ネットワーク階層と設定を設計

新しいネットワーク インフラストラクチャの設計

[設計（Design）]領域では、ネットワーク全体のデバイスに適用可能な物理トポロジ、ネットワーク設定、デバイスのタイプやプロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。既

存のインフラストラクチャがある場合は、**ディスカバリ**機能を使用します。詳細については、「ディスカバリについて」を参照してください。

これらのタスクは、[設計（Design）] 領域で実行します。

ステップ 1 ネットワーク階層を作成します。詳細については、ネットワーク階層のサイトの作成 （3 ページ）を参照してください。

ステップ 2 グローバル ネットワーク設定を定義します。詳細については、グローバル ネットワーク設定について （50 ページ）を参照してください。

ステップ 3 ネットワーク プロファイルを定義します。

ネットワーク階層について

ネットワークの地理的な場所を表すネットワーク階層を作成できます。ネットワーク階層には、ビルディングやエリアを含むサイトを含めることができます。サイト ID とビルディング ID を作成すると、後で、設計の設定や構成を適用する場所を簡単に特定できます。デフォルトでは、**グローバル**と呼ばれる 1 つのサイトがあります。

ネットワーク階層は、次の事前設定された階層をもちます。

- [エリア（Areas）] や [サイト（Sites）] には、物理的なアドレス（例、米国）はありません。エリアは最大の要素だと考えることができます。エリアにはビルディングとサブエリアを含めることができます。たとえば、米国というエリアには、カリフォルニアというサブエリアが含まれ、カリフォルニアというサブエリアにはサンノゼというサブエリアが含まれることができます。
- [ビルディング（Buildings）]には物理アドレスがあり、フロアとフロア プランが含まれています。ビルディングを作成する場合、物理アドレスおよび緯度と経度の座標を指定する必要があります。ビルディングにエリアを含めることはできません。ビルディングを作成することで、特定のエリアに設定を適用できます。
- [フロア（Floors）] は建物内にあり、キュービクル、壁に囲まれたオフィス、配線クローゼットなどで構成されています。フロアはビルディングにのみ追加できます。

実行できるタスクのリストを以下に示します。

- 新しいネットワーク階層を作成する。詳細については、「ネットワーク階層のサイトの作成 （3 ページ）」を参照してください。
- Cisco Prime Infrastructure から既存のネットワーク階層をアップロードする。詳細については、「既存のサイト階層をアップロード （5 ページ）」を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

- マップのイメージファイルを .jpg、.gif、.png、.dxf、.dwg などの形式で保存できるグラフィカル アプリケーションを使用します。
- イメージ画像の寸法が、キャンパスマップに追加する予定のすべてのビルディングと屋外領域の合計寸法よりも大きいことを確認します。
- マップのイメージファイルのサイズはさまざまです。Cisco DNA Center は元のイメージを完全な定義でデータベースにインポートしますが、表示中は、ワークスペースに合わせてサイズが自動的に変更されます。
- インポートする前に、サイトの縦と横の寸法をフィートまたはメートル単位で取得してください。これにより、マップ インポート時にこれらの寸法を指定できます。

ネットワーク階層のサイトの作成

Cisco DNA Center では、物理サイトを簡単に定義し、それらのサイトの共有リソースを特定することができます。**[設計（Design）]** アプリケーションは、直観的な操作のために階層型の形式を使用し、デバイスをプロビジョニングするときに同じリソースを複数の場所で再定義する必要性を排除しています。デフォルトでは、**グローバル**と呼ばれる 1 つのサイトがあります。ネットワーク階層には、複数のサイト、ビルディング、およびエリアを追加できます。プロビジョニング機能を使用する前に、少なくとも 1 つのサイトを作成する必要があります。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

世界のマップが表示されます。

ステップ 2 **[ネットワーク階層（Network Hierarchy）]** ウィンドウで、**[+ サイトの追加（+ Add Site）]** をクリックするか、または左側のペインにある親サイトの隣にある歯車アイコン をクリックして、適切なオプションを選択します。

ステップ 3 既存の階層をアップロードすることもできます。詳細については、既存のサイト階層をアップロード （5 ページ）を参照してください。

ステップ 4 サイトの名前を入力し、親ノードを選択します。デフォルトでは、**[グローバル（Global）]** が親ノードです。

ステップ 5 [Add]をクリックします。

左側のメニューの親ノードの下にサイトが作成されます。

Cisco Prime Infrastructure からサイト階層をエクスポートして Cisco DNA Center にインポートする

ネットワーク階層はネットワークの地理的な場所を表します。サイト ID とビルディング ID を作成すると、後で、設計の設定や構成を適用する場所を簡単に特定できます。Cisco Prime

Infrastructure に既存のネットワーク階層がある場合は、Cisco DNA Center にインポートして、新しいネットワーク階層の作成に費やす時間と労力を節減できます。

これは、ロケーショングループまたはサイト情報を含む CSV ファイルと、ネットワーク階層内のさまざまなフロアマップを含むマップアーカイブファイルとして、Cisco Prime Infrastructure から 2 つのファイルをエクスポートするために必要な単純なプロセスです。

この手順では、Cisco Prime Infrastructure から Cisco DNA Center に既存のサイト階層をエクスポートする方法について説明します。Cisco Prime Infrastructure リリース 3.2 以降のバージョンからサイト階層をエクスポートできます。

始める前に

- シスコ ワイヤレス コントローラとアクセスポイントを検出し、Cisco DNA Center の [Inventory] ページに一覧表示されます。
- フロアマップ上に AP を追加して配置します。
- Cisco Prime Infrastructure にあるサイトを Cisco DNA Center で手動作成した場合は、Cisco DNA Center にインポートする前にそれらのサイトを手動で削除する必要があります。

ステップ 1 最初のステップとして、Cisco Prime Infrastructure からワークステーションに CSV ファイルとしてロケーショングループをエクスポートする必要があります。

ステップ 2 ロケーショングループをエクスポートするには、Cisco Prime Infrastructure で、 [Inventory] > [Group Management] > [Network Device Groups] を選択します。 > >

ステップ 3 [Device Groups] ウィンドウで、[Export Groups] をクリックします。

ステップ 4 [Export Groups] ダイアログボックスで、[APIC-EM] オプションボタンをクリックして CSV ファイルをダウンロードし、[OK] をクリックします。

CSV ファイルがワークステーションにダウンロードされるまで待ちます。CSV ファイルには、さまざまなサイト、ビルディング、およびフロアの地理的場所と、ネットワーク内の階層に関する情報が含まれています。

ステップ 5 次に、Cisco Prime Infrastructure からマップをエクスポートします。これにより、Cisco Prime Infrastructure の各フロアに適用されている RF 減衰モデルなどのフロア寸法やキャリブレーション情報などのマップ情報がダウンロードされます。

ステップ 6 マップをエクスポートするには、**[Maps]** > **[Wireless Maps]** > **[Site Maps (New)]** を選択します。

ステップ 7 **[Export]** ドロップダウンリストから **[Map Archive]** を選択します。

[Export Map Archive] ウィンドウが表示され、デフォルトで [Select Sites] ウィンドウが表示されます。

ステップ 8 特定のサイト、キャンパス、ビルディング、またはフロアのチェックボックスをオンにするか、 [Select All] チェックボックスをオンにしてすべてのマップをエクスポートします。

ステップ 9 [Map Information] と [Calibration Information] が選択されているかどうかを確認します。必ずオプション 1 つを選択する必要があります。選択されていない場合は、[Map Information] および [Calibration Information] に対して [On] ボタンをクリックします。

ステップ 10 [Map Information] を選択すると、長さ、幅、高さなどのフロアの寸法がエクスポートされます。また、フロアマップ上に配置された AP に関する詳細、および Cisco Prime Infrastructure 内のフロアマップ上にオーバーレイされた障害物とエリアもエクスポートされます。

ステップ 11 [Calibration Information] を選択すると、Cisco Prime Infrastructure の各フロアに適用されている無線周波数減衰モデルがエクスポートされます。既存のキャリブレーションデータを Cisco Prime Infrastructure からエクスポートすることをお勧めします。それ以外の場合は、Cisco DNA Center でキャリブレーションの詳細を手動で入力する必要があります。

ステップ 12 [Generate Map Archive] をクリックして、マップアーカイブを生成します。

ネットワーク階層内のさまざまなフロアマップを含む tar ファイルが作成され、お使いのワークステーションに保存されます。

ステップ 13 サイト階層を Cisco DNA Center にインポートするには、Cisco DNA Center のホームページから [Design] > [Network hierarchy] > の順に選択し、[Import] > [Import Sites] > をクリックします。

ステップ 14 [Import Sites] ウィンドウで、Prime Infrastructure のロケーショングループの CSV ファイルをドラッグアンドドロップするか、[Select a file from your computer] をクリックしてファイルがある場所に移動し、[Import] をクリックして、Prime Infrastructure のロケーショングループの CSV ファイルをインポートします。

ステップ 15 次に、フロアマップと関連するマップ情報を含むマップアーカイブファイルをインポートします。

ステップ 16 マップアーカイブファイルをインポートするには、**[Design]** > **[Network Hierarchy]** の順に選択し、**[Import]** > **[Import Maps]** をクリックします。

ステップ 17 [Import Maps Archive] ウィンドウで、マップアーカイブファイルをドラッグアンドドロップするか、お使いのワークステーションからファイルを選択します。

ステップ 18 **[保存（Save）]** をクリックします。

既存のサイト階層をアップロード

既存のネットワーク階層を含んでいる CSV ファイルまたはマップ アーカイブ ファイルをアップロードすることができます。たとえば、Cisco Prime Infrastructure からエクスポートしたロケーション情報を含む CSV ファイルをアップロードできます。詳細については、Prime Infrastructure からマップをエクスポートする方法に関する マップ アーカイブのエクスポート（6 ページ）を参照してください。

（注） マップ アーカイブ ファイルを Cisco DNA Center にインポートする前に、Cisco ワイヤレス コントローラや関連付けられている AP などのデバイスが検出され、Cisco DNA Center インベントリ ページに一覧になっていることを確認してください。

ステップ 1 Cisco DNA Center のホームページから、**[設計（Design）] > [ネットワーク階層（Network Hierrarchy）]** をクリックし、**[インポート（Import）] >[サイトのインポート（Import Site）]** を選択します。

ステップ 2 CSV ファイルをドラッグしてドロップするか、または、CSV ファイルがある場所に移動し、**[インポート（Import）]** をクリックして、Cisco Prime Infrastructure グループ CSV ファイルをインポートします。

既存の CSV ファイルがない場合は、**[テンプレートをダウンロード（Download Template）]** をクリックして、編集可能な CSV ファイルをダウンロードして、その後、アップロードすることができます。

ステップ 3 Cisco Prime Infrastructure マップ tar.gz アーカイブ ファイルをインポートするには、**[インポート（Import）] > [マップのインポート（Map Import）]** をクリックします。

ステップ 4 **[サイト階層アーカイブのインポート（Import Site Hierarchy Archive）]** ダイアログボックスのボックス エリアにマップ アーカイブ ファイルをドラッグしてドロップするか、または、**[クリックして選択（click to select）]** リンクをクリックして、アーカイブ ファイルを参照します。

ステップ 5 **[保存]** を選択してファイルをアップロードします。

[インポート プレビュー（Import Preview）]ウィンドウが表示され、インポートされたファイルが示されます。

マップ アーカイブのエクスポート

Cisco Prime Infrastructure からマップ アーカイブ ファイルをエクスポートし、それらを Cisco DNA Center にインポートできます。

ステップ 1 Cisco Prime Infrastructure のユーザー インターフェイスから、**[マップ（Map）] > [ワイヤレス マップ（Wireless Maps）] > [サイト マップ（新規）（Site Maps (New)）]** を選択します。

ステップ 2 **[エクスポート（Export）]** ドロップダウン リストから **[マップ アーカイブ（Map Archive）]** を選択します。

ステップ 3 [サイトの選択（Select Sites）] ウィンドウで、次のように設定します。マップ アーカイブに含めるマップ情報またはキャリブレーション情報を選択できます。

- マップ情報（Map Information）：アーカイブにマップ情報を含めるには、**オンまたはオフ** ボタンをクリックします。
- キャリブレーション情報（Calibration Information）：キャリブレーション情報をエクスポートするには、**オンまたはオフ** ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] オプション ボタンか、または [すべてのキャリブレーション情報（All Calibration Information）] オプション ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] を選択すると、選択したサイト マップのキャリブレーション情報がエクスポートされます。[すべてのキャリブレーション情報（All Calibration Information）] を選択すると、選択したマップとともに、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。
- 左側のペインの [サイト（Sites）] で、エクスポートするサイト、キャンパス、ビルディング フロア、または屋外領域の 1 つ以上のチェックボックスをオンにします。すべてのマップをエクスポートするには、[Select All] チェックボックスをオンにします。

ステップ 4 **[** マップアーカイブを生成（Generate Map Archive） **]** をクリックします。「データをエクスポートしています（`Exporting data is in progress`）」というメッセージが表示されます。
tar ファイルが作成され、ローカル マシンに保存されます。

ステップ 5 [Done] をクリックします。

ネットワーク階層の検索

ネットワーク階層を検索し、サイト、ビルディング、またはエリアをすばやく見つけることができます。これは、多くのサイトやエリア、ビルディングを追加した後に特に役立ちます。

ツリー階層を検索するには、左ペインの **[階層の検索（Find Hierarchy）]** で、検索するサイト、ビルディング、フロア名の名称の一部または正式名称をのどちらかを入力します。ツリー階層は、検索フィールドに入力したテキストに基づきフィルタリングされます。

サイトの編集

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。
ステップ 2 左側のツリー ペインで、編集するサイトに移動します。
ステップ 3 サイトの横にある歯車アイコン をクリックし、[サイトの編集（Edit Site）] を選択します。
ステップ 4 必要な変更を行って、[更新（Update）] をクリックします。

サイトの削除

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。
ステップ 2 左側のペインで、削除するサイトに移動します。
ステップ 3 対応するサイトの隣にある歯車アイコン をクリックし、[サイトの削除（Delete Site）] を選択します。
ステップ 4 削除を確認します。

ビルディングの追加

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

世界のマップが表示されます。

ステップ 2 [ネットワーク階層（Network Hierarchy）] ウィンドウで、[+サイトの追加（Add Site）] をクリックするか、または左側のツリー ペインの親サイトの隣にある歯車アイコン をクリックして、[ビルディングの追加（Add Building）] を選択します。

ステップ 3 既存の階層をアップロードすることもできます。既存のサイト階層をアップロード （5 ページ）を参照してください。

ステップ 4 ビルディングの名前を入力します。

ステップ 5 [アドレス（Address）]テキストフィールドに、アドレスを入力します。インターネットに接続している場合、アドレスを入力すると同時に、設計アプリケーションが、入力されたアドレスを既知のアドレスを絞り込みます。適切なアドレスがウィンドウに表示されたことを確認したら、それを選択します。既知の所在地を選択すると、[経度（Longitude）]および[緯度（Latitude）]の座標フィールドが自動的に設定されます。

ステップ 6 [Add]をクリックします。

左側のメニューの親サイトの下に、作成したビルディングが追加されます。

ステップ 7 別のエリアまたはビルディングを追加するには、階層フレームで、既存のエリアまたは親ノードにしたいビルディングの隣にある歯車アイコン をクリックします。

ビルディングの編集

ステップ 1 **[設計（Design）] > [ネットワーク階層（Network Hierarchy）]** を選択します。

ステップ 2 左側のツリー ペインで、編集するビルディングに移動します。

ステップ 3 ビルディングの横にある歯車アイコン をクリックし、[ビルディングの編集（Edit Building）] を選択します。

ステップ 4 [ビルディングの編集（Edit Building）] ウィンドウで必要な変更を加え、[更新（Update）] をクリックします。

ビルディングの削除

ステップ 1 Cisco DNA Center のホームページで、**[Design] > [Network Hierarchy]** の順に選択します。

ステップ 2 左側のペインで、削除するビルディングに移動します。

ステップ 3 ビルディングの隣にある歯車アイコン をクリックし、[ビルディングの削除（Delete Building）]を選択します。

ステップ 4 削除を確認します。

（注） ビルディングを削除すると、そのコンテナマップもすべて削除されます。APは、削除されたマップから未割り当ての状態に移動します。

ビルディングへのフロアの追加

ビルディングを追加したら、フロアを作成し、フロア マップをアップロードします。

ステップ 1 Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] を選択します。

ステップ 2 [グローバル（Global）]サイトと以前に作成した領域を展開し、以前に作成したすべてのビルディングを確認します。

ステップ 3 フロアを追加するビルディングの横にある歯車アイコンをクリックし、次に[フロアを追加（Add Floor）]をクリックします。

ステップ 4 フロアの名前を入力します。フロア名には21文字の制限があります。フロア名は文字またはハイフン（-）で始める必要があり、最初の文字に続く文字列は、次の 1 つ以上を含めることができます。

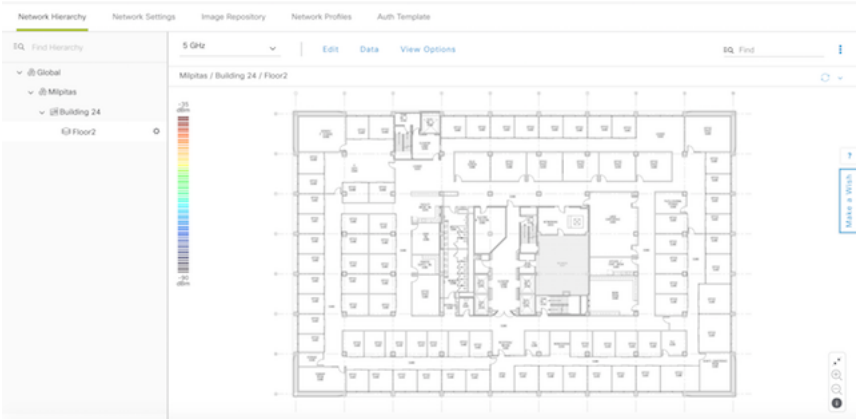
- 大文字または小文字、またはその両方
- 数字
- アンダースコア（_）
- ハイフン（-）
- ピリオド(.)
- スペース ( )

ステップ 5 [タイプ（RFモデル）（Type（RF Model））] ドロップダウン リストから無線周波数（RF）モデルを選択して、フロアのタイプを定義します（[屋内天井高（Indoor High Ceiling）]、[屋外オープンスペース（Outdoor Open Space）]、[乾式壁オフィスのみ（Drywall Office Only）]、および [キューブと壁で囲まれたオフィス（Cubes And Walled Offices）]）。これにより、フロアがオープンスペースであるか、乾式壁のオフィスであるかなどを定義します。選択した RF モデルに基づいて、ワイヤレス信号強度、ヒートマップの分布が計算されます。

ステップ 6 フロア プランをマップにドラッグしたり、ファイルをアップロードしたりできます。Cisco DNA Center は、.jpg、.gif、.png、dxf、および .dwg の各ファイル タイプをサポートしています。

マップをインポートした後は、必ず [オーバーレイの可視性（Overlay Visibility）] を [ON] にしてください（[フロア（Floor）]>[表示オプション（View Option）]>[オーバーレイ（Overlays）]）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

図 *1:* フロア プランの例



ステップ 7 [追加（Add）] をクリックします。

フロアの編集

フロアを追加したら、フロア上にある障害物、エリア、および AP が含まれるようにフロア マップを編集できます。

ステップ 1 Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] を選択します。

ステップ 2 ネットワーク階層を展開して編集するフロアを見つけるか、または左側のペインで [階層の検索（Search Hierarchy）] テキスト フィールドにフロア名を入力します。

ステップ 3 [フロアの編集（Edit Floor）] ダイアログ ウィンドウで必要な変更を加え、[更新（Update）] をクリックします。

フロア マップのモニタリング

[Floor View] ナビゲーションウィンドウでは、次のような複数のマップ機能にアクセスできます。

- フロア マップ ウィンドウの右上隅にある [検索（Find）] 機能を使用して、AP、センサー、クライアントなど特定のフロア要素を検索します。検索基準に一致する要素は、右側のペインでテーブルとともにフロア マップに表示されます。マウスをテーブルの上に置くと、フロア マップ上の検索要素が接続線で示されます。

- フロア マップ ウィンドウの右上隅にある アイコンをクリックして、次の作業を行います。
  - フロア プランを PDF としてエクスポートします。

- フロア マップで距離を測定します。
- スケールを設定してフロア面積を変更します。

- フロア マップ ウィンドウの右下隅にある アイコンをクリックして、場所をズームインします。ズームレベルは画像の解像度によって異なります。高解像度画像では、より高いズーム レベルを使用できます。各ズーム レベルはさまざまなスケールで表示される各種スタイル マップで構成されていて、対応する詳細が表示されます。マップの中にはスケールを小さくしても大きくしても同じ状態のマップもあります。
- アイコンをクリックすると、広範囲のマップが表示されます。
- アイコンをクリックすると、マップ アイコンの凡例が表示されます。

表 *1:* マップ アイコン

フロアマップアイコン	説明
AP Mode	
L	[ローカル（Local）]
F	FlexConnect
B	Bridge
ヘルススコア	
	良好
	普通
	不良
AP Status	
	センサーのカバー外
	センサーのカバー内
無線帯域またはモード	
5	802.11 a/n/ac（5GHZ）
2.4	802.11 b/g/n（2.4 GHZ）

フロアマップアイコン	説明
n	802.11 a/b/g/n（2.4GHZ）
Se	センサー
M	5 GHzをモニタ
m	2.4 GHzをモニタ
Mx	XOR モードをモニタ
R	不正検出
...	Other
無線ステータス	
5	Ok
5	マイナーな障害
5	Down
--	管理者無効
アイコン	
	アクセス ポイント（Access Points）
	センサー
	マーカー
Rx ネイバー回線	
	2.4 GHz
	5 GHz

フロア要素とオーバーレイの編集

フロア領域で使用できる **[編集（Edit）]** オプションにより、次の操作を実行できます。

- 次のフロア要素を追加、配置、および削除します。
  - アクセス ポイント（Access Points）
  - Sensor
- 次のオーバーレイ オブジェクトを追加、編集、および削除します。
  - カバレッジ エリア
  - 障害物
  - ロケーション リージョン
  - Rails
  - マーカー

アクセス ポイントの配置に関するガイドライン

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿ってアクセスポイントを設置します。このようなカバレッジ領域の中心に設置されたアクセスポイントからは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関しても有益なデータが得られます。
- AP 全体の密度を高め、AP をカバレッジ エリアの周辺部に近づけることにより、位置精度を向上させることができます。
- 細長いカバレッジ領域では、直線的に AP を配置しないようにします。各 AP でデバイス ロケーションのスナップショットが他と異なるように、それらを交互にずらします。
- 設計では高帯域幅アプリケーションにも十分に対応できる AP 密度が提供されますが、位置に関しては、単一デバイスの各 AP ビューが似ているという弱点があります。そのことが位置の判別を困難にしています。AP をカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。

AP の追加、配置、および削除

Cisco DNA Center によって、カバレッジエリアの 無線周波数（RF）信号の相対強度を表示する全体マップのヒートマップが計算されます。このヒートマップは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値に過ぎません。

インベントリにシスコの AP があることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して AP を検出します。「ディスカバリについて」を参照してください。

Cisco DNA Center のリリース 1.3 では、以下の 802.11ax AP が新しくサポートされます。

- Cisco Catalyst 9100 アクセスポイント
- Cisco Catalyst 9115 アクセス ポイント
- Cisco Catalyst 9117 アクセス ポイント
- Cisco Catalyst 9120 アクセス ポイント

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある **[編集（Edit）]** をクリックします。

ステップ 4 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

フロアに割り当てられていないアクセス ポイントが一覧に表示されます。

ステップ 5 [APの追加（Add Aps）] ウィンドウで、アクセス ポイントのチェック ボックスをオンにして AP を一括で選択し、[選択項目の追加（Add Selected）] をクリックします。または、アクセス ポイントに隣接する [追加（Add）] をクリックします。

（注） 使用可能な検索オプションを使用して、アクセスポイントを検索できます。[フィルタ（Filter）] フィールドを使用し、AP 名、MAC アドレス、モデル、シスコ ワイヤレス コントローラのいずれかを使ってアクセス ポイントを検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[追加（Add）] をクリックして、フロア領域に 1 つ以上の AP を追加します。

ステップ 6 フロア領域に AP を割り当てたら、[APの追加（Add APs）] ウィンドウを閉じます。

ステップ 7 新しく追加した AP はフロア マップの右上隅に表示されます。

ステップ 8 [アクセスポイント（Access Points）] の横にある[フロア要素（Floor Elements）] ペインで、 [位置（Position）] をクリックして AP をマップに正しく配置します。

- AP を配置するには、AP をクリックして、フロア マップ上の適切な場所にドラッグアンドドロップします。または、[選択したAPの詳細（Selected AP Details）] ウィンドウで x 座標と y 座標および AP の高さを更新することもできます。マップ上のアクセス ポイントをドラッグすると、その水平（x）と垂直（y）の位置が、テキストフィールドに表示されます。選択すると、右ペインにアクセス ポイントの詳細が表示されます。[選択したAPの詳細（Selected AP Details）] ウィンドウには、次の情報が表示されます。
  - [3点による位置決め（Position by 3 points）] : フロア マップに 3 つの点を記入し、その点を使用して AP の位置決めができます。手順は次のとおりです。
    1. [3ポイントによる位置付け（Position by 3 points）] をクリックします。
    2. ポイントを定義するには、フロア マップの任意の場所をクリックして最初のポイントの描画を開始します。ポイントの描画を終了するには、再度をクリックします。最初の点までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[距離の設定（Set Distance）] をクリックします。

3. 2 番目と 3 番目の点を同様の方法で定義し、[保存（Save）] をクリックします。

- [2つの壁による位置決め（Position by 2 Walls）]：フロア マップに 2 つの壁を定義し、定義した壁の間に AP の位置決めができます。これによって、2 つの壁の間の AP の位置を把握できるようになります。これは、壁の間の AP の位置を把握するのに役立ちます。

  1. [2つの壁による位置付け（Position by 2 Walls）] をクリックします。
  2. 最初の壁を定義するには、フロア マップの任意の場所をクリックして線の描画を開始します。線の描画を終了するには、再度をクリックします。最初の壁までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[Set Distance] をクリックします。
  3. 2 番目の壁を同様の方法で定義し、[保存（Save）] をクリックします。

     AP が、壁の間の定義された距離に従って自動的に配置されます。

- [AP名（AP Name）]：AP 名を表示します。
- [APモデル（AP Model）]：選択したアクセス ポイントの AP モデルを示します。
- [MAC Address]：MAC アドレスが表示されます。
- [X]：マップの水平の距離をフィートで入力します。
- [Y]：マップの垂直の距離をフィートで入力します。
- [AP高さ（AP Height）]：アクセス ポイントの高さを入力します。
- [プロトコル（Protocol）]：このアクセス ポイントのプロトコル：[802.11a/n/ac]、[802.11b/g/n]（ハイパー ロケーション AP の場合）、または [802.11a/b/g/n]。
- [アンテナ（Antenna）]：このアクセス ポイントのアンテナ タイプ。

  （注） 外部の AP の場合は、アンテナを選択する必要があります。選択しなければ、AP はマップに存在しません。

- [Antenna Image]：AP イメージが表示されます。
- [アンテナの方向（Antenna Orientation）]：[方位角（Azimuth）] と [仰角（Elevation）] の方向を度数で入力します。
- [Azimuth]：全方向アンテナのパターンでは方位角が存在しなくなるため、このオプションは表示されません。

ステップ 9 アクセス ポイントの設定と調整が完了したら、[保存（Save）] をクリックします。

ヒートマップは、AP の新しい位置に基づいて生成されます。

Cisco Connected Mobile experience (CMX) が Cisco DNA Center と同期されている場合は、ヒートマップ上のクライアントの場所を表示できます。「Cisco CMX 設定の作成 （43 ページ）」 を参照してください。

ステップ 10 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[削除（Delete）] をクリックします。
[APの削除（Delete APs）] ウィンドウには、割り当てられて、配置されたアクセス ポイントすべてを一覧表示します。

ステップ 11 削除するアクセス ポイントの横にあるチェック ボックスをオンにし、[選択済みの削除（Delete Selected）] をクリックします。

- すべてのアクセス ポイントを削除するには、[すべて選択（Select All）] をクリックし、[選択済みの削除（Delete Selected）] をクリックします。
- フロアからアクセス ポイントを削除するには、[削除（Delete）] アイコンをクリックします。
- **クイック フィルタ** を使用して、AP 名、MAC アドレス、モデル、またはコントローラにより検索します。検索では大文字と小文字は区別されません。検索結果が表に表示されます。[削除（Delete）] アイコンをクリックしてフロア領域から AP を削除します。

AP のクイック ビュー

フロアマップ上の AP アイコンにカーソルを合わせると、AP の詳細、Rx ネイバーの情報、クライアントの情報、およびデバイス 360 の情報が表示されます。

- [Info] をクリックすると、次の AP の詳細が表示されます。
  - [Associated]：AP が関連付けられているかどうかを示します。
  - [Name]：AP 名。
  - [MAC Address]：AP の MAC アドレス。
  - [Model]：AP モデル番号。
  - [Admin/Mode]：AP モードの管理ステータス。
  - [Type]：無線タイプ。
  - [OP/Admin]：動作ステータスおよび AP モード。
  - [Channel]：AP のチャネル番号。
  - [Antenna]：アンテナ名。
  - [Azimuth]：アンテナの方向。
- [Rxネイバー（Rx Neighbors）] ラジオ ボタンをオンにすると、マップ上に選択した AP に隣接する Rx ネイバーが接続回線とともに表示されます。また、フロア マップには AP が関連付けられているかどうかも AP 名とともに表示されます。
- [Device 360] をクリックすると、特定のネットワーク要素（ルータ、スイッチ、AP、またはシスコ ワイヤレス コントローラ）の 360 度ビューが表示されます。Cisco DNA Assurance

ユーザガイドの「デバイスの健全性のモニタとトラブルシューティング」トピックを参照してください。

（注） デバイス 360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。

センサーの追加、配置、および削除

（注） インベントリに Cisco AP 1800S センサーがあることを確認します。Cisco AP 1800S センサーをインベントリで表示するには、プラグアンドプレイを使用してプロビジョニングする必要があります。Cisco DNA Assurance ユーザガイド のトピック「*Provision the Wireless Cisco Aironet 1800s Active Sensor*」を参照してください。

センサー デバイスは AP 1800S センサー専用です。AP 1800S センサーは、PnP を使用してブートストラップされます。アシュアランス サーバに到達可能かどうかの詳細情報を取得してからアシュアランス サーバと直接通信します。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 フロア プランの上にある [編集（Edit）] をクリックします。

ステップ 4 [センサー（Sensors）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

ステップ 5 [Add Sensors] ウィンドウで、追加するセンサーのチェックボックスをオンにするか、またはセンサー行の横にある [Add] をクリックしてセンサーを追加します。

（注） 検索オプションを使用して、特定のセンサーを検索できます。[Filter] フィールドを使用し、センサーの名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[追加（Add）]をクリックして、フロア領域に 1 つ以上のセンサーを追加します。

ステップ 6 フロア マップへセンサーを割り当てたら、[センサーの追加（Add Sensors）] ウィンドウを閉じます。新しく追加したセンサーはフロア マップの右上隅に表示されます。

ステップ 7 センサーを正しく設定するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[位置（Position）] をクリックして、マップに正しくセットします。

ステップ 8 センサーの設定と調整が完了したら、[保存（Save）] をクリックします。

ステップ 9 センサーを削除するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[削除（Delete）] をクリックします。
[Delete Sensors] ウィンドウには、割り当てられて設定されたすべてのセンサーが一覧表示されます。

ステップ 10 削除するセンサーのチェックボックスをオンにし、[Delete Selected] をクリックします。

- すべてのセンサーを削除するには、[すべて選択（Select All）] をクリックし、[選択済みの削除（Delete Selected）] をクリックします。
- フロアからセンサーを削除するには、そのセンサーの横にある [削除（Delete）] アイコンをクリックします。
- [Quick Filter] を使用して、名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[削除（Delete）] アイコンをクリックして、フロア領域から 1 つ以上のセンサーを削除します。

カバレッジ エリアの追加

既定では、フロア領域やビルディング マップの一部として定義されている外部エリアが無線カバレッジ エリアと見なされます。

長方形以外のビルディングがある場合、またはフロア内に長方形以外の領域をマークする場合には、マップ エディタを使用してカバレッジ領域または多角形の領域を描画できます。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある **[編集（Edit）]** をクリックします。

ステップ 4 [オーバーレイ（Overlays）] パネルで、[カバレッジエリア（Coverage Areas）] の横にある [追加（Add）] をクリックします。
[カバレッジの作成（Coverage creation）] ダイアログボックスが表示されます。

ステップ 5 カバレッジ領域を描画するには、[Type] ドロップダウンリストから、[Coverage Area] を選択します。

1. 定義するエリアの名前を入力し、[カバレッジを追加（Add Coverage）] をクリックします。カバレッジエリアは、頂点が3つ以上の多角形でなければなりません。
2. 輪郭を描く領域に描画ツールを移動します。
3. このツールをクリックして、描線を開始および停止します。
4. エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。

（注） マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。

ステップ 6 多角形領域を描画するには、[タイプ（Type）] ドロップダウンリストから、[周辺（Perimeter）] を選択します。

1. 定義する領域の名前を入力し、[Ok] をクリックします。
2. 輪郭を描く領域に描画ツールを移動します。

- このツールをクリックして、描線を開始および停止します。
- エリアの輪郭を描いてからダブルクリックすると、そのエリアがページ上で強調表示されます。

ステップ 7 カバレッジ領域を編集するのには、[オーバーレイ（Overlays）]パネルで、[カバレッジエリア（Coverage Areas）] の横にある [編集（Edit）]をクリックします。

使用可能なカバレッジ領域がマップ上で強調表示されます。

ステップ 8 変更を加え、変更後に [保存（Save）] をクリックします。

ステップ 9 カバレッジ領域を削除するのには、[オーバーレイ（Overlays）]パネルで、[カバレッジエリア（Coverage Areas）] の横にある [削除（Delete）] をクリックします。

使用可能なカバレッジ領域がマップ上で強調表示されます。

ステップ 10 カバレッジ エリアにマウス カーソルを合わせ、クリックして削除します。

ステップ 11 削除後に [保存（Save）] をクリックします。

障害物の作成

アクセス ポイントの RF 予測ヒートマップを計算する際に考慮するための障害を作成することができます。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある **[編集（Edit）]** をクリックします。

ステップ 4 [障害（Obstacles）]の横にある [オーバーレイ（Overlays）]パネルで、[追加（Add）]をクリックします。

ステップ 5 [障害を作成（Obstacle Creation）] ダイアログ ボックスで、[障害のタイプ（Obstacle Type）] ドロップダウン リストから障害のタイプを選択します。作成可能な障害のタイプは、[厚い壁（Thick Wall）]、[薄い壁（Light Wall）]、[重い扉（Heavy Door）]、[軽い扉（Light Door）]、[キュービクル（Cubicle）]、および [ガラス（Glass）] です。
選択した障害のタイプの予測信号損失が自動的に取り込まれます。信号損失は、これらのオブジェクトの周辺の RF 信号強度を計算するために使用されます。

ステップ 6 [障害物の追加（Add Obstacle）] をクリックします。

ステップ 7 障害物を作成する領域に描画ツールを移動します。

ステップ 8 描画ツールをクリックして、描線を開始および停止します。

ステップ 9 エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。

ステップ 10 表示される [障害の作成（Obstacle Creation）] ウィンドウで [完了（Done）] をクリックします。

ステップ 11 [保存（Save）] をクリックして、障害をフロア マップに保存します。

ステップ 12 障害を編集するには、[障害（Obstacles）]の隣にある [オーバーレイ（Overlays）]パネルで、[編集（Edit）] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 13 変更が完了したら、[保存（Save）] をクリックします。

ステップ 14 障害を削除するには、[障害（Obstacles）] の隣にある [オーバーレイ（Overlays）] パネルで、[削除（Delete）] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 15 障害にマウス カーソルを合わせ、クリックして削除します。

ステップ 16 **[保存（Save）]** をクリックします。

ロケーション リージョンの作成

包含領域および除外領域を作成して、フロア上のロケーション計算の精度をさらに高めることができます。計算に含める領域（包含領域）と計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外して、作業領域（小個室、研究室、製造現場など）を含めることができます。

フロア マップ上に包含領域と除外領域を配置するためのガイドライン

- 包含領域と除外領域は多角形領域で表され、最低 3 点で構成される必要があります。
- フロア上の包含リージョンを 1 つだけ定義できます。デフォルトでは、各フロア領域が作成されるときに、各フロア領域に対して包含領域が定義されます。包含領域は、水色の実線で示され、通常はフロア領域全体の輪郭を描きます。
- フロア領域に複数の除外領域を定義することができます。

フロア上の包含リージョンの定義

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[追加（Add）]** をクリックします。

ステップ 4 **[ロケーション リージョンの作成（Location Region Creation）]** ダイアログ ウィンドウで、**[包含タイプ（Inclusion Type）]** ドロップダウン リストからオプションを選択します。

ステップ 5 **[位置領域の追加（Add Location Region）]** をクリックします。

包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 6 包含領域の定義を開始するには、描画ツールをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 7 含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。

再びクリックすると、次の境界線を定義できます。

ステップ 8 領域の輪郭が描画されるまでステップ 7 を繰り返したら、描画アイコンをダブルクリックします。

水色の実線によって包含領域が定義されます。

ステップ 9 **[保存（Save）]** をクリックします。

フロア上の除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外できます。原則として、除外領域は包含領域の境界内に定義されます。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある **[編集（Edit）]** をクリックします。

ステップ 4 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[追加（Add）]** をクリックします。

ステップ 5 **[ロケーション リージョンの作成（Location Region Creation）]** ウィンドウで、**[除外タイプ（Exclusion Type）]** ドロップダウン リストから値を選択します。

ステップ 6 [ロケーションリージョン（Location Region）] をクリックします。

除外領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7 除外領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1回クリックします。

ステップ 8 除外するエリアの境界に沿って描画アイコンを移動させます。

1 回クリックして境界線を開始し、再びクリックして境界線を終了します。

ステップ 9 エリアの輪郭が描画されるまで前の手順を繰り返したら、描画アイコンをダブルクリックします。定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。

ステップ 10 さらに除外領域を定義するには、手順 5 から手順 9 を繰り返します。

ステップ 11 すべての除外領域が定義されている場合は、**[保存（Save）]** をクリックします。

ロケーション リージョンの編集

ステップ 1 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[編集（Edit）]** をクリックします。
使用可能なロケーション リージョンがマップ上で強調表示されます。

ステップ 2 必要な変更を行って、**[保存（Save）]** をクリックします。

ロケーション リージョンの削除

ステップ 1 **[オーバーレイ（Overlays）]**パネルで、**[ロケーション リージョン（Location Regions）]** の横にある **[削除（Delete）]** をクリックします。
使用可能なロケーション リージョンがマップ上で強調表示されます。

ステップ 2 削除する領域の上にマウスのカーソルを合わせ、**[削除（Delete）]** をクリックします。

ステップ 3 **[保存（Save）]** をクリックします。

レールの作成

フロア上にコンベヤベルトを表すレールラインを定義できます。また、レール領域の周囲にスナップ幅とも呼ばれる、ロケーション計算をさらにサポートする領域を定義できます。この領域は、クライアントが表示されると予測される領域を表します。スナップ幅の領域内に配置されたクライアントは、レール ライン上に表示されるか（多数）、スナップ幅領域の外側に表示されます（少数）。

スナップ幅領域は、フィートまたはメートル（ユーザ定義）単位で定義され、レールの片側（東および西、または北および南）からモニタされる距離を表します。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある **[編集（Edit）]** をクリックします。

ステップ 4 **[レール（Rails）]** の横にある **[オーバーレイ（Overlays）]** パネルで、**[追加（Add）]** をクリックします。

ステップ 5 レールのスナップ幅（フィートまたはメートル）を入力して [レールの追加（Add Rail）] をクリックします。

描画アイコンが表示されます。

ステップ 6 レール ラインの開始ポイントで描画アイコンをクリックします。ラインの描画を停止するときやラインの方向を変える際は、再びクリックします。

ステップ 7 フロア マップ上にレール ラインを描画したら、描画アイコンを 2 回クリックします。レールラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。

ステップ 8 [Save] をクリックします。

ステップ 9 **[オーバーレイ（Overlays）]** パネルで、**[レール（Rails）]** の横にある **[編集（Edit）]** をクリックします。

使用可能なレールがマップ上で強調表示されます。

ステップ 10 変更を加えて、[保存（Save）] をクリックします。

ステップ 11 **[オーバーレイ（Overlays）]** パネルで、**[レール（Rails）]** の横にある **[削除（Delete）]** をクリックします。

使用可能なすべてのレール ラインがマップ上で強調表示されます。

ステップ 12 削除するレール ラインの上にマウスのカーソルを合わせ、クリックして削除します。

ステップ 13 **[保存（Save）]** をクリックします。

マーカーの配置

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある **[編集（Edit）]** をクリックします。

ステップ 4 **[オーバーレイ（Overlays）]** パネルで、**[マーカー（Markers）]** の横にある **[追加（Add）]** をクリックします。

描画アイコンが表示されます。

ステップ 5 マーカーの名前を入力し、[マーカーの追加（Add Marker）] をクリックします。

ステップ 6 描画アイコンをクリックし、マーカーをマップ上に配置します。

ステップ 7 **[Save（保存）]** をクリックします。

ステップ 8 [オーバーレイ（Overlays）] パネルで、[マーカー（Markers）] の横にある [編集（Edit）] をクリックします。

使用可能なマーカーがマップ上で強調表示されます。

ステップ 9 変更を加えて、[保存（Save）] をクリックします。

ステップ 10 **[オーバーレイ（Overlays）]** パネルで、**[マーカー（Markers）]** の横にある **[削除（Delete）]** をクリックします。

使用可能なすべてのマーカーがマップ上で強調表示されます。

ステップ 11 削除するマーカーの上にマウスのカーソルを合わせ、クリックして削除します。

ステップ 12 **[保存（Save）]** をクリックします。

フロア ビュー オプション

中央のペインのフロア プランの上にある **[オプションを表示（View Options）]** をクリックします。フロア マップと **[アクセス ポイント（Access Points）]**、**[センサー（Sensor）]**、**[オーバーレイ オブジェクト（Overlay Objects）]**、**[マップ プロパティ（Map Properties）]**、および **[グローバル マップ プロパティ（Global Map Properties）]** の各パネルが右側のペインに表示されます。

フロアマップの外観を変更するには、さまざまなパラメータを選択または選択解除します。たとえば、フロア マップ上のアクセス ポイント情報だけを表示する場合は、[アクセスポイント

（Access Point）] チェックボックスをオンにします。各パネルを展開して、各フロア要素で使用可能なさまざまな設定を構成できます。

アクセス ポイントの表示オプション

アクセス ポイントの横にある [オン（On）]/[オフ（Off）] ボタンをクリックして、アクセス ポイントをマップ上に表示します。[アクセスポイント（Access Points）] パネルを展開して、次の設定を行います。

- [表示ラベル（Display Label）]：ドロップダウン リストから、AP に関してフロア マップに表示するテキスト ラベルを選択します。使用可能な表示ラベルは次のとおりです。
  - [なし（None）]：選択したアクセス ポイントに関してラベルが表示されません。
  - [名前（Name）]：AP 名。
  - [AP MAC アドレス（AP MAC Address）]：AP の MAC アドレス。
  - [コントローラIP（Controller IP）]：アクセス ポイントが接続されているシスコ ワイヤレス コントローラの IP アドレス。
  - [無線 MAC アドレス（Radio MAC Address）]：無線 MAC アドレス。
  - **IP Address**
  - [チャネル（Channel）]：Cisco Radio のチャネル番号または [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。
  - [カバレッジホール（Coverage Holes）]：クライアントが接続を失うまで信号が弱まったクライアントのパーセンテージ。接続されていないアクセス ポイントについては [使用不可（Unavailable）]、monitor-only モードのアクセス ポイントについては [MonitorOnly] と表示されます。
  - [送信電力（TX Power）]：現在の Cisco Radio の送信電力レベル（1 が高い）または [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。無線帯域を変更すると、マップ上の情報もそれに応じて変更されます。

    電力レベルはアクセス ポイントのタイプによって異なります。1000 シリーズの AP では 1 ～ 5 の値、1230 アクセス ポイントでは 1 ～ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ～ 8 の値をとります。
  - [チャネルおよび送信電力（Channel and Tx Power）]：チャネルと送信電力レベルまたは [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。
  - [使用率（Utilization）]：関連付けられたクライアント デバイスで使用されている帯域幅のパーセンテージ（受信、送信、およびチャネル使用率を含む）。アソシエーションを解除されたアクセス ポイントでは **[Unavailable]**、monitor-only モードのアクセス ポイントでは **[MonitorOnly]** が表示されます。
  - [送信使用率（Tx Utilization）]：指定されたインターフェイスの送信（Tx）使用率。
  - [受信使用率（Rx Utilization）]：指定されたインターフェイスの受信（Rx）使用率。

- [チャネル使用率（Ch Utilization）]：指定されたアクセス ポイントのチャネル使用率。
- **関連付けられたClients**）]：関連付けられたクライアントの総数。
- [デュアルバンド無線（Dual-Band Radios）]：Cisco Aironet 2800 および 3800 シリーズ アクセス ポイント上の XOR デュアルバンド無線を識別してマークします。
- [ヘルス スコア（Health Score）]：AP のヘルス スコア。
- **問題数**
- **カバレッジの問題**
- **APダウンの問題**

- [ヒートマップ タイプ（Heatmap Type）]：ヒートマップは、変数から取得した値をマップに色として表した、無線周波数（RF）ワイヤレス データのグラフィック表示です。現在のヒートマップは、RSSI予測モデル、アンテナの方向、およびAP送信電力に基づいて計算されます。[ヒートマップ タイプ（Heatmap Type）] ドロップダウンリストから、ヒートマップのタイプ（[なし（None）] または [カバレッジ（Coverage）]）を選択してください。
  - **None**
  - [カバレッジ（Coverage）]：フロア プランにモニタ モード アクセス ポイントがある場合は、カバレッジ ヒートマップを選択できます。カバレッジ ヒートマップでは、モニタ モード アクセス ポイントは除外されます。
- [ヒートマップの不透明度（%）（Heatmap Opacity (%)）]：スライダを 0 ～ 100 の範囲でドラッグして、ヒートマップの不透明度を設定します。
- [RSSIカットオフ（dBm）（RSSI Cut off (dBm)）]：スライダをドラッグして RSSI カットオフ レベルを設定します。RSSI Cutoff の範囲は -60 dBm ～ -90 dBm です。
- [マップの不透明度（%）（Map Opacity (%)）]：スライダをドラッグしてマップの不透明度を設定します。

AP の詳細はすぐにマップに反映されます。マップ上の AP アイコンにマウス カーソルを合わせると、AP の詳細情報と RX ネイバー情報が表示されます。

センサーオプションの表示

[センサー（Sensors）] ボタンをクリックすると、マップ上にセンサーが表示されます。**[センサー（Sensors）]** パネルを展開して、次の設定を行います。

- [Display Label]：ドロップダウンリストから、選択したアクセスポイントに関してフロアマップに表示するテキストラベルを選択します。使用可能な表示ラベルは次のとおりです。
  - **None**

- [Name]：センサー名。
- [Sensor MAC Address]：センサーの MAC アドレス。

オーバーレイ オブジェクトの表示オプション

展開、**オーバーレイ オブジェクト** これらの設定を構成するパネル。[オン（On）]/[オフ（Off）] ボタンを使用して、これらのオーバーレイ オブジェクトをマップ上に表示します。

- **Coverage Areas**
- **Location Regions**
- **Obstacles**
- **Rails**
- **Markers**

マップ プロパティの設定

[マッププロパティ（Map Properties）] パネルを展開して、以下を構成します。

- **[自動更新（Auto Refresh）]**：間隔のドロップダウンリストを使用して、データベースからマップ データを更新する頻度を設定できます。[自動更新（Auto Refresh）] ドロップダウンリストから、時間間隔（[なし（None）]、[1 分（1 min）]、[2 分（2 mins）]、[5 分（5 mins）]、または [15 分（15 mins）]）を設定してください。

グローバル マップ プロパティの設定

[グローバル マップ プロパティ（Global Map Properties）] パネルを展開し、次のように設定します。

- [測定単位（Unit of Measure）]：ドロップダウンリストを使用して、マップの寸法測定値を [フィート（Feet）] または [メートル（Meters）] のいずれかに設定します。

データのフィルタリング

アクセスポイントデータのフィルタ処理

右側のペインの [Filters] パネルの下にある [Access Point] をクリックします。

- 中央のペインでフロア マップの上にあるドロップダウン リストで無線の種類を選択します（**2.4 GHz**、**5 GHz**、または **2.4 GHz および 5 GHz**）。

- クエリを追加するには、[ルールの追加（Add Rule）] をクリックします。
  - マップ上に表示するアクセスポイントの識別子を選択します。
  - アクセス ポイントをフィルタリングするパラメータを選択します。
  - テキスト ボックスに、該当するパラメータに固有のフィルタ条件を入力し、[検索（Go）] をクリックします。検索結果が表形式で表示されます。
  - [リストにフィルタを適用（Apply Filters to List）] をクリックして、マップ上でフィルタ結果を表示します。マップ上で特定のアクセスポイントを表示するには、表示されたテーブル内でアクセス ポイントのチェック ボックスをオンにし、[マップ上で選択を表示（Show Selected on Maps）] をクリックします。

テーブルの検索結果にカーソルを合わせると、AP の位置がマップ上に線でマークされます。

センサーデータのフィルタ処理

右側のペインの [Filters] パネルの下にある [Sensor] をクリックします。

- 中央のペインでフロア マップの上にあるドロップダウン リストで無線の種類を選択します（**2.4 GHz**、**5 GHz**、または **2.4 GHz および 5 GHz**）。
- クエリを追加するには、[ルールの追加（Add Rule）] をクリックします。
  - マップで表示するセンサーの識別子（名前および MAC アドレス）を選択します。
  - センサーをフィルタリングするパラメータを選択します。
  - テキスト ボックスに、該当するパラメータに固有のフィルタ条件を入力し、[検索（Go）] をクリックします。検索結果が表形式で表示されます。
  - [リストにフィルタを適用（Apply Filters to List）] をクリックして、マップ上でフィルタ結果を表示します。マップ上で特定のセンサーを表示するには、表示されたテーブル内でセンサーのチェックボックスをオンにし、[Show Selected on Maps] をクリックします。

テーブルの検索結果にカーソルを合わせると、センサーの位置がマップ上に線でマークされます。

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、ワイヤレス無線周波数（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 プロファイルの作成は、AP 1800S センサーデバイスにのみ適用されます。

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） すべての 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 Cisco DNA Center のホームページで、[Design] を選択します。

ステップ 2 [Network Settings] ドロップダウンリストから、[Wireless] を選択します。

ステップ 3 [Enterprise Wireless] の下で、[+ **Add**] をクリックします。

[Create an Enterprise Wireless Network] ウィンドウが表示されます。

ステップ 4 [Wireless Network Name (SSID)] テキストボックスに、作成するワイヤレスネットワークまたは SSID の一意の名前を入力します。

名前には、1 つのスペースを含めて、最大 32 文字の英数字を使用できます。< および / を除くすべての特殊文字を使用できます。

. および * のサブストリングの組み合わせは使用できません。

ステップ 5 [エンタープライズネットワークのタイプ (type Of Enterprise network)] ドロップダウンリストから、エンタープライズネットワークのタイプ (**音声とデータ**、または**データのみ**) を選択します。選択タイプは、ワイヤレスネットワークでプロビジョニングされる quality of service を定義します。

[Voice and Data] を選択すると、Quality of Service（QoS）が音声またはデータトラフィックのいずれかのアクセスに対して最適化されます。

[Data Only] オプションを選択した場合、サービス品質はワイヤレス データ トラフィックに対してのみ最適化されます。

ステップ 6 [Fast Lane] チェックボックスをオンにして、このネットワークで fastlane 機能を有効にします。

[Fast Lane] を選択すると、最適化されたレベルのワイヤレス接続と高度な Quality of Service（QoS）を受けるように IOS デバイスを設定できます。

ステップ 7 範囲内のすべてのワイヤレスクライアントに SSID を表示しない場合は、[Broadcast SSID] ボタンをオフにします。

[Broadcast SSID] をオフにすると、この SSID に接続しようとしているクライアントで SSID が非表示になり、ワイヤレス インフラストラクチャの不要な負荷が軽減されます。

ステップ 8 次のいずれかの**ワイヤレスオプション**を選択して、ワイヤレスバンドの設定を行います。

- **デュアルバンド動作 (2.4 ghz および 5 ghz)**: WLAN は2.4 と 5 ghz の両方に対して作成されます。バンド セレクトはデフォルトで無効です。
- **バンド セレクトによるデュアルバンド動作**: WLAN は 2.4 ghz および 5 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 のみ**: WLAN は 5 ghz に対して作成され、バンド セレクトは無効になります。
- [2.4 GHz only]：WLAN が 2.4 GHz 用に作成され、バンドセレクトが無効になります。

ステップ 9 [セキュリティのレベル（Level of Security）] の下で、このネットワークの暗号化および認証のタイプをセットします。セキュリティのオプションは次のとおりです。

- [WPA2 エンタープライズ（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 パーソナル（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 パーソナル（WPA2 Personal）] を選択した場合は、[パスフレーズ（Passphrase）] テキスト ボックスにパスフレーズを入力します。

  （注） 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（32 ページ）」を参照してください。

- **開く**：セキュリティは提供されません。すべてのデバイスが認証なしでワイヤレス ネットワークにアクセスできます。

ステップ 10 次を設定するには、[Show Advanced Settings] をクリックします。

ステップ 11 [Fast Transition (802.11r)] を、[Enable]、[Adaptive]、または [Disable] モードに設定します。

デフォルトでは、[Fast Transition (802.11r)] が [Adaptive] モードに設定されています。

802.r を使用すると、ワイヤレスクライアントが 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。

ステップ 12 [Over the DS] チェックボックスをオンにして、分散システム経由の Fast Transition を有効にします。このオプションは、[Fast Transition] を [Adaptive] モードに設定した場合にのみ指定できます。

デフォルトでは、[Over the DS] が有効になっています。

ステップ 13 [MAC フィルタリング（MAC Filtering）] チェック ボックスをオンにし、SSID での MAC ベースのアクセス制御を有効にします。

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。

ステップ 14 [Session Timeout] チェックボックスをオンにして、値（秒）を入力します。

セッションタイムアウトとは、クライアントセッションがアクティブである最大時間を指します。この時間が経過すると再認証を受ける必要があります。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。値の範囲は 300 ～ 86400 秒です。

ステップ 15 [Client Exclusion] チェックボックスをオンにして、クライアント除外タイマーの設定値を入力します。

ユーザ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対象から除外するため、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に接続できません。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。指定できる範囲は 0 ～ 2147483647 秒です。

ステップ 16 Under **MFP Client Protection**, click one of the radio buttons: **Optional**, **Required**, and **Disabled**.

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、アクセスポイント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、クライアントが CCXv5 MFP をサポートしていて WPA2 にも設定されている場合）のみ、クライアントはアソシエーションを許可されます。

ステップ 17 [11k] で [Neighbor List] チェックボックスをオンにすると、その 11k 対応クライアントは、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ます。

ローミングを容易にするため、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。同じ WLAN 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、AP は応答します。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。

ステップ 18 [11v BSS Transition Support] で、次のように設定します。

ステップ 19 [BSS Max Idle Service] チェックボックスをオンにして、アイドル期間タイマー値を設定します。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。

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関連付け解除しないタイムフレームです。

ステップ 20 [Client User Idle Timeout] チェックボックスをオンにして値を入力し、WLAN のユーザアイドルタイムアウトを設定します。

クライアントが送信するデータがユーザアイドルタイムアウト内で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 コントローラは次のタイムアウト期間中に更新されます。

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

ステップ 21 [Directed Multicast Service] チェックボックスをオンにして、Directed Multicast Service を有効にします。

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。

ステップ 22 [Next] をクリックします。

[ワイヤレス プロファイル（Wireless Profiles）] ウィンドウが表示されます。この SSID をワイヤレスプロファイルと関連付けることができます。

ステップ 23 [ワイヤレス プロファイル（Wireless Profiles）] ウィンドウで [+ 追加（+Add）] をクリックして、新しいワイヤレス プロファイルを作成します。

ステップ 24 [ワイヤレス プロファイルの作成（Create a Wireless Profile）] ウィンドウで、次を設定します。

ステップ 25 [ワイヤレス プロファイル名（Wireless Profile Name）] テキスト ボックスに、ワイヤレス プロファイルの名前を入力します。

ステップ 26 [Yes] または [No] を選択して、SSID がファブリックであるか、非ファブリックであるかを指定します。

ファブリック SSID は、ソフトウェア定義型アクセス (SD アクセス) の一部であるワイヤレスネットワークです。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。

ステップ 27 非ファブリック SSID を作成する場合は、[No] を選択して次のパラメータを設定します。

ステップ 28 [Interface Name] ドロップダウンリストから、SSID のインターフェイス名を選択するか、または [+ create a new wireless interface] をクリックして新しいワイヤレスインターフェイスを作成します。

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。

ステップ 29 [Select Interface] ドロップダウンリストから、SSID のインターフェイス名を選択するか、または [+ Create a Wireless Interface] をクリックして新しいワイヤレスインターフェイスを作成します。

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。

ステップ 30 [Flex Connect Local Switching] チェックボックスをオンにして、WLAN のローカルスイッチングを有効にします。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 アクセスポイントがデータパケットをローカルにスイッチできます。

ステップ 31 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 は、選択したインターフェイス名に基づいて自動的に入力されます。

VLAN ID を変更する場合は、[Local to VLAN] テキストボックスに VLAN ID の新しい値を入力します。

ステップ 32 このプロファイルをサイトに割り当てるには、[Sites] をクリックします。

ステップ 33 [Sites] ウィンドウで、サイトの横にあるチェックボックスをオンにしてこのプロファイルを関連付けます。

親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、すべての子が親サイトから設定を継承します。チェックボックスをオフにして、サイトの選択を解除できます。

ステップ 34 [OK] をクリックします。

ステップ 35 テンプレートをネットワークプロファイルに関連付けるには、[Attach Template(s)] 領域の下にある [+ Add] をクリックします。

ステップ 36 [Device Type]、[Tag Name]、および [Template] ドロップダウンリストから、デバイスのタイプ、タグ、テンプレートを選択します。

ステップ 37 [Add]をクリックします。

[Wireless Profiles] ウィンドウに、作成したプロファイルが表示されます。

ステップ 38 SSID をワイヤレスプロファイルに関連付けるには、[Wireless Profile] ウィンドウで、[Profile Name] チェックボックスをオンにします。

ステップ 39 [完了（Finish）] をクリックします。

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の設定を継承します。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 [設計（Design）] **[ネットワーク設定（Network Settings）]** > **[ワイヤレス（Wireless）]** > を選択します。

ステップ 2 ツリー メニューで、 PSK を編集するサイト、ビルディング、フロアを選択します。

ステップ 3 [エンタープライズ ワイヤレス （Enterprise Wireless）] 配下の [パスフレーズ（Passphrase）] テキストボックスをクリックし、PSK SSID の新しいパスフレーズを入力します。

ステップ 4 [Save] をクリックします。

「SSID のパスフレーズが正常に更新されました」という成功メッセージが表示されます。

SSID の横にある [継承（inherit）] アイコンをクリックすると、元の設定が表示されます。

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。

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 Cisco DNA Center のホームページから、**[Design]** > **[Network Settings]** > **[Wireless]** を選択します。

ステップ 2 [ゲスト ワイヤレス（Guest Wireless）] の下で、[+ 追加（+Add）] をクリックして、新しい SSID を作成します。

[ゲスト ワイヤレス ネットワークの作成（Create a Guest Wireless Network）] ウィンドウが表示されます。

ステップ 3 [ワイヤレス ネットワーク名 (SSID)（Wireless Network Name (SSID)）] テキストボックスに、作成するゲスト SSID の一意の名前を入力します。名前には、1 つのスペースを含めて、最大 32 文字の英数字を使用できます。< および / を除くすべての特殊文字を使用できます。

. および * のサブストリングの組み合わせは使用できません。

ステップ 4 [セキュリティのレベル（Level of Security）] の下で、このゲスト ネットワークの暗号化および認証のタイプを選択します。[Web 認証（Web Auth）] および [オープン（Open）] です。

外部 Web 認証（EWA）では、[セキュリティのレベル（Level of Security）] として [Web 認証（Web Auth）] を選択し、[認証サーバ（Authentication Server）] として [外部認証（External Authentication）] を選択します。

中央 Web 認証（CWA）では、[セキュリティのレベル（Level of Security）] として [Web 認証（Web Auth）] を選択し、[認証サーバ（Authentication Server）] として [ISE 認証（ISE Authentication）] を選択します。

[Web 認証（Web Auth）]の暗号化と認証タイプは、より高いレベルのレイヤ 3 セキュリティを提供します。

[オープン（Open）]暗号化と認証タイプは、セキュリティを提供しません。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。

ステップ 5 [Web 認証（Web Auth）] を選択した場合、認証サーバを [ISE 認証（ISE Authentication）] または [外部認証（External Authentication）] として設定する必要があります。

- [外部認証（External Authentication）] サーバでは、[Web 認証 URL（Web Auth URL）] テキスト ボックスにリダイレクトする URL を入力します。
- [ISE 認証 (ISE Authentication)] を選択した場合は、ドロップダウンリストから、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。

ステップ 6 認証が成功した後にゲストをリダイレクトするには、ドロップダウンリストからを選択します。

- [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。[リダイレクト URL（Redirect URL）] テキスト ボックスにリダイレクト URL を入力します。

SSIDを作成したので、それをワイヤレスプロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

ステップ 7 次の内容を設定するには、[Show Advanced Settings] をクリックします。

ステップ 8 [Client Exclusion] チェックボックスをオンにして、クライアント除外タイマーの設定値を入力します。

ユーザ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対象から除外するため、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に接続できません。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。指定できる範囲は 0 ～ 2147483647 秒です。

ステップ 9 [Session Timeout] チェックボックスをオンにして、値（秒）を入力します。

セッションタイムアウトとは、クライアントセッションがアクティブである最大時間を指します。この時間が経過すると再認証を受ける必要があります。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。値の範囲は 300 ～ 86400 秒です。

ステップ 10 Under **MFP Client Protection**, click one of the radio buttons: **Optional**, **Required**, and **Disabled**.

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、アクセスポイント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 上で設定されていて、クライアントが CCXv5 MFP をサポートしていて WPA2 にも設定されている場合）のみ、クライアントはアソシエーションを許可されます。

ステップ 11 [11v BSS Transition Support] で、次のように設定します。

ステップ 12 [BSS Max Idle Service] チェックボックスをオンにして、アイドル期間タイマー値を設定します。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。

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関連付け解除しないタイムフレームです。

ステップ 13 [Client User Idle Timeout] チェックボックスをオンにして値を入力し、WLAN のユーザアイドルタイムアウトを設定します。

クライアントが送信するデータがユーザアイドルタイムアウト内で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中に更新します。

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

ステップ 14 [Directed Multicast Service] チェックボックスをオンにして、Directed Multicast Service を有効にします。

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。

ステップ 15 [Next] をクリックします。

[ワイヤレス プロファイル（Wireless Profiles）] ウィンドウが表示されます。

ステップ 16 既存のワイヤレスプロファイルがない場合は、[**ワイヤレスプロファイル (Wireless Profiles)**] ウィンドウで [**+ 追加 (+ Add)**] をクリックして、新しいワイヤレスプロファイルを作成します。

ステップ 17 [ワイヤレス プロファイル名（Wireless Profile Name）] テキスト ボックスにプロファイル名を入力します。

ステップ 18 [ファブリック（Fabric）] の隣にある [はい（Yes）] または [いいえ（No）] ラジオ ボタンを選択して、SSID がファブリックであるか、そうでないかを指定します。

ファブリック SSID は、ソフトウェア定義型アクセス (SD アクセス) 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、SDA を使用することが必須です。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。

ステップ 19 ゲスト SSID をゲスト アンカーにする場合、[このゲスト SSID にゲスト アンカーが必要ですか（Do you need a Guest Anchor for this guest SSID）] の隣にある [はい（Yes）] または [いいえ（No）] ラジオ ボタンをクリックします。

ゲストの SSID をゲストアンカーにするには、[**はい (Yes)**] を選択します。

[No] を選択した場合は、[Flex Connect Local Switching] チェックボックスをオンにして、FlexConnect モードを有効にします。FlexConnect を選択すると、トラフィックがローカルに切り替わります。設定に基づき、プロファイルはサイトおよび内部的に作成された Flex グループに適用されます。

ステップ 20 [インターフェイスを選択（Select Interface）] 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、**[+] をクリックして新しいワイヤレス インターフェイスを作成**します。

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。

ステップ 21 サイトにこのプロファイルを割り当てるには、[サイト セレクタ（Site Selector）] テキスト ボックスに、完全なサイト名またはサイト名の一部を入力します。

使用可能なサイトが自動入力され、ドロップダウンリストから目的のサイトを選択することができます。

ステップ 22 [Save] をクリックします。

[ワイヤレス プロファイル（Wireless Profiles）] ウィンドウに、作成したプロファイルが表示されます。

ステップ 23 SSID をワイヤレスプロファイルに関連付けるには、[Wireless Profiles] ウィンドウで、[Profile Name] チェックボックスをオンにして SSID を関連付けてから、[Next] をクリックします。
[ポータルのカスタマイズ（Portal Customization）] ウィンドウが表示され、ゲスト ポータルに SSID を割り当てることができます。

ステップ 24 [ポータルのカスタマイズ（Portal Customization）] ウィンドウで [+ 追加（+ Add）] をクリックして、ゲスト ポータルを作成します。

[ポータル ビルダー（Portal Builder）] ウィンドウが表示されます。

ステップ 25 左側のメニューで [ページ コンテンツ（Page Content）] を展開し、さまざまな変数を組み込みます。

ステップ 26 ポータル テンプレート ウィンドウに変数をドラッグ アンド ドロップし、それらを編集します。

- [Login] ページの変数は、[Access Code]、[Header Text]、[AUP]、および [Text Fields] です。
- [Registration] ページの変数は、[First Name]、[Last Name]、[Phone Number]、[Company]、[Sms Provider]、[Person being visited]、[Reason for a visit]、[Header text]、[User Name]、[Email Address]、および [AUP] です。
- [Registration Success] ページの変数は、[Account Created] および [Header texts] です。
- [成功（Success）] ページの変数：**テキストフィールド**です。

ステップ 27 ポータルのデフォルト カラー スキームをカスタマイズするには、左側のメニューで [色（Color）] を展開し、色を変更します。

ステップ 28 フォントをカスタマイズするには、左側のメニューで [フォント（Font）] を展開し、フォントを変更します。

ステップ 29 [Save] をクリックします。

[ポータルのカスタマイズ（Portal Customization）] ページに作成したポータルが表示されます。

ステップ 30 [ポータル（Portals）] の下で、[ポータル名（Portal Name）] の隣にあるラジオ ボタンをクリックし、ゲスト ポータルに SSID を割り当てます。

ステップ 31 [Finish] をクリックします。

次のタスク

1. CDP または IP アドレス範囲を使用してデバイスを検出します。CDP を使用したネットワークの検出およびDiscover Your Network Using an IP Address Rangeを参照してください。
2. プラグアンドプレイを使用して、新しいデバイスを自動的に追加およびオンボードします。「プラグ アンド プレイ プロビジョニングを使用したデバイスのオンボーディング」を参照してください。
3. ネットワークのポリシーを設定します。「ポリシーの設定」を参照してください。
4. サイトに Cisco Wireless Controller を追加します。「デバイスをサイトに追加する」を参照してください。
5. シスコ ワイヤレス コントローラと Cisco AP をプロビジョニングします。Cisco Wireless Controller をプロビジョニングするおよびシスコ製 AP のプロビジョニング：Day 1 AP プロビジョニングを参照してください。
6. ファブリック ドメインに Cisco Wireless Controller を追加します。「ファブリックへのデバイスの追加」を参照してください。

7. ファブリック ドメインにアクセスできるさまざまなデバイス（ホスト）の設定を構成します。「ホスト オンボーディングの設定」を参照してください。

ゲストポータルページの作成

次のゲストポータルページを作成できます。

- ログイン ページ
- 登録ページ
- 登録成功
- 成功ページ（Success page）

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Guest Wireless]** を選択します。

ステップ 2 作成しているポータルページに移動します。

ステップ 3 [Portal Name] テキストボックスにポータル名を入力します。

ステップ 4 左側のメニューで [Page Content] を展開し、ポータルページの作成中にさまざまな変数を組み込みます。

- ログインページの変数のリスト：
  - Access Code
  - Header Text
  - AUP
  - Text Field
- 登録ページのリスト変数：
  - First Name
  - Last Name
  - Phone Number
  - Company
  - Sms Provider
  - Person being visited
  - Reason for a visit
  - Header text
  - User Name
  - Email Address
  - AUP

- 登録ページの変数のリスト：
  - Account Created
  - Header texts
- 成功ページの変数：
  - Text fields

ステップ 5 ポータルテンプレートページに変数をドラッグアンドドロップし、それらを編集します。

ステップ 6 ポータルのデフォルトカラースキームをカスタマイズするには、左側のメニューで[Color]を展開し、次のページ要素の色を変更します。

- Body text Border
- Link text Page
- Background
- Border Color
- Header Background

ステップ 7 フォントをカスタマイズするには、左側のメニューで [Font] を展開し、次を変更します。

- Typeface
- Header
- Title text
- Body text
- Form label

ステップ 8 [Save] をクリックしてポータルを保存します。

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 Cisco DNA Center のホームページから、**[Design]** > **[Network Settings]** > **[Wireless]** を選択します。

ステップ 2 [ワイヤレス インターフェイス（Wireless Interfaces）] の下で、[+ 追加（+Add）] をクリックします。

[新しいインターフェイス（New Interfaces）] ウィンドウが表示されます。

ステップ 3 [インターフェイス名（Interfaces Name）] テキスト ボックスで、動的なインターフェイスの名前を入力します。

ステップ 4 （オプション）[VLAN ID] テキスト ボックスで、インターフェイスの VLAN ID を入力します。有効な範囲は 0 ～ 4094 です。

ステップ 5 [OK] をクリックします。

ワイヤレス インターフェイスの下に、作成したインターフェイスが表示されます。

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 Cisco DNA Center のホームページから、**[Design]** > **[Network Settings]** > **[Wireless]** を選択します。

ステップ 2 **[ワイヤレス無線周波数プロファイル（Wireless Radio Frequency Profile）]** の下で、**[+ RF を追加（+Add RF）]**をクリックします。

[ワイヤレス無線周波数（Wireless Radio Frequency）] ウィンドウが表示されます。

ステップ 3 [プロファイル名（Profile Name）] テキスト ボックスに、RF プロファイル名を入力します。

ステップ 4 **[オン（On）]/[オフ（Off）]** ボタンを使用して、**[2.4 GHz]** または **[5 GHz]** のいずれかの無線バンドを選択します。無線のうちの 1 つを無効にした場合、この AP プロファイルを設定しようとしている AP の基本の無線が無効になります。

ステップ 5 [2.4 GHz] 無線タイプでは、次を設定します。

- [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、[高（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。保存された [データレート（Data Rate）] および [Tx設定（Tx Configuration）] で設定を変更すると、[親プロファイル（Parent Profile）] は自動的に [カスタム（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） [低（Low）]、[中（標準）（Medium (Typical)）]、および [高（High）] は、事前に定義された RF プロファイルです。事前に定義された RF プロファイルのいずれかを選択した場合、デバイスにあるそれぞれの RF プロファイルが使用され、新しい RF プロファイルはCisco DNA Center で作成されません。

- [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。
  - **[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、チャネル番号の隣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）] をクリックしてチャネル番号を選択します。[すべてを選択（Select All）] チェック ボックスをオンにして、[詳細オプション（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

番号の隣にあるチェックボックスをオンにします。B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。

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

- 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、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。
- [Tx電力構成（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。
  - **電力レベル**：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。
  - **電力しきい値**：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。[電力しきい値（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 dBM ～ 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。

ステップ 6 [5 GHz] 無線タイプでは、次を設定します。

- **[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。保存された [データレート（Data Rate）] および [Tx設定（Tx Configuration）] フィールドで設定を変更すると、[親プロファイル（Parent Profile）] は自動的に [カスタム（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） [低（Low）]、[中（標準）（Medium (Typical)）]、および [高（High）] は、事前に定義された RF プロファイルです。事前に定義された RF プロファイルのいずれかを選択した場合、すでにデバイスにあるそれぞれのRFプロファイルが使用され、新しいRFプロファイルはCisco DNA Center で作成されません。

- [チャネル幅（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を 1 つ選択します：[最適（Best）]、[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または [最適（Best）]。
- [DCA チャネル（DCA Channel）] 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 コントローラでこれらのチャネルをグローバルに設定する必要があります。

- [UNNI-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、1 つまたは複数の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、1 つまたは複数の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。

- 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するには、[データレート（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。
- [Tx電力構成（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。
  - **電力レベル**：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。
  - **電力しきい値**：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。[電力しきい値（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 dBM ～ 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。

ステップ 7 [Save] をクリックします。

ステップ 8 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 9 **[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

ワイヤレス センサー デバイス プロファイルの作成

ワイヤレス センサー デバイス プロファイルの作成は、Cisco Aironet 1800s アクティブ センサーに適用されます。

始める前に

イーサネット モジュールなしで Cisco Aironet AP 1800S センサーを使用している場合は、ワイヤレス コントローラの Cisco プロビジョニング SSID を有効にする必要があります。Cisco DNA Assurance ユーザガイド の「シスコ ワイヤレス コントローラのシスコ プロビジョニング SSID の有効化」を参照してください。

ステップ 1 **[設計（Design）] > [ネットワーク設定（Network Settings）] > [ワイヤレス（Wireless）]** を選択します。

ステップ 2 [センサーの設定（Sensor Settings）] で、[+ 追加（+Add）] をクリックします。

[センサー SSID 割り当ての作成（Create Sensor SSID Assignment）] ウィンドウが開きます。次のパラメータを設定します。

- [設定名（Settings Name）] フィールドに、センサー デバイス プロファイルの名前を入力します。
- [ワイヤレス ネットワーク名（SSID）（Wireless Network Name (SSID)）] フィールドに、SSID の名前を入力します。
- [セキュリティのレベル（Level of Security）] エリアでセキュリティ レベルを選択し、適切なクレデンシャル名を入力します。

（注） 有線接続で Cisco Aironet 1800s アクティブ センサーをプロビジョニングするには、任意のプロキシ名および SSID（例：wired_xyz）を入力し、[セキュリティのレベル（Level of Security）] エリアで、[オープン（Open）] を選択します。

ステップ 3 **[保存（Save）]** をクリックします。

Cisco Connected Mobile Experiences の統合について

Cisco DNA Center は、ワイヤレス マップのためのオンプレミス 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 インターフェイス内で、フロア マップ上でのクライアントの正確な場所を把握できます。

CMX の設定は、ユーザの要件に応じて、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 CMX サーバを Cisco DNA Center に追加するには、Cisco DNA Center のホームページで、歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[CMX Servers]** を選択します。

[CMX Servers] ウィンドウが表示されます。

ステップ 2 ⊕[Add] をクリックします。

[Add CMX Servers] ウィンドウが表示されます。

ステップ 3 [IP Address] フィールドに、CMX Web GUI の有効な IP アドレスを入力します。

ステップ 4 [User Name] および [Password] フィールドに、CMX Web GUI のユーザ名とパスワードのログイン情報を入力します。

ステップ 5 [SSH User Name] および [SSH Password] フィールドに、CMX 管理者のユーザ名とパスワードの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 6 [Add]をクリックします。

CMX サーバが正常に追加されました。

ステップ 7 サイト、ビル、またはフロアに CMX サーバを割り当てるには、次の手順を実行します。

ステップ 8 **[Design]** > **[Network Settings]** > **[Wireless]** を選択します。

ステップ 9 左側の [Tree View] メニューで、[Global] か、興味のあるエリア、ビルディング、フロアを選択します。

ステップ 10 [CMX Servers] の下で、[CMX Servers] ドロップダウンリストから CMX サーバを選択します。

ステップ 11 [Save] をクリックします。

[Create CMX Settings] ページが表示されます。

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。

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。[デバイス 360（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、左側のツリーペインで変更を加えたビルディングやフロアの隣にある歯車アイコンをクリックし、[Sync with CMX] を選択して、変更を手動でプッシュします。

ステップ 13 CMX サーバの詳細を編集するには、Cisco DNA Center で歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[CMX Servers]** を選択します。

ステップ 14 編集する CMX サーバを選択して変更を加え、[Update] をクリックします。

ステップ 15

ステップ 16 CMX サーバを削除するには、Cisco DNA Center で歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[CMX Servers]** を選択します。

ステップ 17 削除する CMX サーバを選択し、[Delete] をクリックします。

ステップ 18 [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 UI 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
```

Flex グループのネイティブ VLAN 設定

ネイティブ VLAN は、AP と シスコ ワイヤレス コントローラ 間の管理トラフィックを伝送します。この機能を使用すると、Cisco DNA Center ユーザ インターフェイスを介してサイトの VLAN を設定できます。グローバル レベルでネイティブ VLAN を設定し、サイト、ビルディング、またはフロア レベルでオーバーライドできます。

ステップ 1 Cisco DNA Center のホーム ページから、**[設計（Design）]** > **[ネットワーク設定（Network Settings）]** > **[ワイヤレス（Wireless）]** を選択します。

ステップ 2 グローバル レベルでネイティブ VLAN を設定する場合、左ペインで [グローバル（Global）] を選択します。

ステップ 3 [ネイティブVLAN（Native VLAN）] の下の [VLAN] テキスト ボックスに、VLAN ID の値を入力します。有効な範囲は 1 ～ 4094 です。

ステップ 4 [Save] をクリックします。

ステップ 5 SSID を設定し、ワイヤレス ネットワーク プロファイルを作成します。**[設計（Design）]** > **[ネットワークの設定（Network Settings）]** > **[ワイヤレス（Wireless）]** ページの [FlexConnect ローカル スイッチング（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、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （28 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 （32 ページ）を参照してください。

ステップ 6 保存済みの VLAN ID 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（Provision）] ページで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 Wireless Controller をプロビジョニングする」を参照してください。

ステップ 7 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。詳細については、「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」を参照してください。

ステップ 8 サイト、ビルディング、またはフロア レベルでネイティブ VLAN をオーバーライドするには、左側のツリー ビュー メニューでサイト、ビルディングまたはフロアを選択します。

ステップ 9 [ネイティブVLAN（Native VLAN）] の下で、VLAN ID の値を入力します。

ステップ 10 ワイヤレス コントローラ および関連付けられているアクセス ポイントを再プロビジョニングします。

ネットワークプロファイルの作成

Cisco DNA Center のホームページから、**[設計（Design）]** > **[ネットワークプロファイル（Network Profiles）]** を選択します。[プロファイルの追加（Add Profile）] をクリックして、次の項目に関するネットワークプロファイルを作成します。

- ルーティングと NFV
- スイッチング
- ワイヤレス

Create Network Profiles for Routing and NFV

このワークフローでは、次を実行する方法を示します。

1. ルータ WAN を設定します。
2. ルータ LAN を設定します。
3. ENCS 統合スイッチを設定します。
4. カスタム構成を作成します。
5. プロファイルの概要を表示します。

ステップ 1 **[設計（Design）] > [ネットワークプロファイル（Network Profiles）]** を選択します。

ステップ 2 [+プロファイルの追加（+Add Profiles）] をクリックし、[ルーティング & NFV（Routing & NFV）] を選択します。

ステップ 3 [ルータWAN構成（Router WAN Configuration）] ウィンドウが表示されます。

- [名前（Name）] テキスト ボックスにプロファイル名を入力します。
- ドロップダウンリストから、[Service Providers] および [Devices] の数を選択します。プロファイルあたり最大 3 つのサービス プロバイダーと 2 つのデバイスがサポートされています。
- ドロップダウンリストから [Service Provider Profile] を選択します。詳細については、「サービス プロバイダー プロファイルの設定 （65 ページ）」を参照してください。
- ドロップダウンリストから [Device Type]デバイスタイプを選択します。
- [Device Tag] に一意の文字列を入力して異なるデバイスを識別するか、ドロップダウンリストから既存のタグを選択します。選択内容は、ネットワークプロファイルに適用される Day-0 および Day-N テンプレートの一致基準の一部として使用されるため、適切なタグを選択してください。
- デバイスごとに1つ以上の回線リンクを有効にするには、[O] をクリックし、[接続（Connect）] の横のチェック ボックスをオンにします。ドロップダウンリストから、[Line Type] を選択します。[OK] をクリックします。

  複数のサービスプロバイダーを選択した場合は、プライマリインターフェイスをギガビットイーサネットとして、セカンダリをセルラーとして、または両方のインターフェイスをギガビットイーサネットとして選択できます。また、プライマリインターフェイスをセルラーとして、セカンダリインターフェイスをギガビットイーサネットとして選択することもできます。

  （注） Cisco 1100 シリーズ サービス統合型ルータ、Cisco 4200 シリーズ サービス統合型ルータ、Cisco 4300 シリーズ サービス統合型ルータ、および Cisco 4400 シリーズ サービス統合型ルータのみが、セルラーインターフェイスをサポートしています。

- [+サービスの追加（+Add Services）] をクリックして、プロファイルにサービスを追加します。[サービスの追加（Add Services）] ウィンドウが表示されます。[ISRv vEdge]、[WAN最適化装置（WAN Optimizer）]、または [ファイアウォール（Firewall）] の横のチェック ボックスをオンにします。または、[+サービスまたはネットワークの追加（+Add Service or Network）] を選択して、プロファイルにカスタム サービスまたはネットワークを追加することもできます。

  （注） このオプションは、Cisco ENCS 5000 シリーズ、Cisco ISR 4300、4400 シリーズ、および Cisco USC デバイスなどの NFV 機能をサポートするデバイスでのみ使用できます。

  ISRv ルータを構成するには、ドロップダウンリストから [Profile] を選択します。詳細については、ソフトウェア イメージのインポートを参照してください。**[保存（Save）]** をクリックします。

  vEdge を構成するには、ドロップダウンリストから [Profile] を選択します。

  WAN 最適化装置を構成するには、ドロップダウンリストから [Services] と [Profile] を選択します。

  ファイアウォールを構成するには、ドロップダウンリストから [Services]、[Profile]、および [Mode] を選択します。

ダイレクト インターネット アクセス（DIA）を有効にするには、[Firewall] を選択し、[DIA] の横のチェックボックスをオンにします。

カスタムネットワークを構成するには、[+Add Custom Service or network] を選択し、[Networks] を選択します。[ネットワーク名（Network Name）] にネットワークの名前を入力します。[接続の種類（Connection Type）] と [ネットワークモード（Network Mode）] を選択します。[VLAN] に VLAN ID を入力し、接続するサービスを選択します。[Save] をクリックします。

カスタムサービスを構成するには、[+Add Service or Network] を選択し、さらに [Service] を選択します。[Add a Custom Service] ウィンドウで、Linux または Windows Server などのサービス名を入力します。[Save] をクリックします。

- **[次へ (Next)]** をクリックします。

ステップ 4 [ルータWAN構成（Router WAN Configuration）] ページが表示されます。

- [L2]、[L3] または [Skip] サービスを選択します。
- [L2] を選択した場合は、ドロップダウンリストから [Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。
- [L3] を選択した場合は、ドロップダウンリストから [Protocol Routing] を選択し、[Protocol Qualifier] を入力します。
- **[Next]** をクリックします。

ステップ 5 ENCS デバイスを選択した場合は、[ENCS Integrated Switch Configuration] ページが表示されます。

- [+Add Row] をクリックします。ドロップダウンリストから、[Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。
- **[Next]** をクリックします。

ステップ 6 [カスタム構成（Custom Configuration）] ページが表示されます。

カスタム構成はオプションです。手順をスキップしても、ネットワーク プロファイルでいつでも構成を適用できます。

カスタム構成の追加を選択した場合：

- 必要に応じて、[Onboarding Template(s)] または [Day-N Templates] タブを選択します。
- ドロップダウンリストからテンプレートを選択します。テンプレートは、[Device Type] と [Tag Name] でフィルタリングされます。
- **[Next]** をクリックします。

ステップ 7 **[概要（Summary）]** ページが表示されます。

このページには、ルータ設定の概要が表示されます。選択されたデバイスとサービスに基づいて、ハードウェアの推奨事項がこのページで提供されます。

- [Save] をクリックします。

ステップ 8 [ネットワークプロファイル（Network Profiles）] ページが表示されます。

[サイトの割り当て（Assign Sites）] をクリックして、ネットワーク プロファイルにサイトを割り当てます。詳細については、「ネットワーク階層のサイトの作成 （3 ページ）」を参照してください。

スイッチ用のネットワークプロファイルの作成

スイッチングプロファイルには、オンボーディングテンプレートと Day N テンプレートの 2 種類の設定テンプレートを適用できます。

始める前に

デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。デバイス設定の変更を自動化するテンプレートの作成を参照してください。

ステップ 1 **[Design]** > **[Network Profiles]** を選択します。

ステップ 2 [+Add Profiles] をクリックし、[Switching] を選択します。

ステップ 3 [Switching Configuration] ウィンドウが表示されます。

作成するテンプレートのタイプに応じて、[OnBoarding Template] または [Day-N Template] のいずれかをクリックします。

- [追加（Add）] をクリックします。
- [Device Type] ドロップダウンリストから、[Switches and Hubs] を選択します。
- ドロップダウンリストから [Tag Name] を選択します。この手順は任意です。選択したタグがすでにテンプレートに関連付けられている場合は、そのテンプレートのみが [Template] ドロップダウンで使用できます。
- ドロップダウンリストから [Device Type] を選択します。
- ドロップダウンリストから [Template] を選択します。すでに作成済みの [Onboarding Configuration] テンプレートを選択できます。

ステップ 4 [Save] をクリックします。

スイッチに設定されているプロファイルは、スイッチのプロビジョニング時に適用されます。サイトを有効にするには、サイトにネットワークプロファイルを追加する必要があります。

ワイヤレス用のネットワークプロファイルの作成

ステップ 1 **[設計（Design）]** > **[ネットワークプロファイル（Network Profiles）]** を選択します。

ステップ 2 [+Add Profiles] をクリックし、[Wireless] を選択します。

ワイヤレス ネットワーク プロファイルを割り当てる前に、**[Design]** > **[Network Settings]** > **[Wireless]** タブでワイヤレス SSID を作成していることを確認します。

ステップ 3 [Add a Network Profile] ウィンドウが表示されます。

ステップ 4 [Profile Name] テキストボックスに有効なプロファイル名を入力します。

ステップ 5 [+ Add SSID] をクリックします。

[Network Settings] > **[Wireless]** タブの下で作成されたこれらの SSID が追加されます。

ステップ 6 [SSID] ドロップダウン リストで、[SSID] を選択します。

SSID タイプが表示されます。

ステップ 7 [Yes] または [No] を選択して、SSID がファブリックであるか、非ファブリックであるかを指定します。

ステップ 8 非ファブリック SSID を作成する場合は、[No] を選択して次のパラメータを設定します。

ステップ 9 [Interface Name] ドロップダウンリストから、SSID のインターフェイス名を選択するか、または [+ create a new wireless interface] をクリックして新しいワイヤレスインターフェイスを作成します。

ステップ 10 [Flex Connect Local Switching] チェックボックスをオンにして、WLAN のローカルスイッチングを有効にします。

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 アクセスポイントがデータパケットをローカルにスイッチできます。

ステップ 11 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 は、選択したインターフェイス名に基づいて自動的に入力されます。

VLAN ID を変更する場合は、[Local to VLAN] テキストボックスに VLAN ID の新しい値を入力します。

ステップ 12 [Save] をクリックして、ネットワークプロファイルを追加します。

新しく追加されたネットワークプロファイルが、**[Design]** > **[Network Profiles]** ページに表示されます。

ステップ 13 このプロファイルをサイトに割り当てるには、[Assign Sites] をクリックします。

ステップ 14 [Add Sites To Profile] ウィンドウで、サイトの横にあるチェック ボックスをオンにして、このプロファイルを関連付けます。

親ノードまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その親ノードの下にある子もすべて選択されます。チェックボックスをオフにして、サイトの選択を解除できます。

ステップ 15 [Select] をクリックします。

グローバル ネットワーク設定について

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、およびNTP、Syslog、SNMP トラップ、NetFlow コレクタなどのサーバ、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などに影響を与えます。
- [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、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。デバイスの可制御性と監査ログの詳細については、the Cisco Digital Network Architecture Center 管理者ガイドを参照してください。

[Design] > [Network settings] を選択し、[Network]、[Device Credentials]、[IP Address Pools]、[SP Profiles]、または [Wireless] などの適切なタブを選択して、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 サーバなどのネットワーク サーバ：詳細については、グローバル ネットワーク サーバの設定 （65 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 （53 ページ）、グローバル SNMPv2c クレデンシャルの設定 （54 ページ）、グローバル SNMPv3 クレデンシャルの設定 （56 ページ）、およびグローバル HTTPS クレデンシャルの設定 （58 ページ）を参照してください。
- IP アドレス プール：詳細については、IP アドレス プールを設定する （62 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 （27 ページ）を参照してください。

デバイス クレデンシャルについて

デバイスクレデンシャルとは、ネットワークデバイスに設定されている CLI、SNMP、HTTPS クレデンシャルを指します。Cisco DNA Center では、これらのクレデンシャルを使用してネットワーク内のデバイスに関する情報を検出および収集します。Cisco DNA Center では、ほとんどのデバイスが使用するクレデンシャルを指定できるため、ディスカバリ ジョブを実行するたびにクレデンシャルを入力する必要はありません。設定したクレデンシャルは、[ディスカバリ（Discovery）] ツールで使用可能になります。

CLI クレデンシャル

ディスカバリ ジョブを実行するには、Cisco DNA Center でネットワーク デバイスの CLI クレデンシャルを設定する必要があります。

これらのクレデンシャルは、ネットワークデバイスの CLI にログインするために Cisco DNA Centerによって使用されます。Cisco DNA Centerは、これらのクレデンシャルを使用して、ネットワークデバイスに関する情報を検出し、収集します。ディスカバリ プロセスの実行時に、Cisco DNA Center は CLI ユーザ名とパスワードを使用してネットワーク デバイスにログインし、**show** コマンドを実行してデバイスのステータスや設定情報を収集します。また、**clear** コマンドやその他のコマンドを実行して、デバイスの設定に保存されていないアクションを実行することもあります。

（注） Cisco DNA Center の実装では、ユーザ名だけがクリアテキストで提供されます。

SNMPv2c のクレデンシャル

簡易ネットワーク管理プロトコル（SNMP）は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージフォーマットを提供します。SNMP は、ネットワーク デバイスをモニタおよび管理するために標準化されたフレームワークと共通言語を提供しています。

SNMPv2c は SNMPv2 に代わるコミュニティ ストリング ベースの管理フレームワークです。SNMPv2c では、認証および暗号化が行われません（noAuthNoPriv セキュリティ レベル）。代わりに、クリアテキストで通常提供されるパスワード タイプとして、コミュニティ ストリングを使用します。

（注） Cisco DNA Center の実装では、セキュリティの理由から SNMP コミュニティ ストリングはクリアテキストで提供されません。

ディスカバリ機能を使用してネットワーク デバイスを検出する前に、SNMPv2c コミュニティ ストリング値を設定する必要があります。設定する SNMPv2c コミュニティ ストリング値は、

ネットワーク デバイスで設定された SNMPv2c 値と一致している必要があります。Cisco DNA Center では、最大 5 つの read コミュニティ ストリングと 5 つの write コミュニティ ストリングを設定できます。

ネットワークで SNMPv2 を使用している場合、最善の結果を実現するには Read Only（RO）コミュニティ ストリング値と Read/Write（RW）コミュニティ ストリング値の両方を指定します。両方を指定できない場合は、RO 値を指定することを推奨します。RO 値を指定しなければ、Cisco DNA Center はデフォルトの RO コミュニティ ストリングの *public* を使用してデバイスを検出しようとします。RW 値のみを指定すると、ディスカバリで RW 値が RO 値として使用されます。

SNMPv3 のクレデンシャル

ディスカバリを使用するために設定する SNMPv3 値は、ネットワーク デバイスで設定された SNMPv3 値と一致している必要があります。最大 5 つの SNMPv3 値を設定できます。

SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージが有効な送信元からのものかどうかを判別します。
- 暗号化：パケット コンテンツのスクランブルによって、不正な送信元から認識できないようにします。

SNMPv3 では、セキュリティモデルとセキュリティレベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザ ロール向けに設定される認証方式です。セキュリティレベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティモデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティモデル内のさまざまなセキュリティレベルは、次のとおりです。

- noAuthNoPriv：認証または暗号化を実行しないセキュリティレベル
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル。
- AuthPriv：認証と暗号化両方を実行するセキュリティレベル

次の表に、セキュリティ モデルとセキュリティ レベルの組み合わせを示します。

表 *2 : SNMPv3* セキュリティ モデルおよびセキュリティ レベル

レベル	認証	暗号化	結果
noAuthNoPriv	ユーザ名	未対応	ユーザ名の照合を使用して認証します。

レベル	認証	暗号化	結果
AuthNoPriv	次のいずれかを行います。 • HMAC-MD5 • HMAC-SHA	なし	ハッシュメッセージ認証コード - セキュア ハッシュ アルゴリズム（HMAC-SHA）に基づく認証を提供します。
AuthPriv	次のいずれかを行います。 • HMAC-MD5 • HMAC-SHA	次のいずれかを行います。 • CBC-DES • CBC-AES-128	HMAC-MD5 または HMAC-SHA に基づく認証を提供します。 暗号ブロック連鎖（CBC）DES（DES-56）標準または CBC モードの AES 暗号化に基づいた認証に加え、データ暗号規格（DES）の 56 ビット暗号化を提供します。

HTTPS クレデンシャル

HTTPS は、特殊な PKI 証明書ストアに基づく HTTP のセキュア バージョンです。Cisco DNA Center では、シスコ エンタープライズ ネットワーク機能仮想化インフラストラクチャ ソフトウェア（NFVIS）デバイスの検出にのみ HTTPS が使用されます。

グローバル デバイス クレデンシャルについて

「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 5 つのグローバル CLIクレデンシャルを設定して保存できます。

ステップ 1 Cisco DNA Center のホームページで、**[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）]** の順に選択します。

ステップ 2 グローバル サイトを選択した状態で、[CLI クレデンシャル（CLI Credentials）] エリアで [追加（Add）] をクリックします。

ステップ 3 次のフィールドに情報を入力します。

表 *3 : 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もう一度入力します。 （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もう一度入力します。 （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 4 **[保存（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、左側の階層にあるサイトをクリックし、クレデンシャルの横にあるボタンを選択して、[保存（Save）] をクリックします。

ステップ 5 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、[今すぐ実行（Now）]ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（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 SNMPv2c 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 SNMPv2c 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 Cisco DNA Centerのホームページで、[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）] の順に選択します。

ステップ 2 グローバルサイトを選択した状態で、[SNMP クレデンシャル（SNMP Credentials）] エリアで [追加（Add）] をクリックします。

ステップ 3 [タイプ（Type）] で、[SNMP v2c] をクリックし、次の情報を入力します。

表 *4 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [名前/説明（Name/Description）] : 追加する SNMP v2c 設定の名前または説明。 • **Read コミュニティ**：デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ ストリング 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	• [名前/説明（Name/Description）] : 追加する SNMP v2c 設定の名前または説明。 • **Write コミュニティ**：デバイス上の SNMP 情報を変更するために使用される write コミュニティ ストリング。 （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 4 **[保存（Save）]** をクリックします。

ステップ 5 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、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（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 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 Cisco DNA Centerのホームページで、[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）] の順に選択します。

ステップ 2 グローバル サイトを選択した状態で、[SNMP クレデンシャル（SNMP Credentials）] エリアで [追加（Add）] をクリックします。

ステップ 3 [タイプ（Type）] で、**[SNMP v3]** をクリックし、次の情報を入力します。

表 *5 : 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**：認証または暗号を提供しません。 • **AuthNoPriv**：認証を提供しますが、暗号は提供しません。 • **AuthPriv**：認証と暗号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。

フィールド	説明
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**：プライバシー設定なし。
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 4 **[保存（Save）]** をクリックします。

ステップ 5 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、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（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 Cisco DNA Center のホームページで、**[Design]** > **[Network Settings]** > **[Device Credentials]** の順に選択します。

ステップ 2 グローバル サイトを選択した状態で、[HTTPS クレデンシャル（HTTPS Credentials）] エリアで [追加（Add）] をクリックします。

ステップ 3 次の情報を入力します。

表 *6 : 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、[読み取り（Read）] または [書き込み（Write）] です。
Read	最大 5 つの HTTPS 読み取りクレデンシャルを設定できます。 • **名前/説明**：追加する HTTPS ログイン情報の名前または説明です。 • **ユーザ名**：HTTPS 接続の認証に使用される名前です。 • **パスワード**：HTTPS 接続の認証に使用されるパスワードです。 • **ポート**：HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 （注） パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、< > @ ' , : ; ! およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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。

フィールド	説明
Write	最大 5 つの HTTPS 書き込みクレデンシャルを設定できます。 • **Name/Description**：追加する HTTPS ログイン情報の名前または説明です。 • **ユーザ名**：HTTPS 接続の認証に使用される名前です。 • **パスワード**：HTTPS 接続の認証に使用されるパスワードです。 • **ポート**：HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 （注） パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<> @ ' , : ; ! およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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 4 **[保存（Save）]** をクリックします。

ステップ 5 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、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（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。

- グローバル デバイス クレデンシャルを編集し、それらの変更を適用する際、Cisco DNA Center ではこの操作がサポートされない一部のデバイス タイプがあります。編集されたグローバル デバイス クレデンシャルを適用できるデバイスのリストは、**[設計（Design）] > [ネットワークの設定（Network Settings）] > [デバイス クレデンシャル（Device Credentials）]** から、任意の[編集（Edit）] ウィンドウ上部にある **[詳細（Learn More）]** リンクをクリックします。

- 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 クレデンシャルをデバイスにプッシュします。
  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、既存のクレデンシャルを更新すると、[プロビジョニング（Provision）] > [デバイス（Devices）] > [インベントリ（Inventory）] 画面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

グローバル デバイス クレデンシャルを編集する場合、変更はグローバル サイトの下のサイトに関連付けられているすべてのデバイスに影響します。グローバル デバイス クレデンシャルを編集および保存した後に、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。

グローバル デバイス クレデンシャルの編集の詳細については、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 （59 ページ）を参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[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）]** の順に選択します。

ステップ 2 グローバル サイトを変更した状態で、変更するデバイス クレデンシャルを選択し、右側の [アクション（Actions）] 列の下にある [編集（Edit）] をクリックします。

（注） グローバル デバイス クレデンシャルを編集し、それらの変更を適用する際、Cisco DNA Center ではこの操作がサポートされない一部のデバイス タイプがあります。編集されたグローバル デバイス クレデンシャルを適用できるデバイスのリストは、**[設計（Design）] > [ネットワークの設定（Network Settings）] > [デバイス クレデンシャル（Device Credentials）]** から、任意の[編集（Edit）] ウィンドウ上部にある **[詳細（Learn More）]** リンクをクリックします。

ステップ 3 必要な変更を行い、[Save] をクリックします。

ステップ 4 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かを選択します。

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

（注） [タイム ゾーン（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。

デバイス クレデンシャルの変更が成功したか、または失敗したかを示すステータス メッセージが表示されます。

ステップ 5 クレデンシャル変更のステータスを表示するには、 のホーム ページで、[プロビジョニング（Provision）] > [デバイス（Devices）] > [インベントリ（Inventory）] の順に選択します。Cisco DNA Center

[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。

- [成功（Success）]：Cisco DNA Center はクレデンシャル変更を正常に適用しました。
- [失敗（Failed）]：Cisco DNA Center はクレデンシャル変更を適用できませんでした。失敗したクレデンシャル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。
- 該当なし（Not Applicable）：クレデンシャルはデバイス 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 失敗したクレデンシャル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 Cisco DNA Center のホームページで、**[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）]** の順に選択します。

ステップ 2 左側のペインの階層からサイトを選択します。

ステップ 3 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 **[保存（Save）]** をクリックします。

デバイスのクレデンシャルとサイトとの関連付けが正常に成功したことを示すメッセージが、画面の下部に表示されます。

ステップ 4 **[リセット（Reset）]** をクリックして、画面上のエントリをクリアします。

IP アドレス プールを設定する

Cisco DNA Center リリース 1.3 以降の IPv4 および IPv6 デュアルスタックをサポートします。

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 Digital Network Architecture Center 管理者ガイドを参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[Design] > [Network Settings] > [IP Address Pools]** の順に選択します。

ステップ 2 **[追加（Add）]** をクリックし、結果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 IP アドレスプールが IP アドレスプール表に表示されます。IPv4 または IPv6 のアドレスプールのみを表示する場合は、[サブネットタイプ（SUBNET TYPE）] の表で [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 Digital Network Architecture Center 管理者ガイドを参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。

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 Cisco DNA Center のホームページで、**[Design]** > **[Network Settings]** > **IP Address Pools]** の順に選択します。

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 [Import] をクリックします。

IP 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 Cisco DNA Center のホームページで、**[設計（Design）] > [ネットワーク設定（Network Settings）] > [IP アドレス プール（IP Address Pools）]** の順に選択します。

ステップ 2 [ネットワーク階層（Network Hierarchy）] ペインで、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 プール名（IP Pool Name）]：予約済み IP アドレスのプールの一意の名前。
- [タイプ（Type）]：IP アドレス プールのタイプ。LAN 自動化のバイアは、**LAN** を選択します。次のオプションがあります。
  - [LAN]：該当する VNF とアンダーレイの 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。管理ネットワークは、VNF 管理用に VNF に接続される専用ネットワークです。
  - [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。サービスネットワークは、VNF 内の通信に使用されます。
  - [WAN]：UCS-E プロビジョニングの場合は NFVIS に IP アドレスを割り当てます。
  - [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/No. of IP Addresses]：グローバル IP アドレスプールのすべてまたは一部を予約するための IP サブネットとマスクアドレス、または予約する IP アドレス数。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 サーバを必要とせずに、自動的に IP アドレスを獲得します）。
- ゲートウェイ IP アドレス（Gateway IP Address）：ゲートウェイ IP アドレス。
- **DHCP Servers**: DHCP サーバの IP 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）、シングルスタック IP プールに戻すことはできません。シングルスタックに戻るには、IP プールをリリースして、それらを新しく割り当てます。

サービス プロバイダー プロファイルの設定

特定の WAN プロバイダーのサービス クラスを定義するサービス プロバイダー（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 Cisco DNA Center のホームページから、**[Design]** > **[Network Settings]** > **[SP Profiles]** を選択します。

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

ステップ 3 **[プロファイル名（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ーを入力するか、既存のプロバイダーを選択します。

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 プロバイダーのプロファイル を参照してください。

グローバル ネットワーク サーバの設定

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 Cisco DNA Center のホームページで、**[設計（Design）] > [ネットワーク設定（Network Settings）] > [ネットワーク（Network）]** の順に選択します。

ステップ 2 **[DHCP サーバ（DHCP Server）]** フィールドに、DHCP サーバの 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 サーバを定義する必要があります。

ステップ 3 **[DNS サーバ（DNS Server）]** フィールドに、DNS サーバ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 サーバを定義する必要があります。

ステップ 4 （任意） Syslog、SNMP トラップ、および NetFlow コレクタ サーバ情報を入力できます。**[サーバの追加（Add Servers）]** をクリックして NTP サーバを追加します。

（注） ファブリック コンプライアンス チェックをトリガするには、Cisco DNA Center の IP アドレスを使用して SNMP サーバを設定します。詳細については、「ファブリックへのデバイスの追加（Add a Device to a Fabric）」を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

Cisco ISE またはその他の AAA サーバの追加

Cisco Identity Services Engine（ISE）サーバまたはその他の同様の AAA サーバを、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 ごとに 1 つの ISE のみがサポートされます。

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 ISE クラスタには独自のサーバグループがあります。RADIUS サーバと TACACS サーバ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 サーバで自動的に更新されます。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。

ステップ 1 Cisco DNA Center のホームページで、**[設計（Design）]** > **[ネットワーク設定（Network Settings）]** > **[ネットワーク（Network）]** の順に選択します。

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

ステップ 3 [サーバの追加（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 サーバをネットワークユーザ、クライアント/エンドポイントユーザ、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 サーバのサーバ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。

- [Network] ドロップダウンリストから、ISE サーバの 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 サーバのすべての IP アドレスが含まれています。ISE の IP を選択すると、選択した 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 WLC 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 ISE 以外の AAA サーバが含まれています。

ステップ 7 **[保存（Save）]** をクリックします。

Cisco DNA Center からのシスコ WLC 高可用性の設定 Cisco DNA Center

シスコ ワイヤレス コントローラ高可用性（HA）を Cisco DNA Center から設定できます。現在、ワイヤレスコントローラ HA の形成がサポートされています。HA およびスイッチオーバーオプションの中断はサポートされていません。

ここでは、次のトピックについて説明します。

ハイ アベイラビリティ用 Cisco ワイヤレス コントローラ設定の前提条件

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の検出機能とインベントリ機能が正常である必要があります。デバイスが [Managed] 状態になっている必要があります。

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 のサービスポートと管理ポートが設定されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長ポートが物理的に接続されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の管理アドレスが同じサブネット内にある必要があります。ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長管理アドレスも同じサブネット内にある必要があります。
- ワイヤレスコントローラで次のブート変数を手動で設定します。

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

シスコ ワイヤレス コントローラ HA の設定

ステップ 1 Cisco DNA Center のホームページから、[Provision] > [Devices] を選択します。

[Devices] > **[Inventory]** ページが表示され、検出されたすべてのデバイスがこのページに一覧表示されます。

ステップ 2 プライマリコントローラとして設定するコントローラ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 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] ページが表示されます。

ステップ 4 [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスをそれぞれテキストボックスに入力します。

冗長性管理 IP およびピア冗長管理 IP に使用される IP アドレスは、シスコワイヤレスコントローラの管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがこのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 5 [Select Secondary WLC] ドロップダウンリストから、セカンダリコントローラを選択します。

ステップ 6 [Configure HA] をクリックします。
HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリ ワイヤレスコントローラが設定されます。成功したら、セカンダリ ワイヤレス コントローラが設定されます。設定が完了したら、両方のワイヤレスコントローラが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 7 HA 設定を確認するには、**[Devices]** > **[Inventory]** ページで、HA デバイスとして設定したデバイスをクリックします。

ステップ 8 [Wireless Info] タブをクリックします。

[Redundancy Summary] には、[Sync Status] が [In Progress] として表示されます。Cisco DNA Center で HA のペアリングが成功したことが検出されると、[Sync Status] が [Complete] に変わります。

これは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリ ワイヤレス コントローラ（ワイヤレスコントローラ 2）は、Cisco DNA Center から削除されます。このフローは、ワイヤレスコントローラでの正常な HA 設定を示しています。

高可用性プロセス中および完了後に起こること

1. Cisco WLC-1 および WLC-2 は、冗長管理、冗長ユニット、および SSO とともに設定されます。ワイヤレス コントローラはロールをアクティブまたはスタンバイとしてネゴシエートするために再起動します。設定は、アクティブからスタンバイに同期されます。
2. [冗長性の概要の表示（Show Redundancy Summary）] ページで、次の設定を確認できます。
   - SSO が有効になっています
   - ワイヤレス コントローラがアクティブ状態になっています
   - ワイヤレス コントローラがホット スタンバイ状態になっています
3. アクティブ ワイヤレス コントローラの管理ポートは、両方のコントローラによって共有され、アクティブ コントローラを指します。スタンバイ ワイヤレス コントローラのユーザー インターフェイス、Telnet、および SSH は機能しません。コンソールとサービス ポート インターフェイスを使用して、スタンバイ ワイヤレス コントローラを制御できます。

高可用性を設定および確認するためのコマンド

シスコ ワイヤレス コントローラ HA を設定するには、Cisco DNA Center で次のコマンドを送信します。

Cisco DNA Center で次のコマンドを ワイヤレス コントローラ 1 に送信します。

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center で次のコマンドを ワイヤレス コントローラ 2 に送信します。

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

ワイヤレス コントローラ から HA 設定を検証するには、次のコマンドを入力します。

- HA 関連の詳細情報を確認する場合：**config redundancy mode sso**
- 設定済みのインターフェイスを確認する場合：**show redundancy summary**