ワイヤレス デバイスの設定

Cisco Prime Infrastructure でのコントローラの表示

Prime Infrastructure データベースのすべてのコントローラの概要を表示できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 ページ上部のコマンド ボタンを使用するには、1 つ以上のコントローラの横にあるチェックボックスをオンにします。次の表に、このページで使用できるフィールドについて説明します。

表 *1*: ワイヤレス コントローラのサマリー情報

フィールド	説明
[管理ステータス（Admin Status）]	ワイヤレス コントローラの管理ステータス。
[DNS 名（DNS Name）]	ワイヤレス コントローラの DNS 名。
[最終インベントリ収集ステータス（Last Inventory Collection Status）]	最後のインベントリ収集のステータス。
[前回正常終了した収集の時間（Last Successful Collection Time）]	前回正常終了した収集の時間。
[クライアント カウント（Client Count）]	現在コントローラに関連付けられているクライアントの合計数を表示します。
[ソフトウェア タイプ（Software Type）]	すべての管理対象デバイスのソフトウェア タイプを表示します。
参照先	ロケーション情報を表示します。
デバイス名（Device Name）	コントローラの名前。デバイスの詳細の表示、コントローラの設定、テンプレートの適用、設定アーカイブの表示およびスケジュール設定、コントローラ ソフトウェア イメージの表示および更新を行うには、デバイス名をクリックします。

フィールド	説明
[到達可能性（Reachability）]	デバイス ステータスのバックグラウンド タスクの最後の実行情報に基づいて、到達可能性ステータスが更新されます。
[IP アドレス/DNS（IP Address/DNS）]	コントローラ管理インターフェイスのローカル ネットワーク IP アドレス。IP アドレスの下のアイコンをクリックすると、コントローラの Web ユーザ インターフェイスが新しいブラウザ ウィンドウで表示されます。
デバイスタイプ（Device Type）	デバイス タイプは、シリーズ別にグループ化されています。次に例を示します。 • [WLC2100]：21xx シリーズ ワイヤレス LAN コントローラ • [2500]：25xx シリーズ ワイヤレス LAN コントローラ • [4400]：44xx シリーズ ワイヤレス LAN コントローラ • [5500]：55xx シリーズ ワイヤレス LAN コントローラ • [7500]：75xx シリーズ ワイヤレス LAN コントローラ • [WiSM]：WiSM（スロット番号、ポート番号） • [WiSM2]：WiSM2（スロット番号、ポート番号）
[AP ディスカバリ ステータス（AP Discovery Status）]	AP ディスカバリが完了したかどうかを示します。
ソフトウェア バージョン（Software Version）	コントローラで現在実行しているコードのオペレーティング システム リリースのバージョンとメンテナンス番号。
[モビリティ グループ名（Mobility Group Name）]	モビリティ グループまたは WPS グループの名前。

ステップ 3 コントローラに関する特定の情報を表示するには、デバイス名をクリックします。

関連トピック

設定テンプレートの展開のためのコントローラ固有のコマンド （4 ページ）

設定テンプレートの展開のためのコントローラ固有のコマンド

[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択してから、左側の [デバイスグループ（Device Groups）] メニューで [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択し、1 つ以上のデバイスのチェックボックスをオンにすると、ページ上部に次のボタンが表示されます。

- [削除（Delete）]：コントローラを削除できます。

- [編集（Edit）]：一般パラメータ、SNMP パラメータ、Telnet/SSH パラメータ、HTTP パラメータ、および IPSec パラメータを編集できます。
- [同期（Sync）]：
- [グループとサイト（Groups & Sites）]：場所グループおよびサイトでコントローラを追加または削除できます。
- [再起動（Reboot）]：設定変更を保存した後にコントローラを再起動するように設定できます。選択できるリブート オプションは次のとおりです。
  - [フラッシュへの設定の保存（Save Config to Flash）]：データはコントローラの不揮発性 RAM（NVRAM）に保存され、電源の再投入時にも保持されます。コントローラを再起動した場合、設定が保存されていないと、適用した変更はすべて失われます。
  - [Reboot APs（AP のリブート）]
  - [AP イメージのスワップ（Swap AP Image）]
- [ダウンロード（Download）]：次のオプションを選択して、コントローラにソフトウェアをダウンロードできます。
  - [ソフトウェアのダウンロード（Download Software）]：[TFTP]、[FTP]、[SFTP] のいずれかを選択して、選択したコントローラ、または設定グループの構築後に選択したグループのすべてのコントローラにソフトウェアをダウンロードします。
  - [IDS シグニチャのダウンロード（Download IDS Signatures）]
  - [カスタマイズされた Web 認証のダウンロード（Download Customized Web Auth）]
  - [ベンダーのデバイス証明書のダウンロード（Download Vendor Device Certificate）]
  - [ベンダーの CA 証明書のダウンロード（Download Vendor CA Certificate）]
  - [コントローラの一括更新（Bulk Update Controllers）]
- 設定（Configure）
  - [フラッシュへの設定の保存（Save Config to Flash）]
  - [コントローラからのテンプレートの検出（Discover Templates from Controller）]
  - [コントローラに適用されているテンプレート（Templates Applied to Controller）]
  - [今すぐ監査する（Audit Now）]
  - 資格情報の更新

関連トピック

Cisco Prime Infrastructure でのコントローラの表示 （3 ページ）
コントローラで使用されている設定テンプレートの確認と関連付けの削除 （6 ページ）
インポートした CSV ファイルを使用したコントローラ クレデンシャルの変更 （8 ページ）
再起動によるコントローラ変更の適用 （9 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）

コントローラで使用されている設定テンプレートの確認と関連付けの削除

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [設定（Configure）] > [今すぐ監査する（Audit Now）] をクリックします。

ステップ 4 ポップアップ ダイアログ ボックスで [OK] をクリックすると、データベース内の設定オブジェクトからテンプレートの関連付けが削除され、関連付けられている設定グループからもこのコントローラのテンプレートの関連付けが削除されます（これはテンプレート ベースの監査のみです）。

テンプレートを関連付ける Prime Infrastructure 設定を指定できます。

検出されたテンプレートは、管理またはローカル ユーザ パスワードを取得しません。

テンプレート検出には次のルールが適用されます。

- テンプレート検出では、 Prime Infrastructure で見つからないテンプレートが検出されます。
- 既存のテンプレートは検出されません。
- テンプレート検出では、コントローラの動的インターフェイスの設定を取得しません。コントローラで動的インターフェイスの設定を適用するには、新しいテンプレートを作成する必要があります。

関連トピック

レポートでのコントローラ監査結果の表示 （7 ページ）
コントローラに適用されているテンプレートの表示 （21 ページ）
コントローラの既存のテンプレートを検出 （20 ページ）
再起動によるコントローラ変更の適用 （9 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）

[ネットワークデバイス（NetworkDevices）]テーブルからのコントローラ クレデンシャルの変更

SNMP と Telnet のクレデンシャルを更新するには、各コントローラで変更を行う必要があります。複数のコントローラの SNMP または Telnet のクレデンシャルの詳細は同時に更新することはできません。

コントローラの設定を変更するには、SNMP 書き込みアクセスパラメータが必要です。読み取り専用アクセスパラメータでは、設定を表示することはできますが、変更することはできません。

SNMP/Telnet クレデンシャルを更新するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [設定（Configure）] > [資格情報の更新（Update Credentials）] をクリックします。

ステップ 4 必須フィールドに入力して、[OK] をクリックします。

関連トピック

インポートした CSV ファイルを使用したコントローラ クレデンシャルの変更 （8 ページ）

レポートでのコントローラ監査結果の表示

コントローラで監査を実行すると、監査レポートに次の情報が表示されます。

- デバイス名（Device Name）
- 監査の時刻
- 監査ステータス
- 適用テンプレートと設定グループ テンプレートの矛盾の情報には、次の内容が含まれます。
  - テンプレートの種類（テンプレート名）
  - テンプレート適用方法
  - 監査ステータス（不一致、同一など）
  - テンプレートの属性
  - Cisco Prime Infrastructure の値
  - コントローラの値
  - その他の Cisco Prime Infrastructure の矛盾には、次の内容が含まれます。
  - 設定の種類（名前）
  - 監査ステータス（不一致、同一など）
  - 属性（Attribute）
  - コントローラの値
  - バックグラウンド監査が有効な設定グループの合計施行数。バックグラウンド監査が有効な設定グループに関する監査で矛盾が検出され、施行が有効である場合、このセクションにコントローラの監査中に行われた施行のリストが表示されます。全体の施行数が 0 より大きい場合、この数値はリンクとして表示されます。このリンクをクリックすると、Cisco Prime Infrastructure から行われた施行のリストが表示されます。
- [バックグラウンド監査が有効な設定グループの失敗施行数（Failed Enforcements for Configuration Groups with background audit enabled）]：失敗した施行数が 0 より大きい場合、

この数値はリンクとして表示されます。このリンクをクリックすると、デバイスによって返された失敗の詳細（失敗の理由など）のリストが表示されます。

- [コントローラへのCisco Prime Infrastructure値の復元（Restore Cisco Prime Infrastructure Values to Controller）] または [コントローラからの設定の更新（Refresh Configuration from Controller）]：監査の結果として設定の相違が見つかった場合は、[コントローラへのPrime Infrastructure値の復元（Restore Prime Infrastructure Values to Controller）] または [コントローラからの設定の更新（Refresh Configuration from Controller）] をクリックして、Cisco Prime Infrastructure 設定をコントローラと同期することができます。
  - 矛盾をデバイスにプッシュする場合は、[コントローラへの Prime Infrastructure 値の復元（Restore Prime Infrastructure Values to Controller）] を選択します。
  - デバイスからこの設定のデバイスをピックアップする場合は、[コントローラからの設定の更新（Refresh Configuration from Controller）] を選択します。[コントローラからの設定の更新（Refresh Configuration from Controller）] をクリックしても、テンプレートは更新されません。

関連トピック

コントローラで使用されている設定テンプレートの確認と関連付けの削除 （6 ページ）

インポートした CSV ファイルを使用したコントローラ クレデンシャルの変更

CSV ファイルをインポートすることで、複数のコントローラのクレデンシャルを更新できます。

コントローラの情報を一括更新するには、次の手順を実行します。

ステップ 1 [接続（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、[ワイヤレス コントローラ（Wireless Controllers）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [ダウンロード（Download）] > [コントローラの一括更新（Bulk Update Controllers）] をクリックします。

ステップ 4 [CSV ファイルの選択（Select CSV File）] テキスト ボックスに CSV ファイル名を入力するか、または [参照（Browse）] をクリックして目的のファイルを特定します。

ステップ 5 [更新と同期（Update and Sync）] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからのコントローラ クレデンシャルの変更 （6 ページ）
再起動によるコントローラ変更の適用 （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）

再起動によるコントローラ変更の適用

再起動する前に、現在のコントローラの設定を保存する必要があります。コントローラを再起動するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[ワイヤレス コントローラ（Wireless Controller）] を選択して、[再起動（Reboot）] > [コントローラの再起動（Reboot Controllers）] をクリックします。

ステップ 2 必要に応じた [コントローラの再起動（Reboot Controllers）] オプションを選択します。

- [フラッシュへの設定の保存（Save Config to Flash）]：データはコントローラの不揮発性 RAM（NVRAM）に保存され、電源の再投入時にも保持されます。コントローラを再起動した場合、設定が保存されていないと、適用した変更はすべて失われます。
- [AP の再起動（Reboot APs）]：他の更新を行った後のアクセス ポイントの再起動を有効にするには、このチェックボックスをオンにします。
- [AP イメージの切り替え（Swap AP Image）]：AP イメージをスワップした際に、コントローラおよび AP を再起動するかどうかを示します。[はい（Yes）] または [いいえ（No）] のいずれかになります。

ステップ 3 [OK] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからのコントローラ クレデンシャルの変更 （6 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）

コントローラへのソフトウェアのダウンロード

コントローラにソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controllers）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [ダウンロード（Download）] をクリックし、次のいずれかのオプションを選択します。

- **[ソフトウェアのダウンロード（TFTP）（Download Software TFTP）]**
- **[ソフトウェアのダウンロード（FTP）（Download Software FTP）]**
- **[ソフトウェアのダウンロード（SFTP）（Download Software SFTP）]**

ステップ 4 必要なフィールドに入力します。

ステップ 5 ダウンロードタイプを選択します。事前ダウンロードオプションは、選択したすべてのコントローラがリリース 7.0.x.x 以降を使用している場合のみ表示されます。

- [今すぐ（Now）]：ソフトウェアのダウンロードをただちに開始します。このオプションを選択した場合は、ステップ 7 に進みます。
- [スケジュール（Scheduled）]：スケジュール設定するダウンロード オプションを指定します。
  - [コントローラへのダウンロードのスケジュール（Schedule download to controller）]：ソフトウェアをコントローラにダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。
  - [AP へのソフトウェアの事前ダウンロード（Pre-download software to APs）]：ソフトウェアを AP に事前ダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。AP にイメージがダウンロードされ、コントローラの再起動時に、AP も再起動されます。AP ごとの [イメージの事前ダウンロード（Image Predownload）] ステータスを確認するには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [システム ジョブ（System Jobs）] > [ワイヤレス ポーラー（Wireless Poller）] > [AP イメージの事前ダウンロード ステータス（AP Image Pre-Download Status）]** でタスクを有効にし、[レポート起動パッド（Report Launch Pad）] から [AP イメージ事前ダウンロード（AP Image Predownload）] レポートを実行します。
  - [FlexConnect AP アップグレード（FlexConnect AP Upgrade）]：ローカル ネットワークのモデルごとに 1 つのアクセス ポイントでイメージをダウンロードできるようにするには、このオプションを選択します。残りのアクセス ポイントは、ローカル ネットワークを介してプリイメージ ダウンロード機能を使用して、マスターアクセスポイントからイメージをダウンロードします。これにより、WAN の遅延時間が短縮されます。

ステップ 6 [スケジュール（Schedule）] オプションを選択します。

すべての AP がソフトウェアの事前ダウンロードを完了できるように、ダウンロードと再起動の間に十分な時間（少なくとも 30 分）をスケジュール設定します。スケジュール設定された再起動時刻に、いずれかの AP で事前ダウンロードが進行中の場合、コントローラは再起動しません。すべての AP の事前ダウンロードが終了するまで待ってから、コントローラを手動で再起動する必要があります。

ステップ 7 ユーザ名、パスワード、およびポートを含めて、FTP クレデンシャルを入力します。

特殊文字の @、#、^、*、~、_、-、+、=、{、}、[、]、:、.、および / をパスワードに使用できます。$、'、\、%、&、(、)、;、"、<、>、,、?、および | のような特殊文字は FTP パスワードに使用できません。特殊文字「!」（感嘆符）は、パスワード ポリシーが無効の場合に使用できます。

ステップ 8 ファイルの格納場所として [ローカル マシン（Local machine）] または [FTP サーバ（FTP Server）] を選択します。[FTP サーバ（FTP Server）] を選択すると、インストール中に指定した FTP ディレクトリにソフトウェア ファイルがアップロードされます。

ステップ 9 [ダウンロード（Download）] をクリックします。

転送がタイムアウトした場合は、[ファイルの格納場所（File is located on）] フィールドで [FTP サーバ（FTP Server）] オプションを選択すると、サーバ ファイル名が読み込まれて Cisco Prime Infrastructure によって再試行されます。

FTP/TFTP サーバへのコントローラ設定とログ ファイルのアップロード

指定した TFP または TFTP サーバに、コントローラ システム設定をファイルとしてアップロードできます。 Prime Infrastructure では、ファイルのアップロードおよびダウンロードに、ファイル FTP および TFTP の両方がサポートされています。コントローラからファイルをアップロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [コマンド（Commands）]** の順に選択します。

ステップ 4 [FTP] または [TFTP] オプション ボタンを選択し、[コントローラからファイルをアップロード（Upload File from ）] を選択して [実行（Go）] をクリックします。

ステップ 5 必要なフィールドに入力します。

Prime Infrastructure は統合 TFTP および FTP サーバを使用します。これは、サードパーティ製の TFTP および FTP サーバを Prime Infrastructure と同じワークステーション上で実行できないことを意味します。 Prime Infrastructure とサードパーティ製サーバが、同一の通信ポートを使用するためです。

ステップ 6 [OK] をクリックします。選択したファイルが、[ファイル名（File Name）] テキスト ボックスに入力した名前で、TFTP または FTP サーバにアップロードされます。

コントローラへの IDS シグネチャのダウンロード

Prime Infrastructure では、コントローラに侵入検知システム（IDS）シグネチャ ファイルをダウンロードできます。ローカル マシンから IDS シグネチャ ファイルをダウンロードするように指定すると、 Prime Infrastructure は次の 2 段階動作を開始します。

1. 管理者ワークステーションから Prime Infrastructure の組み込み TFTP サーバにローカル ファイルがコピーされます。
2. コントローラがそのファイルを取得します。

IDS シグネチャ ファイルが、すでに Prime Infrastructure サーバの TFTP ディレクトリにある場合、ダウンロードした Web ページで自動的にそのファイル名が読み込まれます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、**[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [IDS シグニチャのダウンロード（Download IDS Signatures）]** をクリックします。

ステップ 4 必要なフィールドに入力します。

ステップ 5 [ダウンロード（Download）] をクリックします。

転送がタイムアウトした場合は、[ファイルの格納場所（File is located on）] フィールドで [FTP サーバ（FTP Server）] オプションを選択すると、サーバ ファイル名が読み込まれて Prime Infrastructure によって再試行されます。

関連トピック

Cisco Prime Infrastructure でのコントローラの表示 （3 ページ）
再起動によるコントローラ変更の適用 （9 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）

コントローラへの圧縮された Web 認証ログイン ページ情報のダウンロード

Web 認証ログイン ページの表示に使用するページおよびイメージ ファイルを圧縮して、Web 認証バンドルと呼ばれるファイルをコントローラにダウンロードできます。

コントローラでは、サイズが 1 MB 以下の .tar または .zip ファイルを受け入れます。1 MB の制限には、バンドル内の非圧縮ファイルの合計サイズが含まれます。

カスタマイズ Web 認証バンドルをコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [カスタマイズされた WebAuth のダウンロード（Download Customized WebAuth）]** をクリックします。

ステップ 4 サンプルの login.tar バンドル ファイルをダウンロードするには、表示されたプレビュー イメージをクリックして login.html ファイルを編集し、.tar または .zip ファイルとして保存します。このファイルには、Web 認証の表示に必要なページおよびイメージ ファイルが含まれています。

ステップ 5 .tar または .zip ファイルをコントローラにダウンロードします。

ステップ 6 ファイルが置かれている場所を選択します。

ローカル マシンを選択した場合は、.zip または .tar のファイル タイプでアップロードできます。 Prime Infrastructure は .zip ファイルを .tar ファイルに変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイル以外は指定できません。

ステップ 7 必須フィールドに入力して [ダウンロード（Download）] をクリックします。

転送がタイムアウトした場合は、[ファイルの格納場所（File is located on）] フィールドで [FTP サーバ（FTP Server）] オプションを選択すると、サーバ ファイル名が読み込まれて Prime Infrastructure によって再試行されます。

Prime Infrastructure によってダウンロードが完了すると、新しいページが表示され、認証が可能になります。

関連トピック

Cisco Prime Infrastructure でのコントローラの表示 （3 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）

コントローラへのベンダーデバイス証明書のダウンロード

各ワイヤレス デバイス（コントローラ、アクセス ポイント、およびクライアント）には独自のデバイスの証明書があります。ご自身のベンダー固有のデバイス証明書を使用する場合は、その証明書をコントローラにダウンロードする必要があります。

ベンダー デバイス証明書をコントローラにダウンロードするには、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	**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。	
ステップ 2	**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** の順に選択します（[ワイヤレスコントローラ（Wireless Controller）] を展開し、特定のコントローラ シリーズを選択します）。	
ステップ 3	目的のコントローラの [デバイス名（Device Name）] をクリックします。	
ステップ 4	[設定（Configuration）] タブをクリックします。	

	コマンドまたはアクション	目的
ステップ 5	**[システム（System）] > [コマンド（Commands）]** の順に選択します。	
ステップ 6	[アップロード/ダウンロードコマンド（Upload/Download Commands）] で、転送プロトコルを選択します。	
ステップ 7	インストールする証明書を選択し、[実行（Go）] をクリックします。	
ステップ 8	必要な詳細情報を入力し、[OK] をクリックします。	

関連トピック

コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）
コントローラへの CA 証明書のダウンロード （14 ページ）

TFTPを介したコントローラへのベンダーデバイス証明書のダウンロード

ベンダーデバイス証明書を TFTP のみを介してコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [ダウンロード（Download）] > [ベンダー デバイス証明書のダウンロード（Download Vendor Device Certificate）] をクリックします。

ステップ 4 必須フィールドに入力して [ダウンロード（Download）] をクリックします。

コントローラへの CA 証明書のダウンロード

コントローラとアクセス ポイントには、デバイス証明書の署名と確認に使用される認証局（CA）証明書があります。コントローラには、シスコによりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時にワイヤレス クライアントを認証するために、（PAC を使用していない場合）EAP-TLS と EAP-FAST により使用される場合があります。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、その証明書をコントローラにダウンロードする必要があります。

ベンダー CA 証明書をコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [ベンダー デバイス証明書のダウンロード（Download Vendor Device Certificate）]** をクリックします。

ステップ 4 必須フィールドに入力して [ダウンロード（Download）] をクリックします。

関連トピック

再起動によるコントローラ変更の適用 （9 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）
Cisco Prime Infrastructure でのコントローラの表示 （3 ページ）

ネットワーク アシュアランスの設定

デバイス公開証明書のダウンロードおよびインストール

シスコ ワイヤレス サービス アシュアランスに使用されるデバイス公開証明書は、シスコの CA サーバによって署名された CA 署名付き証明書です。

（注） `cmca2.cer` 証明書は、Prime Infrastructure 3.4 でプレインストールとして提供されています。この証明書は、ダウンロードおよびインストールが不要な場合もあります。

ステップ 1 1.https://www.cisco.com/security/pki/ にアクセスし、シスコの CA とその公開証明書の一覧を確認します。

ステップ 2 FTP サーバ上でネットワーク アシュアランスを有効化する WLC に必要なすべての `.cer` ファイルをダウンロードします。

例：ftp.abc.com

ステップ 3 Prime Infrastructure コマンド シェルに管理者ユーザとしてログインします。

ステップ 4 FTP サーバからデフォルト リポジトリに証明書をコピーします。

例：次のコマンドを使用して、`cmca2` 証明書をコピーします。

```
CLI admin# copy ftp://ftp.abc.com/cmac2.cer disk:/defaultRepo
```

ステップ 5 すべての証明書について、Prime Infrastructure サーバに CA 証明書信頼をインストールします。

例：次のコマンドを使用して、`cmca2.cer` をインストールします。

```
CLI admin# ncs key importcacert cmca2 cmca2.cer repository defaultRepo
```

```
The NCS server is running.Changes will take affect on the next server restart

Importing certificate to trust store
```

ステップ 6 Prime Infrastructure サーバにすべての証明書をインストールしたら、証明書を有効にするため、サーバを再起動する必要があります。

（注） ネットワーク アシュアランス処理によってデバイス処理エラーが報告される場合は、ifm_sam.log ファイルを
デバイスの公開証明書を取得してください。

例：次に、 `ifm_sam.log` ファイルのサンプルを示します。

```
2017-10-30 21:34:01,890 [https-jsse-nio-443-exec-1] ERROR logging - IFM-SAM-ERROR: Sensor device X.50
 mentioned below is not properly signed:
**********START******************************

MIIEdDCCA1ygAwIBAgIKG3upVgAAAA32cTANBgkqhkiG9w0BAQsFADA2MQ4wDAYDVQQKEwVDaXNjbzEkMCIGA1UEAxMbQ2lzY28gT
Y3R1cmluZyBDQSBTSEEyMB4XDTE1MTAwNzIzMDg1OFoXDTI1MTAwNzIzMTg1OFowgZQxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDV
ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczEjMCEGA1UEAxMaQUlSLUNUODUxMC1LOS1mNGNr
wYTI3MDAxIDAeBgkqhkiG9w0BCQEWEXN1cHBvcnRAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3pBr
23KzNGSGB1bAV71Y+YmPt+oJR7fVpZI/Vv39ncFcRGCpP0RH6ics9l20j0O/9BLQOwkRJ19d91GoPvCGc9hfU9W9ctRikg3ZPIOa
23KzNGSGB1bAV71Y+YmPt+oJR7fVpZI/Vv39ncFcRGCpP0RH6ics9l20j0O/9BLQOwkRJ19d91GoPvCGc9hfU9W9ctRikg3ZPIOa
VUjWI/l12zfEAuP9dsXdy29h5I0x19QfTCCjqJUtgTcoDx4QL2WjerZopCmCBlGL5ICFm+SeXADCh9OpZn1lbp4lQIDAQABo4IBIz
AQDAgWgMB0GA1UdDgQWBBQsA0phzTpk5VNFflYOK2mU8OZnmjAfBgNVHSMEGDAWgBR613mVyrtIK7hVFP2jwA+8pw+WGTBABgNVHR
3MDWgM6Axhi9odHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NtY2EyLmNybDBNBggrBgEFBQcBAQRBMD8wPQYI
HMAKGMWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9jbWNhMi5jZXIwPwYJKwYBBAGCNxQCBDIeMABJAFAA
BuAHQAZQByAG0AZQBkAGkAYQB0AGUATwBmAGYAbABpAG4AZTANBgkqhkiG9w0BAQsFAAOCAQEANOilUIBV7mk3H/rhLGCW7acwiPx
WOfSZdy0EukZ8gCoKScZyLHp7IEkDGueb4CMJnPi4oJOeDw2xrxS/AkSLWUw5aQ585Qi2J2JXlLAXQ9pgaatyZ0yjm+jkkISwB18k
by2ApXdI2HqpNateGZvB0NJ4ww6xnJMIUaSdGl+50CrKWLoCssH2DHp6Qo9a8oTZtM6cG/c5wsjDn0tSfFbt4+3JzUPLnPlAff1Sl
a8pODdVe3BFe44pyMdgGCnVZnqJcevZiWtHMCG5OjaggbBhC0RObGJBxKOAGRgNlUej8hg1hWw==

**********END******************************

Check the CA Server for device X.509 Certificate is in Prime: 'ncs key listcacerts'.
```

証明書の詳細を確認し、CA サーバを特定するには、ツールを使用して証明書を Base64 フォーマットから .ce
換する必要があります。上記の例では、使用されている CA サーバは `Cisco Manufacturing CA (cmca2)` です。

関連トピック

コントローラへの NA サーバ CA 証明書のダウンロード （18 ページ）
ネットワーク アシュアランスの自己署名付き証明書を生成 （16 ページ）

ネットワーク アシュアランスの自己署名付き証明書を生成

Cisco Prime Infrastructure では、管理対象 WLC のワイヤレス クライアント情報のコレクションと関連するイベントをサポートしています。このデータ収集には、WLC から各プロセスに HTTPS 要求をルーティングする Prime Infrastructure サーバで実行する Apache HTTPD が必要です。WLC と Prime Infrastructure 間の通信は HTTPS 経由で行われます。つまり、WLC との通信には、PI サーバの秘密キー、証明書ファイル、CA 証明書が必要です。

1. Prime Infrastructure 3.4 をインストールすると、WSA コレクタに対して秘密キーと X.509 自己署名付き証明書のセットが自動的に生成され、次の場所にコピーされます。

   - **秘密キーの場所**：`/opt/CSCOlumos/wsa/apache/cert/server.key`

- **自己署名付き証明書ファイル（X.509 形式）の場所**：/localdisk/tftp または /localdisk/ftp
- **CA 証明書ファイルの場所**：/opt/CSCOlumos/conf/certs/server_rootcacert.pem

上記の場所にある各ファイルをコピーすると、独自の秘密キー、証明書、CA 署名付き証明書を使用できます。

例：https://[prime_server_ip]:8080

2. 自己署名付き証明書は、共通名（CN）として Prime Infrastructure サーバの eth0 インターフェイスの IP アドレスを使用します。自動的に生成された証明書の使用を続ける場合は、eth0 インターフェイスの IP アドレスを Prime Infrastructure サーバで使用する WLC の NA サーバ URL を設定する必要があります（手順 4 を参照）。例：https://[prime_server_ip]:8080

3. WLC との通信には自動的に生成された証明書で十分です。この使用を続ける場合は、以下の証明書を使用して WLC を設定する方法を参照してください。Prime サーバのホスト名または別の IP アドレスを使用して別の証明書セットを生成する場合は、次のコマンドを使用できます。

IP アドレスを使用した証明書の生成

- TFTP の使用：

```
/usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
/localdisk/tftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${IP_ADDR}"
```

- FTP の使用：

```
/usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
/localdisk/ftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${IP_ADDR}"
```

ここで、IP_ADDR は、キーおよび証明書を生成するための Prime Infrastructure サーバの IP アドレスです。

ホスト名を使用した証明書の生成

- TFTP の使用：

```
usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
/localdisk/tftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${PI_FQDN}
```

- FTP の使用：

```
usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
```

```
/localdisk/ftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${PI_FQDN}
```

ここで、PI_FQDN は Prime Infrastructure サーバの完全修飾ホスト名です。

（注） 証明書で指定された共通名（CN）が Prime Infrastructure サーバのホスト名の場合は、DNS が解決可能である必要があります。それ以外の場合は、共通名で Prime サーバの IP アドレスを指定する必要があります。

4. 証明書の生成後、/localdisk/tftp/prime-wsa-apache-server.crt または /localdisk/ftp/prime-wsa-apache-server.crt のファイルを Prime Infrastucture にワイヤレス クライアント情報を送信する各 WLC にアップロードする必要があります。

（注） TFTP/SFTP/FTP サーバを使用して証明書ファイルをプッシュする場合は、そのサーバで指定されたファイルをコピーする必要があります。

関連トピック

コントローラへの NA サーバ CA 証明書のダウンロード （18 ページ）

コントローラへの NA サーバ CA 証明書のダウンロード

WLC が Prime Infrastructure と通信するためには、認証のため、NA サーバ CA 証明書が必要です。

証明書をダウンロードする前に、証明書のセットを生成するか、独自の証明書を特定の場所にアップロードして Prime Infrastructure がそこから取得できるようにすることが必要になる場合があります。詳細については、関連するリンクを参照してください。

（注） HA セットアップでは、WLC に証明書を適用するときは、**[管理（Administration）] > [サーバ（Servers）] > [TFTP/FTP/SFTPサーバ（TFTP/FTP/SFTP Servers）]** で、セカンダリ サーバの IPアドレスを手動で追加する必要があります。証明書をアップロードするときも、ドロップダウン リストからセカンダリ サーバの IP アドレスを選択する必要があります。そうしないと、セカンダリ サーバでのフェールオーバー後に、デフォルトの IP アドレスが プライマリとしてリストされます。

TFTP ロケーションのローカル ディスクからコントローラに CA 証明書をダウンロードするには、次の手順に従います。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [NAサーバCA証明書のダウンロード（Download NA Server CA Certificate）]** の順にクリックします。

ステップ 4 ファイルの場所を選択し、必須フィールドに入力して、[ダウンロード（Download）] をクリックします。

コントローラへの NA サーバ CA 証明書のダウンロード

TFTP ロケーション、FTP ロケーション、SFTP ロケーション、または USB ロケーションから コントローラに CA 証明書をダウンロードするには、次の手順に従います。

（注） HA セットアップでは、WLC に証明書を適用するときは、**[管理（Administration）] > [サーバ（Servers）] > [TFTP/FTP/SFTPサーバ（TFTP/FTP/SFTP Servers）]** で、セカンダリ サーバの IP アドレスを手動で追加する必要があります。証明書をアップロードするときも、ドロップダウン リストからセカンダリ サーバの IP アドレスを選択する必要があります。そうしないと、セカンダリ サーバでのフェールオーバー後に、デフォルトの IP アドレスが プライマリとしてリストされます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 証明書をダウンロードするコントローラをクリックします。

ステップ 3 [設定（Configuration）] タブをクリックします。

ステップ 4 左サイドバーのメニューで、**[システム（System）] > [コマンド（Commands）]** の順にクリックします。

ステップ 5 ファイルの場所を選択し、ドロップダウン メニューから [NAサーバCA証明書のダウンロード（Download NA Server CA Certificate）] を選択します。

（注） このオプションは、AireOS 8.6 および 8.7 を実行している WLC の場合のみ使用可能です。

ステップ 6 [移動（Go）] をクリックします。

ステップ 7 必要な詳細情報を入力し、[OK] をクリックします。

関連トピック

ネットワーク アシュアランスの自己署名付き証明書を生成 （16 ページ）
ネットワーク アシュアランスの設定 （162 ページ）
再起動によるコントローラ変更の適用 （9 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）
Cisco Prime Infrastructure でのコントローラの表示 （3 ページ）

デバイス フラッシュへのコントローラ設定の保存

設定をフラッシュ メモリに保存するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[設定（Configure）] > [フラッシュへの設定の保存（Save Config to Flash）]** をクリックします。

関連トピック

データベースへのコントローラ設定の保存（同期） （20 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）
再起動によるコントローラ変更の適用 （9 ページ）

データベースへのコントローラ設定の保存（同期）

コントローラから設定を同期するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [同期（Sync）] をクリックし、[はい（Yes）] をクリックして続行します

関連トピック

デバイス フラッシュへのコントローラ設定の保存 （20 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）
再起動によるコントローラ変更の適用 （9 ページ）

コントローラの既存のテンプレートを検出

現在のテンプレートを検出するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[設定（Configure）] > [コントローラからのテンプレートの検出（Discover Templates from Controller）]** をクリックします。

[テンプレートの検出（Discover Templates）] ページには、検出されたテンプレートの数、各テンプレートのタイプ、および各テンプレートの名前が表示されます。テンプレート検出ツールでは、テンプレートをサポートしており、Cisco WLC 上で検出可能なすべての機能が検出されます。

ステップ 4 [検出されたテンプレートと上記のデバイスとの関連付けを作成する（Enabling this option will create association between discovered templates and the device listed above）] チェックボックスをオンにすると、検出されたテンプレートがデバイスの設定に関連付けられ、当該のコントローラに適用されていることが表示されます。

テンプレートの検出を実行した場合、実際に検出が実行される前に、コントローラから設定が更新されます。

ステップ 5 検出を続行するには、警告ダイアログボックスで [OK] をクリックします。

TACACS+ サーバ テンプレートの場合、サーバ IP アドレスおよびポート番号が同じで、サーバ タイプが異なるコントローラの設定は、単一のテンプレートに集約されます。このとき、対応するサーバ タイプが検出されたテンプレートに設定されます。TACACS+ サーバ テンプレートの場合、検出されたテンプレートの管理ステータスには、最初に見つかったサーバ IP アドレスおよびポート番号が同じコントローラの設定の管理ステータスが反映されます。

コントローラに適用されているテンプレートの表示

特定のコントローラに現在適用されているすべてのテンプレートを表示できます。 Prime Infrastructure は、パーティションに適用されているテンプレートのみを表示します。

適用されているテンプレートを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [設定（Configure）] > [コントローラに適用されているテンプレート（Templates Applied to a Controller）] をクリックします。

このページに、適用されている各テンプレート名、テンプレート タイプ、テンプレートの最終保存日、およびテンプレートの最終適用日が表示されます。

ステップ 4 テンプレート名のリンクをクリックして、テンプレートの詳細を表示します。詳細については、「コントローラで使用されている設定テンプレートの確認と関連付けの削除」を参照してください。

関連トピック

コントローラで使用されている設定テンプレートの確認と関連付けの削除 （6 ページ）
IP アドレスを保持したままのコントローラ交換 （22 ページ）

IP アドレスを保持したままのコントローラ交換

IP アドレスを変更せずに古いコントローラ モデルを新しいモデルに置き換える場合は、次の手順を実行します。

1. Cisco Prime Infrastructure から古いコントローラを削除して、デバイスが削除されたことを示す確認メッセージを待ちます。
2. 同じ IP アドレスの設定でコントローラを新しいモデルに置き換えます。
3. IP アドレスを Cisco Prime Infrastructure に再度追加します。

関連トピック

デバイス パラメータの編集

コントローラ プロパティの変更

デバイス名、場所、SNMP パラメータ、Telnet/SSH パラメータなどのコントローラ プロパティを変更するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 ワイヤレス コントローラを選択して [編集（Edit）] をクリックします。

ステップ 3 必要に応じてフィールドを変更し、次のいずれかのボタンをクリックします。

- **[更新（Update）]**
- **[更新と同期（Update & Sync）]**
- **[クレデンシャルの確認（Verify Credentials）]**
- [キャンセル（Cancel）]（以前またはデフォルトの設定に戻す場合）

[ネットワークデバイス（Network Devices）] テーブルからコントローラの一般システム プロパティを変更する

現在のコントローラの一般システム パラメータを表示するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [汎用 - システム（General - System）] の順に選択します。一般システム パラメータが表示されます。『*Cisco Prime Infrastructure Reference Guide*』を参照してください。

ステップ 4 必要な変更を行い、[保存（Save）] をクリックします。

コントローラで障害が発生した場合の AP への優先順位の割り当て

コントローラに障害が発生すると、アクセス ポイントに設定されたバックアップ コントローラは、非常に多くの検出と接続要求を急に受信することになります。コントローラが過負荷になった場合、一部のアクセス ポイントが拒否される場合があります。

フェールオーバーの優先順位をアクセス ポイントに割り当てることによって、拒否されるアクセス ポイントを制御できます。バックアップ コントローラが過負荷になった場合、優先度が高く設定されているアクセス ポイントの接続リクエストの方が、優先度の低いアクセス ポイントよりも優先されます。

アクセス ポイントのフェールオーバー優先度設定を設定するには、まず AP Failover Priority 機能を有効にする必要があります。

AP Failover Priority 機能を有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[汎用 - システム（General - System）] を選択します。

ステップ 4 [AP フェールオーバー優先度（AP Failover Priority）] ドロップダウン リストから、[有効（Enabled）] を選択します。

ステップ 5 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には、次の手順を実行します。

a) [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、AP 名を選択します。

b) [AP フェールオーバー優先度（AP Failover Priority）] ドロップダウン リストから、適切な優先度（[低（Low）]、[中（Medium）]、[高（High）]、[重要（Critical）]）を選択します。デフォルトの優先度は [低（Low）] です。

コントローラでの 802.3 ブリッジングの設定

コントローラは、一般的にレジやレジサーバで使用されるような 802.3 フレームおよびそれらを使用するアプリケーションをサポートしています。ただし、これらのアプリケーションをコントローラとともに使用するには、802.3 のフレームがコントローラ上でブリッジされている必要があります。

未加工の 802.3 フレームのサポートにより、コントローラは、IP 上で実行していないアプリケーション用の IP 以外のフレームをブリッジできるようになります。この未加工の 802.3 フレームの形式のみが、現在サポートされています。

Prime Infrastructure を使用して 802.3 ブリッジを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 [システム（System）] > [汎用 - システム（General - System）] の順に選択して、[一般（General）] ページにアクセスします。

ステップ 4 802.3 ブリッジをコントローラ上で有効にする場合は、[802.3 ブリッジ（802.3 Bridging）] ドロップダウン リストから [有効（Enable）] を選択し、無効にする場合は [無効（Disable）] を選択します。デフォルト値は [無効（Disable）] です。

ステップ 5 [保存（Save）] をクリックして変更を確定します。

コントローラでの 802.3 フロー制御の設定

フロー制御は、モデムなどの送信エンティティにより、データを持つ受信エンティティが過負荷にならないようにする手法です。受信側デバイスのバッファに空きがない場合、メッセージが送信側デバイスに送信され、バッファ内のデータが処理されるまで伝送は一時停止されます。

デフォルトでは、フロー制御は無効に設定されています。ポーズ フレームを受信するように Cisco スイッチを設定できますが、送信はできません。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 [システム（System）] > [一般 - システム（General - System）] の順に選択して、[一般（General）] ページにアクセスします。

ステップ 4 [802.3x フロー制御（802.3x Flow Control）] フィールドで [有効（Enable）] をクリックします。

[ネットワークデバイス（NetworkDevices）]テーブルからのLightweight AP Protocol 転送モードの設定

Lightweight Access Point Protocol 転送モードは、コントローラとアクセス ポイント間の通信レイヤを示します。Cisco IOS ベースの Lightweight アクセス ポイントは、レイヤ 2 Lightweight アクセス ポイント モードはサポートしていません。これらのアクセス ポイントは、レイヤ 3 でしか実行できません。

Prime Infrastructure ユーザ インターフェイスを使用して Cisco Unified Wireless Network ソリューションをレイヤ 3 からレイヤ 2 Lightweight アクセス ポイント転送モードに変換するには、次の手順を実行します。この手順を実行すると、コントローラが再起動して、関連付けられていたアクセス ポイントがコントローラと再度関連付けられるまで、アクセス ポイントはオフラインになります。

ステップ 1 コントローラとアクセス ポイントはすべて同じサブネット上に配置するようにします。

変換を実行する前に、コントローラおよび関連付けられるアクセス ポイントをレイヤ 2 モードで動作するように設定する必要があります。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 デバイス名をクリックし、[設定（Configuration）] タブをクリックしてから、**[システム（System）] > [一般 - システム（General - System）]** を選択して [一般（General）] ページにアクセスします。

a) Lightweight アクセス ポイント転送モードを [レイヤ 2（Layer2）] に変更し、[保存（Save）] をクリックします。

b) Prime Infrastructure に次のメッセージが表示された場合は、[OK] をクリックします。

例：

```
Please reboot the system for the CAPWAP Mode change to take effect.
```

ステップ 4 コントローラを選択し、**[再起動（Reboot）] > [コントローラの再起動（Reboot Controllers）]** をクリックします。

ステップ 5 [フラッシュへの設定の保存（Save Config to Flash）] オプションを選択します。

ステップ 6 コントローラが再起動したら、次の手順に従って CAPWAP 転送モードがレイヤ 2 になっていることを確認します。

a) **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。
b) 該当するコントローラのデバイス名をクリックします。
c) **[システム（System）]** > **[一般 - システム（General - System）]** ページで、現在の CAPWAP 転送モードが [レイヤ 2（Layer2）] であることを確認します。

これで、レイヤ 3 からレイヤ 2 への CAPWAP 転送モードの変換が完了しました。オペレーティング システムのソフトウェアによって、同じサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

アグレッシブ ロード バランシングとは

ルーティングでは、ロードバランシングとは、宛先アドレスからの距離が同じすべてのネットワーク ポートを介してトラフィックを分配するルータの機能のことです。優れたロードバランシング アルゴリズムでは、回線速度と信頼性の両方の情報を使用します。ロード バランシングを行うと、ネットワーク セグメントの使用率が増加するため、実質的にネットワーク帯域幅が増加します。

アグレッシブ ロード バランシングは、モバイル クライアントと関連付けられたアクセス ポイントの間で負荷をアクティブに分散させます。

リンク アグリゲーションとは

リンク集約によって、物理ポートをすべてグループ化してリンク集約グループ（LAG）を作成し、コントローラ上のポートを構成するために必要な IP アドレスの数を削減できます。4402 モデルでは、LAG を形成するために 2 つのポートが組み合わされます。4404 モデルでは、4 つのポートすべてが LAG を形成するため組み合わされます。

コントローラ上では、複数の LAG を作成できません。

LAG がコントローラ上で有効な場合、次の設定が変更されます。

- インターフェイス データベース内での設定の矛盾を避けるため、作成した動的インターフェイスが削除されます。
- インターフェイスは [動的 AP マネージャ（Dynamic AP Manager）] フラグを設定した状態では作成できません。

LAG の作成には、次のようなメリットがあります。

- リンクの 1 つがダウンした場合に、常にトラフィックが LAG 内の他のリンクに移動します。物理ポートの 1 つが動作している限り、システムは機能し続けます。
- 各インターフェイスに対して個別にバックアップ ポートを設定する必要がありません。
- アプリケーションは論理ポートを 1 つしか認識しないため、複数の AP-manager インターフェイスは必要ありません。

LAG 設定に変更を加えると、変更を有効にするためにコントローラを再起動する必要があります。

ワイヤレス管理の前提条件

IPsec 動作により、ワイヤレスによる管理は WPA、静的 WEP、または VPN パススルー WLAN でログインしているオペレータのみが実行できます。ワイヤレス管理は、IPsec WLAN を経由してログインしようとしているクライアントは実行できません。

モビリティ アンカー キープアライブ間隔とは

クライアントが別のアクセスポイントへの接続を試みるまでの遅延時間を指定できます。この機能を使用することで、エラーがすばやく特定され、クライアントが問題のあるコントローラから移動し、別のコントローラに接続されるので、コントローラのエラー後にクライアントが別のアクセス ポイントに接続するためにかかる時間が短縮されます。

関連トピック

コントローラへのソフトウェアのダウンロード （9 ページ）
コントローラの工場出荷時設定の復元 （27 ページ）
コントローラでの日時の設定 （28 ページ）

コントローラの工場出荷時設定の復元

コントローラの設定を工場出荷時の初期状態にリセットできます。この操作により、すべての適用および保存されている設定パラメータが上書きされます。コントローラの再初期化を確認するプロンプトが表示されます。

すべての設定データ ファイルが削除され、再起動時にコントローラが元の未設定状態に復元されます。これにより、すべての IP 設定が削除されるため、シリアル接続で基本設定を復元する必要があります。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 このページにアクセスするには、左側のサイドバーのメニューから **[システム（System）]** > **[コマンド（Commands）]** を選択し、[管理コマンド（Administrative Commands）] ドロップダウン リストから [工場出荷時の初期状態にリセット（Reset to Factory Default）] を選択して、[実行（Go）] をクリックします。

ステップ 4 設定の削除を確定した後に、コントローラをリブートし、[保存せずに再起動（Reboot Without Saving）] オプションを選択する必要があります。

関連トピック

コントローラへのソフトウェアのダウンロード （9 ページ）

コントローラでの日時の設定

コントローラで現在の時刻と日付を手動で設定できます。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 このページにアクセスするには、左側のサイドバーのメニューから **[システム（System）]** > **[コマンド（Commands）]** を選択し、[設定コマンド（Configuration Commands）] ドロップダウン リストから [システム時刻の設定（Set System Time）] を選択して [実行（Go）] をクリックします。

ステップ 4 必須パラメータを変更します。

- [現在時刻（Current Time）]：システムで現在使用されている時刻を表示します。
- [月/日/年（Month/Day/Year）]：ドロップダウンリストから、月、日、年を選択します。
- [時/分/秒（Hour/Minutes/Seconds）]：ドロップダウンリストから、時、分、秒を選択します。
- [デルタ（時間）（Delta (hours)）]：GMT（グリニッジ標準時）からのオフセットをプラスまたはマイナスの時間単位で入力します。
- [デルタ（分）（Delta (minutes)）]：GMT（グリニッジ標準時）からのオフセットをプラスまたはマイナスの分単位で入力します。
- [夏時間（Daylight Savings）]：夏時間を有効にする場合は、選択します。

コントローラの設定ファイルおよびログファイルをTFTPサーバにアップロードする

コントローラからローカル TFTP（Trivial File Transfer Protocol）サーバにファイルをアップロードできます。**[管理（Administration）]** > **[システム設定（System Settings）]** > **[サーバ設定（Server Settings）]** ページで、TFTP を有効にして [デフォルト サーバ（Default Server）] オプションを使用する必要があります。

Prime Infrastructure では統合 TFTP サーバを使用しています。これは、サードパーティ製の TFTP サーバが Prime Infrastructure と同じワークステーション上では実行できないことを意味します。 Prime Infrastructure とサードパーティ製の TFTP サーバが、同一の通信ポートを使用するためです。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[コマンド（Commands）]** の順に選択します。

ステップ 4 [アップロード/ダウンロード コマンド（Upload/Download Commands）] ドロップダウン リストから、[コントローラからファイルをアップロード（Upload File from Controller）] を選択して [実行（Go）] をクリックします。

デフォルトでは、コンフィギュレーション ファイルの暗号化は無効になっています。コンフィギュレーション ファイルは暗号化なしでアップロードされるため、安全ではありません。

ステップ 5 ファイルをアップロードする前に暗号化を有効にするには、[コントローラからのファイルのアップロード（Upload File from Controller）] ページの下部にあるリンクをクリックします。

ステップ 6 必須フィールドに入力して [OK] をクリックします。選択したファイルが指定した名前の TFTP サーバにアップロードされます。

関連トピック

コントローラでの日時の設定 （28 ページ）
コントローラへのソフトウェアのダウンロード （9 ページ）
コントローラの工場出荷時設定の復元 （27 ページ）

コントローラへのソフトウェアのダウンロード

ローカル TFTP（Trivial File Transfer Protocol）サーバからコントローラにコンフィギュレーション ファイルをダウンロードできます。

Prime Infrastructure は統合 TFTP サーバを使用します。これは、サードパーティ製の TFTP サーバは Prime Infrastructure と同じワークステーション上では実行できないことを意味します。Cisco Prime Infrastructure とサードパーティ製 TFTP サーバが、同一の通信ポートを使用するためです。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [コマンド（Commands）] の順に選択します。

ステップ 4 [アップロード/ダウンロード コマンド（Upload/Download Commands）] ドロップダウン リストから、[設定のダウンロード（Download Config）] を選択して、[実行（Go）] をクリックします。

ステップ 5 必須フィールドに入力して [OK] をクリックします。

関連トピック

コントローラでの日時の設定 （28 ページ）
コントローラの設定ファイルおよびログ ファイルを TFTP サーバにアップロードする （28 ページ）
コントローラの工場出荷時設定の復元 （27 ページ）

単一コントローラでのインターフェイスの設定

インターフェイスを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [インターフェイス（Interfaces）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、**[インターフェイスの追加（Add Interface）] > [実行（Go）]** を選択します。

ステップ 5 必要なフィールドに入力したら、[保存（Save）] をクリックします。

関連トピック

コントローラでのインターフェイスの表示 （30 ページ）
コントローラからの動的インターフェイスの削除 （31 ページ）
NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （33 ページ）
有線コントローラへのゲスト アカウント アクセスの設定 （38 ページ）

コントローラでのインターフェイスの表示

既存のインターフェイスを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [インターフェイス（Interfaces）]** の順に選択します。次のパラメータが表示されます。

- [チェックボックス（Check box）]：削除する動的インターフェイスを選択するチェックボックス。[コマンドの選択（Select a command）] ドロップダウン リストから [動的インターフェイスの削除（Delete Dynamic Interfaces）] を選択します。

- [インターフェイス名（Interface Name）]：インターフェイスのユーザ定義名（例：Management、Service-Port、Virtual）。
- [VLAN ID（VLAN Id）]：0（タグなし）～ 4096 の VLAN 識別子、または [N/A]。
- [検疫（Quarantine）]：インターフェイスに検疫 VLAN ID が設定されている場合は、このチェックボックスをオンにします。
- [IP アドレス（IP Address）]：インターフェイスの IP アドレス。
- [インターフェイス タイプ（Interface Type）]：[静的（Static）]（管理、AP-Manager、サービス ポート、および仮想インターフェイス）または [動的（Dynamic）]（オペレータ定義インターフェイス）。
- [AP 管理ステータス（AP Management Status）]：AP 管理インターフェイスのステータス。パラメータには [有効（Enabled）]、[無効（Disabled）]、および [N/A] があります。管理ポートのみがリダンダンシー マネジメント インターフェイスのポートとして設定できます。

関連トピック

コントローラ インターフェイス グループの表示と管理 （32 ページ）

コントローラからの動的インターフェイスの削除

インターフェイス グループに割り当てられている動的インターフェイスは削除できません。動的インターフェイスを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから **[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[インターフェイス（Interfaces）]** の順に選択します。

ステップ 4 削除する動的インターフェイスのチェックボックスをオンにして、[コマンドの選択（Select a command）] ドロップダウン リストから [動的インターフェイスの削除（Delete Dynamic Interfaces）] を選択します。

ステップ 5 [OK] をクリックして削除を実行します。

関連トピック

コントローラ インターフェイス グループの表示と管理 （32 ページ）
コントローラでのインターフェイスの表示 （30 ページ）

コントローラ システム インターフェイス グループを使用したコントローラグループへのインターフェイス変更の適用

インターフェイス グループは、インターフェイスの論理的なグループです。インターフェイス グループを使用すると、同じインターフェイス グループを複数の WLAN で設定するユーザ設定や、AP グループごとに WLAN インターフェイスをオーバーライドすることが容易になります。インターフェイス グループには検疫済みまたは検疫済みでないインターフェイスを排他的に含めることができます。1 つのインターフェイスを複数のインターフェイス グループに含めることができます。

コントローラ システム インターフェイス グループを設定する場合は、次の推奨事項に従ってください。

- インターフェイス グループ名とインターフェイス名が異なることを確認します。
- ゲスト LAN インターフェイスは、インターフェイス グループに含めることはできません。

インターフェイス グループ機能は、シスコ ワイヤレス コントローラ ソフトウェア リリース 7.0.116.0 以降でサポートされます。

関連トピック

コントローラ インターフェイス グループの表示と管理 （32 ページ）
NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （33 ページ）

コントローラ インターフェイス グループの表示と管理

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]> [インターフェイス グループ（Interface Groups）]** を選択します。

次のパラメータが表示されます。

- [名前（Name）]：インターフェイス グループのユーザ定義名（例：group1、group2）。
- [説明（Description）]：（任意）インターフェイス グループの説明。
- [インターフェイス（Interfaces）]：グループに属しているインターフェイスの数。

ステップ 4 既存のインターフェイス グループを表示するには、[インターフェイス グループ名（Interface Group Name）] リンクをクリックします。

[インターフェイス グループの詳細（Interface Groups Details）] ページが表示され、インターフェイス グループの詳細と、特定のインターフェイス グループの一部を構成するインターフェイスの詳細が示されます。

ステップ 5 インターフェイス グループを追加するには、次の手順を実行します。

a) [コマンドの選択（Select a command）] ドロップダウン リストから、[インターフェイス グループの追加（Add Interface Group）] を選択し、[実行（Go）] をクリックします。

b) 必須フィールドに入力し、[追加（Add）] をクリックします。

c) [インターフェイス（Interface）] ダイアログボックスが表示されます。

d) グループに追加するインターフェイスを選択して、[選択（Select）] をクリックします。

ステップ 6 インターフェイス グループを削除するには、次のようにします。

a) [コマンドの選択（Select a command）] ドロップダウン リストから、[インターフェイス グループの削除（Delete Interface Group）] を選択し、[実行（Go）] をクリックします。

（注） WLAN、AP グループ、WLAN の外部コントローラ マッピング、WLAN テンプレート、および AP グループ テンプレートに割り当てられているインターフェイス グループを削除できます。

b) [OK] をクリックして削除を実行します。

ステップ 7 [インターフェイス グループ（Interface Group）] ページからインターフェイスを削除するには、インターフェイスを選択して [削除（Remove）] をクリックします。

ステップ 8 [保存（Save）] をクリックして、変更を確定します。

関連トピック

コントローラ システム インターフェイス グループを使用したコントローラ グループへのインターフェイス変更の適用 （32 ページ）
NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （33 ページ）

NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御

Cisco Network Admission Control（NAC）アプライアンス（Cisco Clean Access（CCA）とも呼ばれます）は、ネットワーク管理者がユーザにネットワークへの接続を許可する前に、有線、無線、およびリモート ユーザとそのマシンを認証、承認、評価、修復できる、ネットワーク アドミッション コントロール（NAC）製品です。Cisco NAC アプライアンスは、マシンがセキュリティ ポリシーに準拠しているかどうかを判別し、脆弱性を修復してから、ネットワークへのアクセスを許可します。NAC アプライアンスは、インバンド モードとアウトオブバンド モードの 2 つのモードで利用できます。顧客は、必要に応じて特定の種類のアクセスを対象にし、2 つのモードを展開できます（例：無線ユーザをサポートする場合はインバンド、有線ユーザをサポートする場合はアウトオブバンド）。

関連トピック

SNMP NAC の使用時の前提条件 （34 ページ）
コントローラでの SNMP NAC の設定 （35 ページ）

SNMP NAC の使用時の前提条件

SNMP NAC アウトオブバンド統合を使用する場合は、次のガイドラインに従ってください。

- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。したがって、複数の NAC アプライアンスの導入を必要とする場合があります。
- NACアプライアンスでは静的なVLANマッピングがサポートされているため、コントローラ上で設定されているインターフェイスごとに一意の検疫 VLAN を設定する必要があります。たとえば、コントローラ 1 で 110 という検疫 VLAN を設定し、コントローラ 2 で 120 という検疫 VLAN を設定します。ただし、2 つの WLAN またはゲスト LAN が同一の分散システム インターフェイスを使用している場合、ネットワーク内に導入された NAC アプライアンスが 1 つならば、同じ検疫 VLAN を使用する必要があります。NAC アプライアンスは、検疫とアクセスの一意の VLAN マッピングをサポートします。
- セッションの失効に基づくポスチャ再評価の場合、NAC アプライアンスと WLAN の両方にセッション タイムアウトを設定し、WLAN でのセッションの失効の値が NAC アプライアンスでの失効の値より大きいことを確認します。
- オープン WLAN でセッション タイムアウトが設定されると、[検疫（Quarantine）] 状態にあるクライアントのタイムアウトは NAC アプライアンスのタイマーによって判定されます。Web 認証を使用する WLAN においてセッションがタイムアウトすると、クライアントはコントローラから認証解除されるので、ポスチャ検証を再度実行する必要があります。
- NACアウトオブバンド統合がサポートされるのは、WLANがFlexConnectの中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。
- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アウトオブバンド統合は、WLAN AAA オーバーライド機能では使用できません。
- レイヤ 2 およびレイヤ 3 認証はすべて、検疫 VLAN で実行されます。外部 Web 認証を使用するには、外部 Web サーバからの HTTP トラフィックおよび外部 Web サーバへの HTTP トラフィックを許可するとともに、検疫 VLAN でのリダイレクト URL を許可するように NAC アプライアンスを設定する必要があります。

詳細については、「Cisco NAC Appliance Configuration」を参照してください。

RADIUS NAC の使用時の前提条件

RADIUS NAC を使用する場合には、次のガイドラインに従ってください。

- RADIUS NAC は、802.1x/WPA/WPA2 レイヤ 2 セキュリティを備えた WLAN でのみ使用できます。
- RADIUS NAC は、FlexConnect ローカル スイッチングが有効の場合は有効にできません。
- RADIUS NAC を設定する場合は、AAA オーバーライドを有効にしてください。

関連トピック

NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （33 ページ）

コントローラでの SNMP NAC の設定

SNMP NAC アウトオブバンド統合を設定するには、次のワークフローを実行します。

1. 動的インターフェイスに対して検疫 VLAN を設定します。NAC アプライアンスでは静的な VLAN マッピングがサポートされているため、コントローラ上で設定されているインターフェイスごとに一意の検疫 VLAN を設定する必要があります。
2. WLAN またはゲスト LAN に NAC アウトオブバンド サポートを設定します。アクセス ポイント グループ VLAN で NAC サポートを有効にする場合は、先に WLAN またはゲスト LAN で NAC を有効にする必要があります。
3. 特定の AP グループに対して NAC アウトオブバンド サポートを設定します。特定のアクセス ポイント グループに NAC アウトオブバンド サポートを設定します。

関連トピック

検疫 VLAN の設定（SNMP NAC） （35 ページ）
WLAN またはゲスト LAN での NAC の有効化（SNMP NAC） （36 ページ）
AP グループの NAC アウトオブバンド サポートの設定（SNMP NAC） （37 ページ）

検疫 VLAN の設定（SNMP NAC）

動的インターフェイスに対して検疫 VLAN を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 [IP アドレス（IP Address）] 列でアウトオブバンド統合の設定を行うコントローラをクリックして選択します。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [インターフェイス（Interfaces）]** を選択します。

ステップ 4 [インターフェイス名（Interface Name）] をクリックします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [インターフェイスの追加（Add Interface）] を選択し、[実行（Go）] をクリックします。

ステップ 6 [インターフェイス名（Interface Name）] テキスト ボックスに、「quarantine」など、このインターフェイスの名前を入力します。

ステップ 7 [VLAN ID] テキスト ボックスに、アクセス VLAN ID としてゼロ以外の値（「10」など）を入力します。

ステップ 8 インターフェイスに検疫 VLAN ID が設定されている場合は、[検疫（Quarantine）] チェックボックスをオンにします。

ステップ 9 このインターフェイスの残りのフィールド（[IP アドレス（IP address）]、[ネットマスク（netmask）]、[デフォルト ゲートウェイ（default gateway）] など）を設定します。

（注） ワイヤレス コントローラを Prime Infrastructure に追加する際の問題を避けるため、動的インターフェイスを Prime Infrastructure と同じサブネットに配置しないでください。

ステップ 10 プライマリおよびセカンダリ DHCP サーバの IP アドレスを入力します。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

WLAN またはゲスト LAN での NAC の有効化（SNMP NAC） （36 ページ）
AP グループの NAC アウトオブバンド サポートの設定（SNMP NAC） （37 ページ）

WLAN またはゲスト LAN での NAC の有効化（SNMP NAC）

WLAN またはゲスト LAN で NAC アウトオブバンド サポートを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLANs] > [WLAN] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [WLAN の追加（Add a WLAN）] を選択し、[実行（Go）] をクリックします。

ステップ 5 このコントローラに適用する作成済みのテンプレートがある場合には、ドロップダウン リストからゲスト LAN テンプレート名を選択します。そうでない場合には、[ここをクリック（click here）] リンクをクリックして新しいテンプレートを作成します。

ステップ 6 [詳細設定（Advanced）] タブをクリックします。

ステップ 7 この WLAN またはゲスト LAN に SNMP NAC サポートを設定するには、[] ドロップダウン リストから [SNMP NAC] を選択します。SNMP NAC サポートを無効にするには、[NAC ステージ（NAC Stage）] ドロップダウン リストから [なし（None）]（デフォルト値）を選択します。

ステップ 8 [適用（Apply）] をクリックして、変更を確定します。

関連トピック

AP グループの NAC アウトオブバンド サポートの設定（SNMP NAC） （37 ページ）
有線コントローラへのゲスト アカウント アクセスの設定 （38 ページ）

AP グループの NAC アウトオブバンド サポートの設定（SNMP NAC）

特定の AP グループに NAC アウトオブバンド サポートを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[WLAN（WLANs）] > [AP グループ VLAN（AP Groups VLAN）]** を選択し、[AP グループ（AP Groups）] ページを表示します。

ステップ 4 目的の AP グループの名前をクリックします。

ステップ 5 [インターフェイス名（Interface Name）] ドロップダウン リストから、検疫を有効にしたインターフェイスを選択します。

ステップ 6 この AP グループに SNMP NAC サポートを設定するには、[NAC の状態（Nac State）] ドロップダウン リストから [SNMP NAC] を選択します。NAC アウトオブバンドのサポートを無効にするには、[NAC の状態（NAC State）] ドロップダウン リストから [なし（None）]（デフォルト値）を選択します。

ステップ 7 [適用（Apply）] をクリックして、変更を確定します。

関連トピック

WLAN またはゲスト LAN での NAC の有効化（SNMP NAC） （36 ページ）
有線コントローラへのゲスト アカウント アクセスの設定 （38 ページ）
検疫 VLAN の設定（SNMP NAC） （35 ページ）

ネットワーク クライアントまたはユーザの NAC 状態の表示

クライアントの現在の状態（[検疫（Quarantine）] または [アクセス（Access）]）を表示するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択して、[クライアント（Clients）] を開きます。クライアントの検索を実行します。

ステップ 2 目的のクライアントの MAC アドレスをクリックして、[クライアント（Clients）] > [詳細（Detail）] ページを開きます。[セキュリティ情報（Security Information）] セクションの下に NAC の状態が [アクセス（Access）]、[無効（Invalid）]、または [検疫（Quarantine）] と表示されます。

関連トピック

コントローラでの SNMP NAC の設定 （35 ページ）

有線コントローラへのゲストアカウントアクセスの設定

有線ゲストアクセスでは、ゲストユーザがゲストアクセス用に指定および設定された有線イーサネット接続からゲスト アクセス ネットワークへ接続できます。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。

無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。有線ゲストアクセスは、スタンドアロン設定、またはアンカーおよび外部のコントローラを配置したデュアルコントローラ設定で設定することができます。この後者の設定は、有線ゲスト アクセス トラフィックをさらに分離するために使用されますが、有線ゲスト アクセスの展開には必須ではありません。

有線ゲスト アクセス ポートは、最初、レイヤ 2 アクセス スイッチか、有線ゲストのアクセス トラフィック用 VLAN インターフェイスで設定されたスイッチ ポートで終端します。有線ゲスト トラフィックは、その後、アクセス スイッチからワイヤレス LAN コントローラにトランキングされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。

2つのコントローラが使用されている場合、外部コントローラがスイッチから有線ゲスト トラフィックを受信し、次に有線ゲスト トラフィックをアンカーコントローラに転送します。アンカーコントローラも有線ゲストのアクセスに対して設定されています。有線ゲスト トラフィックがアンカー コントローラに正常に渡されると、外部コントローラとアンカー コントローラ間に双方向の Ethernet over IP（EoIP）トンネルが確立され、このトラフィックを処理します。

2つのコントローラが展開される際、有線ゲスト アクセスはアンカーと外部アンカーによって管理されますが、有線ゲスト アクセス クライアントではモビリティはサポートされません。この場合、DHCP およびクライアントの Web 認証は、アンカー コントローラによって処理されます。

ロールと帯域幅コントラクトを設定して割り当てることで、ネットワーク内の有線ゲスト ユーザに割り当てる帯域幅の量を指定できます。

関連項目

- 有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー

有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー

有線ゲスト ユーザ アクセスを設定して有効にするには、次のワークフローを実行します。

1. 有線ゲストアクセス用の動的インターフェイス（VLAN）を設定する。動的インターフェイスを作成して、有線ゲスト ユーザ アクセスを有効にします。
2. ゲスト ユーザ アクセス用の有線 LAN を設定する。新しい LAN（ゲスト LAN）を設定します。

関連トピック

有線ゲスト ユーザ アクセス用の動的インターフェイスの設定 （39 ページ）
ゲスト ユーザ アクセス用の有線 LAN の設定 （39 ページ）

有線ゲスト ユーザ アクセス用の動的インターフェイスの設定

ネットワークの有線ゲスト ユーザ アクセス用に動的インターフェイス（VLAN）を設定して有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）]>[インターフェイス（Interfaces）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [インターフェイスの追加（Add Interface）] を選択し、[実行（Go）] をクリックします。

ステップ 5 必要なフィールドに入力します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー （38 ページ）

ゲスト ユーザ アクセス用の有線 LAN の設定

ゲスト ユーザ アクセス用の有線 LAN を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックします。

ステップ 3 ゲスト ユーザ アクセス用の有線 LAN を設定するには、左側のサイドバーのメニューから [WLANs] > [WLAN 設定（WLAN configuration）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [WLAN の追加（Add a WLAN）] を選択し、[実行（Go）] をクリックします。

ステップ 5 このコントローラに適用する作成済みのテンプレートがある場合には、ドロップダウン リストからゲスト LAN テンプレート名を選択します。そうでない場合には、[ここをクリック（click here）] リンクをクリックして新しいテンプレートを作成します。

ステップ 6 [WLAN] > [新規テンプレート（New Template）] の [一般（General）] ページで、[プロファイル名（Profile Name）] テキスト ボックスにゲスト LAN を示す名前を入力します。入力する名前には、スペースを使用しないでください。

ステップ 7 [WLAN ステータス（WLAN Status）] フィールドの [有効（Enabled）] チェックボックスをオンにします。

ステップ 8 [入力インターフェイス（Ingress Interface）] ドロップダウン リストから、ステップ 3 で作成した VLAN を選択します。この VLAN は、レイヤ 2 アクセス スイッチを経由して、有線ゲスト クライアントとコントローラとの間のパスを提供します。

ステップ 9 [出力インターフェイス（Egress Interface）] ドロップダウン リストから、インターフェイスの名前を選択します。この WLAN は、有線ゲスト クライアント トラフィック用にコントローラから外部へのパスを提供します。設定にコントローラが 1 つしかない場合は、[出力インターフェイス（Egress Interface）] ドロップダウン リストから [管理（management）] を選択します。

ステップ 10 [セキュリティ（Security）] > [レイヤ 3（Layer 3）] タブをクリックして、デフォルトのセキュリティ ポリシー（Web 認証）を変更するか、または WLAN 固有の Web 認証（ログイン、ログアウト、ログイン失敗）ページとサーバ ソースを割り当てます。

a) セキュリティ ポリシーをパススルーに変更するには、[Web ポリシー（Web Policy）] チェックボックスをオンにして、[パススルー（Passthrough）] オプション ボタンを選択します。これでユーザは、ユーザ名やパスワードを入力しなくてもネットワークにアクセスできます。

[電子メールの入力（Email Input）] チェックボックスが表示されます。ユーザがネットワークに接続しようとした際に、電子メール アドレスの入力を求める場合は、このチェックボックスをオンにします。

b) カスタム Web 認証ページを指定するには、[グローバル Web 認証設定（Global WebAuth Configuration）] の [有効（Enabled）] チェックボックスをオフにします。

[Web 認証タイプ（Web Auth Type）] ドロップダウン リストが表示されたら、次のいずれかのオプションを選択して、無線ゲスト ユーザ用の Web ログイン ページを定義します。

[デフォルト内部（Default Internal）]：コントローラのデフォルト Web ログイン ページを表示します。これがデフォルト値です。

[カスタマイズされた Web 認証（Customized Web Auth）]：カスタム Web ログイン ページ、ログイン失敗ページ、およびログアウト ページを表示します。カスタマイズ オプションを選択した場合は、ログイン ページ、ログイン失敗ページ、およびログアウト ページを選択するための 3 つのドロップダウン リストが表示されます。これら 3 つすべてのオプションについてカスタマイズ ページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン リストで [なし（None）] を選択します。

[外部（External）]：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

外部認証を行う場合は、[Security] > [AAA] ペインで RADIUS サーバまたは LDAP サーバを選択できます。[セキュリティ（Security）] > [AAA] ペインで選択できるように、RADIUS 外部サーバと LDAP 外部サーバを事前に設定しておく必要があります。[RADIUS 認証サーバ（RADIUS Authentication

Servers）]、[TACACS+ 認証サーバ（TACACS+ Authentication Servers）]、および [LDAP サーバ（LDAP Servers）] ページでこれらのサーバを設定できます。

ステップ 11 [Web 認証タイプ（Web Authentication Type）] で [外部（External）] を選択した場合は、[セキュリティ（Security）] > [AAA] を選択し、ドロップダウン リストから RADIUS サーバと LDAP サーバを 3 つまで選択します。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 2 番めの（アンカー）コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

関連トピック

有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー （38 ページ）

コントローラでのゲスト LAN 入力インターフェイスの設定

入力インターフェイスを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）]>[インターフェイス（Interfaces）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [インターフェイスの追加（Add Interface）] を選択し、[実行（Go）] をクリックします。

ステップ 5 [インターフェイス名（Interface Name）] テキスト ボックスに、guestinterface など、このインターフェイスの名前を入力します。

ステップ 6 新しいインターフェイスの VLAN ID を入力します。

ステップ 7 [ゲスト LAN（Guest LAN）] チェックボックスをオンにします。

ステップ 8 プライマリ ポート番号とセカンダリ ポート番号を入力します。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

コントローラでのゲスト LAN 出力インターフェイスの設定 （42 ページ）

コントローラでのゲスト LAN 出力インターフェイスの設定

出力インターフェイスを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [インターフェイス（Interfaces）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [インターフェイスの追加（Add Interface）] を選択し、[実行（Go）] をクリックします。

ステップ 5 [インターフェイス名（Interface Name）] テキスト ボックスに、quarantine など、このインターフェイスの名前を入力します。

ステップ 6 [VLAN ID] テキスト ボックスに、アクセス VLAN ID としてゼロ以外の値（「10」など）を入力します。

ステップ 7 [検疫（Quarantine）] チェックボックスをオンにして、検疫 VLAN 識別子としてゼロ以外の値（「110」など）を入力します。

[検疫（Quarantine）] が有効なインターフェイスの場合、WLAN またはゲスト WLAN テンプレートの [詳細設定（Advanced）] タブで NAC サポートを有効にできます。

ステップ 8 IP アドレス、ネットマスク、およびゲートウェイの情報を入力します。

ステップ 9 プライマリ ポート番号とセカンダリ ポート番号を入力します。

ステップ 10 プライマリおよびセカンダリ DHCP サーバの IP アドレスを入力します。

ステップ 11 このインターフェイスの残りのフィールドを設定し、[保存（Save）] をクリックします。

これで、ゲスト アクセス用の有線 LAN を作成できるようになりました。

関連トピック

コントローラでのゲスト LAN 入力インターフェイスの設定 （41 ページ）

コントローラ サービス ポートでのネットワーク ルートの設定

[ネットワーク ルート（Network Route）] ページでは、コントローラのサービス ポートにルートを追加できます。このルートを使用することで、すべてのサービス ポート トラフィックを指定した管理 IP アドレスに送ることができます。

関連トピック

既存のコントローラ ネットワーク ルートの表示 （43 ページ）
コントローラへのネットワーク ルートの追加 （43 ページ）

既存のコントローラ ネットワーク ルートの表示

既存のネットワーク ルートを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。.

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [ネットワーク ルート（Network Route）]** を選択します。次のパラメータが表示されます。

- [IP アドレス（IP Address）] : ネットワーク ルートの IP アドレス。
- [IP ネットマスク（IP Netmask）] : ルートのネットワーク マスク。
- [ゲートウェイ IP アドレス（Gateway IP Address）] : ネットワーク ルートのゲートウェイ IP アドレス。

関連トピック

コントローラ サービス ポートでのネットワーク ルートの設定 （42 ページ）

コントローラへのネットワーク ルートの追加

ネットワーク ルートを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [ネットワーク ルート（Network Route）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、[ネットワーク ルートの追加（Add Network Route）] を選択します。

ステップ 5 [実行（Go）] をクリックします。

ステップ 6 必須フィールドに入力し、[保存（Save）] をクリックします。

関連トピック

コントローラ サービス ポートでのネットワーク ルートの設定 （42 ページ）

コントローラでの日時の設定 （28 ページ）

コントローラの STP パラメータの表示

スパニング ツリー プロトコル（STP）は、ネットワーク内の有害なループを防止しながら、パスの冗長性を実現するリンク管理プロトコルです。

現在の STP パラメータを表示または管理するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [スパニング ツリー プロトコル（Spanning Tree Protocol）]** を選択します。[スパニングツリー プロトコル（Spanning Tree Protocol）] ページに、次のパラメータが表示されます。

- [プロトコル仕様（Protocol Spec）]：現在のプロトコル仕様。
- [管理ステータス（Admin Status）]：有効にする場合は、このチェックボックスをオンにします。
- [優先度（Priority）]：最適なスイッチのプライオリティ番号。
- [最大保存期間（秒単位）（Maximum Age (seconds)）]：ポートに対して記録された受信プロトコル情報が廃棄されるまでの時間（秒単位）。
- [Hello 時間間隔（秒単位）（Hello Time (seconds)）]：スイッチが hello メッセージをその他のスイッチにブロードキャストする頻度（秒単位）を特定します。
- [転送遅延（Forward Delay (seconds)）]：ポートによるスイッチのラーニング/リスニング ステートでの経過時間（秒単位）。

関連トピック

コントローラ サービス ポートでのネットワーク ルートの設定 （42 ページ）
[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （23 ページ）

モビリティとは

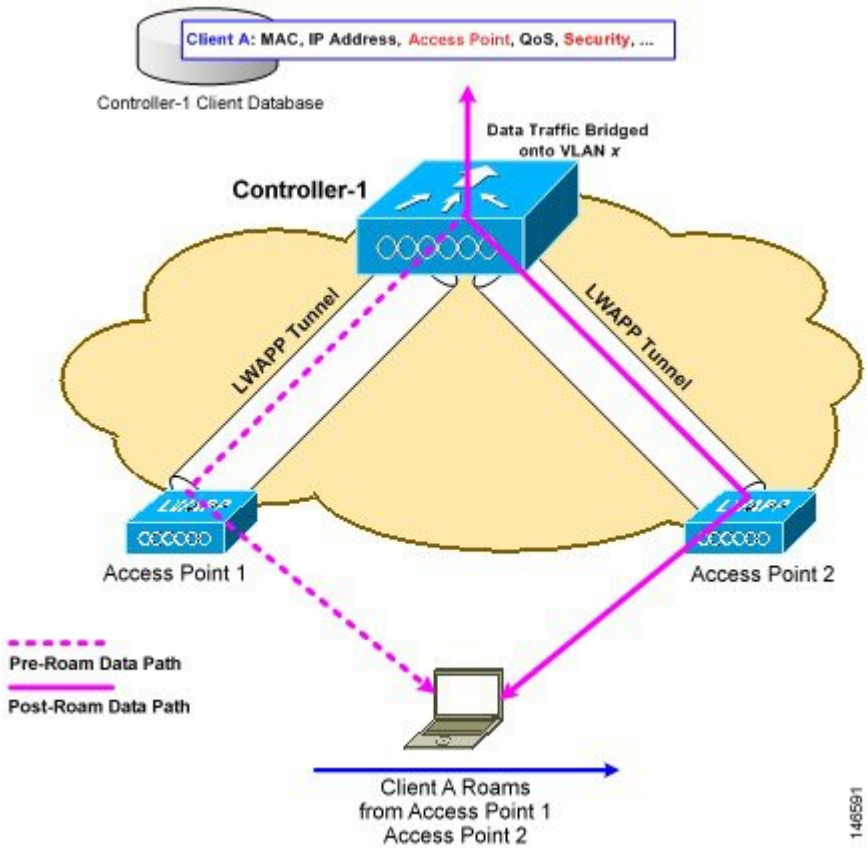
モビリティ（ローミング）は、ワイヤレス ネットワークにおいて、できるだけ遅れることなく、確実かつスムーズに、あるアクセス ポイントから別のアクセス ポイントへアソシエーションを維持するワイヤレス クライアントの機能です。あるワイヤレス クライアントがアクセス ポイントによってアソシエートされ認証されると、コントローラは、クライアント データベー

ス内にそのクライアントのエントリを保管します。このエントリにはクライアントの MAC アドレスと IP アドレス、セキュリティ コンテキストとアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、アソシエートされているアクセス ポイントなどが含まれます。コントローラはこの情報を使用してフレームを転送し、ワイヤレス クライアントとの間のトラフィックを管理します。

コントローラ内ローミングとは

ワイヤレス クライアントがそのアソシエーションを 1 つのアクセス ポイントから別のアクセス ポイントに移動する場合、コントローラは単に、新たにアソシエートされたアクセス ポイントを使ってクライアントデータベースを更新するのみです。必要に応じて、新しいセキュリティ コンテキストとアソシエーションも確立されます。次の図には、2 つのアクセス ポイントが同じコントローラに接続されている場合の両アクセス ポイント間における無線クライアント ローミングが示されています。図 146591

図 *1:* コントローラ内ローミング



関連トピック

モビリティとは （44 ページ）
モビリティ グループとは （49 ページ）
コントローラ間ローミングとは （46 ページ）

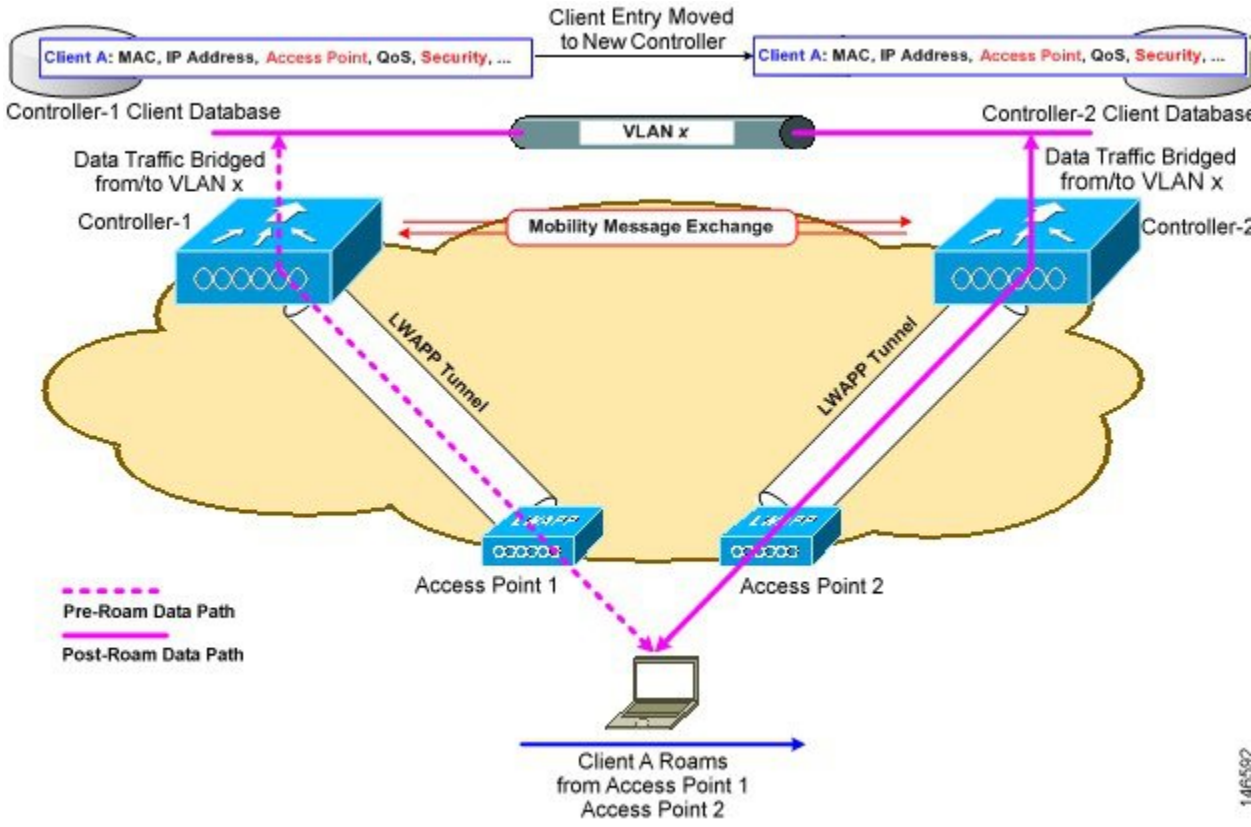
コントローラ間ローミングとは

1つのコントローラに接続されているアクセスポイントから別のコントローラに接続されているアクセスポイントにクライアントがローミングする際のプロセスは、同じサブネットでコントローラが動作しているかどうかによっても異なります。次の図は、コントローラの無線LANインターフェイスが同じ IP サブネット上に存在する場合に発生するコントローラ間ローミングを表しています。

新しいコントローラに接続されたアクセスポイントにクライアントがアソシエートされる際、新しいコントローラは元のコントローラとモビリティメッセージを交換し、クライアントデータベース エントリが新しいコントローラに移動されます。必要に応じて新しいセキュリティコンテキストとアソシエーションが確立され、新しいアクセスポイントに関してクライアントデータベース エントリが更新されます。このプロセスはユーザには見えません。

802.1X/Wi-Fi Protected Access（WPA）セキュリティで設定されたすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

図 *2:* コントローラ間ローミング



関連トピック

モビリティとは （44 ページ）
モビリティ グループとは （49 ページ）
コントローラ内ローミングとは （45 ページ）

コントローラをモビリティ グループに追加するための前提条件 （51 ページ）

サブネット間ローミングとは

サブネット間ローミングは、クライアント ローミング方法に関するモビリティ メッセージをコントローラが交換するという点で、コントローラ間ローミングと似ています。ただし、クライアントデータベースエントリを新しいコントローラに移動するのではなく、元のコントローラのクライアントデータベース内で、該当するクライアントに「アンカー」エントリのマークが付けられます。このデータベースエントリが新しいコントローラのクライアントデータベースにコピーされ、新しいコントローラ内で「外部」エントリのマークが付けられます。ローミングは無線クライアントには見えません。また、クライアントは元の IP アドレスを保持します。

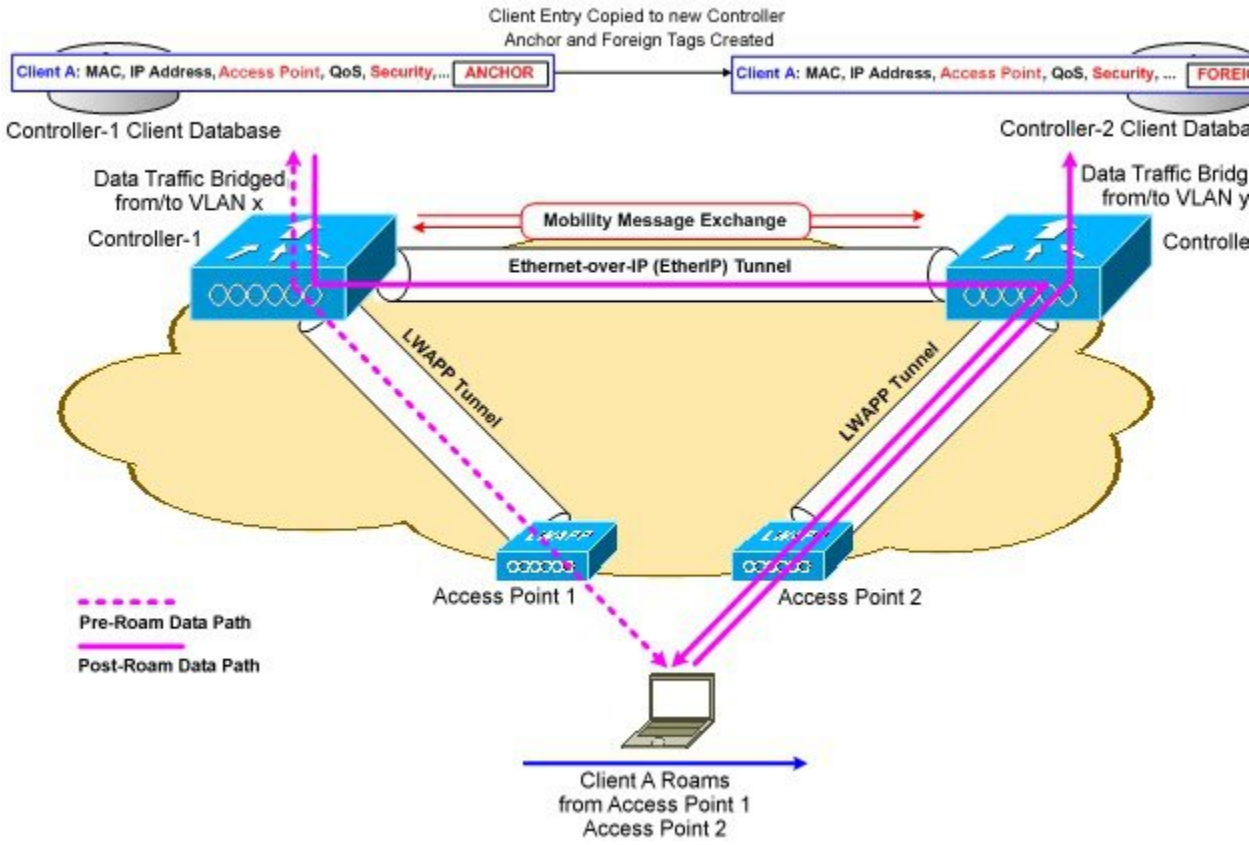
サブネット間ローミングの後は、無線クライアントとの間の非対称トラフィック パスでデータが伝送されます。クライアントからネットワークへのトラフィックは、外部コントローラによってネットワークに直接転送されます。クライアントへのトラフィックはアンカー コントローラに到達し、そこから EtherIP トンネルで外部コントローラにトラフィックが転送されます。その後、外部コントローラがそのデータをクライアントに転送します。無線クライアントが新しい外部コントローラへローミングする場合は、クライアント データベース エントリが元の外部コントローラから新しい外部コントローラに移動されますが、元のアンカー コントローラは常に保持されます。クライアントが元のコントローラに戻ると、再びローカルになります。

サブネット間ローミングでは、アンカーと外部の両方のコントローラの WLAN に同じネットワーク アクセス権限を設定する必要があり、ソースベースのルーティングやソースベースのファイアウォールを設定しないでおく必要があります。そうしないと、ハンドオフ後にクライアントにネットワーク接続の問題が発生する可能性があります。

サブネット間ローミングはマルチキャスト トラフィックをサポートしていません（プッシュツートークの使用時に Spectralink 電話によって使われるトラフィックなど）。

次の図 146593 は、コントローラの無線 LAN インターフェイスが異なる IP サブネット上に存在する場合に発生するサブネット間ローミングを表しています。

図 *3:*



関連トピック

モビリティとは （44 ページ）
モビリティ グループとは （49 ページ）
コントローラ内ローミングとは （45 ページ）
コントローラ間ローミングとは （46 ページ）
コントローラをモビリティ グループに追加するための前提条件 （51 ページ）

対称トンネリングとは

シンメトリック モビリティ トンネリングを使用すると、コントローラでは 1 つのアクセス ポイントから無線 LAN 内の別のアクセス ポイントへローミングするクライアントに対して、サブネット間のモビリティが提供されます。有線ネットワーク上のクライアント トラフィックは、外部コントローラによって直接ルーティングされます。ルータでリバース パス フィルタリング（RPF）が有効になっている場合、着信パケットで追加確認が実行され、通信はブロックされます。シンメトリック モビリティ トンネリングを使用すると、RPF が有効になっている場合でも、アンカーとして指定されたコントローラにクライアント トラフィックが到達できます。モビリティ グループ内のすべてのコントローラは、同じシンメトリック トンネリング モードを備えている必要があります。

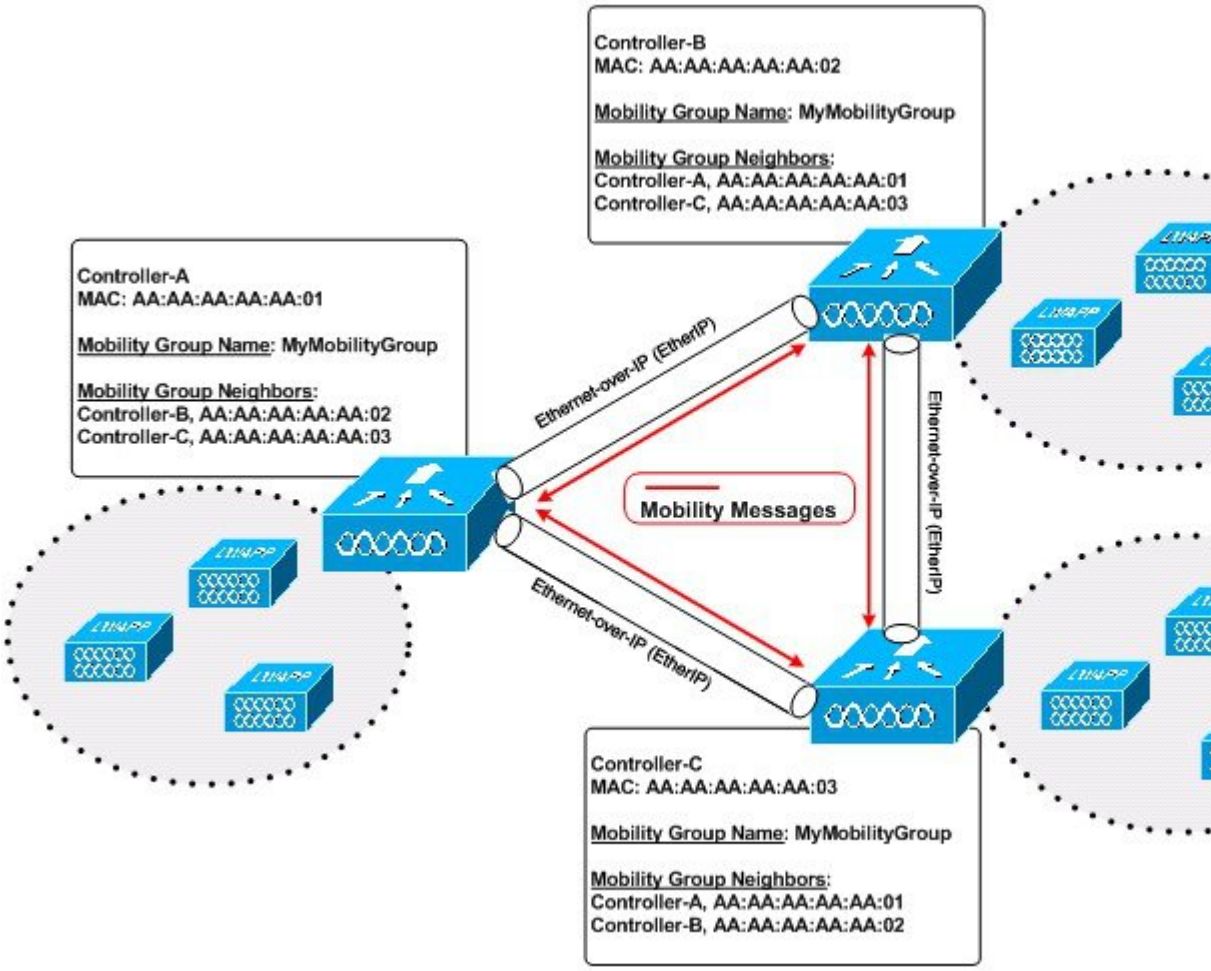
この機能を使用すると、コントローラの障害後にクライアントが別のアクセス ポイントに接続するための時間が短縮されます。障害がすばやく特定され、問題のあるコントローラからクライアントが移動し、別のコントローラに関連付けられるためです。

モビリティ グループとは

コントローラのセットをモビリティ グループとして設定すると、コントローラのグループ内でクライアント ローミングをスムーズに実行できるようになります。これにより、コントローラ間またはサブネット間のローミングが発生した際に、複数のコントローラが動的に情報を共有してデータ トラフィックを転送できるようになります。コントローラは、クライアントおよびコントローラ ロード情報のコンテキストと状態を共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。クライアントは、モビリティ グループ間でローミングしません。

次の図は、モビリティ グループの例を示します。

図 *4:* シングル モビリティ グループ



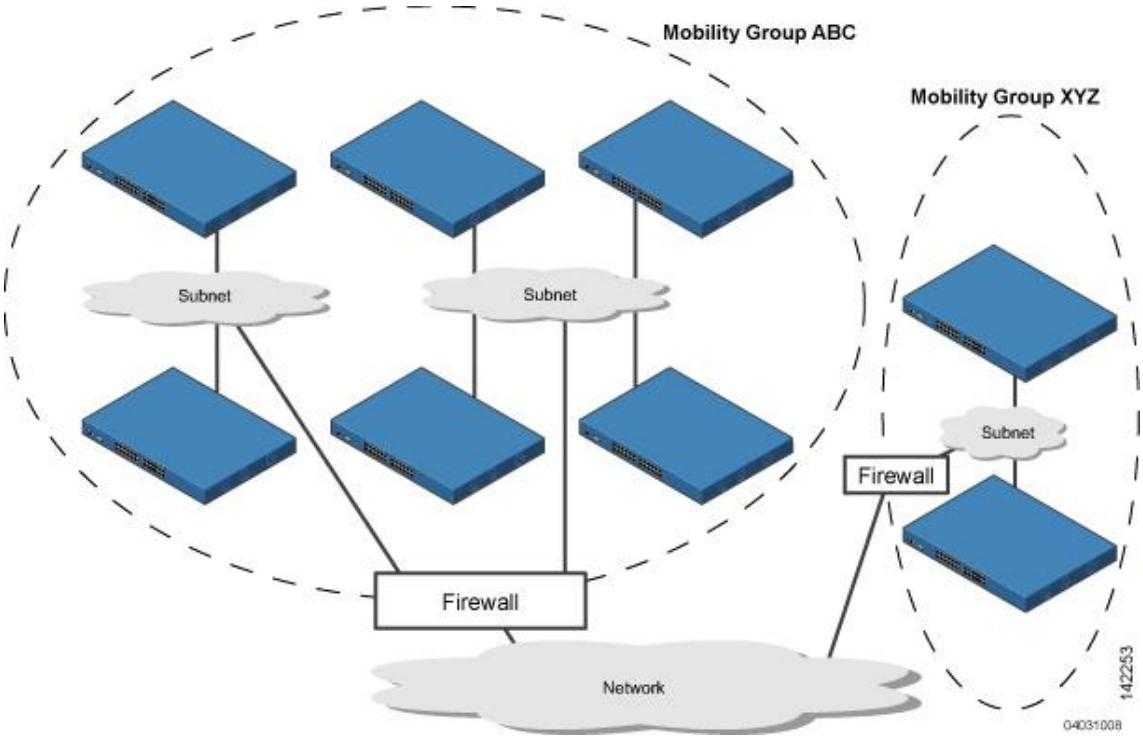
上の図に示すように、各コントローラはモビリティ グループの別メンバーのリストを使用して設定されています。新しいクライアントがコントローラに追加されると、コントローラはユニキャスト メッセージをそのモビリティ グループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを伝送します。コントローラ間のすべてのモビリティ交換トラフィックが CAPWAP トンネルで実行されます。

次に、例を示します。

1. 4404-100 コントローラは、最大で 100 アクセス ポイントをサポートします。したがって、24 個の 4404-100 コントローラで構成されるモビリティ グループは、最大 2400 個のアクセス ポイント（24 * 100 = 2400 アクセス ポイント）をサポートします。
2. 4402-25 コントローラは最大で 25 アクセス ポイントをサポートし、4402-50 コントローラは最大で 50 アクセス ポイントをサポートします。したがって、12 個の 4402-25 コントローラと 12 個の 4402-50 コントローラで構成されるモビリティ グループは最大 900 個のアクセス ポイント（12 * 25 + 12 * 50 = 300 + 600 = 900 アクセス ポイント）をサポートします。

モビリティ グループを使用すると、異なるモビリティ グループ名を同じ無線ネットワーク内の異なるコントローラに割り当てることで、1つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。次の図には、2つのコントローラ グループに異なるモビリティ グループ名を作成した結果が示されています。

図 *5:2* つのモビリティ グループ



ABC モビリティ グループ内のコントローラは、アクセス ポイントと共有サブネットを使用して相互に認識し、通信します。ABC モビリティ グループのコントローラは、異なるモビリティ グループ内の XYZ コントローラを認識せず、通信を行いません。同様に、XYZ モビリティ グループのコントローラは、ABC モビリティ グループのコントローラを認識せず、通信を行い

ません。この機能により、ネットワークでモビリティ グループが確実に分離されます。クライアントは、異なるモビリティ グループのアクセス ポイント間をローミングすることがあります（ただしアクセスポイントを検出できる場合）。ただし、そのセッション情報は、異なるモビリティ グループのコントローラ間で伝送されません。

関連トピック

コントローラをモビリティ グループに追加するための前提条件 （51 ページ）
コントローラのモビリティ グループ メッセージングの仕組み （51 ページ）

コントローラをモビリティ グループに追加するための前提条件

モビリティ グループにコントローラを追加する前に、そのグループに含めるすべてのコントローラに対して、次の前提条件が満たされていることを確認する必要があります。

- すべてのコントローラには同じ CAPWAP 転送モードを設定する必要があります（レイヤ 2 またはレイヤ 3）。
- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。
- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。
- すべてのコントローラは、同じ仮想インターフェイス IP アドレスで設定する必要があります。
- モビリティ グループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報が必要となるのは、他のすべてのモビリティ グループ メンバーの MAC アドレスと IP アドレスを使用してすべてのコントローラを設定するからです。
- ネットワーク内のワイヤレス クライアントをあるコントローラに接続されたアクセス ポイントから別のコントローラに接続されたアクセス ポイントにローミング可能な場合は、両方のコントローラは同じモビリティ グループ内に存在する必要があります。

関連トピック

モビリティ グループとは （49 ページ）
コントローラのモビリティ グループ メッセージングの仕組み （51 ページ）

コントローラのモビリティ グループ メッセージングの仕組み

コントローラでは、モビリティ メッセージをその他のメンバー コントローラに送信することにより、クライアントに対してサブネット間のモビリティが提供されます。モビリティ リストで最大 72 のメンバーをサポートします（同じモビリティ グループでは最大 24 まで）。Cisco Prime Infrastructure Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、モビリティ メッセージングに対して次の 2 つの改良が行われました。いずれも、モビリティ メンバーの全リストにメッセージを送信する場合に役立ちます。

- Mobile Announce メッセージを、まず同じグループ内に送信してから、リスト内の他のグループに送信する

コントローラは、新しいクライアントが関連付けられるたびに、モビリティ リスト内のメンバーに Mobile Announce メッセージを送信します。5.0 より前のソフトウェア リリースでは、

所属するグループに関係なく、リスト内のすべてのメンバーにコントローラがこのメッセージを送信します。しかし、ソフトウェア リリース 5.0 では、コントローラは自分と同じグループに属するメンバーに対してのみメッセージを送信した後、再試行を送信しながら、他のメンバーをすべて加えます。

- ユニキャストではなくマルチキャストを使用して Mobile Annouce メッセージを送信する

Cisco Prime Infrastructure および 5.0 よりも前のコントローラ ソフトウェア リリースでは、コントローラはマルチキャストを使用して、Mobile Announce メッセージを送信するように設定される場合がありますが、これには、すべてのモビリティ メンバにメッセージのコピーを送信する必要があります。多くのメッセージ（Mobile Announce、ペアワイズ マスター キー（PMK）更新、AP リスト更新、侵入検知システム（IDS）Shun など）がグループ内のすべてのメンバー向けであるため、この動作は効率的ではありません。Cisco Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、コントローラでマルチキャスト モードを使用して Mobile Announce メッセージを送信します。これにより、コントローラからネットワークに送られるメッセージは 1 コピーのみになります。このコピーはモビリティ メンバーすべてを含むマルチキャスト グループに宛てて送られます。マルチキャスト メッセージングを最大限活用するには、グループ メンバーすべてに対してこの機能を有効または無効にすることを推奨します。

関連トピック

モビリティ グループとは （49 ページ）
コントローラをモビリティ グループに追加するための前提条件 （51 ページ）
モビリティ グループの設定：ワークフロー （52 ページ）

モビリティ グループの設定：ワークフロー

モビリティ グループを設定する際は、次のワークフローに従います。

1. コントローラをモビリティ グループに追加するための前提条件 （51 ページ） で説明されているように、必要な情報を収集し、参加するコントローラが適切に構成されていることを確認してください。
2. モビリティ グループに個々のコントローラを追加します。モビリティ グループが存在しない場合は、場合によって手動で追加する必要があります。また、**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** ページから追加しようとするとコントローラが表示されない場合があります。
3. モビリティ グループの規模およびメッセージング パラメータを設定します。

コントローラをモビリティ グループに追加するための前提条件

モビリティ グループにコントローラを追加する前に、そのグループに含めるすべてのコントローラに対して、次の前提条件が満たされていることを確認する必要があります。

- すべてのコントローラには同じ CAPWAP 転送モードを設定する必要があります（レイヤ 2 またはレイヤ 3）。
- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。

- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。
- すべてのコントローラは、同じ仮想インターフェイス IP アドレスで設定する必要があります。
- モビリティ グループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報が必要となるのは、他のすべてのモビリティ グループ メンバーの MAC アドレスと IP アドレスを使用してすべてのコントローラを設定するからです。
- ネットワーク内のワイヤレス クライアントをあるコントローラに接続されたアクセス ポイントから別のコントローラに接続されたアクセス ポイントにローミング可能な場合は、両方のコントローラは同じモビリティ グループ内に存在する必要があります。

関連トピック

モビリティ グループとは （49 ページ）
コントローラのモビリティ グループ メッセージングの仕組み （51 ページ）

モビリティ グループに属しているコントローラの表示

現在のモビリティ グループ メンバーを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [モビリティ グループ（Mobility Groups）]** を選択します。

関連トピック

[ネットワークデバイス（Network Devices）] テーブルからコントローラをモビリティ グループに追加する （53 ページ）

[ネットワークデバイス（Network Devices）] テーブルからコントローラをモビリティ グループに追加する

既存のコントローラのリストからモビリティ グループ メンバーを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[モビリティ グループ（Mobility Groups）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [グループ メンバーの追加（Add Group Members）] を選択します。

ステップ 5 [実行（Go）] をクリックします。

ステップ 6 モビリティ グループに追加するコントローラのチェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 手順 6 でコントローラの一覧が表示されない場合は、次の操作を実行して手動で追加できます。

a) [モビリティ グループ メンバーの詳細（Mobility Group Member details）] ページで [ここをクリック（click here）] リンクをクリックします。

b) [メンバーの MAC アドレス（Member MAC Address）] テキスト ボックスに、追加するコントローラの MAC アドレスを入力します。

c) [メンバーの IP アドレス（Member IP Address）] テキスト ボックスに、追加するコントローラの管理インターフェイス IP アドレスを入力します。

ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する場合は、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でのモビリティが失敗します。

d) マルチキャスト モビリティ メッセージに使用するマルチキャスト グループ IP アドレスを [マルチキャスト アドレス（Multicast Address）] テキスト ボックスに入力します。ローカル モビリティ メンバーのグループ アドレスは、ローカル コントローラのグループ アドレスと同じである必要があります。

e) [グループ名（Group Name）] テキスト ボックスに、モビリティ グループ名を入力します。

f) [保存（Save）] をクリックします。

残りのシスコ ワイヤレス コントローラ デバイスに対して上記の手順を繰り返します。

関連トピック

モビリティ グループに属しているコントローラの表示 （53 ページ）

モビリティ メンバーへのメッセージ用にマルチキャスト モードを設定する

はじめる前に

モビリティ スケーラビリティ パラメータを設定するには、事前にモビリティ グループを設定しておく必要があります。

モビリティ メッセージ パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 ソフトウェア バージョンが 5.0 以降のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [一般（General）]** を選択します。

ステップ 4 [マルチキャスト モビリティ モード（Multicast Mobility Mode）] ドロップダウン リストで、マルチキャスト モードを使用してモビリティ メンバーに Mobile Announce メッセージを送信する機能を、このコントローラに対して有効または無効にするかを指定します。

ステップ 5 マルチキャストモビリティモードを有効に設定してマルチキャストメッセージングを有効にした場合は、[モビリティ グループ マルチキャスト アドレス（Mobility Group Multicast-address）] フィールドにグループ IP アドレスを入力してマルチキャスト モビリティ メッセージングを開始する必要があります。この IP アドレスの設定はローカル モビリティ グループに対しては必須ですが、モビリティ リスト内のその他のグループに対してはオプションです。その他の（非ローカル）グループに IP アドレスを設定しない場合、コントローラはユニキャスト モードを使用してこれらのメンバーにモビリティ メッセージを送信します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

コントローラでのマルチキャスト モードおよび IGMP スヌーピングの設定 （68 ページ）
[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （23 ページ）

コントローラへの NTP サーバの追加

新しい NTP サーバを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [ネットワーク タイム プロトコル（Network Time Protocol）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [NTP サーバの追加（Add NTP Server）] を選択します。

ステップ 5 [実行（Go）] をクリックします。

ステップ 6 [このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）] ドロップダウン リストから、このコントローラに適用する適切なテンプレートを選択します。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システムプロパティを変更する （23 ページ）

メッシュ ネットワーク バック グラウンド スキャン用のコント ローラーを構成します。

バックグラウンド スキャンにより、Cisco Aironet 1510 アクセス ポイントは、より最適なパスと親を探すために、能動的に連続してネイバー チャネルをモニタできます。アクセス ポイントは現在のチャネルだけでなくネイバーチャネル上でも検索を実行するため、最適な代替パスおよび親のリストは大きくなります。

親を喪失する前にこの情報を特定すると、より高速な転送速度およびそのアクセスポイントにとって最適なリンクが実現します。さらに、新しいチャネル上のリンクが、ホップの少なさ、信号対雑音比（SNR）の強さなどの点で、現在のチャネルよりも良好であると判明した場合は、アクセス ポイントはそのチャネルに切り替わる場合があります。

その他のチャネル上でのバックグラウンドスキャンおよびそれらのチャネル上のネイバーからのデータ収集は、2 つのアクセス ポイント間のプライマリ バックホール上で実行されます。

1510 のプライマリ バックホールは、802.11a リンク上で動作します。

バックグラウンド スキャンは、アクセス ポイントの関連付けされたコントローラ上でグローバルに有効にされます。音声コールが新しいチャネルに切り替わると、遅延が大きくなる場合があります。

EMEA 規制ドメインでは、DFS 要件が前提となるため、その他のチャネル上でのネイバーの検索に時間がかかる場合があります。

関連トピック

メッシュ ネットワーク バックグラウンド スキャンのシナリオ （56 ページ）

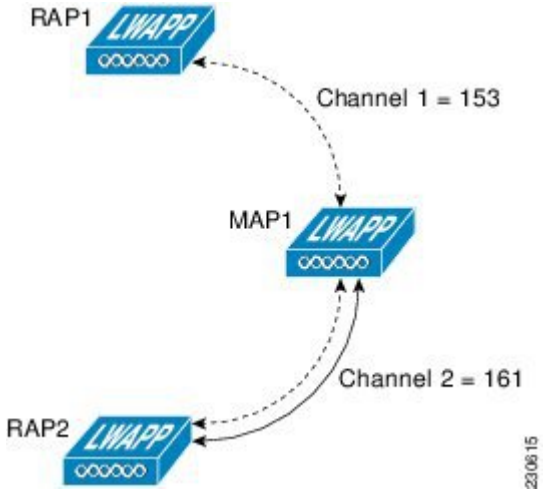
コントローラでのメッシュ ネットワーク バックグラウンド スキャンの有効化 （58 ページ）

メッシュ ネットワーク バックグラウンド スキャンのシナリオ

バックグラウンドスキャンの動作をより詳しく説明するために、いくつかのシナリオを示します。

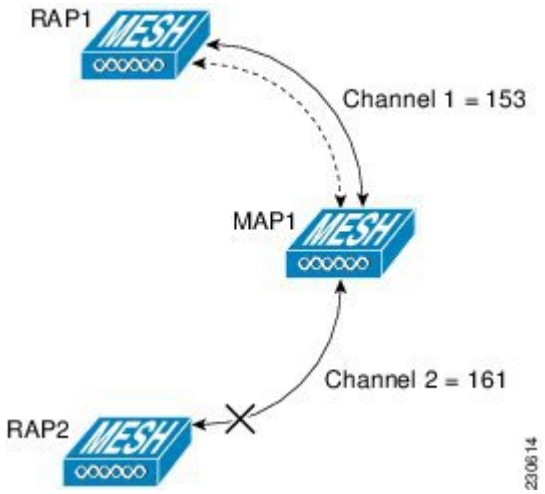
次の図では、メッシュ アクセス ポイント（MAP1）は、初回のアップ時に、ルート アクセス ポイント（RAP1 および RAP2）の両方が親になる可能性があると認識しています。ここでは、ホップ、SNR などの点で RAP2 を経由したルートの方が良好であるため、RAP2 が親として選択されています。リンクの確立後、バックグラウンドスキャン（有効にした場合）は、すべてのチャネルを継続的にモニタし、より最適なパスおよび親を検索します。RAP2 は、リンクがダウンするか、より最適なパスが別のチャネルで見つかるまで、MAP1 の親としての動作を継続し、チャネル 2 上で通信を続けます。

図 *6:* メッシュ アクセス ポイント（***MAP1***）による親の選択



次の図 230614 では、MAP1 と RAP2 間のリンクが失われています。現在実行中のバックグラウンド スキャンからのデータにより、RAP1 と Channel 1 が、MAP1 にとって 2 番めに最適な親および通信パスであると識別されるため、RAP2 とのリンクがダウンした後に、追加のスキャンなしでリンクがただちに確立されます。

図 *7:* バックグラウンド スキャンによる新しい親の識別



関連トピック

コントローラでのメッシュ ネットワーク バックグラウンド スキャンの有効化 （58 ページ）

コントローラでのメッシュ ネットワーク バックグラウンド スキャンの有効化

AP1510 RAP または MAP でバックグラウンド スキャンを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラの IP アドレスをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[メッシュ（Mesh）] > [メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 バックグラウンドスキャンを有効にする場合は [バックグラウンドスキャン（Background Scanning）] チェックボックスをオンにし、この機能を無効にする場合はオフにします。デフォルトでは、無効に設定されています。

ステップ 5 この機能により、すべてのチャネルをスキャンすることによりチャネル全体にわたって親を検索するという時間のかかるタスクが削減されます。オフチャネル手順は、選択したチャネルでブロードキャスト パケットを送信し（3 秒間隔、オフチャネルあたり最大 50 ミリ秒）、すべての「到達可能」ネイバーからパケットを受信します。これにより、子 MAP はチャネル全体にわたるネイバー情報で更新され、新しいネイバーに「切り替え」てアップリンクの親として使用することができます。「切り替え」は、親損失の検出でトリガーされる必要はありませんが、より良い親の識別時にトリガーされます。ただし、子 MAP では現在の親アップリンクがアクティブなままとなります。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

メッシュ ネットワーク バックグラウンド スキャンのシナリオ （56 ページ）

コントローラ QoS プロファイルの設定

QoS プロファイルを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラの IP アドレスをクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [QoS プロファイル（QoS Profiles）] の順に選択します。次のパラメータが表示されます。

- [ブロンズ（Bronze）]：バックグラウンド用
- [ゴールド（Gold）]：ビデオ アプリケーション用

- [プラチナ（Platinum）]：音声アプリケーション用
- [シルバー（Silver）]：ベスト エフォート用

ステップ 4 該当するプロファイルをクリックして、プロファイル パラメータを表示または編集します。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （23 ページ）

内部 DHCP サーバに関する情報

Cisco コントローラには、DHCP（Dynamic Host Configuration Protocol）リレー エージェントが組み込まれています。ただし、別個の DHCP サーバを持たないネットワーク セグメントを求められる場合、コントローラに IP アドレスとサブネット マスクをワイヤレス クライアントに割り当てる組み込みの DHCP スコープを設定できます。一般に、1 つのコントローラには、それぞれある範囲の IP アドレスを指定する複数の DHCP スコープを設定できます。

（注） この機能は、Cisco Mobility Express リリース 8.3 以降に適用されます。

現在の DHCP スコープの表示

現在の DHCP（Dynamic Host Configuration Protocol）スコープを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [DHCPスコープ（DHCP Scopes）]** の順に選択します。次のパラメータが表示されます。

- スコープ名
- プール アドレス
- リース時間
- プール使用率。これは、Cisco Mobility Express DHCP スコープにのみ表示されます。

DHCP スコープの設定

新しい DHCP スコープを追加するには、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	**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** > **[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[システム（System）]** > **[DHCPスコープ（DHCP Scopes）]** の順に選択します。	
ステップ 4	[コマンドの選択（Select a command）] ドロップダウン リストから、[DHCP スコープの追加（Add DHCP Scope）] を選択して新しい DHCP スコープを追加し、[実行（Go）] をクリックします。	
ステップ 5	[スコープ名（Scope Name）]テキストボックスに、新しい DHCP スコープの名前を入力します。	
ステップ 6	[VLAN-ID] テキスト ボックスに VLAN ID を入力します。	
ステップ 7	[リース時間（Lease Time）]テキスト ボックスに、IP アドレスをクライアントに対して許可する時間（0 ～ 65,536 秒）を入力します。	
ステップ 8	[ネットワーク（Network）] テキストボックスに、この DHCP スコープの対象となるネットワークを入力します。この IP アドレスは、[Interfaces] ページで設定されている、ネットマスクが適用された管理インターフェイスによって使用されます。	
ステップ 9	[ネットマスク（Netmask）] テキストボックスに、すべての無線クライアントに割り当てられたサブネット マスクを入力します。	
ステップ 10	[プール開始アドレス（Pool Start Address）] テキストボックスに、クライアントに割り当てられた範囲の開始IPアドレスを入力します。このプールは、各 DHCP スコープで一意でなければならず、ルー	

	コマンドまたはアクション	目的
	タまたは他のサーバの固定 IP アドレスを含めることはできません。	
ステップ 11	[プール終了アドレス（Pool End Address）] テキスト ボックスに、クライアントに割り当てられた範囲の終了IPアドレスを入力します。このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。	
ステップ 12	[デフォルト ゲートウェイ（Default Gateway）] テキスト ボックスに、オプションのゲートウェイの IP アドレスを入力します。	
ステップ 13	[DNS ドメイン名（DNS Domain Name）] テキスト ボックスに、1 つまたは複数の DNS サーバで使用する、この DHCP スコープのオプションの DNS 名を入力します。	
ステップ 14	[DNS サーバ（DNS Servers）] テキストボックスに、オプションの DNS サーバの IP アドレスを入力します。各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。	
ステップ 15	[保存（Save）] をクリックします。	

DHCP スコープの削除

（注） DHCP スコープを削除するのには、最初にその管理状態を無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	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	

	コマンドまたはアクション	目的
ステップ 3	左側のサイドバーのメニューから、**[システム（System）] > [DHCPスコープ（DHCP Scopes）]** の順に選択します。	
ステップ 4	削除する DHCP スコープのチェックボックスをオンにします。	
ステップ 5	[コマンドの選択（Select a command）] ドロップダウンリストから、[DHCP スコープの削除（Delete DHCP Scope）] を選択し、[実行（Go）] をクリックします。	

DHCP スコープの詳細のエクスポート

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[システム（System）] > [DHCPスコープ（DHCP Scopes）]** の順に選択します。	
ステップ 4	[コマンドの選択（Select a command）] ドロップダウン リストから、[DHCPLeases] を選択し、[実行（Go）] をクリックします。	
ステップ 5	[MAC アドレス（MAC Address）] の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックして DHCP スコープの詳細を csv ファイルとしてエクスポートします。	

コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの表示

コントローラの現在のローカルネットユーザ ロールを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[ユーザ ロール（User Roles）]** を選択します。

ローカル ネット ユーザ ロールのパラメータが表示されます。

ステップ 4 テンプレート名をクリックして、ユーザ ロールの詳細を表示します。

関連トピック

コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの設定 （63 ページ）

コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの設定

新しいローカルネットユーザ ロールをコントローラに追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [ユーザ ロール（User Roles）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、[ユーザ ロールの追加（Add User Role）] を選択します。

ステップ 5 [このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）] ドロップダウン リストからテンプレートを選択します。

ステップ 6 [適用（Apply）] をクリックします。

関連トピック

コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの表示 （63 ページ）
[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （23 ページ）

コントローラに接続する AP のコントローラ ユーザ名とパスワードの設定

[AP ユーザ名のパスワード（AP Username Password）] ページでは、すべてのアクセス ポイントがコントローラに接続する際に継承する、グローバル パスワードを設定できます。また、アクセス ポイントを追加する際に、このグローバル ユーザ名およびパスワードを受け入れるか、アクセス ポイント単位で上書きするかを選択できます。

さらにコントローラ ソフトウェア リリース 5.0 では、アクセス ポイントをコントローラに接続すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、アクセス ポイントのコンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

グローバル ユーザ名とパスワードを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 リリース 5.0 以降のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [AP ユーザ名のパスワード（AP Username Password）] の順に選択します。

ステップ 4 コントローラに接続するすべてのアクセス ポイントで継承されるユーザ名およびパスワードを入力します。

Cisco IOS アクセス ポイントの場合は、イネーブル パスワードも入力して確認する必要があります。

ステップ 5 [保存（Save）] をクリックします。

コントローラでの CDP の設定

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。

CDP は、ブリッジのイーサネット ポートおよび無線ポート上で、デフォルトで有効になっています。

グローバル インターフェイス CDP 設定は、AP レベルで CDP を有効にした AP のみに適用されます。

グローバル CDP を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [グローバル CDP 設定（Global CDP Configuration）] の順に選択します。[グローバル CDP 設定（Global CDP Configuration）] ページが表示されます。

ステップ 4 [グローバル CDP 設定（Global CDP Configuration）] ページで必要なフィールドを設定します。[Global CDP] グループ ボックスで、次のパラメータを設定します。

- [コントローラ上の CDP（CDP on controller）]：コントローラで CDP を有効にするか、無効にするかを選択します。この設定は、WiSM2 コントローラには適用できません。
- [AP 上のグローバル CDP（Global CDP on APs）]：アクセス ポイントで CDP を有効にするか、無効にするかを選択します。
- [リフレッシュ時間間隔（秒単位）（Refresh-time Interval (seconds)）]：[リフレッシュ時間間隔（Refresh Time Interval）] フィールドに、CDP メッセージが生成される時間を秒単位で入力します。デフォルトは 60 です。
- [保持時間（秒）（Holdtime (seconds)）]：CDP ネイバー エントリの期限が切れるまでの時間を秒単位で入力します。デフォルトは 180 です。
- [CDP アドバタイズメントのバージョン（CDP Advertisement Version）]：使用する CDP プロトコルのバージョンを入力します。デフォルトは v1 です。

ステップ 5 [イーサネット インターフェイスの CDP（CDP for Ethernet Interfaces）] グループ ボックスで、CDP を有効にするイーサネット インターフェイスのスロットを選択します。

[イーサネット インターフェイス用の CDP（CDP for Ethernet Interfaces）] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 6 [無線インターフェイスの CDP（CDP for Radio Interfaces）] グループ ボックスで、CDP を有効にする無線インターフェイスのスロットを選択します。

[無線インターフェイスの CDP（CDP for Radio Interfaces）] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システムプロパティを変更する （23 ページ）

コントローラへの 802.1X 認証の設定

Lightweight アクセス ポイントとスイッチ間の 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。すべてのアクセス ポイントがコントローラ接続時に継承するグローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。

必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセスポイントに割り当てることができます。

グローバル サプリカント クレデンシャルを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [AP 802.1X サプリカント クレデンシャル（AP 802.1X Supplicant Credentials）] の順に選択します。

ステップ 4 [グローバル サプリカント クレデンシャル（Global Supplicant Credentials）] チェックボックスをオンにします。

ステップ 5 サプリカント ユーザ名を入力します。

ステップ 6 適切なパスワードを入力して確定します。

ステップ 7 ドロップダウン メニューから [サプリカントEAPタイプ（Supplicant EAP Type）] を選択します。

（注） バージョン 8.7 以降のコントローラおよび ME に適用されます。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システムプロパティを変更する （23 ページ）

デバイスの 802.11 パラメータの設定 （143 ページ）

コントローラへの 802.1X 認証の設定

Lightweight アクセス ポイントとスイッチ間の 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。すべてのアクセス ポイントがコントローラ接続時に継承するグ

ローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。

必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセスポイントに割り当てることができます。

グローバル サプリカント クレデンシャルを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [AP 802.1X サプリカント クレデンシャル（AP 802.1X Supplicant Credentials）] の順に選択します。

ステップ 4 [グローバル サプリカント クレデンシャル（Global Supplicant Credentials）] チェックボックスをオンにします。

ステップ 5 サプリカント ユーザ名を入力します。

ステップ 6 適切なパスワードを入力して確定します。

ステップ 7 ドロップダウン メニューから [サプリカントEAPタイプ（Supplicant EAP Type）] を選択します。

（注） バージョン 8.7 以降のコントローラおよび ME に適用されます。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （23 ページ）
デバイスの 802.11 パラメータの設定 （143 ページ）

コントローラでの DHCP の設定

コントローラの DHCP（Dynamic Host Configuration Protocol）情報を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [DHCP] の順に選択します。

ステップ 4 次のパラメータを追加または変更します。

- [DHCP オプション 82 リモート ID フィールドのフォーマット（DHCP Option 82 Remote Id Field Format）]：ドロップダウン リストから [AP-MAC]、[AP-MAC-SSID]、[AP-ETHMAC]、または [AP-NAME-SSID] を選択します。

Ap-Mac を選択した場合に [DHCP オプション 82（DHCP option 82）] の [RemoteID] フィールドにフォーマットを設定するには、RemoteID フォーマットを *AP-Mac* として設定します。[AP-MAC-SSID] を選択した場合、RemoteID のフォーマットは「*AP-Mac:SSID*」として設定されます。

- [DHCP プロキシ（DHCP Proxy）]：プロキシで DHCP を有効にする場合は、このチェックボックスをオンにします。

DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。そのため、少なくとも 1 つの DHCP サーバが、WLAN に関連付けられたインターフェイスか WLAN 自体で設定されている必要があります。

ステップ 5 [DHCP タイムアウト（DHCP Timeout）] を秒単位で入力します。この時間を過ぎると DHCP 要求がタイムアウトします。デフォルト設定は 5 です。有効値の範囲は 5 ～ 120 秒です。DHCP タイムアウトは、リリース 7.0.114.74 以降のコントローラで適用されます。

ステップ 6 [保存（Save）] をクリックします。

保存後に、[監査（Audit）] をクリックして、このコントローラで監査を実行できます。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （23 ページ）

コントローラでのマルチキャスト モードおよび IGMP スヌーピングの設定

Prime Infrastructure では、コントローラ上の IGMP（インターネット グループ管理プロトコル）スヌーピングおよびタイムアウト値を設定するオプションが提供されています。

IGMP

コントローラのマルチキャスト モードおよび IGMP スヌーピングを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [マルチキャスト（Multicast）]** を選択します。

ステップ 4 [イーサネット マルチキャスト サポート（Ethernet Multicast Support）] ドロップダウン リストから、該当するイーサネット マルチキャスト サポート（[ユニキャスト（Unicast）] または [マルチキャスト（Multicast）]）を選択します。

ステップ 5 [マルチキャスト（Multicast）] を選択した場合は、マルチキャスト グループ IP アドレスを入力します。

ステップ 6 マルチキャスト モードをグローバルに使用可能にするには、[グローバル マルチキャスト モード（Global Multicast Mode）] チェックボックスをオンにします。

IGMP スヌーピングおよびタイムアウトは、イーサネット マルチキャスト モードが有効の場合のみ設定できます。IGMP スヌーピングを選択して有効にします。

ステップ 7 [マルチキャスト モビリティ モード（Multicast Mobility Mode）] ドロップダウン リストから [有効（Enable）] を選択して、IGMP スヌーピング ステータスを変更するか、または IGMP タイムアウトを設定します。IGMP スヌーピングが有効の場合、コントローラはクライアントから IGMP レポートを収集した後、いずれかのマルチキャスト グループをリッスンしているクライアントのリストをアクセス ポイントに送信します。その後、アクセス ポイントはこれらのクライアントのみにマルチキャスト パケットを転送します。

タイムアウト間隔の範囲は 3 ～ 300 で、デフォルト値は 60 です。タイムアウトが経過すると、コントローラはすべての WLAN に対してクエリを送信します。その後、マルチキャスト グループ内でリッスンしているクライアントは、コントローラにパケットを送り返します。

ステップ 8 マルチキャスト モビリティ モードを有効にしている場合は、モビリティ グループ マルチキャスト アドレスを入力します。

ステップ 9 ワイヤレス ネットワークを介したビデオ ストリームを有効にするには、[マルチキャスト ダイレクト（Multicast Direct）] チェックボックスをオンにします。

ステップ 10 [マルチキャスト モビリティ モード（Multicast Mobility Mode）] ドロップダウン リストから [有効（Enable）] を選択して、MLD 設定を変更します。

ステップ 11 IPv6 MLD スヌーピングを有効にする場合は、[MLD スヌーピングの有効化（Enable MLD Snooping）] チェックボックスをオンにします。このチェックボックスをオンにした場合は、次のパラメータを設定します。

- [MLD タイムアウト（MLD Timeout）]：MLD タイムアウト値を秒単位で入力します。タイムアウトの範囲は 3 ～ 7200 で、デフォルト値は 60 です。
- [MLD クエリ間隔（MLD Query Interval）]：MLD クエリ間隔のタイムアウト値を秒単位で入力します。間隔の範囲は 15 ～ 2400 で、デフォルト値は 20 です。

インターネット グループ管理プロトコル（IGMP）スヌーピングを使用することにより、IPv4 のマルチキャスト トラフィックのフラッディングを抑制できます。IPv6 の場合は、マルチキャスト リスナー検出（MLD）スヌーピングが使用されます。

ステップ 12 セッション バナー情報を設定します。これは、クライアントがメディア ストリームから拒否またはドロップされた場合に、クライアントに送信されるエラー情報です。

ステップ 13 [保存（Save）] をクリックします。

保存後に、[監査（Audit）] をクリックして、このコントローラで監査を実行できます。

関連トピック

[ネットワーク デバイス（Network Devices）] テーブルからコントローラの一般システム プロパティを変更する （23 ページ）

障害検出時間を短縮するコントローラの拡張タイマーの設定

Prime Infrastructure のコントローラには、FlexConnect およびローカル モード用の拡張タイマー設定を使用できます。

この機能は、リリース 6.0 以降のコントローラのみでサポートされています。

拡張タイマーを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 タイマーを設定するコントローラを選択します。

ステップ 3 左側のサイドバーのメニューから、[システム（System）] > [AP タイマー（AP Timers）] の順に選択します。

ステップ 4 [AP タイマー（AP Timers）] ページで、該当するアクセス ポイント モードのリンク（[ローカル モード（Local Mode）] または [FlexConnect モード（FlexConnect Mode）]）をクリックします。

ステップ 5 この選択に応じて、[ローカル モード AP タイマー設定（Local Mode AP Timer Settings）] ページまたは [FlexConnect モード AP タイマー設定（FlexConnect Mode AP Timer Settings）] ページで必要なパラメータを設定します。

- [ローカル モード AP タイマー設定（Local Mode AP Timer Settings）]：障害検出時間を短縮するには、高速ハートビート間隔（コントローラとアクセス ポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの期限（ハートビート間隔ごと）を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラに送信します。この場合、10 ～ 15 秒の値を入力できます。
- [FlexConnect 用の AP タイマー設定（AP timer settings for FlexConnect）]：選択すると、FlexConnect タイムアウト値を設定できます。[AP プライム検出タイムアウト（AP Primary Discovery Timeout）] チェックボックスをオンにして、タイムアウト値を有効にします。30 ～ 3600 秒の値を入力します。5500 シリーズ コントローラは、1 ～ 10 の範囲のアクセス ポイント高速ハートビート タイマー値を受け入れます。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

コントローラでの WLAN の作成 （71 ページ）

コントローラでの WLAN の作成

コントローラは 512 WLAN 設定をサポートできるため、 Prime Infrastructure は、特定のコントローラに対して、指定した時刻に複数の WLAN を有効または無効にする効率的な方法を提供します。

ネットワーク上に設定した Wireless Local Access Network（WLAN）のサマリーを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[WLAN（WLANs）]** > **[WLANの設定（WLAN Configuration）]** を選択します。

ステップ 4 [WLAN サマリーの設定（Configure WLAN Summary）] ページの必須フィールドを設定します。

関連トピック

コントローラで構成されている WLAN の表示 （71 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （72 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （73 ページ）
コントローラへの WLAN の追加 （76 ページ）
コントローラからの WLAN の削除 （77 ページ）
コントローラの WLAN の管理ステータスを変更する （77 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （78 ページ）
コントローラの WLAN AP グループの設定 （82 ページ）

コントローラで構成されている WLAN の表示

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 WLAN 設定を表示するワイヤレス コントローラのデバイス名をクリックします。

ステップ 3 [設定（Configuration）] タブをクリックします。

ステップ 4 [機能（Features）] で **[WLAN（WLANs）]** > **[WLAN の設定（WLAN Configuration）]** を選択します。[WLAN 設定のサマリー（WLAN Configuration Summary）] ページに、コントローラで現在設定されている WLAN のリストが表示されます。リストには次の各項目が含まれます。

- WLAN ID

- WLAN 設定プロファイルの名前
- WLAN SSID
- アクティブなセキュリティ ポリシーの名前
- WLAN の現在の管理ステータス（有効または無効）
- 現在スケジュール設定されているすべての WLAN 設定タスクのリストへのリンク

ステップ 5 WLAN設定の詳細を表示するには、**WLAN ID** をクリックします。[WLAN設定の詳細（WLAN Configuration Details）] ページが表示されます。

ステップ 6 タブ（[一般（General）]、[セキュリティ（Security）]、[QoS]、[詳細設定（Advanced）]）を使用して、WLAN のパラメータを表示または編集します。パラメータを変更した場合は、[保存（Save）] をクリックします。

関連トピック

コントローラ上の WLAN へのセキュリティ ポリシーの追加 （72 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （73 ページ）
コントローラへの WLAN の追加 （76 ページ）
コントローラからの WLAN の削除 （77 ページ）
コントローラの WLAN の管理ステータスを変更する （77 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （78 ページ）

コントローラ上の WLAN へのセキュリティ ポリシーの追加

ステップ 1 「コントローラで構成されている WLAN の表示」で説明されているように、[WLANの設定（WLAN Configuration）] 詳細ページに移動します。

ステップ 2 [ポリシーマッピング（Policy Mappings）] タブをクリックします。

ステップ 3 [行の追加（Add Row）] をクリックします。

ステップ 4 ドロップダウン リストから、WLAN にマッピングするポリシー名を選択します。

ステップ 5 プライオリティを入力します。プライオリティの範囲は、1 ～ 16 です。

2 つのポリシーに同じプライオリティを設定することはできません。

ステップ 6 [保存（Save）] をクリックします。

ポリシーを削除するには、削除するポリシーに対応するチェックボックスをオンにして、[削除（Delete）] をクリックします。

関連トピック

コントローラで構成されている WLAN の表示 （71 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （73 ページ）

コントローラでのモバイルコンシェルジュ（802.11u）の設定

シスコ モバイル コンシェルジュは、事前認証を行わずに外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュは、クライアントにサービスのアベイラビリティに関する情報を提供します。これにより、クライアントは使用可能なネットワークに、よりすばやく、簡単かつ安全に関連付けできます。

ネットワークから提供されるサービスは、次の 2 つのプロトコルに大きく分類できます。

- 802.11u MSAP
- 802.11u HotSpot 2.0

モバイル コンシェルジュには、次のガイドラインと制限事項が適用されます。

- モバイル コンシェルジュは FlexConnect アクセス ポイントではサポートされません。
- 802.11u 設定アップロードはサポートされません。設定のアップグレードを実行し、設定をコントローラにアップロードすると、WLAN の HotSpot の設定は失われます。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 モバイル コンシェルジュを設定するワイヤレス コントローラのデバイス名をクリックします。

ステップ 3 [設定（Configuration）] タブをクリックします。

ステップ 4 [機能（Features）] で **[WLAN（WLANs）]** > **[WLAN の設定（WLAN Configuration）]>** を選択します。[WLAN 設定（WLAN Configuration）] 要約ページに、コントローラで現在設定されている WLAN のリストが表示されます。

ステップ 5 モバイル コンシェルジュを設定する WLAN の WLAN ID をクリックします。

ステップ 6 [ホット スポット（Hot Spot）] タブをクリックします。

ステップ 7 [802.11u 設定（802.11u Configuration）] サブタブをクリックし、次のようにフィールドを設定します。

a) [802.11u ステータス（802.11u Status）] チェックボックスをオンにして WLAN の 802.11u を有効にします。

b) [インターネット アクセス（Internet Access）] チェックボックスをオンにして、この WLAN からインターネット サービスを提供できるようにします。

c) [ネットワーク タイプ（Network Type）] ドロップダウン リストから、この WLAN に設定する 802.11u サービスに適した説明を選択します。次のオプションを使用できます。

- **[プライベート ネットワーク（Private Network）]**

- **[ゲスト アクセスでのプライベート ネットワーク（Private Network with Guest Access）]**
- **[有料のパブリック ネットワーク（Chargeable Public Network）]**
- **[無料のパブリック ネットワーク（Free Public Network）]**
- **[緊急サービス専用ネットワーク（Emergency Services Only Network）]**
- **[個人のデバイス ネットワーク（Personal Device Network）]**
- **[テストまたは実験用（Test or Experimental）]**
- **ワイルドカード**

d) このネットワークの 802.11u パラメータ用に設定する認証タイプを選択します。

- [未設定（Not configured）]
- [規約への同意（Acceptance of Terms and Conditions）]
- [オンライン登録（Online Enrollment）]
- [DNS リダイレクト（DNS Redirection）]
- [HTTP/HTTPS リダイレクト（HTTP/HTTPS Redirection）]

e) [HESSID] フィールドに、同種拡張サービスセット識別子の値を入力します。HESSID は、同種 ESS を識別する 6 オクテットの MAC アドレスです。

f) [IPv4 アドレス タイプ（IPv4 Address Type）] フィールドで、IPv4 アドレスの割り当て方式を選択します。

- **使用不可（Not Available）**
- **パブリック（Public）**
- **[制限付きポート（Port Restricted）]**
- **[シングル NAT プライベート（Single NAT Private）]**
- **[ダブル NAT プライベート（Double NAT Private）]**
- **[制限付きポートおよびシングル NAT プライベート（Port Restricted and Single NAT Private）]**
- **[制限付きポートおよびダブル NAT プライベート（Port Restricted and Double NAT Private）]**
- **不明**

g) [IPv6 アドレス タイプ（IPv6 Address Type）] フィールドで、IPv6 アドレスの割り当て方式を選択します。

- **使用不可（Not Available）**
- **応対可**
- **不明**

ステップ 8 [その他（Others）] サブタブをクリックし、次のようにフィールドを設定します。

a) [OUI リスト（OUI List）] グループ ボックスで、[行の追加（Add Row）] をクリックして次の詳細情報を入力します。

- [OUI 名（OUI name）]
- [ビーコン（Is Beacon）]
- [OUI インデックス（OUI Index）]

[保存（Save）] をクリックすると、OUI（組織固有識別子）エントリがこの WLAN に追加されます。

b) [ドメイン リスト（Domain List）] グループ ボックスで、[行の追加（Add Row）] をクリックして次の詳細情報を入力します。

- [ドメイン名（Domain Name）]：802.11 アクセス ネットワークで稼働するドメイン名。
- [ドメイン インデックス（Domain Index）]：ドロップダウン リストからドメイン インデックスを選択します。

[保存（Save）] をクリックすると、ドメイン エントリがこの WLAN に追加されます。

c) [セルラー（Cellular）]セクションで、[行の追加（Add Row）] をクリックして次の詳細情報を入力します。

- [国コード（Country Code）]：3 文字のセルラー国コード。
- [ネットワーク コード（Network Code）]：3 文字のセルラー ネットワーク コード。

[保存（Save）] をクリックすると、セルラー エントリがこの WLAN に追加されます。

ステップ 9 [レルム（Realm）] サブタブをクリックし、次のようにフィールドを設定します。

a) [行の追加（Add Row）] をクリックしてレルム名を入力します。
b) [保存（Save）] をクリックすると、レルム エントリがこの WLAN に追加されます。

ステップ 10 [サービス アドバタイズメント（Service Advertisements）]サブタブをクリックし、次のようにフィールドを設定します。

a) [MSAP を有効にする（MSAP Enable）]チェックボックスをオンにし、サービス アドバタイズメントを有効にします。
b) MSAP を有効にする場合は、この WLAN のサーバ インデックスを入力します。サーバ インデックス フィールドは、BSSID を使用して到達可能である場所を提供する MSAP サーバ インスタンスを一意に識別します。

MSAP（Mobility Services Advertisement Protocol）は、ネットワーク接続を確立するためのポリシー セットを使用して設定されたモバイル デバイスで主に使用するために設計されています。これらのサービスは、上位層サービスを提供するデバイス、つまりサービス プロバイダー経由で有効にされるネットワーク サービス向けです。サービス アドバタイズメントは、MSAP を使用して、Wi-Fi アクセス ネットワークへの関連付け前にサービスをモバイル デバイスに提供します。この情報はサービス アドバタイズメントで伝送されます。シングルモードまたはデュアルモード モバイル デバイスは、関連付けの前にサービス ネットワークをネットワークにクエリします。デバイスによるネットワークの検出および選択機能では、ネットワークへの参加に関する判断においてサービス アドバタイズメントを使用する場合があります。

ステップ 11 [Hotspot 2.0] サブタブをクリックし、次のようにフィールドを設定します。

a) [HotSpot2 の有効化（HotSpot2 Enable）] ドロップダウン リストから [有効（Enable）] オプションを選択します。
b) [WAM メトリック（WAM Metrics）] グループ ボックスで、次の項目を指定します。

- [WAN リンク ステータス（WAN Link Status）]：リンク ステータス。有効な範囲は 1 ～ 3 です。
- [WAN SIM リンク ステータス（WAN SIM Link Status）]：対称リンク ステータス。たとえば、アップリンクとダウンリンクに異なる速度または同じ速度を設定できます。
- [アップリンク速度（Up Link Speed）]：アップリンク速度。最大値は 4,194,304 kbps です。

- [ダウンリンク速度（Down Link Speed）]：ダウンリンク速度。最大値は 4,194,304 kbps です。

c) [オペレータ名リスト（Operator Name List）] で、[行の追加（Add Row）] をクリックして次の詳細情報を入力します。

- [オペレータ名（Operator Name）]：802.11 オペレータの名前を指定します。
- [オペレータ インデックス（Operator Index）]：オペレータ インデックスを選択します。指定できる範囲は 1 ～ 32 です。
- [言語コード（Language Code）]：言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。

[保存（Save）] をクリックすると、オペレータがリストに追加されます。

d) [ポート設定リスト（Port Config List）] で、[行の追加（Add Row）] をクリックして次の詳細情報を入力します。

- [IP プロトコル（IP Protocol）]：有効にする IP プロトコルを選択します。オプションは、ESP、FTP、ICMP、および IKEV2 です。
- [ポート番号（Port No）]：この WLAN で有効になっているポート番号。
- [ステータス（Status）]：ポートのステータス。

[保存（Save）] をクリックすると、ポート設定がリストに追加されます。

ステップ 12 [保存（Save）] をクリックして、モバイル コンシェルジュ設定を保存します。

関連トピック

コントローラで構成されている WLAN の表示 （71 ページ）
コントローラへの WLAN の追加 （76 ページ）
コントローラからの WLAN の削除 （77 ページ）
コントローラの WLAN の管理ステータスを変更する （77 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （72 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （78 ページ）

コントローラへの WLAN の追加

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [WLAN（WLANs）]** [WLANの設定（WLAN Configuration）] の順に選択します。

ステップ 2 テンプレート タイプの横にあるツール チップにマウスのカーソルを合わせ、[新規（New）] をクリックします。

ステップ 3 [一般（General）]、[セキュリティ（Security）]、[QoS]、[詳細設定（Advanced）]、[HotSpot]、[ポリシー マッピング（Policy Mappings）] タブで必須フィールドに値を入力し、[新しいテンプレートとして保存（Save as New Template）] をクリックします。

ステップ 4 [展開（Deploy）] をクリックして、テンプレートの展開を続行します。

関連トピック

コントローラで構成されている WLAN の表示 （71 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （73 ページ）
コントローラからの WLAN の削除 （77 ページ）
コントローラの WLAN の管理ステータスを変更する （77 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （72 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （78 ページ）
コントローラの WLAN AP グループの設定 （82 ページ）

コントローラからの WLAN の削除

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[WLAN（WLANs）] > [WLANの設定（WLAN Configuration）]** の順に選択します。

ステップ 4 削除する WLAN のチェックボックスをオンにします。

ステップ 5 **[コマンドの選択（Select a Command）] > [WLAN の削除（Delete a WLAN）] > [実行（Go）]** を選択します。

ステップ 6 [OK] をクリックして削除を実行します。

関連トピック

コントローラで構成されている WLAN の表示 （71 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （73 ページ）
コントローラへの WLAN の追加 （76 ページ）
コントローラの WLAN の管理ステータスを変更する （77 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （72 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （78 ページ）

コントローラの WLAN の管理ステータスを変更する

Prime Infrastructure では、特定のコントローラ上で、複数の WLAN のステータスを一度に変更できます。複数の WLAN を選択して、そのステータスが変更される日時を選択できます。

ステップ 1 [設定（Configuration）]>[ネットワーク（Network）]>[ネットワーク デバイス（Network Devices）] を選択し、[デバイス タイプ（Device Type）]>[ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLANs]>[WLAN 設定（WLAN Configuration）] の順に選択します。

ステップ 4 ステータス変更をスケジュールする WLAN のチェックボックスをオンにします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから、[ステータスのスケジュール（Schedule Status）] を選択して [WLAN スケジュールのタスク詳細（WLAN Schedule Task Detail）] ページを開きます。

選択した WLAN は、ページの上部にリストされます。

ステップ 6 スケジュール設定済みタスク名を入力して、このステータス変更スケジュールを特定します。

ステップ 7 ドロップダウン リストから、新しい管理ステータス（[有効（Enabled）] または [無効（Disabled）]）を選択します。

ステップ 8 スケジュール時刻を、[時（hours）] および [分（minutes）] ドロップダウン リストを使用して選択します。

ステップ 9 カレンダーアイコンをクリックしてスケジュール日を選択するか、テキスト ボックスに日付を入力します（MM/DD/YYYY 形式）。

ステップ 10 適切な [繰り返し（Recurrence）] オプション ボタンを選択して、ステータス変更の頻度を決めます（[毎日（Daily）]、[毎週（Weekly）]、または [繰り返しなし（No Recurrence）]）。

ステップ 11 [送信（Submit）] をクリックしてステータス変更スケジュールを開始します。

関連トピック

コントローラで構成されている WLAN の表示 （71 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （73 ページ）
コントローラへの WLAN の追加 （76 ページ）
コントローラからの WLAN の削除 （77 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （72 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （78 ページ）

コントローラ WLAN のモビリティ アンカーの表示

モビリティ アンカーは WLAN のアンカーとして定義されたコントローラです。クライアント（ラップトップなどの 802.11 モバイル ステーション）は、常にいずれかのアンカーに接続しています。

モビリティ アンカーを使用すると、クライアントのネットワーク エントリ ポイントに関係なく、WLAN を単一のサブネットに制限できます。ユーザは企業全体にわたりパブリック WLAN やゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。また、

WLANは建物の特定のセクション（ロビー、レストランなど）を表すことができるため、ゲスト WLAN で地理的ロード バランシングを実現できます。

クライアントが WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初に関連付けると、クライアントはローカルでそのコントローラに関連付けし、クライアントのローカル セッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティ グループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが、WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初に関連付けすると、クライアントはローカルでそのコントローラに関連付けし、ローカル セッションがクライアントのために作成され、コントローラは同じモビリティ グループの別のコントローラへ通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに連絡をとり、ローカル スイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは暗号化され、有線ネットワークに配信されます。クライアントへのパケットは、アンカー コントローラで受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットをカプセル化してクライアントへ転送します。

2000 シリーズ コントローラを WLAN のアンカーとして指定することはできません。ただし、2000 シリーズ コントローラ上に作成された WLAN に 4100 シリーズ コントローラまたは 4400 シリーズ コントローラをアンカーとして指定できます。

L2TP レイヤ 3 セキュリティ ポリシーは、モビリティ アンカーで設定された WLAN には使用できません。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[WLAN（WLANs）] > [WLANの設定（WLAN Configuration）]** の順に選択します。

ステップ 4 [WLAN ID] をクリックして、特定の WLAN のパラメータを表示します。

ステップ 5 [詳細（Advanced）] タブをクリックします。

ステップ 6 [モビリティ アンカー（Mobility Anchors）] リンクをクリックします。 Prime Infrastructure に各アンカーの IP アドレスおよび現在のステータス（到達可能など）が表示されます。

関連トピック

コントローラで構成されている WLAN の表示 （71 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （73 ページ）
コントローラへの WLAN の追加 （76 ページ）
コントローラからの WLAN の削除 （77 ページ）
コントローラの WLAN の管理ステータスを変更する （77 ページ）

コントローラ上の WLAN へのセキュリティ ポリシーの追加 （72 ページ）

802.11r Fast Transition の設定

802.11r 対応の WLAN は、ワイヤレス クライアント デバイスに迅速かつ効果的なローミング環境を提供します。ただし、堅牢で安全なネットワーク情報交換（ビーコンまたはプローブでの応答）における Fast Transition（FT）認証キー管理（AKM）を認識しない従来のデバイスは、802.11r 対応 WLAN に接続できません。

手順

	コマンドまたはアクション	目的
ステップ 1	すべてのワイヤレス コントローラを表示するには、**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、次に **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。	
ステップ 2	対応するコントローラの名前をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[WLAN（WLANs）] > [WLAN 設定（WLAN configuration）]** を選択して [WLAN 設定（WLAN Configuration）] ページにアクセスします。	
ステップ 4	対応する WLAN ID をクリックして、その特定の WLAN のパラメータを表示します。	
ステップ 5	**[セキュリティ（Security）] > [レイヤ 2（Layer 2）]** タブをクリックします。	
ステップ 6	[レイヤ 2 セキュリティ（Layer 2 Security）] ドロップダウン リストから、[WPA+WPA2] を選択します。	Fast Transition の認証キー管理パラメータが表示されます。
ステップ 7	[Fast Transition] チェックボックスをオンまたはオフにして、Fast Transition を有効または無効にします。Fast Transition は、Cisco WLC リリース 8.3 以降から新しい WLAN を作成する場合、デフォルトで有効になります。ただし、既存の WLAN は以前のリリースからリリース 8.3 へ Cisco WLC をアップグレードする場合に現在の設定を保持します。	
ステップ 8	[Over the DS] チェックボックスをオンまたはオフにして、分散システム経由の Fast Transition を有効または無効にします。このオプションは、Fast	

	コマンドまたはアクション	目的
	Transition を有効にしたとき、または Fast Transition が適応型の場合のみ指定できます。	
ステップ 9	[再アソシエーション タイムアウト（Reassociation Timeout）] フィールドに、AP へのクライアントの再関連付けの試行がタイムアウトになる秒数を入力します。有効な値の範囲は 1 ～ 100 秒です。	このオプションは、Fast Transition を有効にした場合だけ使用できます。
ステップ 10	[認証キーの管理（Authentication Key Management）] で、[FT 802.1X] または [FT PSK] を選択します。キーを有効または無効にするには、対応するチェックボックスをオンまたはオフにします。[FT PSK] チェックボックスをオンにした場合は、[PSK 形式（PSK Format）] ドロップダウン リストから [ASCII] または [HEX] を選択して、キー値を入力します。	適応型 Fast Transition が有効になっている場合は、[802.1X] および [PSK] のみを使用できます。
ステップ 11	[保存（Save）] をクリックして設定を保存します。	

Fastlane QoS の設定

Fastlane QoS 機能は、Apple クライアントの場合に、その他のワイヤレス クライアントと比較して Quality of Service（QoS）処理が優れています。この機能は、デフォルトではディセーブルになっています。

（注） この機能は、少数のクライアントが接続されているときのメンテナンス時間にのみ有効または無効にできます。これは、すべての WLAN とネットワークが無効または有効に戻る時にサービスが中断されるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	対応するコントローラの名前をクリックします。	
ステップ 3	左側のサイドバー メニューから、**[WLAN（WLANs）] > [WLANの設定（WLAN Configuration）]** の順に選択します。	

	コマンドまたはアクション	目的
ステップ 4	対応する WLAN ID をクリックして、その特定の WLAN のパラメータを表示します。	
ステップ 5	[QoS] タブをクリックします。	
ステップ 6	Fastlane QoS を有効にするには、[Fastlane] チェックボックスをオンにします。	
ステップ 7	[保存（Save）] をクリックして設定を保存します。	

Fastlane QoS の無効化

（注） Fastlane QoS を無効にする前に、すべての WLAN で Fastlane を無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	**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラの [デバイス名（Device Name）] をクリックします。	
ステップ 3	左側のサイドバー メニューから、**[WLAN（WLANs）]** > **[WLANの設定（WLAN Configuration）]** の順に選択します。	
ステップ 4	[コマンドの選択（Select a command）] ドロップダウン リストから [Fastlane の無効化（Disable Fastlane）] を選択します。	
ステップ 5	[保存（Save）] をクリックして設定を保存します。	

コントローラの WLAN AP グループの設定

サイト固有の VLAN または AP（アクセス ポイント）グループを使用すると、WLAN を異なるブロードキャスト ドメインにセグメント化することができます。これにより、ブロードキャスト ドメインの総数を最小限に抑えられ、より効率的なロード バランシングおよび帯域幅割り当てが可能になります。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLAN] > [AP グループ（AP Groups）] の順に選択します。[AP グループのサマリー（AP groups summary）] ページが表示されます。

このページには、ネットワーク上に設定されている AP グループのサマリーが表示されます。

このページから、AP グループの削除または詳細の表示ができます。

ステップ 4 [アクセス ポイント（Access Points）] タブで AP グループ名をクリックして、そのアクセス ポイントを表示または編集します。

ステップ 5 [WLAN プロファイル（WLAN Profiles）] タブをクリックして、WLAN プロファイルを表示、編集、追加、または削除します。

関連トピック

コントローラの WLAN AP グループの作成 （83 ページ）
コントローラの WLAN AP グループの削除 （85 ページ）
コントローラでの WLAN の作成 （71 ページ）
構成の違いを特定するためのコントローラ WLAN AP グループの監査 （86 ページ）

コントローラの WLAN AP グループの作成

AP（アクセス ポイント）グループを追加するには、[AP グループの詳細（AP Groups detail）] ページを使用します。バージョン 5.2 より前のターゲット コントローラでは、*AP グループ*が *AP グループ VLAN* と呼ばれることに注意してください。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[WLAN] > [AP グループ（AP Groups）]** を選択します。

ステップ 4 **[コマンドの選択（Select a command）] > [AP グループの追加（Add AP Groups）] > [実行（Go）]** を選択します。[AP グループの詳細（AP Groups detail）] ページが表示されます。

ステップ 5 次のように、新しい AP グループを作成します。

a) AP グループの名前を入力します。
b) 新しい AP グループの説明を入力します（このグループの説明は任意です）。

ステップ 6 次のように、新しい AP グループにアクセス ポイントを追加します。

a) [アクセス ポイント（Access Points）] タブをクリックします。

b) [追加（Add）] をクリックします。[アクセス ポイント（Access Point）] ページに、使用できるアクセス ポイントのリストが表示されます。
c) 追加するアクセス ポイントのチェックボックスをオンにします。
d) [選択（Select）] をクリックします。

ステップ 7 次のように、WLAN プロファイルを追加します。

a) [WLAN プロファイル（WLAN Profiles）] タブをクリックします。
b) [追加（Add）] をクリックします。

使用可能なすべての WLAN プロファイル名を表示するには、テキスト ボックスから現在の WLAN プロファイル名を削除します。テキスト ボックスから現在の WLAN プロファイルの名前を削除すると、使用可能なすべての WLAN プロファイルがドロップダウン リストに表示されます。

各アクセスポイントは16個のWLANプロファイルに限定されます。各アクセスポイントは、WLAN オーバーライド機能が有効にされない限り、すべての WLAN プロファイルをブロードキャストします。WLAN オーバーライド機能によって、アクセス ポイントごとに 16 個の任意の WLAN プロファイルを無効にできます。

WLAN オーバーライド機能は、512 個の WLAN 機能をサポートしていない（最大 512 個の WLAN プロファイルをサポートできる）古いコントローラのみに適用されます。

c) WLAN プロファイル名を入力するか、[WLAN プロファイル名（WLAN Profile Name）] ドロップダウン リストからいずれか 1 つを選択します。
d) インターフェイス/インターフェイス グループを入力するか、[インターフェイス/インターフェイス グループ（Interface/Interface Group）] ドロップダウン リストからいずれか 1 つを選択します。

使用できるすべてのインターフェイスを表示するには、[インターフェイス（Interface）] テキスト ボックスから現在のインターフェイスを削除します。[インターフェイス（Interface）]テキストボックスから現在のインターフェイスを削除すると、使用可能なすべてのインターフェイスがドロップダウン リストに表示されます。

e) 該当する場合は、[NAC オーバーライド（NAC Override）]チェックボックスをオンにします。デフォルトでは、NAC オーバーライドは無効になっています。
f) [追加/編集（Add/Edit）] リンクをクリックして、ポリシー設定パラメータを指定します。

- [ポリシー名（Policy Name）]：ポリシーの名前。
- [ポリシー プライオリティ（Policy Priority）]：1 ～ 16 のポリシー プライオリティを設定します。2 個のポリシーが同じプライオリティを持つことはできません。

WLAN 1 つあたり 16 個までポリシー マッピングが許可されます。マッピングに選択されたポリシー テンプレートは、コントローラにポリシーがない場合に最初に適用されます。

g) アクセス ポイントおよび WLAN プロファイルを追加したら、[保存（Save）] をクリックします。

ステップ 8 （任意）次のように、RF プロファイルを追加します。

a) [RF プロファイル（RF Profiles）] タブをクリックします。
b) 次のようにフィールドに入力します。

- [802.11a]：802.11a 無線の AP 用の RF プロファイルを選択します。
- [802.11b]：802.11b 無線の AP 用の RF プロファイルを選択します。

ステップ 9 Hyperlocation 設定パラメータは、次のように追加します。

- [ロケーション設定（Location Settings）] タブをクリックし、次の項目を設定します。
  - [Hyperlocation]：このオプションを有効にすると、そのコントローラに関連付けられた Hyperlocation モジュールがあるすべての AP が有効になります。
  - [最小パケット検出 RSSI（Packet Detection RSSI Minimum）]：この値を調整して、位置計算から精度の低い RSSI 測定値を除外します。
  - [アイドル クライアント検出のスキャン カウントしきい値（Scan Count Threshold for Idle Client Detection）]：スキャン中に検出されるアイドル クライアントの最大許容数。
  - [NTP サーバの IP アドレス（NTP Server IP Address）]：有効な NTP サーバの IP アドレスを入力します。この IP アドレスは、時刻同期のためにすべての AP で使用されます。

ステップ 10 新しい AP グループへの AP、WLAN プロファイル、RF プロファイルの追加が終了したら、[保存（Save）] をクリックします。

AP グループの WLAN インターフェイス マッピングを変更すると、このグループの FlexConnect AP のローカル VLAN マッピングが削除されます。これらのマッピングは、この変更を適用した後に再度設定する必要があります。

関連トピック

コントローラの WLAN AP グループの設定 （82 ページ）
コントローラの WLAN AP グループの削除 （85 ページ）
構成の違いを特定するためのコントローラ WLAN AP グループの監査 （86 ページ）

コントローラの WLAN AP グループの削除

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLAN] > [AP グループ（AP Groups）] の順に選択します。

ステップ 4 削除する AP グループのチェックボックスをオンにします。

ステップ 5 [コマンドの選択（Select a Command）] > [AP グループの削除（Delete AP Groups）] > [実行（Go）] の順に選択します。

ステップ 6 [OK] をクリックして削除を実行します。

関連トピック

コントローラの WLAN AP グループの設定 （82 ページ）
コントローラの WLAN AP グループの作成 （83 ページ）
構成の違いを特定するためのコントローラ WLAN AP グループの監査 （86 ページ）

構成の違いを特定するためのコントローラ WLAN AP グループの監査

Prime Infrastructure が AP グループについて保存した値と、現在のコントローラおよびアクセスポイントのデバイス設定に保存されている実際の値の間で違いが生じる可能性があります。AP グループを監査することで、相違が生じているかどうかを特定して解決することができます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLAN] > [AP グループ（AP Groups）] の順に選択します。

ステップ 4 監査するアクセス ポイント グループの名前をクリックします。

ステップ 5 [監査（Audit）] をクリックします。

[監査（Audit）] ボタンは、ページ下部の [保存（Save）] ボタンと [キャンセル（Cancel）] ボタンの横にあります。

関連トピック

コントローラの WLAN AP グループの作成 （83 ページ）
コントローラの WLAN AP グループの削除 （85 ページ）
コントローラでの WLAN の作成 （71 ページ）

キャプティブ ポータル バイパスに関する情報

キャプティブ ポータルは、ユーザがネットワークに接続したときにリダイレクトされる Web ページです。通常は、利用規約に関する情報が表示され、ログインにも使用されます。認証 WISPr は、ユーザが異なるワイヤレス サービス プロバイダー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 要求をコントローラに送信します。コントローラはユーザ エージェントの詳細をチェックし、コントローラでの Web 認証代行受信により HTTP 要求をトリガーします。ユーザ 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に、コントローラによってクライアントはキャプティブ 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、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と（設定された RADIUS サーバが URL を指定）、WISPr 要求が非常に短い間隔で発信されるので、スプラッシュ ページが表示されることはなく、いずれかのクエリーが指定のサーバに到達できるとただちに、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中断されます。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 に送られます。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。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、ユーザが、ユーザ コンテキストでスプラッシュ ページ 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。

キャプティブ ネットワーク ポータル バイパスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	デバイス名をクリックして [設定（Configuration）] タブをクリックします。	
ステップ 3	**[システム（System）] > [一般 - システム（General - System）]** を選択して、[一般（General）] ページにアクセスします。	
ステップ 4	[キャプティブネットワークアシスタント（Captive Network Assistant）]バイパス ドロップダウンリストから、[有効（Enable）] を選択します。	

WLAN ごとのキャプティブ ネットワーク ポータル バイパスの設定

手順

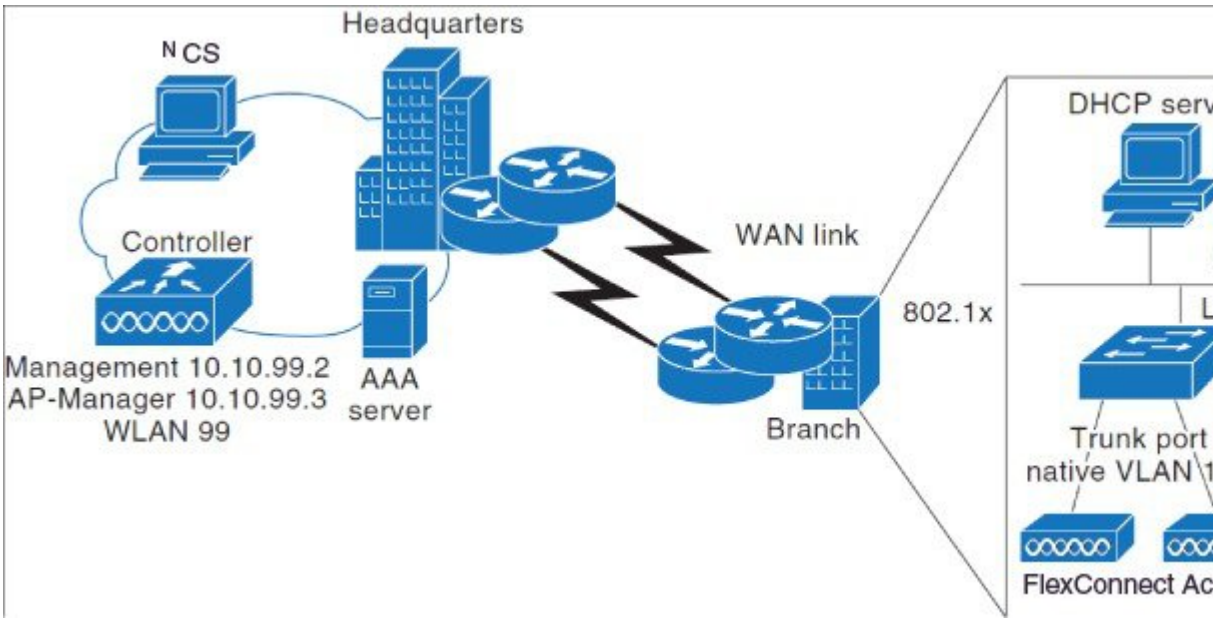
	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	デバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[WLAN（WLANs）] > [WLAN 設定（WLAN Configuration）]** を選択します。	
ステップ 4	[WLAN ID] をクリックします。	
ステップ 5	**[セキュリティ（Security）] > [レイヤ 3（Layer 3）]** タブをクリックしてデフォルトのセキュリティ ポリシーを変更します。	
ステップ 6	[キャプティブネットワークアシスタント（Captive Network Assistant）]バイパス ドロップダウンリストから、[有効（Enable）] を選択します。	
ステップ 7	[保存（Save）] をクリックします。	

FlexConnect を使用した AP の設定とモニタ

FlexConnect により、各オフィスにコントローラを導入しなくても、本社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、リモート ロケーションの AP を設定および制御できるようになります。FlexConnect AP は、コントローラへの接続を失うと、クライアント データ トラフィックを切り替えてクライアント認証をローカルで実行します。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

次の図に、一般的な FlexConnect の導入を示します。

図 *8 : FlexConnect* の導入



関連トピック

FlexConnect がサポートされるデバイス （89 ページ）
FlexConnect の使用時の前提条件 （90 ページ）
FlexConnect が認証を実行する仕組み （91 ページ）
FlexConnect 動作モード：[接続中（Connected）]および[スタンドアロン（Standalone）]（91 ページ）
FlexConnect の状態 （92 ページ）

FlexConnect がサポートされるデバイス

FlexConnect は次のコンポーネントでのみサポートされます。

- 1130AG、1240AG、1142、および 1252 の AP
- Cisco 2000 および 4400 シリーズ コントローラ
- Catalyst 3750G 統合型ワイヤレス LAN コントローラ スイッチ
- Cisco Wireless Services Module（WiSM）
- サービス統合型ルータ用のコントローラ ネットワーク モジュール

関連トピック

FlexConnect の使用時の前提条件 （90 ページ）
FlexConnect が認証を実行する仕組み （91 ページ）
FlexConnect 動作モード：[接続中（Connected）]および[スタンドアロン（Standalone）]（91 ページ）
FlexConnect の状態 （92 ページ）

FlexConnect の使用時の前提条件

FlexConnect の設定時は、次のガイドラインに従います。

- 静的 IP アドレスまたは DHCP アドレスのいずれかを持つ FlexConnect を導入することができます。DHCP サーバがローカルで使用可能になっており、ブート時に AP に IP アドレスを提供できる必要があります。
- 最大伝送ユニット（MTU）は、500 バイト以上にする必要があります。
- ラウンドトリップ遅延は、AP とコントローラ間で 300 ミリ秒を超えないようにする必要があります。ラウンドトリップ遅延を 300 ミリ秒以下に抑えられない場合は、ローカル認証を実行するよう AP を設定します。
- コントローラは、ユニキャスト パケットまたはマルチキャスト パケットの形式でマルチキャスト パケットを AP に送信できます。FlexConnect モードでは、AP はユニキャスト形式でのみマルチキャスト パケットを受信できます。
- FlexConnect は CCKM 完全認証をサポートしますが、CCKM 高速ローミングをサポートしません。
- FlexConnect は、真のマルチキャストを除くすべての機能に対して、1 対 1 ネットワーク アドレス変換（NAT）設定とポート アドレス変換（PAT）をサポートします。NAT 境界を越えるマルチキャストもサポートされます（ユニキャスト オプションを使用して設定されている場合）。
- VPN、IPsec、L2TP、PPTP、Fortress 認証、および Cranite 認証は、これらのセキュリティ タイプが AP でローカルにアクセス可能である場合、ローカル スイッチングのトラフィックに対してサポートされます。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。
- FlexConnect AP の場合、FlexConnect ローカル スイッチングが設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとして AP で継承されます。これは SSID ごと、FlexConnect AP ごとに簡単に変更できます。FlexConnect 以外の AP では、すべてのトラフィックがトンネルを通じてコントローラに戻され、VLAN タギングは WLAN の各インターフェイス マッピングによって決定されます。
- デフォルトでは、FlexConnect AP で VLAN は有効化されていません。FlexConnect を有効にすると、AP は WLAN に関連付けられた VLAN ID を継承します。この設定は AP で保存され、接続応答が成功した後に受信されます。デフォルトでは、ネイティブ VLAN は 1 です。VLAN が有効化されているドメインの FlexConnect AP ごとに、ネイティブ VLAN を 1 つ設定する必要があります。設定しないと、AP はコントローラとの間でパケットを送受信できません。クライアントが RADIUS サーバから VLAN を割り当てられている場合、その VLAN はローカル スイッチングの WLAN に関連付けられます。

関連トピック

FlexConnect が認証を実行する仕組み （91 ページ）

FlexConnect が認証を実行する仕組み

FlexConnect AP は、ブート時にコントローラを検索します。AP はそのコントローラに接続し、コントローラから最新のソフトウェアイメージと設定情報をダウンロードして、無線を初期化します。スタンドアロン モードで使用するために、ダウンロードした設定を不揮発性メモリに保存します。

FlexConnect AP は、次のいずれかの方法でコントローラの IP アドレスを識別します。

- AP が IP アドレスを DHCP サーバから割り当てられている場合、通常の CAPWAP 検出プロセス（レイヤ 3 ブロードキャスト、無線プロビジョニング（OTAP）、DNS、または DHCP オプション 43）によりコントローラを検出します。OTAP は AP の初回ブート時には動作しません。
- AP が静的 IP アドレスを割り当てられている場合、DHCP オプション 43 を除く CAPWAP 検出プロセスのいずれかのメソッドを使用してコントローラを検出します。AP がレイヤ 3 ブロードキャストでも OTAP でもコントローラを検出できない場合は、DNS 解決を使用することを推奨します。DNS を使用すれば、静的 IP アドレスを持ち DNS サーバを認識している AP は、最低 1 つのコントローラを見つけることができます。
- AP で CAPWAP 検出メカニズムを使用できないリモート ネットワークからコントローラを検出させる場合には、プライミングを使用できます。この方法を使用すると、AP の接続先のコントローラを（AP のコマンドライン インターフェイスにより）指定できます。

関連トピック

FlexConnect がサポートされるデバイス （89 ページ）
FlexConnect の使用時の前提条件 （90 ページ）
FlexConnect 動作モード：[接続中（Connected）] および [スタンドアロン（Standalone）] （91 ページ）
FlexConnect の状態 （92 ページ）

FlexConnect 動作モード：[接続中（Connected）] および [スタンドアロン（Standalone）]

FlexConnect AP の動作モードは次の 2 種類です。

- 接続モード：このモードでは、FlexConnect AP とコントローラが CAPWAP 接続されます。
- スタンドアロン モード：コントローラが到達不能な場合、FlexConnect AP はスタンドアロン モードになり、独自にクライアントを認証します。

FlexConnect AP がスタンドアロン モードになると、以下が実行されます。

-
  - 中央でスイッチされる WLAN 上のすべてのクライアントが関連付けを解除されます。
  - 802.1X または Web 認証 WLAN の場合、既存クライアントは関連付けを解除されませんが、FlexConnect AP は関連付けされたクライアントの数がゼロになると、ビーコンの送信を停止します。
  - 802.1X または Web 認証 WLAN に関連付けしている新規クライアントに関連付け解除のメッセージが送信されます。

- 802.1X 認証、NAC、および Web 認証（ゲスト アクセス）などのコントローラ依存アクティビティが無効になり、APはコントローラに侵入検知システム（IDS）レポートを送信しません。
- 無線リソース管理（RRM）機能（ネイバー ディスカバリ、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバーリストの使用、不正阻止および検出など）が無効にされます。ただし、FlexConnect APではスタンドアロンモードで動的周波数選択がサポートされています。

FlexConnect APは、スタンドアロンモードになった後も、クライアントの接続を維持します。ただし、APがコントローラとの接続を再確立すると、すべてのクライアントを関連付け解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

AP 上の LED は、デバイスが異なる FlexConnect モードになると変化します。

関連トピック

FlexConnect がサポートされるデバイス （89 ページ）
FlexConnect の使用時の前提条件 （90 ページ）
FlexConnect が認証を実行する仕組み （91 ページ）
FlexConnect の状態 （92 ページ）

FlexConnect の状態

FlexConnect WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- **中央認証、中央スイッチング**：この状態では、コントローラがクライアント認証を処理し、すべてのクライアントデータはトンネルを通じてコントローラに戻されます。この状態は、接続済みモードの場合にだけ有効です。
- **中央認証、ローカル スイッチング**：この状態では、コントローラがクライアント認証を処理し、FlexConnect AP がデータ パケットをローカルにスイッチします。この状態は、FlexConnect AP が接続モードの場合にのみサポートされます。
- **ローカル認証、ローカル スイッチング**：この状態では、FlexConnect APがクライアント認証を処理し、クライアントデータ パケットをローカルにスイッチします。AP自体で認証できるため、遅延要件が軽減されます。ローカル認証は、ローカル スイッチング モードの FlexConnect AP の WLAN でのみ有効にできます。この状態はスタンドアロン モードおよび接続モードで有効です。

ローカル認証は、次の条件を満たすことができない場合に役立ちます。

- 128 kbps の最小帯域幅。
- 100 ms 以下のラウンドトリップ遅延。
- 500 バイト以上の最大伝送ユニット（MTU）。

ローカル認証は次をサポートしません。

- ゲスト認証。
- RRM 情報。

- ローカル RADIUS。
- グループ内の WLC およびその他の FlexConnect AP でクライアント情報が更新される前のローミング。

- **認証ダウン、スイッチング ダウン**：この状態になると、WLAN は既存クライアントの関連付けを解除し、ビーコン応答とプローブ応答の送信を停止します。この状態はスタンドアロン モードでのみ有効です。
- **認証ダウン、ローカル スイッチング**：この状態では、WLAN は新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。この状態はスタンドアロン モードでのみ有効です。

FlexConnect AP がスタンドアロン モードになると、WLAN は次の状態になります。

- WLAN がオープン、共有、WPA-PSK、または WPA2-PSK 認証として設定されており、新しいクライアントの認証を続行する場合は、ローカル認証、ローカル スイッチングの状態。
- WLAN が中央スイッチングを行うように設定されている場合は、認証ダウン、スイッチング ダウンの状態。
- WLAN がローカル スイッチングを行うように設定されている場合は、認証ダウン、ローカル スイッチングの状態。

関連トピック

FlexConnect がサポートされるデバイス （89 ページ）
FlexConnect の使用時の前提条件 （90 ページ）
FlexConnect が認証を実行する仕組み （91 ページ）
FlexConnect 動作モード：[接続中（Connected）]および[スタンドアロン（Standalone）]（91 ページ）
FlexConnect の設定方法と使用方法：ワークフロー （93 ページ）

FlexConnect の設定方法と使用方法：ワークフロー

FlexConnect を設定するには、この項の手順を次の順序で実行する必要があります。

1. FlexConnect のリモート スイッチの設定
2. FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定
3. FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定
4. ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定
5. AP での FlexConnect の設定
6. クライアント デバイスの WLAN への接続（FlexConnect）

FlexConnect のリモート スイッチの設定

リモート サイトでスイッチを準備するには、次の手順を実行します。

ステップ 1 FlexConnect に有効な AP をトランクに接続するか、またはスイッチ上のポートにアクセスします。

ステップ 2 FlexConnect AP をサポートするようにスイッチを設定します。

関連トピック

例：リモート サイトでスイッチに FlexConnect を設定する （94 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （95 ページ）
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 （96 ページ）
ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定 （96 ページ）

例：リモート サイトでスイッチに FlexConnect を設定する

この設定例の場合：

- FlexConnect AP は、トランク インターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。AP は、このネイティブ VLAN 上での IP 接続を必要とします。
- リモート サイトのローカル サーバとリソースは、VLAN 101 上にあります。
- DHCP プールがスイッチの両 VLAN のローカル スイッチ内に作成されます。
- 最初の DHCP プール（ネイティブ）は FlexConnect AP により使用され、2 つ目の DHCP プール（ローカル スイッチング）は、クライアントがローカルでスイッチされる WLAN に関連付ける場合、クライアントにより使用されます。

この設定例のアドレスは、図示のみを目的としています。使用するアドレスは、アップストリーム ネットワークに適合している必要があります。

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1

!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1

!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

関連トピック

FlexConnect のリモート スイッチの設定 （93 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （95 ページ）
FlexConnect用のローカルでスイッチングされるWLANコントローラの設定 （96ページ）
ゲストアクセス用の中央でスイッチングされるWLANコントローラの設定 （96ページ）

FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定

中央でスイッチされる WLAN を作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLAN] > [WLAN 設定（WLAN Configuration）] を選択して [WLAN 設定（WLAN Configuration）] ページにアクセスします。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [WLAN の追加（Add a WLAN）] を選択し、[実行（Go）] をクリックします。

Cisco AP はコントローラごとに最大 16 の WLAN をサポートできます。ただし Cisco AP の中には、WLAN ID が 9 以上の WLAN をサポートしないものがあります。この場合、WLAN を作成しようとすると次のメッセージが表示されます。

「*AP のすべてのタイプが 8 個より多い WLAN ID をサポートするとは限りませんが、続行しますか。（Not all types of AP support WLAN ID greater than 8, do you wish to continue?）*」

[OK] をクリックすると、次に使用可能な WLAN ID を持つ WLAN が作成されます。

WLAN ID が 8 未満の WLAN が削除されている場合、次に作成する WLAN にその ID が適用されます。

ステップ 5 コントローラに適用するテンプレートをドロップダウン リストから選択します。

新しい WLAN テンプレートを作成する場合は、[ここをクリック（Click here）] リンクをクリックするとテンプレート作成ページにリダイレクトされます。

ステップ 6 [レイヤ 2 セキュリティ（Layer 2 Security）] ドロップダウン リストから [WPA1+WPA2] を選択します。

ステップ 7 [一般ポリシー（General Policies）] の下にある [ステータス（Status）] チェックボックスをオンにして WLAN を有効にします。

NAC が有効で、これで使用する検疫 VLAN を作成済みである場合は、[一般ポリシー（General Policies）] の下にある [インターフェイス（Interface）] ドロップダウン リストから選択してください。また、[AAA オーバーライドを許可する（Allow AAA Override）] チェックボックスをオンにして、コントローラが確実に検疫 VLAN 割り当てを検証するようにします。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

FlexConnect のリモート スイッチの設定 （93 ページ）

FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定

ローカルでスイッチされる WLAN を作成するには、次の手順を実行します。

ステップ 1 「FlexConnect用の中央でスイッチングされるWLANコントローラの設定」のステップ1～5の説明に従って、新しい WLAN を作成します。

ステップ 2 WLAN ID をクリックして設定パラメータを変更します。

[レイヤ2セキュリティ（Layer 2 Security）] ドロップダウン リストから [WPA1+WPA2] を選択します。PSK 認証キー管理を選択し、事前共有キーを入力してください。

ステップ 3 この WLAN の [管理ステータス（Admin Status）] チェックボックスをオンにします。

ステップ 4 [FlexConnect ローカル スイッチング（FlexConnect Local Switching）] チェックボックスをオンにし、ローカル スイッチングを有効にします。

ステップ 5 [保存（Save）] をクリックして変更を確定します。

関連トピック

FlexConnect のリモート スイッチの設定 （93 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （95 ページ）
ゲストアクセス用の中央でスイッチングされるWLANコントローラの設定 （96ページ）

ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定

ゲスト アクセス用に中央でスイッチされる WLAN を作成し、トンネルを通じてゲスト トラフィックがコントローラに渡されるようにするには、次の手順を実行します。

ステップ 1 「*FlexConnect* 用の中央でスイッチングされる *WLAN* コントローラの設定」のステップ 1 ～ 5 の説明に従って、新しい WLAN を作成します。

ステップ 2 WLAN をクリックして次の設定パラメータを変更します。

a) [セキュリティ（Security）] タブの [レイヤ 2 セキュリティ（Layer 2 Security）] および [レイヤ 3 セキュリティ（Layer 3 Security）] ドロップダウン リストから [なし（None）] を選択します。

b) [Web ポリシー（Web Policy）] チェックボックスをオンにします。

c) [認証（Authentication）] を選択します。

d) 外部 Web サーバを使用する場合は、WLAN で事前認証アクセス コントロール リスト（ACL）を設定し、WLAN 事前認証 ACL としてこの ACL を選択します。

ステップ 3 [一般ポリシー（General Policies）] の下にある [ステータス（Status）] チェックボックスをオンにして WLAN を有効にします。

ステップ 4 [保存（Save）] をクリックして、変更内容を確定します。

次のタスク

関連項目

- FlexConnect のリモート スイッチの設定
- FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定
- FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定
- ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定
- （テンプレートの章）

関連トピック

FlexConnect のリモート スイッチの設定 （93 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （95 ページ）
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 （96 ページ）
コントローラ WLAN の Web 認証タイプの設定

中央でスイッチングされる WLAN へのゲストの追加（FlexConnect）

ローカル ユーザを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [ローカルネットユーザ（Local Net Users）]** を選択します。

ステップ 3 必要なフィールドに入力します。

ステップ 4 [プロファイル（Profile）] ドロップダウン リストから、適切な SSID を選択します。

ステップ 5 ゲスト ユーザ アカウントの説明を入力します。

ステップ 6 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

関連トピック

ゲストアクセス用の中央でスイッチングされる WLAN コントローラの設定 （96 ページ）

AP での FlexConnect の設定

FlexConnect に AP を設定するには、次の手順を実行します。

ステップ 1 AP をネットワークに物理的に追加します。

ステップ 2 [設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）] を選択します。

ステップ 3 [AP 名（AP Name）] リストから、AP を選択します。

ステップ 4 [設定（Configuration）] > [テンプレート（Templates）] > [Lightweight アクセス ポイント（Lightweight Acess Points）]、または [AP モード（AP Mode）] フィールドに FlexConnect が表示されない場合は [自律型アクセスポイント（Autonomous Access Points）] を選択します。

[AP モード（AP Mode）] フィールドに [FlexConnect] が表示される場合は、ステップ 8 に進みます。

ステップ 5 [AP 名（AP Name）] リストから、AP を選択します。[Lightweight AP テンプレートの詳細（Lightweight AP Template Detail）] ページが表示されます。

ステップ 6 [FlexConnect モードをサポート（FlexConnect Mode supported）] チェックボックスをオンにして、すべてのプロファイル マッピングを表示します。

モードを FlexConnect に変更する際に、AP がまだ FlexConnect モードでない場合、他のすべての FlexConnect パラメータはその AP に適用されません。

ステップ 7 [VLAN サポート（VLAN Support）] チェックボックスをオンにして、[ネイティブ VLAN ID（Native VLAN ID）] テキスト ボックスにリモート ネットワーク上のネイティブ VLAN の番号を入力します。

ステップ 8 [適用/スケジュール（Apply/Schedule）] タブをクリックして変更を保存します。

ステップ 9 [ローカルでスイッチされる VLAN（Locally Switched VLANs）] セクションの [編集（Edit）] リンクをクリックして、クライアント IP アドレスの取得元となる VLAN の数を変更します。

ステップ 10 [保存（Save）] をクリックして変更内容を保存します。

リモート サイトで FlexConnect に設定する必要があるすべての追加 AP にこの手順を繰り返します。

関連トピック

FlexConnect のリモート スイッチの設定 （93 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （95 ページ）
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 （96 ページ）

クライアント デバイスの WLAN への接続（FlexConnect）

次の指示に従って、クライアント デバイスでコントローラの設定時に作成した WLAN に接続するプロファイルを作成します。

この例では、クライアント上で 3 つのプロファイルを作成します。

1. 中央でスイッチされる WLAN に接続するには、WPA/WPA2 と PEAP-MSCHAPV2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、コントローラの管理 VLAN から IP アドレスが取得されます。
2. ローカルでスイッチされる WLAN に接続するには、WPA/WPA2 認証を使用するクライアント プロファイルを作成します。クライアントが認証されると、ローカル スイッチの VLAN 101 から IP アドレスが取得されます。
3. ゲスト アクセス用の中央でスイッチされる WLAN に接続するには、オープン認証を使用するプロファイルを作成します。クライアントが認証されると、AP へのネットワーク ローカル上の VLAN 101 から IP アドレスが取得されます。クライアントが接続されると、ローカル ユーザは任意の HTTP アドレスを Web ブラウザに入力します。Web 認証プロセスを完了するため、コントローラに自動的に誘導されます。Web ログイン ページが表示されたら、ユーザ名とパスワードを入力します。

クライアントのデータ トラフィックがローカル スイッチングか中央スイッチングかを確認するには、[モニタ（Monitor）] > [デバイス（Devices）] > [クライアント（Clients）] の順に選択します。

関連トピック

FlexConnect のリモート スイッチの設定 （93 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （95 ページ）
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 （96 ページ）
ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定 （96 ページ）

FlexConnect で使用する AP グループの作成

FlexConnect により、各ロケーションにコントローラを導入しなくても、ワイドエリア ネットワーク（WAN）リンク経由で、リモート ロケーションの AP を設定および制御できるようになります。ロケーションごとの FlexConnect AP の数に関する導入制限はありませんが、AP を整理してグループ化できます。

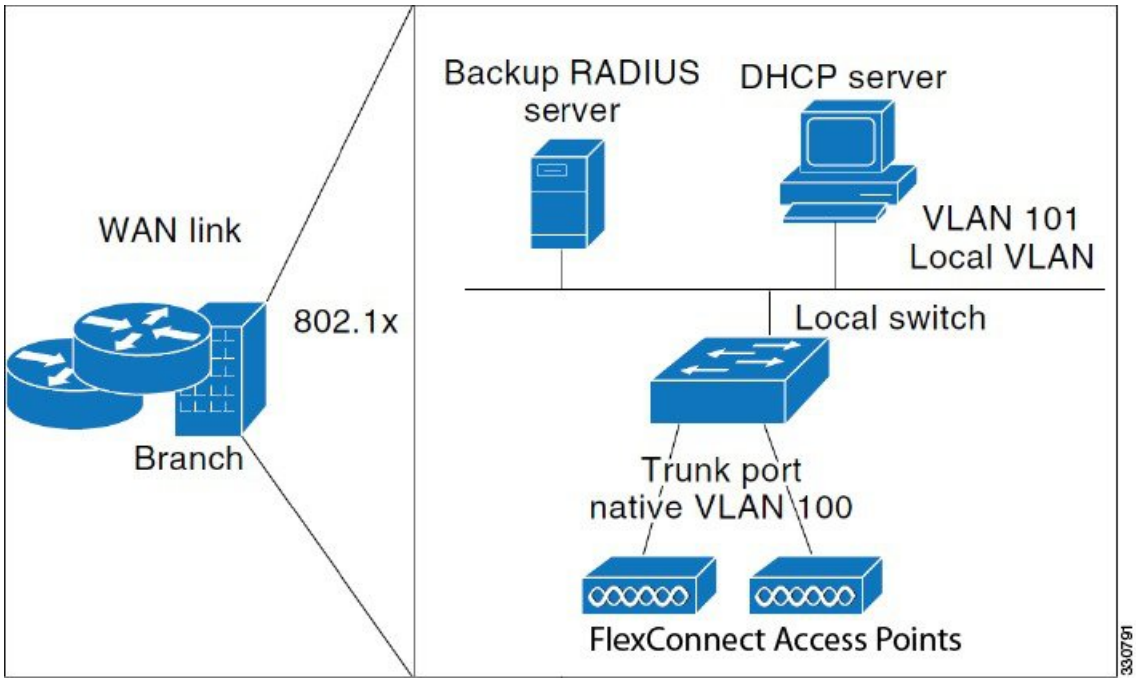
同じ設定で AP グループを作成することによって、個別にコントローラにアクセスするよりも CCKM 高速ローミングなどをより速く処理できます。

たとえば、CCKM 高速ローミングをアクティブにするには、FlexConnect AP が関連付ける可能性のあるすべてのデバイスの CCKM キャッシュを認識している必要があります。300 個の AP と 1000 台のデバイスが接続可能なコントローラを使用している場合は、1000 台のすべてのデバイスにではなく、FlexConnect グループに対して CCKM キャッシュを処理して送信する方が迅速かつ実用的です。ある特定の FlexConnect グループを少数の AP に集中させ、そのグループ内のデバイスがそれらの少数の AP に接続してローミングできるようにすることができます。確立されたグループでは、CCKM キャッシュやバックアップ RADIUS などの機能が各 AP で設定されるのではなく、FlexConnect グループ全体に設定されます。

グループ内のすべての FlexConnect AP は、同じ WLAN、バックアップ RADIUS サーバ、CCKM、およびローカル認証設定情報を共有します。この機能は、複数の FlexConnect AP がリモート オフィスやビルディングのフロアにあり、すべてを一度に設定する場合に役立ちます。たとえば、各 AP に同じサーバを設定する必要なく、FlexConnect グループのバックアップ RADIUS サーバを設定できます。

次の図に、ブランチ オフィスでのバックアップ RADIUS サーバを備えた一般的な FlexConnect グループの展開を示します。

図 *9 : FlexConnect* グループの導入



関連項目

- FlexConnect グループおよびバックアップ RADIUS サーバ
- FlexConnect グループおよび CCKM
- FlexConnect グループおよびローカル認証
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect グループおよびバックアップ RADIUS サーバ

スタンドアロン モードの FlexConnect AP がバックアップ RADIUS サーバに対して完全な 802.1x 認証を実行できるように、コントローラを設定することができます。プライマリ RADIUS サーバを設定することも、プライマリとセカンダリの両方の RADIUS サーバを設定することもできます。

関連項目

- FlexConnect グループおよび CCKM
- FlexConnect グループおよびローカル認証
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect グループおよび CCKM

CCKM 高速ローミングには FlexConnect グループが必要です。CCKM 高速セキュア ローミング用に WLAN を設定した場合、EAP が有効になっているクライアントは、RADIUS サーバで再認証せずに、あるアクセス ポイントから別のアクセス ポイントに安全にローミングを行いま

す。CCKM を使用すると、アクセス ポイントは高速キー再生成技術を使用します。これによりシスコのクライアント デバイスは、アクセス ポイント間のローミングを通常 150 ミリ秒未満で行えます。CCKM 高速セキュア ローミングでは、遅延に敏感なアプリケーションで認識できるほどの遅延は発生しません。FlexConnect アクセス ポイントは、関連付けられる可能性のあるすべてのクライアントに対する CCKM キャッシュ情報を取得します。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。

たとえば、AP が 300 あるコントローラで、関連付けを行う可能性のあるクライアントが 100 台ある場合、100 台すべてのクライアントに対して CCKM キャッシュを送信することは現実的ではありません。限られた数の AP で構成される FlexConnect グループを作成すると、クライアントは 4 つの AP 間でのみローミングし、クライアントがそれらのいずれかに関連付けられている場合にのみ、4 つの AP 間で CCKM キャッシュが分散されます。

FlexConnect AP と非 FlexConnect AP 間の CCKM 高速ローミングはサポートされていません。

関連項目

- FlexConnect グループおよびバックアップ RADIUS サーバ
- FlexConnect グループおよびローカル認証
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect グループおよびローカル認証

スタンドアロン モードの FlexConnect AP が、最大 20 人の静的に設定されたユーザに対して LEAP または EAP-FAST 認証を実行できるように、コントローラを設定できます。コントローラは、各 FlexConnect AP がコントローラに接続した際に、ユーザ名とパスワードの静的リストをその AP に送信します。グループ内の各 AP は、そのアクセス ポイントに関連付けられたクライアントのみを認証します。

この機能は、Autonomous AP ネットワークから Lightweight FlexConnect AP ネットワークに移行する際に、大きなユーザ データベースを保持したくない場合や、Autonomous AP で利用可能な RADIUS サーバ機能を置き換える際に別のハードウェア デバイスを追加したくない場合に適しています。

LEAP または EAP-FAST 認証は、FlexConnect バックアップ RADIUS サーバと組み合わせて使用できます。FlexConnect グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect AP は常に、まずプライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。その後、セカンダリ バックアップ RADIUS サーバで試行し（プライマリに到達できない場合）、最後に FlexConnect AP 自身で試行します（プライマリおよびセカンダリの RADIUS サーバに到達できない場合）。

関連項目

- FlexConnect グループおよびバックアップ RADIUS サーバ
- FlexConnect グループおよび CCKM
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

既存の FlexConnect AP グループの表示

既存の FlexConnect AP グループのリストを表示できます。個々の AP が FlexConnect グループに属していることを確認するには、[グループで設定されているユーザ（Users configured in the group）] リンクをクリックします。[FlexConnect AP グループ（FlexConnect AP Group）] ページが開き、グループの名前と、そのグループに属している AP が表示されます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect] > [FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。[FlexConnect AP グループ（FlexConnect AP Groups）] ページが開きます。

ステップ 4 グループ名をクリックして FlexConnect AP グループに関する詳細を表示します。

関連トピック

構成の違いを特定するためのコントローラ WLAN AP グループの監査 （86 ページ）

FlexConnect AP グループの設定

FlexConnect AP グループを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect] > [FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストで、[FlexConnect AP グループの追加（Add FlexConnect AP Group）] をクリックし、[FlexConnect AP グループ（FlexConnect AP Group）] > [テンプレートから追加（Add From Template）] ペインを開きます。

ステップ 5 [このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）] ドロップダウン リストからテンプレートを選択します。

ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 必要な FlexConnect AP グループ パラメータを設定します。必要なタブをクリックして、次のマッピングを追加、編集、または削除できます。

- [VLAN-ACL マッピング（VLAN-ACL Mapping）]：有効な VLAN ID の範囲は 1 ～ 4094 です。
- [WLAN-ACL マッピング（WLAN-ACL Mapping）]：外部 Web 認証用の FlexConnect アクセス コントロール リストを選択します。最大 16 個の Web 認証 ACL を追加できます。

- [Web ポリシー ACL（WebPolicy ACL）]：Web ポリシーとして追加する FlexConnect アクセス コントロール リストを選択します。最大 16 個の Web ポリシー ACL を追加できます。
- [ローカル分割（Local Split）]
- [中央 DHCP（Central DHCP）]
  - [中央 DHCP（Central DHCP）]：この機能を有効にすると、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。
  - [DNS のオーバーライド（Override DNS）]：ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバ アドレスのオーバーライドを有効または無効にできます。中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
  - [NAT-PAT]：ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）を有効または無効にできます。NAT および PAT を有効にするには、[中央 DHCP 処理（Central DHCP Processing）] を有効にする必要があります。

ステップ 8 個々のアクセス ポイントが FlexConnect グループに属していることを確認するには、[グループに設定されているユーザ（Users configured in the group）] リンクをクリックします。[FlexConnect AP グループ（FlexConnect AP Group）] ページに、グループの名前と、そのグループに属しているアクセス ポイントが表示されます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 既存の FlexConnect AP グループを削除するには、削除するグループのチェックボックスをオンにし、[コマンドの選択（Select a command）] ドロップダウン リストから [FlexConnect AP グループの削除（Delete FlexConnect AP Group）] を選択します。

関連トピック

既存の FlexConnect AP グループの表示 （102 ページ）

構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect 設定が Cisco Prime Infrastructure またはコントローラ上で時間とともに変化した場合は、設定を監査できます。変化は、後続の画面に表示されます。Cisco Prime Infrastructure またはコントローラを更新して、設定の同期を選択できます。

関連トピック

FlexConnect AP グループの設定 （102 ページ）
既存の FlexConnect AP グループの表示 （102 ページ）

デフォルト FlexConnect グループ

デフォルト FlexConnect グループは、管理者が設定した FlexConnect グループの一部ではない FlexConnect AP がコントローラに加わると自動的に追加されるコンテナです。デフォルト FlexConnect グループは、コントローラの起動時（以前のリリースからアップグレードした後）に作成され、保存されます。このグループを手動で追加または削除することはできません。また、デフォルト FlexConnect グループでアクセス ポイントを手動で追加または削除することはできません。デフォルト FlexConnect グループ内の AP は、グループの共通設定を継承します。グループの設定のどれかを変更すると、その変更は、グループ内のすべての AP に反映されます。

管理者が作成したグループが削除されると、そのグループからのすべての AP がデフォルト FlexConnect グループに移動され、このグループの設定を継承します。同様に、他のグループから手動で削除された AP もデフォルト FlexConnect グループに追加されます。

デフォルト FlexConnect グループからの AP がカスタマイズされたグループに追加されると、（デフォルト FlexConnect グループからの）既存の設定が削除され、カスタマイズされたグループの設定が AP にプッシュされます。スタンバイ コントローラがある場合は、デフォルト FlexConnect グループとその設定も同期化されます。

AP がローカルから FlexConnect モードに変換され、管理者が設定した FlexConnect グループの一部でない場合、AP はデフォルト FlexConnect グループの一部になります。

（注） AP イメージを効率的にアップグレードする機能は、デフォルト FlexConnect AP グループではサポートされません。

関連項目

- デフォルトの FlexConnect AP グループから別の FlexConnect グループへの AP の移動
- デフォルト FlexConnect グループ

デフォルトの FlexConnect AP グループから別の FlexConnect グループへの AP の移動

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect] > [FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。

ステップ 4 [FlexConnect AP グループ（FlexConnect AP Groups）] からグループ名をクリックします。

ステップ 5 [FlexConnect AP] タブで、[AP の追加（+ Add AP）] をクリックします。[FlexConnect AP の追加（Add FlexConnect AP）] ページに、デフォルト FlexConnect グループの AP が表示されます。

ステップ 6 任意の AP 名を選択し、[追加（Add）] をクリックします。

選択した AP は、自動的に新しいグループに追加され、デフォルト FlexConnect グループから削除されます。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

デフォルト FlexConnect グループ （104 ページ）

FlexConnect AP グループの削除

（注） デフォルト FlexConnect グループは削除できません。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect]** > **[FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。

ステップ 4 グループ名をクリックしてから、[コマンドの選択（Select a Command）] ドロップダウン リストから [FlexConnect AP グループの削除（Delete FlexConnect AP Group）] を選択します。

ステップ 5 [OK] をクリックして削除を実行します。

関連トピック

デフォルト FlexConnect グループ （104 ページ）
FlexConnect を使用した AP の設定とモニタ （88 ページ）

コントローラまたはデバイスのセキュリティ設定の構成

- コントローラのアクセス コントロール リスト（ACL）の設定
- コントローラ CPU 用の ACL セキュリティの追加
- コントローラの設定済み IDS セキュリティ センサーの表示
- コントローラでの IP Sec CA 証明書の設定
- コントローラでのネットワーク アイデンティティ（ID）証明書の設定
- コントローラでのワイヤレス保護ポリシーの設定
- コントローラでの不正 AP ポリシーの設定
- コントローラでの不正 AP ポリシーの表示
- コントローラでのクライアント除外ポリシーの設定
- コントローラに適用されるシスコが提供する IDS 署名の表示
- カスタム IDS 署名の作成
- コントローラの AP 認証と管理フレーム保護の設定
- アクセス コントロール リストの設定

コントローラの TFTP ファイル暗号化の設定

TFTP サーバへのコントローラ コンフィギュレーション ファイルのアップロードまたはダウンロードの際に、データが暗号化されるように、ファイル暗号化を設定できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [File Encryption（ファイル暗号化）]** を選択します。

ステップ 4 [ファイル暗号化] チェックボックスをオンにします。

ステップ 5 [暗号化キー（Encryption Key）] フィールドに、正確に 16 文字のテキスト文字列を入力します。[暗号化キーの確認（Confirm Encryption Key）] フィールドにキーをもう一度入力します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

コントローラまたはデバイスのセキュリティ設定の構成 （105 ページ）

コントローラへの AAA セキュリティの設定

ここでは、コントローラのセキュリティ AAA パラメータの設定方法について説明します。内容は次のとおりです。

- コントローラの AAA 一般パラメータの設定
- コントローラの AAA RADIUS 認証サーバの表示
- コントローラの AAA RADIUS アカウンティング サーバの表示

- コントローラでの AAA RADIUS フォールバック パラメータの設定
- コントローラでの AAA LDAP サーバの設定
- コントローラでの AAA TACACS サーバの設定 （113 ページ）
- コントローラの AAA ローカル ネット ユーザの表示
- コントローラでの AAA MAC フィルタリングの設定
- コントローラでの AAA AP/MSE 認証の設定
- コントローラでの AAA Web 認証の設定

コントローラの AAA 一般パラメータの設定

[一般（General）] ページでは、コントローラ上のローカル データベース エントリを設定できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [一般 - AAA（General - AAA）]** を選択します。

ステップ 4 許可されるデータベース エントリの最大数を入力します。有効な範囲は 512 ～ 2048 です。

ステップ 5 [管理ユーザの再認証間隔（Mgmt User Re-auth Interval）] で、管理ユーザを停止する間隔を設定します。

ステップ 6 サーバを再起動して変更を適用します。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラの AAA RADIUS 認証サーバの表示

既存の RADIUS 認証サーバのサマリーを表示できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUS 認証サーバ（RADIUS Auth Servers）]** を選択します。次の RADIUS 認証サーバのパラメータが表示されます。

- [サーバインデックス（Server Index）]：RADIUS サーバのアクセス プライオリティ番号（表示のみ）。[IP アドレスの設定（Configure IPaddr）] > [RADIUS 認証サーバ（RADIUS Authentication Server）] の順にクリックして移動します。
- [サーバ アドレス（Server Address）]：RADIUS サーバの IP アドレス（読み取り専用）。
- [ポート番号（Port Number）]：コントローラのポート番号（読み取り専用）。

- [管理ステータス（Admin Status）]：[有効（Enable）] または [無効（Disable）]。
- [ネットワーク ユーザ（Network User）]：[有効（Enable）] または [無効（Disable）]。
- [管理ユーザ（Management User）]：[有効（Enable）] または [無効（Disable）]。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）
コントローラへの AAA 認証サーバの追加 （108 ページ）

コントローラへの AAA 認証サーバの追加

認証サーバを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）]** > **[AAA]** > **[RADIUS認証サーバ（RADIUS Auth Servers）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [認証サーバの追加（Add Auth Server）] 選択して、[Radius 認証サーバ（Radius Authentication Server）]>[テンプレートから追加（Add From Template）] ページを開きます。

ステップ 5 [このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）] ドロップダウン リストからテンプレートを選択します。

ステップ 6 [適用（Apply）] をクリックします。

Radius 認証サーバの新しいテンプレートを作成するには、**[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features and Technologies）]** を選択します。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）
コントローラの AAA RADIUS アカウンティング サーバの表示 （108 ページ）

コントローラの AAA RADIUS アカウンティング サーバの表示

既存の RADIUS アカウンティング サーバのサマリーを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUSアカウンティングサーバ（RADIUS Acct Servers）]** の順に選択します。RADIUS アカウンティング サーバのパラメータには、次のようなものがあります。

- [サーバ インデックス（Server Index）]：RADIUS サーバのアクセス プライオリティ番号（読み取り専用）。クリックして [RADIUS アカウンティング サーバの詳細（Radius Acct Servers Details）] ページを開きます。
- 現在のアカウンティング サーバのパラメータを編集または監査するには、該当するアカウンティング サーバのサーバ インデックスをクリックします。
- [サーバ アドレス（Server Address）]：RADIUS サーバの IP アドレス（読み取り専用）。
- [ポート番号（Port Number）]：コントローラのポート番号（読み取り専用）。
- [管理ステータス（Admin Status）]：[有効（Enable）] または [無効（Disable）]。
- [ネットワーク ユーザ（Network User）]：[有効（Enable）] または [無効（Disable）]。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）
コントローラへの AAA アカウンティング サーバの追加 （109 ページ）

コントローラへの AAA アカウンティング サーバの追加

アカウンティング サーバを追加するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [AAA] > [RADIUS アカウンティング サーバ（RADIUS Acct Servers）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [アカウンティング サーバの追加（Add Acct Server）] 選択して、[RADIUS アカウンティング サーバの詳細（Radius Acct Servers Details）] > [テンプレートから追加（Add From Template）] ページを開きます。

ステップ 5 [このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）] ドロップダウン リストからテンプレートを選択します。

ステップ 6 ドロップダウン リストから、このテンプレートに適用するコントローラを選択します。

ステップ 7 [適用（Apply）] をクリックします。

RADIUS アカウンティング サーバの新しいテンプレートを作成するには、[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features and Technologies）] > [コントローラ（Controller）] > [セキュリティ（Security）] > [AAA] > [RADIUS Acct サーバ（RADIUS Acct Servers）] を選択します。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）
コントローラの AAA RADIUS アカウンティング サーバの表示 （108 ページ）

コントローラからの AAA アカウンティング サーバの削除

アカウンティング サーバを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUSアカウンティングサーバ（RADIUS Acct Servers）]** の順に選択します。

ステップ 4 該当するアカウンティング サーバのチェックボックスをオンにします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [アカウンティング サーバの削除（Delete Acct Server）] を選択します。

ステップ 6 [実行（Go）] をクリックします。

ステップ 7 ポップアップ ダイアログボックスで [OK] をクリックして、削除を確定します。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）
コントローラの AAA RADIUS アカウンティング サーバの表示 （108 ページ）

コントローラでの AAA RADIUS フォールバック パラメータの設定

RADIUS フォールバック パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUS フォールバック（RADIUS Fallback）]** を選択します。

ステップ 4 必要な変更を行い、[保存（Save）] をクリックします。

ステップ 5 [監査（Audit）] をクリックして、Cisco Prime Infrastructure およびコントローラの現在の設定ステータスを確認します。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラでの AAA LDAP サーバの設定

コントローラに対して LDAP サーバを追加および削除できます。 Prime Infrastructure は、匿名バインドおよび認証済みバインドの両方の LDAP 設定をサポートします。

[LDAP サーバ（LDAP Servers）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [LDAPサーバ（LDAP Servers）]** の順に選択します。

このページには、現在このコントローラが使用している LDAP サーバが表示されます。次のパラメータが含まれます。

- [チェックボックス（Check box）] : チェックボックスをオンにして、削除する LDAP サーバを選択します。
- [サーバ インデックス（Server Index）] : LDAP サーバを識別するために割り当てられた番号。LDAP サーバの設定ページに移動するには、インデックス番号をクリックします。
- [サーバ アドレス（Server Address）] : LDAP サーバの IP アドレス。
- [ポート番号（Port Number）] : LDAP サーバとの通信に使用されるポート番号。
- [管理ステータス（Admin Status）] : サーバ テンプレートのステータス。
- LDAP サーバ テンプレートの使用が有効か無効かを示します。

ステップ 4 情報を昇順または降順に並べ替えるには、列のタイトルをクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）
コントローラでの新しい AAA LDAP バインド要求の設定 （112 ページ）

コントローラへの AAA LDAP サーバの追加

LDAP サーバを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [LDAPサーバ（LDAP Servers）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [LDAP サーバの追加（Add LDAP Server）] を選択します。

ステップ 5 [移動（Go）] をクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラからの AAA LDAP サーバの削除

LDAP サーバを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [LDAPサーバ（LDAP Servers）]** の順に選択します。

ステップ 4 削除する LDAP サーバのチェックボックスをオンにします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [LDAP サーバの削除（Delete LDAP Servers）] を選択します。

ステップ 6 [移動（Go）] をクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラでの新しい AAA LDAP バインド要求の設定

Prime Infrastructure は匿名バインドおよび認証済みバインドの両方の LDAP 設定をサポートします。バインドは、検索処理を実行する空きソケットです。

LDAP バインド要求を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [LDAPサーバ（LDAP Servers）]** の順に選択します。

ステップ 4 [サーバ インデックス（Server Index）] 列の下の値をクリックします。

ステップ 5 [バインド タイプ（Bind Type）] ドロップダウン リストから、[認証済み（Authenticated）] または [匿名（Anonymous）] を選択します。[認証済み（Authenticated）] を選択した場合、バインド ユーザ名およびパスワードも入力する必要があります。

ステップ 6 [サーバ ユーザ ベース DN（Server User Base DN）] テキスト ボックスに、ユーザすべてのリストを含む LDAP サーバ内のサブツリーの識別名を入力します。

ステップ 7 [サーバ ユーザ属性（Server User Attribute）] テキスト ボックスに LDAP サーバのユーザ名を含む属性を入力します。

ステップ 8 [サーバ ユーザ タイプ（Server User Type）] テキスト ボックスにユーザを識別する ObjectType 属性を入力します。

ステップ 9 [再転送タイムアウト（Retransmit Timeout）] テキスト ボックスに再転送までの時間を秒単位で入力します。有効な値の範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

ステップ 10 LDAP サーバに管理権限を付与する場合は、[管理ステータス（Admin Status）] チェックボックスをオンにします。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラでの AAA TACACS サーバの設定

コントローラから TACACS+ サーバを削除できます。[TACACS+ サーバ（TACACS+ Servers）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [TACACS+ サーバ（TACACS+ Servers）]** を選択します。

このページには、現在このコントローラが使用している TACACS+ サーバが表示されます。次のパラメータが含まれます。

- [チェックボックス（Check box）]：チェックボックスをオンにして、削除する TACACS+ サーバを選択します。
- [サーバ タイプ（Server Type）]：TACACS+ のサーバ タイプ（アカウンティング、許可、または認証）。
- [サーバ インデックス（Server Index）]：TACACS+ サーバを識別し、使用プライオリティを設定するために割り当てられた番号。TACACS+ サーバの設定ページに移動するには、インデックス番号をクリックします。
- [サーバ アドレス（Server Address）]：TACACS+ サーバの IP アドレス。
- [ポート番号（Port Number）]：TACACS+ サーバとの通信に使用されるポート番号。
- [管理ステータス（Admin Status）]：サーバ テンプレートのステータス。TACACS+ サーバ テンプレートの使用が有効かを示します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [TACACS+ サーバの削除（Delete TACACS+ Servers）] を選択し、[実行（Go）] をクリックして、選択したチェックボックスのすべての TACACS+ サーバをコントローラから削除します。

ステップ 5 情報を昇順または降順に並べ替えるには、列のタイトルをクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラの AAA ローカル ネット ユーザの表示

特定の WLAN へのアクセスが許可されているクライアントの、既存のローカル ネットワーク ユーザ コントローラのサマリーを表示できます。これは、RADIUS 認証プロセスの管理バイパスです。レイヤ 3 Web 認証を有効にする必要があります。クライアント情報は、まず RADIUS 認証サーバに渡され、クライアント情報が RADIUS データベースのエントリと一致しない場合は、このローカルデータベースに対してポーリングが実行されます。RADIUS 認証が失敗した場合、または存在しない場合は、このデータベースで見つかったクライアントがネットワーク サービスへのアクセスを付与されます。

既存のローカル ネットワーク ユーザを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [ローカル ネット ユーザ（Local Net Users）]** を選択します。[ローカル ネット ユーザ（Local Net Users）] ページには、次のローカル ネット ユーザ パラメータが表示されます。

- [ユーザ名（Username）]：ユーザ定義の ID。
- [WLAN ID]：任意の WLAN ID（1 ～ 16）。すべての WLAN の場合は 0、このローカル ネット ユーザがアクセスできるサードパーティ製 WLAN の場合は 17。
- [説明（Description）]：オプションのユーザが定義した説明。

関連トピック

コントローラでのローカル EAP の設定 （119 ページ）
コントローラからの AAA ローカル ネット ユーザの削除 （114 ページ）

コントローラからの AAA ローカル ネット ユーザの削除

ローカル ネット ユーザを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [ローカル ネット ユーザ（Local Net Users）]** を選択します。

ステップ 4 該当するローカル ネット ユーザのチェックボックスをオンにします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから、[ローカル ネット ユーザの削除（Delete Local Net Users）] を選択します。

ステップ 6 [実行（Go）] をクリックします。

ステップ 7 ダイアログボックスで [OK] をクリックして、削除を確定します。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラでの AAA MAC フィルタリングの設定

MAC フィルタ情報を表示できます。ブロードキャスト範囲では MAC アドレスを使用できません。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [MAC フィルタリング（MAC Filtering）]** を選択します。[MAC フィルタリング（MAC Filtering）] ページには、次のパラメータが表示されます。

- [MAC フィルタ パラメータ（MAC Filter Parameters）]
  - [RADIUS 互換性モード（RADIUS Compatibility Mode）]：ユーザ定義の RADIUS サーバの互換性（[Cisco ACS]、[FreeRADIUS]、または [その他（Other）]）。
  - [MAC デリミタ（MAC Delimiter）]：MAC デリミタは、RADIUS サーバの要件に応じて、コロン（xx:xx:xx:xx:xx:xx）、ハイフン（xx-xx-xx-xx-xx-xx）、シングル ハイフン（xxxxxx-xxxxxx）、またはデリミタなし（xxxxxxxxxxxx）に設定できます。
- [MAC フィルタ（MAC Filters）]
  - [MAC アドレス（MAC Address）]：クライアント MAC アドレス。クリックして [IP アドレスの設定（Configure IPaddr）] > [MAC フィルタ（MAC Filter）] を開きます。
  - [WLAN ID]：1 ～ 16（17 = サードパーティ製 AP WLAN、0 = すべての WLAN）。
  - [インターフェイス（Interface）]：関連付けられるインターフェイス名を表示します。
  - [説明（Description）]：オプションのユーザ定義の説明を表示します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [MAC フィルタの追加（Add MAC Filters）] を選択して MAC フィルタを追加するか、[MAC フィルタの削除（Delete MAC Filters）] を選択してテンプレートを削除するか、[MAC フィルタ パラメータの編集（Edit MAC Filter Parameters）] を選択して MAC フィルタを編集します。

ステップ 5 [移動（Go）] をクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラでの AAA AP/MSE 認証の設定

[AP/MSE 認可（AP/MSE Authorization）] ページには、アクセス ポイント ポリシーおよび認可されたアクセス ポイントのリストが表示されます。このリストには、アクセス ポイントで認可に使用する証明書のタイプも示されます。

ブロードキャスト範囲では MAC アドレスを使用できません。

[AP/MSE 認可（AP/MSE Authorization）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [AP または MSE 認証（AP or MSE Authorization）]** を選択します。[AP/MSE 認可（AP/MSE Authorization）] ページに次のパラメータが表示されます。

- [AP ポリシー（AP Policies）]
  - [AP の認可（Authorize APs）]：有効または無効。
  - [SSC-AP の受け入れ（Accept SSC-APs）]：有効または無効。
- [AP/MSE 認可（AP/MSE Authorization）]
  - [AP/MSE ベース無線の MAC アドレス（AP/MSE Base Radio MAC Address）]：認可されたアクセス ポイントの MAC アドレス。[AP/MSE ベース無線の MAC アドレス（AP/MSE Base Radio MAC Address）] をクリックすると、AP/MSE 認可の詳細が表示されます。
  - タイプ（Type）
  - [証明書タイプ（Certificate Type）]：MIC または SSC。
  - [キー ハッシュ（Key Hash）]：40 文字の長さの 16 進数 SHA1 キー ハッシュ。キー ハッシュは、証明書のタイプが SSC の場合のみ表示されます。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）
コントローラでの AAA AP/MSE ポリシーの編集 （116 ページ）

コントローラでの AAA AP/MSE ポリシーの編集

AP/MSE 認可アクセス ポイント ポリシーを編集するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [AP または MSE 認証（AP or MSE Authorization）]** を選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [AP ポリシーの編集（Edit AP Policies）] を選択し、[実行（Go）] をクリックします。

ステップ 5 必要に応じて、次のパラメータを編集します。

- [AP の認可（Authorize APs）]：アクセス ポイント認可を有効にする場合は、このチェックボックスをオンにします。
- [SSC-AP の受け入れ（Accept SSC-APs）]：SSE アクセス ポイントの承認を有効にする場合は、このチェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックして変更を確定するか、[監査（Audit）] をクリックしてこれらのデバイス値の監査を実行するか、[キャンセル（Cancel）] をクリックしてこのページを変更せずに閉じます。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラでの AAA Web 認証の設定

[Web 認証設定（Web Auth Configuration）] ページでは、Web 認証の設定タイプを設定できます。このタイプをカスタマイズに設定した場合は、コントローラにより提供された内部 Web 認証ページが、ユーザのダウンロードした Web 認証に置き換わります。

[Web 認証設定（Web Auth Configuration）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [Web 認証設定（Web Auth Configuration）]** を選択します。

ステップ 4 ドロップダウンリストから Web 認証タイプを選択します。

ステップ 5 選択したタイプに応じて、Web 認証パラメータを設定します。

- [デフォルト内部（Default Internal）]

- [カスタム リダイレクト URL（Custom Redirect URL）]：認証が成功した後にユーザがリダイレクトされる URL。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。
- [ロゴの表示（Logo Display）]：ロゴの表示を有効または無効にします。
- [Web 認証ページ タイトル（Web Auth Page Title）]：Web 認証ページに表示されるタイトル。
- [Web 認証ページのメッセージ（Web Auth Page Message）]：認証ページに表示されるメッセージ。

- [カスタマイズ Web 認証（Customized Web Auth）]

  サンプルのログイン ページをダウンロードして、そのページをカスタマイズできます。カスタマイズ Web 認証ページを使用する場合は、サーバからサンプルの login.tar バンドル ファイルをダウンロードし、login.html ファイルを編集して .tar または .zip ファイルとして保存してから、.tar または .zip ファイルをコントローラにダウンロードする必要があります。

  プレビュー イメージをクリックして、このサンプル ログイン ページを TAR としてダウンロードします。HTML の編集後にここをクリックすると [Web 認証のダウンロード（Download Web Auth）] ページにリダイレクトされます。詳細については、「コントローラへの圧縮された Web 認証ログイン ページ情報のダウンロード」を参照してください。

- [外部（External）]
  - [拡張リダイレクト URL（External Redirect URL）]：ネットワーク上の外部サーバにある login.html の場所。

    外部 Web 認証サーバが設定されていない場合は、外部 Web 認証サーバを設定するオプションがあります。

コントローラでの AAA パスワード ポリシーの設定

このページでは、パスワード ポリシーを決定できます。

既存のパスワード ポリシーを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [パスワード ポリシー（Password Policy）]** を選択します。

ステップ 4 パスワード ポリシーのパラメータを必要に応じて変更します。

ステップ 5 [保存（Save）] をクリックします。

パスワードポリシーオプションを無効にすると、「強いパスワード検査を無効にすると弱いパスワードが許可されるため、セキュリティ上のリスクが発生します（Disabling the strong password check(s) will be a security risk as it allows weak passwords）」というメッセージが表示されます。

関連トピック

コントローラへの AAA セキュリティの設定 （106 ページ）

コントローラでのローカル EAP の設定

ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンドシステムが妨害されたり、外部認証サーバがダウンしたりした場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。

ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバから独立します。ローカル EAP は、ローカル ユーザ 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の資格情報を取得して、ユーザを認証します。

関連トピック

コントローラでのローカル EAP 一般パラメータの設定 （119 ページ）
コントローラで使用されるローカル EAP プロファイルの表示 （120 ページ）
コントローラでのローカル EAP 一般 EAP-Fast パラメータの設定
コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定 （122 ページ）

コントローラでのローカル EAP 一般パラメータの設定

ローカル EAP のタイムアウト値を指定できます。その後、このタイムアウト値を持つテンプレートを追加したり、既存のテンプレートを変更したりできます。

コントローラ上でRADIUSサーバが設定されている場合は、コントローラはまずRADIUSサーバ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サーバがタイムアウトしていたり、RADIUS サーバが設定されていなかったりした場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初のRADIUSサーバを使用してクライアントの認証を試行し、次に 2 番目の RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントで手動で再認証を試みると、コントローラは 3 番目の RADIUS サーバを試行し、次に 4 番目の RADIUS サーバ、その次にローカル EAP を試行します。

ローカル EAP のタイムアウト値を指定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）]** > **[ローカル EAP（Local EAP）]** > **[一般 - ローカル EAP(General - Local EAP)]** を選択します。

ステップ 4 [ローカル認証アクティブ タイムアウト（Local Auth Active Timeout）] テキスト ボックスにローカル認証アクティブ タイムアウトを入力します（秒単位）。ローカル認証アクティブ タイムアウトは、すべての RADIUS サーバが失敗した後、ローカル EAP が必ず使用されるタイムアウト時間を指します。

ステップ 5 EAP-FAST、手動パスワード入力、ワンタイム パスワード、または 7920/7921 電話を使用する際は、次の値を調整する必要があります。

自動プロビジョニングを使用している PAC をクライアントで取得する場合、コントローラで 802.1x のタイムアウト値を大きくする必要があります（デフォルトは 2 秒）。Cisco ACS サーバでは、デフォルトの 20 秒を推奨します。

- [ローカル EAP 識別要求タイムアウト（Local EAP Identify Request Timeout）] = 1（秒単位）
- [ローカル EAP ID 要求最大試行（Local EAP Identity Request Maximum Retries）] = 20（秒単位）
- [ローカル EAP 動的 Wep キー インデックス（Local EAP Dynamic Wep Key Index）] = 0
- [ローカル EAP 要求タイムアウト（Local EAP Request Timeout）] = 20（秒単位）
- [ローカル EAP 要求最大試行回数（Local EAP Request Maximum Retries）] = 2
- [EAPOL キー タイムアウト（EAPOL-Key Timeout）] = 1000（ミリ秒単位）
- [EAPOL キー最大試行回数（EAPOL-Key Max Retries）] = 2
- [最大ログイン無視 ID 応答（Max-Login Ignore Identity Response）]

複数のコントローラでこれらの値が同じ設定でないと、ローミングが失敗します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

コントローラでのローカル EAP の設定 （119 ページ）
コントローラで使用されるローカル EAP プロファイルの表示 （120 ページ）
コントローラでのローカル EAP 一般 EAP-Fast パラメータの設定
コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定 （122 ページ）

コントローラで使用されるローカル EAP プロファイルの表示

ローカル EAP プロファイルのテンプレートを適用したり、既存のテンプレートを変更したりすることができます。

LDAP バックエンド データベースは、証明書による EAP-TLS および EAP-FAST のローカル EAP メソッドだけをサポートします。LDAP バックエンド データベースでは、LEAP および PAC による EAP-FAST はサポートされません。

既存のローカル EAP プロファイルを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ローカル EAP（Local EAP）] > [ローカル EAP プロファイル（Local EAP Profiles）]** を選択します。[ローカル EAP プロファイル（Local EAP Profiles）] ページには、次のパラメータが表示されます。

- [EAP プロファイル名（EAP Profile Name）]：ユーザ定義の ID。
- [LEAP]：Cisco Key Integrity Protocol（CKIP）と MMH Message Integrity Check（MIC）を使用してデータを保護する認証タイプ。ユーザ名とパスワードを使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。
- [EAP-FAST]：3 段階のトンネル認証プロセスを使用して高度な 802.1x EAP 相互認証を実行する認証タイプ（Flexible Authentication via Secure Tunneling）。ユーザ名、パスワード、および PAC（保護されたアクセス クレデンシャル）を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。
- [TLS]：クライアント アダプタと RADIUS サーバから生成した動的なセッション ベースの WEP キーを使用してデータを暗号化する認証タイプ。認証のためにクライアント証明書を必要とします。
- [PEAP]：保護拡張認証プロトコル。

関連トピック

コントローラでのローカル EAP の設定 （119 ページ）
コントローラへのローカル EAP プロファイルの追加 （121 ページ）

コントローラへのローカル EAP プロファイルの追加

ローカル EAP プロファイルを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ローカルEAP（Local EAP）] > [ローカルEAPプロファイル（Local EAP Profile）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [ローカル EAP プロファイルの追加（Add Local EAP Profile）] を選択します。

ステップ 5 [このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）] ドロップダウン リストからテンプレートを選択します。

ステップ 6 [適用（Apply）] をクリックします。

関連トピック

コントローラでのローカル EAP の設定 （119 ページ）
コントローラでのローカル EAP 一般パラメータの設定 （119 ページ）
コントローラで使用されるローカル EAP プロファイルの表示 （120 ページ）
コントローラでのローカル EAP 一般 EAP-Fast パラメータの設定

コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定 （122 ページ）

コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定

LDAP とローカル データベースがユーザ クレデンシャル情報を取得するために使用する順序を指定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[セキュリティ（Security）] > [ローカル EAP（Local EAP）] > [ネットワーク ユーザの優先度（Network Users Priority）]** を選択します。

ステップ 4 左右の矢印を使用して、右端のリストにネットワーク クレデンシャルを含めたり、除外したりすることができます。

ステップ 5 上下のボタンを使用してクレデンシャルを試行する順序を決定します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

コントローラでのローカル EAP の設定 （119 ページ）
コントローラでのローカル EAP 一般パラメータの設定 （119 ページ）
コントローラの Web 認証証明書の設定 （122 ページ）
コントローラでの IP Sec CA 証明書の設定 （127 ページ）

コントローラの Web 認証証明書の設定

Web 認証証明書をダウンロードしたり、内部生成 Web 認証証明書を再生成したりすることができます。

注意 各証明書には、可変長 RSA キーが組み込まれています。RSA キーは、比較的に安全性が低い 512 ビットから、安全性がかなり高い数千ビットまでさまざまです。認証局（Microsoft CA など）から新しい証明書を取得する場合は、証明書に組み込まれている RSA キーが 768 ビット以上であることを確認してください。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [Web 認証証明書（Web Auth Certificate）] の順に選択します。

ステップ 4 [Web 認証証明書のダウンロード（Download Web Auth Certificate）] をクリックして [Web 認証証明書のコントローラへのダウンロード（Download Web Auth Certificate to Controller）] ページにアクセスします。

関連トピック

コントローラでのローカル EAP 一般パラメータの設定 （119 ページ）
コントローラでのローカル EAP の設定 （119 ページ）

コントローラのユーザ ログイン ポリシーの設定

コントローラにユーザ ログイン ポリシーを設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [ユーザ ログイン ポリシー（User Login Policies）] を選択します。

ステップ 4 1 つのユーザ名で同時にログインできる最大数を入力します。

ステップ 5 [保存（Save）] をクリックします。

デバイスの手動で無効化されるクライアントの設定

[Disabled Clients] ページでは、除外された（ブラックリストに掲載された）クライアントの情報を表示できます。

関連付けを試行した際に、3 回認証に失敗したクライアントはオペレータが定義したタイムアウトの間、再度関連付けを試行できないように、自動的にブロック（または除外）されます。除外タイムアウトが経過すると、クライアントは認証の再試行を許可され、関連付けることができます。このとき、認証に失敗すると再び除外されます。

ブロードキャスト範囲では MAC アドレスを使用できません。

[手動で無効にされたクライアント（Manually Disabled Clients）] ページにアクセスするには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）]>[手動で無効にされたクライアント（Manually Disabled Clients）] の順に選択します。[手動で無効にされたクライアント（Manually Disabled Clients）] ページには、次のパラメータが表示されます。

- [MAC アドレス（MAC Address）]：無効にされたクライアントの MAC アドレス。リスト項目をクリックして、無効にされたクライアントの説明を編集します。
- [説明（Description）]：無効にされたクライアントのオプションの説明。

コントローラのアクセス コントロール リスト（ACL）の設定

コントローラの新しいアクセス コントロール リスト（ACL）を表示、編集、または追加できます。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [アクセス コントロール リスト（Access Control Lists）] を選択します。

a) チェックボックスをオンにして、1 つ以上の ACL を削除します。

または

b) ACL 項目をクリックすると、そのパラメータを表示できます。

コントローラ ACL ルールの設定 （124 ページ）
コントローラ CPU 用の ACL セキュリティの追加 （126 ページ）

コントローラ ACL ルールの設定

コントローラに適用するアクセス コントロール リスト（ACL）のルールを作成および変更できます。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [アクセス コントロール リスト（Access Control Lists）] の順に選択します。

ステップ 4 ACL 名をクリックし、パラメータを表示して変更します。

ステップ 5 必要に応じて、アクセス コントロール リスト ルールのチェックボックスをオンします。

新しいコントローラの ACL ルールの作成

ステップ 1 **[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）]** > **[アクセス コントロール リスト（Access Control Lists）]** を選択します。

ステップ 4 ACL 名をクリックします。

ステップ 5 該当する [連番（Seq#）] をクリックするか、[新規ルールの追加（Add New Rule）] を選択してこのページにアクセスします。

コントローラ ACL ルールの設定 （124 ページ）
コントローラ CPU 用の ACL セキュリティの追加 （126 ページ）

コントローラの FlexConnect ACL セキュリティの設定

FlexConnect 上の ACL は、ローカルでスイッチされた、アクセス ポイントからのデータ トラフィックの保護および完全性のために、FlexConnect アクセス ポイントで必要とされるアクセス コントロールを提供するメカニズムを提供します。

コントローラでの FlexConnect ACL の追加 （125 ページ）
コントローラの FlexConnect ACL の削除 （126 ページ）

コントローラでの FlexConnect ACL の追加

FlexConnect アクセス ポイントのアクセス コントロール リストを追加するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [FlexConnect ACL（FlexConnect ACLs）] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、[FlexConnect ACL の追加（Add FlexConnect ACLs）] を選択します。

ステップ 5 [実行（Go）] をクリックします。

テンプレートが作成されていない場合は、FlexConnect ACL は追加できません。使用できるテンプレートが存在しない状態で FlexConnect ACL の作成を試行した場合は、[新規コントローラ テンプレート（New Controller Templates）] ページにリダイレクトされます。ここで、FlexConnect ACL 用のテンプレートを作成できます。

ステップ 6 ドロップダウン リストからコントローラに適用するテンプレートを選択して、[適用（Apply）] をクリックします。

作成した FlexConnect ACL が、[設定（Configure）] > [コントローラ（Controllers）] > [IP アドレス（IP Address）] > [セキュリティ（Security）] > [FlexConnect ACLs] に表示されます。

コントローラの FlexConnect ACL セキュリティの設定 （125 ページ）

コントローラの FlexConnect ACL の削除

FlexConnect ACL を削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [FlexConnect ACL（FlexConnect ACLs）]** を選択します。

ステップ 4 [FlexConnect ACLs] ページから、削除する FlexConnect ACL を 1 つ以上選択します。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [FlexConnect ACL の削除（Delete FlexConnect ACLs）] を選択します。

ステップ 6 [実行（Go）] をクリックします。

コントローラの FlexConnect ACL セキュリティの設定 （125 ページ）

コントローラ CPU 用の ACL セキュリティの追加

アクセス コントロール リスト（ACL）は、コントローラの CPU に適用して、その CPU へのトラフィックを制御できます。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [CPU アクセス コントロール リスト（CPU Access Control Lists）] の順に選択します。

ステップ 4 [CPU ACL の有効化（Enable CPU ACL）] チェックボックスをオンにして、CPU ACL を有効にします。次のパラメータを使用できます。

- [ACL 名（ACL Name）]：[ACL 名（ACL Name）] ドロップダウン リストから使用する ACL を選択します。
- [CPU ACL モード（CPU ACL Mode）]：この CPU ACL リストで制御するデータ トラフィックの方向を選択します。

コントローラの FlexConnect ACL セキュリティの設定 （125 ページ）
コントローラのアクセス コントロール リスト（ACL）の設定 （124 ページ）
コントローラ ACL ルールの設定 （124 ページ）

コントローラの設定済み IDS セキュリティ センサーの表示

センサーが攻撃を識別した場合は、攻撃しているクライアントを回避するようにコントローラに警告します。新しい IDS（侵入検知システム）センサーを追加した場合は、回避したクライアントのレポートをセンサーがコントローラに送信できるように、コントローラをその IDS センサーに登録します。また、コントローラは定期的にセンサーをポーリングします。

IDS センサーを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[セキュリティ（Security）] > [IDS センサー リスト（IDS Sensor Lists）]** を選択します。

[IDS センサー（IDS Sensor）] ページには、このコントローラに設定されているすべての IDS センサーのリストが表示されます。IP アドレスをクリックして、特定の IDS センサーの詳細を表示します。

コントローラでの IP Sec CA 証明書の設定

認証局（CA）の証明書は、ある認証局（CA）が別の認定 CA に対して発行したデジタル証明書です。

コントローラへの IP Sec 証明書のインポート （127 ページ）
コントローラへの IP Sec 証明書の貼り付け （128 ページ）

コントローラへの IP Sec 証明書のインポート

ファイルから CA 証明書をインポートするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec 証明書（IP Sec Certificates）] > [CA 証明書（CA Certificate）]** を選択します。

ステップ 4 [参照（Browse）] をクリックして該当する証明書ファイルにナビゲートします。

ステップ 5 [開く（Open）] をクリックしてから [保存（Save）] をクリックします。

コントローラでの IP Sec CA 証明書の設定 （127 ページ）

コントローラへの IP Sec 証明書の貼り付け

CA 証明書を直接貼り付けるには、次の手順を実行します。

ステップ 1 コンピュータのクリップボードに CA 証明書をコピーします。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 該当するコントローラのデバイス名をクリックします。

ステップ 4 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec 証明書（IP Sec Certificates）] > [CA 証明書（CA Certificate）]** を選択します。

ステップ 5 [貼り付け（Paste）] チェックボックスをオンにします。

ステップ 6 証明書をテキスト ボックスに直接貼り付けます。

ステップ 7 [保存（Save）] をクリックします。

コントローラでの IP Sec CA 証明書の設定 （127 ページ）
コントローラでのネットワーク アイデンティティ（ID）証明書の設定 （128 ページ）
コントローラの Web 認証証明書の設定 （122 ページ）

コントローラでのネットワーク アイデンティティ（ID）証明書の設定

このページには、既存のネットワーク アイデンティティ（ID）証明書が証明書名別に一覧表示されます。ID 証明書は、Web サーバのオペレータが、安全なサーバの動作を確保するために使用します。ID 証明書は、コントローラが Cisco Unified Wireless Network のソフトウェア バージョン 3.2 以降を実行している場合のみ、使用できます。

コントローラへの IP Sec 証明書のインポート （127 ページ）
コントローラへの IP Sec 証明書の貼り付け （128 ページ）

コントローラへの ID 証明書のインポート

ファイルから ID 証明書をインポートするには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec証明書（IP Sec Certificates）] > [ID証明書（ID Certificate）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [証明書の追加（Add Certificate）] を選択します。

ステップ 5 [実行（Go）] をクリックします。

ステップ 6 名前とパスワードを入力します。

ステップ 7 [参照（Browse）] をクリックして該当する証明書ファイルにナビゲートします。

ステップ 8 [開く（Open）] をクリックしてから [保存（Save）] をクリックします。

コントローラでのネットワーク アイデンティティ（ID）証明書の設定 （128 ページ）

コントローラへの ID 証明書の貼り付け

ID 証明書を直接貼り付けるには、次の手順を実行します。

ステップ 1 コンピュータのクリップボードに ID 証明書をコピーします。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 該当するコントローラのデバイス名をクリックします。

ステップ 4 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec証明書（IP Sec Certificates）] > [ID証明書（ID Certificate）]** の順に選択します。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [証明書の追加（Add Certificate）] を選択します。

ステップ 6 [実行（Go）] をクリックします。

ステップ 7 名前とパスワードを入力します。

ステップ 8 [貼り付け（Paste）] チェックボックスをオンにします。

ステップ 9 証明書をテキスト ボックスに直接貼り付けます。

ステップ 10 [保存（Save）] をクリックします。

コントローラでの IP Sec CA 証明書の設定 （127 ページ）
コントローラでのネットワーク アイデンティティ（ID）証明書の設定 （128 ページ）

コントローラでのワイヤレス保護ポリシーの設定

ここでは、ワイヤレス保護ポリシーの設定について説明します。内容は次のとおりです。

コントローラでの不正 AP ポリシーの設定

不正アクセス ポイントのポリシーを設定できます。必要なアクセス ポイントで不正検出が有効になっていることを確認します。コントローラに接続されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効化されます（OfficeExtend アクセス ポイントを除く）。ただし、Cisco Prime Infrastructure ソフトウェア リリース 6.0 以降では、[アクセス ポイントの詳細（Access Point Details）] ページで [不正検出（Rogue Detection）] チェックボックスをオンまたはオフにすることにより、アクセス ポイントごとに不正検出を有効または無効にできます。

家庭の環境で展開されるアクセス ポイントは大量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はデフォルトでは無効です。

[不正ポリシー（Rogue Policies）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）][コントローラ（Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [不正ポリシー（Rogue Policies）]** を選択します。次のパラメータが表示されます。

- [不正ロケーション検出プロトコル（Rogue Location Discovery Protocol）]：RLDP は、企業の有線ネットワークへの不正な接続の有無を判断します。ドロップダウン リストから、次のいずれかを選択します。
  - [無効（Disable）]：すべてのアクセス ポイント上で RLDP を無効にします。これがデフォルト値です。
  - [すべての AP（All APs）]：すべてのアクセス ポイント上で RLDP を有効にします。
  - [モニタ モード AP（Monitor Mode APs）]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。
- [不正 AP（Rogue APs）]
  - [不正 AP および不正クライアント エントリの有効期限タイムアウト（秒単位）（Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)）]：不正なアクセス ポイントおよびクライアントの

エントリがリストから削除されるまでの秒数を入力します。有効な値の範囲は 240 ～ 3600 秒で、デフォルト値は 1200 秒です。

不正なアクセス ポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても [警告（Alert）] または [脅威（Threat）] である場合には、コントローラから削除されます。

- [不正検出レポート間隔（Rogue Detection Report Interval）]：AP からコントローラに不正検出レポートを送信する間隔を秒数で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。この機能は、モニタ モードの AP のみに適用されます。
- [不正検出最小 RSSI（Rogue Detection Minimum RSSI）]：AP で不正が検出され、コントローラで不正エントリが作成されるために必要な最小 RSSI 値を入力します。有効な範囲は -70 ～ -128 dBm で、デフォルト値は -128 dBm です。この機能は、すべての AP モードに適用できます。

  RSSI 値が非常に低く、不正解析にとって有益な情報とならない不正が多く存在する可能性があります。そのため、このオプションを使用して AP が不正を検出する最小 RSSI 値を指定することで、不正をフィルタできます。
- [不正検出の一時的な間隔（Rogue Detection Transient Interval）]：最初に不正がスキャンされた後、AP が継続的に不正をスキャンする必要のある間隔を入力します。一時的な間隔を入力することで、AP が不正をスキャンする間隔を制御できます。AP は、一時的な間隔の値に基づいて、不正をフィルタできます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。この機能は、モニタ モードの AP のみに適用されます。

- [不正クライアント（Rogue Clients）]
  - [AAA に対する不正クライアントの検証（Validate rogue clients against AAA）]：AAA サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントかどうかを検証するには、このチェックボックスをオンにします。デフォルト値はオフです。
  - [アドホック ネットワークの検出とレポート（Detect and report Adhoc networks）]：アドホック不正検出およびレポートを有効にするには、このチェックボックスをオンにします。デフォルト値はオンです。

コントローラでの不正 AP ポリシーの表示 （131 ページ）
コントローラでのクライアント除外ポリシーの設定 （132 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （133 ページ）
カスタム IDS 署名の作成 （138 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （139 ページ）
コントローラでのワイヤレス保護ポリシーの設定 （130 ページ）

コントローラでの不正 AP ポリシーの表示

このページでは、現在の不正 AP ルールを表示および編集できます。

[不正 AP ルール（Rogue AP Rules）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [不正 AP ルール（Rogue AP Rules）]** を選択します。[不正 AP ルール（Rogue AP Rules）] に、不正 AP ルール、ルール タイプ（[悪意のある（Malicious）] または [危険性のない（Friendly）]）、およびルールの順序が表示されます。

ステップ 4 ルールの詳細を表示または編集するには、[不正 AP ルール（Rogue AP Rule）] をクリックします。

コントローラでのクライアント除外ポリシーの設定 （132 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （133 ページ）
カスタム IDS 署名の作成 （138 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （139 ページ）
コントローラでのワイヤレス保護ポリシーの設定 （130 ページ）

コントローラでのクライアント除外ポリシーの設定

このページでは、コントローラに適用されているクライアント除外ポリシーを設定、有効化、または無効化できます。

[クライアント除外ポリシー（Client Exclusion Policies）] ページにアクセスするには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [クライアント除外ポリシー（Client Exclusion Policies）] の順に選択します。次のパラメータが表示されます。

- [802.11a 関連付けの過剰な失敗（Excessive 802.11a Association Failures）]：有効にした場合、クライアントは 802.11 関連付けの試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [802.11a 認証の過剰な失敗（Excessive 802.11a Authentication Failures）]：有効にした場合、クライアントは 802.11 認証の試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [802.11x 認証の過剰な失敗（Excessive 802.11x Authentication Failures）]：有効にした場合、クライアントは 802.1X 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [802.11 Web 認証の過剰な失敗（Excessive 802.11 Web Authentication Failures）]：有効にした場合、クライアントは Web 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。

- [IP の盗難または再使用（IP Theft Or Reuse）]：有効にした場合、IP アドレスがすでに別のデバイスに割り当てられていると、クライアントが除外されます。

ステップ 4 [保存（Save）] をクリックし、クライアント除外ポリシーに対する変更を保存して前のページに戻るか、[監査（Audit）] をクリックしてコントローラで使用された値と Prime Infrastructure の値を比較します。

コントローラでの不正 AP ポリシーの表示 （131 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （133 ページ）
カスタム IDS 署名の作成 （138 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （139 ページ）
コントローラでのワイヤレス保護ポリシーの設定 （130 ページ）

デバイスの IDS 署名の設定

コントローラ上で、IDS シグネチャ、つまり、受信 802.11 パケットにおけるさまざまなタイプの攻撃を特定するのに使用されるビット パターンのマッチング ルールを設定することができます。シグネチャが有効にされると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグネチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が取られます。

シスコではコントローラの 17 の標準シグネチャをサポートしています。

コントローラに適用されるシスコが提供する IDS 署名の表示 （133 ページ）
カスタム IDS 署名の作成 （138 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （139 ページ）

コントローラに適用されるシスコが提供する IDS 署名の表示

[標準シグネチャ パラメータ（Standard Signature Parameters）] ページには、現在コントローラ上にあるシスコ提供のシグネチャの一覧が表示されます。

[標準シグネチャ（Standard Signatures）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [標準シグネチャ（Standard Signatures）]** を選択します。このページには、次のパラメータが表示されます。

- [優先度（Precedence）]：コントローラがシグネチャ チェックを実行する順序。
- [名前（Name）]：シグネチャによって検出を試みる攻撃の種類。

- [フレームの種類（Frame Type）]：シグネチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータ フレームの種類。
- [アクション（Action）]：シグネチャによって攻撃が検出された際に実行する、コントローラへの指示。次に例を示します。
  - [なし（None）]：アクションが実行されません。
  - [報告（Report）]：検出を報告します。
- [状態（State）]：有効または無効。
- [説明（Description）]：シグネチャによって検出を試みる攻撃の種類の詳細説明。

ステップ 4 シグネチャの名前をクリックして個々のパラメータを表示し、シグネチャを有効または無効にします。

関連トピック

デバイスの IDS 署名の設定 （133 ページ）
コントローラからの IDS 署名ファイルのアップロード （135 ページ）
コントローラ上のすべての IDS 署名の有効化と無効化 （136 ページ）

コントローラへの IDS 署名ファイルのダウンロード

シグネチャ ファイルをダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）][コントローラ（Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [標準シグネチャ（Standard Signatures）]** または **[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [カスタムシグネチャ（Custom Signatures）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、[シグネチャ ファイルのダウンロード（Download Signature Files）] を選択します。

ステップ 5 [実行（Go）] をクリックします。

ステップ 6 シグネチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 7 [ファイルの格納場所（File is located on）] から [ローカル マシン（Local machine）] を選択します。ファイル名および、サーバのルートディレクトリに対して相対的なパスがわかる場合は、[TFTP サーバ（TFTP server）] を選択することもできます。

ステップ 8 [最大回数（Maximum Retries）] に、コントローラがシグネチャ ファイルのダウンロードを試みる最大回数を入力します。

ステップ 9 [タイムアウト（Timeout）] に、シグネチャ ファイルのダウンロードを試行する際、コントローラがタイムアウトになるまでの最大時間を秒単位で入力します。

ステップ 10 ファイルは c:\tftp ディレクトリにアップロードされます。そのディレクトリ内のローカル ファイル名を指定するか、[参照（Browse）] をクリックしてナビゲートします。シグネチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグネチャ ファイルか、またはサイトに合わせたカスタム シグネチャ ファイルかを指定します（カスタム シグネチャ ファイルには revision=custom が必須）。

何らかの理由で転送がタイムアウトになった場合、[ファイルの格納場所（File is located on）] フィールドで [TFTP サーバ（TFTP server）] オプションを選択すると、サーバ ファイル名が自動的に入力され、再試行されます。ローカルマシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure 独自の組み込みの TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、ダウンロードした Web ページで自動的にそのファイル名が読み込まれます。

ステップ 11 [OK] をクリックします。

関連トピック

デバイスの IDS 署名の設定 （133 ページ）

コントローラからの IDS 署名ファイルのアップロード

コントローラからシグネチャ ファイルをアップロードできます。シグネチャのダウンロードに Trivial File Transfer Protocol（TFTP）サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティングできないため、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 1 シスコからシグネチャ ファイルを入手します（標準シグネチャ ファイル）。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 該当するコントローラのデバイス名をクリックします。

ステップ 4 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [標準シグネチャ（Standard Signatures）]** または **[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [カスタムシグネチャ（Custom Signatures）]** の順に選択します。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから、[コントローラからのシグネチャ ファイルのアップロード（Upload Signature Files from controller）] を選択します。

ステップ 6 転送に使用している TFTP サーバ名を指定します。

ステップ 7 TFTP サーバが新しい場合は、[サーバ IP アドレス（Server IP Address）] フィールドで TFTP IP アドレスを入力します。

ステップ 8 [ファイル タイプ（File Type）] ドロップダウン リストから [シグネチャ ファイル（Signature Files）] を選択します。

このシグネチャ ファイルは、TFTP サーバによる使用に対して設定されたルート ディレクトリにアップロードされます。[ファイルのアップロード先（Upload to File）] フィールドで別のディレクトリに変更できます（このフィールドは、[サーバ名（Server Name）] がデフォルト サーバの場合のみ表示）。コントローラはベース ネームとしてこのローカル ファイル名を使用し、標準シグネチャ ファイルのサフィクスとして _std.sig を、カスタム シグネチャ ファイルのサフィクスとして _custom.sig を追加します。

ステップ 9 [OK] をクリックします。

デバイスの IDS 署名の設定 （133 ページ）
コントローラへの IDS シグネチャのダウンロード （11 ページ）

コントローラ上のすべての IDS 署名の有効化と無効化

このコマンドは、個々に選択して有効にしたシグニチャすべてを有効にします。このチェックボックスをオフのままにすると、以前に有効にしていても、すべてのファイルは無効になります。シグネチャが有効にされると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグネチャ分析が行われ、整合性がない場合はコントローラに報告されます。

現在コントローラ上にあるすべての標準シグネチャおよびカスタム シグネチャを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから [シグネチャ パラメータの編集（Edit Signature Parameters）] を選択します。

ステップ 4 [実行（Go）] をクリックします。

ステップ 5 [すべての標準シグネチャおよびカスタム シグネチャのチェックを有効にする（Enable Check for All Standard and Custom Signatures）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

デバイスの IDS 署名の設定 （133 ページ）

コントローラでの単一の IDS シグニチャの有効化と無効化

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから [シグネチャ パラメータの編集（Edit Signature Parameters）] を選択します。

ステップ 4 有効または無効にする攻撃のタイプの、該当する名前をクリックします。

[標準シグネチャ パラメータ（Standard Signature Parameters）] ページには、現在コントローラ上にあるシスコ提供のシグネチャの一覧が表示されます。[カスタム シグネチャ（Custom Signatures）] ページには、現在コントローラ上に存在する、ユーザ提供のシグネチャのリストが表示されます。次のパラメータは、シグネチャ ページと詳細シグネチャ ページの両方に表示されます。

- [優先度（Precedence）]：コントローラがシグネチャ チェックを行う順序、または優先順位。
- [名前（Name）]：シグネチャによって検出を試みる攻撃の種類。
- [説明（Description）]：シグネチャによって検出を試みる攻撃の種類の詳細説明。
- [フレームの種類（Frame Type）]：シグネチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータ フレームの種類。
- [アクション（Action）]：シグネチャによって攻撃が検出された際に実行する、コントローラへの指示。アクションを実行しない場合は [なし（None）]、検出を報告する場合は [レポート（Report）] となります。
- [頻度（Frequency）]：シグネチャの頻度。攻撃が検出される前に、アクセス ポイント レベルの検出において識別する必要のある、間隔ごとのシグネチャと一致するパケット数です。有効な範囲は間隔あたり 1 ～ 32,000 パケットです。デフォルト値は間隔あたり 50 パケットです。
- [停止時間（Quiet Time）]：各アクセス ポイント レベルで攻撃が検出されなくなってから、アラームを停止するまでの時間の長さ（秒単位）。この設定は、[MAC 情報（MAC Information）] の設定が [すべて（all）] もしくは [両方（both）] の場合にのみ表示されます。有効な範囲は 60 ～ 32,000 秒で、デフォルト値は 300 秒です。
- [MAC 情報（MAC Information）]：アクセス ポイント レベルの検出においてシグネチャをネットワークごとまたは MAC アドレスごと、または両方で追跡するどうか。
- [MAC の頻度（MAC Frequency）]：シグネチャ MAC の頻度。攻撃が検出される前に、コントローラ レベルにおいて識別する必要のある、間隔ごとのシグネチャと一致するパケット数です。有効な範囲は間隔あたり 1 ～ 32,000 パケットです。デフォルト値は間隔あたり 30 パケットです。
- [間隔（Interval）]：設定した間隔内でシグネチャの頻度しきい値に達するまでに経過する必要のある秒数を入力します。有効な範囲は 1 ～ 3600 秒で、デフォルト値は 1 秒です。
- [有効（Enable）]：このシグネチャによりセキュリティ攻撃が検出されるようにする場合はこのチェックボックスをオンにし、このシグネチャを無効にする場合はオフにします。

- [シグネチャ パターン（Signature Patterns）]：セキュリティ攻撃の検出に使用されるパターン。

ステップ 5 [有効（Enable）] ドロップダウン リストから、[はい（Yes）] を選択します。カスタマイズされたシグネチャをダウンロードしているため、_custom.sgi という名前の付いたファイルを有効にし、同じ名前で異なる拡張子を持つ標準シグネチャを無効にする必要があります。たとえば、ブロードキャスト プローブ フラッドをカスタマイズしている場合に、ブロードキャスト プローブ フラッドを標準シグネチャでは無効にし、カスタム シグネチャでは有効にします。

ステップ 6 [保存（Save）] をクリックします。

デバイスの IDS 署名の設定 （133 ページ）
コントローラでの不正 AP ポリシーの設定 （130 ページ）
コントローラでの不正 AP ポリシーの表示 （131 ページ）
カスタム IDS 署名の作成 （138 ページ）
コントローラでのクライアント除外ポリシーの設定 （132 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （139 ページ）

カスタム IDS 署名の作成

[Custom Signature] ページには、現在コントローラ上に存在する、ユーザ提供のシグニチャのリストが表示されます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [カスタム シグネチャ（Custom Signatures）]** を選択します。このページには、次のパラメータが表示されます。

- [優先度（Precedence）]：コントローラがシグネチャ チェックを実行する順序。
- [名前（Name）]：シグネチャによって検出を試みる攻撃の種類。
- [フレームの種類（Frame Type）]：シグネチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータ フレームの種類。
- [アクション（Action）]：シグネチャによって攻撃が検出された際に実行する、コントローラへの指示。次に例を示します。
  - [なし（None）]：アクションが実行されません。
  - [報告（Report）]：検出を報告します。
- [状態（State）]：有効または無効。
- [説明（Description）]：シグネチャによって検出を試みる攻撃の種類の詳細説明。

ステップ 4 シグネチャの名前をクリックして各パラメータを表示し、シグネチャを有効または無効にします。

デバイスの IDS 署名の設定 （133 ページ）
コントローラでの不正 AP ポリシーの設定 （130 ページ）
コントローラでの不正 AP ポリシーの表示 （131 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （139 ページ）

コントローラの AP 認証と管理フレーム保護の設定

アクセス ポイント認証ポリシーと管理フレーム保護（MFP）を設定できます。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [AP 認証および MFP（AP Authentication and MFP）] の順に選択します。

このページには、次のフィールドが表示されます。

- [RF ネットワーク名（RF Network Name）]：このテキスト ボックスは編集できません。[一般パラメータ（General parameters）] ページに入力した RF ネットワーク名がここに表示されます。
- [保護タイプ（Protection Type）]：ドロップダウン リストから、次のいずれかの認証ポリシーを選択します。
  - [なし（None）]：アクセス ポイント認証ポリシーなし。
  - [AP 認証（AP Authentication）]：認証ポリシーを適用します。
  - [MFP]：管理フレーム保護を適用します。
  - [アラームがトリガーされるしきい値（Alarm Trigger Threshold）]：（[保護タイプ（Protection Type）] で [AP 認証（AP Authentication）] を選択した場合のみ表示）。アラームを発生させるまでに無視する、未知のアクセス ポイントからのヒット数を設定します。

値の範囲は 1 ～ 255 です。デフォルト値は 255 です。

デバイスの IDS 署名の設定 （133 ページ）
コントローラでの不正 AP ポリシーの設定 （130 ページ）
コントローラでの不正 AP ポリシーの表示 （131 ページ）
カスタム IDS 署名の作成 （138 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （133 ページ）

URL ACL の構成

URL フィルタリング機能により、インターネットの Web サイトへのアクセスを制御できます。この処理を行うには、URL アクセス コントロール リスト（ACL）に含まれる情報に基づいて、特定の Web サイトへのアクセスを許可または拒否します。その後、URL フィルタリングにより、ACL リストに基づいてアクセスを制限します。

ロケーション ベースのフィルタリングを使用して、AP はさまざまな AP グループにまとめられます。また、WLAN プロファイルにより、同じ SSID の信頼できるクライアントと信頼できないクライアントが分けられます。これにより、信頼できるクライアントが信頼できない AP に移動する場合、あるいはその逆の場合、再認証と新しい VLAN の使用が強制されます。

ワイヤレス コントローラ（WLC）は、最大で 64 個の ACL をサポートします。各 ACL では最大 100 個の URL を指定できます。これらの ACL では、要求を許可または拒否するよう設定できます。また、これらの ACL を各種のインターフェイス（WLAN や LAN など）に関連付けて、フィルタリングを効果性を高めることができます。ポリシーは、適用されたグローバル ポリシーとは異なる WLAN または AP グループでローカルで実装することができます。

各 ACL でサポートされるルール（URL）の数は WLC ごとに異なります。

- Cisco 5508 WLC および WiSM2 は URL ACL ごとに 64 件のルールをサポートできます。
- Cisco 5520、8510、8540 WLC は URL ACL ごとに 100 件のルールをサポートできます。

URL フィルタリングと NAT の制限

- Cisco 2504 WLC、vWLC、Mobility Express ではサポートされていません。
- WLAN 中央スイッチングはサポートされますが、ローカル スイッチングはサポートされていません。
- ローカル スイッチングを使用したフレックス モードではサポートされていません。
- URL 名の長さは 32 文字に制限されています。
- 一致した URL の AVC プロファイルはありません。一致した URL は ACL アクションでサポートされています。
- ホワイト リストとブラックリストのリストを、ACL の「*」暗黙ルールを使用して作成し、要求を個別に許可または拒否することができます。
- HTTPS URL はサポートされていません。
- 次の状況では ACL はフィルタできない場合があります。
  - URL がフラグメント化されたパケットにまたがっている。
  - IP パケットがフラグメント化されている。
  - URL の代わりに直接 IP アドレスまたはプロキシ設定が使用されている。
- これらは現在サポートされていません。次の条件と一致する URL は、フィルタリングの対象になりません。
  - ワイルドカードの URL（例：www.uresour*loc.com）
  - サブ URL（例：www.uresour* loc.com/support）
  - サブドメイン（例：reach.url.com や sub1.url.com）

- テンプレートの作成時に、重複する URL がある場合、重複 URL ルールは考慮されません。

アクセス コントロール リストの設定

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [URL ACLs] を選択します。

このページには、次のフィールドが表示されます。

- [チェックボックス（Check box）]：チェックボックスを使用して、削除する URL ACL を 1 つ以上選択します。
- [URL ACL 名（URL ACL 名）]：このテンプレートのユーザ定義名。URL ACL 項目をクリックし、説明を表示します。

ステップ 4 URL ACL をクリックします。

ステップ 5 [ルール（Rules）] の下にある [行の追加（Add Row）] をクリックして URL ACL ルールを追加します。

- [URL] テキスト ボックスに URL ACL の名前を入力します。
- [ルールアクション（Rule Action）] ドロップダウン リストから、[許可（Allow）] または [拒否（Deny）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

コントローラまたはデバイスのセキュリティ設定の構成 （105 ページ）
URL ACL の削除 （141 ページ）

URL ACL の削除

URL ACL を削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 コントローラ デバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [URL ACLs]** を選択します。

ステップ 4 [URL ACLs] ページから、削除する URL ACL を 1 つ以上選択します。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [URL ACL の削除（Delete URL ACLs）] を選択します。

ステップ 6 [移動（Go）] をクリックします。

（注） ACL のカウンタをクリアする場合は、[コマンドの選択（Select a command）] ドロップダウン リストから [クリア（Clear）] を選択します。

関連トピック

アクセス コントロール リストの設定 （141 ページ）

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（FRA）は、Cisco Aironet 2800 および 3800 シリーズ アクセス ポイントで NDP 測定を分析し、新しいフレキシブル ラジオ（2.4 GHz、5 GHz、またはモニタ）の役割を判断するために使用するハードウェアを管理するために Radio Resource Management（RRM; 無線リソース管理）に追加された新しいコア アルゴリズムです。

FRA 機能により、対応可能な AP を手動で設定したり、これらの AP が、使用可能な RF 環境に基づいて統合無線の動作の役割をインテリジェントに決定したりできます。フレキシブル ラジオを備えた AP は、多数のデバイスがネットワークに接続しているときを自動的に検出し、アクセス ポイントのデュアル無線を 2.4 GHz/5 GHz から 5 GHz/5 GHz に変更し、より多くのクライアントにサービスを提供できます。AP は、パフォーマンスに影響を与える RF 干渉およびセキュリティ脅威に対しネットワークを監視しながら、このタスクを実行します。FRA により、高密度ネットワークのモバイル ユーザ エクスペリエンスが向上します。また、この機能によって、2.4GHz 無線の一部に冗長化のマークを付け、5GHz（クライアント側の役割）またはモニタの役割（2.4GHz および 5GHz）に切り替えることで、2.4GHz セルの輻輳が低減されます。無線の役割を設定するには、CLI または GUI を使用します。

フレキシブル ラジオを備えた AP は、次のモードで動作できます。

- デフォルトの動作モード：一方の無線では 2.4 GHz モードでクライアントにサービスを提供し、他方の無線では、5 GHz モードでサービスを提供します。
- デュアル 5 GHz モード：両方の無線が 5 GHz 帯域で動作し、802.11ac Wave 2 の利点を最大化し、クライアント デバイスのキャパシティを増やすために積極的にクライアントにサービスを提供します。
- ワイヤレス セキュリティ モニタリング：一方の無線では 5 GHz でクライアントにサービスを提供し、他方の無線では、wIPS 攻撃者、CleanAir 干渉源、不正なデバイスに対し 2.4 GHz 帯域および 5 GHz 帯域の両方でスキャンを行います。

フレキシブル ラジオ アサインメントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ**	

	コマンドまたはアクション	目的
	（**Device Type**）] > [ワイヤレスコントローラ（**Wireless Controller**）] を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[802.11]** > **[フレキシブル ラジオ アサインメント（Flexible Radio Assignment）]** を選択します。[フレキシブル ラジオ アサインメント（Flexible Radio Assignment）] ページで次の内容を設定します。 • [フレキシブル ラジオ アサイメント（Flexible Radio Assignment）]：デフォルトでは FRA 機能は無効になっています。FRA を有効にし、 次のパラメータを設定するには、チェックボックスをオンにします。 • [感度（Sensitivity）]：FRA 感度しきい値を調整します。これにより、無線を冗長と見なす必要がある COF のパーセンテージ が設定されます。次の値をサポートしています。 • 低（Low） • 中 • 高 • [間隔（Interval）]：FRA の実行間隔を設定します。有効な範囲は 1 ～ 24 時間です。デフォルトの設定は1 時間です。FRA は DCA に依存しているため、FRA の間隔は、DCA の間隔を下回ることはできません。	

デバイスの 802.11 パラメータの設定

ここでは、次の項について説明します。

- 802.11 コントローラでの複数の国コードの設定
- どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング）
- AP チャネル干渉を抑えるバンド選択の有効化
- MediaStream を使用した IP マルチキャスト配信の確保

- AP グループで使用できる RF プロファイルの作成

802.11 コントローラでの複数の国コードの設定

モビリティ グループに含まれていない単一のコントローラを複数の国をサポートするように設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [一般（General）]** を選択します。

ステップ 4 チェックボックスをオンにして追加する国を選択します。アクセス ポイント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。国コードを設定して、国の規制に準拠するようにすることができます。

運用する国向けに設計されていない場合、アクセス ポイントは正しく動作しない可能性があります。たとえば、部品番号が AIR-AP1030-A-K9（米国の規制ドメインに含まれている）のアクセス ポイントは、オーストラリアでは使用できません。必ず自国の規制ドメインに合ったアクセス ポイントを購入するようにしてください。製品ごとのサポートされる国コードの完全なリストについては、http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html を参照してください。

ステップ 5 認証応答がタイムアウトになるまでの時間（秒単位）を入力します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

どのようなときにコントローラが追加のクライアント アソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （144 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （146 ページ）
MediaStream を使用した IP マルチキャスト配信の確保 （148 ページ）
AP グループで使用できる RF プロファイルの作成 （149 ページ）

どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング）

コントローラ上でアグレッシブ ロード バランシングを有効にすると、Lightweight アクセス ポイント間で、アクセス ポイント全体のワイヤレス クライアントのロード バランスを行うことができます。クライアントのロード バランスは、同じコントローラ上のアクセス ポイント間で行われます。別のコントローラ上のアクセス ポイントとの間では、ロード バランシングは行われません。

ワイヤレス クライアントが Lightweight アクセス ポイントへの関連付けを試みると、関連付け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。このコードは、アクセス ポイントがそれ以

上関連付けを受け付けることが可能かどうかを示します。アクセス ポイントへの負荷が高すぎる場合は、クライアントはそのエリア内の別のアクセス ポイントへの関連付けを試みます。アクセス ポイントの負荷が高いかどうかは、そのクライアントからアクセス可能な、近隣の他のアクセス ポイントと比べて相対的に判断されます。

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 ウィンドウの和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。クライアントが AP1 に関連付けようとすると、ステータス コード 17 が含まれている 802.11 応答パケットがクライアントに送信されます。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 ポイントへの関連付けを試みます。

10回までクライアント関連付けを拒否するようコントローラを設定できます（クライアントが 11 回関連付けを試行した場合、11 回目の試行では関連付けが許可されます）。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。

アグレッシブ ロード バランシングを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [ロード バランシング（Load Balancing）]** を選択します。[ロード バランシング（Load Balancing）] ページが表示されます。

ステップ 4 クライアントのウィンドウ サイズとして 1 ～ 20 までの値を入力します。このページ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント関連付けを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ページ + 最も負荷が低い AP 上のクライアント関連付け数 = ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、関連付けしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアントのページ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント関連付けの数がこのしきい値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントが関連付けできるのは、クライアント数がしきい値を下回るアクセス ポイントのみとなります。

ステップ 5 拒否の最大数として 0 ～ 10 までの値を入力します。拒否数は、ロード バランシング中の関連付け拒否の最大数を設定します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 特定の WLAN でアグレッシブ ロード バランシングを有効または無効にするには、[WLAN 設定（WLAN Configuration）] ページを参照して、[詳細設定（Advanced）] タブをクリックします。[WLAN 設定（WLAN

Configuration）] ページの使用方法については、「関連項目」の「コントローラ WLAN の設定」を参照してください。

関連トピック

802.11 コントローラでの複数の国コードの設定 （144 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （146 ページ）
MediaStream を使用した IP マルチキャスト配信の確保 （148 ページ）
AP グループで使用できる RF プロファイルの作成 （149 ページ）
コントローラでの WLAN の作成 （71 ページ）

AP チャネル干渉を抑えるバンド選択の有効化

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、混雑の少ない 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よくあります。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発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。これらの干渉の原因を緩和して、ネットワーク全体のパフォーマンスを向上させるには、コントローラで帯域選択を設定できます。

帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。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。

帯域選択をコントローラ上でグローバルに有効にすることも、特定の WLAN 上の帯域選択を有効または無効にすることもできます。後者は、特定のクライアントのグループ（遅延に敏感な音声クライアントなど）に対して帯域選択を無効にする場合に便利です。

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ので、音声や映像のような、遅延に敏感なアプリケーションはサポートされません。

帯域選択の使用に関するガイドライン

帯域選択を使用する際には、次のガイドラインに従ってください。

- 帯域選択を使用できるのは、アクセス ポイントが Cisco Aironet 1140 または 1250 シリーズである場合だけです。
- 帯域選択が動作するのは、コントローラに接続されたアクセス ポイントに対してのみです。コントローラに接続しない FlexConnect アクセス ポイントは、リブート後に帯域選択を実行しません。
- 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、同じアクセス ポイントの 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、アクセス ポイントで 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。
- コントローラ上で帯域選択とアグレッシブ ロード バランシングの両方を有効にすることができます。これらは独立して動作し、相互に影響を与えることはありません。

帯域選択を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [帯域選択（Band Select）]** を選択します。[帯域選択（Band Select）] ページが表示されます。

ステップ 4 プローブ サイクル回数として 1 ～ 10 までの値を入力します。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 5 スキャン サイクル期間の閾値として 1 ～ 1000 ミリ秒までの値を入力します。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 6 [エージング アウト抑制（age out suppression）] フィールドに 10 ～ 200 秒までの値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g 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 7 [エージング アウト デュアル バンド（age out dual band）] フィールドに 10 ～ 300 秒までの値を入力します。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 60 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 8 [許容されるクライアント RSSI（acceptable client RSSI）] フィールドに –20 ～ –90 dBm までの値を入力します。このフィールドは、クライアントがプローブに応答するための最小 RSSI を設定します。デフォルト値は -80 dBm です。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 特定の WLAN で帯域選択を有効または無効にするには、[WLAN 設定（WLAN Configuration）] ページを参照して、[詳細設定（Advanced）] タブをクリックします。[WLAN 設定（WLAN Configuration）] ページの使用方法については、「関連項目」の「コントローラ WLAN の設定」を参照してください。

802.11 コントローラでの複数の国コードの設定 （144 ページ）
どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （144 ページ）
MediaStream を使用した IP マルチキャスト配信の確保 （148 ページ）
AP グループで使用できる RF プロファイルの作成 （149 ページ）
コントローラでの WLAN の作成 （71 ページ）

SIP コールの優先度の制御

優先コール機能を使用すると、特定の番号に対して行う SIP コールに最高の優先度を指定できます。高い優先度を設定するには、設定済みの音声プールに使用可能な音声帯域幅がない場合でも、そのような優先 SIP コールに帯域幅を割り当てます。この機能は、WCS または WLC で帯域幅割り当てに SIP ベースの CAC を使用するクライアントのみでサポートされます。

コントローラごとに最大 6 個の番号を設定できます。

優先コール サポートを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [優先コール（Preferred Call）]** を選択します。既存の優先コールがある場合は、次のフィールドが表示されます。

- [説明（Description）]：優先コールの説明。
- [番号 ID（Number Id）]：コントローラの固有識別子を示し、コントローラに割り当てられている 6 個の優先コール番号の 1 つを示します。
- [優先番号（Preferred Number）]：優先コール番号を示します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、[番号の追加（Add Number）] を選択します。

ステップ 5 このコントローラに適用するテンプレートを選択します。

選択したコントローラに適用するテンプレートを選択する必要があります。優先コール番号用の新しいテンプレートを作成するには、「関連項目」の「優先コール テンプレートの設定」を参照してください。

ステップ 6 [適用（Apply）] をクリックします。

優先コールを削除するには、該当する優先コール番号のチェックボックスをオンにして、[コマンドの選択（Select a command）] ドロップダウン リストから [削除（Delete）] を選択します。[実行（Go）] をクリックし、[OK] をクリックして削除を確認します。

関連トピック

802.11 コントローラでの複数の国コードの設定 （144 ページ）
どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （144 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （146 ページ）
AP グループで使用できる RF プロファイルの作成 （149 ページ）

MediaStream を使用した IP マルチキャスト配信の確保

802.11 のメディア パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11]** > **[メディア ストリーム（Media Stream）]** を選択します。

ステップ 4 [メディア ストリームの設定（Media Stream Configuration）] セクションで、次のパラメータを設定します。

- [メディア ストリーム名（Media Stream Name）]
- [マルチキャストの宛先開始 IP（Multicast Destination Start IP）]：マルチキャストまでのメディア ストリームの開始 IP アドレス
- [マルチキャストの宛先終了 IP（Multicast Destination End IP）]：マルチキャストまでのメディア ストリームの終了 IP アドレス
- [最大期待帯域幅（Maximum Expected Bandwidth）]：メディア ストリームが使用できる最大帯域幅

ステップ 5 [リソース予約コントロール（RRC）パラメータ（Resource Reservation Control (RRC) Parameters）] グループボックスで、次のパラメータを設定します。

- [平均パケット サイズ（Average Packet Size）]：メディア ストリームが使用できる平均パケット サイズ。
- [RRC 定期更新（RRC Periodical Update）]：定期的に更新されるリソース予約コントロールの計算。無効にすると、RRC の計算は、クライアントがメディア ストリームに加入した際に、1 回のみ行われます。
- [RRC 優先度（RRC Priority）]：最高が 1、最低が 8 の RRC の優先度。
- [トラフィック プロファイル違反（Traffic Profile Violation）]：ストリームが QoS ビデオ プロファイルに違反した際に、ストリームがドロップされるか、ベストエフォート キューに入れられる場合に表示されます。
- [ポリシー（Policy）]：メディア ストリームが許可されるか拒否される場合に表示されます。

ステップ 6 [保存（Save）] をクリックします。

AP グループで使用できる RF プロファイルの作成

[RF プロファイル（RF Profiles）] ページでは、AP グループに関連付ける RF プロファイルを作成または変更できます。

コントローラの RF プロファイルを設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 [RF プロファイル（RF Profiles）] をクリックするか、左側のサイドバー メニューから [802.11] > [RF プロファイル（RF Profiles）] を選択します。[RF プロファイル（RF Profiles）] ページが表示されます。このページには、既存の RF プロファイル テンプレートがリストされます。

ステップ 4 RF プロファイルを追加する場合は、[コマンドの選択（Select a command）] ドロップダウン リストから [RF プロファイルの追加（Add RF Profile）] を選択します。

ステップ 5 [実行（Go）] をクリックします。[新規コントローラ テンプレート（New Controller Template）] ページが表示されます。

ステップ 6 次の情報を設定します。

- 一般
  - [テンプレート名（Template Name）]：テンプレートのユーザ定義の名前。[プロファイル名（Profile Name）]：現在のプロファイルのユーザ定義の名前。[説明（Description）]：テンプレートの説明。
  - [無線タイプ（Radio Type）]：アクセス ポイントの無線タイプ。これは、802.11a または 802.11b 無線がある AP の RF プロファイルを選択できるドロップダウン リストです。
- [TCP（送信電力制御）（TCP (Transmit Power Control)）]
  - [最小電力レベルの割り当て（-10 ～ 30 dBm）（Minimum Power Level Assignment (-10 to 30 dBm)）]：割り当てられている最小電力を示します。範囲は -10 ～ 30 dB で、デフォルト値は 30 dB です。
  - [最大電力レベルの割り当て（-10 ～ 30 dBm）（Maximum Power Level Assignment (-10 to 30 dBm)）]：割り当てられている最大電力を示します。範囲は -10 ～ 30 dB で、デフォルト値は 30 dB です。
  - [電力しきい値 v1（-80 から -50 dBm）（Power Threshold v1(-80 to -50 dBm)）]：送信電力しきい値を示します。[電力しきい値 v2（-80 から -50 dBm）（Power Threshold v2(-80 to -50 dBm)）]：送信電力しきい値を示します。
- [データ レート（Data Rates）]：アクセス ポイントとクライアント間でデータを送信できるレートを指定するには、[データ レート（Data Rates）] ドロップダウン リストを使用します。次のデータ レートが使用可能です。
  - [802.11a]：6、9、12、18、24、36、48、および 54 Mbps。
  - [802.11b/g]：1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps。

  各データ レートに対して、次のオプションのいずれかを選択します。
  - [必須（Mandatory）]：このコントローラ上のアクセス ポイントに関連付けるには、クライアントがこのデータ レートをサポートしている必要があります。
  - [サポート（Supported）]：関連付けられたクライアントは、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、関連付けは可能です。
  - [無効（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 7 [保存（Save）] をクリックします。

関連トピック

802.11 コントローラでの複数の国コードの設定 （144 ページ）
どのようなときにコントローラが追加のクライアント アソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （144 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （146 ページ）

デバイスの 802.11a/n パラメータの設定

特定のコントローラの 802.11a/n パラメータを表示するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、次のいずれかを選択します。

- [802.11a/n] > [パラメータ（Parameters）]：パラメータを表示または編集します。
- [802.11a、または n あるいは ac（802.11a or n or ac）] > [dot11a-RRM] > [RRM しきい値（RRM Thresholds）]：802.11a/n RRM しきい値コントローラを設定します。
- [802.11a/n] > [RRM 間隔（RRM Intervals）] または [802.11b/g/n] > [RRM 間隔（RRM Intervals）]：個々のコントローラに 802.11a/n または 802.11b/g/n の RRM しきい値を設定します。
- [802.11a/n-RRM] > [TPC] ：802.11a/n または 802.11b/g/n の RRM 伝送パワー コントロールを設定します。
- [802.11a または n あるいは ac（802.11a or n or ac）] > [dot11a-RRM] > [DCA]：RRM 動的チャネル割り当てを設定します。
- [802.11a/n] > [RRM] > [RF グループ化（RF Grouping）] ：個々のコントローラに 802.11a/n または 802.11b/g/n の RRM 無線のグループ化を設定します。
- [802.11a/n] > [メディア パラメータ（Media Parameters）]：802.11a/n にメディア パラメータを設定します。
- [802.11a/n] > [EDCA パラメータ（EDCA Parameters）] または [802.11b/g/n] > [EDCA]：個々のコントローラに 802.11a/n または 802.11b/g/n の EDCA パラメータを設定します。
- [802.11a/n] > [ローミング パラメータ（Roaming Parameters）]：802.11a/n または 802.11b/g/n のローミング パラメータを設定します。
- [802.11a/n] > [802.11h] または [802.11b/g/n] > [802.11h]：個々のコントローラに 802.11h パラメータを設定します。
- 802.11a/n または 802.11b/g/n 高スループット パラメータを設定する場合は、[802.11a/n] > [高スループット（High Throughput）] または [802.11b/g/n] > [高スループット（High Throughput）]。
- [802.11a/n] > [CleanAir]：802.11a/n CleanAir パラメータを設定します。

ステップ 4 [保存（Save）] をクリックします。

デバイスの 802.11b/g/n パラメータの設定

特定のコントローラの 802.11b/g/n パラメータを表示するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、次のいずれかを選択します。

- [802.11b/g/n パラメータ（802.11b/g/n Parameters）]：パラメータを表示または編集します。
- [802.11b または g あるいは n（802.11b or g or n）] > [dot11b-RRM] > [しきい値（Tresholds）]：802.11b/g/n RRM しきい値を設定します。
- [802.11a/n] > [RRM 間隔（RRM Intervals）] または [802.11b/g/n] > [RRM 間隔（RRM Intervals）]：802.11b/g/n RRM 間隔を設定します。
- [802.11b/g/n-RRM] > [TPC]：802.11b/g/n RRM 伝送パワー コントロール パラメータを設定します。
- [802.11b または g あるいは n（802.11b or g or n）] > [dot11b-RRM] > [DCA]：個々のコントローラに 802.11a/n または 802.11b/g/n の RRM DCA チャネルを設定します。
- [802.11b/g/n] > [RRM] > [RF グループ化（RF Grouping）：個々のコントローラに 802.11a/n または 802.11b/g/n の RRM 無線グループ化を設定します。
- [802.11b/g/n] > [メディア パラメータ（Media Parameters）]：802.11b/g/n にメディア パラメータを設定します。
- [802.11a/n] > [EDCA パラメータ（EDCA Parameters）] または [802.11b/g/n] > [EDCA]：個々のコントローラに 802.11a/n または 802.11b/g/n の EDCA パラメータを設定します。
- [802.11a/n] > [ローミング パラメータ（Roaming Parameters）] または [802.11b/g/n] > [ローミング パラメータ（Roaming Parameters）]：802.11a/n または 802.11b/g/n の EDCA パラメータを設定します。
- 802.11a/n または 802.11b/g/n 高スループット パラメータを設定する場合は、[802.11a/n] > [高スループット（High Throughput）] または [802.11b/g/n] > [高スループット（High Throughput）]。
- [802.11b/g/n] > [CleanAir]：802.11b/g/n CleanAir パラメータを設定します。

ステップ 4 [保存（Save）] をクリックします。

デバイスのメッシュ パラメータの設定

個々のコントローラのメッシュ パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[メッシュ（Mesh）] > [メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 次のメッシュ パラメータを表示または編集します。

- [RootAP から MeshAP までの範囲（RootAP to MeshAP Range）]：デフォルトでは、この値は 12,000 フィートです。150 ～ 132,000 フィートの値を入力できます。ルート アクセス ポイントとメッシュ アクセス ポイント間の適切な距離をフィート単位で入力します。このグローバル フィールドは、コントローラにアクセス ポイントが接続されるとすべてのアクセス ポイントに適用され、ネットワーク内に存在するすべての既存のアクセス ポイントにも適用されます。

- [バックホール リンクのクライアント アクセス（Client Access on Backhaul Link）]：この機能を有効にすると、802.11a バックホールを介してメッシュ アクセス ポイントを 802.11a ワイヤレス クライアントに関連付けることができます。これは、ルートとメッシュ アクセス ポイント間の 802.11a バックホール上の既存の通信に追加されます。この機能は 2 つの無線のあるアクセス ポイントだけに適用されます。バックホール クライアント アクセスを変更すると、すべてのメッシュ アクセス ポイントが再起動されます。詳細については、「関連項目」の「1524SB デュアル バックホールでのクライアント アクセス」を参照してください。

  メッシュのバックグラウンド スキャンおよび自動親選択機能により、メッシュ アクセス ポイント（MAP）は全チャネルにわたってより良い潜在的親を検索して接続し、常に最良の親にアップリンクすることができます。

  この機能により、すべてのチャネルをスキャンすることによりチャネル全体にわたって親を検索するという時間のかかるタスクが削減されます。オフチャネル手順は、選択したチャネルでブロードキャスト パケットを送信し（3 秒間隔、オフチャネルあたり最大 50 ミリ秒）、すべての「到達可能」ネイバーからパケットを受信します。これにより、子 MAP はチャネル全体にわたるネイバー情報で更新され、新しいネイバーに「切り替え」てアップリンクの親として使用することができます。「切り替え」は、親損失の検出でトリガーされる必要はありませんが、より良い親の識別時にトリガーされます。ただし、子 MAP では現在の親アップリンクがアクティブなままとなります。

- [バックグラウンド スキャン（Background Scanning）]：メッシュのバックグラウンド スキャン機能を有効にするには、[バックグラウンド スキャン（Background Scanning）] チェックボックスをオンにします。デフォルトでは、無効に設定されています。

- [メッシュ DCA チャネル（Mesh DCA Channels）]：このオプションを有効にすると、DCA チャネル リストを使用してコントローラでバックホール チャネルを選択解除できるようになります。コントローラ DCA リスト内のチャネルに対する変更はすべて、関連付けられたアクセス ポイントに適用されます。このオプションは、1524SB メッシュ アクセス ポイントのみに適用可能です。詳細については、「関連項目」の「コントローラでのバックホール チャネル選択解除」を参照してください。
- [メッシュ RAP ダウンリンク バックホール（Mesh RAP Downlink Backhaul）]：バックホール ダウンリンク スロットを変更すると、すべてのメッシュ AP がリブートされます。
- [UNII 1 帯域チャネルの屋外アクセス（Outdoor Access For UNII 1 Band Channels）]

- [グローバル パブリック セーフティ（Global Public Safety）]：このオプションを有効にすると、802.11a バックホール無線のチャネルをオンにすることで、4.9 GHz をバックホール リンクで使用できます。公共安全帯域と見なされる 4.9 GHz は、一部のサービス プロバイダーに制限されます。この設定は、コントローラ レベルで適用されます。
- [セキュリティ モード（Security Mode）]：[セキュリティ モード（Security Mode）] ドロップダウン リストから [EAP]（拡張認証プロトコル）または [PSK]（事前共有キー）を選択します。セキュリティを変更すると、すべてのメッシュ アクセス ポイントが再起動されます。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化 （154 ページ）
コントローラでのバックホール チャネル選択解除の有効化 （155 ページ）

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化

1524 シリアル バックホール（SB）アクセス ポイントは、3 つの無線スロットで構成されます。

- スロット 0 の無線は 2.4 GHz の周波数帯域で動作し、クライアント アクセスに使用されます。
- スロット 1 とスロット 2 の無線は 5.8 GHz 帯域で動作し、主にバックホールに使用されます。

2 つの 802.11a バックホール無線は、同じ MAC アドレスを使用します。同じ WLAN が複数のスロット内の同じ BSSID にマップされることがあります。

デフォルトでは、両方のバックホール無線を介したクライアントアクセスが無効になります。

無線スロットを有効または無効にする場合は、これらのガイドラインに従う必要があります。

- スロット 2 でのクライアント アクセスが無効の場合でも、スロット 1 でクライアント アクセスを有効にできます。
- スロット 1 でのクライアント アクセスが有効の場合のみ、スロット 2 でクライアント アクセスを有効にできます。
- スロット 1 でクライアント アクセスを無効にすると、スロット 2 でのクライアント アクセスは自動的に無効になります。
- クライアント アクセスを有効または無効にすると常に、すべてのメッシュ アクセス ポイントが再起動されます。

ユニバーサル クライアント アクセス機能を使用すると、スロット 1 とスロット 2 の両方の無線でクライアントアクセスが可能です。次のいずれかから、バックホール無線によるクライアント アクセスを設定できます。

- コントローラのコマンドライン インターフェイス（CLI）
- コントローラのグラフィカル ユーザ インターフェイス（GUI）
- Prime Infrastructure GUI。

2 つのバックホール無線でクライアント アクセスを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[メッシュ（Mesh）] > [メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 [バックホール リンクでのクライアント アクセス（Client Access on Backhaul Link）] チェックボックスをオンにします。

ステップ 5 [拡張バックホール クライアント アクセス（Extended Backhaul Client Access）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

警告メッセージが表示されます。

例：

```
Enabling client access on both backhaul slots will use same BSSIDs on both the slots. Changing
Backhaul Client Access will reboot all Mesh APs.
```

ステップ 7 [OK] をクリックします。

ユニバーサル クライアント アクセスが、両方の無線で設定されます。

関連トピック

コントローラでのバックホール チャネル選択解除の有効化 （155 ページ）
デバイスのメッシュ パラメータの設定 （152 ページ）

コントローラでのバックホール チャネル選択解除の有効化

バックホール チャネルの選択解除を設定するには、次の手順を実行します。

ステップ 1 コントローラでメッシュ DCA チャネル フラグを設定します。「関連項目」の「1524 SB AP でのバックホール無線へのクライアント アクセスの無効化」を参照してください。

ステップ 2 設定グループを使用してチャネル リストを変更します。「関連項目」の「Prime Infrastructure 設定グループを使用したコントローラ チャネル リストの変更」を参照してください。

関連トピック

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化 （154 ページ）
デバイスのメッシュ パラメータの設定 （152 ページ）
Cisco Prime Infrastructure 設定グループを使用したコントローラ チャネル リストの変更 （156 ページ）

コントローラから 1524 SB AP へのチャネル変更のプッシュ

1 つ以上のコントローラでの各チャネルの変更を、関連付けられたすべての 1524SB アクセス ポイントに適用するよう、メッシュ DCA チャネル フラグを設定できます。この機能を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[メッシュ（Mesh）] > [メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 [メッシュ DCA チャネル（Mesh DCA Channels）] チェックボックスをオンにしてチャネル選択を有効にします。このオプションは、デフォルトではオフにされています。

コントローラでのチャネルの変更が、関連付けられた 1524SB アクセス ポイントに適用されます。

Cisco Prime Infrastructure 設定グループを使用したコントローラ チャネル リストの変更

コントローラの設定グループを使用して、バックホール チャネルの選択解除を設定できます。設定グループを作成して、必要なコントローラをグループに追加し、[国/DCA（Country/DCA）] タブを使用してそのグループ内のコントローラのチャネルを選択または選択解除できます。

設定グループを使用してバックホール チャネルの選択解除を設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [コントローラ設定グループ（Controller Configuration Groups）] を選択します。

ステップ 2 設定グループの詳細を表示する設定グループを選択します。

ステップ 3 [設定グループ（Configuration Group）] 詳細ページで、[国/DCA（Country/DCA）] タブをクリックします。

ステップ 4 [国/DCA の更新（Update Country/DCA）] チェックボックスをオンまたはオフにします。

関連トピック

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化 （154 ページ）
コントローラでのバックホール チャネル選択解除の有効化 （155 ページ）
デバイスのメッシュ パラメータの設定 （152 ページ）
コントローラから 1524 SB AP へのチャネル変更のプッシュ （156 ページ）

デバイスのポート パラメータの設定

個々のコントローラのポート パラメータを設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するデバイスをクリックします。

ステップ 3 左側のサイドバー メニューから、[ポート（Ports）] > [ポート設定（Port Settings）] を選択します。

ステップ 4 該当するポート番号をクリックして、[ポート設定の詳細（Port Settings Details）] ページを開きます。次のようなパラメータが表示されます。

- [一般パラメータ（General Parameters）] :
  - [ポート番号（Port Number）] : 読み取り専用。
  - [管理ステータス（Admin Status）] : ドロップダウン リストから [有効（Enabled）] または [無効（Disabled）] を選択します。
  - [物理モード（Physical Mode）] : 自動ネゴシエーション（読み取り専用）。
  - [物理ステータス（Physical Status）] : 全二重 1000 Mbps（読み取り専用）。
  - [STP モード（STP Mode）] : [802.1D]、[高速（Fast）]、または [オフ（Off）] を選択します。
  - [リンク トラップ（Link Traps）] : [有効（Enabled）] または [無効（Disabled）] を選択します。
  - Power Over Ethernet
  - [マルチキャスト アプリケーション モード（Multicast Application Mode）] : [有効（Enabled）] または [無効（Disabled）] を選択します。
  - [ポート モード SFP タイプ（Port Mode SFP Type）] : 読み取り専用。
- [スパニング ツリー プロトコル パラメータ（Spanning Tree Protocol Parameters）] :
  - [優先度（Priority）] : 最適なスイッチのプライオリティ番号。
  - [パス コスト（Path Cost）] : ネットワーク管理者によって割り当てられ、インターネットワーク環境で最も望ましいパス（コストが低いほど、適したパスになります）を判別するために使用される値（通常、ホップ カウント、メディア帯域幅、またはその他の測定に基づく）。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

デバイスのメッシュ パラメータの設定 （152 ページ）
コントローラの管理パラメータの設定 （158 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （169 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （171 ページ）
コントローラのロケーション情報の設定 （166 ページ）
コントローラのマルチキャスト DNS（mDNS）設定の構成 （175 ページ）
コントローラの Application Visibility and Control（AVC）パラメータの設定 （177 ページ）
コントローラの NetFlow 設定の構成 （179 ページ）

コントローラの管理パラメータの設定

コントローラの次の管理パラメータを設定できます。

- [トラップ レシーバ（Trap Receivers）]
- [トラップ コントロール（Trap Control）]
- [Telnet および SSH（Telnet and SSH）]
- [複数の Syslog サーバ（Multiple Syslog servers）]
- [Web 管理（Web Admin）]
- [ローカル管理ユーザ（Local Management Users）]
- [認証優先度（Authentication Priority）]

関連トピック

コントローラ トラップの設定 （159 ページ）
コントローラでの Syslog サーバの設定 （162 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （161 ページ）
コントローラでの Web 管理の設定 （163 ページ）
コントローラでのローカル管理ユーザの設定 （165 ページ）
コントローラの管理認証サーバ優先度の設定 （166 ページ）

コントローラのトラップ レシーバの設定

トラップ レシーバ パラメータは、個々のワイヤレス コントローラに設定できます。ワイヤレス コントローラに対してこのパラメータを追加および削除できます。[設定（Configuration）] > [機能およびテクノロジー（Features & Technologies）] でテンプレートを作成することで、トラップ レシーバを追加できます。

個々のコントローラのトラップ レシーバを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [トラップ レシーバ（Trap Receiver）]** を選択します。

ステップ 4 現在のトラップ レシーバについて、次のパラメータが表示されます。

- [コミュニティ名（Community Name）]：トラップ レシーバの名前。
- [IP アドレス（IP Address）]：サーバの IP アドレス。
- [管理ステータス（Admin Status）]：SNMP トラップをレシーバに送信するには、ステータスを有効にする必要があります。

ステップ 5 詳細にアクセスするには、レシーバ名をクリックします。

ステップ 6 トラップ レシーバを有効にするには、[管理ステータス（Admin Status）]チェックボックスをオンにします。トラップ レシーバを無効にするには、このチェックボックスをオフにします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 レシーバを削除するには、該当するレシーバのチェックボックス（複数可）をオンにします。

ステップ 9 [コマンドの選択（Select a command）] ドロップダウン リストから [レシーバの削除（Delete Receivers）] を選択します。

ステップ 10 [実行（Go）] をクリックします。

ステップ 11 確認メッセージで [OK] をクリックします。

コントローラ トラップの設定

個々のコントローラのトラップ制御パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [トラップ コントロール（Trap Control）]** を選択します。

ステップ 4 このコントローラの次のトラップを有効にできます。

- [その他のトラップ（Miscellaneous Traps）] :
  - [SNMP 認証（SNMP Authentication）] : SNMPv2 エンティティが、適切に認証されていないプロトコルメッセージを受信しました。SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。[リンク（ポート）アップ/ダウン（Link (Port) Up/Down）] : リンクのステータスは、アップまたはダウンから変更されます。[複数のユーザ（Multiple Users）] : 2 人のユーザが同じログイン ID でログインしています。[スパニング ツリー（Spanning Tree）] : スパニング ツリー トラップ。個々のパラメータについては、STP 仕様を参照してください。[不正 AP（Rogue AP）] : 不正 AP が検出されるたびに、このトラップが MAC アドレスとともに送信されます。以前に検出された不正 AP については、存在しなくなるとこのトラップが送信されます。[設定の保存（Config Save）] : コントローラ設定が変更されると送信される通知。[RFID 制限到達しきい値（RFID Limit Reached Threshold）] : RFID 制限の最大許容値です。

- [クライアント関連トラップ（Client Related Traps）] :
  - [802.11 関連付け（802.11 Association）] : クライアントが関連付けフレームを送信すると、関連付け通知が送信されます。[802.11 関連付け解除（802.11 Disassociation）] : クライアントが関連付け解除フレームを送信すると、関連付け解除通知が送信されます。[802.11 認証解除（802.11 Deauthentication）] : クライアントが認証解除フレームを送信すると、認証解除通知が送信されます。[802.11 認証の失敗（802.11 Failed Authentication）] : クライアントが「成功（successful）」以

外のステータス コードの認証フレームを送信すると、認証エラー通知が送信されます。[802.11 関連付けの失敗（802.11 Failed Association）]：クライアントが「成功（successful）」以外のステータス コードの関連付けフレームを送信すると、関連付けエラー通知が送信されます。[除外（Excluded）]：クライアントが除外されると、関連付けエラー通知が送信されます。[802.11 認証済み（802.11 Authenticated）]：クライアントがステータス コード「成功」で認証フレームを送信すると、認証通知が送信されます。[最大クライアント制限到達しきい値（MaxClients Limit Reached Threshold）]：許可されるクライアントの最大許容数です。

- [Cisco AP トラップ（Cisco AP Traps）]：
  - [AP 登録（AP Register）]：アクセス ポイントがコントローラとアソシエートまたはアソシエート解除すると送信される通知です。[AP インターフェイスのアップ/ダウン（AP Interface Up/Down）]：アクセス ポイント インターフェイス（802.11a または 802.11b/g）のステータスがアップまたはダウンになると送信される通知。

- [自動 RF プロファイル トラップ（Auto RF Profile Traps）]：
  - [ロード プロファイル（Load Profile）]：ロード プロファイルの状態が PASS と FAIL の間で変更されると送信される通知。[ノイズ プロファイル（Noise Profile）]：ノイズ プロファイルの状態が PASS と FAIL の間で変更されると送信される通知。[干渉プロファイル（Interference Profile）]：干渉プロファイルの状態が PASS と FAIL の間で変更されると送信される通知。[カバレッジ プロファイル（Coverage Profile）]：カバレッジ プロファイルの状態が PASS と FAIL の間で変更されると送信される通知。

- [自動 RF 更新トラップ（Auto RF Update Traps）]：
  - [チャネルの更新（Channel Update）]：アクセス ポイントの動的チャネル アルゴリズムが更新されると送信される通知。[送信電力の更新（Tx Power Update）]：アクセス ポイントの動的送信電力アルゴリズムが更新されると送信される通知。

- [AAA トラップ（AAA Traps）]：^
  - [ユーザ認証の失敗（User Auth Failure）]：このトラップは、クライアントの RADIUS 認証の失敗が発生したことを通知します。[RADIUS サーバの応答なし（RADIUS Server No Response）]：このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。

- [802.11 セキュリティ トラップ（802.11 Security Traps）]：
  - [WEP 復号エラー（WEP Decrypt Error）]：コントローラが WEP 復号エラーを検出すると送信される通知です。[シグネチャ攻撃（Signature Attack）]：シグネチャ攻撃が RADIUS 認証を使用するワイヤレス コントローラで検出されると送信される通知です。

ステップ 5 該当するパラメータの選択後に、[保存（Save）] をクリックします。

関連トピック

コントローラのトラップ レシーバの設定 （158 ページ）

コントローラでの Syslog サーバの設定 （162 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （161 ページ）
コントローラでの Web 管理の設定 （163 ページ）
コントローラでのローカル管理ユーザの設定 （165 ページ）
コントローラの管理認証サーバ優先度の設定 （166 ページ）

コントローラの Telnet SSH セッション パラメータの設定

個々のコントローラの Telnet SSH（セキュア シェル）パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [Telnet SSH]** を選択します。

次のパラメータを設定できます。

- [セッション タイムアウト（Session Timeout）]：ログオフされるまでに Telnet セッションが非アクティブの状態を継続できる分数を示します。0 は、タイムアウトしないことを意味します。0 ～ 160 までの数値で指定できます。工場出荷時のデフォルトは 5 です。
- [最大セッション（Maximum Sessions）]：ドロップダウン リストから、0 ～ 5 までの値を選択します。このオブジェクトは、許可される同時 Telnet セッションの数を示します。
- [新規 Telnet セッションを許可する（Allow New Telnet Sessions）]：[いいえ（no）] に設定すると、DS ポートでは新しい Telnet セッションが許可されません。工場出荷時のデフォルト値は [いいえ（no）] です。DS（ネットワーク）ポートでの新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。
- [新規 SSH セッションを許可する（Allow New SSH Sessions）]：[いいえ（no）] に設定すると、新しいセキュア シェル Telnet セッションが許可されません。工場出荷時のデフォルト値は [はい（yes）] です。

ステップ 4 該当するパラメータを設定した後、[保存（Save）] をクリックします。

関連トピック

コントローラのトラップ レシーバの設定 （158 ページ）
コントローラでの Syslog サーバの設定 （162 ページ）
コントローラでの Web 管理の設定 （163 ページ）
コントローラでのローカル管理ユーザの設定 （165 ページ）
コントローラの管理認証サーバ優先度の設定 （166 ページ）

コントローラでの Syslog サーバの設定

リリース 5.0.148.0 以降のコントローラでは、WLAN コントローラで複数（3 つまで）の Syslog サーバを設定できます。それぞれのメッセージが記録されると、メッセージの重大度が設定済みの Syslog フィルタ重大度レベル以上である場合、コントローラは、メッセージのコピーを設定済みの各 Syslog ホストに送信します。

個々のコントローラの Syslog を有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [複数の Syslog（Multiple Syslog）]** を選択します。

適用されるテンプレートが示されます。

[Syslog サーバ アドレス（Syslog Server Address）] : 該当する Syslog のサーバ アドレスを示します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 syslog サーバを削除するには、syslog サーバのチェックボックスをオンにします。

ステップ 6 [コマンドの選択（Select a command）] ドロップダウン リストから [Syslog サーバの削除（Delete Syslog Servers）] を選択します。

ステップ 7 [実行（Go）] をクリックします。

ステップ 8 確認メッセージで [OK] をクリックします。

関連トピック

コントローラのトラップ レシーバの設定 （158 ページ）
コントローラ トラップの設定 （159 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （161 ページ）
コントローラでの Web 管理の設定 （163 ページ）
コントローラでのローカル管理ユーザの設定 （165 ページ）
コントローラの管理認証サーバ優先度の設定 （166 ページ）

ネットワーク アシュアランスの設定

クライアントに関連するデータを Web サーバに定期的にプッシュするには、通常の WLC の機能に加え、ネットワーク アシュアランスを有効にします。このデータは、新たに導入されたアシュアランス関連のダッシュボードへのインプットとして使用されます。コントローラにネットワーク アシュアランスを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）]** > **[ネットワークアシュアランス（Network Assurance）]** の順に選択します。

ステップ 4 適用されているテンプレートを表示し、次のパラメータを設定することができます。

- [アシュアランスサーバにデータをパブリッシュする（Publish Data to Assurance Server）]：ネットワーク アシュアランス機能を制御するグローバル レベルのフィールドです。
- [データの外部化（Data Externalization）]：データ モデルに関するコントローラ設定です。ネットワーク アシュアランスを有効にするには、最初に [データの外部化（Data Externalization）] を有効にする必要があります。[データの外部化（Data Externalization）] フィールドの値を変更するには、WLC の再起動が必要です。
- [NAサーバのURL（NA Server URL）]：WLC がクライアント データを定期的にポストするサーバのアドレスです。サーバ アドレスには、ホスト ベースまたは IP アドレス ベースのアドレスを指定できます。[NAサーバのURL（NA Server URL）] がホスト ベースの場合、NA サーバの CA 証明書はホスト名に対して生成する必要があります。同様に、URL が IP アドレス ベースの場合は、証明書は IP アドレスで生成する必要があります。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラへの NA サーバ CA 証明書のダウンロード （18 ページ）
ネットワーク アシュアランスの自己署名付き証明書を生成 （16 ページ）
コントローラのトラップ レシーバの設定 （158 ページ）
コントローラでの Syslog サーバの設定 （162 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （161 ページ）
コントローラでの Web 管理の設定 （163 ページ）
コントローラでのローカル管理ユーザの設定 （165 ページ）
コントローラの管理認証サーバ優先度の設定 （166 ページ）

コントローラでの Web 管理の設定

この項では、ディストリビューション システム ポートを Web ポート（HTTP を使用）またはセキュア Web ポート（HTTPS を使用）として有効にする手順について説明します。HTTPS を有効にすると、GUI との通信を保護できます。HTTPS は、Secure Socket Layer（SSL）プロトコルを使用して HTTP ブラウザ セッションを保護します。HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。外部で生成された証明書をダウンロードできます。

個々のコントローラの WEB 管理パラメータを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [Web 管理（Web Admin）]** を選択します。

次のパラメータを設定できます。

- [Web モード（WEB Mode）] : ドロップダウン リストから [有効（Enable）] または [無効（Disable）] を選択します。有効にすると、ユーザは、*http:ip-address* を使用してコントローラの GUI にアクセスできます。デフォルトは [無効（Disabled）] です。Web モードの接続は、セキュリティで保護されません。
- [セキュア Web モード（Secure Web Mode）] : ドロップダウン リストから [有効（Enable）] または [無効（Disable）] を選択します。有効にした場合、ユーザは *https://ip-address* を使用してコントローラ GUI にアクセスできます。デフォルトは [有効（Enabled）] です。
- .[証明書タイプ（Certificate Type）] : Web 管理証明書をダウンロードする必要があります。新しい Web 管理証明書を有効にするには、コントローラを再起動する必要があります。
  - [Web 管理証明書のダウンロード（Download Web Admin Certificate）] : [コントローラへの Web 管理証明書のダウンロード（Download Web Admin Certificate to Controller）] ページにアクセスする場合にクリックします。詳細については、「**コントローラへの Web 認証または Web 管理証明書のダウンロード**」を参照してください。

コントローラへの Web 認証または Web 管理証明書のダウンロード

Web 認証または Web 管理証明書をコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 [Web 管理証明書のダウンロード（Download Web Admin Certificate）] リンクまたは [Web 認証証明書のダウンロード（Download Web Auth Certificate）] リンクをクリックします。

ステップ 2 [ファイルが存在する場所（File is located on）] フィールドで、ローカル マシンまたは TFTP サーバを指定します。証明書が TFTP サーバにある場合は、サーバ ファイル名を入力します。ローカル マシンにある場合は、[参照（Browse）] をクリックして、ローカル ファイル名を入力します。

ステップ 3 [サーバ名（Server Name）] テキスト ボックスに TFTP サーバ名を入力します。デフォルトは Prime Infrastructure サーバです。

ステップ 4 サーバの IP アドレスを入力します。

ステップ 5 [最大試行回数（Maximum Retries）] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 6 [タイムアウト（Time Out）] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 7 [Local File Name] テキスト ボックスに、証明書のディレクトリ パスを入力します。
ステップ 8 [サーバ ファイル名（Server File Name）] テキスト ボックスに、証明書の名前を入力します。
ステップ 9 [証明書のパスワード（Certificate Password）] テキスト ボックスにパスワードを入力します。
ステップ 10 [パスワードの確認（Confirm Password）] テキスト ボックスに上記のパスワードを再入力します。
ステップ 11 [OK] をクリックします。
ステップ 12 [証明書の再生成（Regenerate Cert）] をクリックして証明書を再生成します。

関連トピック

コントローラのトラップ レシーバの設定 （158 ページ）
コントローラ トラップの設定 （159 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （161 ページ）
コントローラでの Web 管理の設定 （163 ページ）
コントローラでのローカル管理ユーザの設定 （165 ページ）
コントローラの管理認証サーバ優先度の設定 （166 ページ）

コントローラでのローカル管理ユーザの設定

このページには、ローカル管理ユーザの名前やアクセス権限の一覧が表示されます。ローカル管理ユーザを削除することもできます。

[ローカル管理ユーザ（Local Management Users）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。
ステップ 2 該当するコントローラのデバイス名をクリックします。
ステップ 3 左側のサイドバーのメニューから、 **[管理（Management）] > [ローカル管理ユーザ（Local Management Users）]** を選択します。
ステップ 4 ユーザ名をクリックします。

- [ユーザ名（読み取り専用）（User Name (read-only)）] : ユーザの名前。
- [アクセス レベル（読み取り専用）（Access Level (read-only)）] : [読み取り/書き込み（Read Write）] または [読み取り専用（Read Only）]。

ステップ 5 ローカル管理ユーザを削除するには、ユーザのチェックボックスをオンにします。
ステップ 6 [コマンドの選択（Select a command）] ドロップリストから、[ローカル管理ユーザの削除（Delete Local Management Users）] を選択します。
ステップ 7 [移動（Go）] をクリックします。
ステップ 8 確認メッセージで [OK] をクリックします。

コントローラの管理認証サーバ優先度の設定

認証の優先度を設定して、コントローラの管理ユーザの認証に使用する認証サーバの順序を制御します。

[認証の優先度（Authentication Priority）]ページにアクセスするには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[ネットワーク（Network）]>[ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）]>[ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、[管理（Management）]>[認証の優先度（Authentication Priority）] の順に選択します。

ステップ 4 最初にローカル データベースが検索されます。RADIUS または TACACS+ のどちらかを次の検索対象に選択します。ローカルデータベースを使用した認証に失敗した場合に、コントローラは次の種類のサーバを使用します。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラのロケーション情報の設定

Wi-Fi クライアントは、プローブによる AP の検出を軽減する傾向を示しています。スマートフォンではバッテリの電力節約のためにこれを実行します。スマートフォンのアプリケーションはプローブ要求を生成できなくても、簡単にデータ パケットを生成できるため、アプリケーションの拡張ロケーションをトリガーできます。Hyperlocation は WLC 8.1MR および Prime Infrastructure から設定します。これはビーコン、インベントリ、個人のモバイルデバイスの位

置をかなり精密に特定します。一部のネットワークでは複数のアクセス ポイントを使用して精度が 5 ～ 7 m 以内の位置座標を取得しますが、Hyperlocation は 1 m 以内まで位置を追跡できます。

個々のコントローラのロケーションを設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[ロケーション（Location）] > [ロケーションの設定（Location Configuration）] を選択します。

[ロケーションの設定（Location Configuration）] ページには、[一般（General）] と [詳細設定（Advanced）] の 2 つのタブが表示されます。

ステップ 4 次の [一般（General）] パラメータを追加または変更します。

- [RFID タグ データ収集（RFID Tag Data Collection）]：タグでデータの収集を有効にするには、このチェックボックスをオンにします。

ロケーション サーバがコントローラからアセット タグ データを収集する前に、コントローラで CLI コマンド config rfid status enable を使用して、アクティブ RFID タグの検出を有効にする必要があります。

- [ロケーション パス損失設定（Location Path Loss Configuration）]
  - [調整クライアント（Calibrating Client）]：クライアントの調整を有効にするには、このチェックボックスをオンにします。コントローラは、クライアントを調整するために、アクセス ポイントを介して（クライアントの機能に応じて）通常の S36 または S60 要求を送信します。パケットは、すべてのチャネルで送信されます。すべてのアクセス ポイントが、それぞれの場所でクライアントから RSSI データを収集します。これらの追加送信およびチャネル変更によって、同時に発生する音声またはビデオ トラフィックの質が低下する場合があります。
  - [通常のクライアント（Normal Client）]：非調整クライアントを使用するには、このチェックボックスをオンにします。S36 要求はクライアントに送信されません。S36 が CCXv2 以降と互換性があるのに対し、S60 は CCXv4 以降と互換性があります。
- [測定通知間隔（秒単位）（Measurement Notification Interval (in secs)）]
  - [タグ、クライアント、不正 AP/クライアント（Tags, Clients, and Rogue APs/Clients）]：クライアント、タグ、および不正に関する NMSP 測定通知間隔を設定できます。見つかった要素（タグ、クライアント、および不正アクセス ポイントやクライアント）が通知されるまでの秒数を指定します。

コントローラでこの値を設定すると、[サーバの同期（Synchronize Servers）] ページで表示できる同期外れ通知が生成されます。コントローラと Mobility Services Engine 間に別の測定間隔が存在する場合、2 つの設定のうち最長の間隔設定が Mobility Services Engine によって採用されます。

このコントローラが Mobility Services Engine と同期されると、Mobility Services Engine で新しい値が設定されます。測定通知間隔に変更を行う場合は、Mobility Services Engine に同期する必要があります。

- [RSS 失効タイムアウト（秒単位）（RSS Expiry Timeout (in secs)）]
  - [クライアント用（For Clients）]：通常の（非調整）クライアントの RSSI 測定を廃棄するまでの秒数を入力します。
  - [調整クライアント用（For Calibrating Clients）]：調整クライアントの RSSI 測定を廃棄するまでの秒数を入力します。
  - [タグ用（For Tags）]：タグの RSSI 測定を廃棄するまでの秒数を入力します。
  - [不正 AP 用（For Rogue APs）]：不正アクセス ポイントの RSSI 測定を廃棄するまでの秒数を入力します。

ステップ 5 次の [詳細設定（Advanced）] パラメータを追加または変更します。

- [RFID タグ データ タイムアウト（秒単位）（RFID Tag Data Timeout (in secs)）]：RFID タグ データ タイムアウトを設定するための値（秒単位）を入力します。
- [ロケーション パス損失設定（Location Path Loss Configuration）]
  - [調整クライアント マルチバンド（Calibrating Client Multiband）]：すべてのチャネルで S36 および S60 パケット（該当する場合）を送信するには、[有効（Enable）] チェックボックスをオンにします。調整クライアントは、[一般（general）] タブでも有効にする必要があります。使用可能なすべての無線（802.11a/b/g/n）を使用するには、マルチバンドを有効にする必要があります。
- [Hyperlocation 設定のパラメータ（Hyperlocation Config Parameters）]
  - [Hyperlocation]：このオプションを有効にすると、そのコントローラに関連付けられた Hyperlocation モジュールがあるすべての AP が有効になります。
  - [最小パケット検出 RSSI（Packet Detection RSSI Minimum）]：この値を調整して、位置計算から精度の低い RSSI 測定値を除外します。
  - [アイドル クライアント検出のスキャン カウントしきい値（Scan Count Threshold for Idle Client Detection）]：スキャン中に検出されるアイドル クライアントの最大許容数。
  - [NTP サーバの IP アドレス（NTP Server IP Address）]：有効な NTP サーバの IP アドレスを入力します。この IP アドレスは、時刻同期のためにすべての AP で使用されます。
  - 方位角角度：方位角の正しい値については、次の表を参照してください。

表 *2*：方位角の値

設置位置	矢印方向	方位角（単位：度）	垂直角（単位：度）
天井設置型	South	90	0（上）
東側の壁面に設置	East	[0]	90（下）
南側の壁面に設置	South	90	90（下）
西側の壁面に設置	West	180	90（下）
北側の壁面に設置	North	270	90（下）
北側の壁面に対し 45 度	North	270	45（下）

ヒント　可能であれば、天井グリッド上に AP を設置し、AP の Hyperlocation 矢印を、すべて同じ方向を指すように合わせます。推奨事項は、デフォルトの方向に AP を設置することです。

ステップ 6　[保存（Save）] をクリックします。

関連トピック

コントローラの管理パラメータの設定 （158 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （169 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （171 ページ）
デバイスのメッシュ パラメータの設定 （152 ページ）
デバイスのポート パラメータの設定 （156 ページ）
コントローラのマルチキャスト DNS（mDNS）設定の構成 （175 ページ）
コントローラの Application Visibility and Control（AVC）パラメータの設定 （177 ページ）
コントローラの NetFlow 設定の構成 （179 ページ）

コントローラの IPv6 ネイバー バインドと RA パラメータの設定

IPv6はネイバーバインディングタイマーおよびルータアドバタイズメント（RA）のパラメータを使用して設定できます。

関連トピック

コントローラのネイバー バインド タイマーの設定 （169 ページ）
コントローラでのルータ アドバタイズメント スロットリングの設定 （170 ページ）
コントローラでの RA ガードの設定 （171 ページ）

コントローラのネイバー バインド タイマーの設定

ネイバー バインディング タイマーを設定するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2　該当するコントローラのデバイス名をクリックします。

ステップ 3　左側のサイドバーのメニューから、**[IPv6] > [ネイバーバインディングタイマー（Neighbor Binding Timers）]** を選択します。

ステップ 4　適用されるテンプレートが表示されます。次のパラメータを追加または変更します。

- [ダウン ライフタイム間隔（Down Lifetime Interval）]：これは最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。
- [到達可能ライフタイム間隔（Reachable Lifetime Interval）]：これは最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。

- [ステイル ライフタイム間隔（Stale Lifetime Interval）]：これは最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。

ステップ 5 [保存（Save）] をクリックします。

コントローラでのルータ アドバタイズメント スロットリングの設定

[RA スロットル ポリシー（RA Throttle Policy）] を使用すると、ワイヤレス ネットワークで循環するマルチキャスト ルータ アドバタイズメント（RA）の量を制限できます。

[RA スロットル ポリシー（RA Throttle Policy）] を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[IPv6] > [RA スロットル ポリシー（RA Throttle Policy）]** を選択します。

ステップ 4 RA スロットル ポリシーを有効にするには、[有効（Enable）] チェックボックスをオンにし、次のパラメータを設定します。

- [スロットル期間（Throttle Period）]：スロットル期間（秒単位）。範囲は 10 ～ 86,400 秒です。
- [最大通過数（Max Through）]：ある期間または無制限の期間にわたって通過する RA の数。[無制限（No Limit）] チェックボックスがオフになっている場合、最大パススルー数を指定できます。
- [間隔オプション（Interval Option）]：RA で間隔オプションが指定されている場合の動作を示します。
  - [無視（Ignore）]
  - [パススルー（Passthrough）]
  - [スロットル（Throttle）]
- [許容される最小数（Allow At-least）]：ルータ単位で抑制されない RA の最小数を示します。
- [許容される最大数（Allow At-most）]：ルータ単位で抑制されない RA の最大数または無制限数を示します。[無制限（No Limit）] チェックボックスがオフになっている場合、ルータ単位で抑制されない RA の最大数を指定できます。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラのネイバー バインド タイマーの設定 （169 ページ）
コントローラでの RA ガードの設定 （171 ページ）

コントローラでの RA ガードの設定

RA ガードは、ワイヤレス クライアントから RA をドロップするための Unified Wireless のソリューションです。これはグローバルに設定され、デフォルトで有効です。[IPv6 ルータ アドバタイズメント（IPv6 Router Advertisement）] パラメータを設定できます。

RA ガードを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[IPv6] > [RA ガード（RA Guard）]** を選択します。

ステップ 4 [ルータ アドバタイズメント ガード（Router Advertisement Guard）] を有効にするには、[有効（Enable）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラのネイバー バインド タイマーの設定 （169 ページ）
コントローラでのルータ アドバタイズメント スロットリングの設定 （170 ページ）

コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定

プロキシ モバイル IPv6 は、任意の IP モビリティ関連シグナリングでモバイル ノードのプロキシとして動作することによってモバイル ノードをサポートする、ネットワーク ベースのモバイル管理プロトコルです。ネットワークのモビリティ エンティティは、モバイル ノードの移動を追跡し、モビリティ シグナリングを起動して必要なルーティング状態を設定します。

主要な機能エンティティは、ローカルモビリティ アンカー（LMA）とモバイルアクセス ゲートウェイ（MAG）です。LMA はモバイル ノードの到達可能性状態を維持し、モバイル ノードの IP アドレス用のトポロジ アンカー ポイントになります。MAG はモバイル ノードの代わりにモビリティ管理を行います。MAGはモバイル ノードがアンカーされているアクセス リンクに存在します。コントローラは MAG 機能を実装します。

関連トピック

コントローラでの PMIP グローバル パラメータの設定 （172 ページ）
コントローラでの PMIP ローカル モビリティ アンカーの設定 （173 ページ）
コントローラでの PMIP プロファイルの設定 （173 ページ）

コントローラでの PMIP グローバル パラメータの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[[PMIP] > [グローバル設定（Global Config）]** を選択します。

ステップ 4 次のフィールドを設定します。

- [ドメイン名（Domain Name）]：読み取り専用。
- [MAG 名（MAG Name）]：読み取り専用。
- [MAG インターフェイス（MAG Interface）]：読み取り専用。
- [許可される最大バインディング数（Maximum Bindings Allowed）]：コントローラが MAG に送信できるバインディング アップデートの最大数。有効な範囲は 0 ～ 40000 です。
- [バインディング ライフタイム（Binding Lifetime）]：コントローラのバインディング エントリのライフタイム。有効な範囲は 10 ～ 65535 秒です。デフォルト値は 65535 です。バインディング ライフタイムは 4 秒の倍数であることが必要です。
- [バインディング リフレッシュ時間（Binding Refresh Time）]：コントローラのバインディング エントリのリフレッシュ時間。有効な範囲は 4 ～ 65535 秒です。デフォルト値は 300 秒です。バインディング リフレッシュ時間は 4 秒の倍数であることが必要です。
- [バインディング初期試行タイムアウト（Binding Initial Retry Timeout）]：コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシバインディング アップデート（PBU）間の初期タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 1000 秒です。
- [バインディング最大試行タイムアウト（Binding Maximum Retry Timeout）]：コントローラがプロキシバインディング確認（PBA）を受信しない場合のプロキシバインディング アップデート（PBU）間の最大タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 32000 秒です。
- [リプレイ保護タイムスタンプ（Replay Protection Timestamp）]：受信したプロキシ バインディング確認のタイムスタンプと現在の日時との時間差の上限。有効範囲は 1 ～ 255 ミリ秒です。デフォルト値は、7 ミリ秒です。
- [最小 BRI 再送信タイムアウト（Minimum BRI Retransmit Timeout）]：コントローラが BRI メッセージを再送信するまでに待機する時間の最小値。有効な範囲は 500 ～ 65535 秒です。
- [最大 BRI 再送信タイムアウト（Maximum BRI Retransmit Timeout）]：コントローラが Binding Revocation Indication（BRI）メッセージを再送信するまでに待機する時間の最大値。有効な範囲は 500 ～ 65535 秒です。デフォルト値は 2000 秒です。
- [BRI 再試行回数（BRI Retries）]：BRI の再試行回数。
- [MAG APN]：MAG のアクセス ポイント ノードの名前。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （171 ページ）
コントローラでの PMIP ローカル モビリティ アンカーの設定 （173 ページ）
コントローラでの PMIP プロファイルの設定 （173 ページ）

コントローラでの PMIP ローカル モビリティ アンカーの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[PMIP] > [LMA 設定（LMA Config）]** を選択します。

ステップ 4 次のフィールドを設定します。

- [LMA 名（LMA Name）]：コントローラに接続された LMA の名前。
- [LMA IP アドレス（LMA IP Address）]：コントローラに接続された LMA の IP アドレス。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 LMA 設定を削除するには、該当する LMA 設定のチェックボックスをオンにします。

ステップ 7 [コマンドの選択（Select a command）] ドロップリストから、[PMIP ローカル設定の削除（Delete PMIP Local Configs）] を選択します。

ステップ 8 [実行（Go）] をクリックします。

ステップ 9 確認メッセージで [OK] をクリックします。

関連トピック

コントローラでの PMIP グローバル パラメータの設定 （172 ページ）
コントローラでの PMIP プロファイルの設定 （173 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （171 ページ）

コントローラでの PMIP プロファイルの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[PMIP] > [PMIP プロファイル（PMIP Profile）] を選択します。

ステップ 4 プロファイル名を入力します。

ステップ 5 [追加（Add）] をクリックし、次のフィールドを設定します。

- [ネットワーク アクセス識別子（Network Access Identifier）]：プロファイルに関連付けられたネットワーク アクセス識別子（NAI）の名前。
- [LMA 名（LMA Name）]：プロファイルを関連付ける LMA の名前。
- [アクセス ポイント ノード（Access Point Node）]：コントローラに接続されているアクセス ポイント ノードの名前。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 PMIP プロファイルを削除するには、必要な PMIP プロファイルのチェックボックスをオンにします。

ステップ 8 [コマンドの選択（Select a command）] ドロップリストから、[PMIP ローカル設定の削除（Delete PMIP Local Configs）] を選択します。

ステップ 9 [実行（Go）] をクリックします。

ステップ 10 確認メッセージで [OK] をクリックします。

関連トピック

コントローラでの PMIP グローバル パラメータの設定 （172 ページ）
コントローラでの PMIP ローカル モビリティ アンカーの設定 （173 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （171 ページ）

コントローラの EoGRE トンネリングの設定

Ethernet over GRE（EoGRE）は、ホットスポットから Wi-Fi トラフィックを集約するための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）デバイスがエンドホストから着信するイーサネット トラフィックをブリッジし、そのトラフィックを IP GRE トンネルを介してイーサネット 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 プロバイダーのブロードバンド ネットワーク ゲートウェイで終わる場合、エンド ホストのトラフィックは終了し、サブスクライバ セッションがエンド ホスト用に開始します。

EoGRE トンネリングを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[トンネリング（Tunneling）] > [EoGRE]** を選択します。

ステップ 4 [インターフェイス名（Interface Name）] ドロップダウン リストから、トンネルする送信元インターフェイスを選択します。

ステップ 5 トンネル ゲートウェイを作成するには、次の手順を実行します。

- [Heartbeat Interval] を設定します。デフォルト インターバルは 60 秒です。

- [最大ハートビート スキップ数（Max Heartbeat Skip Count）] を設定します。デフォルト値は 3 に設定されています。3 回のキープアライブ ping 後にトンネル ゲートウェイ（TWG）が応答しない場合、Cisco WLC はその TGW を非稼働とマークします。スキップ カウントの数値は、TGW が非稼働であると Cisco WLC が判断するまでに、TGW がスキップできる連続した応答の回数を決定します。
- [トンネル ゲートウェイ（Tunnel Gateway）] で、[行の追加（Add Row）] をクリックします。このようなゲートウェイを 10 個作成できます。
  1. [トンネル ゲートウェイ名（Tunnel Gateway Name）] フィールドにトンネル ゲートウェイの名前を入力します。
  2. [トンネル IP アドレス（Tunnel IP Address）] フィールドにトンネルの IP アドレスを入力します。IPv4 および IPv6 の両方のアドレス形式がサポートされています。
  3. [保存（Save）] をクリックします。

     デフォルトのトンネル タイプは EoGRE です。
  4. [ステータス（Status）] は収集したトラップに応じて [アップ（UP）] または [ダウン（DOWN）] になります。
- [ドメイン（Domain）] の下にある [行の追加（Add Row）] をクリックして、ドメインを設定します（ドメインは、2 つのトンネル ゲートウェイのグループです）。
  1. [ドメイン名（Domain Name）] テキスト ボックスに、ドメイン名を入力します。
  2. [プライマリ ゲートウェイ（Primary Gateway）] ドロップダウン リストから、プライマリ トンネル ゲートウェイを選択します。
  3. [セカンダリ ゲートウェイ（Secondary Gateway）] ドロップダウン リストから、セカンダリ トンネル ゲートウェイを選択します。

ステップ 6 [保存（Save）] をクリックします。

コントローラのマルチキャスト DNS（mDNS）設定の構成

マルチキャスト DNS（mDNS）サービス検出では、ローカル ネットワーク上のサービスをアナウンスし、検出するための手段を提供します。mDNS は、IP マルチキャストで DNS クエリを実行し、ゼロ コンフィギュレーション IP ネットワーキングをサポートしています。

コントローラが mDNS サービスについて学習し、すべてのクライアントにこれらのサービスをアドバタイズできるように mDNS を設定できます。

mDNS には [サービス（Services）] と [プロファイル（Profiles）] の 2 つのタブがあります。

- [サービス（Services）] タブ：このタブでは、グローバル mDNS パラメータを設定し、Master Services データベースを更新できます。
- [プロファイル（Profiles）] タブ：このタブでは、コントローラに設定されている mDNS プロファイルを表示し、新しい mDNS プロファイルを作成できます。新しいプロファイ

ルを作成した後、インターフェイス グループ、インターフェイス、または WLAN にプロファイルをマッピングする必要があります。クライアントはプロファイルに関連付けられたサービスのみのサービス アドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマッピングされます。デフォルトで、コントローラにはmDNSプロファイル default-mdns-profile があります。これは削除できません。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[mDNS] > [mDNS] の順に選択します。

ステップ 4 [サービス（Services）] タブで、次のパラメータを設定します。

- [適用されるテンプレート（Template Applied）] : このコントローラに適用されるテンプレートの名前。
- [mDNS グローバル スヌーピング（mDNS Global Snooping）] : mDNS パケットのスヌーピングを有効にするチェックボックス。mDNS スヌーピングを有効にしても、コントローラは IPv6 mDNS パケットをサポートしません。
- [クエリ間隔（Query Interval）]（10 ～ 120）：ユーザが設定できる mDNS クエリ間隔（分単位）。この間隔は、WLC によって、サービス アドバタイズメントを自動的に送信しないサービスに対して、そのサービスが開始された後に定期的なmDNSクエリ メッセージを送信するために使用されます。範囲は、10 ～ 120 分です。デフォルト値は 15 分です。
- [マスター サービス（Master Services）] : [行の追加（Add Row）] をクリックし、次のフィールドを設定します。
  - [マスター サービス名（Master Service Name）] : ドロップダウン リストから、照会可能なサポートされているサービスを選択できます。新しいサービスを追加するには、サービス名を入力または選択し、そのサービス文字列を入力して、サービス ステータスを選択します。次のサービスを使用できます。
  - AirTunes
  - AirPrint
  - AppleTV
  - HP Photosmart Printer1
  - HP Photosmart Printer2
  - Apple File Sharing Protocol（AFP）
  - スキャナ
  - プリンタ
  - FTP
  - iTunes Music Sharing
  - iTunes Home Sharing
  - iTunes Wireless Device Syncing
  - Apple Remote Desktop
  - Apple CD/DVD Sharing

- Time Capsule Backup

- [マスター サービス名（Master Service Name）]：mDNS サービスの名前。
- [サービス文字列（Service String）]：mDNS サービスに関連付けられた一意の文字列。たとえば、_airplay._tcp.local. は、AppleTV に関連付けられたサービス文字列です。
- [クエリ ステータス（Query Status）]：サービスの mDNS クエリを有効にするために選択するチェックボックス。定期的な mDNS クエリ メッセージは、クエリのステータスが有効な場合だけ、WLC によって、サービスに対して設定されたクエリ間隔で送信されます。それ以外の場合、サービスは、クエリのステータスが無効になっているその他のサービス（たとえば AppleTV）に自動的にアドバタイズする場合があります。

ステップ 5 [プロファイル（Profiles）] タブで、次のパラメータを設定します。

- [プロファイル（Profiles）]：[プロファイルの追加（Add Profile）] をクリックし、次のフィールドを設定します。
  - [プロファイル名（Profile Name）]：mDNS プロファイルの名前。最大 16 個のプロファイルを作成できます。
  - [サービス（Services）]：mDNS プロファイルにマップするサービスを選択します（チェックボックスを使用）。
- [編集（Edit）] および [削除（Delete）] をそれぞれクリックすると、既存のプロファイルを編集または削除できます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

デフォルトでは、コントローラによってアクセス ポリシー default-mdns-policy が作成されます。これは削除できません。これには、[グループ名（Group Name）] および [説明（Description）] が表示されます。[サービス グループ（Service Group）] の詳細を表示するポリシーを選択します。

フィールドを編集して、[保存（Save）] をクリックします。

コントローラの Application Visibility and Control（AVC）パラメータの設定

Application Visibility and Control（AVC）は、Network Based Application Recognition（NBAR）ディープ パケット インスペクション テクノロジーを使用して、使用するプロトコルに基づいてアプリケーションを分類します。AVC を使用して、コントローラはレイヤ 4 ～レイヤ 7 の 1400 を超えるプロトコルを検出できます。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、コストの掛かるネットワーク 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することができるようになります。

AVC は、Cisco 2500 および 5500 シリーズ コントローラ、Cisco Flex 7500 および Cisco 8500 シリーズ コントローラでだけサポートされています。

コントローラでの AVC プロファイルの設定

AVC プロファイルを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility and Control）] > [AVC プロファイル（AVC Profile）]** を選択します。

ステップ 4 設定する AVC プロファイル名をクリックします。

ステップ 5 AVC ルールを作成するには、[追加（Add）] をクリックします。

ステップ 6 次のパラメータを設定します。

- [アプリケーション名（Application Name）]：アプリケーションの名前。
- [アプリケーション グループ名（Application Group Name）]：アプリケーションが属するアプリケーション グループの名前。
- [アクション（Action）]：ドロップダウン リストから、次の項目を選択できます。
  - [ドロップ（Drop）]：選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをドロップします。
  - [マーク（Mark）]：[DiffServ コードポイント（DSCP）（Differentiated Services Code Point (DSCP)）] ドロップダウン リストで指定する DSCP 値と選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをマークします。DSCP 値を使用して、QoS レベルに基づいて差別化サービスを提供できます。
  - [レート制限（Rate Limit）]：アクションとして [レート制限（Rate Limit）] を選択すると、クライアント 1 台あたりの平均レート制限とバースト データ レート制限を指定できます。レート制限アプリケーションの数は 3 に制限されています。デフォルト アクションは、すべてのアプリケーションを許可します。
- [DSCP]：インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コード。DSCP 値は次の QoS レベルにマッピングされます。
  - [プラチナ（音声）（Platinum (Voice)）]：Voice over Wireless の高い QoS を保証します。
  - [ゴールド（ビデオ）（Gold (Video)）]：高品質のビデオ アプリケーションをサポートします。
  - [シルバー（ベスト エフォート）（Silver (Best Effort)）]：クライアントの通常の帯域幅をサポートします。
  - [ブロンズ（バックグラウンド）（Bronze (Background)）]：ゲスト サービス用の最小の帯域幅を提供します。
  - [カスタム（Custom）]：DSCP 値を指定します。指定できる範囲は 0 ～ 63 です。

- [DSCP 値（DSCP Value）]：この値は、[DSCP] ドロップダウン リストで [カスタム（Custom）] を選択した場合にのみ入力できます。
- 平均レート制限（Kbps）（Avg. Rate Limit (in Kbps)）]：アクションとして [レート制限（Rate Limit）] を選択した場合は、そのアプリケーションの平均帯域幅制限である、クライアントごとの平均レート制限を指定できます。
- [バースト レート制限（Kbps）（Burst Rate Limit (in Kbps)）]：アクションに [レート制限（Rate Limit）] を選択した場合は、そのアプリケーションのピーク制限である、バースト レート制限を指定できます。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

コントローラのマルチキャスト DNS（mDNS）設定の構成 （175 ページ）
コントローラの NetFlow 設定の構成 （179 ページ）
デバイスのメッシュ パラメータの設定 （152 ページ）
デバイスのポート パラメータの設定 （156 ページ）
コントローラの管理パラメータの設定 （158 ページ）
コントローラのロケーション情報の設定 （166 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （169 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （171 ページ）

コントローラの NetFlow 設定の構成

NetFlow は、ネットワーク デバイスから IP トラフィック情報を収集することで、ネットワーク ユーザとアプリケーション、ピーク時の使用時間、およびトラフィック ルーティングに関する貴重な情報を提供するプロトコルです。NetFlow アーキテクチャは、次のコンポーネントで構成されています。

- コレクタ：さまざまなネットワーク要素から IP トラフィック情報をすべて収集するエンティティ。
- エクスポータ：IP トラフィック情報を使用してテンプレートをエクスポートするネットワーク エンティティ。コントローラは、エクスポータとして機能します。

コントローラでの NetFlow モニタの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[NetFlow] > [モニタ（Monitor）]** を選択します。

ステップ 4 次のパラメータを設定します。

- [モニタ名（Monitor Name）]：NetFlow モニタの名前。モニタ名は最大 127 文字の英数字で、大文字と小文字を区別します。コントローラでは 1 つのみモニタを設定できます。
- [レコード名（Record Name）]：NetFlow レコードの名前。コントローラの NetFlow レコードには、特定のフロー内のトラフィックに関する次の情報が含まれます。
  - クライアント MAC アドレス
  - クライアント送信元 IP アドレス
  - WLAN ID
  - アプリケーション ID（Application ID）
  - データの着信バイト数
  - データの発信バイト数
  - 着信パケット
  - 発信パケット
  - 着信 DSCP
  - 発信 DSCP
  - 最後の AP の名前

ステップ 5 [エクスポータ名（Exporter Name）]：エクスポータの名前。コントローラでは 1 つのみモニタを設定できます。

ステップ 6 [エクスポータ IP（Exporter IP）]：コレクタの IP アドレス。

ステップ 7 [ポート番号（Port Number）]：NetFlow レコードをコントローラからエクスポートする UDP ポート。

ステップ 8 [保存（Save）] をクリックします。

コントローラでの NetFlow エクスポータの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[NetFlow] > [エクスポータ（Exporter）]** を選択します。

ステップ 4 次のパラメータを設定します。

- [エクスポータ名（Exporter Name）]：エクスポータの名前。
- [エクスポータ IP（Exporter IP）]：エクスポータの IP アドレス。

- [ポート番号（Port Number）]：NetFlow レコードをエクスポートする UDP ポート。

関連トピック

コントローラのマルチキャスト DNS（mDNS）設定の構成 （175 ページ）
コントローラの NetFlow 設定の構成 （179 ページ）
デバイスのメッシュ パラメータの設定 （152 ページ）
デバイスのポート パラメータの設定 （156 ページ）
コントローラの管理パラメータの設定 （158 ページ）
コントローラのロケーション情報の設定 （166 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （169 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （171 ページ）

サードパーティ製コントローラまたはアクセスポイントの設定

Cisco Prime Infrastructure では、サードパーティのコントローラおよびアクセス ポイントを追加することができます。この機能の一部として、次の機能を実行できます。

- Cisco Prime Infrastructure にサードパーティのコントローラを追加します。
- サードパーティのコントローラの状態をモニタします。
- サードパーティのコントローラと、関連付けされたアクセス ポイントのインベントリ情報を取得します。
- サードパーティのコントローラおよびアクセス ポイントの動作ステータスを表示するには、バックグラウンド タスクを使用します。

関連トピック

サードパーティ製コントローラの追加 （181 ページ）
サードパーティ製コントローラの動作ステータスの表示 （182 ページ）
サードパーティ アクセス ポイントの設定の表示 （183 ページ）
サードパーティ アクセス ポイントの削除 （184 ページ）
サードパーティ製コントローラの動作ステータスの表示 （182 ページ）

サードパーティ製コントローラの追加

サードパーティのコントローラを追加するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] > [サードパーティワイヤレスコントローラ（Third Party Wireless Controllers）] を選択します。

ステップ 2 [デバイスの追加（Add Device）] をクリックします。

ステップ 3 [デバイスの追加（Add Device）] ページの次のタブで必須パラメータを入力します。

- 一般
- SNMP
- [Telnet/SSH]
- [HTTP/HTTPS]
- IPSec

ステップ 4 [追加（Add）] をクリックします。

関連トピック

サードパーティ製コントローラの動作ステータスの表示 （182 ページ）
サードパーティ アクセス ポイントの設定の表示 （183 ページ）
サードパーティ アクセス ポイントの削除 （184 ページ）
サードパーティ製コントローラの動作ステータスの表示 （182 ページ）

サードパーティ製コントローラの動作ステータスの表示

[サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] ページを表示するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [バックグラウンドタスク（Background Tasks）]** の順に選択します。

ステップ 2 このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] チェックボックスをオンにします。[コマンドの選択（Select a command）] ドロップダウン リストから、[今すぐ実行（Execute Now）] を選択し、[実行（Go）] をクリックします。[有効（Enabled）] 列にステータス変更が表示されます。

- タスクを有効にする。

  [サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] チェックボックスをオンにします。[コマンドの選択（Select a command）] ドロップダウン リストから、[タスクを有効にする（Enable Tasks）] を選択し、[実行（Go）] をクリックします。[有効（Enabled）] 列のタスクが灰色から使用可能な状態に変わります。

- タスクを無効にする。

  [サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] チェックボックスをオンにします。[コマンドの選択（Select a command）] ドロップダウン リストから、[タスクを無効にする（Disable Tasks）] を選択し、[実行（Go）] をクリックします。無効化が完了すると、[有効（Enabled）] 列のタスクが灰色になります。

ステップ 3 タスクを変更するには、[バックグラウンド タスク（Background Tasks）] 列の [サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] リンクをクリックします。

[サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] ページには、最終実行情報が表示されます。

- 開始時刻。
- 終了時間。
- タスクの経過時間（秒）。
- 結果（成功またはエラー）。
- メッセージ（このタスクに関するテキスト メッセージ）。

ステップ 4 [タスクの詳細（Task Details）] セクションで、次の項目を表示または編集します。

- [説明（Description）]：表示のみ。タスクの名前を表示します。
- [有効（Enabled）]：チェックボックスをオンにすると、このタスクが有効になります。
- [間隔（Interval）]：タスクの頻度（分）を示します。デフォルトは 3 時間です。

ステップ 5 完了したら、[保存（Save）] をクリックしてタスクの変更を確定します。

関連トピック

サードパーティ製コントローラの追加 （181 ページ）
サードパーティ アクセス ポイントの設定の表示 （183 ページ）
サードパーティ アクセス ポイントの削除 （184 ページ）

サードパーティ アクセス ポイントの設定の表示

サードパーティのアクセスポイントは、サードパーティのコントローラを追加すると検出されます。

サードパーティのアクセス ポイントの設定を表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク デバイス（Network Devices）] > [サードパーティのアクセス ポイント（Third Party Access Points）]** を選択します。

ステップ 2 詳細を表示する AP 名のリンクをクリックします。そのサードパーティのアクセス ポイントの [一般（General）] タブが表示されます。

関連トピック

サードパーティ製コントローラの追加 （181 ページ）
サードパーティ製コントローラの動作ステータスの表示 （182 ページ）
サードパーティ アクセス ポイントの削除 （184 ページ）

サードパーティ製コントローラの動作ステータスの表示 （182 ページ）

サードパーティ アクセス ポイントの削除

サードパーティのアクセス ポイントを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク デバイス（Network Devices）] > [サードパーティのアクセス ポイント（Third Party Access Points）]** を選択します。

ステップ 2 削除するアクセス ポイントのチェックボックスをオンにします。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 確認メッセージが表示されます。

ステップ 5 [はい（Yes）] をクリックします。

関連トピック

サードパーティ製コントローラの追加 （181 ページ）
サードパーティ製コントローラの動作ステータスの表示 （182 ページ）
サードパーティ アクセス ポイントの設定の表示 （183 ページ）
サードパーティ製コントローラの動作ステータスの表示 （182 ページ）

サードパーティ アクセス ポイントの動作ステータスの表示

[サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] ページを表示するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [バックグラウンドタスク（Background Tasks）]** の順に選択します。

ステップ 2 このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] チェックボックスをオンにします。[コマンドの選択（Select a command）] ドロップダウン リストから、[今すぐ実行（Execute Now）] を選択し、[実行（Go）] をクリックします。[有効（Enabled）] 列にステータス変更が表示されます。

- タスクを有効にする。

  [サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] チェックボックスをオンにします。[コマンドの選択（Select a command）] ドロップダウン リストから、[タスクを有効にする（Enable Tasks）] を選択し、[実行（Go）] をクリックします。[有効（Enabled）] 列のタスクが灰色から使用可能な状態に変わります。

- タスクを無効にする。

[サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] チェックボックスをオンにします。[コマンドの選択（Select a command）] ドロップダウン リストから、[タスクを無効にする（Disable Tasks）] を選択し、[実行（Go）] をクリックします。無効化が完了すると、[有効（Enabled）] 列のタスクが灰色になります。

ステップ 3 タスクを変更するには、[バックグラウンド タスク（Background Tasks）] 列の [サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] リンクをクリックします。

[サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] ページには、最終実行情報が表示されます。

- 開始時刻。
- 終了時間。
- タスクの経過時間（秒）。
- 結果（成功またはエラー）。
- メッセージ（このタスクに関するテキスト メッセージ）。

ステップ 4 [タスクの編集（Edit Task）] グループ ボックスで、次の項目を表示または編集します。

- [説明（Description）]：表示のみ。タスクの名前を表示します。
- [有効（Enabled）]：チェックボックスをオンにすると、このタスクが有効になります。
- [間隔（Interval）]：タスクの頻度（分）を示します。デフォルトは 3 時間です。

ステップ 5 完了したら、[保存（Save）] をクリックしてタスクの変更を確定します。

関連トピック

サードパーティ製コントローラの追加 （181 ページ）
サードパーティ製コントローラの動作ステータスの表示 （182 ページ）
サードパーティ アクセス ポイントの設定の表示 （183 ページ）
サードパーティ アクセス ポイントの削除 （184 ページ）

スイッチ設定の表示

Cisco Prime Infrastructure データベースのすべてのスイッチのサマリーを表示するには、**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] > [デバイスタイプ（Device Type）] > [スイッチおよびハブ（Switches and Hubs）]** を選択します。任意の列見出しをクリックして、その列で情報をソートします。列見出しを複数回クリックすることで、昇順のソートと降順のソートを切り替えることができます。

関連トピック

スイッチの詳細の表示 （186 ページ）

スイッチの詳細の表示

Cisco Prime Infrastructure データベースのすべてのスイッチのサマリーを表示するには、**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** > **[デバイスタイプ（Device Type）]** > **[スイッチおよびハブ（Switches and Hubs）]** を選択します。デバイス名をクリックすると、そのスイッチの詳細情報が表示されます。

関連トピック

例：スイッチでの SNMPv3 の設定 （188 ページ）

スイッチの SNMP パラメータの変更

スイッチの SNMP パラメータを変更するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチおよびハブ（Switches and Hubs）] を選択して、SNMP クレデンシャルを変更するスイッチの横にあるチェックボックスをクリックします。

ステップ 2 [編集（Edit）] をクリックします。

ステップ 3 必要な [SNMP パラメータ（SNMP Parameters）] フィールドを変更して、次のいずれかをクリックします。

- [リセット（Reset）]：以前に保存したパラメータを復元します。
- [保存（Save）]：行った変更を保存して適用します。
- [キャンセル（Cancel）]：変更を保存せずに終了して、前の画面に戻ります。

関連トピック

スイッチ設定の表示 （185 ページ）
例：スイッチでの SNMPv3 の設定 （188 ページ）
スイッチの Telnet/SSH クレデンシャルの変更 （186 ページ）

スイッチの Telnet/SSH クレデンシャルの変更

スイッチの Telnet または SSH パラメータを変更するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチおよびハブ（Switches and Hubs）] を選択して、Telnet または SSH クレデンシャルを変更するスイッチの横にあるチェックボックスをクリックします。

ステップ 2 [編集（Edit）] をクリックします。

ステップ 3 必要な [Telnet/SSH パラメータ（Telnet/SSH Parameters）] フィールドを変更して、次のいずれかをクリックします。

- [リセット（Reset）]：以前に保存したパラメータを復元します。

- [保存（Save）]：行った変更を保存して適用します。
- [キャンセル（Cancel）]：変更を保存せずに終了して、前の画面に戻ります。

関連トピック

スイッチ設定の表示 （185 ページ）
例：スイッチでの SNMPv3 の設定 （188 ページ）
スイッチの SNMP パラメータの変更 （186 ページ）

スイッチの追加

スイッチを Prime Infrastructure データベースに追加して、全体的なスイッチ ヘルスとエンドポイントのモニタを表示し、スイッチポート トレースを実行できます。次のスイッチを設定できます。

- 3750
- 3560
- 3750E
- 3560E
- 2960

Prime Infrastructure の設定メニューにスイッチ機能が表示されますが、 Prime Infrastructure を使用してスイッチ機能を設定することはできません。設定できるのは Prime Infrastructure システムのみです。

Prime Infrastructure では、次を実行できます。

- [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] ページでスイッチを追加し、CLI および SNMP クレデンシャルを指定します。
- Mobility Services Engine と Prime Infrastructure によって有線クライアントを追跡するために、[設定（Configuration）]>[ネットワーク（Network）]>[ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] ページでロケーション対応スイッチを追加します。
- [モニタ（Monitor）]>[ネットワーク デバイス（Network Devices）] を選択してスイッチをモニタします。
- [レポート（Reports）] メニューを使用してスイッチ関連レポートを実行します。

Prime Infrastructure データベースにスイッチを追加すると、デフォルトでは、 Prime Infrastructure はスイッチの SNMP クレデンシャルを検査します。デバイスのクレデンシャルが正しくない場合、SNMP 失敗メッセージが表示されますが、スイッチは Prime Infrastructure データベースに追加されます。

スイッチ タイプ別に使用可能な機能

Prime Infrastructure にスイッチを追加する場合は、スイッチの管理方法を指定します。これに基づいて、 Prime Infrastructure は使用できる機能を判別します。

- [モニタ対象スイッチ（Monitored switches）]：スイッチを追加（[設定（Configuration）]>[ネットワーク（Network）]>[ネットワーク デバイス（Network Devices）]>[デバイス タイプ（Device Type）]>[ワイヤレス コントローラ（Wireless Controller）] を選択）して、スイッチの動作をモニタ（[モニタ（Monitor）]>[ネットワーク デバイス（Network Devices）] を選択）できます。それぞれのスイッチは、ライセンスの合計デバイス数に対して 1 つのデバイスとしてカウントされます。ライセンスエンジンで使用可能な未使用のデバイス数がある場合は、スイッチを Prime Infrastructure に追加できます。使用可能なデバイス数が残っていない場合は、別のスイッチを Prime Infrastructure に追加できません。
- [スイッチ ポート トレーシング（SPT）専用スイッチ（Switch Port Tracing (SPT) only switches）]：スイッチは、スイッチ ポート トレースのみを実行します。SPT 専用スイッチは、[設定（Configuration）]>[ネットワーク（Network）]>[ネットワーク デバイス（Network Devices）]>[デバイス タイプ（Device Type）]>[スイッチおよびハブ（Switches and Hubs）] ページとインベントリ レポートに表示されます。ライセンスは SPT スイッチには適用されません。

スイッチを Prime Infrastructure に追加するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[ネットワーク（Network）]>[ネットワーク デバイス（Network Devices）]>[デバイス タイプ（Device Type）]>[スイッチおよびハブ（Switches and Hubs）] を選択し、[デバイスの追加（Add Device）] をクリックします。

ステップ 2 表示されるフィールドに適切な情報を入力します。

詳細については、『Cisco Pime Infrastrucutre Reference Guide』を参照してください。

ステップ 3 [追加（Add）] をクリックしてスイッチを追加するか、[キャンセル（Cancel）] をクリックして操作をキャンセルし、スイッチのリストに戻ります。

関連トピック

CSV ファイルからのスイッチのインポート （189 ページ）
例：スイッチでの SNMPv3 の設定 （188 ページ）

例：スイッチでの SNMPv3 の設定

次に、スイッチでの SNMPv3 の設定例を示します。

snmp-server view v3default iso includedsnmp-server group v3group v3 auth write v3default
snmp-server user <username> <v3group> v3 auth <md5 or sha> <authentication password>

スイッチに VLAN がある場合、各 VLAN を設定する必要があります。設定しないと、スイッチ ポート トレーシングは失敗します。次に、スイッチに VLAN 1 および 20 がある場合の例を示します。

snmp-server group v3group v3 auth context vlan-1 write v3defaultsnmp-server group v3group v3 auth context vlan-20 write v3default

snmp-server group v3group v3 auth context vlan-20 write v3default

SNMP v3 ビューの作成時に、すべての OID を含めてください。

関連トピック

CSV ファイルからのスイッチのインポート （189 ページ）

CSV ファイルからのスイッチのインポート

CSV ファイルを使用してスイッチを Cisco Prime Infrastructure データベースにインポートできます。CSV ファイルの最初の行は、含まれている列の説明に使用されます。IP アドレス列は必須です。

次に、CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type,
 snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
16.1.1.3,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
16.1.1.4,255.255.255.0,v2,public,,,,,,3,10,ssh2,cisco,cisco,cisco,60
16.1.1.5,255.255.255.0,v2,public,,,,,,3,10,,cisco,cisco,cisco,60
16.1.1.6,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
3.3.3.3,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4
4.4.4.4,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4,telnet,cisco,cisco,cisco,60
```

[シビックロケーション（Civic Location）] ペインのフィールドは、シビック情報をインポートした後に読み込まれます。

詳細については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

関連トピック

スイッチの追加 （187 ページ）
例：スイッチでの SNMPv3 の設定 （188 ページ）

スイッチの削除

Prime Infrastructure データベースからスイッチを削除すると、次の機能が実行されます。

- そのスイッチのインベントリ情報が、データベースから削除されます。
- スイッチのアラームは、ステータスが [クリア（Clear）] のデータベース内に残ります。デフォルトでは、クリアされたアラームは Prime Infrastructure インターフェイスに表示されません。
- 保存したレポートは、レポートを実行したスイッチが削除されてもデータベースに残ります。

Prime Infrastructure からスイッチを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチおよびハブ（Switches and Hubs）]** を選択して、削除するスイッチの横にあるチェックボックスをクリックします。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして削除を実行します。

関連トピック

スイッチの追加 （187 ページ）

例：有線クライアントのスイッチ トラップと Syslog の設定

次の Cisco IOS の設定例では、この Cisco IOS スイッチ機能が MAC 通知用に SNMP トラップをスイッチから Prime Infrastructure サーバに転送する方法を示します（802.1x クライアントの場合）。

```
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of Prime Infrastructure server> version 2c <community-string>
 mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change


interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface level config for MAC Notification

  snmp trap mac-notification change removed <- interface level config for MAC Notification
```

debug コマンドは次のとおりです。

```
debug snmp packets
```

show コマンドは次のとおりです。

```
show mac address-table notification change
```

詳細については、『Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide』を参照してください。

例：IOS を使用した Catalyst スイッチの Syslog 転送の設定

syslog 設定は、syslog メッセージを Catalyst スイッチから Prime Infrastructure サーバに転送します。この機能は ID クライアントの検出に使用されます。次の Cisco IOS の設定例は、この Cisco IOS スイッチが syslog メッセージを Catalyst スイッチから Prime Infrastructure サーバに転送する方法を示しています。

```
archive
 log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of Prime Infrastructure server>
```

詳細については、『Catalyst 3750 Software Configuration Guide』を参照してください。

Cisco Prime Infrastructure での Cisco OfficeExtend AP の使用

OfficeExtend アクセス ポイントは、リモート ロケーションでコントローラからアクセス ポイントへの安全な通信を提供し、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。ホーム オフィスでのテレワーカーのエクスペリエンスは、本社オフィスでのエクスペリエンスとまったく同じです。アクセス ポイントとコントローラの間の Datagram Transport Layer Security（DTLS）による暗号化は、すべての通信のセキュリティを最高レベルにします。

図 25-1 **205774.jpg** に、典型的な OfficeExtend アクセス ポイントの設定を示します。

OfficeExtend アクセス ポイントは、ルータまたはネットワーク アドレス変換（NAT）を使用するその他のゲートウェイ デバイスを越えて動作するよう設計されています。NAT により、ルータなどのデバイスはインターネット（パブリック）と個人ネットワーク（プライベート）間のエージェントとして動作でき、これにより、コンピュータのグループ全体を単一の IP アドレスとすることができます。コントローラ リリース 6.0 では、単一の NAT デバイスの後方では単一の OfficeExtend アクセス ポイントのみを展開可能です。

現時点では、WPLUS ライセンスにより Cisco 5500 シリーズのコントローラに接続された Cisco Aironet 1130 シリーズおよび 1140 シリーズのアクセス ポイントだけを OfficeExtend アクセス ポイントとして設定できます。

ファイアウォールは、アクセス ポイントからの CAPWAP を使用するトラフィックを許可するよう設定されている必要があります。UDP ポート 5246 および 5247 が有効であり、アクセス ポイントがコントローラに接続できないようにすることがある中間デバイスによりブロックされていないことを確認してください。

OfficeExtend アクセス ポイントのライセンスを購入する前に、WPlus ライセンスが 5500 シリーズ コントローラにインストールされていることを確認してください。ライセンスのインストール後、1130 シリーズまたは 1140 シリーズ アクセス ポイントで OfficeExtend モードを有効にすることができます。

オペレーティング システムのソフトウェアによってアクセス ポイントが自動的に検出され、Cisco Prime Infrastructure データベース内の既存のコントローラに関連付けられると Cisco Prime Infrastructure データベースに追加されます。

AP とコントローラ間のリンクを測定するためのリンク遅延の設定

コントローラでリンク遅延を設定して、アクセス ポイントおよびコントローラの間のリンクを計測できます。この機能は、コントローラに接続されたすべてのアクセス ポイントで使用できますが、特に、リンクの速度が低いか、信頼性の低い WAN 接続の可能性がある FlexConnect アクセス ポイントで役立ちます。

リンク遅延は、接続モードの FlexConnect アクセス ポイントでのみサポートされます。スタンドアロン モードの FlexConnect アクセス ポイントはサポートされません。

リンク遅延は、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントにおける CAPWAP ハートビート パケット（エコー要求および応答）のラウンドトリップ時間をモニタします。この時間は、ネットワーク リンク速度およびコントローラの処理負荷に

よって異なります。アクセスポイントは、コントローラへの発信エコー要求およびコントローラから受信するエコー応答をタイムスタンプ記録します。アクセスポイントはこのデルタ時間をシステムのラウンドトリップ時間としてコントローラに送信します。アクセスポイントは、30 秒のデフォルト間隔でコントローラにハートビート パケットを送信します。

リンク遅延はアクセス ポイントとコントローラ間の CAPWAP 応答時間を計算します。ネットワーク遅延や ping 応答は計測しません。

コントローラにより、現在のラウンドトリップ時間および継続的な最短および最長ラウンドトリップ時間が表示されます。最短および最長時間はコントローラが動作している限り維持され、クリアして再開することもできます。

リンク遅延を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [統合型 AP（Unified AP）]** を選択し、デバイス名をクリックします。

ステップ 2 [リンク遅延を有効にする（Enable Link Latency）] チェックボックスをオンにして、このアクセス ポイントのリンク遅延を有効にするか、またはオフにして、エコー応答受信ごとにアクセス ポイントがコントローラにラウンドトリップ時間を送信しないようにします。デフォルト値はオフです。

ステップ 3 [保存（Save）] をクリックして変更内容を保存します。

リンク遅延の結果は、[リンク遅延を有効にする（Enable Link Latency）] チェックボックスの下に表示されます。

1. [現在（Current）] : アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの現在のラウンドトリップ時間（ミリ秒単位）。
2. [最小（Minimum）] : リンク遅延が有効になったか、またはリセットされたために生じる、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最短ラウンドトリップ時間（ミリ秒単位）。
3. [最大（Maximum）] : リンク遅延が有効になったか、またはリセットされたために生じる、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最長ラウンドトリップ時間（ミリ秒単位）。

ステップ 4 このアクセス ポイントのコントローラ上の現在、最小、および最大のリンク遅延統計をクリアするには、[リンク遅延のリセット（Reset Link Latency）] をクリックします。[最小（Minimum）] フィールドおよび [最大（Maximum）] フィールドに更新された統計情報が表示されます。

ユニファイド AP の設定

[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [統合型 AP（Unified AP）] ページを使用して、統合型アクセス ポイントを表示し、設定できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当する IP アドレスをクリックして次のパラメータを表示します。

- [AP 名（AP Name）] : アクセス ポイント名をクリックして、アクセス ポイントの詳細を表示または設定します。
- [ベース無線 MAC（Base Radio MAC）]
- [管理ステータス（Admin Status）]
- [AP モード（AP Mode）]
- ソフトウェア バージョン（Software Version）
- [プライマリ コントローラ名（Primary Controller Name）]

ステップ 3 アクセス ポイント名をクリックして、アクセス ポイントの詳細を表示または設定します。表示される情報は、アクセス ポイントのタイプに応じて異なります。

ユニファイドアクセスポイントでSniffer機能を有効にする（AiroPeek）

アクセス ポイントでスニファ機能を有効にした場合、そのアクセス ポイントはスニファとして機能し、特定チャネル上のすべてのパケットを取得して、AiroPeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

スニファ機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合だけ有効になります。AiroPeek の詳細は、次の URL を参照してください。www.wildpackets.com/products/airopeek/overview

はじめる前に

スニファ機能を使用する前に、次の作業を完了しておく必要があります。

- リモート サイトで、スニファ モードでアクセス ポイントを設定します。スニファ モードでアクセス ポイントを設定する方法については、「関連項目」の「Web ユーザ インターフェイスを使用したスニファ モードでの AP の設定」を参照してください。
- Windows XP マシンで AiroPeek バージョン 2.05 以降をインストールします。
  - 次の dll ファイルをダウンロードするには、WildPackets のメンテナンス メンバーである必要があります。次の URL を参照してください。
    https://wpdn.wildpackets.com/view_submission.php?id=30
- 次の dll ファイルをコピーします。

- socket.dll ファイルを Plugins フォルダ（C:\ProgramFiles\WildPackets\AiroPeek\Plugins など）へ
- socketres.dll ファイルを PluginRes フォルダ（C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes など）へ

関連トピック

デバイスの 802.11 パラメータの設定 （143 ページ）

リモート マシンでの AiroPeek スニファの設定

リモート マシンで AiroPeek を設定するには、次の手順を実行します。

ステップ 1 AiroPeek アプリケーションを開始して、[ツール（Tools）] タブで [オプション（Options）] をクリックします。

ステップ 2 [オプション（Options）] ページで [モジュールの分析（Analysis Module）] をクリックします。

ステップ 3 ページ内を右クリックして、[すべてを無効にする（Disable All）] オプションを選択します。

ステップ 4 [Cisco リモート モジュール（Cisco remote module）] 列を見つけて、有効にします。[OK] をクリックして変更を保存します。

ステップ 5 [新しいキャプチャ（New capture）] をクリックして、[キャプチャ オプション（capture option）] ページを表示します。

ステップ 6 アダプタ モジュールのリストからリモート Cisco アダプタを選択します。

ステップ 7 展開して、新しいリモートアダプタ オプションを見つけます。ダブルクリックして新規ページを開き、表示されるテキスト ボックスに名前を入力して、[IP アドレス（IP address）] 列にコントローラ管理インターフェイス IP を入力します。

ステップ 8 [OK] をクリックします。新しいアダプタがリモート Cisco アダプタに追加されます。

ステップ 9 アクセス ポイントを使用してリモートの airopeek キャプチャ用の新規アダプタを選択します。

ステップ 10 [キャプチャ（capture）] ページで [ソケット キャプチャの開始（start socket capture）] をクリックして、リモート キャプチャ プロセスを開始します。

ステップ 11 コントローラの CLI からアクセス ポイントを起動して、config ap mode sniffer ap-name コマンドを入力してスニファ モードに設定します。

アクセス ポイントが再起動し、スニファ モードでアップ状態になります。

Cisco Prime Infrastructure を使用したスニファ モードでの AP の設定

Web ユーザ インターフェイスを使用してスニッファ モードで AP を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[AP 名（AP Name）] 列の項目をクリックしてこのページに移動します。

ステップ 2 [一般（General）] グループ ボックスで、ドロップダウン リストを使用して AP モードを [スニファ（Sniffer）] に設定し、[適用（Apply）] をクリックします。

ステップ 3 [無線インターフェイス（Radio Interfaces）] グループ ボックスの [プロトコル（Protocol）] 列でプロトコル（802.11a/802.11b/g）をクリックします。これによって、設定ページが開きます。

ステップ 4 スニファ パラメータを表示するには、[スニファ（Sniff）] チェックボックスをオンにします。スニファ対象チャネルを選択し、サーバ（AiroPeek が実行されているリモート マシン）の IP アドレスを入力します。

ステップ 5 [保存（Save）] をクリックして、変更内容を保存します。

AP での Flex+Bridge モードの有効化

AP で Flex+Bridge モードを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [Lightweightアクセスポイント（Lightweight Access Points）]** の順にクリックします。

ステップ 2 関連する AP テンプレートをクリックするか、新しいテンプレートを追加します。

ステップ 3 [APパラメータ（AP Parameters）] タブをクリックし、[APモード（AP Mode）] チェックボックスをオンにします。

ステップ 4 ドロップダウン リストから [Flex+Bridge] を選択し、[保存（Save）] をクリックします。

- AP モードを Flex+Bridge にまたは Flex+Bridge から切り替える場合、AP は再起動します。
- Flex+Bridge モードは API 暗号化および AP 再送信間隔をサポートしておらず、重要 AP のフェールオーバー条件のみをサポートします。
- [FlexConnect] タブおよび [メッシュ（Mesh）] タブで行われた設定は、AP モードを変更するとプロビジョニングされなくなります。まず AP モードを Flex+Bridge モードに変更し、その後で [FlexConnect] タブおよび [メッシュ（Mesh）] でパラメータを設定する必要があります。

コントローラ冗長性の設定

「コントローラの冗長性」は、コントローラに組み込まれているハイアベイラビリティ（HA）フレームワークを指しています。ワイヤレス ネットワーク コントローラの冗長性により、ネットワークのダウンタイムを削減することができます。冗長アーキテクチャでは、1 台のコントローラがアクティブ状態となり、もう 1 台のコントローラがスタンバイ状態となります。スタンバイ コントローラは、冗長ポートを使用してアクティブ コントローラのヘルスを常時モニタします。両方のコントローラは管理インターフェイスの IP アドレスを含め、同じ設定を共有します。

コントローラのスタンバイ状態およびアクティブ状態は、製造時に付けられる固有デバイス識別子（UDI）である、冗長在庫管理単位（SKU）によって決まります。冗長 SKU UDI を持つ

コントローラは、起動されて永続カウントライセンスを実行するコントローラとペアになる場合、最初はスタンバイ状態です。永続カウントライセンスを持つコントローラの場合、コントローラがアクティブ状態であるか、スタンバイ状態であるかを手動で設定できます。

Cisco Prime Infrastructure は、アクセス ポイントのステートフル スイッチオーバー（「AP SSO」ともいう）をサポートしています。AP SSO により、コントローラのスイッチオーバーが発生しても AP セッションがそのまま維持されます。コントローラの冗長性の詳細については、「関連項目」の「ワイヤレス冗長性の設定」を参照してください。

コントローラの冗長性は、Cisco Prime Infrastructure サーバのダウンタイムを削減するために使用される Cisco Prime Infrastructure HA フレームワークと似ていますが、別個のものです。詳細については、「関連項目」の「ハイ アベイラビリティの設定」を参照してください。

詳細については、『Cisco Prime Infrastructire Administrator Guide』を参照してください。

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定

Cisco Prime Infrastructure は、プロファイルを使用してワイヤレス脅威保護機能をすばやくアクティブにする Cisco 適応型ワイヤレス侵入防御システム（Cisco Adaptive wIPS または wIPS）をサポートしています。

Cisco Prime Infrastructure は、顧客タイプ、建築タイプ、および「教育」、「財務」、「軍事」、「見本市」などのような業種に基づいて事前定義された wIPS プロファイルのリストを提供します。これらのプロファイルは「そのまま」使用することも、要件に合わせてカスタマイズすることもできます。そして、選択した Mobility Services Engine とコントローラにプロファイルを適用できます。

Cisco Adaptive wIPS は Cisco Prime Infrastructure パーティション分割機能をサポートしていません。

詳細については、『Cisco Wireless Intrusion Prevention System Configuration Guide』を参照してください。

関連トピック

wIPS プロファイルの表示 （196 ページ）
wIPS プロファイルの追加 （197 ページ）
wIPS プロファイルの編集 （198 ページ）
wIPS プロファイルの適用 （200 ページ）
wIPS プロファイルの削除 （201 ページ）

wIPS プロファイルの表示

Prime Infrastructure の [wIPS プロファイル リスト（wIPS Profiles List）] ページから wIPS プロファイルにアクセスできます。このページでは、現在の wIPS プロファイルを表示、編集、適用、削除したり、新しい wIPS プロファイルを作成したりすることができます。

[サービス（Services）]>[モビリティサービス（Mobility Services）]>[wIPSプロファイル（wIPS Profiles）] の順に選択します。[wIPS プロファイル リスト（wIPS Profiles List）] に現在の wIPS プロファイルが一覧表示されます。このリストには、既存のプロファイルごとに次の情報が表示されます。

- [プロファイル名（Profile Name）]：wIPS プロファイルのユーザ定義名。

  wIPS プロファイルを表示または編集するには、[プロファイル名（Profile Name）] をクリックします。その後、「関連項目」の「wIPS プロファイルの編集」の手順を実行します。

- [プロファイル ID（Profile ID）]：プロファイルの固有識別子。
- [バージョン（Version）]：プロファイルのバージョン。
- [適用されている MSE（MSE(s) Applied To）]：このプロファイルが適用されている Mobility Services Engine（MSE）の数を示します。MSE 数をクリックすると、プロファイルの割り当ての詳細が表示されます。
- [適用されているコントローラ（Controller(s) Applied To）]：このプロファイルが適用されているコントローラの数を示します。コントローラ数をクリックすると、プロファイルの割り当ての詳細が表示されます。

関連トピック

wIPS プロファイルの追加 （197 ページ）
wIPS プロファイルの編集 （198 ページ）
wIPS プロファイルの適用 （200 ページ）
wIPS プロファイルの削除 （201 ページ）
SSID グループの作成 （202 ページ）

wIPS プロファイルの追加

デフォルト プロファイルまたは現在設定済みのプロファイルを使用して、新しい wIPS プロファイルを作成できます。

ステップ 1 [サービス（Services）]>[モビリティ サービス（Mobility Services）]>[wIPS プロファイル（wIPS Profiles）] を選択します。

ステップ 2 [コマンドの選択（Select a Command）]>[プロファイルの追加（Add Profile）]>[実行（Go）] の順に選択します。

ステップ 3 [プロファイル パラメータ（Profile Parameters）] ページの [プロファイル名（Profile Name）] テキスト ボックスにプロファイル名を入力します。

ステップ 4 ドロップダウン リストから、該当する定義済みのプロファイルを選択するか、[デフォルト（Default）] を選択します。定義済みのプロファイルには次のものがあります。

- [教育（Education）]
- [EnterpriseBest]

- [EnterpriseRogue]
- [金融（Financial）]
- [医療（HealthCare）]
- [HotSpotOpen]
- [Hotspot8021x]
- [軍（Military）]
- [小売（Retail）]
- [トレードショー（Tradeshow）]
- [ウェアハウス（Warehouse）]

ステップ 5 次をクリックします。

- 変更および割り当てを行わずにwIPSプロファイルを保存する場合は、[保存（Save）]をクリックします。プロファイルはプロファイル リストに表示されます。後で編集および割り当てを行う場合は、「関連項目」の「wIPS プロファイルへのアクセス」の説明に従ってプロファイルにアクセスできます。
- プロファイルを保存して設定を編集し、Mobility Services Engine とコントローラに割り当てる場合は、[保存および編集（Save and Edit）] をクリックします。詳細については、「関連項目」の「wIPS プロファイルの編集」を参照してください。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
wIPS プロファイルの表示 （196 ページ）
wIPS プロファイルの編集 （198 ページ）

wIPS プロファイルの編集

wIPS プロファイル エディタを使用すると、次の内容を含むプロファイルの詳細を設定できます。

- [SSID グループ（SSID groups）]：wIPS プロファイルを適用する SSID グループを選択します。
- [ポリシーの包含（Policy inclusion）]：プロファイルに含めるポリシーを決定します。
- [ポリシー レベル設定（Policy level settings）]：しきい値、重大度、通知の種類、ACL/SSID グループなど、プロファイルに含まれる各ポリシーの設定を行います。
- [MSE/コントローラ アプリケーション（MSE/controller applications）]：プロファイルを適用する MSE およびコントローラを選択します。

ステップ 1 次の手順で wIPS プロファイル エディタにアクセスします。

- 新しい wIPS プロファイルを作成し、[保存および編集（Save and Edit）] をクリックします。
- **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [wIPS プロファイル（wIPS Profiles）]** を選択し、編集する wIPS プロファイルのプロファイル名をクリックします。

  Prime Infrastructure に [SSID グループ リスト（SSID Group List）] ページが表示されます。このページを使用して、現在の SSID グループの編集および削除、または新しいグループの追加を行うことができます。SSID グループのグローバル リストから選択することもできます。詳細については、「関連項目」の「SSID グループと wIPS プロファイルの関連付け」を参照してください。

ステップ 2 wIPS プロファイルに関連付ける SSID グループを選択し、[保存（Save）] をクリックします。

ステップ 3 [次へ（Next）] をクリックします。[プロファイル設定（Profile Configuration）] ページが表示されます。

ステップ 4 [ポリシーの選択（Select Policy）] ペインのポリシー ツリーで、現在のプロファイルで有効または無効にするポリシーのチェックボックスをオンにします。

該当するブランチまたはポリシーのチェックボックスをオンにすることで、ブランチ全体または個別のポリシーを有効または無効にできます。

デフォルトでは、すべてのポリシーが選択されています。

ステップ 5 [プロファイル設定（Profile Configuration）] ページで、個々のポリシーをクリックしてポリシーの説明を表示したり、現在のポリシー ルール設定を表示または変更したりします。各ポリシーで次のオプションを使用できます。

- [追加（Add）]：このポリシーに新しいルールを作成するには、[追加（Add）] をクリックして [ポリシー ルール設定（Policy Rule Configuration）] ページにアクセスします。
- [編集（Edit）]：このルールの設定を編集するには、該当するルールのチェックボックスをオンにし、[編集（Edit）] をクリックして [ポリシー ルール設定（Policy Rule Configuration）] ページにアクセスします。
- [削除（Delete）]：削除するルールのチェックボックスをオンにし、[削除（Delete）] をクリックします。[OK] をクリックして削除を実行します。

  1 つ以上のポリシー ルールが存在する必要があります。リスト内に 1 つしかない場合、そのポリシー ルールは削除できません。
- [上に移動（Move UP）]：リスト内で上に移動するルールのチェックボックスをオンにします。[上に移動（Move UP）] をクリックします。
- [下に移動（Move DOWN）]：リスト内で下に移動するルールのチェックボックスをオンにします。[下に移動（Move DOWN）] をクリックします。

  ポリシー レベルで次の設定を行うことができます。
- [しきい値（Threshold）]（すべてのポリシーに適用されるわけではありません）：選択したポリシーに関連付けられたしきい値または上限を示します。ポリシーのしきい値に達すると、アラームがトリガーされます。

すべてのポリシーに 1 つ以上のしきい値が含まれている必要があるため、標準的なワイヤレス ネットワークの問題に基づいて、各ポリシーにデフォルトのしきい値が定義されています。

しきい値オプションは、選択したポリシーに応じて異なります。

Cisco Adaptive wIPS DoS およびセキュリティ ペネトレーション攻撃からのアラームは、セキュリティ アラームとして分類されます。これらの攻撃の概要は [セキュリティ サマリー（Security Summary）] ページにあります。このページにアクセスするには、[モニタ（Monitor）]>[セキュリティ（Security）] の順に選択します。wIPS の攻撃は [脅威および攻撃（Threats and Attacks）] セクションにあります。

- [重大度（Severity）]：選択したポリシーの重大度を示します。パラメータとしては、[重大（critical）]、[やや重大（major）]、[情報（info）]、および [警告（warning）] があります。このフィールドの値は、ワイヤレス ネットワークに応じて変わります。
- [通知（Notification）]：しきい値に関連付けられた通知の種類を示します。
- [ACL/SSID グループ（ACL/SSID Group）]：この閾値が適用される ACL または SSID グループを示します。

  選択されたグループのみポリシーをトリガーします。

ステップ 6 プロファイル設定が完了したら、[保存（Save）] をクリックして変更内容をプロファイルに保存します。

ステップ 7 [次へ（Next）] をクリックすると [MSE/コントローラ（MSE/Controller(s)）] ページが表示されます。

ステップ 8 [プロファイルの適用（Apply Profile）] ページで、現在のプロファイルを適用する MSE とコントローラのチェックボックスをオンにします。

ステップ 9 選択が完了したら、[適用（Apply）] をクリックして現在のプロファイルを選択した MSE とコントローラに適用します。

新しく作成したプロファイルを [プロファイル リスト（Profile List）] ページから直接適用することもできます。「関連項目」の「wIPS プロファイルの適用」を参照してください。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
wIPS プロファイルの表示 （196 ページ）
wIPS プロファイルの適用 （200 ページ）
wIPS プロファイルの削除 （201 ページ）
SSID グループの作成 （202 ページ）

wIPS プロファイルの適用

ステップ 1 [サービス（Services）]>[モビリティ サービス（Mobility Services）]>[wIPS プロファイル（wIPS Profiles）] の順に選択します。

ステップ 2 適用する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3 [コマンドの選択（Select a Command）] > [プロファイルの適用（Apply Profile）] > [実行（Go）] の順に選択します。

ステップ 4 プロファイルを適用する Mobility Services Engine とコントローラを選択します。

新しいプロファイルの割り当てが現在の割り当てと異なる場合、プロファイルを別の名前で保存するよう求められます。

ステップ 5 [適用（Apply）] をクリックします。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
SSID グループの作成 （202 ページ）

wIPS プロファイルの削除

MSE とコントローラに現在適用されているプロファイルは削除できません。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 削除する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3 **[コマンドの選択（Select a Command）] > [プロファイルの削除（Delete Profile）] > [実行（Go）]** を選択します。

ステップ 4 [OK] をクリックして削除を実行します。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
wIPS プロファイルの追加 （197 ページ）
wIPS プロファイルの編集 （198 ページ）
wIPS プロファイルの適用 （200 ページ）

SSID グループと wIPS プロファイルの関連付け

SSID（Service Set IDentifier）は、802.11（Wi-Fi）ネットワークを識別するトークンまたはキーです。802.11 ネットワークに参加するには SSID が必要になります。

SSID を wIPS プロファイルに関連付けるには、SSID を SSID グループに追加して、その SSID グループを wIPS プロファイルに関連付けます。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
wIPS プロファイルの削除 （201 ページ）
SSID グループの作成 （202 ページ）
SSID グループの編集 （202 ページ）

SSID グループの作成

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 いずれかの wIPS プロファイルのプロファイル名をクリックします。 Prime Infrastructure に [SSID グループリスト（SSID Group List）] ページが表示されます。

ステップ 3 **[コマンドの選択（Select a Command）] > [グループの追加（Add Groups）] > [実行（Go）]** を選択します。

ステップ 4 テキスト ボックスに SSID グループ名を入力します。

ステップ 5 [SSID リスト（SSID List）] テキスト ボックスに SSID を入力します。複数の SSID を入力するには、各 SSID の後に改行を入れます。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
SSID グループと wIPS プロファイルの関連付け （201 ページ）

SSID グループの編集

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 いずれかの wIPS プロファイルのプロファイル名をクリックします。 Prime Infrastructure に [SSID グループリスト（SSID Group List）] ページが表示されます。

ステップ 3 編集する SSID グループのチェックボックスをオンにします。

ステップ 4 **[コマンドの選択（Select a Command）] > [グループの編集（Edit Group）] > [実行（Go）]** を選択します。

ステップ 5 [SSID グループ名（SSID Group Name）] または [SSID リスト（SSID List）] に必要な変更を加えます。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
wIPS プロファイルの表示 （196 ページ）

SSID グループの削除

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 いずれかの wIPS プロファイルのプロファイル名をクリックします。 Prime Infrastructure に [SSIDグループリスト（SSID Group List）] ページが表示されます。

ステップ 3 削除する SSID グループのチェックボックスをオンにします。

ステップ 4 **[コマンドの選択（Select a Command）] > [グループの削除（Delete Group）] > [実行（Go）]** を選択します。

ステップ 5 [OK] をクリックして削除を実行します。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （196 ページ）
wIPS プロファイルの表示 （196 ページ）
wIPS プロファイルの編集 （198 ページ）

MSE サーバの高可用性の設定

Cisco Prime Infrastructure を使用して、MSE ハイ アベイラビリティ（HA）が設定された Cisco モビリティ サービス エンジン（MSE）デバイスをペアリングおよび管理することができます。その方法と関連タスクの実行方法については、下記の「関連項目」を参照してください。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （203 ページ）
MSE HA サーバの構成 （204 ページ）
プライマリおよびセカンダリ MSE HA サーバに関する詳細の表示 （205 ページ）
MSE サーバの HA ステータスの表示 （206 ページ）
MSE HA の手動フェールオーバーまたはフェールバックのトリガー （207 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （208 ページ）

MSE HA サーバのフェールオーバーとフェールバック

MSE HA は、プライマリ MSE に障害が発生しても MSE サービスに引き続きアクセスできるようにするための機能です。セカンダリ MSE がプライマリ MSE のデータの完全なコピーを保持して、バックアップとして機能します。ヘルス モニタおよび「ハートビート」のプロセスがプライマリとセカンダリの両方で実行されることで、各サーバは互いの状態を常に把握できます。

プライマリ MSE で障害が発生すると、必ずセカンダリ MSE への「フェールオーバー」がトリガーされます。Prime Infrastructure は、プライマリの問題が解決するまで、プライマリではなくセカンダリのモビリティ サービスを使用します。

プライマリが復旧すると「フェールバック」がトリガーされます。プライマリ MSE に制御が戻され、フェールオーバー中のネットワークの状態に関するデータがセカンダリ MSE からプライマリに複製されます。

MSE HA を設定する場合、自動または手動のどちらでフェールオーバーをトリガーするか選択できます。フェールバックについても同様の選択肢があります。

MSE HA を手動フェールオーバーまたはフェールバックに設定した場合は、プライマリに障害が発生した際や、サービスが復旧した際に送信される重大アラームに応じて、それぞれの動作をユーザがトリガーする必要があります。

自動フェールオーバーを行うように MSE HA を設定すると、ネットワーク管理者による MSE HA の管理の必要性が減少します。また、セカンダリ サーバが自動的に起動されるため、約 10 秒以内（デフォルト）でプライマリの障害が検出され、フェールオーバーの発生原因となった状況への対応に要する時間が削減されます。MSE HA が自動フェールバックに設定されている場合、システムは 1 分に 1 回送信される ping メッセージを 30 回正常に受信するまでフェールバックをトリガーしません。

関連トピック

MSE HA サーバの構成 （204 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （208 ページ）
MSE サーバの高可用性の設定 （203 ページ）

MSE HA サーバの構成

MSE デバイスのハイ アベイラビリティをアクティブ化するには、1 台の MSE サーバがプライマリ MSE デバイスとして動作し、別の 1 台がセカンダリ MSE として動作するペアリングを作成する必要があります。

ペアリングできるのは、次の状態の MSE デバイスのみです。

- 「関連項目」の「MSE ハイ アベイラビリティの設定」の説明に従って、MSE ハイ アベイラビリティで使用できるよう適切に設定されている。
- 「関連項目」の「Prime Infrastructure への MSE の追加」の説明に従って、 Prime Infrastructure に追加されている。

はじめる前に

ペアリングを作成するには、次の情報が必要です。

- プライマリ MSE サーバのデバイス名。
- セカンダリ MSE サーバのデバイス名。これは、以前に割り当てたデバイス名か、サーバのペアリング時に割り当てる新しい名前になります。
- セカンダリ MSE HA サーバの IP アドレス。HA 用に MSE サーバを設定した際に割り当てた、HA ヘルス モニタの IP アドレスです。
- セカンダリ MSE HA サーバのパスワード。HA 用に MSE サーバを設定した際に割り当てた Prime Infrastructure 通信パスワードです。

また、手動または自動フェールバックのどちらで MSE HA サーバを設定するかを決める必要があります。ガイドラインについては、「関連項目」の「MSE HA の自動および手動のフェールオーバーとフェールバック」を参照してください。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。既存の MSE のリストが表示されます。

ステップ 2 リストで、プライマリ MSE HA サーバとして動作させる MSE を見つけます。

ステップ 3 MSE リストの [セカンダリ サーバ（Secondary Server）] 列には、「N/A（ここをクリックして設定してください）（N/A (Click here to configure)）」というメッセージが表示されます。このリンクをクリックして、プライマリ MSE の HA 設定ページを表示します。

ステップ 4 該当するフィールドに、セカンダリ MSE のデバイス名、ヘルス モニタの IP アドレス、および Prime Infrastructure 通信パスワードを入力します。

ステップ 5 フェールオーバーおよびフェールバックのタイプを指定します。[手動（Manual）] または [自動（Automatic）] のいずれかを選択できます。

ステップ 6 [長時間のフェールオーバー待機（Long Failover Wait）] を指定します。これは、プライマリ MSE の障害が検出された後、システムが自動フェールオーバーをトリガーするまでに待機する最大時間です。デフォルトは 10 秒で、最大は 120 秒です。

ステップ 7 [保存（Save）] をクリックします。 Prime Infrastructure は、これらの MSE のペアリングを確認するプロンプトを表示します。[OK] をクリックして確認します。

Prime Infrastructure は、ペアリングと同期を自動的に実行します。これらのプロセスは、ネットワーク帯域幅やその他の要因に応じて、完了までに最大 20 分かかる場合があります。これらのプロセスの進捗を確認するには、**[サービス（Services）] > [モビリティ サービス エンジン（Mobility Services Engine）] > [システム（System）] > [サービス高可用性（Services High Availability）] > [HA ステータス（HA Status）]** を選択します。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （203 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （208 ページ）
MSE サーバの高可用性の設定 （203 ページ）

プライマリおよびセカンダリ MSE HA サーバに関する詳細の表示

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 HA パラメータを表示する方法は次のとおりです。

- プライマリ MSE HA サーバの場合は、[デバイス名（Device Name）] 列でサーバの名前をクリックします。
- セカンダリ MSE HA サーバの場合は、[セカンダリ サーバ（Secondary Server）] 列でサーバの名前をクリックします。

Prime Infrastructure に、選択したサーバのモビリティ サービスの設定ページが表示されます。

ステップ 3 左側のサイドバーのメニューから [HA設定（HA Configuration）] を選択します。[HA 設定（HA Configuration）] ページに次の情報が表示されます。

- [プライマリ ヘルス モニタ IP（Primary Health Monitor IP）]
- [セカンダリ デバイス名（Secondary Device Name）]
- セカンダリ IP アドレス（Secondary IP Address）
- [セカンダリ パスワード（Secondary Password）]

- [セカンダリ プラットフォーム UDI（Secondary Platform UDI）]
- [セカンダリ アクティベーション ステータス（Secondary Activation Status）]
- [フェールオーバー タイプ（Failover Type）]
- フェールバック タイプ（Failback Type）
- [長時間のフェールオーバー待機（Long Failover Wait）]

関連トピック

MSE HA サーバの構成 （204 ページ）
MSE HA の手動フェールオーバーまたはフェールバックのトリガー （207 ページ）
MSE サーバの HA ステータスの表示 （206 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （208 ページ）
MSE サーバの高可用性の設定 （203 ページ）

MSE サーバの HA ステータスの表示

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 HA ステータスを表示する方法は次のとおりです。

- プライマリ MSE HA サーバの場合は、[デバイス名（Device Name）] 列でサーバの名前をクリックします。
- セカンダリ MSE HA サーバの場合は、[セカンダリ サーバ（Secondary Server）] 列でサーバの名前をクリックします。

Prime Infrastructure に、選択したサーバのモビリティ サービスの設定ページが表示されます。

ステップ 3 左側のサイドバーのメニューで [HA ステータス（HA Status）] を選択します。[現在の高可用性ステータス（Current High Availability Status）] ページに、次の情報が表示されます。

- [ステータス（Status）]：MSE HA サーバがアクティブで正しく同期されているかどうかが表示されます。
- [ハートビート（Heartbeats）]：MSE HA サーバがパートナーとハートビート信号を交換しているかどうかが表示されます。
- [データ レプリケーション（Data Replication）]：MSE HA サーバがパートナーのデータを複製しているかどうかが表示されます。
- [平均ハートビート応答時間（Mean Heartbeat Response Time）]：サーバ間の平均ハートビート応答時間が表示されます。
- [イベント ログ（Events Log）]：MSE サーバが生成した直近 20 個のイベントが表示されます。

ステップ 4 MSA サーバの HA ステータス情報とイベント ログを更新するには、[ステータスの更新（Refresh Status）] をクリックします。

関連トピック

MSE HA サーバの構成 （204 ページ）
プライマリおよびセカンダリ MSE HA サーバに関する詳細の表示 （205 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （208 ページ）
MSE サーバの高可用性の設定 （203 ページ）

MSE HA の手動フェールオーバーまたはフェールバックのトリガー

手動フェールオーバーとフェールバックはデフォルトで有効になっています。手動設定の場合、システム アラームに応じて、Prime Infrastructure の管理者がフェールオーバーおよびフェールバックを手動でトリガーする必要があります。

ペアリングした MSE HA サーバを自動フェールオーバーおよびフェールバックに設定することもできます（「関連項目」を参照）。

ステップ 1 **[サービス（Services）]>[モビリティ サービス（Mobility Services）]>[モビリティ サービス エンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 トリガーする方法は次のとおりです。

- プライマリからセカンダリへのフェールオーバーをトリガーするには、[デバイス名（Device Name）] 列でプライマリ MSE HA サーバの名前をクリックします。
- セカンダリからプライマリへのフェールバックをトリガーするには、[セカンダリ サーバ（Secondary Server）] 列でセカンダリ MSE HA サーバの名前をクリックします。

Prime Infrastructure に、選択したサーバのモビリティ サービスの設定ページが表示されます。

ステップ 3 左側のサイドバーのメニューから [HA設定（HA Configuration）] を選択します。[HA 設定（HA Configuration）] ページに、選択したサーバの HA 設定情報が表示されます。

ステップ 4 フェールオーバーまたはフェールバックを開始するには、[スイッチオーバー（Switchover）] をクリックします。

ステップ 5 [OK] をクリックして、スイッチオーバーの開始を確定します。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （203 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （208 ページ）
MSE サーバの高可用性の設定 （203 ページ）

MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定

手動フェールオーバーとフェールバックはデフォルトで有効になっています。ペアリングした MSE HA サーバを自動フェールオーバーおよびフェールバックに設定すると、次のように自動的に変更されます。

- プライマリからセカンダリへのフェールオーバー：セカンダリがプライマリの障害を検出するとすぐにトリガーされます。
- セカンダリからプライマリへのフェールバック：セカンダリからプライマリへの ping メッセージの送信が 30 回成功するとトリガーされます。ping 要求は、1 分間に 1 回送信されます。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [MSE 高可用性（MSE High Availability）]** を選択します。

ステップ 2 [デバイス名（Device Name）] 列でプライマリ MSE HA サーバの名前をクリックします。

Prime Infrastructure にプライマリ MSE HA サーバの [HA 設定（HA Configuration）] ページが表示されます。

ステップ 3 [フェールオーバー タイプ（Failover Type）] および [フェールバック タイプ（Failback Type）] リスト ボックスで [自動（Automatic）] を選択します。

ステップ 4 必要に応じて、プライマリでの障害の検出から自動フェールオーバーまでの最大遅延を制御するには、[長時間のフェイルオーバー待機（Long Failover Wait）] の値を変更します。デフォルトは 10 秒です。

ステップ 5 [保存（Save）] をクリックして変更内容を保存します。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （203 ページ）
MSE HA の手動フェールオーバーまたはフェールバックのトリガー （207 ページ）
MSE サーバの高可用性の設定 （203 ページ）

MSE HA サーバのペアリング解除

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [MSE 高可用性（MSE High Availability）]** を選択します。

ステップ 2 [デバイス名（Device Name）] 列でプライマリ MSE HA サーバの名前をクリックします。

Prime Infrastructure にプライマリ MSE HA サーバの [HA 設定（HA Configuration）] ページが表示されます。

ステップ 3 [削除（Delete）] をクリックして、MSE HA サーバのペアリングを解除します。

ステップ 4 [OK] をクリックして、MSE HA サーバのペアリング解除を確定します。

関連トピック

MSE HA サーバの構成 （204 ページ）
MSE サーバの高可用性の設定 （203 ページ）

プラグ アンド プレイを使用したコントローラの設定

自動プロビジョニングは、Cisco Prime Infrastructure による現在のワイヤレス LAN コントローラ（WLC）の新規設定や置き換えを自動化するための機能です。Cisco Prime Infrastructure の自動プロビジョニング機能を使用すると、多数のコントローラから構成される顧客向けの展開を簡素化できます。

自動プロビジョニングの権限を有効にするには、Admin、Root、または SuperUser ステータスでログインしている必要があります。

ユーザの自動プロビジョニング権限を有効または無効にするには、Cisco Prime Infrastructure の [管理設定（Administration Settings）] > [ユーザ、ロール、およびAAA（Users, Roles, and AAA）] > [ユーザグループ（User Groups）] > [グループ名] > [許可されているタスクのリスト（List of Tasks Permitted）] で、許可されているタスクを編集します。各チェックボックスをオンまたはオフにして、これらの権限の有効と無効を切り替えます。

コントローラの無線および b/g ネットワークは、Cisco Prime Infrastructure のダウンロードされたスタートアップ コンフィギュレーション ファイルで最初は無効になっています。必要に応じて、テンプレートを使用し、それらの無線ネットワークを有効にできます。テンプレートは、自動化されたテンプレートの 1 つとして含まれている必要があります。

自動プロビジョニング フィルタ コンテンツを指定するには、アプリケーションに直接詳細を入力するか、CSV ファイルから詳細をインポートします。自動プロビジョニング機能は、5500 シリーズのコントローラと 5500 シリーズ以外のコントローラをサポートしています。5500 シリーズ以外のコントローラでは、AP マネージャ インターフェイスのコンフィギュレーション情報が定義されているのに対し、5500 シリーズのコントローラにはこの情報がありません。

自動プロビジョニング機能にアクセスするには、**[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [WLC自動プロビジョニング（WLC Auto Provisioning）]** を選択します。