



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 \(2 ページ\)](#)
- [ネットワーク階層について \(2 ページ\)](#)
- [フロア マップのモニターリング \(12 ページ\)](#)
- [フロア要素とオーバーレイの編集 \(12 ページ\)](#)
- [フロア ビュー オプション \(26 ページ\)](#)
- [データのフィルタリング \(31 ページ\)](#)
- [Ekahau プロジェクトファイルを使用したフロアマップの作成 \(33 ページ\)](#)
- [インタラクティブフロアプランニングについて \(36 ページ\)](#)
- [グローバルワイヤレス設定の構成 \(39 ページ\)](#)
- [ネットワークプロファイルの作成 \(67 ページ\)](#)
- [グローバルネットワーク設定について \(78 ページ\)](#)
- [デバイス クレデンシアルについて \(79 ページ\)](#)
- [グローバルデバイス クレデンシアルについて \(81 ページ\)](#)
- [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 \(88 ページ\)](#)
- [グローバルデバイス クレデンシアルの編集 \(89 ページ\)](#)
- [デバイス クレデンシアルのサイトへの関連付け \(90 ページ\)](#)
- [IP アドレス プールを設定する \(91 ページ\)](#)
- [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 \(91 ページ\)](#)
- [CSV ファイルから IP アドレスプールをインポートする \(92 ページ\)](#)
- [IP プールの予約 \(92 ページ\)](#)
- [IP プールの編集 \(93 ページ\)](#)
- [IP プールの削除 \(94 ページ\)](#)
- [IP プールの複製 \(94 ページ\)](#)
- [IP プールのリリース \(95 ページ\)](#)
- [IP アドレスプールの表示 \(95 ページ\)](#)
- [サービス プロバイダ プロファイルの設定 \(97 ページ\)](#)
- [グローバル ネットワーク サーバーの設定 \(97 ページ\)](#)
- [Cisco ISE またはその他の AAA サーバーの追加 \(98 ページ\)](#)

新しいネットワーク インフラストラクチャの設計

[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、[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 \(78 ページ\)](#) 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。

プロビジョニングされていないデバイスのサイト階層は、サイトマップ上の AP の場所を維持したまま変更できます。ただし、既存のフロアを別の建物に移動することはできません。

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。[Design] エリアは、直観的な操作のために階層型になっており、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がありません。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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。

世界地図が右側のペインに表示されます。

ステップ 2 [Network Hierarchy] ウィンドウで、 [+ Add Site] > [Add Area] > または左側ペインの親サイトの横にある歯車アイコン (⚙) をクリックして、 [Add Area] をクリックします。

ステップ 3 サイトの名前を [Area Name] フィールドに入力します。

ステップ 4 [Parent] ドロップダウンリストから、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。

左側ペインの親ノードにサイトが作成されます。

既存の階層をアップロードすることもできます。

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

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削減できます。

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 以降からサイト階層をエクスポートできます。

始める前に

- インベントリに シスコ ワイヤレス コントローラとアクセスポイントがあることを確認します。ない場合は、[Discovery] 機能を使用して検出します。
- 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 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します。Cisco Prime Infrastructure で、**[Inventory] > [Group Management] > [Network Device Groups]** の順に選択します。

ステップ 2 [Device Groups] ウィンドウで、[Export Groups] をクリックします。

ステップ 3 [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 4 Cisco Prime Infrastructure からマップをエクスポートします。これにより、フロア寸法などのマップ情報と Cisco Prime Infrastructure の各フロアに適用されている無線周波数 (RF) 減衰モデルなどのキャリブレーション情報がダウンロードされます。

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

ステップ 5 **[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。

[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 6** エクスポートする特定のサイト、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します。すべてのマップをエクスポートする場合は、[Select All] チェックボックスをオンにします。
- ステップ 7** [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。
- [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。
 - [Calibration Information] を選択すると、Cisco Prime Infrastructure の各フロアに適用されている RF 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 8** [マップアーカイブを生成 (Generate Map Archive)] をクリックします。
- 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 9** サイト階層を Cisco DNA Center にインポートするには、Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックして [Design] > [Network Hierarchy] の順に選択し、[Import] > [Import Sites] の順に選択します。
- 世界地図が右側のペインに表示されます。
- ステップ 10** [Import Sites] ウィンドウで、Cisco 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します。または、[Select CSV 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 Cisco 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 11** 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。[Design] > [Network Hierarchy] の順に選択し、[Import] > [Import Prime Maps] の順に選択します。
- ステップ 12** [Import Prime 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、[click to select] をクリックして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 13** [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。(Cisco Prime Infrastructure からのマップのエクスポートについては、[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、シスコ 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 GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Hierarchy] の順に選択し、[Import] > [Import Sites]を選択します。

世界地図が右側のペインに表示されます。

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、[Import] をクリックします。

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[Import] > [Map Import]を選択します。

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、[On] または [Off] 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、[On] または [Off] 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。

グローバルマップアーカイブのエクスポート

ネットワーク全体のグローバルな階層マップをエクスポートできます。階層マップからアーカイブファイルにダウンロードするサイト、ビルディング、フロアの階層を選択することもできます。マップアーカイブファイルには、日時、フロアの数、APなどのデータが格納されます。



(注) 最大 500 のフロアをエクスポートできます。

始める前に

次のタスクを実行するには、**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。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy] の順に選択します。

ステップ 2 ネットワーク全体のマップをエクスポートするには、[Export] > [Export Maps] の順に選択します。あるいは、左側のペインで目的のサイト、ビルディング、またはフロアの横にある歯車アイコンをクリックし、[Export Maps] を選択します。

- サイトを選択して [Export Maps] をクリックすると、すべてのサブサイト、ビルディング、およびフロアを含むサイトマップがエクスポートされます。
- ビルディングを選択して [Export Maps] をクリックすると、すべてのフロアを含むビルディングマップがエクスポートされます。
- フロアを選択して [Export Maps] をクリックすると、選択したフロアのフロアマップのみがエクスポートされます。

ステップ 3 [Export Maps Archive] ウィンドウで、次のいずれかを実行します。

- [File Name] フィールドにファイル名を入力し、[Export] をクリックして、[OK] をクリックします。
選択したマップのアーカイブファイルを含む新しい tar ファイルが作成されてコンピュータに保存されます。
- [File Name] フィールドに既存のファイル名を入力し、[Click to select] リンクをクリックしてコンピュータから既存のファイルを選択します。[OK] をクリックします。
マップが選択したファイルにアーカイブされてコンピュータに保存されます。

サイト階層のエクスポート

ダウンロードするサイトの完全な階層を CSV 形式のファイルにエクスポートできます。サイト階層ファイルには、サイト名、親階層、フロア数、場所、サイトアドレスなどの詳細が含まれています。

次の手順では、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。

始める前に

次のタスクを実行するには、**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。

-
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します **[Design] > [Network Hierarchy]**。
 - ステップ 2** サイト階層全体をエクスポートするには、**[Export] > [Export Sites]** の順に選択します。あるいは、[Global] の横にある [More] アイコンをクリックし、[Export Sites] を選択します。
 - ステップ 3** [Export Sites] ダイアログボックスで [OK] をクリックします。
サイト名、親階層、フロア数、場所、住所を含む完全なサイト階層ファイルが CSV 形式でエクスポートされ、コンピュータに保存されます。

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 GUIで[Menu]アイコン (☰) をクリックして選択します[Design]>[Network Hierarchy]。
 - 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 GUIで[Menu]アイコン (☰) をクリックして選択します[Design]>[Network Hierarchy]。
 - 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 GUIで[Menu]アイコン (☰) をクリックして選択します[Design]>[Network Hierarchy]。
世界地図が右側のペインに表示されます。
 - ステップ2 [Network Hierarchy] ウィンドウで、[+Add Site]>[Add Building] の順にクリックするか、左側のペインの親サイトの横にある歯車アイコン ⚙ をクリックして[Add Building] を選択します。
既存の階層をアップロードすることもできます。
 - ステップ3 [Building Name] フィールドに建物の名前を入力します。
建物名には、(、)、&、?、!、/、<、> を除く、すべての特殊文字を使用できます。
 - ステップ4 [Parent] ドロップダウンリストから、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 [Address] 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。ユーザーはマーカーを移動してマップ上の位置を変更できます。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 Cisco DNA Center GUI で [Menu] アイコン () をクリックして選択します **[Design] > [Network Hierarchy]**。

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 GUI で [Menu] アイコン () をクリックして選択します **[Design] > [Network Hierarchy]**。

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、[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 GUI で [Menu] アイコン () をクリックして選択します **[Design] > [Network Hierarchy]**。

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 [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。フロア名には最大 21 文字を使用できます。

フロア名には、&、>、<、?、!、/、[、] を除く、すべての特殊文字を使用できます。

フロア名は文字またはハイフン (-) で始め、最初の文字に続く文字列に、次の 1 つ以上の文字を含めることができます。

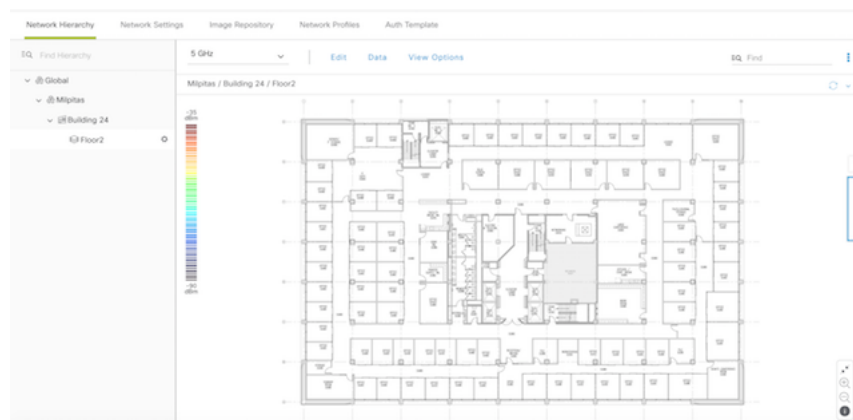
- 大文字または小文字、またはその両方
- 数字
- アンダースコア (_)
- ハイフン (-)
- ピリオド (.)
- スペース ()

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loor 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 [Overlay Visibility] を [ON] にしてください ([Floor] > [View Option] > [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loor プランの例



ステップ 7 [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 GUI で [Menu] アイコン (≡) をクリックして選択します [Design] > [Network Hierarchy]。

- 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ーリング

[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 [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。

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
- GPS 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 AP 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 AP 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する有益なデータが得られません。
- 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。
- フロアマップでのヒートマップの表示を最適化するには、AP の高さを約 10 フィート (3 m) 以下に設定します。

AP の追加、配置、および削除

Cisco DNA Center 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 Cisco DNA Center では、次の 802.11ax AP がサポートされています。

- Cisco Catalyst 9120 アクセス ポイント

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

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
- 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 [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** [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、[Add Selected] をクリックします。または、アクセスポイントの横にある [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。
 - [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。

- [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 Name] : AP 名が表示されます。
- [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] : マップの水平スパンを、選択した測定単位 (フィートまたはメートル) で示します。
- [y] : マップの垂直スパンを、選択した測定単位 (フィートまたはメートル) で示します。
- [AP Height] : アクセスポイントの高さを、選択した測定単位 (フィートまたはメートル) で示します。

アクセスポイントの無線ごと :

- [Protocol] : 無線のプロトコル (802.11a/n/ac、802.11b/g/n、または 802.11a/b/g/n) 。
- [Antenna] : 無線のアンテナタイプ。
 - (注) 内部無線には1つのアンテナタイプしかありませんが、複数の外部アンテナタイプから選択できます。
- [Antenna Image] : アンテナ画像 (内部アンテナの場合は AP 画像) を表示します。
- [Antenna Orientation] : [Azimuth] と [Elevation] の方向の度数を示します。
- [Azimuth] : x 軸に対して時計回りに測定されたアンテナの水平方向の角度 (方位角が 0 であることは、アンテナが右を向いていることを示します)。方位角の範囲は 0 - 360 です。
 - (注) ほとんどの指向性アンテナは方位角を向くことで最大ゲインに達しますが、一部のアンテナは方位角から 90 度離れた方向を向くことで最大ゲインに達します。このような場合、AP の方位角を 0 (右向き) に設定すると、生成されたヒートマップの最大ゲインは下向きになります。また、方位角を 270 (上向き) に設定すると、生成されたヒートマップの最大ゲインは右向きになります。
- [Elevation] : アンテナの垂直角度。壁面取り付けアンテナでは、仰角は水平軸に対して測定されます。したがって、45 度はアンテナが 45 度上を指していることを示し、-45 度はアンテナが 45

度下を指していることを意味します。天井取り付けアンテナでは、仰角は垂直軸に対して測定されます。したがって、45度はアンテナが方位角に向かって45度を指していることを示し、-45度はアンテナが反対方向に45度を指していることを意味します。仰角の範囲は-90～90度です。

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。

APの新しい位置に基づいてヒートマップが生成されます。

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 \(61 ページ\)](#)』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。

[Delete APs] ウィンドウが表示され、割り当てられて設定されたすべてのアクセスポイントが一覧表示されます。

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、[Select All] をクリックし、[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。
- [Quick Filter] を使用し、AP名、MACアドレス、モデル、コントローラ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。

Cisco Prime Infrastructure から一括 AP をエクスポートして Cisco DNA Center にインポートする

Cisco DNA Center では、アクセスポイントのコレクションをフロアマップにインポート、割り当て、および配置できます。Cisco Prime Infrastructure にアクセスポイントの既存のコレクションがある場合は、それを Cisco DNA Center にインポートすると、フロアマップへのアクセスポイントのインポート、割り当て、および配置に費やす時間と労力を節約できます。

この手順では、Cisco Prime Infrastructure からアクセスポイントの既存のコレクションをエクスポートして Cisco DNA Center にインポートする方法について説明します。

始める前に

- 次のタスクを実行するには、**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。
- インベントリに AP があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。

- フロアマップ上にAPを追加して配置します。
- サイト、ビルディング、およびフロアは、サイト階層に存在する必要があります。

ステップ1 一括AP位置をCSVファイルとしてCisco Prime Infrastructureからワークステーションにエクスポートします。

ステップ2 Cisco DNA Center GUIで[Menu]アイコン(☰)をクリックして選択します[Design]>[Network Hierarchy]。世界地図が右側のペインに表示されます。

ステップ3 一括APをインポートするには、左側のペインで目的のサイトを選択し、[Import]ドロップダウンリストから[Import Bulk AP]を選択するか、左側のペインで目的のサイトの横にある歯車アイコンをクリックし、[Import Bulk AP]を選択します。

ステップ4 [Import Bulk AP]ウィンドウで、APファイルをドラッグアンドドロップするか、[Choose a file]をクリックしてワークステーションからファイルを選択します。

- (注)
- Prime テンプレートを使用して [AP Positions] CSV ファイルを手動で作成するには、[Download Prime Template] をクリックして、Prime テンプレートをワークステーションにエクスポートします。Prime テンプレートは、ネストされたファイルをサポートしていません。
 - Cisco DNA テンプレートを使用して [AP Positions] CSV ファイルを手動で作成するには、[Download Template] をクリックして、Cisco DNA テンプレートをワークステーションにエクスポートします。Cisco DNA テンプレートは、ネストされたファイルをサポートしています。

CSVファイルがダウンロードされるまで待ちます。CSVファイルには、ネットワーク内のさまざまなサイトのAP位置に関する情報が含まれています。

ステップ5 [Import] をクリックします。

[Import Summary] ウィンドウが表示されます。

- [Information] タブに、正常にインポートされたAPのリストが表示されます。
- [Warning] タブをクリックすると、警告のリストが表示されます。
- [Error] タブをクリックすると、エラーのリストが表示されます。

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 のチャンネル番号。
 - [Antenna] : アンテナ名。
 - [Azimuth] : アンテナの方向。
- [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 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。



(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 Aironet 1800s アクティブ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。

センサーデバイスは AP 1800s センサー専用です。Cisco Aironet 1800s アクティブセンサーは、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ー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ーと直接通信します。

- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
- 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。[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 GUIで[Menu]アイコン (☰) をクリックして選択します[Design]>[Network Hierarchy]。
- 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 [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** カバレッジエリアを削除するには、[Overlays] パネルの [Coverage Areas] の隣で [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** カバレッジ領域にカーソルを合わせ、[delete] をクリックします。
- 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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
- 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 [Edit] をクリックします。

- ステップ 4** [Obstacles] の横にある [Overlays] パネルで、[Add] をクリックします。
- ステップ 5** [Obstacle Creation] ダイアログ ボックスで、[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、[Thick Wall]、[Light Wall]、[Heavy Door]、[Light Door]、[Cubicle]、および [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** [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** エリアの輪郭を描画したら、そのエリアをダブルクリックして強調表示します。
- ステップ 10** [Obstacle Creation] ウィンドウで [Done] をクリックします。
- ステップ 11** [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、[Obstacles] の隣にある [Overlays] パネルで、[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、[Save] をクリックします。
- ステップ 14** 障害を削除するには、[Obstacles] の隣にある [Overlays] パネルで、[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** [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たびに、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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
- ステップ 2** 左ペインで、フロアを選択します。
- ステップ 3** [Overlays] パネルで、[Location Regions] の横にある [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** [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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
- 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 [Edit] をクリックします。
- ステップ 4** [Overlays] パネルで、[Location Regions] の横にある [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** [Overlays] パネルで、[Location Regions] の横にある [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、[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** [Overlays] パネルで、[Location Regions] の横にある [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、[Delete] をクリックします。
- ステップ 3** [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（ユーザー定義）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）からモニターされる距離を表します。

-
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
- 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 [Edit] をクリックします。
- ステップ 4** [Rails] の横にある [Overlays] パネルで、[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、[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** [Overlays] パネルで、[Rails] の横にある [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、[Save] をクリックします。
- ステップ 11** [Overlays] パネルで、[Rails] の横にある [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、[Delete] をクリックします。
- ステップ 13** [Save] をクリックします。
-

マーカーの配置

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
- 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 [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] 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、[Delete] をクリックします。

ステップ 12 [Save] をクリックします。

GPS マーカーの追加

クライアントの位置の精度を高めるために、Cisco DNA Center の GPS マーカーを使用して、世界地図上で建物の実際の位置を見つけることができます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。

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 [Edit] をクリックします。

ステップ 4 [Overlays] パネルで、[GPS Markers] の横にある [Add] をクリックします。

ロケーションアイコンが表示されます。

ステップ 5 フロアマップでロケーションアイコンを見つけます。

(注) • GPS マーカーは、相互に最小しきい値距離の 25 フィート (約 7.5 m) 以上離して配置する必要があります。

• GPS マーカーは、一直線に配置しないでください。

フロアマップ上の GPS マーカーの物理アドレス、緯度、および経度の座標を指定するための [Place Marker] ダイアログボックスが表示されます。

ステップ 6 [GPS マーカーの追加 (Add GPS Marker)] をクリックします。

(注) 少なくとも 3 つの GPS マーカーを多角形状でフロアマップに追加する必要があります。

ステップ 7 [保存 (Save)] をクリックします。

(注) GPS マーカーは、ビルディングの属性であり、ビルディングのすべてのフロアに適用できます。

GPS マーカーの編集

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。

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 [Edit] をクリックします。

ステップ 4 [Overlays] パネルで、[GPS Markers] の横にある [Edit] をクリックします。

ステップ 5 編集するマップ上の GPS マーカーをクリックします。

フロアマップ上の GPS マーカーの物理アドレス、緯度、および経度の座標を変更するための [Place Marker] ダイアログボックスが表示されます。

ステップ 6 [Edit GPS Marker] をクリックします。

ステップ 7 [Save] をクリックします。

GPS マーカーの削除

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。

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 [Edit] をクリックします。

ステップ 4 [Overlays] パネルで、[GPS Markers] の横にある [Delete] をクリックします。

ステップ 5 削除するマップ上の GPS マーカーをクリックします。

ステップ 6 [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 [View Options] をクリックします。フロアマップと [Access Points]、[Sensor]、[Overlay Objects]、[Map Properties]、および [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、[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

アクセスポイントをマップ上に表示するには、[Access Points] の横にある [On/Off] ボタンをクリックします。[Access Points] 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、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。
 - [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。
 - [Name] : AP 名。
 - [AP MAC Address] : AP の MAC アドレス。
 - [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。

- [Radio MAC Address] : 無線 MAC アドレス。
- **IP Address**
- [Channel] : Cisco Radio のチャンネル番号または [Unavailable] (アクセスポイントが接続されていない場合)。
- [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。
- [TX Power] : 現在の Cisco Radio の送信電力レベル (1 が高い) または [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。Cisco Aironet 1000 シリーズ Lightweight アクセスポイントは **1 ~ 5** の値を受け入れます。Cisco Aironet 1230AG シリーズアクセスポイントは **1 ~ 7** の値を受け入れます。Cisco Aironet 1240AG シリーズアクセスポイントおよび Cisco Aironet 1100 シリーズアクセスポイントは **1 ~ 8** の値を受け入れます。
- [Channel and Tx Power] : チャンネルと送信電力レベルまたは [Unavailable] (アクセスポイントが接続されていない場合)。
- [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、およびチャンネル使用率を含む)。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。
- [Tx Utilization] : 指定されたインターフェイスの送信 (Tx) 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。
- [Ch Utilization] : 指定されたアクセスポイントのチャンネル使用率。
- 関連付けられた **Clients** : 関連付けられたクライアントの総数。
- [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。
- [Health Score] : AP の正常性スコア。
- **問題数**
- **カバレッジの問題**
- **APダウンの問題**
- [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。[Heatmap

Type] ドロップダウンリストからヒートマップのタイプを選択してください。ヒートマップのタイプは次のとおりです。

- [None]
- [APRSSI] : 特定の帯域のワイヤレス信号の強度を特定するカバレッジヒートマップ。
 - [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。
 - [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。
 - [Heatmap Color Scheme] : 緑色はヒートマップカバレッジ状態が良好であることを示し、赤色はヒートマップカバレッジ状態が悪いことを示します。
- [Client Density] : 関連付けられたクライアントの密度。
 - [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。
- [IDS] : ワイヤレスクライアントに提供されるモニターモードアクセスポイントカバレッジをフロアマップ上に示すヒートマップ。
- [Planned Heatmap] : 計画ヒートマップは、フロアマップ上の計画アクセスポイントの可能なカバレッジを示す架空のヒートマップです。
- [Coverage] : モニターモードアクセスポイントが除外されたヒートマップ (モニターモードアクセスポイントがフロアプラン上にある場合にのみ利用可能) 。

APの詳細はすぐにマップに反映されます。マップ上のAPアイコンにカーソルを合わせると、APの詳細、RXネイバーの詳細、クライアントの詳細、およびスイッチの情報が表示されます。

センサーオプションの表示

[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。[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

オーバーレイオブジェクト をこれらの設定を構成するパネルに展開します。[On]/[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]

スイッチの表示オプション

スイッチの横にある [On]/[Off] ボタンをクリックすると、そのスイッチで使用できる AP のリストがマップ上に表示されます。

[Switch] パネルを展開して、表示ラベルの設定を行います。

- [Display Label] : ドロップダウンリストから、選択したスイッチの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
 - 名前
 - スイッチMACアドレス
 - AP 数
 - クライアント数
 - SSID の数

選択したスイッチの AP の詳細がマップにすぐに反映されます。マップでスイッチのアイコンにカーソルを合わせると、スイッチの詳細が表示されます。

スイッチ名をクリックすると、次の詳細が表示されます。

- スイッチ MAS アドレス
- AP 数
- クライアント数
- SSID の数
- ヒートマップ : 対応するオプションボタンをクリックして、すべての AP、特定のスイッチに属する AP、または他のスイッチに属する AP のヒートマップを表示できます。
- 所有している AP : このスイッチに属する AP のリストが表示されます。

マッププロパティの設定

[Map Properties] パネルを展開して、以下を構成します。

- [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。[Auto Refresh] ドロップダウンリストから、時間間隔 ([None]、[1 min]、[2 mins]、[5 mins]、または [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

[Global Map Properties] パネルを展開し、次のように設定します。

- [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 [Feet] または [Meters] のいずれかに設定します。

フロアマップでのワイヤレス干渉源の特定

Cisco DNA Center は、干渉を検出し、フロアマップ上の特定の帯域に対する干渉源を無効にします。2.4GHz帯域に干渉があると、802.11 ワイヤレスネットワークのネットワークトラフィックが中断します。

Cisco DNA Center は、干渉源の場所、影響範囲、および強度を特定します。

この手順では、フロアマップ上のネットワーク干渉源を特定する方法を示します。

始める前に

Cisco Connected Mobile Experiences (CMX) または Cisco DNA Spaces が Cisco DNA Center と同期されていることを確認します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します **[Design] > [Network Hierarchy]**。

世界地図が右側のペインに表示されます。

左側のペインで、干渉源を特定するフロアに移動します。

ステップ 2 サイト階層ペインで、フロアの横にある歯車アイコンをクリックし、[Sync: DNA Spaces/CMX] を選択して、[DNA Spaces] または [CMX] をフロアと同期します。

(注) (オプション) 世界地図で、フロアにカーソルを合わせ、[Sync: DNA Spaces/CMX] を選択して、[DNA Spaces] または [CMX] をフロアと同期します。

ステップ 3 [Network Hierarchy] ウィンドウで、[View Options] をクリックします。

ステップ 4 [View Options] ウィンドウで下にスクロールし、[Interferers] の横にある [On/Off] トグルボタンをクリックして、フロアマップに干渉源を表示します。

ステップ 5 [Interferers] を展開し、[Show Zone of Impact] の横にある [On/Off] トグルボタンをクリックして、干渉の影響ゾーンをフロアマップに表示します。

(注) デフォルトでは、[Zone of Impact] はオフになっています。

ステップ 6 世界地図で、干渉源にカーソルを合わせ、影響を受けるチャンネルをクリックして干渉源デバイスの詳細を表示します。

[Interferer] ウィンドウには、特定された干渉源の次の属性が表示されます。

- タイプ
- 状態
- 名前
- CMX または Cisco DNA Spaces によってレポートされた干渉源
- MAC アドレス
- AP の検出
- デューティサイクル
- 影響を受けるチャンネル
- 影響ゾーン
- First detected
- 最後のレポート

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せん。

クライアントデータのフィルタ処理

-
- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。
 - ステップ 2 左側のペインで、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 [Data] をクリックします。
 - ステップ 4 [Filters] パネルで、[Clients] をクリックします。
 - ステップ 5 [+] アイコンをクリックしてルールを追加します。
 - ステップ 6 [Filtering Criteria] ドロップダウンリストから、マップに表示するクライアント ID を選択します。
 - ステップ 7 選択したクライアント ID の各パラメータを選択します。
 - ステップ 8 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ます。
 - ステップ 9 [Apply Filters to List] をクリックして、マップ上の次のフィルタ結果に基づいてクライアントリストを絞り込みます。[User Name]、[Average Health Score]、[Issues Count]、[IP Address]、[MAC Address]、[Status]、[Band]、[SSID]、[Vendor]、[AP Name]、[Operating System]、[Average RSSI (dBm)]、[Average SNR (dB)]、および [Average Data Rate]。

検索結果が表形式で表示されます。

ステップ 10 マップ上で特定のセンサーを表示するには、テーブル内でクライアントの横にある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。

(注) テーブル内の検索結果の上にカーソルを合わせると、実線と点線が表示されます。

- 実線は、マップ上のクライアントの場所を示します。
- 点線は、マップ上のアクセスポイントとクライアントの関連付けを示します。

Ekahau プロジェクトファイルを使用したフロアマップの作成

始める前に

Ekahau Pro ツールを使用すると、フロアレイアウト、AP の場所、障害物など、企業の完全なネットワーク計画を作成できます。フロアレイアウトを作成した後、シミュレートされたネットワーク計画と実際のサイト調査データを、Cisco DNA Center が使用可能な形式にエクスポートできます。Ekahau プロジェクトファイルを Cisco DNA Center にインポートして、さらに計画を立てることができます。

Ekahau Pro ツールバージョン 10.2 では、サイト階層を自動的に作成し、それをプロジェクトファイルとして保存して、Cisco DNA Center にインポートできます。



(注) Ekahau プロジェクトは予測モードでのみサポートされ、設計モードではサポートされません。

ステップ 1 Ekahau Pro ツールでフロアレイアウトを計画します。

- ビルディングとフロアを作成します。
- フロアプランをインポートします。
- 計画された AP または仮定の AP を追加します。
- ビルディングの座標を追加します。
- サイト名を定義します。

ここで指定した AP 名は、ワイヤレスコントローラの設定中に、シスコワイヤレスコントローラの AP 名を更新するために使用されます。

- 障害物を追加します。
- プロジェクトを PDF としてエクスポートします。

ステップ 2 フロアレイアウトで設計された場所に計画された AP を展開します。

- 物理 AP は、フロアレイアウトで指定された設計済みの場所に取り付けられます。計画された AP の MAC アドレスが、物理 AP の MAC アドレスで更新されます。
- 物理 AP は、目的のワイヤレスコントローラの VLAN に接続されています。

ステップ 3 シスコワイヤレスコントローラを設定します。

- 検出されたワイヤレスコントローラと AP が [Inventory] ウィンドウにリストされるように、**検出**ジョブを実行して、ネットワーク内のシスコワイヤレスコントローラと AP を検出します。
- フロアプランニング中に Ekahau Pro プロジェクトで指定された AP 名を使用して、ワイヤレスコントローラの AP 名を更新します。

ステップ 4 Ekahau プロジェクトを Cisco DNA Center にインポートします。

ステップ 5 計画された AP を Cisco DNA Center の実際 AP にマッピングします。

Cisco DNA Center への Ekahau プロジェクトのインポート

ステップ 1 サイト、ビルディング、フロアなどのネットワーク階層を設計します。

詳細については、[ネットワーク階層のサイトの作成 \(3 ページ\)](#)、[ビルディングの追加 \(9 ページ\)](#)、および[ビルディングへのフロアの追加 \(10 ページ\)](#) を参照してください。

フロアを追加する際には、必ず、Ekahau プロジェクトで指定されたものと同じ名前でフロアを作成してください。

ステップ 2 左側のペインで、Ekahau プロジェクトをインポート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、[Import Ekahau Project] をクリックします。

[Import Ekahau Project] ダイアログボックスが表示されます。

ステップ 4 [Import Ekahau Project] ダイアログボックスのボックスエリアに .esx ファイルをドラッグアンドドロップするか、または [click to select] リンクをクリックして .esx ファイルを参照します。

インポートが成功すると、各計画された AP は、AP 名を使用してインベントリ内の既存の実際 AP にマッピングされます。計画された AP は、フロアマップ上にアイコン [P] とともに表示されます。たとえば、計画済みの AP の名前が SJC01-02-AP-B-1 の場合、インポートプロセスでは同じ名前実際の AP が検索されます。

ステップ 5 インベントリで AP が見つからず、マッピングが解除されたままの場合、計画された AP はフロア上に保持されます。

不一致の理由を表示するには、フロアマップ上の計画された AP アイコンの上にカーソルを置いて、[Import History] をクリックします。

次の試行は、計画された AP を実際の AP にマッピングするために行われます。

- 新たに検出された AP が計画された AP と一致する場合、計画された AP は検出された実際の AP で置き換えられます。
- 計画された AP がマッピング解除されたままの場合は、計画された AP を実際の AP で手動で置き換えて、失敗の原因を示すことができます。

ステップ 6 実際の AP に計画された AP を手動で割り当てるには、フロアマップ上の計画された AP アイコンの上にカーソルを合わせて、[Assign] > [Assign] > をクリックします。

[Assign Planned APs] パネルが表示されます。

ステップ 7 [Assign Planned APs] パネルで、AP 名、AP タイプ、またはすべての AP によって計画された AP を実際の AP にマッピングします。

ステップ 8 AP 名の横にあるオプションボタンを選択し、[Assign] をクリックして、計画済みの AP を手動で割り当てます。

ステップ 9 [Save] をクリックします。

Cisco DNA Center からの Ekahau プロジェクトのエクスポート

事前設定済み作業フロアを拡張するために、Cisco DNA Center では、Cisco DNA Center から作業フロアを Ekahau プロジェクトとしてエクスポートし、プロジェクトを Ekahau Pro ツールにインポートできます。

始める前に

Ekahau Pro ツールのバージョン 10.2.0 が必要です。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。世界地図が右側のペインに表示されます。

ステップ 2 左側のペインで、目的のサイト、建物、またはフロアを選択します。

ステップ 3 サイトまたは建物の Ekahau プロジェクトをエクスポートするには、[Export] ドロップダウンリストから [Export Maps] を選択するか、左側のペインで目的のサイトまたは建物の横にある歯車アイコンをクリックして [Export Maps] を選択します。

フロアマップの Ekahau プロジェクトをエクスポートするには、左側のペインで、目的のフロアの横にある歯車アイコンをクリックし、[Export Maps] を選択します。

[Information] ダイアログボックスが表示されます。

ステップ 4 [Information] ダイアログボックスで、[Ekahau Project] エクスポート形式を選択します。

ステップ5 [Yes] をクリックします。

ESX 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6 ESX ファイルを Ekahau Pro ツールにインポートし、フロアを拡張して、ファイルを保存します。

ステップ7 Ekahau プロジェクトをサイトの下の Cisco DNA Center にインポートします。詳細については、「[Cisco DNA Center への Ekahau プロジェクトのインポート](#)」を参照してください。

インタラクティブフロアプランニングについて

インタラクティブプランニングは、計画された AP または仮想 AP や障害物をラスターイメージや CAD フロアプランで描画することによって、フロアレイアウトのプランを支援します。フロアマップを PDF としてエクスポートして、AP を設置している技術者と共有できます。フロアの描画は、技術者がフロアのレイアウトと正確な AP の設置場所を可視化するのに役に立ちます。

インタラクティブフロアプランニングにより、次のことが可能になります。

- キャンバスとしてラスターまたは CAD フロアプランを使用してフロアレイアウトを作成する。
- 信号カバレッジ要件に基づいて、計画された AP または仮想 AP をフロアマップに配置する。これらの仮想 AP または計画された AP は、Cisco DNA Center によってまだインストールまたは検出されていません。
- アンテナのタイプと方向を割り当てる。
- フロアに障害物を描画する。
- すべての AP を順番に計画する。
- フロアマップを PDF としてエクスポートする。

インタラクティブフロアプランニング

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Hierarchy]。

ステップ2 サイト、ビルディング、フロアなどのネットワーク階層を設計します。


ステップ3 左側のメニューで、フロアを選択します。

選択したフロアに計画された AP と障害物を描画できます。

ステップ4 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5 [Floor Elements] パネルで、[Planned Access Points] の横にある [Add] をクリックします。

[Add Planned AP] ウィンドウが表示されます。

- ステップ 6** [AP Name] テキストボックスに、計画された AP の名前を入力します。
- ステップ 7** (オプション) [MAC Address] テキストボックスに、計画された AP の MAC アドレスを入力します。
- ステップ 8** [AP Model] ドロップダウンリストから、AP モデルを選択します。
- ステップ 9** [x] および [y] テキストボックスには、マップの水平方向スパンと垂直方向スパンをフィート単位で入力します。
- ステップ 10** [Ap Height] テキストボックスに、AP の高さを入力します。
- ステップ 11** [Radio band] タブをクリックして、アンテナタイプ、方位角、および垂直面の方向を設定します。
- ステップ 12** [Antenna] ドロップダウンリストから、この AP の適切なアンテナタイプを選択します。
アンテナイメージは、選択されたアンテナを反映しています。
- ステップ 13** アンテナタイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。
- ステップ 14** [Save] をクリックします。
新しく追加された計画された AP がフロアマップに表示されます。
- ステップ 15** 水平方向と垂直方向のスパン（つまり、x 座標と y 座標）を指定していない場合、計画された AP はフロアマップの右上隅に表示されます。
- ステップ 16** マップ上の適切な場所にドラッグアンドドロップして、計画された AP をマップに正しく配置します。
- ステップ 17** [Save] をクリックします。
- ステップ 18** 計画可能な次の AP は、フロアマップの右上隅に表示されます。
- ステップ 19** 次の AP を計画するには、ステップ 6 ~ 14 を繰り返します。
- ステップ 20** 障害物を描画するには、[Overlays] パネルで [Obstacles] の横にある [Add] をクリックします。
詳細については、「[障害物の作成 \(20 ページ\)](#)」を参照してください。
- ステップ 21** フロアプランを PDF としてエクスポートするには、[Network Hierarchy] ウィンドウの右上隅にある  アイコンをクリックし、[Export] を選択します。
- ステップ 22** [Export] ウィンドウで PDF としてエクスポートするには、[PDF] チェックボックスをオンにします。
- ステップ 23** [エクスポート (Export)] をクリックします。
ODF が作成され、ローカルマシンにダウンロードされます。PDF には、設定した計画された AP の詳細とともにフロアマップが含まれています。計画された AP は、AP モデルに基づいて一覧表示されます。

AP モデルカタログを使用したフロアマップへの計画済みアクセスポイントの配置

AP モデルカタログ機能を使用すると、フロア上の 1 つの AP を AP モデル、アンテナタイプ、方位角、および垂直面の方向で設定し、同じモデルタイプに属する残りの AP にその構成を複製できます。

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン () をクリックして選択します [Design] > [Network Hierarchy]。

- ステップ 2** サイト、ビルディング、フロアなどのネットワーク階層を設計します。
- ステップ 3** 左側のメニューで、フロアを選択します。
選択したフロアに計画された AP と障害物を描画できます。
- ステップ 4** 中央のペインのフロアプランの上にある [Unlock Floor] アイコン (🔒) をクリックします。
特定のフロアで使用可能な AP モデルのリストが、フロアマップの左側に表示されます。
- ステップ 5** 新しい AP モデルをフロアに追加するには、[Add model] をクリックします。
[Select AP models to add] ダイアログボックスが表示されます。
- ステップ 6** [Select AP models to add] ドロップダウンリストから、AP モデルを選択し、[Add AP models] をクリックします。
新しい AP モデルがフロアに追加されます。
- ステップ 7** AP モデルを削除するには、AP モデル名の上にある [X] をクリックします。
AP モデルを削除できるのは、そのモデルタイプの AP がフロアマップに追加されていない場合のみです。
- ステップ 8** 計画済み AP をフロアマップに追加するには、AP モデルをクリックして選択し、カーソルをフロアマップ上の適切な場所に移動してから、もう一度クリックします。
選択したモデルの計画済み AP がフロアマップに追加され、右側に [Edit Planned AP] ペインが表示されます。このペインには、デフォルトで AP 名が追加されます。
- ステップ 9** [Edit Planned AP] ペインで、[AP Name] フィールドの横にある歯車アイコンをクリックします。
[Name pattern] ダイアログボックスが表示されます。
- ステップ 10** 最初の AP をフロアに追加するときは、SJC-BLD21-FL2-AP ##### などの有効な名前パターンを入力してから、[Set name pattern] をクリックするようにしてください。
(注) 計画済み AP は Cisco DNA Center 内で一意である必要があるため、名前パターンでフロアを識別できるようにします。
名前パターンの ##### は、[AP Name] の番号に置き換えられます (SJC-BLD21-FL2-AP0001 や SJC-BLD21-FL2-AP0002 など)。
- ステップ 11** [Edit Planned AP] ペインの [Antenna] ドロップダウンリストから、AP の各無線スロットに適切なアンテナタイプを選択します。
アンテナイメージは、選択されたアンテナを反映しています。
- ステップ 12** アンテナタイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。
- ステップ 13** 作成した AP と同じ AP プロパティを持つ別の AP を追加するには、その新しい AP を配置するフロアマップ内の場所をクリックします。
BLD1-AP0002-TX のように、新しい AP がマップに表示されます。すべてのプロパティが継承され、AP 名が付加されています。

- ステップ 14 同じプロパティを持ち、AP 名が付加された AP をさらに追加するには、フロアマップをクリックします。
- ステップ 15 フロアマップへの AP の追加を止めるには、**Esc** を押すか、フロアマップを右クリックします。
- ステップ 16 AP を配置するには、AP をフロアマップ内の適切な場所にドラッグアンドドロップします。
- ステップ 17 [Save] をクリックして変更を保存するか、[X] をクリックして変更を破棄します。
- ステップ 18 計画済み AP を削除するには、フロアマップ上の AP 名を右クリックし、[Delete] をクリックします。
- ステップ 19 計画済み AP を編集するには、フロアマップ上の AP 名を右クリックし、[Edit] をクリックします。
- [Edit Planned AP] ウィンドウが表示されます。[Edit Planned AP] ウィンドウで変更を行い、[Save] をクリックします。
- ステップ 20 詳細を表示するには、フロアマップ上の AP 名を右クリックし、[View Details] をクリックします。

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、Cisco Aironet 1800s アクティブ 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) 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 GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] を選択し、[Wireless] タブをクリックします。
- ステップ 2 [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 3 [Basic Settings] の手順を完了します。
- a) [Wireless Network Name (SSID)] フィールドに、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。

(注) SSID 名には、最大 32 文字の英数字と先頭のスペースを含めることができます。<./.* を除くすべての特殊文字を使用できます（末尾のスペースは不可）。

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。

b) [Wireless Option] で、ワイヤレス帯域設定を選択します。

- [Dual band operation (2.4 GHz and 5 GHz)] : WLAN は 2.4 GHz 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。
- [Dual band operation with band select] : WLAN が 2.4 GHz および 5 GHz 用に作成され、バンドセレクトが有効になります。
- [5 GHz only] : WLAN が 5 GHz 用に作成され、バンドセレクトが無効になります。
- [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。

c) [Type of Enterprise Network] で、ワイヤレスネットワークでの Quality of Service (QoS) のプロビジョニング方法を選択します。

- [Voice and Data] : QoS が音声およびデータトラフィックに対して最適化されます。
- [Data Only] : QoS 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。

d) [SSID STATE] で、次の設定をカスタマイズします。

- [Admin Status] : 管理ステータスを有効または無効にするには、このトグルを使用します。
- [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、このトグルを使用します。

e) [Next] をクリックします。

ステップ 4 [Security Settings] の手順を完了します。

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。

- [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タイプを設定できます。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。

(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。

- [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タイプを設定できます。[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間のペアワイズマスターキー (PMK) として使用されます。

(注) WPA3-Personal 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 \(44 ページ\)](#) を参照してください。

- [Open Secured] : [Assign Open SSID] ドロップダウンリストから、クライアントをリダイレクトしてセキュアな SSID を開くためのオープン SSID を選択します。オープンでセキュアなポリシーは、最小限のセキュリティを提供します。
- [Open] : 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接続できます。

b) [Authentication, Authorization, and Accounting Configuration] で、AAA 関連設定を指定します。

- [Configure AAA] で、 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、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](#)」を参照してください。
- [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 enhanced Quality of Service (QoS) を受信するように IOS デバイスを設定できます。
- [Identity PSK] : 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。
- [Deny LLA Clients] : ランダム 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。

c) [Next] をクリックします。

ステップ 5 [Advance Settings] の手順を完了します。

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] 設定を選択します。

(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、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] オプションボタンが選択されています。[Required] オプションボタンをクリックすると、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。

c) [11K] で、次の設定を指定します。

• [Neighbor List] : 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するには、このチェックボックスをオンにします。

(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。同じ WLAN にあるネイバー AP の Wi-Fi チャン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。

• [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。セッションタイムアウトの範囲は 300 ~ 86400 秒です。

• [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。範囲は 0 ~ 2147483647 秒です。

d) [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関連付け解除しないタイムフレームです。

• [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、バッテリーの電力が節約されます。

e) [Next] をクリックします。

ステップ 6 [Associate SSID to Profile] の手順を完了します。


a) [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。


- [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。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、次を選択します。

- [Interface] : [Interface Management] ドロップダウンリストをクリックして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をクリックして 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。
- [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 をアダプ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。

(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。

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

ステップ 7 [Summary] ステップを確認し、必要に応じてステップの [Edit] をクリックして、変更を行うステップに戻ります。

ステップ 8 SSID 設定が完了した場合は、[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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [Wireless] の順に選択します。

ステップ 2 左側のメニューで、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 の新しいパスワードを入力します。

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 はグローバルパスワード値にリセットされます。

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

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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [Wireless] の順に選択します。

ステップ 2 [Enterprise Wireless] 領域の [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。

[Configure AAA Server for SSID] ウィンドウが表示されます。

ステップ 3 [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] 機能は、Mobility Express (ME) および Evolved Converged Access (ECA) デバイスではサポートされていません。

ステップ 4 [+] をクリックして、追加のサーバーを追加します。

(注) 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 5 [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 6 (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 7 [構成] をクリックします。


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。「[デバイスのプロビジョニング](#)」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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Settings] > [Wireless] の順に選択します。

ステップ 2  Create の下で、[Guest] をクリックして、新しい SSID を作成します。

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

ステップ 3 [Wireless Network Name (SSID)] フィールドに、作成するゲスト SSID の一意の名前を入力します。

SSID 名には、最大 32 文字の英数字と先頭のスペースを含めることができます。</.* を除くすべての特殊文字を使用できます (末尾のスペースは不可)。

. 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** [Type of Enterprise Network] の下で、[Voice and Data] または [Data Only] をクリックします。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、サービス品質が音声およびデータトラフィック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 5** 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。
- [Dual band operation (2.4 GHz and 5 GHz)] : WLAN は 2.4 GHz 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。
 - [Dual band operation with band select] : WLAN が 2.4 GHz および 5 GHz 用に作成され、バンドセレクトが有効になります。
 - [5 GHz only] : WLAN が 5 GHz 用に作成され、バンドセレクトが無効になります。
 - [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 6** [SSID STATE] で、次のように設定します。
- [Admin Status] ボタンをオフにして、管理ステータスを無効にします。
 - 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 7** [Level Of Security] の下で、レイヤ 2 およびレイヤ 3 セキュリティポリシーを設定します。
- ステップ 8** [L2 Security] の下で、このネットワークの暗号化および認証タイプを設定します。
- ステップ 9** [Enterprise]、[Personal]、[Open Secured]、[Open] のいずれかのオプションボタンをクリックして、対応するセキュリティ認証を設定します。
- [Enterprise] : **WPA2** と **WPA3** の両方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。
- 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。
- [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。
- 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。

- [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。

- [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。

ステップ 10 [L3 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 [Web Policy] と [Open] から選択します。

ステップ 11 オープンなポリシー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 12 [Web Policy] を選択した場合、認証サーバーを [ISE Authentication]、[Web Authentication]、または [Web Passthrough] として設定する必要があります。

[Web Policy] の暗号化と認証タイプは、レイヤ 3 のセキュリティを強化します。

- 外部 Web 認証 (EWA) では、セキュリティレベルとして [L3 Security] の下の [Web Policy] オプションボタンをクリックし、認証サーバーとして [Authentication] ドロップダウンリストから [Web Authentication External] をクリックします。
- 中央 Web 認証 (CWA) では、セキュリティレベルとして [L3 Security] の下の [Web Policy] をクリックし、認証サーバーとして [Authentication] ドロップダウンリストから [ISE Authentication] をクリックします。

ステップ 13 [Authentication Server] で、SSID の認証サーバーを設定できます。

ステップ 14 [ISE Authentication] 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から、作成するポータルタイプを選択します。

- [SelfRegistered] : 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。

[WHERE WILL YOUR GUESTS REDIRECT AFTER SUCCESSFUL AUTHENTICATION ?] ドロップダウンリストから、認証の成功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。

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 15 [Web Authentication] または [Web Passthrough] を選択した場合は、認証タイプとして [Internal] または [External] を設定します。

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 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に、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参照できます。

- [Authentication Server] ドロップダウンリストから [Web Authentication Internal] または [Web Passthrough Internal] を選択した場合、ページはシスコ ワイヤレス コントローラによって再構築されます。
- [Authentication Server] ドロップダウンリストから [Web Authentication External] または [Web Passthrough External] を選択した場合、クライアントは指定した 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 を入力する必要があります。

ステップ 16 [TIMEOUT SETTINGS FOR SLEEPING CLIENTS] の下で、スリープ状態のクライアントの認証を設定します。[Always authenticate] または [Authenticate after] を選択できます。

Web 認証に成功したゲストアクセスを持つクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効範囲は 10 ~ 43200 分、デフォルトは 720 分です。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、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。

- スリープ状態のクライアントの認証を有効にするには、[Always authenticate] オプションボタンをクリックします。
- [Authenticate after] オプションボタンをクリックし、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。有効な範囲は 10 ~ 43200 分、デフォルト期間は 720 分です。

ステップ 17 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 18 [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。

802.11r を使用すると、ワイヤレスクライアントがある 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。

ステップ 19 分散システム経路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。このオプションは、[Fast Transition (802.11r)] が [Adaptive] または [Enable] モードの場合のみ指定できます。

デフォルトでは、[Over the DS] チェックボックスが有効になっています。

- ステップ 20** [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。同じ WLAN にあるネイバー AP の Wi-Fi チャン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 21** [Client Exclusion] チェックボックスをオンにして、[in (secs)] フィールドに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 22** [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 23** 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) 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。
- ステップ 24** [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 チャン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 25** [11v BSS Transition Support] で、次のように設定します。
- ステップ 26** [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 27 [Client User Idle Timeout] チェックボックスをオンにして、[Client User Idle Timeout] フィールドに WLAN のユーザーアイドルタイムアウトの設定値を入力します。

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 秒のユーザーアイドルタイムアウト付きで有効になります。

ステップ 28 [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、バッテリーの電力が節約されます。

ステップ 29 [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 サーバーを追加し、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](#)」を参照してください。

ステップ 30 [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 31 既存のワイヤレスプロファイルがない場合は、[Wireless Profiles] ウィンドウで [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 32 [Wireless Profile Name] フィールドにプロファイル名を入力します。

ステップ 33 [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 34 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 SSID をゲストアンカーにするには、[Yes] をクリックします。

ステップ 35 [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 36 [No] をクリックした場合は、[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。

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。

ステップ 37 [Local to VLAN] フィールドに VLAN ID の値を入力します。

ステップ 38 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 39 [Sites] ウィンドウで、このプロファイルを関連付けるサイトの横にあるチェックボックスをオンにして、[OK] をクリックします。

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 40 [+ Add Model Config] をクリックして、モデル設定設計をワイヤレスプロファイルに関連付けます。

[Add Model Config] ウィンドウが表示されます。

ステップ 41 [Device Type(s)] ドロップダウンリストから、デバイスタイプを選択します。

[Search...] フィールドに名前を入力してデバイス名を検索するか、または [Wireless Controller] を展開してデバイスタイプを選択できます。

ステップ 42 [APPLICABILITY] の [Tags] ドロップダウンリストから、該当するタグを選択します。

ステップ 43 [Add] をクリックします。

ステップ 44 [Save] 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 45 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 46 [Portal Customization] ウィンドウで [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 47 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 48 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] ページの変数は次のとおりです。

- Access Code
- Header Text
- AUP
- Text Field

• [Registration] ページの変数は次のとおりです。

- [名 (First Name)]
 - 姓 (Last Name)
 - Phone Number
 - 会社 (Company)
 - SMS プロバイダ (SMS Provider)
 - Person being visited
 - Reason for a visit
 - Header text
 - [User Name]
 - 電子メール アドレス (Email Address)
 - AUP
- [Registration Success] ページの変数は次のとおりです。
- Account Created
 - Header texts
- [成功 (Success)] ページの変数：テキストフィールドです。

- ステップ 49** 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 50** 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 51** [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 52** [Portals] の下で、[Portal Name] の横にあるオプション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 53** [完了 (Finish)] をクリックします。

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

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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Settings] > [Wireless] の順に選択します。

ステップ 2 [Guest Wireless] 領域の [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。

[Configure AAA Server for SSID] ウィンドウが表示されます。

ステップ 3 [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] 機能は、Mobility Express (ME) および Evolved Converged Access (ECA) デバイスではサポートされていません。

ステップ 4 [+] をクリックして、追加のサーバーを追加します。

(注) 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 5 [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 6 (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 7 [構成] をクリックします。

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。「[デバイスのプロビジョニング](#)」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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [Wireless]。
- 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。
-

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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [Wireless] の順に選択します。
- ステップ 2** [VLAN Group] で、[VLAN Group Name] 列と [VLAN ID] 列を表示できます。

- ステップ 3** [Add] をクリックします。
[Add VLAN Group] ダイアログボックスが開きます。
- 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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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** [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右下隅に表示されます。

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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Settings] > [Wireless]。
- 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 (Typical)]、[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。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。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イ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。

- **[チャンネル幅 (Channel Width)]** ドロップダウンリストから、チャン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 チャンネル (DCA Channel)]** を設定して、チャン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ン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ンネルは、[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ンネルを含めるか、チャン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ンネルは、[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ンネルを含めるか、1 つまたは複数のチャン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ンネルは、[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ンネルを含めるか、1 つまたは複数のチャン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イトを設定するには、[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イトは、[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 packets 検出開始しきい値 (RX SOP) は、AP の無線が packets 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。

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 (INFRAVN-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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Settings] > [Wireless] の順に選択します。
- ステップ 2** [Add Create] をクリックし、[Enterprise] を選択します。
- ステップ 3** [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 4** [Next] をクリックします。
- ステップ 5** [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開きます。
- ステップ 6** [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 7** [Finish] をクリックします。
- ステップ 8** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Provision] > [Network Devices] > [Inventory] の順に選択します。
- ステップ 9** 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 10** [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 11** [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 12** [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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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] > [Backhaul Settings] タブをクリックします。

[Backhaul Settings] ウィンドウが表示されます。

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 ワイヤレスマップのためのコネクテッドモバイルエクスペリエンス (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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [System] > [Settings] > [External Services] > [CMX Servers] の順に選択します。

[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 のユーザー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 管理者のユーザー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 サーバーが正常に追加されました。
- ステップ 7** 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、[Menu] アイコンをクリックし、[Design] > [Network Settings] > [Wireless] の順に選択します。
- ステップ 8** 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 9** [CMX Servers] の下で、[CMX Servers] ドロップダウンリストから 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] 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 11** 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 12** 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) Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [System] > [Settings] > [External Services] > [CMX Servers] の順に選択します。

- b) 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。
- c) 削除する CMX サーバーを選択し、[Delete] をクリックします。
- d) [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 DNA 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 DNA 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 DNA Spaces の統合をサポートします。Cisco DNA 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 DNA 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 DNA 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 DNA Spaces と Cisco DNA Center の統合

Cisco DNA 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 DNA 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 DNA Spaces にログインし、[Continue] をクリックします。
[Select Customer] ダイアログボックスが表示されます。
- 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 DNA Spaces GUI で [Menu] アイコンをクリックし、[Setup] > [Wireless Networks] の順に選択します。
[Connect your wireless network] ウィンドウが表示されます。
- d) [Connect your wireless network] ウィンドウで、Cisco DNS コンフィギュレーションガイド [英語] に記載されている手順 1 – 3 を実行して、Cisco DNA Spaces クライアントをオンボードします。
Cisco DNS コンフィギュレーションガイド [英語] には、[Need Help?] の下にある右側のペインからアクセスできます。[View Configuration Steps] を選択します。

ステップ 2 Cisco DNA Spaces Enabler Package ソフトウェアを Cisco DNA Center に展開します。

- a) Cisco DNA Spaces Enabler Package ソフトウェアの入手方法については、シスコのアカウント担当者にお問い合わせください。
- b) Cisco DNA Center にログインします。
- c) Cisco DNA Center GUI で、[?] アイコンをクリックして、Cisco DNA Center で最新のリリースが実行されていることを確認します。
- d) Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[System] > [Software Updates] の順に選択します。
[Software Updates] ページが開き、Cisco DNA Spaces Enabler Package が [Application Updates] のリストに表示されます。
- e) [Install All] をクリックします。
[Select Any Package To Continue] ダイアログボックスが表示されます。
- f) [Cisco DNA Spaces Enabler Package] を選択し、[Continue] をクリックします。
[System Readiness Check] ダイアログボックスが表示されます。
- g) [Continue] をクリックします。
[Success] ダイアログボックスに、パッケージがまもなくインストールされることが示されます。

ステップ 3 Cisco DNA Center を Cisco DNA Spaces に登録します。

- a) 電子メール ID を使用して Cisco DNA Spaces にログインし、[Continue] をクリックします。
[Select Customer] ダイアログボックスが表示されます。

- 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 DNA Spaces GUI で [Menu] アイコンをクリックし、[Integrations] > [Cisco DNA Center] の順に選択します。
[DNAC Integration] ウィンドウが表示されます。
- 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表示されます。
- 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、[Menu] アイコンをクリックし、[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 [DNA Spaces/CMX Servers] を選択します。
[DNA Spaces/CMX Servers] ウィンドウが表示されます。
- j) [Cisco DNA Spaces] エリアで、[Activate] を選択します。
[Integrate DNA Spaces] ダイアログボックスが表示されます。
- k) [Tenant Token] テキストボックスで、Ctrl+V キーを押して Cisco DNA 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 DNA Spaces successfully.`
[DNA Spaces/CMX Servers] ウィンドウに緑色の ✓ [Activated] ステータスが表示され、Cisco DNA Spaces で選択したテナント（たとえば、dna-center-dev-US）が [Tenant] フィールドに表示されます。

ステップ 4 Cisco DNA Spaces を Cisco DNA Center のサイトに割り当てます。

- a) Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックして、[Design] > [Network Settings] > [Wireless] の順に選択します。
- b) 左側のツリービューメニューで、[Global] か、Cisco DNA 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。
- c) [DNA Spaces/CMX Servers] で、[Location Services] ドロップダウンリストからサイトを選択します（たとえば、DNA Spaces - dna-center-dev-US）。
- d) [保存 (Save)] をクリックします。

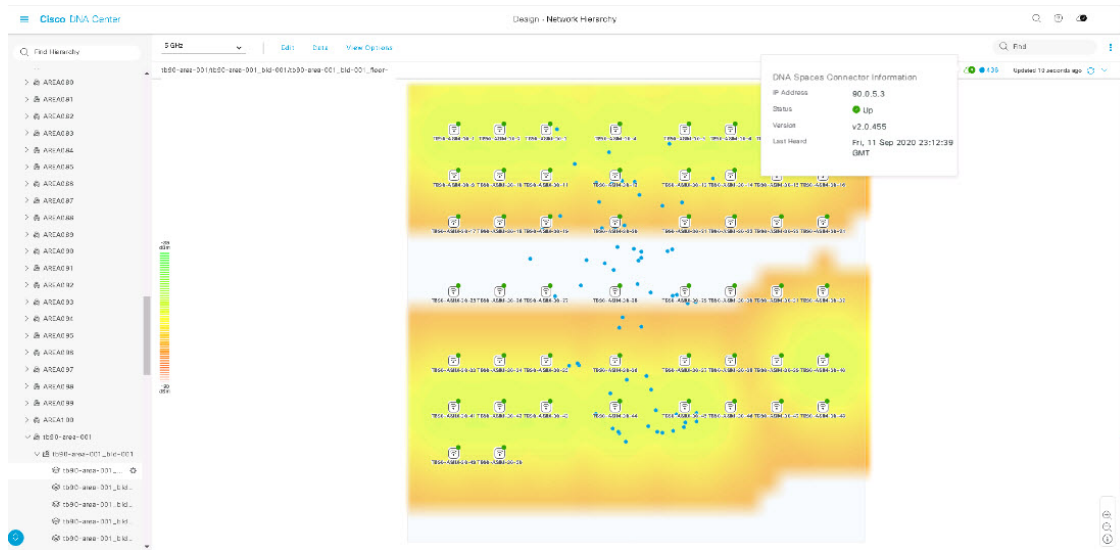
ステップ 5 Cisco DNA Spaces を使用して Cisco DNA Center のサイトをモニターします。

- a) Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックして、[Design] > [Network Hierarchy] の順に選択します。
- b) 左側のツリービューメニューで、[Global] か、Cisco DNA 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 DNA Spaces に自動的に展開されます。

- c) Cisco DNA 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 DNA 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 2: Cisco DNA Spaces ステータスアイコン



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 ユーザー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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Settings] > [Wireless]。
- 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 \(39 ページ\)](#) および [ゲスト ワイヤレス ネットワークの SSID の作成 \(45 ページ\)](#) 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 AireOS コントローラのプロビジョニング](#)」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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Profiles] を選択し、[Add Profile] をクリックして次の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
- ファイアウォール
- スイッチング
- ワイヤレス

NFVIS 用のネットワークプロファイルの作成

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. ENCS 統合スイッチを設定します。



(注) このオプションは、ENCS 5400 デバイスでのみ使用できます。

3. カスタム構成を作成します。
4. プロファイルの概要を表示します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Profiles] の順に選択します。

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

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

- [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 プロファイルの設定 \(97 ページ\)](#) 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、[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。
- [+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。[Router]、[Firewall]、[Application] のいずれかのアイコンをクリックして図にドラッグします。選択内容に基づいて、デフォルトのネットワーク接続が自動的に作成されます。または、[Custom- Net] 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。

ルータを設定するには、ルータをクリックして [Configuration] を選択します。ドロップダウンリストから [Type]、[Image]、[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。[vNIC Mapping] のフィールドを必要に応じて設定します。

ファイアウォールを設定するには、ファイアウォールをクリックして [Configuration] を選択します。ドロップダウンリストから [Type]、[Image]、[Profile] を選択します。[Type] のドロップダウンリストは、システムにインストールされているファイアウォールプラグインに基づいて入力されます。[vNIC Mapping] のフィールドを必要に応じて設定します。

アプリケーションを設定するには、アプリケーションをクリックして [Configuration] を選択します。ドロップダウンリストから [Type]、[Image]、[Profile] を選択します。[Type] のドロップダウンリストは、システムにインストールされているアプリケーションプラグインに基づいて入力されます。[vNIC Mapping] のフィールドを必要に応じて設定します。

カスタムネットワークを設定するには、[custom-net interface] をクリックします。[Connect from] を選択し、カスタムネットワークを追加するノードをクリックして [Connect to] を選択します。[custom-net] をクリックし、[Add Configuration] を選択します。[Network Mode] を選択し、[VLAN] に VLAN ID を入力します。

[Save] をクリックします。

- [Next] をクリックします。

ステップ4 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 5 [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。この手順をスキップしても、[Network Profiles] ページ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] でフィルタ処理されます。
- [Next] をクリックします。

ステップ 6 [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 7 [Network Profiles] ページが表示されます。

[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。

ルーティング用のネットワークプロファイルの作成

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. 統合スイッチ構成を設定します。
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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Profiles] の順に選択します。

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

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

- [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と10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プロファイルの設定 \(97 ページ\)](#) 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。2つ以上のデバイスが同じタイプの場合は、デバイスタグを使用します。すべてのデバイスが異なるタイプの場合、デバイスタグはオプションです。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、[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。

- [Next] をクリックします。

ステップ4 [Router WAN Configuration] ページが表示されます。

- [Configure Connection] オプションボタンをクリックし、[L2] または [L3]、あるいはその両方を選択します。
- [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。

[Skip] をクリックして、設定をスキップできます。

- [Next] をクリックします。

ステップ5 [Integrated Switch Configuration] ページが表示されます。

統合スイッチの設定では、新しい VLAN を追加したり、ルータの LAN 設定で選択した以前の設定を保持したりすることができます。

- 1 つ以上の新しい VLAN を追加するには、[+] をクリックします。
- VLAN を削除するには、[x] をクリックします。
- [Next] をクリックします。

(注) Switchport インターフェイスのサポートは、Cisco 1100 シリーズおよび Cisco 4000 シリーズ サービス統合型ルータでのみ使用できます。

ステップ 6 [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。この手順をスキップしても、[Network Profiles] ページ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] タブをクリックします。
- 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] でフィルタ処理されます。
- [Next] をクリックします。

ステップ 7 [Summary] ページで、[Save] をクリックします。

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提供されます。

ステップ 8 [Network Profiles] ページが表示されます。

[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。

ファイアウォール用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. カスタム構成を作成します。
2. Firepower Threat Defense (FTD) 構成を作成します。
3. プロファイルの概要を表示します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Profiles] の順に選択します。

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

[Firewall Type] ページが表示されます。

ステップ 3 適応型セキュリティアプライアンス (ASA) ファイアウォールなどの通常のファイアウォール用のカスタム構成を作成するには、次の手順を実行します。

- a) [Name] フィールドに、プロファイルの名前を入力します。
- b) [Devices] ドロップダウンリストからデバイスの番号を選択します。
(注) プロファイルごとに最大 10 のデバイスを選択できます。

- c) [Device Type] ドロップダウンリストからデバイスのタイプを選択します。
- d) (任意) [Device Tag] ドロップダウンリストからデバイスタグを選択します。
- e) [Next] をクリックします。

[Custom Configuration] ページが表示されます。

- f) [Template] ドロップダウンリストからテンプレートを選択します。
(注) テンプレートがない場合は、[Tools] > [Template Editor] で少なくとも 1 つのテンプレートを作成する必要があります。詳細については、[テンプレートの作成](#)を参照してください。

- g) [Next] をクリックします。

[Summary] ページが表示されます。このページには、カスタム構成の概要が表示されます。選択されたデバイスタイプに基づいて、ハードウェアの推奨事項が提示されます。

- h) [Save] をクリックします。

[Network Profiles] ページが表示されます。

- i) ネットワークプロファイルにサイトを割り当てるには、[Assign Sites] をクリックします。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 4 FTD デバイスを設定するための FTD 構成を作成するには、次の手順を実行します。

- a) [Name] フィールドに、プロファイルの名前を入力します。
- b) [Devices] ドロップダウンリストからデバイスの番号を選択します。
(注) プロファイルごとに最大 10 のデバイスを選択できます。

- c) FTD ファイアウォールをプロビジョニングするには、[FTD] チェックボックスをオンにします。
- d) [Device Type] ドロップダウンリストからデバイスのタイプを選択します。
- e) (任意) [Device Tag] ドロップダウンリストからデバイスタグを選択します。
- f) [Next] をクリックします。

[FTD Configuration] ページが表示されます。

- g) [Routed Mode] または [Transparent Mode] オプションボタンをクリックします。
- h) [Next] をクリックします。

[Summary] ページが表示されます。このページには、FTD 構成の概要が表示されます。選択されたデバイスタイプに基づいて、このページにハードウェアの推奨事項が示されます。

- i) [Save] をクリックします。
[Network Profiles] ページが表示されます。
- j) ネットワークプロファイルにサイトを割り当てるには、[Assign Sites] をクリックします。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、次の 2 つのタイプの設定テンプレートを適用できます。

- オンボーディングテンプレート
- Day N テンプレート

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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Profiles] の順に選択します。

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

ステップ 3 [Switching profile] ウィンドウで、[Profile Name] テキストボックスにプロファイル名を入力します。

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

- [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] ドロップダウンリストで使用できます。
- 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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Profiles] の順に選択します。
- ステップ 2** [+Add Profile] 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] ウィンドウで、[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 4** [+ SSID の追加 (+ Add SSID)] をクリックします。
作成した SSID が入力されます。
- ステップ 5** [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 6** [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 7** 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 8** [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 9** [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。
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。
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。
- ステップ 10** 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 11** [+ Add Model Config] をクリックして、モデル設定設計をネットワークプロファイルに追加します。
[Add Model Config] ウィンドウが表示されます。
- ステップ 12** [Device Type(s)] ドロップダウンリストから、デバイスタイプを選択します。

[search] フィールドに名前を入力してデバイス名を検索するか、または [Wireless Controller] を展開してデバイスタイプを選択できます。

ステップ 13 [Wireless] を展開し、このワイヤレスプロファイルに関連付けるモデル設定設計を選択します。

ステップ 14 [APPLICABILITY] の [Tags] ドロップダウンリストから、該当するタグを選択します。

ステップ 15 [Add] をクリックします。

関連付けられたモデル設定が [Add a Network Profile] ウィンドウの [Attach Model Config] 領域に表示されます。

ステップ 16 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 17 [Device Type(s)] ドロップダウンリストから、デバイスタイプを選択します。

[search] フィールドに名前を入力してデバイス名を検索するか、または [Wireless Controller] を展開してデバイスタイプを選択できます。

ステップ 18 [Device Tag] と [Template] のドロップダウンリストから、デバイスタグとテンプレートを選択できます。テンプレートではタグを使用できます。これを使用するのは、デバイスタグに基づいて同じデバイスタイプに対して異なるテンプレートをプッシュする必要がある場合だけです。

ステップ 19 [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 20 [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 21 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 22 [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に関連付けます。

親ノードまたは個々のサイトを選択できます。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 23 [Save] をクリックします。

ネットワークプロファイルの AP グループ、Flex グループ、およびサイトタグの事前プロビジョニング

Cisco DNA Center では、ネットワークプロファイルに AP グループ、Flex グループ、およびサイトタグを事前プロビジョニングできます。事前プロビジョニングすると、反復的な構成変更の必要がなくなることで AP プロビジョニング時の時間を節約でき、デバイス間の一貫性を確保できます。

- AP グループ構成は、AireOS イメージを実行するワイヤレス LAN コントローラに適用できます。
- Flex グループ構成は、AireOS イメージを実行するワイヤレス LAN コントローラに適用できます。
- サイトタグ構成は、Catalyst 9800 シリーズ ワイヤレス コントローラに適用できます

始める前に

AP グループ、Flex グループ、およびサイトタグを作成できるようにするには、ネットワークプロファイルを作成し、そのネットワークプロファイルにサイト（フロア）を割り当てる必要があります。

-
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します **[Design] > [Network Profiles]** の順に選択します。
- ステップ 2** [Edit] をクリックします。
- ステップ 3** [Show Advanced Settings] をクリックします。
- ステップ 4** ネットワークプロファイルに AP グループを作成するには、[AP Group] を展開し、[+ Create an AP Group] をクリックします。
- [Create an AP Group] ウィンドウが表示されます。
- ステップ 5** [AP Group Name] フィールドに、AP グループ名を入力します。
- ステップ 6** [RF Profile] 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。
- オプションは、[High]、[Typical]、[Low]、[custom_rf_profile2]、および [rf_prof1_custom] です。
- ステップ 7** [Select Sites] フィールドで、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。
- ステップ 8** (オプション) [Save & Add another] をクリックして別の AP グループを追加します。
- ステップ 9** [保存 (Save)] をクリックします。
- AP グループは、[Edit Network Profile] ウィンドウの [AP Group] 領域で選択した RF プロファイルに基づいて作成されます。
- ステップ 10** ネットワークプロファイルで Flex グループを有効にするには、[Flex Connect Local Switching] チェックボックスをオンにし、[Local to VLAN] テキストボックスに VLAN ID を定義して、非ファブリック SSID を Flex ベースの SSID としてマークします。
- 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。
- [Flex Group] オプションは、[View Advanced Settings] で有効になります。
- ステップ 11** ネットワークプロファイルに Flex グループを作成するには、[Flex Group] を展開し、[+ Create Flex Group] をクリックします。
- [Create Flex Group] ウィンドウが表示されます。

- ステップ 12** [Flex Group] フィールドに、Flex グループ名を入力します。
- ステップ 13** [Select Sites] フィールドで、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。
- ステップ 14** (オプション) [Save & Add another] をクリックして別の Flex グループを追加します。
- ステップ 15** [保存 (Save)] をクリックします。
- Flex グループは、[Edit Network Profile] ウィンドウの [Flex Group] 領域に作成されます。
- ステップ 16** ネットワークプロファイルにサイトタグを作成するには、[Site Tag] を展開し、[+ Create a Site Tag] をクリックします。
- [Create a Site Tag] ウィンドウが表示されます。
- ステップ 17** [Site Tag] フィールドに、サイトタグ名を入力します。
- ステップ 18** [Flex Profile Name] 名前フィールドに、Flex プロファイル名を入力します。
- (注) [Flex Profile Name] 名前フィールドを有効にするには、[Edit Network Profile] ウィンドウの [Flex Connect Local Switching] チェックボックスをオンにします。
- ステップ 19** [Select Sites] フィールドで、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。
- ステップ 20** (オプション) [Save & Add another] をクリックして別のサイトタグを追加します。
- ステップ 21** [保存 (Save)] をクリックします。
- サイトタグは、[Edit Network Profile] ウィンドウの [Site Tag] 領域の下に作成されます。

Cisco DNA トラフィック テレメトリアプライアンスのネットワークプロファイルの作成

始める前に

テレメトリアプライアンスに適用するテンプレートを定義します。『[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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Profiles] の順に選択します。
- ステップ 2** [+Add Profile] をクリックし、[Telemetry Appliance] を選択します。
- ステップ 3** [Telemetry Appliance Type] ウィンドウで、次の情報を入力します。
- [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。
 - [Devices] ドロップダウンリストから、デバイスの数を選択します。

- c) [Device Tag] ドロップダウンリストから、Cisco DNA Center で定義されている既存のデバイスタグを選択するか、新しいタグを入力します。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]ドロップダウンリストで使用できます。
- d) [Next] をクリックします。

ステップ 4 [Custom Configuration] ウィンドウで、テンプレートを選択します。選択したテンプレートは、デバイスが Cisco DNA Center のインベントリで管理されるようになると、そのデバイスに適用されます。

ステップ 5 [Next] をクリックします。

ステップ 6 [Summary] ウィンドウで、[Save] 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 \(97 ページ\)](#) 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 \(82 ページ\)](#)、[グローバル SNMPv2c クレデンシャルの設定](#)

(83 ページ)、グローバル SNMPv3 クレデンシャルの設定 (84 ページ)、およびグローバル HTTPS クレデンシャルの設定 (86 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 (91 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 (39 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。

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 ユーザー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、ユーザー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 デバイスをモニター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 10 の読み取りコミュニティストリングと 10 の書き込み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。

プラグアンドプレイの場合は、SNMPv2c の読み取り専用と読み取り/書き込みの両方のログイン情報を指定する必要があります。

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 10 個の 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、ユーザーおよびユーザー 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] : 認証も暗号化も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] : 認証と暗号化の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 1: 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	ユーザー名	未対応	ユーザ名の照合を使用して認証します。
AuthNoPriv	次のいずれかを行います。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA 	次のいずれかを行います。 <ul style="list-style-type: none"> • 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。

セキュリティレベルは、SNMPv3 ユーザーとそのユーザーが属する SNMPv3 グループで同じである必要があります。SNMPv3 ユーザーとそのユーザーの SNMPv3 グループのセキュリティレベルが異なる場合に、Cisco DNA Center が SNMPv3 トラップホストを設定すると、デバイスの SNMP 到達可能性が阻害される可能性があります。

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。

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 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]。Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します > >

ステップ 2 グローバル サイトを選択した状態で、[CLI Credentials] エリアで [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 2: 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 4 [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、[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、[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) [TimeZone] 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。



- (注) プラグアンドプレイの場合は、SNMPv2c の読み取り専用と読み取り/書き込みの両方の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 [Design]>[Network Settings]>[Device Credentials]。Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します>>

ステップ 2 グローバル サイトを選択した状態で、[SNMP Credentials] エリアで [Add] をクリックします。

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

表 3: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> [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。 <p>(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。</p>

ステップ 4 [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、[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 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]。Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します > >

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

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

表 4: 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。 <ul style="list-style-type: none"> • [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。

フィールド	説明
Auth Type	<p>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。</p> <ul style="list-style-type: none"> • [SHA] : HMAC-SHA に基づく認証。 • [MD5] : HMAC-MD5 に基づく認証。
Auth Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> •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	<p>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。</p> <ul style="list-style-type: none"> • [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。
Privacy Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> •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 [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、[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 [Design]>[Network Settings]>[Device Credentials]。Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します > >

ステップ 2 グローバルサイトを選択した状態で、[HTTPS Credentials] エリアで [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 5: 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 [White] です。

フィールド	説明
Read	<p>最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>

ステップ4 [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、[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

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。

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [Device Credentials]。
- ステップ 2** グローバルサイトを選択した状態で、変更するデバイスログイン情報を選択し、右側の [Actions] 列の下にある [Edit] をクリックします。
- ステップ 3** [EDIT CLI Credentials] ダイアログボックスで、[Save] をクリックします。
- ステップ 4** [APPLY CLI Credentials] ダイアログボックスで、[Cancel] をクリックします。
- ステップ 5** [Device Credentials] ウィンドウの下部で、[Save] をクリックします。
次のメッセージが表示されます。
Created Common Settings successfully.
- ステップ 6** [Device Credentials] ウィンドウに戻り、目的のデバイスログイン情報の [Edit] をクリックします。
- ステップ 7** [EDIT CLI Credentials] ダイアログボックスで、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 ~ 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 8** 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、[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。

ステータスメッセージに、デバイスログイン情報の変更が成功したか、失敗したかが示されます。

ステップ 9 ログイン情報の変更のステータスを表示するには、Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [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せん。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 GUI で [Menu] アイコン (☰) をクリックして選択します [Design] > [Network Settings] > [Device Credentials]。

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 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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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 [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 GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [IP Address Pools]。

ステップ2 [hierarchy] ペインを展開し、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 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/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 プールの編集

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します [Design] > [Network Settings] > [IP Address Pools]。

ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。

ステップ 3 すべての IP 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 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 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 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 プールの削除

- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [IP Address Pools] の順に選択します。
 - ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。
 - ステップ 3 すべての IP 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 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 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 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 プールの複製

サイトレベルで既存の IP プールを複製できます。IP 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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [IP Address Pools]。
 - ステップ 2 階層ツリーを展開し、サイトを選択します。
 - ステップ 3 目的の IP プールを見つけ、[Actions] 領域で [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 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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [IP Address Pools]。
- ステップ 2** グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。
- ステップ 3** すべての IP 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。
- [Actions] ドロップダウンリストから、[Release All] を選択します。
 - [Warning] メッセージで [Yes] をクリックします。
 - プロンプトで [Release] をクリックします。
- ステップ 4** 目的の IP プールのみをリリースするには、次の手順を実行します。
- 目的の IP 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。
 - 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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Design] > [Network Settings] > [IP Address Pools] 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** 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 プールが 10 個以上の場合、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 プールが 10 個未満の場合、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を示すツールチップが表示されます。
 - [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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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 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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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。

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 サーバークラスターの下に送信元インターフェイスを設定できます。各 Cisco ISE クラスターには独自のサーバークラスターがあります。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。

- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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 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。

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。