。証明書がルート CA によって発行されている場合、インポート手順を実行する必要はありません。

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoint] タブをクリックします。

ステップ 3 [Import] をクリックします。

ステップ 4 [CA Certificate] フィールドで、CA 証明書をコピーして貼り付けます。複数の CA 証明書（.pem 形式）をリンクします。

ステップ 5 [Apply to Device] をクリックします。

Trustpool への CA 証明書のインポート（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。

ステップ 2	**crypto pki trust pool import terminal**
	例：
	`Device(config)# crypto pki trust pool import terminal`
	`% Enter PEM-formatted CA certificate.`
	`% End with a blank line or "quit" on a line by itself.`
	`-----BEGIN CERTIFICATE-----`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`-----END CERTIFICATE-----`
	`Aug 23 02:47:33.450: %PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS: Trustpool Download is successful`
		ルート証明書をインポートします。インポートするためには、digicert.com から CA 証明書を貼り付ける必要があります。

ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

Trustpool にインポートされた CA 証明書のクリーニング（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoint] タブをクリックします。

ステップ 3 [Clean] をクリックします。

（注） ダウンロードした CA 証明書バンドルが消去されますが、組み込みの CA 証明書バンドルは消去されません。

ステップ 4 **[はい（Yes）]** をクリックします。

Trustpool にインポートされた CA 証明書のクリーニング（CLI）

特定の CA 証明書を Trustpool から削除することはできません。ただし、Trustpool にインポートされた CA 証明書はすべてクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto pki trustpool clean** 例： `デバイス(config)# crypto pki trustpool clean`	ダウンロードした CA 証明書バンドルが消去されますが、組み込みの CA 証明書バンドルは消去されません。
ステップ 3	**end** 例： `デバイス(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。

単一の CA 証明書専用の新しいトラストポイントの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto pki trustpoint** *tp-name* 例： `デバイス(config)# crypto pki trustpoint tp_name`	トラストポイントを作成します。
ステップ 3	**enrollment terminal** 例： `デバイス(ca-trustpoint)# enrollment terminal`	トラストポイントの登録端末を作成します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `デバイス(ca-trustpoint)# exit`	トラストポイント設定を終了します。

ステップ 5	**crypto pki authenticate** *tp-name*
	例：
	`デバイス(config)# crypto pki authenticate tp_name`
	`<<< PASTE CA-CERT in PEM format followed by quit >>>`
		トラストポイントを認証します。

LSC 設定の確認

ワイヤレス管理トラストポイントの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless management trustpoint

Trustpoint  Name : microsoft-ca
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
 Private key Info : Available
```

AP の LSC プロビジョン関連の設定に関する詳細を表示するには、次のコマンドを使用します。

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : microsoft-ca
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048

AP LSC-provision List : Enabled
Total number of APs in provision list: 3

Mac Address
-----------
0038.df24.5fd0
2c5a.0f22.d4ca
e4c7.22cd.b74f

Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : lsc-root-tp
```

```
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash : 7f9d05183deecac4e5a79db65d538245685e8e30
LSC Revert Count in AP reboots : 1

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 2

Mac Addresses :
--------------
1880.90f5.1540
2c5a.0f70.84dc
```

LSC の管理トラストポイントの設定（GUI）

手順

ステップ 1 **[Administration]** > **[Management]** > **[HTTP/HTTPS]** の順に選択します。

ステップ 2 [HTTP Trust Point Configuration] セクションで、[Enable Trust Point] を [Enabled] 状態に設定します。

ステップ 3 [Trust Points] ドロップダウンリストから、適切なトラストポイントを選択します。

ステップ 4 設定を保存します。

LSC の管理トラストポイントの設定（CLI）

LSC のプロビジョニング後、AP は自動的に再起動し、ブートアップ後に LSC モードで参加します。同様に、AP LSC のプロビジョニングを削除すると、AP は再起動し、非 LSC モードで接続します。

EWC では、内部 AP は自動的には再起動しません。LSC モードと非 LSC モードで動作させるには、内部 AP を手動で再起動する必要があります。

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 management trustpoint** *trustpoint_name* 例： `デバイス(config)# wireless management trustpoint microsoft-ca`	LSC の管理トラストポイントを設定します。 内部 AP はリロードの前に参加できなくなるため、次の手順を実行して内部 AP をリロードします。
ステップ 3	**write memory** 例： `Device(config)# write memory`	設定を保存します。
ステップ 4	**wireless ewc-ap ap reload** 例： `Device(config)# write memory`	内部 AP をリロードします。これにより、AP 上のコントローラもリロードされます。
ステップ 5	**end** 例： `デバイス(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。

コントローラに接続する MIC および LSC アクセスポイントに関する情報

コントローラに接続する MIC および LSC アクセスポイントのサポートの概要

Cisco IOS XE Bengaluru 17.4.1 以前のリリースでは、デフォルトの証明書（製造元でインストールされる証明書（MIC）または Secure Unique Device Identifier（SUDI））を持つ AP は、ローカルで有効な証明書（LSC）が展開されたコントローラには接続できません。このコントローラの管理証明書は LSC です。この問題を解決するには、LSC が展開されたコントローラに移動する前に、プロビジョニング コントローラを使用してそれらの AP に LSC をプロビジョニングする必要があります。

Cisco IOS XE Bengaluru 17.5.1 以降では、新しい認証ポリシー設定により、MIC AP が LSC が展開されたコントローラに接続でき、LSC と MIC AP がコントローラ内で同時に共存できるようになりました。

推奨事項および制約事項

- CA サーバーが証明書署名要求（CSR）を受け入れるように手動登録（手動介入）で構成されている場合、コントローラは CA サーバーが保留中の応答を送信するのを待ちます。10 分間 CA サーバーからの応答がない場合、フォールバックモードが有効になります。
  - Cisco Wave 2 AP が CSR を再生成し、新しい CSR が CA サーバーに送信されます。
  - Cisco IOS AP が再起動すると、Cisco IOS AP から新しい CSR が送信され、CA サーバーにも送信されます。
- コントローラのローカルで有効な証明書（LSC）は、パスワードチャレンジでは機能しません。このため、LSC を機能させるには、CA サーバーでパスワードの確認を無効にする必要があります。
- Microsoft CA を使用している場合は、CA サーバーとして Windows Server 2012 以降を使用することをお勧めします。

設定ワークフロー

1. コントローラでの LSC の設定（CLI） （762 ページ）
2. AP での AP 証明書ポリシーの有効化（CLI） （763 ページ）
3. AP ポリシー証明書の設定（GUI） （764 ページ）
4. コントローラに接続するための AP の許可リストの設定（CLI） （765 ページ）

コントローラでの LSC の設定（CLI）

CAPWAP-DTLS のコントローラによって使用されるサーバー証明書は、次の設定に基づいています。

始める前に

- 次のワイヤレス管理サービスに適切なトラストポイントを設定して、LSC を有効にしてください。
  - AP 接続プロセス：CAPWAP DTLS サーバー証明書
  - モビリティ接続：モビリティ DTLS 証明書
  - NMSP および CMX 接続：NMSP TLS 証明書

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	**[no] wireless management trustpoint** *trustpoint-name* 例： `Device(config)# wireless management trustpoint trustpoint-name`	LSC 展開コントローラで LSC トラストポイントを設定します。

AP での AP 証明書ポリシーの有効化（CLI）

- 管理トラストポイントが LSC の場合、デフォルトでは、MIC AP はコントローラに接続できません。この設定は、MIC AP がコントローラに接続できるようにするコンフィギュレーションノブの有効化または無効化として機能します。
- この設定は、DTLS ハンドシェイク時に AP が MIC に接続できるようにするコントローラ認証です。

製造元でインストールされる証明書（MIC）の期限切れによる失敗を防ぐには、次に示すようにポリシーを設定してください。

- 証明書マップを作成し、ルールを追加します。

```
configure terminal
crypto pki certificate map map1 1
issuer-name co Cisco Manufacturing CA
```

（注） 同じマップの下に、複数のルールとフィルタを追加できます。前述の例に記載されているルールでは、発行者名に Cisco Manufacturing CA（大文字と小文字を区別しない）が含まれているすべての証明書がこのマップの下で選択されることが指定されています。

- Trustpool ポリシーの下で証明書マップを使用します。

```
configure terminal
crypto pki trustpool policy
match certificate map1 allow expired-certificate
```

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 auth-list ap-cert-policy allow-mic-ap trustpoint** *trustpoint-name* 例： `Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name`	コントローラ証明書チェーンのトラストポイント名を設定します。 （注） **allow-mic-ap trustpoint** コマンドは、仮想コントローラ（クラウド向け Cisco Catalyst 9800-CL ワイヤレス コントローラ）にのみ必要です。他のすべてのアプライアンス コントローラ プラットフォームでは、デフォルトの証明書が選択されています。このデフォルトの証明書は、製造元がインストールした SUDI です。
ステップ 3	**ap auth-list ap-cert-policy allow-mic-ap** 例： `Device(config)# ap auth-list ap-cert-policy allow-mic-ap`	CAPWAP-DTLS ハンドシェイク中に AP 証明書ポリシーを有効にします。
ステップ 4	**ap auth-list ap-cert-policy** {**mac-address** *H.H.H* | **serial-number** *serial-number-ap*} **policy-type mic** 例： `Device(config)# ap auth-list ap-cert-policy mac-address 1111.1111.1111 policy-type mic`	AP 証明書ポリシーを MIC として有効にします。

AP ポリシー証明書の設定（GUI）

手順

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

ステップ 2 [All Access Points] ウィンドウで、[AP Certificate Policy] をクリックします。

ステップ 3 [AP Policy Certificate] ウィンドウで、以下のアクションを実行します。

a) [Authorize APs join with MIC] トグルボタンをクリックして、AP 認証を有効にします。
b) [Trustpoint Name] ドロップダウンリストから、必要なトラストポイントを選択します。
c) [Add MAC or Serial Number] をクリックして、MAC アドレスまたはシリアル番号を手動で追加するか、.csv ファイルを使用して追加します。
[Add MAC or Serial Number] ウィンドウが表示されます。
d) [AP Authlist Type] をクリックし、MAC アドレスまたはシリアル番号を入力します。.csv ファイルをアップロードするか、リストボックスに MAC アドレスを入力します。
新しく追加された MAC アドレスとシリアル番号は、[List of MAC Address and Serial Numbers] の下に表示されます。
e) [Apply] をクリックします。

AP 証明書ポリシーが [AP Inventory] ウィンドウに追加されます。

（注） MIC を使用して新しい AP を追加するには、「AP ポリシー証明書の設定（GUI）」の項で説明されているステップ 1 ～ 3 を実行します。LSC を使用して新しい AP を追加するには、「AP LSC プロビジョンリストの設定（GUI）」と「AP ポリシー証明書の設定（GUI）」のステップ 1 ～ 3 で説明されている手順を実行します。

コントローラに接続するための AP の許可リストの設定（CLI）

AP の許可リストは、イーサネット MAC アドレスまたは AP のシリアル番号に基づいて入力できます。

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 auth-list ap-cert-policy** {**mac-address** *AP-Ethernet-MAC-address* | **serial-number** *AP-serial-number*} **policy-type mic** 例： `Device# ap auth-list ap-cert-policy mac-address 00b0.e192.0d98 policy-type mic`	イーサネット MAC アドレスまたは AP のアセンブリシリアル番号に基づいて AP 証明書ポリシーを設定します。

設定ステータスの確認

AP が AP 証明書ポリシーによって承認されているかどうかを確認するには、次のコマンドを使用します。

```
Device# show ap auth-list ap-cert-policy
Authorize APs joining with MIC : ENABLED
MIC AP policy trustpoint
Name : CISCO_IDEVID_SUDI
Certificate status : Available
Certificate Type : MIC
Certificate Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

AP の MAC アドレスとシリアル番号に関する AP 証明書ポリシーを確認するには、次のコマンドを使用します。

```
Device# show ap auth-list ap-cert-policy mac-address
MAC address      AP cert policy
---------------------------------
1111.2222.3333   MIC
```

```
Device# show ap auth-list ap-cert-policy serial-number
Serial number    AP cert policy
---------------------------------
F1234567890      MIC
```

（注） 無効なトラストポイント（SSC 以外）を設定すると、**allow-mic-ap policy** は有効になりません。無効なトラストポイントを設定すると、次のエラーがコンソールに表示されます。

```
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint lsc-root-tp
Dec 18 07:38:29.944: %CERT_MGR_ERRMSG-3-CERT_MGR_GENERAL_ERR: Chassis 1 R0/0: wncd:
General error: MIC AP Policy trustpoint: 'lsc-root-tp' cert-chain type is LSC, It must
be either MIC or vWLC-SSC
```

LSC フォールバック アクセス ポイント

LSC フォールバック AP について

AP が CAPWAP 用の LSC を使用して設定されているが、DTLS 接続を確立できない場合、AP は再起動し、一定の回数再試行します。LSC を使用した AP の設定方法については、LSC 証明書による AP の接続試行回数の設定（CLI） （748 ページ）を参照してください。

AP は、最大失敗回数に達すると、CAPWAP 用のデフォルトの証明書（MIC）にフォールバックします。この状態は、LSC フォールバックと呼ばれます。

（注） MIC は SUDI 証明書とも呼ばれます。

LSC フォールバック状態のトラブルシューティング

LSC フォールバック状態の AP がコントローラに参加すると、次の syslog が生成されます。

```
Jun 15 23:24:14.836: %APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/0: wncd: Error
in AP: 'AP2c5a.0f70.84dc' with address 70db.9888.cc20 is joined with MIC, while
```

```
configuration
requires LSC. No WLANs will be pushed.
```

コントローラはそのような AP が MIC に参加することを許可し（AP 証明書ポリシーで許可されている場合）、AP は誤って設定された状態で保持されます。

（注） このような状態では、AP は WLAN または SSID 構成をブロードキャストしません。これにより、管理者は以前の障害の理由を調べて AP を回復できます。

次のように **show wireless summary** を使用して、**LSC フォールバック** AP を特定できます。

```
Device# show wireless summary
…
Access Point Summary
…
DTLS LSC fallback APs     20 (No WLANs will be pushed to these APs)
…
For more information on DTLS LSC fallback APs,
    execute 'wireless config validate' and look for reported errors in
    'show wireless config validation status' CLI output.

Use 'show ap config general | inc AP Name | LSC fallback' to list DTLS LSC fallback APs.
Examine LSC fallback reasons / DTLS handshake failures with LSC then
    issue 'ap lsc dtls-fallback clear-certificate / clear-flag' to recover APs
```

リカバリ手順

- **ap lsc dtls-fallback clear-flag** を使用して AP の LSC フォールバックフラグをクリアし、リロードするよう AP に指示します。

（注） AP は、リロード後に CAPWAP DTLS 接続に LSC を再利用します。

- **ap lsc dtls-fallback clear-certificate** を使用して LSC をクリアし、リロードするよう AP に指示します。

（注） AP は、リロード後に CAPWAP-DTLS に MIC を使用します。Dot1x ポート認証に LSC が使用されている場合は、AP 認証のためにスイッチポートでさらにリカバリが必要になります。

（注）

- AP で LSC を保持するには、**ap lsc dtls-fallback clear-flag** コマンドで十分です。**ap lsc dtls-fallback clear-flag** コマンドと **ap lsc dtls-fallback clear-certificate** コマンドを同時に使用する必要はありません。
- リカバリコマンドを発行するときは、AP が接続状態である必要があります。後で **LSC フォールバック**の AP が参加した場合は、コマンドを再発行する必要があります。

第 61 章

証明書の管理

公開キーインフラストラクチャ管理について（GUI）

[Public Key Infrastructure (PKI) Management] ページには、次のタブが表示されます。

[Trustpoints] タブ：新しいトラストポイントを追加、作成、または登録するために使用します。このページには、コントローラに設定されている現在のトラストポイントとトラストポイントのその他の詳細も表示されます。トラストポイントがいずれかの機能に使用されているかどうかも確認できます。たとえば、Webadmin や AP 接続（ワイヤレス管理インターフェイス）などの機能。

[CA Server] タブ：コントローラの認証局（CA）サーバー機能を有効または無効にするために使用します。コントローラで自己署名証明書（SSC）を生成するためには、CA サーバー機能を有効にする必要があります。

[Key Pair Generation] タブ：キーペアを生成するために使用します。

[Certificate Management] タブ：証明書の生成と管理、およびコントローラ上でのすべての証明書関連操作の実行に使用します。

PKI トラストポイントの認証と登録（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoints] タブをクリックします。

ステップ 3 [Add Trustpoint] ダイアログボックスで、次の情報を入力します。

a) [Label] フィールドに、RSA キーラベルを入力します。
b) [Enrollment URL] フィールドに、登録 URL を入力します。
c) [Authenticate] チェックボックスをオンにして、登録 URL の公開証明書を認証します。
d) [Subject Name] セクションで、[Country Code]、[State]、[Location]、[Organisation]、[Domain Name]、および [Email Address] を入力します。
e) [Key Generated] チェック ボックスをオンにして、使用可能な RSA キーペアを表示します。[Available RSA Keypairs] ドロップダウンリストからオプションを選択します。
f) [Enroll Trustpoint] チェックボックスをオンにします。
g) [Password] フィールドにパスワードを入力します。
h) [Re-Enter Password] フィールドで、パスワードを確認します。
i) [Apply to Device] をクリックします。

新しいトラストポイントがトラストポイント名リストに追加されます。

AP 自己署名証明書の生成（GUI）

（注） この項は、仮想コントローラ（クラウド向け Cisco Catalyst 9800-CL ワイヤレスコントローラ）にのみ有効であり、アプライアンスベースのコントローラ（Cisco Catalyst 9800-40 ワイヤレスコントローラ、Cisco Catalyst 9800-80 ワイヤレスコントローラ、Cisco Catalyst 9800-L ワイヤレスコントローラ（銅線アップリンク）、および Cisco Catalyst 9800-L ワイヤレスコントローラ（光ファイバアップリンク））には適用されません。

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。
ステップ 2 [AP SSC Trustpoint] 領域で、[Generate] をクリックして AP SSC トラストポイントを生成します。
ステップ 3 [RSA Key-Size] ドロップダウンリストから、キー サイズを選択します。
ステップ 4 [Signature Algorithm] ドロップダウンリストから、オプションを選択します。
ステップ 5 [Password Type] ドロップダウンリストから、パスワードタイプを選択します。
ステップ 6 [Password] フィールドに、パスワードを入力します。有効な範囲は 8 ～ 32 文字です。
ステップ 7 [Apply to Device] をクリックします。

認証局サーバーの追加（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[CA Server] タブをクリックします。

ステップ 3 [CA Server] セクションで、[Shutdown Status] トグルボタンをクリックして、ステータスを有効にします。シャットダウンステータスとして [Enabled] を選択した場合は、パスワードを入力して確認する必要があります。

ステップ 4 シャットダウンステータスとして [Disabled] を選択した場合は、[Country Code]、[State]、[Location]、[Organisation]、[Domain Name]、および [Email Address] を入力する必要があります。

ステップ 5 [Apply] をクリックして CA サーバーを追加します。

ステップ 6 CA サーバーを削除するには、[Remove CA Server] をクリックします。

PKI トラストポイントの RSA または EC キーの追加（GUI）

手順

ステップ 1 [Configuration] > [Security] > [PKI Management] を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Key Pair Generation] タブをクリックします。

ステップ 3 [Key Pair Generation] セクションで、[Add] をクリックします。

ステップ 4 表示されるダイアログボックスで、次の情報を指定します。

a) [Key Name] フィールドに、キーの名前を入力します。

b) [Key Type] オプションで、[RSA Key] または [EC Key] を選択します。

c) [Modulus Size] フィールドに、RSA キーまたは EC キーのモジュラス値を入力します。RSA キーのデフォルトのモジュラスサイズは 4096 で、EC キーのデフォルト値は 521 です。

d) キーをエクスポートするには、[Key Exportable] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオンになっています。

e) [Generate] をクリックします。

証明書の追加と管理

証明書を追加および管理するには、次のいずれかの方法を使用します。

方法 1

手順

ステップ 1 [Configuration] > [Security] > [PKI Management] > [Add Certificate] を選択します。

ステップ 2 [Generate Certificate Signing Request] をクリックします。

a) [Certificate Name] フィールドに証明書名を入力します。

b) [Key Name] ドロップダウンリストから、RSA キーペアを選択します（[Key Pair Generation] タブの下にあるプラス [+] アイコンをクリックして、新しい RSA キーペアを作成します）。

c) [Country Code]、[Location]、[Organisation]、[State]、[Organizational Unit]、および [Domain Name] フィールドに値を入力します。

d) [Generate] をクリックします。
生成された証明書署名要求（CSR）が右側に表示されます。[Copy] をクリックして、ローカルコピーをコピーして保存します。[Save to Device] をクリックして、生成された CSR を /bootflash/csr ディレクトリに保存します。

ステップ 3 [Authenticate Root CA] をクリックします。

a) [Trustpoint] ドロップダウンリストから、ステップ 2 で生成されたトラストポイントラベル、または認証する他のトラストポイントラベルを選択します。

b) [Root CA Certificate (.pem)] フィールドに、CA から受け取った証明書をコピーして貼り付けます。

（注） デバイス証明書の発行元 CA の PEM Base64 証明書をコピーして貼り付けてください。

c) [認証（Authenticate）] をクリックします。

ステップ 4 [Import Device Certificate] をクリックします。

a) [Trustpoint] ドロップダウンリストから、ステップ 2 で生成されたトラストポイントラベル、または認証する他のトラストポイントラベルを選択します。

b) [Signed Certificate (.pem)] フィールドに、CA から受け取った署名証明書をコピーして貼り付けます。

c) [Import] をクリックします。

これでデバイス証明書のインポートプロセスが完了し、証明書を機能に割り当てることができます。

方法 2

手順

[Import PKCS12 Certificate] をクリックします。

（注） さまざまな転送タイプを使用して、証明書チェーン全体をPKCS12形式でインポートできます。

a) [Transport Type] ドロップダウンリストから、[FTP]、[SFTP]、[TFTP]、[SCP]、または [Desktop (HTTPS)] のいずれかを選択します。

[FTP]、[SFTP]、および [SCP] の場合、[Server IP Address (IPv4/IPv6)]、[Username]、[Password]、[Certificate File Path]、[Certificate Destination File Name]、および [Certificate Password] フィールドに値を入力します。

[TFTP] の場合は、[Server IP Address (IPv4/IPv6)]、[Certificate File Path]、[Certificate Destination File Name]、および [Certificate Password] フィールドに値を入力します。

[Desktop (HTTPS)] の場合、[Source File Path] および [Certificate Password] フィールドに値を入力します。

b) **[インポート (Import)]** をクリックします。

第 62 章

ユーザーおよびエンティティの行動分析

ユーザーおよびエンティティの行動分析に関する情報

ユーザーおよびエンティティの行動分析（UEBA）は、異常が発生したときにネットワーク内の潜在的な脅威や標的型攻撃を特定するために、ユーザーとデバイスの動作をプロファイリングおよび追跡できる多くのセキュリティ技術を備えたソリューションです。

たとえば、企業の従業員は、バックドアや企業秘密の漏洩を含む可能性のある悪意のあるソフトウェアを意図せずにダウンロードすることがあります。これは、確立された基準と比較して、ネットワーク内の 1 つ以上のデバイスやユーザーからの通信パターンの変化によって検出されます。

ユーザーおよびエンティティの行動分析は、次の 2 つの方法を使用して展開できます。

- ユーザー データグラム プロトコル（UDP）コレクタ（Cisco Digital Network Architecture（DNA）Center は UDP コレクタです）。
- Stealthwatch Cloud（SwC）：組み込みワイヤレスコントローラ（EWC）は、データを SwC に直接アップロードします。

ユーザーおよびエンティティの行動分析の設定（UDP コレクタを使用）

Cisco DNA Center ベースの展開では、コントローラは、Cisco DNA Center に送信される NetFlow 情報のコレクタとして機能します。次に、Cisco DNA Center は SwC の情報を圧縮します。コントローラは、アクセスポイント（AP）で Application Visibility and Control（AVC）を有効にし、Cisco DNA Center との通信チャネルを維持します。

EWC では、UDP を介して FnFv9 データを UDP コレクタに送信することもできます。

Cisco DNAC ベース以外の展開では、FnF フローレコードはコントローラから SwC に直接送信されます。

ユーザーおよびエンティティの行動分析の設定（Stealthwatch Cloud を使用）

後続の各項では、Stealthwatch Cloud（GUI および CLI）を使用したユーザーおよびエンティティの行動分析ソリューションの設定に関する情報を提供します。

Stealthwatch Cloud を使用したユーザーおよびエンティティの行動分析の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Threat Defense] を選択します。

ステップ 2 [Cisco StealthWatch Integration] をクリックします。

ステップ 3 [Stealthwatch] ページの [Service Key] フィールドに、Stealthwatch Cloud サービスキーを入力します。

ステップ 4 クラウドアイコンをクリックして、Stealthwatch の詳細な統計を表示します。

ステップ 5 [Sensor Name] フィールドに、Stealthwatch Cloud 登録用のセンサー名を入力します。

ステップ 6 [URL] フィールドに、Stealthwatch Cloud サーバーの URL を入力します。

ステップ 7 [Apply] をクリックします。

ステップ 8 （任意）[Unconfigure StealthWatch] をクリックして、Stealthwatch Cloud の設定を解除します。

次のタスク

Stealthwatch Cloud の正常性ステータスは、[Stealthwatch Health Status] で確認できます。

Stealthwatch Cloud 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。
ステップ 2	**stealthwatch-cloud-monitor** 例： `Device(config)# stealthwatch-cloud-monitor`	Stealthwatch Cloud モニターを設定します。Stealthwatch Cloud モニター 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	**service-key** *swc-service-key* 例： `Device(config-stealthwatch-cloud-monitor)# service-key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`	（任意）Stealthwatch Cloud サービスキーを設定します。サービスキーは、SwC ポータルによって提供されます。サービスキーの代替策として、IP アドレス許可リストを使用した認証があります。サービスキーと許可リストの詳細については、適切な SwC ガイドを参照してください。
ステップ 4	**sensor-name** *swc-sensor-name* 例： `Device(config-stealthwatch-cloud-monitor)# sensor-name swc-sensor-name`	（任意）Stealthwatch Cloud 登録のセンサー名を指定します。デバイスのシリアル番号がデフォルト値です。
ステップ 5	**url** *SwC-server-url* 例： `Device(config-stealthwatch-cloud-monitor)# url https://sensors.eu-2.obsrvbl.com`	Stealthwatch Cloud サーバーの URL を設定します。

フロー測定への Stealthwatch Cloud のマッピング

Stealthwatch Cloud をフロー測定にマッピングするオプションには、フローエクスポータ構成とフローモニター構成の 2 つがあります。

（注） 任意の時点で、アクティブなフローエクスポータは内部と外部でそれぞれ 1 つのみ存在できます。アクティブなフローエクスポータは、ワイヤレス プロファイルにバインドされているフローモニターにバインドされているエクスポータです。

Stealthwatch Cloud のフローエクスポータの設定

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	**flow exporter** *flow-exporter-name* 例： `Device(config)# flow exporter flow-exporter-name`	フローエクスポータを定義すします。 （注） 任意の時点で、アクティブなフローエクスポータは内部と外部でそれぞれ 1 つのみ存在できます。アクティブなフローエクスポータは、ワイヤレスプロファイルにバインドされているフローモニターにバインドされているエクスポータです。
ステップ 3	**destination stealthwatch-cloud** 例： `Device(config-flow-exporter)# destination stealthwatch-cloud`	フロー情報を Stealthwatch Cloud にエクスポートします。

Stealthwatch Cloud のフローモニターの設定

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	**flow monitor** *flow-monitor-name* 例： `Device(config)# flow monitor flow-monitor-name`	フローモニターを定義します。
ステップ 3	**exporter** *flow-exporter-name* 例：	フロー情報をエクスポータにエクスポートします。

	コマンドまたはアクション	目的
	`Device(config-flow-monitor)# exporter flow-exporter-name`	
ステップ 4	**record wireless avc basic** 例： `Device(config-flow-monitor)# record wireless avc basic`	基本の IPv4 ワイヤレス AVC テンプレートを使用してフローレコードを指定します。
ステップ 5	**end** 例： `Device(config-flow-monitor)# 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。

例：Stealthwatch Cloud の設定

次の例は、Stealthwatch Cloud の完全な CLI 設定を示しています。

```
stealthwatch-cloud-monitor
  service-key XXXXXXXXXXXXXXXXXXXXXXXXXXXX
  sensor-name ewc-sensor
  url https://sensors.eu-2.obsrvbl.com

flow exporter fexp-swc
 destination stealthwatch-cloud

flow monitor fm-avc-swc
 exporter fexp-swc
 record wireless avc basic

wireless profile policy swc-policy-profile
 ipv4 flow monitor fm-avc-swc input
 ipv4 flow monitor fm-avc-swc output
 ipv6 flow monitor fm-avc-swc input
 ipv6 flow monitor fm-avc-swc output

wlan my-wlan 1 my-wlan

wireless tag policy swc-policy-tag
 wlan my-wlan policy swc-policy-profile

ap 0000.0000.0001
 policy-tag swc-policy-tag
```

Stealthwatch Cloud の詳細の確認

Stealthwatch Cloud の状態と統計を確認するには、**show stealthwatch-cloud wireless-shim** コマンドを使用します。

```
Device# show stealthwatch-cloud wireless-shim
Stealthwatch-Cloud wireless shim

Total
```

```
 RX records        : 15
 RX bytes          : 2345
 TX records        : 10
 TX bytes          : 1234
 TX batches        : 1
 Failed batches    : 0
 Non-SWC records   : 5

Buffers
 Status        : TX
 Size          : 1272000
 Compressed    : 8
 Uncompressed  : 0
 Records       : 8

 Status        : Filling
 Size          : 1272000
 Compressed    : 2
 Uncompressed  : 0
 Records       : 2
```

Stealthwatch Cloud 接続の詳細を確認するには、**show stealthwatch-cloud connection** コマンドを使用します。

```
Device# show stealthwatch-cloud connection
Stealthwatch-Cloud details
  Registration
    #ID         : 0xe6000001
    URL         : https://sensors.eu-2.obsrvbl.com
    Service Key : XXXXXXXXXXXXXXXXXXXXXXXXXXXX
    Sensor Name : ewc-sensor
    Registered  : Yes
  Connection
    Status               : UP
    Last status update   : 03/17/2020 21:44:55
    # Flaps              : 0
    # Heartbeats         : 9
    # Lost heartbeats    : 1
    Total RX bytes       : 4567
    Total TX bytes       : 1234
    Upload Speed (B/s)   : 247
    Download Speed (B/s) : 269
    # Open sessions      : 0
    # Redirections       : 0
    # Timeouts           : 0

  HTTP Events
    GET response                  : 1
    GET request                   : 1
    GET Status Code 2XX           : 1
    PUT response                  : 1
    PUT request                   : 1
    PUT Status Code 2XX           : 1
    POST response                 : 12
    POST request                  : 12
    POST Status Code 2XX          : 11
    POST Status Code 4XX          : 1
API Events
    Abort                         : 1

  Event History
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
```

```
03/21/2020 10:42:06.161 9        HEARTBEAT_OK         0

03/20/2020 06:49:05.717 1        HEARTBEAT_FAIL       0 HTTPCON_EV_TIMEOUT (6)

03/20/2020 06:47:05.717 1        SEND_START           0 ID:0001
03/20/2020 06:49:05.717 3        SIGNAL_DATA_FAIL     0 ID:0001, attempt : 3
03/18/2020 09:23:39.375 1        REGISTER_OK          0

03/18/2020 09:23:13.276 1        REGISTER_SEND        0

03/18/2020 09:23:12.154 1        SEND_ABORT_ALL       0 config change

03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 URL
https://sensor.staging.obsrvbl.com
03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 Service-key
XXXXXXXXXXXXXXXXXXXXXXXXX
03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 Host ewc-sensor => reset

03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 cfg-mode manual => reset
```

第 VII 部

モビリティ

第 63 章

組み込みワイヤレスコントローラでのNATサポート

NAT サポートについて

ネットワークアドレス変換（NAT）を使用すると、デバイスがインターネット（パブリック）とローカルネットワーク（プライベート）間のエージェントとして動作できます。これにより、コントローラのイントラネット IP アドレスが、対応する外部アドレスにマッピングされます。コントローラが Discovery Response で適切な IP アドレスを送信できるように、外部 NAT IP アドレスを使用してコントローラの AP マネージャインターフェイスを設定する必要があります。

組み込みワイヤレスコントローラ（EWC）ネットワークのマスターAPは、ワイヤレスクライアントトラフィックでNATを実行します。これは、クライアントのパブリック IP アドレスとプライベート IP アドレスを変換することによって実現されます。NAT の配置と数に応じて、トンネルの一端または両端で変換が必要になる場合があります。

マスター AP は、ゲスト WLAN に対して NAT を実行します。ただし、これは従業員 WLAN には必要ありません。ゲスト WLAN に接続されたクライアントの IP アドレスは、マスター AP で実行されている内部 DHCP サーバーによって提供されますが、従業員 WLAN に接続されたクライアントは、外部 DHCP サーバーから IP アドレスを取得します。

マスター AP は、NAT 対象の WLAN に接続されたクライアントからのトラフィックへのゲートウェイとして機能し、アドレス変換を実行します。非 NAT 対象の WLAN に接続されたクライアントは、外部DHCPサーバーによって提供されるゲートウェイを使用してトラフィックを送信します。

集中型NAT WLANの場合、コントローラは特定のWLANへのVLANマッピングをプロビジョニングします。NAT を実行する場合、プライベート IP アドレス（NAT デバイスの前のネット

ワーク内のアドレス）とパブリック IP アドレス（パブリックネットワーク内のアドレス）の両方を設定する必要があります。

外部 DHCP サーバーは、AP の IP アドレスを提供します。マスター AP には 2 つの IP アドレスが必要です。1 つは内部 AP に使用するアドレスで、もう 1 つはワイヤレスコントローラとして機能する場合に使用するアドレスです。内部 DHCP サーバーは、ネットワークに接続されている AP に IP アドレスを割り当てるためには使用されません。外部 DHCP サーバーは、非 NAT 対象の WLAN 上のクライアントに IP アドレスを提供するために使用されます。

NAT サポートの制約事項

- 集中型 NAT が有効になっている場合、同じ VLAN 上の有線からワイヤレスへのクライアントトラフィックはサポートされません。
- 集中型 NAT が有効になっている WLAN も、マスター AP でプロビジョニングする必要があります。
- 集中型 NAT が機能するには、クライアント DHCP サーバーが EWC 上で実行されている必要があります。外部 DHCP サーバーはサポートされていません。

VLAN での集中型 NAT の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless ewc-ap centralized-nat vlan** *vlan-id* 例： `Device(config)# wireless ewc-ap centralized-nat test-vlan 10`	VLAN で集中型 NAT を有効にします。
ステップ 3	（任意） **wireless ewc-ap centralized-nat vlan** *vlan-id* **peer-blocking** 例： `Device(config)# wireless ewc-ap centralized-nat test-vlan 10 peer-blocking`	ピアブロッキングを設定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

NAT サポートの確認

集中型 NAT の AP データパスプログラミングの履歴を表示するには、次のコマンドを使用します。

```
Device# show wireless mob-exp centralized-nat history

Centralized NAT Global event history:
Timestamp Event RC Context
------------------------- ----------- ---- -------
06/17/2019 05:28:39.962760 Route add 0 100.100.100.0/255.255.255.0 0.0.0.0 2
06/17/2019 05:28:39.961794 VLAN update 0 0-4095 0,10 1,100 1
06/17/2019 05:28:39.961162 Route add 0 10.10.10.0/255.255.255.0 0.0.0.0 1
Centralized NAT AP DP plumbing client event history:
Timestamp Event RC Context
------------------------- ----------- ---- -------
06/17/2019 05:37:55.827602 Client del 0 10.10.10.3
06/17/2019 05:37:55.826296 Client del 0 10.10.10.3
06/17/2019 05:37:32.160737 Client add 0 MAC b8:27:eb:27:f3:f6, IP 10.10.10.4, WLAN 2
06/17/2019 05:37:31.454851 Client del 0 10.10.10.4
06/17/2019 05:37:31.453479 Client del 0 10.10.10.4
06/17/2019 05:36:25.659639 Client add 0 MAC b8:27:eb:27:f3:f6, IP 10.10.10.4, WLAN 1
06/17/2019 05:35:52.513500 Client add 0 MAC b8:27:eb:be:08:ea, IP 10.10.10.3, WLAN 1
```

NAT ステータスを表示するには、AP で次のコマンドを使用します。

```
Device# show flexconnect ewc-ap nat status
Programmed WLC IP
9.9.71.50
Programmed Vlan Config
output 0: vlan 0-9,11-4095
output 1: vlan 10
Programmed Route Table
0.0.0.0/0 1.1.1.1                       0
10.10.10.0/24 -                         2
NAT and P2P Block Status:
WLAN    NAT-Enabled        P2P-Block
  0       false              false
  1       true               false
```

第 VIII 部

ハイ アベイラビリティ

第 64 章

ハイ アベイラビリティ

高可用性アクティブおよびスタンバイ

Cisco Embedded Wireless Controller on Catalyst Access Points（EWC）は、Cisco Catalyst 9100 シリーズ AP でサポートされています。アクティブ AP 選択プロセスにより、どの Cisco Catalyst 9100 シリーズ AP が EWC コントローラ機能を実行するように選択されるかが決定されます。アクティブ AP が選択された後に EWC 対応の他の従属 Cisco Catalyst 9100 シリーズ AP がアクティブ AP に参加するとスタンバイ AP が選択され、冗長構成が形成されます。

この高可用性（HA）アーキテクチャは、Cisco Catalyst 9800 HA アーキテクチャをベースにしながら、さらに次の特徴があります。

EWC では HA ペアリングの仕組みが異なります。最初の起動では、EWC アクティブ AP はすべての AP がコントローラに参加するまで待機します。次に、アクティブ AP は（自動選択または構成によって）指定されたスタンバイ AP を選択し、そのロールと HA パラメータ（ローカル/ピア IP、キープアライブ間隔、優先順位）を CAPWAP 制御メッセージを介して選択した AP に送信します。

（注） 停電後、EWC HA ペアではスタンバイ AP は起動しません。スタンバイ AP は起動を試みますが失敗します。その後、別の EWC 対応 AP がスタンバイとして選択されますが、起動に失敗します。この状況を回避するには、HA ペアとして選択される AP の IP バージョンが同じであることを確認してください。

選択したスタンバイ AP が起動し、手動操作なしで HA パラメータが動的に設定されます。

アクティブアクセスポイントとスタンバイアクセスポイント間の冗長性のモニタリング

アクティブ AP とスタンバイ AP 間の冗長性を表示するには、次の手順に従います。

手順

ステップ 1 Cisco Embedded Wireless Controller on Catalyst Access Points の GUI を開きます。

ステップ 2 [Monitoring] > [General] > [System] の順に選択します。

ステップ 3 [Redundancy] タブをクリックします。

[General] タブで、アクティブ AP とスタンバイ AP の現在の状態、ピアの状態、冗長性モード、シャーシの詳細を表示できます。

アクティブアクセスポイントの選択プロセス

EWC 選択プロセスは、コントローラを起動する AP を選択するためのプロセスです。Virtual Router Redundancy Protocol（VRRP）を使用してアクティブ AP を選択します。EWC アクティブ AP とスタンバイ AP を選択するために使用されるロジックについては、次のセクションで説明します。

アクティブ EWC アクセスポイントの選択

アクティブ EWC AP を比較および選択するために、次の方法が使用されます。

- 優先コントローラとして設定されている AP が最も優先されます。
- 次に AP のタイプが比較されます。モデル番号が大きい AP ほど値が高くなり、最も高い値の AP がアクティブ AP になります。
- AP のタイプが同じ場合は、クライアントの負荷（関連付けられたクライアントの数）が比較され、クライアントの負荷が一番小さい AP が選択されます。
- 上記の方法で決まらない場合（AP 間ですべて同じ場合）、MAC アドレスが最も小さい AP がアクティブ AP になります。

スタンバイ EWC アクセスポイントの選択

スタンバイ EWC AP は VRRP では選択されません。Day-0 のスタンバイ EWC AP の選択プロセスは次のとおりです。

- アクティブ EWC AP が選択された後、アクティブ AP は外部 AP が参加するまで待機してから、スタンバイ AP の選択を開始します。
- 外部 AP が参加すると、アクティブ AP によって参加したすべての AP に優先順位が割り当てられます。優先順位が最も高い AP がスタンバイ AP として選択されます。最も高い優先順位を持つ AP が複数ある場合、MAC アドレスが最も小さい AP が選択されます。EWC イメージがインストールされている EWC 対応 AP のみが選択プロセスの対象となります。
- 優先順位は、次のパラメータに基づいて計算されます。
  - ユーザーによる明示的な構成：次の優先コントローラとして優先順位が最も高い AP を選択します。
  - AP タイプ
  - AP 参加時刻

（注） Day-0 にはスタンバイの概念はありません。Day-0 では、1 つのアクティブ EWC AP のみが存在します。何らかの理由でアクティブ EWC AP がダウンすると、新しいアクティブ EWC AP を選択するために VRRP による選択が再度行われます。

（注） 1 台の AP でコントローラが実行されると、この AP はコントローラとして機能していない他の AP よりも優先順位が高くなります。たとえば、Cisco Catalyst 9115AX AP が 1 台起動すると、選択できる他の AP がないため、この AP がアクティブ AP になってコントローラを起動します。その後、このネットワークで Cisco Catalyst 9117AX シリーズ AP を起動しても、（Cisco Catalyst 9115AX シリーズ AP よりモデル番号は大きいですが）すでにネットワーク内で稼働しているコントローラがあるため、コントローラにはなりません。選択プロセスは、2 つの AP を同時に起動した場合にのみ実行されます。

優先コントローラの選択

優先コントローラを選択してコントローラにするには、以下の手順に従います。

始める前に

アクティブ EWC AP とスタンバイ EWC AP は、前のトピックで説明したプロセスで選択されます。何らかの理由で別の AP をスタンバイとして選択する場合は、GUI から任意の EWC 対応 AP を優先コントローラとして選択できます。

（注） 現在スタンバイ AP ではない別の AP を優先コントローラとして選択すると、現在のスタンバイ AP がダウンし、選択した新しい EWC AP がスタンバイ EWC AP になります。

手順

ステップ 1 Cisco Embedded Wireless Controller on Catalyst Access Points の GUI を開きます。

ステップ 2 [Configuration] > [Wireless] > [Access Points] を選択します。

ステップ 3 優先コントローラにする AP をクリックします。
[Edit AP] ウィンドウが表示されます。

ステップ 4 [Advanced] タブをクリックします。

ステップ 5 [Embedded Wireless Controller] セクションで、[Preferred Controller] チェックボックスをオンにします。

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

次のタスク

[Advanced] タブに戻り、[Make Controller] をクリックします。[Update & Apply to Device] をクリックします。

（注） この操作によってコントローラがリセットされるため、ネットワークが中断されることを示す警告メッセージが表示されます。

第 IX 部

QoS

第 65 章

QoS

ワイヤレス QoS の概要

Quality of Service（QoS）では、特定のトラフィックを他のトラフィック タイプよりも優先的に処理することで、トラフィックに優先順位を付けることができます。QoS を設定しない場合、デバイスはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。デバイスは信頼性、遅延限界、スループットを保証せずにパケットを送信します。

ターゲットは、ポリシーが適用されるエンティティです。SSID およびクライアントに対するワイヤレスQoSポリシーは、アップストリーム方向やダウンストリーム方向で適用されます。有線ソースからワイヤレス ターゲットへのトラフィック フローは、ダウンストリーム トラフィックと呼ばれます。ワイヤレスソースから有線ターゲットへのトラフィックフローは、アップストリーム トラフィックと呼ばれます。

次は、ワイヤレス QoS によって提供される特定の機能の一部です。

- ワイヤレス QoS ターゲットに対する SSID ポリシーおよびクライアント ポリシー
- ワイヤレストラフィックのマーキングおよびポリシング（レート制限とも呼ばれる）

ワイヤレス QoS ターゲット

ここでは、デバイスで使用可能なさまざまなワイヤレスQoSターゲットについて説明します。

SSID ポリシー

入力と出力の両方向でSSIDのQoSポリシーを作成できます。設定されていない場合は、SSIDポリシーは適用されません。

このポリシーは、SSID ごと、AP ごとに適用されます。

SSID のポリシング ポリシーとマーキング ポリシーを設定できます。

クライアント ポリシー

クライアントポリシーは、入力方向と出力方向に適用できます。クライアントではポリシングポリシーおよびマーキング ポリシーを設定できます。AAA オーバーライドもサポートされます。

ワイヤレス ターゲットでサポートされる QoS 機能

次の表に、ワイヤレス ターゲットで使用可能なさまざまな機能について説明します。

表 *36 :* ワイヤレス ターゲットで使用可能な *QoS* 機能

ターゲット	機能	ポリシーが適用される方向
SSID	• Set • ポリシング • ドロップ	アップストリームおよびダウンストリーム
クライアント	• Set • ポリシング • ドロップ	アップストリームおよびダウンストリーム

（注） ドロップサポートの場合、ドロップアクションは次の設定によって実現します。

```
police <rate>
   conform-action drop
   exceed-action drop
```

直接**action drop**はサポートされていません。

ワイヤレス QoS の貴金属ポリシー

貴金属ポリシーは、組み込みワイヤレスコントローラで使用可能なシステム定義のポリシーです。これらのポリシーは削除または変更できません。

次のポリシーを使用できます。

- プラチナ：VoIP クライアントに使用されます。
- ゴールド：ビデオ クライアントに使用されます。
- シルバー：ベスト エフォートであると考えられるトラフィックに使用されます。
- ブロンズ：NRT トラフィックに使用されます。

これらのポリシーは事前に設定されています。変更はできません。

クライアントのメタル ポリシーは、AAA を使用してプッシュできます。

適用されたポリシーに基づいて、パケット内の 802.11e（WMM）および DSCP フィールドが影響を受けます。

メタルポリシー形式の詳細については、メタルポリシー形式（801 ページ）セクションを参照してください。

DSCP から UP へのマッピングの詳細については、Architecture for Voice, Video and Integrated Data（AVVID）（808 ページ）の表を参照してください。

ワイヤレス QoS の前提条件

ワイヤレス QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- ワイヤレスの概念とネットワーク トポロジ。
- QoS 実装について。
- モジュラ QoS CLI（MQC）モジュラ QoS の詳細については、MQC ガイドを参照してください。
- 使用するアプリケーションのタイプおよびネットワークのトラフィックパターン
- ネットワークの帯域幅要件および速度

ワイヤレス ターゲットの QoS に関する制約事項

一般的な制約事項

ターゲットとは、ポリシーが適用されるエンティティです。ポリシーはワイヤレスターゲットに適用できます。ワイヤレスターゲットになるのはダウンストリーム方向またはアップストリーム方向の SSID またはクライアントターゲットです。ダウンストリームは、トラフィックがコントローラからワイヤレスクライアントに流れていることを示します。アップストリームは、トラフィックがワイヤレスクライアントからコントローラに流れていることを示します。

- 階層型（親ポリシーと子ポリシー）QoS はサポートされていません。
- 方向単位ターゲットあたり 1 つのポリシーがサポートされています。
- 両方向で、BSSID とクライアントターゲットのみがサポートされています。
- 次のポリシー形式がサポートされています。
  - QoS ポリシーアクション
    - Police：

      ```
      police [cir | rate] bps [conform-action action] [exceed-action action]
      ```

      ポリサーアクションタイプは **transmit** または **drop** です。

    - Set:

      ```
      set dscp
       set wlan user-priority
      ```

（注） **set wlan user-priority** （ダウンストリームのみ、BSSID のみ）

  - QoS ポリシー分類

    ```
    match [not] access-group
     match [not] dscp
     match [not] protocol
    ```

AP 側の制限事項

- Cisco組み込みワイヤレスコントローラ、FlexConnectローカルスイッチング、およびSDA展開では、QoS ポリシーが AP に適用されます。この AP 側の制限により、ポリシングアクション（レート制限など）は、クライアント単位ではなく、フロー単位（5 タプル）レベルでのみ適用されます。

コントロールプレーンのレート制限とポリシング

コントローラでコントロールプレーンのレート制限またはポリシングを明示的に設定する必要はありません。コントローラには、CPU へ向かうコントロール プレーン トラフィックをポリシングして CPU を保護するメカニズム（ポリサーなど）が組み込まれています。AireOS から IOS-XE に移行する場合、この変更はコードレベルで処理されます。

メタルポリシー形式

メタルポリシー形式

メタルポリシーはシステム定義であり、変更も削除もできません。メタルポリシーには、Platinum、Gold、Silver、Bronze の 4 つのレベルがあります。

（注） 各メタルポリシーでは、DSCP または UP マーキングが特定の値を超えないように DSCP 上限を定義します。

Platinum の値は 46、Gold は AF41、Silver は 22、Bronze は CS1 です。

[Policy Name]	ポリシーマップ形式	クラスマップ形式
platinum	policy-map platinum class cm-dscp-34 set dscp af41 class cm-dscp-45 set dscp 45 class cm-dscp-46 set dscp ef class cm-dscp-47 set dscp 47	class-map match-any cm-dscp-34 match dscp af41 class-map match-any cm-dscp-45 match dscp 45 class-map match-any cm-dscp-46 match dscp ef class-map match-any cm-dscp-47 match dscp 47 class-map match-any cm-dscp-0 match dscp default
Gold	policy-map gold class cm-dscp-45 set dscp af41 class cm-dscp-46 set dscp af41 class cm-dscp-47 set dscp af41	
silver	policy-map silver class cm-dscp-34 set dscp default class cm-dscp-45 set dscp default class cm-dscp-46 set dscp default class cm-dscp-47 set dscp default	
bronze	policy-map bronze class cm-dscp-0 set dscp cs1 class cm-dscp-34 set dscp cs1 class cm-dscp-45 set dscp cs1 class cm-dscp-46 set dscp cs1 class cm-dscp-47 set dscp cs1	

[Policy Name]	ポリシーマップ形式	クラスマップ形式

platinum-up	policy-map platinum-up
	 class cm-dscp-set1-for-up-4
	  set dscp af41
	 class cm-dscp-set2-for-up-4
	  set dscp af41
	 class cm-dscp-for-up-5
	  set dscp af41
	 class cm-dscp-for-up-6
	  set dscp ef
	 class cm-dscp-for-up-7
	  set dscp ef
		class-map match-any
		cm-dscp-for-up-0
		  match dscp default
		  match dscp cs2
		
		class-map match-any
		cm-dscp-for-up-1
		  match dscp cs1
		
		class-map match-any
		cm-dscp-set1-for-up-4
		  match dscp cs3
		  match dscp af31
		  match dscp af32
		  match dscp af33
		
		class-map match-any
		cm-dscp-set2-for-up-4
		  match dscp af41
		  match dscp af42
		  match dscp af43
		
		class-map match-any
		cm-dscp-for-up-5
		  match dscp cs4
		  match dscp cs5
		
		class-map match-any
		cm-dscp-for-up-6
		  match dscp 44
		  match dscp ef
		
		class-map match-any
		cm-dscp-for-up-7
		  match dscp cs6
		  match dscp cs7

gold-up	policy-map gold-up
	 class cm-dscp-for-up-6
	  set dscp af41
	 class cm-dscp-for-up-7
	  set dscp af41	

silver-up	policy-map silver-up
	 class cm-dscp-set1-for-up-4
	  set dscp default
	 class cm-dscp-set2-for-up-4
	  set dscp default
	 class cm-dscp-for-up-5
	  set dscp default
	 class cm-dscp-for-up-6
	  set dscp default
	 class cm-dscp-for-up-7
	  set dscp default	

bronze-up	policy-map bronze-up
	 class cm-dscp-for-up-0
	  set dscp cs1
	 class cm-dscp-for-up-1
	  set dscp cs1
	 class cm-dscp-set1-for-up-4
	  set dscp cs1
	 class cm-dscp-set2-for-up-4
	  set dscp cs1
	 class cm-dscp-for-up-5
	  set dscp cs1
	 class cm-dscp-for-up-6
	  set dscp cs1
	 class cm-dscp-for-up-7
	  set dscp cs1	

[Policy Name]	ポリシーマップ形式	クラスマップ形式
clwmm-platinum	policy-map clwmm-platinum class voice-plat set dscp ef class video-plat set dscp af41 class class-default set dscp default	class-map match-any voice-plat match dscp ef class-map match-any video-plat match dscp af41 class-map match-any voice-gold match dscp ef class-map match-any video-gold match dscp af41
clwmm-gold	policy-map clwmm-gold class voice-gold set dscp af41 class video-gold set dscp af41 class class-default set dscp default	
clnon-wmm-platinum	policy-map clnon-wmm-platinum class class-default set dscp ef	
clnon-wmm-gold	policy-map clnon-wmm-gold class class-default set dscp af41	
clsilver	policy-map clsilver class class-default set dscp default	
clbronze	policy-map clbronze class class-default set dscp cs1	

自動 QoS ポリシー形式

[Policy Name]	ポリシーマップ形式	クラスマップ形式
enterprise-avc	policy-map AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy class AutoQos-4.0-wlan-Voip-Data-Class set dscp ef class AutoQos-4.0-wlan-Voip-Signal-Class set dscp cs3 class AutoQos-4.0-wlan-Multimedia-Conf-Class set dscp af41 class AutoQos-4.0-wlan-Transaction-Class set dscp af21 class AutoQos-4.0-wlan-Bulk-Data-Class set dscp af11 class AutoQos-4.0-wlan-Scavanger-Class set dscp cs1 class class-default set dscp default policy-map AutoQos-4.0-wlan-ET-SSID-Output-Policy class AutoQos-4.0-RT1-Class set dscp ef class AutoQos-4.0-RT2-Class set dscp af31 class class-default	

[Policy Name]	ポリシーマップ形式	クラスマップ形式
		class-map match-any AutoQos-4.0-wlan-Voip-Data-Class match dscp ef class-map match-any AutoQos-4.0-wlan-Voip-Signal-Class match protocol skinny match protocol cisco-jabber-control match protocol sip match protocol sip-tls class-map match-any AutoQos-4.0-wlan-Multimedia-Conf-Class match protocol cisco-phone-video match protocol cisco-jabber-video match protocol ms-lync-video match protocol webex-media class-map match-any AutoQos-4.0-wlan-Transaction-Class match protocol cisco-jabber-im match protocol ms-office-web-apps match protocol salesforce match protocol sap class-map match-any AutoQos-4.0-wlan-Bulk-Data-Class match protocol ftp match protocol ftp-data match protocol ftps-data match protocol cifs class-map match-any AutoQos-4.0-wlan-Scavanger-Class match protocol netflix match protocol youtube

[Policy Name]	ポリシーマップ形式	クラスマップ形式
		match protocol skype match protocol bittorrent class-map match-any AutoQos-4.0-RT1-Class match dscp ef match dscp cs6 class-map match-any AutoQos-4.0-RT2-Class match dscp cs4 match dscp cs3 match dscp af41
voice	policy-map platinum-up class dscp-for-up-4 set dscp 34 class dscp-for-up-5 set dscp 34 class dscp-for-up-6 set dscp 46 class dscp-for-up-7 set dscp 46 policy-map platinum class cm-dscp-34 set dscp 34 class cm-dscp-46 set dscp 46	
guest	Policy Map AutoQos-4.0-wlan-GT-SSID-Output-Policy Class class-default set dscp default Policy Map AutoQos-4.0-wlan-GT-SSID-Input-Policy Class class-default set dscp default	
port （ローカルモードにのみ適用）	policy-map AutoQos-4.0-wlan-Port-Output-Policy class AutoQos-4.0-Output-CAPWAP-C-Class priority level 1 class AutoQos-4.0-Output-Voice-Class priority level 2 class class-default ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C permit udp any eq 5246 16666 any	class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C class-map match-any AutoQos-4.0-Output-Voice-Class match dscp ef

Architecture for Voice, Video and Integrated Data（AVVID）

IETF DiffServ サービスクラス	DSCP	IEEE 802.11e	
		ユーザー優先度	アクセス カテゴリ
ネットワーク制御	（CS7） CS6	0	AC_BE
テレフォニー	EF	6	AC_VO
VOICE-ADMIT	44	6	AC_VO
シグナリング	CS5	5	AC_VI
マルチメディア会議	AF41 AF42 AF43	4	AC_VI
リアルタイムインタラクティブ	CS4	5	AC_VI
マルチメディア ストリーミング	AF31 AF32 AF33	4	AC_VI
ブロードキャスト ビデオ	CS3	4	AC_VI
低遅延データ	AF21 AF22 AF23	3	AC_BE
OAM	CS2	0	AC_BE
高スループットデータ	AF11 AF12 AF13	2	AC_BK
標準	DF	0	AC_BE
優先順位の低いデータ	CS1	1	AC_BK
Remaining	Remaining	0	

双方向のレート制限の適用方法

双方向のレート制限に関する情報

双方向のレート制限（BDRL）機能により、アップストリームとダウンストリームの両方のトラフィックのレート制限が定義されます。これらのレート制限は個別に設定されています。レート制限は、QoS プロファイルの代わりに WLAN 上で直接設定でき、その値で QoS プロファイル値がオーバーライドされます。WLAN レート制限は、コントローラおよびクライアントのグローバル QoS 設定より常に優先されます。

BDRL機能により、ワイヤレスネットワーク上のクライアントのスループット制限が定義されるため、特定のクライアントセットに優先サービスを設定できます。

次の 4 つの QoS プロファイルを使用して、レート制限を設定できます。

- Gold
- Platinum
- Silver
- ブロンズ

QoS プロファイルは、関連付けられた SSID 上のすべてのクライアントに適用されるため、同じ SSID に接続されているすべてのクライアントのレート制限は同じになります。

BDRL を設定するには、QoS プロファイルを選択し、さまざまなレート制限パラメータを設定します。レート制限パラメータが 0 に設定されている場合、レート制限機能は機能しません。各 WLAN には、QoS プロファイル内の設定に加えて、QoS プロファイルが関連付けられています。

（注） モビリティアンカーのBDRL：外部セットアップは、アンカーコントローラとフォーリンコントローラの両方で設定する必要があります。ベストプラクティスとして、機能の破損を避けるために、両方のコントローラで同じ設定を実行することをお勧めします。

BDRL は、ゲストアンカーシナリオでサポートされています。この機能は、AireOS をゲストアンカーまたはゲストフォーリンとして使用する IRCM ゲストシナリオでサポートされています。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、[Policing] オプションを使用してトラフィックをレート制限します。

BDRL でメタルポリシーを適用するには、次のタスクを実行します。

- SSID でのメタルポリシーの設定
- クライアントでのメタルポリシーの設定
- 全トラフィックに対する双方向のレート制限の設定 （811 ページ）

- トラフィック分類に基づいた双方向のレート制限の設定 （812 ページ）
- ポリシープロファイルへの双方向のレート制限ポリシーマップの適用 （814 ページ）
- 双方向のレート制限によるメタルポリシーの適用 （815 ページ）

双方向のレート制限の前提条件

- クライアントメタルポリシーは、AAA オーバーライドによって適用されます。
- ISE サーバーでメタルポリシーを指定する必要があります。
- ポリシープロファイルで AAA オーバーライドを有効にする必要があります。

SSID でのメタルポリシーの設定

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 profile policy** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-profile1`	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	**description** 説明 例： `Device(config-wireless-policy)# description policy-profile1`	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	**service-policy input** *input-policy* 例： `Device(config-wireless-policy)# service-policy input platinum-up`	入力の Platinum ポリシーを設定します。
ステップ 5	**service-policy output** *output-policy* 例： `Device(config-wireless-policy)# service-policy output platinum`	出力の Platinum ポリシーを設定します。

クライアントでのメタルポリシーの設定

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 profile policy** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-profile1`	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	**description** 説明 例： `Device(config-wireless-policy)# description profile with aaa override`	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	WLAN の AAA オーバーライドをイネーブルにします。 （注） AAA オーバーライドが有効になり、ISE サーバーがポリシーの送信を開始すると、サービスポリシー クライアントに定義されているクライアントポリシーは有効になりません。

全トラフィックに対する双方向のレート制限の設定

ポリシーマップでポリシングアクションを使用して、BDRL を設定します。

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	**policy-map** ポリシーマップ 例：	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。ポリシーマッ

	コマンドまたはアクション	目的
	`Device(config)# policy-map policy-sample 1`	プ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	**class** *class-map-name* 例： `Device(config-pmap)# class class-default`	クラスマップをポリシーマップに関連付け、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 4	**police** *rate* 例： `Device(config-pmap-c)# police 500000`	トラフィックポリシングを設定します（平均レート、1 秒あたりのビット数）。有効値は 8000 ～ 200000000 です。

トラフィック分類に基づいた双方向のレート制限の設定

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	**policy-map** ポリシーマップ 例： `Device(config)# policy-map policy-sample2`	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。ポリシーマップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	**class** *class-map-name* 例： `Device(config-pmap)# class class-sample-youtube`	クラスマップをポリシーマップに関連付け、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 4	**police** *rate* 例： `Device(config-pmap-c)# police 1000000`	トラフィックポリシングを設定します（平均レート、1 秒あたりのビット数）。有効値は 8000 ～ 200000000 です。

	コマンドまたはアクション	目的
ステップ 5	**conform-action drop** 例： `Device(config-pmap-c-police)# conform-action drop`	レート制限に適合したパケットに対して実行するドロップアクションを指定します。
ステップ 6	**exceed-action drop** 例： `Device(config-pmap-c-police)# exceed-action drop`	レート制限を超過したパケットに対して実行するドロップアクションを指定します。
ステップ 7	**exit** 例： `Device(config-pmap-c-police)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 8	**set dscp default** 例： `Device(config-pmap-c)# set dscp default`	DSCP 値をデフォルトに設定します。
ステップ 9	**police** *rate* 例： `Device(config-pmap-c)# police 500000`	トラフィックポリシングを設定します（平均レート、1 秒あたりのビット数）。有効値は 8000 ～ 200000000 です。
ステップ 10	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 11	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 12	**class-map match-any** *class-map-name* 例： `Device(config)# class-map match-any class-sample-youtube`	クラスマップを選択します。
ステップ 13	**match protocol** *protocol* 例： `Device(config-cmap)# match protocol youtube`	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。

ポリシープロファイルへの双方向のレート制限ポリシーマップの適用

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** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-profile3`	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	**description** 説明 例： `Device(config-wireless-policy)# description policy-profile3`	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	**service-policy client input** *input-policy* 例： `Device(config-wireless-policy)# service-policy client input platinum-up`	入力クライアント サービス ポリシーを Platinum として設定します。
ステップ 5	**service-policy client output** *output-policy* 例： `Device(config-wireless-policy)# service-policy client output platinum`	出力クライアント サービス ポリシーを Platinum として設定します。
ステップ 6	**service-policy input** *input-policy* 例： `Device(config-wireless-policy)# service-policy input platinum-up`	入力サービスポリシーを Platinum として設定します。
ステップ 7	**service-policy output** *output-policy* 例： `Device(config-wireless-policy)# service-policy output platinum`	出力サービスポリシーを Platinum として設定します。

双方向のレート制限によるメタルポリシーの適用

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** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-profile3`	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	**description** 説明 例： `Device(config-wireless-policy)# description policy-profile3`	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	**service-policy client input** *input-policy* 例： `Device(config-wireless-policy)# service-policy client input platinum-up`	入力クライアント サービス ポリシーを Platinum として設定します。
ステップ 5	**service-policy client output** *output-policy* 例： `Device(config-wireless-policy)# service-policy client output platinum`	出力クライアント サービス ポリシーを Platinum として設定します。
ステップ 6	**service-policy input** *input-policy* 例： `Device(config-wireless-policy)# service-policy input platinum-up`	入力サービスポリシーを Platinum として設定します。
ステップ 7	**service-policy output** *output-policy* 例： `Device(config-wireless-policy)# service-policy output platinum`	出力サービスポリシーを Platinum として設定します。
ステップ 8	**exit** 例： `Device(config-wireless-policy)# exit`	ポリシー コンフィギュレーション モードを終了します。
ステップ 9	**policy-map** ポリシーマップ 例：	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付き

	コマンドまたはアクション	目的
	`Device(config)# policy-map policy-sample 1`	オブジェクトを作成します。ポリシーマップ名は、最大40文字の英字、ハイフン、またはアンダースコアを使用でき、大文字と小文字が区別されます。
ステップ10	**class** *class-map-name* 例： `Device(config-pmap)# class class-default`	クラスマップをポリシーマップに関連付け、指定されたシステムクラスのコンフィギュレーションモードを開始します。
ステップ11	**police** *rate* 例： `Device(config-pmap-c)# police 500000`	トラフィックポリシングを設定します（平均レート、1秒あたりのビット数）。有効値は8000 ～ 200000000です。

クライアントごとの双方向のレート制限の適用方法

クライアントごとの双方向のレート制限に関する情報

クライアントごとの双方向のレート制限機能は、Flexローカルスイッチング構成の802.11ac Wave 2 APの各ワイヤレスクライアントに双方向のレート制限を追加します。以前は、Wave 2 APは、ワイヤレスクライアントのフローごとのレート制限のみをサポートしていました。ワイヤレスクライアントが複数のトラフィックのストリームを開始すると、クライアントベースのレート制限が期待どおりに機能しませんが、この制限は、この機能によって対処されます。

たとえば、コントローラにQoSポリシーが設定されており、各クライアントのレート上限が1000 kbpsであることが予想される場合、APのフローごとのレート制限により、ワイヤレスクライアントがYoutubeストリームとFTPストリームを開始すると、各ストリームが1000 Kbpsにレート制限されるため、クライアントは2000 Kbpsレートになります。これは望ましくありません。

ユースケース

クライアントごとの双方向のレート制限機能でサポートされるユースケースは次のとおりです。

ユースケース：1

デフォルトクラスマップのみの設定

ポリシーマップがデフォルトクラスマップだけで設定され、QoSクライアントポリシーだけにマッピングされている場合、APは、そのAPに接続されているクライアントに対してクライアントごとのレート制限を実行します。

ユースケース：2

クライアントごとのレート制限からフローごとのレート制限への変更

ポリシーマップがデフォルトクラスマップとともに別のクラスマップで設定され、QoS クライアントポリシーにマッピングされている場合、AP はクライアントへのフローごとのレート制限を実行します。ポリシーマップには、デフォルトクラスマップとともに別のクラスマップがあるため、AP が以前にクライアントごとのレート制限を設定している場合、クライアントごとのレート制限値はクリアされます。

ポリシーマップに複数のクラスマップがある場合は、デフォルトクラスマップとともに追加のクラスマップが設定されるため、レート制限はクライアントごとからフローごとに適用されます。クライアントごとのレート制限値は、レート情報トークンバケットから削除されます。

ユースケース：3

フローごとのレート制限からクライアントごとのレート制限への変更

ポリシーマップから別のクラスマップが削除され、そのポリシーマップにデフォルトクラスマップが 1 つしかない場合、AP はクライアントに対してクライアントごとのレート制限を実行します。

以下では、クライアントごとの双方向のレート制限機能の高レベルの手順について説明します。

1. ポリシープロファイルを使用して、WLAN へのポリシーマップを設定します。
2. QoS 関連のポリシーマップを WLAN にマッピングします。
3. デフォルトクラスマップを使用してポリシーマップを設定します。
4. クラスのデフォルトマップに異なるポリシングレート値を設定します。

（注） ポリシーマップに有効なポリシングレート値を持つクラスのデフォルトがある場合、AP はそのレート制限をクライアント データ トラフィック フロー全体に適用します。

5. WLAN ポリシープロファイルの QoS クライアントポリシーに、クラスのデフォルトのポリシーマップを適用します。

クライアントごとの双方向のレート制限の前提条件

- この機能は、QoS クライアントポリシー専用です。つまり、ポリシープロファイルには、クライアントとして QoS ポリシーまたはポリシーターゲットのみが含まれている必要があります。
- ポリシーマップに有効なポリシングレート値を持つクラスデフォルトがある場合、AP はそのレート制限値をクライアント データ トラフィック フロー全体に適用します。

クライアントごとの双方向のレート制限に関する制約事項

- ポリシーマップにクラスのデフォルトマップ以外のクラスマップがある場合、クライアントごとのレート制限は AP では機能しません。

クライアントごとの双方向のレート制限の設定（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 Name] をクリックします。

[Edit Policy Profile] ウィンドウが表示されます。

（注） [Edit Policy Profile] ウィンドウは、デフォルトクラスマップでのみ表示および設定されます。

ステップ 3 [QoS and AVC] タブを選択します。

ステップ 4 [QoS Client Policy] 設定で、[Egress] および [Ingress] ドロップダウンリストからポリシーを選択します。

（注） デフォルトのポリシーマップを QoS クライアントポリシーに適用する必要があります。

ステップ 5 [Update & Apply to Device] をクリックします。

クライアントごとの双方向のレート制限の確認

クライアントごとに AP で適用されているかどうかを確認するには、次のコマンドを使用します。

```
Device# show rate-limit client
Config:
              mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out
nrt_rate_in nrt_burst_out nrt_burst_in
A0:D3:7A:12:6C:5E   0           0          0            0           0            0
      0            0            0
Statistics:
            name     up down
        Unshaped      0    0
  Client RT pass 697610 8200
 Client NRT pass      0    0
 Client RT drops      0    0
Client NRT drops      0   16
               9    180    0
Per client rate limit:
              mac vap rate_out rate_in            policy
A0:D3:7A:12:6C:5E   0       88      23 per_client_rate_2
```

AAA オーバーライドを使用した BDRL 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 profile policy** *profile-name* 例： `Device (config)# wireless profile policy default-policy-profile`	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	**aaa-override** 例： `Device(config-wireless-policy)# aaa`	AAA サーバーまたは Cisco Identify Services Engine（ISE）サーバーから受信したポリシーを適用するように AAA オーバーライドを設定します。 RADIUS サーバーでは、次の属性を使用できます。 • Airespace-Data-Bandwidth-Average-Contract: 8001 • Airespace-Real-Time-Bandwidth-Average-Contract: 8002 • Airespace-Data-Bandwidth-Burst-Contract: 8003 • Airespace-Real-Time-Bandwidth-Burst-Contract: 8004 • Airespace-Data-Bandwidth-Average-Contract-Upstream: 8005 • Airespace-Real-Time-Bandwidth-Average-Contract-Upstream: 8006 • Airespace-Data-Bandwidth-Burst-Contract-Upstream: 8007 • Airespace-Real-Time-Bandwidth-Burst-Contract-Upstream: 8008 （注） 8001、8002、8003、8004、8005、8006、8007、および 8008 は、例として設定された望ましいレート制限値です。

双方向のレート制限の確認

双方向のレート制限を確認するには、次のコマンドを使用します。

```
Device# show wireless client mac-address E8-8E-00-00-00-71 detailClient MAC Address :
e88e.0000.0071
Client MAC Type     : Universally Administered Address
Client IPv4 Address : 100.0.7.94
Client Username     : e88e00000071
AP MAC Address      : 0a0b.0c00.0200
AP Name             : AP6B8B4567-0002
AP slot             : 0
Client State        : Associated
Policy Profile      : dnas_qos_profile_policy
Flex Profile        : N/A
Wireless LAN Id     : 10
WLAN Profile Name   : QoS_wlan
Wireless LAN Network Name (SSID): QoS_wlan
BSSID : 0a0b.0c00.0200
Connected For       : 28 seconds
Protocol            : 802.11n - 2.4 GHz
Channel             : 1
Client IIF-ID       : 0xa0000034
Association Id      : 10
Authentication Algorithm : Open System
Idle state timeout  : N/A
Session Timeout     : 1800 sec (Remaining time: 1777 sec)
Session Warning Time : Timer not running
Input Policy Name    : None
Input Policy State   : None
Input Policy Source  : None
Output Policy Name   : None
Output Policy State  : None
Output Policy Source : None
WMM Support          : Enabled
U-APSD Support       : Disabled
Fastlane Support     : Disabled
Client Active State  : In-Active
Power Save           : OFF
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream              : 8005 (kbps)
  QoS Realtime Average Data Rate Upstream     : 8006 (kbps)
  QoS Burst Data Rate Upstream                : 8007 (kbps)
  QoS Realtime Burst Data Rate Upstream       : 8008 (kbps)
  QoS Average Data Rate Downstream            : 8001 (kbps)
  QoS Realtime Average Data Rate Downstream   : 8002 (kbps)
  QoS Burst Data Rate Downstream              : 80300 (kbps)
  QoS Realtime Burst Data Rate Downstream     : 8004 (kbps)
```

AP 端末からレート制限の詳細を確認するには、次のコマンドを使用します。

```
Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in
nrt_burst_out nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
```

```
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy
```

ワイヤレス QoS の設定方法

クラスマップを使用したポリシーマップの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[QoS]** を選択します。

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

ステップ 3 [Policy Name] の横にあるテキストボックスに、追加する新しいポリシーマップの名前を入力します。

ステップ 4 [Add Class-Maps] をクリックします。

ステップ 5 [AVC] ベースのポリシーまたは [User Defined] のポリシーを設定します。**AVC**ベースのポリシーを有効にするには、次のように設定します。

a) [Match Any] または [Match All] のいずれかを選択します。

b) 必要な [Mark Type] を選択します。[DSCP] または [User Priority] を選択した場合は、適切な [Mark Value] を指定する必要があります。

c) 特定の送信元からのトラフィックをドロップするには、[Drop] チェック ボックスをオンにします。

（注） [Drop] が有効になっている場合、[Mark Type] および [Police(kbps)] オプションは無効になります。

d) 選択した [Match Type] に基づいて、[Available Protocol(s)] リストから必要なプロトコルを選択し、[Selected Protocol(s)] リストに移動します。選択したこれらのプロトコルによってトラフィックがドロップされます。

e) [Save] をクリックします。

（注） さらにクラスマップを追加するには、ステップ 4 と 5 を繰り返します。

ステップ 6 [User-Defined] の QoS ポリシーを有効にするには、次のように設定します。

a) [Match Any] または [Match All] のいずれかを選択します。

b) ドロップダウンリストから [Match Type] として [ACL] または [DSCP] を選択し、適切な [Match Value] を指定します。

c) 必要な [Mark Type] を選択してマーク ラベルに関連付けます。[DSCP] を選択した場合は、適切な [Mark Value] を指定する必要があります。

d) 特定の送信元からのトラフィックをドロップするには、[Drop] チェック ボックスをオンにします。

（注） [Drop] が有効になっている場合、[Mark Type] および [Police(kbps)] オプションは無効になります。

e) [Save] をクリックします。

（注） 残りのすべてのトラフィックに対するアクションを定義するには、[Class Default] で、対応する [Mark] や [Police(kbps)] を選択します。

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

クラス マップの設定（CLI）

音声およびビデオ トラフィックのクラス マップを設定するには、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： `デバイス# 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	**class-map** *class-map-name* 例： `デバイス(config)# class-map test`	クラス マップを作成します。
ステップ 3	**match dscp** *dscp-value* 例： `デバイス(config-cmap)# match dscp 46`	IPv4 および IPv6 パケットの DSCP 値を照合します。 （注） クラス マップのデフォルトでは、値は match-all です。
ステップ 4	**end** 例： `デバイス(config-cmap)# end`	クラス マップ 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 class-map** *class-map-name* 例： `Device# show class-map class_map_name`	クラスマップの詳細を確認します。

QoS ポリシーを適用するためのポリシープロファイルの設定（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ます。

ステップ 3 [Edit Policy Profile] ウィンドウで [QoS and AVC] タブをクリックします。

ステップ 4 [QoS SSID Policy] で、WLAN の適切な [Ingress] および [Egress] ポリシーを選択します。

（注） 入力ポリシーを出力ポリシーと区別するには、サフィックス -up を使用します。たとえば、Platinum 入力ポリシーは platinum-up という名前になります。

ステップ 5 [QoS Client Policy] で、クライアントの適切な [Ingress] および [Egress] ポリシーを選択します。

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

（注） カスタムポリシーのみが [QoS Client Policy] の下に表示されます。自動 QoS ポリシーは自動生成され、ユーザーの選択肢には表示されません。

QoS ポリシーを適用するためのポリシープロファイルの設定（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： `デバイス# 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 qostest`	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	**service-policy client** {**input** | **output**} *policy-name* 例： `デバイス(config-wireless-policy)# service-policy client input policy-map-client`	ポリシーを適用します。選択できるオプションは、次のとおりです。 • **input**：クライアント ポリシーをポリシー プロファイルの入力方向に割り当てます。

	コマンドまたはアクション	目的
		• **output**：クライアント ポリシーをポリシー プロファイルの出力方向に割り当てます。
ステップ 4	**service-policy** {**input** | **output**} *policy-name* 例： デバイス(config-wireless-policy)# **service-policy input policy-map-ssid**	ポリシーを BSSID に適用します。選択できるオプションは、次のとおりです。 • **input**：WLAN のすべてのクライアントにポリシー マップを割り当てます。 • **output**：WLAN のすべてのクライアントにポリシー マップを割り当てます。
ステップ 5	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ワイヤレス ポリシー プロファイルを有効にします。

ポリシータグへのポリシープロファイルの適用（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] ページの [Policy] タブで [Add] をクリックします。

ステップ 3 表示される [Add Policy Tag] ウィンドウに、ポリシー タグの名前と説明を入力します。

ステップ 4 必要な WLAN ID および WLAN プロファイルを適切なポリシー プロファイルにマッピングします。

ステップ 5 [Update & Apply to Device] をクリックします。

ポリシータグへのポリシープロファイルの適用（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：	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
	デバイス# **configure terminal**	
ステップ 2	**wireless tag policy** *policy-tag-name* 例： `Device(config-policy-tag)# wireless tag policy qostag`	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 test policy qostest`	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`	設定されたポリシータグを表示します。 （注） ポリシー タグの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 タグの付加

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： デバイス# **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。
ステップ 3	**policy-tag** *policy-tag-name* 例：	ポリシー 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)# policy-tag qostag`	
ステップ 4	**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 5	**show ap tag summary** 例： `Device# show ap tag summary`	AP の詳細と AP に関連付けられているタグを表示します。

第 66 章

ワイヤレス自動 QoS

-
- 自動 QoS について （827 ページ）
- ワイヤレス自動 QoS の設定方法 （828 ページ）

自動 QoS について

ワイヤレス自動 QoS は、ワイヤレス QoS 機能の展開を自動化します。事前定義された一連のプロファイルが含まれており、顧客はこれを変更してさまざまなトラフィック フローに優先順位を付けることができます。自動 QoS はトラフィックを照合し、各一致パケットを qos-group に割り当てます。これにより、出力ポリシー マップは、プライオリティ キューを含む特定のキューに、特定の qos-group を配置できます。

自動 QoS ポリシー設定

表 *37*：自動 *QoS* ポリシー設定

モード	クライアント入力	クライアント出力	BSSID 入力	BSSID 出力	ポート入力	ポート出力	無線機
音声	該当なし	該当なし	P3	P4	該当なし	P7	ACM
Guest	該当なし	該当なし	P5	P6	該当なし	P7	
Fastlane	該当なし	該当なし	該当なし	該当なし	該当なし	P7	edca-parameters fastlane
エンタープライズ AVC	該当なし	該当なし	P1	P2	該当なし	P7	

P1	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
P2	AutoQos-4.0-wlan-ET-SSID-Output-Policy

P3	platinum-up
P4	platinum
P5	AutoQos-4.0-wlan-GT-SSID-Input-Policy
P6	AutoQos-4.0-wlan-GT-SSID-Output-Policy
P7	AutoQos-4.0-wlan-Port-Output-Policy

ワイヤレス自動 QoS の設定方法

プロファイル ポリシーのワイヤレス自動 QoS の設定

プロファイル ポリシーの自動 QoS を有効にすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス# enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**wireless autoqos policy-profile** *policy-name***mode { enterprise-avc | fastlane | guest | voice}** 例： `デバイス# wireless autoqos policy-profile test-profile mode voice`	自動 QoS ワイヤレス ポリシーを設定します。 • enterprise-avc：自動 QoS ワイヤレス エンタープライズ AVC ポリシーを有効にします。 • fastlane：自動 QoS ワイヤレス fastlane ポリシーを有効にします。 • guest：自動 QoS ワイヤレスゲスト ポリシーを有効にします。 • voice：自動 QoS ワイヤレス音声ポリシーを有効にします。 （注） 自動 QoS MIB 属性は、サービス ポリシーの完全な機能をサポートしていません。サービス ポリシーは手動で設定する必要があります。現在は自動 QoS モードのみがサポートされています。

次のタスク

（注） 自動 QoS を有効にした後、ポリシーがインストールされるまで数秒待ってから、必要に応じて自動 QoS ポリシー マップの変更を試みるか、変更が拒否された場合は再試行します。

ワイヤレス自動 QoS の無効化

ワイヤレス自動 QoS をグローバルに無効化する手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス# **enable**	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**shutdown** 例： デバイス# **shutdown**	ポリシー プロファイルをシャット ダウンします。
ステップ 3	**wireless autoqos disable** 例： デバイス# **wireless autoqos disable**	ワイヤレス自動 QoS をグローバルに無効化します。
ステップ 4	**[no] shutdown** 例： デバイス# no shutdown	ワイヤレス ポリシー プロファイルを有効にします。 （注） 自動 QoS を無効にしても、CAC や EDCA パラメータなどのグローバル無線構成はリセットされません。

自動 QoS 設定のロールバック（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[QoS]** を選択します。

ステップ 2 [Disable AutoQoS] をクリックします。

ステップ 3 確認のために [はい（Yes）] をクリックします。

自動 QoS 設定のロールバック

始める前に

（注） 自動 QoS MIB 属性は、サービス ポリシーの完全な機能をサポートしていません。現在は自動 QoS モードのみがサポートされています。サービス ポリシーは手動で設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス**enable**	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**clear platform software autoqos config template { enterprise_avc | guest}** 例： デバイス# **clear platform software autoqos config template guest**	自動 QoS 設定をリセットします。 • enterprise-avc：自動 QoS エンタープライズ AVC ポリシー テンプレートをリセットします。 • guest：自動 QoS ゲスト ポリシー テンプレートをリセットします。

ワイヤレス自動 QoS ポリシープロファイルのクリア（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 Name] をクリックします。
ステップ 3 [QOS and AVC] タブに移動します。
ステップ 4 [Auto Qos] ドロップダウンリストから、[None] を選択します。
ステップ 5 [Update & Apply to Device] をクリックします。

ワイヤレス自動 QoS ポリシー プロファイルのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス# **enable**	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**shutdown** 例： デバイス# **shutdown**	ポリシー プロファイルをシャット ダウンします。
ステップ 3	**wireless autoqos policy-profile** *policy-name***mode clear** 例： デバイス# **wireless autoqos policy-profile test-profile mode clear**	設定されている自動 QoS ワイヤレス ポリシーをクリアします。
ステップ 4	**[no] shutdown** 例： no shutdown	ワイヤレス ポリシー プロファイルを有効にします。

ポリシー プロファイルの自動 QoS の表示

始める前に

自動 QoS は、ローカルモードと Flex モードでサポートされています。自動 QoS により、テンプレートに応じて一連のポリシーと無線の設定が設定されます。自動 QoS によって設定されたサービスポリシーはオーバーライドできます。最新の設定が有効になり、AAA オーバーライドポリシーが最も優先されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス**enable**	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**show wireless profile policy detailed** *policy-profile-name* 例：	ポリシー プロファイル詳細パラメータを表示します。

	コマンドまたはアクション	目的
	デバイス# **show wireless profile policy detailed testqos**	

第 67 章

ネイティブ プロファイリング

ネイティブ プロファイリングについて

HTTP と DHCP に基づいてデバイスをプロファイルし、ネットワーク上のエンドデバイスを識別できます。デバイス ベースのポリシーを設定して、ネットワーク上でユーザーまたはデバイス ポリシーごとに適用できます。

ポリシーを使用すれば、モバイルデバイスのプロファイリングと、プロファイルしたデバイスの特定の VLAN への基本オンボーディングが可能になります。また、ACL と QoS を割り当てたり、セッション タイムアウトを設定したりできます。

ポリシーは 2 つの異なるコンポーネントとして設定できます。

- ネットワークに接続しているクライアントに固有のサービステンプレートとしてポリシー属性を定義し、ポリシー一致基準を適用する。
- ポリシーへの一致基準の適用。

（注） ネイティブ プロファイルの設定に進む前に、HTTP プロファイリングと DHCP プロファイリングが有効になっていることを確認してください。

ネイティブ プロファイリングを設定するには、次のいずれかの手順を使用します。

- サービス テンプレートを作成する
- クラス マップの作成

（注） サービス テンプレートは、クラス マップまたはパラメータ マップのいずれかを使用して適用できます。

- パラメータ マップを作成し、サービス テンプレートをパラメータ マップに関連付ける
  - ポリシー マップの作成
    1. クラス マップを使用する場合：クラス マップをポリシー マップに関連付けて、サービス テンプレートをクラス マップに関連付けます。
    2. パラメータ マップを使用する合：パラメータ マップをポリシー マップに関連付けます。
  - ポリシー マップをポリシー プロファイルに関連付けます。

クラス マップの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[QoS]** をクリックします。

ステップ 2 [Qos – Policy] 領域で、[Add] をクリックして新しい QoS ポリシーを作成するか、編集するポリシーをクリックします。

ステップ 3 [Add Class Map] を追加し、詳細を入力します。

ステップ 4 [Save] をクリックします。

ステップ 5 [Update and Apply to Device] をクリックします。

クラス マップの作成（CLI）

（注） CLI によるクラスマップの設定には、GUI よりも多くのオプションがあり、詳細に設定できます。

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	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_user`	クラスマップのタイプと名前を指定します。
ステップ 3	**match username** *username* 例： `Device(config-filter-control-classmap)# match username ciscoise`	クラスマップ属性フィルタ基準を指定します。
ステップ 4	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_userrole`	クラスマップのタイプと名前を指定します。
ステップ 5	**match user-role** ユーザー ロール 例： `Device(config-filter-control-classmap)# match user-role engineer`	クラスマップ属性フィルタ基準を指定します。
ステップ 6	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_oui`	クラスマップのタイプと名前を指定します。
ステップ 7	**match oui** *oui-address* 例： `Device(config-filter-control-classmap)# match oui 48.f8.b3`	クラスマップ属性フィルタ基準を指定します。
ステップ 8	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_mac`	クラスマップのタイプと名前を指定します。

	コマンドまたはアクション	目的
ステップ 9	**match mac-address** *mac-address* 例： `Device(config-filter-control-classmap)# match mac-address 0040.96b9.4a0d`	クラスマップ属性フィルタ基準を指定します。
ステップ 10	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_devtype`	クラスマップのタイプと名前を指定します。
ステップ 11	**match device-type** *device-type* 例： `Device(config-filter-control-classmap)# match device-type windows`	クラスマップ属性フィルタ基準を指定します。
ステップ 12	**match join-time-of-day** *start-time end-time* 例： `Device(config-filter-control-classmap)# match join-time-of-day 10:30 12:30`	時刻の一致を指定します。 ここで照合の対象となるのは、接続時刻です。たとえば、一致フィルタが午前 11:00 から午後 2:00 に設定されている場合、午前 10:59 に接続したデバイスは、クレデンシャルの取得が午前 11:00 以降であっても一致と見なされません。 ここで、各変数は次のように定義されます。 *start-time* と *end-time* は 24 時間形式で指定します。 設定を確認するには、**show class-map type control subscriber name** *name* コマンドを使用します。 （注） このコマンドを使用するには、AAA オーバーライドも無効にする必要があります。

サービス テンプレートの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Local Policy]** を選択します。

ステップ 2 [Local Policy] ページの [Service Template] タブで、[ADD] をクリックします。

ステップ 3 [Create Service Template] ウィンドウで、次のパラメータを入力します。

- [Service Template Name]：テンプレートの名前を入力します。
- [VLAN ID]：テンプレートの VLAN ID を入力します。有効な範囲は 1 ～ 4094 です。
- [Session Timeout (secs)]：テンプレートのタイムアウト時間を設定します。有効な範囲は 1 ～ 65535 です。
- [Access Control List]：ドロップダウンリストからアクセス制御リストを選択します。
- [Ingress QOS]：ドロップダウンリストからクライアントの入力 QoS ポリシーを選択します
- [Egress QOS]：ドロップダウンリストからクライアントの出力 QoS ポリシーを選択します

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

サービス テンプレートの作成（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。
ステップ 2	**service-template** *service-template-name* 例： `Device(config)# service-template svc1`	サービス テンプレート 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	**access-group** *access-list-name* 例： `Device(config-service-template)# access-group acl-auto`	適用するアクセス リストを指定します。

	コマンドまたはアクション	目的
ステップ 4	**vlan** *vlan-id* 例： `Device(config-service-template)# vlan 10`	VLAN ID を指定します。有効な範囲は 1 ～ 4094 です。
ステップ 5	**absolute-timer** *timer* 例： `Device(config-service-template)# absolute-timer 1000`	サービス テンプレートのセッション タイムアウト値を指定します。有効な範囲は 1 ～ 65535 です。
ステップ 6	**service-policy qos input** *qos-policy* 例： `Device(config-service-template)# service-policy qos input in_qos`	クライアントの入力 QoS ポリシーを設定します。
ステップ 7	**service-policy qos output** *qos-policy* 例： `Device(config-service-template)# service-policy qos output out_qos`	クライアントの出力 QoS ポリシーを設定します。

パラメータ マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル設定モードを開始します。
ステップ 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* 例： `Device(config)# parameter-map type subscriber attribute-to-service param`	パラメータ マップのタイプと名前を指定します。
ステップ 3	*map-index***map device-type eq***filter-name* 例： `Device(config-parameter-map-filter)# 1 map device-type eq "windows" mac-address eq 3c77.e602.2f91 username eq "cisco"`	パラメータ マップ属性フィルタ基準を指定します。ここに示す例では、複数のフィルタが使用されています。

	コマンドまたはアクション	目的
ステップ 4	*map-index* **service-template** *service-template-name* **precedence** *precedence-num* 例： `Device(config-parameter-map-filter-submode)# 1 service-template svc1 precedence 150`	サービス テンプレートとその優先順位を指定します。

ポリシー マップの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Local Policy]** > **[Policy Map]** タブを選択します。

ステップ 2 [Policy Map Name] テキスト フィールドに、ポリシー マップの名前を入力します。

ステップ 3 [Add] をクリックします。

ステップ 4 [Service Template] ドロップダウンリストからサービス テンプレートを選択します。

ステップ 5 次のパラメータでは、ドロップダウンリストからフィルタのタイプを選択し、必要な一致基準を入力します。

- Device Type
- ユーザー ロール
- ユーザー名
- OUI
- MAC アドレス

ステップ 6 [Add Criteria] をクリックします。

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

ポリシー マップの作成（CLI）

始める前に

ポリシー マップまたはパラメータ マップを削除する場合は、事前にターゲットから削除するか、WLAN プロファイルをシャット ダウンするか、セッションを削除する必要があります。

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	**policy-map type control subscriber** *policy-map-name* 例： `Device(config)# policy-map type control subscriber polmap5`	ポリシーマップ タイプを指定します。
ステップ 3	**event identity-update match-all** 例： `Device(config-event-control-policymap)# event identity-update match-all`	ポリシーマップに対して一致基準を指定します。

ステップ 4	次に示すように、クラスマップまたはパラメータ マップのいずれかを使用してサービステンプレートを適用できます。
	• *class-num* **class** *class-map-name* **do-until-failure**
	• *action-index* **activate service-template** *service-template-name*
	• *action-index* **map attribute-to-service table** *parameter-map-name*
	例：
	次の例は、サービステンプレートを含むクラスマップを適用する方法を示しています。
	`Device(config-class-control-policymap)# 10 class cls_mac do-until-failure`
	`Device(config-action-control-policymap)# 10 activate service-template svc1`
	例：
	次の例は、パラメータ マップを適用する方法を示しています（パラメータ マップ「param」の作成時にサービステンプレートがすでに関連付けられています）。
	`Device(config-action-control-policymap)#1 map attribute-to-service table param`
		ローカルプロファイリング ポリシーのクラスマップ番号を設定し、アクションの実行方法を指定するか、サービステンプレートをアクティブ化するか、identity-update 属性を自動設定テンプレート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-action-control-policymap)# end`	コンフィギュレーション モードを終了します。
ステップ 6	**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 7	**wireless profile policy** *wlan-policy-profile-name* 例： `Device(config)# wireless profile policy wlan-policy-profilename`	ワイヤレス ポリシー プロファイルを設定します。 **注意** 名前付きワイヤレス プロファイル ポリシーでネイティブ プロファイリングの AAA オーバーライドを設定しないでください。ネイティブ プロファイリングは、AAA ポリシーよりも低い優先順位で適用されます。AAA オーバーライドが有効になっている場合、AAA ポリシーでネイティブ プロファイル ポリシーがオーバーライドされます。
ステップ 8	**description** *profile-policy-description* 例： `Device(config-wireless-policy)# description "default policy profile"`	ポリシー プロファイルの説明を追加します。
ステップ 9	**dhcp-tlv-caching** 例： `Device(config-wireless-policy)# dhcp-tlv-caching`	WLAN で DHCP TLV キャッシングを設定します。
ステップ 10	**http-tlv-caching** 例： `Device(config-wireless-policy)# http-tlv-caching`	WLAN でクライアント HTTP TLV キャッシングを設定します。
ステップ 11	**subscriber-policy-name** *policy-name* 例：	サブスクライバ ポリシー名を設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# subscriber-policy-name polmap5`	
ステップ 12	**vlan** *vlan-id* 例： `Device(config-wireless-policy)# vlan 1`	VLAN 名または VLAN ID を設定します。
ステップ 13	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	設定を保存します。

ローカルモードでのネイティブプロファイリングの設定

ローカルモードでネイティブプロファイリングを設定するには、ポリシーマップの作成（CLI）（839 ページ）で説明されている手順に従う必要があります。ポリシープロファイルでは、ネイティブプロファイリングを設定するには、以下の手順の説明に従い、中央スイッチングを有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。

ネイティブ プロファイル設定の確認

ネイティブ プロファイル設定を確認するには、次の **show** コマンドを使用します。

```
Device# show wireless client device summary

Active classified device summary
MAC Address       Device-type                      User-role
   Protocol-map
-----------------------------------------------------------------------------------------------
1491.82b8.f94b    Microsoft-Workstation            sales
               9
1491.82bc.2fd5    Windows7-Workstation             sales
              41


Device# show wireless client device cache

Cached classified device info
```

```
MAC Address       Device-type                       User-role
   Protocol-map
-------------------------------------------------------------------------------------------------
2477.031b.aa18    Microsoft-Workstation
               9
30a8.db3b.a753    Un-Classified Device
               9
4400.1011.e8b5    Un-Classified Device
               9
980c.a569.7dd0    Un-Classified Device
```

```
Device# show wireless client mac-address 4c34.8845.e32c detail | s
Session Manager:
  Interface :
  IIF ID            : 0x90000002
  Device Type       : Microsoft-Workstation
  Protocol Map      : 0x000009
  Authorized        : TRUE
  Session timeout   : 1800
  Common Session ID: 78380209000000174BF2B5B9
  Acct Session ID   : 0
  Auth Method Status List
   Method : MAB
    SM State         : TERMINATE
    Authen Status    : Success
  Local Polices:
   Service Template : wlan_svc_C414.3CCA.0A51 (priority 254)
    Absolute-Timer   : 1800
  Server Polices:
  Resultant Policies:
  Filter-ID         : acl-auto
  Input QOS         : in_qos
  Output QOS        : out_qos
  Idle timeout      : 60 sec
  VLAN               : 10
  Absolute-Timer    : 1000
```

クラス マップ名のクラス マップの詳細を確認するには、次の **show** コマンドを使用します。

```
Device# show class-map type control subscriber name test
Class-map               Action                        Exec  Hit  Miss  Comp
---------                ------                       ----  ---  ----   ---
match-any test     match day Monday                     0     0    0     0
match-any test     match join-time-of-day 8:00 18:00    0     0    0     0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```

第 X 部

IPv6

第 68 章

IPv6 クライアントのアドレス ラーニング

IPv6 クライアント アドレス ラーニングについて

クライアント アドレス ラーニングは、ワイヤレスクライアントの IPv4 および IPv6 アドレスを学習し、アソシエーションおよびタイムアウト時に組み込みワイヤレスコントローラによって維持されるクライアント遷移状態を学習するために、組み込みワイヤレスコントローラで設定します。

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLAAC）
- ステートフル DHCPv6
- 静的設定

これらすべての方法において、IPv6 クライアントは常にネイバー送信要求 DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。 組み込みワイヤレスコントローラは、クライアントのネイバー探索プロトコル（NDP）およびDHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習します。

SLAAC を使用したアドレス割り当て

IPv6 クライアントアドレス割り当ての最も一般的な方法は SLAAC です。SLAAC は、クライアントが IPv6 プレフィクスに基づいてアドレスを自己割り当てする、シンプルなプラグアンドプレイ接続を提供します。

SLAAC は次のように設定されます。

- ホストは、ルータ送信要求メッセージを送信します。

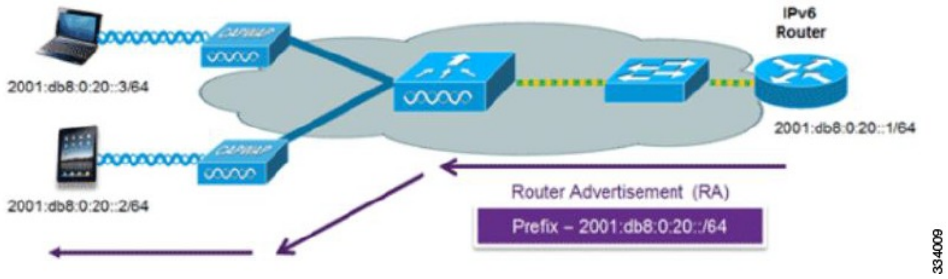
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 選択されるランダムアドレスが他のクライアントと競合しないように、IPv6 クライアントによって重複アドレス検出が実行されます。

（注） アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

IPv6 アドレスの最後の 64 ビットは、次のアルゴリズムに基づいて学習できます。

- インターフェイスの MAC アドレスに基づく EUI-64
- ランダムに生成されるプライベートアドレス

図 *24 : SLAAC* を使用したアドレス割り当て



Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントをイネーブルにします。

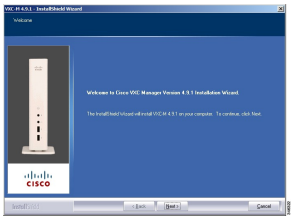
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

ステートフル DHCPv6 アドレス割り当て

DHCPv6 の使用は、SLAAC がすでに導入されている場合は、IPv6 クライアント接続で要求されません。DHCPv6 にはステートレスおよびステートフルという 2 種類の動作モードがあります。

DHCPv6 ステートレスモードは、ルータアドバタイズメントで使用できない追加のネットワーク情報をクライアントに提供するために使用されますが、IPv6 アドレスは、SLAAC によってすでに提供されているため提供されません。情報には、DNS ドメイン名、DNS サーバー、その他の DHCP ベンダー固有のオプションが含まれます。

図 *25 :* ステートフル *DHCPv6* アドレス割り当て



このインターフェイス設定は、SLAAC を有効にしてステートレス DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

静的 IP アドレス割り当て

クライアントにスタティックに設定されたアドレス。

ルータ要求

ルータ送信要求メッセージは、コントローラがローカルルーティングに関する情報を入手できる、またはステートレス自動設定を設定できるルータアドバタイズメントを送信するようにローカルルータを促すために、ホストコントローラによって発行されます。ルータ アドバタイズメントは定期的に送信され、起動時または再起動操作後などに、ホストはルータ送信要求を使用して即時ルータ アドバタイズメントを要求します。

ルータ アドバタイズメント

ルータ アドバタイズメント メッセージは、ルータから定期的に送信されるか、ホストからのルータ送信要求メッセージへの応答として送信されます。これらのメッセージに含まれる情報は、ホストでステートレス自動設定を実行し、ルーティングテーブルを変更するために使用されます。

ネイバー探索

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。ネイバー探索は、IPv4 で使用されていた Address Resolution Protocol（ARP）、Internet Control Message Protocol（ICMP）ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー探索検査によってネイバー探索メッセージが分析され、準拠しない IPv6 ネイバー探索パケットはドロップされます。 内のネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。クライアントは、ネイバー バインディング タイマーに従って、テーブルから消去されます。

ネイバー探索抑制

ワイヤレスクライアントの IPv6 アドレスは、deviceによってキャッシュされます。deviceが IPv6 アドレスを検索する NS マルチキャストを受信して、deviceによって特定された目的のアドレスがクライアントのいずれかに属している場合、deviceはクライアントに代わって NA メッセージで応答します。このプロセスの最後に IPv4 の ARP テーブルと同等のものが生成されますが、使用するメッセージが少ないため、より効率的です。

（注） deviceがプロキシのように動作し NA で応答するのは、ipv6 nd suppress コマンドが設定されている場合だけです。

deviceにワイヤレスクライアントの IPv6 アドレスがない場合、deviceは NA で応答せず、NS パケットをワイヤレス側に転送します。この問題を解決するために、NS マルチキャスト フォワーディング ノブが用意されています。このノブがイネーブルの場合、deviceは存在しない（キャッシュ欠落）IPv6 アドレスの NS パケットを取得し、ワイヤレス側に転送します。このパケットは、目的のワイヤレスクライアントに到達し、クライアントは NA で応答します。

このキャッシュミスシナリオが発生するのはまれで、完全な IPv6 スタックが実装されていないクライアントが、NDP 時にそれらの IPv6 アドレスをアドバタイズしない可能性はほとんどありません。

ルータ アドバタイズメント ガード

- フレームが受信されるポート
- IPv6 送信元アドレス
- プレフィックス リスト
- ルータ アドバタイズメント ガード メッセージを受信するための信頼できるポートまたは信頼できないポート
- ルータアドバタイズメント送信者の信頼できるまたは信頼できない送信元 IPv6 アドレス

- 信頼できる/信頼できないプレフィックス リストおよびプレフィックス範囲
- ルータプリファレンス

ルータ アドバタイズメント スロットリング

RA スロットリングを使用すると、コントローラがワイヤレスネットワーク宛ての RA パケットを強制的に制限できます。RA スロットリングを有効にすると、多数の RA パケットを送信するルータを最小周波数に調整でき、IPv6 クライアントの接続も維持されます。クライアントが RS パケットを送信すると、RA がクライアントに返送されます。この RA は、コントローラを通過でき、クライアントにユニキャストされます。このプロセスによって、新しいクライアントやローミング クライアントが RA スロットリングの影響を受けないようにすることができます。

IPv6 クライアント アドレス ラーニングの前提条件

IPv6 クライアント アドレス ラーニングを設定する前に、IPv6 をサポートするように 組み込みワイヤレスコントローラクライアントを設定します。

組み込みワイヤレスコントローラ インターフェイスでの IPv6 の設定

インターフェイスで IPv6 を設定するには、次の手順に従います。

始める前に

クライアント上の IPv6 および有線インフラストラクチャ上の IPv6 サポートをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： デバイス# **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 3	**interface GigabitEthernet0** 例： デバイス(config)# **interface GigabitEthernet0**	GigabitEthernetインターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address fe80::1 link-local** 例： デバイス(config-if)# **ip address 198.51.100.1 255.255.255.0** デバイス(config-if)# **ipv6 address fe80::1 link-local** デバイス(config-if)# **ipv6 address 2001:DB8:0:1:FFFF:1234::5/64** デバイス(config-if)# **ipv6 address 2001:DB8:0:0:E000::F/64**	リンクローカルオプションを使用して、GigabitEthernetインターフェイスでIPv6アドレスを設定します。
ステップ 5	**ipv6 enable** 例： デバイス(config)# **ipv6 enable**	（任意）GigabitEthernetインターフェイスで IPv6 を有効にします。
ステップ 6	**end** 例： デバイス(config)# **end**	インターフェイスモードを終了します。

ネイティブ IPv6

IPv6 について

IPv6 は、デジタル ネットワーク上のデータ、音声、およびビデオ トラフィックの交換に使用されるパケットベースのプロトコルです。IPv6 は IP に基づいていますがアドレス空間が大幅に拡大されており、メインヘッダーと拡張ヘッダーが簡素化されるなどの改善が行われています。IPv6 のアーキテクチャは、既存の IPv4 ユーザーがエンドツーエンドのセキュリティ、Quality Of Service（QoS）、およびグローバルに一意のアドレスなどのサービスを引き続き利用しながら、簡単に IPv6 へ移行できるように設計されています。拡大された IPv6 アドレス空間により、ネットワークのスケーラビリティが可能となり、グローバルな到達可能性が提供されます。

（注） IPv4 アドレスを使用して IPv4 ネットワークで動作する機能は、IPv6 アドレスを使用して IPv6 ネットワークでも動作します。

一般的な注意事項

- IPv6機能を動作させるため、ipv6 unicast-routingコマンドを組み込みワイヤレスコントローラで設定する必要があります。
- ワイヤレス管理インターフェイスには、スタティック IPv6 アドレスを 1 つだけ設定する必要があります。
- ワイヤレス管理インターフェイスおよびクライアント VLAN でルータアドバタイズメントを抑制する必要があります（IPv6 がクライアント VLAN で設定されている場合）。
- 優先モードは、AP 接続プロファイルに含まれます。優先モードを IPv6 として設定すると、AP は最初に IPv6 を介した接続を試みます。無効にしなかった場合、AP は IPv4 にフォールバックします。
- AP およびクライアントの RA トレースには MAC アドレスを使用する必要があります。

サポートされない機能

- UDP Lite はサポートされていません。
- IPv6 を介した AP スニッファはサポートされていません。
- IPv6 は、HA ポート インターフェイスではサポートされていません。
- IPv6 を介した自動 RF グループ化はサポートされていません。静的 RF グループ化のみがサポートされます。

IPv6 アドレッシングの設定

IPv6 アドレッシングを設定するには、次の手順に従います。

（注） IPv4 アドレスを使用して IPv4 ネットワークで動作する機能はすべて、IPv6 アドレスを使用して IPv6 ネットワークでも動作します。

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	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。

	コマンドまたはアクション	目的
ステップ 3	**interface GigabitEthernet0** 例： `デバイス(config)# interface GigabitEthernet0`	GigabitEthernet インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** *ipv6-address* 例： `Device(config-if)# ipv6 address FD09:9:2:49::53/64`	グローバル IPv6 アドレスを指定します。
ステップ 5	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	インターフェイス上で IPv6 をイネーブルにします。
ステップ 6	**ipv6 nd ra suppress all** 例： `Device(config-if)# ipv6 nd ra suppress all`	インターフェイス上で IPv6 ルータ アドバタイズメントの送信を抑制します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**wireless management interface gigabitEthernet** *gigabitEthernet-interface-vlan 64* 例： `Device(config)# wireless management interface gigabitEthernet vlan 64`	ワイヤレス管理インターフェイスで、サポートされている AP に接続されているポートを設定します。
ステップ 9	**ipv6 route** *ipv6-address* 例： `Device(config)# ipv6 route ::/0 FD09:9:2:49::1`	IPv6 スタティック ルートを指定します。

AP 接続プロファイルの作成（GUI）

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] ウィンドウで [General] タブをクリックし、[Add] をクリックします。

ステップ 3 [Name] フィールドに、AP 接続プロファイルの名前を入力します。

ステップ 4 （任意）AP 接続プロファイルの説明を入力します。

ステップ 5 **[CAPWAP]** > **[Advanced]** を選択します。

ステップ 6 [Advanced] タブの下にある [Preferred Mode] ドロップダウンリストから、[IPv6] を選択します。AP の優先モードが IPv6 に設定されます。

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

AP 接続プロファイルの作成（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。
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。
ステップ 3	**description** *ap-profile-name* 例： `Device(config-ap-profile)# description "xyz ap profile"`	AP プロファイルの説明を追加します。
ステップ 4	**preferred-mode ipv6** 例： `Device(config-ap-profile)# preferred-mode ipv6`	APの優先モードをIPv6に設定します。

プライマリコントローラとバックアップ 組み込みワイヤレスコントローラの設定（GUI）

始める前に

プライマリコントローラとバックアップ 組み込みワイヤレスコントローラを設定する前に、AP 接続プロファイルが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] > [AP Join] > > を選択します。

ステップ 2 [AP Join Profile] ウィンドウで、AP 接続プロファイル名をクリックします。

ステップ 3 [Edit AP Join Profile] ウィンドウで [CAPWAP] タブをクリックします。

ステップ 4 [Backup Controller Configuration] の [High Availability] タブで、[Enable Fallback] チェックボックスをオンにします。

ステップ 5 プライマリ コントローラとセカンダリ コントローラの名前および IP アドレスを入力します。

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

プライマリ コントローラとバックアップ コントローラの設定（CLI）

選択した AP のプライマリおよびセカンダリコントローラを設定するには、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	**ap profile** *profile-name* 例： `Device(config)# ap profile yy-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。
ステップ 3	**capwap backup primary** *primary-controller-name primary-controller-ip* 例： `Device(config)# capwap backup primary WLAN-Controller-A 2001:DB8:1::1`	プライマリ バックアップ コントローラの名前を使用してAPCAPWAPパラメータを設定します。 （注） **capwap backup primary** と **capwap backup secondary** を機能させるには、高速ハートビートを有効にする必要があります。 コントローラと AP 間のリンクの信頼性が低い場合に、高速ハートビートが有効になっていると、APの切断が発生する可能性があります。

	コマンドまたはアクション	目的
ステップ 4	**ap capwap backup secondary** *secondary-controller-name secondary-controller-ip* 例： `Device(config)# capwap backup secondary WLAN-Controller-B 2001:DB8:1::1`	セカンダリ バックアップ コントローラの名前を使用して AP CAPWAP パラメータを設定します。
ステップ 5	**syslog host** *ipaddress* 例： `Device(config)# syslog host 2001:DB8:1::1`	AP のシステムログの設定を設定します。
ステップ 6	**tftp-downgrade** *tftp-server-ip imagename* 例： `Device(config)# tftp-downgrade 2001:DB8:1::1 testimage`	すべての AP の TFTP サーバーから AP イメージのダウングレードを開始します。

IPv6 設定の確認

次の **show** コマンドを使用して、IPv6 設定を確認します。

```
Device# show wireless interface summary

Interface Name   Interface Type VLAN ID IP Address   IP Netmask     NAT-IP Address   MAC
 Address
-------------------------------------------------------------------------------------------------
GigabitEthernet0 Management     0       0.0.0.0     255.255.255.0  0.0.0.0
d4c9.3ce6.b854
                                        fd09:9:2:49::54/64
```

第 69 章

IPv6 ACL

IPv6 ACL について

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。deviceで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは中央処理装置（CPU）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

Web 認証用に事前認証 ACL を作成することもできます。このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

ACL のタイプ

ユーザーあたりの IPv6 ACL

ユーザーあたりの ACL の場合、テキスト文字列としての完全なアクセス コントロール エントリ（ACE）が Cisco Secure Access Control Server（Cisco Secure ACS）で設定されます。

ACE はコントローラ組み込みワイヤレスコントローラで設定されません。ACE は `ACCESS-Accept` 属性でdeviceに送信され、クライアント用に直接適用されます。ワイヤレス クライアントが外部deviceにローミングするときに、ACE が、AAA 属性としてモビリティ ハンドオフ メッセージで外部deviceに送信されます。ユーザーあたりの ACL を使用した出力方向はサポートされていません。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がdeviceで設定され、`filter-id` のみが Cisco Secure ACS で設定されます。

`filter-id` は ACCESS-Accept 属性でdeviceに送信され、deviceは ACE の filter-id をルックアップしてから、クライアントに ACE を適用します。クライアント L2 が外部deviceにローミングするときに、filter-id だけがモビリティ ハンドオフ メッセージで外部deviceに送信されます。ユーザーあたりの ACL を使用した出力フィルタ ACL はサポートされていません。外部deviceは filter-id と ACE を事前に設定する必要があります。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL（dACL）の場合、完全な ACE および `dacl` 名は Cisco Secure ACS のみで設定されます。

Cisco Secure ACS はその `ACCESS-Accept` 属性で `dacl` 名をdeviceに送信します。デバイスは `dacl` 名を取得し、ACE のために `dACL` 名を `ACCESS-request` 属性を使用して Cisco Secure ACS に送り返します。

IPv6 ACL の設定の前提条件

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチが Network Essentials ライセンスで稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

IPv6 ACL の設定の制約事項

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

deviceは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- deviceは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- deviceは再帰 ACL（**reflect** キーワード）をサポートしません。
- deviceは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、deviceはインターフェイスで ACL がサポートされるかどうかを判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロール エントリ（ACE）を追加しようとする場合、deviceは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングするには、次の手順に従います。

1. IPv6 ACL を作成し、IPv6 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。
2. IPv6 ACL が、トラフィックをブロックする（deny）または通過させる（permit）よう設定します。
3. トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。
4. インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージ プロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。
- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 3	**ipv6 access-list** *acl_name* 例： デバイス# **ipv6 access-list access-list-name**	名前を使用して IPv6 アクセス リストを定義し、IPv6 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。
ステップ 4	**{deny|permit} protocol** 例： `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。

	コマンドまたはアクション	目的
		source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。destination-ipv6-prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）port-number は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。log-input を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
		• （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	**{deny|permit} tcp** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3 で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビットセット • established：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビットセット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット
ステップ 6	**{deny|permit} udp** 例： `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length`	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator

	コマンドまたはアクション	目的
		[port]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 7	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]`	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、icmp を入力します。ICMP パラメータはステップ 3a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • icmp-type：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-code：ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-message：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンドリファレンスを参照してください。
ステップ 8	**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。
ステップ 9	**show ipv6 access-list** 例：	アクセス リストの設定を確認します。

	コマンドまたはアクション	目的
	`show ipv6 access-list`	
ステップ 10	**copy running-config startup-config** 例： `copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

WLAN IPv6 ACL の作成

IPv6 ACL の確認

IPv6 ACL の表示

IPv6 ACL を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 3	**show access-list** 例： デバイス# **show access-lists**	deviceに設定されたすべてのアクセス リストを表示します。
ステップ 4	**show ipv6 access-list** *acl_name* 例： デバイス# **show ipv6 access-list** *[access-list-name]*	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番めの許可エントリは必要です。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
デバイス(config)# ipv6 access-list CISCO
デバイス(config-ipv6-acl)# deny tcp any any gt 5000
デバイス (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
デバイス(config-ipv6-acl)# permit icmp any any
デバイス(config-ipv6-acl)# permit any any
```

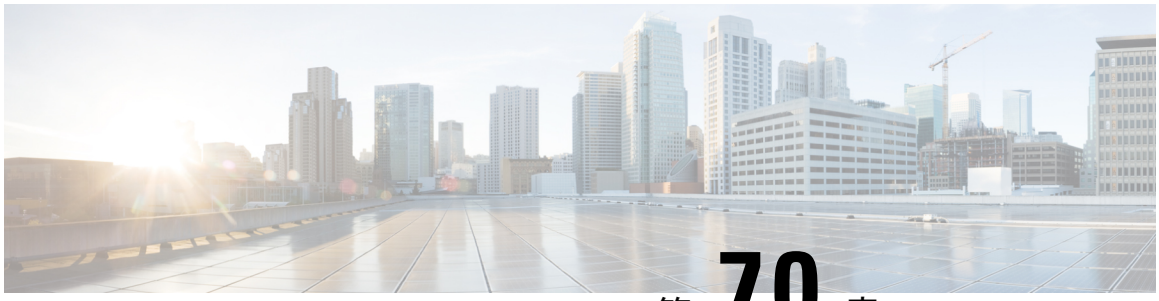
例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
デバイス #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
デバイス# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```



第 70 章

IPv6 対応認定

IPv6 対応認定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

この機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

表 *38 : IPv6* 対応認定の機能履歴

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.1	IPv6 対応認証	この機能は、最新の RFC 仕様に準拠するために必要なさまざまな IPv6 機能を実装することで拡張されています。

IPv6 対応認定

Cisco IOS XE Bengaluru 17.6.1 には、IPv6 対応認定の最新の RFC 仕様に準拠するために必要なさまざまな IPv6 機能が実装されています。新しく実装された IPv6 の機能は次のとおりです。

- Fragment Processing and Reassembly（RFC8200）：最初のフラグメントには、RFC 8200 で指定されているように、最初の上位レベルプロトコル（ULP）ヘッダーまでの必須拡張ヘッダーが含まれている必要があります。
- Handling Atomic Fragments in Neighbor Discovery（RFC6980）：断片化されたネイバー探索パケットは破棄する必要があります。

- Packet too Big（RFC8201）：アトミック フラグメンテーションはサポートされていません。IPv6 MTU 要件の 1280 を満たしていないパケットはドロップされます。
- Route Information Options (RIO) in IPv6 Router Advertisements（RFC4191）：ルータからホストへの特定のルートを伝達するために、新しい RIO が IPv6 ルータ アドバタイズメント メッセージに追加されました。明示的なルート構成により、必要なルートのみがホストにアドバタイズされます。
- IPv6 Hop-by-Hop Processing（RFC 8200）：この拡張機能により、ホップバイホップ オプション ヘッダー処理を必要とするパケットの配信パスに沿って、ノードを明示的に構成できます。

IPv6 ルート情報の設定

IPv6 ルータ アドバタイズメント メッセージのルート情報オプション（RIO）は、ルータからホストへの特定のルートの通信に役立ちます。そのため、ホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合、ホストが適切なデフォルトルータを選択する機能が向上します。明示的なルート構成により、必要なルートのみがホストにアドバタイズされます。

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	**interface** *interface* **例：** `Device(config)# interface gigabitethernet1.1`	インターフェイスを指定し、インターフェイス 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	**ipv6 nd ra specific-route** *prefix/length* **lifetime** *lifetime/infinity* [**preference** *preference*] **例：** `Device(config-if)# ipv6 nd ra specific-route 3::3/116 lifetime 11 preference medium`	IPv6 ルータ アドバタイズメント メッセージの RIO を設定します。 詳細については、ipv6 nd ra specific route コマンドを参照してください。

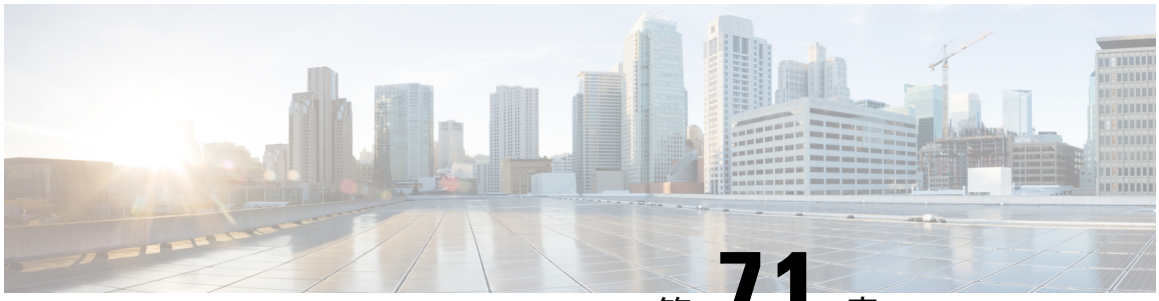
IPv6 ルート情報の確認

ルータアドバタイズメントで送信される特定のルートを識別するには、次のコマンドを使用します。

```
Device# show ipv6 nd ra specific-route

IPv6 Prefix/Length Lifetime Preference Interface
----------------------------------------- -------- ---------- ----------
1234::12/127 1000 High GigabitEthernet2
```

第 XI 部

CleanAir



第 71 章

Cisco CleanAir

Cisco CleanAir について

Cisco CleanAir は、共有ワイヤレス スペクトラムに関する問題の予防的な管理を目的に設計されたソリューションです。この機能を使用すると、共有スペクトラムの全ユーザーを確認できます（ネイティブデバイスと外部干渉源の両方）。また、この情報に基づいてネットワークが対処できるようにします。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルを変更して干渉を受けないようにすることができます。CleanAir は、スペクトラム管理と無線周波数（RF）の可視性を提供します。

Cisco CleanAir システムは CleanAir 対応アクセス ポイントで構成されます。アクセスポイントは工業、科学、医療用（ISM）帯域で動作するすべてのデバイスの情報を収集し、これらの情報を潜在的な干渉源として特定および評価して 組み込みワイヤレスコントローラに転送します。コントローラ 組み込みワイヤレスコントローラ はアクセスポイントを制御して。

ライセンス不要の帯域で動作している各デバイスについては、Cisco CleanAir はその種類、ワイヤレス ネットワークに与える影響の程度、取るべき対策を提示します。これによって RF がシンプルになります。

ワイヤレス LAN システムは、ライセンス不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。電子レンジやコードレス電話、そして Bluetooth デバイスなどの多くのデバイスもこれらの帯域で稼働するため、Wi-Fi の動作に悪影響を与える可能性があります。

Voice over Wireless や IEEE 802.11 無線通信などの非常に高度な WLAN サービスの一部は、ISM 帯域を合法的に使用する他のユーザーによる干渉によって、重大な影響を受ける可能性があります。Cisco CleanAir 機能の統合により、この RF 干渉の問題に対処できます。

Cisco CleanAir 関連の用語

表 *39 : CleanAir* 関連の用語

用語	説明
AQI	電波品質の指標。AQI は空気汚染物質に基づいた電波品質の指標です。AQI が 0 の場合は不良で、AQI が 85 より大きいと良好です。
AQR	電波品質レポート。AQR には、特定されたすべての発生源からの干渉全体に関する情報（AQI で表される）や、最も重大な干渉カテゴリの概要が示されます。AQR は 15 分ごとにモビリティ コントローラに送信され、30 秒ごとに迅速モードで送信されます。
DC	デューティ サイクル。チャネルがデバイスで使用される時間の割合。
EDRRM	イベント駆動型 RRM。EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスし、すぐにチャネルを変更できるようにします。
IDR	アクセスポイントが 組み込みワイヤレスコントローラに送信する干渉デバイス レポート。
ISI	干渉のシビラティ（重大度）指標。ISI は、干渉のシビラティ（重大度）の指標です。
RSSI	受信信号強度インジケータ。RSSI は受信した無線信号における電力の測定値です。アクセス ポイントはこの電力で干渉デバイスを認識します。

Cisco CleanAir のコンポーネント

Cisco CleanAir の基本的なアーキテクチャは、Cisco CleanAir 対応 AP およびdeviceで構成されます。

Cisco CleanAir テクノロジーを搭載したアクセスポイントは、非 Wi-Fi 干渉源に関する情報を収集処理します。アクセスポイントは、電波品質レポート（AQR）および干渉デバイスレポート（IDR）を 組み込みワイヤレスコントローラに送信します。

コントローラは CleanAir 対応のアクセス ポイントを制御および設定し、スペクトラム データを収集および処理します。はCleanAirの基本機能およびサービスを設定し、現在のスペクトラム情報を表示するローカル ユーザー インターフェイス（GUI および CLI）を提供します。また、は RRM TPC と DCA を使用して、干渉デバイスを検出、マージ、および軽減します。詳細については、「干渉デバイスのマージ」を参照してください。

Cisco CleanAir システムにおいて、deviceは次のような処理を実行します。

- アクセス ポイントにおける Cisco CleanAir 機能を設定する。
- Cisco CleanAir の機能の設定やデータ収集のためのインターフェイス（、CLI）を提供する。
- スペクトラム データを表示する。

- アクセス ポイントから AQR を収集して処理し、電波品質データベースに保存する。AQR には、特定されたすべての発生源からの干渉全体に関する情報（電波品質の指標（AQI）で表す）や、最も重大な干渉カテゴリの概要が示されます。また CleanAir システムでは、干渉の種類別レポートに未分類の干渉情報を含めることができ、未分類の干渉デバイスによる干渉が頻繁に生じる場合に対処することができます。
- アクセス ポイントから IDR を収集して処理し、干渉デバイス データベースに保存する。

Cisco CleanAir で検出できる干渉の種類

Cisco CleanAir することができます。

Wi-Fi チップをベースとする RF 管理システムには、次のような共通の特性があります。

- Wi-Fi 信号として識別できない RF エネルギーはノイズとして報告される。
- チャネル計画の割り当てに使用するノイズの測定値は、一部のクライアントデバイスに悪影響を及ぼす可能性のある不安定さや急速な変化を避けるために、一定の期間において平均化される傾向がある。
- 測定値が平均化されることで、測定値の精度が低下する。そのため、平均化された後、クライアントに混乱をもたらす信号が緩和を必要とするものに見えない場合がある。
- 現在使用できる RF 管理システムは、本質的にはすべて事後対応型である。

Cisco CleanAir はこれらと異なり、ノイズの発生源だけでなく、WLAN に対する潜在的な影響まで明確に特定することができます。このような情報を入手することにより、ネットワーク内におけるノイズを考慮し、理にかなった、可能であれば予防的な判断を行うことができます。

（注） イベント駆動型 RRM は、Cisco CleanAir 対応でローカル モードにあるアクセス ポイントによってのみ動作します。

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir のスペクトラム イベント駆動型 RRM 機能を使用すると、電波品質（AQ）のしきい値を設定できます。このしきい値を超過した場合は、影響を受けたアクセス ポイントに対してチャネル変更がただちに行われます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。Cisco CleanAir では干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

電子レンジ、屋外のイーサネットブリッジの 2 つは、永続的として評価される分類のデバイスです。一度検出されれば、これらのデバイスは継続的に無作為なタイミングで問題となり、移動することもないと考えられるからです。これらのタイプのデバイスに関しては、検出された

チャネルの検出された AP においてクライアントに影響する干渉の発生する可能性が高いことをRRMが「覚えておける」ように、RRMに影響を受けたチャネルの検出とバイアスの適用を指示できます。詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_0100.html?bookSearch=true#id_15217を参照してください。

CleanAir PDA デバイスは次のとおりです。

- 電子レンジ
- WiMax Fixed
- WiMax Mobile
- Motorola Canopy

Bluetooth デバイスの場合、Cisco CleanAir 対応のアクセス ポイントで干渉の検出と報告を行うことができるのは、そのデバイスがアクティブに送信しているときだけです。Bluetoothデバイスには、さまざまな省電力モードがあります。たとえば、接続されたデバイス間でデータまたは音声がストリーム化されている最中に干渉が検出されます。

EDRRM および AQR の更新モード

EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスしてすぐにチャネルを変更できるようにするための機能です。CleanAir アクセス ポイントは AQ を常に監視し、AQ を 15 分ごとに報告します。AQは分類された干渉デバイスのみを報告します。EDRRM の主なメリットは短い処理時間です。干渉デバイスがアクティブ チャネルで動作しており、EDRRM をトリガーするのに十分な AQ の低下を引き起こした場合、クライアントはそのチャネルまたはアクセス ポイントを使用できなくなります。チャネルからアクセス ポイントを削除する必要があります。EDRRM はデフォルトではイネーブルになっていません。最初に CleanAir をイネーブルにしてから、EDRRM をイネーブルにします。

CleanAir の前提条件

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

次のアクセス ポイント モードを使用して、Cisco CleanAir スペクトラム モニタリングを実行できるのは、Cisco CleanAir 対応のアクセス ポイントだけです。

- Local：このモードでは、Cisco CleanAir 対応の各アクセス ポイント無線によって、現在の動作チャネルだけに関する電波品質と干渉検出のレポートが作成されます。AP は、Wi-Fi フレームの送信でビジー状態でない場合にのみ電波品質と干渉を測定できます。これは、AP のチャネル使用率が高い場合、CleanAir 検出が大幅に低下することを意味します。
- Monitor：Cisco CleanAir が監視モードで有効になっていると、そのアクセス ポイントによって、モニターされているすべてのチャネルに関する電波品質と干渉検出のレポートが作成されます。

  次のオプションを使用できます。

- All：すべてのチャネル
- DCA：DCA リストによって管理されるチャネル選択
- Country：規制ドメイン内で合法なすべてのチャネル

CleanAir の制約事項

- 監視モードのアクセス ポイントは、Wi-Fi トラフィックまたは 802.11 パケットを送信しません。これらは無線リソース管理（RRM）計画から除外され、隣接アクセス ポイントのリストに含まれません。IDR クラスタリングは、deviceがネットワーク内の隣接アクセス ポイントを検出する機能に依存しています。複数のアクセスポイントから関係する干渉デバイスを検出する機能を使用できるのは、監視モードのアクセス ポイント間に限られます。
- 4800 AP スロット 1 の場合、5 GHz は専用であり、個別にモニターモードに移動することはできません。ただし、スロット 0 は XOR であり、2.4/5 GHz と同様にモニターに移動できます。スロット 2 は専用モニターであり、5 GHz で動作し、AP モニターモードでは、モニター無線が 2.4/5 GHz の両方ですでに使用可能であるため、スロット 2 は無効になります。3700 AP には専用の 2.4GHz（slot0）と 5GHz（slot1）があります。
- SE Connect モードでは、コントローラの物理ポートにアクセスポイントを直接接続しないでください。
- チャネル幅が 160 MHz の場合、CleanAir はサポートされません。

CleanAir の設定方法

2.4 GHz 帯域の CleanAir の有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。
ステップ 2 [CleanAir] ページで **[2.4 GHz Band]** > **[General]** タブをクリックします。
ステップ 3 [Enable CleanAir] チェックボックスをオンにします。
ステップ 4 [Apply] をクリックします。

2.4 GHz 帯域の CleanAir の有効化（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。

ステップ 2	**ap dot11 24ghz cleanair**
	例：
	`デバイス(config)#ap dot11 24ghz cleanair`
	`デバイス(config)#no ap dot11 24ghz cleanair`
		802.11b ネットワークで CleanAir 機能を有効にします。802.11b ネットワークで CleanAir を無効にするには、このコマンドの **no** 形式を実行します。

ステップ 3	**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。

2.4 GHz デバイスの干渉レポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。

ステップ 2 [2.4 GHz Band] タブをクリックします。

ステップ 3 干渉タイプを選択し、[Interference Types to detect] セクションに追加します。

次の干渉タイプを使用できます。

- BLE Beacon：Bluetooth Low Energy ビーコン
- Bluetooth 検出
- Bluetooth リンク
- Canopy
- 連続トランスミッタ
- DECT-like Phone：Digital Enhanced Cordless Technology 電話機
- 802.11 FH：802.11 周波数ホッピング デバイス

- WiFi Inverted：スペクトル反転 Wi-Fi 信号を使用するデバイス
- Jammer
- 電子レンジ
- WiFi Invalid Channel：非標準の Wi-Fi チャネルを使用するデバイス
- TDD トランスミッタ
- Video Camera
- SuperAG：802.11 SuperAG デバイス
- WiMax Mobile
- WiMax Fixed
- 802.15.4
- Microsoft Device
- SI_FHSS

ステップ 4 [Apply] をクリックします。

2.4 GHz デバイスの干渉レポートの設定（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。

ステップ 2	**ap dot11 24ghz cleanair device** {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** }
	例：
	`デバイス(config)# ap dot11 24ghz cleanair device bt-discovery`
	`デバイス(config)# ap dot11 24ghz cleanair device bt-link`
		deviceに報告するように 2.4 GHz 干渉デバイスを設定します。設定を無効にするには、このコマンドの **no** 形式を実行します。
		次に、キーワードの説明のリストを示します。
		• **bt-discovery**：Bluetooth の検出
		• **bt-link**：Bluetooth リンク
		• **canopy**：Canopy デバイス
		• **cont-tx**：連続トランスミッタ

	コマンドまたはアクション	目的
	デバイス(config)# **ap dot11 24ghz cleanair device canopy** デバイス(config)# **ap dot11 24ghz cleanair device cont-tx** デバイス(config)# **ap dot11 24ghz cleanair device dect-like** デバイス(config)# **ap dot11 24ghz cleanair device fh** デバイス(config)# **ap dot11 24ghz cleanair device inv** デバイス(config)# **ap dot11 24ghz cleanair device jammer** デバイス(config)# **ap dot11 24ghz cleanair device mw-oven** デバイス(config)# **ap dot11 24ghz cleanair device nonstd** デバイス(config)# **ap dot11 24ghz cleanair device report** デバイス(config)# **ap dot11 24ghz cleanair device superag** デバイス(config)# **ap dot11 24ghz cleanair device tdd-tx** デバイス(config)# **ap dot11 24ghz cleanair device video** デバイス(config)# **ap dot11 24ghz cleanair device wimax-fixed** デバイス(config)# **ap dot11 24ghz cleanair device wimax-mobile** デバイス(config)# **ap dot11 24ghz cleanair device xbox** デバイス(config)# **ap dot11 24ghz cleanair device zigbee** デバイス(config)# **ap dot11 24ghz cleanair device alarm**	• **dect-like**：Digital Enhanced Cordless Communication 方式の電話機 • **fh**：802.11 周波数ホッピング デバイス • **inv**：スペクトル反転 Wi-Fi 信号を使用するデバイス • **jammer**：電波妨害装 • **mw-oven**：電子レンジ • **nonstd**：非標準 Wi-Fi チャネルを使用するデバイス • **report**：干渉デバイスのレポート • **superag**：802.11 SuperAG デバイス • **tdd-tx**：TDD トランスミッタ • **video**：ビデオ カメラ • **wimax-fixed**：WiMax 固定 • **wimax-mobile**：WiMax モバイル • **msft-xbox**：Microsoft Xbox デバイス • **zigbee**：802.15.4 デバイス
ステップ 3	**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。

5 GHz 帯域の CleanAir の有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。
ステップ 2 [CleanAir] ページで **[5 GHz Band]** > **[General]** タブをクリックします。
ステップ 3 [Enable CleanAir] チェックボックスをオンにします。
ステップ 4 [Apply] をクリックします。

5 GHz 帯域の CleanAir の有効化（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。

ステップ 2	**ap dot11 5ghz cleanair**
	例：
	`デバイス(config)#ap dot11 5ghz cleanair`
	
	`デバイス(config)#no ap dot11 5ghz cleanair`
		802.11a ネットワークで CleanAir 機能を有効にします。802.11a ネットワークで CleanAir を無効にするには、このコマンドの **no** 形式を実行します。

ステップ 3	**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。

5 GHz デバイスの干渉レポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。
ステップ 2 [5 GHz Band] タブをクリックします。
ステップ 3 干渉タイプを選択し、[Interference Types to detect] セクションに追加します。

次の干渉タイプを使用できます。

- Canopy
- 連続トランスミッタ
- DECT-like Phone：Digital Enhanced Cordless Technology 電話機
- 802.11 FH：802.11 周波数ホッピング デバイス
- WiFi Inverted：スペクトル反転 Wi-Fi 信号を使用するデバイス
- Jammer
- WiFi Invalid Channel：非標準の Wi-Fi チャネルを使用するデバイス
- SuperAG：802.11 SuperAG デバイス
- TDD トランスミッタ
- WiMax Mobile
- WiMax Fixed
- Video Camera

ステップ 4 [Apply] をクリックします。

5 GHz デバイスの干渉レポートの設定（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。

ステップ 2	**ap dot11 5ghz cleanair device**{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}
	例：
	`デバイス(config)#ap dot11 5ghz cleanair device canopy`
	`デバイス(config)#ap dot11 5ghz cleanair device cont-tx`
		deviceに報告するように 5 GHz 干渉デバイスを設定します。干渉デバイスのレポートを無効にするには、このコマンドの **no** 形式を実行します。
		次に、キーワードの説明のリストを示します。
		• **canopy**：Canopy デバイス
		• **cont-tx**：連続トランスミッタ
		• **dect-like**：Digital Enhanced Cordless Communication 方式の電話機

	コマンドまたはアクション	目的
	デバイス(config)#**ap dot11 5ghz cleanair device dect-like** デバイス(config)#**ap dot11 5ghz cleanair device inv** デバイス(config)#**ap dot11 5ghz cleanair device jammer** デバイス(config)#**ap dot11 5ghz cleanair device nonstd** デバイス(config)#**ap dot11 5ghz cleanair device report** デバイス(config)#**ap dot11 5ghz cleanair device superag** デバイス(config)#**ap dot11 5ghz cleanair device tdd-tx** デバイス(config)#**ap dot11 5ghz cleanair device video** デバイス(config)#**ap dot11 5ghz cleanair device wimax-fixed** デバイス(config)#**ap dot11 5ghz cleanair device wimax-mobile** デバイス(config)#**ap dot11 5ghz cleanair device si_fhss** デバイス(config)#**ap dot11 5ghz cleanair device alarm**	• **fh**：802.11 周波数ホッピング デバイス • **inv**：スペクトル反転 Wi-Fi 信号を使用するデバイス • **jammer**：電波妨害装 • **nonstd**：非標準 Wi-Fi チャネルを使用するデバイス • **superag**：802.11 SuperAG デバイス • **tdd-tx**：TDD トランスミッタ • **video**：ビデオ カメラ • **wimax-fixed**：WiMax 固定 • **wimax-mobile**：WiMax モバイル
ステップ 3	**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。

CleanAir イベントのイベント駆動型 RRM の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。
[Radio Resource Management] ページが表示されます。

ステップ 2 [DCA] タブをクリックします。

ステップ 3 [Event Driven RRM] セクションで、CleanAir 対応 AP が重大なレベルの干渉を検出したときに RRM を実行するには、[EDRRM] チェックボックスをオンにします。

ステップ 4 次のオプションから、RRM を起動する必要がある [Sensitivity Threshold] レベルを設定します。

- [Low]：環境の変化への感度が低いことを表します。値は 35 に設定されます。
- [Medium]：環境の変化への感度が中程度であることを表します。値は 50 に設定されます。
- [High]：環境の変化への感度が高いことを表します。値は 60 に設定されます。
- [Custom]：このオプションを選択した場合は、[Custom Threshold] ボックスでカスタム値を指定する必要があります。

ステップ 5 不正デューティ サイクルを設定するには、[Rogue Contribution] チェックボックスをオンにしてから、[Rogue Duty-Cycle] でパーセント値を指定します。不正デューティ サイクルのデフォルト値は 80 パーセントです。

（注） 不正コントリビューションは、ED-RRM 機能に含まれている新しいコンポーネントです。不正コントリビューションにより、識別された不正チャネルの使用率に基づいて ED-RRM をトリガーできます。これは、CleanAir メトリックとは完全に分離されています。不正デューティサイクルは、通常のオフチャネル RRM メトリックから取得され、隣接する不正な干渉に基づいてチャネル変更が呼び出されます。RRM メトリックからとられており、CleanAir からではないため、通常 180 秒のオフ チャネル間隔と想定されるタイミングは、長くとも 3 分（180 秒）以内です。これは、CleanAir ED-RRM とは別に設定されており、デフォルトでは無効になっています。これにより、自身のネットワーク以外で発生し、個々の AP で測定される Wi-Fi の干渉に、AP が反応できるようになります。

ステップ 6 設定を保存します。

CleanAir イベントの EDRRM 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。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** 例： `デバイス(config)#ap dot11 24ghz rrm channel cleanair-event`	EDRRM の CleanAir イベントを有効にします。EDRRM を無効にするには、このコマンドの **no** 形式を実行します。

	コマンドまたはアクション	目的
	デバイス(config)#**no ap dot11 24ghz rrm channel cleanair-event**	
ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high | low | medium**}] 例： デバイス(config)#**ap dot11 24ghz rrm channel cleanair-event sensitivity high**	CleanAir イベントの EDRRM 感度を設定します。 次に、キーワードの説明のリストを示します。 • [High]：AQ 値によって示される非 Wi-Fi 干渉に対する最も高い感度を指定します。 • [Low]：AQ 値によって示される非 Wi-Fi 干渉に対する最も低い感度を指定します。 • [Medium]：AQ 値によって示される非 Wi-Fi 干渉に対する中間の感度を指定します。
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。

CleanAir パラメータの確認

次のコマンドを使用して CleanAir パラメータを確認できます。

表 *40 : CleanAir* の確認用コマンド

コマンド名	説明
show ap dot11 24ghz cleanair device type all	2.4 GHz 帯域のすべての CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type bt-discovery	2.4 GHz 帯域の BT Discovery タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type bt-link	2.4 GHz 帯域の BT Link タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type canopy	2.4 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します。

コマンド名	説明
show ap dot11 24ghz cleanair device type cont-tx	2.4 GHz 帯域の Continuous transmitter タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type dect-like	2.4 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type fh	2.4 GHz 帯域の 802.11FH タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type inv	2.4 GHz 帯域の Wi-Fi Inverted タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type jammer	2.4 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type mw-oven	2.4 GHz 帯域の MW Oven タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type nonstd	2.4 GHz 帯域の Wi-Fi inverted channel タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type superag	2.4 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type tdd-tx	2.4 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type video	2.4 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type wimax-fixed	2.4 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します。

干渉デバイスのモニターリング

CleanAir対応のアクセスポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意の ID を割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラム センサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。このようなデバイスは、スペクトラムデータベースから適切に削除されます。特定のデバイスに対する干渉源検出がすべてレポートされる場合は、デバイス検出が増大しないように、クラスタ ID が長期間にわたって有効になります。同じデバイスが再度検出された場合は、元のクラスタ ID とマージして、そのデバイスの検出履歴を保持します。

たとえば、Bluetooth 対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAir では、このようなデバイスを管理するために、クラスタ ID をより長く保持し、検出時には同じ 1 つのレコードに再度マージされます。この処理によってユーザー レコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。

CleanAir の設定例

次に、チャネルで動作する 2.4 GHz 帯域の CleanAir とアクセス ポイントをイネーブルにする例を示します。

```
デバイス#configure terminal
デバイス(config)#ap dot11 24ghz cleanair
デバイス(config)#exit
デバイス#ap name TAP1 dot11 24ghz cleanair
デバイス#end
```

次に、2.4 GHz 帯域の EDRRM の CleanAir イベントを有効にして、非 Wi-Fi 干渉に対する高い感度を設定する例を示します。

```
デバイス#configure terminal
デバイス(config)#ap dot11 24ghz rrm channel cleanair-event
デバイス(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
デバイス(config)#end
```

CleanAir に関する FAQ

Q. 複数のアクセス ポイントが同じ干渉デバイスを検出します。ところが、deviceにはそれらが別個のクラスタ、または疑いのあるさまざまなデバイスがクラスタ化された状態で表示されます。このようになるのはなぜですか。

A. deviceがこれらのアクセス ポイントによって検出されたデバイスのマージを検討するためには、アクセス ポイントが RF ネイバーである必要があります。アクセス ポイントがネイバー関係を確立するためには時間がかかります。deviceが再起動してから数分後、または RF グループの変更などのイベントの後は、クラスタリングがあまり正確ではありません。

Q. ネイバー アクセス ポイントを表示するにはどうすればよいですか。

A. ネイバー アクセス ポイントを表示するには、**show ap** *ap_name* **auto-rf dot11**{**24ghz** | **5ghz**} コマンドを使用します。

次に、ネイバー アクセス ポイントを表示する例を示します。

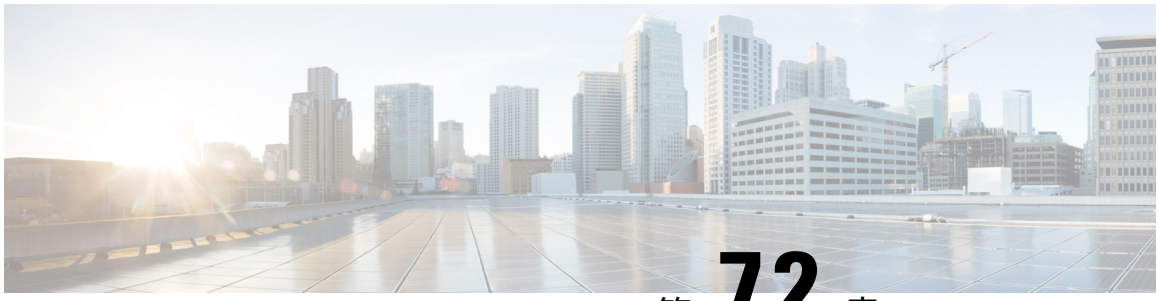
```
デバイス#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                        :  -12 dBm on   1 (10.10.0.5)
```

```
  AP 0C85.25AB.CCA0 slot 0                          :  -24 dBm on   6 (10.10.0.5)

  AP 0C85.25C7.B7A0 slot 0                          :  -26 dBm on  11 (10.10.0.5)

  AP 0C85.25DE.2C10 slot 0                          :  -24 dBm on   6 (10.10.0.5)

  AP 0C85.25DE.C8E0 slot 0                          :  -14 dBm on  11 (10.10.0.5)

  AP 0C85.25DF.3280 slot 0                          :  -31 dBm on   6 (10.10.0.5)

  AP 0CD9.96BA.5600 slot 0                          :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                          :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. CleanAir で利用可能な AP デバッグコマンドは何ですか。

A. CleanAir の AP デバッグコマンドは次のとおりです。

-
-



第 72 章

スペクトル インテリジェンス

スペクトル インテリジェンス

スペクトル インテリジェンス機能は、2.4 および 5 GHz 帯域で非 Wi-Fi 無線干渉をスキャンします。スペクトル インテリジェンスは、マイクロ波、連続波（ビデオ ブリッジやベビー モニターなど）、Wi-Fi および周波数ホッピング（Bluetooth および周波数ホッピング スペクトラム拡散（FHSS）コードレス電話）の 3 種類の干渉を検出する基本的な機能を提供します。

次の Cisco アクセス ポイント（AP）は、スペクトル インテリジェンス機能をサポートしています。

- Cisco Catalyst 9115 シリーズ Wi-Fi 6 AP
- Cisco Aironet 1852E/I AP
- Cisco Aironet 1832I AP
- Cisco Aironet 1815W/T/I/M AP
- Cisco Aironet 1810W/T AP
- Cisco Aironet 1800I/S AP
- Cisco Aironet 1542D/I AP

（注） Cisco DNA Center アシュアランス AP ヘルスでノイズ、電波品質、干渉、無線使用率などの無線の詳細情報を取得するには、Cisco Aironet 1832 および 1852 シリーズの AP でスペクトル インテリジェンス機能を有効にする必要があります。

制約事項

- SI AP は、ローカル モードで 1 つの干渉タイプのみを報告します。
- SI は、電波品質または干渉レポートのハイ アベイラビリティをサポートしていません。報告された干渉レポート/デバイスはスイッチオーバー後にスタンバイにコピーされないため、高可用性はサポートされません。干渉源がまだそこにある場合は、AP から再送信されると想定しています。
- スペクトル インテリジェンスは、次の 3 タイプのデバイスのみを検出します。
  - マイクロ波
  - 連続波：ビデオ レコーダー、ベビー モニター
  - SI-FHSS：Bluetooth、周波数ホッピング Digital European Cordless Telecommunication（DECT）電話機

スペクトル インテリジェンスの設定

スペクトル インテリジェンスを設定するには、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	**ap dot11** {**24ghz** | **5ghz**} **SI** 例： `Device(config)# ap dot11 24ghz SI`	802.11a または 802.11b ネットワークで 2.4 GHz または 5 GHz スペクトル インテリジェンス機能を設定します。 802.11a または 802.11b ネットワークで SI を無効にするには、コマンドの **no** 形式を追加します。

スペクトル インテリジェンスの情報の確認

スペクトル インテリジェンスの情報を確認するには、次のコマンドを使用します。

2.4 GHz または 5 GHz 帯域の SI 情報を表示するには、次のコマンドを使用します。

```
Device# show ap dot11 24ghz SI config

SI Solution..................................... : Enabled
Interference Device Settings:
```

```
        SI_FHSS.................................. : Enabled
    Interference Device Types Triggering Alarms:
        SI_FHSS.................................. : Disabled
```

2.4 GHz 帯域の連続トランスミッタ タイプの SI 干渉源を表示するには、次のコマンドを使用します。

```
Device# show ap dot11 24ghz SI device type cont_tx

DC    = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
AP type = CA, clean air, SI spectrum intelligence

No  ClusterID       DevID  Type     AP Type AP Name                 ISI  RSSI  DC
Channel
--- --------------- ------ -------- ------- ----------------- ---- ----- ----  ---
------
   xx:xx:xx:xx  0014  BT     CA    myAP1              --   -69 00  133
   xx:xx:xx:xx  0014  BT     SI    myAP1              --   -69 00  133
```

5 GHz の特定の AP に関する 802.11a 干渉デバイス情報を表示するには、次のコマンドを使用します。

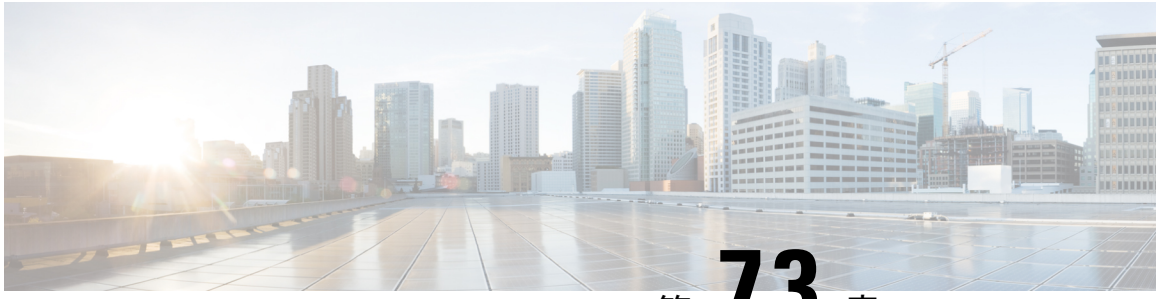
```
Device# show ap dot11 5ghz SI device type ap

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
AP type = CA, clean air, SI spectrum intelligence

No  ClusterID/BSSID    DevID  Type    AP Type AP Name                 ISI  RSSI  DC
Channel
--- ------------------ ------ ------- ------  ----------------------- ---- ----- ----
----------
```

2.4 GHz 帯域のすべての Cisco CleanAir 干渉源を表示するには、次のコマンドを使用します。

```
Device# show ap dot11 24ghz cleanair device type all
```

第 XII 部

メッシュ アクセス ポイント



第 73 章

メッシュ アクセス ポイント

メッシュの概要

Cisco IOS XE 17.6.1 リリースでは、Cisco 組み込みワイヤレスコントローラ（EWC）は Cisco Catalyst 9124AX シリーズの屋外アクセスポイントで実行され、メッシュ展開でルートアクセスポイント（RAP）として機能します。メッシュネットワーキングでは、Cisco Aironet の屋外メッシュアクセスポイントと Cisco 組み込みワイヤレスコントローラを組み合わせて、拡張性、集中管理、および展開間のモビリティが提供されます。Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルは、ネットワークへのメッシュ アクセス ポイントの接続を管理します。

メッシュネットワーク内のアクセスポイントは、次のいずれかの方法で動作します。

- ルート アクセス ポイント（RAP）
- メッシュ アクセス ポイント（MAP）

EWC は RAP で機能します。RAP はコントローラに有線接続され、MAP はコントローラにワイヤレス接続されます。メッシュ AP は、802.11a/n 無線バックホール経由のワイヤレス接続を使用して、親メッシュ AP および子メッシュ AP と通信します。MAP では Cisco Adaptive Wireless Path Protocol（AWPP）を使用して、他のメッシュ アクセス ポイントを介したコントローラへの最適なパスを決定します。メッシュアクセスポイントでは、CAPWAP ディスカバリを開始する前にすでにコントローラに接続されている親メッシュ AP との AWPP リンクが確立されます。

ワイヤレス メッシュは、有線ネットワークの 2 地点で終端します。1 つ目はルート アクセス ポイント（RAP）が有線ネットワークに接続される場所です。すべてのブリッジトラフィックがその場所で有線ネットワークに接続されます。2 つ目は CAPWAP コントローラが有線ネットワークに接続する場所です。ここでは、メッシュ ネットワークからの WLAN クライアント トラフィックが有線ネットワークに接続されます。CAPWAP からの WLAN クライアント トラ

フィックは、レイヤ 2 にトンネリングされます。一致する WLAN は、ワイヤレス コントローラが同じ場所に設置されている同じスイッチ VLAN で終端する必要があります。メッシュ上の各 WLAN のセキュリティとネットワークの設定は、ワイヤレス コントローラが接続されているネットワークのセキュリティ機能によって異なります。

メッシュ ネットワーク内のエンドツーエンドのセキュリティは、ワイヤレス メッシュ アクセス ポイントと Wi-Fi Protected Access 2（WPA2）クライアントの間で Advanced Encryption Standard（AES）の暗号化を採用することでサポートされています。メッシュアクセスポイント（MAP）ワイヤレス クライアントへの接続（MAP 同士や MAP とルート アクセス ポイントなど）では、WPA2 が適用されます。

新しい設定モデルでは、コントローラにデフォルトのメッシュプロファイルがあります。このプロファイルは、デフォルトの AP 接続プロファイルにマッピングされた後、デフォルトのサイトタグにマッピングされます。名前付きメッシュプロファイルを作成する場合は、これらのマッピングが行われていること、および該当する AP が対応するサイト タグに追加されていることを確認します。

（注） メッシュプロファイルのセキュリティモード、BGN、クライアントアクセス、および範囲の変更に関する設定を変更すると、メッシュ AP がリロードされます。EWC では、内部 AP をアクティブな EWC に自動的にリロードすることはできません。リロード後にスタンバイ EWC ノードが動作し始めてから、内部 AP を手動でリロードする必要があります。

スケール番号

Cisco Catalyst 9124 シリーズ屋外アクセスポイントは、100 の AP と 2000 のクライアントの規模をサポートします。

制約事項と制限

- メッシュ機能は、Cisco 組み込みワイヤレスコントローラの Cisco Catalyst 9124 シリーズアクセスポイントでのみサポートされています。
- EWC は、同じコントローラ内の親メッシュ AP 間の AP ローミングのみをサポートします。
- EWC メッシュトポロジでは、ワイヤレスネットワークを拡張するために MAP の子として展開する場合、すべての FlexConnect EWC 対応 AP を CAPWAP モードにする必要があります。AP が CAPWAP モードではない場合、コントローラが生成されます。

メッシュ展開

メッシュ展開は次のとおりです。

- [Wireless Bridging]：ワイヤレスブリッジングは、ポイントツーポイントまたはポイントツーマルチポイントにすることができます。ワイヤレスブリッジにより、ケーブルが利用できない場合にネットワークが無線で拡張されます。RAP と MAP 間の無線リンクは、パイプとして扱われます。このタイプの展開では、通常、RAP と 1 レベルの MAP を使用します。MAP の第 1 レベルの下に子 MAP はありません。SSID は展開されません。
  - [Point-to-Point Wireless Bridging]：ポイントツーポイントブリッジング シナリオでは、バックホール無線を使用してスイッチドネットワークの 2 つのセグメントをブリッジ接続することにより、Cisco Catalyst 9124 シリーズ メッシュ AP を使用してリモートネットワークを拡張できます。これは基本的には、1 つの MAP があり、WLAN クライアントがないワイヤレス メッシュ ネットワークです。ポイントツーマルチポイント ネットワークと同様に、イーサネット ブリッジングを有効にすることでクライアントアクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。
  - [Point-to-Multipoint]：ポイントツーマルチポイントブリッジング シナリオでは、ルートブリッジとして機能する RAP が、アソシエートされた有線 LAN を使用して複数の MAP を非ルートブリッジとして接続します。デフォルトでは、この機能はすべての MAP に対して無効になっています。イーサネット ブリッジングを使用する場合、各 MAP および RAP のコントローラでイーサネットブリッジングをイネーブルにする必要があります。
- [Mesh with Wi-Fi Clients]：Wi-Fi ネットワークを拡張するための、マルチレベル MAP とワイヤレスクライアントを使用したメッシュ展開。Cisco のワイヤレス屋外メッシュ ネットワークでは、複数のメッシュ アクセス ポイントによって、安全でスケーラブルな屋外ワイヤレス LAN を提供するネットワークが構成されます。

MAC 認証

MAP をコントローラに接続させるには、AP の MAC アドレスをコントローラに入力する必要があります。コントローラは、認証リストで使用可能な MAP からの CAPWAP 要求にのみ応答します。AP の背面に記載されている MAC アドレスを必ず使用してください。

イーサネット経由でコントローラに接続された MAP の MAC 認証は、CAPWAP 接続プロセス中に行われます。無線でコントローラに接続する MAP の場合、対応する AP が親 MAP との Adaptive Wireless Path Protocol（AWPP）リンクを保護しようとすると、MAC 認証が行われます。AWPP は、Cisco メッシュネットワークで使用されるプロトコルです。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、内部での MAC 認証と、外部 AAA サーバーを使用した認証をサポートしています。

MAC 認証の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** > **[AAA Advanced]** > **[Device Authentication]** を選択します。

ステップ 2 [Add] をクリックします。
[Quick Step: MAC Filtering] ウィンドウが表示されます。

ステップ 3 [Quick Step: MAC Filtering] ウィンドウで、次の手順を実行します。

a) [MAC Address] を入力します。MAC アドレスは、xx:xx:xx:xx:xx:xx、xx-xx-xx-xx-xx-xx、または xxxx.xxxx.xxxx のいずれかの形式で指定できます。
b) ドロップダウンリストから [Attribute List Name] を選択します。
c) ドロップダウンリストから [WLAN Profile Name] を選択します。
d) [Apply to Device] をクリックします。

ステップ 4 **[Configuration]** > **[Security]** > **[AAA]** > **[AAA Method List]** > **[Authorization]** を選択します。

ステップ 5 [Add] をクリックします。
[Quick Step: AAA Authorization] ウィンドウが表示されます。

ステップ 6 [Quick Step: AAA Authorization] ウィンドウで、次の手順を実行します。

a) [Method List Name] を入力します。
b) ドロップダウンリストから [Type] を選択します。
c) ドロップダウンリストから [Group Type] を選択します。
d) [Fallback to Local] チェックボックスをオンにします。
e) [Authenticated] チェックボックスをオンにします。
f) 必要なサーバーを [Available Server Groups] から [Assigned Server Groups] に移動します。
g) [Apply to Device] をクリックします。

ステップ 7 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 8 メッシュプロファイルをクリックします。
[Edit Mesh Profile] ウィンドウが表示されます。

ステップ 9 [Advanced] タブをクリックします。

ステップ 10 [Security] 設定の [Method] ドロップダウンリストから、[EAP] を選択します。

ステップ 11 ドロップダウンリストから [Authentication Method] を選択します。

ステップ 12 ドロップダウンリストから [Authorization Method] を選択します。

ステップ 13 [Update & Apply to Device] をクリックします。

MAC 認証の設定（CLI）

ブリッジ モード AP の MAC アドレスをコントローラに追加するには、次の手順に従います。

始める前に

- コントローラでは、ブリッジ モード AP の MAC フィルタリングがデフォルトで有効になっています。したがって、設定する必要があるのは MAC アドレスだけです。使用する MAC アドレスは、該当する AP の背面に記載されています。
- MAC 認証は内部での認証と、外部 AAA サーバーを使用した認証がサポートされます。

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	**username** *user-name* 例： `Device(config)# username username1`	ユーザー名がMACアドレスであるMACフィルタリングのユーザー名認証を設定します。
ステップ 3	**aaa authorization credential-download** *method-name* **local** 例： `Device(config)# aaa authorization credential-download list1 local`	ローカルログイン情報を使用するための認可方式リストを設定します。
ステップ 4	**aaa authorization credential-download** *method-name* **radius group** *server-group-name* 例： `Device(config)# aaa authorization credential-download auth1 radius group radius-server-1`	RADIUSサーバーグループを使用するための認可方式リストを設定します。
ステップ 5	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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 6	**method authorization** *method-name* 例： `Device(config-wireless-mesh-profile)# method authorization auth1`	メッシュAP認証の認証方式を設定します。

事前共有キーのプロビジョニング

メッシュ展開では、MAP がネットワークから移動して別のメッシュ ネットワークに接続することがあります。これは、両方のメッシュ展開がワイルドカードの MAC フィルタリングで AAA を使用して MAP のアソシエーションを許可する場合に発生します。MAP は EAP-FAST を使用する可能性があるので、この動作を制御することはできません。EAP セキュリティに AP の MAC アドレスとタイプの組み合わせが使用されて、制御設定を使用できないためです。デフォルトのパスフレーズを使用した事前共有キー（PSK）オプションには、セキュリティ リスクも存在します。

この問題は、MAP が移動車両（公共交通機関、フェリー、船など）で使用される場合に、2 つのサービス プロバイダのオーバーラップ導入環境で顕著に現れます。この場合、サービス プロバイダのメッシュ ネットワークに残る MAP に制限はなく、MAP がハイジャックされたり、別のサービス プロバイダのネットワークで使用されたりして、導入環境で本来のサービス プロバイダの対象顧客にサービスを提供できなくなる可能性があります。

PSK キープロビジョニング機能を使用すると、コントローラからプロビジョニング可能な PSK 機能が有効になります。これにより、メッシュ展開の制御が容易になり、デフォルトよりも MAP セキュリティが強化されます。この機能によってカスタム PSK が設定された MAP は、PSK キーを使用して RAP およびコントローラで認証を行います。

PSK プロビジョニングの設定（GUI）

PSK プロビジョニングを設定するには、次の手順に従います。

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** を選択します。

ステップ 2 [Global Config] タブをクリックします。

ステップ 3 [Security] の設定で、[PSK Provisioning] チェックボックスをオンにして、次の手順を実行します。

a) ドロップダウンリストの番号から [PSK Inuse Index] を選択します。

b) [Keys Configuration] の設定で、追加アイコン [+] をクリックしてキーを設定します。

c) ドロップダウンリストから [Key] を選択します。

d) 設定するキーの [Name] と [Description] を入力します。

e) [Password Type] として [UNENCRYPTED] または [AES Encrypted] を選択します。

f) [Apply] をクリックします。キーは、設定されたキーのリストに表示されます。

ステップ 4 [Default PSK] チェックボックスをオンにします。

ステップ 5 [Apply] をクリックします。

PSK プロビジョニングの設定（CLI）

PSK プロビジョニングが有効になっている場合、AP は最初にデフォルト PSK を使用して接続します。PSK プロビジョニング キーが設定された後は、新しく接続した AP に設定済みのキーがプッシュされます。

PSK を設定するには、以下の手順に従います。

始める前に

プロビジョニングされた PSK は、メッシュセキュリティとして PSK が設定されているすべての AP にプッシュされている必要があります。

（注）
- PSK は、コントローラおよび対応するメッシュ AP のリブート後も保存されます。
- コントローラは、合計 5 つの PSK と 1 つのデフォルト PSK を保持できます。
- メッシュ AP は、初期設定へのリセット時にのみプロビジョニング済み PSK を削除します。
- メッシュ AP は、最初のプロビジョニング済み PSK を受信した後はデフォルトの PSK を使用しません。

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	**wireless mesh security psk provisioning** 例： `Device(config)# wireless mesh security psk provisioning`	ワイヤレスのセキュリティ方式を PSK として設定します。 （注） プロビジョニングされた PSK は、メッシュ セキュリティ方式として PSK が設定されている AP にのみプッシュされます。
ステップ 3	**wireless mesh security psk provisioning key** *index* {**0** | **8**} *pre-shared-key description* 例： `Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key`	メッシュ AP の新しい PSK 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	**wireless mesh security psk provisioning default-psk** 例： `Device(config)# wireless mesh security psk provisioning default-psk`	デフォルトの PSK ベースの認証を有効にします。
ステップ 5	**wireless mesh security psk provisioning inuse** *index* 例： `Device(config)# wireless mesh security psk provisioning inuse 1`	アクティブに使用する PSK を指定します。 （注） PSK インデックスを指すグローバル設定で、使用中のキー インデックスを明示的に設定する必要があります。

EAP 認証

ローカル EAP は、ユーザーおよびワイヤレス クライアントのローカル認証をコントローラで可能にする認証方式です。バックエンドシステムが妨害されたり、外部認証サーバーがダウンした場合でも、ワイヤレス クライアントとの接続を維持する必要があるリモート オフィスでの使用を目的として設計されています。ローカル EAP を有効にすると、コントローラは認証サーバーおよびローカル ユーザー データベースとして機能するため、外部認証サーバーに依存する必要がなくなります。ローカル EAP は、ローカル ユーザー データベースまたは LDAP バックエンドデータベースからユーザーの資格情報を取得して、ユーザーを認証します。ローカル EAP では、コントローラとワイヤレス クライアント間の MAP 認証で、EAP-FAST 認証方式のみがサポートされます。

ローカル EAP はバックエンド データベースとして LDAP サーバーを使用し、コントローラとワイヤレス クライアント間の MAP 認証のユーザー ログイン情報を取得します。LDAP バックエンドデータベースを使用すると、コントローラで、特定のユーザーの資格情報（ユーザー名およびパスワード）を LDAP サーバーから検索できるようになります。これらの資格情報は、ユーザーの認証に使用されます。

（注） コントローラ上で RADIUS サーバーが設定されている場合、コントローラはまず RADIUS サーバーを使用してワイヤレス クライアントを認証しようとします。ローカル EAP は、RADIUS サーバーが見つからない、タイムアウトになっている、または設定されていない場合にのみ試行されます。

LSC による EAP 認証

ローカルで有効な証明書ベース（LSC ベース）の EAP 認証も MAP でサポートされています。この機能を使用するには、認証局の制御、生成された証明書のポリシー、有効期間、制限、および使用方法の定義、AP とコントローラでインストールされたこれらの証明書の取得を行うために、公開キー インフラストラクチャ（PKI）が必要です。

これらのユーザー生成証明書または LSC が AP とコントローラで使用可能になると、デバイスはこれらの LSC を使用して接続、認証、およびセッション キーの取得を開始できます。

LSC によって AP から既存の証明書が削除されることはありません。AP は LSC と製造元でインストールされる証明書（MIC）の両方を保持できます。ただし、AP が LSC でプロビジョニングされた後は、起動時に MIC 証明書が使用されなくなります。LSC から MIC に変更する場合は、該当する AP をリブートする必要があります。

次の目的で、コントローラは指定サーバーに対する EAP 認証を使用したメッシュ セキュリティもサポートしています。

- メッシュ子 AP の認証
- パケット暗号化のためのマスター セッション キー（MSK）の生成

ブリッジ グループ名

ブリッジ グループ名（BGN）は、親メッシュ AP への MAP のアソシエーションを制御します。BGN を使用して無線を論理的にグループ分けしておくと、同じチャネルにある 2 つのネットワークが相互に通信することを防止できます。この設定はまた、同一セクター（領域）のネットワーク内に複数の RAP がある場合にも便利です。BGN は最大 10 文字から成る文字列です。

NULL VALUE という BGN が製造時にデフォルトで割り当てられます。このグループ名は表示されませんが、これにより、ネットワーク固有の BGN を割り当てる前に MAP をネットワークに参加させることができます。

同一セクターのネットワーク内に（より大きなキャパシティを得るために）RAP が 2 つある場合は、別々のチャネルで 2 つの RAP に同じ BGN を設定することをお勧めします。

完全一致 BGN を MAP で有効にすると、一致する BGN 親を見つけるためにスキャンが 10 回行われます。10 回スキャンしても一致する BGN 親を見つけられない場合、AP は一致しない BGN に接続して 15 分間接続を維持します。15 分後に AP は再び 10 回スキャンを行い、このサイクルが繰り返されます。デフォルトの BGN の機能は完全一致 BGN が有効な場合も同じです。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、メッシュ プロファイルに BGN が設定されています。MAP がコントローラに参加するたびに、コントローラはメッシュ プロファイルに設定されている BGN を AP にプッシュします。

（注） EWC HA ペアでは、BGN 設定を変更するとスイッチオーバーが発生します。設定された BGN をメッシュプロファイルから削除すると、スイッチオーバーがトリガーされます。

優先される親（Preferred Parent）の選択

MAP の優先される親を使用すると、メッシュ環境で線形トポロジを適用できます。この機能を使用すると、Adaptive Wireless Path Protocol で定義された（AWPP 定義）親選択メカニズムをオーバーライドして、優先される親に MAP を強制的に移動できます。

Cisco Wave 1 AP の場合、優先される親を設定する際には、目的の親に対して実際のメッシュネイバーの MAC アドレスを指定してください。この MAC アドレスは base radio MAC アドレスで、最後の文字が「f」になります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:0f を指定する必要があります。

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f
```

Cisco Wave 2 AP の場合、優先される親を設定すると、MAC アドレスは、最後の 2 文字に「0x11」が追加された base radio MAC アドレスになります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:11 を指定する必要があります。

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11
```

ブリッジグループ名の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Advanced] タブの [Bridge Group] の設定で、[Bridge Group Name] を入力します。

ステップ 4 [Bridge Group] の設定で、[Strict Match] チェックボックスをオンにして機能を有効にします。完全一致 BGN を MAP で有効にすると、一致する BGN 親を見つけるためにスキャンが 10 回行われます。

ステップ 5 [Apply to Device] をクリックします。

ブリッジグループ名の設定（CLI）

- ブリッジグループ名（BGN）がメッシュプロファイルに設定されている場合、MAP がコントローラに接続するたびに、メッシュプロファイルに設定されている BGN が AP にプッシュされます。

- メッシュ AP が AireOS コントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに移動するたびに、メッシュ プロファイルに設定されている BGN がその AP にプッシュされて保存されます。

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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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	**bridge-group name** *bridge-grp-name* 例： `Device(config-wireless-mesh-profile)# bridge-group name bgn1`	ブリッジ グループ名を設定します。
ステップ 4	**bridge-group strict-match** 例： `Device(config-wireless-mesh-profile)# bridge-group strict-match`	ブリッジ グループの厳密な照合を設定します。

2.4 GHz および 5 GHz のメッシュバックホール

バックホールは、MAP 間でワイヤレス接続のみを作成するために使用されます。バックホール インターフェイスは 802.11a/n/ac/g です（AP によって異なります）。デフォルトのバックホール インターフェイスは 5 GHz です。利用可能な無線周波数スペクトラムを効果的に使用するには、レート選択が重要です。このレートは、クライアントデバイスのスループットにも影響を与える可能性があります（スループットはベンダーデバイスを評価するために業界出版物で使用される重要なメトリックです）。

メッシュ バックホールは、2.4 GHz および 5 GHz でサポートされています。ただし特定の国では、5 GHz のバックホール ネットワークでメッシュ ネットワークを使用することは許可されていません。2.4 GHz の無線周波数を使用すると、より大きなメッシュまたはブリッジ距離を実現できます。RAP はスロット変更設定を取得すると、すべての子 MAP に伝達します。すべての MAP は接続を解除し、新たに設定されたバックホール スロットに接続します。

メッシュバックホールの設定（CLI）

ここでは、2.4 GHz でメッシュバックホールを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap_name* **mesh backhaul radio dot11** *24ghz* 例： `Device # ap name test-ap mesh backhaul radio dot11 24ghz`	メッシュバックホールを2.4 GHzに変更します。

Dynamic Frequency Selection（動的周波数選択）

既存のレーダーサービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要があるデバイスに対して、動的周波数選択（DFS）プロトコルに従って動作することを求めています。DFSに準拠するために、無線デバイスがレーダー信号の存在を検出できることが義務付けられています。無線でレーダー信号が検出された場合、最低 30 分間は伝送を停止してそのサービスを保護する必要があります。その後、無線は別のチャネルを選択しますが、伝送する前にこのチャネルをモニターリングする必要があります。使用する予定のチャネルで 1 分間以上レーダーが検出されなかった場合は、新しい無線サービス デバイスがそのチャネルで伝送を開始できます。DFS 機能により、メッシュ AP はセクター内のいずれかのメッシュ AP でレーダーイベントが検出されたときに、ただちにチャネルを切り替えることができます。

動的周波数選択の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 [Add] をクリックします。
[Add Mesh Profile] ウィンドウが表示されます。

ステップ 3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。

ステップ 4 プロファイル名を入力します。

ステップ 5 [Full sector DFS status] チェックボックスをオンにして、動的周波数選択を有効にします。

ステップ 6 [Apply to Device] をクリックします。

動的周波数選択の設定（CLI）

DFSは、DFSチャネルでライセンスを必要としない操作の特定のタイマーとともに検出されるレーダー波形のタイプを指定します。

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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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	**full-sector-dfs** 例： `Device(config-wireless-mesh-profile)# full-sector-dfs`	DFS を有効にします。 （注） DFS 機能により、レーダー信号を検出したMAPはそれをRAPまで伝送することができ、RAP はレーダーを経験したことがあるかのように動作し、セクターを移動します。このプロセスは、コーディネイテッド チャネル変更と呼ばれます。Cisco Wave 2 以降のバージョンでは、コーディネイテッド チャネル変更が常に有効になっています。Cisco Wave 1 AP でのみ、コーディネイテッドチャネル変更を無効にできます。

国コード

コントローラおよびAPは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。AP 内の無線は、製造時に特定の規制ドメイン（ヨーロッパの場合にはEなど）に割り当てられていますが、国コードを使用すると、稼働する特定の国を指定できます（フランスの場合にはFR、スペインの場合にはESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

国によっては、屋内と屋外の AP に次のような違いがあります。

- 規制ドメイン コード
- サポートされるチャネル セット

• 送信電力レベル

侵入検知システム

Cisco 侵入検知システム/侵入防御システム（CIDS/CIPS）は、特定のクライアントに関わる攻撃がレイヤ 3 ～レイヤ 7 で検出されたとき、これらのクライアントによるワイヤレス ネットワークへのアクセスをブロックするよう、コントローラに指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーション不正使用などの脅威を検出、分類、阻止することで、強力なネットワーク保護を提供します。

侵入検知システムの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 [Add] をクリックします。
[Add Mesh Profile] ウィンドウが表示されます。

ステップ 3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。

ステップ 4 プロファイル名を入力します。

ステップ 5 [IDS (Rogue/Signature Detection)] チェックボックスをオンにして、侵入検知システムを有効にします。

ステップ 6 [Apply to Device] をクリックします。

侵入検知システムの設定（CLI）

侵入検知システムを有効にすると、クライアントアクセスのすべてのトラフィックに関するレポートが生成されます。ただし、バックホール トラフィックは対象になりません。

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 mesh** *profile-name* **例：** `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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。

	コマンドまたはアクション	目的
ステップ 3	**ids** 例： `Device(config-wireless-mesh-profile)# ids`	メッシュ AP の侵入検知システムレポートを設定します。

コントローラ間のメッシュ相互運用性

AireOS と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの間の相互運用性が維持され、次のサポートが提供されます。

- MAP は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続された AP によって形成されたメッシュ ネットワークを介して AireOS コントローラに接続できます。
- MAP は、AireOS コントローラに接続された AP によって形成されたメッシュ ネットワークを介して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続できます。
- AireOS に接続されている親メッシュ AP と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの間で、PMK キャッシュを使用した MAP ローミングがサポートされます。

（注） シームレスな相互運用性を実現するためには、AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが同じモビリティ グループに属し、IRCM をサポートするイメージ バージョンを使用する必要があります。

メッシュ コンバージェンス

メッシュ コンバージェンスにより、MAP は現在の親とのバックホール接続が失われた場合に、コントローラとの接続を再確立できます。コンバージェンス時間を短縮するために、各メッシュ AP はチャネルのサブセットを維持して将来のスキャン/シークに使用し、ネイバー リストのサブセットで親を識別します。

次のコンバージェンス方式がサポートされています。

表 *41 :* メッシュ コンバージェンス

メッシュ コンバージェンス	親の損失検出/キープアライブタイマー
規格	21 / 3 秒
速い	7 / 3 秒
Very Fast	4 / 2 秒

メッシュ コンバージェンス	親の損失検出/キープアライブタイマー
ノイズトレラント高速	21 / 3 秒

ノイズトレラント高速

ノイズトレラント高速検出は、現在の親を 21 秒ごとに標準方式で評価する AWPP ネイバー要求に対する応答を取得できないことが前提になります。親への要求とともに、各ネイバーに 3 秒ごとにユニキャスト要求が送信されます。親からの応答を取得できないときは、ローミング（ネイバーが同じチャネルで使用可能な場合）または新しい親のフル スキャンが開始されます。

メッシュ コンバージェンスの設定（CLI）

ここでは、メッシュコンバージェンスを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュプロファイルを作成します。
ステップ 3	**convergence {fast | noise-tolerant-fast | standard | very-fast}** 例： `Device(config-wireless-mesh-profile)# convergence fast`	メッシュプロファイルのメッシュコンバージェンス方式を設定します。

イーサネット ブリッジング

セキュリティ上の理由により、デフォルトではすべての MAP でイーサネット ポートが無効になっています。有効にするには、ルートおよび各 MAP でイーサネット ブリッジングを設定します。

タグ付きパケットとタグなしパケットの両方が、セカンダリ イーサネット インターフェイスでサポートされています。

ポイントツーポイント ブリッジング シナリオでは、バックホール無線を使用してスイッチド ネットワークの複数のセグメントをブリッジ接続することにより、Cisco Aironet 1500 シリーズ MAP を使用してリモートネットワークを拡張できます。これは基本的には、1 つの MAP があり、WLAN クライアントがないワイヤレス メッシュ ネットワークです。ポイントツーマルチポイント ネットワークと同様に、イーサネット ブリッジングを有効にすることでクライアント アクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。イーサネット ブリッジド アプリケーションを使用するには、RAP およびそのセクター内のすべての MAP でブリッジング機能を有効にする必要があります。

イーサネット ブリッジングは、次の場合に有効にする必要があります。

- メッシュ ノードをブリッジとして使用する。
- MAP でイーサネット ポートを使用してイーサネットデバイス（ビデオ カメラなど）を接続する。

（注） メッシュ AP からコントローラへのパスを取るすべての親メッシュ AP に対してイーサネット ブリッジングを有効にしてください。

イーサネットブリッジング用の VLAN がサポートされたメッシュ環境では、MAP 上のセカンダリ イーサネット インターフェイスにコントローラから VLAN を個別に割り当てます。すべてのバックホール ブリッジ リンク（有線とワイヤレスの両方）は、すべての VLAN が有効になっているトランク リンクです。非イーサネット ブリッジド トラフィック、およびタグなしイーサネット ブリッジド トラフィックは、メッシュ内の AP のネイティブ VLAN を使用してメッシュに沿って伝送されます。これは、AP がサービスを提供しているワイヤレス クライアントで送受信されるすべてのトラフィックで同様です。VLAN タグ付きパケットは、ワイヤレス バックホール リンクを介して AWPP でトンネリングされます。

MAP イーサネット クライアントの VLAN タギング

メッシュ AP のバックホール インターフェイスはプライマリ インターフェイスと呼ばれ、他のインターフェイスはセカンダリ インターフェイスと呼ばれます。

イーサネット VLAN タギングを使用すると、無線メッシュ ネットワーク内で特定のアプリケーション トラフィックをセグメント化して、有線 LAN に転送（ブリッジング）するか（アクセス モード）、別の無線メッシュ ネットワークにブリッジングすることができます（トランク モード）。

イーサネットブリッジングの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、メッシュプロファイルの [Name] を入力します。

ステップ 4 [Advanced] タブで、[VLAN Transparent] チェックボックスをオンにして、VLAN 透過性を有効にします。

ステップ 5 [Advanced] タブで、[Ethernet Bridging] チェックボックスをオンにします。

ステップ 6 [Apply to Device] をクリックします。

イーサネットブリッジングの設定（CLI）

MAPのイーサネットポートはデフォルトで無効になっています。有効にするには、ルートAPと他の各 MAP でイーサネット ブリッジングを設定する必要があります。

イーサネット ブリッジングは、次の場合に有効にできます。

- メッシュ ノードをブリッジとして使用する。
- MAPのイーサネットポートを使用してイーサネットデバイス（ビデオ カメラなど）を接続する。

始める前に

- イーサネット ブリッジングを有効にするには、メッシュ プロファイル設定で次のコマンドを設定してください。
  - ethernet-bridging：AP でイーサネットブリッジング機能を有効にします。
  - no ethernet-vlan-transparent：ワイヤレスメッシュブリッジ VLAN を認識させます。次の AP コマンドを使用して VLAN フィルタリングを許可します。**[no] mesh ethernet** {**0** | **1** | **2** | **3**} **mode trunk vlan allowed**

（注） すべての VLAN をブリッジする場合 （ブリッジが有線の一部として機能する場合）、VLAN透過性を有効にして、すべてのVLANが通過できるようにする必要があります。VLAN トランスペアレントモードを使用する場合は、ネットワークの有線側でVLANをフィルタリングして、不要なトラフィックによってネットワークがフラッディングしないようにすることをお勧めします。

- イーサネットブリッジングが機能するように、ルートAPが接続されているスイッチポートをトランク ポートとして設定する必要があります。
- ブリッジモード AP の場合は、**ap name** *name-of-rap* **mesh vlan-trunking native** *vlan-id* コマンドを使用して対応する RAP でトランク VLAN を設定します。イーサネット ブリッジング機能は、このコマンドが設定されていない AP では有効になりません。

- フレックス + ブリッジ AP の場合は、対応する flex プロファイルでネイティブ VLAN ID を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode access** *vlan-id* 例： `Device# ap name ap1 mesh ethernet 1 mode access 21`	AP のイーサネットポートを設定し、モードをトランクとして設定します。
ステップ 3	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan** *vlan-id* 例： `Device# ap name ap1 mesh ethernet 1 mode trunk vlan native 21`	ネイティブ VLAN をトランク ポート用に設定します。
ステップ 4	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan allowed** *vlan-id* 例： `Device# ap name ap1 mesh ethernet 1 mode trunk vlan allowed 21`	トランク ポートの許可 VLAN を設定します。 メッシュまたはルートアクセスポイントのイーサネットポートで VLAN フィルタリングを許可します。メッシュプロファイルで VLAN 透過性が無効になっている場合にのみアクティブです。

メッシュ デイジー チェーン接続

メッシュ AP には、MAP として機能する AP をデイジーチェーン接続する機能があります。デイジー チェーン接続された MAP では、AP をシリアル バックホールとして運用する（アップリンク アクセスとダウンリンク アクセスに別々のチャネルを使用できるためバックホール帯域幅が向上する）ことも、ユニバーサルアクセスを拡張することもできます。ユニバーサルアクセスの拡張により、ローカルモードまたは FlexConnect モードのメッシュ AP を MAP のイーサネットポートに接続できるため、ネットワークが拡張され、より良いクライアントアクセスを提供できます。

デイジー チェーン接続された AP は、AP の電源供給方法に応じて異なる方法でケーブル接続する必要があります。DC 電源を使用して AP に電力が供給されている場合は、プライマリ AP の LAN ポートから下位 AP の PoE 入力ポートにイーサネットケーブルを直接接続する必要があります。

デイジー チェーン接続モードに関するガイドラインは次のとおりです。

- プライマリ MAP は、メッシュ AP として設定する必要があります。
- 下位 MAP は、ルート AP として設定する必要があります。
- デイジーチェーン接続は、プライマリ MAP と下位 MAP の両方で有効にする必要があります。
- ブリッジ モードのすべての AP でイーサネット ブリッジングを有効にする必要があります。メッシュ プロファイルでイーサネット ブリッジングを有効にして、セクター内のすべてのブリッジ モード AP を同じメッシュ プロファイルにマッピングします。
- VLAN サポートは、ネイティブ VLAN を適切に設定して、有線ルート AP、下位 MAP、およびプライマリ MAP で有効にする必要があります。

メッシュ イーサネット デイジー チェーン接続の制約事項

- この機能は、Cisco Industrial Wireless 3702 AP にのみ適用されます。
- この機能は、ブリッジモードおよび Flex + ブリッジモードでのみ動作する AP に適用されます。
- Flex+ブリッジモードでは、ローカルスイッチング WLAN が有効になっている場合、ワークグループブリッジ（WGB）マルチ VLAN はサポートされません。
- イーサネット デイジー チェーン トポロジをサポートするには、Cisco Industrial Wireless 3702 PoE 出力ポートをポート内の他の Cisco Industrial Wireless 3702 PoE に接続しないで、パワーインジェクタを AP の電源として使用する必要があります。
- チェーン内の AP の数が増えると、ネットワーク コンバージェンス時間が長くなります。
- デイジーチェーンの一部であり、RAP ロールが割り当てられている EWC 対応 AP は、CAPWAP モード（ap-type capwap）である必要があります。

メッシュ イーサネット デイジー チェーン接続の前提条件

- AP ロールがルート AP として設定されていることを確認します。
- 対応する AP でイーサネットブリッジングと厳密な有線アップリンクが有効になっていることを確認します。
- VLAN 透過性が無効になっていることを確認します。
- ブリッジモード AP の各ルート AP における VLAN サポートを有効にするには、**ap name** *name-of-rap* **mesh vlan-trunking [native]** *vlan-id* コマンドを使用して対応する RAP でトランク VLAN を設定します。
- Flex + ブリッジ AP の各ルート AP における VLAN サポートを有効にするには、対応する Flex プロファイルでネイティブ VLAN ID を設定する必要があります。

- 1000 Mbps をサポートする 4 ペアケーブルを使用してください。この機能は、100 Mbps をサポートする 2 ペアケーブルでは正しく動作しません。

メッシュ イーサネット デイジー チェーン接続の設定（CLI）

ここでは、メッシュ AP でメッシュ イーサネット デイジー チェーン接続機能を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap profile default-ap-profile** 例： `Device(config)# ap profile default-ap-profile`	AP プロファイルを指定します。
ステップ 3	**ssid broadcast persistent** 例： `Device(config-ap-profile)# ssid broadcast persistent`	永続的 SSID ブロードキャストを設定し、厳密な有線アップリンクを確保します。このコマンドを設定すると、RAP はワイヤレスバックホールに切り替わりません。

メッシュ イーサネット ブリッジング ネットワーク経由のマルチキャスト

メッシュ マルチキャスト モードによって、ブリッジング対応 AP（MAP や RAP など）がメッシュ ネットワーク内のイーサネット LAN 間でマルチキャスト パケットを送信する方法が決まります。メッシュ マルチキャスト モードは非 CAPWAP マルチキャスト トラフィックのみを管理します。CAPWAP マルチキャスト トラフィックは異なるメカニズムで管理されます。

異なるメッシュ マルチキャスト モードを使用して、すべての MAP でマルチキャストおよびブロードキャストパケットを管理できます。イネーブルになっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

メッシュ マルチキャスト モードは次のとおりです。

- regular モード：マルチキャストの通常モードは、EWC 上の Cisco Catalyst 9124 シリーズ屋外アクセスポイントではサポートされていません。

- in-only モード：MAP がイーサネットから受信するマルチキャストパケットは、対応する RAP のイーサネットネットワークに転送されます。他の転送は行われないので、RAP が受信した非 CAPWAP マルチキャストはメッシュ ネットワーク内の MAP イーサネットネットワーク（発信元）に返送されず、MAP から MAP へのマルチキャストはフィルタで除去されるため発生しません。
- in-out モード：RAP と MAP は別々の方法でマルチキャストを実行します。
  - イーサネット経由で MAP が受信したマルチキャスト パケットは RAP に送信されますが、イーサネット経由で他の MAP に送信されることはありません。MAP から MAP へのパケットはマルチキャストからフィルタで除去されます。
  - マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要があります。

メッシュを介したマルチキャストモードの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 [Add] をクリックします。
[Add Mesh Profile] ウィンドウが表示されます。

ステップ 3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。

ステップ 4 プロファイル名を入力します。

ステップ 5 ドロップダウンリストから、次のいずれかの [Multicast Modes] を選択します。

a) [Regular]：このモードでは、データは、ブリッジ対応の RAP および MAP によってメッシュネットワーク全体とすべてのセグメントにマルチキャストされます。
b) [In]：このモードでは、MAP がイーサネットから受信するマルチキャストパケットは、対応する RAP のイーサネットネットワークに転送されます。
c) [In-Out]：このモードでは、RAP と MAP は別々の方法でマルチキャストを実行します。

ステップ 6 [Apply to Device] をクリックします。

メッシュを介したマルチキャストモードの設定

- マルチキャスト パケットがイーサネット経由で MAP で受信された場合は、RAP に送信されます。ただし、他の MAP には送信されません。MAP から MAP へのパケットは、マルチキャストからフィルタで除去されます。

- マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。
- in-out モードがデフォルトのモードです。in-out モードで動作中の場合、1 台の RAP によって送信されたマルチキャストを同じイーサネットセグメント上の別の RAP が受信してネットワークに戻さないよう、ネットワークを適切に分割する必要があります。

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 mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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	**multicast** {**in-only** | **in-out** | **regular**} 例： `Device(config-wireless-mesh-profile)# multicast regular`	メッシュ マルチキャスト モードを設定します。

メッシュでの無線リソース管理

Radio Resource Management（RRM）ソフトウェアはコントローラに組み込まれており、無線ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、コントローラは関連する Lightweight AP を継続的にモニターリングして、トラフィック負荷、干渉、ノイズ、カバレッジ、およびその他の隣接 AP に関する情報を取得できます。

メッシュ AP バックホールの RRM 測定は、次の条件に基づいて有効になります。

- メッシュ AP にルート AP ロールがある。
- ルート AP がイーサネット リンクを使用して接続している。
- ルート AP が子 AP にサービスを提供していない。

メッシュバックホールの RRM の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Global Config]** を選択します。

ステップ 2 [Backhaul] セクションで、[RRM] チェックボックスをオンにして、メッシュでの無線リソース管理を有効にします。

ステップ 3 [Apply] をクリックします。

メッシュバックホールの RRM の設定（CLI）

メッシュ AP バックホールの RRM 測定は、次の条件に基づいて有効になります。

- メッシュ AP にルート AP ロールがある。
- ルート AP がイーサネット リンクを使用して接続している。
- ルート AP が子 AP にサービスを提供していない。

（注） メッシュバックホールで RRM を有効にした場合、AP によって報告された RRM ノイズ情報は、イーサネットリンクを介して参加していて子 MAP が接続されていない RAP でのみ利用できます。

メッシュ バックホールで RRM 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 mesh backhaul rrm** 例： `Device(config)# wireless mesh backhaul rrm`	メッシュバックホールの RRM を設定します。

メッシュ リーフ ノード

リーフ ノードとしてのみ動作するパフォーマンスの低いMAPを設定できます。メッシュ ネットワークが形成および統合されると、リーフ ノードは子MAPとしてのみ動作でき、他のMAPが親MAPとして選択することはできなくなります。したがって、ワイヤレスバックホールパフォーマンスはダウングレードされません。

メッシュリーフノードの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ 2 [Access Point] をクリックします。
ステップ 3 [Mesh] タブで、[Block Child] チェックボックスをオンにします。
ステップ 4 [Update & Apply to Device] をクリックします。

メッシュリーフノードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name***mesh block-child** 例： `Device# #ap name ap1 mesh block-child`	リーフ ノードとしてのみ動作するように AP を設定します。他の MAP がこの AP を親 MAP として選択することはできません。 （注） 通常のAPに変更するには、このコマンドの**no**形式を使用します。

フレックス + ブリッジ モード

フレックス + ブリッジ モードは、メッシュ（ブリッジ モード）AP 上で FlexConnect の機能を有効にするために使用されます。メッシュ AP は接続先のルート AP から VLAN を継承します。

MAP に接続されている Flex モードの EWC 対応 AP は、CAPWAP モード（AP-type CAPWAP）である必要があります。

次のいずれかのモードの各 AP で、VLAN トランキングを有効または無効にしたり、ネイティブ VLAN ID を設定したりできます。

- FlexConnect
- Flex + ブリッジ（FlexConnect + メッシュ）

バックホール クライアント アクセス

バックホール クライアント アクセスが有効な場合は、無線バックホールを介したワイヤレス クライアント アソシエーションが許可されます。バックホール無線は 2.4 または 5 GHz 無線です。つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント関連付けはアクセス無線でのみ実行されます。

（注） バックホール クライアント アクセスはデフォルトで無効になっています。バックホール クライアント アクセスを有効にすると、デイジーチェーン接続展開の下位 AP と子 AP を除くすべての MAP が再起動します。

バックホール クライアント アクセスの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 プロファイルを選択します。

ステップ 3 [General] タブで、[Backhaul Client Access] チェックボックスをオンにします。

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

バックホール クライアント アクセスの設定（CLI）

（注） バックホール クライアント アクセスはデフォルトで無効になっています。有効にすると、デイジーチェーン接続展開の下位 AP と子 AP を除くすべての MAP が再起動します。

メッシュ プロファイルでバックホール クライアント アクセスを有効にするには、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 profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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	**client-access** 例： `Device(config-wireless-mesh-profile)# client-access`	クライアント アクセス AP を使用してバックホールを設定します。

アクセスポイントごとのメッシュバックホールでの Dot11ax レートの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] を選択します。
ネットワーク内のすべての設定済み AP が一覧表示される [All Access Points] セクションが、対応する詳細とともに表示されます。

ステップ 2 設定されたメッシュ AP をクリックします。
[Edit AP] ウィンドウが表示されます。

ステップ 3 [Mesh] タブを選択します。

ステップ 4 [General] セクションの [Backhaul] セクションに、デフォルトの [Backhaul Radio Type]、[Backhaul Slot ID]、および [Rate Types] フィールドの詳細が表示されます。[Backhaul Radio Type] と [Backhaul Slot ID] の値は、ルート AP に対してのみ変更できることに注意してください。

ステップ 5 [Rate Types] ドロップダウンリストから、バックホールレートタイプを選択します。

選択内容に基づいて、表示される対応するフィールドに詳細を入力します。バックホールインターフェイスは、AP によって、自動レートおよび 802.11a/b/g/n/ac/ax レートが異なります。Cisco Catalyst 9124AX 屋外アクセスポイントは、メッシュバックホールで 11ax バックホールレートをサポートする唯一の AP です。

ステップ 6 [Backhaul MCS Index] フィールドに、AP 間で送信できる変調符号化方式（MCS）レートを入力します。有効な範囲は、両方の帯域で 0 ～ 11 です。

ステップ 7 [Spatial Stream] フィールドに、サポートされている空間ストリームの数を入力します。5 GHz 無線帯域の 1 つの無線でサポートされる空間ストリームの最大数は 8 ですが、2.4 GHz 無線帯域では 4 つの空間ストリームがサポートされます。

ステップ 8 [Update and Apply to Device] をクリックします。

メッシュプロファイルのメッシュバックホールでの Dot11ax レートの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。

ステップ 2 [Add] をクリックします。
[Add Mesh Profile] ウィンドウが表示されます。

ステップ 3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。

ステップ 4 [Name] フィールドに、メッシュプロファイルの名前を入力します。

ステップ 5 [Advanced] タブをクリックします。

ステップ 6 [5 GHz Band Backhaul] セクションと [2.4 GHz Band Backhaul] セクションで、[Rate Types] ドロップダウンリストから [dot11ax] バックホールレートタイプを選択します。

（注） Cisco Catalyst 9124AXI/D シリーズ屋外アクセスポイントは、メッシュバックホールで 11ax バックホールレートをサポートする唯一の AP です。

ステップ 7 [Dot11ax MCS index] フィールドで、AP 間でデータを送信可能な MCS レートを指定します。値の範囲は、両方の無線帯域で 0 ～ 11 です。

ステップ 8 [Spatial Stream] フィールドに値を入力します。5 GHz 無線帯域の 1 つの無線でサポートされる空間ストリームの最大数は 8 ですが、2.4 GHz 無線帯域では 4 つの空間ストリームがサポートされます。

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

AP ごとのデータレートの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh backhaul rate dot11ax mcs** *<0-11>* **ss** *<1-8>* 例： `Device# ap name ap1 mesh backhaul rate dot11ax 5 ss 4`	2.4 GHz および 5 GHz 帯域のメッシュバックホール 11ax レートを設定します。

メッシュプロファイルを使用したデータレートの設定（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。
ステップ 2	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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	**backhaul rate dot11** {**24ghz** | **5ghz**} **dot11ax mcs** *<0-11>* **spatial-stream** *<1-8>*
	例：
	`Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11ax mcs 5 spatial-stream 6`
	`Device(config-wireless-mesh-profile)#`
		2.4 GHz 帯域および 5 GHz 帯域のバックホール転送速度を設定します。2.4 GHz 帯域の 802.11ax 空間ストリーム値は 1 ～ 4、5 GHz 帯域の空間ストリーム値は 1 ～ 8 です。

	コマンドまたはアクション	目的
	`backhaul rate dot11 24ghz dot11ax mcs 5 spatial-stream 4`	

ルート AP のバックホールスロットの指定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、メッシュプロファイルの [Name] を入力します。

ステップ 4 [Advanced] タブで、[5 GHz Band Backhaul] および [2.4 GHz Band Backhaul] の [Rate Types] ドロップダウンリストからレートタイプを選択します。

ステップ 5 [Apply to Device] をクリックします。

ルート AP のバックホールスロットの指定（CLI）

メッシュバックホールレートを設定するには、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	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *rap-name* **mesh backhaul radio dot11**{**24ghz** | **5ghz**} [**slot** *slot-id*] 例： `Device# ap name rap1 mesh backhaul radio dot11 24ghz slot 2`	メッシュバックホール無線スロットを設定します。

ワイヤレスバックホールのデータ レートの設定（CLI）

バックホールは、AP 間のワイヤレス接続を作成するために使用されます。AP に応じて 802.11bg/a/n/ac のバックホール インターフェイスを使用できます。レート選択によって、利用可能な RF スペクトラムを効果的に使用できます。データ レートは、RF カバレッジとネット

ワーク パフォーマンスにも影響を与えます。低データレート（6 Mbps など）のほうが、高データレート（1300 Mbps など）よりも AP からの距離を延長できます。結果として、データ レートはセル カバレッジ、および必要な AP の数に影響を与えます。

（注） バックホールデータレートは設定できます（可能な場合は、メッシュプロファイルを使用）。特定のデータレートが必要な場合は、コマンドを使用して AP ごとのデータレートを設定します。

特権 EXEC モードまたはメッシュ プロファイル コンフィギュレーション モードでワイヤレス バックホール データ レートを設定するには、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	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh backhaul rate** {**auto** | **dot11abg** | **dot11ac** |**dot11n**} 例： `Device# #ap name ap1 mesh backhaul rate auto`	バックホール転送速度を設定します。
ステップ 3	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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 4	**backhaul rate dot11** {**24ghz** | **5ghz**}**dot11n RATE_6M** 例： `Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n mcs 31`	バックホール転送速度を設定します。 （注） APに設定されたレート（ステップ2）は、メッシュプロファイルに設定されたレート（ステップ4）と一致する必要があることに注意してください。

メッシュバックホールでのリンクテストの使用（GUI）

手順

ステップ 1 **[Monitoring]** > **[Wireless]** > **[AP Statistics]** > **[General]** を選択します。

ステップ 2 [Access Point] をクリックします。

ステップ 3 **[Mesh]** > **[Neighbor]** > **[Linktest]** を選択します。

ステップ 4 [Date Rates]、[Packets to be sent (per second)]、[Packet Size (bytes)]、および [Test Duration (seconds)] ドロップダウンリストから目的の値を選択します。

ステップ 5 [Start] をクリックします。

メッシュ バックホールでのリンク テストの使用

ネイバーメッシュ AP 間のリンクテストをトリガーするには、次の手順に従います。

（注） AP からリンクテストを実行するには、**test mesh linktest mac-address** *neighbor-ap-mac* **rate** *data-rate* **fps** *frames-per-second* **frame-size** *frame-size* コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh linktest** *dest-ap-mac data-rate packet-per-sec packet-size test-duration* 例： `Device# #ap name ap1 mesh linktest F866.F267.7DFB 24 234 1200 200`	リンク テスト パラメータを設定します。

メッシュ CAC

コールアドミッション制御（CAC）を使用すると、メッシュアクセスポイントはコントローラで制御されている Quality of Service（QoS）を維持して、メッシュネットワークの音声品質を管理できます。帯域幅に基づく、静的な CAC を使用すると、クライアントで新しいコールを受信するために必要な帯域幅または共有メディア時間を指定することができます。各アクセスポイントは、使用可能な帯域幅を確認して特定のコールに対応できるかどうかを判断し、そのコールに必要な帯域幅と比較します。品質を許容できる最大可能コール数を維持するために十分な帯域幅が使用できない場合、メッシュ アクセス ポイントはコールを拒否します。

- クライアントが同じサイト内にある MAP 間でローミングすると、アクティブ コールの新しいツリーで帯域幅の可用性が再度チェックされます。
- MAP が新しい親にローミングしても、アクティブ コールが終了することはなく、サブ ツリー内の他のアクティブ コールで引き続きアクティブなままになります。
- MAP のハイ アベイラビリティ（HA）はサポートされていません。MAP のアクセス無線に接続されたコールは HA スイッチオーバー時に終了します。
- RAP の HA はサポートされているため、RAP のアクセス無線に接続されたコールは、スイッチオーバー後も新しいコントローラでアクティブのままになります。
- メッシュ CAC アルゴリズムは、音声コールにのみ適用されます。
- メッシュ バックホール無線帯域幅の計算では、スタティック CAC が適用されます。AP でメッシュ バックホールの負荷ベース CAC がサポートされていないため、負荷ベース CAC は使用されません。
- 無線で使用可能な帯域幅に基づいてコールが許可されます。コール アドミッションでは Air Time Fairness（ATF）が考慮されず、ATF ポリシーが適用されるコールには ATF ウェイトに従って帯域幅が割り当てられます。

メッシュ CAC は、次のシナリオではサポートされていません。

- メッシュ ツリー内の AP に異なるサイト タグが割り当てられている場合。
- メッシュ ツリー内の AP にデフォルトのサイト タグが割り当てられている場合。

メッシュ CAC 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 mesh cac** 例： `Device(config)# wireless mesh cac`	メッシュ CAC モードを有効にします。

アップリンクゲートウェイの到達可能性障害の高速検出によるメッシュネットワークの回復の高速化

すべての 802.11ac Wave 2 AP では、アップリンクゲートウェイの到達可能性障害を迅速に検出することにより、メッシュネットワークの回復メカニズムの速度が向上します。メッシュ AP のアップリンクゲートウェイの到達可能性は、IPv4 または IPv6 のデフォルトゲートウェイへの ICMP ping を使用してチェックされます。

メッシュ AP は、次の 2 つのシナリオで到達可能性チェックをトリガーします。

- 新しいアップリンクが選択された後、メッシュ AP がコントローラに接続するまで

  新しいアップリンクが選択された後、メッシュ AP には、選択したアップリンクを介して（静的 IP または DHCP 経由で）ゲートウェイに到達するための 45 秒の時間帯があります。45 秒経過してもメッシュ AP がゲートウェイに到達できない場合、現在のアップリンクはブロックリストにあるため、アップリンクの選択プロセスが再開されます。AP がこの 45 秒の時間帯内にコントローラに接続すると、到達可能性チェックは停止します。その後、通常動作中はゲートウェイの到達可能性チェックは実行されません。

- メッシュ AP がコントローラとの接続をタイムアウトした直後

  メッシュ AP がコントローラとの接続をタイムアウトし、AP が 5 秒以内にゲートウェイに到達できないと、現在のアップリンクがブロックリストにすぐに追加されて、アップリンクの選択プロセスが再開されます。

メッシュ展開の高速ティアダウン

メッシュ展開では、ルートアクセスポイントがワイヤレスマイクロ波リンクなどの信頼できないリンクを介してコントローラに接続することがあります。データアップリンクの障害が発生すると、クライアントは障害の原因を検出するために接続を失います。この機能を使用すると、メッシュ展開でルートアクセスポイントのアップリンク障害をより迅速に検出し、ルートアクセスポイントでアップリンク障害が発生した場合にメッシュネットワークの高速ティアダウンに対処できます。

（注） メッシュ AP の高速ティアダウンは、Cisco Industrial Wireless（IW）3702 アクセスポイントではサポートされていません。

ワイヤレス メッシュ プロファイルの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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	**fast-teardown** 例： `Device(config-wireless-profile-mesh)# fast-teardown`	メッシュネットワークの高速ティアダウンを有効にし、機能のパラメータを設定します。

AP プロファイルへのワイヤレスメッシュの関連付け（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。
ステップ 2	**ap profile** *ap-profile-name* 例： `Device(config)# ap profile default-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。
ステップ 3	**mesh-profile** *mesh-profile-name* 例： `Device(config-ap-profile)# mesh-profile test1`	APプロファイル コンフィギュレーション モードで、メッシュプロファイルを設定します。

メッシュ AP プロファイルの高速ティアダウンの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Add Mesh Profile] ウィンドウで [Advanced] をクリックします。

ステップ 4 セキュリティモード、認証方式、認可方式を選択します。

ステップ 5 必要に応じて、[Ethernet bridging] を有効にします。

ステップ 6 ブリッジグループ名を入力し、完全一致 BGN を有効にします。

ステップ 7 無線のバンドバックホール転送速度を選択します。

ステップ 8 [Fast Roaming] セクションで次のアクションを実行します。

- [Fast Teardown] チェックボックスをオンにして、メッシュ展開でルートアクセスポイントのアップリンク障害をより迅速に検出し、アップリンク障害が発生したときにメッシュネットワークの高速なティアダウンに対処します。
- [Number of Retries] フィールドに、ゲートウェイが到達不能と見なされるまで許可される再試行回数を入力します。有効な範囲は 1 ～ 10 です。
- [Interval value] フィールドに、再試行の値を入力します。有効な範囲は 1 ～ 10 秒です。
- [Latency Threshold] フィールドに、AP とコントローラ間のラウンドトリップ遅延のしきい値を入力します。有効な範囲は 1 ～ 500 ミリ秒です。
- [Latency Exceeded Threshold] フィールドに、指定した時間以内に少なくとも 1 つの ping が成功する必要がある遅延間隔を入力します。有効な範囲は 1 ～ 30 秒です。
- [Uplink Recovery Interval] フィールドに、子接続を受け入れるためにルートアクセスポイントのアップリンクが安定している必要がある時間を入力します。有効な範囲は 1 ～ 3600 秒です。

ステップ 9 [Apply to Device] をクリックします。

メッシュ AP プロファイルの高速ティアダウンの設定（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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュプロファイルを設定し、メッシュ 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	**fast-teardown** 例： `Device(config-wireless-mesh-profile)# fast-teardown`	メッシュネットワークの高速ティアダウンを有効にし、機能のパラメータを設定します。
ステップ 4	**enabled** 例： `Device(config-wireless-mesh-profile-fast-teardown)# enabled`	高速ティアダウン機能を有効にします。
ステップ 5	**interval** *duration* 例： `Device(config-wireless-mesh-profile-fast-teardown)# interval 5`	（任意）再試行間隔を設定します。有効な値の範囲は 1 ～ 10 秒です。
ステップ 6	**latency-exceeded-threshold** *duration* 例： `Device(config-wireless-mesh-profile-fast-teardown)# latency-exceeded-threshold 20`	（任意）しきい値の時間未満で少なくとも 1 つの ping が成功する必要がある遅延間隔を指定します。有効な値の範囲は 1 ～ 30 秒です。
ステップ 7	**latency-threshold** *threshold range* 例： `Device(config-wireless-mesh-profile-fast-teardown)# latency-threshold 20`	（任意）遅延しきい値を指定します。有効な値の範囲は 1 ～ 500 ミリ秒です。
ステップ 8	**retries** *retry limit* 例： `Device(config-wireless-mesh-profile-fast-teardown)# retries 1`	（任意）ゲートウェイが到達不能と見なされるまでの再試行回数を指定します。有効な値の範囲は 1 ～ 10 です。
ステップ 9	**uplink-recovery-intervals** *recovery interval* 例： `Device(config-wireless-mesh-profile-fast-teardown)# uplink-recovery-intervals 1`	（任意）子接続を受け入れるためにルートアクセスポイントのアップリンクが安定している必要がある時間を指定します。有効な値の範囲は 1 ～ 3600 秒です。

デフォルトのメッシュプロファイルによる高速ティアダウンの確認

default-mesh-profile による高速ティアダウンを確認するには、次のコマンドを使用します。

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name            default-mesh-profile
------------------------------------------------
Fast Teardown                          : ENABLED
Number of Retries                      : 4
Interval in sec                        : 1
Latency Threshold in msec              : 10
Latency Exceeded Threshold in sec      : 8
Uplink Recovery Interval in sec        : 60
```

サブセットチャネル同期の設定

コントローラ内のすべてのRAPで使用されるすべてのチャネルが、以降の検索とコンバージェンスのためにすべてのMAPに送信されます。コントローラは、各ブリッジグループ名（BGN）のサブセット チャネルのリストを保持します。また、サブセット チャネルのリストはモビリティ グループ内のすべてのコントローラで共有されます。

サブセットチャネルリストは、特定のBGNのRAPが動作しているチャネルのリストです。このリストは、コントローラ内およびコントローラ間のすべてのMAPに伝達されます。サブセットチャネルリストは、メッシュ APのより高速なコンバージェンスのためのリストです。コンバージェンス方式はメッシュプロファイルで選択できます。コンバージェンス方式が標準的な方式でない場合、サブセットチャネルリストがMAPにプッシュされます。

モビリティグループのサブセットチャネルの同期を設定するには、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 mesh subset-channel-sync mac** **例：** `Device(config)# wireless mesh subset-channel-sync`	モビリティ グループのサブセット チャネルの同期を設定します。

優先される親の選択（GUI）

手順

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

ステップ2 [Access Point] をクリックします。

ステップ3 [Mesh] タブで、[Preferred Parent MAC] を入力します。

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

優先される親の選択（CLI）

MAP の優先される親を設定するには、次の手順に従います。

このメカニズムを使用すると、AWPP で定義された親選択メカニズムをオーバーライドして、優先される親にメッシュ AP を強制的に移動できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh parent preferred** *mac-address* 例：	AP のメッシュ パラメータを設定し、メッシュで優先される親の MAC アドレスを設定します。

	コマンドまたはアクション	目的

	`Device# ap name ap1 mesh parent preferred 00:0d:ed:dd:25:8F`	（注） 優先される親の無線 MAC アドレスを使用してください。
		
		Cisco Wave 1 AP の場合、優先される親を設定する際には、目的の親に対して実際のメッシュネイバーの MAC アドレスを指定してください。この MAC アドレスは base radio MAC アドレスで、最後の文字が「f」になります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:0f を指定する必要があります。
		
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f`
		
		Cisco Wave 2 AP の場合、優先される親を設定すると、MAC アドレスは、最後の 2 文字に「0x11」が追加された base radio MAC アドレスになります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:11 を指定する必要があります。
		
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11`

AP のロールの変更（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ 2 [Access Point] をクリックします。
ステップ 3 [Mesh] タブで、[Role] ドロップダウンリストから [Root] または [Mesh] を選択します。
ステップ 4 [Update & Apply to Device] をクリックします。

ロールの変更がトリガーされると、AP が再起動します。

AP のロールの変更（CLI）

AP を MAP から RAP（またはその逆）に変更するには、次の手順に従います。

デフォルトでは、AP はメッシュ AP ロールでコントローラに参加します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **role** {**mesh-ap** | **root-ap**} 例： `Device# #ap name ap1 root-ap`	ブリッジモードの Cisco AP のロールを変更します。ロールの変更がトリガーされると、AP が再起動します。

メッシュ AP のバッテリ状態の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mesh]** > **[Profiles]** を選択します。
ステップ 2 プロファイルを選択します。
ステップ 3 [General] タブで、[Battery State for an AP] チェックボックスをオンにします。

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

メッシュ AP のバッテリ状態の設定

一部のシスコ屋外 AP には、バッテリ バックアップのオプションが付属しています。ビデオ監視カメラに電力を供給できる PoE 出力も用意されています。外部電源が使用できないとき、内部バッテリを一時的にバックアップ電源として使用できます。

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 mesh** *profile-name* **例：** `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ 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	**battery-state** **例：** `Device(config-wireless-mesh-profile)# battery-state`	AP のバッテリ状態を設定します。

組み込みワイヤレスコントローラでのメッシュ設定の確認

メッシュ設定の確認

次の **show** コマンドを使用して、メッシュ設定のさまざまな要素を確認します。

- **show wireless mesh stats** *ap-name*
- **show wireless mesh security-stats** {*all* | *ap-name*}
- **show wireless mesh queue-stats** {*all* | *ap-name*}
- **show wireless mesh per-stats summary** {*all* | *ap-name*}
- **show wireless mesh neighbor summary** {*all* | *ap-name*}
- **show wireless mesh neighbor detail** *ap-name*

- **show wireless mesh ap summary**
- **show wireless mesh ap tree**
- **show wireless mesh ap backhaul**
- **show wireless mesh config**
- **show wireless mesh convergence detail** *bridge-group-name*
- **show wireless mesh convergence subset-channels**
- **show wireless mesh neighbor**
- **show wireless profile mesh detailed** *mesh-profile-name*
- **show wireless stats mesh security**
- **show wireless stats mesh queue**
- **show wireless stats mesh packet error**
- **show wireless mesh ap summary**
- **show ap name** *ap-name* **mesh backhaul**
- **show ap name** *ap-name* **mesh neighbor detail**
- **show ap name** *ap-name* **mesh path**
- **show ap name** *ap-name* **mesh stats packet error**
- **show ap name** *ap-name* **mesh stats queue**
- **show ap name** *ap-name* **mesh stats security**
- **show ap name** *ap-name* **mesh stats**
- **show ap name** *ap-name* **mesh bhrate**
- **show ap name** *ap-name* **config ethernet**
- **show ap name** *ap-name* **cablemodem**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **gps location**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **mesh linktest data** *dest-mac*
- **show ap environment**
- **show ap gps location**

これらのコマンドの詳細については、『Cisco Catalyst 9800 Series Wireless Controller Command Reference』ドキュメントを参照してください。

MAC 認証

次の show コマンドを使用して、MAC 認証の設定を確認します。

```
Device# show run aaa
aaa authentication dot1x CENTRAL_LOCAL local
aaa authorization credential-download CENTRAL_AUTHOR local
username 002cc8de4f31 mac
username 00425a0a53b1 mac

ewlc_eft#sh wireless profile mesh detailed madhu-mesh-profile

Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abbc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
...
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

PSK プロビジョニング

次の show コマンドを使用して、PSK プロビジョニングの設定を確認します。

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Bridge Group Name

次の show コマンドを使用して、ブリッジグループ名の設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
```

```
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
Channel Change Notification     : DISABLED
Backhaul client access          : ENABLED
Ethernet Bridging               : ENABLED
Ethernet Vlan Transparent       : DISABLED
Full Sector DFS                 : ENABLED
IDS                             : ENABLED
Multicast Mode                  : In-Out
Range in feet                   : 12000
Security Mode                   : EAP
Convergence Method              : Fast
LSC only Authentication         : DISABLED
Battery State                   : ENABLED
Authorization Method            : CENTRAL_AUTHOR
Authentication Method           : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)      : auto
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

バックホール クライアント アクセス

次の show コマンドを使用して、バックホール クライアント アクセスの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
Channel Change Notification     : DISABLED
Backhaul client access          : ENABLED
Ethernet Bridging               : ENABLED
Ethernet Vlan Transparent       : DISABLED
...
Backhaul tx rate(802.11bg)      : auto
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

無線バックホールのデータ レート

次の show コマンドを使用して、ワイヤレスバックホールのデータレートの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
...
Authorization Method            : CENTRAL_AUTHOR
Authentication Method           : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)      : auto
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

Dynamic Frequency Selection（動的周波数選択）

次の show コマンドを使用して、動的周波数選択の設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

侵入検知システム

次のshowコマンドを使用して、ワイヤレスバックホールのデータレートの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

イーサネット ブリッジング

次の show コマンドを使用して、イーサネットブリッジングの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

メッシュを介したマルチキャスト

次の show コマンドを使用して、メッシュを介したマルチキャストの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

メッシュバックホールの RRM

次の show コマンドを使用して、メッシュバックホールの RRM の設定を確認します。

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

優先される親（Preferred Parent）の選択

次の show コマンドを使用して、優先される親の設定を確認します。

```
Device# show wireless mesh ap tree
=========================================================================
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=========================================================================

[Sector 1]
```

```
-----------
1542-RAP [0, 0, bgn-madhu, (165), 0000.0000.0000, 1%, 0]
   |-MAP-2700 [1, 67, bgn-madhu, (165), 7070.8b7a.6fb8, 0%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1

(*)  Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller
```

AP ロールの変更

次の show コマンドを使用して、AP ロールの変更の設定を確認します。

```
Device# show wireless mesh ap summary
AP Name                          AP Model BVI MAC        BGN        AP Role
-------                          -------- -------        ---        -------
1542-RAP                         1542D    002c.c8de.1338 bgn-abc  Root AP
MAP-2700                         2702I    500f.8095.01e4 bgn-abc  Mesh AP

Number of Bridge APs         :   2
Number of RAPs               :   1
Number of MAPs               :   1
Number of Flex+Bridge APs    :   0
Number of Flex+Bridge RAPs   :   0
Number of Flex+Bridge MAPs   :   0
```

メッシュ リーフ ノード

次の show コマンドを使用して、メッシュリーフノードの設定を確認します。

```
Device# show ap name MAP-2700 config general
Cisco AP Name   : MAP-2700
=================================================

Cisco AP Identifier                             : 7070.8bbc.d3e0
Country Code                                    : Multiple Countries : IN,US,IO,J4
Regulatory Domain Allowed by Country            : 802.11bg:-AEJPQU   802.11a:-ABDJNPQU
AP Country Code                                 : IN  - India
AP Regulatory Domain
  Slot 0                                        : -A
  Slot 1                                        : -D
MAC Address                                     : 500f.8095.01e4
...
AP Mode                                         : Bridge
Mesh profile name                               : abc-mesh-profile
AP Role                                         : Mesh AP
Backhaul radio type                             : 802.11a
Backhaul slot id                                : 1
Backhaul tx rate                                : auto
Ethernet Bridging                               : Enabled
Daisy Chaining                                  : Disabled
Strict Daisy Rap                                : Disabled
Bridge Group Name                               : bgn-abc
Strict-Matching BGN                             : Enabled
Preferred Parent Address                        : 7070.8b7a.6fb8
Block child state                               : Disabled
PSK Key Timestamp                               : Not Configured
...
FIPS status                                     : Disabled
WLANCC status                                   : Disabled
GAS rate limit Admin status                     : Disabled
```

```
WPA3 Capability                                 : Disabled
EWC-AP Capability                                : Disabled
AWIPS Capability                                : Disabled
Proxy Hostname                                  : Not Configured
Proxy Port                                      : Not Configured
Proxy NO_PROXY list                             : Not Configured
GRPC server status                              : Disabled
```

サブセットチャネルの同期

次の show コマンドを使用して、サブセットチャネルの同期の設定を確認します。

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

ブリッジモードおよびメッシュ AP 用の LSC のプロビジョニング

次の show コマンドを使用して、ブリッジモードおよびメッシュ AP 用の LSC のプロビジョニングに関する設定を確認します。

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                   : default mesh profile
Bridge Group Name             : bgn-abc
Strict match BGN              : DISABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : ENABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : DISABLED
Ethernet Vlan Transparent     : ENABLED
Full Sector DFS               : ENABLED
IDS                           : DISABLED
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
```

```
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : default
Authentication Method         : default
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : auto
```

ルート AP のバックホールスロットの指定

次の show コマンドを使用して、ルート AP のバックホールスロットの設定を確認します。

```
Device# show ap name 1542-RAP mesh backhaul
MAC Address : 380e.4d85.5e60
  Current Backhaul Slot: 1
  Radio Type: 0
  Radio Subband: All
  Mesh Radio Role: DOWNLINK
  Administrative State: Enabled
  Operation State: Up
  Current Tx Power Level:
  Current Channel: (165)
  Antenna Type: N/A
  Internal Antenna Gain (in .5 dBm units): 18
```

メッシュ バックホールでのリンク テストの使用

次の show コマンドを使用して、メッシュバックホールでのリンクテストの使用の設定を確認します。

```
Device# show ap name 1542-RAP mesh linktest data 7070.8bbc.d3ef
380e.4d85.5e60 ==> 7070.8bbc.d3ef

Started at : 05/11/2020 20:56:28
Status: In progress

Configuration:
==============
Data rate:  Mbps
Packets per sec: : 234
Packet Size: : 1200
Duration: : 200
```

メッシュ CAC

次の show コマンドを使用して、メッシュ CAC の設定を確認します。

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3
```

```
Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

メッシュコンバージェンスの確認

次に、使用されたメッシュコンバージェンス方式を表示する show wireless profile mesh detailed コマンドの出力例を示します。

```
Device# show wireless profile mesh detailed default-mesh-profile

Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                 : default mesh profile
Convergence Method          : Fast
```

次に、選択されたブリッジグループ名のサブセットチャネルを表示する show wireless mesh convergence subset-channels コマンドの出力例を示します。

```
Device# show wireless mesh convergence subset-channels

Bridge group name                Channel
-----------------------------------------
Default                          132
```

メッシュバックホールの確認

次に、2.4 GHz でのメッシュバックホールの詳細を表示する show ap name mesh backhaul コマンドの出力例を示します。

```
Device# show ap name test-ap mesh backhaul

MAC Address : xxxx.xxxx.xxxx
Current Backhaul Slot: 0
Radio Type: 0
Radio Subband: All
Mesh Radio Role: DOWNLINK
Administrative State: Enabled
Operation State: Up
Current Tx Power Level:
Current Channel: (11)
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 0
```

次に、メッシュバックホールの詳細を表示する show wireless mesh ap backhaul コマンドの出力例を示します。

```
Device# show wireless mesh ap backhaul

MAC Address : xxxx.xxxx.0x11
Current Backhaul Slot: 1
Radio Type: Main
Radio Subband: All
```

```
Mesh Radio Role: Downlink
Administrative State: Enabled
Operation State: Up
Current Tx Power Level: 6
Current Channel: (100)*
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 10
```

次に、無線 MAC アドレスおよび対応する AP 名を表示する **show ap summary** コマンドの出力例を示します。

```
Device# show ap summary
Number of APs: 1
AP Name    Slots  AP Model         Ethernet       MAC Radio MAC  Location         Country
 IP Address   State
-------------------------------------------------------------------------------------------------
AP-Cisco-1  2     AIR-APXXXXX-E-K9 xxxx.xxxx.xxd4 xxxx.xxxx.0x11 default location  DE
   10.11.70.170 Registered
```

メッシュ イーサネット デイジー チェーン接続の確認

- 次に、永続的 SSID が AP に設定されているかどうかを表示する show ap config general コマンドの出力例を示します。

```
Device# show ap 3702-RAP config general

Persistent SSID Broadcast                  Enabled/Disabled
```

- 次に、すべてのブリッジ RAP の永続的 SSID ブロードキャストステータスを表示する show wireless mesh persistent-ssid-broadcast summary コマンドの出力例を示します。

```
Device# show wireless mesh persistent-ssid-broadcast summary

 AP Name     AP Model BVI MAC        BGN        AP Role               Persistent
SSID state
-------     -------- -------        ---        -------
----------------------
3702-RAP     3702     5c71.0d07.db50 ap_name    Root AP               Enabled
1560-RAP    1562E    380e.4dbf.c6b0 ap_name    Root AP              Disabled
```

メッシュバックホールでの Dot11ax レートの確認

メッシュプロファイルのメッシュバックホールの 802.11ax レートを確認するには、次のコマンドを使用します。

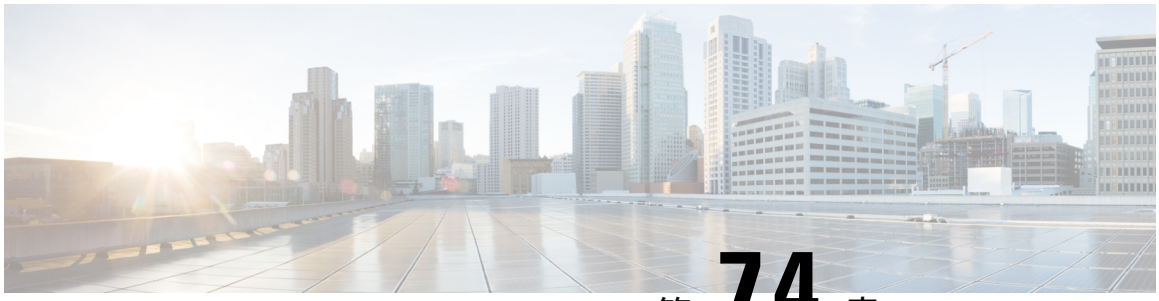
```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                   : default mesh profile
.
.
Backhaul tx rate(802.11bg)    : 802.11ax mcs7 ss1
Backhaul tx rate(802.11a)     : 802.11ax mcs9 ss2
```

AP の一般的な設定でメッシュバックホールの 802.11ax レートを確認するには、次のコマンドを使用します。

```
Device# show ap config general
Cisco AP Identifier             : 5c71.0d17.49e0
.
.
Backhaul slot id                : 1
Backhaul tx rate                : 802.11ax mcs7 ss1
```

第 XIII 部

WLAN



第 74 章

WLAN

WLAN について

この機能により、Lightweight アクセスポイントに対して WLAN を制御できます。各 WLAN には識別子である WLAN ID、プロファイル名、および WLAN SSID があります。アクセスポイントはすべて、最大 16 の WLAN をアドバタイズできます。ただし、最大 4096 の WLAN を作成し、作成した WLAN を（プロファイルとタグを使用して）別の AP に選択的にアドバタイズして、管理性を向上できます。

異なる SSID または同じ SSID で WLAN を設定できます。SSID は、コントローラがアクセスする必要がある特定の無線ネットワークを識別します。

バンドの選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、輻輳の少ない 5 GHz アクセスポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセスポイントからの同一チャネル干渉も受けます。これは、802.11b/g では、重複しないチャネルの数が 3 つに制限されているためです。このような干渉源を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、device で帯域選択を設定します。

オフチャネル スキャンの保留

通常の動作状態では、Lightweight アクセスポイントは定期的にオフチャネルになり、別のチャネルをスキャンします。これは、次のような RRM 動作を実行するためのものです。

- 他の AP を使用したネイバー探索プロトコル（NDP）パケットの送受信
- 不正 AP とクライアントの検出
- ノイズと干渉の測定

オフチャネル期間は通常は約 70 ミリ秒で、この期間は AP は対応するチャネル上でデータの送受信ができません。したがって、パフォーマンスに若干の影響が及び、一部のクライアント送信がドロップされることがあります。

AP が重要なデータを送受信している間はオフチャネルスキャンを保留するように設定して、APがオフチャネルにならず、通常動作に影響を与えないようにすることができます。オフチャネルスキャンの保留は、指定した時間しきい値（ミリ秒単位）でWMMUPクラス単位でWLANごとに設定できます。AP が指定されたしきい値内の所定の UP クラスでマークされたデータフレームを特定の WLAN 上で送受信している場合、その AP は次の RRM オフチャネル スキャンを保留します。たとえば、デフォルトでは、オフチャネルスキャンの保留は UP クラス 4、5、および 6 に対して 100 ミリ秒の時間しきい値で有効になります。したがって、RRM がオフチャネル スキャンを実行しようとしているときに直近の 100 ミリ秒内に UP 4、5、または 6 でマークされたデータ フレームを受信すると、RRM はオフチャネルになるのを保留します。音声サンプルを送受信している音声コールがアクティブな 20 ミリ秒ごとに UP 6 としてマークされる場合、AP 無線はオフチャネルになりません。

オフチャネル スキャンの保留ではトレードオフが生じます。オフチャネル スキャンは、設定やトラフィック パターンなどに応じて 2% 以上の影響をスループットに与える可能性があります。すべてのトラフィック クラスに対してオフチャネル スキャンの保留を有効にし、時間しきい値を引き上げると、スループットが若干改善する可能性があります。ただし、オフチャネルにならないようにすることによって、RRM は AP ネイバーや不正を識別できず、セキュリティ、DCA、TPC、および 802.11k メッセージに悪影響が及びます。

DTIM 周期

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

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

ただし、DTIM 値は 255 まで設定できます（255 回のビーコンごとにブロードキャストフレームおよびマルチキャストフレームを送信します）。推奨される DTIM 値は 1 と 2 のみです。DTIM の値を高くすると、通信の問題が発生する可能性があります。

（注） ビーコン期間は、deviceでミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位（TU）（1 TU＝1.024 ミリ秒）に、内部的に変換されます。AP モデルによっては、実際のビーコン期間はわずかに異なる場合があります。たとえば、100 ミリ秒のビーコン期間は、実際には 104.448 ミリ秒に相当します。

セッション タイムアウト

WLAN にセッション タイムアウトを設定できます。セッション タイムアウトとは、クライアント セッションが再認証を要求することなくアクティブである最大時間を指します。

WLAN がレイヤ 2 セキュリティ（WPA2-PSK など）を使用して設定されていて、レイヤ 3 認証も設定されている場合、WLAN セッションタイムアウト値は 802.1X 再認証タイムアウト値で上書きされます。APF 再認証タイムアウト値が 65535 より大きい場合、WLAN セッションタイムアウトはデフォルトで 65535 に設定されます。65535 以下の場合、設定済みの 802.1X 再認証タイムアウト値が WLAN セッションタイムアウトとして適用されます。

ここでは、次の内容について説明します。

Cisco Client Extensions

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

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

ピアツーピア ブロック

ピアツーピアブロッキングは個別のWLANに対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピア ツー ピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックがdevice内でローカルにブリッジされたり、deviceによってドロップされたり、またはアップストリーム VLAN に転送されるように選択することができます。

ピアツーピアブロッキングは、ローカルおよび中央スイッチングの WLAN にアソシエートされているクライアントに対してサポートされています。

（注） ピアツーピアブロッキング機能は VLAN ベースです。ピアツーピアブロッキング機能が有効になっている場合、同じ VLAN を使用する WLAN で影響が生じます。

診断チャネル

クライアントの WLAN による通信で問題が生じる理由についてトラブルシューティングする診断チャネルを選択できます。クライアントで発生している問題を識別し、ネットワーク上でクライアントを動作させるための修正措置を講じるために、クライアントとアクセスポイントをテストできます。診断チャネルを有効にするには、deviceの GUI または CLI を使用します。また、診断テストを実行するには、device **diag-channel**の CLI を使用します。

（注） 診断チャネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。CCX 診断機能は Cisco ADU カードを持つクライアントでのみテストされています。

WLAN の前提条件

- 最大 16 個の WLAN を各のポリシータグに特定のアクセスポイントを割り当てることができます。
- devicesが VLAN トラフィックを正常にルーティングできるように、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てることをお勧めします。

WLAN の制約事項

- WLAN で PSK と CCKM を設定しないでください。この設定はサポートされておらず、クライアントの接続フローに影響します。

- WPA1 設定で TKIP または AES 暗号が有効になっていることを確認してください。有効になっていない場合、アップグレードプロセス中に ISSU が壊れる可能性があります。
- WLAN のプロファイル名を変更すると、FlexConnect AP（AP 固有の VLAN マッピングを使用する）が WLAN 固有になります。FlexConnect グループが設定されている場合、VLAN マッピングはグループ固有になります。
- Flex ローカル認証が有効にされている WLAN では、Fast Transition 802.1X キー管理でクライアント関連付けがサポートされないため、IEEE 802.1X Fast Transition を有効にしないでください。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- FlexConnect では、特定の FlexConnect AP または一部の AP のみにピアツーピア ブロッキング設定を適用することはできません。SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- WLAN 名と SSID は 32 文字以内にする必要があります。
- WLAN および SSID 名では、次の ASCII 文字のみサポートされます。
  - 数字：48 から 57 の 16 進数（0 ～ 9）
  - アルファベット（大文字）：65 から 90 の 16 進数（A ～ Z）
  - アルファベット（小文字）：97 から 122 の 16 進数（a ～ z）
  - ASCII スペース：20 の 16 進数
  - 印刷可能な特殊文字：21 から 2F、3A から 40、および 5B から 60 の 16 進数。つまり、! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- WLAN 名はキーワードにはできません。たとえば、**wlan s** コマンドを入力して、「s」という名前で WLAN を作成しようとすると、「s」はシャットダウン用のキーワードとして使用されているため、すべての WLAN がシャットダウンします。
- WLAN を VLAN 0 にマッピングすることはできません。同様に、WLAN を VLAN 1002 ～ 1006にマッピングすることはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- Cisco 9800 コントローラで IPv4 と IPv6 が設定されているデュアルスタックでは、IPv4 トンネルが消去される前に AP が IPv6 トンネルを使用してコントローラに接続しようとすると、トレースバックが表示され、AP の接続は失敗します。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。
- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。

- 新しく設定された SSID が 5 GHz DFS チャネル上にある場合、ビーコンはすぐには開始されません。
- RADIUS サーバーの上書きは、WLAN ごとではなく、AAA サーバーグループごとに設定されます。
- ダウンロード可能な ACL（dACL）は、FlexConnect モードやローカルモードではサポートされていません。

⚠

注意 一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。この WLAN 機能を使用する際は注意してください。

WLAN の設定方法

WLAN の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** ページで、[Add] をクリックします。

[Add WLAN] ウィンドウが表示されます。

ステップ 2 [General] タブで、[Profile Name] フィールドに WLAN の名前を入力します。名前には、32 ～ 126 文字の ASCII 文字を使用できます（先頭と末尾のスペースはなし）。

ステップ 3 [Save & Apply to Device] をクリックします。

WLAN の作成（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。
ステップ 2	**wlan** *profile-name wlan-id* [*ssid*] 例：	WLAN の名前と ID を指定します。

	コマンドまたはアクション	目的
	デバイス(config)# **wlan mywlan 34 mywlan-ssid**	• *profile-name* に、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*に、WLAN ID を入力します。範囲は 1 ～ 512 です。 • *ssid* では、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。 （注） • SSID は、GUI または CLI を使用して作成できますが、CLI を使用して作成することをお勧めします。 • WLAN はデフォルトでディセーブルにされています。
ステップ 3	**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。

WLAN の削除（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** ページで、削除する WLAN の隣にあるチェックボックスをオンにします。

複数の WLAN を削除するには、複数の WLAN のチェックボックスをオンにします。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 確認ウィンドウで [Yes] をクリックして WLAN を削除します。

WLAN の削除

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	**no wlan** *wlan-name wlan-id ssid* 例： `デバイス(config)# no wlan test2`	WLAN を削除します。引数は次のとおりです。 • *wlan-name*は WLAN プロファイル名です。 • *wlan-id*は、WLAN ID です。 • *ssid* は WLAN に設定された WLAN SSID 名前です。
ステップ 3	**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。

WLAN の検索（CLI）

コントローラで設定されているすべての WLAN のリストを確認するには、次の show コマンドを使用します。

```
Device# show wlan summary
Number of WLANs: 4

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test1                            test1-ssid                     137  UP
3    test2                            test2-ssid                     136  UP
2    test3                            test3-ssid                     1    UP
45   test4                            test4-ssid                     1    DOWN
```

ワイルドカードを使用して WLAN を検索するには、次の `show` コマンドを使用します。

```
Device# show wlan summary | include test-wlan-ssid
1    test-wlan                       test-wlan-ssid                   137   UP
```

WLAN の有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 [WLANs] ページで、WLAN 名をクリックします。
ステップ 3 [Edit WLAN] ウィンドウで、[Status] ボタンを [ENABLED] に切り替えます。
ステップ 4 [Update & Apply to Device] をクリックします。

WLAN のイネーブル化（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。
ステップ 2	**wlan** *profile-name* 例： `Device(config)# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
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。

WLAN の無効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 [WLANs] ウィンドウで、WLAN 名をクリックします。
ステップ 3 [Edit WLAN] ウィンドウで、[Status] トグルボタンを [DISABLED] に設定します。

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

WLAN のディセーブル（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。
ステップ 2	**wlan** *profile-name* 例： `Device(config)# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

汎用 WLAN プロパティの設定（CLI）

次のパラメータを設定できます。

- メディア ストリーム
- ブロードキャスト SSID
- Radio

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** *profile-name* 例： `Device(config)# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**broadcast-ssid** 例： `Device(config-wlan)# broadcast-ssid`	この WLAN の SSID をブロードキャストします。
ステップ 5	**radio** {**dot11a** | **dot11ag** | **dot11bg** | **dot11g**} 例： `Device(config-wlan)# radio dot11g`	WLAN で無線をイネーブルにします。キーワードは次のとおりです。 • **dot1a**：802.11a の無線帯域だけに WLAN を設定します。 • **dot11g**：802.11ag の無線帯域でのみ WLAN を設定します。 • **dot11bg**：802.11b/g の無線帯域でのみ WLAN を設定します（802.11g が無効の場合、802.11b のみ）。 • **dot11ag**：802.11g の無線帯域だけに無線 LAN を設定します。
ステップ 6	**media-stream multicast-direct** 例： `Device(config-wlan)# media-stream multicast-direct`	この WLAN でマルチキャスト VLAN をイネーブルにします。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 8	**end** 例：	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
	`Device(config-wlan)# end`	

高度な WLAN プロパティの設定（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。
ステップ 2	**wlan** *profile-name* 例： `Device(config)# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**chd** 例： `Device(config-wlan)# chd`	この WLAN のカバレッジ ホールの検出をイネーブルにします。
ステップ 4	**ccx aironet-iesupport** 例： `Device(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet IE のサポートをイネーブルにします。
ステップ 5	**client association limit** {*clients-per-wlan* | **ap** *clients-per-ap-per-wlan* | **radio***clients-per-ap-radio--per-wlan*} 例： `Device(config-wlan)# client association limit ap 400`	WLAN で設定できるクライアント、AP あたりのクライアント、または AP 無線あたりのクライアントの最大数を設定します。
ステップ 6	**ip access-group web** *acl-name* 例： `Device(config-wlan)# ip access-group web test-acl-name`	IPv4 WLAN の Web ACL を設定します。可変 *acl* 名前はユーザー定義する IPv4 ACL の名前を指定します。
ステップ 7	**peer-blocking** ［**drop** | **forward-upstream**］ 例： `Device(config-wlan)# peer-blocking drop`	ピアツーピア ブロッキング パラメータを設定します。キーワードは次のとおりです。 • **drop**：ドロップ アクションのピアツーピア ブロッキングをイネーブルにします。

	コマンドまたはアクション	目的
		• forward-upstream：何もせず、パケットをアップストリームに転送します。
ステップ 8	**channel-scan** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} 例： `Device(config-wlan)# channel-scan defer-priority 6`	チャネルスキャンの延期プライオリティと延期時間を設定します。引数は次のとおりです。 • **defer-priority**：オフチャネルスキャンを延期できるパケットのプライオリティ マーキングを指定します。範囲は 0 ～ 7 です。デフォルト値は 3 です。 • **defer-time**：延期時間（ミリ秒単位）。範囲は 0 ～ 6000 です。デフォルトは 100 です。
ステップ 9	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。

高度な WLAN プロパティの設定（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 参加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]** > **[Wireless]** > **[WLANs]** > **[Wireless Networks]** の順に選択します。

ステップ 2 [Wireless Networks] ウィンドウで、[Add] をクリックします。

ステップ 3 [Advanced] タブで、[Coverage Hole Detection] チェックボックスをオンにします。

ステップ 4 [Aironet IE] チェック ボックスをオンにして、WLAN で Aironet IE を有効にします。

ステップ 5 [Diagnostic Channel] チェック ボックスをオンにして、WLAN で診断チャネルを有効にします。

ステップ 6 [P2P Blocking Action] ドロップダウンリストから、必要な値を選択します。

ステップ 7 [Multicast Buffer] トグルボタンを [enabled] または [diabled] に設定します。

ステップ 8 [Media Stream Multicast-Direct] 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 9 [Max Client Connections] セクションで、次についてクライアント接続の最大数を指定します。

- [Per WLAN] フィールドに、値を入力します。有効な範囲は 1 ～ 10000 です。
- [Per AP Per WLAN] フィールドに、値を入力します。有効な範囲は、0 ～ 400 です。
- [Per AP Radio Per WLAN] フィールドに、値を入力します。有効な範囲は、0 ～ 200 です。

ステップ 10 [11v BSS Transition Support] セクションで、次の設定タスクを実行します。

a) [BSS Transition] チェック ボックスをオンにして、802.11v BSS 移行サポートを有効にします。

b) [Disassociation Imminent] フィールドに、値を入力します。有効な範囲は、0 ～ 3000 です。

c) [Optimized Roaming Disassociation Timer] フィールドに、値を入力します。有効な範囲は、0 ～ 40 です。

d) チェック ボックスをオンにして以下の項目を有効にします。

- BSS Max Idle Service
- BSS Max Idle Protected
- Disassociation Imminent Service
- Directed Multicast Service
- Universal Admin
- Load Balance
- 帯域選択
- IP ソース ガード

ステップ 11 [WMM Policy] ドロップダウンリストから、ポリシーとして [Allowed] 、[Disabled]、または [Required] を選択します。デフォルトでは、WMM ポリシーが許可されています。

ステップ 12 [Off Channel Scanning Defer] セクションで、適切な [Defer Priority] 値を選択し、必要な [Scan Defer Time] の値をミリ秒単位で指定します。

ステップ 13 [Assisted Roaming (11k)] 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。

- Prediction Optimization
- ネイバー リスト
- Dual-Band Neighbor List

ステップ 14 [DTIM Period (in beacon intervals)] セクションで、802.11a/n 無線と 802.11b/g/n 無線の値を指定します。有効な範囲は 1 ～ 255 です。

ステップ 15 **[Save & Apply to Device] をクリックします。**

WLAN プロパティの確認（CLI）

WLAN ID に基づいて WLAN プロパティを確認するには、次の show コマンドを使用します。

```
Device# show wlan id wlan-id
```

WLAN 名に基づいて WLAN プロパティを確認するには、次の show コマンドを使用します。

```
Device# show wlan name wlan-name
```

設定されているすべての WLAN の WLAN プロパティを確認するには、次の show コマンドを使用します。

```
Device# show wlan all
```

すべての WLAN のサマリーを表示するには、次の show コマンドを使用します。

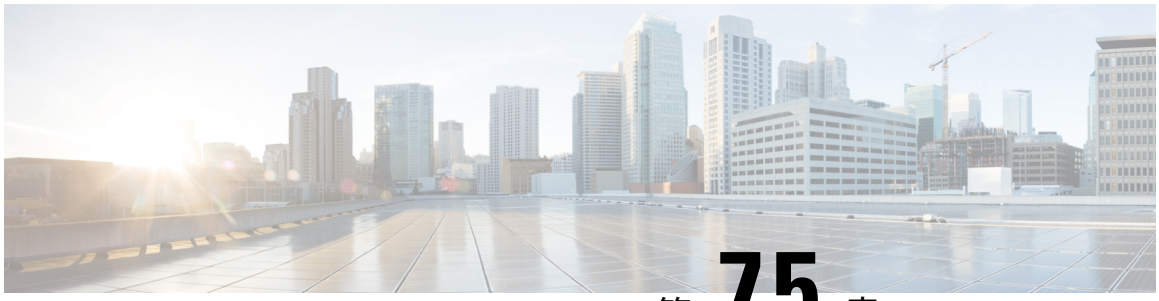
```
Device# show wlan summary
```

WLAN 名に基づいて WLAN の実行中コンフィギュレーションを確認するには、次の show コマンドを使用します。

```
Device# show running-config wlan wlan-name
```

すべての WLAN の実行中コンフィギュレーションを確認するには、次の show コマンドを使用します。

```
Device# show running-config wlan
```



第 75 章

ネットワーク アクセス サーバー識別子

ネットワーク アクセス サーバー識別子について

ネットワーク アクセス サーバー識別子（NAS-ID）は、送信元に RADIUS アクセス要求を通知するために使用されます。これにより、RADIUS サーバーはその要求のポリシーを選択できます。各 WLAN プロファイル、または VLAN インターフェイスで 1 つ設定できます。NAS-ID は、ユーザーをさまざまなグループに分類する認証要求を使用して組み込みワイヤレスコントローラによって RADIUS サーバーに送信されます。これにより、RADIUS サーバーはカスタマイズした認証応答を送信できるようになります。

（注） acct-session-id は、ポリシープロファイルでアカウンティングが有効になっている場合にのみ、RADIUS アクセス要求とともに送信されます。

同様に、WLAN プロファイルに対して NAS-ID を設定すると、VLAN インターフェイスに対して設定されている NAS-ID がオーバーライドされます。

Cisco IOS XE Cupertino 17.7.1 以降、custom-string（カスタム文字列）という新しい文字列が追加されています。

NAS ID には、次のオプションを設定できます。

- sys-name（システム名）
- sys-ip（システム IP アドレス）
- sys-mac（システム MAC アドレス）

- ap-ip（AP の IP アドレス）
- ap-name（AP の名前）
- ap-mac（AP の MAC アドレス）
- ap-eth-mac（AP のイーサネット MAC アドレス）
- ap-policy-tag（AP のポリシー タグ名）
- ap-site-tag（AP のサイト タグ名）
- ssid（SSID 名）
- ap-location（AP の場所）
- custom-string（カスタム文字列）

NAS ID ポリシーの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless AAA Policy]** の順に選択します。

ステップ 2 [Wireless AAA Policy] ページで、[Policy] の名前をクリックするか、[Add] をクリックして新しいポリシーを作成します。

ステップ 3 表示される [Add/Edit Wireless AAA Policy] ウィンドウで、[Policy Name] フィールドにポリシーの名前を入力します。

ステップ 4 [Option 1] ドロップダウンリストから、いずれかの NAS ID オプションを選択します。

ステップ 5 [Option 2] ドロップダウンリストから、いずれかの NAS ID オプションを選択します。

ステップ 6 [Option 3] ドロップダウンリストから、いずれかの NAS ID オプションを選択します。

ステップ 7 設定を保存します。

NAS ID ポリシーの作成

NAS ID ポリシーを作成するには、次の手順に従います。

始める前に

- NAS ID には、複数の NAS ID オプションの組み合わせ（3 個まで）を使用できます。
- NAS ID 属性の最大長は 253 です。新しい属性を追加する前に属性バッファがチェックされ、十分なスペースがない場合は新しい属性が無視されます。

- デフォルトでは、ワイヤレス AAA ポリシー（default-aaa-policy）がデフォルト設定（sys-name）で作成されます。このポリシーをさまざまな NAS ID オプションを使用して更新できます。ただし、default-aaa-policy を削除することはできません。
- NAS ID が設定されていない場合、デフォルトの sys-name が、組み込みワイヤレスコントローラから送信されるすべてのワイヤレス固有 RADIUS パケット（認証およびアカウンティング）の NAS ID と見なされます。
- Cisco IOS XE Cupertino 17.7.1 以降、RADIUS パケットの NAS ID として、option1、option2、および option3（**nas-id option3 custom-string** *custom-string*）のさまざまな組み合わせでカスタム文字列を設定できます。

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 aaa policy** *policy-name* 例： `Device(config)# wireless aaa policy test`	新しい AAA ポリシーを設定します。
ステップ 3	**nas-id option1 sys-name** 例： `Device(config-aaa-policy)# nas-id option1 sys-name`	option1 の NAS ID を設定します。
ステップ 4	**nas-id option2 sys-ip** 例： `Device(config-aaa-policy)# nas-id option2 sys-ip`	option2 の NAS ID を設定します。
ステップ 5	**nas-id option3 sys-mac** 例： `Device(config-aaa-policy)# nas-id option3 sys-mac`	option3 の NAS ID を設定します。

タグへのポリシーの付加（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] ページを選択し、[Policy] タブをクリックします。

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 プロファイルとポリシー プロファイルをマッピングします。

ステップ 5 適切な [Policy Profile] を使用してマッピングする [WLAN Profile] 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。

タグへのポリシーの適用（CLI）

NAS ID ポリシーをタグに適用するには、次の手順に従います。

手順

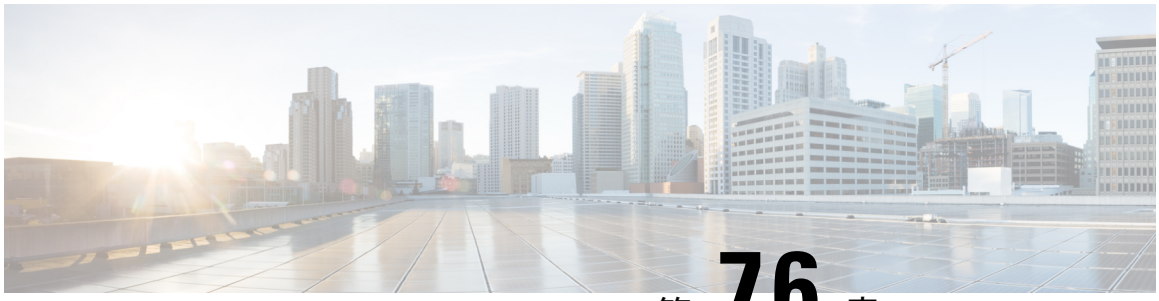
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy test1`	WLAN ポリシー プロファイルを設定します。
ステップ 3	**aaa-policy** *aaa-policy-name* 例： `Device(config-wireless-policy)# aaa-policy policy-aaa`	AAA ポリシー プロファイルを設定します。
ステップ 4	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**wireless tag policy** *policy-tag* 例：	ワイヤレス 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
	`Device(config)# wireless tag policy policy-tag1`	
ステップ 6	**wlan wlan1 policy** *policy-name* 例： `Device(config)# wlan wlan1 policy test1`	WLAN プロファイルをポリシー プロファイルにマッピングします。 （注） **ap-tag** オプションを使用してAP グループにNAS-ID を設定することもできます。この場合、WLAN プロファイルまたは VLAN インターフェイスに対して設定されている NAS ID がオーバーライドされます。

NAS ID 設定の確認

NAS ID 設定を確認するには、次の **show** コマンドを使用します。

```
Device# show wireless profile policy detailed test1

Policy Profile Name           : test1
Description                   :
Status                        : ENABLED
VLAN                          : 1
Client count                  : 0

:
:
AAA Policy Params
  AAA Override                : DISABLED
  NAC                         : DISABLED
  AAA Policy name             : test
```



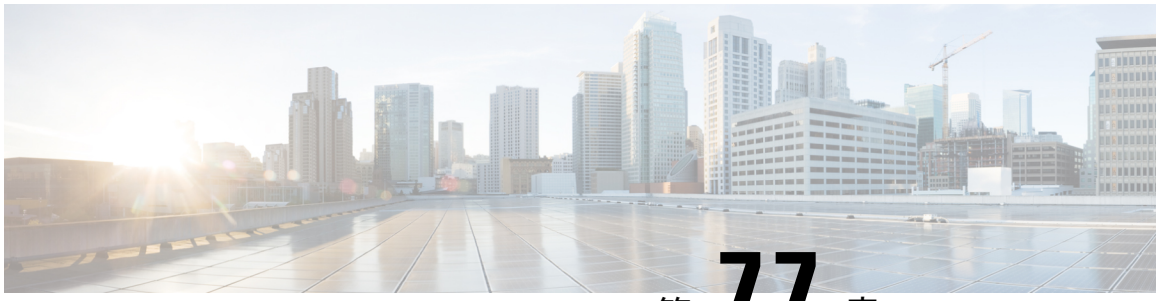
第 76 章

WLAN の DHCP

WLAN の DHCP

ワイヤレスクライアントによって送信された DHCP パケットは、AP によるブロードキャストとしてそれぞれの VLAN でリリースされます。これは、その VLAN のネットワークゲートウェイが要求を DHCP サーバーに転送することに基づいています。

（注） 内部 DHCP サーバーは EWC ではサポートされません。



第 77 章

WLAN セキュリティ

AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

レイヤ 2 セキュリティの前提条件

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。使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし（オープン WLAN）
- WPA+WPA2

（注）
- 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access（WPA）/Temporal Key Integrity Protocol（TKIP）で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。
- TKIP サポートが設定された WLAN は RM3000AC モジュールでは有効になりません。

- スタティック WEP（Wave 2 AP ではサポートされません）

WLAN セキュリティの設定方法

静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI）

始める前に

管理者特権が必要です。

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	**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。

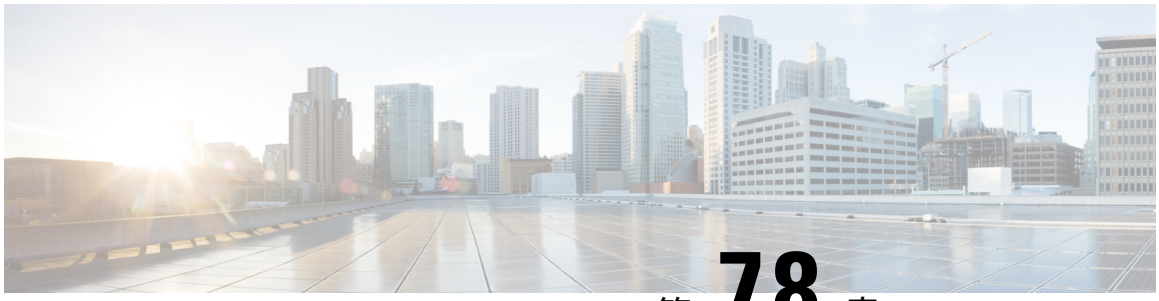
WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI）

始める前に

管理者特権が必要です。

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	**security wpa** 例： `デバイス(config-wlan)# security wpa`	
ステップ 3	**security wpa wpa1** 例： `デバイス(config-wlan)# security wpa wpa1`	を有効にします。
ステップ 4	**security wpa wpa1 ciphers**［**aes** | **tkip**］ 例： `デバイス(config-wlan)# security wpa wpa1 ciphers aes`	WPA1 暗号を指定します。次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指定します。 • **tkip**：WPA/TKIP のサポートを指定します。
ステップ 5	**security wpa wpa2** 例： `デバイス(config-wlan)# security wpa wpa2`	WPA2 を有効にします。
ステップ 6	**security wpa wpa2 ciphers aes** 例： `デバイス(config-wlan)# security wpa wpa2` 例：	WPA2 暗号化を設定します。



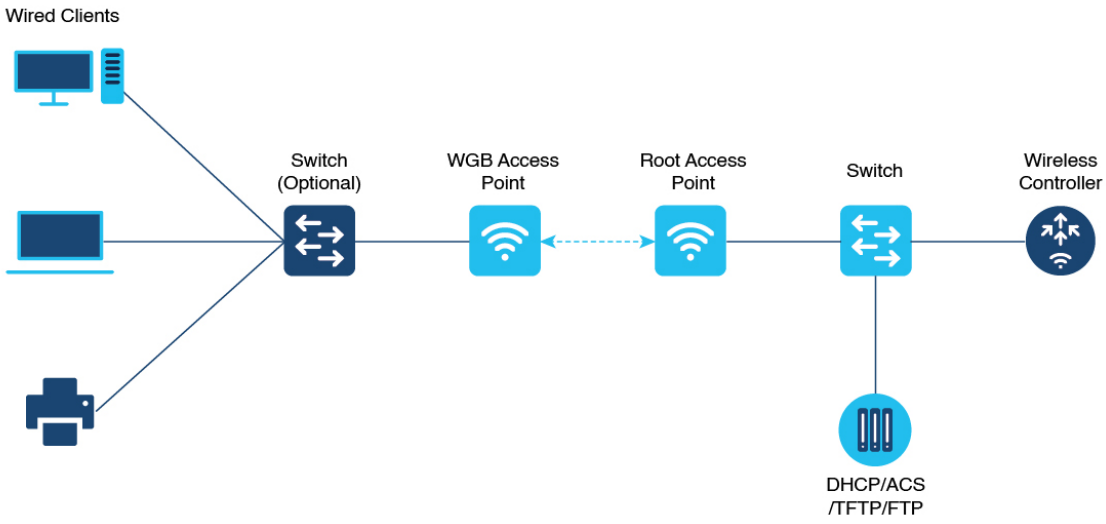
第 78 章

ワークグループ ブリッジ

Cisco ワークグループ ブリッジ

アクセスポイント（AP）モードのワークグループブリッジ（WGB）は、イーサネットポートで WGB AP に接続される有線クライアントへのワイヤレス接続を提供します。WGB はイーサネットインターフェイス上の有線クライアントの MAC アドレスを学習し、Internet Access Point Protocol（IAPP）メッセージングを使用してインフラストラクチャ AP 経由で WLC に報告することで、1 つのワイヤレスセグメントを介して有線ネットワークに接続します。WGB はルート AP への単一のワイヤレス接続を確立し、ルート AP は WGB をワイヤレスクライアントとして扱います。

図 *26 : WGB* の例



組み込みワイヤレスコントローラ の WGB でサポートされるモードは次のとおりです。

• Flex モード：中央認証とローカルスイッチング。

（注） 中央認証は Wave 1 および Wave 2 AP でサポートされていますが、ローカルスイッチングは Wave 2 AP でのみサポートされています。

次の機能は WGB での使用をサポートされています。

表 *42 : WGB* 機能マトリックス

機能	Cisco Wave 1 AP	Cisco Wave 2
802.11r	サポート対象	サポート対象
QOS	サポート対象	サポート対象
UWGB モード	サポートあり	Wave 2 AP ではサポート対象
IGMP スヌーピングまたはマルチキャスト	サポート対象	サポート対象
802.11W	サポート対象	サポート対象
PI サポート（SNMP なし）	サポート対象	サポート対象外
IPv6	サポート対象	サポート対象
VLAN	サポート対象	サポート対象
802.11i（WPAv2）	サポート対象	サポート対象
ブロードキャストのタグ付け/複製	サポート対象	サポート対象
ユニファイド VLAN クライアント	暗黙的にサポート（CLI は不要）	サポートあり
WGB クライアント	サポート対象	サポート対象
802.1x：PEAP、EAP-FAST、EAP-TLS	サポート対象	サポート対象
NTP	サポート対象	サポート対象
すべての LAN ポートで有線クライアントをサポート	Wired-0 および Wired-1 インターフェイスでサポート	すべての Wired-0、1 および LAN ポート 1、2、3 でサポート

表 *43 :* サポートされるアクセスポイントと要件

アクセスポイント	要件
Cisco Aironet 2700、3700、1572 シリーズ	自律イメージが必要
Cisco Aironet 1800、2800、3800、4800、1562、および Cisco Catalyst 9105、9115、9120、IW6300、ESW6300 シリーズ	Cisco AireOS 8.8 リリース以降の CAPWAP イメージ

表 *44 : AP* での *WGB* サポート

WGB の WLAN サポート	**Cisco Wave 1 AP**	**Cisco Wave 2 AP**
[Central Authentication]	サポート対象	サポート対象
ローカル スイッチング	未サポート	サポート対象

- MAC フィルタリングは、有線クライアントではサポートされていません。
- アイドル タイムアウトは、WGB と有線のどちらのクライアントでもサポートされません。
- セッション タイムアウトは、有線クライアントには適用されません。
- Web 認証はサポートされていません。
- WGB は最大 20 のクライアントのみをサポートします。
- 証明書のチェーンを使用する場合は、すべての CA 証明書をファイルにコピーし、WGB のトラストポイントにインストールします。そうしないと、サーバー証明書の検証が失敗する可能性があります。
- WGB に接続している有線クライアントは、セキュリティについて認証されません。代わりに WGB が、アソシエートしているアクセス ポイントに対して認証されます。そのため、WGB の有線側を物理的に保護することをお勧めします。
- WGB に接続された有線クライアントは、WGB の QoS および AAA オーバーライド属性を継承します。
- WGB がルート AP と通信できるようにするには、WLAN を作成し、[Advanced] 設定で Aironet IE が有効になっていることを確認します。

WLAN でのワークグループ ブリッジの設定

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	**wlan** *profile-name* 例： `Device(config)# wlan wlan-profile`	WLAN コンフィギュレーション サブモードを開始します。wlan-profile は設定されている WLAN のプロファイル名です。
ステップ 3	**ccx aironet-iesupport** 例： `Device(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet IE のサポートをイネーブルにします。
ステップ 4	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	WLAN を再起動します。

ワークグループブリッジのステータスの確認

- WGB の数を表示するには、次のコマンドを使用します。

  show wireless wgb summary

  次に、出力例を示します。

```
Device#show wireless wgb summary
Number of WGBs: 1
MAC Address    AP Name                             WLAN State              Clients
-------------------------------------------------------------------------------------
7070.8b7a.7030 Ed2-JFW-AP1                         1    Run                1
```

- WGB の詳細を表示するには、次のコマンドを使用します。

  show wireless wgb mac-address *MAC-address* **detail**

  次に、出力例を示します。

```
Device#show wireless wgb mac-address 7XXX.8XXa.7XXX detail

Work Group Bridge
```

```
MAC Address         : 7XXX.8XXa.7XXX
AP Name             : Ed2-JFW-AP1
WLAN ID             : 1
State               : Run

Number of Clients: 1

MAC Address
------------
d8XX.97XX.bXXX
```

- コントローラのクライアントの詳細を表示するには、次のコマンドを使用します。

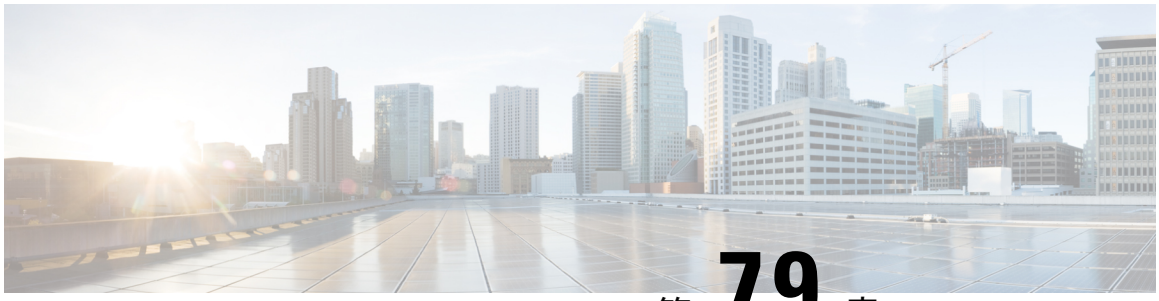
  show wireless client mac-address *MAC-address* **detail**

  次に、出力例を示します。

```
Device#show wireless client mac-address 7XXX.8bXX.70XX detail

Workgroup Bridge
Wired Client count : 1
```

- 次に、出力例を示します。

```
Device#show wireless client mac-address d8XX.97XX.b0XX detail
Workgroup Bridge Client
WGB MAC Address : 7XXX.8bXX.70XX
```



第 79 章

ピアツーピア クライアント サポート

ピアツーピア クライアント サポートについて

ピアツーピア クライアント サポートは個別の WLAN に適用でき、各クライアントがアソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピアツーピア クライアント サポート機能を使用すると、トラフィックの送信方法を細かく制御できます。たとえば、トラフィックをデバイス内でローカルにブリッジしたり、デバイスによってドロップしたり、アップストリーム VLAN に転送したりするように指定できます。

ローカル スイッチングの WLAN にアソシエートしたクライアントに対して、ピアツーピアブロッキングはサポートされています。

制約事項

- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- ピアツーピア ブロッキングは、デフォルトでは有効になっていません。
- FlexConnect では、特定の FlexConnect AP または一部の AP のみにピアツーピア ブロッキング設定を適用することはできません。SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- FlexConnect 中央スイッチングのクライアントではピアツーピア アップストリーム転送がサポートされます。ただし、これは FlexConnect ローカルスイッチングではサポートされません。これはピア ツー ピア ドロップとして処理され、クライアント パケットはドロップされます。

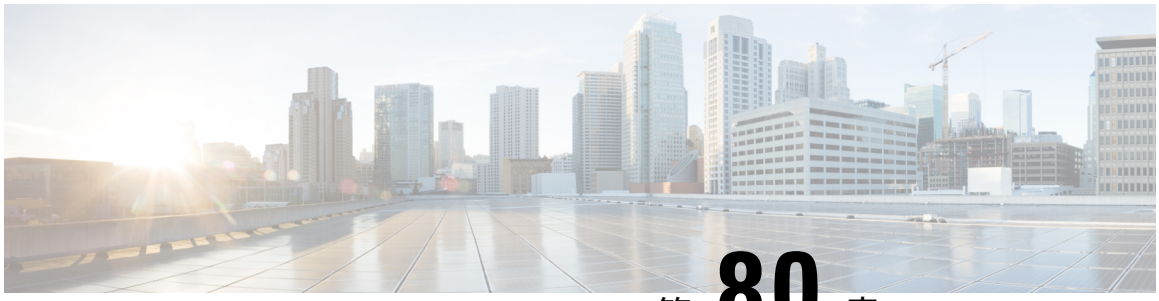
  FlexConnect 中央スイッチングのクライアントでは、異なる AP に関連付けられたクライアントに対するピアツーピアブロッキングがサポートされます。ただし、FlexConnect ローカルスイッチングの場合、このソリューションでは、同一の AP に接続するクライアントだけがターゲットとなります。FlexConnect ACL は、この制限の回避策として使用できます。

ピアツーピア クライアント サポートの設定

ピアツーピア クライアント サポートを設定するには、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	**wlan** *profile-name* 例： `Device(config)# wlan wlan1`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**peer-blocking** ［**drop** | **forward-upstream**］ 例： `Device(config-wlan)# peer-blocking drop`	ピアツーピア ブロッキング パラメータを設定します。キーワードは次のとおりです。 • **drop**：ドロップ アクションのピアツーピア ブロッキングをイネーブルにします。 • forward-upstream：何もせず、パケットをアップストリームに転送します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show wlan id** *wlan-id* 例： `Device# show wlan id 12`	選択した WLAN の詳細を表示します。



第 80 章

802.11r BSS Fast Transition

802.11R 高速移行について

高速ローミングの IEEE 標準である 802.11r では、対応するクライアントがターゲット アクセス ポイントにローミングする前でも、新しい AP との最初のハンドシェイクが実行される、ローミングの新しい概念が導入されています。この概念は高速移行と呼ばれます。最初のハンドシェイクによって、クライアントとアクセス ポイントは Pairwise Transient Key（PTK）を事前に計算できます。これらの PTK キーは、クライアントが再アソシエーション要求に応答するか、新しいターゲット アクセス ポイントとの交換に応答した後で、クライアントと AP に適用されます。

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。WLAN 設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

クライアント ローミング

クライアントが FT プロトコルを使用して現在の AP からターゲット AP に移動する場合、メッセージ交換は次のいずれかの方法を使用して実行されます。

- Over-the-Air：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。

- Over-the-Distribution System（DS）：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP との通信は、クライアントと現在の AP の間の FT アクション フレームで実行されてから、デバイスによって送信されます。

図 *27 : Over–the–Air* クライアント ローミングが設定されている場合のメッセージ交換

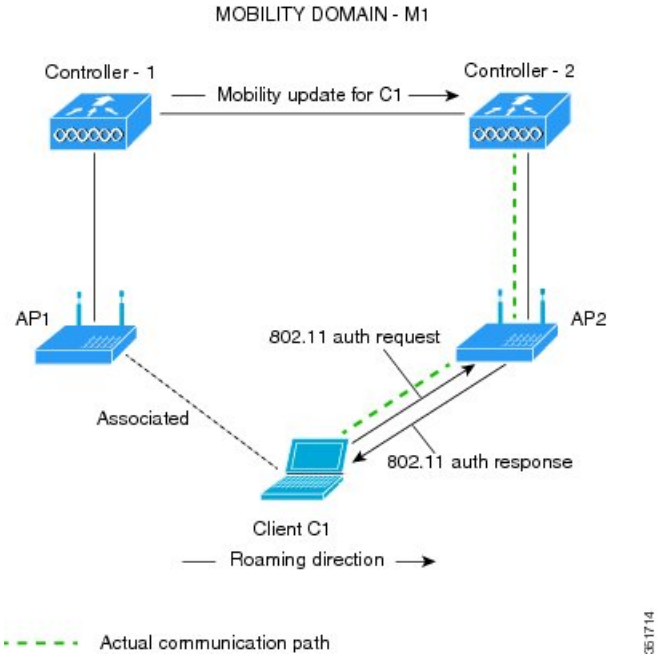
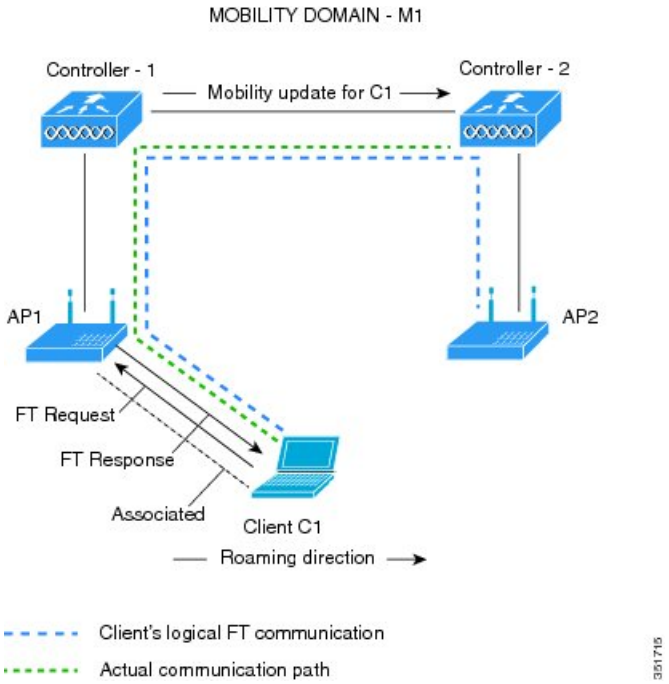


図 *28 : Over–the–DS* クライアント ローミングが設定されている場合のメッセージ交換



802.11R 高速移行の制約事項

- EAP LEAP 方式はサポートされません。
- トラフィック仕様（TSPEC）は802.11r高速ローミングではサポートされません。したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。音声またはデータの最大遅延を確認する必要があります。Cisco WLC は、Over-the-Air と Over-the-DS のどちらの方式でもローミング時に 802.11r 高速移行の認証要求を処理します。
- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。802.11r 対応クライアントは、802.11i と 802.11r の両方の認証キー管理スイートが有効になっている WLAN で 802.11i クライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作できるようにするか、アップグレードすることです。これにより、レガシー クライアントは 802.11r 対応 WLAN と正常にアソシエートできます。

  もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。
- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。また、リソース要求プロトコルはオプションのプロトコルです。
- サービス不能（DoS）攻撃を回避するため、Cisco WLC では、異なる AP と最大 3 つの高速移行ハンドシェイクが可能です。
- 非 802.11r 対応デバイスは FT 対応 WLAN にアソシエートできなくなります。
- 802.11r FT + PMF は推奨されません。
- FlexConnect 導入には 802.11r FT Over-the-Air ローミングをお勧めします。

802.11r 高速移行の監視（CLI）

次のコマンドを使用して、802.11r の高速移行を監視できます。

コマンド	説明
show wlan name *wlan-name*	WLAN に設定されているパラメータの要約を表示します。

コマンド	説明

show wireless client mac-address *mac-address*	クライアントの 802.11r 認証キー管理の設定の概要を表示します。
	
	. . .
	. . .
	Client Capabilities
	  CF Pollable : Not implemented
	  CF Poll Request : Not implemented
	  Short Preamble : Not implemented
	  PBCC : Not implemented
	  Channel Agility : Not implemented
	  Listen Interval : 15
	  Fast BSS Transition : Implemented
	Fast BSS Transition Details :
	Client Statistics:
	  Number of Bytes Received : 9019
	  Number of Bytes Sent : 3765
	  Number of Packets Received : 130
	  Number of Packets Sent : 36
	  Number of EAP Id Request Msg Timeouts : 0
	
	  Number of EAP Request Msg Timeouts : 0
	  Number of EAP Key Msg Timeouts : 0
	  Number of Data Retries : 1
	  Number of RTS Retries : 0
	  Number of Duplicate Received Packets : 1
	  Number of Decrypt Failed Packets : 0
	  Number of Mic Failured Packets : 0
	  Number of Mic Missing Packets : 0
	  Number of Policy Errors : 0
	  Radio Signal Strength Indicator : -48 dBm
	
	  Signal to Noise Ratio : 40 dB
	. . .
	. . .

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（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。
ステップ 2	**wlan** *profile-name* 例：	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設

	コマンドまたはアクション	目的
	デバイス# **wlan test4**	定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： デバイス(config-wlan)# **client vlan 0120**	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**security dot1x authentication-list default** 例： デバイス(config-wlan)# **security dot1x authentication-list default**	dot1x セキュリティ用のセキュリティ認証リストを有効にします。この設定は、すべての dot1x セキュリティ WLAN で類似しています。
ステップ 5	**security ft** 例： デバイス(config-wlan)# **security ft**	WLAN で 802.11r 高速移行を有効にします。
ステップ 6	**security wpa akm ft dot1x** 例： デバイス(config-wlan)# **security wpa akm ft dot1x**	WLAN 上で 802.1x セキュリティをイネーブルにします。
ステップ 7	**no shutdown** 例： デバイス(config-wlan)# **no shutdown**	WLAN をイネーブルにします。
ステップ 8	**end** 例： デバイス(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。

オープン WLAN での 802.11r 高速移行の設定（GUI）

手順

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

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 **[Security]** > **[Layer2]** タブで、AP 間の [Fast Transition] の適切なステータスを選択します。

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

オープン WLAN での 802.11r 高速移行の設定（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。
ステップ 2	**wlan** *profile-name* 例： `デバイス# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-id* 例： `デバイス(config-wlan)# client vlan 0120`	WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa** 例： `デバイス(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no security wpa akm dot1x** 例： `デバイス(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2** 例： `デバイス(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 7	**no wpa wpa2 ciphers aes** 例： `デバイス(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 8	**security ft** 例： `デバイス(config-wlan)# security ft`	802.11r 高速移行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
ステップ 9	**no shutdown** 例： `デバイス(config-wlan)# shutdown`	WLAN をシャット ダウンします。
ステップ 10	**end** 例： `デバイス(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。

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（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。
ステップ 2	**wlan** *profile-name* 例： `デバイス# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： `デバイス(config-wlan)# client vlan 0120`	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa akm dot1x** 例： `デバイス(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**security wpa akm ft psk** 例： `デバイス(config-wlan)# security wpa akm ft psk`	高速移行 PSK サポートを設定します。
ステップ 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}}	PSK AKM の共有キーを設定します。

	コマンドまたはアクション	目的
	例： デバイス(config-wlan)# **security wpa akm psk set-key ascii 0 test**	
ステップ 7	**security ft** 例： デバイス(config-wlan)# **security ft**	802.11r 高速移行を設定します。
ステップ 8	**no shutdown** 例： デバイス(config-wlan)# **no shutdown**	WLAN をイネーブルにします。
ステップ 9	**end** 例： デバイス(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。

802.11r 高速移行の無効化（GUI）

手順

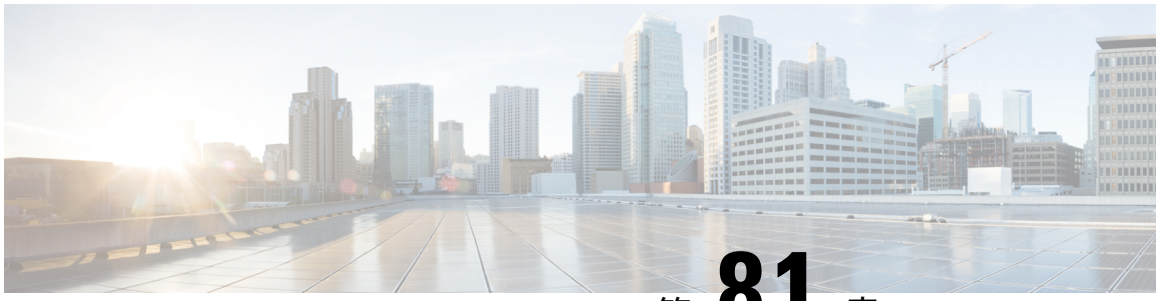
ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 [WLANs] ページで、WLAN 名をクリックします。
ステップ 3 [Edit WLAN] ウィンドウで **[Security]** > **[Layer2]** タブをクリックします。
ステップ 4 [Fast Transition] ドロップダウンリストから [Disabled] を選択します。
ステップ 5 [Update & Apply to Device] をクリックします。

802.11r 高速移行のディセーブル（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	**wlan** *profile-name* 例： デバイス# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] 例： デバイス(config-wlan)# **no security ft over-the-ds**	WLAN の 802.11r 高速移行をディセーブルにします。
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。



第 81 章

経由ローミング

802.11k ネイバーリストと経由ローミング

802.11k 標準を使用すると、AP は 802.11k 対応クライアントに隣接する BSSID（同じ SSID の AP）を通知できるため、クライアントがスキャンとローミングの動作を最適化するのに役立ちます。さらに、Assisted Roaming Prediction Optimization 機能を非 802.11k のクライアントで使用して、最適でない AP へのローミングを防止できます。

予測ベースのローミング：802.11k 以外のクライアントの経由ローミング

各クライアントに対し、予測ネイバー リストを生成することで、802.11k ネイバー リスト要求を送信する必要がなくなり、802.11k 以外のクライアントに対するローミングを最適化できます。予測ベースのローミングを WLAN で有効にすると、クライアントがアソシエーションまたは再アソシエーションに成功する度に、同一のネイバー リスト最適化が 802.11k 以外のクライアントに適用され、生成されたネイバーリストがモバイル ステーションのソフトウェア データ構造内に格納されます。クライアントは通常、アソシエーションまたは再アソシエーションを行う前にプローブを行うため、クライアント プローブの RSSI 値はネイバーごとに異なります。このため、異なる場所にあるクライアントには、それぞれ異なるネイバー リストが生成されます。このリストは最新のプローブ データによって生成され、クライアントがローミングする可能性の高い次の AP を予測します。

AP へのアソシエーション要求が、格納済みの予測ネイバー リスト内のエントリと一致しない場合、無線インフラストラクチャはアソシエーションを拒否し、好ましくないネイバーへのクライアントのローミングを抑止します。

- 拒否数：クライアントが関連付けを拒否される最大回数。

- 予測しきい値：経由ローミング機能をアクティブにするために必要な予測リストの最小エントリ数。

詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/Chapter-11.html#pgfId-1140097を参照してください。

経由ローミングの制約事項

- この機能は、802.11n 対応の屋内アクセス ポイントでのみサポートされています。 1 つの帯域構成の場合、最大 6 のネイバーがネイバー リストに表示されます。デュアル バンド構成の場合、最大 12 のネイバーが表示されます。
- device CLI をのみを使用して経由ローミングを設定できます。

経由ローミングの設定方法

経由ローミングの設定（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。
ステップ 2	**wireless assisted-roaming floor-bias** *dBm* 例： `デバイス(config)# wireless assisted-roaming floor-bias 20`	ネイバー フロア ラベル バイアスを設定します。有効な範囲は–5 ～ 25 dBm で、デフォルト値は –15 dBm です。
ステップ 3	**wlan** *wlan-id* 例： `デバイス(config)# wlan wlan1`	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* は設定されている WLAN のプロファイル名です。
ステップ 4	**assisted-roaming neighbor-list** 例： `デバイス(wlan)# assisted-roaming neighbor-list`	WLAN の 802.11k ネイバー リストを設定します。WLANを作成すると、デフォルトで assisted roaming がネイバー リストで有効になります。コマンドの **no** 形式を実行すると、経由ローミングのネイバー リストが無効になります。

	コマンドまたはアクション	目的
ステップ 5	**assisted-roaming dual-list** 例： `デバイス(wlan)# assisted-roaming dual-list`	WLAN のデュアル バンド 802.11k デュアル リストを設定します。WLAN を作成すると、デフォルトで assisted roaming がデュアル リストで有効になります。コマンドの **no** 形式を実行すると、経由ローミングのデュアル リストが無効になります。
ステップ 6	**assisted-roaming prediction** 例： `デバイス(wlan)# assisted-roaming prediction`	WLAN の経由ローミング予測リスト機能を設定します。デフォルトでは、経由ローミング予測リストはディセーブルです。 （注） ロード バランシングが WLAN に対してすでにイネーブルである場合、警告メッセージが表示され、ロード バランシングが WLAN に対してディセーブルになります。
ステップ 7	**wireless assisted-roaming prediction-minimum** *count* 例： `デバイス# wireless assisted-roaming prediction-minimum`	予測リスト機能が動作するために必要な予測 AP の最小数を設定します。デフォルト値は 3 です。 （注） クライアントに割り当てられた Forecast、AP が指定した数よりもこの値が小さい場合、経由ローミング機能はこのルールに適用されません。
ステップ 8	**wireless assisted-roaming denial-maximum** *count* 例： `デバイス# wireless assisted-roaming denial-maximum 8`	AP に送信されたアソシエーション要求が予測の AP に一致しない場合に、クライアントでアソシエーションを拒否できる最大回数を設定します。有効な範囲は 1 ～ 10 で、デフォルト値は 5 です。
ステップ 9	**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。

経由ローミングの確認

次のコマンドを使用して、WLAN に設定された経由ローミングを確認できます。

コマンド	説明
show wlan id *wlan-id*	WLAN の WLAN パラメータを表示します。

経由ローミングの設定例

次に、ネイバー フロア ラベル バイアスを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless assisted-roaming floor-bias 10
デバイス(config)# end
デバイス# show wlan id 23
```

次に、特定の WLAN のネイバー リストをディセーブルにする例を示します。

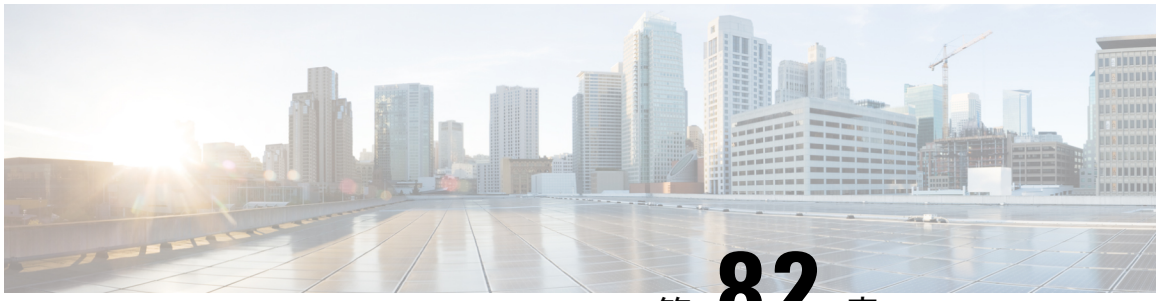
```
デバイス# configure terminal
デバイス(config)# wlan test1
デバイス(config (wlan)# no assisted-roaming neighbor-list
デバイス(config)(wlan)# end
デバイス# show wlan id 23
```

次に、特定の WLAN の予測リストを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wlan test1
デバイス(config)(wlan)# assisted-roaming prediction
デバイス(config)(wlan)# end
デバイス# show wlan id 23
```

次に、特定の WLAN の経由ローミングの予測しきい値および最大の拒否数に基づいて予測リストを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless assisted-roaming prediction-minimum 4
デバイス(config)# wireless assisted-roaming denial-maximum 4
デバイス(config)(wlan)# end
デバイス# show wlan id 23
```



第 82 章

802.11v

802.11v に関する情報

組み込みワイヤレスコントローラは、ワイヤレスネットワークに関する 802.11v 改訂をサポートします。この改訂には、ワイヤレスネットワーク管理に対するさまざまな機能拡張が記述されています。

このような機能拡張の 1 つに、クライアントでスリープ時間を延ばしてバッテリ寿命を改善できるようにするネットワーク支援型電力節約があります。たとえば、多くのモバイルデバイスは、特定のアイドル期間を利用してアクセス ポイントとの接続を維持するため、ワイヤレスネットワークで以降のタスクを実行するときにより多くの電力を消費します。

もう 1 つの機能拡張は、WLAN 上で関連するクライアントに要求を送信して、クライアントにアソシエートするより適切な AP をアドバタイズ可能なネットワーク支援型ローミングです。これは、ロード バランシングと、接続が不安定なクライアントの管理の両方に役立ちます。

802.11v ネットワーク支援型電力節約の有効化

ワイヤレスデバイスはクライアントへの接続を維持するためにさまざまな方法でバッテリを消費します。

- 定期的にスリープ解除し、DTIM を含むアクセス ポイント ビーコンをリッスンします。DTIM は、アクセス ポイントがクライアントに送信する、ブロードキャストまたはマルチキャスト トラフィックがバッファされていることを示します。
- アクセス ポイントとの接続を維持するために、null フレームをキープアライブ メッセージの形式でアクセス ポイントに送信します。

- デバイスは、定期的に、ビーコンをリッスン（DTIM フィールドがない場合も）して、対応するアクセス ポイントとクロックを同期させます。

このすべてのプロセスがバッテリを消費し、その消費は特にデバイス（Apple など）に影響します。これは、これらのデバイスが保守的なセッション タイムアウト推定を使用しているために、頻繁にスリープ解除してキープアライブ メッセージを送信するためです。802.11 標準は、802.11v なしのローカル クライアントのセッション タイムアウトの無線クライアントと通信するため、コントローラまたはアクセス ポイントの機能は含まれていません。

ワイヤレス ネットワーク上の上記タスクによるクライアントの電力を節約するために、802.11v 標準の次の機能が使用されます。

- Directed Multicast Service
- Base Station Subsystem（BSS）最大アイドル期間

Directed Multicast Service

Directed Multicast Service（DMS）を使用して、クライアントは、必要なマルチキャスト パケットをユニキャスト フレームとして送信するようにアクセス ポイントに要求します。これにより、クライアントは、スリープ モードでは無視していたマルチキャスト パケットを受信でき、レイヤ 2 の信頼性も保証されます。また、ユニキャスト フレームができるだけ高いワイヤレス リンク レートでクライアントに送信されるため、クライアントは無線の持続期間を短縮してパケットをすばやく受信できるようになり、バッテリの電力が節約されます。ワイヤレス クライアントはマルチキャスト トラフィックを受信するために DTIM 間隔ごとにスリープ解除する必要がないため、スリープ間隔を延ばすことができます。

BSS の最大アイドル時間

BSS 最大アイドル期間は、アクセス ポイント（AP）が接続先のクライアントからフレームが受信されないという理由でそのクライアントをアソシエート解除しないタイムフレームです。これにより、クライアント デバイスがキープアライブ メッセージを頻繁に送信しないことが保証されます。アイドル期間タイマー値は、アクセス ポイントからクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。このアイドル時間値は、クライアントがアクセス ポイントにフレームを送信せずにアイドル状態を維持できる最大時間を示します。したがって、クライアントは、キープアライブ メッセージを頻繁に送信することなく、より長い間スリープ モードを維持します。これがバッテリの電力の節約につながります。

802.11v の実装の前提条件

- Apple iOS バージョン 7 以降で動作する Apple iPad や iPhone などの Apple クライアントに適用されます。
- ローカル モードをサポートしています。中央認証モードだけ FlexConnect のアクセス ポイントをサポートします。

802.11v に関する制約事項

クライアントは 802.11v BSS 移行をサポートする必要があります。

802.11v BSS 移行管理の有効化

802.11v BSS 移行は次の 3 つのシナリオに適用されます。

- 要請された要求：クライアントは、再度関連付ける AP のより適切なオプションをローミングする前に、802.11v 基本サービス セット（BSS）移行管理クエリを送信できます。
- 要請されないロード バランシング要求：AP は負荷が高い場合、関連付けられたクライアントに 802.11v BSS 移行管理要求を送信します。
- 要請されない最適化ローミング要求：クライアントの RSSI とレートが要件を満たしていない場合は、対応する AP はこのクライアントに 802.11v BSS 移行管理要求を送信します。

（注） 802.11v BSS 移行管理要求は、クライアントが従うか無視するか選択できる、クライアントに与えられた提案事項（つまりアドバイス）です。クライアントの関連付け解除を強制するには、関連付け解除イミネント機能をオンにします。これにより、クライアントは別の AP に再アソシエートしないと一定時間後にアソシエート解除されます。

802.11v BSS 移行管理の設定（GUI）

手順

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

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 [Advanced] タブおよび [11v BSS Transition Support] セクションで、[BSS Transition] チェック ボックスをオンにして WLAN ごとの BSS 移行を有効にします。

ステップ 4 [Disassociation Imminent] の値を入力します。有効な範囲は 0 ～ 3000 TBTT です。

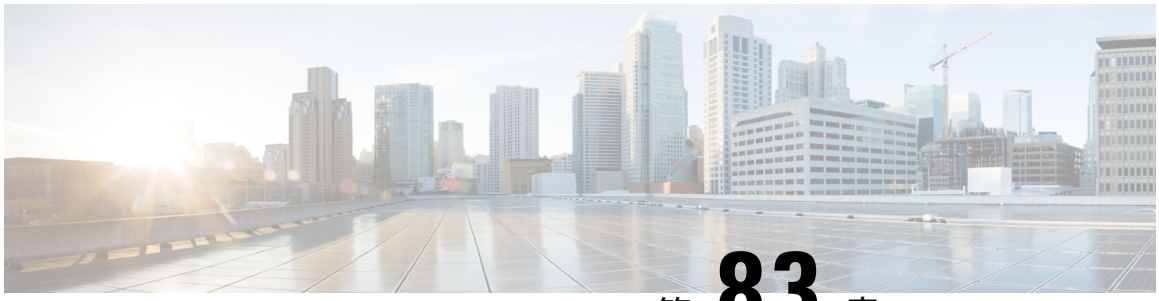
ステップ 5 [Save & Apply to Device] をクリックします。

802.11v BSS 移行管理の設定（CLI）

802.11v BSS 移行は次の 3 つのシナリオに適用されます。

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	**wlan** *profile-name* 例： `Device(config)# wlan test-wlan`	WLAN プロファイルを設定し、WLAN 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	**shut** 例： `Device(config-wlan)# shut`	WLAN プロファイルをシャットダウンします。
ステップ 4	**bss-transition** 例： `Device(config-wlan)# bss-transition`	WLAN ごとの BSS 移行を設定します。
ステップ 5	**bss-transition disassociation-imminent** 例： `Device(config-wlan)# bss-transition disassociation-imminent`	WLAN ごとの BSS 移行関連付け解除イミネントを設定します。
ステップ 6	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN プロファイルを有効にします。
ステップ 7	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。または、Ctrl+Z キーを押してグローバル コンフィギュレーション モードを終了できます。



第 83 章

802.11W

802.11w に関する情報

Wi-Fi は、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャストメディアです。認証、認証解除、アソシエーション、アソシエーション解除、ビーコン、プローブなどの管理フレームは、ワイヤレスクライアントがネットワーク サービスのセッションを開始および切断するために使用します。暗号化により、一定レベルの機密保持を実現できるデータ トラフィックとは異なり、これらのフレームはすべてのクライアントによって受信および解釈される必要があるため、オープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。たとえば、攻撃者は AP にアソシエートされたクライアントを攻撃するために、AP からの管理フレームをスプーフィングする可能性があります。

802.11w プロトコルは、保護管理フレーム（PMF）サービスによって保護された一連の堅牢な管理フレームにのみ適用されます。これには、アソシエーション解除フレーム、認証解除フレーム、ロバスト アクション フレームなどが含まれます。

したがって、ロバストアクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトル管理
- QoS
- DLS
- ブロック ACK

- 無線測定
- 高速 BSS 移行
- SA クエリ
- 保護されたデュアル パブリック アクション
- ベンダー固有保護

802.11w が無線メディアで実行されると、次のことが行われます。

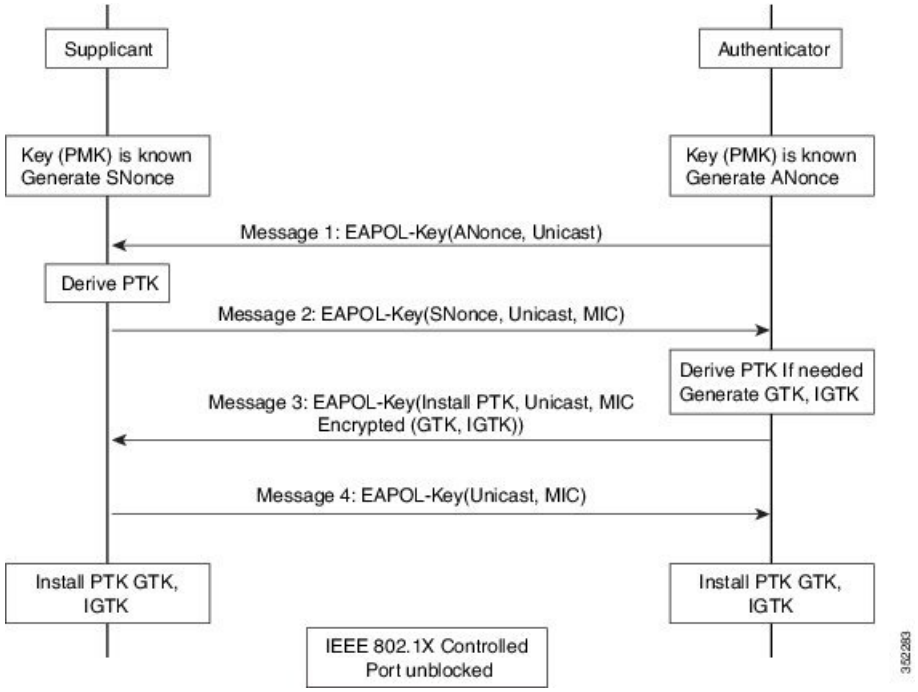
- AP が認証解除フレームと関連付け解除フレームに暗号保護を追加することでクライアント保護が追加され、DoS 攻撃でのスプーフィングを阻止します。
- アソシエーション復帰期間とセキュリティ アソシエーション（SA）クエリの手順で構成される SA ティアダウン保護メカニズムを追加することでインフラストラクチャ保護が追加され、スプーフィングされたアソシエーション要求によって接続済みのクライアントが切断されることを阻止します。

802.11w で新たに導入された IGTK キーは、ブロードキャスト/マルチキャストの堅牢な管理フレームを保護するために使用されます。

- IGTK はオーセンティケータ STA（WLC）によって割り当てられるランダムな値で、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用されます。

管理フレーム保護のネゴシエーション時に、AP は 4 ウェイ ハンドシェイクのメッセージ 3 で送信される EAPOL キー フレーム内の GTK 値と IGTK 値を暗号化します。

図 *29 : 4* ウェイ ハンドシェイクでの *IGTK* 交換

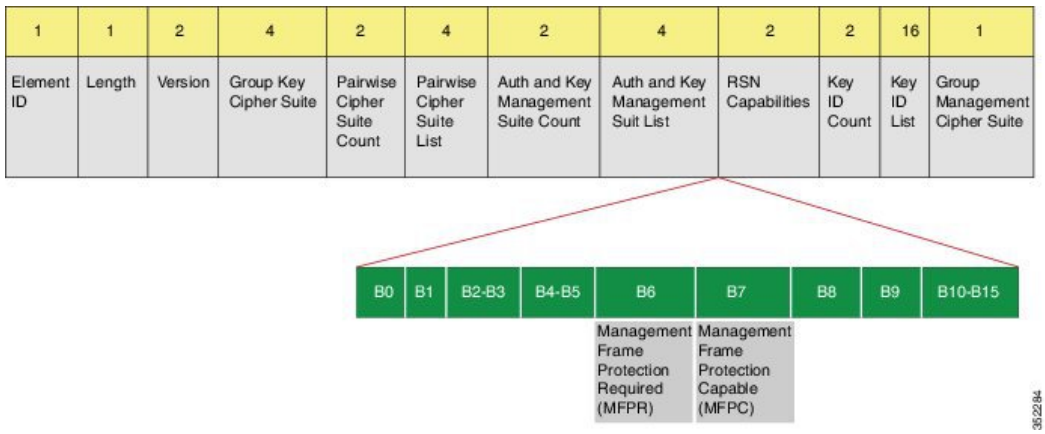


- AP は後で GTK を変更した場合には、グループ キー ハンドシェイクを使用して新しい GTK と IGTK をクライアントに送信します。

802.11w では、新たに Broadcast/Multicast Integrity Protocol（BIP）が定義されています。このプロトコルは、IGTKSA が正常に確立された後、ブロードキャスト/マルチキャストの堅牢な管理フレームにおけるデータの整合性、およびリプレイ保護を提供し、共有 IGTK キーを使用して計算される MIC を追加します。

802.11w の情報要素（IE）

図 *30 : 802.11w* の情報要素



1. RSNIE の RSN 機能フィールドに変更が加えられています。

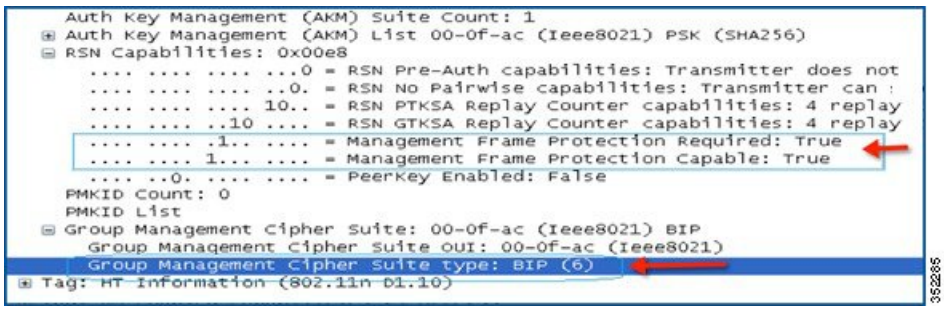
1. ビット 6：Management Frame Protection Required（MFPR）
2. ビット 7：Management Frame Protection Capable（MFPC）

2. 2 つの新しい AKM スイート 5 および 6 が AKM スイート セレクタ用に追加されています。
3. BIP に対応するため、タイプ 6 の新たな暗号スイートが追加されました。

この変更された RSNIE を WLC はアソシエーション応答と再アソシエーション応答に追加し、AP はビーコン応答とプローブ応答に追加します。

次の Wireshark キャプチャ画面は、RSNIE 機能とグループ管理暗号スイートの要素を示します。

図 *31 : 802.11w* の情報要素



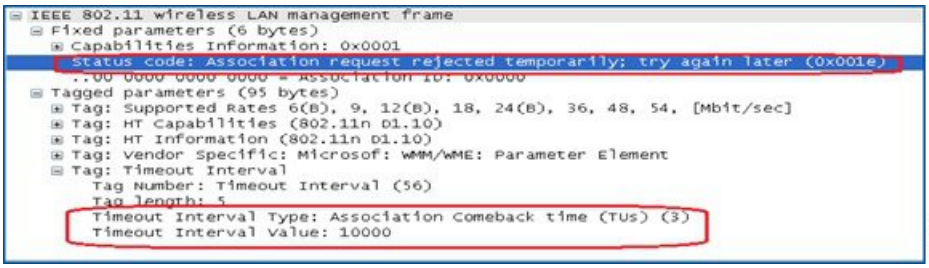
セキュリティ アソシエーション（SA）ティアダウン保護

SA ティアダウン保護は、リプレイ攻撃によって既存のクライアントのセッションが切断されるのを防止するメカニズムです。アソシエーションの復帰期間と SA クエリの手順を組み合わせることで、スプーフィングされたアソシエーション要求により、接続済みのクライアントが切断されることを防止します。

クライアントが有効なセキュリティ アソシエーションを有し、802.11w をネゴシエートしている場合は、AP はステータス コード 30 を使用して、新たなアソシエーション要求を拒否します。このステータス コードは、「アソシエーション要求が一時的に拒否されました。後でやり直してください」ということを意味します。AP は、SA クエリ手順によって元の SA が無効であると判断されない限り、既存アソシエーションを切断したり、その状態を変更したりすることはできません。また、APのアソシエーション応答には、APがこのクライアントとのアソシエーションを受け入れる準備が整うまでの時間を指定したアソシエーション復帰期間の情報要素が含められます。

次の図は、ステータス コード 0x1e（30）のアソシエーション拒否メッセージと、10 秒に設定されたアソシエーション復帰期間を示しています。

図 *32* : アソシエーション拒否と復帰期間



クライアントとの SA クエリがまだ実行されていない場合、AP は一致する SA クエリ応答を受信するか、アソシエーション復帰期間が経過するまで、SA クエリを発行します。AP は有効な保護フレームを受信すると、SA クエリが正常に完了したと解釈します。

一致するトランザクション識別子を含む SA クエリ応答が期間内に行われると、AP は追加の SA クエリ手順を開始せずに、アソシエーション プロセスの開始を許可します。

802.11w の前提条件

- 任意および必須の 802.11w 機能を設定するには、WPA および AKM を設定する必要があります。

（注） Robust Secure Network（RNS）IE は AES 暗号化とともにイネーブルにする必要があります。

802.11w の制約事項

- 802.11w はオープン WLAN、 WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用されていません。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ Apple 以外のクライアントに対しては、802.11w + PMF の組み合わせがサポートされています。ただし、Apple iOS バージョン 11 以前で関連付けの問題を解決するには、Apple iOS 側からの修正が必要です。
- クライアントで802.11wPMFが使用されていない場合、コントローラはクライアントから送信された関連付け解除または認証解除フレームを無視します。クライアントで PMF が使用されている場合、クライアントエントリは該当フレームを受信した場合のみすぐに削除されます。これは、PMF のないフレームは安全ではないため、悪意のあるデバイスによるサービス妨害を回避するためです。

802.11w の設定方法

802.11w の設定（GUI）

始める前に

WPA および AKM を設定する必要があります。

手順

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

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 **[Security]** > **[Layer2]** タブで、[Protected Management Frame] セクションに移動します。

ステップ 4 [PMF] で [Disabled]、[Optional]、または [Required] を選択します。デフォルトでは、PMF は無効になっています。

[PMF] で [Optional]、または [Required] を選択した場合は、次のフィールドが表示されます。

- [Association Comeback Timer]：1 ～ 10 秒の値を入力して、802.11w のアソシエーション復帰期間を設定します。
- [SA Query Time]：100 ～ 500（ミリ秒）の値を入力します。これは、クライアントが WLAN の 802.11w PMF 保護をネゴシエートするために必要です。

ステップ 5 [Save & Apply to Device] をクリックします。

802.11w の設定（CLI）

始める前に

WPA および AKM を設定する必要があります。

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	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan wlan-test 12 alpha`	WLANを設定し、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	**security wpa akm pmf dot1x** 例： `Device(config-wlan)#security wpa akm pmf dot1x`	802.1x のサポートを設定します。
ステップ 4	**security pmf association-comeback** *comeback-interval* 例： `Device(config-wlan)# security pmf association-comeback 10`	802.11wアソシエーション復帰時間を設定します。
ステップ 5	**security pmf mandatory** 例： `Device(config-wlan)# security pmf mandatory`	クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることを要求します。
ステップ 6	**security pmf saquery-retry-time** *timeout* 例： `Device(config-wlan)# security pmf saquery-retry-time 100`	SA クエリ応答を受け取るまでの時間（ミリ秒単位）です。デバイスが応答を受け取らなかった場合、別の SQ クエリが試行されます。

802.11w の無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan wlan-test 12 alpha`	WLANを設定し、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 security wpa akm pmf dot1x** 例： `Device(config-wlan)# no security wpa akm pmf dot1x`	802.1x サポートを無効にします。

	コマンドまたはアクション	目的
ステップ 4	**no security pmf association-comeback** *comeback-interval* 例： `Device(config-wlan)# no security pmf association-comeback 10`	802.11wのアソシエーション復帰期間を無効にします。
ステップ 5	**no security pmf mandatory** 例： `Device(config-wlan)# no security pmf mandatory`	クライアントによる WLAN の 802.11w PMF 保護のネゴシエートを無効にします。
ステップ 6	**no security pmf saquery-retry-time** *timeout* 例： `Device(config-wlan)# no security pmf saquery-retry-time 100`	SQ クエリの再試行を無効にします。

802.11w のモニターリング

802.11w をモニターリングするには、次のコマンドを使用します。

手順

ステップ 1 **show wlan name** *wlan-name*

WLAN の WLAN パラメータを表示します。PMF パラメータが表示されます。

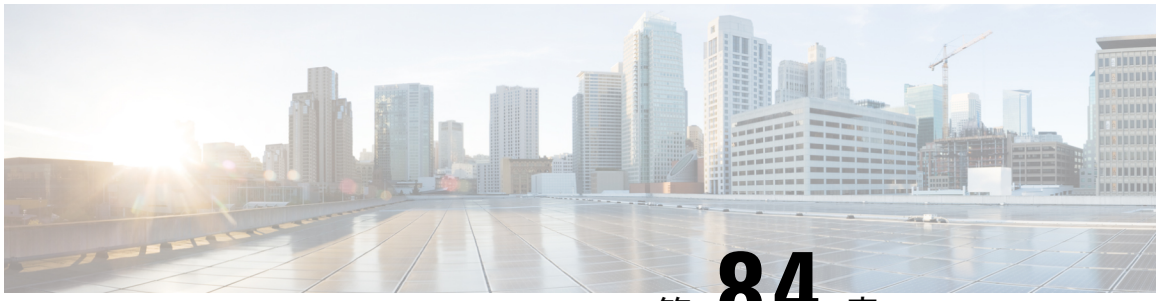
```
. . . .
. . . .
Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            FT SAE                              : Disabled
            Dot1x-SHA256                        : Enabled
            PSK-SHA256                          : Disabled
            SAE                                 : Disabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Adaptive
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Required
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 500
```

```
. . . .
. . . .
```

ステップ 2 **show wireless client mac-address** *mac-address***detail**

クライアントの 802.11w 認証キー管理設定の概要を表示します。

```
. . . .
. . . .
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 497 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x-SHA256
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : Yes
EAP Type : LEAP
VLAN : 39
Multicast VLAN : 0
Access VLAN : 39
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
. . . .
. . . .
```



第 84 章

仮想アクセスポイントごとの 802.11ax

仮想アクセスポイントごとの 802.11ax モードに関する情報

Cisco IOS XE Bengaluru リリース 17.4.1 より前では、802.11ax モードは無線帯域ごとに設定されていました。この構成では、無線ごとに構成されたすべての仮想アクセスポイント（AP）に対して 11ax モードが一度に有効化または無効化されていました。無線ごとに 11ax が有効になっている場合、ビーコンに 11ax 情報要素があると、11ac クライアントは SSID をスキャンしたり、SSID に接続したりできませんでした。ビーコンに 11ax IE がある場合、クライアントはアクセスポイント（AP）をプローブできませんでした。

そのため、Cisco IOS XE Bengaluru リリース 17.5.1 以降、仮想 AP ごとに 11ax のコンフィギュレーションノブが導入されています。このノブは、WLAN プロファイルの下に導入されています。デフォルトでは、VAP ごとの 11ax ノブがコントローラで有効になっています。

（注） 6 GHz 無線の場合、802.11ax パラメータは、AP の対応する 6 GHz RF プロファイルにタグ付けされたマルチ BSSID プロファイルから取得されます。したがって、6 GHz の場合、WLAN dot11ax パラメータはマルチ BSSID プロファイルのパラメータによってオーバーライドされます。2.4 GHz および 5 GHz 帯域の WLAN に変更はありません。802.11ax の WLAN パラメータが引き続き使用されます。

仮想アクセスポイントごとの 802.11ax モードの設定（GUI）

手順

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

ステップ 2 [Add] をクリックします。
[Add WLAN] ウィンドウが表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [11ax] セクションで、[Enable 11ax] チェックボックスをオンにして、WLAN の 802.11ax 動作ステータスを有効にします。

（注） 11ax が無効になっている場合、ビーコンには 11ax IE は表示されず、WLAN 上のすべての 11ax 機能が操作上無効になります。

ステップ 5 [Apply to Device] をクリックします。

仮想アクセスポイントごとの 802.11ax モードの設定

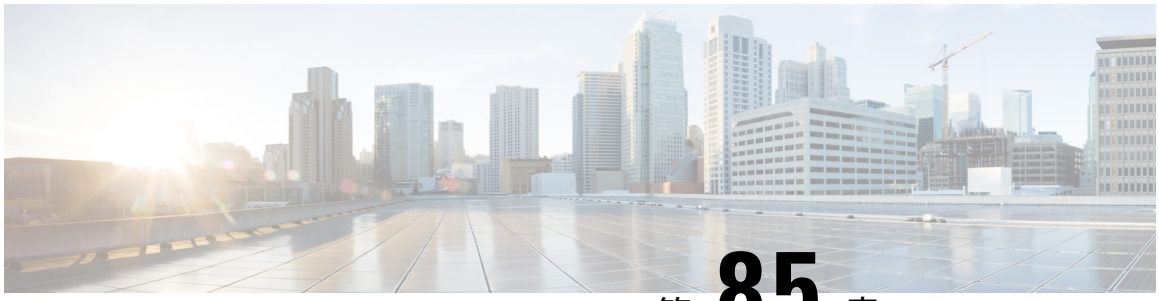
手順

	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	**wlan** *wlan-profile-name* 例： `Device(config)# wlan wlan-profile`	WLAN 名を指定し、WLAN 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	**dot11ax** 例： `Device(config-wlan)# dot11ax`	WLAN で 802.11ax を設定します。
ステップ 4	**no dot11ax** 例： `Device(config-wlan)# no dot11ax`	WLAN プロファイルの 802.11ax を無効にします。

仮想アクセスポイントごとの 802.11ax モードの確認

11ax パラメータのステータスを表示するには、次のコマンドを実行します。

```
Device# show wlan id 6
WLAN Profile Name     : power
================================================
Identifier                                      : 6
Description                                     :
Network Name (SSID)                             : power
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Advertise-Apname                                : Disabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
.
.
.
802.11ac MU-MIMO                                : Enabled
802.11ax parameters
    802.11ax Operation Status                   : Enabled
    OFDMA Downlink                              : Enabled
    OFDMA Uplink                                : Enabled
    MU-MIMO Downlink                            : Enabled
    MU-MIMO Uplink                              : Enabled
    BSS Target Wake Up Time                     : Enabled
    BSS Target Wake Up Time Broadcast Support   : Enabled
.
.
.
```



第 85 章

カレンダープロファイルを使用した Deny ワイヤレス クライアント セッションの確立

ワイヤレスクライアントセッションの確立の拒否について

クライアントセッション確立拒否機能により、コントローラはクライアントセッションの確立を特定の時間に基づいて停止できます。これにより、手動で操作することなく、ネットワークを効率的かつ制御された方法で管理できます。

組み込みワイヤレスコントローラでは、次の反復間隔に基づいてワイヤレスクライアントセッションを拒否できます。

- 毎日
- 毎週
- 毎月

作成されたカレンダープロファイルは、ポリシープロファイルにマッピングされます。カレンダープロファイルをポリシープロファイルに適用することで、ポリシープロファイルに対して異なるポリシータグを使用して異なる繰り返しを作成できます。

（注） 日単位、週単位、および月単位のサブカテゴリごとに個別のカレンダープロファイルを作成する必要があります。

次に、ワイヤレス クライアント セッション確立拒否機能のワークフローを示します。

- カレンダープロファイルを作成します。
- ポリシープロファイルにカレンダープロファイルを適用します。

（注） 最大 100 個のカレンダープロファイルを設定でき、最大 5 つのカレンダープロファイルをポリシープロファイルに関連付けることができます。

注意事項

コントローラを起動すると、システムが起動してから 1 分後にクライアントセッション確立拒否機能が起動します。

カレンダープロファイルがポリシープロファイルに関連付けられた後にシステム時刻を変更した場合は、新しいクロックタイミングに合わせて最大 30 秒の遅延が発生することが予想されます。

（注） カレンダープロファイルをポリシー プロファイルに関連付けるときに、**no action deny-client** コマンドを使用してアクションを無効にすることはできません。

action コマンドを無効にする場合は、ポリシープロファイルからカレンダープロファイルの関連付けを解除し、再度設定し直す必要があります。

日次カレンダープロファイルの設定

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 calendar-profile name** *name* 例： `Device(config)# wireless profile calendar-profile name daily_calendar_profile`	カレンダープロファイルを設定します。 ここで、各変数は次のように定義されます。 *name* は、カレンダー プロファイルの名前を指します。
ステップ 3	**start** *start_time* **end** *end_time* 例： `Device(config-calendar-profile)# start 09:00:00 end 17:00:00`	カレンダープロファイルの開始時刻と終了時刻を設定します。 ここで、各変数は次のように定義されます。 *start_time* は、カレンダープロファイルの開始時刻です。開始時刻は **HH:MM:SS** 形式で入力する必要があります。 *end_time* は、カレンダープロファイルの終了時刻です。終了時刻は **HH:MM:SS** 形式で入力する必要があります。
ステップ 4	**recurrence daily** 例： `Device(config-calendar-profile)# recurrence daily`	カレンダープロファイルの日次繰り返し数を設定します。
ステップ 5	**end** 例： `Device(config-calendar-profile)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。 （注） カレンダープロファイルが作動すると、イーサネット速度に対して定義されている AP 電力プロファイルルール（無線状態や USB デバイス状態など）は適用されず、固定電力プロファイルに従って継続されます。

週次カレンダープロファイルの設定

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 profile calendar-profile name** *name* 例： `Device(config)# wireless profile calendar-profile name weekly_calendar_profile`	カレンダープロファイルを設定します。 ここで、各変数は次のように定義されます。 *name* は、カレンダー プロファイルの名前を指します。
ステップ 3	**start** *start_time* **end** *end_time* 例： `Device(config-calendar-profile)# start 18:00:00 end 19:00:00`	カレンダープロファイルの開始時刻と終了時刻を設定します。 ここで、各変数は次のように定義されます。 *start_time* は、カレンダープロファイルの開始時刻です。開始時刻は **HH:MM:SS** 形式で入力する必要があります。 *end_time* は、カレンダープロファイルの終了時刻です。終了時刻は **HH:MM:SS** 形式で入力する必要があります。
ステップ 4	**recurrence weekly** 例： `Device(config-calendar-profile)# recurrence weekly`	カレンダープロファイルの週次繰り返し数を設定します。

ステップ 5	**day** {**friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday**}
	例：
	`Device(config-calendar-profile)# day friday`
	`Device(config-calendar-profile)# day monday`
		週次カレンダーをアクティブにする必要がある日を設定します。
		（注） このコマンドで複数の日を設定できます。

ステップ 6	**end** 例：	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
	`Device(config-calendar-profile)# end`	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。

月次カレンダープロファイルの設定

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 profile calendar-profile name** *name* 例： `Device(config)# wireless profile calendar-profile name monthly_calendar_profile`	カレンダープロファイルを設定します。 ここで、各変数は次のように定義されます。 *name* は、カレンダー プロファイルの名前を指します。
ステップ 3	**start** *start_time* **end** *end_time* 例： `Device(config-calendar-profile)# start 18:00:00 end 19:00:00`	カレンダープロファイルの開始時刻と終了時刻を設定します。 ここで、各変数は次のように定義されます。 *start_time* は、カレンダープロファイルの開始時刻です。開始時刻は **HH:MM:SS** 形式で入力する必要があります。 *end_time* は、カレンダープロファイルの終了時刻です。終了時刻は **HH:MM:SS** 形式で入力する必要があります。
ステップ 4	**recurrence monthly** 例： `Device(config-calendar-profile)# recurrence monthly`	カレンダープロファイルの月次繰り返し数を設定します。
ステップ 5	**date** *value* 例：	カレンダープロファイルの日付を設定します。

	コマンドまたはアクション	目的
	`Device(config-calendar-profile)# date 25`	（注） たとえば毎月の 2 日、10 日、25 日などの特定のタイミングでサービス拒否を実行する必要がある場合は、**date** コマンドを使用してこれら 3 日分のすべてを設定する必要があります。日付には範囲はありません。要件に従って日付を設定する必要があります。
ステップ 6	**end** 例： `Device(config-calendar-profile)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシープロファイルへの日次カレンダープロファイルのマッピング

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-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**calender-profile name** *calendar-profile-name* 例： `Device(config-wireless-policy)# calender-profile name daily_calendar_profile`	カレンダープロファイルをポリシープロファイルにマッピングします。 *calendar-profile-name* は、日次カレンダープロファイルの設定（1022ページ）で作成したカレンダープロファイルの名前です。

	コマンドまたはアクション	目的
		（注） カレンダープロファイルをポリシープロファイルに関連付ける前に、ポリシープロファイルを無効にする必要があります。次の作業を実行する必要があります。 `Device(config-wireless-policy)# shutdown`
ステップ 4	**action deny-client** 例： `Device(config-policy-profile-calender)# action deny-client`	カレンダープロファイル間隔中にクライアントセッションの確立の拒否を設定します。 （注） クライアントの関連付けは毎日、タイムスロット 9:00:00 ～ 17:00:00 の間で拒否されます。開始時刻と終了時刻の詳細については、日次カレンダープロファイルの設定（1022ページ）を参照してください。
ステップ 5	**end** 例： `Device(config-policy-profile-calender)# 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週次のカレンダープロファイルのマッピング

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-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。

	コマンドまたはアクション	目的
ステップ 3	**calender-profile name** *calendar-profile-name* 例： `Device(config-wireless-policy)# calender-profile name weekly_calendar_profile`	カレンダープロファイルをポリシープロファイルにマッピングします。 *calendar-profile-name* は、週次カレンダープロファイルの設定（1024ページ）で作成したカレンダープロファイルの名前です。 （注） カレンダープロファイルをポリシープロファイルに関連付ける前に、ポリシープロファイルを無効にする必要があります。次の作業を実行する必要があります。 `Device(config-wireless-policy)# shutdown`
ステップ 4	**action deny-client** 例： `Device(config-policy-profile-calender)# action deny-client`	カレンダープロファイル間隔中にクライアントセッションの確立の拒否を設定します。 （注） クライアントの関連付けは毎日、タイムスロット 9:00:00 ～ 17:00:00 の間で拒否されます。開始時刻と終了時刻の詳細については、週次カレンダープロファイルの設定（1024ページ）を参照してください。 月曜日と火曜日に、クライアントは通常の 9:00:00 ～ 17:00:00 の他に、17:30:00 ～ 19:00:00 の間で拒否されます。 毎月 25 日に、クライアントは通常の 9:00:00 ～ 17:00:00 の他に、18:00:00 ～ 19:00:00 の間で拒否されます。
ステップ 5	**end** 例： `Device(config-policy-profile-calender)# 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月次カレンダープロファイルのマッピング

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-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**calender-profile name** *calendar-profile-name* 例： `Device(config-wireless-policy)# calender-profile name monthly_calendar_profile`	カレンダープロファイルをポリシープロファイルにマッピングします。 *calendar-profile-name* は、月次カレンダープロファイルの設定（1025 ページ）で作成したカレンダープロファイルの名前です。
ステップ 4	**action deny-client** 例： `Device(config-policy-profile-calender)# action deny-client`	定義されたカレンダープロファイル間隔についてクライアントセッションの確立の拒否を設定します。

	コマンドまたはアクション	目的
		（注） クライアントの関連付けは毎日、タイムスロット 9:00:00 ～ 17:00:00 の間で拒否されます。開始時刻と終了時刻の詳細については、月次カレンダープロファイルの設定（1025ページ）を参照してください。 月曜日と火曜日に、クライアントは通常の 9:00:00 ～ 17:00:00 の他に、17:30:00 ～ 19:00:00 の間で拒否されます。 毎月 25 日に、クライアントは通常の 9:00:00 ～ 17:00:00 の他に、18:00:00 ～ 19:00:00 の間で拒否されます。
ステップ 5	**end** 例： `Device(config-policy-profile-calender)# 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。

カレンダープロファイルの設定の確認

カレンダープロファイル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 wireless profile calendar-profile summary
Number of Calendar Profiles: 3

Profile-Name
---------------------------------
monthly_25_profile
weekly_mon_profile
daily_calendar_profile
```

特定のプロファイル名に対するカレンダープロファイルの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless profile calendar-profile detailed daily_calendar_profile
Calendar profiles                              : daily_calendar_profile
-------------------------------------------------------------------
Recurrence                                     : DAILY
Start Time                                     : 09:00:00
End Time                                       : 17:00:00
```

ポリシープロファイルの設定の確認

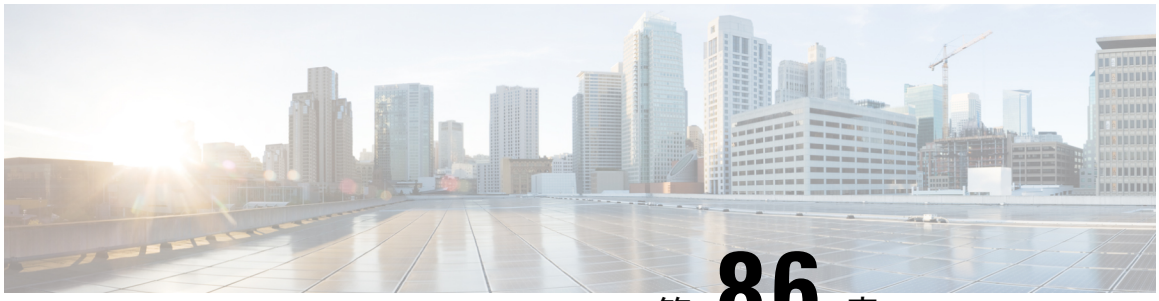
特定のポリシープロファイルに対する詳細パラメータを表示するには、次のコマンドを使用します。

```
Device# show wireless profile policy detailed default-policy-profile
Tunnel Profile
  Profile Name                        : Not Configured
Calendar Profile
  Profile Name                        : monthly_25_profile
  Wlan Enable                         : Not Configured
  Client Block                        : Client Block Configured
  ----------------------------------------------------
  Profile Name                        : weekly_mon_profile
  Wlan Enable                         : Not Configured
  Client Block                        : Client Block Configured
  ----------------------------------------------------
  Profile Name                        : daily_calendar_profile
  Wlan Enable                         : Not Configured
  Client Block                        : Client Block Configured
  ----------------------------------------------------
Fabric Profile
  Profile Name                        : Not Configured
```

ポリシープロファイルの下で設定されているカレンダープロファイル情報を表示するには、次のコマンドを使用します。

```
Device# show wireless profile policy all
Tunnel Profile
Profile Name : Not Configured
Calendar Profile
Profile Name : daily_calendar_profile
Wlan Enable : Not Configured
Client Block : Client Block Configured
----------------------------------------------------
Profile Name : weekly_calendar_profile
Wlan Enable : Not Configured
Client Block : Client Block Configured
----------------------------------------------------
Fabric Profile
Profile Name : Not Configured
```

（注） アンカーの優先順位は常にローカルとして表示されます。優先順位は、フォーリンコントローラに割り当てることができます。



第 86 章

Ethernet over GRE トンネル

EoGRE の概要

Ethernet over GRE（EoGRE）は、ホットスポットから Wi-Fi トラフィックをグループ化するための集約ソリューションです。このソリューションでは、顧客宅内機器（CPE）デバイスにおいて、エンドホストから届いたイーサネットトラフィックをブリッジし、そのトラフィックを IP Generic Routing Encapsulation（GRE）トンネルでイーサネットパケットにカプセル化できます。IP GRE トンネルがサービスプロバイダのブロードバンド ネットワーク ゲートウェイで終端すると、エンドホストのトラフィックが転送され、サブスクライバセッションが開始されます。

クライアント IPv6

WLAN の EoGRE

WLAN の EoGRE を有効にするには、ワイヤレス ポリシー プロファイルをトンネルプロファイルにマッピングする必要があります。これには次のものが含まれる可能性があります。

- AAA オーバーライド：クライアントのルールフィルタリングをバイパスできます。
- ゲートウェイ RADIUS プロキシ：トンネルゲートウェイへの AAA 要求の転送を許可します。
- トンネルルール：各レルムに使用するドメインを定義します。また、トンネルゲートウェイに向かうクライアントトラフィックの VLAN タグ付けも定義します。

• DHCP オプション 82：一連の定義済みフィールドを提供します。

複数のトンネルゲートウェイを使用した EoGRE の導入

組み込みワイヤレスコントローラは、キープアライブ ping をプライマリおよびセカンダリ トンネル ゲートウェイに送信し、失われた ping を追跡します。失われた ping について特定のしきい値レベルに達すると、スイッチオーバーが実行され、セカンダリトンネルがアクティブとしてマークされます。このスイッチオーバーによって、すべてのクライアントが認証解除され、アクセスポイント（AP）に再び参加できるようになります。プライマリトンネルがオンラインに戻ると、すべてのクライアントトラフィックがプライマリトンネルに戻されます。ただし、この動作は冗長性のタイプによって異なります。

EtherChannel でのロードバランシング

Etherchannel を介してトンネリングされるトラフィックのロードバランシングは、トンネルエンドポイントペアの送信元または宛先の IP アドレスまたは mac アドレスをハッシュすることによって機能します。トンネルの数はクライアントの数と比較すると非常に制限されるため（各トンネルは多数のクライアントのトラフィックを伝送します）、ハッシュの拡散効果が大幅に低下し、Etherchannel リンクの最適な使用率が得られなくなる可能性があります。

EoGRE 設定モデルを使用すると、各トンネルインターフェイスの *tunnel source* オプションを使用して、ロードバランシングのパラメータを調整し、複数のリンク間でトンネルを分散することができます。

トンネルごとに異なる送信元インターフェイスを使用して、送信元または宛先 IP アドレスに基づくロードバランシングを実現できます。その場合は、送信元と宛先の IP ペアごとにトラフィックフローが異なるリンクをたどるように、送信元インターフェイスの IP アドレスを選択します。次に、4 つのポートを使用した例を示します。

```
Client traffic on Tunnel1 - Src IP: 40.143.0.72  Dest IP: 40.253.0.2
Client traffic on Tunnel2 - Src IP: 40.146.0.94  Dest IP: 40.253.0.6
Client traffic on Tunnel3 - Src IP: 40.147.0.74  Dest IP: 40.253.0.10
```

特定のフローがたどるリンクを調べるには、**show platform software port-channel link-select interface port-channel 4 ipv4** *src_ip dest_ip* コマンドを使用します。

EoGRE 設定の概要

EoGRE ソリューションは、次の 2 つの異なる方法で展開できます。

• 中央スイッチング：EoGRE トンネルによって 組み込みワイヤレスコントローラがトンネルゲートウェイに接続されます。

• フレックスまたはローカルスイッチング：EoGRE トンネルは、AP で開始され、トンネルゲートウェイで終端されます。

EoGRE を設定するには、以下のタスクを実行します。

1. 一連のトンネルゲートウェイを作成します。

2. 一連のトンネルドメインを作成します。
3. クライアントをドメインに照合する方法を定義するルールを使用して、トンネルプロファイルを作成します。
4. ポリシープロファイルを作成し、トンネルプロファイルを適用します。
5. ポリシータグを使用して、WLAN にポリシープロファイルをマッピングします。

（注） 最後の測定期間に、*max-skip-count* の ping に失敗すると、セカンダリトンネルへの EoGRE トンネルフォールバックがトリガーされます。測定期間の開始および終了のインスタンスに基づいて、フォールバックには設定されている期間よりも長くかかる場合があります。

表 *45 : EoGRE* 認証方式

メソッド名	サポートされるようになった最初のリリース	モード
PSK	17.2.1	ローカル/Flex（中央認証）
開く	16.12.1	ローカル/Flex（中央認証）
LWA	16.12.1	ローカル/Flex（中央認証）
Dot1x	16.12.1	ローカル/Flex（中央認証）
CWA	16.12.1	ローカル/Flex（中央認証）

トンネルゲートウェイの作成

（注） Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラでは、トンネルゲートウェイはトンネルインターフェイスとしてモデル化されています。

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	**interface tunnel** *tunnel_number* 例： `Device(config)# interface tunnel 21`	トンネル インターフェイスを設定し、インターフェイス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	**tunnel source** *source_intf* 例： `Device(config-if)# tunnel source 22`	トンネルインターフェイスの送信元アドレスを設定します。VLAN、ギガビットイーサネット、またはループバックを送信元インターフェイスにすることができます。
ステップ 4	**tunnel destination** *tunnel-address* 例： `Device(config-if)# tunnel destination 10.11.12.13`	トンネルの宛先アドレスを設定します。
ステップ 5	**tunnel mode ethernet gre** {**ipv4** | **ipv6**} **p2p** 例： `Device(config-if)# tunnel mode ethernet gre ipv4 p2p`	GRE IPv4 を介するイーサネットまたは GRE IPv6 を介するイーサネットへのトンネルのカプセル化モードを設定します。

トンネルドメインの設定

（注） トンネルドメインは、トンネルの冗長グループです。次の設定手順では、プライマリトンネルとセカンダリトンネルを冗長モデルとともに指定します。

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。

	コマンドまたはアクション	目的
ステップ 2	**tunnel eogre domain** *domain* 例： `Device(config)# tunnel eogre domain dom1`	EoGRE 冗長ドメインを設定します。
ステップ 3	**primary tunnel** *primary-tunnel_intf* 例： `Device(config-eogre-domain)# primary tunnel 21`	プライマリトンネルを設定します。
ステップ 4	**secondary tunnel** *secondary-tunnel_intf* 例： `Device(config-eogre-domain)# secondary tunnel 22`	セカンダリトンネルを設定します。
ステップ 5	**redundancy revertive** 例： `Device(config-eogre-domain)# redundancy revertive`	冗長モデルをリバーティブとして設定します。 冗長性がリバーティブに設定されている場合、プライマリトンネルがダウンすると、セカンダリトンネルへのスイッチオーバーが実行されます。プライマリトンネルが回復すると、プライマリトンネルがセカンダリトンネルよりも優先されるため、プライマリトンネルへのスイッチオーバーが実行されます。 冗長性がリバーティブに設定されていない場合、トンネルは同じプライオリティになります。この場合、アクティブトンネルがセカンダリトンネルであると、プライマリトンネルが回復してもプライマリトンネルへのスイッチオーバーは実行されません。

EoGRE グローバルパラメータの設定

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	**tunnel eogre heartbeat interval** *interval-value* 例： `Device(config)# tunnel eogre heartbeat interval 600`	EoGRE トンネルハートビートの定期的な間隔を設定します。
ステップ 3	**tunnel eogre heartbeat max-skip-count** *skip-count* 例： `Device(config)# tunnel eogre heartbeat max-skip-count 7`	許容されるドロップハートビートの最大数を設定します。 ドロップできるハートビートの最大数に到達すると、トンネルはダウンとして宣言され、スイッチオーバーが実行されます。
ステップ 4	**tunnel eogre source loopback** *tunnel_source* 例： `Device(config)# tunnel eogre source loopback 12`	トンネル EoGRE の送信元インターフェイスを設定します。
ステップ 5	**tunnel eogre interface tunnel** *tunnel-intf* **aaa proxy key** *key key-name* 例： `Device(config)# tunnel eogre interface tunnel 21 aaa proxy key 0 mykey`	（任意）AAA プロキシ設定の AAA プロキシ RADIUS キーを設定します。 （注） トンネルゲートウェイが AAA プロキシサーバーとして動作している場合は、この手順だけが設定に必要です。

トンネル プロファイルの設定

始める前に

コントローラで宛先 VLAN を定義していることを確認してください。VLAN を定義しないと、クライアントは接続できません。

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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy-name* 例： `Device(config)# wireless profile policy eogre_policy`	WLAN ポリシープロファイルを設定します。
ステップ 3	**tunnel-profile** *tunnel-profile-name* 例： `Device(config-wireless-policy)# tunnel-profile tunnel1`	トンネルプロファイルを作成します。
ステップ 4	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**wireless profile tunnel** *tunnel-profile-name* 例： `Device(config)# wireless profile tunnel wl-tunnel-1`	ワイヤレス トンネルプロファイルを設定します。
ステップ 6	**dhcp-opt82 enable** 例： `Device(config-tunnel-profile)# dhcp-opt82 enable`	トンネリングされたクライアントに対して DHCP オプション 82 をアクティブにします。
ステップ 7	**dhcp-opt82 remote-id** *remote-id* 例： `Device(config-tunnel-profile)# dhcp-opt82 remote-id vlan`	リモート ID オプションを設定します。 **ap-mac**, **ap-ethmac**, **ap-name**, **ap-group-name**, **flex-group-name**, **ap-location**, **vlan**, **ssid-name**, **ssid-type**, **client-mac** などの、カンマ区切りのオプションリストから選択します。
ステップ 8	**aaa-override** 例： `Device(config-tunnel-profile)# aaa-override`	AAA ポリシーのオーバーライドを有効にします。
ステップ 9	**gateway-radius-proxy** 例： `Device(config-tunnel-profile)# gateway-radius-proxy`	ゲートウェイの RADIUS プロキシを有効にします。
ステップ 10	**gateway-accounting-radius-proxy** 例： `Device(config-tunnel-profile)# gateway-accounting-radius-proxy`	ゲートウェイのアカウンティング RADIUS プロキシを有効にします。

	コマンドまたはアクション	目的
ステップ 11	**rule** *priority* **realm-filter** *realm* **domain** *domain-name* **vlan** *vlan-id* 例： `Device(config-tunnel-profile)# rule 12 realm-filter realm domain dom1 vlan 5`	クライアントのネットワークアクセス識別子（NAI）、トンネリングドメイン名、および宛先 VLAN について、レルムフィルタを使用してドメインを選択するためのルールを作成します。

ワイヤレスポリシープロファイルへの WLAN の関連付け

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 eogre_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 eogre_open_eogre policy eogre_policy`	EoGRE 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。

AP へのポリシータグとサイトタグの付加

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** *mac-address* 例： `Device(config)# ap 80E8.6FD4.0BB0`	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。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag eogre_tag`	EoGRE 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 sp-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`	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。

EoGRE トンネル設定の確認

`show tunnel eogre` コマンドは、ローカルモードでの EoGRE クライアント、ドメイン、ゲートウェイ、グローバル設定、およびマネージャ情報を表示します。

ローカルモードでの EoGRE ドメイン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 tunnel eogre domain summary

Domain Name          Primary GW   Secondary GW      Active GW      Redundancy
-------------------------------------------------------------------------------
domain1              Tunnel1      Tunnel2           Tunnel1        Non-Revertive
eogre_domain         Tunnel1      Tunnel2           Tunnel1        Non-Revertive
```

ローカルモードでの EoGRE ドメインの詳細を表示するには、次のコマンドを使用します。

```
Device# show tunnel eogre domain detailed domain-name

Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
```

ローカルモードでの EoGRE トンネルゲートウェイのサマリーと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 tunnel eogre gateway summary

Name               Type  Address                                 AdminState  State
Clients
```

```
-------------------------------------------------------------------------------------------
Tunnel1            IPv4  9.51.1.11                                Up          Up      0

Tunnel2            IPv4  9.51.1.12                                Up          Down    0

Tunnel10           IPv6  fd09:9:8:21::90                          Down        Down    0

Tunnel11           IPv4  9.51.1.11                                Up          Up      0

Tunnel12           IPv6  fd09:9:8:21::90                          Up          Down    0

Tunnel100          IPv4  9.51.1.100                               Up          Down    0
```

ローカルモードでの EoGRE トンネルゲートウェイの詳細を表示するには、次のコマンドを使用します。

```
Device# show tunnel eogre gateway detailed gateway-name

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 Source : Vlan51 / 9.51.1.1
 State  : Up
 SLA ID : 56
 MTU    : 1480
 Up Time: 4 minutes 45 seconds

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
 Keepalives
  Total Number of Lost Keepalives       : 0
  Total Number of Received Keepalives   : 5
  Total Number of Transmitted Keepalives: 5
  Windows                               : 1
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window    : 2
```

ローカルモードでの EoGRE のクライアント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 tunnel eogre client summary

Client MAC      AP MAC          Domain                              Tunnel        VLAN
Local
-------------------------------------------------------------------------------------------
74da.3828.88b0  80e8.6fd4.9520  eogre_domain                        N/A           2121
No
```

ローカルモードでの EoGRE グローバル コンフィギュレーションの詳細を表示するには、次のコマンドを使用します。

```
Device# show tunnel eogre global-configuration

Heartbeat interval       : 60
```

```
Max Heartbeat skip count : 3
Source Interface         : (none)
```

ローカルモードでのグローバル トンネル マネージャ統計情報の詳細を表示するには、次のコマンドを使用します。

```
Device# show tunnel eogre manager stats global

Tunnel Global Statistics
Last Updated                     : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                       : 6
  Domains                        : 2

EoGRE Flex Objects
  AP Gateways                    : 2
  AP Domains                     : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates             : 806
  IOS Domain updates             : 88
  Global updates                 : 48
  Tunnel Profile updates         : 120
  Tunnel Rule updates            : 16
  AAA proxy key updates          : 0

AP events
  Flex AP Join                   : 1
  Flex AP Leave                  : 0
  Local AP Join                  : 0
  Local AP leave                 : 0
  Tunnel status (rx)             : 4
  Domain status (rx)             : 1
  IAPP stats msg (rx)            : 3
  Client count (rx)              : 6
  VAP Payload msg (tx)           : 4
  Domain config (tx)             : 1
  Global config (tx)             : 1
  Client delete (tx)             : 1
  Client delete per domain (tx)  : 3
  DHCP option 82 (tx)            : 4

Client events
  Add-mobile                     : 2
  Run-State                      : 3
  Delete                         : 1
  Cleanup                        : 0
  Join                           : 2
  Plumb                          : 0
  Join Errors                    : 0
  HandOff                        : 0
  MsPayload                      : 2
  FT Recover                     : 0
  Zombie GW counter increase     : 0
  Zombie GW counter decrease     : 0
  Tunnel Profile reset           : 88
  Client deauth                  : 0
  HA reconciliation              : 0

Client Join Events
  Generic Error                  : 0
  MSPayload Fail                 : 0
```

```
  Invalid VLAN                  : 0
  Invalid Domain                : 0
  No GWs in Domain              : 0
  Domain Shut                   : 0
  Invalid GWs                   : 0
  GWs Down                      : 0
  Rule Match Error              : 0
  AAA-override                  : 0
  Flex No Active GW             : 0
  Open Auth join attempt        : 2
  Dot1x join attempt            : 2
  Mobility join attempt         : 0
  Tunnel Profile not valid      : 2
  Tunnel Profile valid          : 2
  No rule match                 : 0
  Rule match                    : 2
  AAA proxy                     : 0
  AAA proxy accounting          : 0
  AAA eogre attributes          : 0
  Has aaa override              : 0
  Error in handoff payload      : 0
  Handoff AAA override          : 0
  Handoff no AAA override       : 0
  Handoff payload received      : 0
  Handoff payload sent          : 0

SNMP Traps
  Client                        : 0
  Tunnel                        : 2
  Domain                        : 0

IPC
  IOSd TX messages              : 0

Zombie Client
  Entries                       : 0
```

ローカルモードにおける特定のプロセスインスタンスのトンネルマネージャ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 tunnel eogre manager stats instance instance-number

Tunnel Manager statistics for process instance : 0
Last Updated                    : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                      : 6
  Domains                       : 2

EoGRE Flex Objects
  AP Gateways                   : 2
  AP Domains                    : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates            : 102
  IOS Domain updates            : 11
  Global updates                : 6
  Tunnel Profile updates        : 15
  Tunnel Rule updates           : 2
  AAA proxy key updates         : 0

AP events
```

```
  Flex AP Join                    : 1
  Flex AP Leave                   : 0
  Local AP Join                   : 0
  Local AP leave                  : 0
  Tunnel status (rx)              : 4
  Domain status (rx)              : 1
  IAPP stats msg (rx)             : 3
  Client count (rx)               : 6
  VAP Payload msg (tx)            : 4
  Domain config (tx)              : 1
  Global config (tx)              : 1
  Client delete (tx)              : 1
  Client delete per domain (tx)   : 3
  DHCP option 82 (tx)             : 4

Client events
  Add-mobile                      : 2
  Run-State                       : 3
  Delete                          : 1
  Cleanup                         : 0
  Join                            : 2
  Plumb                           : 0
  Join Errors                     : 0
  HandOff                         : 0
  MsPayload                       : 2
  FT Recover                      : 0
  Zombie GW counter increase      : 0
  Zombie GW counter decrease      : 0
  Tunnel Profile reset            : 11
  Client deauth                   : 0
  HA reconciliation               : 0

Client Join Events
  Generic Error                   : 0
  MSPayload Fail                  : 0
  Invalid VLAN                    : 0
  Invalid Domain                  : 0
  No GWs in Domain                : 0
  Domain Shut                     : 0
  Invalid GWs                     : 0
  GWs Down                        : 0
  Rule Match Error                : 0
  AAA-override                    : 0
  Flex No Active GW               : 0
  Open Auth join attempt          : 2
  Dot1x join attempt              : 2
  Mobility join attempt           : 0
  Tunnel Profile not valid        : 2
  Tunnel Profile valid            : 2
  No rule match                   : 0
  Rule match                      : 2
  AAA proxy                       : 0
  AAA proxy accounting            : 0
  AAA eogre attributes            : 0
  Has aaa override                : 0
  Error in handoff payload        : 0
  Handoff AAA override            : 0
  Handoff no AAA override         : 0
  Handoff payload received        : 0
  Handoff payload sent            : 0

SNMP Traps
  Client                          : 0
  Tunnel                          : 2
```

```
  Domain                          : 0

IPC
  IOSd TX messages                : 0

Zombie Client
  Entries                         : 0
```

`show ap tunnel eogre` コマンドを実行すると、flex モードでのトンネルドメイン情報、EoGRE イベント、および AP のトンネルゲートウェイのステータスが表示されます。

flex モードでの EoGRE トンネルゲートウェイのサマリー情報を表示するには、次のコマンドを使用します。

```
Device# show ap tunnel eogre domain summary

AP MAC          Domain                            Active Gateway
-------------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain                      Tunnel1
```

ワイヤレス トンネル プロファイル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 wireless profile tunnel summary

Profile Name                    AAA-Override AAA-Proxy DHCP Opt82 Enabled
------------------------------- ------------ --------- ---------- ---------
eogre_tunnel                              No        No        Yes       Yes
eogre_tunnel_set                          No        No        Yes        No
eogre_tunnel_snmp                         No        No         No        No
```

ワイヤレス トンネル プロファイルの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless profile tunnel detailed profile-name

Profile Name : eogre_tunnel
Status : Enabled
 AAA-Proxy/Accounting-Proxy: Disabled / Disabled
 AAA-Override : Disabled
 DHCP Option82 : Enabled
  Circuit-ID : ap-mac,ap-ethmac,ap-location,vlan
  Remote-ID : ssid-name,ssid-type,client-mac,ap-name

Tunnel Rules

Priority Realm                Vlan Domain (Status/Primary GW/Secondary GW)
-------- -------------------- ---- ---------------------------------------------
1        *                    2121 eogre_domain (Enabled/Tunnel1/Tunnel2)
```

EoGRE トンネルドメインのステータスに関する詳細情報を表示するには、次のコマンドを使用します。

```
Device# show ap tunnel eogre domain detailed

Domain     : eogre_domain
AP MAC     : 80e8.6fd4.9520
Active GW  : Tunnel1
```

AP の EoGRE イベントを表示するには、次のコマンドを使用します。

```
Device# show ap tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
---------------------------------------
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2       CLIENT_JOIN         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1       CLIENT_LEAVE        0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:47:33.127 1        DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4        AP_TUNNEL_STATUS     0 Tunnel2 Dn

02/18/2019 23:47:33.124 1        MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2        TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3        MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2        AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4        AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

EoGRE トンネルゲートウェイのサマリー情報を表示するには、次のコマンドを使用します。

```
Device# show ap tunnel eogre gateway summary

AP MAC          Gateway          Type  IP                                        State
Clients
-------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                                 Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                                 Down   0
```

EoGRE トンネルゲートウェイに関する詳細情報を表示するには、次のコマンドを使用します。

```
Device# show ap tunnel eogre gateway detailed gateway-name

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 State  : Up
 MTU    : 1476
 Up Time: 14 hours 25 minutes 2 seconds
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 1
 Traffic
  Total Number of Received Packets      : 6
  Total Number of Received Bytes        : 2643
  Total Number of Transmitted Packets   : 94
  Total Number of Transmitted Bytes     : 20629
  Total Number of Lost Keepalive        : 3
```

EoGRE トンネルゲートウェイのステータスに関するサマリー情報を表示するには、次のコマンドを使用します。

```
Device# show ap tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-----------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain                    Tunnel1
```

AP の EoGRE イベントに関する情報を表示するには、次のコマンドを使用します。

```
Device# show ap name ap-name tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2       CLIENT_JOIN         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1       CLIENT_LEAVE        0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:47:33.127 1        DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4        AP_TUNNEL_STATUS     0 Tunnel2 Dn

02/18/2019 23:47:33.124 1        MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2        TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3        MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2        AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4        AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

APのEoGREトンネルドメインのステータスに関するサマリー情報を表示するには、次のコマンドを使用します。

```
Device# show ap name ap-name tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-----------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain
```

AP の EoGRE トンネルドメインに関する詳細情報を表示するには、次のコマンドを使用します。

```
Device# show ap name ap-name tunnel eogre domain detailed

Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
 AdminState    : Up
```

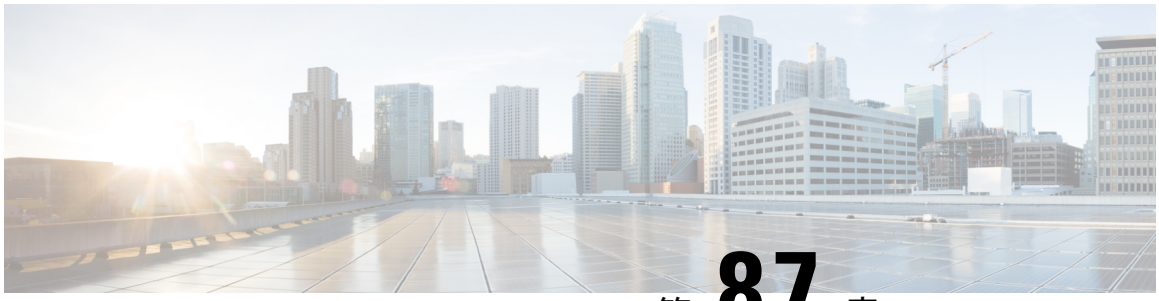
APのEoGREトンネルゲートウェイに関するサマリー情報を表示するには、次のコマンドを使用します。

```
Device# show ap name ap-name tunnel eogre gateway summary
```

```
AP MAC          Gateway          Type  IP                                      State
Clients
-------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                               Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                               Down   0
```

APのEoGREトンネルゲートウェイのステータスに関する詳細情報を表示するには、次のコマンドを使用します。

```
Device# show ap name ap-name tunnel eogre gateway detailed gateway-name

Gateway : Tunnel2
 Mode   : IPv4
 IP     : 9.51.1.12
 State  : Down
 MTU    : 0
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
  Total Number of Lost Keepalive        : 151
```



第 87 章

集中型 EoGRE を使用するゲストアンカー

集中型 EoGRE を使用するゲストアンカーの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

この機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースでも使用できます。

表 *46 :* 集中型 *EoGRE* を使用するゲストアンカーの機能履歴

リリース	機能	機能情報
Cisco IOS XE Cupertino 17.7.1	集中型 EoGRE を使用するゲストアンカー	Cisco Embedded Wireless Controller（EWC）の集中型 EoGRE 機能を備えたゲストアンカーを使用すると、ワイヤレス ゲスト クライアントにインターネットサービスを提供できます。

集中型 EoGRE を使用するゲストアンカーについて

Cisco Embedded Wireless Controller（EWC）で集中型 EoGRE 機能を備えたゲストアンカーを使用すると、ゲスト ワイヤレス クライアントにインターネットサービスを提供すると同時に、会社の内部情報やインフラストラクチャ資産を保護できます。EWC のゲストアンカー機能では、EWC プラットフォーム上のプライマリアクセスポイント（AP）とゲートウェイルーター間のトンネルとして EoGRE を使用します。クライアントトラフィックは、下位 AP からプライマリ AP に流れてから EoGRE トンネルゲートウェイに向かいます。

集中型 EoGRE を使用するゲストアンカーの注意事項と制約事項

Cisco EWC は AP およびクライアント SSO をサポートしていません。スイッチオーバー後、ゲストクライアントがクリーンアップされるため、クライアントトラフィックの中断が発生します。スイッチオーバー後にゲストクライアントが再参加してトラフィックが再確立されます。

集中型 EoGRE を使用するゲストアンカーの有効化

集中型 EoGRE を使用したゲストアンカーリングをサポートするには、次の構成を所定の順序で行います。

- 必要な設定
  1. ワイヤレスプロファイルポリシーでのワイヤレスプロファイルトンネルの設定（CLI）（1052 ページ）
  2. 中央転送の設定（CLI）（1054 ページ）
  3. ポリシープロファイルで必要な DHCP の設定（CLI）（1054 ページ）
- 推奨構成の例
  - ゲストクライアントの ACL の構成例（1055 ページ）

ワイヤレス プロファイル ポリシーでのワイヤレス プロファイル トンネルの設定（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。
ステップ 2	**wireless profile policy** *policy_profile_name* 例： `Device(config)# wireless profile policy open_policy`	ワイヤレス 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。

	コマンドまたはアクション	目的
ステップ 3	**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 4	**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 5	**ipv4 dhcp required** 例： `Device(config-wireless-policy)# ipv4 dhcp required`	FlexConnect DHCP-Required 機能を有効にします。
ステップ 6	**tunnel-profile** *tunnel-profile-name* 例： `Device(config-wireless-policy)# tunnel-profile eogre_central`	トンネルプロファイルを設定します。
ステップ 7	**vlan** *vlan-id* 例： `Device(config-wireless-policy)# vlan 2121`	VLAN 名または ID を設定します。
ステップ 8	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイルポリシーを有効にします。

中央転送の設定（GUI）

手順

ステップ 1 Cisco Embedded Wireless Controller for Catalyst Access Points の GUI から、[Configuration] > [Tags & Profiles] > [EoGRE] の順に選択します。

ステップ 2 [Tunnel Profiles] タブをクリックします。

ステップ 3 [Tunnel Profiles] タブで、[Add] をクリックします。
[Add Tunnel Profile] ウィンドウが表示されます。

ステップ 4 [Central Forwarding] トグルボタンをクリックして中央転送機能を有効にします。

ステップ 5 [Apply to Device] をクリックします。

中央転送の設定（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。
ステップ 2	**wireless profile tunnel** *tunnel-profile-name* 例： `Device(config)# wireless profile tunnel tunnel-profile-name`	ワイヤレス トンネル プロファイルを設定し、トンネル 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	**central-forwarding** 例： `Device(config-tunnel-profile)# central-forwarding`	集中型転送を有効にします。

ポリシープロファイルで必要な DHCP 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。
ステップ 2	**wireless profile policy** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-profile-name`	ポリシープロファイルを設定します。
ステップ 3	**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。

ゲストクライアントの ACL の構成例

ゲストクライアントとローカルクライアントは、同じネットワークリソースを使用します。したがって、ゲストトラフィックに関してローカル クライアント トラフィックを保護するために、デフォルトの ACL がゲストクライアントにプッシュされます。

WLAN に EoGRE ゲスト トンネル プロファイルがある場合は、ローカルサブネットへのトラフィックをブロックするデフォルトの ACL をプッシュし、ゲストクライアントのマルチキャストトラフィックをブロックする ACL をプッシュできます。

次の例は、ゲストクライアントの ACL の推奨構成を示しています。

IPv4 ACL

```
Device# configure terminal
Device(config)# ip access-list extended igmp
Device(config-ext-nacl)# 10 deny igmp any any
Device(config-ext-nacl)# 20 permit ip any any

Device(config)# wireless profile flex igmp-flex
Device(config-wireless-flex-profile)# acl-policy igmp

Device(config)# wireless tag site sp-flex-site
Device(config-site-tag)# flex-profile igmp-flex
Device(config-site-tag)# no local-site

Device# show ip access-lists
Extended IP access list igmp
    1 deny igmp any any
    2 permit ip any any
```

IPv6 ACL

```
Device(config)# wireless profile flex igmp-flex
Device(config-wireless-flex-profile)# acl-policy igmp
Device(config-wireless-flex-profile)# acl-policy mldv6

Device(config)# ipv6 access-list igmp
Device(config-ipv6-acl)# sequence 10 deny icmp any any mld-query
Device(config-ipv6-acl)# sequence 20 deny icmp any any mld-reduction
Device(config-ipv6-acl)# sequence 30 deny icmp any any mld-report
Device(config-ipv6-acl)# sequence 40 deny icmp any any mld-v2-report
Device(config-ipv6-acl)# sequence 50 permit ipv6 any any
Device(config-ipv6-acl)# acl-policy mldv6

Device# show ipv6 access-list
Extended IPv6 access list mldv6
    10 deny 58 any any
    20 deny 58 any any
    30 deny 58 any any
    40 deny 58 any any
    50 permit ipv6 any any

Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)# ipv4 acl igmp
Device(config-wireless-policy)# ipv6 acl mldv6
```

集中型 EoGRE ゲストクライアントの確認

集中型 EoGRE ゲストクライアントを確認するには、次のコマンドを実行します。

```
Device# show tunnel eogre client central-forwarding summary
Client MAC      AP MAC          Domain                                Tunnel        VLAN
-------------------------------------------------------------------------------------
74xx.38xx.88xx  0cxx.f8xx.9cxx  domain1                               N/A           2121
74xx.38xx.88xx  0cd0.f8xx.9cxx  domain1                               N/A           2121
74xx.38xx.88xx  0cd0.f8xx.9cxx  domain1                               N/A           2121
```

第 XIV 部

Bonjour 向け Cisco DNA サービス

第 88 章

Bonjour 向け Cisco DNA サービス ソリューションの概要

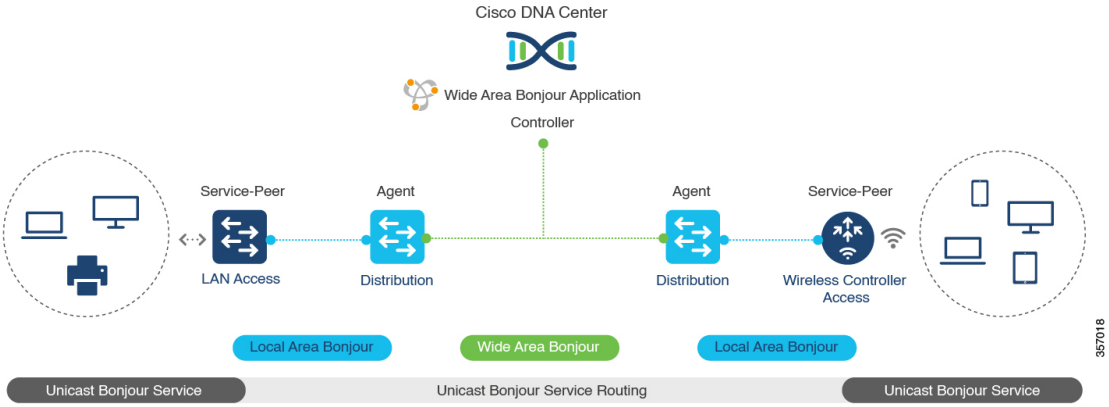
Bonjour 向け Cisco DNA サービス ソリューションについて

Apple Bonjour プロトコルは、豊富なサービスをシンプルにする設定不要のソリューションです。接続デバイス、サービス、およびアプリケーション間の直感的なエクスペリエンスを実現します。Bonjour を使用すると、最小限の介入と技術知識で、IT 管理、ピアツーピア、オーディオとビデオ、またはモノのインターネット（IoT）サービスを検出して使用できます。Bonjour の当初の設計では、ホームネットワークやブランチネットワークといった単一レイヤ 2 の中小規模のネットワークを対象にしていました。Bonjour 向け Cisco DNA サービス ソリューションは、単一のレイヤ 2 ドメインの制約を排除し、Cisco Software-Defined Access（SD-Access）や VXLAN を備えた業界標準の BGP EVPN といったオーバーレイネットワークを含む、エンタープライズグレードの従来型有線およびワイヤレスネットワークまで対応範囲を拡張します。Cisco Catalyst 9000 シリーズ LAN スイッチ、Cisco Nexus 9300 シリーズ スイッチ、および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、業界標準である RFC 6762 ベースのマルチキャスト DNS（mDNS）仕様に準拠しており、エンタープライズ ネットワーク内の互換性のあるさまざまな消費者向け有線およびワイヤレス製品との相互運用性をサポートします。

Cisco Wide Area Bonjour 上の Cisco DNA Center アプリケーションにより、mDNS サービスルーティングでは、エンタープライズグレードの有線およびワイヤレスネットワークでサービスをアドバタイズおよび検出できます。この新しい分散型アーキテクチャは、mDNS フラッド境界を排除して、ユニキャストベースのサービスルーティングに移行するように設計されており、ポリシー適用ポイントを提供し、Bonjour サービスの管理を可能にします。

次の図は、2 つの統合サービス ルーティング ドメインにおける Cisco Wide Area Bonjour アプリケーションの動作を示しています。

図 *33 : Cisco Wide Area Bonjour* ソリューションのアーキテクチャ



- **ローカルエリアサービス検出ゲートウェイドメイン - ユニキャストモード**：新しい拡張レイヤ 2 ユニキャストポリシーベースの導入モデル。レイヤ 2 ユニキャストアドレスを使用した新しい mDNS サービスの検出と配信により、フラッドフリーな LAN およびワイヤレスネットワークが実現します。レイヤ 2 モードの Cisco Catalyst スイッチおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ では、ネットワークでの新しいユニキャストベースのサービスルーティングをサポートするために、従来の flood-n-learn に代わる新しいサービスピアロールが導入されます。また、サービスピアスイッチと ワイヤレスコントローラは、mDNS flood-n-learn を、RFC 6762 mDNS 互換の有線およびワイヤレスエンドポイントとのユニキャストベースの通信に置き換えます。

- **ワイドエリアサービス検出ゲートウェイドメイン**：Wide Area Bonjour ドメインはコントローラベースのソリューションです。Cisco Catalyst および Cisco Nexus 9300 シリーズ スイッチ の Bonjour ゲートウェイのロールと役割は、単一の SDG スイッチから SDG エージェントに拡張され、単一の IP ゲートウェイを超えた Wide Area Bonjour サービスルーティングが可能になります。ネットワーク分散型 SDG エージェントデバイスにより、Cisco Wide Area Bonjour アプリケーションを実行する集中型 Cisco DNA Center コントローラとの軽量かつステートフルで信頼性の高い通信チャネルが確立されます。SDG エージェントは、エクスポートポリシーに基づいて、ローカルで検出されたサービスをルーティングします。

（注） セキュリティとロケーションベースのポリシー適用を強化するため、従来のレイヤ 2 マルチキャスト flood-n-learn は、特定の制限付きで有線およびワイヤレスネットワークで引き続きサポートされます。レイヤ 3 境界にある Cisco Catalyst および Cisco Nexus 9300 シリーズ スイッチ は、適用されたポリシーに基づいてローカルの有線またはワイヤレス VLAN 間のサービスを検出し配信するための SDG として機能します。

ソリューションのコンポーネント

Bonjour 向け Cisco DNA サービス ソリューションは、ローカルエリアおよび Wide Area Bonjour ドメイン全体でユニキャストベースのサービスルーティングを可能にする次の主要コンポーネントとシステムロールを含むエンドツーエンドソリューションです。

- **シスコサービスピア**：レイヤ 2 アクセスの Cisco Catalyst スイッチおよび シスコ ワイヤレス コントローラ はサービスピアモードで機能し、ローカル接続エンドポイントとのユニキャストベースの通信をサポートします。また、ディストリビューション層のアップストリーム Cisco Catalyst SDG エージェントにサービス情報をエクスポートします。

（注） Cisco Nexus 9300 シリーズ スイッチ は、ダウンストリームのレイヤ 2 アクセス ネットワーク デバイスによるユニキャストベースのサービスルーティングをサポートしていません。

- **Cisco SDG エージェント**：Cisco Catalyst スイッチと Cisco Nexus 9300 シリーズ スイッチ は SDG エージェントとして機能し、レイヤ 3 アクセスモードで Bonjour サービスのエンドポイントと通信します。SDG エージェントはディストリビューション層でダウンストリームのシスコサービスピアスイッチやワイヤレスコントローラ、またはレイヤ2ネットワークから情報を集約し、中央 Cisco DNA コントローラにその情報をエクスポートします。

（注） Cisco Nexus 9300 シリーズ スイッチ はマルチレイヤの LAN ユニキャスト展開モードをサポートしていません。

- **Cisco DNA コントローラ**：Cisco DNA コントローラは、ネットワーク全体に分散された信頼できる SDG エージェントを使用した Wide Area Bonjour ドメインを構築します。セキュアな通信チャネルを使用して、サービス管理の一元化とサービスルーティングの制御を実現します。
- **エンドポイント**：Bonjour エンドポイントは、RFC 6762 に準拠する Bonjour サービスをアドバタイズまたは照会する任意のデバイスです。Bonjour エンドポイントは、LAN または WLAN に配置できます。Cisco Wide Area Bonjour アプリケーションは、AirPlay、Google Chrome キャスト、AirPrint など、RFC 6762 準拠の Bonjour サービスと統合するように設計されています。

サポートされるプラットフォーム

サポートされるコントローラとサポートされるハードウェアおよびソフトウェアバージョンを次の表に示します。

表 *47 :* サポートされるコントローラとサポートされるハードウェアおよびソフトウェアバージョン

サポートされるコントローラ	ハードウェア	ソフトウェア バージョン
Cisco DNA Center アプライアンス	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	Cisco DNA Center、リリース 2.3.2.3
Cisco Wide Area Bonjour アプリケーション	—	2.4.264.12003

サポートされる SDG エージェントのライセンスとソフトウェア要件を次の表に示します。

表 *48 :* サポートされる *SDG* エージェントとサポートされるライセンスおよびソフトウェア要件

サポートされるプラットフォーム	サポートされるロール	ローカルエリア SDG	ワイドエリア SDG	最小ソフトウェア
Cisco Catalyst 9200 シリーズ スイッチ	SDG エージェント	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9200L シリーズ スイッチ	—	Unsupported	Unsupported	—
Cisco Catalyst 9300 シリーズ スイッチ	サービスピア SDG エージェント	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9400 シリーズ スイッチ	サービスピア SDG エージェント	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9500 シリーズ スイッチ	サービスピア SDG エージェント	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9500 ハイ パフォーマンス シリーズ スイッチ	サービスピア SDG エージェント	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9600 シリーズスイッチ	サービスピア SDG エージェント	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2

サポートされるプラットフォーム	サポートされるロール	ローカルエリア SDG	ワイドエリア SDG	最小ソフトウェア
Cisco Catalyst 9800 ワイヤレスコントローラ	サービスピア	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9800-L ワイヤレス コントローラ	サービスピア	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.2
Cisco Nexus 9300 シリーズ スイッチ	SDG エージェント	Cisco DNA Advantage	Cisco DNA Advantage	Cisco NX-OS リリース 10.2(3)F

サポートされるネットワーク設計

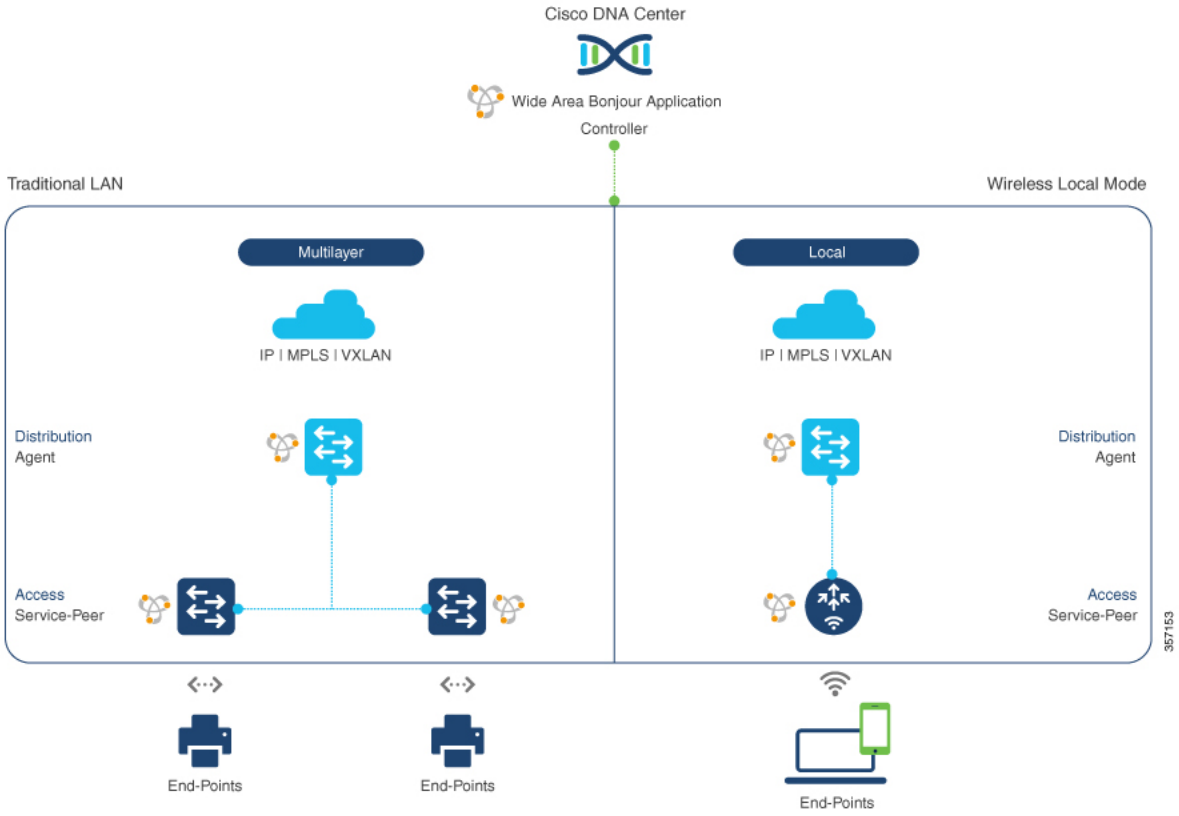
Bonjour 向け Cisco DNA サービス は、幅広いエンタープライズグレード ネットワークをサポートします。エンドツーエンドのユニキャストベース Bonjour サービスルーティングは、従来の Cisco SD-Access および BGP EVPN 対応の有線およびワイヤレスネットワークでサポートされます。

従来の有線およびワイヤレスネットワーク

従来のネットワークは、エンタープライズ ネットワークに展開される従来型の有線およびワイヤレスモードのレイヤ 2 またはレイヤ 3 です。Bonjour 向け Cisco DNA サービス は、エンドツーエンドのサービスルーティングを可能にする幅広いネットワーク設計をサポートしており、flood-n-learn ベースの導入をユニキャストモードベースのソリューションに置き換えます。

次の図は、一般的に企業で導入されている従来型の LAN と中央スイッチング ワイヤレス ローカル モード ネットワークの設計を示しています。

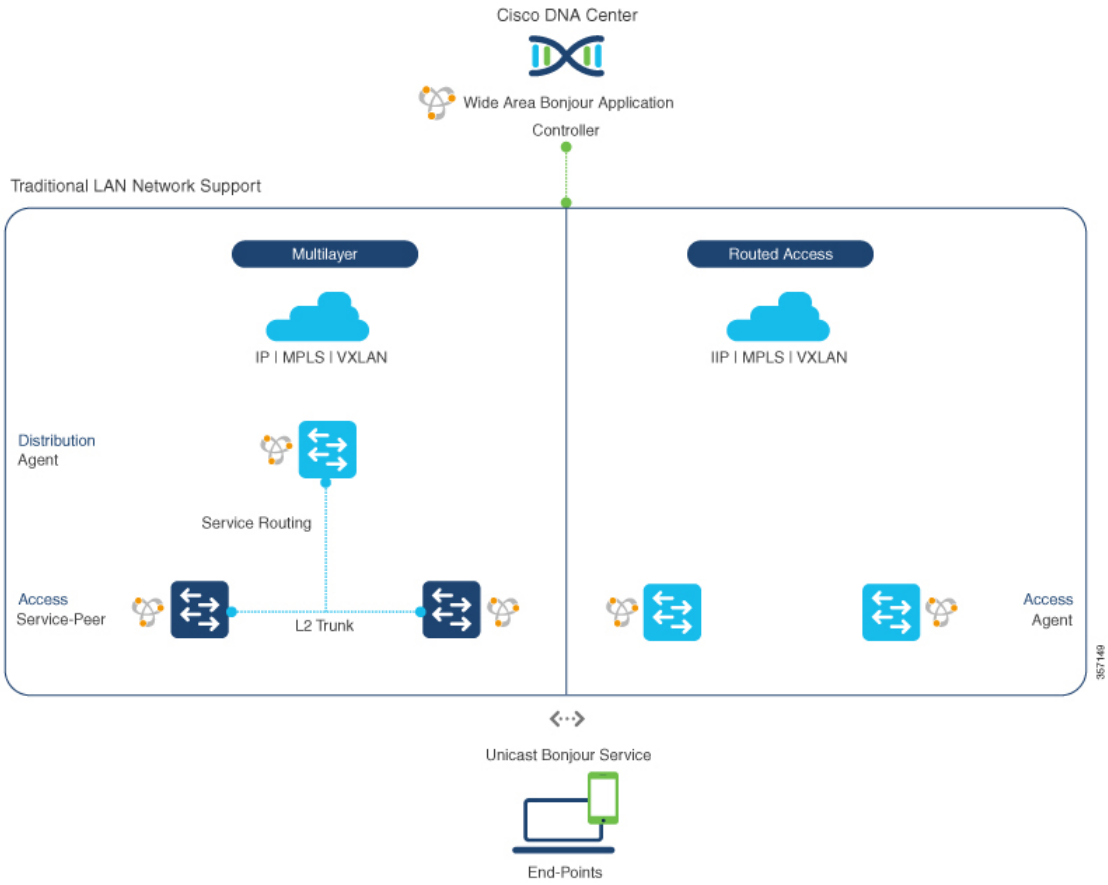
図 *34* : 企業の従来型 *LAN* およびワイヤレス ローカル モード ネットワークの設計



有線ネットワーク

次の図は、企業で一般的に導入されている、サポート対象の従来型 LAN ネットワーク設計を示しています。

図 *35* : エンタープライズ有線マルチレイヤおよびルーテッド アクセス ネットワークの設計



Bonjour ゲートウェイ機能を提供する SDG エージェントロールの Cisco Catalyst や Cisco Nexus 9300 シリーズ スイッチは、一般的に有線エンドポイントの IP ゲートウェイです。マルチレイヤネットワーク設計ではディストリビューション層、レイヤ 3 ルーテッドアクセス ネットワーク設計ではアクセス層に配置されます。

- **マルチレイヤ LAN - ユニキャストモード**：この展開モードにおいて、レイヤ 2 アクセススイッチは、ローカルに接続された有線エンドポイントにファーストホップ mDNS ゲートウェイ機能を提供します。ユニキャストモードでは、mDNS サービスはディストリビューション層のシステムにルーティングされ、IP ゲートウェイと SDG エージェントモードを提供します。SDG エージェント間のポリシーベースのサービスルーティングは、Cisco DNA Center コントローラによって実行されます。

- **マルチレイヤ LAN - Flood-n-Learn**：この展開モードでは、レイヤ 2 アクセススイッチまたは ワイヤレスコントローラ は、SDG エージェントモードで動作する Cisco Catalyst や Cisco Nexus 9300 シリーズ スイッチ を使用した mDNS パススルーモードになります。ネットワークのディストリビューション層の mDNS ゲートウェイ機能は、VLAN 間の mDNS ローカルプロキシを実現します。また、Cisco DNA Center を使用して Wide Area Bonjour ユニキャスト サービス ルーティングを確立し、単一の IP ゲートウェイを超えて mDNS サービスを検出または配信します。

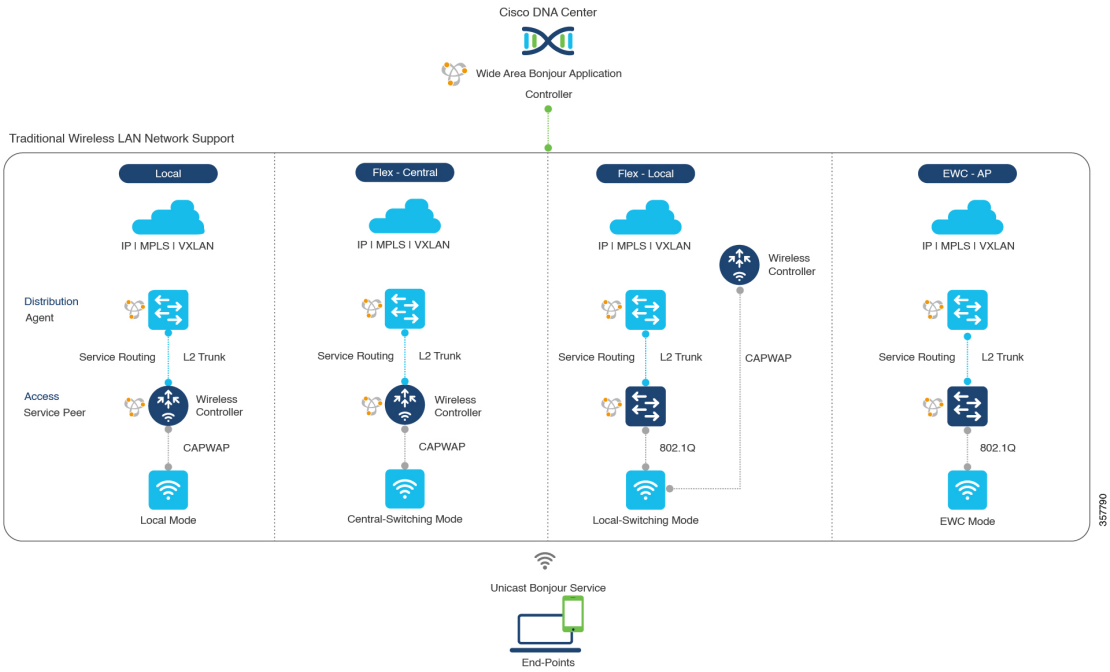
- **ルーテッドアクセス**：この展開モードでは、ファーストホップ Cisco Catalyst または Cisco Nexus 9300 シリーズ スイッチ は IP ゲートウェイ境界であるため、SDG エージェントのロールも実行する必要があります。SDGエージェント間のポリシーベースのサービスルーティングは、Cisco DNA Center コントローラによって実行されます。

無線ネットワーク

Bonjour 向け Cisco DNA サービス は、単一の ワイヤレスコントローラ mDNS ゲートウェイ機能を Wide Area Bonjour ソリューションに拡張します。Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ 上の mDNS ゲートウェイは、サービスピアとして拡張モードで展開できます。このモードでは、ワイヤレスコントローラ は、エンドツーエンドの mDNS サービス検出のために、アップストリームの Cisco Catalyst ゲートウェイスイッチを使用してユニキャスト サービス ルーティングを確立します。有線ネットワークからの従来の flood-n-learn mDNS サービが、mDNS AP などの方法を使用して置き換えられます。

次の図は、企業で一般的に導入されている、サポート対象の従来型ワイヤレスLANネットワーク設計を示しています。mDNS ゲートウェイ機能はワイヤレスネットワークの設計に基づいて、ローカルスイッチングモードで ワイヤレスコントローラ またはのアクセスポイントのファーストホップ レイヤ 2 またはレイヤ 3 イーサネットスイッチ上に配置されます。

図 *36*：企業の従来型ワイヤレス *LAN* ネットワークの設計



Bonjour 向け Cisco DNA サービス は、ワイヤレス LAN ネットワークで次のモードをサポートしています。

- **ローカルモード**：中央スイッチングワイヤレス導入モードでは、ローカルモードのシスコアクセスポイントからの m-DNS トラフィックは Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ で終端します。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、

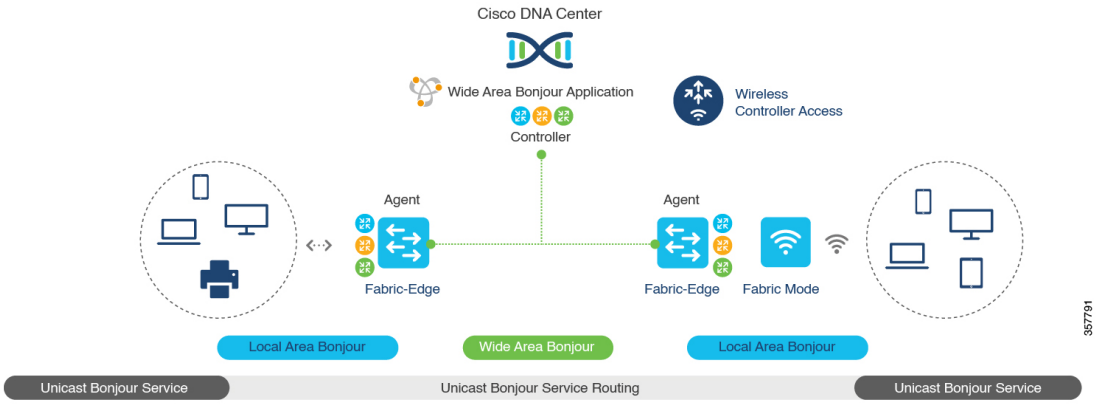
mDNS ゲートウェイ機能を新しいサービスピアモードに拡張します。ワイヤレスコントローラ は、サービスを検出してローカルのワイヤレスユーザーに配信し、IP ゲートウェイおよび SDG エージェントとして機能するディストリビューション 層のアップストリーム Cisco Catalyst スイッチへのワイヤレス管理インターフェイスを介してユニキャスト サービス ルーティングを実行できます。

- **FlexConnect - 中央**：FlexConnect 中央スイッチ SSID のシスコアクセスポイントの mDNS ゲートウェイ機能は、「**ローカルモード**」で説明されているように一貫性があります。シスコ ワイヤレス コントローラ の新しい拡張 mDNS ゲートウェイモードおよび SDG エージェントを使用したアップストリーム サービス ルーティングは、ポリシーとロケーションに基づいてネットワーク全体でサービスを検出するために一貫して動作します。
- **FlexConnect - ローカル**：FlexConnect ローカルスイッチングモードでは、mDNS ゲートウェイ サービス ピア モードのレイヤ 2 アクセススイッチが、ローカル接続した有線やワイヤレスユーザーに対してポリシーベースの mDNS ゲートウェイ機能を提供します。ディストリビューション層の Cisco Catalyst スイッチは SDG エージェントとして機能し、すべてのレイヤ 2 イーサネットスイッチ間で mDNS サービスルーティングを可能にし、LAN およびワイヤレス LAN ユーザーグループへのユニキャストベースのサービスルーティングをサポートします。
- **組み込みワイヤレスコントローラ - アクセスポイント**：サービスピアモードのレイヤ 2 アクセススイッチは、Cisco Catalyst 9100 シリーズ アクセスポイント上の Cisco Embedded Wireless Controller に関連付けられた有線およびワイヤレス エンドポイントに統合 mDNS ゲートウェイ機能を提供します。ディストリビューション層のの SDG エージェントは、mDNS フラッディングを発生させずに、レイヤ 2 ネットワークブロック内のすべてのレイヤ 2 サービスピアスイッチにユニキャスト サービス ルーティングを提供します。

Cisco SD-Access 有線およびワイヤレスネットワーク

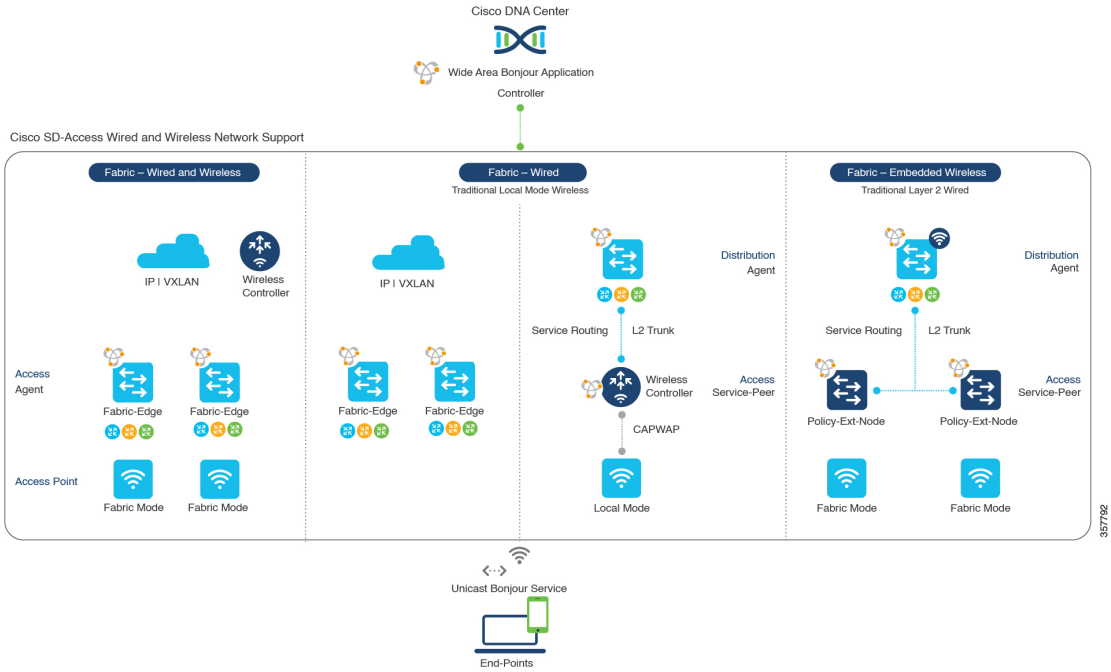
Cisco SD-Access 対応の有線およびワイヤレスネットワークでは、ファブリックネットワーク全体にわたって Bonjour 向け Cisco DNA サービス がサポートされています。Cisco Catalyst 9000 シリーズ スイッチは、仮想ネットワークにおける安全でセグメント化された mDNS サービスの検出と配信管理を実現するため、VRF に対応した Wide Area Bonjour サービスルーティングをサポートしています。VRF 対応のユニキャスト サービス ルーティングにより、レイヤ 2 のフラッディング機能を拡張する必要がなくなるため、ファブリック コア ネットワークとエンドポイントの拡張性とパフォーマンスが向上します。

図 *37 : Cisco SD-Access* 有線およびワイヤレスネットワークの設計



Cisco SD-Access は柔軟性に優れた有線およびワイヤレスネットワーク設計の代替案をサポートしているため、分散、統合され、下位互換性のある従来のネットワークインフラストラクチャをすべて管理できます。Wide Area Bonjour のサービスルーティング機能はすべてのネットワーク設計でサポートされ、直感的なユーザーエクスペリエンスを提供します。次の図は、SD-Access 対応の有線およびワイヤレスネットワーク設計のさまざまな代替案を示しています。

図 *38 : Cisco SD-Access* 有線およびワイヤレスネットワーク設計の代替案



SD-Access 対応の有線およびファブリックや従来モードのワイヤレスネットワーク向けの Bonjour 向け Cisco DNA サービスは、2 階層のサービスルーティング機能を使用して、エンドツーエンドのユニキャストベースの mDNS ソリューションを提供します。各ソリューション コンポーネントは、ネットワーク設計に基づいて、Wide Area Bonjour ドメインをサポートするために独自の役割を担っています。

- **ファブリックエッジ SDG エージェント**：SDG エージェントとして設定されたアクセス層のレイヤ 3 Cisco Catalyst ファブリックエッジスイッチは、ローカルに接続された有線およびワイヤレスエンドポイントにユニキャストベースの mDNS ゲートウェイ機能を提供します。VRF 対応の mDNS サービスポリシーは、仮想ネットワーク環境でネットワークサービスのセキュリティとセグメンテーションを提供します。mDNS サービスは、集中管理型の Cisco DNA Center を介してローカル配信およびルーティングできます。
- **ポリシー拡張ノード**：レイヤ 2 Cisco Catalyst アクセスレイヤスイッチは、レイヤ 2 ブロードキャストドメイン全体でフラッディングを発生させることのないファーストホップ mDNS ゲートウェイ機能を実現します。ディストリビューション層でのアップストリーム ファブリック エッジ スイッチを使用したユニキャスト ベースのサービス ルーティングにより、同じレイヤ 2 ネットワークブロック内で mDNS サービスのルーティングが可能になります。また、集中管理型の Cisco DNA Center からリモートサービスの検出と配布を実行することもできます。
- **シスコ ワイヤレス コントローラ** ：シスコ ワイヤレス コントローラ は次のワイヤレス導入モードに応じて独自の機能をサポートし、Cisco SD-Access 対応ネットワークで mDNS サービスのルーティングを可能にします。
  - **ファブリック対応ワイヤレス**：シスコ ワイヤレス コントローラ では、分散ファブリック対応のワイヤレス導入で、mDNS ゲートウェイ機能を有効にする必要はありません。
  - **ローカルモードワイヤレス**：シスコ ワイヤレス コントローラは中央集中型コントロールおよびデータ プレーンの終端を提供するのとともに、ワイヤレスエンドポイントにサービスピアモードで mDNS ゲートウェイを提供します。ワイヤレスコントローラは、ローカルに関連付けられたワイヤレスクライアント間に mDNS ゲートウェイを提供します。ワイヤレスコントローラ はアップストリーム SDG エージェント Catalyst スイッチを使用してサービスルーティングを構築し、ワイヤレスエンドポイントに IP ゲートウェイとサービスルーティング機能を提供します。
  - **組み込みワイヤレスコントローラ（スイッチ）**：Cisco Embedded Wireless Controller ソリューションは、Cisco Catalyst 9300 シリーズ スイッチ内で軽量の統合型 ワイヤレス コントローラ 機能を実現します。ディストリビューション層の Cisco Catalyst スイッチは、有線およびワイヤレスエンドポイントに対する SDG エージェントとして機能します。ディストリビューション層の SDG エージェントは、mDNS フラッディングを発生させずに、すべてのワイヤレスアクセスポイントおよびレイヤ 2 サービスピア スイッチにユニキャスト サービス ルーティングを提供します。
- **Cisco DNA Center コントローラ**：Cisco DNA Center 上の Cisco Wide Area Bonjour アプリケーションは、ネットワーク全体に分散するファブリックエッジスイッチ間でのポリシーおよびロケーションベースサービスの検出と配信を SDG エージェントモードでサポートします。

SDG エージェントとコントローラ間の Wide Area Bonjour 通信は、ネットワークアンダーレイを介して実行されます。SDG エージェントは、ポリシーに基づき、ファブリックアンダーレイを介して、エンドポイントのアナウンスやクエリを Cisco DNA Center に転送します。エンドポ

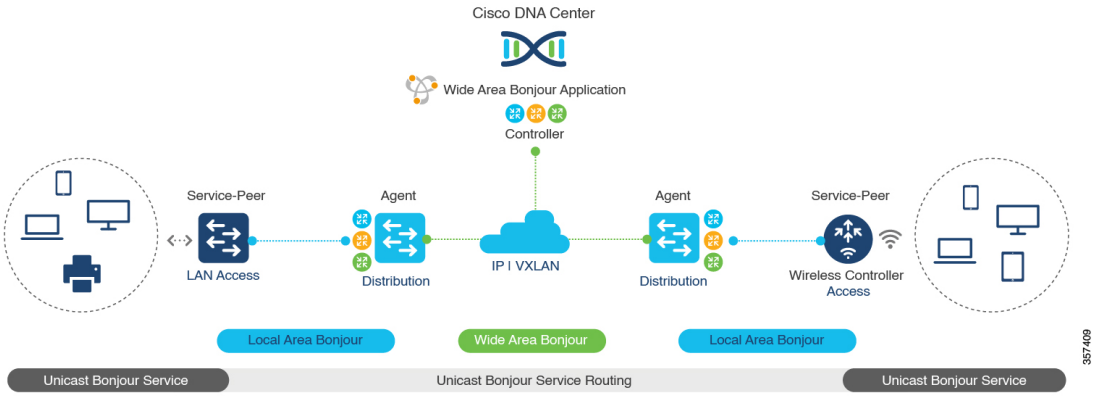
イントはサービスを検出した後、同じ仮想ネットワーク内のファブリックオーバーレイを介して直接ユニキャスト通信を確立できます。仮想ネットワーク間のユニキャスト通信は、フュージョンルータまたは外部ファイアウォールシステムを介して行われます。この通信は、オーバーレイ IP ルーティングポリシーおよびセキュリティグループタグ（SGT）ポリシーに従います。

BGP EVPN ネットワーク

BGP EVPN ベースのテクノロジーは、柔軟性のあるレイヤ 3 セグメンテーションおよびレイヤ 2 拡張オーバーレイネットワークを実現します。VRF および EVPN VXLAN 対応の Wide Area Bonjour サービスルーティングは、安全でセグメント化された mDNS サービスソリューションを提供します。オーバーレイネットワークは、EVPN 対応のレイヤ 2 拡張ネットワーク上の mDNS フラッディングを排除し、ファブリック内のレイヤ 3 でセグメント化されたルーテッドネットワークのサービス到達可能性に関する問題を解決します。

次の図は、ディストリビューション モードの BGP EVPN リーフスイッチを示しています。このスイッチは、さまざまなタイプのレイヤ 2 ネットワークおよびレイヤ 3 セグメント化 VRF 認識ネットワークを介して相互接続される BGP EVPN 対応の従来型レイヤ 2 有線アクセススイッチおよび従来型ワイヤレスローカルモードのエンタープライズネットワークに対するオーバーレイ Bonjour サービスルーティングをサポートします。

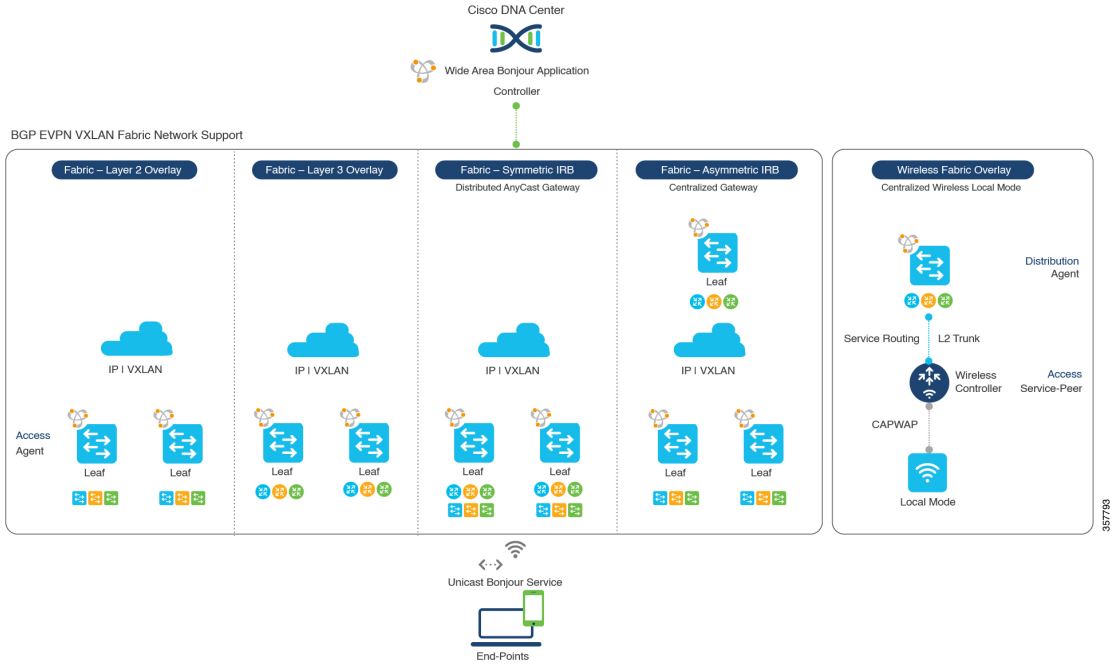
図 *39 : BGP EVPN* 対応エンタープライズ ネットワークのオーバーレイ *Bonjour* サービス



Bonjour 向け Cisco DNA サービス は、業界標準のオーバーレイネットワーク設計をすべてサポートしており、エンドツーエンドのユニキャストベースの mDNS サービスルーティングを可能にします。また、有線およびワイヤレスネットワーク全体でフラッディングとサービス境界の制限を防ぎます。

次の図は、さまざまな BGP EVPN VXLAN リファレンス オーバーレイ ネットワーク設計の代替案を示しています。このネットワーク設計により、オーバーレイ ネットワーク ポリシーに基づいたエンドツーエンドの mDNS サービスの検出と配信が可能になります。

図 *40 : BGP EVPN VXLAN* 有線およびワイヤレス設計の代替案



Cisco Catalyst および Cisco Nexus 9000 シリーズスイッチ は、幅広いオーバーレイネットワークの mDNS サービスルーティングをサポートするレイヤ 2 またはレイヤ 3 リーフロールに導入できます。どのロールでも、mDNS 通信はローカルに制限され、Wide Area Bonjour ドメイン全体でエンドツーエンドのユニキャストベースのサービスルーティングをサポートします。

- **レイヤ 2 リーフ SDG エージェント**：Cisco Catalyst または Cisco Nexus スイッチは、BGP EVPN VXLAN ファブリックネットワーク内またはそれを超えて、IP ゲートウェイを備えたエンドツーエンドのブリッジネットワークをサポートするレイヤ2 リーフとして展開できます。デフォルトでは、mDNS はファブリック対応のコアネットワーク上でブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）としてフラッディングされます。この mDNS フラッディングは、ネットワークのパフォーマンスとセキュリティに影響を与える可能性があります。SDG エージェントとして設定されているレイヤ 2 リーフは、VXLAN 上の mDNS フラッディングを防ぎ、ユニキャストベースのサービスルーティングをサポートします。

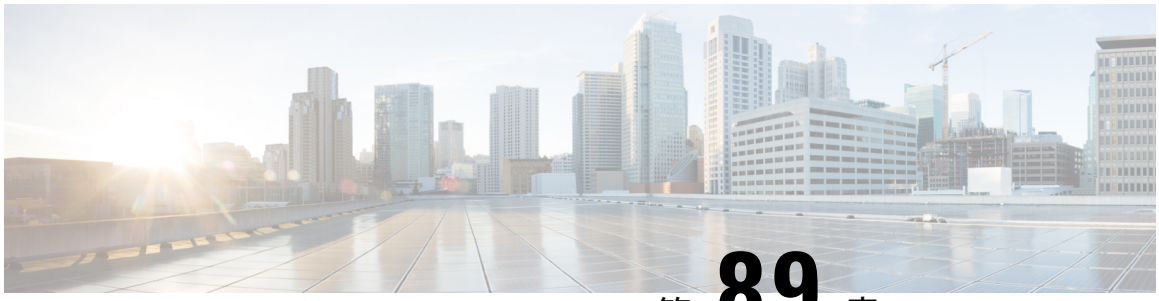
- **レイヤ 3 リーフ SDG エージェント**：Cisco Catalyst または Cisco Nexus スイッチは、BGP EVPN VXLAN ファブリック内でレイヤ 3 オーバーレイネットワークをサポートする SDG エージェントとして展開できます。IP ゲートウェイと mDNS サービスの境界は SDG エージェントスイッチで終端し、リモートサービスは集中管理型の Cisco DNA Center によって検出または配信できます。

- **ローカルモードワイヤレス**：集中管理型のワイヤレス ローカル モード ネットワークは、EVPN VXLAN ファブリック ドメインの内部または外部で終端するため、ネットワークのセグメント化とワイヤレスエンドポイントのサービス検出を保持できます。サービスピアモードの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、ディストリビューション層の IP および SDG エージェントの Cisco Catalyst スイッチを使用してユニキャスト サー

ビス ルーティングを確立し、BGP EVPN VXLAN ファブリック オーバーレイ ネットワークからサービスを検出します。

- **Cisco DNA Center**：Cisco DNA Center はレイヤ 2 またはレイヤ 3 仮想ネットワーク ID（VNID）ポリシーに基づいて mDNS サービスを動的に検出および配信し、ネットワーク内の SDG エージェントスイッチ間で mDNS サービスをルーティングする Wide Area Bonjour 機能をサポートします。

BGP EVPN ネットワークの詳細については、『Bonjour 向け Cisco DNA サービス Configuration Guide、Cisco IOS XE Bengaluru 17.6.x（Catalyst 9600 Switches）』を参照してください。



第 89 章

組み込みワイヤレスコントローラ アクセスポイント モードの Local Area Bonjour の設定

組み込みワイヤレスコントローラ アクセスポイント モードの Local Area Bonjour の概要

Cisco Embedded Wireless Controller on Catalyst Access Points では、Local Area Bonjour ネットワークドメインにユニキャストモード機能が導入されています。有線およびワイヤレスネットワークのファーストホップにおける拡張ゲートウェイ機能は、業界標準の RFC 6762 準拠のマルチキャスト DNS（mDNS）エンドポイントとレイヤ 2 ユニキャストモードで直接通信します。

Cisco Catalyst 9100 シリーズ アクセスポイント（AP）は、ローカルスイッチングモードの組み込みワイヤレスコントローラ（EWC）での分散型ワイヤレス転送をサポートします。Catalyst 9000 シリーズ LAN スイッチでは、ユニキャストモードでローカルに接続された有線エンドポ

イントとワイヤレスエンドポイントの mDNS ゲートウェイをサポートする新しいサービスピアモードが導入されています。アップストリーム SDG エージェントスイッチにより、mDNS サービスの検出と配信の境界が単一ゲートウェイからエンドツーエンドのサービスルーティングに拡張され、ネットワークでのユニキャストモード、拡張性、パフォーマンス、および復元力の向上が実現されます。

組み込みワイヤレスコントローラ アクセスポイント モードの Local Area Bonjour に関する制約事項

- EWC Cisco Catalyst 9100 シリーズ アクセスポイントの mDNS ゲートウェイは、サービスルーティングおよびユニキャストモードの mDNS 通信を可能にするサービスピアモードをサポートしていません。
- EWC Catalyst 9100 シリーズ アクセスポイントの mDNS ゲートウェイは、無効な状態にする必要があります。
- ローカルに接続されたサービスピアモードの mDNS ゲートウェイレイヤ 2 アクセススイッチから mDNS サービスの検出と配信を実行できるようにする、mDNS ブリッジングが必要です。
- サービスピアモードの Catalyst 9000 シリーズ スイッチは、EWC モードのアクセスポイントに接続されたワイヤレスユーザーおよび有線エンドポイントに対して、レイヤ 2 アクセススイッチレベルごとのロケーションベースのサービスをサポートします。

組み込みワイヤレスコントローラ アクセスポイント モードの Local Area Bonjour の前提条件

EWC AP モードのワイヤレスネットワーク用に Cisco Local Area Bonjour を実装する前に、EWC モードの Cisco Catalyst 9100 シリーズ アクセスポイントを正しく設定して動作させる必要があります。

EWC モードの AP、およびサービスピアモード（有線ユーザーとワイヤレスユーザー向けの mDNS ゲートウェイをサポート）で展開されたレイヤ 2 アクセス Cisco Catalyst 9000 シリーズ スイッチで検証された前提条件を以下に示します。

- EWC モードの Cisco Catalyst 9100 シリーズ アクセスポイントは、ワイヤレスネットワークおよびその他の高度なパラメータを実装するように事前設定されている必要があります。詳細については、『Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide』を参照してください。
- EWC モードの Cisco Catalyst 9100 シリーズ アクセスポイントでは、推奨される IOS-XE ソフトウェアバージョンを実行できます。EWC モードの AP では、Local Area Bonjour ゲー

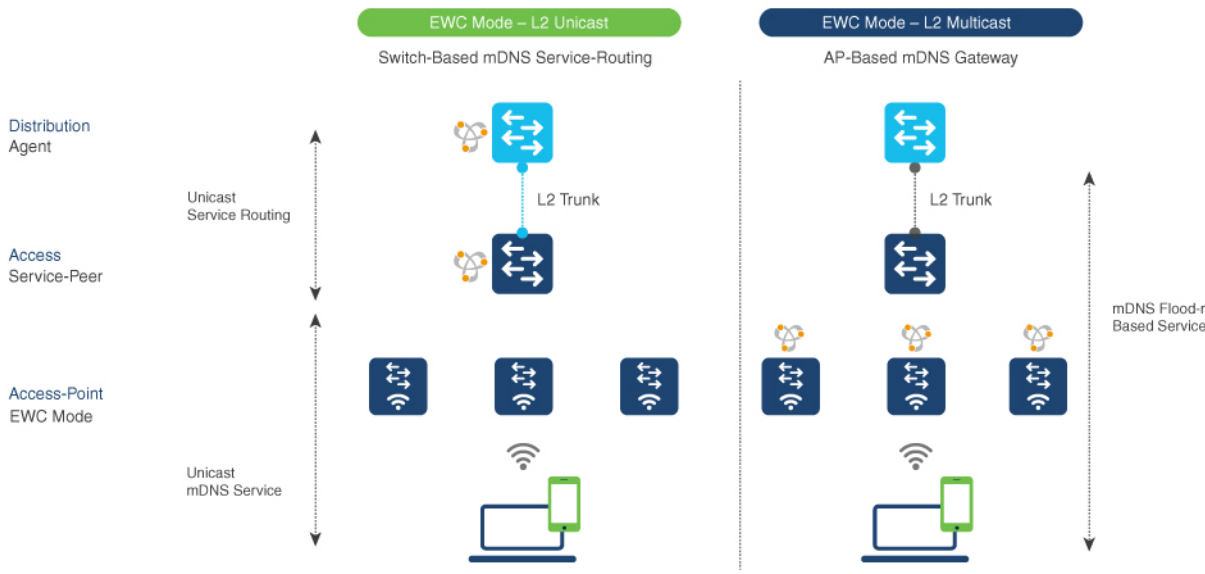
トウェイを有効にするために、mDNS の要件とソフトウェアバージョンの依存関係はありません。

- サービスピアロールの対象となるコントローラで必要な Cisco IOS XE ソフトウェアバージョンが実行されていることを確認します。
- 有効な Cisco DNA-Advantage ライセンスがコントローラで実行されていることを確認します。
- SDG エージェントモードのアップストリーム ディストリビューション層 Cisco Catalyst スイッチで有効な Cisco DNA-Advantage ライセンスが実行されていることを確認します。
- ディストリビューション層の SDG エージェントとコントローラサービスピアとの間でレイヤ 2 ユニキャスト サービスルーティングが実行されている場合、マルチレイヤネットワークでコントローラがレイヤ2 トランクとして相互接続されていることを確認します。
- IPv4 サブネット（スイッチ管理 IP ネットワーク）を介して Catalyst 9000 アクセスレイヤスイッチから SDG エージェントモードのアップストリーム Cisco Catalyst 9000 シリーズスイッチに IP 到達可能であることを確認します。

EWC モードの mDNS ゲートウェイの代替手段について

Cisco Catalyst コントローラは、エンタープライズ ネットワークの進化するビジネス上および技術上の要件に対応するために、mDNS ゲートウェイ機能を継続的に革新しています。EWC モードのアクセスポイントベースのワイヤレスネットワークでは、以下の図に示すように、2 つの方法を使用して mDNS ゲートウェイを実装できます。

図 *41 : EWC* モードのアクセスポイントの *mDNS* ゲートウェイの代替手段



EWC モードのアクセスポイントのワイヤレスネットワーク用の mDNS ゲートウェイを、ネットワーク運用環境に基づいて次のいずれかのモードで実装し、サービスの検出と配信に対応できます。

- **スイッチベースの mDNS ゲートウェイ**：レイヤ 2 アクセスの Catalyst 9000 シリーズ スイッチは、サービスピアロールの mDNS ゲートウェイとして実装できます。これには、次の主な利点があります。
  - flood-n-learn を、ローカルに接続された有線ユーザーおよび EWC モードのアクセスポイントのワイヤレスユーザーとの新しい強化されたユニキャストベースの mDNS 通信に置き換えます。
  - Catalyst 9000 は、LAN ディストリビューションへのユニキャスト サービスルーティングにより、mDNS フラッドを排除します。LAN ディストリビューション層とレイヤ 2 アクセス層のスイッチ間のユニキャスト サービスルーティングは、Local Area Bonjour ドメインを形成して、ポリシーおよびロケーションベースのサービスの検出と配信を可能にします。レイヤ 2 トランクを介したユニキャストベースのサービスルーティングにより、mDNS フラッドが排除され、サービス指向の有線およびワイヤレスネットワークが実現されます。
  - スイッチベースの mDNS ゲートウェイソリューションでは、有線ネットワークのトラフィックをワイヤレス AP に転送する必要がなくなり、ワイヤレスの拡張性、パフォーマンス、ネットワークの信頼性が向上します。
- **AP ベースの mDNS ゲートウェイ**：Cisco EWC モードのアクセスポイントは、サポートされていない LAN アクセススイッチに接続されている場合に mDNS ゲートウェイとして代わりに実装できます。この従来の方法では、mDNS サービスの検出と配信は、レイヤ 2 の有線およびワイヤレスネットワーク上の flood-n-learn のメカニズムに従います。AP ベースの mDNS ゲートウェイを実装するには、『Cisco Embedded Wireless Controller Configuration Guide, Release 17.3.1』のマルチキャスト ドメイン ネーム システムに関する章を参照してください。

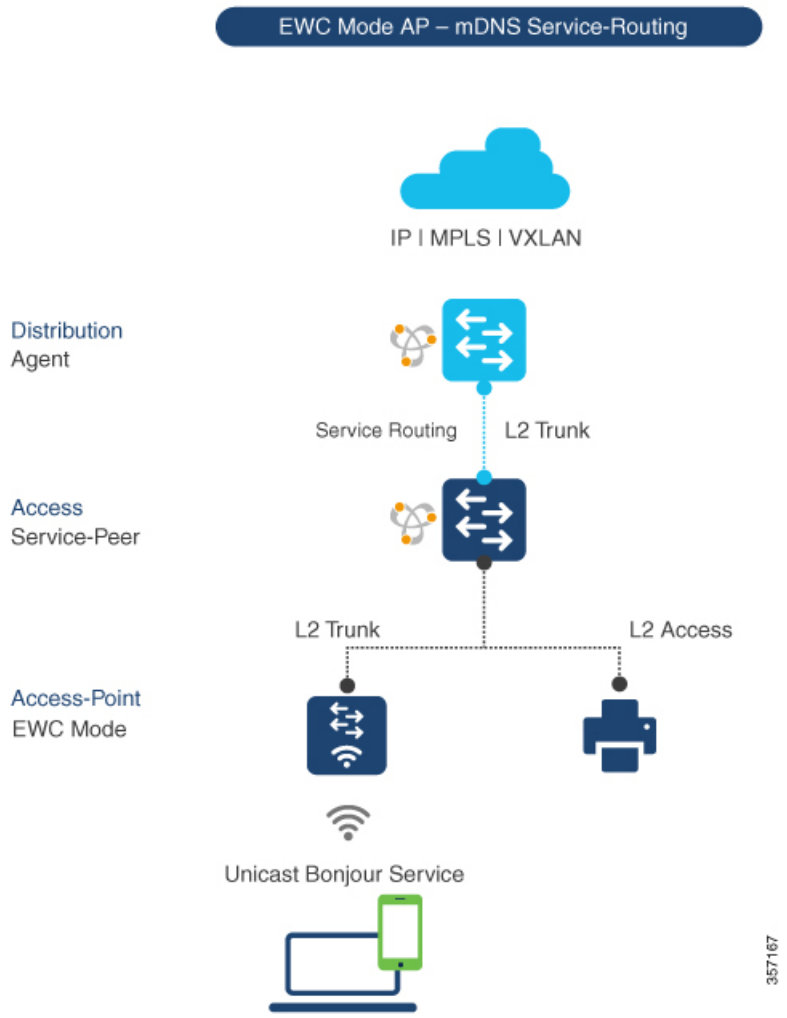
組み込みワイヤレスコントローラ アクセスポイントモードの Local Area Bonjour について

Cisco Catalyst LAN スイッチおよび WLC は、各種の有線ネットワークとワイヤレスネットワークに対応するさまざまな進歩を備えた mDNS ゲートウェイ機能をサポートしています。企業の要件拡大に合わせて、IT 部門は新しいネットワーク導入モデルを採用し、モバイルデバイスや設定不要の分散型サービスをサポートして、ミッションクリティカルなネットワークの拡張性、きめ細かいセキュリティ管理、復元力を向上させています。Catalyst 9000 シリーズ LAN スイッチと EWC モードの Catalyst 9100 シリーズ アクセスポイント全体にわたる共通の統合 Cisco IOS-XE オペレーティングシステムは、ネットワークエッジで分散型 Bonjour ゲートウェイ機能を実現します。この新しいソリューションでは、エンドツーエンドの Wide Area Bonjour

サービスルーティングを使用して、直感的なユーザー体験を備えたサービス指向のエンタープライズ ネットワークが実現されます。

次の図は、ローカルに接続されたEWCモードのワイヤレスユーザーと有線ユーザーへのmDNSゲートウェイ機能をサポートする EWC モードのアクセスポイントに接続された Cisco Catalyst 9000 シリーズ スイッチを示しています。

図 *42 : Cisco Catalyst* スイッチと *EWC* モードのアクセスポイント



レイヤ 2 アクセス層とレイヤ 3 ディストリビューション層の Cisco Catalyst 9000 シリーズ スイッチは、同じレイヤ 2 ネットワークブロック内の有線ユーザーと EWC モードのアクセスポイントモードのワイヤレスユーザー間でユニキャストベースの mDNS サービスルーティングを有効にするために、次の mDNS ゲートウェイモードで設定する必要があります。

- **サービスピア**：EWC モードのワイヤレスアクセスポイントに接続するレイヤ 2 アクセススイッチは、サービスピアモードの mDNS ゲートウェイを使用して設定する必要があります。各レイヤ 2 アクセススイッチは、ローカルに接続された有線ユーザーと EWC モードのアクセスポイントのワイヤレスユーザーの間に mDNS ゲートウェイ機能を提供しま

す。同じまたは異なる VLAN 内でのユニキャストベースの mDNS サービスの検出と配信は、単一のレイヤ 2 アクセススイッチ上の双方向 mDNS ポリシーでサポートされます。

- **SDG エージェント**：レイヤ 2 ネットワークの mDNS flood-n-learn ベース方式は、サービスピアモードのレイヤ 2 アクセススイッチと mDNS ゲートウェイ SDG エージェントモードのアップストリームディストリビューション層との間のシンプルなユニキャストベースのサービスルーティングに置き換えられます。ユニキャストベースの mDNS サービスルーティングにより、レイヤ 2 トランクポートでの mDNS フラッドが排除され、有線ネットワークと EWC モードのアクセスポイントのワイヤレスネットワークにおける帯域幅の増加、セキュリティの強化、ロケーションベースのサービス、フラッド制御管理が実現されます。

組み込みワイヤレスコントローラ アクセスポイント モードの Local Area Bonjour の設定

このトピックでは、レイヤ 2 アクセス層 Cisco Catalyst 9000 シリーズ スイッチを mDNS ゲートウェイとして実装し、レイヤ2アクセス層スイッチでのサービスピアと SDG エージェントモードを有効にするための構成手順について説明します。複数のレイヤ 2 アクセススイッチ間で mDNS サービスの検出と配信を有効にするには、SDG エージェントモードのアップストリーム ディストリビューション層 Cisco Catalyst 9000 シリーズ スイッチでサービスルーティングを有効にして、Local Area Bonjour サービス ルーティング ドメインを構築する必要があります。

（注） mDNS ゲートウェイは、EWC モードの Catalyst 9100 シリーズ アクセスポイントでグローバルに無効にする必要があります。

mDNS ゲートウェイモードの設定（CLI）

レイヤ 2 アクセススイッチで mDNS ゲートウェイとサービスピアモードを有効にし、レイヤ 3ディストリビューション層スイッチで SDG エージェントモードを有効にするには、以下の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**mdns-sd gateway** 例： `Device(config)# mdns-sd gateway`	レイヤ 2 Catalyst スイッチで mDNS を有効にし、mDNS ゲートウェイ コンフィギュレーション モードを開始します。 （オプション）次の追加のパラメータを設定できます。 • **air-print-helper**：iPhone や iPad などの Apple iOS デバイス間の通信を有効にして、ドライバレス AirPrint 機能をサポートしていない古いプリンタを使用します。 • **cache-memory-max** ：キャッシュのメモリの割合を設定します。 • **ingress-client**：入力クライアントのパケットチューナーを設定します。 • **rate-limit**：着信 mDNS パケットのレート制限を有効にします。 • **service-announcement-count**：最大アドバタイズメント数を設定します。 • **service-announcement-timer** ：アドバタイズメント アナウンス タイマーの周期を設定します。 • **service-query-count**：最大クエリ数を設定します • **service-query-timer**：クエリ転送タイマーの周期を設定します • **service-type-enumeration**：サービスの列挙を設定します。

	コマンドまたはアクション	目的
		（注） **cache-memory-max**、**ingress-client**、**rate-limit**、**service-announcement-count**、**service-announcement-timer**、**service-query-count**、**service-query-timer**、**service-type-enumeration** コマンドの場合、一般的な展開に関する各パラメータのデフォルト値を保持できます。必要に応じて、特定の展開の場合は異なる値を設定します。
ステップ 4	**mode** {**service-peer** | **sdg-agent**} 例： `Device(config-mdns-sd)# mode service-peer`	システム設定に基づいて、次のいずれかのモードで mDNS ゲートウェイを設定します。 • **Service-Peer**：mDNS サービスピアモードでレイヤ 2 Catalyst アクセススイッチを有効にします。 • **SDG Agent**：デフォルト。SDG エージェントモードのレイヤ 3 ディストリビューション層 Catalyst スイッチが、Wide Area Bonjour サービスルーティングのために中央 Cisco DNA Center コントローラとピアリングできるようにします。
ステップ 5	**exit** 例： `Device(config-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

mDNS サービスポリシーの設定（CLI）

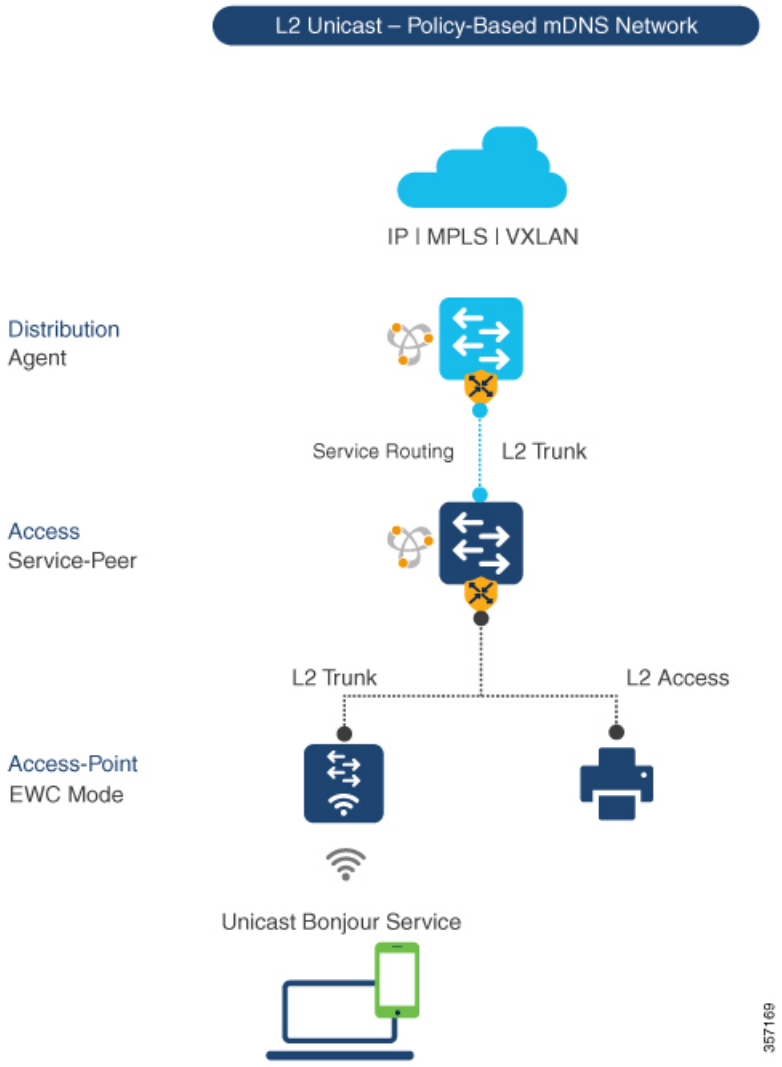
mDNS サービスポリシーを設定するには、以下の手順に従います。

1. 組み込みサービスタイプまたはユーザー定義のカスタムサービスタイプを許可するサービスリストを作成します。
2. サービスリストをサービスポリシーに関連付けて、入力または出力方向に適用します。
3. 新しい VLAN コンフィギュレーション モードにサービスポリシーを適用します。

（注） レイヤ 2 Catalyst スイッチの場合はサービスピアモードで、レイヤ 3 Catalyst スイッチの場合は SDG エージェントモードで、この構成を行う必要があります。

次の図は、サービスピアモードと SDG エージェントモードの Catalyst スイッチで mDNS ポリシーを設定する方法を示しています。

図 *43 : Catalyst* サービスピアおよび *SDG* エージェントの *mDNS* サービスポリシーの構成



サービスピアモードと SDG エージェントモードでサービスポリシーを構築してターゲット VLAN に適用するには、以下の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**mdns-sd service-list** *service-list-name* {**in** | **out**}
	例：
	`Device(config)# mdns-sd service-list VLAN100-LIST-IN in`
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
		mDNS サービスリストを設定して、1 つ以上のサービスタイプを分類します。固有のサービスリストは、着信 mDNS メッセージと、要求側のローカルに接続された有線エンドポイントまたは EWC モードのアクセスポイントのエンドポイントへのアウトバウンド応答を処理するために必要です。

ステップ 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
	例：
	`Device(config)# mdns-sd service-list VLAN100-LIST-IN in`
	`Device(config-mdns-sl-in)# match APPLE-TV`
	`Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`
		インバウンドサービスリストに一致します。
		Catalyst スイッチは、検証を行い、ローカルに接続された有線エンドポイントまたは EWC モードのアクセスポイントのワイヤレスエンドポイントからの着信 mDNS サービスタイプ（Apple TV など）のアドバタイズメントまたはクエリ一致メッセージタイプを受け入れるかドロップします。サービスリストの最後に暗黙的な拒否が含まれています。
		デフォルトの message-type は **any** です。

ステップ 5	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
	例：
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
	`Device(config-mdns-sl-in)# match APPLE-TV`
	`Device(config-mdns-sl-in)# match PRINTER-IPPS`
		アウトバウンドサービスリストに一致します。
		Catalyst スイッチは、要求側エンドポイントに一致するサービスタイプで応答することで、ローカルサービスプロキシ機能を提供します。たとえば、VLAN 100 から学習した Apple-TV とプリンタは、同じ VLAN 100 の EWC モードのアクセスポイントのワイヤレスエンド

	コマンドまたはアクション	目的
		ポイントに配信されます。サービスリストの最後に暗黙的な拒否が含まれています。 アウトバウンドサービスリストのメッセージタイプは必要ありません。
ステップ 6	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy VLAN100-POLICY`	グローバル コンフィギュレーション モードで固有の mDNS サービスポリシーを作成します。

ステップ 7	**service-list** *service-list-name* {**in** | **out**}
	例：
	`Device(config)# mdns-sd service-policy VLAN100-POLICY`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-IN in`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-OUT out`
		各方向のサービスリストに関連付ける mDNS サービスポリシーを設定します。

ステップ 8	**vlan configuration** *ID* 例： `Device(config)# vlan configuration 100`	詳細なサービスパラメータの有線ユーザーまたは EWC モードのアクセスポイントのユーザーの VLAN 構成を有効にします。同じ設定に対して 1 つ以上の VLAN を作成できます。 この *ID* は VLAN 構成 ID を指します。たとえば、*vlan configuration 101-110,200* のように範囲を指定すると、連続する VLAN ID と連続しない VLAN ID を設定できます。
ステップ 9	**mdns-sd gateway** 例： `Device(config-vlan)# mdns-sd gateway`	設定した有線ユーザーまたはEWCモードのアクセスポイントのワイヤレスユーザーの VLAN ID で mDNS ゲートウェイを有効にします。
ステップ 10	**service-policy** *service-policy-name* 例： `Device(config-vlan-mdns)# service-policy VLAN100-POLICY`	設定した有線ユーザーまたはEWCモードのアクセスポイントのワイヤレスユーザーの VLAN ID に mDNS サービスポリシーを関連付けます。
ステップ 11	**exit** 例：	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

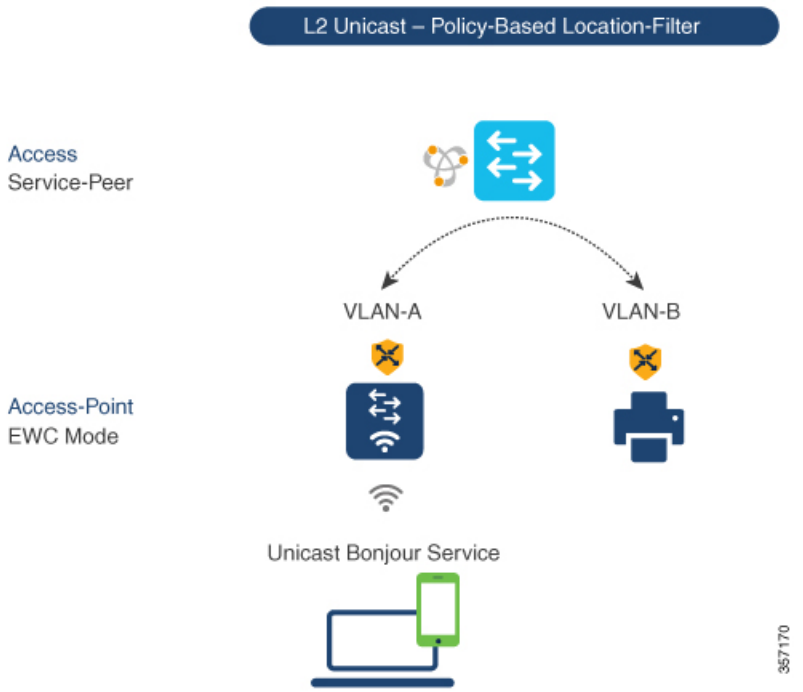
	コマンドまたはアクション	目的
	`Device(config-vlan-mdns)# exit`	

mDNS ロケーションフィルタの設定（CLI）

サービスピアモードのレイヤ 2 Cisco Catalyst アクセスレイヤスイッチは、デフォルトで、mDNS サービスプロバイダーと、有線またはワイヤレス EWC モードのアクセスポイント ユーザー ネットワークに関連付けられた同じレイヤ 2 VLAN に接続されている受信者との間に、ローカルサービスプロキシを提供します。必要に応じ、mDNS ロケーションフィルタを設定して、有線またはワイヤレス EWC モードのアクセスポイントユーザー ネットワークに関連付けられたローカル設定の VLAN ID 間でサービスの検出と配信を行うこともできます。

次の図は、有線およびワイヤレス EWC モードのアクセスポイント ユーザー VLAN 間での mDNS サービスの検出と配信を許可する、サービスピアモードの Catalyst スイッチ上のロケーションフィルタ ポリシーを示しています。

図 *44 : Catalyst* サービスピア *mDNS* ロケーションフィルタ構成



サービスピアモードの Cisco Catalyst スイッチでローカルサービスプロキシを有効にし、ローカルの有線ユーザーと EWC モードのアクセスポイントのワイヤレスユーザーの VLAN 間で mDNS サービスを検出するには、以下の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**mdns-sd location-filter** *location-filter-name* 例： `Device(config)# mdns-sd location-filter LOCAL-PROXY`	グローバル コンフィギュレーション モードで一意のロケーションフィルタを設定します。

ステップ 4	**match location-group** {**all** | **default** | **ID**} **vlan** [*ID*]
	例：
	`Device(config-mdns-loc-filter)# match location-group default vlan 100`
	`Device(config-mdns-loc-filter)# match location-group default vlan 101`
		グループ化された VLAN 間で許可されたサービスを相互に配信する一致基準を設定します。たとえば、EWC モードのアクセスポイントのワイヤレスユーザー VLAN ID 100 と有線ユーザー VLAN ID 101 の間でユニキャストモードを使用して、mDNS サービスを検出および配信できます。

ステップ 5	**mdns-sd service-list** *service-list-name* {**in** | **out**} 例： `Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`	mDNS サービスリストを設定して、1 つ以上のサービスタイプを分類します。 固有のサービスリストは、着信 mDNS メッセージと、要求側の有線ユーザーエンドポイントまたは EWC モードのアクセスポイントのユーザーエンドポイントへのアウトバウンド応答を処理するために必要です。

ステップ 6	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
	例：
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
	`Device(config-mdns-sl-out)# match APPLE-TV location-filter LOCAL-PROXY`
		ロケーションフィルタを 1 つ以上のサービスタイプに関連付けて、ローカル VLAN 間のローカルプロキシを有効にします。たとえば、VLAN 100 と VLAN 101 から学習した Apple-TV は、VLAN 100 の受信者に配信されます。

	コマンドまたはアクション	目的
		（注） サービスリストの最後に暗黙的な拒否が含まれています。 アウトバウンドサービスリストの場合、**message-type** は必要ありません。
ステップ 7	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy VLAN100-POLICY`	グローバル コンフィギュレーション モードで固有の mDNS サービスポリシーを作成します。

ステップ 8	**service-list** *service-list-name* {**in** | **out**}
	例：
	`Device(config)# mdns-sd service-policy VLAN100-POLICY`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-OUT out`
		各方向のサービスリストに関連付ける mDNS サービスポリシーを設定します。

ステップ 9	**vlan configuration** *ID* 例： `Device(config)# vlan configuration 100`	詳細なサービスパラメータの VLAN 設定を有効にします。同じ設定を使用して 1 つ以上の VLAN を作成できます。 この *ID* は VLAN 構成 ID を指します。たとえば、*vlan configuration 101-110,200* のように範囲を指定すると、連続する VLAN ID と連続しない VLAN ID を設定できます。
ステップ 10	**mdns-sd gateway** 例： `Device(config-vlan-config)# mdns-sd gateway`	設定した VLAN ID で mDNS ゲートウェイを有効にします。
ステップ 11	**service-policy** *service-policy-name* 例： `Device(config-vlan-mdns-sd)# service-policy VLAN100-POLICY`	設定した VLAN ID に mDNS サービスポリシーを関連付けます。
ステップ 12	**exit** 例： `Device(config-vlan-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

カスタムサービス定義の設定（CLI）

Cisco IOS-XE は、主要な mDNS PTR レコードとわかりやすい名前にマッピングされる、さまざまな組み込み mDNS サービス定義のタイプをサポートしています。たとえば、組み込みの Apple-TV サービスタイプは、ネットワーク内のサービスを正常に有効にするために、_airplay._tcp.local および _raop._tcp.local PTR レコードに関連付けられます。ネットワーク管理者は、一致する mDNS PTR レコードを使用してカスタムサービス定義を作成し、ネットワークで mDNS サービスルーティングを有効にできます。

カスタムサービス定義をサービスリストに関連付けるには、以下の手順に従います。

手順

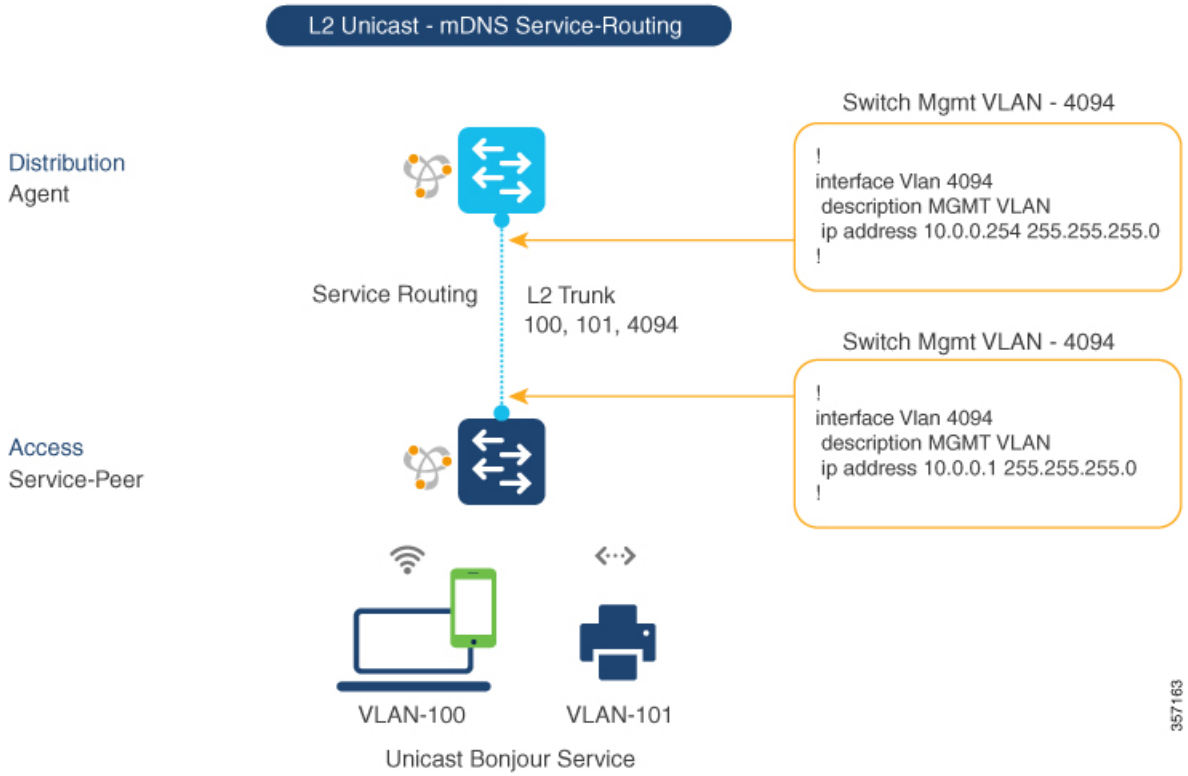
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mdns-sd service-definition** *service-definition-name* 例： `Device(config)# mdns-sd service-definition APPLE-CLASSROOM`	カスタムサービスタイプの一意のサービス定義名を作成します。
ステップ 4	**service-type** *custom-mDNS-PTR* 例： `Device(config-mdns-ser-def)# service-type _classroom._tcp.local`	カスタム mDNS ポインタ（PTR）レコードの正規表現文字列を設定します。
ステップ 5	**exit** 例： `Device(config-mdns-ser-def)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

サービスピアでのサービスルーティングの設定（CLI）

サービスピアモードのレイヤ 2 Cisco Catalyst スイッチは、SDG エージェントモードのアップストリームディストリビューション層スイッチでサービスルーティングを構築します。レイヤ 2 Cisco Catalyst スイッチでサービスルーティングを構築するには、アップストリームの SDG エージェント Catalyst スイッチに到達するための有効な IP アドレスを持つ少なくとも 1 つのインターフェイスが必要です。スイッチ管理ポートはサポートされていません。

次の図は、サービスピアモードのアクセスレイヤ Catalyst スイッチと SDG エージェントモードのディストリビューション層 Catalyst スイッチ間のレイヤ 2 トランクを介したユニキャストベースのサービスルーティングを有効にするトポロジを示しています。

図 *45 : Catalyst* サービスピア サービスルーティング構成



サービスピアモードの Cisco Catalyst スイッチでサービスルーティングを有効にし、mDNS 信頼インターフェイスの設定をセットアップするには、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	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**vlan configuration** *ID* 例： `Device(config)# vlan configuration 100`	詳細なサービスパラメータの有線ユーザーと EWC モードの AP ワイヤレスユーザーの VLAN 構成を有効にします。

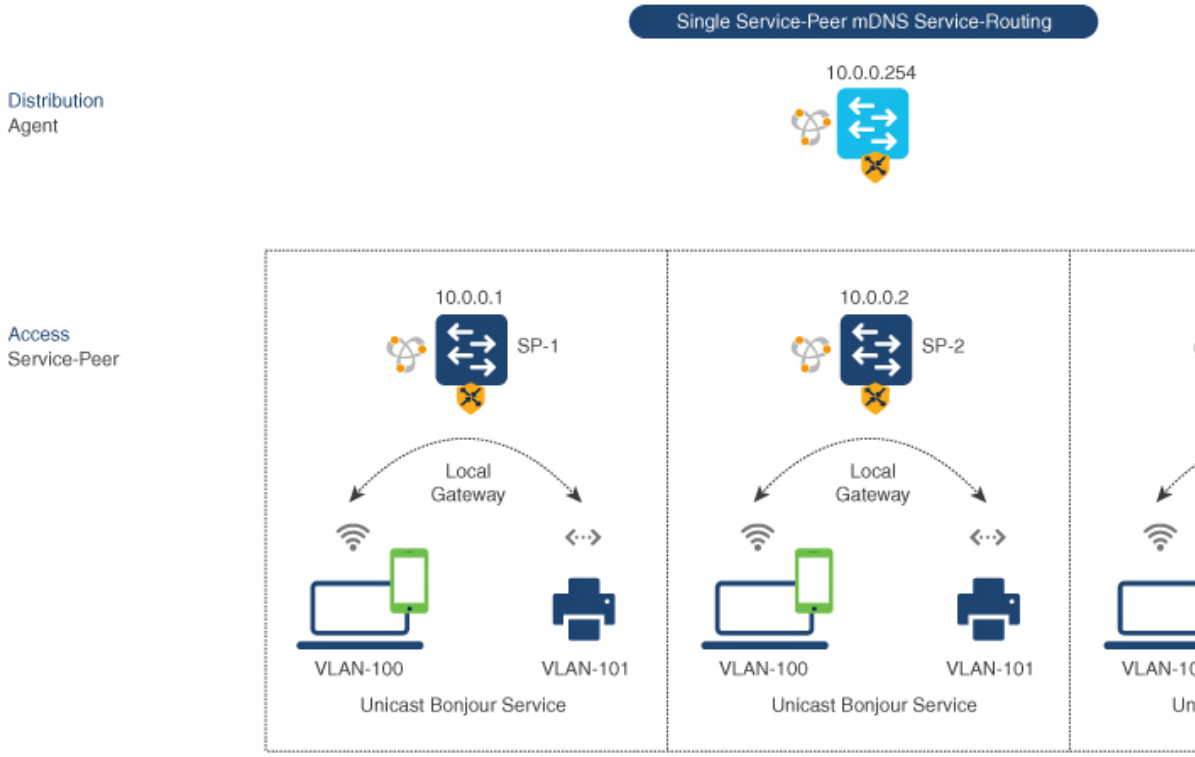
	コマンドまたはアクション	目的
		同じ設定に対して 1 つ以上の VLAN を作成できます。 この *ID* は VLAN 構成 ID を指します。たとえば、*vlan configuration 101-110, 200* のように範囲を指定すると、連続する VLAN ID と連続しない VLAN ID を設定できます。
ステップ 4	**mdns-sd gateway** 例： `Device(config-vlan-config)# mdns-sd gateway`	設定した VLAN ID で mDNS ゲートウェイを有効にします。 それぞれの機能を有効にするには、mDNS ゲートウェイ コンフィギュレーション モードで次のコマンドを入力します。 • **active-query timer [sec]**：検出されたサービスとサービスのレコードを、許可されたサービスタイプの定期的な mDNS クエリメッセージで更新可能にします。有効な範囲は 60 ～ 3600 秒です。推奨値は 3600 秒です。 • **service-mdns-query {ptr | srv | txt}**：特定のクエリタイプの処理を許可します。デフォルトのクエリタイプは PTR です。 • **transport {ipv4 | ipv6 | both}**：IPv4、IPv6、または両方の処理を許可します。冗長な処理と、2 つのネットワークタイプでの同じ情報による応答を減らすために、1 つのネットワークタイプを使用することを推奨します。デフォルトのネットワークタイプは IPv4 です。
ステップ 5	**source-interface** *ID* 例： `Device(config-vlan-mdns-sd)# source-interface vlan 4094`	アップストリーム Cisco Catalyst SDG エージェントスイッチとのサービスルーティング セッションを送信する有効な IP アドレスを持つインターフェイスを選択します。通常は管理VLANインターフェイスを使用できます。

	コマンドまたはアクション	目的
ステップ 6	**sdg-agent** [*IPv4_address*] 例： `Device(config-vlan-mdns-sd)# sdg-agent 10.0.0.254`	SDG エージェントの IPv4 アドレス（通常は管理 VLAN ゲートウェイアドレス）を設定します。FHRP モードの場合は、管理 VLAN の FHRP 仮想 IP アドレスを使用します。
ステップ 7	**exit** 例： `Device(config-vlan-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

ロケーションベースの mDNS の設定

デフォルトでは、サービスピアモードのレイヤ 2 Catalyst スイッチでは、スイッチにローカルに接続された有線ユーザーと EWC モードのアクセスポイントのワイヤレスユーザー間でのスイッチごとの mDNS の検出と配信が有効になります。このスイッチごとのデフォルトのロケーションベースの mDNS は、有線ユーザーと EWC モードのアクセスポイントのワイヤレスユーザーの VLAN がユーザーモビリティのために複数のレイヤ 2 Catalyst スイッチにまたがって拡張されている場合でもサポートされます。ポリシーベースの mDNS サービスプロバイダーおよび受信者情報をダウンストリーム サービスピア アクセスレイヤ スイッチから受け入れるには、mDNS サービスポリシー構成の SDG エージェントが必要です。

図 *46* : スイッチごとのロケーションベースの有線および *EWC* モードのアクセスポイント構成



（注） 次の構成手順に進む前に、ディストリビューション層の SDG エージェントスイッチで mDNS サービスポリシーを設定してください。詳細は、mDNS サービスポリシーの設定（CLI）（1080 ページ）のセクションを参照してください。

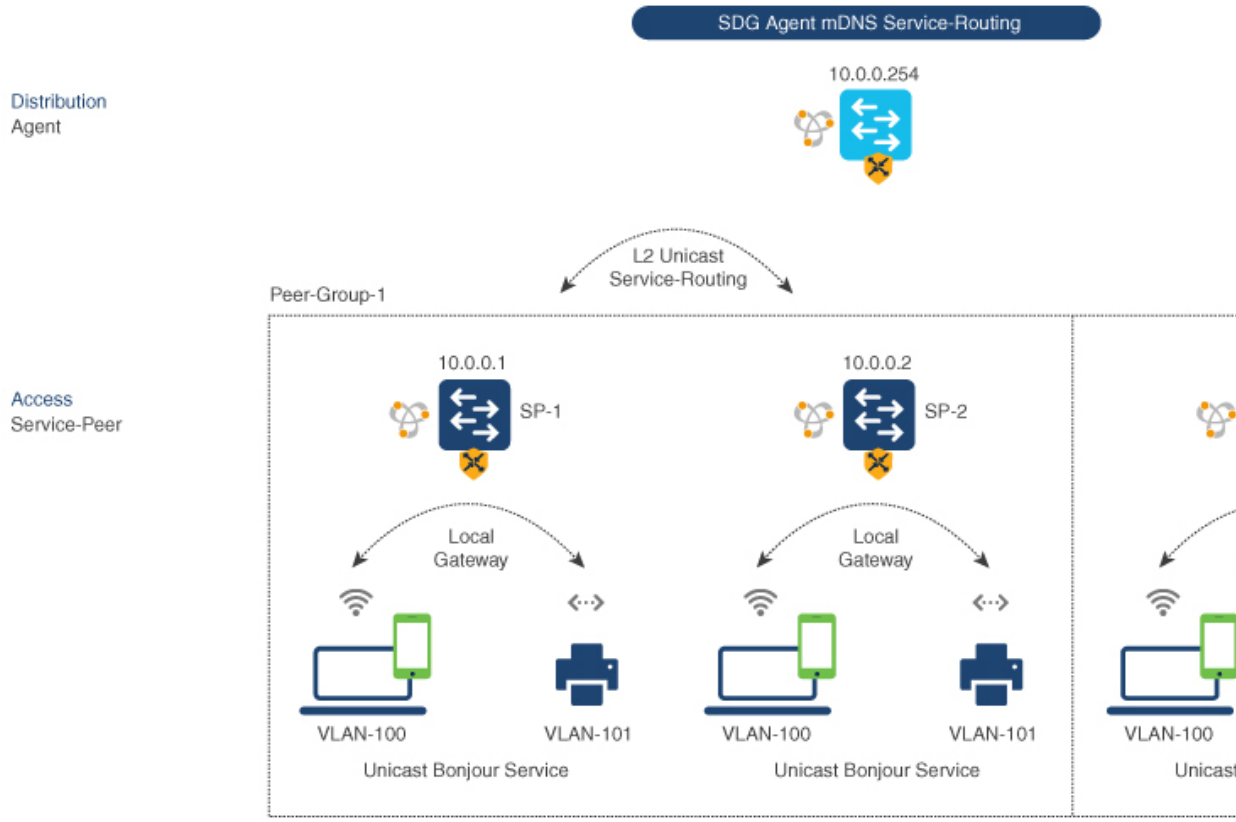
SDG エージェントでのサービスルーティングの設定（CLI）

Cisco Catalyst 9000 シリーズ スイッチは、ディストリビューション層で SDG エージェントモードを自動的にサポートし、有線ユーザーと EWC モードのアクセスポイントのワイヤレスユーザーに接続されたダウンストリームレイヤ 2 アクセス層のイーサネットスイッチでユニキャストモード Bonjour サービスルーティングを有効にします。ダウンストリーム サービスピア スイッチからの mDNS サービスキャッシュを受け入れるには、有線ユーザーまたは EWC モードのアクセスポイントのワイヤレスユーザーの VLAN で mDNS サービスポリシーを使用して SDG エージェントを設定する必要があります。

このセクションでは、サービスピアモードでローカルにペアリングされたレイヤ 2 アクセス ネットワーク スイッチ間でポリシーベースのサービスの検出と配信を有効にするための段階的な構成手順を示します。

次の図は、SDGエージェントとサービスピアモードのダウンストリームレイヤ2アクセス ネットワーク スイッチでのユニキャスト サービスルーティングを示しています。

図 *47 : Catalyst SDG* エージェントのサービスルーティング構成



（注） 次の構成手順に進む前に、ディストリビューション層の SDG エージェントスイッチで mDNS サービスポリシーを設定してください。詳細については、mDNS サービスポリシーの設定（CLI） （1080 ページ）を参照してください。

SDG エージェントスイッチで mDNS サービスポリシーとピアグループを有効にし、サービスピアモードのレイヤ 2 アクセス ネットワーク スイッチでユニキャスト モード サービスルーティングを有効にするには、以下の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Device# enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**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 3	**mdns-sd service-peer group** *service-peer-group-name* 例： `Device(config)# mdns-sd service-peer group service-peer-group-name`	グローバル コンフィギュレーション モードで一意のサービスピアグループを設定します。
ステップ 4	**peer-group** [*ID*] 例： `Device(config-mdns-svc-peer)# peer-group 1`	一意のピアグループ ID を割り当てて、mDNS サービスの検出と割り当てられたグループリスト内での配信を許可するサービスピアをペアリングします。 有効なピアグループの範囲は、SDG エージェントスイッチごとに 1 ー 1000 です。
ステップ 5	**service-policy** *service-policy-name* 例： `Device(config-mdns-svc-peer-grp)# service-policy VLAN100-POLICY`	ペアリングされたサービスピアからのサービスのアドバタイズメントとクエリを受け入れるように、mDNS サービスポリシーを関連付けます。

ステップ 6	**service-peer** [*IPv4_address*] **location-group** {**all** | **default** | **id**}
	例：
	`Device(config-mdns-svc-peer-grp)# service-peer 10.0.0.1 location-group default`
	`Device(config-mdns-svc-peer-grp)# service-peer 10.0.0.2 location-group default`
		mDNS サービスのアドバタイズメントまたはクエリメッセージを受け入れるように、少なくとも 1 つのサービスピアを設定します。複数のサービスピアでグループ化されている場合、設定されたピア間のレイヤ 2 ユニキャスト モード ルーティングが SDG エージェントによって提供されます。
		たとえば、SDG エージェントは、関連付けられたサービスポリシーに一致する 3 つ（10.0.0.1 と 10.0.0.2）のレイヤ 2 サービスピアスイッチ間にユニキャストベースのサービスゲートウェイ機能を提供します。
		ペアリングされていないレイヤ 2 サービスピア（10.0.0.3）からの mDNS サービス情報では、他のグループ化されたサービスピア（10.0.0.1 と 10.0.0.2）との mDNS サービスを通知または受信できません。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-mdns-svc-peer-grp)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

サービスピアモードの Local Area Bonjour の確認

このセクションでは、サービスピアモードのコントローラ上のさまざまな Local Area Bonjour ドメイン mDNS サービス構成パラメータ、キャッシュレコード、統計などを確認するためのガイドラインを示します。

表 *49 :*

コマンドまたはアクション	目的
show mdns-sd cache {all | interface | mac | name | service-peer | static | type | vlan}	複数の変数をサポートする使用可能な mDNS キャッシュレコードを表示し、有線ユーザーまたは EWC モードの AP ワイヤレスユーザーの VLAN から受信したソースのきめ細かな詳細情報を提供します。変数は次のとおりです。 • all：システムの複数のソース接続から検出された、使用可能なすべてのキャッシュレコードを表示します。 • interface：指定したレイヤ 3 インターフェイスから検出された、使用可能なキャッシュレコードを表示します。 • mac：指定した MAC アドレスから検出された、使用可能なキャッシュレコードを表示します。 • name：サービスプロバイダーが通知した名前に基づいて、使用可能なキャッシュレコードを表示します。 • service-peer：指定したレイヤ 2 サービスピアから検出された、使用可能なキャッシュレコードを表示します。 • static：ローカルで設定された静的 mDNS キャッシュエントリを表示します。 • type：特定の mDNS レコードタイプ（PTR、SRV、TXT、A、AAAA など）に基づいて、使用可能なキャッシュレコードを表示します。 • vlan：ユニキャストモードで指定されたレイヤ 2 VLAN ID から検出された、使用可能なキャッシュレコードを表示します。
show mdns-sd service-definition {name | type}	サービス名を mDNS PTR レコードにマッピングする、組み込みおよびユーザー定義のカスタムサービス定義を表示します。サービス定義は、名前またはタイプでフィルタリングできます。

コマンドまたはアクション	目的
show mdns-sd service-list {direction | name}	サービスポリシーに一致するサービスタイプを分類する、設定済みのサービスリストのインバウンドまたはアウトバウンド方向のリストを表示します。リストは、名前または特定の方向でフィルタリングできます。
show mdns-sd service-policy {interface | name}	インバウンドまたはアウトバウンドのサービスリストにマッピングされた mDNS サービスポリシーのリストを表示します。サービスポリシーリストは、関連付けられた指定インターフェイスまたは名前でフィルタ処理できます。
show mdns-sd statistics {all | cache | debug | interface | service-list | service-policy | services | vlan}	ユニキャストモードで mDNS が設定されている各 mDNS ゲートウェイ対応 VLAN でシステムによって双方向に処理された詳細な mDNS 統計を表示します。mDNS 統計の expanded キーワードは、インターフェイス、ポリシー、サービスリスト、およびサービスに関する詳細ビューを提供します。
show mdns-sd summary {interface | vlan}	mDNS ゲートウェイに関する簡単な情報や、システムのすべての有線ユーザーと EWC モードの AP ワイヤレスユーザーの VLAN およびインターフェイスの主要な構成ステータスを表示します。

SDG エージェントモードの Local Area Bonjour の確認

このセクションでは、SDG エージェントモードのコントローラ上のさまざまな Local Area Bonjour ドメイン mDNS サービス構成パラメータ、キャッシュレコード、統計などを確認するためのガイドラインを示します。

表 *50*：

コマンドまたはアクション	目的
show mdns-sd cache {all | interface | mac | name | service-peer | static | type | vlan | vrf}	複数の変数をサポートする使用可能な mDNS キャッシュレコードを表示し、ソースのきめ細かな詳細情報を提供します。変数は次のとおりです。 • all：システムの複数のソース接続から検出された、使用可能なすべてのキャッシュレコードを表示します。 • interface：指定したレイヤ 3 インターフェイスから検出された、使用可能なキャッシュレコードを表示します。 • mac：指定した MAC アドレスから検出された、使用可能なキャッシュレコードを表示します。 • name：サービスプロバイダーが通知した名前に基づいて、使用可能なキャッシュレコードを表示します。 • service-peer：指定したレイヤ 2 サービスピアから検出された、使用可能なキャッシュレコードを表示します。 • static：ローカルで設定された静的 mDNS キャッシュエントリを表示します。 • type：特定の mDNS レコードタイプ（PTR、SRV、TXT、A、AAAA など）に基づいて、使用可能なキャッシュレコードを表示します。 • vlan：ユニキャストモードで指定されたレイヤ 2 VLAN ID から検出された、使用可能なキャッシュレコードを表示します。 • vrf：特定の mDNS レコードタイプ（PTR、SRV、TXT、A、または AAAA）に基づいて、各 VRF の使用可能なキャッシュレコードを表示します。

コマンドまたはアクション	目的
show mdns-sd service-definition {name | type}	サービス名を mDNS PTR レコードにマッピングする組み込みおよびユーザー定義のカスタムサービス定義を表示します。サービス定義は、名前またはタイプでフィルタリングできます。
show mdns-sd service-list {direction | name}	サービスポリシーに一致するサービスタイプを分類する、設定済みのサービスリストのインバウンドまたはアウトバウンド方向のリストを表示します。リストは、名前または特定の方向でフィルタリングできます。
show mdns-sd service-policy {interface | name}	インバウンドまたはアウトバウンドのサービスリストにマッピングされた mDNS サービスポリシーのリストを表示します。サービスポリシーリストは、関連付けられた指定インターフェイスまたは名前でフィルタ処理できます。
show mdns-sd statistics {all | cache | debug | interface | service-list | service-policy | services | vlan}	ユニキャストモードで mDNS が設定されている各 mDNS ゲートウェイ対応 VLAN でシステムによって双方向に処理された詳細な mDNS 統計を表示します。mDNS 統計のキーワードは、インターフェイス、ポリシー、サービスリスト、およびサービスに関する詳細ビューを提供できます。
show mdns-sd summary {interface | vlan}	mDNS ゲートウェイに関する簡単な情報と、システムのすべてのVLANおよびインターフェイスの主要な構成ステータスを表示します。

参照先

表 *51 :* 参照先

関連項目	マニュアル タイトル
Cisco Embedded Wireless Controller on Catalyst Access Points CCO Configuration Guide	Catalyst アクセスポイント、IOS XE Bengaluru 17.5.x 上の Cisco 組み込みワイヤレスコントローラのコンフィギュレーション ガイド
DNA Service for Bonjour Deployment on Cisco Catalyst 9600 Switch	Cisco Catalyst 9600 Series Switch Software Configuration Guide, Release 17.4.X

関連項目	マニュアル タイトル
DNA Service for Bonjour Deployment on Cisco Catalyst 9500 Switch	Cisco Catalyst 9500 Series Switch Software Configuration Guide, Release 17.4.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9400 Switch	Cisco Catalyst 9400 Series Switch Software Configuration Guide, Release 17.4.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9300 Switch	Cisco Catalyst 9300 Series Switch Software Configuration Guide, Release 17.4.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9800 Wireless LAN Controller	Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.5.x
Cisco DNA Center Cisco Wide Area Bonjour アプリケーション ユーザー ガイド	Cisco Wide Area Bonjour Application on Cisco DNA Center User Guide, Release 2.2.x

参照先

第 XV 部

マルチキャスト ドメイン ネーム システム

第 90 章

マルチキャスト ドメイン ネーム システム

mDNS ゲートウェイの概要

マルチキャスト ドメイン ネーム システム（mDNS）は、mDNS サービスレコードを使用してローカルネットワーク上のデバイスとサービスを検出する Apple のサービス検出プロトコルです。

Bonjour プロトコルは、サービスアナウンスメントおよびクエリで動作します。各クエリやアドバタイズメントは、Bonjour マルチキャスト アドレス ipv4 224.0.0.251（ipv6 FF02::FB）に送信されます。このプロトコルは、UDP ポート 5353 で mDNS を使用します。

Bonjour プロトコルが使用するアドレスはリンクローカル マルチキャスト アドレスであるため、ローカル L2 ネットワークにのみ転送されます。マルチキャスト DNS は、クライアントが同じ L2 ドメインに属している必要があるサービスを検出できるように、L2 ドメインに制限されますが、大規模な導入や企業では常にこのことが可能になるとは限りません。

この問題に対処するため、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Bonjour ゲートウェイとして動作します。これにより、コントローラは Bonjour サービスをリッスンし、ソースまたはホストからの Bonjour アドバタイズメント（AirPlay、AirPrint など）をキャッシュします。たとえば Apple TV は、Bonjour クライアントがサービスを依頼または要求したときに、それらに応答します。このようにして、異なるサブネットのソースとクライアントを使用できます。

デフォルトでは、mDNS ゲートウェイはコントローラで無効になっています。mDNS ゲートウェイ機能を有効にするには、CLI または Web UI を使用して mDNS ゲートウェイを明示的に設定する必要があります。

前提条件

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、Bonjour ゲートウェイとして機能している場合、キャッシュされたサービスに応答してアドバタイズするため、mDNS が許可または使用されているすべての VLAN に、有効な IP アドレスを持つ SVI インターフェイスが必要です。これは、mDNS ゲートウェイとして機能するコントローラから送信される mDNS パケットの送信元 IP アドレスになります。

mDNS ゲートウェイの有効化（GUI）

手順

ステップ 1 [Configuration] > [Services] > [mDNS] を選択します。

ステップ 2 [Global] セクションでスライダを切り替えて、[mDNS Gateway] を有効または無効にします。

ステップ 3 [Transport] ドロップダウンリストから次のいずれかのタイプを選択します。

- **ipv4**
- **ipv6**
- **both**

ステップ 4 [Active-Query Timer] に適切なタイマー値を入力します。有効な範囲は、15 ～ 120 分です。デフォルトは 30 分です。

ステップ 5 [mDNS-AP Service Policy] ドロップダウンリストから、mDNS サービスポリシーを選択します。

（注） サービスポリシーの選択は任意です（mDNS-AP が設定されている場合のみ）。mDNS-AP が設定されていない場合、default-service-policy が使用されます。

ステップ 6 [Apply] をクリックします。

mDNS ゲートウェイの有効化または無効化（CLI）

（注）
- mDNS ゲートウェイは、デフォルトではコントローラ上でグローバルに無効になっています。
- mDNS ゲートウェイを有効にするには、グローバルと WLAN の両方の設定が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 **EXEC** モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**mdns-sd gateway** 例： `Device(config)# mdns-sd gateway`	MDNS ゲートウェイを有効にします。
ステップ 4	**transport** {**ipv4** | **ipv6** | **both**} 例： `Device(config-mdns-sd)# transport ipv4`	特定のトランスポートでmDNSメッセージを処理します。 ここで、各変数は次のように定義されます。 **ipv4** は、IPv4 mDNS メッセージの処理が有効になっていることを示します。これはデフォルト値です。 **ipv6** は、IPv6 mDNS メッセージの処理が有効になっていることを示します。

	コマンドまたはアクション	目的
		both は、各ネットワークに対して IPv4 と IPv6 の mDNS メッセージが有効になっていることを示します。
ステップ 5	**active-query timer** *active-query-periodicity* 例： `Device(config-mdns-sd)# active-query timer 15`	mDNS マルチキャスト アクティブ クエリの周期を変更します。 （注） アクティブクエリは、動的キャッシュを更新するための定期的な mDNS クエリです。 ここで、各変数は次のように定義されます。 *active-query-periodicity* は、アクティブなクエリ周期を分単位で示します。有効な範囲は 15 ～ 120 分です。アクティブなクエリは、デフォルトである 30分の周期で実行されます。
ステップ 6	**exit** 例： `Device(config-mdns-sd)# exit`	グローバル コンフィギュレーション モードに戻ります。

カスタムサービス定義の作成（GUI）

手順

ステップ 1 [Configuration] > [Services] > [mDNS] を選択します。

ステップ 2 [Service Definition] セクションで、[Add] をクリックします。

ステップ 3 表示される [Quick Setup: Service Definition] ページで、サービス定義の名前と説明を入力します。

ステップ 4 サービスタイプを入力し、[+] をクリックしてサービスタイプを追加します。

ステップ 5 [Apply to Device] をクリックします。

カスタムサービス定義の作成

サービス定義は、1 つ以上の mDNS サービスタイプまたは PTR（ポインタリソースレコード）名に管理者フレンドリ名を提供する構造体です。

デフォルトでは、いくつかの組み込みサービス定義が事前に定義されており、管理者が使用できるようになっています。

組み込みのサービス定義に加えて、管理者はカスタムサービス定義を定義することもできます。

次のコマンドを実行して、すべてのサービス定義（組み込みおよびカスタム）のリストを表示できます。

```
Device# show mdns-sd master-service-list
```

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 **EXEC** モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**mdns-sd service-definition** *service-definition-name* 例： `Device(config)# mdns-sd service-definition CUSTOM1`	mDNS サービス定義を設定します。 （注） • 作成されたカスタム サービス定義はすべて、プライマリサービスリストに追加されます。 • プライマリサービスリストは、カスタムおよび組み込みのサービス定義のリストで構成されます。
ステップ 4	**service-type** *string* 例： `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	mDNS サービスタイプを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-mdns-ser-def)# exit`	グローバル コンフィギュレーション モードに戻ります。

サービスリストの作成（GUI）

手順

ステップ 1 [Configuration] > [Services] > [mDNS] を選択します。

ステップ 2 [Service List] セクションで、[Add] をクリックします。

ステップ 3 表示される [Quick Setup: Service List] ページで、サービスリストの名前を入力します。

ステップ 4 [Direction] ドロップダウンリストから、インバウンドフィルタリングの場合は [IN] を、アウトバウンド フィルタリングの場合は [OUT] を選択します。

ステップ 5 [Available Services] ドロップダウンリストから、サービスリストに一致するサービスタイプを選択します。

（注） すべてのサービスを許可するには、[all] オプションを選択します。

ステップ 6 [Add Services（サービスの追加）] をクリックします。

ステップ 7 [Message Type] ドロップダウンリストで、照合するメッセージタイプを次のオプションから選択します。

- [any]：すべてのメッセージを許可します。
- [announcement]：デバイスのサービスアドバタイズメントまたはアナウンスメントのみを許可します。
- [query]：ネットワーク内のサービスに対するクライアントからのクエリのみを許可します。

ステップ 8 [Save] をクリックしてサービスを追加します。

ステップ 9 [Apply to Device] をクリックします。

サービスリストの作成

mDNS サービスリストは、サービス定義の集合です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 **EXEC** モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**mdns-sd service-list** *service-list-name* {**IN** | **OUT**}
	例：
	`Device(config)# mdns-sd service-list Basic-In IN`
	`Device(config)# mdns-sd service-list Basic-Out OUT`
		mDNS サービスリストを設定します。
		• [IN]：インバウンドフィルタリングを提供します。
		• [Out]：アウトバウンド フィルタリングを提供します。

ステップ 4	**match** *service-definition-name* **message-type** {**announcement** | **any** | **query**} 例： `Device(config-mdns-sl-in)# match CUSTOM1 message-type query`	サービスをメッセージタイプと照合します。 ここで、*service-definition-name* は、airplay、airserver、airtunes などのサービスの名前を指します。 （注） サービスを追加するには、サービス名がプライマリ サービスリストに含まれている必要があります。 mDNS サービスリストが [IN] に設定されている場合は、次のコマンドが表示されます：**match service-definition-name message-type {announcement | any | query}**。 mDNS サービスリストが [Out] に設定されている場合は、次のコマンドが表示されます。match service-definition-name。
ステップ 5	**show mdns-sd service-list {direction | name }**	サービスポリシーに一致するサービスタイプを分類する、設定済みのサービスリストのインバウンドまたはアウトバウン

	コマンドまたはアクション	目的
		ド方向のリストを表示します。リストは、名前または特定の方向でフィルタリングできます。
ステップ 6	**exit** 例： `Device(config-mdns-sl-in)# exit`	グローバル コンフィギュレーション モードに戻ります。

サービスポリシーの作成（GUI）

手順

ステップ 1 [Configuration] > [Services] > [mDNS] を選択します。
ステップ 2 [Service Policy] セクションで、[Add] をクリックします。
ステップ 3 表示される [Quick Setup: Service Policy] ページで、サービスポリシーの名前を入力します。
ステップ 4 [Service List Input] ドロップダウンリストから、いずれかのタイプを選択します。
ステップ 5 [Service List Output] ドロップダウンリストから、いずれかのタイプを選択します。
ステップ 6 [Location] ドロップダウンリストから、サービスリストに関連付けるロケーションを選択します。
ステップ 7 [Apply to Device] をクリックします。

サービスポリシーの作成

mDNS サービスポリシーは、サービスの学習中やクエリへの応答中のサービスフィルタリングに使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 **EXEC** モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**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 3	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy mdns-policy1`	mDNS サービスポリシーを有効にします。
ステップ 4	**location** {**lss** | **site-tag**} 例： `Device(config-mdns-ser-pol)# location lss`	LSS またはサイトタグに基づいて mDNS サービスタイプをフィルタリングします。 （注） ロケーション固有サービス（LSS）ベースのフィルタリングでは、mDNS ゲートウェイは、クエリ中のクライアント AP の隣接 AP から学習したサービスインスタンスで応答します。それ以外の AP の他のサービスインスタンスはフィルタリングされます。 サイトタグベースのフィルタリングでは、mDNS ゲートウェイは、クエリ中のクライアントと同じサイトタグに属するサービスインスタンスで応答します。 mDNS ゲートウェイは、ロケーションベースのフィルタリングが設定されている場合でも、有線サービスを使用して応答を返します。
ステップ 5	**service-list** *service-list-name* {**IN** | **OUT**} 例：	さまざまなサービスリスト名を IN および OUT 方向に設定します。

	コマンドまたはアクション	目的
	`Device(config-mdns-ser-pol)# service-list VLAN100-list IN`	（注） 管理者がカスタムサービスポリシーの作成または使用を決めた場合、両方向（IN および OUT）のサービスリストでカスタムサービスポリシーを設定する必要があります。そうしないと、mDNS ゲートウェイは機能しません（IN サービスリストがない場合、サービスを学習しません。OUT サービスリストがない場合、学習したサービスに応答しないか、サービスがアナウンスされません）。
ステップ 6	**exit** 例： `Device(config-mdns-ser-pol)# exit`	グローバル コンフィギュレーション モードに戻ります。

mDNS ポリシー用のローカルまたはネイティブプロファイルの設定

管理者は、ローカル認証と許可を設定し、AAA サーバーから mDNS ポリシーを取得することを想定していない場合、ローカルプロファイルまたはネイティブプロファイルを設定して、ユーザー、ロール、またはデバイスタイプに基づいて mDNS ポリシーを選択できます。このローカルプロファイルまたはネイティブプロファイルがワイヤレス プロファイル ポリシーにマッピングされると、mDNS サービスポリシーは、その WLAN で処理される mDNS パケットに適用されます。

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	**service-template** *template-name* 例： `Device(config)# service-template mdns`	サービステンプレートまたは ID ポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 3	**mdns-service-policy** *mdns-policy-name* 例： `Device(config-service-template)# mdns-service-policy mdnsTV`	mDNS ポリシーを設定します。
ステップ 4	**exit** 例： `Device(config-service-template)# exit`	グローバル コンフィギュレーション モードに戻ります。

mDNS Flex プロファイルの設定（GUI）

手順

ステップ 1 [Configuration] > [Services] > [mDNS] を選択します。

ステップ 2 [mDNS Flex Profile] セクションで、[Add] をクリックします。
[Add mDNS Flex Profile] ウィンドウが表示されます。

ステップ 3 [Profile Name] フィールドに、Flex mDNS プロファイル名を入力します。

ステップ 4 [Service Cache Update Timer] フィールドで、サービスキャッシュの更新時間を指定します。デフォルト値は 1 分です。有効な範囲は 1 ～ 100 分です。

ステップ 5 [Statistics Update Timer] フィールドで、統計更新タイマーを指定します。デフォルト値は 1 分です。有効な範囲は 1 ～ 100 分です。

ステップ 6 [VLANs] フィールドで、VLAN ID を指定します。複数の VLAN ID をカンマで区切って入力するか、VLAN ID の範囲を入力できます。許容される VLAN の最大数は 16 です。

ステップ 7 [Apply to Device] をクリックします。

mDNS Flex プロファイルの設定（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	**mdns-sd flex-profile** *mdns-flex-profile-name* 例： `Device(config)# mdns-sd flex-profile mdns-flex-profile-name`	mDNS Flex プロファイルモードを開始します。
ステップ 3	**update-timer service-cache** *service-cache timer-value <1-100>* 例： `Device(config-mdns-flex-profile)# update-timer service-cache 60`	Flex プロファイルの mDNS アップデート サービス キャッシュ タイマーを設定します。 デフォルト値は 1 分です。値の範囲は 1 ～ 100 分です。
ステップ 4	**update-timer statistics** *statistics timer-value <1-100>* 例： `Device(config-mdns-flex-profile)# update-timer statistics 65`	Flex プロファイルの mDNS アップデート統計タイマーを設定します。 デフォルト値は1分です。有効な範囲は 1 ～ 100 分です。
ステップ 5	**wired-vlan-range** *wired-vlan-range value* 例： `Device(config-mdns-flex-profile)# wired-vlan-range 10 - 20`	Flex プロファイルの mDNS 有線 VLAN 範囲を設定します。 デフォルト値は1分です。有効な範囲は 1 ～ 100 分です。

ワイヤレス Flex Connect プロファイルへの mDNS Flex プロファイルの適用（GUI）

手順

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

ステップ 2 [Add] をクリックします。
[Add Flex Profile] ウィンドウが表示されます。

ステップ 3 [General] タブの [mDNS Flex Profile] ドロップダウンリストから、Flex プロファイル名を選択します。

ステップ 4 [Apply to Device] をクリックします。

ワイヤレス Flex Connect プロファイルへの mDNS Flex プロファイルの適用（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。
ステップ 2	**wireless profile flex** *wireless-flex-profile-name* 例： `Device# wireless profile flex wireless-flex-profile-name`	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	**mdns-sd** *mdns-flex-profile* 例： `Device(config-wireless-flex-profile)# mdns-sd mdns-flex-profile-name`	プロファイル内のすべての AP の mDNS 機能を有効にします。

ロケーションベースのサービスのフィルタリング

ロケーションベースのサービスのフィルタリングにおける前提条件

サービス定義とサービスポリシーを作成する必要があります。詳細については、「カスタム サービス定義の作成」および「サービスポリシーの作成」を参照してください。

SSID を使用した mDNS ロケーションベースのフィルタリングの設定

サービスポリシーでロケーション名として SSID が設定されている場合、クエリへの応答は、その SSID で学習されたサービスになります。

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	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy mdns-policy1`	サービス ポリシーを設定します。
ステップ 3	**location ssid** 例： `Device(config-mdns-ser-pol)# location ssid`	SSID を使用してロケーションベースのフィルタリングを設定します。
ステップ 4	**end** 例： `Device(config-mdns-ser-pol)# 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。

AP 名を使用した mDNS ロケーションベースのフィルタリングの設定

サービスポリシーで、 AP 名がロケーションとして設定されている場合、クエリへの応答は、その AP 名で学習されたサービスになります。

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	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy mdns-policy1`	サービス ポリシーを設定します。
ステップ 3	**location ap-name** 例： `Device(config-mdns-ser-pol)# location ap-name`	AP 名を使用してロケーションベースのフィルタリングを設定します。
ステップ 4	**end** 例： `Device(config-mdns-ser-pol)# 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。

APロケーションを使用したmDNSロケーションベースのフィルタリングの設定

サービスポリシーで、ロケーションが AP ロケーションとして設定されている場合、クエリへの応答は、同じAP「ロケーション」名（「site-tag」とは異なる）を使用して、すべてのAPで学習されたサービスになります。

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	**mdns-sd service-policy** *service-policy-name* **例：** `Device(config)# mdns-sd service-policy mdns-policy1`	サービス ポリシーを設定します。
ステップ 3	**location ap-location** **例：** `Device(config-mdns-ser-pol)# location ap-location`	AP ロケーションを使用してロケーションベースのフィルタリングを設定します。
ステップ 4	**end** **例：** `Device(config-mdns-ser-pol)# 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。

正規表現を使用したmDNSロケーションベースのフィルタリングの設定

- サービスポリシーで、対応する AP 名と一致する正規表現としてロケーションが設定されている場合、クエリへの応答は、その AP 名に基づいて AP のグループで学習されたサービスになります。
- サービスポリシーで、対応する AP 名と一致する正規表現としてロケーションが設定されている場合、クエリへの応答は、その AP ロケーションに基づいて AP のグループで学習されたサービスになります。

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	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy mdns-policy1`	サービス ポリシーを設定します。

ステップ 3	**location regex** {**ap-location** *regular-expression* | **ap-name** *regular-expression*}
	例：
	`Device(config-mdns-ser-pol)# location regex ap-location dns_location`
	`Device(config-mdns-ser-pol)# location regex ap-name dns_name`
		正規表現を使用したロケーションベースのフィルタリングを設定します。

ステップ 4	**end** 例： `Device(config-mdns-ser-pol)# end` （注） *AP-2FLR-SJC-123* などの特定のキーワードが含まれるAP名のサービスをフィルタ処理するには、*AP-2FLR-* のように正規表現の AP 名を使用して、一連のアクセスポイントから学習したサービスと一致させることができます。	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。

mDNS AP の設定

ほとんどの展開では、APが有線側で受信できるサービスをVLAN（APが直接接続されているスイッチポートで許可されるVLAN、独自のVLAN、スイッチポートがトランクの場合はさらに多くの VLAN）で利用できる場合があります。

次に、mDNS AP を設定する手順を示します。

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	**mdns-sd gateway** 例： `Device(config)# mdns-sd gateway`	mDNS ゲートウェイを設定します。
ステップ 3	**ap name** *ap-name* **mdns-ap enable vlan** *vlan-id* 例： `Device# ap name ap1 mdns-ap enable vlan 22`	AP 上で mDNS を有効にし、mDNS AP の VLAN を設定します。
ステップ 4	**ap name** *ap-name* **mdns-ap vlan add** *vlan-id* 例： `Device# ap name ap1 mdns-ap vlan add 200`	VLAN を mDNS AP に追加します。vlan-id の範囲は 1 ～ 4096 です。
ステップ 5	**ap name** *ap-name* **mdns-ap vlan del** *vlan-id* 例： `Device# ap name ap1 mdns-ap vlan del 2`	mDNS AP から VLAN を削除します。
ステップ 6	**ap name** *ap-name* **mdns-ap disable** 例： `Device# ap name ap1 mdns-ap disable`	（任意）mDNS AP を無効にします。
ステップ 7	**end** 例： `Device# 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 ごとに最大 10 の VLAN を設定できます。

mDNS サービスポリシーとワイヤレス プロファイル ポリシーの関連付け（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 Name] をクリックします。

ステップ 3 [Advanced] タブで、[mDNS Service Policy] ドロップダウンリストから mDNS サービスポリシーを選択します。

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

mDNS サービスポリシーとワイヤレス プロファイル ポリシーの関連付け

（注） mDNS サービスポリシーをグローバルに設定してから、ワイヤレス プロファイル ポリシーに関連付ける必要があります。

デフォルトの mDNS サービスポリシーは、ワイヤレス プロファイル ポリシーが作成された時点ですでに接続されています。次のコマンドを使用して、デフォルトの mDNS サービスポリシーを目的のサービスポリシーに上書きできます。

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 プロファイル ポリシーを設定します。 ここで、*profile-policy* は WLAN ポリシー プロファイルの名前を指します。

	コマンドまたはアクション	目的
ステップ 3	**mdns-sd service-policy** *custom-mdns-service-policy* 例： `Device(config-wireless-policy)# mdns-sd service-policy custom-mdns-service-policy`	mDNS サービスポリシーをワイヤレスプロファイルポリシーに関連付けます。 デフォルトの mDNS サービスポリシー名は **default-mdns-service-policy** です。

	コマンドまたはアクション	目的
		（注） **default-mdns-profile-policy** は、mDNS サービスのアナウンスとクエリーをフィルタリングするために、**default-mdns-service-list** 設定を使用します。 ワイヤレスネットワークでは、mDNS パケットは mDNS ゲートウェイによって消費され、クライアントまたはデバイスではこのサービスの学習ができません。サービスをデバイスと共有し、管理者が簡単に設定できるようにするために、いくつかの標準サービスタイプのリストがデフォルトでワイヤレスネットワークで共有されています。この標準サービスタイプのリストのことをデフォルトサービスポリシーと呼び、一連のサービスタイプで構成されています。 この表では、デフォルトサービスポリシーのサービスリストの例について説明します。 **表 *52*：デフォルト名と *mDNS* サービスタイプ** **デフォルト名（Default Name）** / **mDNS サービスタイプ** Apple HomeSharing / _homesharing._tcp.local Printer-IPPS / _ipps._tcp.local google-chromecast / _googlecast._tcp.local

	コマンドまたはアクション	目的
		（注） • ロケーションは、mDNS のデフォルトサービスポリシーでは無効になります。 • mDNS のデフォルトサービスポリシーの内容は変更できません。ただし、個別の mDNS サービスポリシーを作成し、それらをワイヤレスポリシープロファイルの下に関連付けることができます。
ステップ 4	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。

WLAN 用の mDNS ゲートウェイの有効化または無効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 WLAN をクリックします。
ステップ 3 [Advanced] タブの [mDNS Mode] ドロップダウンリストでモードを選択します。
ステップ 4 [Update & Apply to Device] をクリックします。

WLAN 用の mDNS ゲートウェイの有効化または無効化

（注） ブリッジングはデフォルトの動作です。これは、mDNSパケットが常にブリッジングされることを意味します。

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	**wlan** *profile-name wlan-id ssid-name* 例： `Device(config)# wlan test 24 ssid1`	WLAN の名前と ID を指定します。 • *profile-name* は、最大 32 文字の英数字からなる WLAN 名です。 • *wlan-id* はワイヤレス LAN の ID です。有効な範囲は 1 ～ 512 です。 • *ssid-name* は、最大 32 文字の英数字からなる SSID です。 （注） mDNS ゲートウェイを機能させるには、グローバル設定を適切に行う必要があります。

ステップ 3	**mdns-sd-interface** {**gateway** | **drop**}
	例：
	`Device(config-wlan)# mdns-sd gateway`
	`Device(config-wlan)# mdns-sd drop`
		WLAN で mDNS ゲートウェイおよびブリッジ機能を有効または無効にします。

ステップ 4	**exit** 例： `Device(config-wlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**show wlan name** *wlan-name* | **show wlan all** 例： `Device# show wlan name test | show wlan all`	WLAN での mDNS のステータスを確認します。
ステップ 6	**show wireless profile policy** 例： `Device# show wireless profile policy`	WLAN で設定されているサービスポリシーを確認します。

mDNS ゲートウェイの設定の確認

mDNS のサマリーを確認するには、次のコマンドを使用します。

```
Device# show mdns-sd summary
mDNS Gateway: Enabled
Active Query: Enabled
  Periodicity (in minutes): 30
Transport Type: IPv4
```

mDNS のキャッシュを確認するには、次のコマンドを使用します。

```
Device# show mdns-sd cache
------------------------------------------------------------ PTR Records
----------------------------------------
RECORD-NAME                      TTL      WLAN   CLIENT-MAC       RR-RECORD-DATA

_airplay._tcp.local            4500     30     07c5.a4f2.dc01   CUST1._airplay._tcp.local

_ipp._tcp.local                 4500     30     04c5.a4f2.dc01   CUST3._ipp._tcp.local2

_ipp._tcp.local                 4500     15     04c5.a4f2.dc01   CUST3._ipp._tcp.local4

_ipp._tcp.local                 4500     10     04c5.a4f2.dc01   CUST3._ipp._tcp.local6

_veer_custom._tcp.local         4500     10     05c5.a4f2.dc01
CUST2._veer_custom._tcp.local8
```

有線サービスプロバイダからの mDNS キャッシュを確認するには、次のコマンドを使用します。

```
Device# show mdns-sd cache wired
------------------------------------------------------------ PTR Records
----------------------------------------
RECORD-NAME                              TTL      VLAN      CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------
_airplay._tcp.local                      4500     16        0866.98ec.97af
wiredapple._airplay._tcp.local
_raop._tcp.local                         4500     16        0866.98ec.97af
086698EC97AF@wiredapple._raop._tcp.local

------------------------------------------------------------ SRV Records
----------------------------------------
RECORD-NAME                              TTL      VLAN      CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------
wiredapple._airplay._tcp.local           4500     16        0866.98ec.97af   0 0 7000
 wiredapple.local
086698EC97AF@wiredapple._raop._tcp.local 4500     16        0866.98ec.97af   0 0 7000
 wiredapple.local

------------------------------------------------------------ A/AAAA Records
----------------------------------------
RECORD-NAME                              TTL      VLAN      CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------
wiredapple.local                         4500     16        0866.98ec.97af
2001:8:16:16:e5:c446:3218:7437

------------------------------------------------------------ TXT Records
----------------------------------------
RECORD-NAME                              TTL      VLAN      CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------
wiredapple._airplay._tcp.local           4500     16        0866.98ec.97af
```

```
[343]'acl=0''deviceid=08:66:98:EC:97:AF''features=
086698EC97AF@wiredapple._raop._tcp.local   4500     16        0866.98ec.97af
[193]'cn=0,1,2,3''da=true''et=0,3,5''ft=0x5A7FFFF7
```

mdns-sd タイプの PTR を確認するには、次のコマンドを使用します。

```
Device# show mdns-sd cache type {PTR | SRV | A-AAA | TXT}
RECORD-NAME                                    TTL      WLAN      CLIENT-MAC
RR-Record-Data
------------------------------------------------------------------------------------------
_custom1._tcp.local                            4500     2         c869.cda8.77d6
service_t1._custom1._tcp.local
_custom1._tcp.local                            4500     2         c869.cda8.77d6
vk11._custom1._tcp.local
_ipp._tcp.local                                4500     2         c869.cda8.77d6
service-4._ipp._tcp.local
```

クライアント MAC の mdns-sd キャッシュを確認するには、次のコマンドを使用します。

```
Device# show mdns-sd cache {ap-mac <ap-mac> | client-mac <client-mac> | wlan-id <wlan-id>
 | wired}
RECORD-NAME                                    TTL      WLAN      CLIENT-MAC
RR-Record-Data
------------------------------------------------------------------------------------------
_custom1._tcp.local                            4500     2         c869.cda8.77d6
service_t1._custom1._tcp.local
_custom1._tcp.local                            4500     2         c869.cda8.77d6
vk11._custom1._tcp.local
_ipp._tcp.local                                4500     2         c869.cda8.77d6
service-4._ipp._tcp.local

------------------------------------------------------------ SRV Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      WLAN      CLIENT-MAC
RR-Record-Data
------------------------------------------------------------------------------------------
service-4._ipp._tcp.local                      4500     2         c869.cda8.77d6   0 0
1212 mDNS-Client1s-275.local
vk11._custom1._tcp.local                       4500     2         c869.cda8.77d6   0 0
987 mDNS-Client1s-275.local
service_t1._custom1._tcp.local                 4500     2         c869.cda8.77d6   0 0
197 mDNS-Client1s-275.local

------------------------------------------------------------ A/AAAA Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      WLAN      CLIENT-MAC
RR-Record-Data
------------------------------------------------------------------------------------------
mDNS-Client1s-275.local                        4500     2         c869.cda8.77d6
120.1.1.33

------------------------------------------------------------ TXT Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      WLAN      CLIENT-MAC
RR-Record-Data
------------------------------------------------------------------------------------------
service-4._ipp._tcp.local                      4500     2         c869.cda8.77d6
'CLient1'
vk11._custom1._tcp.local                       4500     2         c869.cda8.77d6
'txtvers=11'
service_t1._custom1._tcp.local                 4500     2         c869.cda8.77d6
'txtvers=12'
```

mdns-sd キャッシュの詳細を確認するには、次のコマンドを使用します。

```
Device# show mdns-sd cache detail

Name: _custom1._tcp.local
  Type: PTR
  TTL: 4500
  WLAN: 2
  WLAN Name: mdns120
  VLAN: 120
  Client MAC: c869.cda8.77d6
  AP Ethernet MAC: 7069.5ab8.33d0
  Expiry-Time: 09/09/18 21:50:47
  Site-Tag: default-site-tag
  Rdata: service_t1._custom1._tcp.local
```

mdns-sd の統計情報を確認するには、次のコマンドを使用します。

```
Device# show mdns-sd statistics

-----------------------------------------------------
Consolidated mDNS Packet Statistics
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 61045
  IPv4 sent: 30790
    IPv4 advertisements sent: 234
    IPv4 queries sent: 30556
  IPv6 sent: 30255
    IPv6 advertisements sent: 17
    IPv6 queries sent: 30238
  Multicast sent: 57558
    IPv4 sent: 28938
    IPv6 sent: 28620
mDNS packets received: 72796
  advertisements received: 13604
  queries received: 59192
  IPv4 received: 40600
    IPv4 advertisements received: 6542
    IPv4 queries received: 34058
  IPv6 received: 32196
    IPv6 advertisements received: 7062
    IPv6 queries received: 25134
mDNS packets dropped: 87

-----------------------------------------------------
Wired mDNS Packet Statistics
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 61033
  IPv4 sent: 30778
    IPv4 advertisements sent: 222
    IPv4 queries sent: 30556
  IPv6 sent: 30255
    IPv6 advertisements sent: 17
    IPv6 queries sent: 30238
  Multicast sent: 57558
    IPv4 sent: 28938
    IPv6 sent: 28620
mDNS packets received: 52623
  advertisements received: 1247
  queries received: 51376
  IPv4 received: 32276
    IPv4 advertisements received: 727
    IPv4 queries received: 31549
  IPv6 received: 20347
    IPv6 advertisements received: 520
```

```
    IPv6 queries received: 19827
mDNS packets dropped: 63

-----------------------------------------------------
mDNS Packet Statistics, for WLAN: 2
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 12
  IPv4 sent: 12
    IPv4 advertisements sent: 12
    IPv4 queries sent: 0
  IPv6 sent: 0
    IPv6 advertisements sent: 0
    IPv6 queries sent: 0
  Multicast sent: 0
    IPv4 sent: 0
    IPv6 sent: 0
mDNS packets received: 20173
  advertisements received: 12357
  queries received: 7816
  IPv4 received: 8324
    IPv4 advertisements received: 5815
    IPv4 queries received: 2509
  IPv6 received: 11849
    IPv6 advertisements received: 6542
    IPv6 queries received: 5307
mDNS packets dropped: 24
```

デフォルトサービスリストの詳細を確認するには、次のコマンドを使用します。

```
Device# show mdns-sd default-service-list

-------------------------------------------
        mDNS Default Service List
-------------------------------------------

Service Definition: airplay
Service Names: _airplay._tcp.local

Service Definition: airtunes
Service Names: _raop._tcp.local

Service Definition: homesharing
Service Names: _home-sharing._tcp.local

Service Definition: printer-ipp
Service Names: _ipp._tcp.local

Service Definition: printer-lpd
Service Names: _printer._tcp.local

Service Definition: printer-ipps
Service Names: _ipps._tcp.local

Service Definition: printer-socket
Service Names: _pdl-datastream._tcp.local

Service Definition: google-chromecast
Service Names: _googlecast._tcp.local

Service Definition: itune-wireless-devicesharing2
Service Names: _apple-mobdev2._tcp.local
```

プライマリサービスリストの詳細を確認するには、次のコマンドを使用します。

```
Device# show mdns-sd master-service-list

-----------------------------------------
        mDNS Master Service List
-----------------------------------------

Service Definition: fax
Service Names: _fax-ipp._tcp.local

Service Definition: roku
Service Names: _rsp._tcp.local

Service Definition: airplay
Service Names: _airplay._tcp.local

Service Definition: scanner
Service Names: _scanner._tcp.local

Service Definition: spotify
Service Names: _spotify-connect._tcp.local

Service Definition: airtunes
Service Names: _raop._tcp.local

Service Definition: airserver
Service Names: _airplay._tcp.local
               _airserver._tcp.local

.
.
.

Service Definition: itune-wireless-devicesharing2
Service Names: _apple-mobdev2._tcp.local
```

コントローラで設定されている mDNS と、それに関連付けられている VLAN を確認するには、次のコマンドを使用します。

```
Device# show mdns-sd ap

Number of mDNS APs.............................. 1

AP Name   Ethernet MAC   Number of Vlans   Vlanidentifiers
-----------------------------------------------------------------------------------------------
AP3600-1   7069.5ab8.33d0          1      300
```

追加のデバッグ

mDNS をさらにデバッグするには、次の手順を使用します。

1. コントローラで次のコマンドを実行します。

   ```
   set platform software trace wncd <0-7> chassis active R0 mdns debug
   ```

2. 問題を再現します。

3. 次のコマンドを実行して、有効になっているトレースを収集します。

```
show wireless loadbalance ap affinity wncd 0

AP MAC   Discovery Timestamp  Join Timestamp               Tag    Vlanidentifiers
```

```
--------------------------------------------------------------------------------------
0cd0.f894.0600      06/30/21 12:39:48    06/30/21 12:40:021 default-site-tag     300
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。