ネットワークのプロビジョニング

プロビジョニング

Cisco DNA Center でネットワークのポリシーを設定した後に、デバイスをプロビジョニングできます。この段階で、デバイスにオンボードし、デバイス間にポリシーを導入します。

プロビジョニングデバイスには、次の側面が含まれます。

- プラグ アンド プレイでのデバイスのオンボーディングと、デバイスのインベントリへの追加。
- 必要な設定とポリシーのインベントリ内デバイスへの展開。
- デバイスのサイトへの追加。
- ファブリック ドメインの作成とデバイスのファブリックへの追加。

Cisco DNA Center プロビジョニングでは IBNS 2.0 のみをサポートしています。これにより AAA 設定が変更され、関連するすべての認証コマンドがクラスベースのポリシー言語（CPL）制御ポリシーの対応するコマンドに変換されます。CPL 変換では、変換 CLI **authentication display [legacy|new-style]** が無効になるため、現在の設定をバックアップしておくことを推奨します。また、IBNS 2.0 に合わせた AAA 設定の更新をサポートするように変更管理期間を設定してください。

プラグ アンド プレイ プロビジョニングを使用したオンボードデバイス

プラグ アンド プレイ プロビジョニングは、最小限のネットワーク管理者およびフィールド担当者の関与で、新しいネットワーク デバイスを自動的かつリモートにプロビジョニングおよびオンボードする方法を提供します。

プラグ アンド プレイ プロビジョニングを使用すると、次の操作を実行できます。

- サイトの割り当て、サイト設定の展開、デバイス ソフトウェア イメージのインストール、およびカスタム オンボード設定の適用によって、デバイスをプロビジョニングする。
- インストールの前に、デバイス情報を入力し、プロビジョニング操作を選択してデバイスを計画します。デバイスはオンラインになると Cisco DNA Center に接続します。次に、デバイスのプロビジョニングとオンボーディングが自動で実行されます。
- 事前の計画なしにネットワーク上に表示される新しいデバイスである、要求されていないネットワーク デバイスをプロビジョニングします。
- Cisco スマート アカウントの Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリをプラグ アンド プレイに同期して、すべてのデバイスが Cisco DNA Center に表示されるようにします。
- ネットワーク デバイスの詳細なオンボーディング ステータスを表示します。

前提条件

プラグ アンド プレイ プロビジョニングを使用する前に、次の操作を実行します。

- メインの Cisco DNA Center の設定で、[System] > [Settings] > [Smart Account] を使って、Cisco スマートアカウントのクレデンシャルを設定します。
- [System] > [Settings] > [Device EULA Acceptance] を使用して、メインの Cisco DNA Center の設定でシスコ エンド ユーザー ライセンス契約（EULA）に同意します。
- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Network Plug and Play Troubleshooting Guide for Cisco DNA Center』で、デバイスのクリーンアップとリセットの詳細を参照してください。

ここでは、プラグアンドプレイプロビジョニングの一般的な使用例とワークフローについて説明します。

計画されたプロビジョニング

管理者は、次のように新しいサイトまたはその他のネットワーク デバイス グループのプロビジョニングを計画できます。

1. ネットワーク階層内のサイトを定義します。ネットワーク階層についてを参照してください。
2. 必要に応じて、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。多くの場合、Day 0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。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。
3. 展開するデバイスのタイプについて、ネットワーク プロファイルを定義します。「ネットワーク プロファイルの作成」を参照してください。
4. 展開するデバイスのデバイスログイン情報（CLIおよびSNMP）を定義します。SNMPv2c を使用している場合は、読み取りと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。「デバイス クレデンシャルについて」を参照してください。
5. 必要に応じて、プロビジョニングするデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。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。
6. CSV ファイルを使用して一度にまたは一括で、計画したデバイスに関する詳細を追加します。デバイスの追加または編集 （11 ページ）またはデバイスの一括追加 （13 ページ）を参照してください。
7. デバイスが起動し、自動的にプロビジョニングされます。

要求されていないプロビジョニング。

計画前に新しいネットワーク デバイスをネットワークに追加すると、このネットワーク デバイスは要求のないデバイスとしてラベル付けされます。要求のないデバイスは、管理者が手動で追加することも、コントローラ ディスカバリの前提条件 （4 ページ）で説明されているいずれかの検出方法を使用して自動的に追加することもできます。管理者は、次の方法でデバイスをプロビジョニングできます。

1. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （8 ページ）」を参照してください。
2. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （16 ページ）」を参照してください。

Cisco スマート アカウントの同期およびプロビジョニング

ネットワーク デバイスは、シスコのプラグ アンド プレイ接続クラウド サービスによって Cisco スマート アカウントを通じて自動的に登録されます。管理者は Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。これにより、すべてのデバイスが Cisco DNA Center に表示されます。次に、これらのデバイスを要求してプロビジョニングすることができます。

1. スマートアカウントと同期するバーチャルアカウントを登録して同期します。「バーチャル アカウント プロファイルの登録または編集 （13 ページ）」を参照してください。
2. スマート アカウントからデバイス インベントリを同期します。スマート アカウントからのデバイスの追加 （15 ページ）を参照してください。
3. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （8 ページ）」を参照してください。
4. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （16 ページ）」を参照してください。
5. デバイスが起動し、自動的にプロビジョニングされます。

コントローラ ディスカバリの前提条件

プラグ アンド プレイによってデバイスのオンボーディングが自動化されます。デバイスは、Cisco DNA Centerコントローラを検出して接続できるようにする必要があります。デバイスは、次のいずれかの方法でコントローラを自動的に検出できるようにする必要があります。

- DHCP：DHCP コントローラ ディスカバリ （4 ページ）を参照してください。
- DNS：DNS コントローラ ディスカバリ （6 ページ）を参照してください。
- Cisco Plug and Play Connect クラウドサービス：Plug and Play Connect コントローラ ディスカバリ （6 ページ）を参照してください。

DHCP コントローラ ディスカバリ

シスコのネットワークデバイスは初回起動時にスタートアップ設定を使用しない場合、DHCP オプション 43 を使用して Cisco DNA Center コントローラの検出を試行します。

DHCP による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- DHCP サーバが Cisco Plug and Play のオプション 43 を使用して設定されている。このオプションにより、Cisco DNA Center コントローラの IP アドレスを持つネットワークデバイスが通知されます。

  DHCP サーバが文字列「ciscopnp」を含むオプション 60 を使用してデバイスから DHCP の検出メッセージを受信すると、オプション 43 の情報を含む応答をデバイスに返します。デバイスの Cisco Plug and Play IOS エージェントは、応答から Cisco DNA Center コントローラの IP アドレスを抽出し、このアドレスを使用してコントローラと通信します。

DHCP オプション 43 は、DHCP サーバとして機能する Cisco ルータ CLI で、次のように設定された文字列の値で構成されます。

```
ip dhcp pool pnp_device_pool          <-- Name of DHCP pool
```

```
network 192.168.1.0 255.255.255.0    <-- Range of IP addresses assigned to clients
default-router 192.168.1.1           <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80"    <-- Option 43 string
```

このオプション 43 の文字列には、セミコロンで区切られた次のコンポーネントが含まれています。

- 5A1N;（プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし）。文字列のこの部分は変更する必要がありません。
- B2;（IP アドレスのタイプ）：
  - B1 = ホスト名
  - B2 = IPv4（デフォルト）
- I*xxx.xxx.xxx.xxx*;：Cisco DNA Center コントローラの IP アドレスまたはホスト名（大文字の i の後）。この例では、IP アドレスは 172.19.45.222 です。
- J*xxxx*：Cisco DNA Center コントローラへの接続に使用するポート番号。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。
- K4;：デバイスとコントローラの間で使用されるトランスポート プロトコル。
  - K4 = HTTP（デフォルト）
  - K5 = HTTPS
- T*trustpoolBundleURL*：デフォルト（Cisco DNA Centerコントローラ）以外の別の場所から trustpool バンドルを取得する場合は、このオプション パラメータを使用して trustpool バンドルの外部 URL を指定します。APIC-EM コントローラは、Cisco InfoSec Cloud（http://www.cisco.com/security/pki/）からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Tftp://10.30.30.10/ios.p7b」と指定します。

  trustpool セキュリティを使用していて、T パラメータを指定しない場合、デバイスは Cisco DNA Center コントローラから trustpool バンドルを取得します。
- Z*xxx.xxx.xxx.xxx*;（NTP サーバの IP アドレス）。trustpool セキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

DHCP の設定の詳細については、『*Cisco IOS Command Reference*』を参照してください。

DHCP オプション 43 が設定されていない場合、デバイスが DHCP サーバに接続できない場合、またはこの方法が別の理由で失敗する場合は、ネットワークデバイスは DNS を使用して検出を試行します。詳細については、DNS コントローラ ディスカバリ （6 ページ）を参照してください。

Cisco DNA Center システム証明書に FQDN のみの SAN フィールドがある場合、PnP を開始する前に、シードデバイスの DHCP プールを編集して、FQDN、B2 ー B1、dns-server、および domain-name を含むオプション 43 文字列を含める必要があります。

DHCP プールが Cisco スイッチまたはルータに依存している場合の設定例は次のとおりです。

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80"
domain-name sitdns.com
dns-server 17.1.104.100
```

DNS コントローラ ディスカバリ

DHCP ディスカバリが Cisco DNA Center コントローラの IP アドレスを取得できない場合、ネットワークデバイスは DNS ルックアップ方式にフォールバックします。DHCP サーバから返されたネットワークドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、コントローラの完全修飾ドメイン名（FQDN）を作成します。NTP のサーバ名は、事前設定されたホスト名 pnpserver に基づいています。

たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、ネットワークデバイスは「pnpserver.customer.com」というコントローラの FQDN を作成します。次に、この FQDN の IP アドレスを解決するために、ローカル ネーム サーバを使用します。NTP サーバ名の FQDN は pnpntpserver.customer.com です。

DNS による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- Cisco DNA Center コントローラがホスト名「pnpserver」を使用して展開されている。
- NTP のサーバ名はホスト名「pnpserver」で展開される。

Plug and Play Connect コントローラ ディスカバリ

DHCP または DNS による検出方法の使用がオプションでない場合は、Cisco Plug and Play Connect クラウド サービスによって、デバイスが Cisco DNA Center コントローラの IP アドレスを検出できます。ネットワークデバイスが起動すると、DHCP または DNS を介してコントローラを特定できない場合に、devicehelper.cisco.com に接続して Plug and Play Connect を試行し、組織に定義されている適切なコントローラの IP アドレスを取得します。通信を保護するために、デバイスは Plug and Play Connec に接続するときに、最初に Cisco trustpool バンドルをダウンロードしてインストールします。

次の手順では、検出に Plug and Play Connect を使用して、Cisco Plug and Play でシスコのネットワークデバイスを展開する方法についての概要を説明します。

始める前に

シスコの各種ネットワークデバイスは、Cisco Plug and Play をサポートし、Cisco Plug and Play Connect クラウドサービスに接続している Cisco IOS イメージを実行しています。

ステップ 1 ネットワーク管理者は、Cisco スマートアカウントの Web ポータルにある Plug and Play Connect を使用して、組織に適した Cisco DNA Center コントローラのコントローラ プロファイルを設定します。詳細については、web ポータルのスマートアカウントのマニュアルを参照してください。

ステップ 2 Cisco Commerce Workspace（CCW）を介してプラグアンドプレイ ネットワークデバイスを注文した場合、Cisco スマートアカウントが注文に割り当てられていれば、Plug and Play Connect を使用してネットワークデバイスが自動的に登録されます。Cisco Plug and Play で使用する各デバイスに、NETWORK-PNP-LIC オプションを追加します。

このオプションにより、デバイスのシリアル番号と PID がプラグアンドプレイ用にスマート アカウントで自動登録されます。デフォルト コントローラを指定済みの場合、注文の処理時にデバイスがそのコントローラに自動的に割り当てられます。

ステップ 3 または、Plug and Play Connect の Web ポータルからデバイスを手動で追加することもできます。

ステップ 4 Cisco DNA Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマート アカウントに登録します。バーチャル アカウント プロファイルの登録または編集 （13 ページ）を参照してください。

CCW を通してプラグアンドプレイ ネットワーク デバイスを注文し、これらのネットワークデバイスがスマートアカウント経由で Plug and Play Connect に自動登録される場合には、この手順が必須です。

ステップ 5 Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。

Plug and Play Connect の Web ポータルに登録されたデバイスがコントローラに同期され、SmartAccount のソースとともにプラグ アンド プレイのデバイス リストに表示されます。

ステップ 6 新しく同期されたデバイスを要求します。プラグアンドプレイ対応デバイスのプロビジョニング （16 ページ）を参照してください。

ステップ 7 デバイス インストーラによって、シスコ ネットワークデバイスがインストールされ、電源が投入されます。

ステップ 8 デバイスは、Plug and Play Connect サービスをクエリして Cisco DNA Center コントローラを検出し、Cisco DNA Center でプラグ アンド プレイのシリアル番号によってコントローラを識別します。次に、要求プロセス中に計画された内容に従ってプロビジョニングされます。

（注） デバイスが定義済みの NTP サーバ **time-pnp.cisco.com** または **pool.ntp.org** と同期できない場合、デバイスは Plug and Play Connect のコンタクトに失敗します。この問題を解決するには、これらの 2 つのホスト名への NTP トラフィックをブロック解除するか、これら 2 つの NTP ホスト名を DNS サーバのローカル NTP サーバ アドレスにマップします。

プラグアンドプレイ導入ガイド

プラグアンドプレイを使用する場合は、次の推奨事項に従ってください。

- デバイスの起動順序：一般に、ルーティングとアップストリームデバイスは最初に展開する必要があります。ルータおよびすべてのアップストリームデバイスがアップされてプロビジョニングされると、スイッチとダウンストリームデバイスを展開できます。デバイスのプラグ アンド プレイ エージェントは最初のデバイスの起動時のみ、Cisco DNA Center

コントローラの自動検出を試みます。現時点で、デバイスがコントローラに接続できない場合、デバイス プロビジョニングは失敗するため、アップストリーム デバイスは最初にプロビジョニングする必要があります。

- シスコのルータトランク/アクセスポートの構成：一般的なブランチネットワークには、ルータとスイッチが含まれます。1 つ以上のスイッチは WAN ルータに接続され、IP フォンやアクセス ポイントなどの他のエンドポイントはスイッチに接続します。スイッチがアップストリームルータに接続されると、次の導入モデルはプラグアンドプレイでサポートされます。
  - ダウンストリーム スイッチはルータのスイッチ ポートを使用してルータに接続されます。このタイプの接続では、ルータのスイッチ ポートをトランクまたはアクセスポートとして設定できます。
  - ルータのルーテッド ポートを使用してダウンストリーム スイッチをルータに接続する。この場合、ルーテッド ポートはサブインターフェイスを使用して複数の VLAN をサポートできます。プラグアンドプレイのプロセス中、スイッチはそのポートを自動的にトランクポートとして設定します。大規模ブランチの場合は、ルータとダウンストリーム スイッチ間に複数の VLAN を設置する必要があります。このような使用例をサポートするには、スイッチをルーテッド ポートに接続する必要があります。
- 非 VLAN 1 構成：プラグアンドプレイは、VLAN 1 を使用して、デフォルトでデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリームデバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリームデバイスに「**pnp startup-vlan** *x*」グローバル CLI コマンドを設定して、以降のプラグアンドプレイデバイスにこの CLI をプッシュする必要があります。隣接するアップストリーム デバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、アップストリームに接続された、以降のプラグアンドプレイデバイス上のアクティブインターフェイスは、指定された VLAN に変更されます。このガイドラインは、ルータとスイッチの両方に適用され、アクセスモードではなくトランクモードのシナリオでのみ使用する必要があります。

デバイスの表示

この手順では、プラグアンドプレイデバイスを表示する方法、デバイスでアクションを実行する方法、および新しいデバイスを追加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**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。[Devices] テーブルに、すべてのプラグアンドプレイデバイスが表示されます。

ステップ 3 [Device Status] エリアで、[Unclaimed]、[Error]、[Provisioned]、または [All] をクリックします。

- [Unclaimed]：要求されていないデバイスと要求されているデバイスが表示されます。
- [Error]：要求中にエラーが発生したデバイスが表示されます。
- [Provisioned]：要求されたデバイスが表示されます。

- [All]：すべてのデバイスが表示されます。

ステップ 4 [Focus] ドロップダウンリストから、[Basic] または [Default] を選択します。

- [Basic]：デバイスの詳細情報として、**デバイス名**、**シリアル番号**、**製品 ID**、**IP アドレス**、**送信元**、**状態**、**サイト**、および**最終連絡先**が表示されます。
- [Default]：デバイスの詳細情報として、**デバイス名**、**シリアル番号**、**製品 ID**、**IP アドレス**、**送信元**、**状態**、**オンボーディング進捗状況**、**サイト**、**最終連絡先**、**スマートアカウント**、**バーチャルアカウント**、および**作成日時**が表示されます。

ステップ 5 [Auto-Refresh] ドロップダウンリストから、[30 s]、[1 min]、[5 min]、または [10 min] を選択する（指定した期間で [Devices] テーブルを自動更新する場合）か、[Off] を選択してます（自動更新をオフにする場合）。

ステップ 6 歯車のアイコンをクリックして、[Devices] テーブルの外観をカスタマイズします。

[Table Settings] スライドインペインで、次の手順を実行します。

1. [Table Appearance] をクリックし、[Table Density] で [Default] または [Compact] を選択します。行ごとに色を変える場合は [Table Striping] を有効にします。
2. [Enable Table Columns] をクリックし、テーブルに表示する列を選択します。
3. [Apply] をクリックします。
4. テーブル設定をリセットする場合は、[Reset All Settings] をクリックします。

ステップ 7 特定のデバイスを検索するには、検索またはフィルタのアイコンをクリックします。

ステップ 8 [Refresh Now] をクリックして、[Devices] テーブルを手動で更新します。

ステップ 9 ステータスが [Error] のデバイスについて、[Onboarding Progress] 列の進捗状況バーにカーソルを合わせてエラーを確認します。

エラーの詳細については、デバイスの名前をクリックし、[History] タブでエラーの詳細情報を表示します。

ステップ 10 デバイスの名前をクリックします。

スライドインペインが表示され、デバイスの詳細情報が示されます。

ステップ 11 [Details]、[History]、[Configuration]、または [Stack] タブをクリックして、デバイスに関するさまざまな種類の情報を表示します。

[スタック（Stack）] タブは、スイッチ スタック デバイスの場合にのみ表示されます。

ステップ 12 [Devices] テーブルでデバイスを選択し、[Actions] ドロップダウンリストから次のいずれかのオプションを実行します。

- [Claim]：プラグアンドプレイ対応デバイスのプロビジョニング （16 ページ）を参照してください。
- [Edit]：デバイスの追加または編集 （11 ページ）を参照してください。
- [Reset]：デバイスのリセット （29 ページ）を参照してください。
- [Delete]：デバイスの削除 （28 ページ）を参照してください。

複数のデバイスに対してアクションを実行するには、[Devices] テーブルで各デバイスの横にあるチェックボックスをオンにし、[Actions] ドロップダウンメニューからアクションを選択します。

ステップ 13 [Add Device] をクリックして、新しいデバイスを追加します。

異なる方法でデバイスを追加する方法の詳細については、次のトピックを参照してください。

- デバイスの追加または編集 （11 ページ）
- デバイスの一括追加 （13 ページ）
- スマート アカウントからのデバイスの追加 （15 ページ）

[Devices] テーブルには、各デバイスについて、次の表に示す情報が表示されます。一部の列はソートに対応しています。ソートに対応している場合、列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

デバイステーブルには、各デバイスについて、以下の表に示した情報が表示されます。一部の列はソートに対応しています。ソートに対応している場合、列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

表 *1*: デバイス情報

カラム	説明
#	行番号。
Device Name	デバイスのホスト名。このリンクをクリックすると、デバイスの詳細ウィンドウが開きます。スタックアイコンはスイッチスタックを示します。
Serial Number	デバイスのシリアル番号。
Product ID	デバイスの製品 ID。
IP Address	デバイスの IP アドレス。
Source	デバイスエントリの送信元： • [User]：ユーザーが GUI または API を介してデバイスを追加しました。 • [Network]：コントローラに接続されたデバイスが要求解除されました。 • [SmartAccount]：デバイスはスマートアカウントから同期されました。

カラム	説明
状態	• [Unclaimed]：デバイスはプロビジョニングされていません。 • [Planned]：デバイスはすでに要求されていますが、まだサーバーと接続していません。 • [Onboarding]：デバイスオンボーディングが進行中です。 • [Provisioned]：デバイスは正常にオンボーディングされ、インベントリに追加されています。 • [Error]：デバイスにエラーがあり、プロビジョニングできませんでした。
Onboarding State	デバイスのオンボーディング状態。デバイスの履歴に移動するには、経過表示バーをクリックします。
Site	デバイスが関連付けられているサイト。
Last Contact	デバイスが最後にプラグ アンド プレイに接続した日時。
Smart Account	デバイスが関連付けられている Cisco スマート アカウント。
Virtual Account	デバイスが関連付けられている（Cisco スマート アカウント内の）バーチャル アカウント。
Created	デバイスがプラグ アンド プレイに追加された日時。

デバイスの追加または編集

この手順では、[Plug and Play Devices] リストからデバイスを追加または編集する方法について説明します。代わりに、[編集（Edit）] をクリックしてデバイスの詳細ウィンドウからデバイスを編集することもできます。

表 *2 : [デバイス（Device）] フィールド*

フィールド	説明
[Serial Number]	デバイス シリアル番号（デバイスを編集している場合は読み取り専用）。
Product ID	デバイス製品 ID（デバイスを編集している場合は読み取り専用）。
[Device Name]	デバイス名
Enable SUDI Authorization	セキュアな固有デバイス識別子（SUDI）認証をサポートするデバイスで有効にします。

フィールド	説明
SUDI Serial Numbers	SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号（デバイス ラベルのライセンス SN と呼ばれる）の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加するときは、このフィールドに 1 つまたは複数の SUDI シリアル番号をカンマで区切って入力します。このフィールドは、[SUDI 認証の有効化（Enable SUDI Authorization）] がチェックされている場合にのみ表示されます。
This Device Represents a Stack	デバイスがスタックを表します（デバイスを編集している場合、この項目は読み取り専用です）。サポート対象のスタッカブル スイッチにのみ適用されます。

始める前に

デバイスにログイン情報が必要な場合は、グローバルデバイスログイン情報が **[Design]** > **[Network Settings]** > **[Device Credentials]** ページで設定されていることを確認します。詳細については、グローバル CLI クレデンシャルの設定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**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 次のようにデバイスを追加または編集します。

- デバイスを追加するには、[Add Devices] をクリックし、[Single Device] をクリックします。
- デバイスを編集するには、編集するデバイス名の横にあるチェック ボックスをオンにして、デバイス テーブルの上部にあるメニューバーから [アクション（Actions）]>[編集（Edit）] をクリックします。**[デバイスの編集（Edit Device）]** ダイアログが表示されます。

ステップ 4 必要に応じてフィールドを設定します。詳細については上記の表を参照してください。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- デバイスを追加し、後で要求するには、[デバイスの追加（Add Device）] をクリックします。
- デバイスを追加し、すぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （16 ページ）、を参照してください。
- デバイスを編集する場合は、[デバイスの編集（Edit Device）] をクリックします。

デバイスの一括追加

この手順では、CSV ファイルからデバイスを一括で追加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**[Provision]** > **[Plug and Play]**。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Bulk Devices] をクリックします。

ステップ 4 [Download File Template] をクリックしてファイルテンプレートをダウンロードします。

さまざまなデバイスの必須のフィールドとオプションのフィールドについては、ファイルテンプレートを参照してください。

ステップ 5 各デバイスの情報をファイルに追加し、ファイルを保存します。デバイスタイプによっては、特定のフィールドが必須になることに注意してください。

ステップ 6 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。

- 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。
- **[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 7 **[デバイスのインポート（Import Devices）]** をクリックします。

CSV ファイル内のデバイスがテーブルにリストされます。

ステップ 8 インポートする各デバイスの横にあるチェックボックスをオンにするか、上部にあるチェックボックスをオンにしてすべてのデバイスを選択します。

ステップ 9 次のいずれかの操作を実行して、デバイスを追加します。

- デバイスを追加し、それらを後で要求するには、**[デバイスの追加（Add Devices）]** をクリックします。
- デバイスを追加し、それらをすぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （16 ページ）、を参照してください。

バーチャル アカウント プロファイルの登録または編集

この手順により、Cisco DNA Center コントローラを、リダイレクション サービス向けの Cisco スマート アカウントに、Cisco Plug and Play Connect のデフォルトのコントローラとして登録できます。また、これによって Cisco Plug and Play Connect クラウド ポータルから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

表 *3:* バーチャルアカウント フィールド

フィールド	説明
スマートアカウントの選択	Cisco スマート アカウント名
バーチャルアカウントの選択	バーチャルアカウント名バーチャルアカウントは、Cisco スマートアカウント内のサブアカウントです。
デフォルト コントローラ プロファイルとして使用	Cisco DNA Center コントローラを Cisco プラグアンドプレイ接続のクラウド ポータルにデフォルト コントローラとして登録するには、このボックスにチェックを付けます。
コントローラ IP または FQDN	この Cisco DNA Center コントローラの IP アドレスまたは完全修飾ドメイン名。
プロファイル名	コントローラのプロファイル名

始める前に

メインの Cisco DNA Center の設定で、**[System]** > **[Settings]** > **[Smart Account]** を使って、Cisco スマートアカウントのクレデンシャルを設定します。

ステップ 1 Cisco DNA CenterGUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[システム（System）]** > **[設定（Settings）]** > **[PnP 接続（PnP Connect）]**の順に選択します。

ステップ 2 テーブル内のバーチャルアカウントを表示します。

このテーブルには、登録されている Plug and Play Connect のバーチャル アカウント プロファイルがすべて一覧表示されます。

ステップ 3 次のように、バーチャル アカウント プロファイルを追加または編集します。

- バーチャルアカウントを登録するには、[Register] をクリックします。[Register Virtual Account] ダイアログが表示されます。
- 登録済みのバーチャルアカウントプロファイルを編集するには、編集したいプロファイル名の横にあるラジオボタンをクリックし、テーブルの上にあるメニュー バーの [Edit Profile] をクリックします。[edit virtual account] ダイアログが表示されます。

ステップ 4 上述の [Virtual Account Fields] テーブルを参照して、必要に応じてフィールドを設定します。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- 新しいバーチャルアカウント プロファイルを登録する場合は、[Register] をクリックします。
- バーチャル アカウント プロファイルを編集する場合は、[Change] をクリックします。

次のタスク

Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。詳細については、スマート アカウントからのデバイスの追加 （15 ページ）を参照してください。

スマート アカウントからのデバイスの追加

このタスクにより、Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

バーチャル アカウント テーブルには、プロファイルごとに情報が表示されます。

表 *4*: バーチャル アカウント情報

カラム	説明
バーチャル アカウント	バーチャルアカウント名
スマート アカウント	バーチャルアカウントが関連付けられているスマートアカウント
同期ステータス	直近の同期プロセスのステータス
同期の結果	最後の同期プロセスの結果

始める前に

Cisco プラグアンドプレイ接続クラウド ポータルからデバイスインベントリを同期する前に、バーチャルアカウントを登録する必要があります。バーチャル アカウント プロファイルの登録または編集 （13 ページ）を参照してください。**[Add Devices]** > **[Smart Account Devices]** ダイアログの **[PnP Connect]** リンクをクリックすると、[PnP Connect] 設定ページに直接移動できます。

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**[Provision]** > **[Plug and Play]** を選択します。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Smart Account Devices] をクリックします。

ステップ 4 Cisco.com ID を入力する必要がある場合（Cisco.com ID は「Not Associated（関連付けなし）」として表示されます）、次の手順を実行します。

a) [Add] リンクをクリックします。
b) Cisco.com ユーザ名とパスワードを入力します。
c) ログイン情報を Cisco DNA Center で永続的に保存する場合は [Save For Later] をクリックします。ログイン情報を 1 回のみ使用する場合は、このチェックボックスをオフのままにします。
d) [Submit] をクリックします。`

ステップ 5 デバイスを追加する Plug and Play Connect バーチャル アカウント プロファイルの名前の横にあるラジオ ボタンをクリックします。

PnP Connect バーチャル アカウント プロファイルを登録する必要がある場合は、[PnP Connect] リンクをクリックします。Cisco.com のログイン情報を追加する必要がある場合は、[Cisco.com ID] の横にある [Add] リンクをクリックします。Cisco ID を変更する場合は、[Not me?] リンクをクリックします。

ステップ 6 [Sync] をクリックして、このバーチャル アカウントの Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイに、デバイス インベントリを同期させます。

追加されたデバイスは、SmartAccount に設定されたソースとともに [Plug and Play Devices] テーブルに表示されます。

次のタスク

新しく同期されたデバイスを要求します。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （16 ページ）、を参照してください。

プラグアンドプレイ対応デバイスのプロビジョニング

デバイスのプロビジョニングまたは要求では、イメージとオンボーディングの設定をデバイスに展開するか、ワイヤレスデバイスのネットワークプロファイルを展開して、それをインベントリに追加してプロビジョニングします。デバイスの初起動を要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスをプロビジョニングするためのワークフローは、デバイスのタイプによって次のように異なります。

- スイッチとルータの参照資料： スイッチまたはルータ デバイスのプロビジョニング （16 ページ）
- ワイヤレス LAN コントローラ、アクセスポイント、センサの参照資料： ワイヤレスまたはセンサー デバイスのプロビジョニング （22 ページ）

スイッチまたはルータ デバイスのプロビジョニング

デバイスを要求すると、それをサイトに割り当て、イメージをインストールし、サイト設定とオンボーディング構成を展開してインベントリに追加することでプロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスが要求される場合、Cisco DNA Center からのシステム構成 CLI コマンドの一部はまずデバイスにプッシュされてから、定義した [Onboarding Configuration (Day-0)] テンプレートにプッシュされます。[Onboarding Configuration] テンプレートに同じ CLI コマンドがある場合、これらは最後に適用されるため、システム設定が上書きされます。システムによってプッシュされる CLI コマンドには、次のものがあります。

- デバイスのログイン情報（CLI および SNMP）

- SSH v2 および SCP サーバの有効化
- HTTP および HTTPS サーバの無効化
- スイッチでは、vtp モードの透過が有効になっています

（注） あるデバイスについてデバイスの可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加された、またはサイトに割り当てられたときに、追加の設定がデバイスにプッシュされます。詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください。

この手順では、[Plug and Play Devices] リストからデバイスを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド[英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、「コントローラ ディスカバリの前提条件 （4 ページ）」を参照してください。
- ネットワーク階層内のサイトを定義します。ネットワーク階層についてを参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。SNMPv2c を使用している場合は、読み取りと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。「デバイス クレデンシャルについて」を参照してください。
- （オプション）イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージをアップロードし、イメージリポジトリ内でゴールデンとしてマークされるようにします。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。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ導入プロセスは、後でデバイスイメージの更新時に使用されるプロセスと同じではありません。これはソフトウェアイメージのプロビジョニングで説明されています。プラグアンドプレイプロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- 必要に応じて、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。

（注） [Onboarding Configuration] テンプレートで `ip http client source-interface` CLI コマンドを使用できます。これにより、Cisco DNA Center は、特に複数の IP または VRF のシナリオにおいて、その IP アドレスをデバイスの管理 IP アドレスとして使用できます。

- デバイスのネットワークプロファイルを定義します。ネットワークプロファイル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**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[Actions] > [Claim] をクリックします。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスクレデンシャルの定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスクレデンシャルを定義する必要があります。これらは要求プロセスの前提条件であり、これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （オプション）必要に応じて、最初のカラムのデバイスのホスト名を変更します。

ステップ 6 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトを選択します。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して **[Assign] をクリックします。**

ステップ 7 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 8 （オプション）次のように、デバイステーブルに対するグローバルな変更を行います。

a) テーブルに表示されるカラムを変更するには、テーブル見出しの右端にある3つの点をクリックし、目的のカラムを選択します。[Apply] をクリックして、変更内容を保存します。

b) [Clear Device Certificates] をクリックして、デバイスに対して設定されているすべてのデバイス証明書をクリアします。証明書をクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

c) [Clear Images] をクリックして、デバイス用に設定されたデフォルトイメージをクリアします。イメージをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

d) [Clear Templates] をクリックして、デバイス用に設定されたデフォルトテンプレートをクリアします。テンプレートをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

e) デバイスに設定されているライセンスレベルをクリアするには、[Clear License Level] をクリックします。ライセンスレベルをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

f) デバイスの横にある [Actions] カラムの 3 つの点をクリックし、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択することで、あるデバイスのイメージまたはテンプレートを他のデバイスに適用できます。スタック構成のデバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

ステップ 9 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。

b) （オプション）PKCS12 証明書をデバイスに展開する場合は、[Apply the PKCS12 device certificate on the device] チェックボックスをオンにします。このオプションは、ルータの場合にのみ使用可能です。

c) （オプション）必要に応じて [Device Name] フィールドでデバイスのホスト名を変更します。

d) （オプション）[イメージ（Image）] ドロップダウン リストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。

e) （オプション）[テンプレート（Template）] ドロップダウン リストで、デバイスに適用する [オンボーディングの設定（onboarding configuration）] テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

選択したテンプレートの横にある [Preview] をクリックすると、テンプレートが表示されます。

f) （オプション）スタックの番号を付け直す場合は、[Select a Cabling Scheme] ドロップダウンリストで、スタックのケーブル配線スキームを選択します。

この項目は、スタック構成をサポートしているスイッチが次のいずれかのケーブル配線スキームに従って接続されている場合にのみ表示されます。

図 *1:* ケーブル配線スキーム

g) （オプション）スタックの番号を付け直す場合は、[Select a Top of Stack serial Number] ドロップダウンリストで、スタックスイッチの先頭のシリアル番号を選択します。

この項目は、スタック構成をサポートしているスイッチが図のように接続されている場合にのみ表示されます。

h) （任意）[Select a License Level] ドロップダウンリストで、スタックのライセンスレベルを選択します。

この項目は、スタック構成をサポートしているスイッチにのみ表示されます。

i) 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

ステップ 10 プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 11 **[Next]** をクリックします。

[Provision Templates] ウィンドウが表示されます。ここでは、テンプレートに定義されたパラメータの値を指定できます。

ステップ 12 設定するデバイスの名前をクリックし、次の手順を実行します。

a) デバイスに設定テンプレートが割り当てられている場合は、テンプレートで定義されたパラメータの値を指定します。

各デバイスのフィールドに各パラメータの値を入力します。赤のアスタリスクは、必須フィールドを示します。

b) 選択したデバイスの起動設定に実行中の設定をコピーしたい場合、[Copy running config to startup config] チェックボックスをオンにします。

c) 複数のデバイスを選択してプロビジョニングした場合は、ウィンドウの左側にあるリストで次のデバイスをクリックし、パラメータ値を入力します。これを、すべてのデバイスに対して実行します。

ステップ 13 すべてのデバイスのパラメータ値を一括で指定するには、次の手順を実行します。

a) [Export] をクリックして、CSV テンプレートファイルを保存します。

b) 各パラメータの値をファイルに追加して、ファイルを保存します。
c) [Import] をクリックします。
d) 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 ドロップするか、**[click to select]** と表示されている場所をクリックしてファイルを選択します。
e) [Import] をクリックします。

ステップ 14 [Next] をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 15 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。「テンプレートのプロビジョニング」手順に戻ってパラメータ値やテンプレートを変更したり、[Design] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] オプションボタンをクリックし、[OK] をクリックします。

ステップ 16 Day-0 Config 列のリンクをクリックして、デバイス、その設定、設定プレビューエラーの詳細を確認することができます。

ステップ 17 [要求（Claim）] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 18 [Yes] をクリックしてデバイスを要求します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary]には、デバイスにプッシュされる残りのネットワーク設定が表示されます。詳細については、デバイスのプロビジョニング （29 ページ）を参照してください。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイプロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS Cisco DNA Center の AAA クライアントとして ISE に追加されます (これらが設定されている場合)。

ワイヤレスまたはセンサー デバイスのプロビジョニング

デバイスに設定を割り当て、それをインベントリに追加してワイヤレスデバイスを要求すると、プロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

（注） あるデバイスについてデバイスの可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加された、またはサイトに割り当てられたときに、追加の設定がデバイスにプッシュされます。詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください。

この手順では、[プラグアンドプレイデバイス（Plug And Play Devices）]リストからデバイスを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Network Plug and Play Troubleshooting Guide for Cisco DNA Center』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、「コントローラ ディスカバリの前提条件 （4 ページ）」を参照してください。
- ネットワーク階層内のサイトを定義します。ネットワーク階層についてを参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。デバイス クレデンシャルについてを参照してください。
- ワイヤレス アクセス ポイント デバイスをプロビジョニングするには、ワイヤレス アクセス ポイントを管理しているワイヤレス LAN コントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。これは、Mobility Express アクセスポイントでは必要ありません。
- 必要に応じて、イメージを展開する場合は、プロビジョニングされる Cisco Catalyst 9800-CL デバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。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。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ導入後でデバイスイメージの更新時に使用されるプロセスと同じではありません。これは ソフトウェア イメージのプロビジョニング で説明されています。プラグアンドプレイ プロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- センサー デバイスをプロビジョニングするには、センサーが Cisco DNA Center エンタープライズ IP アドレス（private/enp9s0）を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが Cisco DNA Center の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス enp9s0 IP アドレスから到達可能である必要があります。DHCP サーバで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80」を使用して、NTP サーバ（DHCP オプション 42）とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は enp9s0 インターフェイスに関連付けられた Cisco DNA Center の仮想 IP アドレスです。
- ワイヤレス アクセス ポイント デバイスのワイヤレス無線周波数プロファイルを定義します（Mobility Express アクセスポイントを除く）。「ワイヤレス無線周波数プロファイルの作成」を参照してください。
- Mobility Express アクセスポイントの場合は、IP アドレスプールと管理インターフェイスを定義します。IP アドレス プールを設定する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**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のワイヤレスデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス表の上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスクレデンシャルの定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスクレデンシャルを定義する必要があります。これらは要求プロセスの前提条件であり、これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （任意） 必要に応じて、最初の列のデバイス名を変更します。

ステップ 6 （任意） 必要に応じて、2 番目の列のデバイスタイプを変更します。デバイスが使用しているモードに応じて、AP（アクセスポイント）または ME（Mobility Express）を選択できます。

誤ったモードを選択すると、デバイスのプロビジョニングエラーにつながります。この項目は、ワイヤレス LAN コントローラやセンサーデバイスには表示されません。

ステップ 7 [サイトの選択（Select a Site）] ドロップダウンリストから、各デバイスに割り当てるサイトとフロアを選択します。アクセスポイントデバイスは、ワイヤレスコントローラを備えたフロアに割り当てる必要があります。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。ワイヤレスデバイスは、ビルディング自体ではなくビルディング内のフロアにのみ割り当てることができます。

ステップ 8 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 9 （任意）テーブルに表示される列を変更するには、テーブル見出しの右端にある 3 つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 10 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （任意）[デバイス名（Device Name）] フィールドで、必要に応じてデバイス名を変更します。
c) アクセスポイントデバイスの場合、[Radio Frequency Profile] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1 つのプロファイルをデフォルトとして指定した場合に設定できます。
d) ワイヤレス LAN コントローラの場合、次のフィールドに値を入力します。[Management IP]、[Subnet Mask]、[Gateway]、[IP Interface Name]、また任意で [VLAN ID]。
e) Mobility Express デバイスの場合は、[Wireless management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。
f) ワイヤレスセンサーデバイスの場合、[Sensor Settings] ドロップダウンリストで、デバイスに適用するセンサーデバイスプロファイル（バックホール）を選択します。

（注） ソフトウェアリリース 1.3.1.2 よりも古い Cisco Aironet 1800s アクティブセンサの場合は、センサデバイスプロファイル **CiscoProvisioningSSID** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。

g) 変更した場合は、[保存（Save）] をクリックします。それ以外の場合は、[キャンセル（Cancel）] をクリックしてリストに戻り、他のデバイスを設定します。
h) **[アクション（Actions）]** 列の **[他のデバイスに...を適用（Apply … to Other Devices）]** をクリックして、あるデバイスに割り当てた設定を同じタイプの他のデバイスに適用できます。

ステップ 11 デバイスが Cisco Catalyst 9800-CL ワイヤレスコントローラの場合は、[Configuration] 列の [Image] の横にある [Assign] をクリックし、次の手順を実行します。

a) （オプション）[イメージ（Image）] ドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。
b) [**保存（Save**）] をクリックします。

ステップ 12 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスに**[割り当て（Assign）]**をクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 13 **[Next]** をクリックします。
[概要（Summary）] ウィンドウが表示されます。ここで、デバイスや設定に関する詳細を確認できます。

ステップ 14 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。[割り当ての設定（Assign Configuration）] 手順に戻って設定を変更したり、[設計（Design）] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] オプションボタンをクリックし、[OK] をクリックします。デバイスを管理しているワイヤレス LAN コントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。

ステップ 15 [要求（Claim）] をクリックします。
確認のダイアログボックスが表示されます。

ステップ 16 **[はい（Yes）]** をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary]には、デバイスにプッシュされる残りのネットワーク設定が表示されます。詳細については、デバイスのプロビジョニング （29 ページ）を参照してください。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイ プロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS Cisco DNA Center の AAA クライアントとして ISE に追加されます (これらが設定されている場合)。

Cisco DNA トラフィック テレメトリ アプライアンス のプロビジョニング

この手順では、[Plug And Play Devices] リストから Cisco DNA トラフィック テレメトリ アプライアンス を要求する方法について説明します。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Cisco Digital Network Architecture Center のネットワーク プ

ラグアンドプレイのトラブルシューティング ガイド[英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。

- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。
- ネットワーク階層内のサイトを定義します。ネットワーク階層についてを参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。SNMPv2c を使用している場合は、読み取りと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。「デバイス クレデンシャルについて」を参照してください。

（注） SNMPv3 の制限事項：

- 認証用の SHA とプライバシー用の AES128 がサポートされています。
- MD5 はサポートされていません。

- イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージがアップロードされていて、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。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。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ展開プロセスは、後でデバイスイメージの更新時に使用される展開プロセスとは異なります。詳細については、ソフトウェア イメージのプロビジョニングを参照してください。プロビジョニング中、プラグアンドプレイではデバイスの事前チェック、自動フラッシュクリーンアップ、または事後チェックは実行されません。デバイスは工場出荷時の初期状態である必要があります。

- デバイスのネットワークプロファイルを定義します。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**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] または [Find] オプションを使用して、Cisco DNA トラフィック テレメトリ アプライアンス を見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[Actions] > [Claim] をクリックします。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスログイン情報の定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスログイン情報を定義する必要があります。これらの必須タスクは、要求プロセスの前提条件です。これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （任意） 必要に応じて、最初の列のデバイスのホスト名を変更します。

ステップ 6 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトを選択します。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。

ステップ 7 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 8 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （任意） [Device Name] フィールドで、必要に応じてデバイスのホスト名を変更します。
c) （任意） [Image] ドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。
d) 何らかの変更を行った場合は、[Save] をクリックします。変更していない場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

ステップ 9 プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] をクリックします。すべてのデバイスを設定するまで、設定手順を繰り返します。

ステップ 10 [Next] をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 11 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要のあるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。プロビジョニングエラーを回避するには、デバイスを要求する前に問題を解決する必要があります。場合によっては、[Design] 領域に再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりする必要があります。問題を解決したら、このタブに戻り、[Retrying getting Day-0 configuration preview for failed device(s)] オプションボタンをクリックします。次に [OK] をクリックします。

ステップ 12 Day-0 Config 列のリンクをクリックして、デバイス、その設定、設定プレビューエラーの詳細を確認することができます。

ステップ 13 [要求（Claim）] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 14 [Yes] をクリックしてデバイスを要求します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認できます。詳細については、デバイスのプロビジョニング（29ページ）を参照してください。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイプロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。

デバイスの削除

デバイスを削除すると、デバイスはプラグアンドプレイのデータベースから削除されますが、リセットはされません。エラー状態のデバイスをリセットする場合は、[Reset] を使用します。

この手順では、[Plug and Play Devices] リストからデバイスを削除する方法を示します。代わりに、[削除（Delete）] をクリックしてデバイスの詳細ウィンドウからデバイスを削除することもできます。

（注） デバイスがプロビジョニングの状態の場合は、[Inventory] タブからのみ削除できます。

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**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 削除する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[アクション（Actions）] > [削除（Delete）] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 5 [Yes] クリックして、このデバイスを削除することを確認します。

デバイスのリセット

デバイスのリセットはエラー状態のデバイスにのみ適用され、状態が [Unclaimed] にリセットされデバイスがリロードされますが、プラグアンドプレイ データベースからは削除されません。デバイスを削除する場合は、**[Ddelete]** を使用します。

（注） デバイスで保存された設定が工場出荷時のデフォルトまたは同様の最小限の設定である場合、このオプションを選択すると、デバイスはプロビジョニングプロセスを再起動します。ただし、デバイスに以前に保存されたスタートアップ コンフィギュレーションがある場合は、これによってデバイスのプロビジョニングプロセスの再起動を回避できますが、工場出荷時のデフォルトにリセットする必要があります。ワイヤレスデバイスおよびセンサーデバイスでは、デバイスの状態だけがリセットされ、デバイスはリロードされません。

この手順では、[Plug and Play Devices] リストからデバイスをリセットする方法を示します。代わりに、[Reset] をクリックしてデバイスの詳細ウィンドウからリセット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**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 リセットする 1 個以上のデバイスの横にあるチェック ボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、**[Actions（アクション）] > [Reset（リセット）]** をクリックします。

確認のダイアログボックスが表示されます。

ステップ 5 次のいずれかのオプションを選択します。

- [Reset and keep current claim parameters]：現在の請求パラメータが維持され、デバイスは [Planned] 状態になります。
- [Reset and remove all claim parameters]：現在の請求パラメータを削除し、デバイスが [Unclaimed] 状態になります。

ステップ 6 [**リセット（Reset）**] をクリックします。

デバイスのプロビジョニング

次のセクションでは、さまざまなシスコデバイスをプロビジョニングする方法について説明します。

ワイヤレスデバイスと国コードについて

コントローラおよびアクセスポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセスポイント内の無線は、製造時に特定の規制ドメインに割り当てられています（ヨーロッパの場合はEなど）が、国コードを使用すると、規制ドメイン内で稼働する特定の国を指定できます（フランスの場合はFR、スペインの場合はESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

Cisco DNA Center は、割り当てられたサイトに応じて、国コードを使用してコントローラをプロビジョニングします。コントローラの場合は、複数のサイトに割り当てることができます。そのため、複数の国コードを割り当てることができます。Cisco DNA Center は、プロビジョニング中に、サイトをサイトの国コードとともにコントローラに割り当てます。たとえば、インドと米国の両方のサイトを管理するコントローラには、IN と US の国コードが割り当てられます。

アクセスポイントは、プロビジョニングされると、フロアに割り当てられます。アクセスポイントが ROW AP の場合、Cisco DNA Center は、サイトの国コードを取得して AP に割り当てます。同じフロア上の追加の AP には、同じ国コードが割り当てられます。

国コード情報は、コントローラとアクセスポイントのデバイス 360 ページに表示されます。

サポートされている国コードの製品ごとの完全なリストについては、https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html を参照してください。

Cisco AireOS コントローラのプロビジョニング

始める前に

- シスコ ワイヤレス コントローラ をプロビジョニングする前に、次のグローバル ネットワーク設定を定義したことを確認します。
  - AAA、DHCP、および DNS 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 サーバーの設定を参照してください。
  - CLI、SNMP、HTTP、HTTPS 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、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、およびグローバル HTTPS クレデンシャルの設定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」を参照してください。
  - SSID、ワイヤレス インターフェイス、およびワイヤレス無線周波数プロファイルなどのワイヤレス設定です。

    詳細については、「グローバル ワイヤレス設定の構成」を参照してください。

- インベントリに シスコ ワイヤレス コントローラがあることを確認します。ない場合は、[Discovery] 機能を使用してコントローラを検出します。
- サイトに シスコ ワイヤレス コントローラ が追加されたことを確認してください。詳細については、デバイスをサイトに追加するを参照してください。
- デバイスで既存の VLAN を再利用することはできません。デバイスにすでに存在する同じ VLAN を Cisco DNA Center がプッシュすると、プロビジョニングは失敗します。
- Cisco DNA Center によって管理されている ワイヤレスコントローラ の設定に手動で変更を加えることはできません。Cisco DNA Center GUI からすべての設定を実行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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [DEVICE TYPE] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能な ワイヤレスコントローラ のリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 6 [Choose a site] をクリックして ワイヤレスコントローラ にサイトを割り当てます。

ステップ 7 [Add Sites] ウィンドウで、ワイヤレスコントローラを関連付けるサイト名の横にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 8 [Apply] をクリックします。

ステップ 9 **[次へ (Next)]** をクリックします。

[設定（Configuration）] ウィンドウが表示されます。

ステップ 10 ワイヤレスコントローラのロールを選択します（[Active Main WLC] または [Guest Anchor WLC]）。

ステップ 11 [Select Primary Managed AP Locations] をクリックして、ワイヤレスコントローラ の管理 AP の場所を選択します。

ステップ 12 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。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、親サイトの下にある子は自動的に選択されます。

（注） 管理 AP の場所を継承することで、サイトをその下のビルディングやフロアとともに自動で選択できます。1 つの ワイヤレスコントローラ で管理できるのは 1 つのサイトのみです。

ステップ 13 **[Save]** をクリックします。

ステップ 14 [Interface and VLAN Configuration] で [+ Add] をクリックして、アクティブメイン ワイヤレスコントローラ のインターフェイスと VLAN の詳細を設定します。

インターフェイスおよび VLAN の設定は、非ファブリックの ワイヤレスコントローラ プロビジョニングにのみ適用できます。

[インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウが表示されます。

ステップ 15 [インターフェイス名（Interface Name）] ドロップダウン リストからインターフェイス名を選択します。

ステップ 16 [VLAN ID] フィールドに、VLAN の値を入力します。

ステップ 17 [Interface IP Address] フィールドに、インターフェイス IP アドレスの値を入力します。

ステップ 18 [Interface Net Mask (in bits)] フィールドに、インターフェイスのサブネットマスクを入力します。

ステップ 19 [Gateway IP Address] フィールドにゲートウェイ IP アドレスを入力します。

ステップ 20 [LAG/Port Number] ドロップダウンリストから、リンク集約またはポート番号を選択します。

ステップ 21 [OK] をクリックします。

ステップ 22 （オプション）ゲスト アンカー ワイヤレスコントローラ の場合、[Assign Guest SSIDs to DMZ site] で [VLAN ID] を変更して、VLAN ID 設定を変更します。

ステップ 23 [Mobility Group] で [Configure] をクリックして、ワイヤレスコントローラをモビリティピアとして設定します。

[Configure Mobility Group] サイドパネルが表示されます。

ステップ 24 [Mobility Group Name] ドロップダウンリストで、[+] をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択します。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 25 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 26 [Mobility Peers] で [Add] をクリックして、ワイヤレスコントローラをモビリティピアとして設定します。

ステップ 27 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 28 **[Save]** をクリックします。

ステップ 29 モビリティグループ名と RF グループ名をリセットするには、次のいずれかを実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > **[Configuration]** ページの [Mobility Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

ステップ 30 [Next] をクリックします。

[Model Configuration] ウィンドウが表示されます。

ステップ 31 [Devices] ペインで、[Find] フィールドにモデル設定設計の名前を入力して検索するか、デバイスを展開してモデル設定設計を選択します。

選択したモデル設定設計が右側のペインに表示されます。

ステップ 32 プロビジョニングするモデル設定設計の [Design Name] の横にあるチェックボックスをオンにし、[Configure] をクリックして編集します。

この手順では、すべての設定を編集することはできません。

ステップ 33 必要な変更を加えて、[Apply] をクリックします。

ステップ 34 [Next] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 35 [Devices] パネルでデバイスまたはテンプレートを検索します。

ステップ 36 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力します。

ステップ 37 [Next] をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **Device Details**
- **ネットワーク設定**
- **SSID**
- **Managed Sites**
- **Interfaces**
- **Advanced Configuration**
- **モビリティ グループの設定**
- **モデル設定**

ステップ 38 [Deploy] をクリックして、コントローラをプロビジョニングします。

ステップ 39 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] メッセージで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] メッセージが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。

- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

  （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 40 セカンダリコントローラをプロビジョニングします。

ステップ 41 展開が正常に完了すると、[Device Inventory] ウィンドウの [Status] 列に「SUCCESS」と表示されます。

プロビジョニング後に何らかの変更を行う場合は、[Design] をクリックしてサイトのプロファイルを変更し、もう一度 ワイヤレスコントローラ をプロビジョニングします。

ステップ 42 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 43 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、実行する必要があるアクションのリストを表示します。

ステップ 44 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 45 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 46 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。

[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも表示されます。

ステップ 47 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

Cisco DNA Center からのシスコ ワイヤレス コントローラの高可用性の設定

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

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

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の検出機能とインベントリ機能が正常である必要があります。デバイスが [Managed] 状態になっている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 のサービスポートと管理ポートが設定されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長ポートが物理的に接続されている必要があります。

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の管理アドレスが同じサブネット内にある必要があります。ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長管理アドレスも同じサブネット内にある必要があります。
- ワイヤレスコントローラで次のブート変数を手動で設定します。

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

show boot.  (IOSXE cli)

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

シスコ ワイヤレス コントローラ HA の設定

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

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとして設定するコントローラ名の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] ページが表示されます。

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

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

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

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

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

ステップ 8 [Wireless Info] タブをクリックします。

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

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

高可用性プロセス中および完了後に起こること

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

高可用性を設定および確認するためのコマンド

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

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

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

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

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

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

- HA 関連の詳細情報を確認する場合：**config redundancy mode sso**

- 設定済みのインターフェイスを確認する場合：**show redundancy summary**

Cisco DNA Center からの高可用性設定済みブラウンフィールドデバイスの無効化

Cisco DNA Center の高可用性無効化機能は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ と Cisco AireOS コントローラでサポートされています。

始める前に

高可用性ブラウンフィールドデバイスが Cisco DNA Center の外部で設定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**[Provision]** > **[Device]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 無効にする高可用性機能を持つワイヤレスコントローラの名前の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] ページが表示されます。

[High Availability] ページには、Cisco DNA Center の外部から設定された、選択されたワイヤレスコントローラの**冗長性の概要**が表示されます。

ステップ 4 **[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

選択されたワイヤレスコントローラの高可用性が正常に無効になったことを示す成功メッセージが画面の下部に表示されます。

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

始める前に

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。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。詳細については、ネットワークの検出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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

（注） 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することがします。選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

デバイスファミリや到達可能性ステータスなどのさまざまな基準に基づいてデバイスをフィルタ処理するには、[Filter] をクリックして、必要な選択を行い、[Apply] をクリックします。

ステップ 2 プロビジョニングする AP の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 4 [Assign Site] ステップで、次のパラメータを設定します。

a) [Choose a floor] をクリックし、サイトに AP を割り当てます。
b) [Choose a Floor] スライドインペインで、AP が存在するフロアを選択し、[Save] をクリックします。
c) [Next] をクリックします。

ステップ 5 [Configuration] ステップで、次のパラメータを設定します。

a) [Advanced Configuration] をクリックして、アンテナスロットの無線アンテナプロファイルを設定します。

（注） 高度な設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア リリース 17.6 以降を搭載した Cisco Catalyst 9130AXE ユニファイド アクセス ポイントでサポートされています。

b) [Slot 1] および [Slot 2] ドロップダウンリストから、AP 無線スロット 1 およびスロット 2 のビーム選択値を設定します。
c) [**保存（Save）**] をクリックします。
d) [RF Profile] ドロップダウンリストで、デフォルト設定をそのままにするか、リストから別の値を選択します。オプションは、**高**、**標準**、**低**です。

デフォルトの RF プロファイルは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Wireless Radio Frequency Profile]** でデフォルトとマークしたカスタムプロファイルです。

e) [Mesh Role] ドロップダウンリストで、[Root] または [Mesh] を選択します。
f) [Next] をクリックします。

ステップ 6 [Summary] ステップでデバイスの詳細を確認し、[Deploy] をクリックして AP をプロビジョニングします。

[Provision Device] スライドインペインが表示されます。

ステップ 7 [Provision Device] スライドインペインで、次の手順を実行します。

- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- CLI 設定をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックします。

ステップ 8 AP グループの作成または変更が進行中であることを示すメッセージに続き、プロビジョニング後に AP がリブートすることを示すメッセージが表示されます。[OK] をクリックします。

展開が正常に完了した場合、[Inventory] ウィンドウの [Last Sync Status] 列に「SUCCESS」と表示されます。

FlexConnect モードの AP への ICMP ping の有効化

到達不能状態にある FlexConnect モードの AP への Internet Control Message Protocol（ICMP）ping を有効にすることができます。Cisco DNA Center は、ICMP を使用して、到達不能状態にある FlexConnect AP への ping を 5 分ごとに実行することで到達可能性を強化してから、[Inventory] ウィンドウの到達可能性ステータスを更新します。

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

ステップ 2 [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにして ICMP ping を有効にします。

ステップ 3 [保存（**Save**）] をクリックします。

「ICMP Ping status updated successfully」という成功メッセージが表示されます。

Cisco DNA Center は、シスコ ワイヤレス コントローラとの関連付けは解除されているが到達可能な FlexConnect AP への ping を開始します。到達可能性ステータスは [Inventory] ウィンドウで確認できます。

ステップ 4 到達可能性ステータスを確認するには、**[Provision]** > **[Inventory]** を選択します。

ステップ 5 デバイスが ICMP ping によって到達可能である場合、[Reachabilty] 列に [Ping Reachable] と表示されます。

Cisco AireOS Mobility Express AP の Day 0 ワークフロー

始める前に

Cisco Mobility Express ワイヤレス ネットワーク ソリューションは、1 つ以上の 802.11ac Wave 2 Cisco Aironet シリーズのアクセスポイント（AP）と、ネットワーク内のその他の AP を管理する内蔵ソフトウェアベースの ワイヤレスコントローラ で構成されます。ワイヤレスコントローラ として機能している AP をプライマリ AP といい、このプライマリ AP によって管理される Cisco Mobility Express ネットワーク内のその他の AP を下位 AP といいます。

- 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、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、およびグローバル SNMPv3 クレデンシャルの設定を参照してください。
- WLAN、インターフェイス、RF プロファイルを作成します。

- DHCP サーバーにオプション #43 とオプション #60 を設定します。これは Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。これを使用して、AP は PnP サーバーに接続し、設定をダウンロードします。
- インベントリに Mobility Express AP があることを確認してください。ない場合は、ディスカバリ機能を使用して検出します。詳細については、CDP を使用したネットワークの検出、IP アドレス範囲を使用したネットワークの検出、およびインベントリについてを参照してください。
- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

ステップ 1 Cisco Mobility Express は DHCP サーバーに接続し、Cisco DNA Center プラグアンドプレイサーバーに接続します。

ステップ 2 DHCP サーバーは、オプション #43 を使用して IP アドレスを割り当てます。オプション #43 は、 Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。

ステップ 3 Mobility Express AP は PnP エージェントを開始し、PnP サーバーに接続します。

（注） ネットワーク内に一連の Mobility Express AP がある場合、内部プロトコルを通過します。プロトコルは 1 つの Mobility Express AP を選択します。これは、シスコ ワイヤレス コントローラ で、PnP サーバーに到達するためのプライマリ AP として設定されます。

ステップ 4 [Provision] > [Devices] > [Plug and Play] タブで未要求 AP を検索します。 > >

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onbording Status] が [Initialized] になるまで待機する必要があります。

ステップ 5 この AP を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 6 デバイステーブルの上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

[Claim Devices] ウィンドウが表示されます。

ステップ 7 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 10 [Configuration for device name] ページで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 11 [Save] をクリックします。

ステップ 12 [Next] をクリックします。

[Summary] ページが表示されます。

ステップ 13 [Summary] ページで [Claim] をクリックします。

Mobility Express AP が要求されると、設定された IP アドレスが Mobility Express AP に割り当てられます。

ステップ 14 要求されたデバイス（AP）と ワイヤレスコントローラ は、**[Provision]** > **[Device Inventory]** > **[Inventory]** ページで確認できるようになりました。

ステップ 15 また、CSV ファイルからデバイスを一括して追加することもできます。

詳細については、「デバイスの一括追加 （13 ページ）」を参照してください。

CSV を使用して Mobility Express AP を一括インポートすると、すべての Mobility Express AP が **[Device]** > **[Plug and Play]** ページに表示されます。VRRP プロトコルに基づいて、インポートされた Mobility Express AP のうち 1 台だけがプライマリ AP になって要求に応じ、残りは下位 AP になります。プライマリ AP を要求した後、下位 AP を要求する必要はありません。Cisco DNA Center は、[Plug and Play] ページから下位 AP をクリアしません。これらの下位 AP は、**[Devices]** > **[Plug and Play]**ページから手動で削除する必要があります。

ステップ 16 シスコ ワイヤレス コントローラ をプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （30 ページ） を参照してください。

ステップ 17 AP をプロビジョニングするには、#unique_185 を参照してください。

Cisco AireOS コントローラのためのブラウンフィールドのサポート

始める前に

Cisco DNA Center を使用すると、シスコ ワイヤレス コントローラなどのブラウンフィールド デバイスをネットワークに追加してプロビジョニングできます。ブラウンフィールドとは、既存サイトの以前から存在しているインフラストラクチャに属しているデバイスのことです。

この手順では、Cisco DNA Center を使用して、ブラウンフィールド Cisco AireOS コントローラをプロビジョニングする方法を示します。

- 初めに、デバイスについてディスカバリを実行します。すべてのデバイスが [インベントリ（Inventory）] ウィンドウに表示されます。詳細については、ネットワークの検出およびインベントリについてを参照してください。
- ワイヤレスコントローラ は到達可能で、 [インベントリ（Inventory）] ウィンドウで管理状態でなければなりません。詳細については、インベントリについて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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 [フィルタ（Filter）] をクリックして、選択したフィルタ フィールドに適切な値を入力します。たとえば、[デバイス名（Device Name）] フィルタの場合、デバイスの名前を入力します。

[デバイス（Devices）] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 3 プロビジョニングする ワイヤレスコントローラ デバイス名の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択します。

ステップ 5 [Assign Site] ステップで、サイトをコントローラに関連付けます。

a) [Choose a site] をクリックして、コントローラにサイトを割り当てます。

b) [Choose a site] スライドインペインで、ワイヤレスコントローラ を関連付けるサイトを選択し、[Save] をクリックします。

c) [Next] をクリックします。

ステップ 6 [Resolve Conflict] ステップに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。

ステップ 7 [Next]をクリックします。

ステップ 8 [Design Object] ウィンドウに、学習したすべての設定が一覧表示されます。

a) 左ペインで [Network] をクリックします。

右側のペインに、デバイス設定学習の一部として学習されたネットワーク設定と、次の情報が表示されます。

- **[** AAA サーバー（AAA Server） **]** の詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。
- [DHCP Server] の詳細。
- AAA サーバーの共有秘密を入力します。

b) 左ペインで [ワイヤレス（Wireless）] をクリックします。

右側のペインには、企業 SSID、ゲスト SSID、アンテナ無線プロファイル、およびワイヤレスインターフェイスの詳細が一覧表示されます。

事前共有キー（PSK）を使用する SSID の場合、事前共有キーを入力します。

c) 左ペインで [破棄された設定（Discarded Config）] をクリックします。

右ペインに、Cisco DNA Center 上で競合する設定、または既に存在する設定が一覧表示されます。破棄された設定エントリは、次のように分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイス設定

d) [Next]をクリックします。

[ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

e) **[Save]** をクリックします。

「ブラウンフィールド設定に成功しました（`Brownfield Configuration is Successful`）」というメッセージが表示されます。

ステップ 9 **[Design]** > **[Network Profile]** を選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 10 [Network Profiles] ウィンドウで、次の項目を設定します。

a) [Assign Site] をクリックして、選択したプロファイルにサイトを追加します。

b) [サイトをプロファイルに追加（Add Sites to Profile）] ウィンドウでドロップダウンリストからサイトを選択して、[保存（Save）] をクリックします。

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。

a) [Filter] をクリックして、プロビジョニングするデバイスを見つけます。

[デバイス（Devices）] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

b) プロビジョニングするコントローラ デバイス名の隣にあるチェック ボックスをオンにします。

c) [アクション（Actions）] ドロップダウン リストから、[プロビジョニング（Provision）]を選択します。

d) [サイトの割り当て（Assign Site）] ウィンドウで詳細を確認して、[次へ（Next）] をクリックします。

[Configurations] ステップが表示されます。

e) [インターフェイスと VLAN の設定（Interface and VLAN Configuration）] で、[+ 追加（+ Add）] をクリックしてインターフェイスと VLAN の詳細を設定します。

f) [インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。

g) [Next] をクリックします。

ステップ 12 次の情報が表示される [Summary] ステップを確認します。

- **Device Details**
- **ネットワークの設定**
- **SSID**
- **Managed Sites**
- **Interfaces**

ステップ 13 [展開（Deploy）] をクリックします。

ステップ 14 [Provision Devices] スライドインペインで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。

- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

（注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク用に構築された次世代のワイヤレスコントローラです。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Cisco IOS XE ベースであり、Aironet の優れた RF 性能と Cisco IOS XE のインテントベースのネットワーキング機能を統合して、組織にクラス最高水準のワイヤレスエクスペリエンスを生み出します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラはモジュール型オペレーティングシステムに基づいて構築され、オープンでプログラマブルな API 機能が搭載されていて、0 日目から N 日目のネットワーク運用を自動化できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、次のような複数のフォームファクタで使用できます。

- Catalyst 9800-40 ワイヤレスコントローラ。
- Catalyst 9800-80 ワイヤレスコントローラ。
- Catalyst 9800-CL Cloud ワイヤレスコントローラ：プライベートクラウド（ESXi、KVM、Cisco ENCS、および Hyper-V）に展開可能、Cisco DNA Center で管理可能。

- Catalyst 9300 シリーズ スイッチ、Catalyst 9400 シリーズ スイッチ、および Catalyst 9500H シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ。
- Cisco Catalyst 9800-L ワイヤレスコントローラ：中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされている仮想プラットフォームおよびハードウェア プラットフォームを一覧表示します。

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレスコントローラ	最大 6000 アクセスポイントと 64,000 クライアントをサポートします。 最大 80 Gbps のスループットをサポートし、2 ラックユニットスペースを使用します。 最大 100-GE のアップリンクおよびシームレスなソフトウェアアップデートを搭載したモジュール型ワイヤレスコントローラ。
Cisco Catalyst 9800-40 ワイヤレスコントローラ	シームレスなソフトウェアアップデートを備えた、中小企業やキャンパスでの導入向けの固定ワイヤレスコントローラ。 最大 2000 アクセスポイントと 32,000 クライアントをサポートします。 最大 40 Gbps のスループットをサポートし、1 ラックユニットスペースを使用します。 4 つの 1-GE または 10-GE アップリンクポートを提供します。
Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ	Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、プライベートクラウドまたはパブリッククラウドに Infrastructure as a Service（IaaS）として導入できます。 Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、ハイアベイラビリティとセキュリティを実現するために構築された次世代のエンタープライズクラスの仮想ワイヤレスコントローラです。 Cisco Catalyst 9800-CL クラウド ワイヤレスコントローラの仮想フォームファクタは、ESXi、KVM、Cisco ENCS、および Hyper-V ハイパーバイザをサポートするプライベートクラウド向けです。
Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ	Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラは、有線およびワイヤレス インフラストラクチャを一貫したポリシーと管理とともに提供します。 この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションである Cisco SD-Access でのみサポートされます。組み込みコントローラは、ファブリックモードでのみアクセスポイント（AP）をサポートします。

プラットフォーム	説明
Cisco Catalyst 9800-L ワイヤレス コントローラ	Cisco Catalyst 9800-L ワイヤレスコントローラは、中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。 • Cisco Catalyst 9800-L Copper シリーズ ワイヤレス コントローラ（9800-L-C RJ45） • Cisco Catalyst 9800-L ファイバ シリーズ ワイヤレス コントローラ（9800-L-F SFP）

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされているホスト環境を一覧表示します。

ホスト環境	ソフトウェア バージョン
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5[1] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Red Hat Enterprise Linux 7.1 および 7.2 をベースとした Linux KVM • Ubuntu 14.04.5 LTS、Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 および 3.9.1

[1] ESXi vSphere を使用した C9800-CL の .ova ファイルのインストールは機能しません。これは C9800 ova に限定されませんが、他の製品に影響します。シスコと VMware は、問題解決に向けて積極的に取り組んでいます。問題が修正されたかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。VMware 6.5 および C9800-CL OVA ファイルの展開に固有の問題があります。「必要なディスクイメージがありません。（A required disk image was missing）」という警告が表示され、「VM の展開に失敗しました：postNFCData に失敗しました：ディスク以外のファイルに POST できません。（Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files.）」というエラーで展開が失敗します。VMware ESXi 6.5 に C9800-CL をインストールするには、次のいずれかを実行します。1）ESXi 組み込み GUI を使用して C9800-CL の .iso ファイルをインストールする（ESXI 6.5 クライアントバージョン 1.29.0 はテスト済みで必須）。2）OVF ツールを使用して C9800-CL の .ova ファイルをインストールする。

次の表に、Cisco DNA Center でサポートされている Cisco Enterprise Network Function Virtualization Infrastructure Software（NFVIS）のバージョンを示します。

（注） Cisco Enterprise NFVIS デバイスは、N-1 から N へのアップグレードパスのみをサポートします。たとえば、Cisco Enterprise NFVIS 3.11.x からは Cisco Enterprise NFVIS 3.12.x へのアップグレードのみがサポートされています。Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 4.1.x へのアップグレードはサポートされていません。

Cisco Enterprise NFVIS バージョン	エンタープライズ ネットワーク コンピューティング システム デバイス プラットフォーム	注記
4.1.2 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	Cisco DNA Center は、次の NFVIS アップグレードパスをサポートします。NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2。 Cisco Enterprise NFVIS 3.12.1 は、Cisco DNA Center のいずれのバージョンでもサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 3.12.1 へのアップグレードはサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.12.1 から Cisco Enterprise NFVIS 3.12.2 へのアップグレードはサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.11.2 から 3.12.2 へのアップグレードはサポートされていません。 Cisco Enterprise NFVIS 3.12.2 は、Cisco DNA Center でサポートされています。
3.12.2 3.11.3 3.11.2 3.11.1	ENCS 5100	Cisco 5100 ENCS は、Cisco Enterprise NFVIS 3.10.x をサポートしていません。

Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、『CISCO DNA Center インストール ガイド』を参照してください。

2. ソフトウェアイメージのアップグレードに関する詳細については、Cisco Catalyst 9800 シリーズワイヤレスコントローラでのソフトウェアイメージのアップグレードのサポート（51 ページ） を参照してください。

3. Cisco DNA Center GUI にログインし、必要なアプリケーションが [Running] 状態であることを確認します。

   Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[System Settings]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

4. Cisco Identity Services Engine と Cisco DNA Center を連動させます。統合後、関連する設定やデータとともに Cisco DNA Center が検出されたデバイスは、Cisco ISEにプッシュされます。

5. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

   詳細については、CDP を使用したネットワークの検出またはIP アドレス範囲を使用したネットワークの検出を参照してください。

   ワイヤレス管理 IP アドレスを手動で追加する必要があります。

   [Discovery] ウィンドウで Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して検出を実行する場合は、[Preferred Management IP] ドロップダウンリストから [Use Loopback] を選択して、デバイスのループバック インターフェイスの IP アドレスを指定します。

6. 検出されたデバイスが [Device Inventory] ページに [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

   デバイスが [Managed] 状態になるまで待機する必要があります。

7. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアシュアランス接続を確認するには、次のコマンドを使用します。

   - **#show crypto pki trustpoints | sec DNAC-CA**

   ```
   Trustpoint DNAC-CA
       Subject Name:
       cn=kube-ca
             Serial Number (hex): 00E***************
       Certificate configured.
   ```

   - **#show crypto pki trustpoints | sec sdn-network**

   ```
   Trustpoint sdn-network-infra-iwan:
       Subject Name:
       cn=sdn-network-infra-ca
   ```

```
        Serial Number (hex): 378***************
    Certificate configured.
```

- **#show telemetry ietf subscription all**

```
Telemetry subscription brief

  ID               Type        State       Filter type
  ------------------------------------------------------
  1011             Configured  Valid       tdl-uri
  1012             Configured  Valid       tdl-uri
  1013             Configured  Valid       tdl-uri
```

- **#show telemetry internal connection**

```
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------
IP address 25103 tls-native Active sdn-network-infra-iwan
```

- **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. 認証サーバーとポリシーサーバーの設定時に TACACS サーバーを設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでユーザー名をローカルに設定している場合、TACACS の設定は必須ではありません。

9. サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、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るようになります。

新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロードを参照してください。

新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

10. AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「AP の追加、配置、および削除」を参照してください。

11. AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

詳細については、グローバルネットワーク設定の管理、グローバル ネットワーク サーバーの設定、および「AAA サーバーの追加」を参照してください。

12. カスタムとして、親プロファイルでワイヤレス無線周波数プロファイルを作成します。

    詳細については、「ワイヤレス無線周波数プロファイルの作成」を参照してください。

13. IP アドレスプールをグローバルレベルで作成します。

    Cisco DNA Center Cisco DNA Center は、IP アドレスプールを使用して、SD-Access ネットワークの設定と展開を自動化します。

    IP アドレスプールを作成するには、IP アドレス プールを設定するを参照してください。

    プロビジョニングするビルディング用に IP アドレスプールを予約する必要があります。詳細については、「LAN アンダーレイのプロビジョニング」を参照してください。

14. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義します。次に、Cisco DNA Centerは地理的な場所全体でさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず SSID を作成し、次に作成した SSID をワイヤレス ネットワーク 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。

    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 の作成およびゲスト ワイヤレス ネットワークの SSID の作成を参照してください。その他のワイヤレス設定については、グローバル ワイヤレス設定の構成を参照してください。

15. バックホールの設定を行います。詳細については、「バックホールの設定の管理」を参照してください。

16. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの [Policy] ウィンドウで、次のように設定します。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、仮想ネットワークを参照してください。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加する。詳細については、「グループベースのアクセス コントロール ポリシーの作成」を参照してください。

17. 高可用性を設定します。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する （52 ページ）」を参照してください。

18. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （68 ページ）」を参照してください。

19. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアプリケーションポリシーを設定および展開します。

    詳細については、アプリケーション ポリシーの作成、アプリケーション ポリシーの展開、およびアプリケーション ポリシーの編集を参照してください。

（注） アプリケーションポリシーを展開する前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラデバイスをプロビジョニングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、2 つの異なる SSID で異なるビジネスとの関連性を持つ2つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは機能しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのソフトウェアイメージのアップグレードのサポート

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

  Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出するには、NETCONF を有効にしてポートを 830 に設定します。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。これにより、コントローラでワイヤレスサービスが有効になります。

  詳細については、CDP を使用したネットワークの検出またはIP アドレス範囲を使用したネットワークの検出を参照してください。

- デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

  詳細については、インベントリについておよびインベントリに関する情報の表示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]** > **[Image Repository]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 ローカルコンピュータまたは URL から、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェアイメージをインポートします。

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。

ステップ 3 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て」を参照してください。

ステップ 4 デバイスファミリまたは特定のデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークできます。

詳細については、「ゴールデン ソフトウェア イメージの指定」を参照してください。

ステップ 5 ソフトウェアイメージのプロビジョニング

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

ステップ 6 [Inventory] ウィンドウで、イメージをアップグレードする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の横にあるチェックボックスをオンにします。

ステップ 7 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** の順に選択します。

詳細については、ソフトウェア イメージのプロビジョニングを参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性（HA）を設定するには、次の前提条件を満たす必要があります。

- 両方の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスが同じソフトウェアバージョンを実行していて、プライマリ Catalyst 9800 シリーズ ワイヤレス コントローラ上にアクティブなソフトウェアイメージがあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 のサービスポートおよび管理ポートが設定されています。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の冗長ポートが物理的に接続されています。
- インターフェイス設定、ルート追加、SSH回線設定、NETCONF-YANG設定などの事前設定は、Catalyst 9800 シリーズ ワイヤレス コントローラアプライアンスで完了します。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の管理インターフェイスは同じサブネット内にあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 デバイスおよび Catalyst 9800 シリーズ ワイヤレス コントローラ 2 デバイスのディスカバリとインベントリは、Cisco DNA Center から正常に実行されます。
- デバイスは到達可能で、[Managed] 状態になっています。

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**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出済みで到達可能なワイヤレスコントローラのリストを取得します。

ステップ 4 [Inventory] ウィンドウで目的の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 名をクリックし、プライマリコントローラとして設定します。

ステップ 5 [High Availability] タブをクリックします

デフォルトで選択された Catalyst 9800 シリーズ ワイヤレス コントローラがプライマリコントローラになり、[Primary C9800] フィールドはグレー表示されます。

ステップ 6 [Select Primary Interface] および [Secondary Interface] ドロップダウンリストから、HA 接続に使用するインターフェイスを選択します。

HA インターフェイスは次の目的で使用されます。

- IOSd が起動する前に、コントローラペア間の通信を有効にする。
- すべてのコントローラペアに IPC のトランスポートを提供する。
- コントローラペア間で交換される制御メッセージ全体の冗長性を有効にする。制御メッセージには、HA ロールの解決、キープアライブ、通知、HA 統計情報などがあります。

ステップ 7 [Select Secondary C9800] ドロップダウン リストから、HA ペアを作成するセカンダリコントローラを選択します。

ステップ 8 各フィールドに [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスを入力します。

（注） 冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、Catalyst 9800 シリーズ ワイヤレス コントローラの管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがそのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 9 [Netmask] フィールドに、ネットマスクアドレスを入力します。

ステップ 10 [Configure HA] をクリックします。

HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリコントローラが設定されます。成功すると、セカンダリコントローラが設定されます。HA が有効になると、両方のデバイスが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 11 HA が開始されたら、[High Availability] タブの [Redundancy Summary] に、[Sync Status] が [HA Pairing is in Progress]として表示されます。HA ペアリングが成功したことを Cisco DNA Center が検出すると、[Sync Status] が [Complete] になります。

これは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリコントローラ（Catalyst 9800 シリーズ ワイヤレス コントローラ 2）が Cisco DNA Center から削除されます。このフローは、Catalyst 9800 シリーズ ワイヤレス コントローラ での正常な HA 設定を示しています。

ステップ 12 手動でコントローラを再同期するには、**[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラを選択します。

ステップ 13 [Actions] ドロップダウンリストから、[Resync] を選択します。

ステップ 14 プロセスが完了した後に発生するアクションのリストを次に示します。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 は、冗長性管理、冗長性単位、およびシングルサインオン（SSO）を使用して設定されます。デバイスは、ロールをアクティブコントローラまたはスタンバイコントローラとしてネゴシエートするために再起動します。設定はアクティブからスタンバイへと同期されます。
- [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
  - SSO は有効
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 1 がアクティブ状態である
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 2 がスタンバイ状態である

ハイ アベイラビリティについて

高可用性（HA）によって、コントローラのフェールオーバーが原因で生じるワイヤレスネットワークのダウンタイムを短縮できます。Cisco DNA Center を介して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定するためのコマンド

ステップ 1 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプライマリに高可用性を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 3 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 2 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのセカンダリに高可用性を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
  ```

ステップ 3 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

ステップ 4 Cisco Catalyst 9800-40 ワイヤレスコントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのプライマリに HA を設定するには、次のコマンドを使用します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 5 次のコマンドを使用して、Cisco Catalyst 9800-40 ワイヤレス コントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのセカンダリに HA を設定します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
  ```

ステップ 6 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性を確認するためのコマンド

次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラから高可用性設定を検証します。

- **config redundancy mode sso** コマンドを実行して、HA 関連の詳細情報を確認します。

- **show chassis** コマンドを実行して HA ペアのシャーシ設定を表示します。これには、MAC アドレス、ロール、スイッチプライオリティ、および冗長 HA ペア内の各コントローラデバイスの現在の状態が含まれています。
- **show ip interface brief** コマンドを実行して、プラットフォームで設定されている設定モードではなく、デバイスで実行されている実際に稼働中の冗長モードを表示します。
- **show redundancy states** コマンドを実行して、アクティブコントローラとスタンバイコントローラの冗長性状態を表示します。
- **show redundancy summary** コマンドを実行して、設定されているインターフェイスを確認します。
- ハイアベイラビリティ設定の詳細を確認するには、**show romvar** コマンドを実行します。

N+1 高可用性

N+1 高可用性の概要

Cisco DNA Center は、シスコ ワイヤレス コントローラ および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォームで N+1 高可用性（HA）をサポートします。

HA-SKU を使用した N+1 HA は、Cisco 2504、5500、7500、および 8500 シリーズのスタンドアロン ワイヤレス コントローラおよび WiSM2 コントローラでサポートされています。

N+1 HA アーキテクチャは、低い導入コストで、地理的に離れたデータセンター間のコントローラに冗長性をもたらします。

N+1 HA では、単一の シスコ ワイヤレス コントローラ を複数のプライマリコントローラのバックアップコントローラとして使用できます。これらのワイヤレスコントローラは互いに独立していて、インターフェイスの設定や IP アドレスを共有しません。

Cisco DNA Center は、N+1 HA のプライマリおよびセカンダリコントローラの設定をサポートします。

N+1 HA は AP レベルごとに設定され、設定はグローバルレベルではなく AP に直接プッシュされます。

AP フォールバックオプションが有効の場合、プライマリ ワイヤレスコントローラ が動作を再開すると、AP はバックアップ ワイヤレスコントローラ からプライマリ ワイヤレスコントローラ に自動的にフォールバックします。

（注） プライマリコントローラとセカンダリコントローラは、同じデバイスタイプである必要があります。たとえば、プライマリデバイスが Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、セカンダリデバイスも Cisco Catalyst 9800 シリーズ ワイヤレス コントローラである必要があります。

プライマリコントローラで高い優先順位が設定されている AP は、優先順位の低い AP が排除されることになっても、常に最初にバックアップコントローラに接続されます。

このリリースでは、N+1 HA 設定に次の制限があります。

- VLAN ID の設定が原因で、セカンダリコントローラの自動プロビジョニングはサポートされていません。
- プライマリコントローラに変更を加えた場合、最新の設計の設定を使用してセカンダリコントローラを手動で再プロビジョニングする必要があります。
- 耐障害性はサポートされていません。
- アクセスポイントのステートフル スイッチ オーバー（AP SSO）機能は、N+1 HA ではサポートされていません。AP Control and Provisioning of Wireless Access Points（CAPWAP）ステートマシンは、プライマリコントローラに障害が発生したときに再起動されます。

Cisco DNA Center から N+1 高可用性を設定するための前提条件

- [Discovery] 機能を実行して、プライマリコントローラとセカンダリコントローラを検出します。

  詳細については、CDP を使用したネットワークの検出またはIP アドレス範囲を使用したネットワークの検出を参照してください。

- ワイヤレスコントローラが到達可能で、[Managed] 状態である必要があります。

  詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

- デバイス間のネットワーク接続を確認します。プライマリコントローラがダウンした場合、AP が N+1 の設定に従ってセカンダリコントローラに参加できるようにする必要があります。

- 2 つのビルディングを作成して、両方のデバイスのプライマリおよびセカンダリの場所を管理します。たとえば、ビルディング A とビルディング B のような 2 つのビルディングを作成し、ビルディング A をコントローラ 1 のプライマリ管理場所かつコントローラ 2 のセカンダリ管理場所に設定し、ビルディング B をコントローラ 2 のプライマリ管理場所としてのみ設定できます。

  詳細については、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

- 設計フェーズ中にカバレッジヒートマップが可視化されるようにするには、フロアマップに AP を追加して配置します。

  詳細については、「AP の追加、配置、および削除」を参照してください。

- 2つの SSID を作成し、バックホール SSID として関連付けます。

  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 の作成とゲスト ワイヤレス ネットワークの SSID の作成を参照してください。

Cisco DNA Center からの N+1 高可用性の設定

この手順では、シスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで N+1 高可用性（HA）を設定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**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとしてプロビジョニングするには、目的のコントローラの隣にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 4 プライマリコントローラのプライマリ管理 AP 場所を割り当てるには、[Choose a site] をクリックします。

ステップ 5 [Choose a site] ウィンドウで、サイトを選択して [Save] をクリックします。

ステップ 6 [Next] をクリックします。

[Configuration] ウィンドウが表示され、プライマリデバイスのプライマリ管理対象 AP の場所が表示されます。

ステップ 7 [Select Primary Managed AP Locations] をクリックして、プライマリコントローラの管理対象 AP のロケーションを追加または更新できます。

ステップ 8 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] 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。

ステップ 9 インターフェイスと VLAN の詳細を設定します。

ステップ 10 [Configure Interface and VLAN] 領域で、IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 11 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 12 [Summary] ウィンドウでプライマリコントローラの管理対象 AP の場所およびその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 13 次に、セカンダリコントローラをプロビジョニングします。

ステップ 14 [Inventory] ウィンドウで目的のコントローラの隣にあるチェックボックスをオンにし、セカンダリコントローラとしてプロビジョニングします。

ステップ 15 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 16 セカンダリコントローラの管理対象 AP の場所を割り当てるには、[Choose a site] をクリックします。

セカンダリコントローラの管理対象 AP の場所は、プライマリコントローラの管理対象 AP の場所と同じにする必要があります。

ステップ 17 [Choose a site] ウィンドウで、セカンダリコントローラを関連付けるサイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 18 **[Next]** をクリックします。

[Configuration] ウィンドウが表示され、セカンダリデバイスのプライマリ管理対象 AP の場所とセカンダリ管理対象 AP の場所が表示されます。

ステップ 19 [Select Secondary Managed AP Locations] をクリックして、セカンダリコントローラの管理対象 AP の場所を追加または更新できます。

ステップ 20 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] 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。

ステップ 21 セカンダリコントローラのインターフェイスと VLAN の詳細を設定します。

ステップ 22 [Configure Interface and VLAN] 領域で、セカンダリコントローラの IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 23 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 24 [Summary] ウィンドウで、セカンダリコントローラの管理対象 AP の場所やその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 25 プライマリコントローラおよびセカンダリコントローラの管理対象場所を確認するには、**[Provision]** > **[Devices]** > **[Inventory]** ウィンドウでプロビジョニングしたコントローラのデバイス名をクリックします。

ステップ 26 [Device details] ウィンドウで、[Managed ap locations] タブをクリックして、プライマリおよびセカンダリの管理対象場所の詳細を表示します。

ステップ 27 プライマリコントローラの AP をプロビジョニングします。

ステップ 28 **[Devices]** > **[Inventory]** ウィンドウで、プロビジョニングする AP の横にあるチェックボックスをオンにします。

ステップ 29 [Action] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

ステップ 30 [Assign Site] ウィンドウで、[Choose a Floor] をクリックして、プライマリの管理対象場所からフロアを選択します。

ステップ 31 **[次へ (Next)]** をクリックします。

[設定（Configuration）] ウィンドウが表示されます。

ステップ 32 デフォルトでは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Wireless Radio Frequency Profile]** でデフォルトとマークしたカスタムRFプロファイルが、[RF Profile] ドロップダウンリストで選択されています。

[RF Profile] ドロップダウンリストから値を選択して、AP のデフォルト RF プロファイル値を変更できます。

ステップ 33 **[Next]** をクリックします。

ステップ 34 [Summary] ウィンドウで、詳細を確認します。

ステップ 35 [Deploy] をクリックして、プライマリ AP をプロビジョニングします。

ステップ 36 AP グループの作成または変更が進行中であることを示すメッセージが表示されます。

「プロビジョニング後にAPがリブートします。続行しますか?（After provisioning AP(s) will reboot. Do you want to continue?）」というメッセージが表示されます。

ステップ 37 [OK] をクリックします。

展開が成功すると、[Device Inventory] ウィンドウの [Last Sync Status] 列に、[SUCCESS] と表示されます。

モビリティ設定の概要

Cisco DNA Center のモビリティ設定では、一連の シスコ ワイヤレス コントローラ をモビリティグループにグループ化して、ワイヤレスクライアントのシームレスなローミング体験を実現できます。

モビリティグループを作成すると、ネットワーク内で複数のワイヤレスコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータトラフィックを転送できます。異なるモビリティグループ名を同じ無線ネットワーク内の異なるワイヤレスコントローラに割り当てると、モビリティグループによって、1つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。

Cisco DNA Center では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラなどのさまざまなプラットフォーム間でモビリティグループを作成できます。

モビリティ設定には、次の注意事項および制限事項があります。

- [Provision] ページでは、モビリティを設定するために複数のコントローラを選択することはできません。
- グループ名をデフォルトにしてモビリティグループを作成することはできません。これにより、モビリティおよびRFグループ名がデフォルトとしてリセットされ、すべてのピアが削除されます。
- アンカーコントローラでモビリティグループ名を設定することはできません。
- Cisco AireOS コントローラでモビリティグループを設定しているときに仮想IPアドレスが変更された場合は、ワイヤレスコントローラ を手動で再起動する必要があります。

- 同じモビリティグループ名を持つワイヤレスコントローラは、自動的に1つのモビリティグループにグループ化され、互いにピアとして追加されます。
- Cisco AireOS コントローラでモビリティグループを設定するときに、ワイヤレスコントローラ に IP アドレス 192.0.2.1 がない場合、Cisco DNA Center は仮想 IP アドレス 192.0.2.1 をすべての ワイヤレスコントローラ にプッシュします。
- ゲストアンカーコントローラをモビリティグループに明示的に追加しないでください。プロビジョニングされたゲストアンカーコントローラは、[Mobility Configuration] ページでピアを追加している間、ドロップダウンリストに表示されません。
- ワイヤレスコントローラをゲストアンカーとしてプロビジョニングする場合は、それがモビリティグループに追加されていないことを確認します。

モビリティ設定ワークフロー

次に、シスコ ワイヤレス コントローラ でモビリティを設定するために使用できるワークフローを示します。

- モビリティを設定するには、モビリティグループ名、RF グループ名、およびモビリティピアを使用して ワイヤレスコントローラ をプロビジョニングする必要があります。
- ワイヤレスコントローラのプロビジョニング中に適用される設定は、そのグループに設定されているすべてのモビリティピアに自動的に複製されます。
- ワイヤレスコントローラ を再同期して、最新のトンネルステータスを取得します。

モビリティ設定の使用例

次の使用例では、コントローラ間のモビリティの設定手順について説明します。

使用例 1

シスコ ワイヤレス コントローラ 1、ワイヤレスコントローラ 2、およびワイヤレスコントローラ 3 は、モビリティグループ名（デフォルト）を使用して Cisco DNA Center に新たに追加されていて、まだプロビジョニングされていません。

1. モビリティグループ名、RF グループ名を設定し、ワイヤレスコントローラ 2 および ワイヤレスコントローラ 3 をピアとして追加することによって、ワイヤレスコントローラ 1 をプロビジョニングします。
2. ワイヤレスコントローラ 2 をプロビジョニングします。

   [Provision] ウィンドウでは、ワイヤレスコントローラ 2 のモビリティ設定がグループ名とピアとともに自動的に入力されます。
3. ワイヤレスコントローラ 3 をプロビジョニングします。
4. すべての ワイヤレスコントローラ をプロビジョニング後、ワイヤレスコントローラ を再同期して、最新のトンネルステータスを受信します。

使用例 2

異なるモビリティグループ名を持つシスコ ワイヤレス コントローラ 1、ワイヤレスコントローラ 2、および ワイヤレスコントローラ 3はすでに Cisco DNA Center に追加され、プロビジョニングされています。

1. モビリティグループ名、RF グループ名を設定してワイヤレスコントローラ 1 をプロビジョニングし、ピアとしてワイヤレスコントローラ 2 およびワイヤレスコントローラ 3 を追加します。
2. モビリティ設定は、 ワイヤレスコントローラ 2、 ワイヤレスコントローラ 3 などの他のピア間で自動的に複製されます。
   - ワイヤレスコントローラ 1 のプロビジョニングが成功すると、 ワイヤレスコントローラ 2 と ワイヤレスコントローラ 3 がピアとして ワイヤレスコントローラ 1 に追加されます。
   - ワイヤレスコントローラ 1 と ワイヤレスコントローラ 3 は、ワイヤレスコントローラ 2 のピアとして追加されます。
   - ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 は、ワイヤレスコントローラ 3 のピアとして追加されます。

モビリティグループの設定

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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたすべてのデバイスが一覧表示されます。

ステップ 2 **[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 3 モビリティを設定する Catalyst 9800 シリーズ ワイヤレス コントローラ の名前の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision WLC Mobility]** の順に選択します。

[Configure Mobility Group] サイドパネルが表示されます。

詳細については、「モビリティ設定の概要 （60 ページ）」を参照してください。

ステップ 5 [Mobility Group Name] ドロップダウンリストで、[+] をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択できます。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 6 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 7 モビリティの暗号化設定を有効または無効にするには、[DTLS High Cipher Only] ボタンをクリックします。

暗号方式の設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.5 以降に適用されます。変更を有効にするには、デバイスを手動で再起動する必要があります。

ステップ 8 DTLS（Data Datagram Transport Layer Security）暗号方式の設定を変更した後にデバイスを手動で再起動して、プロビジョニング後に変更を有効にするには、[Restart for DTLS Ciphers to take effect] ボタンをクリックします。

ステップ 9 DTLS データ暗号化を有効にするには、[Data Link Encryption] ボタンをクリックします。

ステップ 10 [Mobility Peers] で [Add] をクリックして、モビリティピアを設定します。

ステップ 11 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、 Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 12 **[Save]** をクリックします。

ステップ 13 モビリティグループ名と RF グループ名をリセットするには、次のいずれかの方法を実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > **[Configuration]** ページの [Mobility Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

DTLS 暗号スイートについて

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。

リリース 17.5 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ、および Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ プラットフォームでは複数の DTLS（Data Datagram Transport Layer Security）暗号スイートを設定できます。

複数の DTLS 暗号スイートの設定

DTLS 暗号スイートは、グローバルレベルまたはサイトレベルで設定できます。

始める前に

- **[System]** > **[Settings]** > **[Device Settings]** > **[Device Controllability]** ページでデバイス可制御性機能が有効になっていることを確認します。
- 検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

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 同じ DTLS 暗号スイート設定ですべてのサイトを設定するには、左側のツリーメニューで [Global] を選択します。

DTLS暗号スイートをサイトレベルで設定するには、左側のツリーメニューでサイトを選択します。DTLS暗号スイートの設定は、その特定のサイトで使用可能なコントローラにプッシュされます。

ステップ 3 暗号スイートをデバイスの可制御性の一部として設定するには、[Skip DTLS Ciphersuite Config] チェックボックスをオフにします。

ステップ 4 デフォルト暗号スイートまたはカスタム暗号スイートを設定します。

デフォルトでは、**デフォルト**暗号スイートが選択されています。

[Default Ciphersuite] ボックスにはデフォルト暗号スイートのリストが示され、これらの暗号スイートが、デバイスでデフォルトとして設定されています。これらのデフォルト暗号スイートの優先順位は変更できません。

ステップ 5 カスタム暗号スイートを設定するには、[Custom] ボタンをクリックします。

カスタム暗号スイートは、優先順位に従ってデフォルト暗号スイートを上書きします。

ステップ 6 [Version] ドロップダウンリストから、DTLS のバージョンを選択します。

Cisco DNA Center は、DTLS のバージョンに基づいて、使用可能な暗号スイートを表示します。

ステップ 7 暗号スイートを適用しない場合は、その暗号スイートの横にある青色のボタンをクリックします。

ステップ 8 暗号スイートの優先順位を変更するには、各暗号スイートをクリックしたままドラッグします。

ステップ 9 [**保存（Save）**] をクリックします。

「DTLS Ciphersuite Config Saved successfully」というメッセージが表示されます。

ステップ 10 暗号スイートの設定を適用するには、デバイスをプロビジョニングする必要があります。

詳細については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （68 ページ）を参照してください。

N+1 ローリング AP アップグレードについて

Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの N+1 高可用性設定では、ローリング AP アップグレード機能がサポートされます。この機能は、ワイヤレス LAN ネットワーク内の Cisco AireOS コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに関連付けられている AP のソフトウェアイメージをアップグレードするのに便利です。ゼロダウンタイムを実現するために、N+1 ローリング AP アップグレード機能を使用して、段階的に AP をアップグレードすることができます。

プライマリコントローラは、無線リソース管理ネイバー AP マップを使用して、候補の AP を識別します。アップグレードプロセスは、イメージが候補の AP に事前ダウンロードされてい

る間に、ソフトウェアイメージをプライマリコントローラにダウンロードすることから始まります。候補の AP がアップグレードされて再起動されると、これらの AP は、セカンダリコントローラに段階的に参加します。すべての AP がセカンダリコントローラに参加した後、プライマリコントローラは再起動します。これらの AP は、再起動された後、段階的にプライマリコントローラに再度参加します。

次に、ローリング AP アップグレードを設定するための前提条件を示します。

- 2 つの ワイヤレスコントローラ（1 つはプライマリコントローラ、もう 1 つはセカンダリとして）の N+1 ハイアベイラビリティ設定。
- プライマリコントローラと N+1 コントローラの設定は同じで、ネットワーク内の同じ場所を管理します。
- N+1 コントローラではすでにゴールデンイメージが実行されているため、ローリング AP アップグレードはダウンタイムなしで動作します。

  ゴールデンイメージは、ネットワークデバイスの標準化されたイメージであり、Cisco DNA Center は Cisco.com からイメージを自動的にダウンロードします。イメージの標準化は、デバイスのセキュリティと、デバイスのパフォーマンスの最適化に役立ちます。
- N+1 コントローラはに到達可能であり、Cisco DNA Center で [Managed] 状態になっています。
- 両方のコントローラが同じモビリティグループの一部であり、プライマリコントローラと N+1 コントローラの間にモビリティトンネルが確立されます。プライマリコントローラと N+1 コントローラ間のアップグレード情報は、モビリティトンネルを介して交換されます。

ローリング AP アップグレードを設定するワークフロー

この手順では、Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでローリング AP アップグレードを設定する方法を示します。

（注） N+1 ローリング AP アップグレードは、ファブリックおよび非ファブリックの展開でサポートされています。

ステップ 1 Cisco DNA Center をインストールします。

詳細については、Cisco Digital Network Architecture Center 設置ガイド [英語] を参照してください。

ステップ 2 Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

ステップ 3 ディスカバリ機能を使用して ワイヤレスコントローラを検出します。

Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

詳細については、CDP を使用したネットワークの検出またはIP アドレス範囲を使用したネットワークの検出を参照してください。

ステップ 4 検出されたデバイスが [Device Inventory] ウィンドウに [Managed] 状態で表示されていることを確認します。

詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

デバイスが [Managed] になるまで待機する必要があります。

ステップ 5 サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、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るようになります。

新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロードを参照してください。

新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

ステップ 6 AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「AP の追加、配置、および削除」を参照してください。

ステップ 7 プライマリ管理対象 AP の場所、およびローリング AP アップグレードが有効になっていて、モビリティグループがセカンダリコントローラをピアとして設定されている状態で、プライマリコントローラをプロビジョニングします。

これを行うには、**[Provision]** > **[Devices]** > **[Inventory]** の順に選択し、プライマリコントローラ名の横にあるチェックボックスをオンにします。

ステップ 8 モビリティグループ設定で、モビリティピアとして N+1 コントローラを設定します。

詳細については、「モビリティ設定の概要 （60 ページ）」を参照してください。

ステップ 9 プライマリコントローラのプライマリ管理対象 AP の場所を N+1 コントローラのセカンダリ管理対象 AP の場所として設定することによって、N+1 HA コントローラをプロビジョニングします。これにより、セカンダリコントローラが N+1 コントローラとして設定されます。

詳細については、Cisco AireOS コントローラのプロビジョニング （30 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （68 ページ）を参照してください。

ステップ 10 プライマリ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します。

詳細については、「#unique_185」を参照してください。

ステップ 11 ソフトウェアイメージをリポジトリにインポートします。

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。

ステップ 12 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て」を参照してください。

ステップ 13 デバイスファミリまたはデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークします。

詳細については、ゴールデン ソフトウェア イメージの指定を参照してください。

ステップ 14 イメージをアップグレードする前に、両方のデバイスでイメージの準備状況チェックが成功していることを確認してください。

また、[N+1 Device Check] と [Mobility Tunnel Check] のステータスに緑色のチェックマークが付いていることも確認してください。

- イメージ更新の準備状況チェックを実行するには、**[Provision]** > **[Devices]** > **[Software Images]** の順に選択します。
- イメージをアップグレードするデバイスを選択します。
- デバイスの事前チェックが成功すると、[Image Precheck Status] 列の [Status] リンクに緑色のチェックマークが付きます。デバイスのアップグレード準備状況の事前チェックのいずれかが失敗した場合、[Image Precheck Status] リンクのマークが赤色に変わり、そのデバイスの OS イメージは更新できません。先に進む前に [Status] リンクをクリックし、エラーを修正します。

ステップ 15 プライマリコントローラでアップグレードを開始します。

ステップ 16 **[Provision]** > **[Devices]** > **[Software Images]** ページで、プライマリコントローラの横にあるチェックボックスをオンにします。

ステップ 17 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** の順に選択します。

詳細については、ソフトウェア イメージのプロビジョニングを参照してください。

ステップ 18 イメージのアップグレードの進行状況をモニターするには、[Software Image] 列で [In Progress] をクリックします。

[Device Status] ページには、次の情報が表示されます。

- [Distribution Operation]：イメージ配信プロセスに関する情報が表示されます。イメージは Cisco DNA Center からプライマリデバイスにコピーされます。配信プロセスが完了すると、アクティブ化操作が開始されます。
- [Activate Operation]：アクティブ化操作の詳細が表示されます。このプロセス中に、ローリング AP アップグレードが開始されます。
- [Rolling AP Upgrade Operation]：ローリング AP アップグレードタスクが完了したかどうか、保留中の AP の数、再起動中の AP の数、N+1 コントローラに参加している AP の数など、ローリング AP アップグレードの概要が表示されます。

[View AP Status] をクリックすると、プライマリコントローラ、N+1 コントローラ、デバイス名、現在のステータス、および反復に関する詳細が表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニングを行う前に、Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー （47 ページ） の手順を完了したことを確認します。

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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたすべてのデバイスが一覧表示されます。

ステップ 2 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ 名の横にあるチェックボックスをオンにします。

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

ステップ 4 [Assign Site] ウィンドウで、[Assign Site] をクリックしてサイトを割り当てます。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。

ステップ 6 [Save] をクリックします。

ステップ 7 [Next] をクリックします。

[Configuration] ウィンドウが表示されます。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのブラウンフィールドサポート

Cisco DNA Center を使用すると、シスコ ワイヤレス コントローラや Cisco Catalyst 9800 シリーズ ワイヤレス コントローラなどのブラウンフィールドデバイスをネットワークに追加してプロビジョニングできます。ブラウンフィールドとは、既存サイトの以前から存在しているインフラストラクチャに属しているデバイスのことです。

ここでは、Cisco DNA Center でブラウンフィールドの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをプロビジョニングする方法を説明します。

始める前に

- インベントリに Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ があることを確認します。ない場合は、ディスカバリ機能を使用して検出します。

  Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。

  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。

- Catalyst 9800 シリーズ ワイヤレス コントローラ は到達可能で、[Inventory] ウィンドウで [Managed] 状態でなければなりません。詳細については、インベントリについてを参照してください。

- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、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るようになります。新しいネットワーク階層を作成できるほか、Cisco Prime Infrastructure に既存のネットワーク階層がある場合はその階層を Cisco DNA Center にインポートすることもできます。

  既存のネットワーク階層のインポートとアップロードの詳細については、既存のサイト階層をアップロードを参照してください。

  新しいネットワーク階層の作成については、ネットワーク階層のサイトの作成、ビルディングの追加、ビルディングへのフロアの追加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**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示されます。このウィンドウには、ネットワークで使用できる検出済みのすべてのデバイスが一覧表示されます。

ステップ 2 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択します。

ステップ 4 [Assign Site] ウィンドウで、[Choose a Site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラにサイトを割り当てます。

ステップ 5 [Choose a site] ウィンドウで、Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けるサイトを選択し、[Save] をクリックします。

ステップ 6 **[次へ (Next)]** をクリックします。

ステップ 7 [Resolve Conflict] ウィンドウに Cisco DNA Center および Catalyst 9800 シリーズ ワイヤレス コントローラで使用可能な構成が表示されます。解決する必要がある、競合する構成は、赤いボックスで強調表示されています。

[Choose this config in Cisco DNA Center] セクションに Cisco DNA Center で使用可能な構成が表示され、[Choose this config in Device] セクションに Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスで使用可能な構成が表示されます。

1. Cisco DNA Center の構成を保持するには、[Choose this config] セクションで対応する赤色のボックスをクリックして、保持する構成を選択します。これにより、デバイス設定が上書きされます。

   たとえば、Cisco DNA Center が SSID の認証タイプとして Open を使用していて、デバイスが認証タイプとして wpa2_enterprise を使用している場合、保持する構成を決定できます。Cisco DNA Center の構成を保持するには、[Choose this config] で [Open] を選択します。Cisco DNA Center の構成を保持すると、デバイスの構成が上書きされます。

   デバイスの構成を保持するには、[Choose this config in Device] セクションで対応する赤色のボックスをクリックして、保持する構成を選択します。デバイスの構成を保持すると、Cisco DNA Center の構成が上書きされることに注意してください。

2. [Warning] ダイアログボックスで [OK] をクリックします。

ステップ 8 **[次へ (Next)]** をクリックします。

[Design Object] ウィンドウに、デバイスで学習された構成が一覧表示されます。

ステップ 9 左ペインで [Network] をクリックします。

右側のペインに、デバイス構成学習プロセスの一部として学習されたネットワーク構成と、次の情報が表示されます。

- [AAA サーバー（AAA Server）] の詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。
- [HCP Server] には、デバイスで使用可能なすべての DHCP サーバーに関する詳細が表示されます。
- [NTP Server] には、デバイスで使用可能なすべての NTP サーバーに関する詳細が表示されます。

ステップ 10 AAA サーバーの共有秘密を入力します。

ステップ 11 左ペインで [ワイヤレス（Wireless）] をクリックします。

デバイスに存在するエンタープライズ SSID、ゲスト SSID、ワイヤレスインターフェイス、および RF プロファイルが一覧表示されます。

ステップ 12 事前共有キー（PSK）を使用する SSID の場合、[事前共有キー] を指定する必要があります。

ステップ 13 左ペインで [破棄された設定（Discarded Config）] をクリックします。

Cisco DNA Center の競合する構成と既存の構成が表示されます。破棄される構成エントリは次のカテゴリに分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイスの設定

ステップ 14 [Next]をクリックします。

[ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

ステップ 15 **[Save]** をクリックします。

「ブラウンフィールド設定に成功しました（Brownfield Configuration is Successful）」というメッセージが表示されます。

ステップ 16 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]** の順に選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 17 [ネットワーク プロファイル（Network Profile）] ページで [サイトの割り当て（Assign Site）] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 18 [Add Sites To Profile] ウィンドウで、サイトの横にあるチェック ボックスをオンにして、このプロファイルを関連付けます。

ステップ 19 **[Save]** をクリックします。

ステップ 20 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

ステップ 21 [フィルタ（Filter）] をクリックして、選択したフィルタ フィールドに適切な値を入力します。

[デバイス（Devices）]テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 22 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ 名の横にあるチェックボックスをオンにします。

ステップ 23 [Actions] ドロップダウンリストから、**[Provision]** > > **[Provision Device]** の順に選択します。

ステップ 24 [サイトの割り当て（Assign Site）] ウィンドウで詳細を確認して、[次へ（Next）] をクリックします。

[設定（Configurations）] ウィンドウが表示されます。

ステップ 25 [インターフェイスと VLAN の設定（Interface and VLAN Configuration）] で、[+ 追加（+ Add）] をクリックしてインターフェイスと VLAN の詳細を設定します。

ステップ 26 [インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。

ステップ 27 [Next] をクリックします。

ステップ 28 [Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **Device Details**
- **ネットワークの設定**
- **SSID**
- **Managed Sites**
- **ローリング AP アップグレード**
- **Interfaces**

ステップ 29 [展開（Deploy）] をクリックして、デバイスをプロビジョニングします。

ステップ 30 デバイスを今すぐ展開するか、または展開を後の時間でスケジュールするかどうかを求められます。

- デバイスを今すぐ展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 31 AP をプロビジョニングします。

詳細については、#unique_185を参照してください。

Cisco Embedded Wireless Controller on Catalyst Access Points 対応 Day 0 ワークフロー

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ（EWC-AP）は、次世代の Wi-Fi ソリューションであり、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に Cisco Catalyst 9100 シリーズ アクセスポイントを統合し、進化および成長し続ける組織にそのクラスで最高のワイヤレスエクスペリエンスをもたらします。

始める前に

- 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、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。

  詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、およびグローバル SNMPv3 クレデンシャルの設定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を作成します。

  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、ゲスト ワイヤレス ネットワークの SSID の作成、ワイヤレスインターフェイスの作成、およびワイヤレス無線周波数プロファイルの作成を参照してください。

（注） Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ では、Flex ベースの SSID の作成のみがサポートされています。

- Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が接続されているスイッチでオプション #43 を使用して DHCP サーバーを設定します。これは Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。この IP アドレスを使用して、AP は PnP サーバーに接続し、設定をダウンロードします。

- インベントリに Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ 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。詳細については、CDP を使用したネットワークの検出、IP アドレス範囲を使用したネットワークの検出、およびインベントリについてを参照してください。

- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ は、次のような複数のフォームファクタで使用できます。

- Catalyst 9115AX アクセスポイント上の Cisco 組み込みワイヤレスコントローラ
- Catalyst 9117AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9120AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9130AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ

ステップ 1 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が DHCP サーバーと通信します。

DHCP サーバーからの応答で、IP アドレスとともに、Cisco プラグアンドプレイサーバーの IP アドレスを含むオプション #43 が返されます。

ステップ 2 オプション #43 に基づいて、 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ はプラグアンドプレイ エージェントをオンにし、Cisco DNA Center プラグアンドプレイサーバーに接続します。

（注） ネットワーク内に Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ のセットがある場合、それらは内部プロトコルを通過します。プロトコルは、PnP サーバーに到達するために シスコ ワイヤレス コントローラ 上でプライマリ AP として設定されている 1 つの Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を選択します。

ステップ 3 **[Provision]** > **[Network Devices]** > **[Plug and Play]** タブで未要求 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を検索します。

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onboarding State] 列の下でオンボーディングステータスが [Initialized] になるまで待つ必要があります。

ステップ 4 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 5 デバイステーブルの上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

[Claim Devices] ウィンドウが表示されます。

ステップ 6 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 7 **[次へ (Next)]** をクリックします。

ステップ 8 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 9 [Configuration for device name] ページで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 10 [Save] をクリックします。

ステップ 11 [Next] をクリックします。

[Summary] ページが表示されます。

ステップ 12 [Summary] ページで [Claim] をクリックします。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が要求されると、設定された IP アドレスが Cisco Embedded Wireless Controller に割り当てられます。

要求したデバイス（内部 AP を備えた Cisco 組み込みワイヤレスコントローラ）が **[Provision]** > **[Network Devices]** > **[Inventory]** に表示されることを確認します。

ステップ 13 追加のコントローラをプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （30 ページ）を参照してください。

ステップ 14 CSV ファイルからデバイスを一括インポートするには、デバイスの一括追加 （13 ページ） を参照してください。

ステップ 15 デバイスを手動で追加するには、「デバイスの追加または編集」を参照してください。

Cisco DNA Center を使用した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの Cisco AireOS コントローラの移行

始める前に

- 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。
- ディスカバリ機能を実行して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出し、インベントリに追加します。デバイスステータスが到達可能で、管理対象状態になっていることを確認します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。NETCONF は、ネットワークの設定をインストール、操作、削除するためのメカニズムです。
- Cisco AireOS コントローラを検出して、インベントリに追加します。デバイスステータスが到達可能で、管理対象状態になっ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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Cisco AireOS コントローラの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Assign Device to Site]** の順に選択します。

ステップ 4 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 5 [Add Sites] ウィンドウで、Cisco AireOS コントローラと関連付けるサイト名の横にあるチェックボックスをオンにします。

ステップ 6 [**保存（Save**）] をクリックします。

ステップ 7 [Action] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択して、Cisco AireOS コントローラデバイスから構成を学習します。

ステップ 8 [Assign Site] ウィンドウで、[Next] をクリックします。

ステップ 9 [Resolve Conflict] ウィンドウに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。[Next]をクリックします。

ステップ 10 [Design Object] ウィンドウで、[Next] をクリックします。

ステップ 11 左側のペインで [Network] をクリックします。

右側のペインに、デバイス構成学習プロセスの一部として学習されたネットワーク構成と、次の情報が表示されます。

- AAA サーバーの詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。パスワードは暗号化されており、Cisco DNA Center はパスワードを学習できないため、AAA サーバーの共有秘密を入力します。
- HCP サーバー。デバイスで使用可能なすべての DHCP サーバーに関する詳細が表示されます。
- NTP サーバー。デバイスで使用可能なすべての NTP サーバーに関する詳細が表示されます。

ステップ 12 [Next] をクリックします。

ステップ 13 左ペインで [Wireless] をクリックします。

[Wireless] ウィンドウに、デバイスに存在するエンタープライズ SSID、ゲスト SSID、ワイヤレスインターフェイス、および RF プロファイルが一覧表示されます。

ステップ 14 事前共有キー（PSK）を使用する SSID の場合、事前共有キーを入力します。

ステップ 15 左ペインで、[Discarded Config] をクリックします。

Cisco DNA Center の競合する設定と既存の設定が表示されます。破棄される構成エントリは次のカテゴリに分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイスの設定

ステップ 16 [Next]をクリックします。

ステップ 17 [ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

ステップ 18 **[Save]** をクリックします。

成功メッセージが表示されます。

ステップ 19 **[Design]** > **[Network Settings]** > **[Wireless]** の順に選択して、Cisco DNA Center が Cisco AireOS コントローラから学習した SSID とインターフェイス設定を表示します。

ステップ 20 **[Design]** > **[Network Profile]** を選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 21 [ネットワーク プロファイル（Network Profile）] ページで [サイトの割り当て（Assign Site）] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 22 [Add Sites to Profile] ウィンドウでドロップダウンリストからサイトを選択して、[Save] をクリックします。

ステップ 23 [プロビジョニング（Provision）] タブをクリックします。

ステップ 24 プロビジョニングする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

ステップ 25 [アクション（Actions）] ドロップダウン リストから、[プロビジョニング（Provision）]を選択します。

ステップ 26 [Choose a site] をクリックして Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ にサイトを割り当てます。

ステップ 27 [Choose a site] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラを関連付けます。

ステップ 28 **[次へ (Next)]** をクリックします。

[設定（Configuration） **]** ウィンドウが表示されます。

ステップ 29 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 30 プライマリ コントローラの管理 AP の場所を設定するには、[Select Primary Managed AP Locations] をクリックします。

ステップ 31 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。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、その親サイトの下にある子は自動的に選択されます。

ステップ 32 [Save] をクリックします。

ステップ 33 [Next] をクリックします。

ステップ 34 [Summary] ウィンドウには、Cisco AireOS コントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにプッシュされる設定が表示されます。

次の詳細情報を確認します。

- デバイスの詳細
- ネットワークの設定
- SSID
- 管理サイト
- インターフェイス
- 詳細設定

ステップ 35 [Deploy] をクリックして、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをプロビジョニングします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 36 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 37 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、実行する必要があるアクションのリストを表示します。

ステップ 38 手動で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを再同期するには、**[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラを選択します。

ステップ 39 [Actions] ドロップダウンリストから、[Resync] を選択します。

ステップ 40 AP をプロビジョニングします。

Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング

サポートされているハードウェア プラットフォーム

デバイスロール	プラットフォーム
組み込みワイヤレスコントローラ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ
ファブリックエッジ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ Cisco Catalyst 3600 シリーズ スイッチ Cisco Catalyst 3850 シリーズ スイッチ
AP	Cisco 802.11ac Wave 2 AP： • Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント • Cisco Aironet 1810W シリーズ アクセス ポイント • Cisco Aironet 1815i アクセスポイント • Cisco Aironet 1815w アクセスポイント • Cisco Aironet 1815m アクセスポイント

デバイスロール	プラットフォーム
	• Cisco 1830 Aironet シリーズ アクセスポイント • Cisco Aironet 1850 シリーズ アクセス ポイント • Cisco Aironet 2800 シリーズ アクセス ポイント • Cisco Aironet 3800 シリーズ アクセス ポイント • Cisco Aironet 4800 シリーズ アクセス ポイント Cisco 802.11ac Wave 1 AP • Cisco Aironet 1700 シリーズ アクセス ポイント • Cisco Aironet 2700 シリーズ アクセス ポイント • Cisco Aironet 3700 シリーズ アクセス ポイント

事前設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで、スイッチが **aaa new-model** ですでに設定されている場合は、次のコマンドが存在することを確認してください。

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

これは、NETCONF の設定では必須です。プロビジョニングに自動アンダーレイを使用している場合、これらの設定は必要ありません。

Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、『CISCO DNA Center インストール ガイド』を参照してください。

2. Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

   Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

3. Cisco Identity Services Engine と Cisco DNA Center を連動させます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。

4. Cisco Catalyst 9000 シリーズスイッチおよびエッジスイッチを検出します。

Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。

エッジスイッチを検出するために NETCONF を有効にする必要はありません。

詳細については、CDP を使用したネットワークの検出およびIP アドレス範囲を使用したネットワークの検出を参照してください。

[Preferred Management IP] を [Use Loopback] に変更します。

5. デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

   デバイスが**管理対象**状態になっていることを確認します。

6. 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設計します。サイト、ビルディング、フロアを作成すると、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るようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロードを参照してください。

   新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

7. 非ファブリックネットワークで設計フェーズ中にヒートマップの可視化を取得するには、フロアマップに AP を追加して配置します。

   ファブリックネットワークの場合、設計時にフロアマップに AP を配置することはできません。APは、ファブリックネットワークにデバイスを追加した後にオンボードされます。

   詳細については、「AP の追加、配置、および削除」を参照してください。

8. AAA（Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。

   詳細については、グローバルネットワーク設定の管理、グローバル ネットワーク サーバーの設定、および「AAA サーバーの追加」を参照してください。

9. CLI、SNMP、HTTP などのデバイスのログイン情報を設定します。

   詳細については、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 CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、グローバル HTTPS クレデンシャルの設定を参照してください。

10. IP アドレスプールをグローバルレベルで設定します。

IPアドレスプールを設定するには、IPアドレス プールを設定するを参照してください。

プロビジョニングするビルディングの IP アドレスプールを予約するには、「LAN アンダーレイのプロビジョニング」を参照してください。

11. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義すると、Cisco DNA Center はあらゆる場所にあるさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず、[Wireless] ページで SSID を作成する必要があります。次に、作成した SSID をワイヤレス ネットワーク プロファイルに関連付けます。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。

    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 の作成およびゲスト ワイヤレス ネットワークの SSID の作成を参照してください。

12. バックホールの設定を行います。詳細については、

13. [Policy] ページで、次のように設定します。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、仮想ネットワークおよび仮想ネットワークの作成を参照してください。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加します。詳細については、「グループベースのアクセス コントロール ポリシーの作成」を参照してください。

14. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9000 シリーズスイッチとエッジノードスイッチをプロビジョニングします。

    - ファブリックドメインを作成します。
    - CP+ボーダー+エッジまたはCP+ボーダーを作成して、デバイスをファブリックネットワークに追加します。
    - Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラで、組み込みワイヤレス機能を有効にします。
    - ファブリックドメイン内のオンボード AP。

    デバイスが正常に展開されると、展開ステータスが [Configuring] から [Success] に変わります。

Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング

始める前に

Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラをプロビジョニングする前に、Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコン

トローラを設定するためのワークフロー （78 ページ）の手順を完了していることを確認します。

この手順では、Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9400 シリーズ スイッチ、および Cisco Catalyst 9500H シリーズ スイッチに組み込みワイヤレスを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**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Catalyst 9000 シリーズ スイッチデバイスと、サイトに関連付けるエッジスイッチの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Assign Device to Site]** の順に選択します。

ステップ 4 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 5 [Choose a site] 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、デバイスを関連付けます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。
次の手順では、設計フェーズ中に追加された設定を使用して、Catalyst 9000 シリーズ スイッチとエッジノードをプロビジョニングします。

ステップ 8 **[Devices]** > **[Inventory]** ウィンドウで、プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 9 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ステップ 10 **[Next]** をクリックします。

ステップ 11 [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

ステップ 12 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activity]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

  （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 13 エッジスイッチをプロビジョニングするには、プロビジョニングするエッジスイッチの横にあるチェックボックスをオンにします。

ステップ 14 [Actions] ドロップダウンリストから、[Provision] を選択します。

ステップ 15 **[Next]** をクリックします。

ステップ 16 [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 17 ファブリックドメインにデバイスを追加するには、Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[Provision]** > **[Fabric]** の順に選択します。

ステップ 18 ファブリック LAN を作成します。詳細については、

ステップ 19 IP トランジットネットワークを追加します。

ステップ 20 デバイスを追加して、ファブリックドメインに仮想ネットワークを関連付けます。

ステップ 21 Cisco Catalyst 9000 シリーズ スイッチをコントロールプレーン、ボーダーノード、およびエッジノードか、またはコントロールプレーンとボーダーノードとして追加します。

デバイスをクリックし、[Add as CP+Border+Edge] または [Add as CP+Border] を選択します。

ステップ 22 エッジノードをクリックして、[Add to Fabric] を選択します。

ステップ 23 **[Save]** をクリックします。

ステップ 24 デバイス上で組み込みのワイヤレスを有効にするには、[Edge]、[CP+Border+Edge] または [CP+Border] として追加されたデバイスをクリックし、[Embedded Wireless] をクリックします。

ワイヤレス機能を有効にする前に Cisco Catalyst 9000 シリーズ スイッチにワイヤレスパッケージをインストールしなかった場合は、Cisco DNA Center に「機能を有効にするには、`9800-SW` イメージが必要です`[OK]` をクリックして、`9800-SW` イメージを手動でインポートしてください。（`9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually`）」という警告メッセージが表示されます。

ステップ 25 [OK] をクリックして、イメージを手動でインストールします。

ステップ 26 [Download Image] ウィンドウで、[Choose File] をクリックしてローカルに保存されているソフトウェアイメージに移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。

ステップ 27 [Import] をクリックします。

インポートの進捗状況が表示されます。

ステップ 28 [Activate image on device] をクリックします。

「デバイスでイメージが有効化されると、デバイスがリブートします。デバイスをリブートしてもよろしいですか。（Activate image on device will reboot the device. Are you sure you want to reboot the device?）」という警告メッセージが表示されます。

ステップ 29 [Yes] をクリックします。

デバイスパッケージのアップグレードが完了すると、デバイスがリブートし、オンラインになります。

ステップ 30 表示されるダイアログボックスに、コントローラで管理されている AP の場所が表示されます。ここからサイトの変更、削除、または再割り当てができます。

ステップ 31 **[Next]** をクリックします。

ステップ 32 [Summary] ウィンドウで詳細を確認し、[Save] をクリックします。

ステップ 33 [Modify Fabric Domain] ウィンドウで、[Now] をクリックして変更を確定し、[Apply] をクリックして設定を適用します。
次の手順では、ファブリックドメインで AP をオンボードします。

ステップ 34 Cisco DNA Center GUI で、[Provision] タブをクリックします。

ステップ 35 **[Fabric]** タブをクリックします。

ファブリックドメインのリストが表示されます。

ステップ 36 作成したファブリックドメインを選択し、[Host Onboarding] タブをクリックして、AP の IP プールを有効にします。

ステップ 37 ファブリックドメイン内のデバイスに適用される認証テンプレートを選択します。これらのテンプレートは、Cisco ISE から取得される事前定義済みの設定です。認証テンプレートを選択したら、[Save] をクリックします。

ステップ 38 [Virtual Networks] の下で、[INFRA_VN] をクリックして、選択した仮想ネットワークに 1 つ以上の IP プールを関連付けます。

ステップ 39 [Virtual Network] の下で、ゲスト仮想ネットワークをクリックして、選択したゲスト仮想ネットワークの IP プールを関連付けます。

ステップ 40 設計フェーズ中に AP 用に作成された [IP Pool Name] チェックボックスをオンにします。

ステップ 41 [Update] をクリックして設定を保存します。

AP は、指定したプールから IP アドレスを取得します。このプールは、AP VLAN に関連付けられていて、いずれかの検出方法を通じてシスコ ワイヤレス コントローラに登録されます。

ステップ 42 ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。[Wireless SSID] セクションで、ゲスト SSID または企業 SSID を選択してアドレスプールを割り当ててから、[Save] をクリックします。

ステップ 43 [Inventory] > [Resync] を実行して手動で再同期をトリガーし、組み込みのワイヤレス用の Cisco DNA Center で AP を確認します。
検出された AP が [Provision] ページの [Inventory] に表示され、[Status] は [Not Provisioned] として表示されます。

ステップ 44 AP をプロビジョニングします。

詳細については、#unique_185を参照してください。

ステップ 45 アプリケーションポリシーを設定および展開します。詳細については、アプリケーション ポリシーの作成、アプリケーション ポリシーの展開、およびアプリケーション ポリシーの編集を参照してください。

アプリケーションポリシーを展開する前に、Catalyst 9300 シリーズ スイッチおよび Cisco Catalyst 9500H シリーズ スイッチをプロビジョニングします。

2 つの異なる SSID で異なるビジネスとの関連性を持つ 2 つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは動作しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9000 シリーズスイッチに Catalyst 9800 組み込みワイヤレスを搭載したファブリックインアボックス

ファブリックインアボックスに関する情報

Cisco Catalyst 9000 シリーズ スイッチには、Cisco DNA Center を使用して設定できる、単一のスイッチでファブリックエッジ、コントロールプレーン、ボーダー、および組み込みのワイヤレス機能をホストする機能があります。

この機能を使用すると、小規模サイトの場所での設定が簡素化され、Cisco SD-Access の導入コストが削減されます。

Cisco Catalyst 9000 シリーズスイッチに CP+ ボーダー + エッジノードを追加する方法については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （68 ページ）を参照してください。

拡張性に関する情報

次の表に、デバイスの拡張性に関する情報を示します。

ファブリックの構造	Cisco Catalyst 9300 シリーズ スイッチ	Cisco Catalyst 9400 シリーズスイッチ	Cisco Catalyst 9500 シリーズスイッチ	Cisco Catalyst 9500-H シリーズスイッチ
仮想ネットワーク	256	256	256	256
ローカルエンドポイント/ホスト	4 K	4 K	4 K	4 K
SGT/DGT テーブル	8K	8K	8K	8K

ファブリックの構造	Cisco Catalyst 9300 シリーズ スイッチ	Cisco Catalyst 9400 シリーズ スイッチ	Cisco Catalyst 9500 シリーズ スイッチ	Cisco Catalyst 9500-H シリーズ スイッチ
SGACL（セキュリティ ACE）	5K	18K	18K	18K

リリース間コントローラモビリティの概要

リリース間コントローラモビリティ（IRCM）は、異なるソフトウェアバージョンのさまざまな シスコ ワイヤレス コントローラ で実行されるシームレスなモビリティとワイヤレスサービスをサポートします。

Cisco DNA Center Cisco DNA Center は、次のデバイスの組み合わせでゲストアンカー機能をサポートしています。

- アンカーコントローラとしての Cisco AireOS コントローラとフォーリンコントローラとしての Cisco AireOS コントローラの設定。
- フォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとゲストアンカーコントローラとしての Cisco AireOS コントローラの設定。
- アンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとフォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定。

コントローラデバイスでの IRCM の設定には、次の制約事項があります。

- フォーリンコントローラとしての Cisco AireOS コントローラの設定、およびアンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定はサポートされていません。
- ファブリックゲストアンカーの設定はサポートされていません。
- 複数のアンカーコントローラの設定、および 1 つのフォーリンコントローラの設定はサポートされていません。
- ゲスト SSID のみがサポートされています。
- ゲストアンカーモードでの非ゲストアンカー SSID のブロードキャストはサポートされていません。
- モビリティトンネルは暗号化されません。

ゲスト アンカーの設定とプロビジョニング

ゲスト アンカー シスコ ワイヤレス コントローラ を設定するには、次の手順に従います。

（注） ゲストアンカーの構成は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラではサポートされていません。

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、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

ステップ 2 AAA、DHCP、DNS サーバーなどのネットワーク サーバーを設定します。詳細については、グローバル ネットワーク サーバーの設定およびCisco ISE またはその他の AAA サーバーの追加を参照してください。

ステップ 3 Cisco Identity Services Engine を設定し、外部 Web 認証と中央 Web 認証を使用してゲスト ワイヤレス ネットワークの SSID を作成します。詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成」を参照してください。

ステップ 4 Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して ワイヤレスコントローラ を検出し、そのデバイスが **[Devices]** > **[Inventory]** ウィンドウに [Managed] 状態で表示されていることを確認します。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。

ステップ 5 アクティブなメイン ワイヤレスコントローラ として外部 ワイヤレスコントローラ をプロビジョニングします。「Cisco AireOS コントローラのプロビジョニング （30 ページ）」を参照してください。

ステップ 6 ゲスト アンカーとして ワイヤレスコントローラ のロールを選択し、ゲスト アンカー コントローラをプロビジョニングします。詳細については、「Cisco AireOS コントローラのプロビジョニング （30 ページ）」を参照してください。

ステップ 7 CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャルを設定します。詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、およびグローバル HTTPS クレデンシャルの設定を参照してください。

IRCM：Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラを検出します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

  詳細については、CDP を使用したネットワークの検出またはIP アドレス範囲を使用したネットワークの検出を参照してください。

- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、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るようになります。

新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

- AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

  詳細については、「AP の追加、配置、および削除」を参照してください。

- AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

  詳細については、グローバルネットワーク設定の管理、グローバル ネットワーク サーバーの設定、および「AAA サーバーの追加」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 を作成します。

  詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成」を参照してください。

- フォーリンコントローラとアンカーコントローラの WLAN プロファイル名は、モビリティに対して同じに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**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 フォーリンコントローラとしてプロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

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

ステップ 4 [Assign Site] ウィンドウで、[Choose a Site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスにサイトを割り当てます。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 10 アクティブなメイン ワイヤレスコントローラ では、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 11 [Assign Interface] エリアで、次の操作を実行します。

- [VLAN ID]：VLAN ID の値を入力します。
- [IP Address]：インターフェイス IP アドレスを入力します。

- [Gateway IP Address]：ゲートウェイ IP アドレスを入力します。
- [Subnet Mask (in bits)]：インターフェイスのネットマスクの詳細を入力します。

（注） Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを割り当てる必要はありません。

ステップ 12 [Next] をクリックします。

ステップ 13 [Summary] ウィンドウで、設定の詳細を確認します。

ステップ 14 [Deploy] をクリックし、Catalyst 9800 シリーズ ワイヤレス コントローラ をフォーリンコントローラとしてプロビジョニングします。

ステップ 15 **[Devices]** > **[Inventory]** ウィンドウで、ゲストアンカーコントローラとしてプロビジョニングする Cisco AireOS コントローラの横にあるチェックボックスをオンにします。

ステップ 16 手順 3 ～ 8 を繰り返します。

ステップ 17 Cisco AireOS コントローラのロールを [Guest Anchor] として選択します。

ステップ 18 ゲストアンカー ワイヤレスコントローラ の場合は、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 19 手順 11 ～ 14 を繰り返します。

Meraki デバイスのプロビジョニング

この手順では、Meraki ダッシュボードによって管理されている Cisco Meraki デバイスに SSID をプロビジョニングする方法について説明します。

始める前に

- Meraki ダッシュボードを Cisco DNA Center と統合します。Meraki ダッシュボードの統合を参照してください。
- SSID を作成します。エンタープライズ ワイヤレス ネットワーク用 SSID の作成を参照してください。

（注） Meraki ダッシュボードは、次の種類の SSID をサポートしています。

- [Open]：この SSID は、Meraki ダッシュボードの [Open] に対応しています。
- [WPA2 Personal]：この SSID は、Meraki ダッシュボードの [preshared key with WAP2] に対応しています。
- [WPA2 Enterprise]：この SSID は、Cisco Meraki ダッシュボードの Meraki 認証またはマイ Radius サーバーを使用した WAP-2 暗号化に対応しています。Cisco DNA Center におけるビルディングレベルのクライアントおよびエンドポイントの認証用に AAA サーバーまたは Cisco ISE サーバーを定義している場合は、その設定が Cisco Meraki ダッシュボードの [my Radius server] にプロビジョニングされます。それ以外の場合は、Meraki デバイスによる認証に [Meraki Radius] が使用されます。

すべての SSID に対して、インターフェイス名を選択できます。Cisco DNA Center で [Management] インターフェイスを選択した場合、VLAN ID は 0 です。つまり、Cisco Meraki ダッシュボードではサポートされないため、Cisco Meraki ダッシュボードでは VLAN タギングは無効になります。Cisco DNA Center で SSID のカスタムインターフェイスを作成すると、Cisco Meraki ダッシュボードで、カスタムインターフェイス名と VLAN ID を使用して AP タグが作成されます。

- ネットワークプロファイルを作成し、SSID がプロビジョニングされるサイトに割り当てます。

（注） Cisco DNA Center のネットワーク階層 [Sites] > [Buildings]は、Meraki ダッシュボードの [Organization] > [Network] に対応しています。ワークフローの [Add Sites to Profile] ウィンドウで、[Buildings] を選択することをお勧めします。

（注） Cisco DNA Center Meraki ネットワークを作成して、SSID をネットワークにプロビジョニングします。Meraki ダッシュボードは、Meraki ネットワーク構成を Meraki デバイスにプロビジョニングします。

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**[Provision]**。

[Network Devices] > **[Inventory]** ウィンドウが表示され、検出されたすべてのデバイスが示されます。

ステップ 2 Meraki ダッシュボードを表示するには、左側のペインで [Global] サイトを展開し、ビルディングを選択します。

選択したビルディングで使用可能なすべての Meraki ダッシュボードが表示されます。

ステップ 3 プロビジョニングする Meraki ダッシュボードの横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Assign Site] ウィンドウが表示され、Meraki ダッシュボードと関連付けられたビルディングを確認できます。

ステップ 5 関連付けられたビルディングを変更するには、[Choose a site] をクリックします。

ステップ 6 [Choose a site] ウィンドウで、ビルディングを選択して [Save] をクリックします。

ステップ 7 **[次へ (Next)]** をクリックします。

[設定（Configuration）] ウィンドウが表示されます。管理ビルディングは、プライマリロケーションで表示できます。

ステップ 8 Meraki ダッシュボードのセカンダリ管理ロケーションを選択するには、[Select Secondary Managed AP Locations] をクリックします。

ステップ 9 [Managed AP Location] ウィンドウで、ビルディング名の横にあるチェックボックスをオンにします。

ステップ 10 [Save] をクリックします。

ステップ 11 [Next] をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **Device Details**
- **ネットワーク設定**
- **SSID**

  （注） Meraki 展開では、各ネットワークで最大 15 の SSID がサポートされています。

- **管理サイト**

ステップ 12 [展開（Deploy）] をクリックします。

ステップ 13 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

展開が正常に完了すると、[デバイス インベントリ （Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。

ルーティングおよび NFV プロファイルのプロビジョニング

始める前に

ルーティングと NFV プロファイルをプロビジョニングする前に、次のグローバルネットワーク設定を定義したことを確認します。

- AAA、DHCP、および DNS 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 サーバーの設定を参照してください。
- CLI、SNMP、HTTP、HTTPS 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、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、およびグローバル HTTPS クレデンシャルの設定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」を参照してください。
- SP プロファイル。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」を参照してください。

（注） Cisco Firepower Threat Defense Virtual を NFV プロビジョニングフローを通じてプロビジョニングする場合、デフォルトのクレデンシャルユーザー名が保持され、パスワードはネットワーク設定でサイトに割り当てられたクレデンシャルプロファイルの設定に基づいて更新されます。

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

[Devices] > [Inventory] ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [Routers] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能なデバイスのリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 サイトで [Assign] をクリックすると、[Assign Device to Site] ウィンドウが表示されます。[Choose a Site] をクリックします。

ステップ 6 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

NFVIS デバイスをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。[O] をクリックして WAN の IP アドレスを入力します。[+Edit Services] ウィンドウで詳細を確認します。**[Next]** をクリックします。

  （注） vEdge 関連サービスをプロビジョニングする前に、[System Settings] ページで vManage 設定を構成する必要があります。詳細については、『Cisco DNA Center Administrator Guide』の「Configure vManage Properties」を参照してください。

- [ENCS Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Custom Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Summary] ページで詳細を確認します。

ルータをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。
  - 回線インターフェイスとしてギガビットイーサネットを選択した場合は [O] をクリックし、静的 IP アドレスを選択した場合は WAN IP アドレスを入力します。[DHCP] を選択した場合は、DHCP サーバーの IP アドレスを入力します。プライマリ WAN がすでに PnP を使用して設定されている

場合は、[Do Not Change] を選択して、ドロップダウンリストからプライマリ WAN として設定されているインターフェイスを選択します。

- 回線インターフェイスとしてセルラーを選択した場合は、[O] をクリックして、[IP Negotiated] を選択し、ドロップダウンリストから [Interface Name] を選択して [Access Point Name (APN)] を入力します。サービスプロバイダに応じて、[PAP] チェックボックスまたは [CHAP] チェックボックスをオンにします。
- 複数のサービスプロバイダを利用している場合は、バックアップ WAN インターフェイスの [IP SLA Address] を入力します。

仮想ルータをプロビジョニングしている場合、このウィンドウは表示されません。

- [Router LAN Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。

  [Interface(s)] ドロップダウンリストから 1 つの L3 インターフェイスまたは 1 つまたは複数の L2 インターフェイスを選択できるようになりました。

- [Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Summary] ページで詳細を確認します。

ステップ 7 [展開（Deploy）] をクリックします。

ステップ 8 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activity]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

    （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

展開が正常に完了すると、[デバイス インベントリ（Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。[SUCCESS] をクリックして詳細なプロビジョニング ログ ステータスを確認します。

VPC インベントリ収集

クラウドインベントリ収集が正常に完了すると、[Provision] セクションの [Cloud] タブに、収集した AWS VPC インベントリのビューが表示されます。左側のナビゲーションを展開して、クラウドプロファイルまたはアクセスキーのクラウド領域を表示できます。左側のナビゲーション項目をキーワードでフィルタ処理してクリックすると、選択した領域またはアクセスキーに対してのみ VPC が表示されます。

[VPC Inventory] ビューでは、VPC をクリックして、その VPC のサブネットや仮想インスタンスなどの詳細を確認することもできます。AWS VPC インベントリ収集は、すべてのインベントリ収集のデフォルト間隔で行われるようにスケジュールされており、クラウドアクセスキーの歯車メニューの [Sync] アクションを使用して、オンデマンドでトリガーすることもできます。インベントリ収集のステータスを表示するには、[VPC Inventory] ビューで [Show Sync Status] をクリックします。

ファイアウォール プロファイルのプロビジョニング

この手順では、Firepower Management Center（FMC）によって管理される Firepower Threat Defense（FTD）デバイスをプロビジョニングする方法について説明します。

始める前に

- FMC と Cisco DNA Center を統合します。Firepower Management Center の統合を参照してください。
- ネットワーク階層内でサイトを作成します。ネットワーク階層のサイトの作成を参照してください。
- ファイアウォールのネットワークプロファイルを作成し、FTDデバイスがプロビジョニングされるサイトに割り当てます。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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 プロビジョニングする FTD デバイスの横にあるチェックボックスをオンにして、[Site] 列の下にある [Assign] をクリックします。

ステップ 3 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 4 [Choose a Site] ウィンドウで、階層からサイトを選択して [Save] をクリックします。

ステップ 5 [Next] をクリックします。

ステップ 6 [Now] をクリックしてデバイスをサイトにすぐに割り当てるか、[Later] をクリックして特定の時間にスケジュールします。

ステップ 7 [**Assign**] をクリックします。

（注） **[Activities]** > **[Tasks]** で、サイトへのデバイスの割り当てのステータスを確認できます。

ステップ 8 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Provision Firewall Profile] ウィンドウが表示されます。

ステップ 9 [Confirm Profile] ページで詳細を確認し、[Next] をクリックします。

ステップ 10 [Firewall Type] ページで詳細を確認し、[Next] をクリックします。

[FTD Configuration] ページが表示されます。

ステップ 11 ルーテッドモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

ステップ 12 トランスペアレントモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択します。

b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択します。

c) [Bridge Virtual Interface] エリアを展開し、次の手順を実行します。

- [Bridge Group Number]：ブリッジグループ番号を入力します。有効な値は 1 ー 250 です。
- [IP]：FTD デバイスの IP アドレスを入力します。
- [Subnet Mask]：サブネットマスクを入力します。

ステップ 13 [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、デバイスの仕様の概要が表示されます。

ステップ 14 [Summary] ページで詳細を確認し、[Deploy] をクリックします。

[Provision Firewall device(s)] ダイアログボックスが表示されます。

ステップ 15 [Now]、[Later]、または [Generate configuration preview] オプションボタンをクリックします。

- [Now]：プロビジョニングがすぐに開始されます。
- [Later]：特定の時間にプロビジョニングがスケジュールされます。
- [Generate configuration preview]：選択したデバイスに展開するために後で使用できるプレビューを作成します。

ステップ 16 [Apply] をクリックします。

（注） **[Activities]** > **[Tasks]** で、ファイアウォールデバイスのステータスを確認できます。[Provision Firewall device(s)] ダイアログボックスで [Generate configuration preview] を選択した場合は、**[Activities]** > **[Work Items]** でステータスを表示できます

LAN アンダーレイのプロビジョニング

LAN 自動化を使用して、LAN アンダーレイをプロビジョニングします。

始める前に

- ネットワーク階層を設定します。（デバイスをサイトに追加する を参照）。
- 以下のグローバルネットワーク設定が定義済みであることを確認します。
  - AAA、DHCP、DNS サーバーなどのネットワークサーバー（グローバル ネットワーク サーバーの設定 を参照）。
  - CLI、SNMP、HTTP、HTTPS などのデバイスのクレデンシャル(グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、グローバル HTTPS クレデンシャルの設定を参照)。
  - IP アドレスプール（IP アドレス プールを設定する を参照）。
- インベントリに少なくとも 1 つのデバイス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検出します。

（注） 検出されたサイトがユーザー名「cisco」の CLI ログイン情報を使用して設定されている場合、LAN 自動化はブロックされます。

- ネットワークに Cisco Catalyst 9400 スイッチが設定されている場合は、LAN 自動化で 40G ポートが自動的に有効になるように設定されたスイッチで次の操作が実行されていることを確認します。
  - Day-0 設定はスイッチで実行されます。
  - 40G Quad Small Form-Factor Pluggable（QSFP）トランシーバはスーパバイザのポート 9 またはポート 10 のいずれかに挿入されます。スーパバイザ上の 1 ～ 8 のポートには、10G または 1G Small Form-Factor Pluggable（SFP）トランシーバは挿入されません。デュアル スーパーバイザ エンジンがある場合は、40G QSFP がポート 9 に挿入されていることを確認します。

    Catalyst 9400 シリーズ スーパーバイザの詳細については、『Cisco Catalyst 9400 Series Supervisor Installation Note』を参照してください。

ステップ 1 プロビジョニングするサイト用に IP アドレスプールを予約します。

（注） LAN 自動化 IP アドレスプールのサイズは、25 ビットのネットマスク以上である必要があります。

a) Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。
b) [Network Hierarchy] ペインで、サイトを選択します。
c) [Reserve] をクリックし、[Reserve IP Pool] ウィンドウで次のフィールドに値を入力して、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。
   - [IP Address Space]：[IPv4] または [IPv6] をオンにしてアドレスプールを作成します。デュアルスタックプールを作成するには、[IPv4] と [IPv6] の両方のチェックボックスをオンにします。
   - [Global IP Pool]：IP アドレスのすべてまたは一部を予約する IPv4 アドレスプール。

     （注） LAN 自動化では、IPv4 サブネットのみが使用されます。

   - [Prefix length / Number of IP Addresses]：グローバル IP アドレスプールのすべてまたは一部を予約するために使用する IP サブネットとマスクアドレス、または予約する IP アドレスの数。
   - [Gateway]：ゲートウェイ IP アドレス。
   - [DHCP Server(s)]：DHCP サーバーの IP アドレス。
   - [DNS Server(s)]：DNS サーバーの IP アドレス。
d) [Reserve] をクリックします。

ステップ 2 デバイスを検出してプロビジョニングします。

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

すべての検出されたデバイスが表示されます。

b) [Actions] > [Provision] > [LAN Automation] の順にクリックします。

c) [LAN Automation] ウィンドウで、次のフィールドに値を入力します。

- Primary Site：このサイトからプライマリデバイスを選択します。
- Peer Site：このサイトがピアデバイスの選択に使用されます。このサイトは、プライマリサイトとは異なる場合がありますので注意してください。
- Primary Device：Cisco DNA Center が新しいデバイスを検出しプロビジョニングする起点として使用するプライマリデバイスを選択します。
- Peer Device：ピアデバイスを選択します。
- SELECTED PORTS OF PRIMARY DEVICE：新規デバイスの検出とプロビジョニングに使用するポート。[Modify Selections] をクリックしてポート番号を入力します。
- Discovered Device Site：新たに検出されたすべてのデバイスがこのサイトに割り当てられます。このサイトは、プライマリサイトおよびピアサイトとは異なる場合があります。
- Main IP Pool：LAN 自動化用に予約された IP アドレスプール（ステップ 1 を参照）。
- Link Overlapping IP Pool：他のサイトと共有される IP アドレスプール。アンダーレイでポイントツーポイントリンクに対する /31 IP アドレスを設定するために使用されます。

  リンク重複 IP プールには、親サイトから継承されるサブプールか他のサイトで定義されているサブプールを指定できます。

  リンク重複 IP プールを使用すると、マルチサイト展開で /31 IP アドレスの重複が可能になります。異なるサイトのホストにおいて、/31 リンクで IP アドレスを再利用できます。

  リンク重複 IP プールを定義した場合、[Main IP Pool] フィールドで定義されたアドレスが管理 IP（ループバックアドレスや VLAN アドレスなど）に使用されます。
- ISIS Domain Password: LAN 自動化が開始するときにユーザーが指定する IS-IS パスワード。パスワードがすでにシードデバイスに存在する場合は、再使用され、上書きされることはありません。ユーザーが指定するパスワードが入力され、既存の IS-IS パスワードがデバイスにない場合、ドメインパスワードが使用されます。プライマリとセカンダリシードの両方がドメインパスワードをもつ場合、それらが一致することを確認してください。
- Enable Multicast：このチェックボックスをオンにすると、アンダーレイ ネイティブ マルチキャストが有効になります。LAN 自動化によって、シードデバイスを RP とし、検出されたデバイスをサブスクライバとするマルチキャストツリーが作成されます。
- Device Name Prefix：プロビジョニングしているデバイスの名前プレフィックス。Cisco DNA Center で各デバイスをプロビジョニングするときに、ここで指定されたテキストでデバイスにプレフィックスを付与し、末尾に一意の番号を追加します。たとえば、名前プレフィックスとして **Access** を入力した場合、各デバイスがプロビジョニングされると、Access-1、Access-2、Access-3 のように名前が付けられます。

- Choose a File：[Browse] をクリックして、ホスト名マップファイルを選択します。選択した CSV ファイルに記述されているシリアル番号とホスト名のマッピングを使用して、検出されたデバイスに対してユーザーが指定した名前が設定されます。検出されたデバイスがスタックの場合、スタックのすべてのシリアル番号が CSV ファイルで指定されます。

  CSV ファイルの例を次に示します。

```
standalone-switch,FCW2212L0NF
stack-switch,"FCW2212E00Y,FCW2212L0GV"
```

d) [Start] をクリックします。

Cisco DNA Center は、新規デバイスの検出とプロビジョニングを開始します。

LAN 自動化では、VLAN 1 のシードデバイスで IP アドレスを設定します。シードデバイスのこの VLAN 1 IP アドレスが Cisco DNA Center から到達できない場合は、[LAN Automation Status] ウィンドウにエラーメッセージが表示されます。エラーの詳細および可能な修復アクションを表示するには、このウィンドウの [See Details] リンクにマウスカーソルを合わせます。

ステップ 3 プロビジョニングしているデバイスの進行状況をモニターして確認します。

a) **[Actions]** > **[Provision]** > **[LAN Automation Status]** の順にクリックします。

[LAN Automation Status] ウィンドウに、デバイスのプロビジョニングの進捗状況が表示されます。

（注） 新しいデバイスのプロビジョニングには数分かかる場合があります。

b) すべてのデバイスが検出されてインベントリに追加され、管理状態になったら、[LAN Automation Status] ウィンドウで [Stop] をクリックします。

LAN 自動化プロセスが完了し、新規デバイスがインベントリに追加されます。

Cisco DNA Center システム証明書に FQDN のみの SAN フィールドがある場合、LAN 自動化が開始して In Progress 状態に移行した後、シードデバイスの DHCP プールを編集して、FQDN、B2 ー B1、dns-server、および domain-name を含むオプション 43 文字列を含める必要があります。DHCP プールを変更したときに、[Plug and Play] セクションのデバイスがエラー状態になっている場合は、[Plug and Play] ページから PnP リセットを実行して、デバイスに PnP プロセスを強制的に再起動させる必要があります。

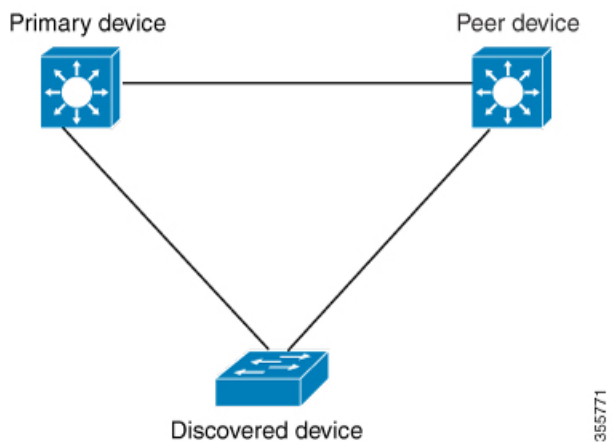
サンプル設定を次に示します。

```
ip dhcp pool nw_orchestration_pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80"
domain-name sitdns.com
dns-server 17.1.104.100
```

LAN 自動化のピアデバイスの使用事例

デュアル ホームのスイッチのプロビジョニング

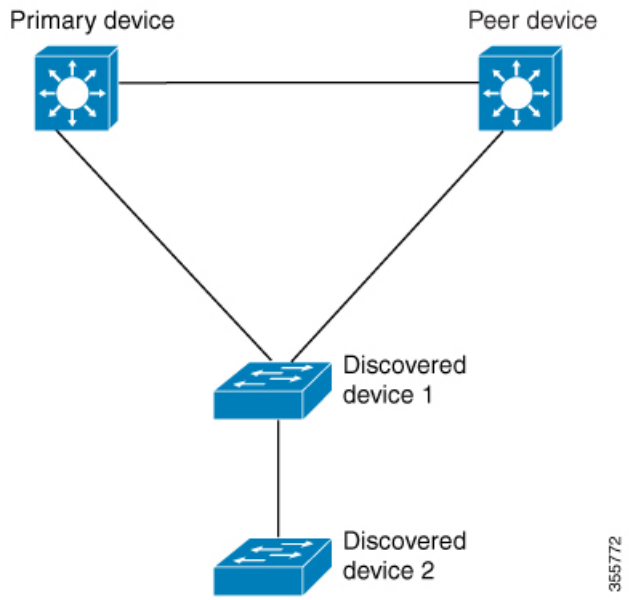
デュアル ホームのスイッチのプロビジョニングのために、常にピア デバイスを選択する必要があります。



Cisco DNA Center プライマリ デバイスで DHCP サーバーを設定します。Cisco DNA Center が検出されたデバイスがプライマリ デバイスとピア デバイスの両方に接続されていることを理解しているため、LAN 自動化タスクが停止されると、2 つのレイヤー 3 ポイントツーポイント接続を設定します。1 つの接続は、検出されたデバイスとプライマリ デバイスの間で確立されます。もう 1 つの接続は検出されたデバイスとピア デバイスの間で確立されます。

（注） LAN 自動化ジョブが実行される前に、プライマリ デバイスとピア デバイスの間のリンクが設定される場合、ピア デバイスを Cisco DNA Center のLAN 自動化設定の一部としてピア デバイスに接続するプライマリ デバイスのインターフェイスを選択する必要があります。

LAN 自動化の 2 段階制限



前述のトポロジの場合、Cisco DNA Center は次のリンクを設定します。

- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から プライマリ デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から ピア デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から 検出されたデバイス *2* に接続するためにルートする

検出されたデバイス *3*という名前のデバイスが以下の検出されたデバイス *2*に直接接続されるシナリオを考えてください。検出されたデバイス *2* と 検出されたデバイス *3*の間の接続は、LAN 自動化ジョブの一部として設定されません。プライマリ デバイスから 2 段階以上離れているためです。

LAN 自動化の状態を確認

実行中の LAN 自動化ジョブのステータスを確認できます。

始める前に

LAN 自動化ジョブを作成し、開始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**[Provision]** > **[Inventory]** の順に選択します。

すべての検出されたデバイスが表示されます。

ステップ 2 **[Actions]** > **[Provision]** > **[LAN Automation Status]** の順に選択します。
[LAN Automation Status] ウィンドウに、実行中と完了のすべての LAN 自動化ジョブのステータスが表示されます。

プロビジョニング後のデバイスの削除

- すでにファブリックドメインに追加されているデバイスを削除する場合、ファブリックドメインからそのデバイスを削除し、次に [Provision] メニューから削除します。
- **[インベントリ（Inventory）]** ウィンドウからデバイスを削除することはできません。代わりに、**[プロビジョニング（Provision）]** メニューからプロビジョニングしたデバイスを削除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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 検出され、プロビジョニングされたすべてのデバイスが表示される **[インベントリ（Inventory）]** タブをクリックします。

ステップ 3 削除するデバイスの横にあるチェックボックスをオンにします。

（注） APは、接続していたコントローラが削除された場合にのみ削除されます。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[デバイスの削除（Delete Device）]** を選択します。

ステップ 5 確認プロンプトで、[OK] 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。