ネットワークの設定

ネットワーク設定の概要

ネットワーク全体のデフォルトになるネットワーク設定を作成できます。ネットワーク内の設定を定義可能な主なエリアは次の 2 つです。

- [Global settings]：ここで定義されている設定はネットワーク全体に適用されます。DHCP、DNS、AAA、NTP などのサーバー、IP アドレスプール、デバイス クレデンシャル プロファイル、Syslog、トラップ、Netflow などのテレメトリの設定が含まれます。
- [Site settings]：ここで定義されている設定はグローバル設定をオーバーライドします。また、サーバー、IPアドレスプール、デバイスのログイン情報プロファイルの設定を含めることができます。

（注） アクティブなファブリックで使用されているネットワーク設定の変更はサポートされていません。それらのネットワーク設定には、サイト階層、IPプールの名前変更など複数の機能が含まれます。

（注） 一部のネットワーク設定は、デバイスの可制御性機能を使用してデバイスに自動的に設定できます。Cisco DNA Center によるデバイスの設定または更新時に、トランザクションが Cisco DNA Center の監査ログにキャプチャされます。監査ログを使用すると、変更を追跡し、問題をトラブルシューティングするのに役立ちます。

[Design] > **[Network Settings]** の順に選択して該当するタブをクリックし、次のグローバルネットワーク設定を定義できます。

- AAA、DHCP、DNS サーバーなどのネットワークサーバー：詳細については、グローバル ネットワーク サーバーの設定 （4 ページ）を参照してください。
- CLI、SNMP、HTTP（S）などのデバイスクレデンシャル：詳細については、グローバル CLI クレデンシャルの設定 （4 ページ）、グローバル SNMPv2c ログイン情報の設定 （5 ページ）、グローバル SNMPv3 クレデンシャルの設定 （6 ページ）、およびグローバル HTTPS クレデンシャルの設定 （8 ページ）を参照してください。
- IP アドレスプールの詳細については、IP アドレス プールを設定する （14 ページ）を参照してください。
- SSID、ワイヤレス インターフェイス、および無線周波数プロファイルなどのワイヤレス設定：詳細については、グローバル ワイヤレス設定の構成 （20 ページ）を参照してください。
- テレメトリを使用して、syslog、SNMP、NetFlow コレクタサーバーなどのグローバルテレメトリ設定を構成します。

Cisco ISE またはその他の AAA サーバーの追加

Cisco Identity Services Engine（ISE）サーバーまたはその他の同様の AAA サーバーを、ネットワーク、クライアント、およびエンドポイント認証のためにサイトまたはグローバル レベルで定義することができます。ネットワーク認証では、RADIUS および TACACS プロトコルがサポートされています。クライアントとエンドポイント認証では、RADIUS のみがサポートされます。Cisco DNA Center あたり、1 つの Cisco ISE のみサポートされます。

マルチ ISE 設定をサポートするために、RADIUS または TACACS サーバーグループの下に送信元インターフェイスを設定できます。各 Cisco ISE ISE クラスタには独自のサーバーグループがあります。RADIUS サーバーと TACACS サーバーに使用される送信元インターフェイスは、次のように決定されます。

- デバイスに Loopback0 インターフェイスが設定されている場合、Loopback0 は送信元インターフェイスとして設定されます。
- それ以外の場合は、Cisco DNA Center を管理 IP として使用するインターフェイスが送信元インターフェイスとして設定されます。

あるサイトに Cisco ISEサーバーを設定すると、サイトに割り当てられているデバイスは、対応する Cisco ISE サーバーで、自動的に a /32 マスクに更新されます。その後、Cisco ISE でこれらのデバイスに変更が行われると、Cisco DNA Center に自動的に送信されます。

FIPS モードの展開の場合、共有秘密は、共有秘密、キーラップ、およびメッセージ認証コードキーで構成されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Network]**。

ステップ 2 [サーバーの追加（Add Servers）] をクリックして AAA サーバーを追加します。

ステップ 3 [サーバーの追加（Add Servers）] ウィンドウで、[AAA] チェック ボックスをオンにし、[OK] をクリックします。

ステップ 4 AAA サーバーをネットワークユーザー、クライアント/エンドポイントユーザー、またはその両方に設定します。

ステップ 5 [Network] または [Client/Endpoint] チェックボックスをオンにし、AAA サーバーのサーバーとプロトコルを設定します。

ステップ 6 認証と認可のための [Servers] を選択します（[ISE] または [AAA]）。

- [ISE] を選択した場合は、次のように設定します。
  - [ネットワーク] ドロップダウンリストから、Cisco ISE サーバーの IP アドレスを選択します。[Network] ドロップダウンリストには、Cisco DNA Center のホームページの [System Settings] に登録されている 、Cisco ISE サーバーのすべての IP アドレスが含まれています。Cisco ISE の IP を選択すると、選択した Cisco ISE のポリシーサービスノード（PSN）の IP アドレスを持つプライマリおよび追加 IP アドレスのドロップダウンリストが表示されます。AAA サーバーの IP アドレスを入力することも、[IP Address (Primary)] と [IP Address (Additional)] ドロップダウンリストから PSN IP アドレスを選択することもできます。
  - [Protocol] を選択します（[RADIUS] または [TACACS]）。

    （注） 特定のワイヤレスコントローラの物理サイトと管理サイトの AAA 設定が一致する必要があります。一致しない場合、プロビジョニングは失敗します。

- [AAA] を選択した場合は、次のように設定します。
  - AAA サーバーの IP アドレスを入力することも、[IP Address（Primary] および [IP Address（Additional] ドロップダウンリストから IP アドレスを選択することもできます。これらのドロップダウンリストには、[System Settings] で登録されている Cisco ISE 以外の AAA サーバーが含まれています。

ステップ 7 [Save] をクリックします。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバルネットワーク設定を上書きできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

ステップ 2 **[DHCP Server]** フィールドに、DHCP サーバーの IP アドレスを入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 3 **[DNS Server]** フィールドに、DNS サーバーのドメイン名を入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 4 [Save] をクリックします。

グローバル デバイス クレデンシャルの概要

「グローバル デバイス クレデンシャル」とは、ネットワーク内のデバイスに関する情報を検出して収集するために Cisco DNA Center で使用される共通の CLI、SNMP、および HTTPS クレデンシャルを指します。Cisco DNA Center は、グローバル クレデンシャルを使用して設定済みデバイス クレデンシャルを共有するネットワーク内のデバイスを認証し、アクセスします。グローバル デバイス クレデンシャルの追加、編集、および削除することができます。また、グローバル サイトまたは特定のサイトにクレデンシャルを関連付けることもできます。

グローバル CLI クレデンシャルの設定

最大 10 のグローバル CLI クレデンシャルを設定して保存できます。

ステップ 1 [Design] > [Network Settings] > [Device Credentials]。メニューアイコン（☰）をクリックして、> >

ステップ 2 左側の階層ツリーから、[Global] を選択します。

ステップ 3 [CLI Credentials] エリアで、[Add] をクリックします。

ステップ 4 次のフィールドに情報を入力します。

表 *1 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 5 [Save] をクリックします。

サイトにクレデンシャルを適用するには、左側の階層ツリーからサイトを選択し、クレデンシャルの横にあるボタンを選択して、[Save] をクリックします。

ステップ 6 既存のクレデンシャルを変更する場合は、[Now] で今すぐクレデンシャルを更新するか、後で更新するスケジュールを設定するかを選択します。

グローバル SNMPv2c ログイン情報の設定

ネットワークデバイスをモニタおよび管理するために、グローバル SNMPv2c クレデンシャルを設定できます。

（注） Cisco DNA Center は、FIPS モードが有効になっている場合、SNMPv2c デバイスクレデンシャルをサポートしません。代わりに、SNMPv3 クレデンシャルを指定する必要があります。

始める前に

ネットワークの SNMP 情報は必須です。

ステップ 1 [設計（Design）] > [ネットワーク設定（Network Settings）] > [デバイスクレデンシャル（Device Credentials）]。メニューアイコン（☰）をクリックして、> >

ステップ 2 左側の階層ツリーから、[Global] を選択します。

ステップ 3 [SNMP Credentials] エリアで、[Add] をクリックします。

ステップ 4 [タイプ（Type）] で、[SNMP v2c] をクリックし、次の情報を入力します。

表 *2 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 5 [Save] をクリックします。

ステップ 6 既存のクレデンシャルを変更する場合は、[Now] で今すぐクレデンシャルを更新するか、後で更新するスケジュールを設定するかを選択します。

グローバル SNMPv3 クレデンシャルの設定

ネットワークデバイスをモニタおよび管理するために、グローバル SNMPv3 クレデンシャルを設定できます。

始める前に

ネットワークの SNMP 情報は必須です。

ステップ 1 [Design] > [Network Settings] > [Device Credentials]。メニューアイコン（☰）をクリックして、> >

ステップ 2 左側の階層ツリーから、[Global] を選択します。

ステップ 3 [SNMP Credentials] エリアで、[Add] をクリックします。

ステップ 4 [Type] で、**[SNMP v3]** をクリックし、次の情報を入力します。

表 *3 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証 • [MD5]：HMAC-MD5 に基づく認証
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [DES]：CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。

フィールド	説明
Privacy Password	DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 5 [Save] をクリックします。

ステップ 6 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[Now] ラジオボタンをクリックし、[Apply] をクリックします。
- 後で更新をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Apply] をクリックします。

（注） [Time Zone] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

グローバル HTTPS クレデンシャルの設定

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Device Credentials]**。

ステップ 2 左側の階層ツリーから、[Global] を選択します。

ステップ 3 [HTTPS Credentials] エリアで、[Add] をクリックします。

ステップ 4 次の情報を入力します。

表 *4 : HTTPS* クレデンシャル

フィールド	説明
[Type]	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[Read] または [Write] です。

フィールド	説明
Read	最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。
Write	最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

ステップ 5 [Save] をクリックします。

ステップ 6 既存のクレデンシャルを変更する場合は、[Now] で今すぐクレデンシャルを更新するか、後で更新するスケジュールを設定するかを選択します。

グローバルデバイスのログイン情報の編集に関する注意事項

既存のグローバル デバイス クレデンシャルの編集に関する注意事項と制約事項は、次のとおりです。

- Cisco DNA Center グローバル デバイス クレデンシャルを編集、保存、および適用する際は、次のプロセスが使用されます。

  1. Cisco DNA Center からローカル認証を持つデバイスにログイン情報がプッシュされます。ローカル認証では、ログイン情報の変更が適用され、Cisco DNA Center はこれらのログイン情報を使用してデバイスを管理します。

     （AAA サーバーが継承または設定されたサイトにあるデバイスには、Cisco DNA Center から CLI ログイン情報の変更はプッシュされません。AAA 認証では、ログイン情報の変更は適用されません。Cisco DNA Center は、同じログイン情報が AAA サーバーに存在する場合にのみ、これらのログイン情報を使用してデバイスを管理します）

  2. クレデンシャルがデバイスに正常にプッシュされると、Cisco DNA Center は新しいクレデンシャルを使用してデバイスに到達できることを確認します。

（注） この手順に失敗すると、Cisco DNA Center が新しいクレデンシャルをデバイスにプッシュしていても、インベントリでは古いクレデンシャルを使用してデバイスが管理されます。この場合、既存のログイン情報を更新すると、**[Provision]** > **[Inventory]** ウィンドウでデバイスが管理対象外であると示される可能性があります。

  3. 新しいクレデンシャルを使用してデバイスに正常に到達すると、Cisco DNA Center のインベントリは、新しいクレデンシャルを使用してデバイスの管理を開始します。

- サイトには、SNMPv2c クレデンシャルと SNMPv3 クレデンシャルを使用するデバイスを含めることができます。SNMPv2c または SNMPv3 のグローバル クレデンシャルを編集して保存すると、Cisco DNA Center はその変更をデバイスにプッシュし、そのクレデンシャルを有効にします。たとえば、SNMPv2c を使用するデバイスがあるのに、SNMPv3 のグローバル クレデンシャルを編集して保存すると、Cisco DNA Center は関連付けられたサイトのすべてのデバイスに新しい SNMPv3 のクレデンシャルをプッシュして、そのクレデンシャルを有効にします。つまり、以前は SNMPv2c が有効になっていたデバイスを含め、すべてのデバイスが SNMPv3 を使用して管理されるようになります。

- 混乱が生じないようにするために、CLI ログイン情報を編集する際は [User Name] を変更してください。これにより、新しいCLIクレデンシャルが作成され、既存のCLIクレデンシャルは変更されません。

グローバル デバイス クレデンシャルの編集

準備が整うまで、Cisco DNA Center でクレデンシャルの変更を適用せずに、グローバル デバイス クレデンシャルを編集および保存できます。変更の適用を決定すると、Cisco DNA Center は、変更したデバイスクレデンシャルを参照するすべてのサイトを検索し、すべてのデバイスに変更をプッシュします。

新しいグローバル デバイス クレデンシャルを更新または作成できますが、Cisco DNA Center はデバイスからクレデンシャルを削除することはありません。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Device Credentials]** の順に選択します。

ステップ 2 左側の階層ツリーから、[Global] を選択します。

ステップ 3 [Manage Credentials] をクリックし、変更するデバイスのログイン情報のチェックボックスをオンにして、**[Actions]** > **[Edit]**の順に選択します。

ステップ 4 [Edit Credentials] ダイアログボックスで、必要な変更を加えて、[Save] をクリックします。

（注） CLI パスワードログイン情報には、*ASCII* 印刷可能文字（文字コード 32 ー 127。https://en.wikipedia.org/wiki/ASCII#Printable_characters を参照）だけを使用できます。

ステップ 5 クレデンシャルタイルで、[Apply] をクリックします。

ステップ 6 [Apply Credentials] ダイアログボックスで、ログイン情報を今すぐ更新する（[Now]）か、後でスケジュールするかを選択します。

ステップ 7 クレデンシャル変更のステータスを表示するには、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[クレデンシャル ステータス（Credential Status）] 列に、次のいずれかのステータスが表示されます。

- [Success]：Cisco DNA Center はログイン情報の変更を正常に適用しました。
- [Failed]：Cisco DNA Center はログイン情報の変更を適用できませんでした。失敗したログイン情報の変更とその理由に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。
- [Not Applicable]：ログイン情報はデバイスタイプに適用できません。

複数のクレデンシャル（CLI、SNMP、HTTPS など）を編集して保存した場合、がいずれかのクレデンシャルを適用できなかったときには、[クレデンシャルステータス（Credential Status）] 列に [失敗（Failed）] と表示されます。Cisco DNA Center 失敗したログイン情報の変更に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。

デバイス クレデンシャルのサイトへの関連付け

グローバルサイトを作成するサイトは、グローバルなデバイスのクレデンシャルを継承できます。または特定サイトの別のデバイスのクレデンシャルを作成することができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Device Credentials]**。

ステップ 2 左側の階層ツリーから、必要なサイトを選択します。

ステップ 3 [Manage Credentials] をクリックします。

ステップ 4 選択したサイトに関連付けるクレデンシャルを選択し、次に [Assign] をクリックします。

デバイスのログイン情報がサイトに正常に関連付けられたことを示す成功メッセージが、画面の下部に表示されます。

デバイス クレデンシャルの管理

ログイン情報管理ワークフローでは、ログイン情報を作成または編集したり、割り当てたり、デバイスに適用することができます。

ログイン情報は、グローバルサイト（[Global]）、または選択したサイト、建物、フロアに割り当てられます。グローバルレベルでログイン情報を割り当てる場合、すべてのサイト、建物、およびフロアは、グローバルレベルから設定を継承します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Device Credentials]** の順に選択します。

ステップ 2 [Global] または必要なエリア、建物、フロアを左側の階層ツリーから、。

ステップ 3 [Manage Credentials] をクリックします。
[Manage Credentials] ウィンドウが開きます。

ステップ 4 [Add] ドロップダウンリストから、ログイン情報のタイプ（CLI、HTTP（HTTPS）読み取り、SNMPv3 など）を選択します。

ステップ 5 [Add New Credentials] ウィンドウで、次の手順を実行します。

1. 必要なフィールドに情報を入力します。
2. [Assign credential to site] チェックボックスをオンにします。

   （注） ボックスがオフの場合、ログイン情報は作成されますが、どのサイトにも割り当てられません。

3. [**保存（Save）**] をクリックします。

新しく作成したログイン情報が [Manage Credentials] ウィンドウに表示されます。

ステップ 6 割り当てるログイン情報を選択し、[Assign] をクリックします。

ステップ 7 ログイン情報を適用するには、次のいずれかを実行します。

- サイト階層全体にログイン情報を適用するには、[Manage Credentials] に移動し、目的のログイン情報の [Actions] メニューにマウスカーソルを合わせて、[Apply] を選択します。
- 特定のサイトだけにログイン情報を適用するには、左側の階層ペインで目的のサイトを選択し、そのログイン情報に対応するカードで [Assign] をクリックします。

ステップ 8 [Apply Credentials] ダイアログボックスで、ログイン情報を今すぐ更新する（[Now]）か、後でスケジュールするかを選択します。

ログイン情報は、該当するすべてのサイトに適用されます。

まだ開始されていないログイン情報適用タスクは、再スケジュールすることができます。

ステップ 9 タスクのステータスを表示するには、次のいずれかを実行します。

- [Device Credentials] ウィンドウで、右上隅にある更新アイコンをクリックします。ログイン情報カードの見出しの横にあるアイコンにマウスカーソルを合わせます。
- **[Provision]** > **[Inventory]** の順に選択します。[Credential Status] 列にステータスが表示されます。
- **[Activities]** > **[Audit Logs]** の順に選択します。

ステップ 10 ログイン情報を編集するには、次の手順を実行します。

1. 対応するログイン情報の横にある編集アイコンをクリックします。

   または、[Manage Credentials] ウィンドウで、ログイン情報名の横にある省略記号のアイコンにカーソルを合わせて、[Edit] をクリックします。
2. [Edit Information] ウィンドウで、[OK] をクリックします。
3. [Edit Credentials] ウィンドウで必要な変更を加えます。
4. [**保存（Save**）] をクリックします。

ステップ 11 ログイン情報適用の開始日時を再スケジュールするには、次のいずれかの手順を実行します。

- **グローバルにスケジュールされたタスク**：[Manage Credentials] ウィンドウで、ログイン情報名の横にある水平の省略記号のアイコンにカーソルを合わせて、[Apply] を選択してから、[Apply] をクリックします。
- **サイト、建物、またはフロアのメインページからスケジュールされたタスク**：タスクが最初にスケジュールされたサイト、建物、またはフロアに戻り、対応するログイン情報カードで [Apply] をクリックします。

（注） タイムゾーンは変更できません。

IP アドレス プールを設定する

Cisco DNA Center IPv4 と IPv6 のデュアルスタック IP プールがサポートされています。

IPv4 および IPv6 アドレスプールは手動で設定できます。

Cisco DNA Center を外部 IP アドレス マネージャと通信するように設定することもできます。詳細については、*Cisco DNA Center* 管理者ガイドを参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Add] をクリックし、[Add IP Pool] ウィンドウの必須入力フィールドをすべて入力します。

Cisco DNA Center が外部の IP アドレスマネージャと通信するように設定した場合、外部 IP アドレスマネージャの既存の IP アドレスプールと重複する IP プールを作成することはできません。

ステップ 3 **[Save]** をクリックします。

新しく追加されたプールが IP アドレスプールテーブルに表示されます。IPv4 または IPv6 のアドレスプールのみを表示する場合は、[SUBNET TYPE] 領域で [IPv4] または [IPv6] オプションをクリックします。

（注） IP アドレス プールを編集して、DHCP を変更すると、その IP アドレス プールを使用してデバイスを再設定する必要はありません。

IP アドレスマネージャから IP アドレスプールをインポートする

Bluecat または Infoblox から IP アドレスプールをインポートできます。

（注） IP アドレスプールはサブプールを持つことができず、IP アドレスプールから割り当てられた IP アドレスを持つことはできません。

外部 IP アドレスマネージャ（IPAM）と通信するには Cisco DNA Center を設定する必要があります。詳細については、*Cisco DNA Center* 管理者ガイドを参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Actions] ドロップダウンリストから、[Import from IPAM Server] を選択し、必須フィールドに値を入力します。

ステップ 3 CIDR を入力し、**[Retrieve]** をクリックして、インポートできる IP プールのリストを取得します。

ステップ 4 [Select All] をクリックするか、またはインポートする IP アドレスプールを選択して [Import] をクリックします。

CSV ファイルから IP アドレスプールをインポートする

CSV ファイルから IP アドレスプールをインポートできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Actions] ドロップダウンリストから、[Import from CSV File] を選択します。

ステップ 3 [Download Template] をクリックして最新のサンプルファイルをダウンロードします。

ステップ 4 ファイルに IP アドレスプールを追加して、ファイルを保存します。

ステップ 5 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

a) ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。

b) **[クリックして選択（click to select）]** が表示される場所をクリックしてファイルを選択します。

ステップ 6 **[インポート (Import)]** をクリックします。

IP アドレスプールの予約

始める前に

1 つまたは複数の IP アドレスプールが作成されていることを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 左側の階層ツリーから、サイトを選択します。

ステップ 3 [Reserve] をクリックして以下のフィールドに入力し、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。

- [IP Address Pool Name]：予約した IP アドレスプールの一意の名前。
- [Type]：IP アドレスプールのタイプ。LAN 自動化の場合は、**LAN** を選択します。次のオプションがあります。
  - [LAN]：該当するアンダーレイの LAN インターフェイスに IP アドレスを割り当てます。
  - [Management]：IP アドレスを管理インターフェイスに割り当てます。
  - [Service]：IP アドレスをサービスインターフェイスに割り当てます。
  - [WAN]：IP アドレスを WAN インターフェイスに割り当てます。
  - [Generic]：他のすべてのネットワークタイプで使用されます。
- [IP Address Space]：すべてまたは一部の IP アドレスを予約する IPv4 および IPv6 アドレスプール。
- **CIDR Prefix/Number of IP Addresses**：IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve. IPv6 IP プールの [CIDR Prefix] として \64 を

選択すると、[SLAAC] オプションがオンになります。（[SLAAC] が選択されている場合、デバイスは DHCP サーバーを必要とせずに、自動的に IP アドレスを獲得します）。

- [Gateway]：ゲートウェイ IP アドレス。
- [DHCP Servers]：DHCP サーバーの IP アドレス。
- [DNS Servers]：DNS サーバーのアドレス。

ステップ 4 [予約（Reserve）] をクリックします。

IPv4 と IPv6 の両方のアドレスプールを予約している場合（ファブリックがデュアルスタック IP プールでプロビジョニングされている場合）で、IPv6 プールがすでに VN に接続されているときは、シングルスタック IP プールに戻すことはできません。

ただし、IPv6 プールが VN に接続されていない場合は、デュアルスタック IPv6 プールからシングルスタック IPv4 プールにダウングレードできます。シングルスタックにダウングレードするには、[IP Address Pools] ウィンドウで、デュアルスタック IP プールの [Edit] をクリックします。[Edit IP Pool] ウィンドウで、[IPv6] チェックボックスをオフにして、[Save] をクリックします。

IP アドレスプールの編集

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 左側の階層ツリーから、必要なサイトを選択します。

ステップ 3 すべての IP アドレスプールを一括で編集するには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Edit All] を選択します。
b) [Warning] メッセージで [Yes] をクリックします。
c) [Edit IP Pool] ウィンドウで、必要な変更を行い、[Save] をクリックします。

ステップ 4 目的の IP アドレスプールのみを編集するには、次の手順を実行します。

a) 目的の IP アドレスプールを選択し、[Actions] ドロップダウンリストから [Edit Selected] をクリックします。

選択した IP アドレスプールに対応する [Edit] をクリックすることもできます。

b) [Edit IP Pool] ウィンドウで、必要な変更を行い、[Save] をクリックします。

IP アドレスプールの削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。

ステップ 2 左側の階層ツリーから、必要なサイトを選択します。

ステップ 3 すべての IP アドレスプールを一括で削除するには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Delete All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

ステップ 4 目的の IP アドレスプールのみを削除するには、次の手順を実行します。

a) 目的の IP アドレスプールを選択し、[Actions] ドロップダウンリストから [Delete Selected] をクリックします。

選択した IP アドレスプールに対応する [Delete] をクリックすることもできます。

b) [Warning] メッセージで [Yes] をクリックします。

IP アドレスプールの複製

サイトレベルで既存の IP アドレスプールを複製できます。IP アドレスプールを複製すると、DHCP サーバーと DNS サーバーの IP アドレスが自動的に入力されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 左側の階層ツリーから、必要なサイトを選択します。

ステップ 3 目的の IP アドレスプールを見つけ、[Actions] エリアで [Clone] をクリックします。

ステップ 4 [Clone IP Pool] ウィンドウで、次の手順を実行します。

a) 必要に応じて、プール名を編集します（タイプ、IP アドレス空間、またはグローバルプール値は、複製元のプールから継承されるため編集できません）。

b) 必要に応じて、CIRD プレフィックス値を編集します。

c) [Clone] をクリックします。

IP アドレスプールのリリース

サイトレベルで予約されているシングルスタックおよびデュアルスタックプールをリリースできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 左側の階層ツリーから、必要なサイトを選択します。

ステップ 3 すべての IP アドレスプールを一括でリリースするには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Release All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

c) プロンプトで [Release] をクリックします。

ステップ 4 目的の IP アドレスプールのみをリリースするには、次の手順を実行します。

a) 目的の IP アドレスプールを選択し、[Actions] ドロップダウンリストから [Release Selected] をクリックします。

b) プロンプトで [Release] をクリックします。

IP アドレスプールの表示

この手順では、テーブルビューとツリービューで 10 個以上の IP アドレスプールを表示する方法を示します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。

ステップ 2 左側の階層ツリーから、必要なサイトを選択します。

ステップ 3 トグルボタンを使用して、テーブルビューとツリービューを切り替えます。

- IP アドレスプールが 10 個以上の場合は、デフォルトではテーブルビューにプールが表示されます。
- IP アドレスプールが 10 個未満の場合は、デフォルトではツリービューにプールが表示されます。

（注） テーブルマップビューとツリーマップビューの切り替えは、UI でのユーザーの選択ではなくプール数に基づきます。

ツリービューは、グローバルプールとサイトプールに適用されます。

ステップ 4 [IP Address Pools] テーブルビューには、[Name]、[Type]、[IPv4 Subnet]、[IPv4 Used]、[IPv6 Subnet]、[IPv6 Used]、および [Actions] に基づいて IP アドレスプールのリストが表示されます。

（注）
- [IPv4 Used] および [IPv6 Used] の横にある [i] アイコンにカーソルを合わせます。[IPv4 Used]、[IPv6 Used]、[Free]、[Unassignable]、[Assigned]、および [Default Assigned] の IP アドレスプールに関する詳細情報がツールチップに表示されます。
- [IPv4] 列と [IPv6] 列で、特定の IP アドレスプールに対応する [IPv4] と [IPv6] の使用率の横にある [i] アイコンにカーソルを合わせます。ツールチップには、[Free]、[Unassignable]、[Assigned]、および [Default Assigned] の IP アドレスプールの割合が表示されます。

ステップ 5 テーブルビューで [IPv4] または [Dual-Stack] のアドレスプールのみを表示する場合は、[Sbunet Type] エリアで [IPv4 only] または [Dual-Stack] オプションをクリックします。

ステップ 6 ツリービューで、目的の IP アドレスプールにカーソルを合わせてクリックすると、次の情報を含むスライドインペインが表示されます。

- IP アドレスプールのサブネットタイプ。
- それぞれのプール下にある使用可能な IP アドレスと [Pool CIDR]、[Gateway]、[DHCP Server(s)]、および [DNS Server(s)] の割合。

- 各プールで使用されている IP アドレスの割合。

ステップ 7 [Used] エリアで、[Assigned] をクリックすると、[Device Name]、[IP Address]、および [Site] に基づいてフィルタ処理されたデバイスに割り当てられた IP アドレスのリストが表示されます。

ステップ 8 [Unassignable] をクリックすると、[Device Name]、[IP Address]、および [Site] に基づいてフィルタ処理されたデバイスに割り当てることができない未割り当て IP アドレスのリストが表示されます。

ステップ 9 [Edit] をクリックして、IP アドレスプールを編集します。

ステップ 10 [Release] をクリックして、IP アドレスプールを解放します。

（注）
- グローバルプールのサイドバーでは、特定のプールについて、すべての子プールにおける使用状況を確認できます。
- グローバル IP アドレスプールとサイト IP アドレスプールには、ブロックリストに登録された IP アドレスを設定できます。
- サブプールにはブロックリストに登録された IP アドレスを含めることはできません。
  - Cisco DNA Center は、ブロックリストに登録された IP アドレスが含まれている場合、CIDR アドレスプールの IP アドレスプール作成要求を拒否します。
  - 次の空き IP アドレスプール要求では、Cisco DNA Center はブロックリストに登録された IP アドレスをスキップして、次の IP アドレス空きプールを見つけます。

ステップ 11 （オプション）テーブルデータをエクスポートするには、サイドバーで [Export] をクリックします。

サービス プロバイダ プロファイルの設定

特定の WAN プロバイダのサービス クラスを定義するサービス プロバイダ（SP）プロファイルを作成することができます。サービスモデルには、4 クラス、5 クラス、6 クラス、および 8 クラスを定義できます。SP プロファイルの作成後、アプリケーションポリシーの範囲内（必要に応じてインターフェイスのサブラインレート設定を含む）のアプリケーションポリシーと WAN インターフェイスにそのプロファイルを割り当てることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[SP Profiles]** の順に選択します。

ステップ 2 **[Qos]** 領域で、**[Add]** をクリックします。

ステップ 3 **[Profile Name]**フィールドに、SP プロファイルの名前を入力します。

ステップ 4 [WAN Provider] ドロップダウンリストから、新しいサービスプロバイダを入力するか、既存のプロバイダを選択します。

ステップ 5 [Model] ドロップダウンリストから、クラスモデル（[4 class]、[5 class]、[6 class]、および [8 class]）のいずれかを選択します。

これらのクラスの詳細については、サービス プロバイダのプロファイル を参照してください。

グローバル ワイヤレス設定の構成

グローバル ワイヤレス ネットワーク設定には、サービスセット識別子（SSID）、ワイヤレス インターフェイス、RF、およびセンサーの設定が含まれます。

（注） ワイヤレス センサー デバイス プロファイルを作成できるのは、Cisco Aironet 1800s アクティブ センサーデバイスに対してのみです。

エンタープライズ ワイヤレス ネットワーク用 SSID の作成

次の手順では、エンタープライズ ワイヤレス ネットワークに SSID を設定する方法を説明しています。

（注） SSID は、グローバルレベルで作成されます。サイト、ビルディング、フロアは、グローバル レベルから設定が継承されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSID] テーブルで、[Add] の上にカーソルを合わせて、[Enterprise] を選択します。

ステップ 5 [Wireless SSID] ワークフローで、[Basic Settings] のセットアップを完了します。

a) [Sensor] トグルボタンが使用可能な場合は、無効になっていることを確認します。

b) [Wireless Network Name (SSID)] フィールドに、ワイヤレスネットワークの一意の名前を入力します。

c) [WLAN Profile Name] フィールドに、WLAN プロファイルの名前を入力します。

Cisco DNA Center は WLAN プロファイル名に基づいて、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシープロファイル名を自動的に生成します。

d) [Wireless Option] の設定で、次のいずれかのオプションボタンをクリックします。

- [Multi band operation（2.4 GHz, 5 GHz, 6GHz）]：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは無効になっています。
- [Multi band operation with band select]：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは有効になっています。

- [5 GHz only]：WLAN が 5 GHz 用に作成され、バンドセレクトは無効になっています。
- [2.4 GHz only]：WLAN が 2.4 GHz 用に作成され、バンドセレクトは無効になっています。
- [6GHz Only] ：WLAN は 6 GHz 用に作成され、バンドセレクトは無効になっています。

e) [Primary Traffic Type] ドロップダウンリストから、次のいずれかのオプションを選択します。

- [VoIP (Platinum)]：ワイヤレスネットワークの QoS は、ワイヤレス音声およびデータトラフィック用に最適化されています。
- [Video (Gold)]：ワイヤレスネットワークの QoS はビデオトラフィック用に最適化されています。
- [Best Effort (Silver)]：ワイヤレスネットワークの QoS は、ワイヤレス データ トラフィック用にのみ最適化されています。
- [Non-real Time (Bronze)]：ワイヤレスネットワークの QoS は、低帯域幅の使用に最適化されています。

f) [SSID STATE] 設定では、トグルボタンをクリックして、次の設定を有効または無効にします。

- [Admin Status]：このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP は ワイヤレスコントローラ に関連付けられたままで、アクセス可能であり、AP には引き続きライセンスが必要です。
- [Broadcast SSID]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にするには、このトグルボタンを使用します。

ステップ 6 [Security Settings] の設定を完了します。

a) [Level of Security] で、このネットワークの暗号化および認証タイプを選択します。サイト、ビルディング、およびフロアは、グローバル階層から設定を継承します。サイト、ビルディング、またはフロアレベルでセキュリティレベルをオーバーライドできます。

- [Enterprise]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。

（注） Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。

WPA3 は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

- [Personal] ：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。デフォルトでは、[WPA2] チェックボックスが有効になっています。[Personal] を選択した場合は、[Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間でペアワイズマスターキー（PMK）として使用されます。

  （注） WPA3 パーソナルは、パスワードベースの堅牢な認証を提供することによって、個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるようになります。

  WPA2 パーソナルの場合は、サイト、ビルディング、またはフロアレベルで、事前共有キー（PSK）をオーバーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。詳細については、事前共有キーのオーバーライド （27 ページ）を参照してください。

  2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

（オプション）WPA2-Personal の場合、次の手順を実行してマルチ事前共有キー（MPSK）サポートを構成します。

1. [Configure MPSK] をクリックします。
2. [Configure MPSK] ダイアログ ボックスで、構成したいMPSK に対し [Add] をクリックします。最大 5 つの MPSK を追加できます。
3. [Priority] ドロップダウンリストから優先順位を選択します。

   （注） 優先順位 0 キーが中央 Web 認証（CWA）フレックスモードで設定されていない場合、WLAN へのクライアント接続が失敗する可能性があります。

4. [Passphrase Type] ドロップダウンリストから、パスフレーズタイプを選択します。
5. [Passphrase] フィールドに、パスフレーズを入力します。
6. [Save] をクリックします。

MPSK はCisco AireOS ワイヤレスコントローラでサポートされていません。 MPSK は、WPA2-Personal の 2 セキュリティ構成に適用されます。

- [Open Secured]：[Assign Open SSID] ドロップダウンリストから、クライアントをオープンでセキュアな SSID にリダイレクトするためのオープン SSID を選択します。オープンでセキュアなポリシーは、セキュリティが最も低くなります。

  （注） Fast Transition は、オープンでセキュアな SSID には適用できません。

  オープンでセキュアな SSID はオープン SSID に依存しているため、オープンでセキュアな SSID でアンカーを有効にする前に、オープン SSID でアンカーを有効にしておく必要があります。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

b) [Authentication, Authorization, and Accounting Configuration] で、[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加および設定します。

詳細については、エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定 （29 ページ）を参照してください。

c) [AAA Override] チェックボックスをオンにして、AAA オーバーライド機能を有効にします。

デフォルトでは、このチェックボックスはグレー表示されています。このチェックボックスを使用するには、[Configure AAA] オプションを使用して AAA サーバを設定する必要があります。

d) 次のチェックボックスをオンにします（複数可）。

- [Fast Lane]：このネットワークで fastlane 機能を有効にするには、このチェックボックスをオンにします。

  （注） fastlane を有効にすると、最適化されたレベルのワイヤレス接続と 拡張 QoS を受信するように Cisco IOS デバイスを設定できます。

- [Identity PSK]（個人レイヤ 2 セキュリティ用）：SSID 内の個人またはユーザーグループのために作成できる一意の事前共有キーを有効にするには、このチェックボックスをオンにします。

- [MAC Filtering]：ワイヤレスネットワークでの MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。

  （注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。

- [Deny RCM Clients]：ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。

- [Enable Posture]：ポスチャ評価を有効にするには、このチェックボックスをオンにします。ポスチャを有効にすると、[Pre-Auth ACL List Name] ドロップダウンリストが表示されます。ポスチャは、Cisco Identity Services Engine（ISE）のサービスです。ポスチャを使用すると、ネットワークに接続されているすべてのエンドポイントの企業セキュリティ ポリシーとのコンプライアンスに関するステート（ポスチャとも呼ばれる）をチェックできます。これにより、ネットワークの防護領域にアクセスするクライアントを制御できます。

- [Pre-Auth ACL List Name]：ドロップダウンリストから、SSID にマッピングするために作成した ACL リスト名を選択します。

  （注） ポスチャには AAA 設定が必須です。[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加します。

e) [Next] をクリックします。

ステップ 7 [Advance Settings] の設定を完了します。

a) [Fast Transition (802.11r)] で、次の手順を実行します。

- [Adaptive]、[Enable]、または [Disable] モードを選択します。

（注） 802.11r を使用すると、ワイヤレスクライアントは、ある AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。

b) [MFP Client Protection] で、[Optional]、[Required]、または [Disabled] を選択します。

（注） 管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、AP とクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは、[Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 が ワイヤレスコントローラ 上で設定されており、クライアントも WPA2 用に設定されていて、CCXv5 MFP をサポートしている場合）にのみ、クライアントはアソシエーションを許可されます。

c) [Protected Management Frame (802.11w)] で、必要なオプションを選択します。

（注） [Protected Management Frame (802.11w)] で使用できるオプションは、[Level of Security] で選択した設定によって異なります。次のオプションを使用できる場合があります。

- **オプション**
- **必須**
- **Disabled**

d) [11K] で、次の設定を指定します。

- [Neighbor List]：このチェックボックスをオンにして、すべての 11k 対応クライアントが、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できるように設定します。

（注） ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバー AP のリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。この応答もアクション フレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

- [Session Timeout]：クライアントセッションがアクティブである最大時間を設定するには、このチェックボックスをオンにします。この時間が経過すると再認証を受ける必要があります。

（注） デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。

- [Client Exclusion]：クライアント除外タイマーを設定するには、このチェックボックスをオンにします。

  （注） ユーザーが認証に失敗すると、ワイヤレスコントローラ はクライアントを接続から除外します。除外タイマーが期限切れになるまで、クライアントはネットワークへの接続を許可されません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。

e) [11v BSS Transition Support] で、次の設定を指定します。

- [BSS Max Idle Service]：アイドル期間タイマー値を設定するには、このチェックボックスをオンにします。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

  （注） BSS最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由でAPがこのクライアントをアソシエート解除しないタイムフレームのことです。

- [Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウトを設定するには、このチェックボックスをオンにします。

  （注） クライアントが送信するデータがユーザー アイドル タイムアウトとして指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラ は別のタイムアウト期間を開始します。

  デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザー アイドル タイムアウト付きで有効になっています。

- [Directed Multicast Service]：Directed Multicast Service 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。

  （注） デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service（DMS）を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するようにAPに要求します。これにより、クライアントは長時間スリープ状態になり、バッテリの電力が節約されます。

f) [Radius Client Profiling] で、このトグルボタンを使用して WLAN での RADIUS プロファイリングを有効または無効にします。

（注） この機能を有効にするには、1 つ以上の AAA または PSN サーバーが必要です。

g) （オプション）[NAS-ID] で、次の設定を指定します。

1. [NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。

   NAS IDのカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大 31 文字の英数字、特殊文字、およびスペースを入力で

きます。Cisco DNA Center はカスタムスクリプトでの特殊文字？" < および末尾のスペースをサポートしていません。

（注） Cisco DNA Center は、Cisco IOS XE リリース 17.7 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。

2. （オプション）[+] をクリックして、別の NAS ID を追加します。最大 3 つの NAS ID を追加できます。

（注） Cisco DNA Center は Cisco AireOS ワイヤレスコントローラ の 1 つの NAS ID のみ適用します。**[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウからサイトレベルで NAS ID を上書きできます。

h) [Configure CCKM]：このトグルボタンを使用して、Cisco DNA Center で認証キー管理オプションとして CCKM を有効にします。

- [Timestamp Tolerance]：このフィールドは、CCKM を有効にしている場合にのみ表示されます。CCKM 許容レベルを入力します。CCKM 許容レベルは、Cisco AireOS ワイヤレスコントローラ プラットフォームには適用されません。

（注） SSID に WPA2 または WPA2+WPA3 のエンタープライズとしてレイヤ 2 セキュリティがある場合にのみ、CCKM を設定できます。

i) （任意）[Configure Client Rate Limit] で、クライアント レート制限の値をビット/秒で入力します。有効な範囲は 8000 ～ 100000000000 です。値は 500 の倍数である必要があります。

（注） この構成は Cisco AireOS ワイヤレスコントローラには適用できません。Cisco AireOS ワイヤレスコントローラ のクライアントレート制限を設定するには、メニューアイコン（☰）をクリックして、 **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[Advanced SSID Configuration]**を選択します。詳細については、高度な SSID のモデル設定設計の作成を参照してください。

Cisco IOS XE デバイスのクライアントレート制限の有効範囲は次のとおりです。

- Cisco Catalyst 9800-L ワイヤレスコントローラ、Cisco Catalyst 9800-40 ワイヤレスコントローラ、および Cisco Catalyst 9800-80 ワイヤレスコントローラの有効範囲は、8000 ～ 67000000000 ビット/秒です。
- Cisco Catalyst 9800-CL ワイヤレスコントローラの有効範囲は、8000 ～ 10000000000 ビット/秒です。
- Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの有効範囲は、8000 ～ 2000000000 ビット/秒です。
- Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの有効範囲は、8000 ～ 100000000000 ビット/秒です。

j) （任意） [Coverage Hole Detection] トグルボタンを使用して、カバレッジホールの検出機能を有効または無効にします。

k) [Next] をクリックします。

ステップ 8 [Associate SSID to Profile] の手順を完了します。

a) 左側のペインからプロファイルを選択し、[Associate Profile] をクリックします。

プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （20 ページ）を参照してください。

b) [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 **[保存 (Save)]** をクリックします。

SSID が作成されます。

事前共有キーのオーバーライド

SSID はグローバル階層に作成されます。サイト、ビルディング、およびフロアは、グローバル階層から設定を継承します。サイト、ビルディング、またはフロア レベルで、事前共有キー（PSK）をオーバーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 左側の階層ツリーから、PSK を編集するサイト、ビルディング、またはフロアを選択します。

ステップ 3 [Enterprise Wireless] の下の [Passphrase] フィールドをクリックし、PSK SSID の新しいパスフレーズを入力します。

ステップ 4 **[保存（Save）]** をクリックします。

「`Passphrase for the SSID(s) updated successfully`」という成功メッセージが表示されます。

SSID の横にある検証アイコン にカーソルを合わせると、この設定の継承元が表示されます。

ステップ 5 PSK オーバーライドをリセットするには、サイト、ビルディング、またはフロアの PSK SSID の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。PSK はグローバルパスフレーズ値にリセットされます。

認証前アクセスコントロールリストの作成

認証前 ACL 機能を使用すると、Web 認証用の認証前 ACL を作成して、認証が完了する前に特定のタイプのトラフィックを許可できます。この ACL は、Cisco Identity Services Engine（ISE）の access-accept で参照され、ACL によって許可されるトラフィックと拒否されるトラフィック

を定義します。シスコ ワイヤレス コントローラで設定した ACL は、管理インターフェイス、AP マネージャインターフェイス、任意の動的インターフェイス、または WLAN に適用されてワイヤレスクライアントとの間の双方向のデータトラフィックを制御します。または、コントローラの中央処理装置（CPU）に適用してCPU宛のすべてのトラフィックを制御します。IPv4 と IPv6 の両方の ACL を設定できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Pre-Auth Access Control Lists] エリアで、[Add] をクリックして新しい認証前 ACL を作成します。

ステップ 5 [New Pre-Auth ACL] スライドインペインで、次のように設定します。

1. [Pre-Auth ACL List Name] フィールドに、ACL リストの名前を入力します。
2. [Pre-Auth ACL Name] フィールドに、認証前 ACL の名前を入力します。
3. [IP Addresses] タブをクリックし、作成する ACL タイプ（[IPV4] または [IPV6]）を選択します。

ステップ 6 [IP Addresses] タブをクリックし、作成する ACL タイプ（[IPV4] または [IPV6]）を選択します。

1. [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコルオプションは、[Any]、[TCP]、または [UDP] です。
2. [Source Port] フィールドに、送信元ポート番号を入力します。指定できる範囲は 0 ～ 65535 です。ポート オプションは、ネットワーキング スタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。
3. [Source IP Address] フィールドに、送信元の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、[Source IP Address] フィールドに送信元の IPv6 アドレスとプレフィックスの長さを入力します。
4. [Source Subnet] ドロップダウンリストから、送信元サブネットの値を選択します。
5. [Destination Port] に宛先ポート番号を入力します。
6. [Destination IP Address] に、宛先の IP アドレスおよびネットマスクを入力します。IPv6 ACL を設定している場合は、宛先の IPv6 アドレスとプレフィックス長を入力します。
7. [Destination Subnet] ドロップダウンリストから、宛先サブネットの値を選択します。
8. 複数のルールを追加するには、⊕アイコンをクリックします。最大256個のルールを追加できます。

ステップ 7 [Walled Garden URLs] タブをクリックして、キャプティブポータルとウォールドガーデンの Web 認証の許可リストに特定の URL を追加します。URL の許可リストにアクセスする際に認証は必要ありません。許可リストに含まれていないサイトにアクセスしようとすると、ログインページにリダイレクトされます。

ステップ 8 [URL] フィールドに URL を入力し、⊕ をクリックして Web 認証の許可リストに URL を追加します。最大 32 個の URL エントリを追加できます。

ステップ 9 **[Save]** をクリックします。

ステップ 10 エンタープライズ ワイヤレス ネットワークの SSID を作成するときに、ACL を SSID にマッピングします。

エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定

始める前に

- **[System Settings]** > **[External Services]** > **[Authentication and Policy Servers]** で、AAA サーバーが定義されていることを確認してください。
- この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSID] テーブルの [Action] 列で、AAA サーバーを設定する SSID に対して [Configure AAA] をクリックします。

ステップ 5 [Configure AAA Server] スライドインペインの [Configure Authentication and Authorization Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、AAA IP アドレスを選択します。

（注） [Configure AAA] オプションは、Mobility Express（ME）デバイスではサポートされていません。

ステップ 6 [+] をクリックして、[Additional Server] を追加します。

（注） Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ のエンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。

ステップ 7 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 8 アカウンティングに AAA サーバーを使用するには、[Copy Same Servers for Accounting] チェックボックスをオンにします。

ステップ 9 SSID に別のアカウンティングサーバーを設定するには、次の手順を実行します。

a) [Configure Accounting Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、アカウンティングサーバーの IP アドレスを選択します。

b) [+] をクリックして、[Additional Server] を追加します。

（注） Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ のエンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つのアカウンティング サーバーを設定できます。

c) [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 10 [構成] をクリックします。

（注） Cisco DNA Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Cisco DNA Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Cisco DNA Center によって作成されます。

サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。ワイヤレスデバイスプロビジョニングの概要を参照してください。

ゲスト ワイヤレス ネットワークの SSID の作成

この手順では、ゲスト ワイヤレス ネットワークの SSID を作成する方法について説明します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSID] テーブルで、[Add] の上にカーソルを合わせて、[Guest] を選択します。

ステップ 5 [Wireless SSID] ワークフローで、[Basic Settings] のセットアップを完了します。

a) [Wireless Network Name (SSID)] フィールドに、ワイヤレスネットワークの一意の名前を入力します。

b) [WLAN Profile Name] フィールドに、WLAN プロファイルの名前を入力します。

Cisco DNA Center は WLAN プロファイル名に基づいて、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシープロファイル名を自動的に生成します。

c) [Wireless Option] の設定で、次のいずれかのオプションボタンをクリックします。

- [Multi band operation（2.4 GHz, 5 GHz, 6GHz）]：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは無効になっています。
- [Multi band operation with band select]：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは有効になっています。
- [5 GHz only]：WLAN が 5 GHz 用に作成され、バンドセレクトは無効になっています。
- [2.4 GHz only]：WLAN が 2.4 GHz 用に作成され、バンドセレクトは無効になっています。
- [6GHz Only]：WLAN は 6 GHz 用に作成され、バンドセレクトは無効になっています。

d) [Primary Traffic Type] ドロップダウンリストから、次のいずれかのオプションを選択します。

- [VoIP (Platinum)]：ワイヤレスネットワークの QoS は、ワイヤレス音声およびデータトラフィック用に最適化されています。
- [Video (Gold)]：ワイヤレスネットワークの QoS はビデオトラフィック用に最適化されています。
- [Best Effort (Silver)]：ワイヤレスネットワークの QoS は、ワイヤレス データ トラフィック用にのみ最適化されています。
- [Non-real Time (Bronze)]：ワイヤレスネットワークの QoS は、低帯域幅の使用に最適化されています。

e) [SSID STATE] 設定では、トグルボタンをクリックして、次の設定を有効または無効にします。

- [Admin Status]：このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP は ワイヤレスコントローラ に関連付けられたままで、アクセス可能であり、AP には引き続きライセンスが必要です。
- [Broadcast SSID]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にするには、このトグルボタンを使用します。

ステップ 6 [Security Settings] の設定を完了します。

a) [L2 Security] 設定で、L2 暗号化および認証タイプを選択します。

- [Enterprise]：[WPA2] または [WPA3] のいずれかのセキュリティ認証タイプを設定するには、それぞれのチェックボックスをオンにします。デフォルトでは、[WPA2] チェックボックスが有効になっています。

  （注） Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。Fast transition は、エンタープライズ WPA2 SSID に適用できます。

  WPA3 セキュリティ認証は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。

  2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

- [Personal]：**WPA2** と **WPA3** の両方を設定したり、**WPA2** と **WPA3** を個別に設定したりするには、それぞれのチェックボックスをオンにします。

（注） WPA3 パーソナルセキュリティ認証は、パスワードベースの堅牢な認証を提供することによって個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるようになります。

[Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間で Pairwise Master Key（PMK; ペアワイズ マスター キー）として使用されます。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

（オプション）WPA2-Personal の場合、次の手順を実行してマルチ事前共有キー（MPSK）サポートを構成します。

1. [Configure MPSK] をクリックします。
2. [Configure MPSK] ダイアログ ボックスで、構成したいMPSK に対し [Add] をクリックします。最大 5 つの MPSK を追加できます。
3. [Priority] ドロップダウンリストから優先順位を選択します。

   （注） 優先順位 0 キーが中央 Web 認証（CWA）フレックスモードで設定されていない場合、WLAN へのクライアント接続が失敗する可能性があります。

4. [Passphrase Type] ドロップダウンリストから、パスフレーズタイプを選択します。
5. [Passphrase] フィールドに、パスフレーズを入力します。
6. [Save] をクリックします。

MPSK はCisco AireOS ワイヤレスコントローラでサポートされていません。 MPSK は、WPA2-Personal の 2 セキュリティ構成に適用されます。

- [Open Secured]：[Assign Open SSID] ドロップダウンリストから、オープン SSID に関連付けるためのオープン SSID を選択します。関連付けにより、オープン SSID が保護されます。オープンでセキュアな SSID に関連付ける前に、オープン SSID が作成されている必要があります。

  （注） Fast Transition は、オープンでセキュアな SSID には適用できません。

  オープンでセキュアな SSID はオープン SSID に依存しているため、オープンでセキュアな SSID でアンカーを有効にする前に、オープン SSID でアンカーを有効にしておく必要があります。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

b) [L3 Security] 設定で、L3 暗号化および認証タイプを選択します。

- [Web Policy]：L3 セキュリティを強化します。

[Authentication Server] で、これらの認証サーバー設定を指定します。

認証サーバ タイプ	説明
Central Web Authentication（中央 Web 認証）	中央 Web 認証（CWA）に AAA サーバーを使用します。 （オプション）CWA に Cisco ISE を選択した場合は、[What kind of portal are you creating today?] ドロップダウンリストで、作成するポータルのタイプを選択します。 • [Self Registered]：ゲストは自己登録ゲストポータルにリダイレクトされ、情報を提供して登録して、自動的にアカウントを作成します。 • [HotSpot]：ゲストはログイン情報なしでネットワークにアクセスできます。 （オプション）CWA に Cisco ISE を選択した場合は、[Where will your guests redirect after successful authentication?] ドロップダウンリストで、認証が成功した後にゲストをリダイレクトする場所を選択します。 • [Success page]：ゲストは **[** Authentication Success **]** ウィンドウにリダイレクトされます。 • [Original URL]：ゲストは最初にリクエストした URL にリダイレクトされます。 • [Custom URL]：ゲストはここで特定されたカスタム URL にリダイレクトされます。[Redirect URL] フィールドにリダイレクト URL を入力します。
• **Web 認証（内部）** • **Web 認証（外部）**	レイヤ 3 セキュリティ方式である Web 認証（Web Auth）を使用すると、クライアントは、何らかの認証方式に合格するまでの間、Dynamic Host Configuration Protocol（DHCP）およびドメインネームシステム（DNS）のトラフィックを通過させることができます。 Web 認証（内部）の場合、クライアントは シスコ ワイヤレス コントローラによって作成されたページにリダイレクトされます。 Web 認証（外部）の場合は、クライアントが、指定された URL にリダイレクトされます。[Web Auth Url] フィールドにリダイレクト URL を入力します。

認証サーバ タイプ	説明
• **Web パススルー（内部）** • **Web パススルー（外部）**	Web パススルーは、ゲストアクセスに使用されるソリューションであり、認証ログイン情報は必要ありません。Web パススルー認証では、ワイヤレスユーザーがインターネットを初めて使用するとき、使用ポリシーページにリダイレクトされます。ポリシーを承認すると、ユーザーはインターネットを使用できます。

- [Open]：レイヤ 3 レベルのセキュリティがなく、どのデバイスも SSID に接続できます。

c) [Web Authentication Internal]、[Web Authentication External]、[Web Passthrough Internal]、または [Web Passthrough External] を選択した場合、[Timeout Settings for sleeping clients] の設定で、スリープしているクライアントの認証を選択します。

- [Always authenticate]：スリープ状態のクライアントの認証が有効になります。
- [Authenticate after]：再認証が必要になるまでスリープ状態にあるクライアントが記憶される期間を入力します。有効範囲は 10 ～ 43200 分、デフォルト期間は 720 分です。

（注） ゲストアクセスで Web 認証済みクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 10 ～ 43200 分、デフォルトは 720 分です。WLAN にマッピングされるユーザ グループ ポリシーと WLAN に、期間を設定できます。スリープ タイマーは、アイドル タイムアウト後に有効になります。クライアントタイムアウトが WLAN のスリープタイマーに設定された時間より短い場合は、クライアントのライフタイムがスリープ時間として使用されます。

d) [Authentication, Authorization, and Accounting Configuration] で、[Configure AAA] をクリックして、ゲスト ワイヤレス ネットワーク SSID 用の AAA サーバーを追加および設定します。

詳細については、ゲスト ワイヤレス ネットワーク用の AAA サーバーの設定 （39 ページ）を参照してください。

e) [AAA Override] チェックボックスをオンにして、AAA オーバーライド機能を有効にします。

デフォルトでは、このチェックボックスはグレー表示されています。このチェックボックスを使用するには、[Configure AAA] オプションを使用して AAA サーバを設定する必要があります。

f) 次のチェックボックスをオンにします（複数可）。

- [Fast Lane]：このネットワークで fastlane 機能を有効にするには、このチェックボックスをオンにします。

（注） fastlane を有効にすると、最適化されたレベルのワイヤレス接続と 拡張 QoS を受信するように Cisco IOS デバイスを設定できます。

- [Identity PSK]（個人 L2 セキュリティ用）：SSID 内の個人またはユーザーグループのために作成できる一意の事前共有キーを有効にするには、このチェックボックスをオンにします。

- [MAC Filtering]：ワイヤレスネットワークでの MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。

  （注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。

- [Deny RCM Clients]：ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。

g) [Next] をクリックします。

ステップ 7 [Advance Settings] の設定を完了します。

a) [Fast Transition (802.11r)] で、次の手順を実行します。

- [Adaptive]、[Enable]、または [Disable] モードを選択します。

  （注） 802.11r を使用すると、ワイヤレスクライアントは、ある AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。

b) [MFP Client Protection] で、[Optional]、[Required]、または [Disabled] を選択します。

（注） 管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、AP とクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは、[Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 が ワイヤレスコントローラ 上で設定されており、クライアントも WPA2 用に設定されていて、CCXv5 MFP をサポートしている場合）にのみ、クライアントはアソシエーションを許可されます。

c) [Protected Management Frame (802.11w)] で、必要なオプションを選択します。

（注） [Protected Management Frame (802.11w)] で使用できるオプションは、[Level of Security] で選択した設定によって異なります。次のオプションを使用できる場合があります。

- **オプション**
- **必須**
- **Disabled**

d) [11K] で、次の設定を指定します。

- [Neighbor List]：このチェックボックスをオンにすると、すべての 11k 対応クライアントが、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できるようになります。

（注） ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバーAPのリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。この応答もアクション フレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

- [Session Timeout]：クライアントセッションがアクティブである最大時間を設定するには、このチェックボックスをオンにします。この時間が経過すると再認証を受ける必要があります。

  （注） デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。

- [Client Exclusion]：クライアント除外タイマーを設定するには、このチェックボックスをオンにします。

  （注） ユーザーが認証に失敗すると、ワイヤレスコントローラ はクライアントを接続から除外します。除外タイマーが期限切れになるまで、クライアントはネットワークへの接続を許可されません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。

e) [11v BSS Transition Support] で、次の設定を指定します。

- [BSS Max Idle Service]：アイドル期間タイマー値を設定するには、このチェックボックスをオンにします。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

  （注） BSS 最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由でAPがこのクライアントをアソシエート解除しないタイムフレームのことです。

- [Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウト期間を設定するには、このチェックボックスをオンにします。

  （注） クライアントが送信するデータがユーザー アイドル タイムアウト期間として指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラは別のタイムアウト期間を開始します。

  デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザー アイドル タイムアウト付きで有効になっています。

- [Directed Multicast Service]：Directed Multicast Service 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。

  （注） デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service（DMS）を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するようにAPに要求します。これにより、クライアントは長時間スリープ状態になり、バッテリの電力が節約されます。

f) （オプション）[NAS-ID] で、次の設定を指定します。

1. [NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。

   （オプション）NAS ID のカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大31 文字の英数字、特殊文字、およびスペースを入力できます。Cisco DNA Center はカスタムスクリプトでの特殊文字 ? " < および末尾のスペースをサポートしていません。

   （注） Cisco DNA Center は、Cisco IOS XE リリース 17.7 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。

2. （オプション）[+] をクリックして、別のネットワーク アクセス サーバー識別子を追加します。最大 3 つの NAS ID を追加できます。

   （注） Cisco DNA Center では Cisco AireOS コントローラに 1 つの NAS ID のみを適用します。**[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウからサイトレベルで NAS ID を上書きできます。

g) （任意） [Configure Client Rate Limit] で、クライアント レート制限の値をビット/秒で入力します。有効な範囲は 8000 ～ 100000000000 です。値は 500 の倍数である必要があります。

（注） この構成は Cisco AireOS ワイヤレスコントローラには適用できません。Cisco AireOS ワイヤレスコントローラのクライアントレート制限を設定するには、メニューアイコン（☰）をクリックして、 **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[Advanced SSID Configuration]**を選択します。詳細については、高度な SSID のモデル設定設計の作成を参照してください。

Cisco IOS XE デバイスのクライアントレート制限の有効範囲は次のとおりです。

- Cisco Catalyst 9800-L ワイヤレスコントローラ、Cisco Catalyst 9800-40 ワイヤレスコントローラ、および Cisco Catalyst 9800-80 ワイヤレスコントローラの有効範囲は、8000 ～ 67000000000 ビット/秒です。
- Cisco Catalyst 9800-CL ワイヤレスコントローラの有効範囲は、8000 ～ 10000000000 ビット/秒です。
- Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラの有効範囲は、8000 ～ 2000000000 ビット/秒です。
- Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの有効範囲は、8000 ～ 100000000000 ビット/秒です。

h) （任意） [Coverage Hole Detection] トグルボタンを使用して、カバレッジホールの検出機能を有効または無効にします。

i) [Next] をクリックします。

ステップ 8 [Associate SSID to Profile] の手順を完了します。

a) 左側のペインで、プロファイルをクリックします。

b) プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。

- [Profile Name]：ワイヤレスプロファイルの名前を入力します。
- （オプション）[WLAN Profile Name]：WLAN プロファイルの名前を入力します。

  Cisco DNA Center は WLAN プロファイル名に基づいて、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシープロファイル名を自動的に生成します。

  （注） SSID がネットワークプロファイルに関連付けられている場合、Cisco DNA Center がプロビジョニング中にこの WLAN プロファイル名を使用します。SSID を複数のネットワークプロファイルに関連付ける必要がある場合は、プロビジョニングの失敗を防ぐために、すべてのネットワークプロファイルで SSID に対して一意の WLAN プロファイル名を入力することをお勧めします。

- [Fabric]：SSID がファブリックか非ファブリックかを指定します。

  （注） ファブリック SSID は、ソフトウェア定義型アクセス（SD-Access）の一部であるワイヤレスネットワークです。SD アクセスは、有線およびワイヤレスネットワークの設定、ポリシー、およびトラブルシューティングを自動化し、簡素化するソリューションです。ファブリック SSID を使用する場合は、SD アクセスが必須です。非ファブリックは、SD アクセスを必要としない従来のワイヤレスネットワークです。

  非ファブリック SSID の場合は、次の設定を選択します。

  - [Interface]：[Interface Management] ドロップダウンリストからインターフェイスを選択するか、プラスアイコン をクリックして新しいワイヤレスインターフェイスを追加します。

    （注） これは、ワイヤレス インターフェイスに関連付けられている VLAN ID です。

  - [VLAN Group]：[VLAN Group Name] ドロップダウンリストから VLAN グループを選択するか、プラスアイコン をクリックして VLAN グループを追加します。

- [Do you need Anchor for this SSID?]：SSID をアンカーにするかどうかを選択します。

  [Yes] を選択した場合は、[Select Anchor Group] ドロップダウンリストから、SSID のアンカーグループを選択します。アンカーグループの詳細については、「アンカーグループの作成 （71 ページ）」を参照してください。

- [Flex Connect Local Switching]：WLAN のローカルスイッチングを有効にするには、チェックボックスをオンにします。ローカルスイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect AP がデータパケットをローカルにスイッチできます。

  （注） SSID に関して [Flex Connect Local Switching] を有効にしている場合、ネットワークプロファイルがマッピングされている特定のフロア上のすべての AP が FlexConnect モードに切り替わります。

c) [Associate Profile] をクリックして、プロファイルを選択します。
d) [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 SSID の設定を保存するには、[Save] をクリックします。

SSID が作成されます。

ゲスト ワイヤレス ネットワーク用の AAA サーバーの設定

始める前に

- **[System Settings]** > **[External Services]** > **[Authentication and Policy Servers]** ウィンドウで、AAA サーバーが定義されていることを確認してください。
- この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSID] テーブルの [Action] 列で、AAA サーバーを設定する SSID の [Configure AAA] をクリックします。

ステップ 5 [Configure AAA Server] スライドインペインの [Server] ドロップダウンリストから、[Search] フィールドに名前を入力して AAA IP アドレスを検索するか、AAA IP アドレスを選択します。

（注）
- ゲスト ワイヤレス ネットワークの中央 Web 認証（CWA）SSID 用に少なくとも 1 つの AAA またはポリシーサービスノード（PSN）サーバーを設定する必要があります。
- Cisco DNA Center では、アイデンティティ サービス エンジンの PSN とサードパーティ AAA IP の任意の組み合わせで AAA サーバーをマッピングできます。
- [Server] ドロップダウンリストで、**AAA** IP アドレスと PSN IP アドレスが対応するセクションにおいてグループ化されています。
- [Configure AAA] オプションは、Mobility Express（ME）デバイスではサポートされていません。

ステップ 6 [+] をクリックして、[Additional Server] を追加します。

（注） Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ のゲスト ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。

ステップ 7 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 8 （任意）サーバーまたは追加のサーバーを削除するには、各サーバーの横にある削除アイコンをクリックします。

ステップ 9 [構成] をクリックします。

（注） Cisco DNA Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Cisco DNA Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Cisco DNA Center によって作成されます。

サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。ワイヤレス デバイス プロビジョニングの概要を参照してください。

[SSID Scheduler] の作成

SSID スケジューラで、タイム ゾーンに基づいた WLAN の切り替えを設定できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 [SSID] テーブルで、[SSID Scheduler] をクリックします。

ステップ 4 [SSID Scheduler] ウィンドウで、[Add] をクリックします。

ステップ 5 [Create Scheduler] スライドインペインで、次の手順を実行します。

a) 作成する SSID スケジューラの一意の名前を入力します。
b) クライアントが SSID に参加することを拒否するには、[Client Deny] オプションボタンをクリックします。
c) [Enable SSID] をクリックして、SSID ブロードキャストをスケジュールします。
d) [Scheduler Type] として [Daily] 、[Weekly] 、または [Monthly] を選択し、必要な設定を完了します。
e) [Time Zone] ドロップダウンリストから、タイムゾーンを選択します。
f) [Save] をクリックします。

作成された SSID スケジューラが、[SSID Scheduler] テーブルに表示されます。

ステップ 6 SSID スケジューラを編集するには、次の手順を実行します。

a) [SSID Scheduler] テーブルから、任意の SSID スケジューラを選択し、[Edit] をクリックします。
b) [Edit SSID Scheduler] スライドインペインで、必要な変更を行い、[Save] をクリックします。

ステップ 7 SSID スケジューラを削除するには、SSID スケジューラを選択して [Delete] をクリックします。

ステップ 8 SSID スケジューラの詳細を表示するには、SSID スケジューラを選択し、[Scheduler History] をクリックします。

（注） [Scheduler History] を表示するには、アシュアランスパッケージをインストールする必要があります。

次のタスク

ワイヤレス コントローラの SSID スケジューラを有効にします。詳細については、ネットワークプロファイルへの SSID の追加を参照してください。

ワイヤレスインターフェイスの作成

非ファブリック展開でのみワイヤレスインターフェイスを作成できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Interfaces] テーブルで、[+Add] をクリックします。

ステップ 5 [Create a Wireless Interface] スライドペインでワイヤレスインターフェイスの設定を指定します。

a) [Interface Name] フィールドに、動的なインターフェイスの名前を入力します。

b) [VLAN ID] フィールドに、このインターフェイスの VLAN ID を入力します。

ステップ 6 [保存（**Save**）] をクリックします。

ワイヤレスインターフェイスが作成され、[Wireless Interfaces] テーブルに表示されます。

非ファブリック展開用のインターフェイスまたは VLAN グループの設計とプロビジョニング

Cisco DNA Center では、異なる VLAN を介して複数のブロードキャストドメインを持つネットワークを設定できます。同じ AP のセットが同じ WLAN をブロードキャストする場合、ブロードキャストドメインは、インターフェイスグループを介して同じ WLAN 上の複数の VLAN によって制御されます。

Cisco DNA Center インターフェイスグループは、ユーザー設定を容易にするインターフェイスの論理グループであり、同じインターフェイスグループを複数の WLAN で設定できます。その一方で、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。WLAN は、インターフェイスまたはインターフェイス グループに関連付けることができます。

（注） インターフェイス グループの名前とインターフェイスの名前を同じにすることはできません。

Cisco DNA Center VLAN グループ機能は、VLAN グループを使用して WLAN を 1 つまたは複数の VLAN にマッピングします。VLAN グループは、ポリシープロファイルに関連付けることができます。

次の手順では、非ファブリック展開のインターフェイスまたは VLAN グループを設計およびプロビジョニングする方法について説明します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 [VLAN Group] テーブルで、[Add] をクリックします。

[Add VLAN Group] スライドインペインが表示されます。

ステップ 4 有効な [VLAN Group Name] を入力し、リストから単一または複数のインターフェイスを選択して、[Save] をクリックします。

（注） 15 を超えるインターフェイスを選択すると、選択したインターフェイスが画面に正しく表示されない場合があります。

ステップ 5 [Edit Network Profile] ページで、VLAN グループが SSID に関連付けられます。

SSID の作成方法については、「エンタープライズ ワイヤレス ネットワーク用 SSID の作成」を参照してください。

ステップ 6 VLAN グループにさらに SSID を追加するには、[Add SSID] をクリックします。

ステップ 7 [Interface] または [VLAN] グループを選択します。

ステップ 8 [Add] アイコンをクリックして、新しいインターフェイスまたは VLAN グループを作成します。

（注） インターフェイスまたは VLAN グループは FlexConnect ローカルスイッチングには適用されません。

ステップ 9 [保存（**Save**）] をクリックします。

ステップ 10 [Configure Interface and VLAN] では、インターフェイス名、インターフェイスグループ名、およびインターフェイスと VLAN の設定に必要なその他のパラメータのリストを確認できます。

（注） インターフェイスグループには、64 を超えるインターフェイスを含めることはできません。

ステップ 11 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 12 デバイスを選択します。

ステップ 13 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 14 [Assign Site]、[Configuration]、[Model Configuration]、[Advanced Configuration]、および [Summary] 画面で詳細を確認します。各画面で、[Next] をクリックして次の画面に進みます。

ステップ 15 [展開（Deploy）] をクリックします。

[Provision Device] ダイアログボックスが表示されます。

ステップ 16 [Now] を選択し、[Apply] をクリックします。

「Task Scheduled view status in Tasks」というメッセージが表示されます。

ワイヤレス無線周波数プロファイルの作成

デフォルトの無線周波数プロファイル（低、標準、高）を使用することも、カスタムの無線周波数プロファイルを作成することもできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[Add] にカーソルを合わせて [Basic RF Profile] を選択します。

ステップ 5 [Create Wireless Radio Frequency Profile] ウィンドウの [Profile Name] フィールドに、RF プロファイル名を入力します。

ステップ 6 [2.4 GHz] タブで次を設定します。

a) [2.4 GHz] トグルボタンが有効になっていることを確認します。

（注） [2.4 GHz] トグルボタンを無効にすると、この RF プロファイルを使用するすべての AP で、該当する無線の管理ステータスが無効になります。Cisco DNA Center

b) [Parent Profile] で、[High]、[Medium（Typica）]、[Low]、[Custom] のいずれかを選択します。（[データレート（Data Rate）] および [Tx設定（Tx Configuration）] フィールドは、選択された親プロファイルによって変更されます。たとえば、[High] を選択した場合、2.4 GHz のデバイスで使用可能なプロファイル設定が追加されます。[Data Rate] および [Tx Configuration] の入力済みの設定を変更すると、[Parent Profile] が自動的に [Custom] に変更されます。選択したカスタムプロファイルに対してのみ、新しい RF プロファイルが作成されることに注意してください。

（注） [Low]、[Medium (Typical)]、および [High] は、デフォルトの RF プロファイルです。デフォルトの RF プロファイルを選択すると、デバイスで該当する RF プロファイルが使用され、Cisco DNA Center では新しい RF プロファイルは作成されません。

c) [DCA Channel] は、RF グループへのチャネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。

- **[すべて選択（Select All）]** チェックボックスをオンにして、DCA チャネル **[1]**、**[6]**、および **[11]** を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。
- **[詳細オプション（Advanced Options）]** の下で **[詳細設定を表示（Show Advanced）]** をクリックし、チャネル番号を選択します。

- [Select All] チェックボックスをオンにして、[Advanced Options] の下にある DCA チャネルを選択するか、個々のチャネル番号の横にあるチェックボックスをオンにします。使用可能なチャネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。

  （注） シスコ ワイヤレス コントローラ でチャネルをグローバルに設定する必要があります。

d) [Supported Data Rate] で、次を構成します。

- [Enable 802.11b data rates] チェックボックスをオンにして、802.11b データレートを有効にします。
- スライダを使用して、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設定します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。

e) [Mandatory Data Rates] で、個々のデータレートの横にあるチェックボックスをオンにします。最大 2 つのデータレートを選択できます。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

使用可能なデータレートは、[Supported Data Rate] で設定されたデータレートに応じて変わります。

f) [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定します。

- **電力レベル**：AP の電力を削減する必要があるかどうかを決定します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBm です。
- [TPC Power Threshold]：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
- **RX SOP**：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットの変調および復調を行う Wi-Fi 信号レベル（dBm 単位）を決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[高（High）]、[中（Medium）]、[低（Low）]、および [自動（Auto）] から選択します。

g) [Coverage Hole Detection] で、次のように設定します。

（注） **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM General Configuration]**で、対応する無線バンドのカバレッジホール検出をグローバルで有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータのモデル構成設計の詳細については、RRM 一般パラメータのモデル設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

h) [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注） Cisco AireOS ワイヤレスコントローラ では、クライアント数の上限はサポートされていません。

- Cisco IOS XE のバージョンが 17.7 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7 以降 17.9 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

i) [802.11ax] では、次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 7 [5 GHz] タブで次を設定します。

a) [5 GHz] トグルボタンが有効になっていることを確認します。

（注） [5 GHz] トグルボタンを無効にすると、Cisco DNA Center は、この RF プロファイルを使用するすべての AP で、該当する無線の管理ステータスを無効にします。

b) **[親プロファイル（Parent Profile）]** ドロップダウン リストから、**[高（High）]**、**[中（標準）（Medium (Typical)）]**、**[低（Low）]**、または**[カスタム（Custom）]** を選択します。（[データレート（Data Rate）] および [Tx設定（Tx Configuration）] フィールドは、選択された親プロファイルによって変更されます。たとえば、[高（High）] を選択した場合、2.4 GHz のデバイスで使用可能な設定が追加されます。[Data Rate] フィールドおよび [Tx Configuration] フィールドの入力済みの設定を変更すると、[Parent Profile] が自動的に [Custom] に変更されます。選択したカスタムプロファイルに対してのみ、新しい RF プロファイルが作成されます。

（注） [Low]、[Medium (Typical)]、および [High] は、デフォルトの RF プロファイルです。デフォルトの RF プロファイルを選択するとデバイスに既に存在するそれぞれの RF プロファイルが使用され、Cisco DNA Center では新しい RF プロファイルは作成されません。

c) [Channel Width] ドロップダウンリストから、チャネル帯域幅オプションとして [Best]、[20 MHz]、[40 MHz]、[80 MHz]、または [160 MHz] のいずれかを選択します。

d) [Zero Wait DFS] チェックボックスをオンにして、5 GHz 無線帯域の AP が待機時間なしで新しいチャネルに切り替えることを許可します。

（注） Cisco DNA Center は、Cisco IOS XE リリース 17.9.1 以降を実行する シスコ ワイヤレス コントローラ のゼロウェイト DFS をサポートします。

e) [DCA Channels] で次を設定して、チャネルの割り当てを管理します。

（注） シスコ ワイヤレス コントローラ でチャネルをグローバルに設定する必要があります。

- [Select All] チェックボックスをオンにして、DCA チャネル**UNII-1 36-48**、**UNII-2 52-144**、および**UNII-3 149-173**を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。
- [Show Advanced] をクリックして、各バンドのチャネル番号を選択します。
- [UNII-1 36-48]：UNII-1 バンドで使用可能なチャネルは、[36]、[40]、[44]、[48] です。[UNII-1 36-48] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-2 52-144]：UNII-2 バンドで使用可能なチャネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。[UNII-2 52-144] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-3 149-165]：UNII-3 バンドで使用可能なチャネルは、[149]、[153]、[157]、[161]、[165] です。[UNII-3 149-165] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。

f) アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[サポートされているデータレート（Supported Data Rate）] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

g) [Mandatory Data Rates] で、個々のデータレートの横にあるチェックボックスをオンにします。最大 2 つのデータレートを選択できます。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

使用可能なデータレートは、[Supported Data Rate] で設定されたデータレートに応じて変わります。

h) [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。

- [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBm です。
- [TPC Power Threshold]：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
- [RX SOP]：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[高（High）]、[中（Medium）]、[低（Low）]、および [自動（Auto）] から選択します。

i) [Coverage Hole Detection] で、次のように設定します。

（注） **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM General Configuration]**で、対応する無線バンドのカバレッジホール検出をグローバルで有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータのモデル構成設計の詳細については、RRM 一般パラメータのモデル設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

j) [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注） Cisco AireOS ワイヤレスコントローラ では、クライアント数の上限はサポートされていません。

- Cisco IOS XE のバージョンが 17.7 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7 以降 17.9 以前の場合、ワイヤレスコントローラのクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

k) [Flexible Radio Assignment（FRA）] で、[Client Aware] チェックボックスをオンにして、クライアント認識機能を有効にします。

この機能は5 GHz の専用無線を監視し、クライアントの負荷がしきい値を超えると、FRA がモニターロールから 5 GHz ロールに自動的に切り替わり、セルの容量をオンデマンドで効率的に倍増します。容量の心配がなくなり、Wi-Fi の負荷が正常に戻ると、無線で前のロールが再開されます。

（注） **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM FRA Configuration]**で、対応する無線バンドの FRA を有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM FRA パラメータのモデル構成設計の詳細については、RRM FRA パラメータのモデルkousei 設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。

クライアント対応機能を有効にする場合は、次のように構成します。

- [Client Select (%)] フィールドに、クライアント選択の値を入力します。有効な範囲は 0 ～ 100% です。デフォルト値は 50% です。
- [Client Reset (%)] フィールドに、クライアントのリセット値を入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 5 パーセントです。

l) [802.11ax] では、次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。

- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 8 [6 GHz] タブで次を設定します。

a) [6 GHz] トグルボタンが有効になっていることを確認します。

（注） 6 GHz 無線は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラでしかサポートされていません。[6 GHz] トグルボタンを無効にすると、Cisco DNA Center は、この RF プロファイルを使用するすべての AP で、該当する無線の管理ステータスを無効にします。

b) [Enable PSC Enforcing] トグルボタンを有効にして、優先スキャンチャネル（PSC）の適用を許可します。

PSC の適用は、PSC 対応チャネルに優先順位を付けることにより、6 GHz デバイスの接続を改善します。

（注） PSC の適用を有効にすると、非 PSC チャネルの隣のチェックボックスがグレー表示になります。

c) [DCA Channels] で次を設定して、チャネルの割り当てを管理します。

- [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。
  - **UNII-5 1-93**
  - **UNII-6 97-113**
  - **UNII-7 117-185**
  - **UNII-8 189-233**
- [Show Advanced] をクリックして、各バンドのチャネル番号を選択します。

（注） シスコ ワイヤレス コントローラ でチャネルをグローバルに設定する必要があります。

d) アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[サポートされているデータレート（Supported Data Rate）] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

e) [Mandatory Data Rates] で、個々のデータレートの横にあるチェックボックスをオンにします。最大 2 つのデータレートを選択できます。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

使用可能なデータレートは、[Supported Data Rate] で設定されたデータレートに応じて変わります。

f) [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。

- [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBm です。
- [TPC Power Threshold]：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
- [RX SOP]：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[高（High）]、[中（Medium）]、[低（Low）]、および [自動（Auto）] から選択します。

g) [Coverage Hole Detection] で、次のように設定します。

（注） **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM General Configuration]**で、対応する無線バンドのカバレッジホール検出をグローバルで有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータのモデル構成設計の詳細については、RRM 一般パラメータのモデル設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

h) [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注） Cisco AireOS ワイヤレスコントローラ では、クライアント数の上限はサポートされていません。

- Cisco IOS XE のバージョンが 17.7 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7 以降 17.9 以前の場合、ワイヤレスコントローラのクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

i) [Flexible Radio Assignment（FRA）] で、次の手順を実行します。

（注）
- **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM FRA Configuration]**で、対応する無線バンドの FRA を有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM FRA パラメータのモデル構成設計の詳細については、RRM FRA パラメータのモデルkousei 設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。
- FRA は、Cisco IOS XE 17.9.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。

- [Client Reset Count] フィールドに、クライアントのリセット回数の値を入力します。有効な範囲は 0 ～ 10 です。デフォルト値は 1 です。
- [Client Utilization Threshold（%）] フィールドに、クライアントの使用率のしきい値を入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 5 パーセントです。

j) 802.11ax では、次の複数の基本サービスセット識別子（BSSID）および空間再利用パラメータを構成します。

- [6 GHz Discovery Frames] ドロップダウンリストから、必要なオプションを [None] 、[Broadcast Probe Response] 、および [FILS Discovery] から選択します。

  6 GHz 無線が唯一の動作可能な無線である場合は、6 GHz 検出フレームが必要です。6 GHz 検出フレームの詳細については、[Learn More] をクリックしてください。
- [Broadcast Probe Response Interval（msec）] フィールドに、ブロードキャストプローブ応答間隔をミリ秒単位で入力します。有効な範囲は 5 ミリ秒から 25 ミリ秒です。デフォルト値は 20 ミリ秒です。
- [MULTI BSSID] で、チェック ボックスをオンにして、次のパラメータを有効にします。
  - ダウンリンク OFDMA
  - アップリンク OFDMA
  - ダウンリンク MU-MIMO
  - アップリンク MU-MIMO
  - ターゲット起動時間
  - TWT ブロードキャストのサポート

（注） 対応する無線バンドの**[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[Dot11ax Configuration]**でBSSIDを有効にし、管理しているワイヤレスコントローラでそれをプロビジョニングする必要があります。Dot11ax のモデル構成設計の詳細については、Dot11ax 設定のモデル設定設計の作成 を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニングを参照してください。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 9 **[Save]** をクリックします。

ステップ 10 プロファイルをデフォルトの RF プロファイルとしてマークするには、[Profile Name] チェックボックスをオンにし、[Mark Default] をクリックします。

ステップ 11 **[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

基本無線周波数プロファイルの編集または削除

次の手順では、基本 RF プロファイルを編集または削除する方法について説明します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Radio Frequency Profile] 領域で、[Basic RF Profile] タブをクリックします。

（注） [Basic RF Profile] テーブルには、[Profile Name] 、[Type] 、[2.4 GHz Data Rates] 、[5 GHz Data Rates] 、[6 GHz Data Rates] 、[Channel Width] 、および [Profile Type] に基づいて作成された 基本 RF プロファイルの数がリストされます。

ステップ 5 編集する基本プロファイル名の横にあるチェックボックスをオンにします。

ステップ 6 [Actions] ドロップダウンリストから、[Edit/View] を選択します。

（注） 一度に 1 つの基本 RF プロファイルを編集できます。

ステップ 7 [Edit Wireless Radio Frequency Profile] ウィンドウで、基本 RF プロファイル設定を構成します。詳細については、ワイヤレス無線周波数プロファイルの作成 （43 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 基本 RF プロファイルを削除するには、基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 10 [Actions] ドロップダウンリストから、[Delete] を選択してから [Yes] をクリックします。

ステップ 11 基本 RF プロファイルをデフォルトとしてマークするには、基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 12 [Action] ドロップダウンリストから、[Mark Default] を選択してから [Yes] をクリックします。

AI 無線周波数プロファイルを設定するための前提条件

- システム設定で Cisco AI Network Analytics を有効にする必要があります。詳細については、*Cisco DNA Center* 管理者ガイドの「Cisco AI Network Analytics データ収集の設定」を参照してください。
- システム設定の [Cisco AI Analytics] で [AI Enhanced RRM] を有効にする必要があります。メニューアイコン（☰）をクリックして、 **[System]** > **[Settings]** > **[External Services]** > **[Cisco AI Analytics]**の順に選択します。

  [Cisco AI Analytics] ウィンドウの [AI ENHANCED RRM] エリアで、トグルボタンをクリックして AI 拡張 RRM を有効にします。
- Cisco AI RF プロファイルは、Cisco IOS XE 17.7.1 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でのみサポートされています。

（注） 3 つの帯域すべて（2.4 GHz、5 GHz、および 6 GHz）の [Group Mode] オプションが、ワイヤレスコントローラで[Auto] または [Leader] として設定されていることを確認します。

- Cisco AI RF プロファイルは Cisco IOS XE 17.9.1 以降を搭載した ワイヤレスコントローラで、6-GHz 無線のみサポートされています。
- **スーパー管理者**または**ネットワーク管理者**である必要があります。

AI 無線周波数プロファイルの作成

次の手順では、建物の AI 無線周波数プロファイルの作成方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （53 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[Add] にカーソルを合わせて [AI RF Profile] を選択します。

ステップ 5 **[Create AI Radio Frequency Profile]** ウィンドウの **[Profile Name]** フィールドに、RF プロファイル名を入力します。

ステップ 6 [Basic Settings] の[Radio Frequency Settings area] エリアで、[2.4 GHz] 、[5 GHz] 、[6 GHz] チェックボックスをオンにします。

無線周波数はデフォルトでオンになっています。無線周波数をオフにすると、その無線周波数の RF 設定が無効になります。

（注） [6 GHz] 無線帯域の AI RF プロファイルは、Cisco IOS XE 17.9.1 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポートされています。

ステップ 7 [Busy Hours] エリアで、サイトのタイムゾーンの開始時刻と終了時刻を定義します。

（注） ビジー時間は、建物のタイムゾーンによって異なります。それぞれの建物のネットワーク設定でタイムゾーンを構成する必要があります。

ステップ 8 [Busy Hour Sensitivity] エリアで、[Low]、[Medium]、または [High] オプションボタンをクリックして、ビジー時間間隔の無線リソース管理（RRM）感度のしきい値を定義します。

ステップ 9 [Enable RF Settings] エリアで、[2.4 GHz] 、[5 GHz] または [6 GHz] 列の下にあるトグルボタンをクリックして、それぞれの RF 設定の無線帯域を有効または無効にします。

サポートされている RF 設定は次のとおりです。

- [Flexible Radio Assignment (FRA)]：FRA は帯域ごとの無線カバレッジを最適化し、冗長無線の最適なロール割り当てを決定します。
- [Dynamic Channel Assignment (DCA)]：DCA は、RF グループへのチャネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。
- [Transmit Power Control (TPC)]：TPC は AP の電力を管理および送信します。また、干渉の低減中に SNR を最大化します。
- [Dynamic Bandwidth Selection (DBS)]：DBS は、チャネル幅を監視および調整して、パフォーマンスと干渉のバランスをとります。

（注）
- FRA の [2.4 GHz] 無線帯域を無効にすると、FRA の [5 GHz] 無線バンドが自動的に無効になります。逆の場合も同様です。
- DCA の [5 GHz] 無線帯域を無効にすると、FRA の [2.4 GHz] 無線帯域と FRA と DBS の [5 GHz] 無線帯域が無効になります。
- DCA および TPC の [2.4 GHz] 無線帯域と、DCA、TPC、および DBS の [5 GHz] 無線帯域を個別に有効にできます。[5 GHz] 無線帯域の場合、DCA と DBS が無効になっているときに DBS を有効にすると、DCA も有効になります。
- DCA および DBS RF 設定で [6 GHz] 無線帯域をまとめて有効または無効にできます。TPC の [6 GHz] 無線帯域を個別に有効にできます。
- FRA は、[6 GHz] 無線帯域ではサポートされていません。

ステップ 10 [Advanced] を展開し、[2.4 GHz] トグルボタンをクリックします。

a) [DCA Channel] エリアで、[Select All] チェックボックスをオンにして、DCA チャネル [1]、[6]、および [11] を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。

b) [Advanced Options] エリアで、[Select All] チェックボックスをオンにして、すべての DCA チャネルを選択します。

c) [Show Advanced] をクリックして、残りのチャネル番号を選択します。

d) 個々のチャネル番号の横にあるチェックボックスをオンにします。プロファイルで使用可能なチャネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。

e) [Supported Data Rate] エリアで、次を構成します。

- [Enable 802.11b data rates] チェックボックスをオンにして、802.11b データレートを有効にします。このアクションにより、[Mandatory Data Rates] エリアの [802.11b supported data rate] チェックボックスも有効になります。
- スライダを使用して、AP とクライアント間でデータを送信できるレートを設定します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。

f) [Mandatory Data Rates] エリアで、個々のデータレートの横にあるチェックボックスをオンにします。最大 2 つのデータレートを選択できます。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。

g) [Tx Power Configuration] エリアで、次を設定します。

- [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネル干渉を軽減できます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。範囲は、-10 ～ 30 dBm です。最小のデフォルトは -10 dBm で、最大のデフォルトは 30 dBm です。
- [TPC Power Threshold] ：RRM を使用したカットオフ信号レベルです。AP の電力レベルを削減するかどうかを判断します。[TPC Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBm で、デフォルトのしきい値は -70 dBm です。

- **RX SOP**：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットの変調および復調を行う Wi-Fi 信号レベル（dBm 単位）を決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[High]、[Medium]、[Low]、および [Auto] から選択します。

h) [Coverage Hole Detection] で、次のように設定します。

（注） **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM General Configuration]**で、対応する無線バンドのカバレッジホール検出をグローバルで有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータのモデル構成設計の詳細については、RRM 一般パラメータのモデル設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

i) [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注）
- Cisco IOS XE のバージョンが 17.7.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7.1 以降 17.9.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9.1 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

j) [802.11ax] では、次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。

- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 11 [Advanced] エリアで、[5 GHz] トグルボタンをクリックします。

a) [Zero Wait DFS] チェックボックスをオンにすると、5 GHz 無線の AP を待機時間なしで新しいチャネルに切り替えることができます。

（注） Cisco DNA Center は、Cisco IOS XE リリース 17.9.1 以降を実行する シスコ ワイヤレスコントローラ のゼロウェイト DFS をサポートします。

b) [DBS Max Width] スライダを使用して、AI RF プロファイルのチャネル幅を設定します。

使用可能なチャネル幅オプションは、[20 MHz]、[40 MHz]、[80 MHz]、または [160 MHz] です。

[Auto Channels Logic] エリアには、Unlicensed National Information Infrastructure（UNII）無線帯域で使用可能なチャネル幅のチャネルが色分けされて表示されます。

DBS が有効な場合にのみ、[DBS Max Width] を選択できます。

DBS を無効にすると、Cisco DNA Centerでは静的チャネル幅を選択できます。

c) [DCA Channel] を設定して、次のチャネルの割り当てを管理します。

- [UNII-1 36-48]：UNII-1 バンドで使用可能なチャネルは、[36]、[40]、[44]、[48] です。
- [UNII-2 52-144]：UNII-2 バンドで使用可能なチャネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。
- [UNII-3 149-165]：UNII-3 バンドで使用可能なチャネルは、[149]、[153]、[157]、[161]、[165] です。

d) [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。

e) [Show Advanced] をクリックして、それぞれの DCA チャネル番号を確認、選択します。

- [UNII-1 36-48] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-1 36-48] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-3 149-165] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。

f) AP とクライアント間でデータを転送できるレートを設定するには、[Supported Data Rate] スライダを使用します。使用可能なデータレートは、[6]、[9]、[11]、[12]、[18]、[24]、[36}、[48}、[54] です。

g) [Mandatory Data Rates] エリアで、個々のデータレートの横にあるチェックボックスをオンにします。最大 2 つのデータレートを選択できます。使用可能なデータレートは、[6] 、[9] 、[11] 、[12] 、[18] 、[24] 、[36} 、[48} 、[54] です。

h) [Tx Power Configuration] エリアで、[Power Level]、[Power Threshold]、および [RX SOP] を設定します。

- [電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。範囲は、-10 ～ 30 dBm です。最小のデフォルトは -10 dBm で、最大のデフォルトは 30 dBm です。
- [TPC Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBm で、デフォルトのしきい値は -70 dBm です。
- [RX SOP] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、および [Auto] から選択します。

i) [Coverage Hole Detection] で、次のように設定します。

（注） **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM General Configuration]**で、対応する無線バンドのカバレッジホール検出をグローバルで有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータのモデル構成設計の詳細については、RRM 一般パラメータのモデル設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

j) [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注）
- Cisco IOS XE のバージョンが 17.7.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7.1 以降 17.9.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9.1 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

k) [802.11ax] では、次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 12 [Advanced] エリアで、[6 GHz] トグルボタンをクリックします。

a) [DBS Width] スライダを使用して、AI RF プロファイルの最小および最大のチャネル幅を設定します。

使用可能なチャネル幅オプションは、[20 MHz]、[40 MHz]、[80 MHz]、または [160 MHz] です。

[Auto Channels Logic] エリアには、UNII 無線帯域で使用可能なチャネル幅のチャネルが色分けされて表示されます。

DBS が有効な場合にのみ、**[DBS Width]** を選択できます。

b) [Enable PSC Enforcing] トグルボタンを有効にして、優先スキャンチャネル（PSC）の適用を許可します。

PSC の適用は、PSC 対応チャネルに優先順位を付けることにより、6 GHz デバイスの接続を改善します。

（注） PSC の適用を有効にすると、非 PSC チャネルの隣のチェックボックスがグレー表示になり、PSC チャネルの隣のチェック ボックスがデフォルトでオンになります。必要に応じて、使用したい PSC チャネルのチェックボックスをオフにできます。

c) **[DCA Channels]** を設定して、次のチャネルの割り当てを管理します。

- UNII-5 1-93：UNII-5 帯域で使用できるチャネルは、1 、5 、9 、13 、17 、21 、25 、29 、33 、37 、41 、45 、49 、53 、57 、61 、65 、69 、73 、77 、81 、85 、89 、および 93 。
- UNII-6 97-113：UNII-6 帯域で使用できるチャネルは、97 、101 、105 、109 、および 113 です。
- UNII-7 117-185 ：UNII-7 帯域で使用可能なチャネルは 117 、121 、125 、129 、133 、137 、141 、145 、149 、153 、157 、161 、165 、169 、173 、177 、181 、および 185 。
- UNII-8 189-233：UNII-8 帯域で使用できるチャネルは、189 、193 、197 、201 、205 、209 、213 、217 、221 、225 、229 、および 233 です。

d) [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。

e) [Show Advanced] をクリックして、残りの DCA チャネル番号を選択します。

- [UNII-5 1-93] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-7 117-185] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-8 189-233] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。

f) AP とクライアント間でデータを転送できるレートを設定するには、[Supported Data Rate] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

g) [Tx Power Configuration] エリアで、[Power Level]、[TPC Power Threshold]、および [RX SOP] を設定します。

- [電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBm です。
- [TPC Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBm で、デフォルトのしきい値は -70 dBm です。
- [RX SOP] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、および [Auto] から選択します。

h) [Coverage Hole Detection] で、次のように設定します。

（注） **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[RRM General Configuration]**で、対応する無線バンドのカバレッジホール検出をグローバルで有効にし、それを管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータのモデル構成設計の詳細については、RRM 一般パラメータのモデル設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

i) [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注）
- Cisco IOS XE のバージョンが 17.7.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7.1 以降 17.9.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9.1 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

j) 802.11ax では、次の複数の基本サービスセット識別子（BSSID）および空間再利用パラメータを構成します。

- [6 GHz Discovery Frames] ドロップダウンリストから、必要なオプションを [None] 、[Broadcast Probe Response] 、および [FILS Discovery] から選択します。

  6 GHz無線が唯一の動作可能な無線である場合は、6 GHz 検出フレームが必要です。6 GHz 検出フレームの詳細については、[Learn More] をクリックしてください。
- [Broadcast Probe Response Interval（msec）] フィールドに、ブロードキャストプローブ応答間隔をミリ秒単位で入力します。有効な範囲は 5 ミリ秒から 25 ミリ秒です。デフォルト値は 20 ミリ秒です。
- [MULTI BSSID] で、チェック ボックスをオンにして、次のパラメータを有効にします。
  - ダウンリンク OFDMA
  - アップリンク OFDMA
  - ダウンリンク MU-MIMO

- アップリンク MU-MIMO
- ターゲット起動時間
- TWT ブロードキャストのサポート

（注） 対応する無線バンドの**[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[Dot11ax Configuration]**でBSSIDを有効にし、管理しているワイヤレスコントローラでそれをプロビジョニングする必要があります。Dot11axのモデル構成設計の詳細については、Dot11ax設定のモデル設定設計の作成を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニングを参照してください。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 13 [Save] をクリックします。

AI 無線周波数プロファイルの編集

次の手順では、AI RF プロファイルを編集する方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （53 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。

[AI RF Profile] テーブルには、[Profile Name]、[Busy Hours]、[Busy Hour Sensitivity]、[FRA]、[DCA]、[DBS]、[TPC]、および [Mapped Buildings] に基づいて作成された AI RF プロファイルの数がリストされます。

ステップ 5 編集する AI RF プロファイル名の横にあるチェックボックスをオンにします。

一度に 1 つの AI RF プロファイルを編集できます。

ステップ 6 [Edit/View] をクリックします。

ステップ 7 [Edit AI RF Profile] ウィンドウで、AI RF プロファイル設定を構成します。詳細については、AI 無線周波数プロファイルの作成 （53 ページ）を参照してください。

ステップ 8 [Save] をクリックします。

AI 無線周波数プロファイルの削除

次の手順では、AI RF プロファイルを削除する方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （53 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。

[AI RF Profile] テーブルには、[Profile Name]、[Busy Hours]、[Busy Hour Sensitivity]、[FRA]、[DCA]、[DBS]、[TPC]、および [Mapped Buildings] に基づいて作成された AI RF プロファイルの数がリストされます。

ステップ 5 AI RF プロファイルを削除するには、削除する AI RF プロファイルの横にあるチェックボックスをオンにします。

ステップ 6 [Delete] をクリックし、[Yes] をクリックします。

（注） Cisco DNA Center では、建物にすでに割り当てられている AI RF プロファイルを削除することはできません。

AI 無線周波数プロファイルの構成

次の手順では、AI RF プロファイルを建物に割り当てる方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （53 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Configure AI RF Profile]**の順に選択します。

ステップ 2 [Assign AI RF Profiles] ウィンドウで、[Let's Do it] をクリックしてワークフローに直接移動します。

ステップ 3 [Configure AI RF Profile] ウィンドウの [Task Name] フィールドにタスク名を入力します。

ステップ 4 [Select Locations to Assign AI RF Profiles] ウィンドウで、AI 対応 RF プロファイルを割り当てる場所を選択します。[Find Hierarchy] フィールドに名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

[Site selection summary] テーブルには、サイト階層内のサイト選択に基づいてサイトがリストされ、選択されたサイトの [Selected Location] と [Impacted Location] が表示されます。

- [Selected Locations]：AI RF プロファイルが有効になっている場所。
- [Impacted Locations]：選択した場所と同じワイヤレスコントローラによって部分的に管理されている場所。

（注） コントローラが複数の建物を管理していて、1 つの建物でのみ AI RF プロファイルを有効にすると、Cisco DNA Center は自動的に他の建物で同じ AI RF プロファイルを有効にします。

たとえば、2 つのコントローラが 3 つの建物を管理していて、1 つの建物で AI RF プロファイルを有効にすると、Cisco DNA Center は自動的に他の 2 つの建物で同じ AI RF プロファイルを有効にします。

ステップ 5 [Select AI RF Profiles to assign] ウィンドウの [Building] テーブルには、[Location]、[Floors]、[Current RF Profiles]、および [Replace with AI RF Profiles] に基づいた AI RF プロファイルが一覧表示されます。

a) [Building] テーブルで、場所の横にあるチェックボックスをオンにして、AI RF プロファイルを選択します。

b) 場所に基づいて、[Replace with AI RF Profiles] の下のドロップダウンリストから AI 対応 RF プロファイルを選択して、現在の AI RF プロファイルに置き換えます。

c) AI RF プロファイルが作成されていない場合は、[Action] 列の下にある 3 つのドットをクリックして新しい AI RF プロファイルを作成するか、現在の RF プロファイルと AI 設定をコピーします。

d) [Select AI RF Profiles to assign] ウィンドウの [Create a new AI RF Profile to apply] リンクから AI RF プロファイルを作成することもできます。詳細については、AI 無線周波数プロファイルの作成 （53 ページ）を参照してください。

ステップ 6 [Details of selected AI RF Profile] ウィンドウで、AI 対応 RF プロファイルの [AI Settings]、[Common Settings]、および [Assignment] の詳細を確認します。

（注） AI 拡張 RRM の計算は 30 分ごとに発生します。RRM の決定は、計算後に更新され、デバイスにプッシュされます。

ステップ 7 [Summary] ウィンドウで、[Task Details]、[Select Locations to Assign AI RF Profiles]、[Select AI RF Profiles to assign] を確認します。

ステップ 8 [Deploy the AI RF Profiles] ウィンドウで、プロファイルを今すぐ展開する（[Now]）か、後でスケジュールするかを選択します。

ステップ 9 [Continue] をクリックします。
タスク完了AI RF Profiles Assigned] ウィンドウが開きます。

ステップ 10 メニューアイコン（☰）をクリックして、**[Activities]** > **[Tasks]**の順に選択します。

ステップ 11 [Tasks] ウィンドウで、タスクのリンクをクリックします。

slide-in paneに、[Assigned Building(s)]、[Selected AI RF Profile]、および [Selected AI RF Profile] が表示されます。

既存の AI RF プロファイルへの場所の割り当て

次の手順では、既存の AI RF プロファイルに場所を割り当てる方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （53 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。
[AI RF Profile] テーブルに、作成された AI RF プロファイルの数が一覧表示されます。

ステップ 5 AI RF プロファイルの [Action] 列の下にある 3 つのドットをクリックします。

ステップ 6 ドロップダウンリストから [Assign Location] を選択します。

[Manage Location Assignment] ウィンドウが開きます。

ステップ 7 [Search] フィールドに名前を入力してサイトを検索するか、[All Sites] を展開してサイトを選択します。

（注）
- サイト階層は、AI 対応の場所を示しています。
- AI プロファイルの対象とならないサイトまたは建物は無効になっています。
- 建物の下のフロアは選択できません。AI 対応 RF プロファイルに建物を選択すると、その下のフロアが自動的に割り当てられます。

同じワイヤレスコントローラが他の建物を管理している場合は、[Confirm Impacted Sites] ウィンドウが開きます。

ステップ 8 確認し、[Confirm] をクリックして、選択したサイトを AI 対応 RF プロファイルに割り当てます。

ステップ 9 [**Assign**] をクリックします。

[Download a Backup of Current RF Settings] ウィンドウが開き、選択した建物全体の RF 設定のバックアップをダウンロードできます。

ステップ 10 （任意） バックアップリンクをクリックして、.csv ファイルをローカルマシンにダウンロードします。

ステップ 11 [Confirm] をクリックします。

ステップ 12 表示される確認ウィンドウで、[Confirm] をクリックします。

[AI RF Profile] テーブルでは、AI RF プロファイルに割り当てられた場所が [Mapped Buildings] 列の下に表示されます。

次のタスク

AI RF プロファイル対応建物のデバイスのプロビジョニング

次の手順では、AI RF プロファイルを展開するためにロケーション全体のデバイスをプロビジョニングする方法について説明します。

1. メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

   [Inventory] ウィンドウの [Device] テーブルには、検出された AI RF プロファイルに関連付けられたデバイスが一覧表示されます。

2. プロビジョニングする AI RF プロファイルに関連付けられたデバイス名の横にあるチェックボックスをオンにします。

3. [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

4. すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。

5. [Summary] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認します。詳細については、ワイヤレスデバイスプロビジョニングの概要を参照してください。

既存の AI RF プロファイルへの場所の割り当ての解除

次の手順では、既存の AI RF プロファイルから場所の割り当てを解除する方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （53 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。
[AI RF Profile] テーブルに、作成された AI RF プロファイルの数が一覧表示されます。

ステップ 5 AI RF プロファイルの [Action] 列の下にある 3 つのドットをクリックします。

ステップ 6 ドロップダウンリストから [Unassign Location] を選択します。

[Unassign AI RF Profile] ウィンドウが開きます。

ステップ 7 サイトの横にあるチェックボックスをオンにして、AI RF プロファイルの割り当てを解除します。

ステップ 8 [Select from available RF Profiles] オプションボタンをクリックして、選択した場所に割り当てる使用可能な RF プロファイルを選択します。

ステップ 9 [Select RF Profile to Replace] ドロップダウンリストから、RF プロファイルを選択します。

[Select RF Profile to Replace] ドロップダウンリストには、AI RF プロファイルと基本 RF プロファイルが表示されます。

ドロップダウンリストから基本的な RF プロファイルを選択すると、[Confirm Impacted Sites] ウィンドウで、同じワイヤレスコントローラが他のサイトを管理しているかどうかが検証されます。

[Confirm Impacted Sites] ウィンドウを確認し、[Confirm] をクリックして、選択したサイトを選択した RF プロファイルに割り当てます。

ステップ 10 [Upload a CSV with RF settings back] をクリックして、ローカルマシンから RF 設定のバックアップをアップロードします。

ステップ 11 [Choose a file] をクリックして CSV ファイルをインポートするか、CSV ファイルをドラッグ アンド ドロップ エリアにドラッグアンドドロップします。

（注） CSV ファイルの最大サイズは 10 MB です。

アップロードされた CSV ファイルから、選択したロケーション名に基づく RF 設定が見つかった場合、[Confirm RF Settings for Selected Locations] ウィンドウに [Location] と [Matched RF Profiles] が表示されます。

ステップ 12 [Confirm RF Settings for Selected Locations] ウィンドウを確認し、[Confirm] をクリックします。

ステップ 13 [Unassign] をクリックします。

ステップ 14 確認ウィンドウで、[Continue] をクリックします。

ステップ 15 メニューアイコン（☰）をクリックして、**[Activities]** > **[Tasks]**を選択して、AI RF プロファイルタスクへの次回、進行中、完了、および失敗したロケーションの割り当て解除を表示します。

次のタスク

AI RF プロファイル対応建物のデバイスのプロビジョニング

次の手順では、AI RF プロファイルが割り当てられたロケーション全体にデバイスをプロビジョニングして、AI RF プロファイルを展開する方法について説明します。

1. メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

   [Inventory] ウィンドウの [Device] テーブルには、検出された AI RF プロファイルに関連付けられたデバイスが一覧表示されます。

2. プロビジョニングする AI RF プロファイルに関連付けられたデバイス名の横にあるチェックボックスをオンにします。
3. [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
4. すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。
5. [概要] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認します。詳細については、ワイヤレス デバイス プロビジョニングの概要を参照してください。

基本無線周波数プロファイルをAI無線周波数プロファイルにアップグレードする

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （53 ページ）を参照してください。

AI 拡張 RRM サービスにサイトをオンボードするには、次のサービスの少なくとも 1 つを有効にする必要があります。

- フレキシブル ラジオ アサインメント（FRA）
- 動的チャネル割り当て（DCA）
- 伝送パワー コントロール（TPC）[でんそうぱわーこんとろーるTPC]
- 動的帯域幅選択（DBS）

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 AI RF プロファイルにアップグレードする基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 5 [Action] ドロップダウンリストから、[Upgrade to AI] を選択します。

ステップ 6 確認ウィンドウで [Yes] をクリックします。

ステップ 7 [Edit AI RF Profile] ウィンドウで、AI RF プロファイル設定を構成します。詳細については、AI 無線周波数プロファイルの作成 （53 ページ）を参照してください。

AP 承認リストの作成

許可された AP のリストをCisco DNA Centerで設定できます。Cisco DNA Centerは、次のタイプの AP 認証をサポートします。

- ローカル認証：ローカルデータベースに対する認証に、AP MAC アドレス、シリアル番号、またはその両方を使用します。
- AAA 認証：認証に AAA サーバーのリストを使用します。

シスコ ワイヤレス コントローラ をプロビジョニングするときに、AP 認証リストを選択できます。シスコ ワイヤレス コントローラ は、AP 認証リストに存在する AP からの認証要求のみにしか応答しません。

（注）
- AP 認証に MAC アドレスとシリアル番号の両方が必要な場合は、両方が AP 認証リストに追加されていることを確認してください。ワイヤレスコントローラにプロビジョニングされたAP 認証リストに認証に必要なエントリが揃っていない場合、その AP はネットワークに入れません。
- メッシュ AP（MAP）の場合、AP 認証用の MAC アドレスを追加する必要があります。
- Cisco AireOS ワイヤレスコントローラ の場合、Cisco DNA Center は MAC アドレスの AP しか認証しません。MAC アドレスとシリアル番号の両方を設定した場合、Cisco AireOS ワイヤレスコントローラはMAC アドレスのみを使用します。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、Cisco DNA Center は Cisco IOS 17.5 以降を搭載した ワイヤレスコントローラ の AP 認証リストしかサポートしません。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Authorization List] テーブルで [Add] をクリックします。

ステップ 5 [AP Authorization List] slide-in pane で、AP 承認リストの名前を入力します。

ステップ 6 ローカル認証を構成するには、次の手順を実行します。

a) [Local Auth] タブで、[Configure Local Authorization] チェックボックスをオンにします。

b) [Type] エリアで、認証タイプを選択します。

- AP MAC アドレスを設定するには、[Mac Address] をクリックします。
- AP シリアル番号を設定するには、[Serial Number] をクリックします。

c) AP の MAC アドレスまたはシリアル番号のデータを入力するには、次のいずれかを実行します。

- AP MAC アドレスまたはシリアル番号を個別に認証リストに追加するには、[Add] をクリックします。[AP Entry] フィールドにデータを入力します。
- データを含む CSV ファイルをアップロードするには、[Upload] をクリックします。ダイアログボックスで、次の操作を実行します。
  1. ドラッグアンドドロップエリアに CSV ファイルをドラッグアンドドロップします。または、[Choose a file] をクリックし、ローカルに保存されている CSV ファイルを参照して選択します。

     （注） CSV ファイルがない場合は、[Download] をクリックして、編集およびアップロードできる CSV ファイルをダウンロードします。

  2. [Save] をクリックします。

d) （任意） 認証に MAC アドレスとシリアル番号の両方を使用するには：
   1. [Mac Address] をクリックし、AP MAC アドレスデータ（6.c （69 ページ））を入力します。
   2. [Serial Number] をクリックし、AP シリアル番号データ（6.c （69 ページ））を入力します。

ステップ 7 AAA 認証を設定するには、次の手順を実行します。

a) [AAA Auth] タブで、[Configure AAA Authorization] チェックボックスをオンにします。
b) AAA サーバの AP 認証要件に基づいて、次のいずれかを実行します。
- AAA サーバが AP 認証に MAC アドレスのみを使用する場合は、[Authorize AP against MAC Address] チェックボックスをオンにします。
- AAA サーバーが AP 承認にシリアル番号のみを使用する場合は、[Authorize AP against Serial Number] チェックボックスをオンにします。
- AAA サーバーが AP 承認に MAC アドレスとシリアル番号の両方を使用する場合は、[Authorize AP against MAC Address] チェックボックスと [Authorize AP against Serial Number] チェックボックスの両方をオンにします。

c) AP エントリを AP 認証リストに追加するには、次のいずれかを実行します。
- 必要な AP エントリの横にあるプラス アイコン（＋）をクリックします。
- AP エントリをクリックし、[Add Selected] をクリックします。

  （注） 複数の AP エントリを選択するには、Shift キーを押しながら AP エントリをクリックし、[Add Selected] をクリックします。

- すべての AP エントリを AP 認証リストに追加するには、[Add All] をクリックします。[Search] フィールドを使用して、AP エントリをフィルタ処理できます。

ステップ 8 [Save] をクリックします。

AP 認証リストの編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Authorization List] テーブルで、編集または削除する認証リスト名の横にあるチェックボックスをオンにします。

- AP 認証リストを編集するには、[Edit] をクリックします。[AP Authorization List] slide-in paneで、必要に応じて設定を編集し、[Save] をクリックします。詳細については、AP 承認リストの作成 （69 ページ）を参照してください。
- AP 認証リストを削除するには、[Delete] をクリックしてから [Yes] をクリックします。

アンカーグループの作成

最大 3 つの シスコ ワイヤレス コントローラ でアンカーグループを作成し、アンカーの優先順位を設定できます。次のデバイスをアンカーとして追加できます。

- Cisco DNA Center によって管理されている シスコ ワイヤレス コントローラ。
- Cisco DNA Center（外部の ワイヤレスコントローラ）によって管理されていない シスコ ワイヤレス コントローラ

（注） アンカーグループには 1 つ以上のアンカーを追加する必要があります。

アンカーの優先順位によって、アンカー間のトラフィック共有が決まります。

- 均等共有：すべてのアンカーの優先順位が同じ場合（例：1、1、および 1）。
- 部分共有：複数のアンカーの優先順位が同じ場合（例：1、1、および 2）。
- 順次共有：アンカーの優先順位が順次である場合（例：1、2、および 3）。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Anchor Group] テーブルで、[Add] をクリックします。

ステップ 5 [Anchor Group] スライドインペインの [Anchor Group Name] フィールドに、アンカーグループ名を入力します。

ステップ 6 管理対象 ワイヤレスコントローラ をアンカーとして追加するには、[Add Managed WLC] をクリックし、[Add Managed WLC] ダイアログボックスで次の手順を実行します。

a) アンカーを追加するデバイス名の横にあるチェックボックスをオンにします。

デバイスを検索するには、[Search Table] の検索フィールドにデバイスの名前の一部または完全な名前を入力し、Enter キーを押します。

b) [Add] をクリックします。

ステップ 7 （任意） 外部の ワイヤレスコントローラ をアンカーとして追加するには、[Add External WLC] をクリックし、[Add External WLC] ダイアログボックスで次の手順を実行します。

a) [Device Name] フィールドに、デバイス名を入力します。
b) [Device Series] ドロップダウンリストからデバイスシリーズを選択します。
c) [Peer IP Address] フィールドに、ピアの IP アドレスを入力します。
d) （任意） [NAT IP Address] フィールドに、ネットワークアドレス変換（NAT）IP アドレスを入力します。
e) [MAC Address] フィールドに、デバイスの MAC アドレスを入力します。
f) [Mobility Group Name] フィールドに、モビリティグループ名を入力します。
g) （任意） [Hash] フィールドに、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のハッシュを入力します。

（注） このフィールドは、Cisco Catalyst 9800-CL ワイヤレスコントローラでのみ使用できます。

h) [Add] をクリックします。

ステップ 8 （任意） 既存の外部の ワイヤレスコントローラ をアンカーとして追加するには、[Add Existing External WLC] をクリックし、[Add Existing External WLC] ダイアログボックスで次の手順を実行します。

a) アンカーを追加するデバイス名の横にあるチェックボックスをオンにします。

デバイスを検索するには、[Search Table] の検索フィールドにデバイスの名前の一部または完全な名前を入力し、Enter キーを押します。

b) [Add] をクリックします。

ステップ 9 （任意） アンカーの優先順位を設定するには、[Priority Order] ドロップダウンリストからアンカー ワイヤレスコントローラ の優先順位を選択します。

ステップ 10 [Save] をクリックします。

アンカーグループを編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Anchor Group] テーブルで、編集または削除するアンカーグループの横にあるチェックボックスをオンにします。

- アンカーグループを編集するには、[Edit] をクリックします。[Anchor Group] スライドインペインで、アンカーを構成し、[Save] をクリックします。詳細については、アンカーグループの作成 （71 ページ）を参照してください。
- アンカーグループを削除するには、[Delete] をクリックし、[Yes] をクリックします。

AP プロファイル

AP プロファイルは、プラグアンドプレイ（PnP）、Cisco Advanced Wireless Intrusion Prevention System（aWIPS）、不正管理、およびメッシュネットワークの AP 認証設定を統合します。AP プロファイルを使い、AP の管理とプロビジョニングで行えます。Cisco DNA Centerでは、Cisco IOS XE デバイスと Cisco AireOS デバイスにデフォルトの AP プロファイルが設定されています。デフォルトの AP プロファイルは編集できますが、削除することはできません。Cisco IOS XE および Cisco AireOS デバイスのカスタム AP プロファイルを作成することもできます。AP プロファイルをサイトに割り当てるには、それをワイヤレス ネットワーク プロファイルに関連付けます。

Cisco IOS XE デバイスの AP プロファイルの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Profile] テーブルで、[Add] にカーソルを合わせて [AP Profile for IOS-XE] を選択します。

ステップ 5 [Create Access Point Profile] ウィンドウで、AP プロファイルの名前を入力します。

ステップ 6 （任意） AP プロファイルの説明を入力します。

ステップ 7 この AP プロファイルがリモートテレワーカー AP または Cisco OfficeExtend AP 用である場合は、[Remote Teleworker] チェックボックスをオンにします。

（注） リモートテレワーカー対応の AP プロファイルは、次の設定をサポートしていません。

- aWIPS アプリケーション
- 不正の検出
- メッシュ
- 電源

ステップ 8 次のタブで必要な設定を行います。

a) [Management]：詳細については、「Cisco IOS XE デバイスの AP プロファイルの管理設定を行う （74 ページ）」を参照してください。

b) [Security]：詳細については、「Cisco IOS XE デバイスの AP プロファイルのセキュリティ設定を行う （75 ページ）」を参照してください。

c) [Mesh]：詳細については、「Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う（76 ページ）」を参照してください。

d) [Power]：詳細については、「Cisco IOS XE デバイスの AP プロファイルの電力設定を行う（77 ページ）」を参照してください。

e) [Additional]：詳細については、「Cisco IOS XE デバイスの AP プロファイルの追加設定を行う（79 ページ）」を参照してください。

ステップ 9 [Save] をクリックします。

Cisco IOS XE デバイスの AP プロファイルの管理設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルに以下を設定します。

- PnP 要求プロセス中に AP を安全にオンボードするための認証設定。Cisco DNA Center のグローバルレベルまたはサイトレベルの階層で行われた認証設定に基づいて、AP を要求する際に PnP から 802.1x（Dot1x）サプリカントと証明書がプッシュされます。AP は、Cisco ISE での認証に 802.1x サプリカントを使用します。
- AP の n 日目の認証に関する認証設定。
- コンソールアクセス、SSH、および Telnet のログイン情報。
- Cisco Discovery Protocol（CDP）を有効にし、隣接デバイスから AP を検出できるようにする。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for IOS-X]**）で、[Management] タブをクリックします。

ステップ 2 [Access Points Authentication] エリアで、認証方式を選択します。

（注） Cisco DNA Center は、AP PnP 要求と n 日目の認証のときにこの認証方式を使用します。認証方式を変更すると、PnP 要求プロセスでオンボードされた AP のサービスに影響します。認証方式を変更する場合は、PnP 要求プロセスでオンボードされた AP の工場出荷時設定へのリセットを実行します。AP が別の Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）方式で参加する場合、EAP 方式は選択した認証方式によって変わります。

選択可能な認証方式は次のとおりです。

- [NO-AUTH]：デフォルトの認証方式。
- [EAP-TLS]：EAP-Transport Level Security（EAP-TLS）では、証明書ベースの認証を使用します。
- [EAP-PEAP]：EAP-Protected Extensible Authentication Protocol（EAP-PEAP）では、相互認証が提供され、脆弱なユーザーログイン情報の機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）およびアクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。EAP-PEAP は、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。

  [EAP-PEAP] を選択した場合は、ユーザー名とパスワードを入力します。Cisco DNA Center は証明書を生成し、PnP 要求プロセス中にその証明書を適用します。

- [EAP-FAST]：EAP-Flexible Authentication through Secure Tunneling（EAP-FAST）では、相互認証が提供され、共有秘密を使用してトンネルが確立されます。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。

  [EAP-FAST] を選択した場合は、ユーザー名とパスワードを入力します。Cisco DNA Center は証明書を生成し、PnP 要求プロセス中にその証明書を適用します。

ステップ 3 [SSH and Telnet] エリアで、次のように設定します。

a) （任意）[SSH] トグルボタンをクリックし、SSH のログイン情報を設定します。

b) （任意）[Telnet] トグルボタンをクリックし、Telnet のログイン情報を設定します。

c) [Username] フィールドに、デバイスの認証に使用する名前を入力します。

ユーザー名にスペースや山カッコ（<>）は使用できません。

（注） SSH と Telnet を無効にした場合、[Username] フィールドの指定は任意となります。

d) [Password] フィールドに、デバイスの認証に使用するパスワードを入力します。

（注） SSH と Telnet を無効にした場合、[Password] フィールドの指定は任意となります。

e) [Enable Password] フィールドにパスワードを入力し、CLI でより高い権限レベルを有効にします。

（注） SSH と Telnet を無効にした場合、[Enable Password] フィールドの指定は任意となります。

ステップ 4 [Cisco Discovery Protocol (CDP) State] エリアで [CDP State] トグルボタンをクリックし、CDP を有効または無効にします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （73 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルのセキュリティ設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルに以下を設定します。

- Cisco Advanced Wireless Intrusion Prevention System（aWIPS）とフォレンジックキャプチャにより、侵入の脅威を検出して軽減します。Cisco DNA Center は、Cisco IOS XE リリース 17.3.1 以降を実行しているデバイスの aWIPS をサポートします。
- 不正検出により、システム管理者からの明示的な許可を得ずにネットワークにインストールされている AP を検出できます。Cisco DNA Center は、Cisco IOS XE リリース 17.4 以降を実行しているデバイスの不正検出をサポートします。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for IOS-XE]**）で、[Security] タブをクリックします。

ステップ 2 [aWIPS and Forensic Capture Enablement] エリアで、次のように設定します。

a) [aWIPS] トグルボタンをクリックし、aWIPS を有効または無効にします。

b) [Forensic Capture Enablement] トグルボタンをクリックし、フォレンジックキャプチャを有効または無効にします。

（注） [Forensic Capture Enablement] トグルボタンを使用するには、[aWIPS] トグルボタンを有効にする必要があります。

ステップ 3 [Rogue Detection] エリアで、[Rogue Detection] トグルボタンをクリックして不正検出を有効または無効にします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （73 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行います。

始める前に

メッシュアクセスポイント（MAP）の MAC アドレスを AP 承認リストに追加してください。詳細については、AP 承認リストの作成 （69 ページ）を参照してください。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for IOS-XE]**）で、[Mesh] タブをクリックします。

ステップ 2 [Mesh] トグルボタンをクリックします。

（注） [Mesh] トグルボタンを無効にすると、既存のカスタムメッシュ設定が削除され、AP プロファイルがデバイスのデフォルトのメッシュプロファイルに関連付けられます。

ステップ 3 （任意） [Range - Root AP to Mesh AP (in feet)] フィールドに、ルートアクセスポイント（RAP）からネットワーク内の MAP までの最大範囲（フィート）を入力します。有効な範囲は 150 フィートから 132,000 フィートです。

ステップ 4 （任意） バックホール無線を介したワイヤレスクライアント関連付けを許可するには、[Backhaul Client Access] チェックボックスをオンにします。

バックホール無線には、大部分の MAP で 5 GHz 帯が使用されます。バックホール無線は、バックホールトラフィックとクライアントトラフィックの両方を伝送できます。

[Backhaul Client Access] チェックボックスがオフになっている場合、Cisco DNA Center はバックホール無線を介してバックホールトラフィックのみを送信し、クライアント関連付けは 2 次的な無線のみを介して送信されます。

ステップ 5 （任意） [RAP Downlink Backhaul] エリアで、必要なオプションを選択します。

お住まいの国で [5 GHz] の使用が禁止されている場合は、[2.4 GHz] を選択してください。お住まいの国で [5 GHz] の使用が許可されている場合でも、[2.4 GHz] の使用を検討してください。2.4 GHz 無線は、より長いメッシュまたはブリッジ距離をカバーできるためです。

（注） RAP 設定を [5 GHz] から [2.4 GHz] に変更すると、Cisco DNA Center は RAP からすべての MAP に更新を伝播します。この時点で、MAP は 5 GHz ネットワークから切断され、2.4 GHz ネットワークに接続します。

ステップ 6 （任意） [Backhaul Data Rates] エリアで、[5GHz Band Radio Type] および [2.4GHz Band Radio Type] ドロップダウンリストからインターフェイスレートを選択します。

有効なバックホールインターフェイス レートは、AP に応じて、[802.11abg]、[802.11n]、[802.11ac]（5GHz 帯域無線のみ）、[802.11ax]、および [Auto] となります。バックホールは、AP 間のワイヤレス接続を作成します。利用可能な RF スペクトラムを効果的に使用するにはレート選択が重要です。このレートは、クライアント デバイスのスループットにも影響を与える可能性があります

[Auto] データレートを使用すると、各リンクは、そのリンク品質に対して可能な限り最高のレートで到達できます。

メッシュバックホールのデータレートは [Auto] に設定することをお勧めします。

ステップ 7 （任意） [Bridge Group] エリアの [Bridge Group Name] フィールドに、ブリッジグループ名（最大 10 文字）を入力します。

ブリッジグループ名によって、MAP の関連付けが制御されます。無線をグループ化すると、同じチャネル上にあってもブリッジグループ名が異なる 2 つのネットワークは互いに通信できません。この設定はまた、同一セクター（エリア）のネットワーク内に複数の RAP がある場合にも便利です。

ブリッジグループ名を入力しない場合、Cisco DNA Center はメッシュプロファイルに**デフォルト**のブリッジグループ名を使用します。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （73 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルの電力設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルに以下を設定します。

- AP 電力プロファイル：AP が必要な電力を受け取っていない場合、AP は AP 電力プロファイルの設定に基づいて、ディレーティング状態で機能します。詳細については、AP 電力プロファイルの作成 （83 ページ）を参照してください。

（注） 電力設定は、Cisco IOS XE リリース 17.10.1 以降を実行しているシスコ ワイヤレス コントローラにのみ適用されます。

- カレンダー電力プロファイル：省電力モードの AP のカレンダー電力プロファイルを作成できます。必要に応じて、複数の AP 電力プロファイルを別のカレンダースケジュールにマッピングできます。Cisco DNA Center は、設定されたスケジュールに基づいて、AP 電力プロファイルで定義されたすべてのルールを同時に実行します。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for IOS-XE]**）で、[Power] タブをクリックします。

ステップ 2 [AP Power Profile] エリアで、[Select Value] ドロップダウンリストから電力プロファイルを選択します。

（電力プロファイルを作成するには、[Create New] をクリックしてパラメータを設定します。詳細については、「AP 電力プロファイルの作成 （83 ページ）」を参照してください。）

ステップ 3 [Calendar Power Profile] エリアで、次の手順を実行します。

a) カレンダー電力プロファイルを追加するには、[Add] をクリックします。[Add Calendar Power Profile] エリアで、次の手順を実行します。

1. [Select Power Profile] ドロップダウンリストから電力プロファイルを選択します。

   電力プロファイルを作成するには、[Create New] をクリックしてパラメータを設定します。詳細については、AP 電力プロファイルの作成 （83 ページ）を参照してください。

2. AP に電力プロファイルルールを適用するための繰り返し頻度を選択します。
   - [Daily]：AP に毎日電力プロファイルルールを適用します。
   - [Weekly]：毎週選択した曜日に AP に電力プロファイルルールを適用します。必要な曜日をクリックして選択します。
   - [Monthly]：毎月選択した日付に AP に電力プロファイルルールを適用します。必要な日付をクリックして選択します。
3. 電力プロファイルルールの開始時刻と終了時刻を指定します。
4. [Save] をクリックします。

b) （任意） 電力プロファイルルールを編集するには、対応する電力プロファイル名の横にあるチェックボックスをオンにし、[Edit] をクリックします。[Edit Power Profile] slide-in paneで、必要なパラメータを編集して [Save] をクリックします。

c) （任意） 電力プロファイルを削除するには、対応する電力プロファイル名の横にあるチェックボックスをオンにし、[Delete]、[Yes] の順にクリックします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （73 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルの追加設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルに以下を設定します。

- 国コード：国コードがまだ設定されていないその他の地域（ROW）ドメイン AP の国コードを設定します。

（注） 国コードの設定は、すでに国コードが設定されている AP には影響しません。

- タイムゾーン：AP のタイムゾーンを選択します。
- クライアント制限：許可されるクライアントの最大数を指定します。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for IOS-XE]**）で、[Additional] タブをクリックします。

ステップ 2 [Country Code] エリアで、[Select Value] ドロップダウンリストから国コードが設定されていない ROW AP の国を選択します。

ステップ 3 [Time Zone] エリアで、次のいずれかのオプションを選択します。

- [Not Configured]：AP は UTC のタイムゾーンで動作します。
- [Controller]：AP は シスコ ワイヤレス コントローラのタイムゾーンで動作します。
- [Delta from Controller]：AP はワイヤレスコントローラのタイムゾーンからのオフセットで動作します。次のオフセット値を設定します。
  - [HH]：時間の値を入力します。有効な範囲は 12 ～ 14 です。
  - [MM]：分の値を入力します。有効な範囲は 0 ～ 59 です。

ステップ 4 [Client Limit] エリアにクライアント数の上限値を入力します。有効な範囲は 0 ～ 1,200 です。

次のタスク

AP プロファイルに必要な設定をすべて指定したら、[Save] をクリックします。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （73 ページ）を参照してください。

Cisco AireOS デバイスの AP プロファイルの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Profile] テーブルで、[Add] にカーソルを合わせて [AP Profile for AireOS] を選択します。

ステップ 5 [Create Access Point Profile] ウィンドウで、AP プロファイルの名前を入力します。

ステップ 6 （任意） AP プロファイルの説明を入力します。

ステップ 7 この AP プロファイルがリモートテレワーカー AP または Cisco OfficeExtend AP 用である場合は、[Remote Teleworker] チェックボックスをオンにします。

（注） リモートテレワーカー対応の AP プロファイルは、次の設定をサポートしていません。

- aWIPS アプリケーション
- 不正の検出
- メッシュ
- 電源

ステップ 8 次のタブで必要な設定を行います。

a) [Management]：詳細については、「Cisco AireOS デバイスの AP プロファイルの管理設定を行う （80 ページ）」を参照してください。

b) [Security]：詳細については、「Cisco AireOS デバイスの AP プロファイルのセキュリティ設定を行う （81 ページ）」を参照してください。

c) [Mesh]：詳細については、「Cisco AireOS デバイスの AP プロファイルのメッシュ設定を行う （81 ページ）」を参照してください。

ステップ 9 [Save] をクリックします。

Cisco AireOS デバイスの AP プロファイルの管理設定を行う

この手順を使用して、Cisco AireOS デバイスの AP プロファイルに以下を設定します。

- コンソールアクセス、SSH、および Telnet のログイン情報。
- Cisco Discovery Protocol（CDP）を有効にし、隣接デバイスから AP を検出できるようにします。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for AireOS]**）で、[Management] タブをクリックします。

ステップ 2 [SSH and Telnet] エリアで、次のように設定します。

a) （任意） [SSH] トグルボタンをクリックし、SSH のログイン情報を設定します。

b) （任意） [Telnet] トグルボタンをクリックし、Telnet のログイン情報を設定します。

c) [Username] フィールドに、デバイスの認証に使用する名前を入力します。

ユーザー名にスペースや山カッコ（<>）は使用できません。

（注） SSH と Telnet を無効にした場合、[Username] フィールドの指定は任意となります。

d) [Password] フィールドに、デバイスの認証に使用するパスワードを入力します。

（注） SSH と Telnet を無効にした場合、[Password] フィールドの指定は任意となります。

e) [Enable Password] フィールドにパスワードを入力し、CLI でより高い権限レベルを有効にします。

（注） SSH と Telnet を無効にした場合、[Enable Password] フィールドの指定は任意となります。

ステップ 3 [Cisco Discovery Protocol (CDP) State] エリアで [CDP State] トグルボタンをクリックし、CDP を有効または無効にします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （79 ページ）を参照してください。

Cisco AireOS デバイスの AP プロファイルのセキュリティ設定を行う

この手順を使用して、Cisco AireOS デバイスの AP プロファイルの不正検出を設定します。不正検出により、システム管理者からの明示的な許可を得ずにネットワークにインストールされている AP を検出できます。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for AireOS]**）で、[Security] タブをクリックします。

ステップ 2 [Rogue Detection] エリアで、[Rogue Detection] トグルボタンをクリックして不正検出を有効または無効にします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （79 ページ）を参照してください。

Cisco AireOS デバイスの AP プロファイルのメッシュ設定を行う

この手順を使用して、Cisco AireOS デバイスの AP プロファイルのメッシュ設定を行います。

始める前に

MAP の MAC アドレスを AP 承認リストに追加してください。詳細については、AP 承認リストの作成 （69 ページ）を参照してください。

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profile]** テーブル > **[Add]** > **[AP Profile for AireOS]**）で、[Mesh] タブをクリックします。

ステップ 2 [Mesh] トグルボタンをクリックします。

ステップ 3 （任意）[RAP Downlink Backhaul] エリアで、必要なオプションの横にあるオプションボタンをクリックします。

お住まいの国で [5 GHz] の使用が禁止されている場合は、[2.4 GHz] を選択してください。お住まいの国で [5 GHz] の使用が許可されている場合でも、[2.4 GHz] の使用を検討してください。2.4 GHz 無線は、より長いメッシュまたはブリッジ距離をカバーできるためです。

（注） RAP 設定を [5 GHz] から [2.4 GHz] に変更すると、Cisco DNA Center は RAP からすべての MAP に更新を伝播します。この時点で、MAP は 5 GHz ネットワークから切断され、2.4 GHz ネットワークに接続します。

ステップ 4 （任意）[Bridge Group] エリアの [Bridge Group Name] フィールドに、ブリッジグループ名（最大 10 文字）を入力します。

ブリッジグループ名によって、MAP の関連付けが制御されます。無線をグループ化すると、同じチャネル上にあってもブリッジグループ名が異なる 2 つのネットワークは互いに通信できません。この設定はまた、同一セクター（エリア）のネットワーク内に複数の RAP がある場合にも便利です。

ブリッジグループ名を入力しない場合、Cisco DNA Center はメッシュプロファイルに**デフォルト**のブリッジグループ名を使用します。

次のタスク

AP プロファイルに必要な設定をすべて指定したら、[Save] をクリックします。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （79 ページ）を参照してください。

AP プロファイルの編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Profile] テーブルで、編集または削除する AP プロファイル名の横にあるチェックボックスをオンにします。

- AP プロファイルを編集するには、[Edit] をクリックします。[Edit Access Point Profile] slide-in paneで、必要に応じて設定を編集し、[Save] をクリックします。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （79 ページ）およびCisco IOS XE デバイスの AP プロファイルの作成 （73 ページ）を参照してください。
- AP プロファイルを削除するには、[Delete] をクリックしてから [Yes] をクリックします。

AP 電力プロファイルの作成

Cisco IOS XE リリース 17.10.1 以降を実行している シスコ ワイヤレス コントローラの AP 電力プロファイルを作成できます。APプロファイルに関連付けることにより、AP電力プロファイルを AP に割り当てます。AP 電力プロファイルの複数のルールを定義し、ルールの順序を指定できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Power Profile] テーブルで、[Add] をクリックします。

ステップ 5 [Create Power Profile] slide-in paneで、AP 電力プロファイルの名前を入力します。

ステップ 6 （任意） AP 電力プロファイルの説明を入力します。

ステップ 7 AP 電力プロファイルのルールを作成するには、[Add] をクリックします。

ステップ 8 [Add Rule] ダイアログボックスで、次の手順実行します。

a) [Interface] ドロップダウンリストからインターフェイスのタイプを選択します。

b) [Interface ID] ドロップダウンリストからインターフェイス ID を選択します。

（注） 使用可能なインターフェイス ID が 1 つだけの場合、Cisco DNA Center で使用可能なインターフェイス ID が自動的に選択されます。

c) [Parameter] ドロップダウンリストからパラメータを選択します。

（注） 使用可能なパラメータが 1 つだけの場合、Cisco DNA Center で使用可能なパラメータが自動的に選択されます。

d) [Parameter Value] ドロップダウンリストからパラメータ値を選択します。

（注） 使用可能なパラメータ値が 1 つだけの場合、Cisco DNA Center で使用可能なパラメータ値が自動的に選択されます。

e) [Add] をクリックします。

ステップ 9 （任意） AP 電力プロファイルの別のルールを作成するには、「ステップ 7 （83 ページ）」と「ステップ 8 （83 ページ）」を繰り返します。

ステップ 10 （任意） [Rules] テーブルのルールの順序を更新するには、対応する アイコンをクリックし、ルールを必要な位置にドラッグアンドドロップします。

ステップ 11 [Save] をクリックします。

次のタスク

AP 電力プロファイルと AP プロファイルを関連付けます。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （73 ページ）を参照してください。

AP 電力プロファイルの編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Power Profile] テーブルで、編集または削除する AP 電力プロファイル名の横にあるチェックボックスをオンにします。

- AP 電力プロファイルを編集するには、[Edit] をクリックします。[Edit Power Profile] slide-in paneで、必要に応じて説明、ルール、順序を編集し、[Save] をクリックします。詳細については、AP 電力プロファイルの作成 （83 ページ）を参照してください。
- AP 電力プロファイルを削除するには、[Delete] をクリックしてから [Yes] をクリックします。

非ファブリック展開用の Cisco センサー SSID のプロビジョニング

- Cisco DNA Center センサーは、Cisco センサー プロビジョニング サービス セット識別子（SSID）を使用して、プラグアンドプレイ（PnP）サーバーと通信し、テストを実行するための Day-0 設定を取得します。

（注） Cisco センサープロビジョニング SSID は、センサーとして動作する AP には適用されません。

- ファブリック展開の場合、Cisco センサープロビジョニング SSID は、Cisco DNA Center と通信するためにインフラストラクチャ仮想ネットワーク アクセスポイント（INFRA VN-AP）プールにマッピングされます。
- 次のプラットフォームは Cisco センサープロビジョニング SSID をサポートしています。
  - Cisco AireOS コントローラ
  - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ファブリック展開と非ファブリック展開の両方）
- Cisco センサープロビジョニング SSID は次のネットワークコントローラをサポートしています。
  - クラウド向け Cisco Catalyst 9800 ワイヤレスコントローラ

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- Cisco AireOS コントローラ

次の手順で、非ファブリック展開の Cisco センサープロビジョニング SSID を設定できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 [SSID] テーブルから、Add にカーソルを合わせて、[Enterprise] を選択します。

ワイヤレス SSID ワークフローが表示されます。

ステップ 4 [Sensor] フィールドを切り替えて、[Next] をクリックします。

（注） SSID のパラメータは自動的に入力され、編集できません。

ステップ 5 [Next] をクリックします。

ステップ 6 [Wireless Profiles] 画面で、[Profiles] のプロファイルを確認します。

[Edit Wireless Profile] ダイアログボックスが表示されます。

ステップ 7 [Fabric] で [Yes] を選択し、[Save] をクリックします。

「Success Profile sensorProfile selected」というメッセージが表示されます。

ステップ 8 [Finish] をクリックします。

ステップ 9 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 10 デバイスを確認し、[Actions] ドロップダウンメニューから **[Provision]** > **[Provision Device]** の順に選択します。

ステップ 11 [Assign Site]、[Configuration]、[Model Configuration]、[Advanced Configuration]、および [Summary] で詳細を確認します。各画面で [Next] をクリックしてください。

ステップ 12 [Deploy] をクリックします。

[Provision Device] ダイアログボックスが表示されます。

ステップ 13 [Now] を選択し、[Apply] をクリックします。

結果：「Task Scheduled view status in Tasks」というメッセージが右下隅に表示されます。

バックホールの設定の管理

ワイヤレスセンサのバックホール設定を表示、作成、管理するには、次の手順を実行します。ワイヤレスセンサーには、Cisco DNA Center と通信するためのバックホール SSID が必要です。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Manage]** > **[Sensors]** の順に選択します。

[Sensor List] ウィンドウが表示されます。

ステップ 2 [Settings] タブにカーソルを合わせ、[Backhaul Settings] を選択します。

ステップ 3 バックホール SSID を追加および管理するには、次の手順を実行します。

a) [Add Backhaul] をクリックします。

[Create Sensor Backhaul SSID Assignment] ウィンドウが表示され、[Wired Backhaul] と [Wireless Backhaul] の 2 つの領域が表示されます。

b) [Settings name] フィールドでバックホール SSID の名前を入力します。

c) [Wired Backhaul] 領域で、次を設定します。

- [Level of Security]：選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
  - [802.1x EAP]：Extensible Authentication Protocol（EAP）を有線 LAN で渡すために使用される規格。
  - [Open]：セキュリティまたは認証は使用されません。
- [EAP Method]：[802.1x EAP] を選択した場合は、ドロップダウンリストからユーザ認証に次のいずれかの EAP 方式を選択する必要があります。
  - [EAP-FAST]：指定されたフィールドにユーザ名とパスワードを入力します。
  - [PEAP-MSCHAPv2]：指定されたフィールドにユーザ名とパスワードを入力します。
  - [EAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。

    [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。
  - [PEAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll using SCEP] を選択します。

    [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。

d) [Wireless Network Name（SSID）] 領域で、ワイヤレスネットワーク（SSID）を選択し、次を設定します。

- [Level of Security]：選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
  - [WPA2 Enterprise]：拡張可能認証プロトコル（EAP）（802.1x）を使用してより高レベルのセキュリティを実現し、リモート RADIUS サーバでネットワークユーザを認証および承認します。

- [WPA2-Personal]：パスフレーズまたは事前共有キー（PSK）を使用して、良好なセキュリティを実現します。ワイヤレスネットワークにアクセスするパスキーがあれば誰でも使用できます。

  [WPA2 Personal] を選択した場合は、[Passphrase] テキストボックスにパスフレーズを入力します。

- [PSK Format]：使用可能な事前共有キーの形式は次のとおりです。
  - [ASCII]：ASCII PSK パスフレーズをサポートします。
  - [HEX]：64 文字の HEX キー PSK パスワードをサポートします。
- [Open]：セキュリティまたは認証は使用されません。

e) [Save] をクリックします。

ステップ 4 既存のバックホール設定を編集するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit] を選択します。

ステップ 5 バックホール設定を削除するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Delete] を選択します。

Cisco Connected Mobile Experiences の統合について

Cisco DNA Centerは、ワイヤレスマップのためのCisco Connected Mobile Experiences（CMX）の統合をサポートしています。CMX を統合すると、Cisco DNA Center ユーザーインターフェイス内で、フロアマップ上でのワイヤレスクライアント、不正アクセスポイントおよび干渉源の正確な場所を把握できます。

CMX の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル（親ノード）で CMX を割り当てることができます。すべての子ノードが親ノードから設定を継承します。中企業の場合はビルディング レベルで CMX を割り当てることができ、小企業の場合はフロアレベルで CMX を割り当てることができます。

（注） セキュリティ上の理由から、CMX は匿名にする必要があります。

Cisco CMX 設定の作成

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] セクションで、[CMX Servers/Cisco DNA Spaces] をクリックします。

[CMX Servers/Cisco DNA Spaces] ウィンドウが開きます。

ステップ 3 [CMX Servers] テーブルから、[Add] をクリックします。

ステップ 4 [Add CMX Server] スライドインペインで、次のフィールドに入力します。

- [IP Address]：CMX Web GUI の有効な IP アドレスを入力します。
- [User Name]：CMX Web GUI のユーザー名を入力します。
- [Password]：パスワードログイン情報を入力します。
- [SSH User Name]：CMX 管理者のユーザー名を入力します。
- [SSH Password]：CMX 管理者のパスワードログイン情報を入力します。

（注） CMX が到達可能であることを確認してください。

ステップ 5 [Add]をクリックします。

CMX サーバーが正常に追加されました。

ステップ 6 CMX サーバーをサイト、建物、またはフロアに割り当てるには、メニューアイコンをクリックし、**[Design]** > **[Network Settings]**の順に選択します。

ステップ 7 [Wireless] タブをクリックします。

ステップ 8 [Global] または必要なエリア、建物、フロアを左側の階層ツリーから、。

ステップ 9 [CMX Servers/Cisco DNA Spaces] セクションで、ドロップダウンリストを使用して、CMX サーバーを選択します。

ステップ 10 **[Save]** をクリックします。

[Create CMX Settings] ウィンドウが開きます。

CMX の追加後に [Network Hierarchy] ページのフロアに変更を加えた場合、その変更は自動的に CMX と同期されます。

CMX が同期されると、Cisco DNA Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。

ステップ 11 フロアマップでは、次のことを実行できます。

- クライアントの場所を表示します。これは青色のドットとして表示されます。
- AP 上にカーソルを移動します。ダイアログボックスは、[Info]、[Rx Neighbor]、[Clients] タブで表示されます。詳細については、各タブをクリックしてください。[Device 360] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアント デバイスの場所を表示します。
- AP をクリックして、AP に関する詳細を含むサイド バーを開きます。
- Intelligent Capture と CMX を統合するときにリアルタイムでクライアント トラッキングを実行します。

ステップ 12 変更を加えたときにCMXがダウンした場合は、手動で同期する必要があります。同期するには、[Network Hierarchy] ページで、左側の階層ツリーで変更を加えた建物やフロアの隣にある省略記号•••の上にカーソルを置き、[Sync：CMX Server/Cisco DNA Spaces] を選択して、変更を手動でプッシュします。

ステップ 13 CMX サーバーの詳細を編集する場合や CMX サーバーを削除する場合は、次の手順を実行します。

a) メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。
b) [External Services] セクションで、[CMX Servers/Cisco DNA Spaces] をクリックします。
c) 編集する CMX サーバーを選択して変更を加え、[Update] をクリックします。
d) 削除する CMX サーバーを選択し、[Delete] をクリックします。
e) [OK] をクリックして削除を実行します。

CMX 認証に失敗した場合

- Cisco DNA Center で CMX 設定の作成時に指定したログイン情報で、CMX Web GUI にログインできるか確認します。
- SSH を使用して CMX コンソールにログインできるかどうかを確認します。
- CMX GUI の API ドキュメンテーションリンクを使用して CMX REST API を使用できるかどうかを確認します。

クライアントが Cisco DNA Center フロアマップに表示されない場合

- 特定のフロアのシスコ ワイヤレス コントローラが CMX で設定されており、アクティブになっているか確認します。
- CMX GUI でフロアマップにクライアントが表示されるか確認します。
- Cisco DNA Center マップ API を使用して、フロアにクライアントをリスト表示します。

```
curl -k -u <user>:<password> -X GET
/api/v1/dna-maps-service/domains/<floor group
id>/clients?associated=true
```

Cisco Spaces の統合について

現実の世界で事業を行っている企業は、これまで、建物内の人々や接続されたアセットの動きを可視化できませんでした。Cisco Spaces は、基盤となるすべてのシスコ ワイヤレス ネットワークによって提供されるロケーション感知インテリジェンスを使用し、データをビジネス対応の洞察に変換することで、この物理的な死角の問題を解決します。

Cisco DNA Center は、Cisco Spaces の統合をサポートします。Cisco Spaces を統合すると、Cisco DNA Center の GUI 内で、フロアマップ上でのワイヤレスクライアント、不正 AP、および干渉源の正確な場所を把握できます。Cisco Spaces の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。

（注） 現在、Cisco DNA Center と Cisco Spaces の統合は、自動マップエクスポートとロケーション階層の同期のみに制限されています。この統合では、キャプティブポータルベースの認証機能はサポートされません。

Cisco Spaces と Cisco DNA Center の統合

Cisco Spaces と Cisco DNA Center を統合するには、次の手順を使用します。

ステップ 1 Cisco Spaces クライアントをオンボードします。

a) 電子メール ID を使用して Cisco Spaces にログインし、[Continue] をクリックします。

b) [Select Customer] ドロップダウンリストから、Cisco DNA Center インスタンスの Spaces テナント（たとえば、dna-center-dev-US）を選択し、[Proceed] をクリックします。

c) Cisco Spaces GUI でメニューアイコンをクリックして、**[Setup]** > **[Wireless Networks]**の順に選択します。

d) [Connect your wireless network] ウィンドウで、『*Cisco Spaces Configuration Guide*』に記載されている手順 1 ー 3 を実行して、Cisco Spaces クライアントをオンボードします。

『*Cisco Spaces Configuration Guide*』には、**[Need Help?]** > **[View Configuration Steps]**の下にある右側のペインからアクセスできます。

ステップ 2 Cisco DNA Center を Cisco Spaces に登録します。

a) 電子メール ID を使用して Cisco Spaces にログインし、[Continue] をクリックします。

b) [Select Customer] ドロップダウンリストから、Cisco DNA Center インスタンスの Spaces テナント（たとえば、dna-center-dev-US）を選択し、[Proceed] をクリックします。

c) Cisco Spaces GUI でメニューアイコンをクリックし、**[Integrations]** > **[Cisco DNA Center]**の順に選択します。

d) [DNAC Integration] ウィンドウで、[Create Token] をクリックします。

[Create new token] ダイアログボックスが開きます。

e) [Instance Name] フィールドに、インスタンスの一意の名前を入力し、[Create Token] をクリックします。

インスタンスの新しいトークンが開きます。

f) トークンの右側までスクロールし、[Copy Token] を選択します。

g) トークンを Cisco DNA Center GUI に貼り付けるには、Cisco DNA Center にログインします。

h) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

i) 左側のナビゲーションウィンドウで、下にスクロールして [CMX Servers/Cisco DNA Spaces] を選択します。

[CMX Servers/Cisco DNA Spaces] ウィンドウが開きます。

j) [Cisco DNA Spaces] エリアで、[Activate] を選択します。

[Integrate Cisco DNA Spaces] ダイアログボックスが開きます。

k) [Tenant Token] テキストボックスで、Ctrl+V キーを押して Cisco Spaces からコピーしたトークンを貼り付け、[Connect] をクリックします。

[Success] ダイアログボックスに次の情報が表示されます。

```
This cluster is integrated with Cisco Spaces successfully.
```

[CMX Servers/Cisco DNA Spaces] ウィンドウに緑色の ✓ [Activated] ステータスが表示され、Cisco Spaces で選択した（dna-center-dev-US などの）テナントが [Tenant] フィールドに表示されます。

ステップ 3 Cisco Spaces を Cisco DNA Center のサイトに割り当てます。

a) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。
b) [Wireless] タブをクリックします。
c) 左側の階層ツリーから、**[Global]** か、Cisco Spaces に割り当てるエリア、ビルディング、またはフロアを選択します。
d) [CMX Servers/Cisco DNA Spaces] セクションのドロップダウンリストを使用して（DNA Spaces - dna-center-dev-US などの）サイトを選択します。
e) [**保存**（**Save**）] をクリックします。

ステップ 4 Cisco Spaces を使用して Cisco DNA Center のサイトをモニターします。

a) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
b) 左側の階層ツリーから、**[Global]** か、Cisco Spaces にモニターさせるエリア、ビルディング、またはフロアを選択します。

Cisco DNA Center により、サイト情報が Cisco Spaces に自動的に展開されます。

c) Cisco Spaces が動作していることを確認するには、次の図に示すように、Cisco Spaces/CMX ステータスアイコンがモニターするフロアに表示されていることを確認します。

図 *1 : Cisco Spaces* ステータスアイコン

FlexConnect VLAN の設定

次の FlexConnect VLAN 設定を指定することができます。

- [Native VLAN]：FlexConnect グループが AP と シスコ ワイヤレス コントローラ の間で管理トラフィックを伝送できるようにします。
- [AAA Override VLAN]：ローカルでスイッチングされるクライアントの動的 VLAN 割り当てを提供します。

これらの設定をグローバルレベルで適用して、サイト、ビルディング、またはフロアレベルの設定をオーバーライドすることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、必要なサイトを選択します。

- [Global]：すべてのサイトに対してグローバルレベルで VLAN を設定します。
- エリア、ビルディング、またはフロア：選択したレベルでのみ VLAN を設定します。

ステップ 4 [Native VLAN ID] フィールドに、VLAN ID の値を入力します。有効な範囲は 1 ～ 4094 です。

ステップ 5 [AAA Override VLAN] 設定の場合は、VLAN ID と VLAN 名のマッピングを、対応する [VLAN ID] フィールドと [VLAN Name] フィールドに入力します。さらにマッピングを追加するには、[Add] アイコンをクリックします。

（注） FlexConnect 展開に対して定義できる VLAN マッピングの最大数は 16 です。ただし、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、この数には、デフォルトの WLAN VLAN と、AAA によってプッシュされた VLAN が含まれます。

ステップ 6 [保存（**Save**）] をクリックします。

次のタスク

ワイヤレス ネットワーク プロファイルを作成するか、SSID を設定します。

- **ワイヤレス ネットワーク プロファイル**：ワイヤレス ネットワーク プロファイルを作成する場合は、[FlexConnect Local Switching] チェックボックスがオンになっていることを確認します。詳細については、ワイヤレス用のネットワークプロファイルの作成を参照してください。
- [SSID]：SSID を設定する場合は、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （20 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （30 ページ）を参照してください。

保存済みの FlexConnect VLAN 設定をワイヤレスコントローラで設定するには、ワイヤレスコントローラをプロビジョニングする必要があります。詳細については、Cisco AireOS コントローラのプロビジョニングまたはCisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニングを参照してください。

ワイヤレスコントローラ のプロビジョニング後に、コントローラに関連付けられている AP をプロビジョニングする必要があります。

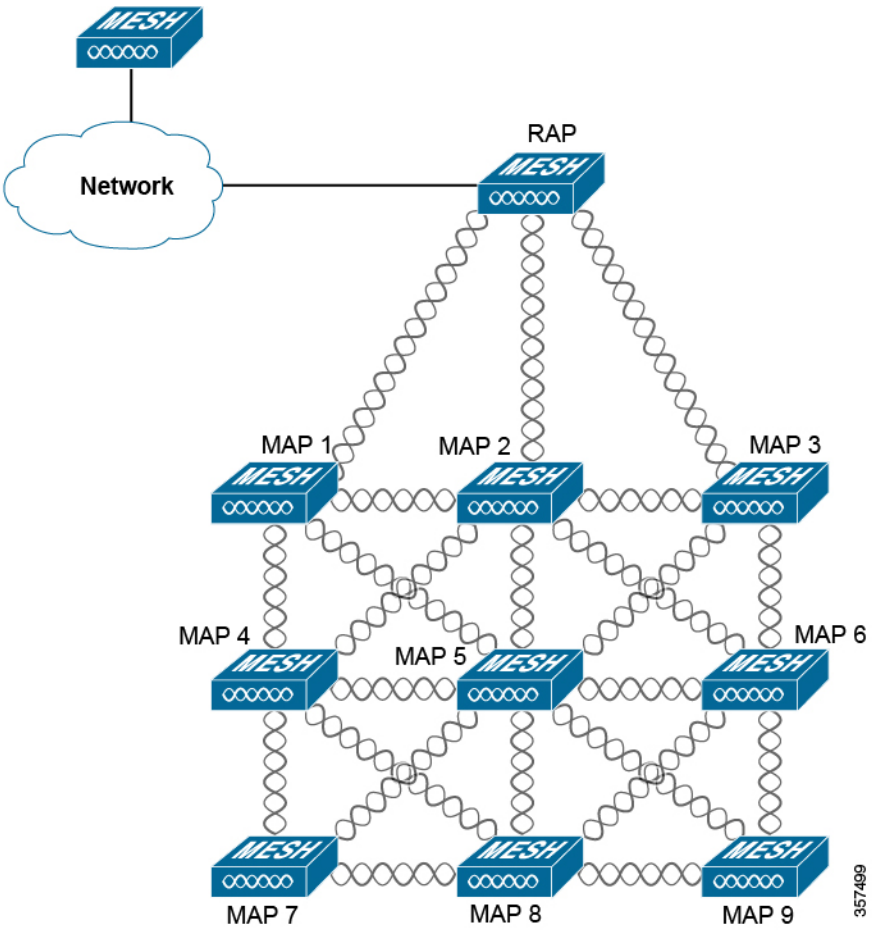
ワイヤレス メッシュ ネットワークについて

シスコ ワイヤレス メッシュ ネットワーク内のアクセスポイント（AP）は、次の 2 つの方法のいずれかで動作します。

- ルートアクセスポイント（RAP）：それぞれの場所で有線ネットワークに接続します。
- メッシュアクセスポイント（MAP）：ワイヤレスで通信し、安全でスケーラブルなワイヤレス LAN を提供します。

（注） すべての AP は MAP として設定され、出荷されています。AP を RAP として使用するには、RAP として再設定する必要があります。すべてのメッシュネットワークで、少なくとも 1 つの RAP があることを確認します。

RAP は、それぞれの場所で有線ネットワークに接続します。すべてのダウンストリーム AP は、MAP として動作し、ワイヤレスリンクを使用して通信します。



MAP と RAP はいずれも WLAN クライアントアクセスを提供します。ただし、一般に、RAP の場所は高い確率でクライアントアクセスの提供に向いていません。

MAP から CAPWAP セッションを終端させるオンサイトコントローラがある建物もありますが、CAPWAP セッションはワイドエリアネットワーク（WAN）を介してコントローラにバックホールできるため、それは必須要件ではありません。

Cisco ワイヤレス バックホール ネットワークでは、トラフィックを MAP と RAP の間でブリッジできます。このトラフィックは、ワイヤレスメッシュによってブリッジされている有線デバイスからのトラフィックか、MAP からの CAPWAP トラフィックになります。このトラフィックは、ワイヤレス バックホールなどのワイヤレス メッシュ リンクを通過する際に必ず AES 暗号化されます。

メッシュネットワークの詳細については、最新の『Cisco Wireless Mesh Access Points, Design and Deployment Guide』を参照してください。

AP Configuration

メッシュネットワークモードで使用する既存の AP がある場合は、最初に [Configure Access Point] ワークフローを使用して AP モードを [Bridge] または [Flex+Bridge] に変更する必要があります。詳細については、AP ワークフローの設定を参照してください。

APを[Bridge]モードまたは[Flex+Bridge]モードに設定すると、[AP 360]ウィンドウにメッシュ設定が表示されます。この時点で、APを新しい設定でプロビジョニングする必要があります。シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング。

シスコ ワイヤレス コントローラ の設定

メッシュネットワークの場合は、コントローラで許可 AP のリストを設定する必要があります。コントローラは、許可リストに含まれている MAP からの要求にのみ応答します。

（注） Cisco DNA Center は、Cisco IOS リリース 17.5 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ での承認リストの設定をサポートしています。

Cisco AireOS ワイヤレスコントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの両方で、Cisco DNA Center を使用してブリッジグループ名（BGN）と RAP ダウンリンク バックホール メッシュの設定を指定することができます。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、MAP の最大範囲、バックホール クライアント アクセス、およびバックホールデータレートを設定することもできます。

これらの設定は、[Create AP Profile]ウィンドウでグローバルサイトに対して指定されます。詳細については、Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う （76 ページ）およびCisco AireOS デバイスの AP プロファイルのメッシュ設定を行う （81 ページ）を参照してください。

証明書失効確認の設定

次の手順を使用して、証明書失効確認を設定します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Security and Trust]** の順に選択します。

ステップ 2 左側の階層ツリーから、サイト、ビルディング、またはフロアを選択します。

ステップ 3 [Revocation Check] ドロップダウンリストでは、[Revocation - Check: CRL None] がデフォルトで選択されています。

ステップ 4 失効確認をスキップするには、[Revocation - Check: None] を選択し、[Save] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。