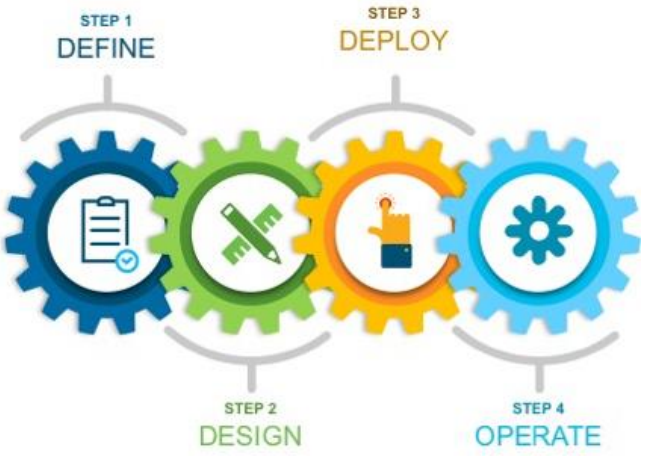
検証済みプロファイル：Cisco DNA Center を使用したワイヤレス自動化の展開

改訂：2024 年 5 月 21 日

Solution Overview

This guide explains how to use Cisco DNA Center 2.3.5.5 to deploy and manage a legacy wireless local area network (WLAN) within an enterprise network, using Cisco Catalyst 9800 シリーズ ワイヤレス コントローラs, Cisco IOS XE Cupertino 17.9.4a.

This guide provides technical guidance to design, deploy, and operate a Cisco WLAN using Cisco DNA Center.



This guide contains the following main sections:

- *Define the wireless network* presents a high-level overview of the campus, remote office, and cloud-based WLAN that is designed and deployed through Cisco DNA Center.
- *Design the wireless network* discusses the integration of Cisco DNA Center with Cisco Identity Services Engine (Cisco ISE); creation of the site hierarchy—including the importing of floor maps—within Cisco DNA Center; configuration of various network services necessary for network operations, such as AAA, DNS, DHCP, NTP, SNMP, and Syslog servers; and configuration of wireless settings, including WLANs/SSIDs, VLANs, and RF profiles for the WLAN deployment.
- *Deploy the wireless network* discusses discovery of the ワイヤレスコントローラs, managing the software images running on the ワイヤレスコントローラs, configuring HA SSO redundancy on the ワイヤレスコントローラs, provisioning the enterprise and guest ワイヤレスコントローラs within Cisco DNA Center, joining APs to the enterprise ワイヤレスコントローラ HA SSO pair, provisioning the APs within Cisco DNA Center, and positioning the APs on the floor maps within Cisco DNA Center.
- *Monitor and operate the wireless network* discusses how to use Cisco DNA Assurance to monitor and troubleshoot the WLAN deployment.

The audience for this guide includes network design engineers and network operations personnel who want to use Cisco DNA Center to deploy a Cisco WLAN within their wireless networks.

前提条件

エンタープライズ ネットワーク内でレガシー WLAN を展開および管理する前に、Cisco DNA Center をインストールし、適切に設定する必要があります。Cisco DNA Center のインストールおよび設定の詳細については、*Cisco DNA Center* 設置ガイド [英語] を参照してください。

次の表に、Cisco DNA Center と指定されたネットワーク要素間のラウンドトリップ時間（RTT）の要件を示します。

Cisco DNA Center アプライアンスと管理対象デバイス間の遅延は、100 ミリ秒 RTT 以下である必要があります。100 ミリ秒経過すると、インベントリ収集、プロビジョニング、イメージ更新（SWIM）などの特定のイベントの実行時間が長くなる可能性があります。シスコでは、300 ミリ秒を超える RTT をサポートしていません。RTT とサポートされるスケールの詳細については、*Cisco DNA Center* データシート [英語] を参照してください。

表 *1*：シスコ推奨の *RTT*

送信元デバイス	ターゲット デバイス	サポートされる最大 RTT
Cisco DNA Center ノード	Cisco DNA Center ノード	10 ミリ秒
Cisco DNA Center ノード	Cisco ISE	300 ミリ秒
Cisco DNA Center ノード	ワイヤレスコントローラ	200 ミリ秒
ワイヤレスコントローラ	アクセスポイント	20 ミリ秒（ローカルモード）
ワイヤレスコントローラ	アクセスポイント	300 ミリ秒（Flex モード）
ワイヤレスコントローラ	Cisco ISE	100 ミリ秒

表 *2*：ワイヤレスコントローラ モデルでシスコがサポートするスケール数値

ワイヤレスコントローラ モデル	最大 AP 数	最大クライアント数
Catalyst 9800-L	250	5000
Catalyst 9800-40	2000	32,000
Catalyst 9800-80	6000	64,000
Catalyst 9800-CL（4 CPU/8 GB RAM）	1000	10,000
Catalyst 9800-CL（6 CPU/16 GB RAM）	3000	32,000
Catalyst 9800-CL（10 CPU/32 GB RAM）	6000	64,000

表 *3 : Cisco DNA Center 1* ノードシステムスケール

SKU	DN-SW-APL	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
レガシーデバイス（スイッチ、ルータ、ワイヤレスコントローラ）	1000	1000	2000	5000
レガシー ワイヤレス アクセス ポイント	4000	4000	6000	13,000
ワイヤレスセンサー	600	600	800	1600
同時エンドポイント	25,000	25,000	40,000	100,000
一時エンドポイント（14 日間以上）	75,000	75,000	120,000	250,000
エンドポイントの比率：有線	いずれか	いずれか	いずれか	いずれか
エンドポイントの比率：ワイヤレス	いずれか	いずれか	いずれか	いずれか
サイト要素	2500	2500	5000	10,000
ワイヤレスコントローラ	500	500	1000	2000
ポート	48,000	48,000	192,000	768,000
API レート制限（API 数/分）	50	50	50	50
NetFlow（フロー/秒）	30,000	30,000	48,000	120,000
ソフトウェアイメージの同時更新	100	100	100	100

表 *4 : 3* ノード *DN2-HW-APL-XL* クラスタのスケール

説明	サポートされるスケール
デバイス（スイッチ、ルータ、ワイヤレスコントローラ）	10,000
ワイヤレス アクセス ポイント	25,000
同時エンドポイント	300,000
一時エンドポイント（14 日間以上）	750,000

説明	サポートされるスケール
NetFlow（フロー/秒）	250,000
フロアの数（ワイヤレスコントローラごと）	1000

必要なネットワークポート

Cisco DNA Center では、アプライアンスとの間で送受信されるトラフィックフローに対して特定のポートが開いている必要があります。ポートを開く方法（ファイアウォール設定またはプロキシゲートウェイを使用）は関係ありません。詳細については、*Cisco DNA Center 第 2 世代アプライアンス設置ガイド* [英語] の「必要なネットワークポート」のトピックを参照してください。

Cisco DNA Center の証明書の管理

Cisco DNA Center のデフォルトでは自己署名証明書が使用されますが、展開時に内部認証局によって署名された証明書を使用できます。デフォルトの証明書を置き換えるには、『*Cisco DNA Center* セキュリティのベストプラクティスガイド』の「証明書の管理」のトピックを参照してください。

ワイヤレスネットワークの定義

ここでは、Cisco DNA Centerを通じて設計および展開されるキャンパス、リモートオフィス、およびクラウドベースの WLAN の概要を示します。

3 種類の一般的なレガシーワイヤレス展開の概要を示す 3 つのシナリオがあります。最初のシナリオでは、ローカルモードの AP を使用したキャンパスのワイヤレス展開で、高可用性（HA）構成のワイヤレスコントローラを使用します。ワイヤレスコントローラは同じキャンパスのビルディングにあります。2 番目のシナリオでは、Flex モードの AP を使用したリモートオフィスのワイヤレス展開で、N+1 構成のワイヤレスコントローラを使用します。ワイヤレスコントローラはデータセンターにあります。3 番目のシナリオでは、企業イベントのワイヤレスネットワークで、Amazon Web Services（AWS）などのクラウド環境でホストされるワイヤレスコントローラを使用します。

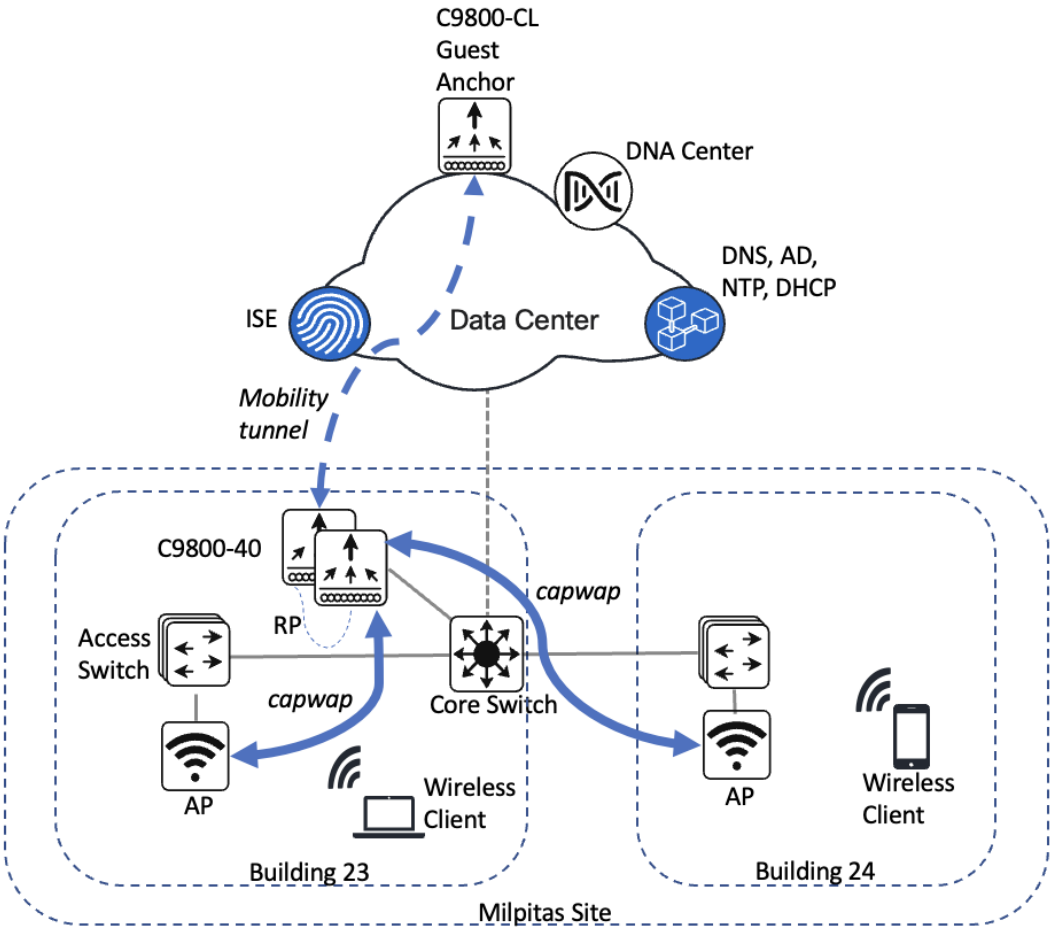
キャンパスのワイヤレス展開

キャンパスのワイヤレス展開では、高可用性（HA）SSO 設定で Cisco Catalyst 9800-40 ワイヤレスコントローラのペアを使用します。キャンパスの複数のビルディング内の複数のフロアに配置されているワイヤレスコントローラ ペアは、ローカルモードのアクセスポイント（AP）のエンタープライズ ワイヤレスコントローラ として機能します。ワイヤレスゲストアクセスは、従来のゲストワイヤレスコントローラとして機能し、エンタープライズ（外部）ワイヤレスコントローラにアンカーされている別の Cisco Catalyst 9800-CL ワイヤレスコントローラを介して提供されます。

WLAN の設計と展開は、インテントベース ネットワーク（IBN）を使用して完全に自動化されています。Cisco DNA Center は IBN 用に設計されており、デバイスレベルのユーザーインターフェイスから抽象化のレベルを提供します。

（注） 実稼働環境では、ゲストアンカー ワイヤレスコントローラ は通常、ファイアウォールの外にある DMZ セグメントに接続され、ゲスト ワイヤレス トラフィックを内部の従業員トラフィックから分離します。このような設計では、エンタープライズフォーリン ワイヤレスコントローラ とゲストアンカー ワイヤレスコントローラ の間で必要なトラフィックを許可するようにファイアウォールポリシーを設定する必要があります。

図 *1*:キャンパスのワイヤレス展開の概要設計



キャンパスのワイヤレス展開には、次の機能が含まれます。

- 単一のエリア（**Milpitas**）と複数のビルディング（**Building 23** および **Building 24**）で構成され、それぞれに複数のフロア（**Floor 1** および **Floor 2**）があるサイト階層
- すべてのワイヤレストラフィックがワイヤレスコントローラにバックホールされる、レガシー中央集中型キャンパスのワイヤレス展開
- エンタープライズ SSID とゲスト SSID
- HA SSO 構成のエンタープライズ Catalyst 9800-40 ワイヤレスコントローラの単一ペア

- エンタープライズ HA SSO ワイヤレスコントローラペアに自動的にアンカーされる専用ゲスト Catalyst 9800-CL ワイヤレスコントローラを介したゲストワイヤレスアクセス

（注） Cisco DNA Center CLI テンプレートは、インテントベースのプロファイルやモデル設定を使用して設定できない内容を設定するために使用できます。このガイドでは、Cisco DNA Center で設定できるワイヤレスコントローラの特定の機能について説明します。

ワイヤレスコントローラは、Cisco DNA Center のプロビジョニングプロセス中にサイトに割り当てる必要があります。この導入ガイドでは、Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（**C9800-40**）が **Milpitas** エリア内の **Building 23** に割り当てられます。1 つのフロアの AP には、一度に 1 つのプライマリエンタープライズ（非ゲスト）ワイヤレスコントローラのみが存在できます。つまり、Cisco DNA Center 内のフロアごとに 1 つのエンタープライズ ワイヤレスコントローラのみをプロビジョニングできます。**Building 23** 内の**Floor 1** と**Floor 2** の AP と**Building 24** 内の**Floor 1** の AP は、Cisco DNA Centerを介して **C9800-40** にプロビジョニングされます。

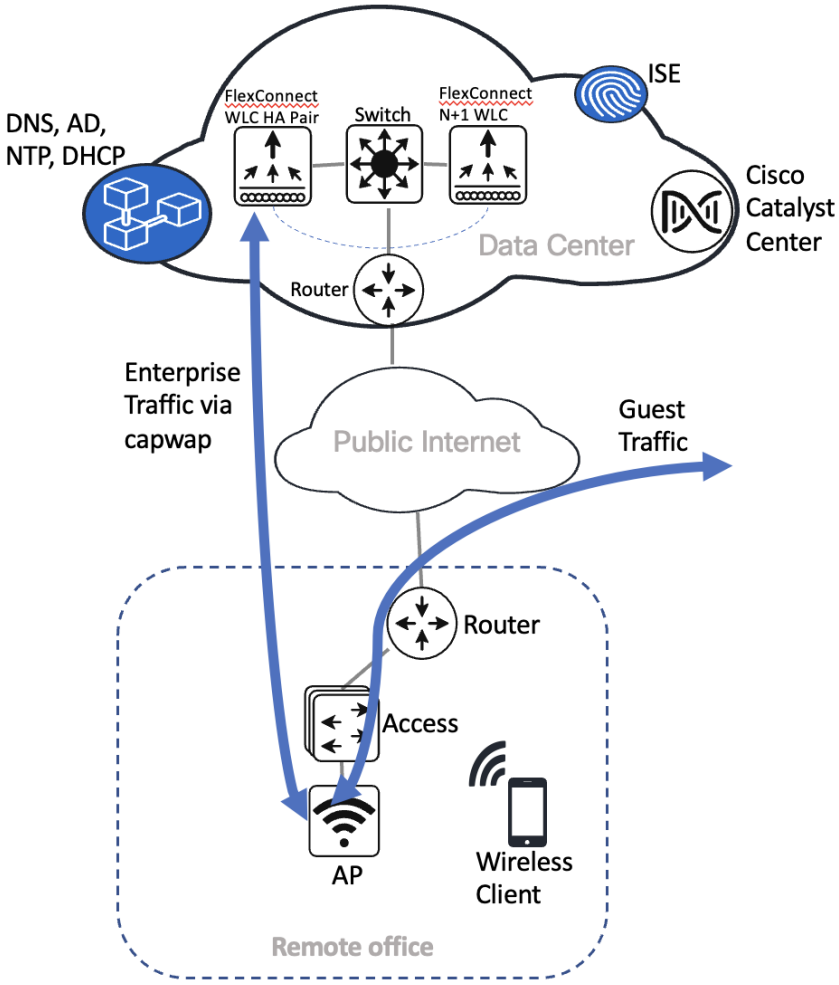
リモートオフィスのワイヤレス展開

リモートオフィスのワイヤレス展開では、高可用性（HA）N+1 構成で Cisco Catalyst 9800-40 ワイヤレスコントローラのペアを使用します。リモートオフィスビル内の複数のフロアにあるワイヤレスコントローラペアは、Flex モードのアクセスポイント（AP）のエンタープライズ ワイヤレスコントローラとして機能します。ワイヤレスゲストアクセスはローカルでスイッチングされ、従業員（非ゲスト）のワイヤレストラフィックは中央でスイッチングされます。従業員（WPA2/802.1X）またはゲスト（WebAuth）ワイヤレストラフィックの場合、すべての認証は Cisco ISE を介して一元的に実行されるため、AAA サーバーとゲストポータルの両方として Cisco ISE を使用することが強く推奨されています。

WLAN の設計と展開は、インテントベース ネットワーク（IBN）を使用して完全に自動化されています。Cisco DNA Center は IBN 用に設計されており、デバイスレベルのユーザーインターフェイスから抽象化のレベルを提供します。

（注） リモートオフィスでのダイレクト インターネット アクセス（DIA）を使用したローカル終端など、ゲスト ワイヤレス トラフィックの代替設計は、WLAN 機能と Cisco SD WAN を組み合わせた場合に実装できます。詳細については、*Cisco SD-WAN：ダイレクト インターネット アクセスの有効化* [英語] を参照してください。

図 *2:* リモートオフィスのワイヤレス展開の概要設計



リモートオフィスのワイヤレス展開には、次の機能が含まれます。

- 単一のエリア（**New York**）と複数のフロア（**Floor 1**、**Floor 2**、**Floor 3**）がある単一のビルディング（**Branch 5**）で構成されるサイト階層
- データトラフィックがエンタープライズ SSID に対して中央でスイッチングされ、ゲスト SSID に対してローカルにスイッチングされるレガシー Flex モード
- エンタープライズ SSID とゲスト SSID
- HA N+1 構成のエンタープライズ Catalyst 9800-40 ワイヤレスコントローラの単一ペア

（注） Cisco DNA Center CLI テンプレートは、インテントベースのプロファイルやモデル設定を使用して設定できない内容を設定するために使用できます。

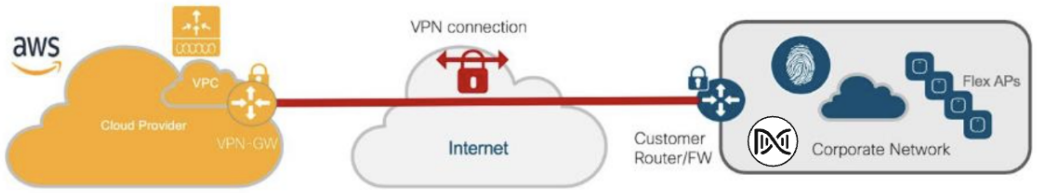
ワイヤレスコントローラは、Cisco DNA Centerのプロビジョニングプロセス中にサイトに割り当てる必要があります。この導入ガイドでは、Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（**C9800-40**）は、データセンターに物理的に配置されている場合でも、**New York** エリア内の **Branch 5** に割り当てられます。1 つのフロアの AP には、一度に 1 つのプライマリエンタープライズ（非ゲスト）ワイヤレスコントローラのみ存在できます。つまり、Cisco DNA Center 内のフロアごとに 1 つのエンタープライズ ワイヤレスコントローラのみをプロビジョニングできます。**New York** の **Branch 5** 内の **Floor 1** と **Floor 2** の AP は、Cisco DNA Centerを介して **C9800-40** にプロビジョニングされます。

AWS 展開でホストされるワイヤレスコントローラ

このワイヤレス展開では、Amazon Web Services（AWS）でホストされる Cisco Catalyst 9800-CL ワイヤレスコントローラを使用します。イベントセンターフロアにあるワイヤレスコントローラは、Flex モードのアクセスポイント（AP）のエンタープライズ ワイヤレスコントローラとして設定されます。従業員（WPA2/802.1X）またはゲスト（WebAuth）のワイヤレストラフィックの場合、すべての認証は Cisco ISE を介して一元的に実行されてデータセンターに配置されます。

Cisco DNA Center は IBN 用に設計されており、デバイスレベルのユーザーインターフェイスから抽象化のレベルを提供します。

図 *3 : AWS* でホストされる *Cisco Catalyst 9800-CL*ワイヤレスコントローラ の概要設計



このワイヤレス展開には、次の機能が含まれます。

- 単一のエリア（**San Jose**）と単一のフロア（**Eventcenterfloor**）があるイベントセンター（**Eventcenter**）で構成されるサイト階層
- すべてのワイヤレストラフィックがワイヤレスコントローラにバックホールされるレガシー Flex ワイヤレス展開
- データトラフィックがローカルにスイッチングされる Flex モード
- エンタープライズ SSID および企業の特別イベント SSID
- AWS でホストされる Catalyst 9800-CL ワイヤレスコントローラ

（注） Cisco DNA Center CLI テンプレートは、インテントベースのプロファイルやモデル設定を使用して設定できない内容を設定するために使用できます。

ワイヤレスコントローラは、Cisco DNA Centerのプロビジョニングプロセス中にサイトに割り当てる必要があります。この導入ガイドでは、AWS 上の Catalyst 9800 ワイヤレスコントローラ（**C9800-CL**）が **San Jose** エリア内の **Eventcenter** に割り当てられます。1 つのフロアの AP には、一度に 1 つのプライマリエンタープライズ（非ゲスト）ワイヤレスコントローラのみ存在できます。つまり、Cisco DNA Center 内のフロアごとに 1 つのエンタープライズ ワイヤレスコン

トローラのみをプロビジョニングできます。**Eventcenter** 内の **Eventcenterfloor** の AP は、Cisco DNA Center を介して AWS 上 の **C9800-CL** にプロビジョニングされます。

レガシーネットワークからの移行

ここでは、Cisco AireOS ワイヤレスコントローラ または Cisco Prime Infrastructure を使用したレガシーネットワークからの次の移行に関する概要について説明します。

- レガシー Cisco AireOS ワイヤレスコントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- Cisco Prime Infrastructure から Cisco DNA Center

レガシー Cisco AireOS ワイヤレスコントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの AP の移行

ここでは、アクセスポイント（AP）をレガシー Cisco AireOS ワイヤレスコントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに移行する方法について説明します。この移行に必要な AireOS の最小バージョンは、IRCM をサポートしている 8.5 です。

手順

ステップ 1 Cisco AireOS ワイヤレスコントローラによって管理されるレガシーサイトに一時的なフロアを追加します。

ステップ 2 Catalyst 9800 シリーズ ワイヤレス コントローラを検出し、新たに追加されたフロアを管理するレガシーサイトに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 3 インターフェイスの詳細（レガシーフローの VLAN など）を入力します。

ステップ 4 Cisco AireOS ワイヤレスコントローラと Catalyst 9800 シリーズ ワイヤレス コントローラの間のモビリティトンネルを設定します。

ステップ 5 次のいずれかの方法を使用して、AP を Catalyst 9800 シリーズ ワイヤレス コントローラに移行します。

（注） AP は、AP 設定ワークフローを使用して新しいワイヤレスコントローラに移行され、新しいワイヤレスコントローラがプライマリ ワイヤレスコントローラとして設定されます。

a) 反復移行：フロア上の特定の AP のみが移行されます（Milpitas/Building 23/Floor2）。

1. 1 つのフロアで、Cisco AireOS ワイヤレスコントローラ から Catalyst 9800 シリーズ ワイヤレス コントローラに移動する必要がある AP をいくつか特定します。

   1 つのフロアにあるすべての AP を選択しないでください。

2. Catalyst 9800 シリーズ ワイヤレス コントローラによって管理される新しい一時的なフロア（Floor 2_1）を作成します。

3. AP 設定ワークフローを使用して、AP のサブセットを Catalyst 9800 シリーズ ワイヤレス コントローラに移動します。

   ワークフローを通じて、Catalyst 9800 シリーズ ワイヤレス コントローラがプライマリ ワイヤレスコントローラとして設定されます。

4. AP のサブセットが Catalyst 9800 シリーズ ワイヤレス コントローラに参加したら、Floor 2_1 の一部である Catalyst 9800 シリーズ ワイヤレス コントローラに AP をプロビジョニングします。

   この時点で、AP のサブセットは Catalyst 9800 シリーズ ワイヤレス コントローラによって管理され、残りの AP は Cisco AireOS ワイヤレスコントローラによって管理されるため、そのフロアではサービスの中断は発生しません。

5. 残りの AP をフロアから Catalyst 9800 シリーズ ワイヤレス コントローラに繰り返し移動します。

b) フロアごとの移行：フロア上の AP のセット全体が Catalyst 9800 シリーズ ワイヤレス コントローラに移行されます。

1. Catalyst 9800 シリーズ ワイヤレス コントローラによって管理される新しい一時的なフロア（Floor 2_1）を作成します。
2. 1 つのフロアにあるすべての AP を Catalyst 9800 シリーズ ワイヤレス コントローラに移動します。
3. Floor 2_1 の一部である Catalyst 9800 シリーズ ワイヤレス コントローラに AP をプロビジョニングします。
4. 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て Floor 2 を管理します。
5. 繰り返し実行するか、フロア全体で、AP を Floor 2 にプロビジョニングします。
6. 一時的なフロア、Floor 2_1 を削除します。
7. 目的のサイト、ビルディング、およびフロアに対して、サブステップ b の最初の 6 つのステップを繰り返します。
8. ステップ 1 で作成した一時的なフロアを削除します。

ステップ 6 （任意）config cleanup オプションを使用して、インベントリから Cisco AireOS ワイヤレスコントローラを削除します。

Cisco Prime Infrastructure から Cisco DNA Center への移行

始める前に

- *Cisco Prime Infrastructure と Cisco DNA Center の互換性マトリックス* [英語] を使用して、Cisco DNA Center のバージョンと互換性のある Prime Data Migration Tool（PDMT）リリースを特定します。
- Cisco Software Download Tool を使用して、互換性のある PDMT リリースをダウンロードします。

手順

ステップ 1 Cisco Prime Infrastructure Cisco DNA Center Assessment and Readiness Tool（PDART）を使用して、準備状況チェックを実行します。

PDART の使用方法の詳細については、『PDART（Cisco DNA Center Readiness Tool）の使用』を参照してください。

ステップ 2 移行の準備状況を評価したら、PDMT を使用して、Cisco Prime Infrastructure から Cisco DNA Center にサイトとデバイスを移行します。

ワイヤレスネットワークの設計

「前提条件」の説明に従って、前提条件が満たされていることを確認します。

ここでは、以下のトピックとプロセスについて説明します。

- Cisco Identity Services Engine（ISE）と Cisco DNA Center の統合
- Cisco ISE とサードパーティ AAA サーバー
- Cisco DNA Center でのサイト階層の設定
- ネットワーク運用のためのネットワークサービスの設定
- キャンパスのワイヤレス展開の設定
- リモートオフィスのワイヤレス展開の設定
- AWS でホストされる Cisco Catalyst 9800-CL ワイヤレスコントローラの設計

Cisco ISE と Cisco DNA Center の統合

Cisco Identity Services Engine（ISE）と Cisco DNA Center を統合することで、2 つのプラットフォーム間で、デバイスやグループ情報などの情報を共有できます。このガイドに固有の統合により、Cisco DNA Center のワークフローを介して Cisco ISE にゲストポータルを作成できます。ゲストポータルは、Cisco DNA Center のワイヤレスプロファイル内でゲスト ワイヤレス ネットワークが定義されると作成されます。詳細については、キャンパスのワイヤレス展開の設定（33 ページ）を参照してください。

次の手順を使用して、Cisco ISE と Cisco DNA Center を統合します。

- Cisco ISE を認証ポリシーサーバーとして設定する

  「Cisco DNA Center に対する認証およびポリシーサーバーとしての Cisco ISE の設定 （13 ページ）」を参照してください。

- Cisco DNA Center から Cisco ISE への pxGrid 接続を許可する

  Cisco pxGrid Cloud ソリューションガイド [英語] の「Cisco pxGrid Cloud and Cisco ISE Integration」のトピックを参照してください。

Cisco ISE とサードパーティ AAA サーバー

Cisco DNA Center では RADIUS および TACACS+ 認証用のサードパーティ AAA サーバーがサポートされていますが、Cisco ISE ではエンドポイントの追加分析が提供されます。

Cisco DNA Center に対する認証およびポリシーサーバーとしての Cisco ISE の設定

始める前に

このアクションを完了するには、ユーザープロファイルに SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE を割り当てる必要があります。

手順

ステップ 1 IP アドレスまたは完全修飾ドメイン名を使用して、Cisco DNA Center Web コンソールにログインします。

例：

https://<Cisco_DNA_Center_IPaddr_or_FQDN>

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 3 左側のペインの [External Service] ドロップダウンリストから、[Authentication and Policy Servers] を選択します。

ステップ 4 [Add] ドロップダウンリストから、[ISE] を選択します。

[Add ISE server] slide-in paneが表示されます。

ステップ 5 必須フィールドにサーバーの詳細を入力します。

次の表に、[Add ISE server] slide-in paneのフィールドの説明を示します。

フィールド	設定	説明
サーバの IP アドレス（Server IP Address）	テキストフィールド	Cisco ISE サーバーの IP アドレス。複数の IP アドレスが設定されている場合は、この IP アドレスが Cisco ISE 展開インスタンスに表示されていることを確認します。
共有秘密鍵（Shared Secret）	テキストフィールド	Cisco ISE サーバーとの通信にネットワークデバイスによって使用される共有秘密。IOS XE デバイス設定内では、PAC キーと呼ばれます。
[ユーザー名（Username）]	テキストフィールド	Cisco ISE のインストール時に作成したデフォルトのネットワーク管理者アカウントのユーザー名。
パスワード（Password）	テキストフィールド	Cisco ISE のインストール時に作成したデフォルトのネットワーク管理者アカウントのパスワード。
[FQDN]	テキストフィールド	Cisco ISE サーバーの完全修飾ドメイン名。

フィールド	設定	説明
Virtual IP Address	テキストフィールド	1 つ以上のポリシーサービスノード（PSN）を単一のロードバランサの背後に配置できます。配置する場合、[Virtual IP] フィールドにロードバランサの IP を追加できます。
[Advanced Settings] > [Protocol]	[Multiple Choice] オプションボタン	認証プロトコルを決定します。次のプロトコルオプションから選択できます。 • [RADIUS]：デフォルト設定。RADIUS プロトコルを使用します。 • [TACACS]：TACACS プロトコルを使用します。
[Advanced Settings] > [Authentication Port]	テキストフィールド	[RADIUS] を選択した場合、デフォルトポートは 1812 です。
[Advanced Settings] > [Accounting Port]	テキストフィールド	[RADIUS] を選択した場合、デフォルトポートは 1813 です。
[Advanced Settings] > [Port]	テキストフィールド	このフィールドは、[TACACS] が選択されている場合にのみ表示されます。デフォルト ポートは 49 です。
[Retries]	番号（Number）	認証が失敗するまでの再試行回数。デフォルトの試行回数は 3 回です。
Timeout (seconds)	番号（Number）	試行がタイムアウトするまでの秒数。デフォルトは 4 秒です。

この設計および導入ガイドでは、次の情報が入力されています。

フィールド	値
サーバの IP アドレス（Server IP Address）	172.23.240.152
Shared Secret	—
Cisco ISE サーバ	点灯
[ユーザー名（Username）]	admin
Password	—
[FQDN]	cvdise31.cagelab.local
Subscriber Name	admin
SSH Key	—
Virtual IP Address	—

フィールド	値
[Advanced Settings] > [Protocol]	RADIUS
[Advanced Settings] > [Authentication Port]	1812
[Advanced Settings] > [Accounting Port]	1813
[Retries]	3
Timeout (seconds)	4

（注） Cisco ISE を追加する前に、次の前提条件を満たしていることを確認します。

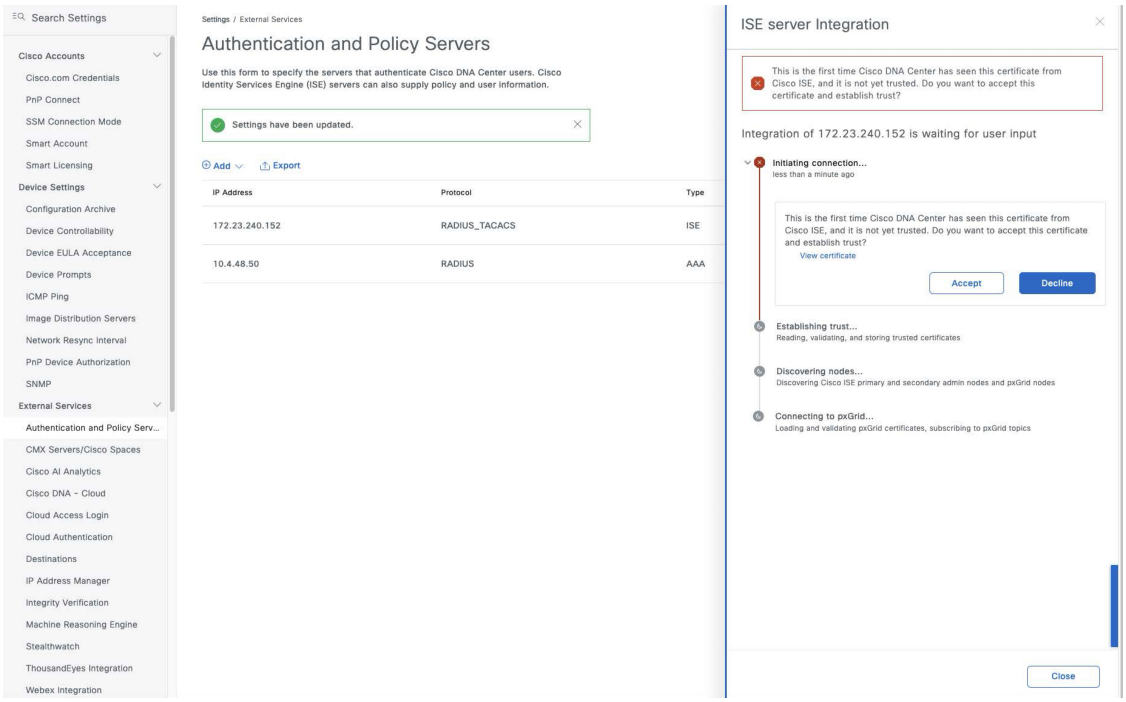
- Cisco ISE のバージョンと Cisco DNA Center のバージョンに互換性がある。

  詳細については、『*Cisco DNA Center* Compatibility Matrix』を参照してください。

- Cisco ISE GUI パスワードが Cisco ISE CLI パスワードと一致している。
- Cisco ISE 展開インスタンスに対して pxGrid が有効になっている。
- Cisco ISE サーバーの ERS が読み取り/書き込みに対して有効になっている。

ステップ 6 [Add] をクリックして、Cisco DNA Center 内に Cisco ISE サーバーを作成します。

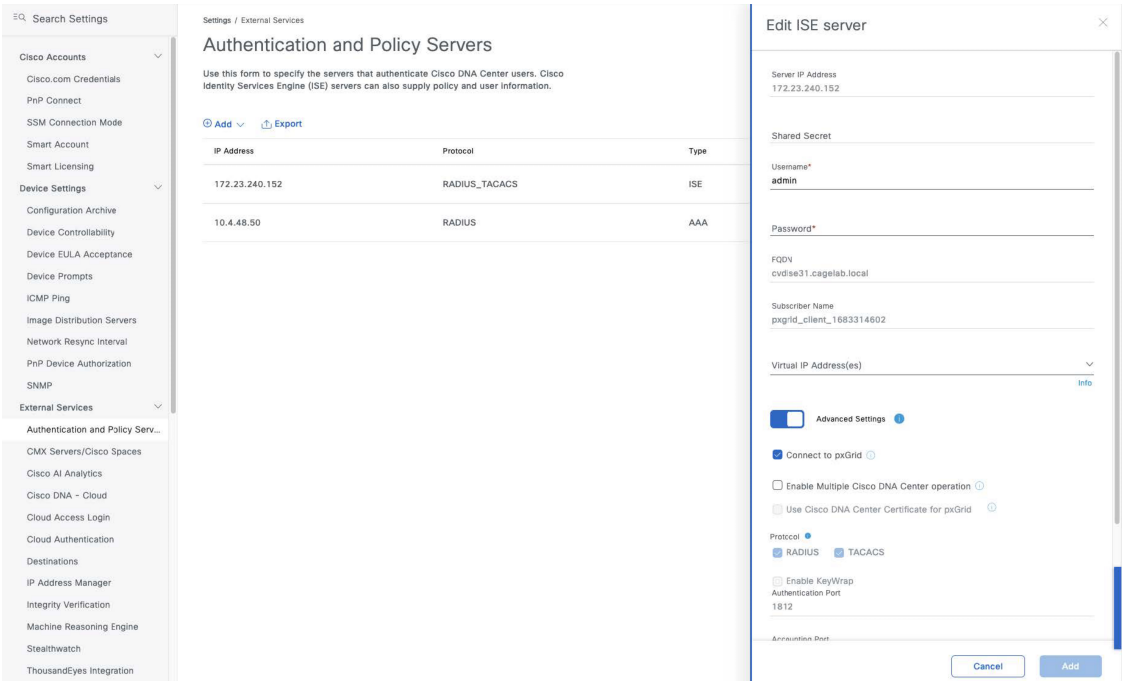
[ISE server Integration] slide-in paneに、Cisco ISE 証明書の受け入れと信頼の確立に関するメッセージが表示されます。



ステップ 7 [承認（Accept）] をクリックします。

統合が完了すると、[Authentication and Policy Servers] ウィンドウが表示されます。新しい Cisco ISE サーバーに [ACTIVE] ステータスが表示されます。

サーバーの設定を変更する場合は、[Actions] 列で省略記号アイコン（ ••• ）の上にカーソルを置き、[Edit] を選択します。



サイト階層の設定とフロアマップのインポート

サイト階層の設定には、展開用のネットワークサイトの定義と、エリア、ビルディング、およびフロアで構成されるネットワークサイトの階層関係の定義が含まれます。子サイトは親サイトから一定の属性を自動的に継承しますが、子サイト内の属性はオーバーライドできます。

次の表に、このガイドのサイト階層の概要を示します。複数のフロア（**Floor 1** と **Floor 2**）がある複数のビルディング（**Building 23** と **Building 24**）を含む単一のエリア（**Milpitas**）がプロビジョニングされます。

名前	サイトのタイプ	Parent	その他の情報
Milpitas	Area	グローバル	—
Building 23	Building	Milpitas	住所：560 McCarthy Boulevard、Milpitas、California 95035
Building 24	Building	Milpitas	住所：510 McCarthy Boulevard、Milpitas、California 95035

名前	サイトのタイプ	Parent	その他の情報
Floor 1	フロアー	Building 23	寸法：約 60 m（200 フィート）X 約 83 m（274 フィート）X 約 3 m（10 フィート） このフロアの AP は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ HA ペアにプロビジョニングされます。
Floor 2	フロアー	Building 23	寸法：約 60 m（200 フィート）X 約 83 m（274 フィート）X 約 3 m（10 フィート） このフロアの AP は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ HA ペアにプロビジョニングされます。
Floor 1	フロアー	Building 24	寸法：約 60 m（200 フィート）X 約 76 m（250 フィート）X 約 3 m（10 フィート） このフロアの AP は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ HA ペアにプロビジョニングされます。
Floor 2	フロアー	Building 24	寸法：約 60 m（200 フィート）X 約 76 m（250 フィート）X 約 3 m（10 フィート） このフロアの AP は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ HA ペアにプロビジョニングされます。

この項には、次のプロセスが含まれています。

- エリアの作成
- エリア内のビルディングの作成
- ビルディングフロアの作成
- Cisco DNA Center GUI を使用するか、Cisco Prime Infrastructure または Ekahau からインポートして、計画済み AP を作成して配置する

エリアの作成

始める前に

このアクションを完了するには、ユーザープロファイルに SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE を割り当てる必要があります。

手順

ステップ 1 IP アドレスまたは完全修飾ドメイン名を使用して、Cisco DNA Center Web コンソールにログインします。

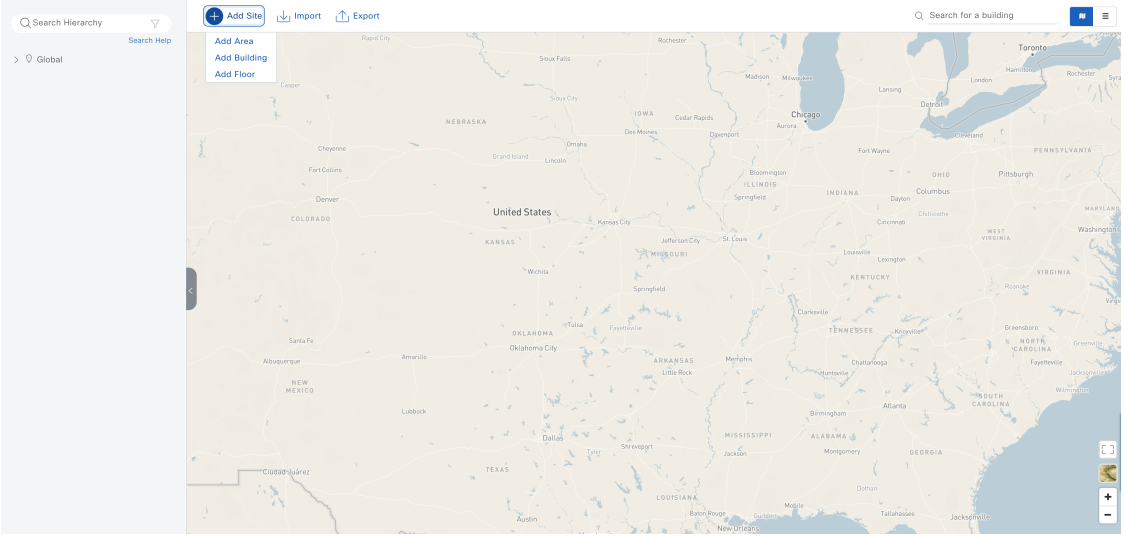
例：

https://<Cisco_DNA_Center_IPaddr_or_FQDN>

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

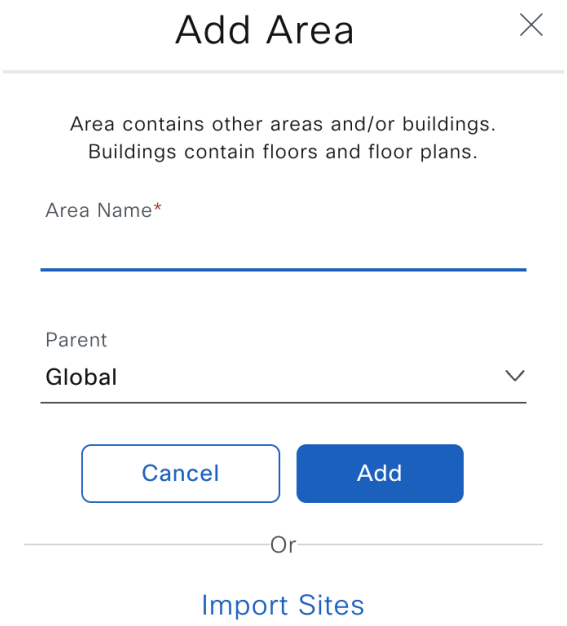
[Network Hierarchy] ウィンドウが表示されます。

初めてネットワーク階層を設定した場合は、左側の階層ペインに 1 つの [Global] エントリのみが表示されることがあります。



ステップ 3 **[+ Add Site]** > **[Add Area]**の順にクリックします。

[Add Area] ダイアログボックスが表示されます。



ステップ 4 [Add Area] ダイアログボックスの [Parent] ドロップダウンリストから、[Area Name] を入力して目的の親を選択します。

この導入ガイドでは、[Parent] として [Global] を選択し、[US] という名前のエリア内に [Milpitas] という名前のエリアを作成します。

ステップ 5 [Add]をクリックします。

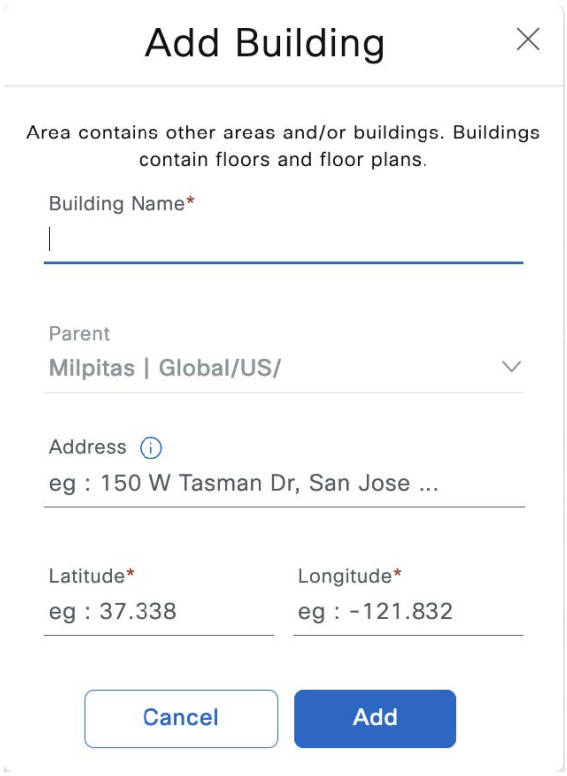
エリア内のビルディングの作成

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 **[+ Add Site]** > **[Add Building]**の順にクリックします。

[Add Building] ダイアログボックスが表示されます。



ステップ 3 [Add Building] ダイアログボックスで、[Building Name] を入力し、[Parent] ドロップダウンリストから目的のエリアを選択します。

この導入ガイドでは、[Building Name] に **Building 23** と入力します。[Parent] で [Milpitas | Global/US] を選択します。

ステップ 4 次のいずれかの方法を使用して、ビルディングの住所または GPS 座標を入力します。

- [Address] フィールドにビルディングの住所を入力し、使用可能なオプションのリストから正しい住所を選択します。選択した住所の [Latitude] フィールドと [Longitude] フィールドに、緯度と経度が自動的に入力されます。
- [Latitude] フィールドと [Longitude] フィールドにビルディングの GPS 座標を入力します。GPS 座標を入力する場合は、住所を入力する必要はありません。

この導入ガイドでは、**Building 23** に設定されている住所 **560 McCarthy Boulevard, Milpitas, California 95035** を入力します。

ステップ 5 [追加（Add）] をクリックします。

この導入ガイドでは、ステップ 1 ～ 5 を繰り返して、**Milpitas** エリアに 2 番目のビルディング **Building 24** を追加します。

ビルディングフロアの作成

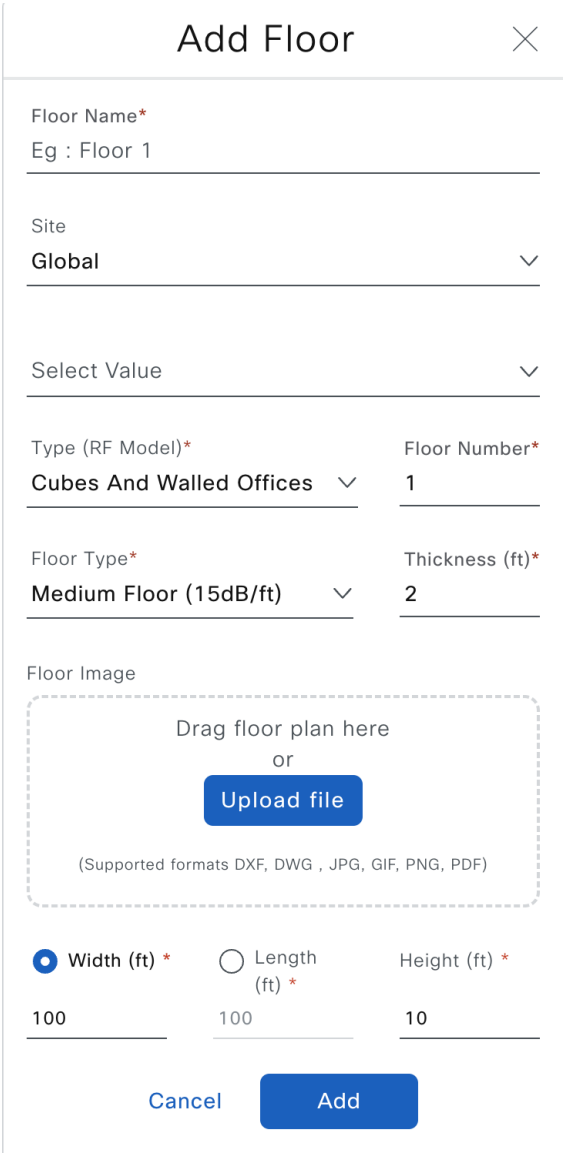
AP の場所とワイヤレスカバレッジ（ヒートマップ）は、フロアマップから表示できます。フロアはワイヤレスプロビジョニング時に参照されます。

手順

ステップ 1　左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2　**[+ Add Site]** > **[Add Floor]**の順にクリックします。

[Add Floor] ダイアログボックスが表示されます。



ステップ 3 [Add Floor] ダイアログボックスで [Floor Name] を入力し、[Site] ドロップダウンリストから目的のエリアを選択します。

この導入ガイドでは、[Floor Name] に **Floor 1** と入力します。[Site] には [Milpitas | Global/US] を選択し、[Building] には [Building 23 | Global/US/Milpitas/] を選択します。

ステップ 4 [Type (RF Model)] ドロップダウンリストから適切なスペースタイプを選択し、関連する [Floor Number] を入力します。

ステップ 5 [Floor Type] ドロップダウンリストから適切なフロアタイプを選択し、関連する [Thickness (ft)] を入力します。

ステップ 6 次のいずれかの方法を使用して、[Floor Image] エリアにフロアプランを追加します。

- フロアプランファイルを [Floor Image] エリアにドラッグアンドドロップします。
- [Upload file] をクリックして、アップロードするフロアプランファイルを選択します。

（注） DXF、DWG、JPG、GIF、または PNG 形式のフロアマップ図がある場合は、定義済みの任意のフロアに追加できます。Cisco Prime Infrastructure からエクスポートされたマップアーカイブをインポートする場合は、Cisco DNA Center で設定されたサイト階層が Cisco Prime Infrastructure で設定されたサイト階層と同じであることを確認します。

ステップ 7 [Width (ft)] オプションボタンをクリックし、フロアの幅をフィート単位で入力します。

ステップ 8 [Length (ft)] オプションボタンをクリックし、フロアの長さをフィート単位で入力します。

ステップ 9 [Height (ft)] フィールドに、天井の高さをフィート単位で入力します。

（注） フロアの幅、フロアの長さ、および天井の高さを追加すると、フロアプランを正しく見積り、ワイヤレスカバレッジ（ヒートマップ）と AP の配置に影響を与えることができます。

この導入ガイドでは、[Width (ft)] に **200**、[Length (ft)] に **275**、[Height (ft)] に **10** と入力します。

ステップ 10 [追加（Add）] をクリックします。

この導入ガイドでは、ステップ 1 ～ 10 を 3 回繰り返して、**Floor 2** を **Building 23** に、**Floor 1** を **Building 24** に、**Floor 2** を **Building 24** に追加します。

Cisco DNA Center での計画済み AP の作成と配置

次の 3 つの方法で、フロアマップの計画済み AP を取得できます。

- Cisco DNA Center UI で計画済み AP を作成する
- Cisco Prime Infrastructure からエクスポートされたマップをインポートする
- Ekahau からエクスポートされたマップをインポートする

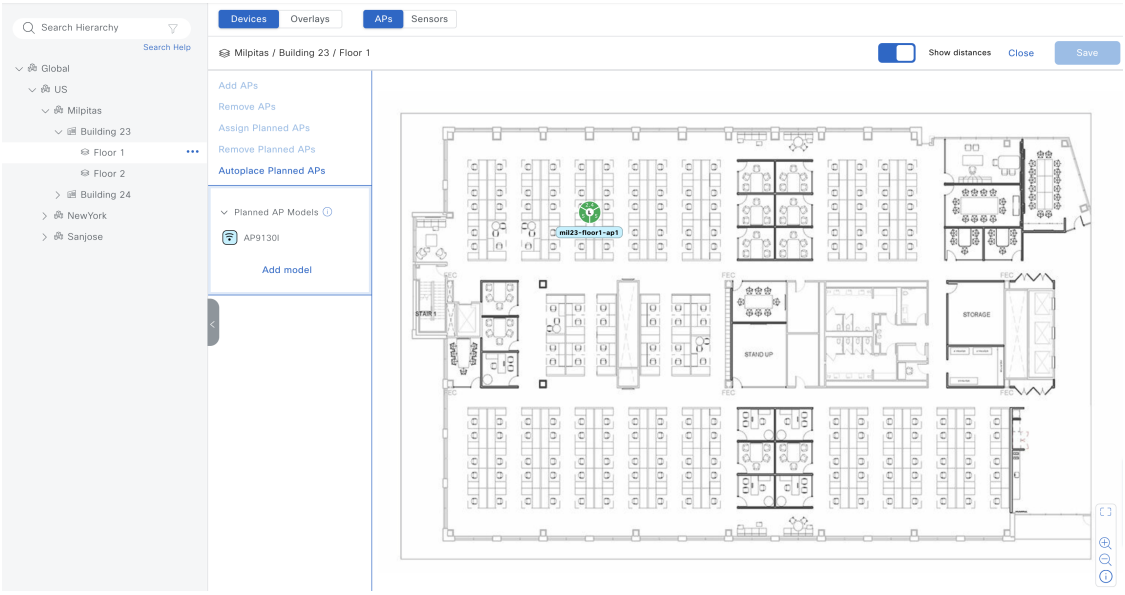
手順

ステップ 1　左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2　左側の階層ペインの [Global] ドロップダウンリストから、AP に必要なフロアを選択します。

ステップ 3　[追加/編集（Add/Edit）] をクリックします。

ステップ 4　[Planned AP Models] ドロップダウンリストから、[Add Model] をクリックします。



ステップ 5　[Select AP models to add] ダイアログボックスで、ドロップダウンリストから AP モデルを選択します。

ステップ 6　[Add AP models] をクリックします。

ステップ 7　[Planned AP Models] ドロップダウンリストから、目的の AP モデルを選択します。

ステップ 8　フロアマップで、AP の目的の場所にカーソルを移動し、その場所をクリックします。

ステップ 9　[Edit Planned AP] スライドインペインで、[Planned AP Name] が実際の AP ホスト名と一致していることを確認します。

X が付いた赤色の 8 角形が表示されている場合は、[Antenna] ドロップダウンリストから [Antenna] を選択します。

ステップ 10　[Save] をクリックします。

Cisco Prime Infrastructure からのマップのインポート

始める前に

ここでは、マップが Cisco Prime Infrastructure からすでにエクスポートされていることを前提としています。詳細については、*Cisco Prime Infrastructure 3.10 ユーザーガイド* [英語] の「Export Maps Archive」のトピックを参照してください。

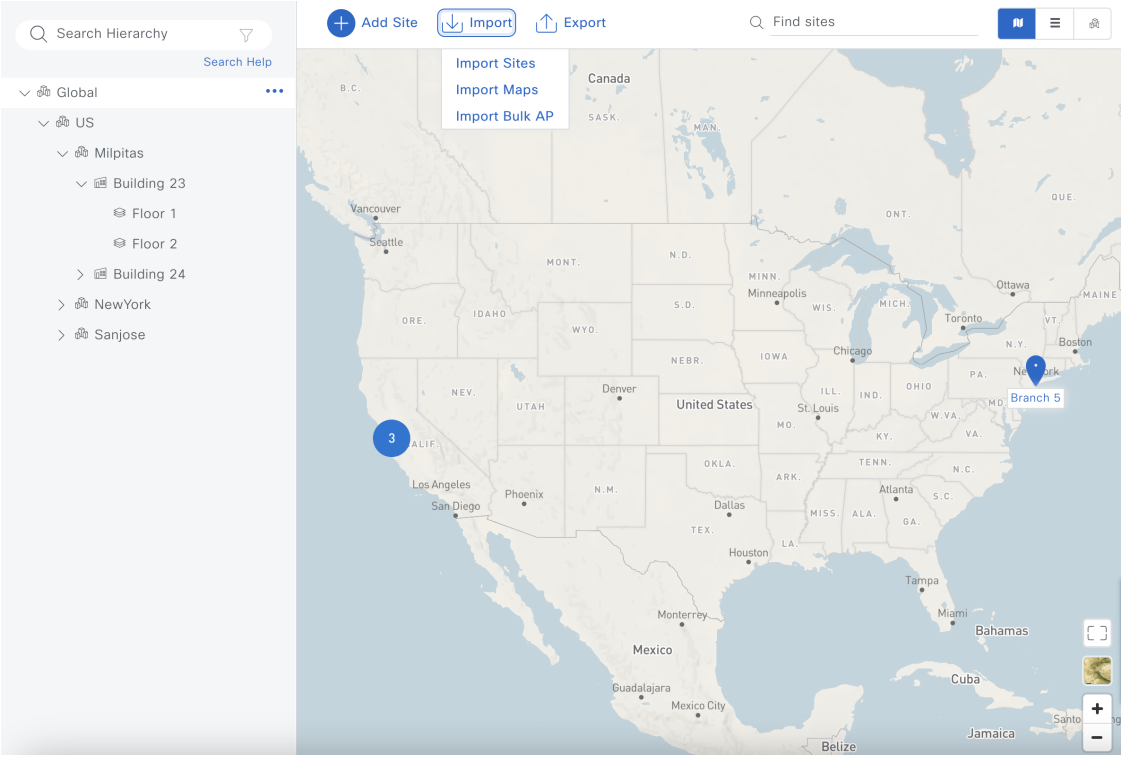
手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側の階層ペインで [Global] を選択します。

Cisco Prime Infrastructure マップは、[Global] レベルでインポートできます。

ステップ 3 **[Import]** > **[Import Maps]**の順にクリックします。



ステップ 4 [Import Maps] ダイアログボックスで、次のいずれかの方法を使用してマップをインポートします。

- [Choose a file] をクリックして、アップロードするマップファイルを選択します。
- マップファイルを [Import Maps] アップロード領域にドラッグアンドドロップします。

ステップ 5 [Import] をクリックします。

Cisco DNA Center から Ekahau プロジェクトファイルとしてマップをエクスポート

Ekahau を使用して計画済み AP を作成して配置するには、まず Cisco DNA Center でサイトを作成し、そのサイトを Ekahau プロジェクトとしてエクスポートします。次に、計画済み AP を Ekahau で作成し、その AP を Ekahau プロジェクトとして保存します。最後に、Ekahau プロジェクトを Cisco DNA Center に再度インポートします。

（注） Ekahau プロジェクトファイルは、ネストされていないサイトレベルでのみエクスポートできます。つまり、選択したサイト内にビルディングがあるサイトは 1 つだけです。

次の手順では、このプロセスについて説明します。

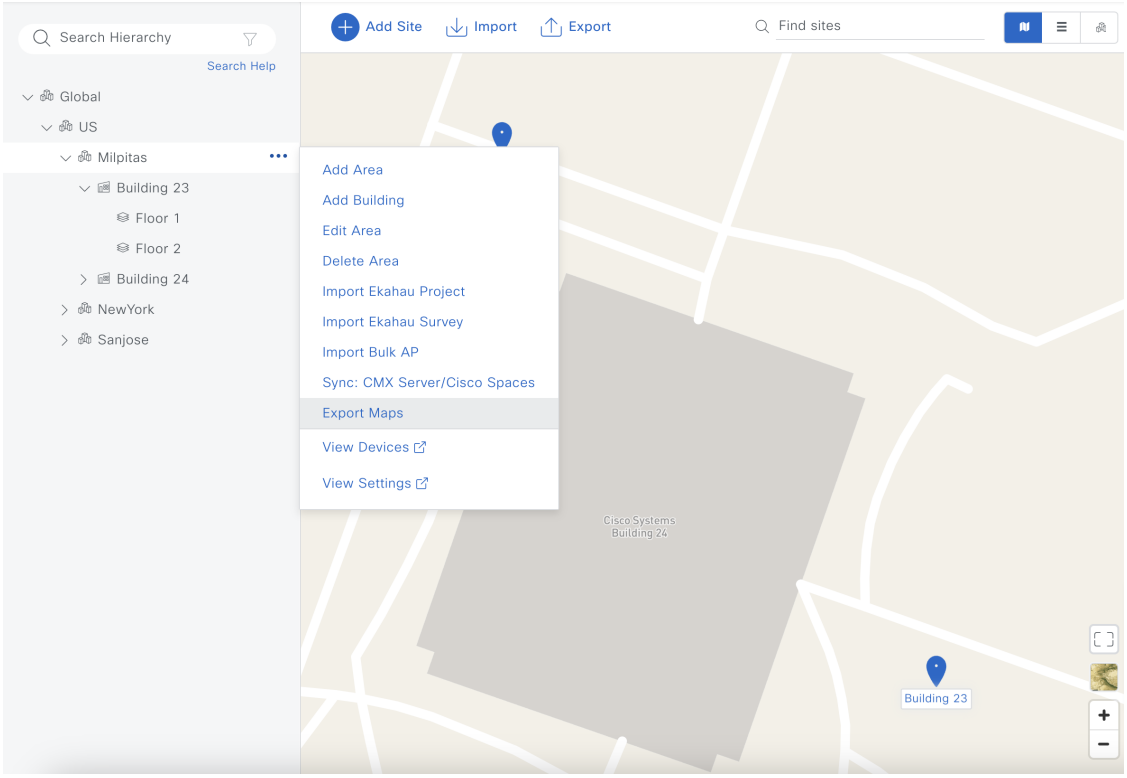
手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

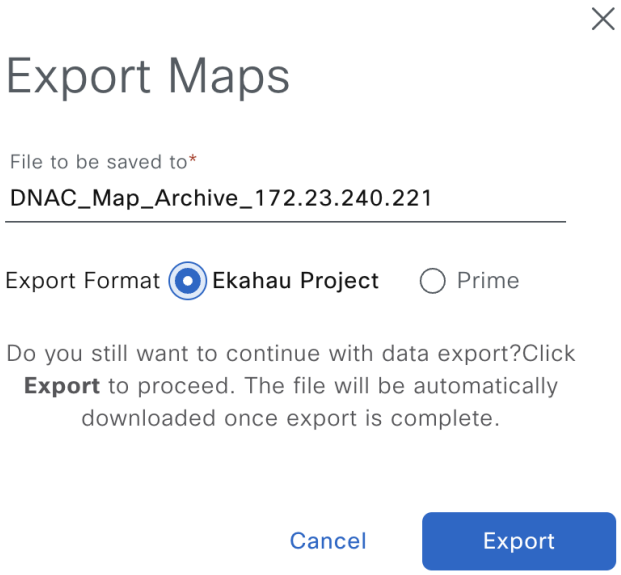
ステップ 2 左側の階層ペインで、マップに適したサイトを選択します。

この導入ガイドでは、**Milpitas** を選択します。

ステップ 3 省略記号アイコン（ ••• ）にカーソルを合わせ、[Export Maps] を選択します。



ステップ 4 [Export Maps] ダイアログボックスで、希望するファイル名を入力し、[Ekahau Project] オプションボタンをクリックします。



ステップ 5 [Export] をクリックします。

Ekahau からのマップのインポート

始める前に

Ekahau からインポートされたマップは、Ekahau プロジェクトファイル形式です。マップがエクスポートされたのと同じサイトレベルからマップがインポートされていることを確認します。たとえば、マップが **Milpitas** サイトからエクスポートされた場合は、**Milpitas** からマップをインポートする必要があります。

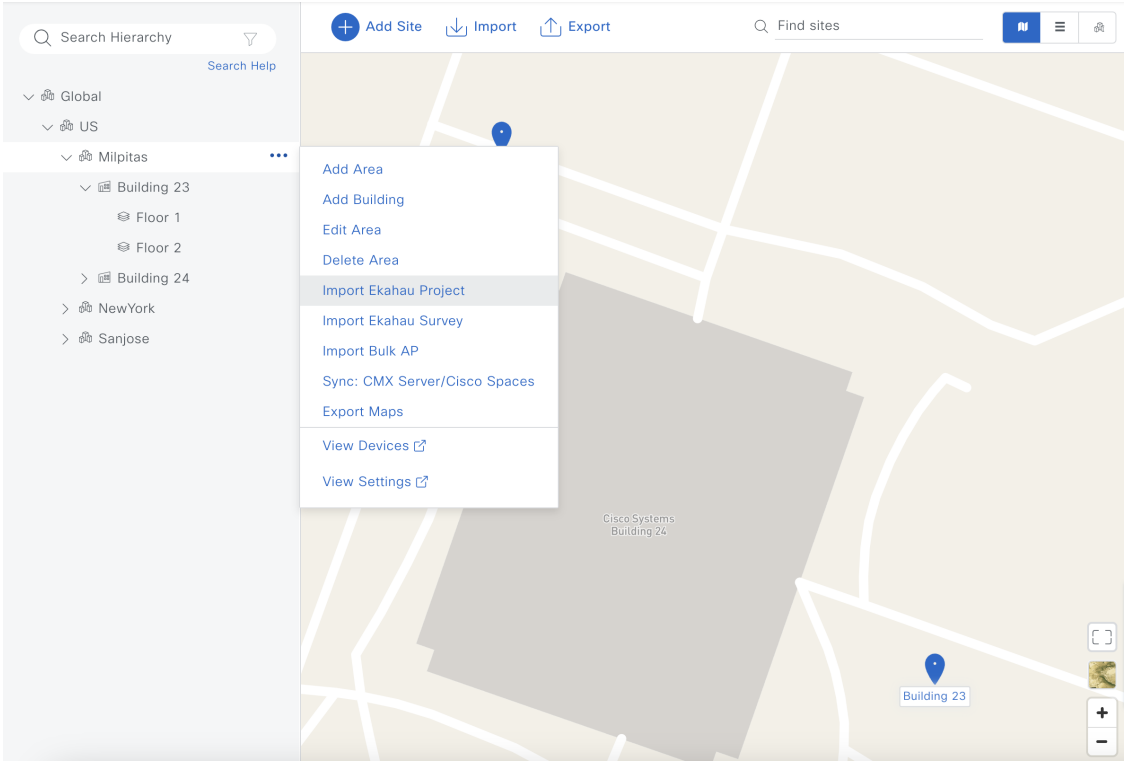
手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側の階層ペインで、マップに適したサイトを選択します。

この導入ガイドでは、[Milpitas] を選択します。

ステップ 3 省略記号アイコン（ ••• ）にカーソルを合わせ、[Import Ekahau Project] を選択します。



ステップ 4 [Import Ekahau Project] ダイアログボックスで、次のいずれかの方法を使用してマップをインポートします。

- [Choose a file] をクリックして、アップロードするプロジェクトファイルを選択します。
- マップファイルを [Import Ekahau Project] アップロード領域にドラッグアンドドロップします。

ステップ 5 [Import] をクリックします。

ネットワーク運用向けのネットワークサービスの設定

ここでは、Cisco DNA Center のサイト階層に合わせて AAA、DHCP、DNS、NTP、SNMP、および syslog サービスを設定する方法について説明します。サイト階層全体で、各サービスで同じサーバーが使用される場合は、サービスをグローバルに設定できます。サイト階層の継承プロパティを使用すると、すべてのサイトでグローバル設定を使用できます。個々のサイトの違いは、サイト単位で適用できます。このガイドでは、グローバルに作成されたネットワークサービスを示します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

ステップ 2 左側の階層ペインで [Global] を選択します。

ステップ 3 [+ Add Servers] をクリックします。

ステップ 4 [Add Servers] ダイアログボックスで、[AAA] チェックボックスと [NTP] チェックボックスをオンにします。

このガイドでは、[Image Distribution] または [Stealthwatch Flow Destination] を展開する必要がないため、[Image Distribution] チェックボックスや [Stealthwatch Flow Destination] チェックボックスはオンにしないでください。

ステップ 5 [OK] をクリックします。

AAA サーバーと NTP サーバーが [Network] ウィンドウに表示されるようになりました。

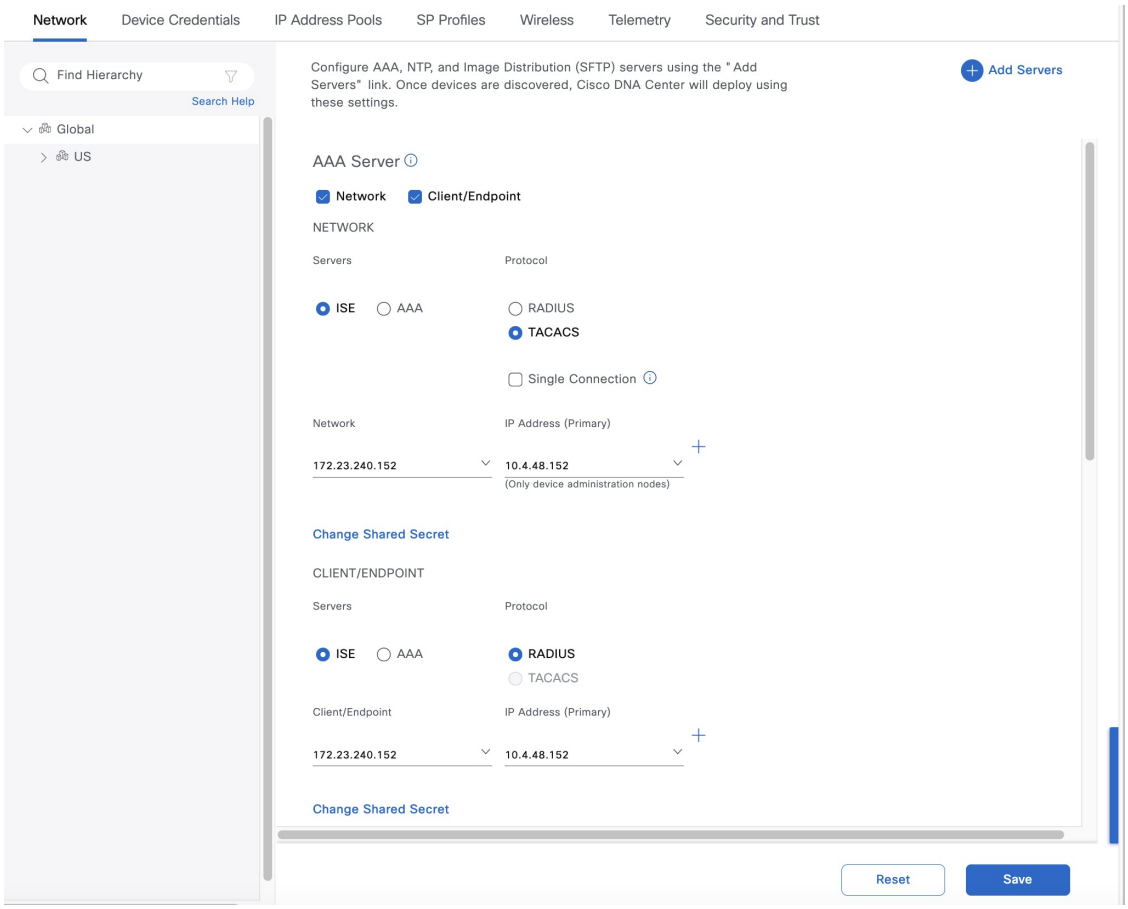
ステップ 6 [AAA Server] の関連フィールドを設定します。

この設計および導入ガイドでは、ネットワークデバイスとワイヤレスクライアントの両方について、Cisco ISE を AAA サーバー（RADIUS プロトコルを使用）として使用します。このガイドでは、[AAA Server] 用に次のフィールドが設定されています。

表 *5 : AAA* サーバー設定

フィールド	値
ネットワーク（Network）	オン
[Client/Endpoint]	オン
[Network] > [Servers]	ISE
[Network] > [Protocol]	TACACS
[Network] > [Network]	172.23.240.152
[Network] > [IP Address (Primary)]	10.4.48.152
[Network] > [Shared Secret]	—
[Client/Endpoint] > [Servers]	ISE
[Client/Endpoint] > [Protocol]	RADIUS
[Client/Endpoint] > [Network]	172.23.240.152
[Client/Endpoint] > [IP Address (Primary)]	10.4.48.152
[Client/Endpoint] > [Shared Secret]	—

図 *4 : Cisco DNA Center* の *AAA* サーバーの設定



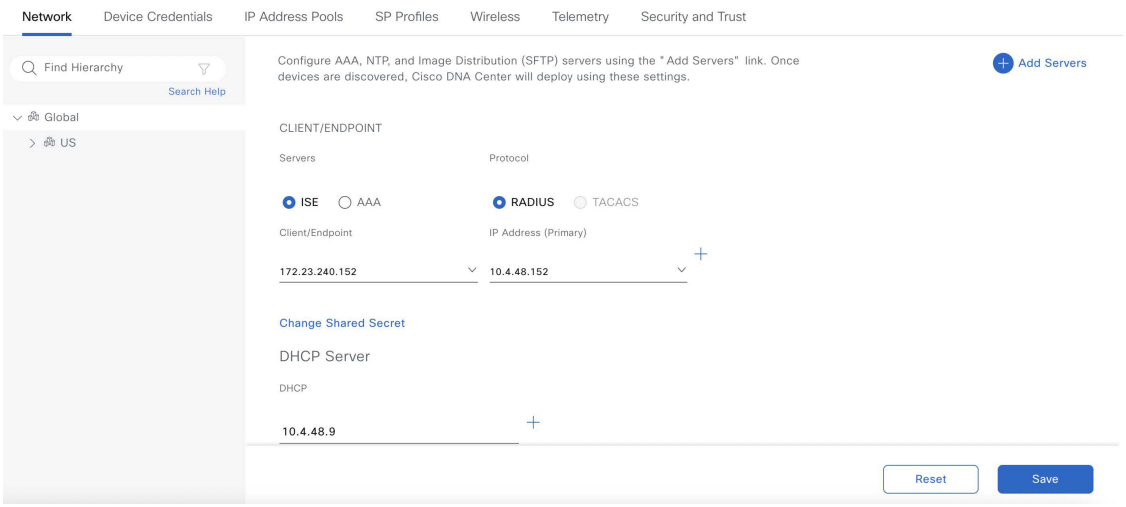
ステップ 7 [DHCP Server] の関連フィールドを設定します。

この設計および導入ガイドでは、ネットワークの DNS サーバーと DHCP サーバーの両方として機能する単一の Microsoft Active Directory（AD）サーバーを使用します。このガイドでは、次のフィールドが [DHCP Server] 用に設定されています。

表 *6 : DHCP* サーバ設定

フィールド	値
DHCP	10.4.48.9

図 *5 : Cisco DNA Center* の *DHCP* サーバーの設定



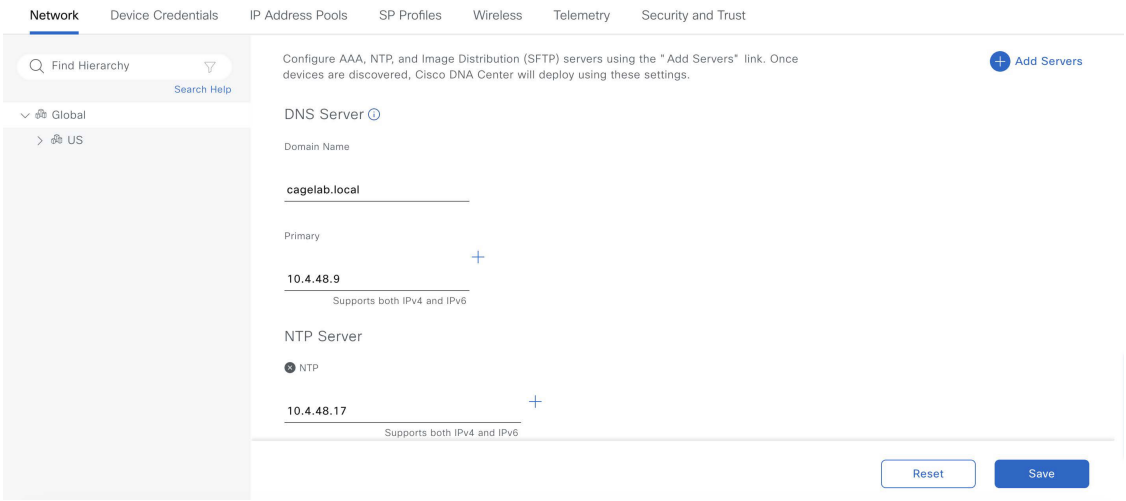
ステップ 8 [DNS Server] の関連フィールドを設定します。

この設計および導入ガイドではラボネットワークを使用するため、[DNS Server] の設定では単一の DNS ドメインのみ使用されています。このガイドでは、[DNS Server] 用に次のフィールドが設定されています。

表 *7 : DNS* サーバ コンフィギュレーション

フィールド	値
ドメイン名	cagelab.local
プライマリ	10.4.48.9

図 *6 : Cisco DNA Center* の *DNS* サーバーの設定



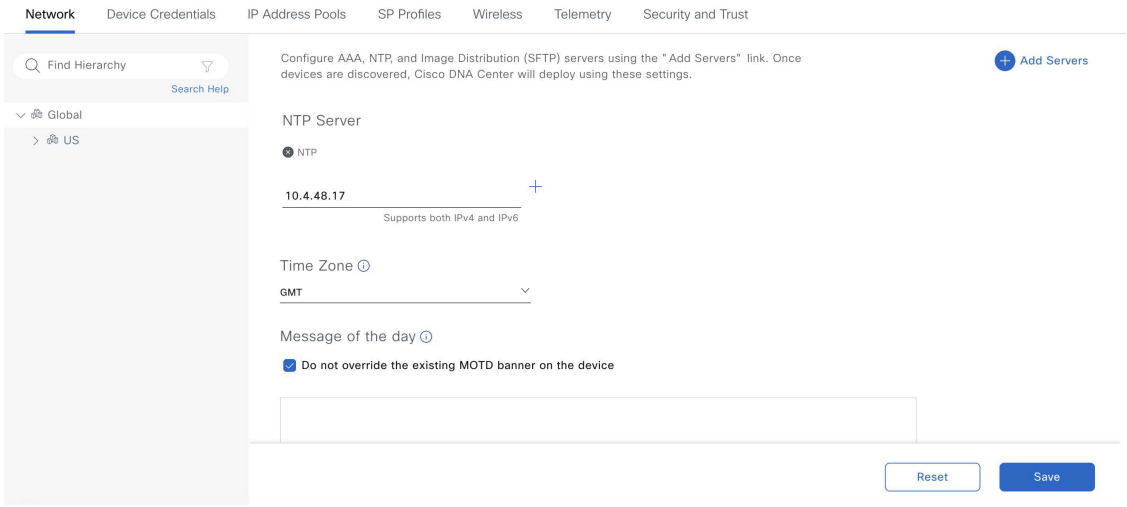
ステップ 9 [NTP Server] の関連フィールドを設定します。

実稼働ネットワークでは、復元力と精度を得るために複数の NTP サーバーを追加できます。ネットワーク内の時刻同期は、ロギング機能や、SSH などのセキュアな接続に不可欠です。この設計および導入ガイドではラボネットワークを使用するため、[NTP Server] の設定では単一の NTP サーバーのみ使用されています。このガイドでは、[NTP Server] 用に次のフィールドが設定されています。

表 *8 : NTP* サーバーの設定

フィールド	値
IPアドレス	10.4.48.17
タイム ゾーン	GMT

図 *7 : Cisco DNA Center* の *NTP* サーバーの設定



ステップ 10 [Time Zone] ドロップダウンリストから必要なタイムゾーンを選択します。

この設計および導入ガイドではラボネットワークを使用するため、サイト階層には単一のタイムゾーンが使用されています。実稼働ネットワークでは、サイト階層内の各サイトにその場所のタイムゾーンが反映されます。

ステップ 11 [Message of the day] で、[Do not overwrite the existing MOTD banner on the device] チェックボックスをオンにするか、テキストボックスに目的のメッセージを入力します。

[Message of the day] フィールドでは、ネットワークデバイスへのログイン時に表示されるメッセージを制御します。この設定は、この設計および導入ガイドには適用されないため、このガイドでは、[Do not overwrite the existing MOTD banner on the device] チェックボックスがオンになっています。

ステップ 12 [Save] をクリックします。

ステップ 13 ウィンドウの上部にある [Telemetry] をクリックします。

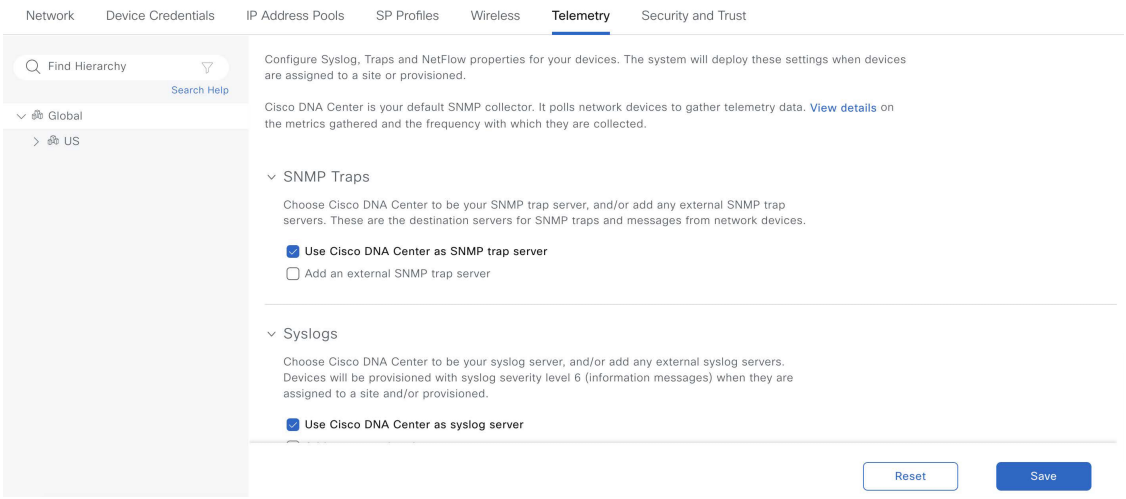
ステップ 14 [SNMP Traps] で、SNMP トラップサーバーを設定します。

この設計および導入ガイドでは、Cisco DNA Center を SNMP サーバーとして使用します。[Use Cisco DNA Center as SNMP server] チェックボックスをオンにすると、SNMP トラップ情報が Cisco AI Network Analytics のために Cisco DNA Center に送信されます。このガイドでは、SNMP サーバー用に次のフィールドが 設定されています。

表 *9 : SNMP* サーバーの設定

フィールド	値
[Use Cisco DNA Center as SNMP server]	オン
[SNMP] > [IP Address]	—

図 *8 : Cisco DNA Center* の *SNMP* サーバーの設定



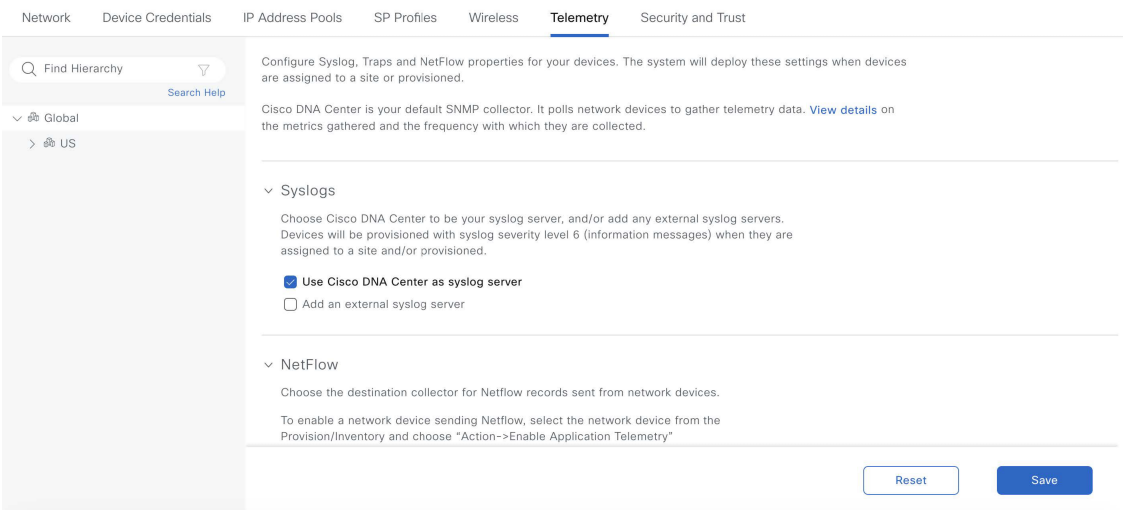
ステップ 15 [Syslogs] から Syslog サーバーを設定します。

この設計および導入ガイドでは、Cisco DNA Center を Syslog サーバーとして使用します。[Use Cisco DNA Center as syslog server] チェックボックスをオンにすると、syslog 情報が Cisco AI Network Analytics のために Cisco DNA Center に送信されます。このガイドでは、Syslog サーバー用に次のフィールドが設定されています。

表 *10 : Syslog* サーバーの設定

フィールド	値
[Use Cisco DNA Center as syslog server]	オン
[Syslog] > [IP Address]	—

図 *9 : Cisco DNA Center* の *Syslog* サーバーの設定



ステップ 16　[Save] をクリックします。

キャンパスのワイヤレス展開の設定

キャンパスのワイヤレス展開設定を設定するには、Cisco DNA Center で以下を作成する必要があります。

- ワイヤレスインターフェイス：ワイヤレストラフィックの終端に使用されるイーサネット インターフェイス（VLAN）。
- エンタープライズ ワイヤレス ネットワーク：展開用の非ゲスト WLAN/SSID で構成されます。
- ゲスト ワイヤレス ネットワーク：展開用のゲスト WLAN/SSID で構成されます。
- ワイヤレス無線周波数（RF）プロファイル：展開用の無線周波数プロファイルが含まれます。
- ワイヤレスセンサーの設定：ワイヤレスセンサーには、WLAN で診断テストを実行し、パケットキャプチャを実行する機能があります。ワイヤレスセンサーの詳細については、ワイヤレスネットワークの監視および操作（205 ページ）を参照してください。
- CMX サーバー：CMX サーバーと統合することで、ワイヤレスクライアントの場所をフロアマップに表示できます。CMX サーバーとの統合の詳細については、ワイヤレスネットワークの監視および操作（205 ページ）を参照してください。
- ネイティブ VLAN：ネイティブ VLAN の設定は、FlexConnect アクセスポイント（AP）展開に固有です。

（注）　この導入ガイドでは、集中型（ローカル）モードで動作する AP を使用したワイヤレスネットワークについて説明します。

推奨事項

キャンパスのワイヤレス展開設定を設定する場合は、次の推奨事項を考慮してください。

- 実稼働展開と同様、ワイヤレス管理インターフェイス（WMI）とは異なる VLAN に AP を配置する必要があります。ステージングやテスト目的の WMI と同じ VLAN に AP を設定する必要がある場合は、AP の数を 100 未満に制限することを推奨します。
- ローカルモードの AP については、アクセスポイントとコントローラ間のラウンドトリップ遅延が 20 ミリ秒を超えないようにします。
- ローカルモードの AP の AP スイッチポートで PortFast を使用し、中央でスイッチされる WLAN のみをサポートします。PortFast のスイッチポートを設定するには、switch port host コマンドまたは PortFast コマンドを使用して、ポートをホストポートとして接続するように設定します。この設定により、APの参加プロセスが高速になります。ローカルモードのAPではVLAN間でトラフィックが直接ブリッジされないため、ループが発生するリスクはありません。ポートはアクセスモードで直接設定できます。
- Flex モードおよびローカルスイッチングの AP の場合、ほとんどのシナリオでスイッチポートをトランクモードにする必要があります。そのような場合は、スイッチポートでスパニングツリー PortFast トランクを使用します。
- CAPWAP でのTCPクライアントトラフィックのカプセル化を最適化するには、TCP最大セグメントサイズ（MSS）機能を常に有効にすることを推奨します。有効にすることで、CAPWAP フラグメンテーションの全体的な量を減らし、ワイヤレスネットワーク全体のパフォーマンスを向上できます。MSS 値は、シスコ ワイヤレス コントローラから AP へのパスのトラフィックタイプと最大伝送ユニット（MTU）に応じて調整する必要があります。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、TCP MSS 調整がデフォルトで有効になっており、値は1,250バイトで、ほとんどの展開で許容可能な値と見なされます。設定に応じて、値をさらに最適化できます。ワイヤレスコントローラで直接設定するか、テンプレートハブを介して設定する必要があります。

ワイヤレスインターフェイスの設定

Cisco DNA Center では、エンタープライズ WLAN とゲスト WLAN がイーサネット VLAN インターフェイスで終端しています。この設計および導入ガイドで使用するエンタープライズWLANおよびゲストWLAN用に作成されたワイヤレスインターフェイスを次の表に示します。

表 *11* : ワイヤレスインターフェイス

名前	VLAN	使用方法
employee	160	従業員の音声およびデータ VLAN
guest-dmz	125	ゲストデータ VLAN
flex	180	Flex クライアント VLAN

手順

ステップ 1 インスタンスの IP アドレスまたは完全修飾ドメイン名を使用して、Cisco DNA Center にログインします。

例：https://<Cisco_DNA_Center_IPaddr_or_FQDN>。入力するログイン情報（ユーザー ID とパスワード）には、SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE 権限が必要です。

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

[Wireless Network Settings] ダッシュボードが表示されます。

図 *10 : [Wireless Network Settings]* ダッシュボード

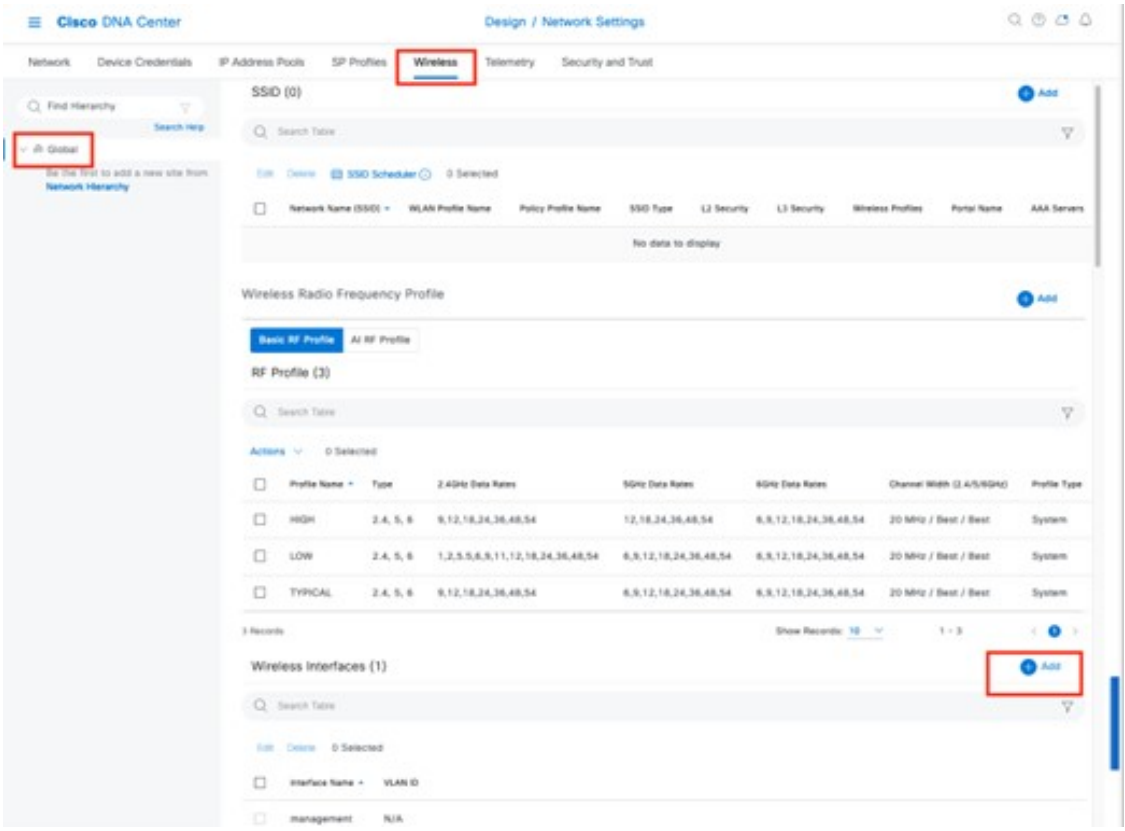
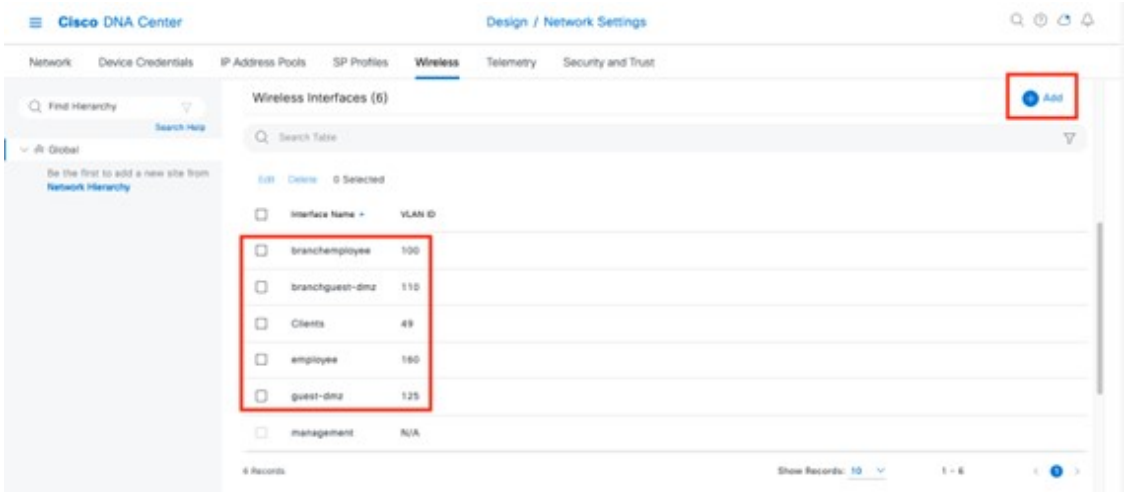


図 *11 : [Wireless Interfaces]* ウィンドウ

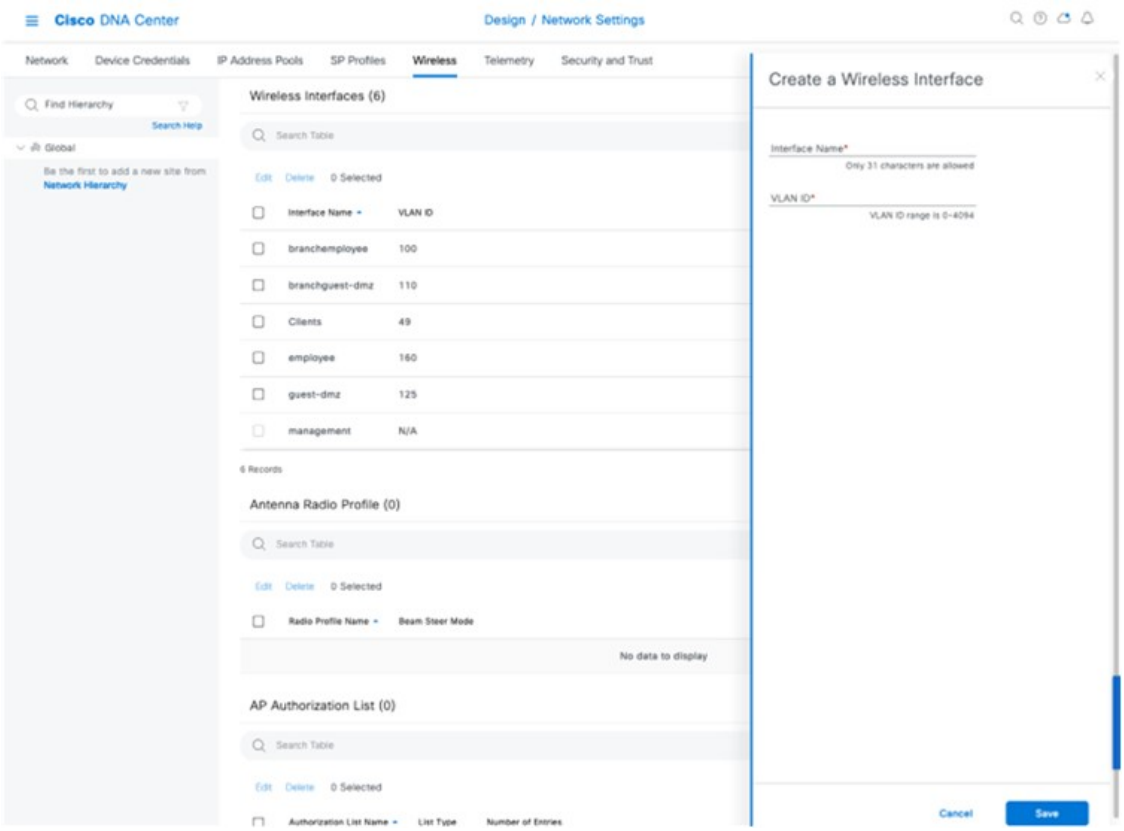


（注） ワイヤレス設定は階層型です。サイト階層の下位レベルで定義された設定で、上位レベルで定義された設定がオーバーライドされます。デフォルトでは、サイト階層の最上位レベルであるグローバルレベルに移動します。サイト階層のグローバルレベルでワイヤレスインターフェイスを定義する必要があります。

ステップ 3 [Wireless Interfaces] の横にある [Add] をクリックします。

[New Wireless Interface] スライドインペインが表示されます。

図 *12 : [New Wireless Interface]* スライドインペイン



ステップ 4 エンタープライズ VLAN（従業員）に対応するワイヤレスインターフェイスの [Interface Name] と [VLAN ID] を入力し、[Add] をクリックします。

この手順を繰り返して、ゲスト VLAN（guest-dmz）のワイヤレスインターフェイスを追加します。2 つの新しいワイヤレスインターフェイスが [Wireless Network Settings] ダッシュボードに表示されます。

エンタープライズワイヤレス SSID の設定

エンタープライズ ワイヤレス ネットワークは、展開全体でブロードキャストに使用できる非ゲスト WLAN/SSID なので、サイト階層のグローバルレベルで定義する必要があります。定義すると、エンタープライズワイヤレス ネットワークをワイヤレスプロファイルに適用し、ワイヤレスプロファイルを階層内の 1 つ以上のサイトに割り当てられます。

（注） コントローラに設定するサービスセット識別子（SSID）の数を制限することを推奨します。（各APの無線ごとに）16 の WLAN/SSID を同時に設定できます。各 WLAN/SSID には、最低の必須レートで送信される個別のプローブ応答とビーコンが必要であり、SSID が追加されると RF 汚染が増加します。

PDA、Wi-Fi 電話機、バーコードスキャナなどの小型ワイヤレスステーションの一部では、多数の基本 SSID（BSSID）を無線で処理できないため、ロックアップ、リロード、または関連付けの失敗が発生します。企業の場合は 1 ～ 3 の SSID を設定し、高密度設計の場合は 1 つの SSID を設定することを推奨します。AAA オーバーライド機能を使用すると、単一の SSID シナリオでユーザーごとに個別の VLAN/設定を割り当てながら、WLAN/SSID の数を減らすことができます。

この導入ガイドでは、**lab3employee** という名前の単一のエンタープライズ WLAN/SSID がプロビジョニングされます。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 [SSIDs] をクリックします。

ステップ 3 [+ Add] にカーソルを合わせて、[Enterprise] を選択します。

[Basic Settings] ウィンドウが表示されます。

図 *13*：エンタープライズワイヤレス *SSID* を作成するための *[Basic Settings]* ウィンドウ

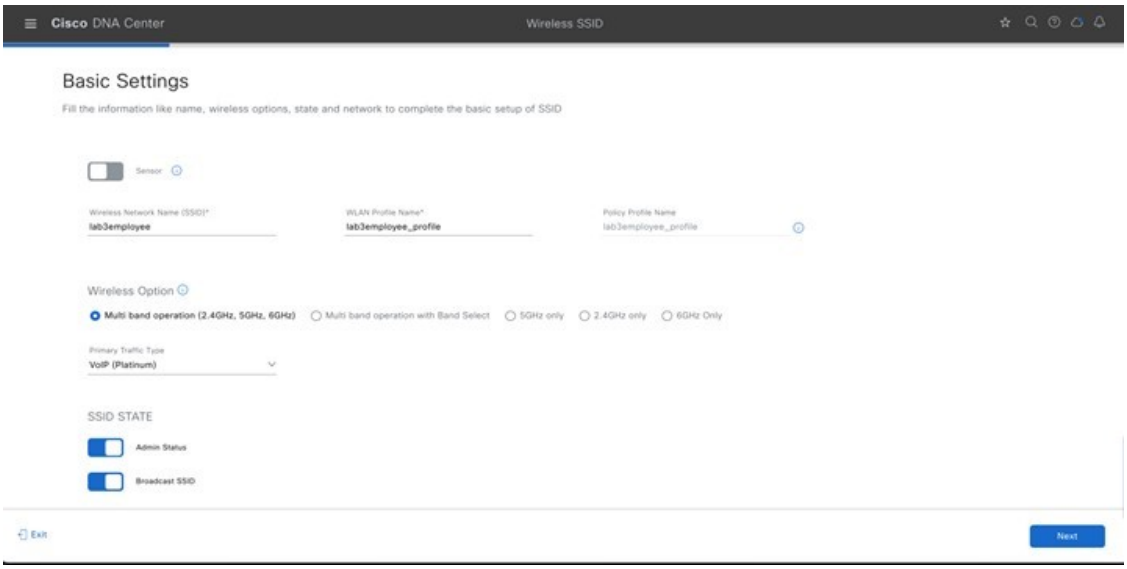


図 *14* : エンタープライズ *SSID* のセキュリティ設定

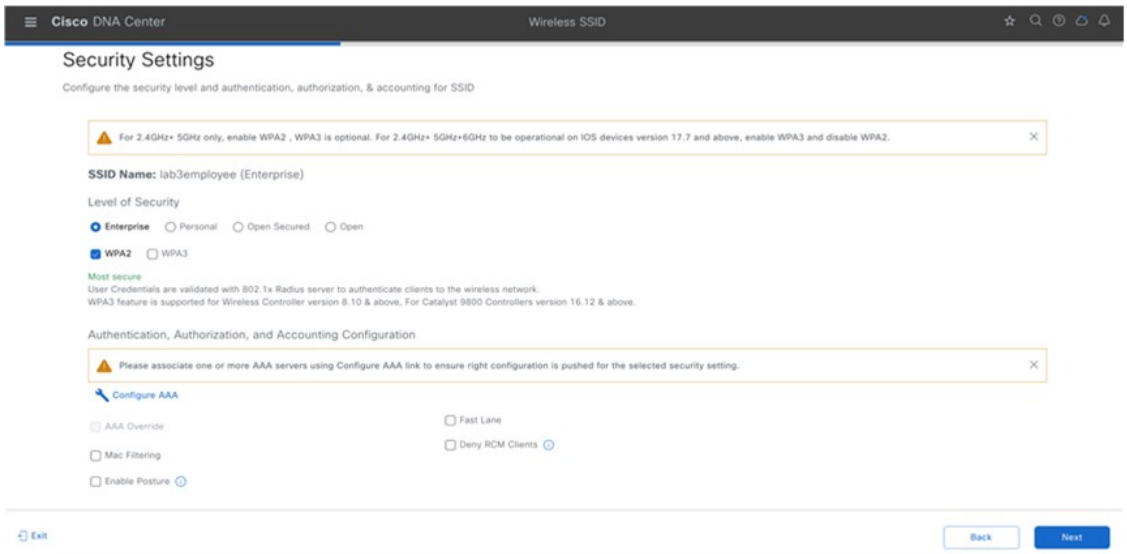


図 *15* : エンタープライズ *SSID* の *AAA* サーバー

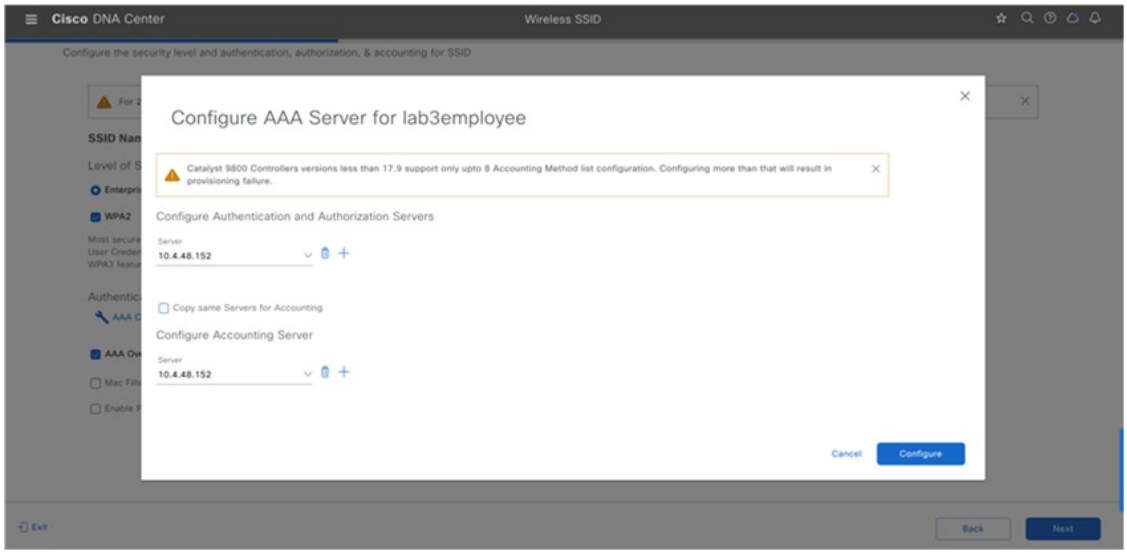


図 *16* : エンタープライズ *SSID* の詳細設定

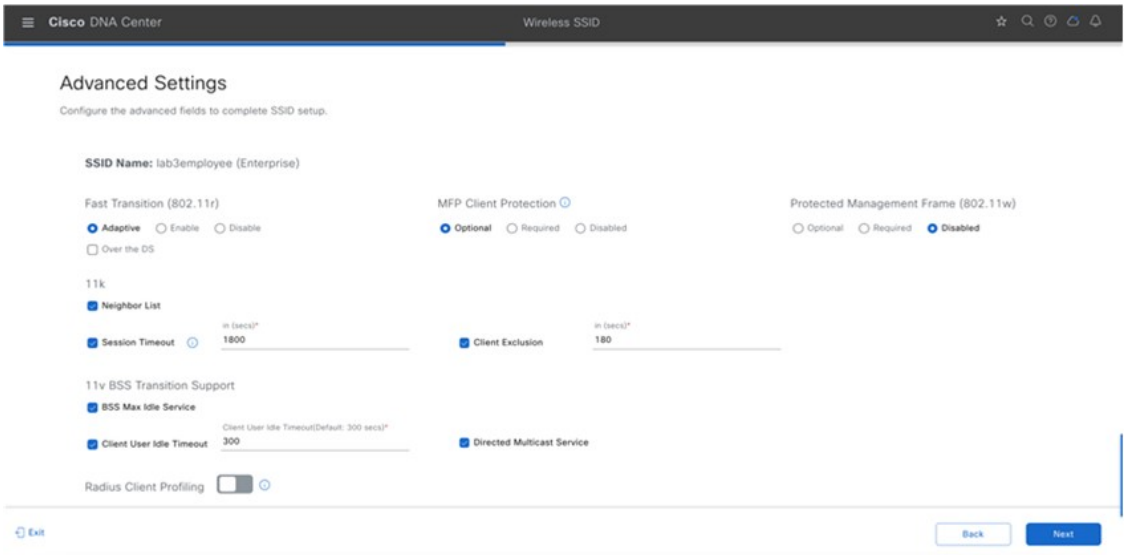
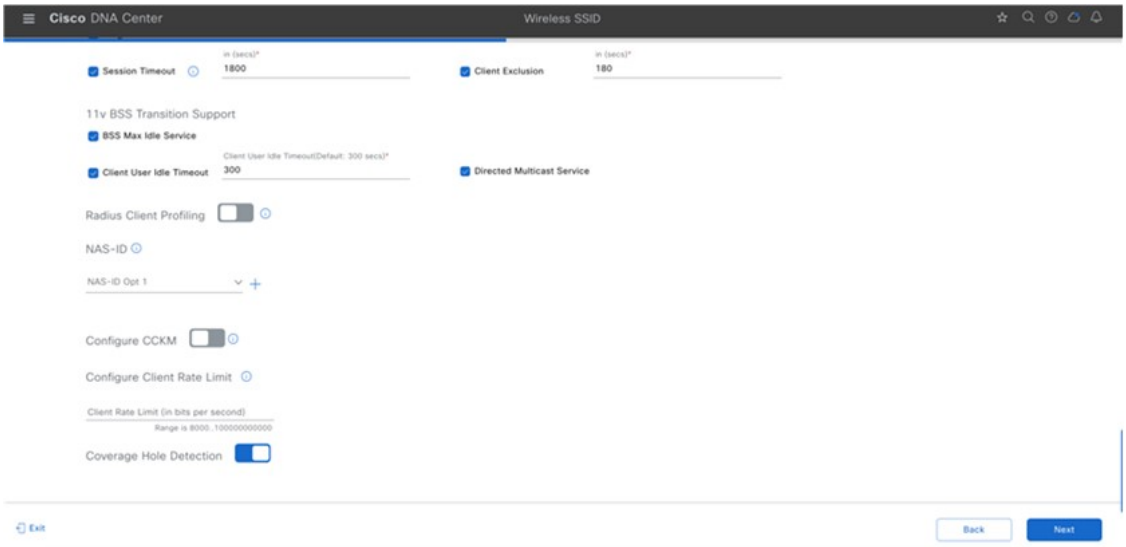


図 *17* : エンタープライズ *SSID* の追加の詳細設定



（注） ネイバーリスト（802.11k）を有効にすると、一部のレガシーデバイスが不明な情報に誤って反応する可能性があります。ほとんどのデバイスでは802.11k情報は（サポートしていない場合でも）無視されますが、一部のデバイスでは切断または関連付けの失敗が発生する可能性があるため、このオプションを有効にする前にテストすることを推奨します。

クライアントがカバレッジエリアに出入りするシナリオや、クライアントがバッテリ駆動で頻繁にスリープ状態になるシナリオでは、クライアントが削除される可能性を減らすために、アイドルタイムアウトを 3,600 秒（60 分）に増やすことを検討してください。

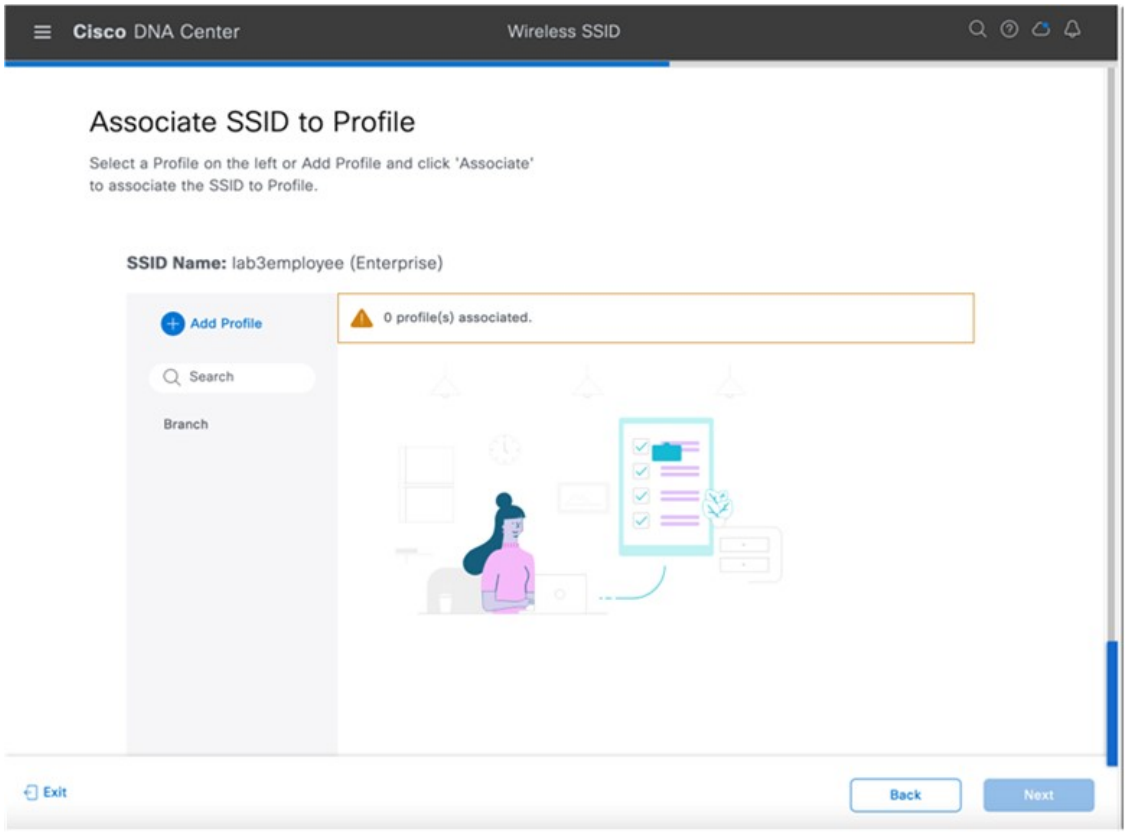
Cisco DNA Center を使用してエンタープライズ ワイヤレス ネットワーク用に設定できる機能については、Cisco DNA Center で設定可能なエンタープライズ ワイヤレス ネットワーク機能 （43 ページ）を参照してください。

ステップ 4 [Basic Settings] の情報を入力し、[Next] をクリックします。

ワークフローの次の画面が表示されます。エンタープライズ ワイヤレス ネットワークを既存のワイヤレスプロファイルに接続したり、新しいワイヤレスプロファイルを作成してエンタープライズ ワイヤレス ネットワークを接続したりできます。

（注） この導入ガイド用に設定されたエンタープライズ ワイヤレス ネットワークの設定については、導入ガイドで設定されているエンタープライズ ワイヤレス ネットワーク設定 （56 ページ）を参照してください。

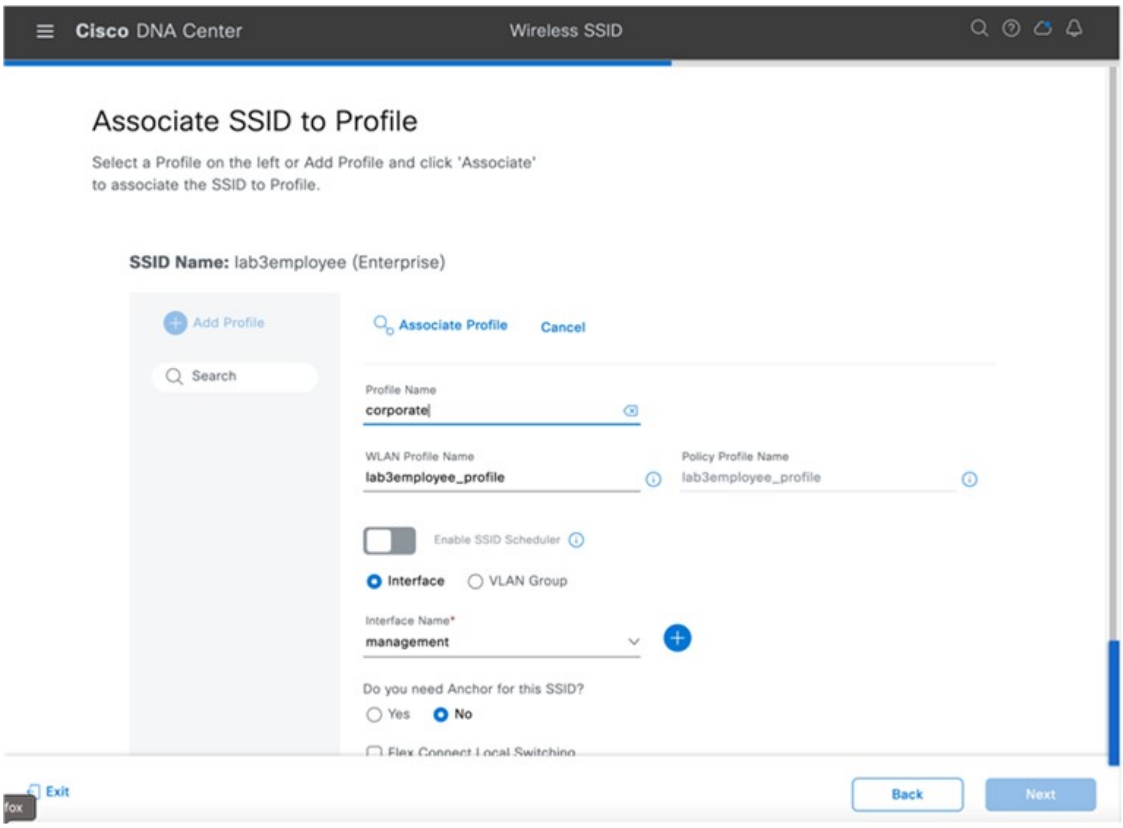
図 *18 :* プロファイルへの *SSID* の関連付け



ステップ 5 [+ Add Profile] をクリックして、新しいワイヤレスプロファイルを作成して追加します。

[Create a Wireless Profile] サイドパネルが表示されます。

図 *19* : 新しいワイヤレスプロファイルの作成



ステップ 6 [Profile Name] に新しいワイヤレスプロファイルの名前を入力し、[Associate Profile] をクリックします。

この導入ガイドでは、**Corporate** という名前のワイヤレスプロファイルを作成します。

ステップ 7 新たに作成したプロファイルをクリックし、そのプロファイルに関連付けるインターフェイスを選択します。

ステップ 8 [Save] をクリックしてから [Next] をクリックします。

ステップ 9 （SD-Access アプリケーションが展開されていない場合は、このステップをスキップします）。[Fabric] で [No] を選択します。

[Select Interface] フィールドが表示されます。この導入ガイドでは、Cisco DNA Center を使用した非 SDA ワイヤレス展開についてのみ説明します。

ステップ 10 [Select Interface] ドロップダウンメニューから従業員を選択し、lab3Employee SSID を前の手順で作成した従業員 VLAN（VLAN 160）で終端します。

ステップ 11 [Guest Anchor] オプションで、[No] を選択します。

ステップ 12 [Flex Connect Local Switching] チェックボックスをオフにし、[Save] をクリックして既存のプロファイルを保存します。

プロファイルが存在しない場合は、新しいプロファイルを作成し、[Save] をクリックします。

ステップ 13 [Next] をクリックします。

ステップ 14 [Network Profile] の概要を確認し、[Save] をクリックします。

ステップ 15 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

ステップ 16 [Wireless Profiles] テーブルの [Sites] 列で、目的のプロファイルの [Assign Site] をクリックします。

この導入ガイドでは、新たに作成したワイヤレスプロファイルである **Corporate** の [Assign Site] をクリックします。

ステップ 17 [Global] セクションで [>] をクリックして、[Milpitas] エリアを表示します。

ステップ 18 [Milpitas] エリアを選択します。

すべての子サイトの場所（**Building 23** の **Floor 1**、**Floor 2**、および **Floor 3**、**Building 24** の **Floor 1**、**Floor 2**、および **Floor 3**）が自動的に選択されます。

ステップ 19 [OK] をクリックして、サイト階層のサイドパネルを閉じます。

ステップ 20 [Network Profiles Attach Template(s)] の 概要の下にある [Edit] をクリックして、エンタープライズ ワイヤレス ネットワーク設定に CLI ベースのテンプレートを追加します。

（注） Cisco DNA Center の [Template Editor] ダッシュボード内ですべてのテンプレートを定義する必要があります。この設計および導入ガイドでは、特定の シスコ ワイヤレス コントローラ プラットフォームに関する CLI 構文の知識が必要なため、テンプレートの追加については取り上げていません。Cisco DNA Center CLI テンプレートは、インテントベースのプロファイルやモデル設定を使用して設定できない内容を設定するために使用できます。

ステップ 21 [Save] をクリックします。

Corporate という名前のワイヤレスプロファイルが Milpitas エリアに割り当てられます。ワイヤレスプロファイルには **lab3employee** SSID が含まれているため、ワイヤレスコントローラと AP が Milpitas エリアに割り当てられると、AP は lab3employee SSID をブロードキャストします。

ステップ 22 [Finish] をクリックして、**lab3employee** エンタープライズ ワイヤレス ネットワークを追加します。

新しいエンタープライズ ワイヤレス ネットワークが [Wireless Network Settings] ダッシュボードに表示されます。

オーバーライドの設定方法の詳細については、サイトのオーバーライドサポートの定義（57 ページ）を参照してください。

Cisco DNA Center で設定可能なエンタープライズ ワイヤレス ネットワーク機能

表 *12 : Cisco DNA Center* で設定可能なエンタープライズ ワイヤレス ネットワーク機能

機能	タイプ	説明
ワイヤレス ネットワーク名（SSID）	テキストフィールド	WLAN の SSID。

機能	タイプ	説明
WLAN Profile Name	テキストフィールド	Cisco DNA Center では、SSID 名に基づいた SSID_Profile がデフォルトと見なされます。WLAN プロファイル名は要件に応じて変更できます。
[Policy Profile Name]	編集不可	[Policy Profile Name] は [WLAN Profile Name] と同じであり、編集できません。 Cisco DNA Center では WLAN プロファイル名に基づいて、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのポリシープロファイル名が自動的に生成されます。
[Broadcast SSID]	[On/Off] トグルボタン	SSID をワイヤレスビーコンおよびプローブ応答でブロードキャストするかどうかを決定します。
[SSID STATE]	[On/Off] トグルボタン	このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP はワイヤレスコントローラに関連付けられたままでアクセス可能ですが、AP には引き続きライセンスが必要です。
センサー	[On/Off] トグルボタン	センサーが無効になっていることを確認します。
[Wireless Option]	オプション ボタン（Radio Button）	SSID がブロードキャストされる RF 帯域を決定します。次のワイヤレスオプションを使用できます。 • マルチバンド動作（2.4 GHz、5 GHz、および 6 GHz）。 • バンドセレクトによるマルチバンド動作。バンドセレクト機能を使用し、2.4 GHz チャネルでのプローブ応答を遅延させることで、2.4 GHz と 5 GHz の両方の帯域で動作可能なクライアント無線を、通常は輻輳の少ない 5 GHz 帯域に移動できます。 • 5 GHz のみ。 • 2.4 GHz のみ。 • 6 GHz のみ。

機能	タイプ	説明
[Level of Security]	オプション ボタン（Radio Button）	

機能	タイプ	説明
		WLANのレイヤ2（L2）セキュリティ設定を決定します。ネットワークの暗号化および認証タイプを選択します。サイト、ビルディング、およびフロアは、グローバル階層から設定を継承します。サイト、ビルディング、またはフロアレベルでセキュリティレベルをオーバーライドできます。次のオプションを利用できます。 • [Enterprise]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。 （注） Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。 WPA3は、WPAの最新バージョンです。これは、Wi-Fiネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。 2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド動作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS リリース 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作可能にするには、WPA3 を有効にし WPA2 を無効にする必要があります。 • [Personal]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。デフォルトでは、[WPA2] チェックボックスが有効になっています。[Personal] を選択した場合は、[Passphrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間でペアワイズマスターキー（PMK）として使用されます。 （注） WPA3 パーソナルは、パスワードベースの堅牢な認証を提供することによって、個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるよ

機能	タイプ	説明
		うになります。 WPA2パーソナルの場合は、サイト、ビルディング、またはフロアレベルで、事前共有キー（PSK）をオーバーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。詳細については、「事前共有キーのオーバーライド」を参照してください。 2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS リリース 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作可能にするには、WPA3 を有効にし WPA2 を無効にする必要があります。 （オプション）WPA2-Personal の場合、次の手順を実行してマルチ事前共有キー（MPSK）サポートを構成します。 **1.** [Configure MPSK] をクリックします。 **2.** [Configure MPSK] ダイアログボックスで、[Add to an MPSK] をクリックします。最大 5 つの MPSK を追加できます。 **3.** [Priority] ドロップダウンリストから優先順位を選択します。 （注） 優先順位 0 キーが中央 Web 認証（CWA）Flex モードで設定されていない場合、WLAN へのクライアント接続が失敗する可能性があります。 [Passphrase Type] ドロップダウンリストから、パスフレーズタイプを選択します。 **4.** [Passphrase] フィールドに、パスフレーズを入力します。 **5.** [Save] をクリックします。 MPSK は、WPA2-Personal のレイヤ 2 セキュリティの設定に適用されます。

機能	タイプ	説明
		• [Open Secured]：[Assign Open SSID] ドロップダウンリストから、クライアントをオープンでセキュアなSSIDにリダイレクトするためのオープン SSID を選択します。オープンでセキュアなポリシーは、セキュリティが最も低くなります。 （注） Fast Transition は、オープンでセキュアな SSID には適用できません。 • [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。
[Primary Traffic Type]	Drop Box	Catalyst 9800 シリーズ ワイヤレス コントローラの場合、この設定により、WLAN/SSID のアップストリームとダウンストリームの両方向に貴金属 QoS SSID ポリシーが適用されます。集中型（ローカルモード）設計では、トラフィックが AP と シスコ ワイヤレス コントローラの間でトンネリングされるため、貴金属ポリシーにより CAPWAP ヘッダー内の最大 DSCP マーキングが制御されます。 次のオプションを利用できます。 • [VoIP (Platinum)]：ワイヤレスネットワークの QoS は、ワイヤレス音声およびデータトラフィック用に最適化されています。 • [Video (Gold)]：ワイヤレスネットワークの QoS はビデオトラフィック用に最適化されています。 • [Best Effort (Silver)]：ワイヤレスネットワークの QoS は、ワイヤレス データ トラフィック用にのみ最適化されています。 • [Non-real Time (Bronze)]：ワイヤレスネットワークの QoS は、低帯域幅の使用に最適化されています。
[Fastlane]	チェックボックス	このチェックボックスは、[Type of Enterprise Network] が [Voice and Data] の場合にのみオンにできます。 Catalyst 9800 シリーズ ワイヤレス コントローラの場合、[Fastlane] チェックボックスをオンにすると、Fastlane モードで自動 QoS が有効になります。Fastlane モードの自動 QoS では、5 GHz 帯域と 2.4 GHz 帯域の両方に Fastlane EDCA プロファイルが設定されますが、[Fastlane] チェックボックスがオンになっている場合、貴金属 QoS SSID ポリシーは WLAN/SSID に適用されません。

機能	タイプ	説明
AAA の設定	リンク	

機能	タイプ	説明
		[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加して設定します。[Drop Box] から [Authentication, Authorization, and Accounting server] を選択します。 [+] をクリックしてサーバーを追加します。 （注） Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ のエンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。 アカウンティングに AAA サーバーを使用するには、[Copy Same Servers for Accounting] チェックボックスをオンにします。 SSID に別のアカウンティングサーバーを設定するには、次の手順を実行します。 **1.** [Configure Accounting Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、アカウンティングサーバーの IP アドレスを選択できます。 **2.** [+] をクリックしてサーバーを追加します。 （注） Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ のエンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つのアカウンティングサーバーを設定できます。 **3.** [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。 Cisco DNA Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Cisco DNA Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Cisco DNA Center によって作成されます。

機能	タイプ	説明
		サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。
RCM クライアントの拒否	チェックボックス	ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。
[Mac Filtering]	チェックボックス	これは、WLAN の MAC アドレスフィルタリングを適用する追加の L2 セキュリティ設定です。
AAA オーバーライド	チェックボックス	AAA オーバーライド機能を有効にするチェックボックス。 デフォルトでは、このチェックボックスはグレー表示されています。このチェックボックスを使用するには、[Configure AAA] オプションを使用して AAA サーバを設定する必要があります。
[Enable Posture]	チェックボックス	ポスチャアセスメントを有効にするには、このチェックボックスをオンにします。ポスチャを有効にすると、[Pre-Auth ACL List Name] ドロップダウンリストが表示されます。ポスチャは Cisco Identity Services Engine（Cisco ISE）のサービスで、ネットワークに接続されている全エンドポイントの企業のセキュリティポリシーとのコンプライアンスに関する状態（ポスチャとも呼ばれる）をチェックできます。これにより、ネットワークの防護領域にアクセスするクライアントを制御できます。
[Pre-Auth ACL List Name]	Drop Box	SSID にマッピングするために作成した ACL リスト名を選択します。 （注） ポスチャには AAA 設定が必須です。[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加します。

機能	タイプ	説明
[Advanced Settings]：[FAST TRANSITION (802.11r)]	オプションボタンとチェックボックス	802.11r Fast Transition（FT）を制御する WLAN の追加の L2 セキュリティ設定。次のオプションボタンを選択できます。 • [Adaptive]：802.11r Fast Transition をサポートするデバイスを使用できます。また、他の 802.11r および非 802.11r デバイスは、非 Fast Transition 状態で関連付けることができます。これがデフォルトの設定です。 • [Enable]：802.11r Fast Transition を有効にします。 • [Disable]：802.11r Fast Transition を無効にします。 [Over the DS]：Over-the-DS（分散システム）Fast Transition を有効にするチェックボックス。Over-the-DS Fast Transition では、ワイヤレスステーションは現在の AP を介してターゲット AP と通信し、ワイヤレスコントローラを介して転送されます。シスコと Apple 社のベストプラクティスは、デフォルトで有効になっている場合でも、Over-the-DS を無効にすることです。
[Advanced Settings]：[Protected Management Frame (802.11w)]	オプション ボタン（Radio Button）	[Protected Management Frame (802.11w)] で使用できるオプションは、[Level of Security] で選択した設定によって異なります。次のオプションを使用できる場合があります。 • 任意 • 必須 • ディセーブル [Required] オプションは、WPA3 では必須です。
[Advanced Settings]：[Session Timeout]	チェックボックスと整数フィールド	再認証することなく、クライアントセッションがアクティブである最大時間を設定します。範囲は 300 ～ 86,400 秒（5 分～ 24 時間）です。デフォルトで有効な時間は 1,800 秒（30 分）です。
[Advanced Settings]：[Client Exclusion]	チェックボックスと整数フィールド	認証失敗の最大回数を超えた後に、ワイヤレスクライアントが認証の試行から除外される時間を設定します。デフォルトで有効な時間は 180 秒（3 分）です。

機能	タイプ	説明
[Advanced Settings]：[MFP Client Protection]	オプション ボタン（Radio Button）	WLAN の 802.11w 保護された管理フレームの使用を制御する追加のセキュリティ設定。次のオプションボタンを選択できます。 • [Optional]：ワイヤレスステーションは、サポートされている 802.11w 保護された管理フレームを使用でき、PMF をサポートしない他のワイヤレスステーションは WLAN 上で共存できます。これがデフォルトの設定です。 • [Required]：ワイヤレスクライアントは、WLAN で保護された管理フレームを使用する必要があります。 • [Disabled]：保護された管理フレームが WLAN で無効になります。
[Advanced Settings]：[11k Neighbor List]	チェックボックス	WLAN の 802.11k 経由ローミングネイバーリストの使用を制御し、ワイヤレスクライアントによるパッシブおよびアクティブスキャンの必要性を制限できます。デフォルト設定は、クライアントが関連付けられている帯域（5 GHz または 2.4 GHz）に対して有効になっています。
[Advanced Settings]：[Client User Idle Timeout]	Check box	[Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウトを設定するには、このチェックボックスをオンにします。 （注） クライアントから送信されたデータがユーザー アイドル タイムアウトとして指定されたしきい値のクォータを超えている場合、そのクライアントはアクティブであると見なされ、 ワイヤレスコントローラで別のタイムアウト期間が開始されます。 デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザー アイドル タイムアウト付きで有効になっています。

機能	タイプ	説明
NAS-ID	ドロップダウン リスト	[NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。 NAS ID のカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大 31 文字の英数字、特殊文字、およびスペースを入力できます。Cisco DNA Center ではカスタムスクリプトに特殊文字 ?、"、<、および末尾のスペースは使用できません。 （注） Cisco DNA Center は、Cisco IOS XE リリース 17.7 以降を実行する Catalyst 9800 シリーズ ワイヤレス コントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。 （オプション）[+] をクリックして、別の NAS ID を追加します。最大 3 つの NAS ID を追加できます。
[Advanced Settings]：[Coverage Hole Detection]	トグル ボタン	[Coverage Hole Detection] トグルボタンを使用して、カバレッジホールの検出機能を有効または無効にします。
[Advanced Settings]：[Client Rate Limit]	整数フィールド	[Configure Client Rate Limit]：クライアントレート制限の値をビット/秒で入力します。有効な範囲は 8,000 ～ 100,000,000,000 です。値は 500 の倍数である必要があります。 Cisco IOS XE デバイスのクライアントレート制限の有効な範囲は次のとおりです。 • Cisco Catalyst 9800-L ワイヤレスコントローラ、Cisco Catalyst 9800-40 ワイヤレスコントローラ、および Cisco Catalyst 9800-80 ワイヤレスコントローラ の有効な範囲は、8,000 ～ 67,000,000,000 ビット/秒です。 • Cisco Catalyst 9800-CL ワイヤレスコントローラの有効な範囲は、8,000 ～ 10,000,000,000 ビット/秒です。 • Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ の有効な範囲は、8,000 ～ 2,000,000,000 ビット/秒です。 • Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ の有効な範囲は、8,000 ～ 100,000,000,000 ビット/秒です。

機能	タイプ	説明
[Advanced Settings]：[Directed Multicast Service]	Check box	[Directed Multicast Service]：Directed Multicast Service を有効にするには、このチェックボックスをオンにします。 （注） デフォルトでは、Directed Multicast Service（DMS）は有効になっています。クライアントはDMSを使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するようにAPに要求するため、クライアントは長時間スリープ状態になり、バッテリ電力を節約できます。
[Advanced Settings]：[Radius Client Profiling]	トグル ボタン	[Radius Client Profiling] で、このトグルボタンを使用して WLAN での RADIUS プロファイリングを有効または無効にします。 （注） この機能を有効にするには、1 つ以上の AAA または PSN サーバーが必要です。
[Advanced Settings]：[CCKM]	トグル ボタン	[Configure CCKM]：このトグルボタンを使用して、Cisco DNA Center で認証キー管理オプションとして CCKM を有効にします。 [Timestamp Tolerance]：このフィールドは、CCKM を有効にしている場合にのみ表示されます。CCKM 許容レベルを入力します。 （注） SSID に WPA2 または WPA2+WPA3 のエンタープライズとしてレイヤ 2 セキュリティがある場合にのみ、CCKM を設定できます。
[Advanced Settings]：[11v BSS Transition Support]	複数のチェックボックスと整数フィールド	WLAN の 802.11v ワイヤレスネットワーク管理（WNM）をサポートするための追加設定。以下の設定を使用できます。 [BSS Max Idle Service]：WLAN の最大アイドルサービスを有効にするチェックボックス。アソシエーションおよび再アソシエーション応答フレーム内で AP がワイヤレスクライアントにタイムアウト値を送信できるようにします。デフォルトの設定はイネーブルです。

導入ガイドで設定されているエンタープライズ ワイヤレス ネットワーク設定

表 *13*：導入ガイドで設定されているエンタープライズ ワイヤレス ネットワーク設定

機能	設定
ワイヤレス ネットワーク名（SSID）	lab3employee
ブロードキャスト SSID	点灯
管理ステータス（Admin Status）	点灯
[Wireless Option]	マルチバンド動作（2.4 GHz、5 GHz、6 GHz）
[Primary Traffic Type]	VoIP（Platinum）
AAA の設定	設定された AAA
[Level of Security]	WPA2
AAA オーバーライド	[有効（Enabled）]
[Enable Posture]	オフ
RCM クライアントの拒否	オフ
[Advanced Security Options]：[Mac Filtering]	オフ
[Advanced Security Options]：[Fast Transition]	適応型
[Type of Enterprise Network]	音声およびデータ
[Fastlane]	オフ
[Advanced Settings]：[FAST TRANSITION (802.11r)]	[Adaptive]、[Over the DS] をオン
[Advanced Settings]：[Mac Filtering]	オン
[Advanced Settings]：[Session Timeout]	オン、1,800 秒
[Advanced Settings]：[Client Exclusion]	オン、180 秒
[Advanced Settings]：[MFP Client Protection]	オプション
[Advanced Settings]：[Protected Management Frame]	ディセーブル
[Advanced Settings]：[11k Neighbor List]	オン
[Advanced Settings]：[Radius Client Profiling]	オフ
[Advanced Settings]：[Client Rate Limit]	空欄
[Advanced Settings]：[Coverage Hole Detection]	オン

機能	設定
CCKM の設定	オフ
NAS-ID	空欄
[Advanced Settings]：[11v BSS Transition Support]	[BSS Max Idle Service]：オン [Client Idle User Timeout]：オン、300 秒 [Directed Multicast Service]：オン

サイトのオーバーライドサポートの定義

異なる AAA 設定で作成された WLAN プロファイルは、異なるサイトレベルで割り当てることができます。サイトレベルでオーバーライドすると、新しい WLAN プロファイルがワイヤレスコントローラにプッシュされます。エリア、ビルディング、およびフロアレベルに基づく設定でグローバル SSID をオーバーライドできます。オーバーライドを設定するには、次の手順を実行します。

手順

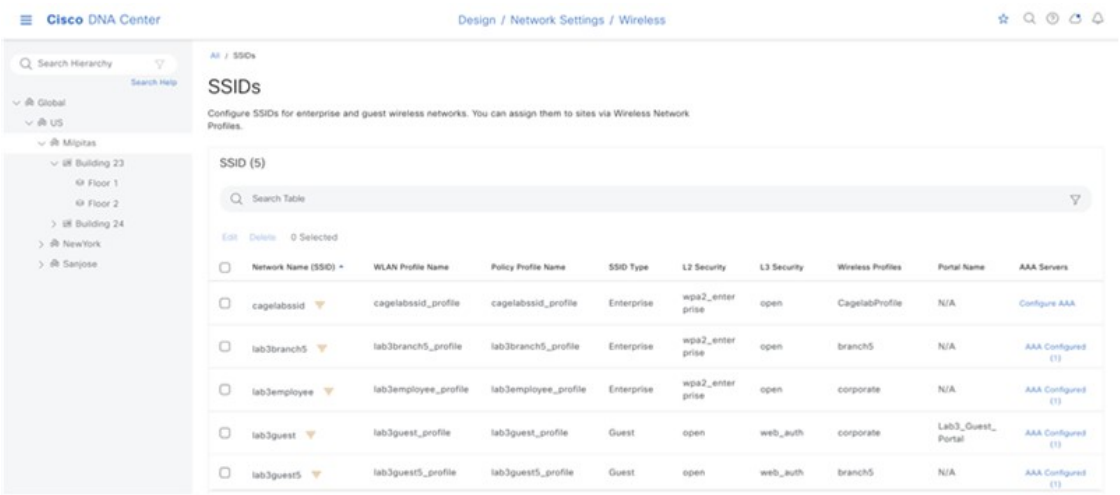
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 [SSIDs] をクリックします。

ステップ 3 サイトを展開し、左側のペインで目的のサイトをクリックします。

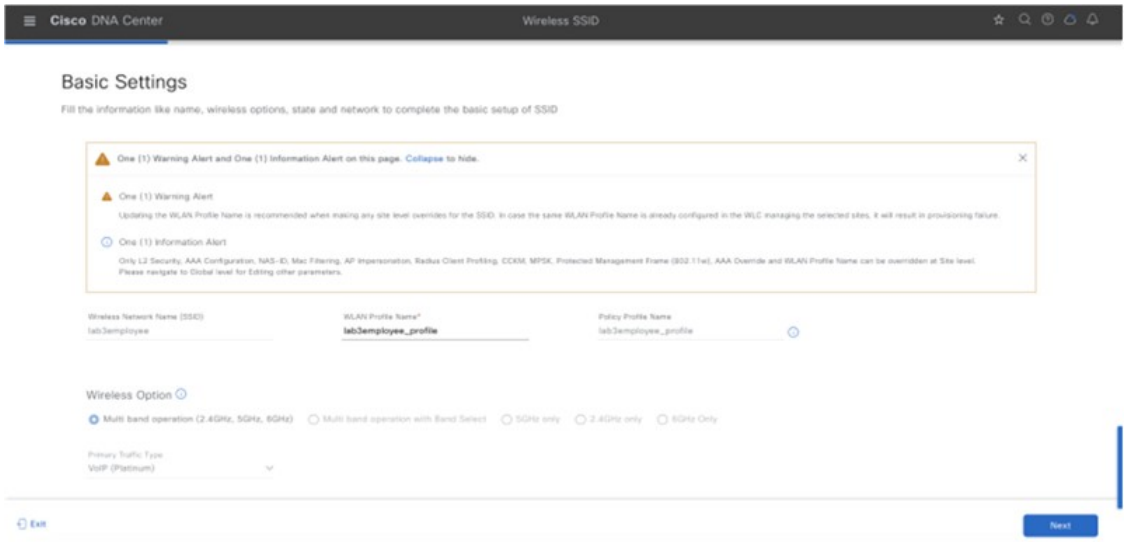
ステップ 4 **lab3employee** SSID を選択し、[Edit] をクリックします。

図 *20 : SSID* サイトオーバーライド設定



ステップ 5 [Next] をクリックし、選択したサイトのオーバーライド設定を設定します。

図 *21* : サイトのオーバーライド設定



ステップ 6 最後のページで [Save] をクリックして、サイトにプロファイルを割り当てます。

ワイヤレスコントローラの次のプロビジョニング時に、そのサイトを管理するワイヤレスコントローラに設定がプッシュされます。

（注） SSID に対してサイトレベルのオーバーライドを行う場合は、WLAN プロファイル名を更新することを推奨します。選択したサイトを管理する ワイヤレスコントローラに同じ WLAN プロファイル名がすでに設定されている場合、プロビジョニングが失敗します。

[L2 Security]、[AAA Configuration]、[NAS-ID]、[Mac Filtering]、[AP Impersonation]、[Radius Client Profiling]、[CCKM, MPSK]、[Protected Management Frame (802.11w)]、[AAA Override]、および [WLAN Profile Name] のみサイトレベルでオーバーライドできます。他のパラメータを編集するには、グローバルレベルに移動します。

ゲストワイヤレス SSID の設定

ゲスト ワイヤレス ネットワークは、サイト階層のグローバルレベルで定義する必要があります。定義すると、ゲスト ワイヤレス ネットワークをワイヤレスプロファイルに適用できます。その後、階層内の 1 つ以上のサイトにワイヤレスプロファイルを割り当てられます。

この導入ガイドでは、**lab3guest** という名前の単一のゲスト ワイヤレス ネットワーク（SSID）がプロビジョニングされます。

手順

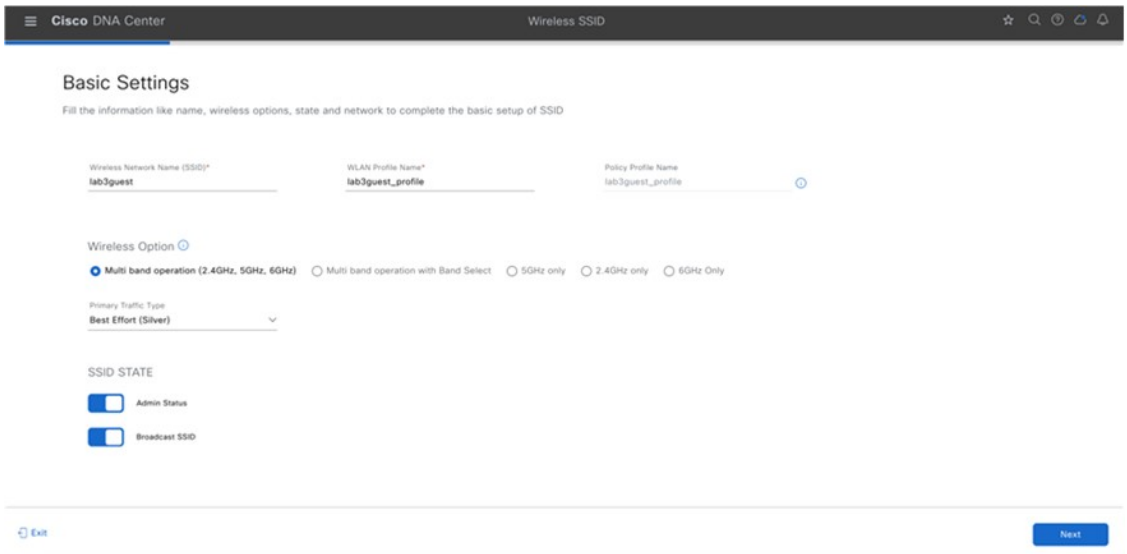
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 [SSIDs] をクリックします。

ステップ 3 [+ Add] にカーソルを合わせて、[Guest] を選択します。

[Basic Settings] ウィンドウが表示されます。

図 *22 : ゲストワイヤレス SSID を作成するための [Basic Settings] ウィンドウ*



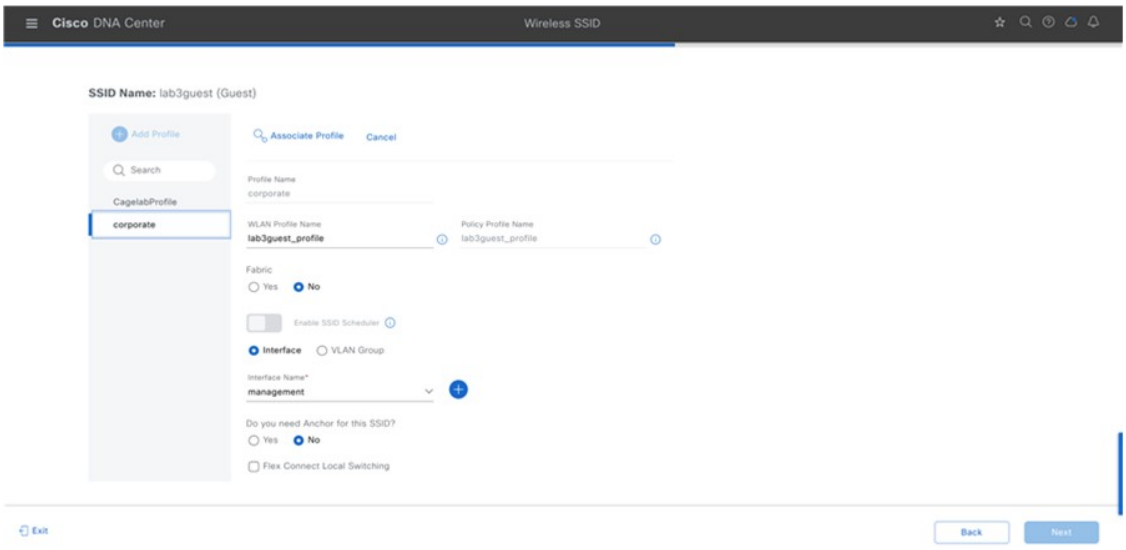
Cisco DNA Center を使用してゲスト ワイヤレス ネットワークに設定できる機能の詳細については、Cisco DNA Center を使用して設定可能なゲスト ワイヤレス ネットワーク機能 （65 ページ）を参照してください。

ステップ 4 [Basic Settings] の情報を入力し、[Next] をクリックします。

ワークフローの次の画面が表示され、ゲスト ワイヤレス ネットワークを企業の既存のワイヤレスプロファイルに接続できます。

この導入ガイド用に設定されたゲスト ワイヤレス ネットワークの設定については、導入ガイドで設定されているゲスト ワイヤレス ネットワーク設定 （78 ページ）を参照してください。

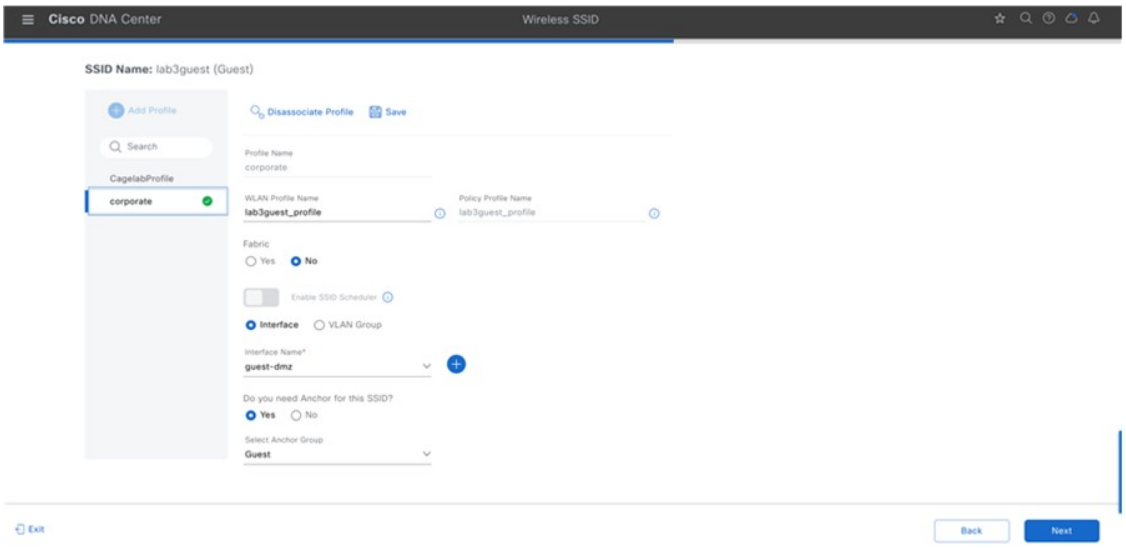
図 *23* : ゲスト ワイヤレス プロファイルの作成



ステップ 5 [Corporate Wireless] プロファイルを選択します。

ステップ 6 [Wireless Profile] サイドパネルで [Edit] をクリックして、ゲスト ワイヤレス ネットワークを追加します。

図 *24* : *[Edit a Wireless Profile]* サイドパネル



ステップ 7 [Fabric] で [No] を選択します。

[No] を選択すると、追加のフィールドが自動的に表示されます。

この導入ガイドでは、Cisco DNA Center を使用した非 SDA ワイヤレス展開についてのみ説明します。

ステップ 8 [Do you need a Guest Anchor for this Guest SSID] の横にある [Yes] を選択します。

企業（外部）とゲスト（アンカー）ワイヤレスコントローラの間に従来の自動アンカー関係が設定されます。通常、ゲスト（アンカー）ワイヤレスコントローラは、キャンパスネットワークのインターネットエッジ DMZ セグメント内にあります。[Yes] を選択した場合は、[Select Anchor Group] ドロップダウンリストから、SSID のアンカーグループを選択します。

アンカーグループを作成するには、次の手順を実行します。

a) 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network settings]**。

b) [Wireless] タブをクリックします。

c) 左側の階層ツリーから、[Global] を選択します。

d) [Anchor Groups] をクリックします。

[Anchor Groups] ウィンドウが開きます。

e) [Anchor Group] テーブルで、[Add] をクリックします。

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

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

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

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

2. [Add] をクリックします。

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

1. [Device Name] フィールドに、デバイス名を入力します。

2. [Device Series] ドロップダウンリストからデバイスシリーズを選択します。

3. [Peer IP Address] フィールドに、ピアの IP アドレスを入力します。

4. （任意）[NAT IP Address] フィールドに、ネットワークアドレス変換（NAT）IP アドレスを入力します。

5. [MAC Address] フィールドに、デバイスの MAC アドレスを入力します。

6. [Mobility Group Name] フィールドに、モビリティグループ名を入力します。

7. （任意）[Hash] フィールドに、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのハッシュを入力します。

（注） このフィールドは、Cisco Catalyst 9800-CL ワイヤレスコントローラにのみ表示されます。

8. [追加（Add）] をクリックします。

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

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

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

2. [Add] をクリックします。

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

k) [Save] をクリックします。

詳細については、『*Cisco DNA Center* ユーザーガイド』の「アンカーグループの作成」のトピックを参照してください。

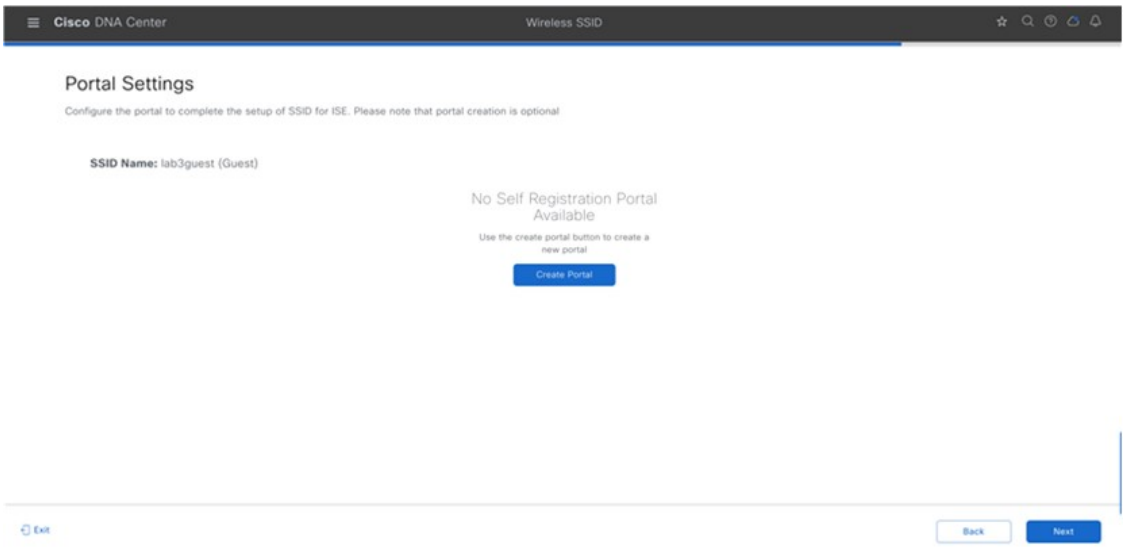
ステップ 9 [Select Interface] ドロップダウンメニューから、[guest-dmz] を選択します。

guest-dmz VLAN（VLAN 125）のゲストトラフィックが終端します。

ステップ 10 [Next] をクリックします。

[Portal Customization] ページが表示されます。

図 *25*：ゲスト ワイヤレス ネットワーク ポータルのカスタマイズの作成

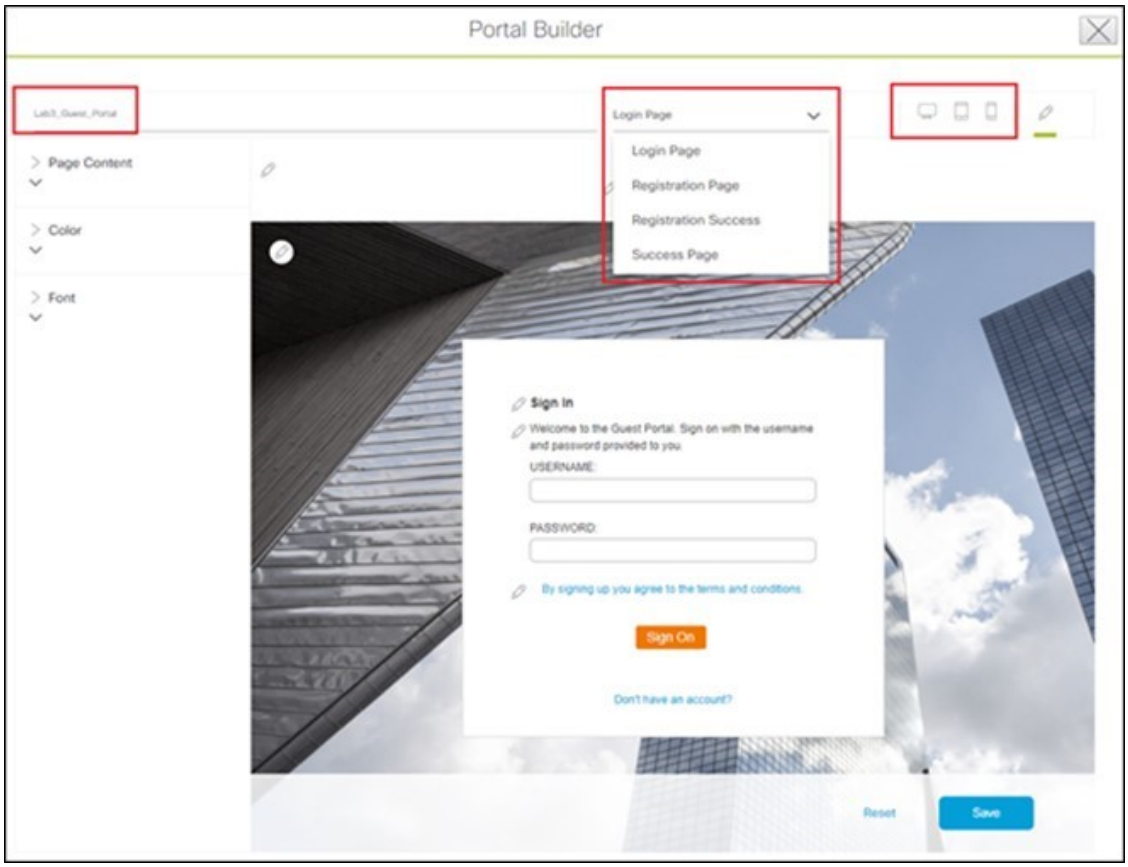


ステップ 11 Cisco ISE 内に新しいゲストポータルを追加するには、[Create Portal] をクリックします。

[Portal Builder] ページが表示されます。

ポータルを作成せずに終了することもできます。

図 *26 : [Portal Builder]* 画面



ステップ 12 必要な情報を入力します。少なくともゲストポータルに名前を付ける必要があります。

この導入ガイドでは、ポータルの名前は **Lab3_Guest_Portal** です。[Portal Builder] の中央の上部にあるドロップダウンメニューを使用すると、ポータルの [Login]、[Registration]、[Registration Success]、および [Success] ページをカスタマイズできます。また、Web ポータルの配色、フォント、ページコンテンツ、ロゴ、および背景をカスタマイズできます。ポータルをプレビューして、スマートフォン、タブレット、およびコンピュータでの表示方法も確認できます。

ステップ 13 [Save] をクリックして、Cisco ISE サーバーに新しいゲストポータルを作成し、ゲスト ワイヤレス ネットワーク ワークフローに戻ります。

新しいゲストポータルが表示されます。

ステップ 14 [Next] をクリックします。

[Guest SSID Configuration] の [Summary] ページが表示されます。

ステップ 15 [Save] をクリックします。

ゲストワイヤレス SSID（lab3guest）が [Wireless Network Settings] ダッシュボードに表示されます。

ステップ 16 ネットワークプロファイルの概要ページで [Sites] をクリックして、サイト階層を表示するパネルを開きます。

ステップ 17 [Global] で [>] をクリックして、[Milpitas] エリアを表示します。

ステップ 18 [Milpitas] エリアを選択します。

子サイトの場所である **Building 23** の **Floor 1**、**Floor 2**、および **Floor 3** と **Building 24** の **Floor 1**、**Floor 2**、および **Floor 3** が自動的に選択されます。

（注） ベストプラクティスは、ワイヤレス ネットワーク プロファイルの割り当てでは、フロアのみを選択することです。フロアを選択すると、大きな中断を伴うことなく、ネットワーク階層からフロアを削除したり、一連の特定のフロアに別のワイヤレス ネットワーク プロファイルを適用したりなどの変更ができます。別のフロアに異なる SSID がある場合、またはフロアごとに異なるプロファイルで 6E を有効にする場合は、異なるネットワークプロファイルが必要になることがあります。同じフロアに異なる SSID のセットを作成する場合は、フロアを複数の異なるネットワークプロファイルに分割する必要があります。

ステップ 19 [OK] をクリックして、サイト階層のサイドパネルを閉じます。

ステップ 20 [Attach Template(s)] の下にある [+ Add] を クリックして、CLI ベースのテンプレートをエンタープライズ ワイヤレス ネットワーク設定に追加します。

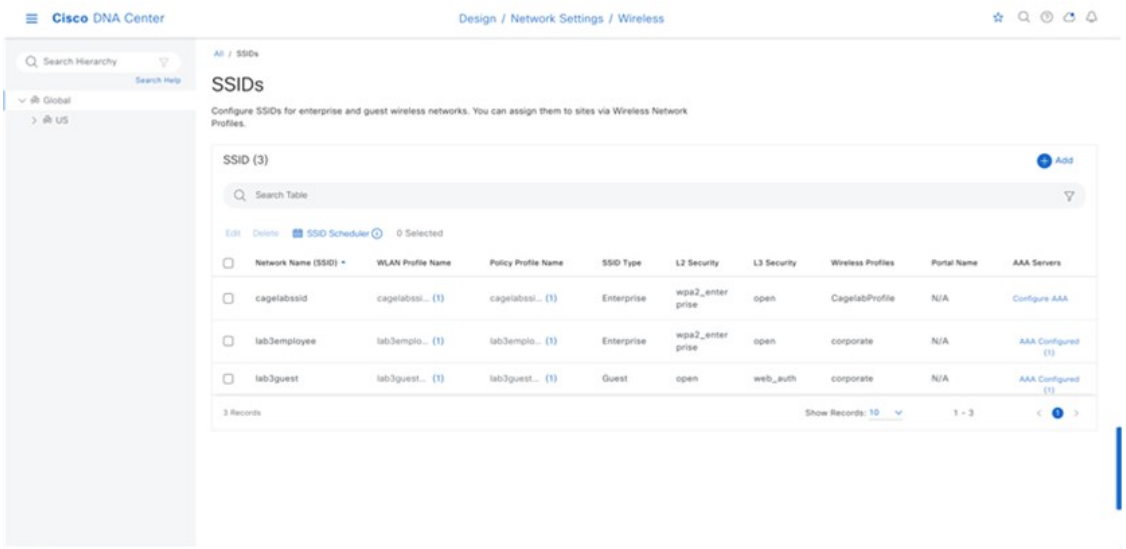
Cisco DNA Center の [Template Editor] ダッシュボード内ですべてのテンプレートを定義する必要があります。この設計および導入ガイドでは、特定の シスコ ワイヤレス コントローラ プラットフォームの CLI 構文に関する知識は不要なため、テンプレートの追加については取り上げていません。Cisco DNA Center の Web ベースのグラフィカル ユーザー インターフェイスでサポートされていないワイヤレス機能は、テンプレートを使用して追加できます。

ステップ 21 [Edit a Wireless Profile] サイドパネルで [Save] をクリックして、編集内容を企業のワイヤレスプロファイルに保存します。

lab3guest SSID が企業のワイヤレスプロファイルに追加されるため、ワイヤレスコントローラと AP が Milpitas エリアに割り当てられると、AP で **lab3guest** SSID がブロードキャストされます。

ステップ 22 [Save] をクリックして、**lab3guest** ゲスト ワイヤレス ネットワークを企業のワイヤレスプロファイルに追加します。

図 *27 :* エンタープライズおよびゲスト ***SSID*** を含む ***[Wireless Network Settings]*** ダッシュボード



Cisco DNA Center からの ISE 設定のプロビジョニングについては、Cisco DNA Center から Cisco ISE 設定をプロビジョニング （79 ページ）を参照してください。

Cisco DNA Center を使用して設定可能なゲスト ワイヤレス ネットワーク機能

表 *14 : Cisco DNA Center* を使用して設定可能なゲスト ワイヤレス ネットワーク機能

機能	タイプ	説明
ワイヤレス ネットワーク名（SSID）	テキストフィールド	WLAN の SSID。
WLAN Profile Name	テキストフィールド	Cisco DNA Center では、SSID 名に基づいて SSID_Profile がデフォルトとして使用されます。WLANプロファイル名は要件に応じて変更できます。
[Policy Profile Name]	編集不可	[Policy Profile Name] は [WLAN Profile Name] と同じであり、編集できません。 Cisco DNA Center では WLAN プロファイル名に基づいて、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのポリシープロファイル名が自動的に生成されます。

機能	タイプ	説明
[Wireless Option]	オプション ボタン（Radio Button）	SSID がブロードキャストされる RF 帯域を決定します。次のオプションを利用できます。 • マルチバンド動作（2.4 GHz、5 GHz、および 6 GHz） • バンドセレクトによるマルチバンド動作。バンドセレクト機能を使用し、2.4 GHz チャネルでのプローブ応答を遅延させることで、2.4 GHz と 5 GHz の両方の帯域で動作可能なクライアント無線を、通常は輻輳の少ない 5 GHz 帯域に移動できます。 • 5 GHz のみ。 • 2.4 GHz のみ。 • 6 GHz のみ。
[Primary Traffic Type]	Drop Box	Catalyst 9800 シリーズ ワイヤレス コントローラの場合、この設定により、WLAN/SSID のアップストリームとダウンストリームの両方向に貴金属 QoS SSID ポリシーが適用されます。集中型（ローカルモード）設計では、トラフィックが AP と シスコ ワイヤレス コントローラの間でトンネリングされるため、貴金属ポリシーにより CAPWAP ヘッダー内の最大 DSCP マーキングが制御されます。 Cisco AireOS ワイヤレスコントローラの場合、この設定により、Platinum QoS プロファイルが WLAN/SSID に適用されます。WLAN/SSID ではアプリケーションの可視性が有効になっていますが、AVC プロファイルは適用されていません。Fastlane EDCA プロファイルは、802.11a/n/ac（5 GHz）無線と 802.11b/g/n（2.4 GHz）無線の両方に設定されます。 • [VoIP (Platinum)]：ワイヤレスネットワークの QoS は、ワイヤレス音声およびデータトラフィック用に最適化されています。 • [Video (Gold)]：ワイヤレスネットワークの QoS はビデオトラフィック用に最適化されています。 • [Best Effort (Silver)]：ワイヤレスネットワークの QoS は、ワイヤレス データ トラフィック用にのみ最適化されています。 • [Nonreal Time (Bronze)]：ワイヤレスネットワークの QoS は、低帯域幅で使用するために最適化されています。
ブロードキャスト SSID	[On/Off] トグル ボタン	SSID をワイヤレスビーコンおよびプローブ応答でブロードキャストするかどうかを決定します。デフォルトの設定は [On] です。
[SSID STATE]	[On/Off] トグル ボタン	このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP はワイヤレスコントローラに関連付けられたままでアクセス可能ですが、AP には引き続きライセンスが必要です。

機能	タイプ	説明
[Level of Security] L2 セキュリティ	オプション ボタン（Radio Button）	

機能	タイプ	説明
		WLANのレイヤ2（L2）セキュリティ設定を決定します。ネットワークの暗号化および認証タイプを選択します。サイト、ビルディング、およびフロアは、グローバル階層から設定を継承します。サイト、ビルディング、またはフロアレベルでセキュリティレベルをオーバーライドできます。 次のオプションを利用できます。 • [Enterprise]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。 （注） Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。 WPA3は、WPAの最新バージョンです。これは、Wi-Fiネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。 2.4 GHzおよび5 GHz帯域のみを使用するマルチバンド動作の場合、WPA2 を有効にする必要があります（WPA3はオプションです）。2.4 GHz、5 GHz、および6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS リリース 17.7 以降を搭載したデバイスで6 GHz 帯域を動作可能にするには、WPA3 を有効にしWPA2 を無効にする必要があります。 • [Personal]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。デフォルトでは、[WPA2] チェックボックスが有効になっています。[Personal] を選択した場合は、[Passphrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間でペアワイズマスターキー（PMK）として使用されます。 （注） WPA3パーソナルは、パスワードベースの堅牢な認証を提供することによって、個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるようになります。 WPA2パーソナルの場合は、サイト、ビルディング、またはフロアレベルで、事前共有キー（PSK）をオー

機能	タイプ	説明
		バーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。詳細については、「事前共有キーのオーバーライド」を参照してください。 2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド動作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS リリース 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作可能にするには、WPA3 を有効にし WPA2 を無効にする必要があります。 （オプション）WPA2-Personal の場合、次の手順を実行してマルチ事前共有キー（MPSK）サポートを構成します。 **1.** [Configure MPSK] をクリックします。 **2.** [Configure MPSK] ダイアログボックスで、[Add to an MPSK] をクリックします。最大 5 つの MPSK を追加できます。 **3.** [Priority] ドロップダウンリストから優先順位を選択します。 （注） 優先順位 0 キーが中央 Web 認証（CWA）Flex モードで設定されていない場合、WLAN へのクライアント接続が失敗する可能性があります。 [Passphrase Type] ドロップダウンリストから、パスフレーズタイプを選択します。 **4.** [Passphrase] フィールドに、パスフレーズを入力します。 **5.** [Save] をクリックします。 MPSK はCisco AireOS ワイヤレスコントローラでサポートされていません。 MPSK は、WPA2-Personal の 2 セキュリティ構成に適用されます。 • [Open Secured]：[Assign Open SSID] ドロップダウンリストから、クライアントをオープンでセキュアな SSID にリダイレクトするためのオープン SSID を選択します。オープンでセキュアなポリシーは、セキュリティが最も低くなります。 （注） Fast Transition は、オープンでセキュアな SSID には適用できません。

機能	タイプ	説明
		• [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。
[Level of Security] L3 セキュリティ	オプション ボタン（Radio Button）	WLAN のレイヤ 3 セキュリティ設定を決定します。次のオプションを使用できます。 • [Web Auth]：Web 認証を指定します。この場合、ゲストデバイスは認証のために Web ポータルにリダイレクトされます。これがデフォルトの設定です。 • [Open]：認証不要のオープン SSID を指定します。

機能	タイプ	説明
[AUTHENTICATION SERVER]	Drop Box	この選択肢は、[Level of Security] 内で [Web Auth] が選択されている場合にのみ選択できます。Web 認証用の Web ポータルおよび認証サーバーを決定します。 • [Central Web Authentication]：この設定では、中央 Web 認証（CWA）を設定します。**[System Settings]** > **[Settings]** > **[Authentication and Policy Servers]**で定義されている Cisco ISE サーバーは、Web ポータルおよび認証サーバーの両方になります。これがデフォルトの設定です。 • [Web Authentication Internal]：レイヤ 3 セキュリティ方式である Web 認証（Web Auth）を使用すると、クライアントは、何らかの認証方式に合格するまで、Dynamic Host Configuration Protocol（DHCP）およびドメインネームシステム（DNS）のトラフィックを通過させることができます。Web 認証（内部）の場合、クライアントは シスコ ワイヤレス コントローラ によって作成されたページにリダイレクトされます。 • [Web Authentication External]：クライアントは、指定された URL にリダイレクトされます。[Web Auth URL] フィールドにリダイレクト URL を入力します。 • [Web Passthrough Internal]：Web パススルーは、ゲストアクセスに使用されるソリューションであり、認証ログイン情報は必要ありません。Web パススルー認証では、ワイヤレスユーザーは、インターネットを初めて使用するときに [Usage Policy] ページにリダイレクトされます。ポリシーを承認すると、クライアントはインターネットを使用できます。 • [Web Passthrough External]：クライアントは、指定された URL にリダイレクトされます。[Web Auth URL] フィールドにリダイレクト URL を入力します。 • [Open]：レイヤ 3 レベルのセキュリティは不要で、すべてのデバイスが SSID に接続できます。
[AUTHENTICATION SERVER] > [ISE Authentication] > [What kind of portal are you creating today?]	ドロップダウンメニュー	この選択肢は、[ISE Authentication] が選択されている場合にのみ選択できます。Cisco ISE サーバー内に作成されるゲストポータルのタイプを決定します。次のオプションを使用できます。 • [Self Registered]：このタイプのポータルでは、ゲストはネットワークに自分自身をオンボーディングします。これがデフォルトの設定です。 • [Hotspot]：802.11u ホットスポットポータルを設定します。

機能	タイプ	説明
[AUTHENTICATION SERVER] > [ISE Authentication] > [Where will your guests redirect after successful authentication?]	ドロップダウンメニュー	この選択肢は、[ISE Authentication] が選択されている場合にのみ選択できます。ゲストがネットワークに正常に認証された後に表示される Web ページを決定します。次のオプションを使用できます。 • [Success Page]：認証が成功したことを示すために作成する専用ページ。このページから、ゲストは到達しようとしていた元の URL を再入力する必要があります。 • [Original URL]：認証が成功すると、ゲストは到達しようとしていた元の URL に自動的にリダイレクトされます。これがデフォルトの設定です。 • [Custom URL]：認証が成功すると、ゲストは選択した URL に自動的にリダイレクトされます。
[AUTHENTICATION SERVER] > [External Authentication] > [Web Auth URL?]	テキストフィールド	この選択肢は、[External Authentication] が選択されている場合にのみ選択できます。Web 認証サーバーの URL を指定します。ゲストはこの URL にリダイレクトされ、ネットワークに認証されます。

機能	タイプ	説明
AAA の設定	リンク	[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加して設定します。[Drop Box] から [Authentication, Authorization, and Accounting server] を選択します。 [+] をクリックしてサーバーを追加します。 （注） Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラのエンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。 アカウンティングに AAA サーバーを使用するには、[Copy Same Servers for Accounting] チェックボックスをオンにします。 SSID に別のアカウンティングサーバーを設定するには、次の手順を実行します。 **1.** [Configure Accounting Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、アカウンティングサーバーの IP アドレスを選択できます。 **2.** [+] をクリックしてサーバーを追加します。 （注） Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラのエンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つのアカウンティングサーバーを設定できます。 **3.** [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。 Cisco DNA Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Cisco DNA Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Cisco DNA Center によって作成されます。 サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。

機能	タイプ	説明
[Mac Filtering]	チェックボックス	ワイヤレスネットワークにおける MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。 （注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。
AAA オーバーライド	チェックボックス	AAA オーバーライド機能を有効にするチェックボックス。 デフォルトでは、このチェックボックスはグレー表示されています。このチェックボックスを使用するには、[Configure AAA] オプションを使用して AAA サーバを設定する必要があります。
スリープ状態のクライアントのタイムアウト設定	[Select] オプションボタン	スリープ状態のクライアントの [Timeout Settings] で [Web Authentication Internal]、[Web Authentication External]、[Web Passthrough Internal]、または [Web Passthrough External] を選択した場合は、次のいずれかの認証オプションを選択します。 [Always authenticate]：スリープ状態のクライアントの認証が有効になります。 [Authenticate after]：再認証が必要になるまでスリープ状態にあるクライアントが記憶される期間を入力します。有効な範囲は 10 ～ 43,200 分で、デフォルト期間は 720 分です。 （注） ゲストアクセスで Web 認証済みクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 10 ～ 43,200 分で、デフォルトは 720 分です。WLAN にマッピングされるユーザ グループ ポリシーと WLAN に、期間を設定できます。スリープタイマーは、アイドルタイムアウト後に有効になります。クライアントタイムアウトが WLAN のスリープタイマーに設定された時間より短い場合は、クライアントのライフタイムがスリープ時間として使用されます。
RCM クライアントの拒否	チェックボックス	ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。
[Pre-Auth ACL List Name]	Drop Box	SSID にマッピングするために作成した ACL リスト名を選択します。

機能	タイプ	説明
[Fastlane]	チェックボックス	このチェックボックスは、[Type of Enterprise Network] が [Voice and Data] として選択されている場合にのみオンにできます。 Catalyst 9800 シリーズ ワイヤレス コントローラの場合、[Fastlane] チェックボックスをオンにすると、Fastlane モードで自動 QoS が有効になります。Fastlane モードの自動 QoS では、5 GHz 帯域と 2.4 GHz 帯域の両方に Fastlane EDCA プロファイルが設定されます。[Fastlane] チェックボックスがオンになっている場合、貴金属 QoS SSID ポリシーは WLAN/SSID に適用されません。 Cisco AireOS ワイヤレスコントローラの場合、この設定により、WLAN/SSID の Fastlane マクロが有効になります。Fastlane マクロを使用すると、Platinum QoS プロファイルが WLAN/SSID に適用されます。アプリケーションの可視性は、AUTOQOS-AVC-PROFILE という名前の AVC プロファイルを使用して WLAN/SSID で有効になっています。QoS マップは、アップストリーム方向の DSCP を信頼するように変更されます。ダウンストリーム方向では、DSCP 値を UP 値にマッピングするときに、シスコのベストプラクティスが実装されます。
[Advanced Settings]：[Session Timeout]	チェックボックスと整数フィールド	再認証することなく、クライアントセッションがアクティブである最大時間を設定します。範囲は 300 ～ 86,400 秒（5 分～ 24 時間）です。デフォルトで有効な時間は 1,800 秒（30 分）です。
[Advanced Settings]：[Client Exclusion]	チェックボックスと整数フィールド	認証失敗の最大回数を超えた後に、ワイヤレスクライアントが認証の試行から除外される時間を設定します。デフォルトで有効な時間は 180 秒（3 分）です。
[Advanced Settings]：[MFP Client Protection]	オプション ボタン（Radio Button）	WLAN の 802.11w 保護された管理フレームの使用を制御する追加のセキュリティ設定。次のオプションを使用できます。 • [Optional]：ワイヤレスステーションは、サポートされている 802.11w 保護された管理フレームを使用でき、PMF をサポートしない他のワイヤレスステーションは WLAN 上で共存できます。これがデフォルトの設定です。 • [Required]：ワイヤレスクライアントは、WLAN で保護された管理フレームを使用する必要があります。 • [Disabled]：保護された管理フレームが WLAN で無効になります。
[Advanced Settings]：[11k Neighbor List]	チェックボックス	WLAN の 802.11k 経由ローミングネイバーリストの使用を制御し、ワイヤレスクライアントによるパッシブおよびアクティブスキャンの必要性を制限できます。デフォルト設定は、クライアントが関連付けられている帯域（5 GHz または 2.4 GHz）に対して有効になっています。

機能	タイプ	説明
[Advanced Settings]：[11v BSS Transition Support]	複数のチェックボックスと整数フィールド	WLAN の 802.11v ワイヤレスネットワーク管理（WNM）をサポートするための追加設定。以下の設定を使用できます。 • [BSS Max Idle Service]：WLAN の最大アイドルサービスを有効にするチェックボックス。アソシエーションおよび再アソシエーション応答フレーム内で AP がワイヤレスクライアントにタイムアウト値を送信できるようにします。デフォルト設定はイネーブルです。 • [Client User Idle Timeout]：WLAN のクライアントからフレームを受信せずに、ワイヤレスクライアントが関連付けられた状態が AP で維持される最大時間を指定する有界整数フィールドのチェックボックス。オンにすると、クライアントのスリープ時間が長くなり、モバイルデバイスのバッテリ使用量が節約されます。デフォルト設定は有効で、時間は 300 秒です。 • [Directed Multicast Service]：クライアントが、マルチキャストストリームをユニキャストストリームとして AP からクライアントに送信するように要求できるようにするチェックボックス。デフォルトで、この設定は有効になっています。
NAS-ID	ドロップダウンリスト	[NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。 NAS ID のカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大 31 文字の英数字、特殊文字、およびスペースを入力できます。Cisco DNA Center ではカスタムスクリプトに特殊文字 ?、"、<、および末尾のスペースは使用できません。 （注） Cisco DNA Center は、Cisco IOS XE リリース 17.7 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。 （オプション）[+] をクリックして、別の NAS ID を追加します。最大 3 つの NAS ID を追加できます。 Cisco DNA Center では Cisco AireOS ワイヤレスコントローラに 1 つの NAS ID のみ適用されます。**[Design]** > **[Network Settings]** > **[Wireless]** からサイトレベルで NAS ID を上書きできます。
[Advanced Settings]：[Coverage Hole Detection]	トグル ボタン	[Coverage Hole Detection] トグルボタンを使用して、カバレッジホールの検出機能を有効または無効にします。

機能	タイプ	説明
[Advanced Settings]：[Client Rate Limit]	整数フィールド	クライアントレート制限を設定するには、クライアントレート制限の値をビット/秒で入力します。有効な範囲 は 8,000 ～ 100,000,000,000 です。値は 500 の倍数である必要があります。 （注） この構成はCisco AireOS ワイヤレスコントローラには適用できません。Cisco AireOS ワイヤレスコントローラ のクライアントレート制限を設定するには、メニューアイコンをクリックして、 **[Tools]** > **[Model Config Editor]** > **[Wireless]** > **[Advanced SSID Configuration]**を選択します。詳細については、「高度な SSID のモデル設定設計の作成」を参照してください。 Cisco IOS XE デバイスのクライアントレート制限の有効な範囲は次のとおりです。 • Cisco Catalyst 9800-L ワイヤレスコントローラ、Cisco Catalyst 9800-40 ワイヤレスコントローラ、および Cisco Catalyst 9800-80 ワイヤレスコントローラ の有効な範囲は、8,000 ～ 67,000,000,000 ビット/秒です。 • Cisco Catalyst 9800-CL ワイヤレスコントローラの有効な範囲は、8,000 ～ 10,000,000,000 ビット/秒です。 • Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ の有効な範囲は、8,000 ～ 2,000,000,000 ビット/秒です。 • Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ の有効な範囲は、8,000 ～ 100,000,000,000 ビット/秒です。
[Advanced Settings]：[Radius Client Profiling]	トグル ボタン	[Radius Client Profiling] で、このトグルボタンを使用して WLAN での RADIUS プロファイリングを有効または無効にします。 （注） この機能を有効にするには、1 つ以上の AAA または PSN サーバーが必要です。
[Advanced Settings]：[CCKM]	トグル ボタン	[Configure CCKM]：このトグルボタンを使用して、Cisco DNA Center で認証キー管理オプションとして CCKM を有効にします。 [Timestamp Tolerance]：このフィールドは、CCKM を有効にしている場合にのみ表示されます。CCKM許容レベルを入力します。CCKM許容レベルは、Cisco AireOS ワイヤレスコントローラ プラットフォームには適用されません。 （注） SSID に WPA2 または WPA2+WPA3 のエンタープライズとしてレイヤ 2 セキュリティがある場合にのみ、CCKM を設定できます。

機能	タイプ	説明
[Advanced Settings]：[Protected Management Frame (802.11w)]	オプション ボタン（Radio Button）	[Protected Management Frame (802.11w)] で使用できるオプションは、[Level of Security] で選択した設定によって異なります。次のオプションを使用できる場合があります。 • 任意 • 必須 • ディセーブル

導入ガイドで設定されているゲスト ワイヤレス ネットワーク設定

表 *15*：導入ガイドで設定されているゲスト ワイヤレス ネットワーク設定

機能	設定
ワイヤレス ネットワーク名（SSID）	lab3guest5
ブロードキャスト SSID	点灯
管理ステータス（Admin Status）	点灯
[Wireless Option]	マルチバンド動作（2.4 GHz、5 GHz、6 GHz）
[Primary Traffic Type]	[Best Effort (Silver)]
[Level of Security]	Web 認証
[AUTHENTICATION SERVER]	ISE 認証
[AUTHENTICATION SERVER] > [ISE Authentication] > [What kind of portal are you creating today?]	自己登録
[AUTHENTICATION SERVER] > [ISE Authentication] > [Where will your guests redirect after successful authentication?]	元の URL
AAA の設定	設定された AAA
AAA オーバーライド	[有効（Enabled）]
[Mac Filtering]	オン
[Fastlane]	オフ
RCM クライアントの拒否	オフ
事前認証 ACL	設定済みの事前認証 ACL を選択
[Advanced Settings]：[FAST TRANSITION (802.11r)]	ディセーブル

機能	設定
[Advanced Settings]：[MFP Client Protection]	オプション
[Advanced Settings]：[Protected Management Frame]	ディセーブル
[Advanced Settings]：[Session Timeout]	オン、1,800 秒
[Advanced Settings]：[Client Exclusion]	オン、180 秒
[Advanced Settings]：[MFP Client Protection]	オプション
[Advanced Settings]：[11k Neighbor List]	オン
[Advanced Settings]：[Radius Client Profiling]	オフ
[Advanced Settings]：[Client Rate Limit]	空欄
[Advanced Settings]：[Coverage Hole Detection]	オン
CCKM の設定	オフ
NAS-ID	空欄
[Advanced Settings]：[11v BSS Transition Support]	[BSS Max Idle Service]：オン [Client Idle User Timeout]：オン、300 秒 [Directed Multicast Service]：オン

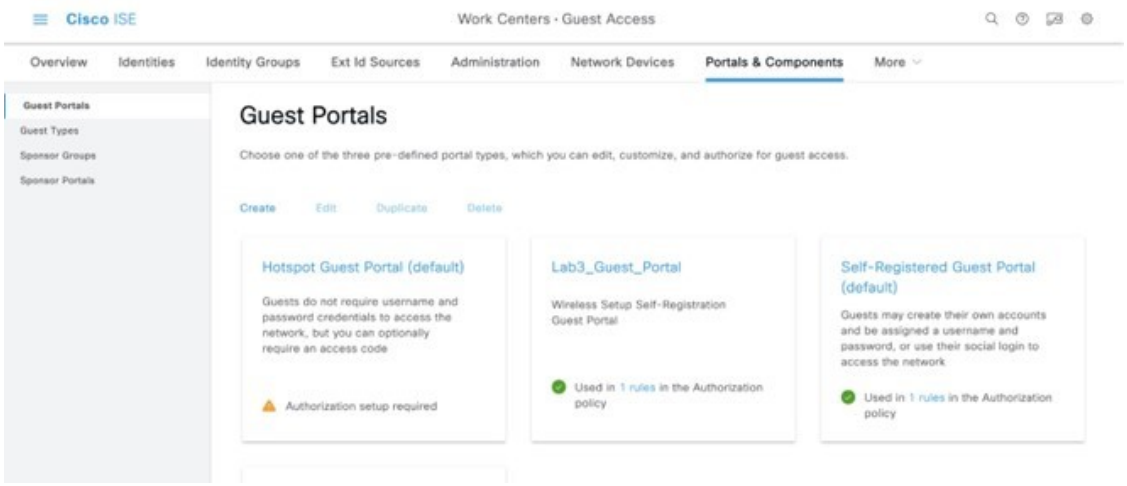
Cisco DNA Center から Cisco ISE 設定をプロビジョニング

ゲスト SSID プロファイルがサイトに割り当てられると、Cisco DNA Center は、ゲスト SSID プロファイルの設定に従って、必要な認証、許可、およびゲストポータルの設定を Cisco ISE にプッシュします。

手順

ステップ 1 [Lab3_Guest_Portal] を選択して、ポータルの詳細を確認します。

図 *28 : Cisco ISE* のゲストポータル



ISE に **Lab3_Guest_Portal** という名前の新しいゲストポータルが表示されます。

.

ステップ 2 [1 rules] リンクをクリックして、Cisco DNA Center によって作成された認証ポリシーを確認します。

図 *29 :* ゲストポータルのリダイレクトポリシー

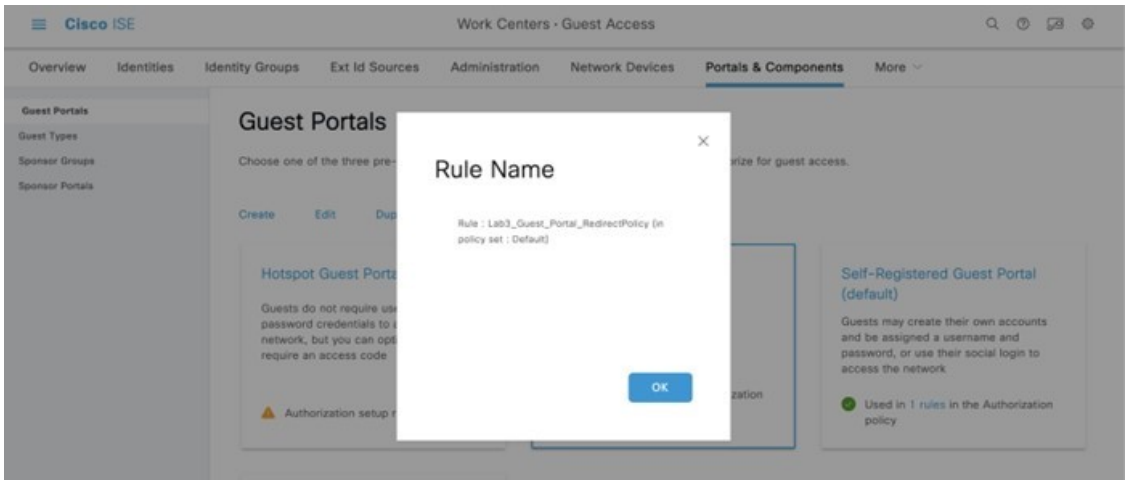
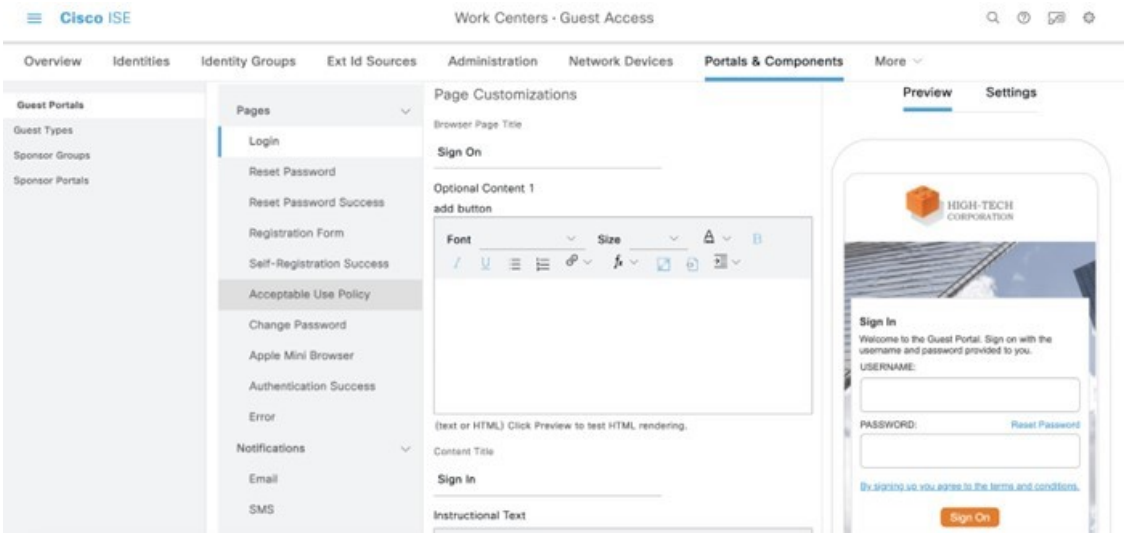


図 *30* : ゲストポータルのプレビュー

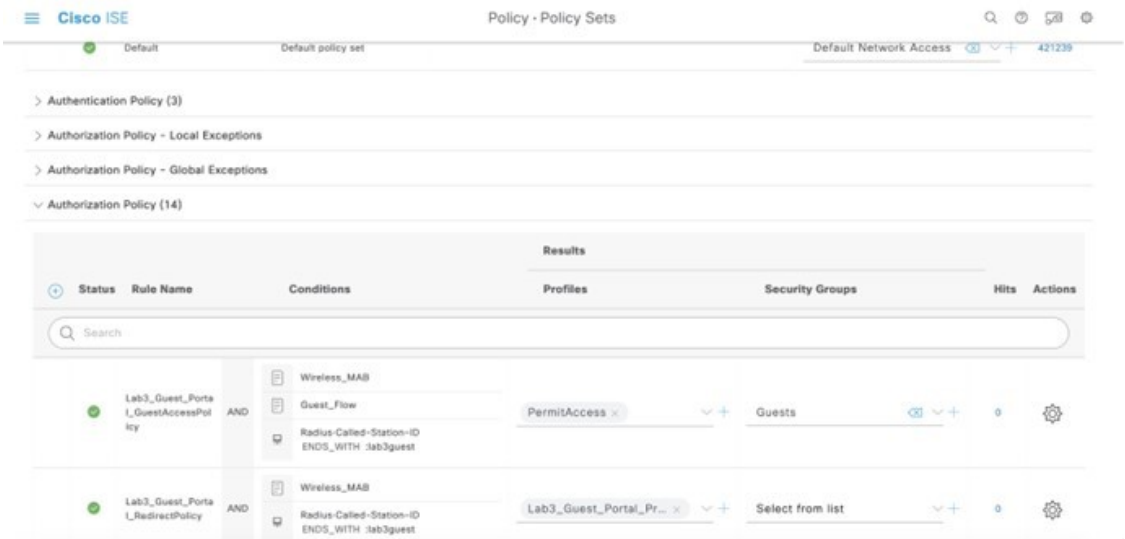


ステップ 3 左上隅にあるメニューアイコンをクリックして、**[Policy]** > **[Policy sets]**の順に選択します。

ステップ 4 [デフォルト（Default）] をクリックします。

ステップ 5 [Authorization Policy] に移動し、Cisco DNA Center によってプッシュされた認証ポリシーを確認します。

図 *31* : ゲスト *SSID* 認証ポリシー



リモートオフィスのワイヤレス展開の設定

ここでは、Cisco DNA Center を使用してプロビジョニングされる AP を FlexConnect モードで使用するリモートオフィスのワイヤレスネットワークの概要について説明します。

サイト階層の構成は次のとおりです。

- ビルディング（**Branch 5**）と複数のフロア（**Floor 1**、**Floor 2**、**Floor 3**）があるブランチエリア（**New York**）。
- 従業員トラフィック用のSSID（**lab3branch5**）とゲストトラフィック用のSSID（**lab3guest5**）。どちらもブランチ内の AP によってアドバタイズされます。
- すべての従業員ブランチのワイヤレストラフィックが中央でスイッチングされる、シスコ以外のSDA（レガシー）リモートオフィスのワイヤレス展開。

ブランチ内のゲスト ワイヤレス トラフィックはローカルにスイッチングされます。シスコ ワイヤレス コントローラは N+1 HA モードになり、Cisco DNA Center プロビジョニングプロセス中にサイトに割り当てる必要があります。

（注） この導入ガイドでは、Catalyst 9800-40 ワイヤレスコントローラ（C9800-Flex-CVD および C9800-CVD-Nplus1）の両方が **New York** エリア内の **Branch 5** のビルディングに割り当てられます。

Cisco DNA Center 内では、AP を含むサイト（エリア、ビルディング、またはフロア）は、プライマリ管理対象 AP の場所やセカンダリ管理対象APの場所として割り当てられます。特定の時点でサイトに割り当てられるプライマリ エンタープライズ ワイヤレスコントローラ は 1 つだけです。つまり、サイトは、一度に 1 つのエンタープライズ ワイヤレスコントローラ のプライマリ管理対象 AP の場所としてのみ割り当てられます。この導入ガイドでは、**Branch 5** 内の **Floor 1** の AP は、Cisco DNA Center を介して C9800-Flex-CVD にプロビジョニングされます。

Cisco DNA Center では、AP 高可用性の設定がサポートされており、AP はプライマリおよびセカンダリ ワイヤレスコントローラとの関連付けを試み、CAPWAP 制御接続を形成しようとします。プライマリ ワイヤレスコントローラが使用できない場合、APはセカンダリ ワイヤレスコントローラへのCAPWAP制御接続を確立しようとします。Cisco DNA Center では、AP を含むサイトをセカンダリ管理対象 AP の場所として設定することで実現されます。

（注） この設計および導入ガイドでは、ワイヤレスコントローラ C9800-Flex-CVD をプロビジョニングして、**Branch 5** の **Floor 1** がプライマリ管理対象 AP の場所になるようにします。**Branch 5** 内の AP の場合、ワイヤレスコントローラ C9800-CVD-Nplus1 は、N+1 ワイヤレスコントローラ冗長構成のセカンダリ ワイヤレスコントローラとして機能します。

推奨事項

リモートオフィスのワイヤレス展開設定を設定する場合は、次の推奨事項を考慮してください。

- FlexConnect モードの AP の AP スイッチポートで PortFast を使用し、中央でスイッチされる WLAN のみをサポートします。PortFast のスイッチポートを設定するには、switch port host コマンドまたは PortFast コマンドを使用して、ポートをホストポートとして接続するように設定します。この設定により、AP の参加プロセスが高速になります。ローカルモードのAPではVLAN間でトラフィックが直接ブリッジされないため、ループが発生するリスクはありません。ポートはアクセスモードで直接設定できます。
- FlexConnect モードの AP で、異なる VLAN にマッピングされたローカルにスイッチされる WLAN を使用する場合（AP スイッチポートはトランクモード）、ポートに存在する VLAN をプルーニングまたは制限して、AP が設定された VLAN と一致させます。

ワイヤレスインターフェイスの設定

Cisco DNA Center では、エンタープライズ WLAN とゲスト WLAN は、イーサネット VLAN インターフェイスと呼ばれるワイヤレスインターフェイスで終端します。次の表に、この設計および導入ガイドでエンタープライズおよびゲスト WLAN 用に作成されたワイヤレスインターフェイスを示します。

表 *16 :* ワイヤレスインターフェイス

名前	VLAN	使用方法
branchemployee	100	中央でスイッチングされる従業員トラフィック用の VLAN。
branchguest-dmz	110	スイッチ上の VLAN でローカルにスイッチングされるゲストトラフィック用の VLAN。

（注） ネイティブ VLAN（AP VLAN）設定は、FlexConnect AP 展開に固有です。FlexConnect のローカルにスイッチングされるトラフィックは、この設計および導入ガイドのワイヤレスプロファイルで設定されている特定の VLAN で終端するため、フィールドは空白のままになります。

次の手順では、Cisco DNA Center 内でワイヤレスインターフェイスを設定する方法について説明します。

始める前に

このアクションを完了するには、SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE 権限が必要です。

手順

ステップ 1 インスタンスの IP アドレスまたは完全修飾ドメイン名を使用して、Cisco DNA Center Web コンソールにログインします。

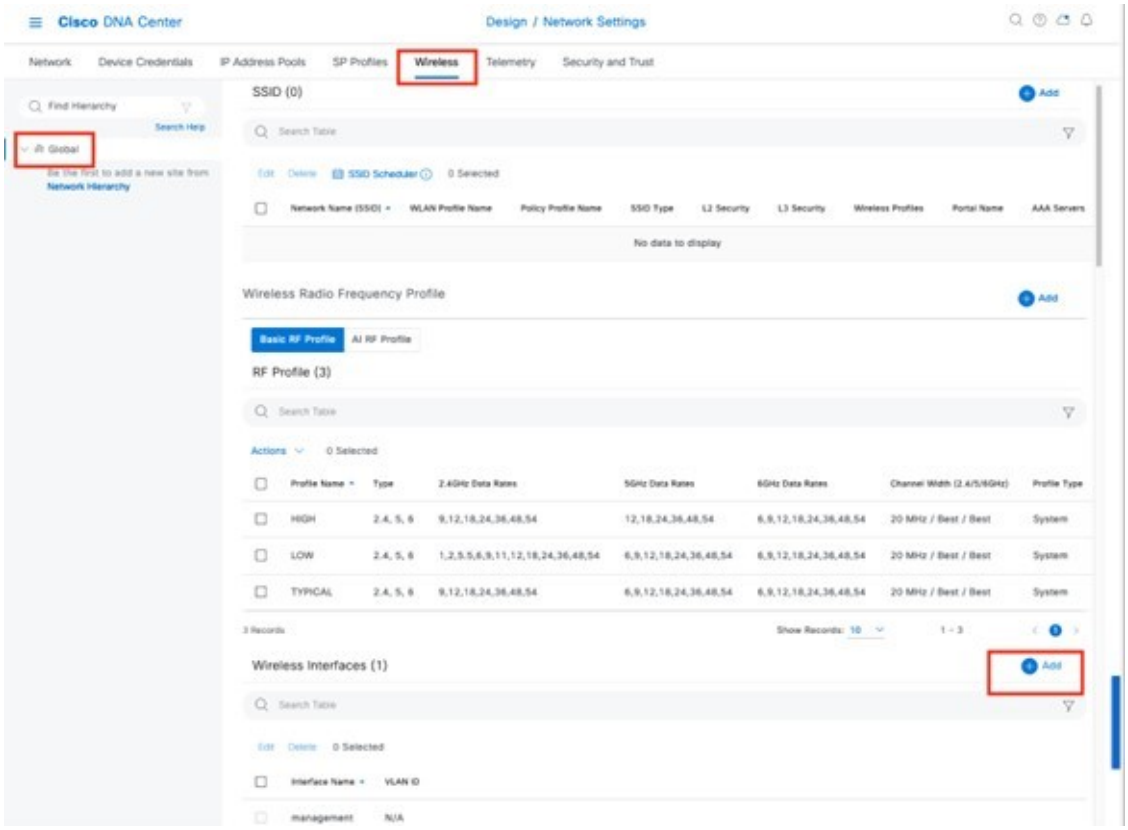
例：

https://<Cisco_DNA_Center_IPaddr_or_FQDN>

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

[Wireless Network Settings] ダッシュボードが表示されます。次の図に例を示します。

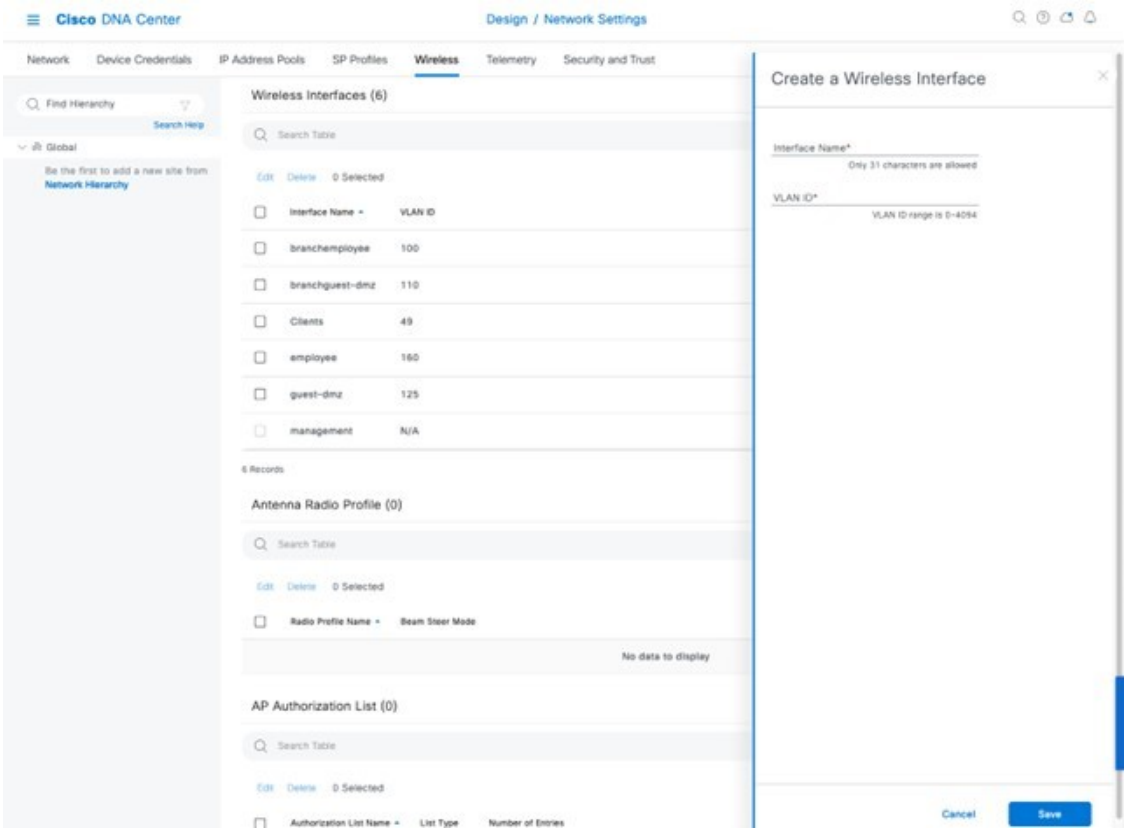
図 *32 :* ワイヤレスインターフェイスの追加



ステップ 3 エンタープライズ VLAN（**branchemployee**）に対応するワイヤレスインターフェイスの [Interface Name] と [VLAN ID] を入力します。

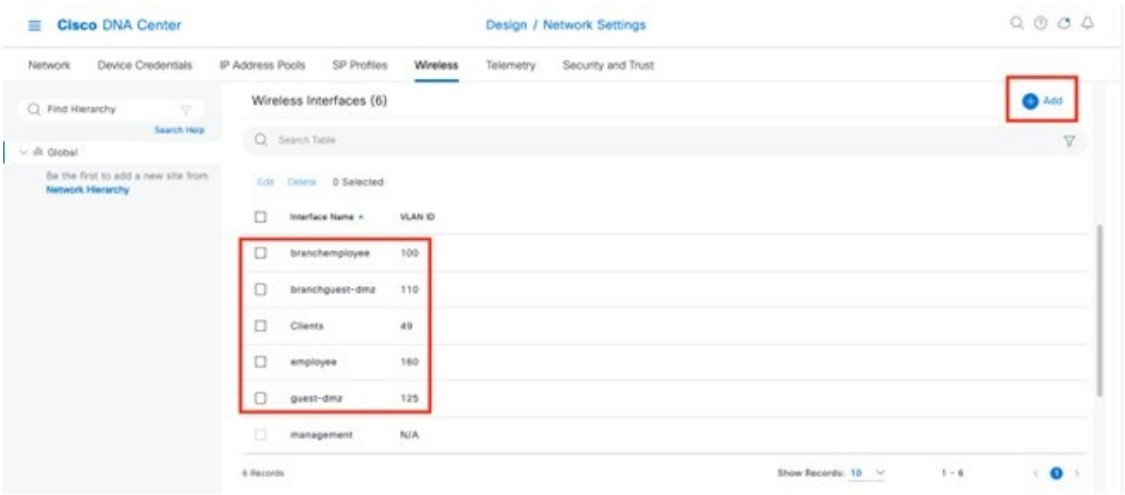
ステップ 4 [追加（Add）] をクリックします。

図 ***33*** *:* ワイヤレスインターフェイスの下にあるインターフェイスと ***VLAN***



この手順を繰り返して、ゲストVLAN（**guest-dmz**）のワイヤレスインターフェイスを追加します。完了すると、次の図に示されているように、2つの新しいワイヤレスインターフェイスが[Wireless Network Settings]ダッシュボードに表示されます。

図 ***34*** *:* 作成されたワイヤレスインターフェイス



エンタープライズワイヤレス SSID の設定

エンタープライズ ワイヤレス ネットワークは、展開全体でブロードキャストに使用できる非ゲスト WLAN/SSID なので、サイト階層のグローバルレベルで定義する必要があります。定義すると、エンタープライズワイヤレス ネットワークをワイヤレスプロファイルに適用し、ワイヤレスプロファイルを階層内の 1 つ以上のサイトに割り当てられます。

この設計および導入ガイドでは、**lab3branch5** という名前の単一のエンタープライズ WLAN SSID がプロビジョニングされます。

手順

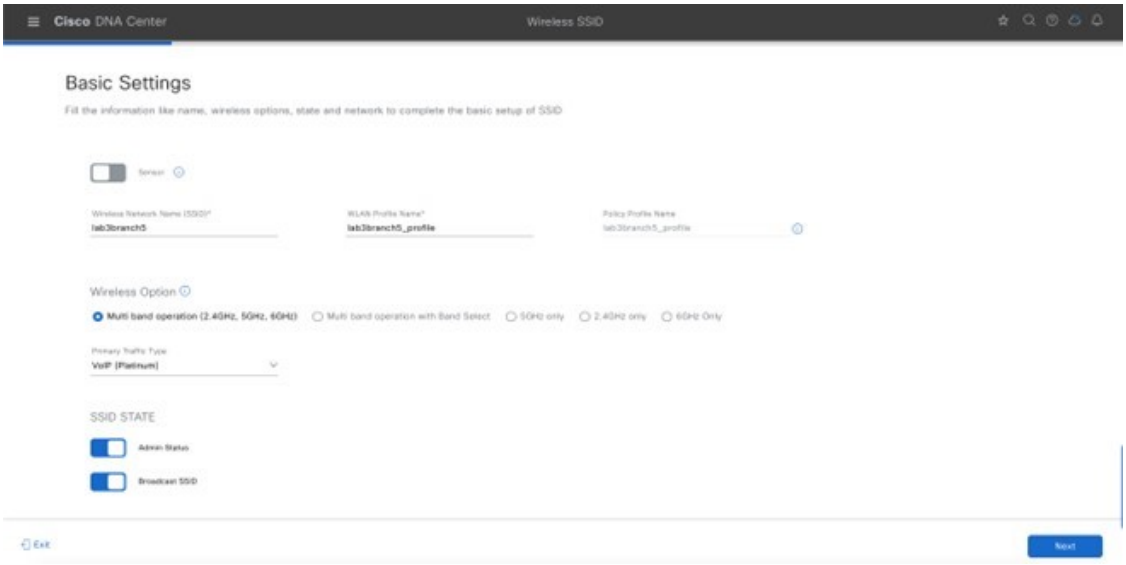
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 [SSIDs] をクリックします。

ステップ 3 [+ Add] にカーソルを合わせて、[Enterprise] を選択します。

[Basic Settings] ウィンドウが表示されます。

図 *35 :* 新しいエンタープライズ *SSID* を作成するための *[Basic Settings]* ウィンドウ



Cisco DNA Center を使用してエンタープライズ ワイヤレス ネットワーク用に設定できる機能については、Cisco DNA Center で設定可能なエンタープライズ ワイヤレス ネットワーク機能 （43 ページ）を参照してください。

ステップ 4 [Basic Settings] の情報を入力し、[Next] をクリックします。

（注） この導入ガイド用に設定されたエンタープライズ ワイヤレス ネットワークの設定については、導入ガイドで設定されているエンタープライズ ワイヤレス ネットワーク設定 （56 ページ）を参照してください。

図 *36* : エンタープライズ *SSID* のセキュリティ設定

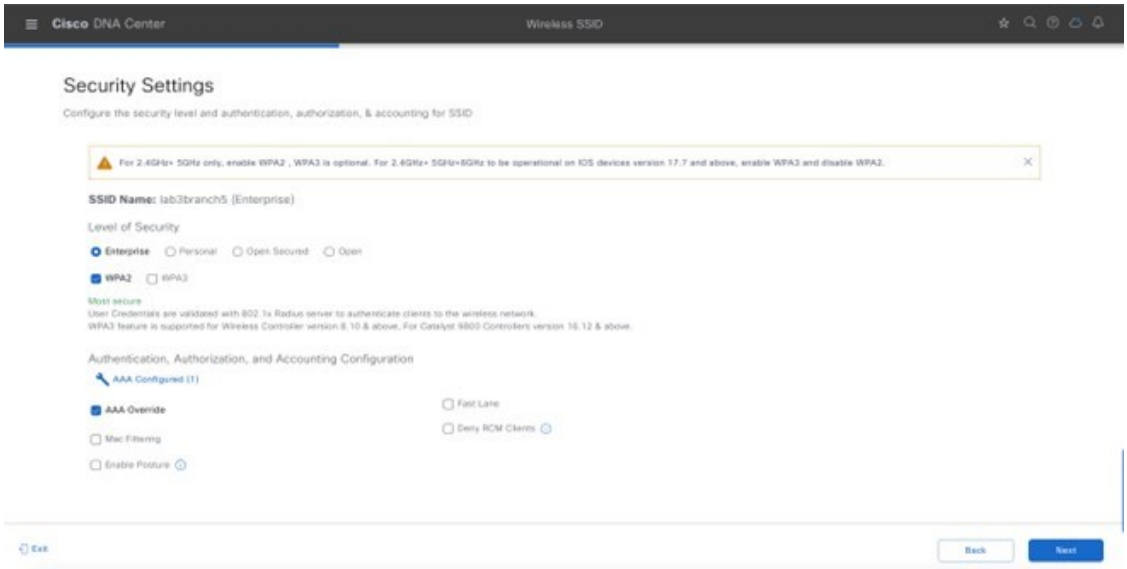
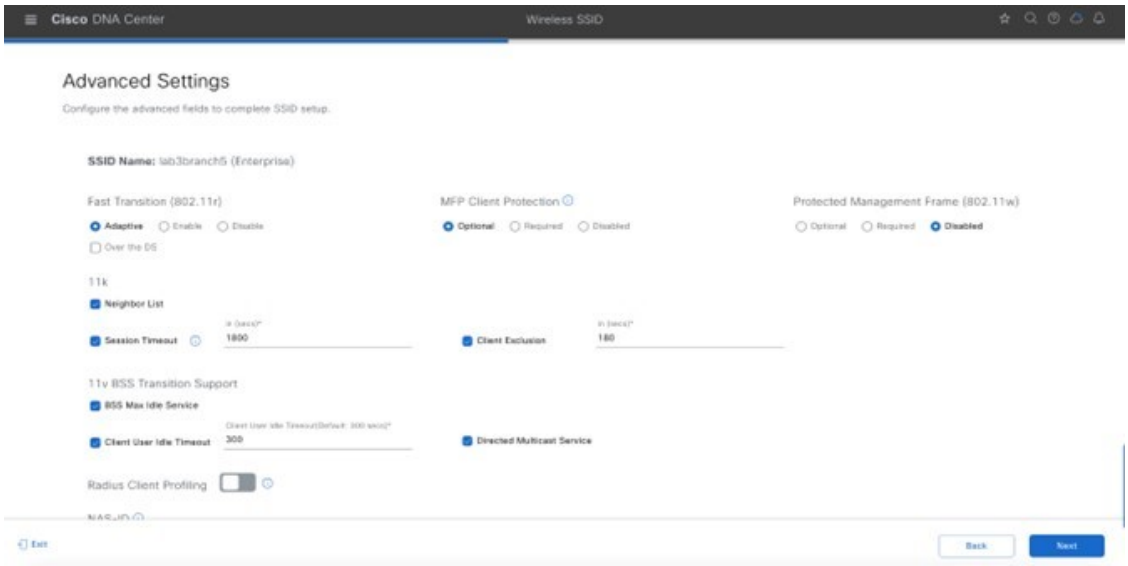


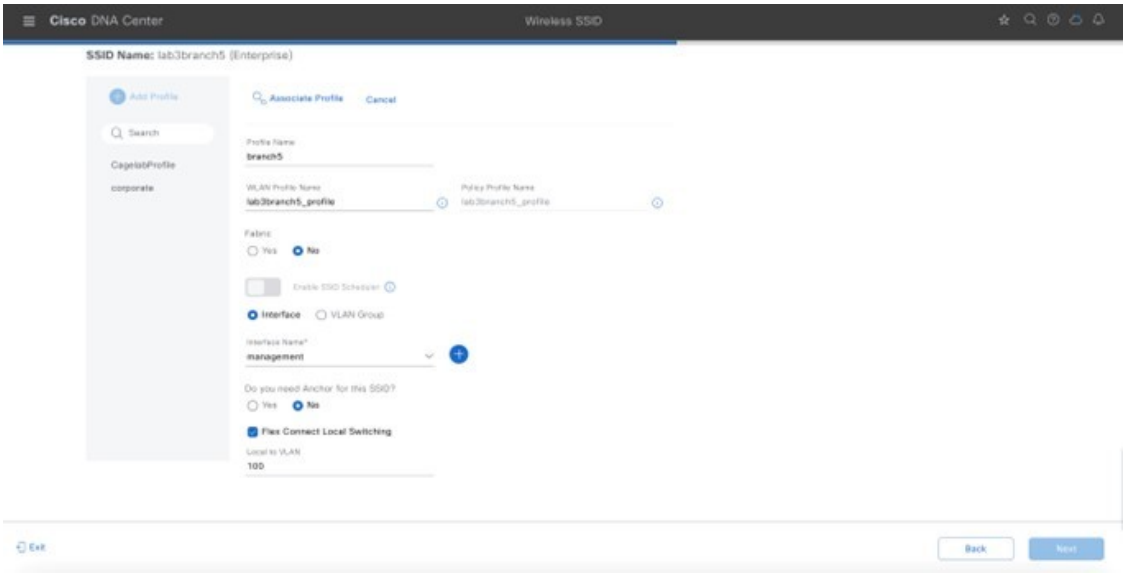
図 *37* : エンタープライズ *SSID* の詳細設定



ステップ 5 [+ Add] をクリックして、新しいワイヤレスプロファイルを追加します。

（注） エンタープライズワイヤレスネットワークを既存のワイヤレスプロファイルに接続したり、新しいワイヤレスプロファイルを作成してエンタープライズワイヤレスネットワークを接続したりできます。

図 *38* : ワイヤレスプロファイルへのエンタープライズ ワイヤレス ネットワークの接続



ステップ 6 [Wireless Profile Name] を入力します。

この導入ガイドでは、**branch5** という名前のワイヤレスプロファイルを作成します。

ステップ 7 （SD-Access アプリケーションが展開されていない場合は、このステップをスキップします）。[Fabric] で [No] を選択します。

[Select Interface] フィールドが表示されます。この導入ガイドでは、Cisco DNA Center を使用した非 SDA ワイヤレス展開についてのみ説明します。

ステップ 8 [Select Interface] ドロップダウンメニューから [branchemployee] を選択します。

ステップ 9 [FlexConnect Local Switching] 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 [Local to VLAN] に「VLAN ID 100」と入力します。

ブランチ従業員のトラフィックを終端するために、エンタープライズ ワイヤレスコントローラの **branchemployee** インターフェイスを選択しましたが、ブランチ従業員のトラフィックはすべてブランチスイッチの VLAN 100 にローカルにスイッチングされます。

ステップ 11 [Next] をクリックします。

[Summary] ページには、SSID の基本設定、セキュリティ、詳細設定、およびネットワークプロファイルが表示されます。

ステップ 12 [Save] をクリックします。

（注） Cisco DNA Center では、複数のネットワークプロファイルを単一の SSID に関連付けられますが、Flex プロファイルと非 Flex プロファイルの両方があるネットワークプロファイルに単一の SSID を関連付けるのは避けてください。それらの各プロファイルでは、AP がそれぞれ異なるモード（Flex とローカル）である必要があります。

ステップ 13 [Configure Network Profiles] をクリックします。

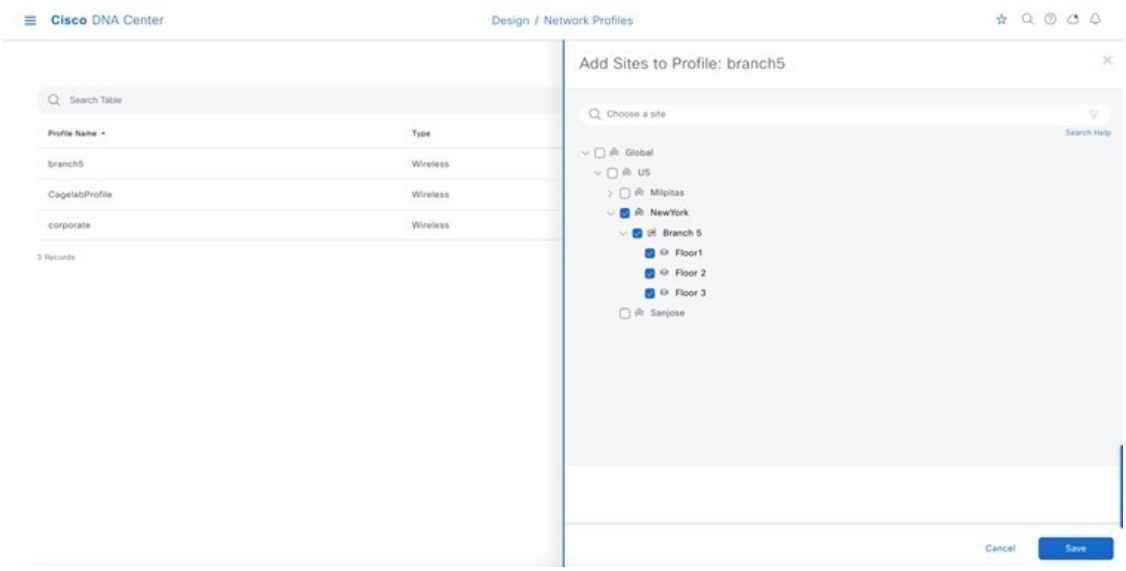
ステップ 14 ブランチ ネットワーク プロファイルで [Assign Sites] をクリックします。

ステップ 15 [New York] エリアを選択します。

すべての子サイトの場所（**Building 23** の **Floor 1**、**Floor 2**、および **Floor 3**、**Building 24** の **Floor 1**、**Floor 2**、および **Floor 3**）が自動的に選択されます。

ステップ 16 [OK] をクリックしてサイト階層のサイドパネルを閉じ、[Create a Wireless Profile] サイドパネルに戻ります。

図 *39 :* ブランチ ネットワーク プロファイルでのサイトの割り当て



ステップ 17 [Attach Template(s)] の下にある [+ Add] をクリックして、CLI ベースのテンプレートをエンタープライズ ワイヤレス ネットワーク設定に追加します。

（注） Cisco DNA Center の [Template Editor] ダッシュボード内にあるすべてのテンプレートを定義しておく必要があります。この設計および導入ガイドでは、特定の シスコ ワイヤレス コントローラ プラットフォームに関する CLI 構文の知識が必要なため、テンプレートの追加については取り上げていません。ただし、Cisco DNA Center の Web ベースの GUI でサポートされていないワイヤレス機能は、テンプレートを使用して追加できます。

新しいエンタープライズ ワイヤレス ネットワーク **lab3branch5** が [Wireless Network Settings] ダッシュボードに表示されます。

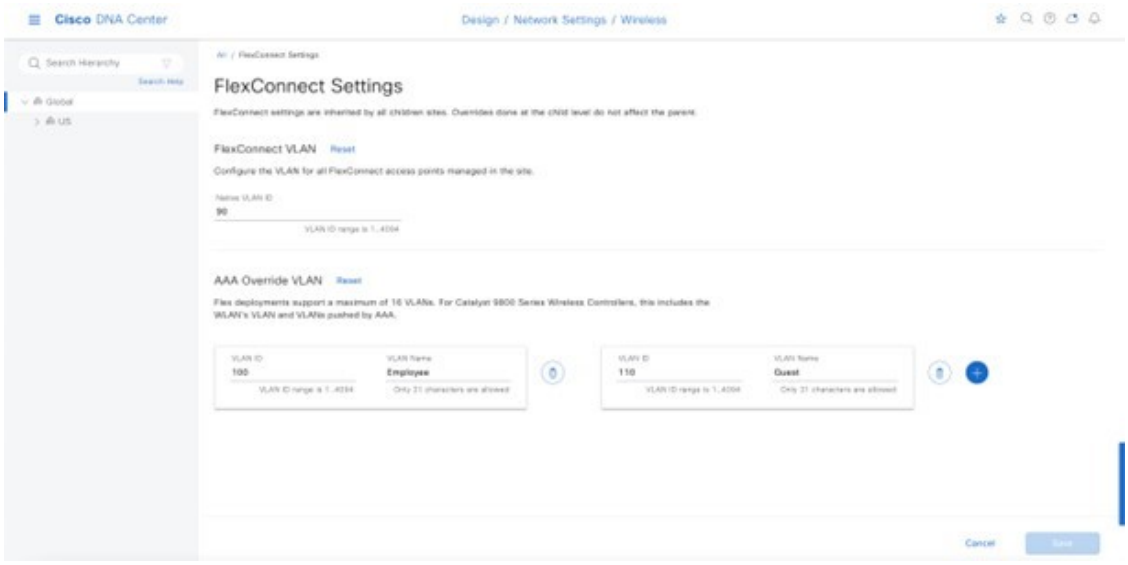
FlexConnect 設定の設定

次の手順では、Cisco DNA Center を使用して FlexConnect を設定する手順について説明します。この手順で、ネイティブ VLAN とクライアント VLAN を設定できます。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** > **[FlexConnect Settings]**の順に選択します。

図 *40 : [FlexConnect Settings]* ページ



ステップ 2 グローバル設定で、[Native VLAN] と [AAA override VLAN] を設定します。

（注） グローバル設定では、エリア、ビルディング、およびフロアレベルでネイティブ VLAN と AAA オーバーライド VLAN をオーバーライドできます。

モデル設定エディタでの FlexConnect の設定

モデル設定は、高レベルのサービスインテントとデバイス固有の CLI テンプレートとともにネットワークデバイスに展開できる、モデルベースの検出可能かつカスタマイズ可能な構成機能のセットです。次の手順では、FlexConnect のモデル設定の実行手順について説明します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[Model Config Editor]** の順に選択します。

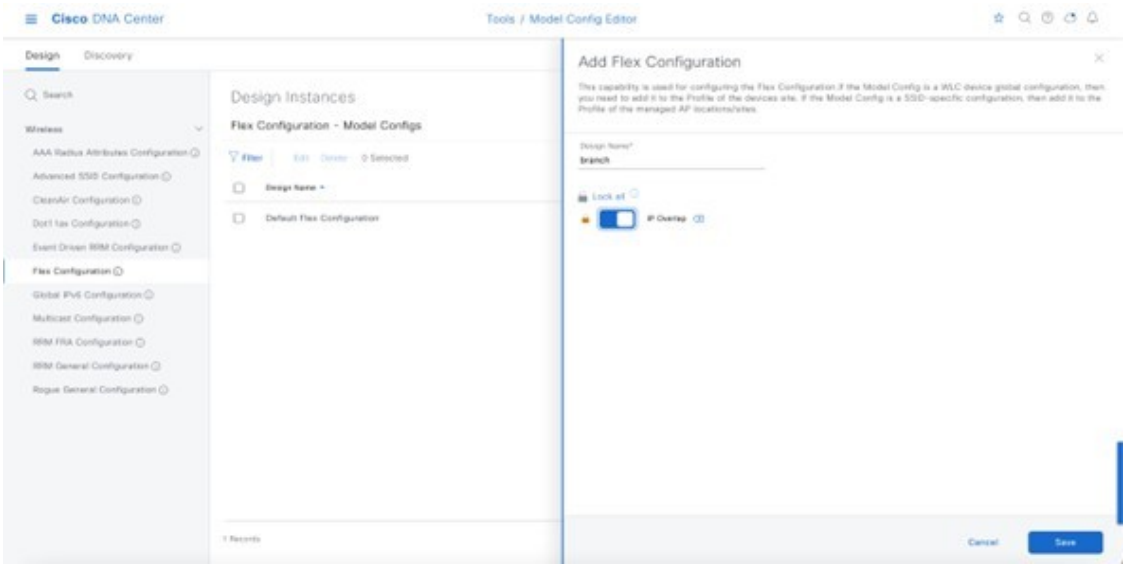
ステップ 2 [Flex Configuration] をクリックします。

ステップ 3 [Add] をクリックし、設計名を入力します。

たとえば、設計名として **branch** と入力します。

ステップ 4 [IP Overlap] を有効にします。

図 *41 : Flex* 設定のモデル設定



ネットワークプロファイルへの FlexConnect モデル設定のマッピング

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

ステップ 2 [Edit branch5] ネットワークプロファイルをクリックします。

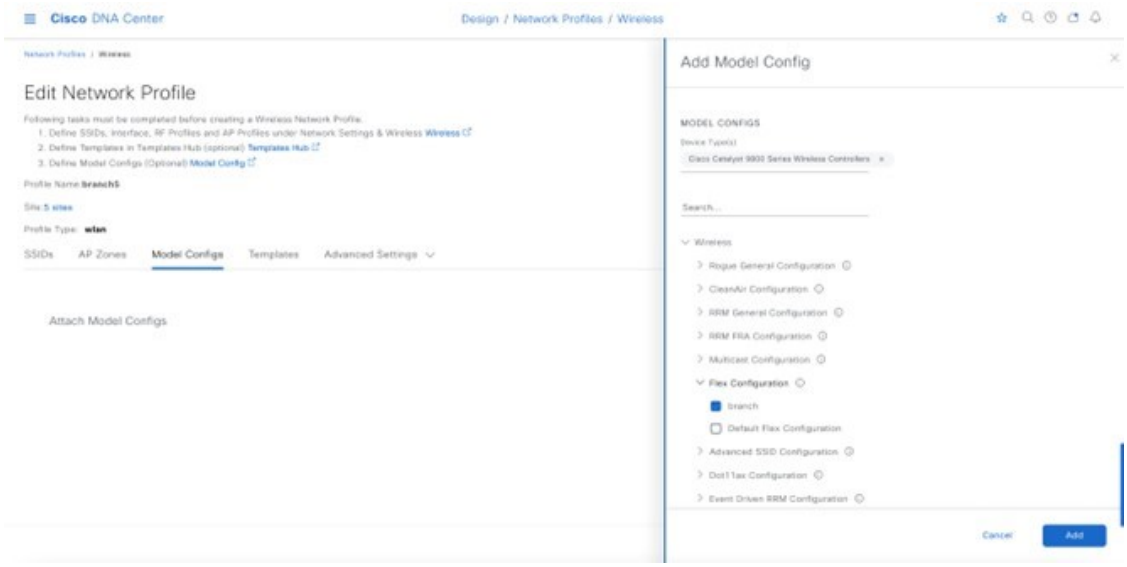
ステップ 3 [Model Config] タブをクリックし、[Add Model Config] をクリックします。

ステップ 4 [Device Type] として [Wireless Controller] を選択します。

ステップ 5 [Wireless] > [Flex Configuration] の順にクリックし、設定されたモデル設定を選択します。

ステップ 6 [Add] をクリックして変更を保存します。

図 *42 : Flex* ネットワークプロファイルへのモデル設定の追加



ゲストワイヤレス SSID の設定

ゲスト ワイヤレス ネットワークは、サイト階層のグローバルレベルで定義する必要があります。定義すると、ゲスト ワイヤレス ネットワークがワイヤレスプロファイルに適用されます。ワイヤレスプロファイルは、階層内の 1 つ以上のサイトに割り当てられます。この導入ガイドでは、**lab3guest5** という名前の単一のゲスト ワイヤレス ネットワーク（SSID）がプロビジョニングされます。

手順

ステップ 1

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 3 [SSIDs] をクリックします。

ステップ 4 [+ Add] にカーソルを合わせて、[Guest] を選択します。

[Basic Settings] ウィンドウが表示されます。

図 *43 :* ゲストワイヤレス *SSID* を作成するための *[Basic Settings]* ウィンドウ

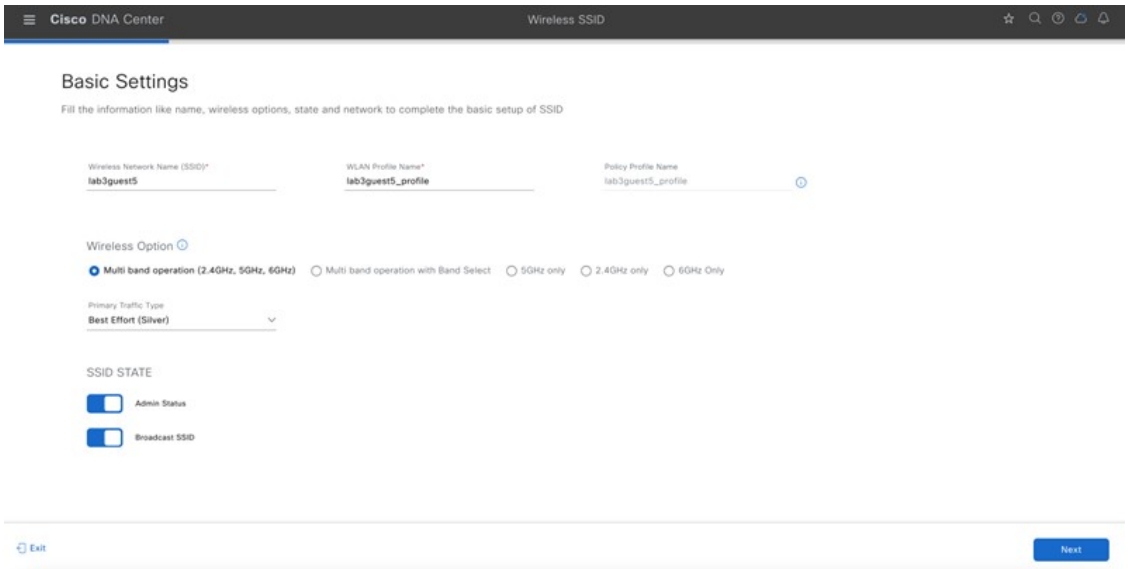


図 *44 :* ゲスト *SSID* のセキュリティ設定

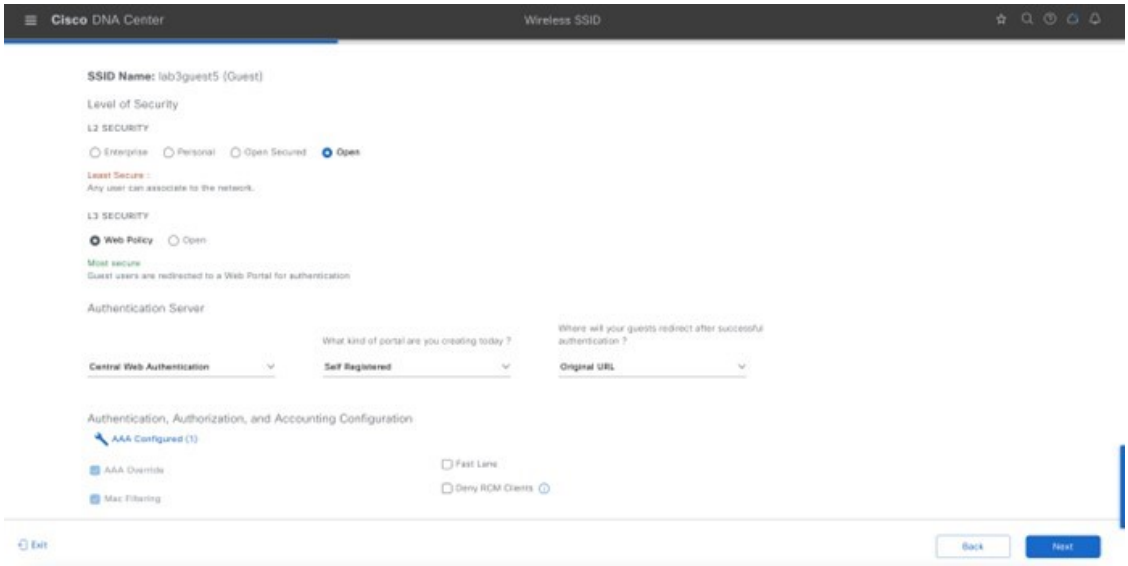


図 *45 : Flex* ゲスト *SSID* の *AAA* 設定

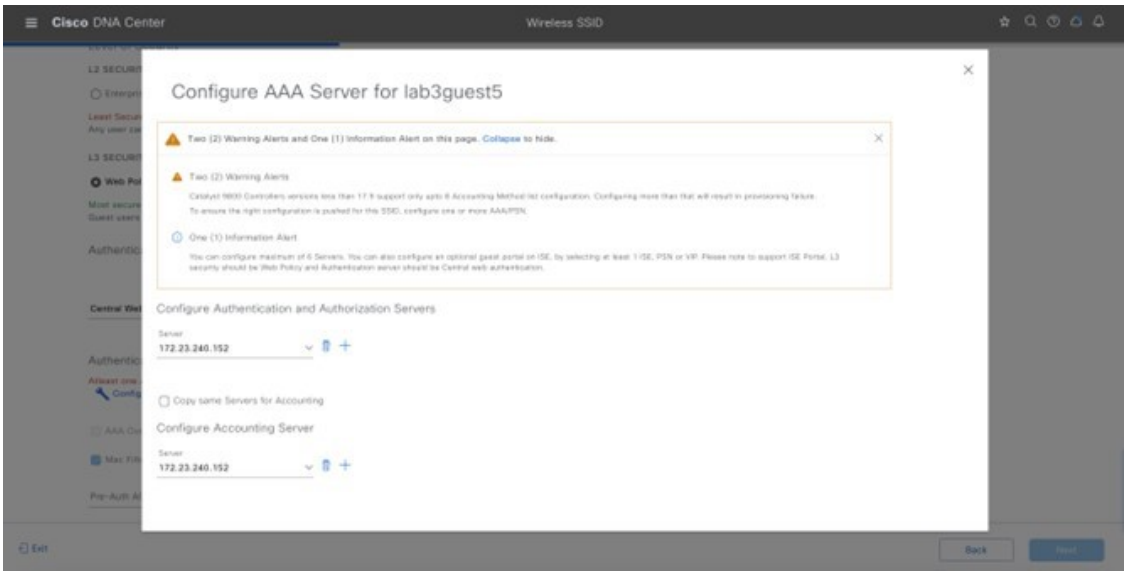
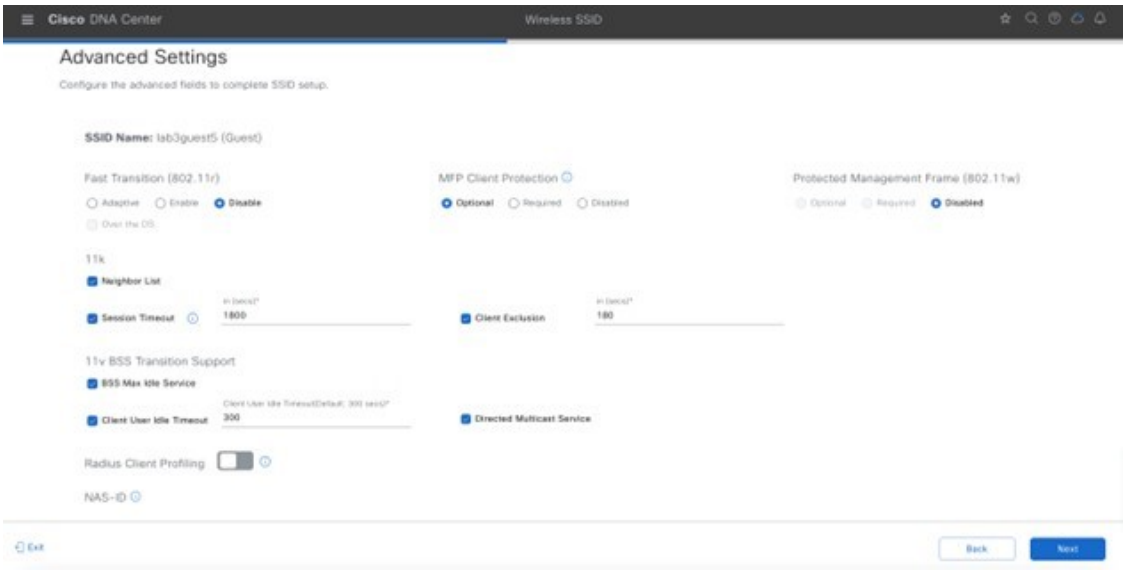


図 *46 : Flex* ゲスト *SSID* の詳細設定



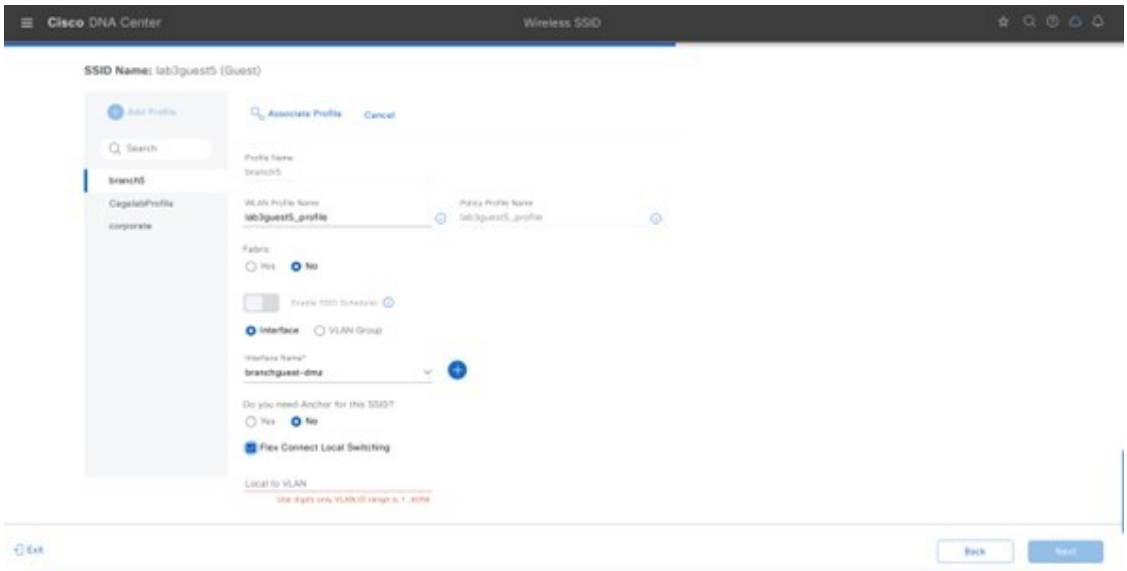
Cisco DNA Center を介してゲスト ワイヤレス ネットワークに設定できる機能の詳細については、Cisco DNA Center を使用して設定可能なゲスト ワイヤレス ネットワーク機能 （65 ページ）を参照してください。

ステップ 5 関連するフィールドに情報を入力し、[Next] をクリックします。

（注） この導入ガイド用に設定されたエンタープライズ ワイヤレス ネットワークの設定については、導入ガイドで設定されているゲスト ワイヤレス ネットワーク設定 （78 ページ）を参照してください。

ステップ 6　ゲスト ワイヤレス ネットワークを既存の **branch5** ワイヤレスプロファイルに接続します。

図 *47 : Flex* ゲスト *SSID* へのワイヤレスプロファイルの接続



ステップ 7　[Select Interface] ドロップダウンメニューから [branchguest-dmz] を選択します。

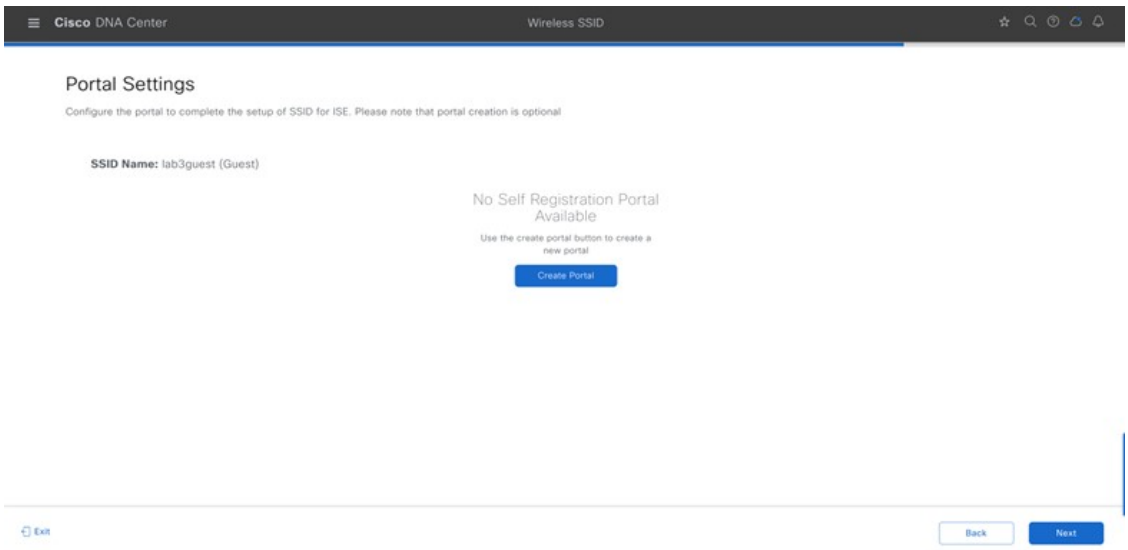
branchguest-dmz VLAN（VLAN 110）のゲストトラフィックは終端します。

ステップ 8　[FlexConnect Local switching] をクリックし、**Local VLAN 110** と入力します。

ステップ 9　[Next] をクリックします。

[Portal Customization] ページが表示されます。

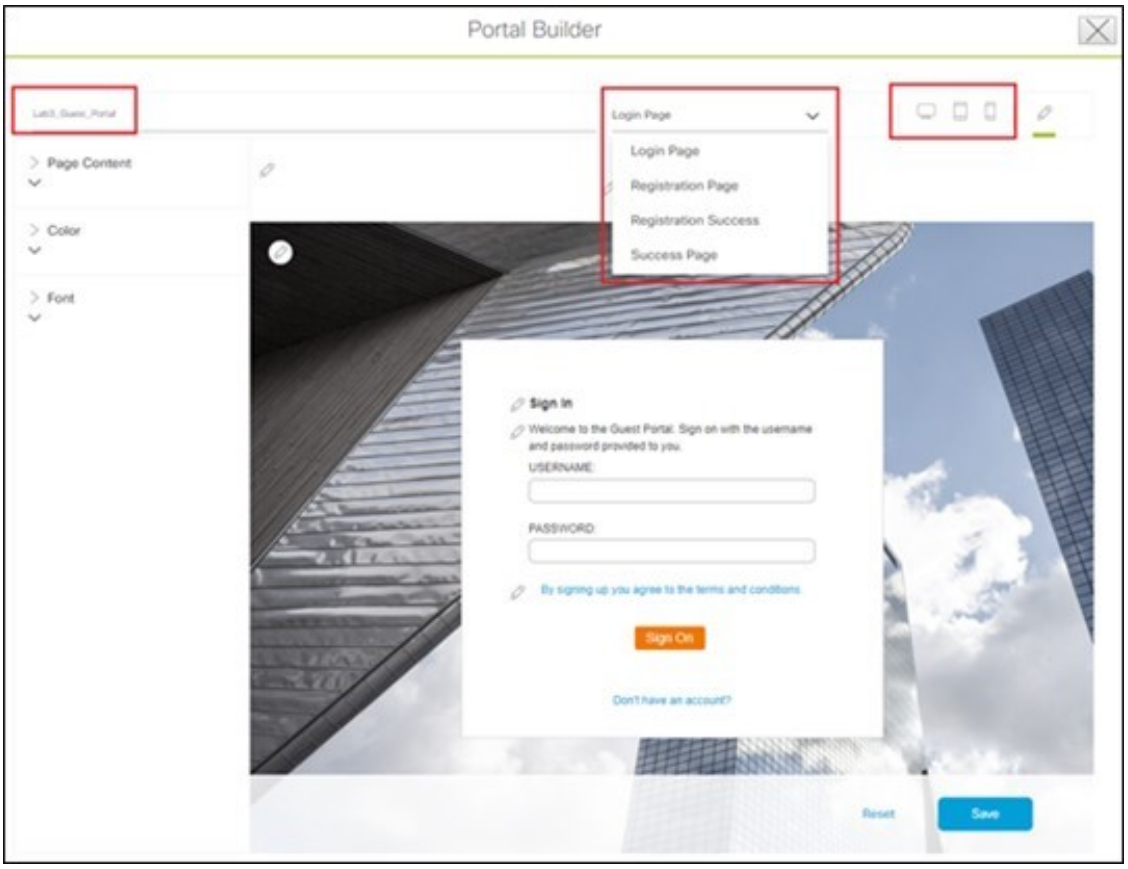
図 *48 : Flex* ゲストワイヤレス *SSID* のゲストポータルのカスタマイズ



ステップ 10　[Create Portal] をクリックして、Cisco ISE に新しいゲストポータルを追加します。

[Portal Builder] ページが表示されます。ポータルを作成せずに終了することもできます。

図 *49 : [Flex Guest SSID Portal Builder]* 画面



ステップ 11 関連情報を入力します。

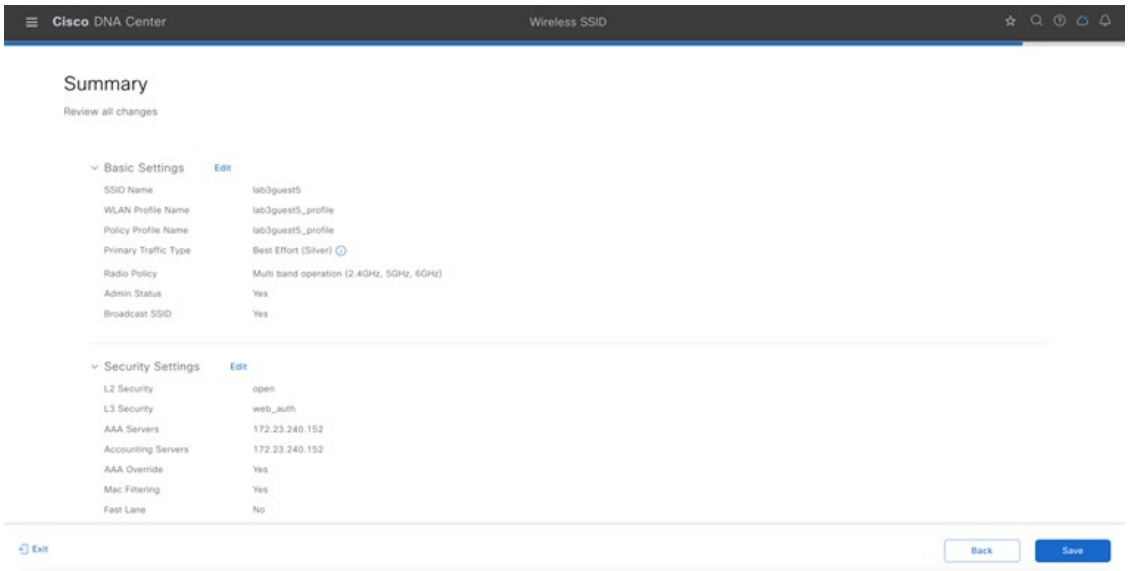
少なくともゲストポータルに名前を付ける必要があります。この導入ガイドでは、ポータルの名前は **Lab3_Guest_Portal** です。[Portal Builder] のドロップダウンメニューを使用すると、ポータルの [Login]、[Registration]、[Registration Success]、および [Success] ページをカスタマイズできます。また、Web ポータルの配色、フォント、ページコンテンツ、ロゴ、および背景をカスタマイズできます。ポータルをプレビューして、スマートフォン、タブレット、およびコンピュータでの表示方法も確認できます。

ステップ 12 [Save] をクリックして、Cisco ISE サーバーに新しいゲストポータルを作成し、ゲスト ワイヤレス ネットワーク ワークフローに戻ります。

ステップ 13 [Next] をクリックします。

[Summary] ページには、SSID の基本設定、セキュリティ、詳細設定、およびネットワークプロファイルが表示されます。

図 *50 : [Flex Guest SSID Summary]* ページ



ステップ 14 [Save] をクリックします。

ステップ 15 [Configure Network Profiles] をクリックします。

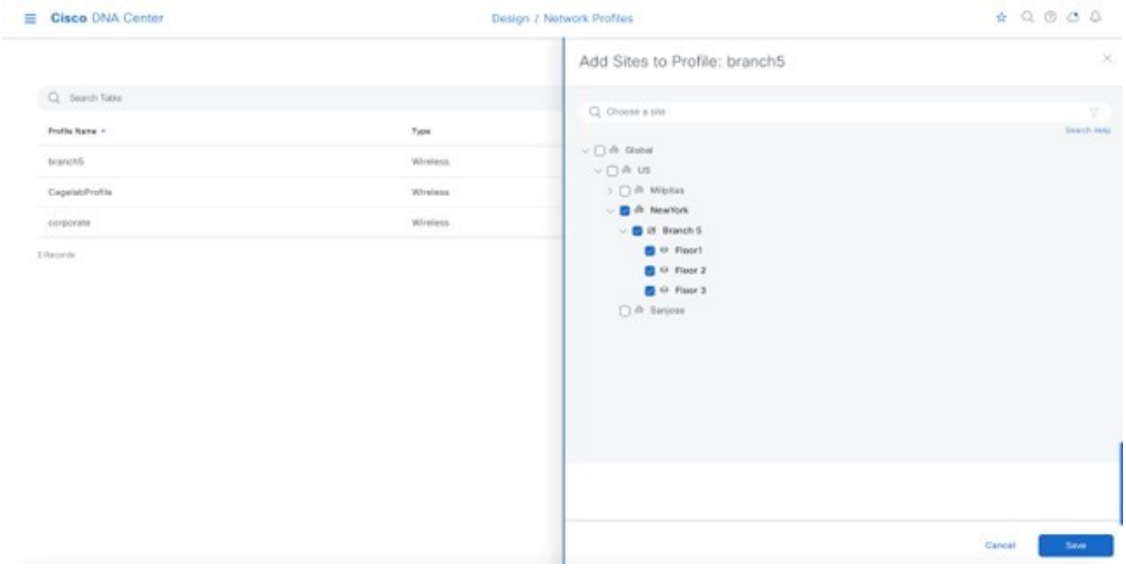
ステップ 16 [Branch Network Profiles] で [Assign Sites] をクリックします。

ステップ 17 [New York] エリアを選択します。子サイトの場所（**Branch 5** の **Floor 1**、**Floor 2**、および **Floor 3**）が自動的に選択されます。

自動的に、子サイトの場所（**Branch 5** の **Floor 1**、**Floor 2**、および **Floor 3**）が選択されます。

ステップ 18 [OK] をクリックしてサイト階層のサイドパネルを閉じ、[Create a Wireless Profile] サイドパネルに戻ります。

図 *51 : Flex* ゲストプロファイルへのサイトの割り当て



ステップ 19 [Attach Template(s)] の下にある [+ Add] をクリックして、CLI ベースのテンプレートをエンタープライズ ワイヤレス ネットワーク設定に追加します。

（注） Cisco DNA Center の [Template Editor] ウィンドウ内にあるすべてのテンプレートを定義しておく必要があります。この設計および導入ガイドでは、特定のシスコ ワイヤレス コントローラ プラットフォームに関する CLI 構文の知識が必要なため、テンプレートの追加については取り上げていません。ただし、Cisco DNA Center の Web ベースの GUI でサポートされていないワイヤレス機能は、テンプレートを使用して追加できます。

新しいエンタープライズ ワイヤレス ネットワーク **lab3branch5** が [Wireless Network Settings] ウィンドウに表示されます。

（注） 異なる AAA 設定で作成された WLAN プロファイルは、異なるサイトレベルで割り当てることができます。サイトレベルでオーバーライドすると、新しい WLAN プロファイルがワイヤレスコントローラにプッシュされます。エリア、ビルディング、およびフロアレベルに基づく設定でグローバル SSID をオーバーライドできます。

SSID に対してサイトレベルのオーバーライドを行う場合は、WLAN プロファイル名を更新することを推奨します。選択したサイトを管理するワイヤレスコントローラに同じ WLAN プロファイル名がすでに設定されている場合、プロビジョニングが失敗します。

[L2 Security]、[AAA Configuration]、[NAS-ID]、[Mac Filtering]、[AP Impersonation]、[Radius Client Profiling]、[CCKM, MPSK]、[Protected Management Frame (802.11w)]、[AAA Override]、および [WLAN Profile Name] のみサイトレベルでオーバーライドできます。他のパラメータを編集するには、グローバルレベルに移動します。

ゲスト SSID 用の FlexConnect 設定の設定

次の手順では、ゲスト SSID の FlexConnect 設定を設定する方法について説明します。

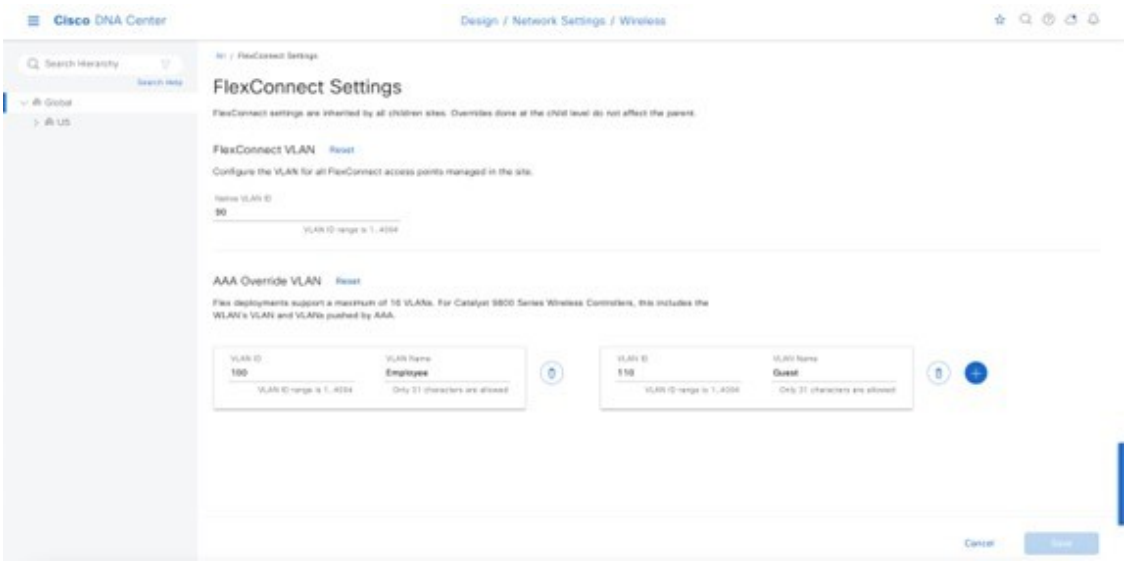
手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network settings]** > **[Wireless Flex connect settings]**の順に選択します。

ステップ 2 グローバル設定でネイティブ VLAN と AAA オーバーライド VLAN を設定します。

（注） エリア、ビルディング、およびフロアレベルのグローバル設定で、ネイティブ VLAN および AAA オーバーライド VLAN をオーバーライドできます。

図 *52 : Flex* ゲスト *SSID* イメージの *FlexConnect* 設定



Flex ゲスト SSID のモデル設定エディタの設定

ここでは、Flex ゲスト SSID のモデル設定を設定する手順について説明します。

手順

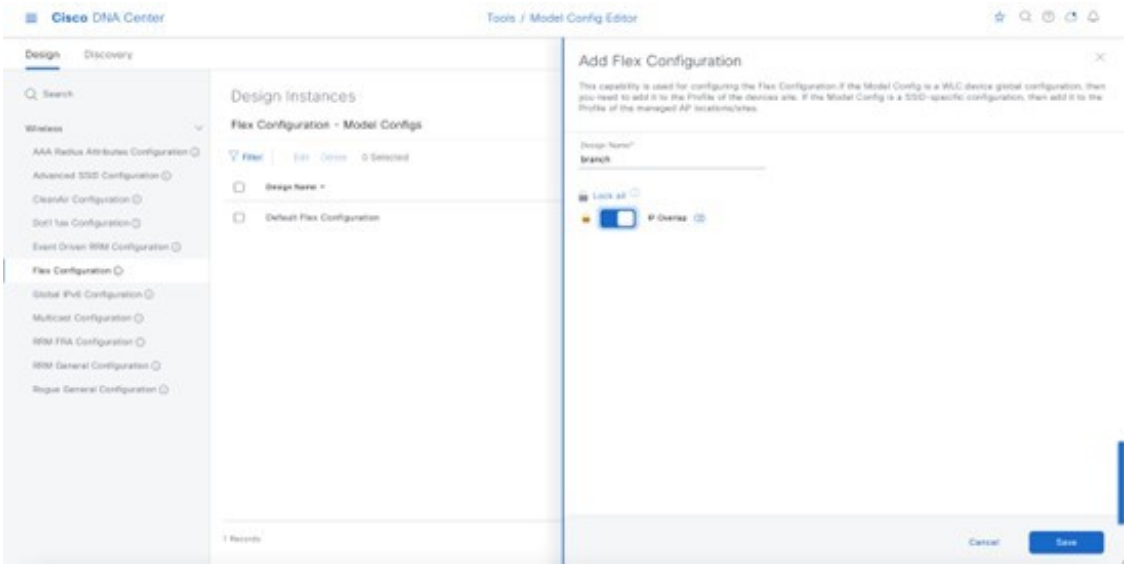
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 [Flex Configuration] をクリックします。

ステップ 3 [Add] をクリックし、ブランチとしての設計名を指定します。

ステップ 4 [IP Overlap] を有効にします。

図 *53 : Flex* ゲスト *SSID* のモデル設定



ネットワークプロファイルへの Flex ゲスト SSID モデル設定のマッピング

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、 [Design] > [Network Profile] の順に選択します。

ステップ 2 [Edit branch5] ネットワークプロファイルを選択します。

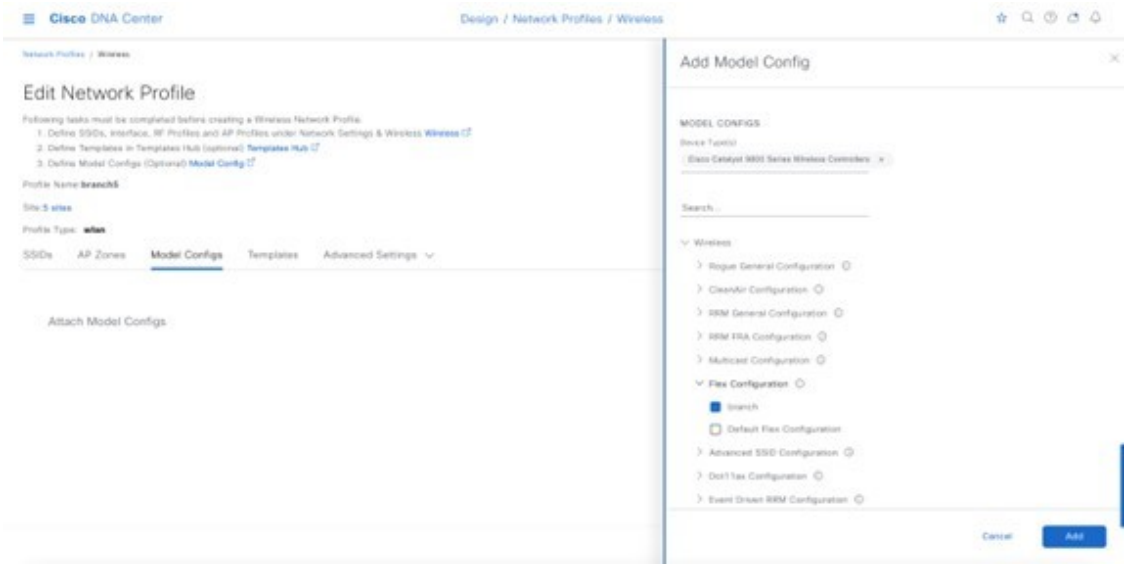
ステップ 3 [Model Config] をクリックして、モデル設定を追加します。

ステップ 4 [Device Type] でワイヤレスコントローラを選択します。

ステップ 5 **[Wireless]** > **[Flex Configuration]**の順にクリックして、設定されたモデル設定を選択します。

ステップ 6 [Add] をクリックして変更を保存します。

図 *54* : ゲスト ネットワーク プロファイルへの *FlexConnect* モデル設定のマッピング



ワイヤレス RF プロファイルのカスタマイズ

[Wireless Settings] ダッシュボードの [Wireless Radio Frequency Profile] セクションでは、次の操作を実行できます。

- Cisco DNA Center 内にある 3 つの事前設定済み RF プロファイルの各設定を視覚的に検査する。3 つの RF プロファイルは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ内でも事前設定されています。
- ワイヤレス展開における RF のさまざまな側面を微調整できるカスタム RF プロファイルを作成する。
- Cisco DNA Center 内の AP に割り当てられるデフォルトの RF プロファイルとして、事前設定済みまたはカスタム RF プロファイルを選択する。

Cisco DNA Center で AP をプロビジョニングすると、[Wireless Settings] ダッシュボード内で設定されたデフォルトの RF プロファイルが適用されますが、この設定は AP ごとにオーバーライドできます。

次の事前設定済み RF プロファイルを使用できます。

- [LOW]：このプロファイルは、低密度クライアントの導入用に両方の帯域（2.4 GHz と 5 GHz）の RF 属性を調整します。
- [TYPICAL]：このプロファイルは、中密度クライアントの導入用に両方の帯域（2.4 GHz と 5 GHz）の RF 属性を調整します。
- [HIGH]：このプロファイルは、スタジアム、講堂などの高密度クライアントの導入用に両方の帯域（2.4 GHz と 5 GHz）の RF 属性を調整します。

（注） Cisco DNA Center 内にある 3 つの事前設定済み RF プロファイルごとの特定の設定については、付録 D を参照してください。

AP 密度と設置高さに基づいて、RF グループに必要な TPC しきい値を設定します。大規模な展開では RF 環境が大幅に変化する可能性があるため、TPC を適切に調整して、各場所で最適なカバレッジを確保することが重要です。

データレートは、送信電力とともに、クライアントのローミング動作に影響を与える主要なメカニズムです。データレートを最低の必須レートに変更すると、クライアントが新しいローミングをトリガーするタイミングが変更されることがあります。この点は、スティッキークライアントの問題が発生する大規模なオープンスペースでは特に重要です。

RF プロファイルを設定する場合は、DCA の計算に悪影響を与える可能性があるため、隣接する AP グループと RF プロファイルを異なる DCA チャネルセットで設定しないでください。

ユーザーは、チャネルが設定された規制ドメインでサポートされていない場合でも、サポートされていないチャネルを RF プロファイル DCA リストに追加できます。設定されたチャネルが使用国のドメインで許可されているか、常に確認することを推奨します。DCA ではサポートされていないチャネルは AP に割り当てられないため、ネットワーク運用には影響を及ぼしませんが、リリース 17.5 以降、C9800 の検証では、追加されたチャネルが許可されているか確認されます。

手順

ステップ 1 [Wireless Network Settings] ダッシュボードで、[Wireless Radio Frequency Profile] セクションを見つけます。

[Wireless Settings] ダッシュボードの [Wireless Radio Frequency Profile] セクションには、サイト階層のグローバルレベルでのみアクセスできます。

ステップ 2 デフォルトでは、TYPICAL RF プロファイルがデフォルトの RF プロファイルとして設定されます。次の図に示されているように、[TYPICAL (Default)] と表示されるため確認できます。RF プロファイルを変更するには、使用可能ないずれかのプロファイルの名前の横にあるチェックボックスをオンにし、[✓] デフォルトボタンをクリックします。

図 *55* : ワイヤレス無線周波数プロファイル

この設計および導入ガイドでは、TYPICAL RF プロファイルが選択されています。これは、中密度のクライアント環境向けの導入であることを示しています。

これで、リモートオフィス用の FlexConnect の設計が完了しました。

AWS でホストされる Cisco Catalyst 9800-CL ワイヤレスコントローラの設計

ここでは、AWS 展開でホストされる ワイヤレスコントローラについて説明します。この展開では、AWS でホストされるクラウドベースの Cisco Catalyst 9800-CL ワイヤレスコントローラを使用します。詳細については、『Amazon Web Services（AWS）でのクラウド（C9800 CL）版 Cisco Catalyst 9800 ワイヤレスコントローラのための導入ガイド』を参照してください。

Cisco Catalyst 9800 の Amazon マシン イメージ（AMI）の起動は、AWS Marketplace から直接実行します。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、Amazon Virtual Private Cloud（VPC）の Amazon EC2 に展開されます。

シスコは、クラウド上の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最初のリリースに対して次のインスタンスタイプをサポートしています。

C5.xlarge：4 つの vCPU、8 GB の RAM、1 つの vNIC を備えた 8GB のディスク

割り当てられたリソースを使用して、インスタンスを 1,000 の AP と 10,000 のクライアントにスケーリングできます。

AWS に Cisco Catalyst 9800-CL ワイヤレスコントローラ を展開するための前提条件

- 企業のネットワークから VPC へのマネージド VPN 接続を作成します。
- Catalyst 9800 シリーズ ワイヤレス コントローラのワイヤレス管理インターフェイス向けに目的のサブネットで VPC を作成します。
- Catalyst 9800 シリーズ ワイヤレス コントローラ CloudFormation テンプレート：テンプレートは起動手順に自動的に統合されるため、CloudFormation テンプレートを設定する必要はありません。必要に応じて、製品の [AWS Marketplace] ページから CloudFormation テンプレートファイルをダウンロードして表示できます。
- 目的の 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用の Amazon マシンインスタンス ID（AMI-ID）。AMI は AWS Marketplace で入手できます。
- セキュリティ上の理由でインスタンスへの AP アクセスを制限できます。たとえば、単一の特定の IP 範囲にある CAPWAP を許可して、それらの AP のみコントローラに登録できるようにします。次の表に、AP が AWS のワイヤレスコントローラと通信できるようにファイアウォールで開く必要があるポートを示します。

表 *17*: ファイアウォールで開く必要があるポート

ポート	**Protocol**
UDP 5246/5247/5248	CAPWAP
TCP 22	SSH、SCP
TCP 21	FTP

ポート	**Protocol**
ICMP	ping
UDP 161、162	SNMP/SNMP トラップ
TCP 443/80	HTTPS/HTTP
TCP/UDP 49	TACACS+
UDP 53	DNS Server
UDP 1812/1645/1813/1646	RADIUS
UDP 123	NTP Server
UDP 514	Syslog

AWS への Cisco Catalyst 9800-CL ワイヤレスコントローラのインストール

手順

ステップ 1 AWS Marketplace にアクセスします。

ステップ 2 AWS Marketplace で「C9800-CL」を検索して、Cisco Catalyst 9800-CL ワイヤレスコントローラ製品ページを見つけます。

ステップ 3 [Cisco Catalyst 9800-CL Wireless Controller for Cloud] を選択し、[Continue to Subscribe] をクリックします。

ステップ 4 フルフィルメントオプション（[Cloud Formation Template]（推奨）または [Amazon Machine Image (AMI)]）を選択します。

AMI を選択した場合は、AWS コンソールまたは AWS Marketplace インターフェイスを使用できます。

両方のフルフィルメントオプションについて、新しい Catalyst 9800-CL ワイヤレスコントローラ インスタンスを起動する手順が示されます。

ステップ 5 インストールプロセス中に、以下の内容の選択を求められます。

- 目的の AWS リージョン。
- Catalyst 9800-CL ワイヤレスコントローラの VPC（カスタムまたはデフォルト）とインストール場所。
- Catalyst 9800-CL ワイヤレスコントローラ管理およびワイヤレス管理インターフェイスに必要な IP サブネット。
- VPC に関連付けられたセキュリティグループ。
- SSH 接続用のキーペア。

ステップ 6 [Review and Launch] をクリックし、情報が正しいことを確認します。

ステップ 7 [Launch Instance] をクリックします。

ステップ 8 [AWS Console] > [EC2] サービスに移動し、インスタンスの状態が**実行中**になるのを待ちます。Catalyst 9800-CL ワイヤレスコントローラ インスタンスに接続できるまで数分待つ必要があります。

ステップ 9 Catalyst 9800-CL ワイヤレスコントローラ インスタンスに割り当てられた IP アドレスに接続し、WebUI ウィザードを使用して Day 0 の設定とセットアップを行います。

ステップ 10 または、SSH クライアントを使用してインスタンスに接続し、必要なログイン情報またはセットアップ時に選択した秘密 SSH キーを指定します。

例：`ssh -i mykeypair.pem ec2-user@<IP of the instance>`

ステップ 11 SSH 接続すると、Catalyst 9800-CL ワイヤレスコントローラに IOS XE コマンドプロンプトが表示されます。これで、インスタンスの設定を開始できます。

エンタープライズ ワイヤレス ネットワーク（SSID）の設定

ワイヤレス設定は階層型です。サイト階層の下位レベルの設定で、上位レベルで定義された設定をオーバーライドできます。デフォルトでは、サイト階層の最上位レベルであるグローバルレベルに移動します。

エンタープライズ ワイヤレス ネットワークは、展開全体でブロードキャストに使用できる非ゲスト WLAN/SSID で、サイト階層のグローバルレベルで定義する必要があります。定義すると、エンタープライズ ワイヤレス ネットワークがワイヤレスプロファイルに適用され、ワイヤレスプロファイルが階層内の 1 つ以上のサイトに割り当てられます。この設計および導入ガイドでは、**corpevent** という名前の単一のエンタープライズ WLAN/SSID がプロビジョニングされます。次の手順では、Cisco DNA Center 内でエンタープライズ ワイヤレス ネットワークを設定する方法について説明します。

始める前に

このアクションを完了するには、ユーザープロファイルに SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE を割り当てる必要があります。

手順

ステップ 1 IP アドレスまたは完全修飾ドメイン名を使用して、Cisco DNA Center Web コンソールにログインします。

例：

http://<Cisco_DNA_Center_IPaddr_or_FQDN>

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 3 [Wireless Network Settings] ダッシュボードで、[+ Add] にカーソルを合わせ、[Enterprise] を選択します。

[Create an Enterprise Wireless Network] ダイアログボックスが表示されます。

図 *56* : ワイヤレスネットワーク設定

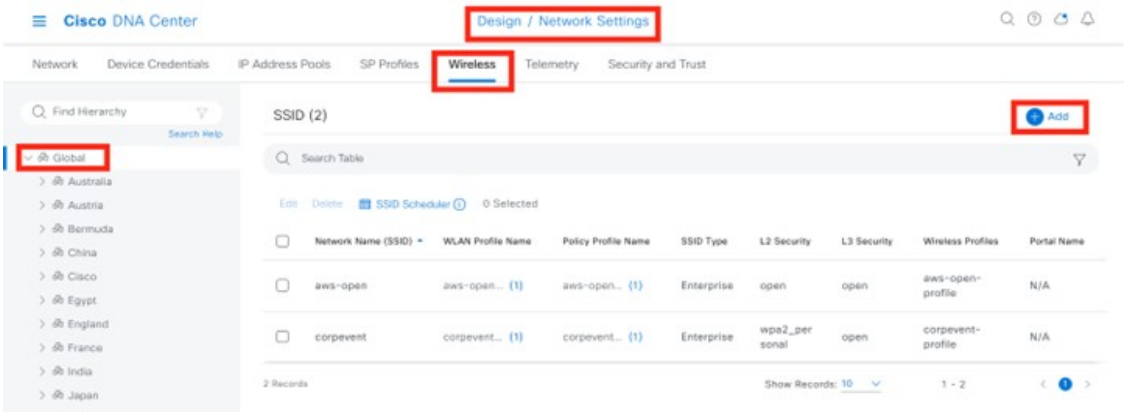
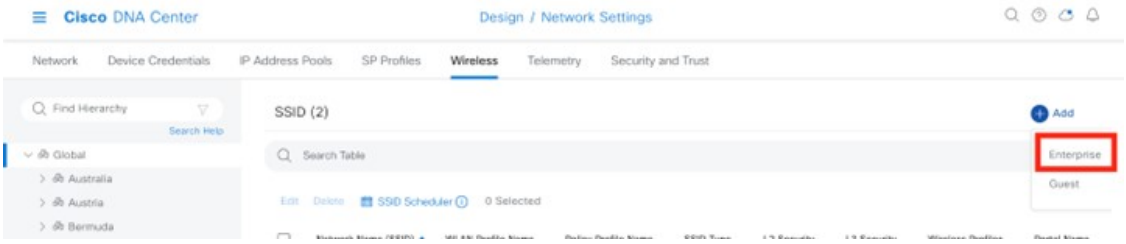


図 *57* : ワイヤレスネットワーク設定用のエンタープライズの選択



ステップ 4 必要な情報を入力し、[Next] をクリックします。

次の表に、この展開で使用される設定を示します。

表 *18* : エンタープライズ *SSID* の設定

機能	設定
ワイヤレス ネットワーク名（SSID）	Corpevent
ブロードキャスト SSID	点灯
[Wireless Option]	マルチバンド動作（2.4GHz、5GHz、6GHz）
[Primary Traffic Type]	[VoIP (Platinum)]
[Level of Security]	パーソナル、WPA2
[Advanced Security Options]：[Mac Filtering]	オフ
パスフレーズタイプ	<パスフレーズを入力>
[Fastlane]	オフ
[Identify PSK]	オフ
[Deny RCM clients]	オフ

機能	設定
[Advanced Settings]：[FAST TRANSITION (802.11r)]	[Adaptive]、[Over the DS] をオフ
[Advanced Settings]：[MFP Client Protection]	オプション
[Advanced Settings]：[Protected Management Frame (802.11w)]	ディセーブル
[Advanced Settings]：[Session Timeout]	オン、1,800 秒
[Advanced Settings]：[Client Exclusion]	オン、300 秒
[Advanced Settings]：[MFP Client Protection]	オプション
[Advanced Settings]：[11k Neighbor List]	オン
[Advanced Settings]：[11v BSS Transition Support]	[BSS Max Idle Service]：オン
	[Client Idle User Timeout]：オン、300 秒
	[Directed Multicast Service]：オン

ステップ 5 ワークフローの次のページが表示されます。エンタープライズ ワイヤレス ネットワークを既存のワイヤレスプロファイルに接続したり、新しいワイヤレスプロファイルを作成してエンタープライズ ワイヤレス ネットワークを接続したりできます。

ステップ 6 [Add] をクリックして、新しいワイヤレスプロファイルを追加します。

図 *58 :* ネットワークプロファイルへの *SSID* の関連付け

ステップ 7 [Wireless Profile Name]フィールドに、新しいワイヤレスプロファイルの名前を入力します。この導入ガイドでは、**corpevent-profile** という名前のワイヤレスプロファイルが作成されます。

ステップ 8 [Fabric] で [No] オプションボタンをクリックします。

この導入ガイドでは、Cisco DNA Center を使用した非 SDA ワイヤレス展開についてのみ説明します。[No] を選択すると、[Select Interface] フィールドが自動的に表示されます。

ステップ 9 [Select Interface] ドロップダウンリストから [Management] を選択します。

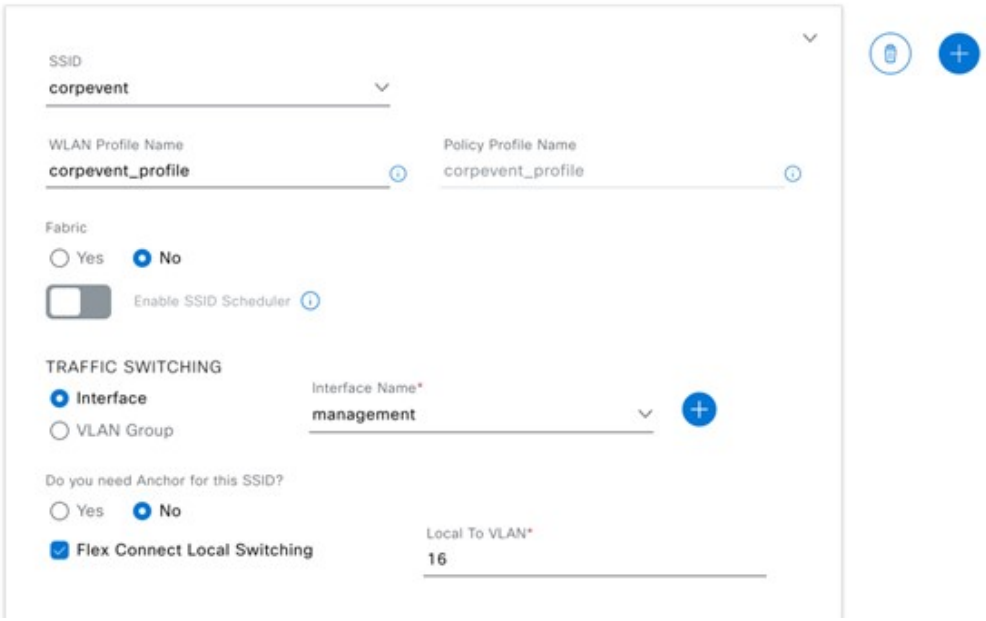
（注） パブリックに展開されたワイヤレスコントローラには必要なく、AWS ワイヤレスコントローラが使用されることはないため、AWS ワイヤレスコントローラではレイヤ 2 VLAN はサポートされていません。AWS または Azure ワイヤレスコントローラで手動設定を実行する場合は、この手順をスキップできますが、Cisco DNA Center プロビジョニングでは、AWS または Azure ワイヤレスコントローラで VLAN が使用されていない場合でも、FlexConnnect フローでは VLAN をプッシュする必要があります。これらのワイヤレスコントローラでは、Flex ローカルスイッチングのみサポートされています。Cisco DNA Center で VLAN がプロビジョニングされないようにするには、インターフェイスの [Management] を選択します。

ステップ 10 [FlexConnect Local Switching] チェックボックスをオンにします。

ステップ 11 [Local to VLAN] フィールドに VLAN ID 16 と入力します。

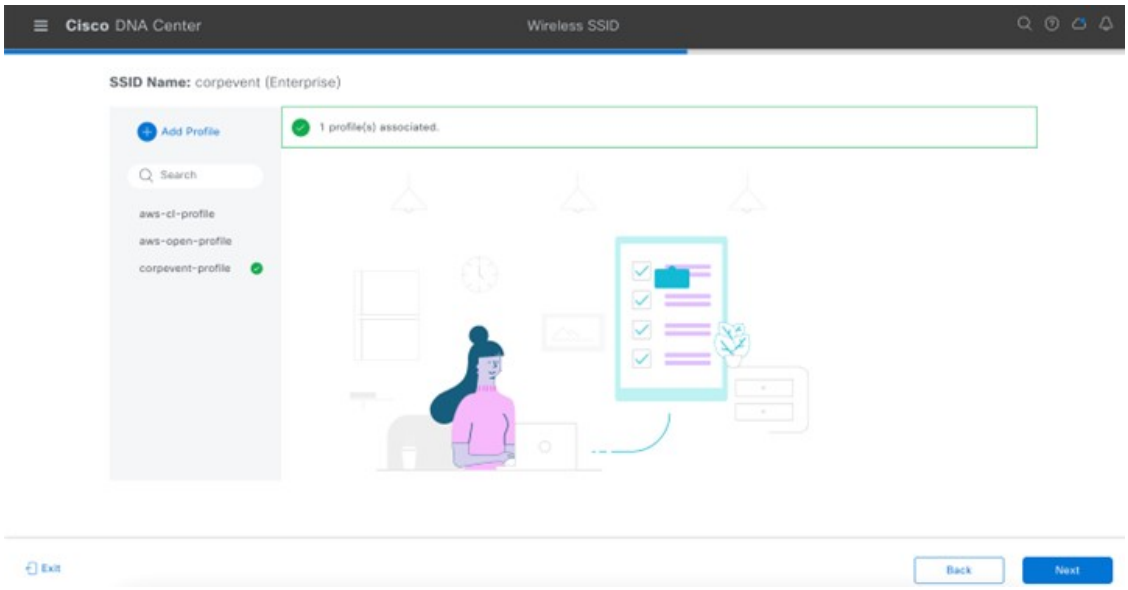
すべてのブランチ従業員トラフィックは、ブランチスイッチの VLAN 16 にローカルにスイッチングされます。

図 *59* : エンタープライズ *SSID* の *VLAN* の割り当て



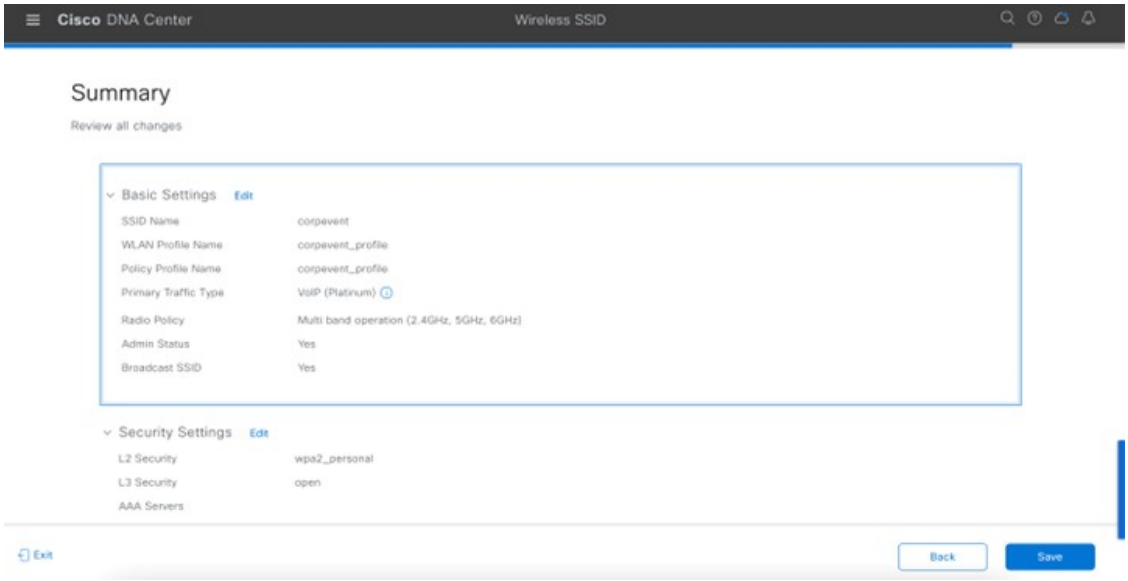
ステップ 12 [Associate Profile] をクリックして、プロファイルをワイヤレス SSID に接続します。

図 *60* : ネットワークプロファイルへの *SSID* の正常な関連付け



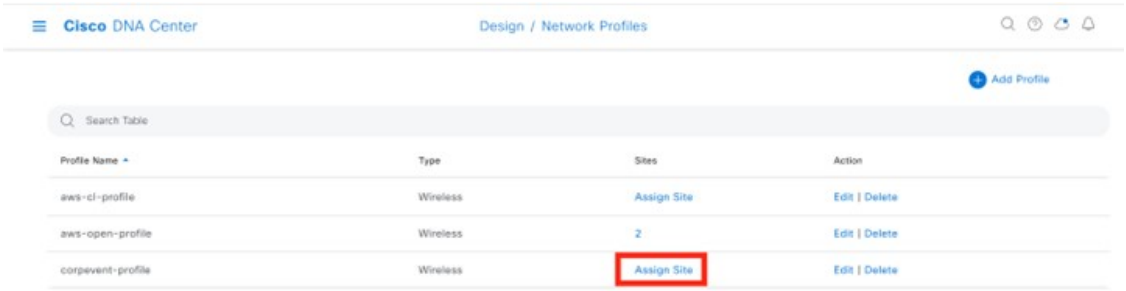
ステップ 13 [Next] をクリックして概要を確認し、[Save] をクリックします。

図 *61* : エンタープライズ *SSID* 設定を確認するための *[Summary]* ページ



ステップ 14 [Configure Network Profile] をクリックして [Network Profiles] ページに移動し、ワイヤレスプロファイルのサイトを割り当てます。

図 *62 :* ネットワークプロファイルのサイトの割り当て



ステップ 15 [Assign Site] をクリックします。

ステップ 16 左側の階層ツリーで、[Global] > [Milpitas] エリアを選択します。

子サイトの場所（**Branch 5**、**Floor 1**、**Floor 2**）が自動的に選択されます。

ステップ 17 [OK] をクリックしてサイト階層のサイドパネルを閉じ、[Create a Wireless Profile] に戻ります。

AWS のワイヤレスコントローラの設計が完了したら、「ワイヤレスネットワークの展開」の項に移動できます。

ワイヤレスネットワークの展開

設計および導入ガイドのこの項では、このマニュアルの「ソリューションの概要」で説明されている使用例を実装します。Cisco DNA Center は、このマニュアルの「ワイヤレスネットワークの設計」で作成されたワイヤレスプロファイルを Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）および Cisco Catalyst 9800-CL ゲスト ワイヤレスコントローラ（WLC-9800-CL）に自動的に展開するために使用されます。

ここでは、以下のトピックとプロセスについて説明します。

- Catalyst 9800 シリーズ ワイヤレス コントローラの検出および管理
- Catalyst 9800 シリーズ ワイヤレス コントローラのソフトウェアイメージの管理
- ソフトウェアイメージ管理（SWIM）を使用した Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェアの更新
- Catalyst 9800-40 エンタープライズ ワイヤレスコントローラでの高可用性（HA）ステートフル スイッチオーバー（SSO）の設定
- Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペアのプロビジョニング
- Catalyst 9800-CL ゲストアンカー ワイヤレスコントローラのプロビジョニング
- エンタープライズ ワイヤレスコントローラ HA SSO ペアへの新しい AP の参加
- 新しい AP のプロビジョニング
- フロアマップへの新しい AP の配置

- ローカル RRM とクラウドベースの RRM
- クラウドベースの RRM の有効化
- 追加のワイヤレス設定用のテンプレートプログラマ

キャンパスのワイヤレス展開用エンタープライズ WLAN

ここでは、Milpitas サイトのキャンパスのワイヤレス展開をプロビジョニングする方法について説明します。このシナリオでは、ワイヤレスコントローラが検出され、コントローラのイメージが更新されてプロビジョニングされます。以下の項では、これらの手順について説明します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの検出と管理

この導入ガイドでは、IPアドレスの範囲を使用して、エンタープライズワイヤレスコントローラとして展開されたCisco Catalyst 9800-40 ワイヤレスコントローラとゲスト ワイヤレスコントローラとして展開された Cisco Catalyst 9800-CL ワイヤレスコントローラ の両方を検出します。検出を開始する前に、デバイスへの IP 接続を有効にする必要があります。IP アドレスの範囲を使用する場合は、範囲をワイヤレスコントローラのみに縮小して検出を高速化できます。

（注） または、検出対象の最初のデバイスを指定し、Cisco DNA Center が Cisco Discovery Protocol（CDP）を使用して、接続されたネイバーを検出するようにできます。

この手順の前提条件は次のとおりです。

- 2 台の Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）は、スタンドアロンワイヤレスコントローラとしてネットワークに接続されます。HA SSO ペアへの 2 台の Catalyst 9800-40 ワイヤレスコントローラの設定は、後のプロセスで Cisco DNA Center 内で行われます。
- NETCONF は、すべての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（WLC-9800-1、WLC-9800-2、および WLC-9800-CL）で有効になっています。
- すべての Catalyst 9800 シリーズ ワイヤレス コントローラ がネットワーク上にあり、到達可能性のために管理 IP アドレスが設定されています。
- SSH アクセスは、ローカル ユーザー データベース内で設定されたユーザー ID とパスワードを使用して、すべての Catalyst 9800 シリーズ ワイヤレス コントローラ で有効になっています。
- すべての Catalyst 9800 シリーズ ワイヤレス コントローラ にはホスト名（WLC-9800-1、WLC-9800-2、および WLC-9800-CL）が設定されているため、検出後に Cisco DNA Center インベントリ内のホスト名によってデバイスを識別できます。

次の表に、この設計および導入ガイドで使用する Cisco DNA Center のホスト名、プラットフォームモデル、および IP アドレスを示します。

表 *19 : Cisco DNA Center* のホスト名、プラットフォームモデル、および *IP* アドレス

ホストネーム（Hostname）	プラットフォームモデル	IPアドレス
WLC-9800-1	Cisco Catalyst 9800-40 ワイヤレスコントローラ	10.4.50.2
WLC-9800-2	Cisco Catalyst 9800-40 ワイヤレスコントローラ	10.4.50.22
WLC-9800-CL	Cisco Catalyst 9800-CL ワイヤレスコントローラ	10.4.48.153

この項には、次のプロセスが含まれています。

- WLAN 展開のエンタープライズ HA SSO ペアとして機能する 2 台の Catalyst 9800-40 ワイヤレスコントローラを検出します。
- WLAN 展開のゲストアンカーワイヤレスコントローラとして機能する Catalyst 9800-CL ワイヤレスコントローラを検出します。

AWS に展開された Cisco Catalyst 9800-CL ワイヤレスコントローラの検出と管理

検出プロセスは、他の Cisco Catalyst 9800-CL ワイヤレスコントローラと同じです。

WLAN 展開用のエンタープライズ HA SSO ペアとして機能する Cisco Catalyst 9800-40 ワイヤレスコントローラの検出

次の手順では、Cisco Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）を検出する方法について説明します。

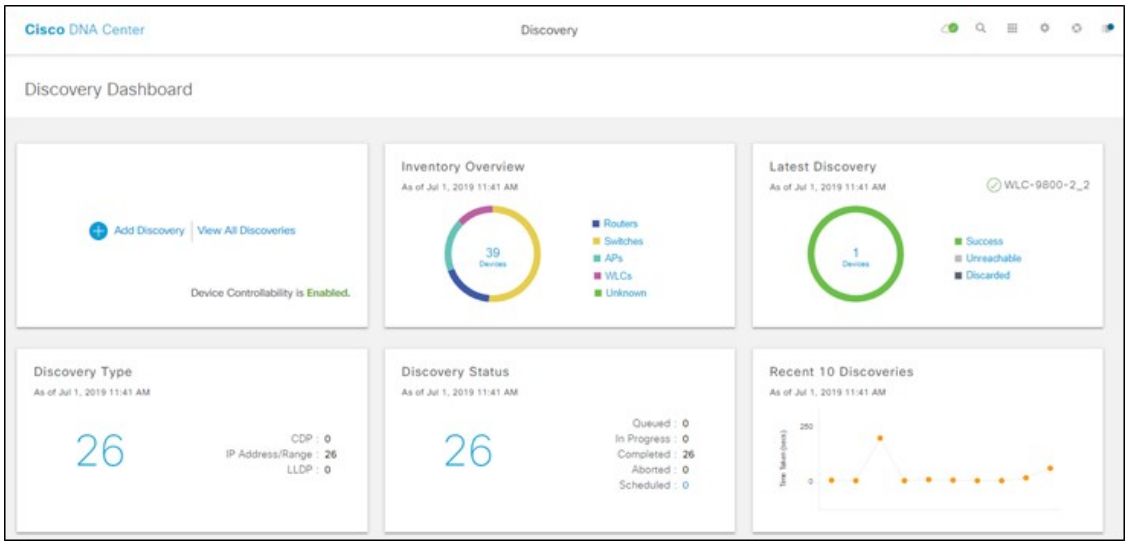
手順

ステップ 1 メインの Cisco DNA Center ダッシュボードに移動します。

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[Discovery]**。

[Discovery Dashboard] が表示されます。

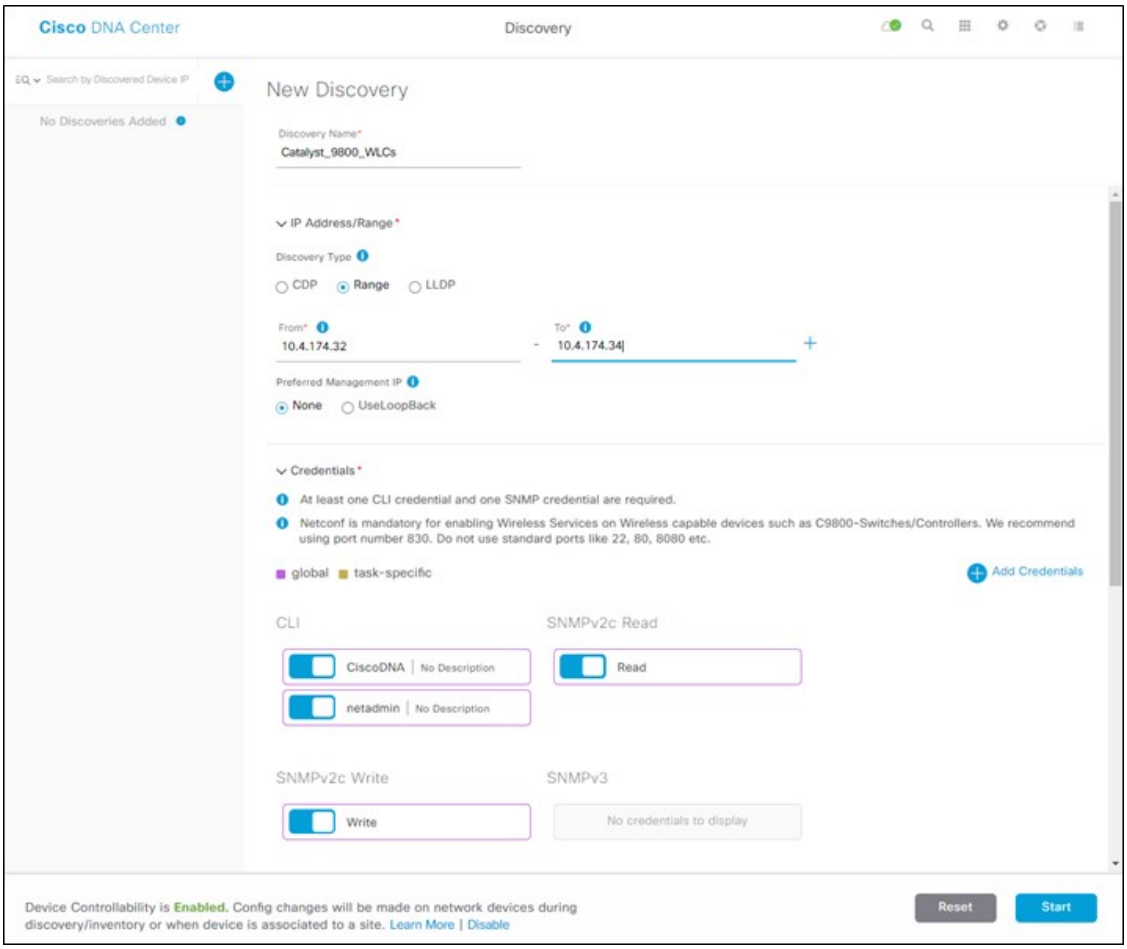
図 *63 :* 検出ダッシュボード



ステップ 3 [+ Add Discovery] をクリックして新しい検出を作成します。

[New Discovery] ウィンドウが表示されます。

図 *64 : [New Discovery]* ウィンドウ



ステップ 4 [IP Address/Range] で [Discovery Type] に対して [Range] オプションボタンをクリックします。

ステップ 5 [From] フィールドに開始 IP アドレスを入力し、[To] フィールドに終了 IP アドレスを入力します。

設定されている範囲は 10.4.50.2 ～ 10.4.50.22 で、2 つの Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）を検出するのに十分な範囲です。

ステップ 6 管理に使用するループバック インターフェイスがデバイスにある場合は、[Preferred Management IP] では [Use Loopback] オプションボタンを選択します。その他の場合は、[None] オプションボタンをクリックします。

この展開では、VLAN 174 インターフェイスがワイヤレス管理インターフェイスとして設定されているため、[Preferred Management IP] は [None] に設定されます。

ステップ 7 [CLI]、[SNMP]、および [NETCONF] ログイン情報のトグルボタンが [On] に設定されていることを確認します。

すべての Catalyst 9800 シリーズ ワイヤレス コントローラには、検出とプロビジョニングのために **NETCONF** が必要です。ワイヤレスコントローラへの NETCONF アクセスに使用されるユーザー ID とパスワードは、SSH パスワードと同じです。

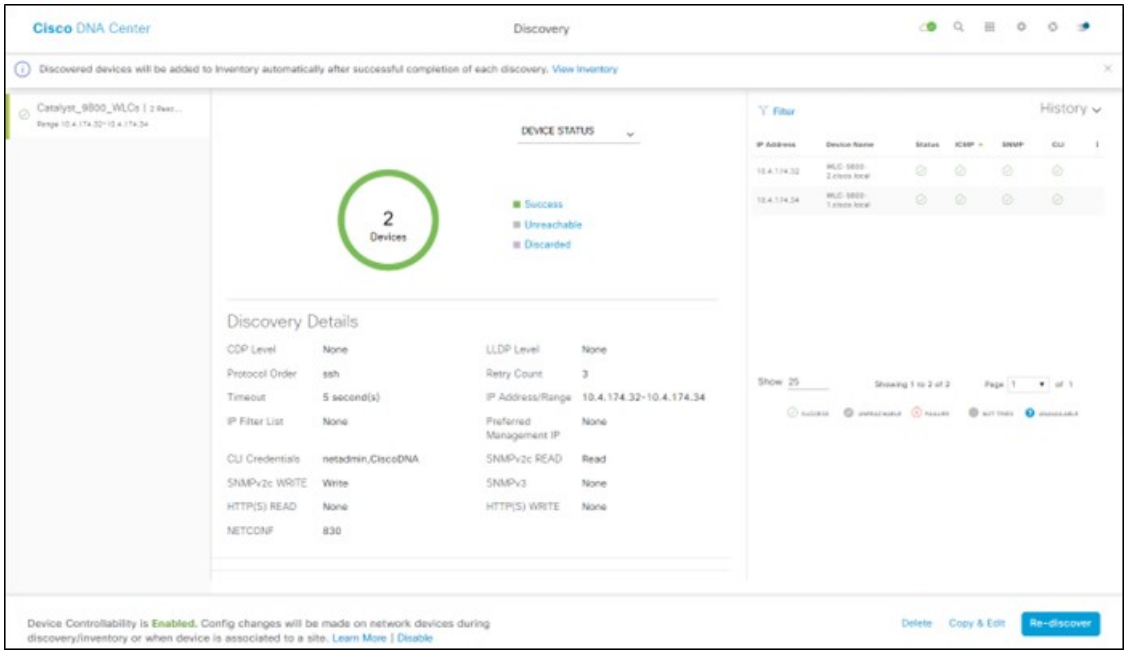
ステップ 8 [Advanced] セクションの [Protocol Order] で、[SSH] チェックボックスをオンにします。

Telnet トラフィックはクリアテキストでネットワーク全体に送信されるため、セキュリティの脆弱性が生じる可能性があり、Telnet の有効化は推奨されません。

ステップ 9 [Start] をクリックして検出を開始します。

検出の実行中は検出の詳細が表示されます。検出が完了すると、検出の詳細が表示されます。

図 *65 :* 検出の詳細



ステップ 10 検出プロセスが完了したら、メインの Cisco DNA Center ダッシュボードに移動します。

ステップ 11 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

Cisco DNA Center に認識されているデバイスのリストが表示されます。リストには、検出された 2 つの Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）が含まれます。Catalyst 9800-40 ワイヤレスコントローラには、[Managed] の [Last Sync Status] が表示されます。

これで、Cisco DNA Center からデバイスにアクセスしてインベントリを同期し、デバイスの設定を変更できます。

WLAN 展開のゲストアンカーワイヤレスコントローラとして機能する Cisco Catalyst 9800-CL ワイヤレスコントローラの検出

Cisco Catalyst 9800-CL ゲスト ワイヤレスコントローラ（WLC-9800-CL）の Cisco Catalyst 9800-40 ワイヤレスコントローラを検出するには、「WLAN 展開用のエンタープライズ HA SSO ペアとして機能する Cisco Catalyst 9800-40 ワイヤレスコントローラの検出」の手順を繰り返します。

この導入ガイドでは、Catalyst 9800-CL ゲスト ワイヤレスコントローラ（WLC-9800-CL）を検出するための IP アドレスの範囲は、1 つの IP アドレス（10.4.174.36 ～ 10.4.174.36）です。

（注） 必要に応じて、Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）と Catalyst 9800-CL ゲスト ワイヤレスコントローラ（WLC-9800-CL）の両方の IP アドレスの範囲を含む 1 回の検出で、すべてのワイヤレスコントローラを検出できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのソフトウェアイメージの管理

このプロセスは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最新のソフトウェアイメージを Cisco DNA Center ソフトウェアイメージリポジトリにアップロードするために使用されます。次の表に、この展開用にアップロードされたプラットフォームとソフトウェアイメージを示します。

表 *20 : Catalyst 9800* シリーズ ワイヤレス コントローラのソフトウェアイメージ

プラットフォーム	ソフトウェア バージョン	ソフトウェア イメージ
Cisco Catalyst 9800-40 ワイヤレスコントローラ	IOS XE リリース 17.9.4a	C9800-40-universalk9_wlc.17.09.04a.SPA.bin
Cisco Catalyst 9800-CL ワイヤレスコントローラ	IOS XE リリース 17.9.4a	C9800-CL-universalk9.17.09.04a.SPA.bin

Catalyst 9800 シリーズ ワイヤレス コントローラと Cisco DNA Center の間で動作させるには、IOS XE リリース 16.10.1 以上が必要です。

このプロセスには、次の手順が含まれます。

- Cisco Catalyst 9800-40 ワイヤレスコントローラのソフトウェアイメージをアップロードします。
- Cisco Catalyst 9800-CL ワイヤレスコントローラのソフトウェアイメージをアップロードします。

Cisco Catalyst 9800-40 ワイヤレスコントローラのソフトウェアイメージのアップロード

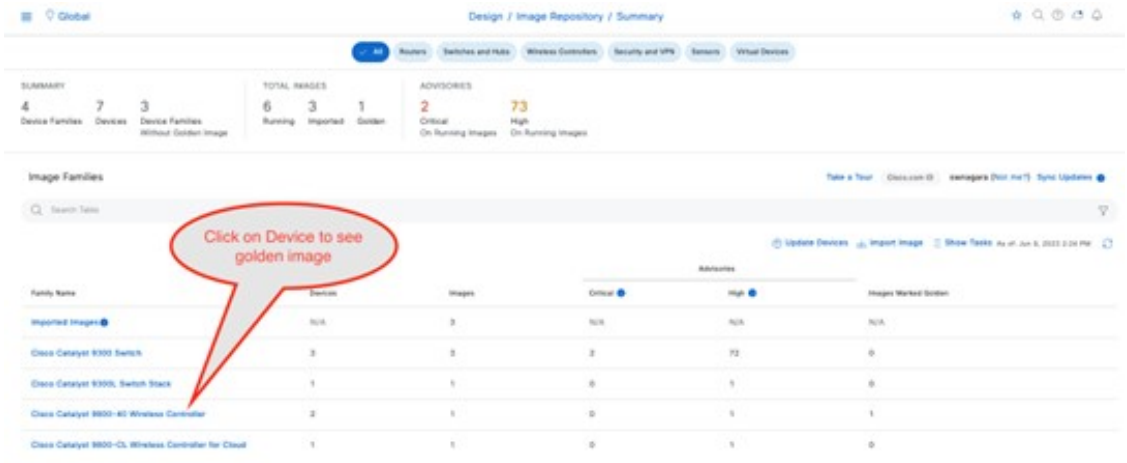
次の手順では、Cisco Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）のイメージのアップロードプロセスについて説明します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Image Repository]**。

次の図に、[Image Repository] ウィンドウを示します。

図 *66* : イメージリポジトリ



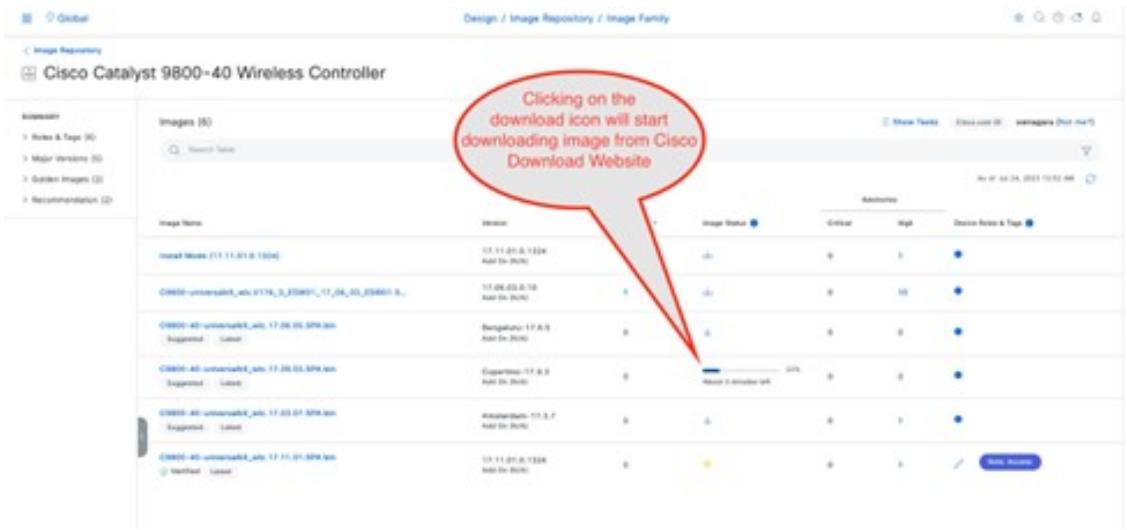
ステップ 2 次のいずれかを実行して、Cisco DNA Center イメージリポジトリに追加する新しいイメージを取得できます。

- シスコの Web サイトからイメージをダウンロードする。
- ローカルマシンからイメージをインポートする。

ステップ 3 目的のイメージの [Download Image] アイコンをクリックします。シスコの Web サイトからイメージがダウンロードされます。

この導入ガイドでは、イメージ 17.9.4a がダウンロードされています。

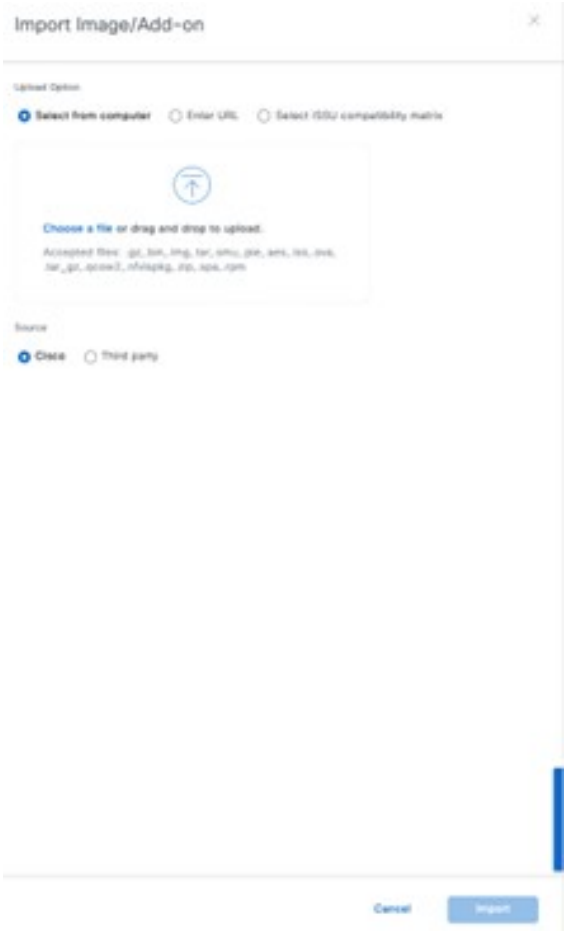
図 *67* : イメージのダウンロード



ステップ 4 または、[Import] をクリックして新しいイメージをインポートします。

[Import Image/Add-on] ダイアログボックスが表示されます。

図 *68 :* イメージのインポート



ステップ 5 [ファイルの選択（Choose File）] をクリックします。

ステップ 6 コンピュータの Catalyst 9800-40 ソフトウェアイメージに移動し、目的のイメージを選択します。

この導入ガイドでは、C9800-40-universalk9_wlc.17.09.04a.SPA.bin が選択されています。

ステップ 7 これはシスコのソフトウェアイメージであるため、[Source] で [Cisco] オプションボタンをクリックします。

ステップ 8 [Import] をクリックして、イメージを Cisco DNA Center イメージリポジトリにアップロードします。

ステータスバーにアップロードの進捗が表示されます。アップロードが完了すると、メインの [Image Repository] ウィンドウが表示されます。

ステップ 9 **[タスクの表示（Show Tasks）]** をクリックして、イメージが正常にインポートされたことを確認します。

[Recent Tasks (Last 50)] サイドパネルが表示されます。新しいイメージの遷移は黄色で表示されます。正常に完了したタスクには、緑色のチェックマークが表示されます。

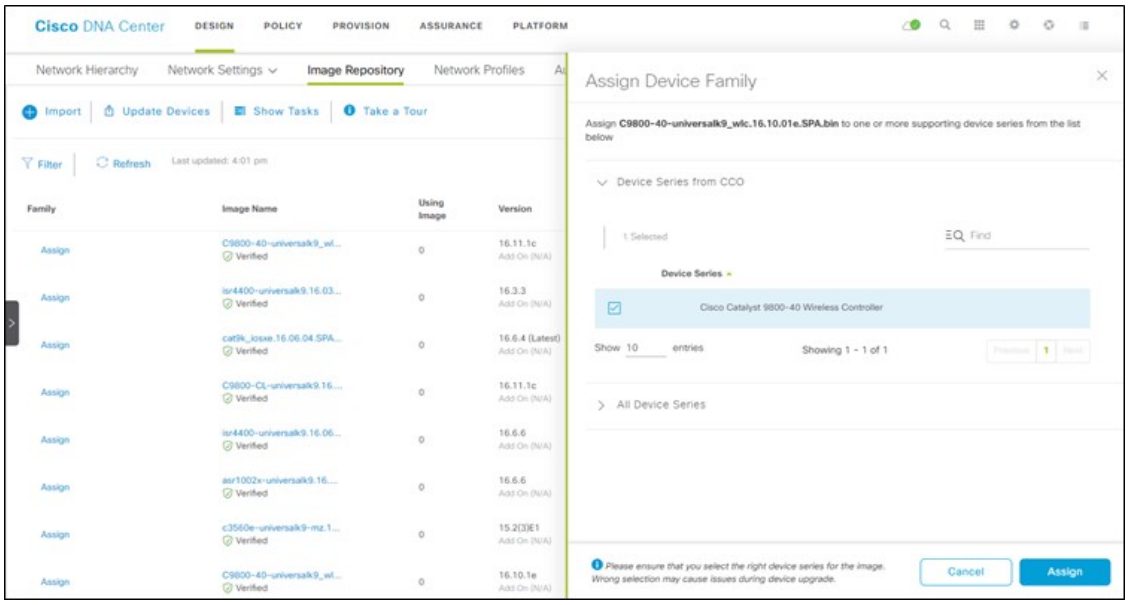
ステップ 10 [Recent Tasks (Last 50)] サイドパネルを閉じます。

ステップ 11 [Image Repository] ウィンドウで、[Imported Images] の横にある [>] をクリックして、インポートされたイメージのリストを展開します。

ステップ 12 アップロードしたイメージファイルの横にある [Assign] をクリックします。

[Assign Device Family] サイドインペインが表示されます。

図 *69 :* デバイスファミリの割り当て



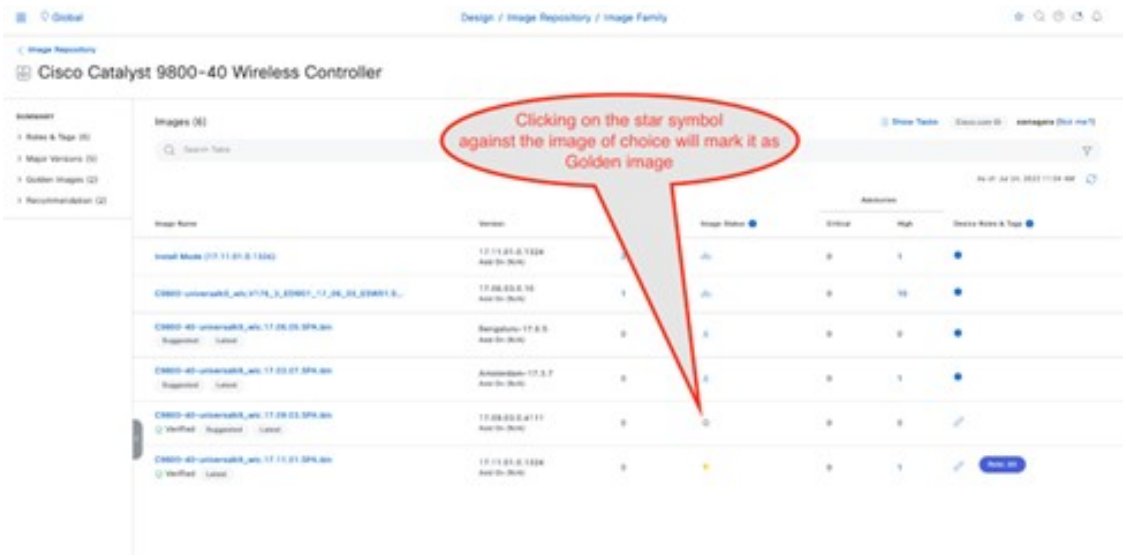
ステップ 13 [Cisco Catalyst 9800-40 ワイヤレスコントローラ] を選択し、[Assign] をクリックして、このイメージをデバイスファミリに割り当てます。

ステップ 14 メインのリポジトリウィンドウにあるデバイスリストの [Family] 列で、Catalyst 9800-40 ワイヤレスコントローラを見つけ、デバイスで使用可能なイメージのリストを展開します。

デバイスファミリで使用可能なイメージのリストに、アップロードした新しいイメージが表示されます。

ステップ 15 [Golden Image] の星印をクリックして、Catalyst 9800-40 ワイヤレスコントローラ プラットフォームの優先イメージとしてそのゴールデンイメージをマークします。

図 *70* : ゴールデンイメージをマーク



Catalyst 9800-CL ゲスト ワイヤレスコントローラ（WLC-9800-CL）に対して手順全体を繰り返します。この導入ガイドでは、Catalyst 9800-CL ゲスト ワイヤレスコントローラのアップロードイメージ名は C9800-CL-universalk9.17.09.04a.SPA.bin です。

Cisco Catalyst 9800-CL ワイヤレスコントローラのソフトウェアイメージの更新

ここでは、イメージがゴールデンとしてマークされた後にワイヤレスコントローラ イメージを更新する手順について説明します。

ソフトウェアイメージ管理（SWIM）を使用した Catalyst 9800 シリーズ ワイヤレスコントローラ ソフトウェアの更新

このプロセスは、次の目的で使用されます。

- Cisco DNA Center イメージリポジトリからワイヤレスコントローラにソフトウェアイメージを配布（ダウンロード）する。
- ワイヤレスコントローラで実行されているソフトウェアイメージをアップグレードする。

両方の手順はすぐに実行することも、既存のネットワーク変更スケジュールに従って、指定した日時に実行するようにスケジュールすることもできます。

Cisco DNA Center ではコンプライアンスチェックを実行し、インベントリ内のデバイスとゴールデンイメージとしてマークされたイメージが比較されます。ゴールデンイメージに対応していないデバイスには、インベントリ内で[Outdated]とマークされます。ゴールデンとマークされたバージョンにイメージを更新する前に、インベントリ収集が正常に完了し、デバイスが [Managed] 状態になっている必要があります。

このプロセスには、次の手順が含まれます。

- Catalyst 9800-40 ワイヤレスコントローラのソフトウェアイメージをアップグレードします。

• Catalyst 9800-CL ワイヤレスコントローラのソフトウェアイメージをアップグレードします。

Cisco Catalyst 9800-40 ワイヤレスコントローラのソフトウェアイメージのアップグレード

次の手順では、Cisco Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）のソフトウェアイメージをアップグレードする方法について説明します。

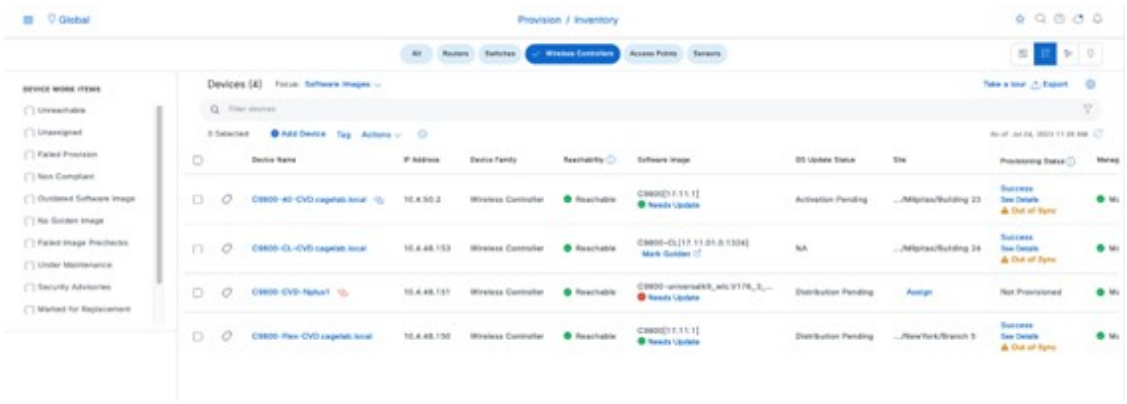
手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 [Focus] ドロップダウンリストから [Software Images] を選択します。

ウィンドウに、インベントリ内の各デバイスで実行されているソフトウェアイメージが表示されます。

図 *71 : [Inventory]* ウィンドウ

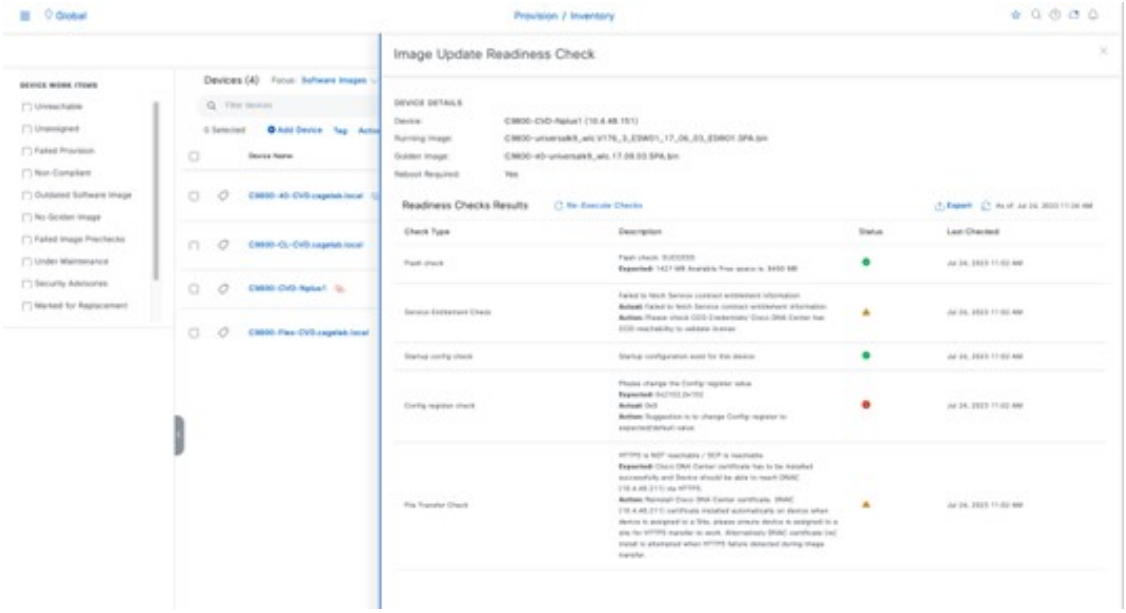


ステップ 3 デバイスのリストから、いずれかの Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 または WLC-9800-2）を見つけます。

ステップ 4 Catalyst 9800-40 ワイヤレスコントローラの [Software Image] 列で、[Needs Update] をクリックします。

[Image Update Readiness Check] slide-in paneが表示されます。

図 *72 : [Image Update Readiness Check]* ウィンドウ



[Status] 列に、成功を示す緑色のアイコンまたは警告を示す黄色のアイコンが表示されていることを確認します。いずれかのチェックで失敗を示す赤色のアイコンが表示されている場合、プラットフォーム上のイメージはアップグレードされていません。この導入ガイドでは、設定レジスタの値は 0x2102 または 0x102 である必要がありますが、デバイスでは 値 0x0 が使用されているため、[Config register check] に赤いアイコンが表示されます。

必要に応じて、障害の原因となっているワイヤレスコントローラの問題を修正します。

ステップ 5 [Re-Execute Check] をクリックして、準備状況アセスメントを再実行します。

（注） `clock timezone` IOS CLI コマンドを使用して IOS XE デバイスでタイムゾーンを設定すると、[Image Update Readiness Check] slide-in paneに警告が表示され、デバイスと Cisco DNA Center の間で大幅に異なる時間が示されることがあります。この警告をクリアするには、デバイスから `clock timezone` コマンドを削除し、インベントリでデバイスを再同期し、[Re-Execute Check] をクリックして準備状況アセスメントを再度実行します。その結果、デバイスの時間形式はローカルタイムゾーンではなく UTC 時間で表示されます。

ステップ 6 失敗を示すチェックをすべて修正したら、[Image Update Readiness Check] slide-in paneを閉じます。

ステップ 7 他の Catalyst 9800-40 ワイヤレスコントローラについて、ステップ 1 ～ 6 を繰り返します。

ステップ 8 両方の Catalyst 9800-40 ワイヤレスコントローラ（ワイヤレスコントローラ-9800-1 および ワイヤレスコントローラ-9800-2）のチェックボックスをオンにします。

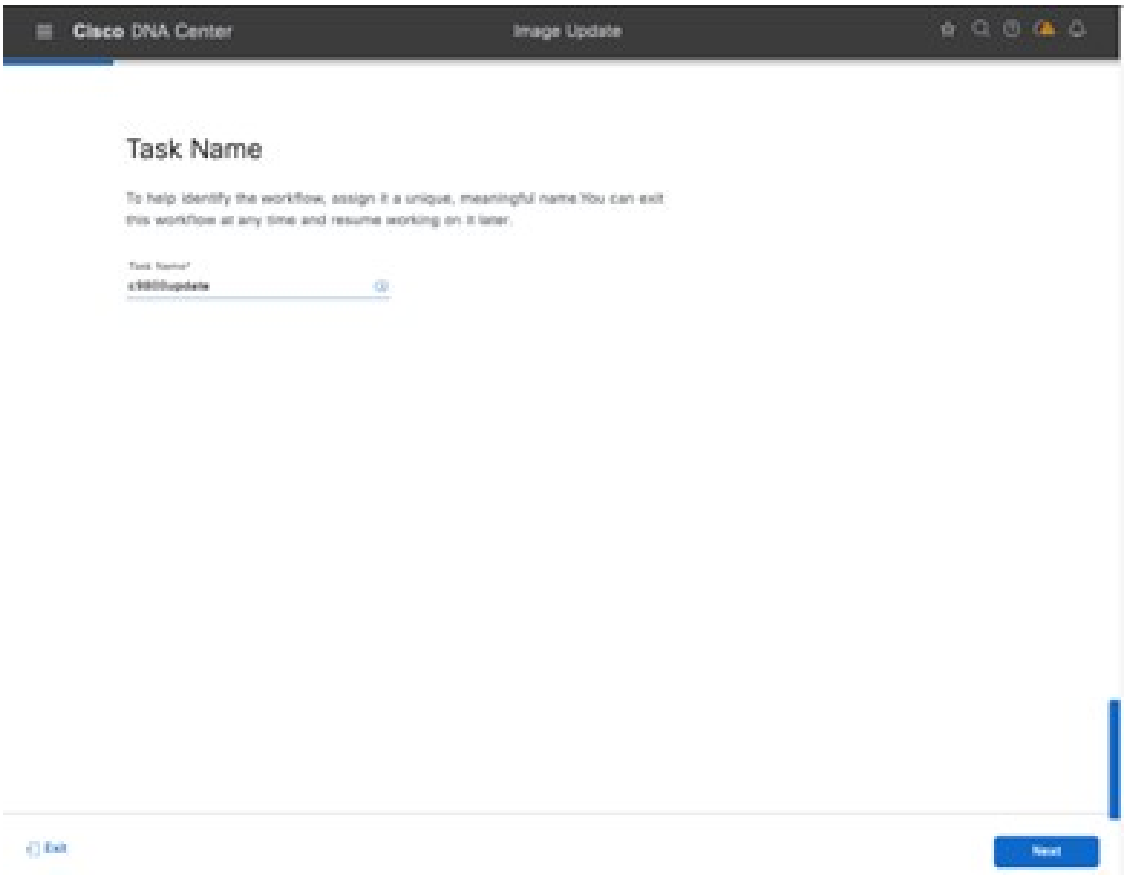
ステップ 9 [Actions] ドロップダウンリストから、**[Software Image]** > **[Image Update]** を選択します。

[Image Update] slide-in paneが表示されます。

a) [Task Name] フィールドに一意の名前を入力します。

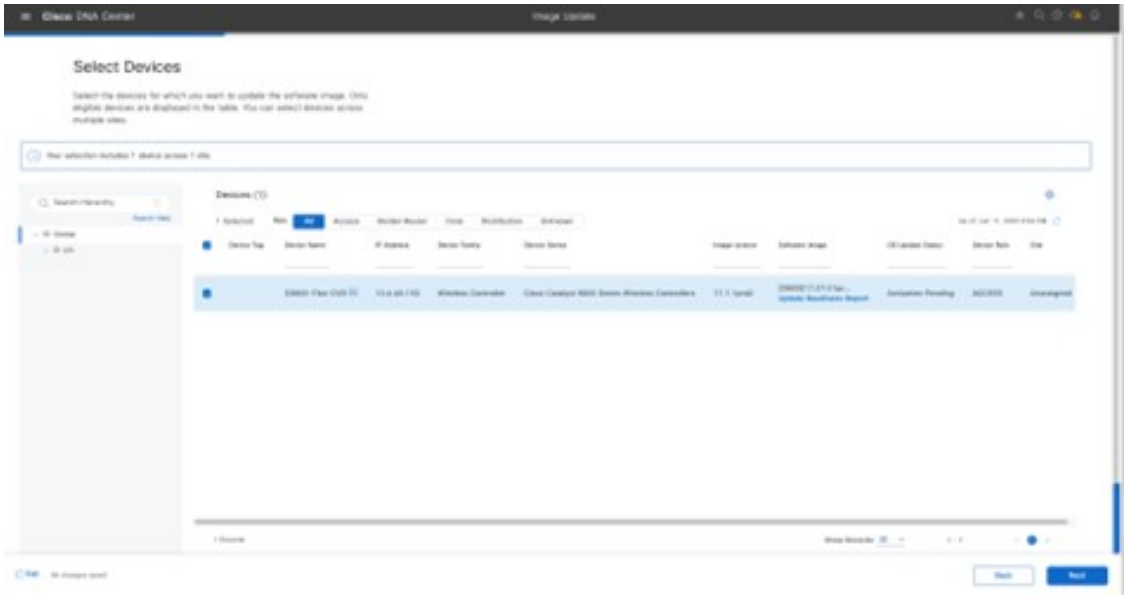
この導入ガイドでは、**c9800update** と入力します。

図 *73* : タスク名の入力



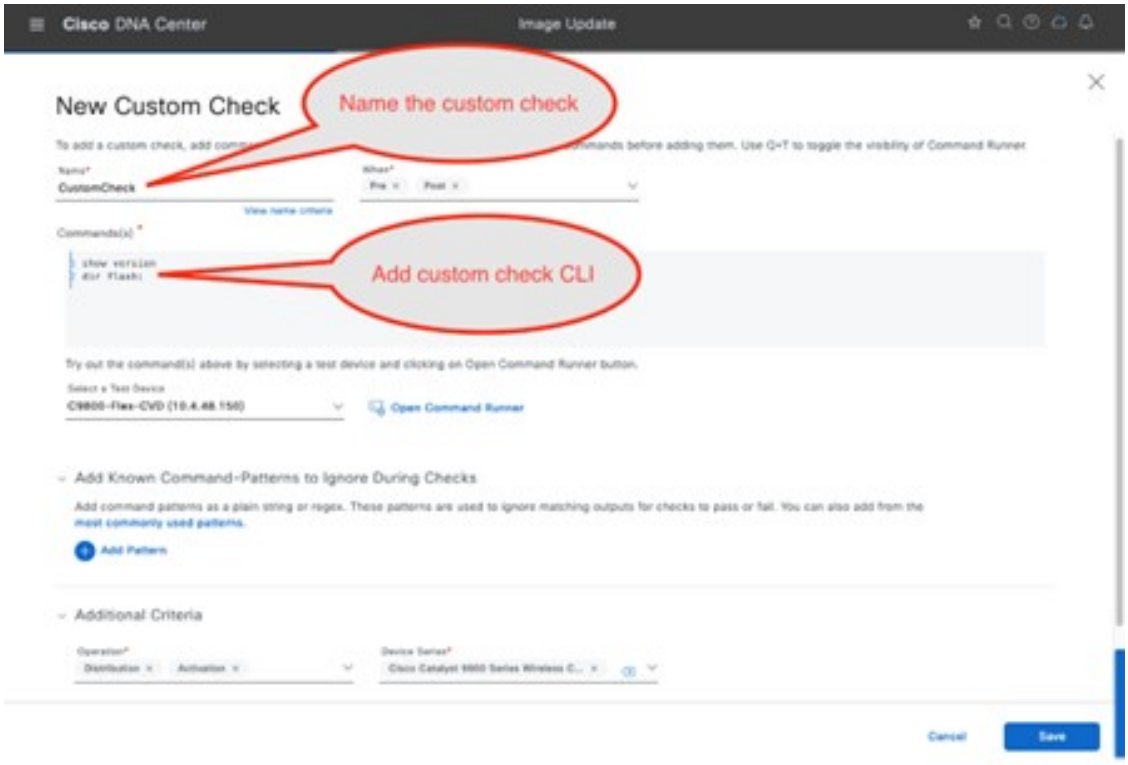
b) [Next] をクリックします。
c) デバイス名のチェックボックスをオンにして、デバイスを選択します。

図 *74 : [*デバイスの選択（***Select Devices***）*]*ウィンドウ



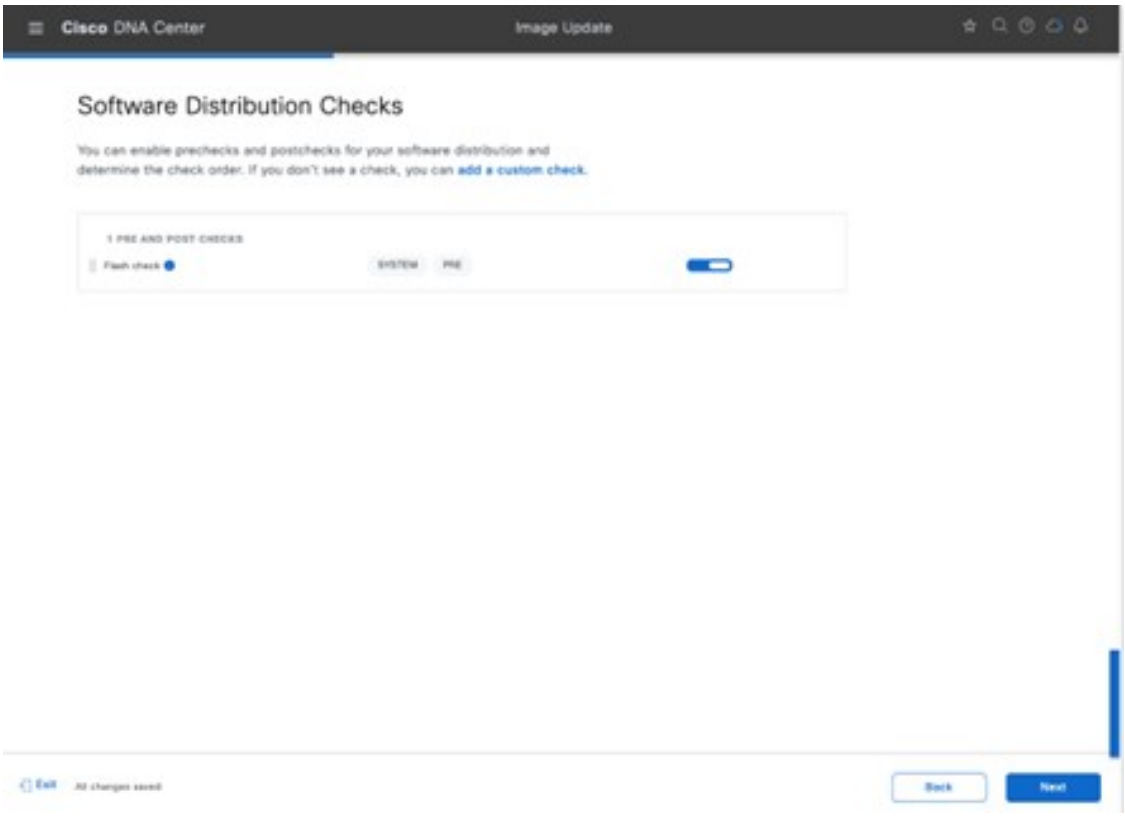
d) [Next] をクリックして、カスタマイズされたソフトウェア配布のチェックに進みます。

図 *75 :* カスタム配布チェック



e) カスタマイズが不要な場合は、デフォルトの [Flash check] の選択は任意です。

図 *76 :* 更新イメージの配信

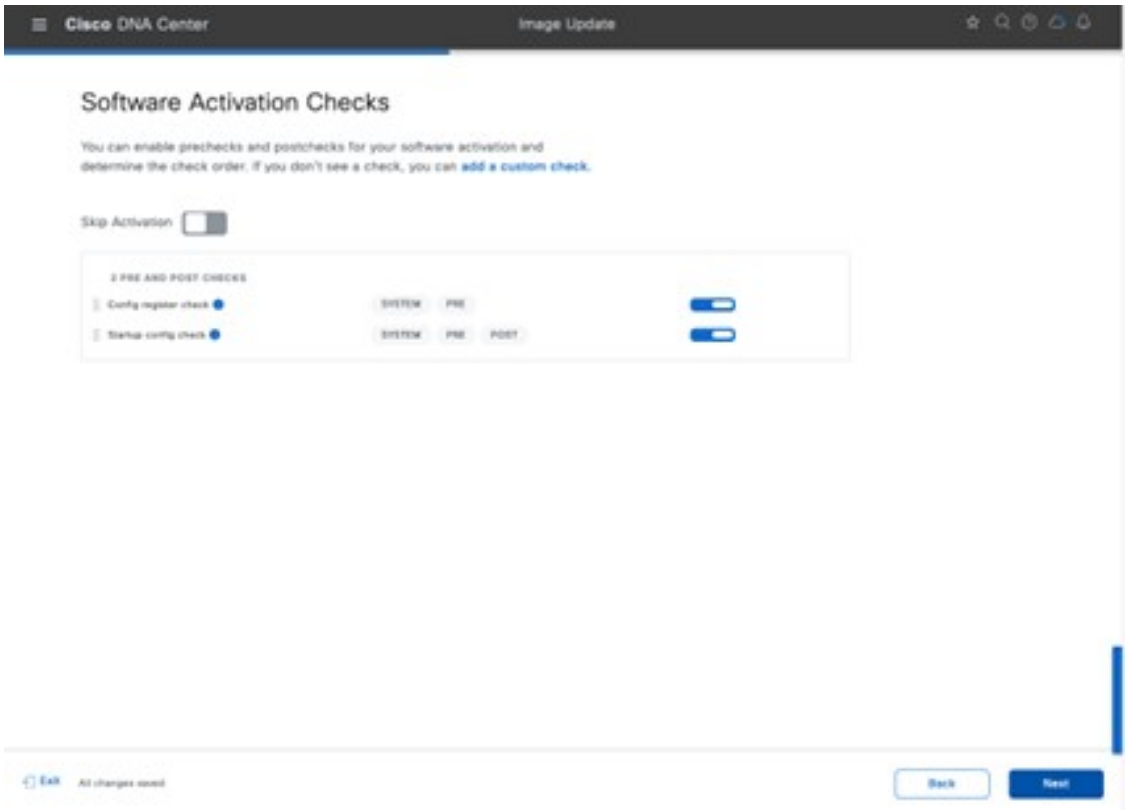


f) [Next] をクリックして、[Software Activation Checks]に進みます。デフォルトでは、[Config register check] と [Startup config check] が選択されています。

g) [Add a custom check] をクリックして、カスタムチェックを追加します。

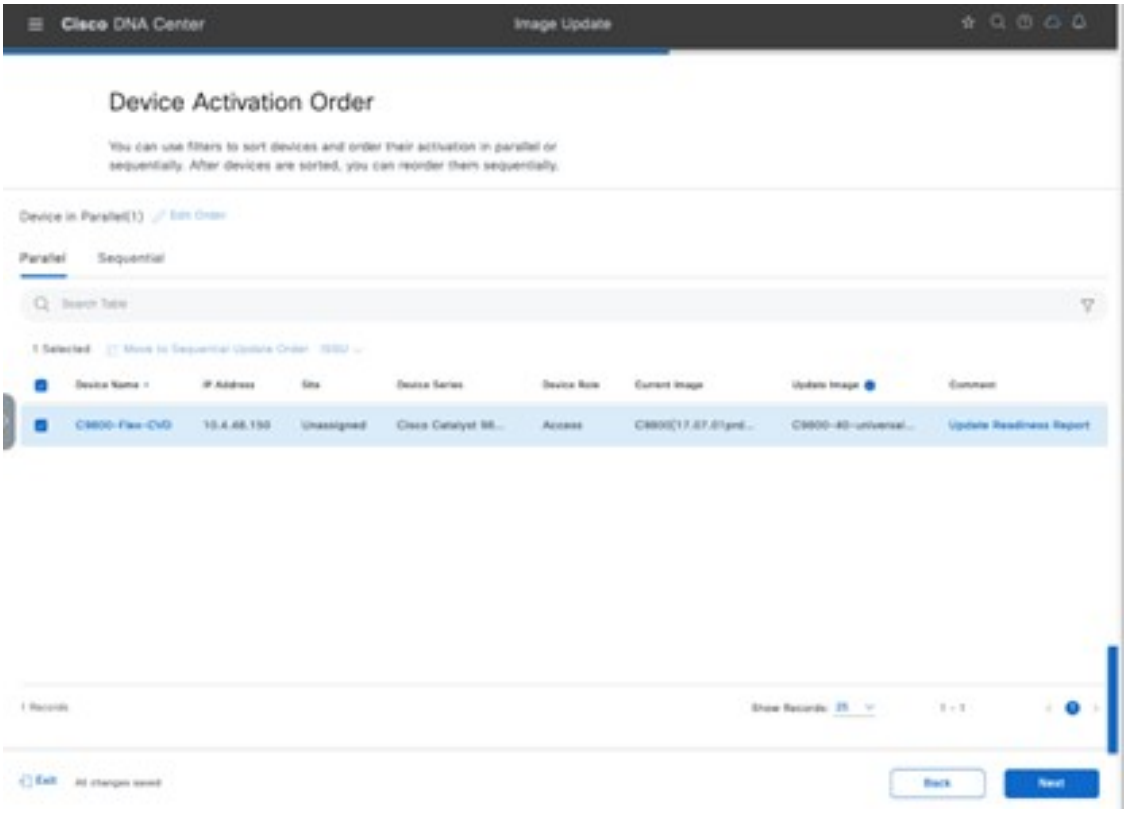
このガイドでは、デフォルトのチェックのみが選択されています。

図 *77 : [Software Activation Checks]*



h) 複数のデバイスがある場合は、[Next] をクリックし、[Device Activation Order] を選択します。このガイドでは、デバイスが 1 つしかないため、そのデバイスのみが選択されています。

図 *78 : [Device Activation Order]*



i) [Next] をクリックして、配布とアクティベーションを後でスケジュールします。配布とアクティベーションをすぐに実行するには、[Now] をクリックします。

ソフトウェアが配布されていない場合（Cisco DNA Center リポジトリからワイヤレスコントローラにダウンロードされていない場合）は、[Now] オプションは選択できませんが、ソフトウェアの配布完了後にただちにソフトウェアをアクティブ化するようにスケジュールしたり、ソフトウェアのアクティベーションを後の日時にスケジュールしたりできます。アクティベーション時刻のスケジュールが配布時刻に近すぎる場合、スケジュールされたアクティベーション時刻の前にデバイスへのイメージの配布が完了しないために、更新が失敗する可能性があるという警告が表示されます。

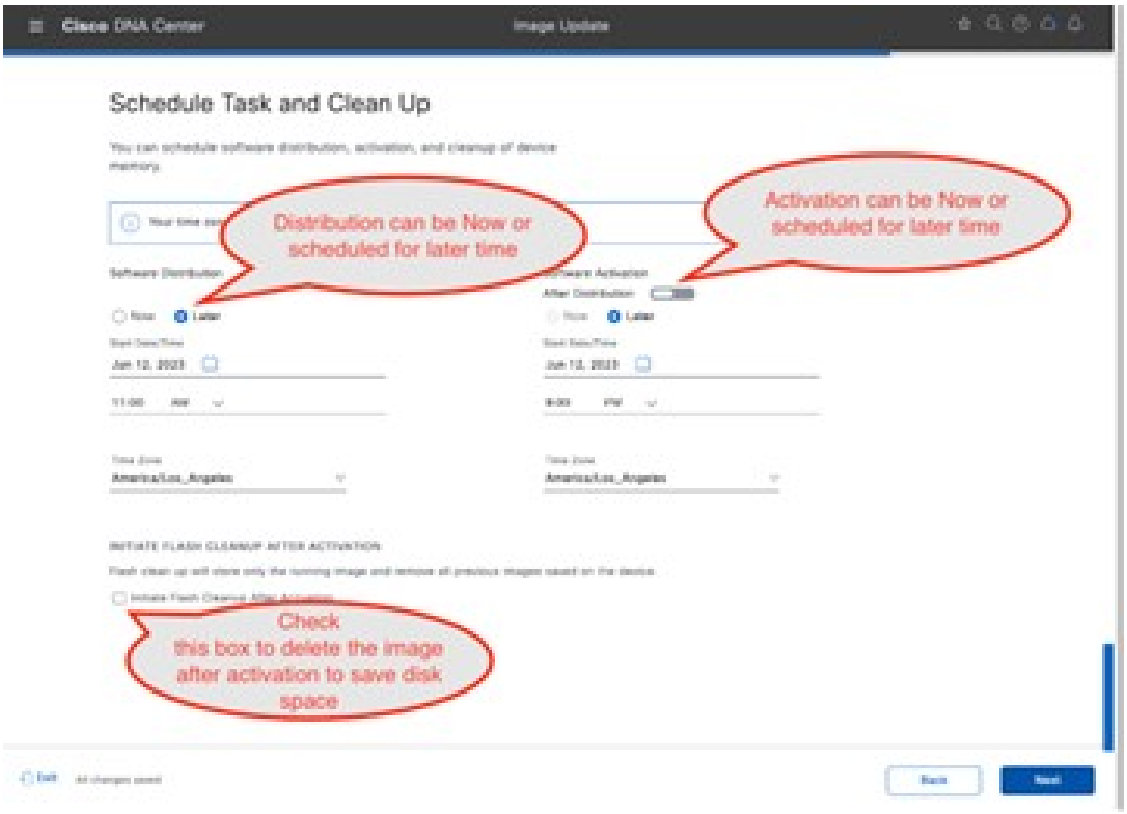
（注） ソフトウェアイメージは、常にスケジュールされたネットワーク運用の変更時間帯にのみアップグレードすることを推奨します。

ステップ 10 [Software Activation After Distribution] を有効にします。

または、[Later] オプションボタンをクリックして、イメージの配信日時を調整します。

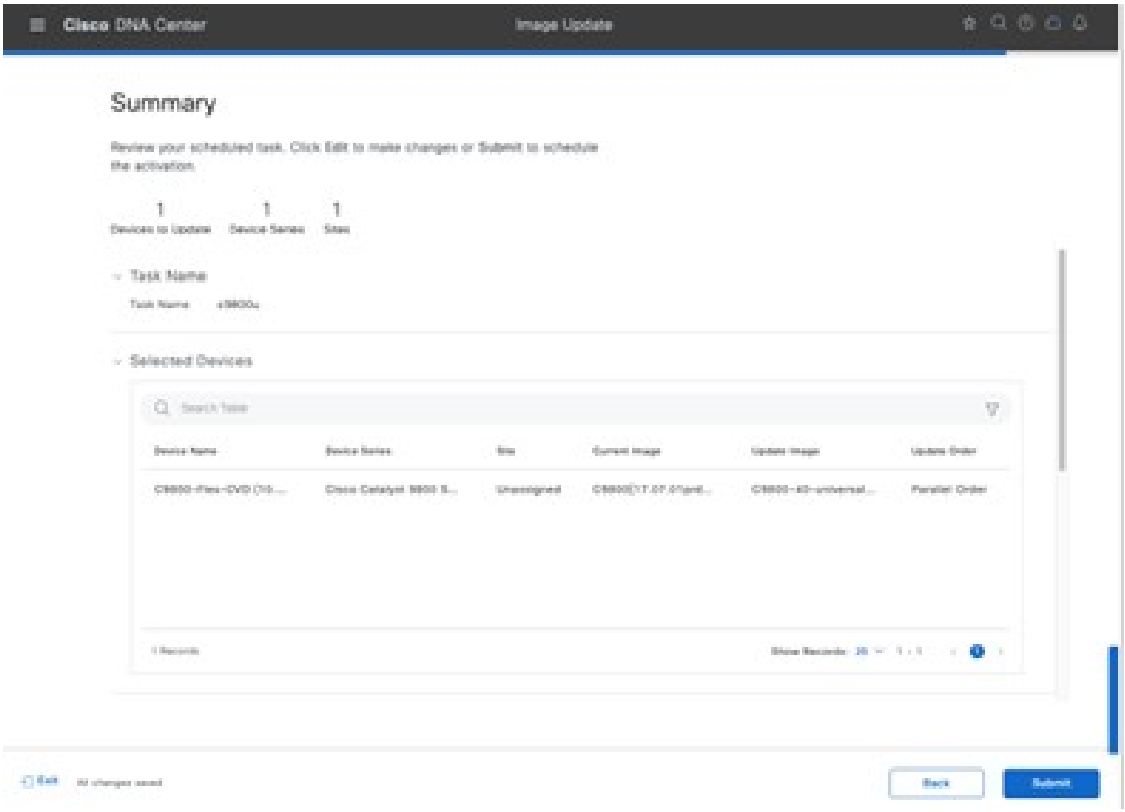
[Software Activation After Distribution] を有効にすると、配布直後にイメージがアクティブ化されます。このアクションは、ダウンロードとアクティベーションを個別にスケジュールするのではなく、イメージのダウンロードとアクティベーションを単一のスケジュールされたプロセスに結合します。

図 *79 : [Distribution and Activation]* ウィンドウ



a) [Next] をクリックして [Summary] ウィンドウに進み、選択内容を確認してから、デバイスイメージの更新タスクを送信します。

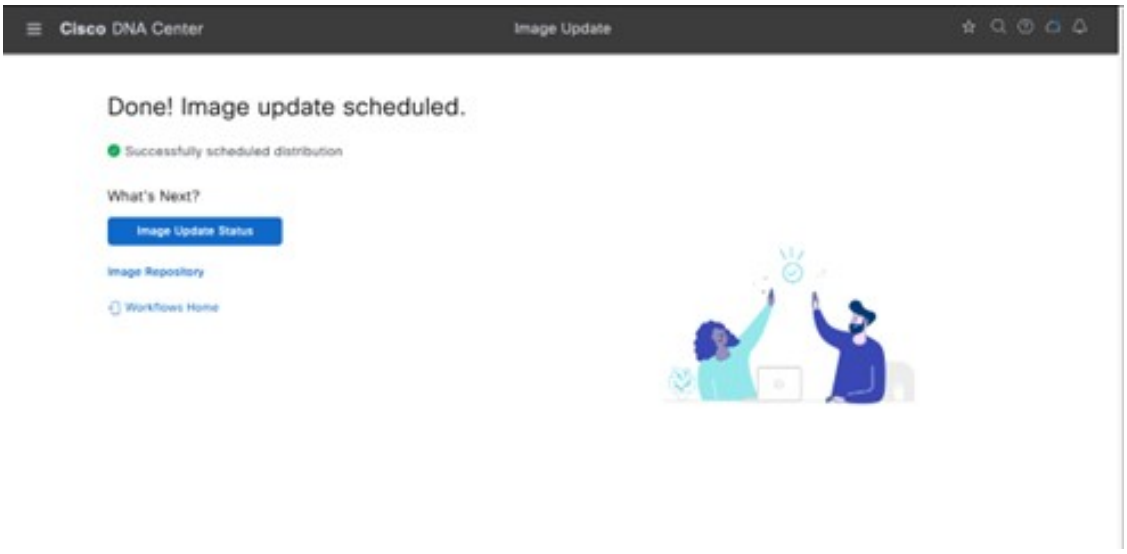
図 *80 :* アップグレードタスクを送信する前の概要の確認



b) [Submit] をクリックします。`

ステータスウィンドウが表示され、更新の進捗状況が示されます。

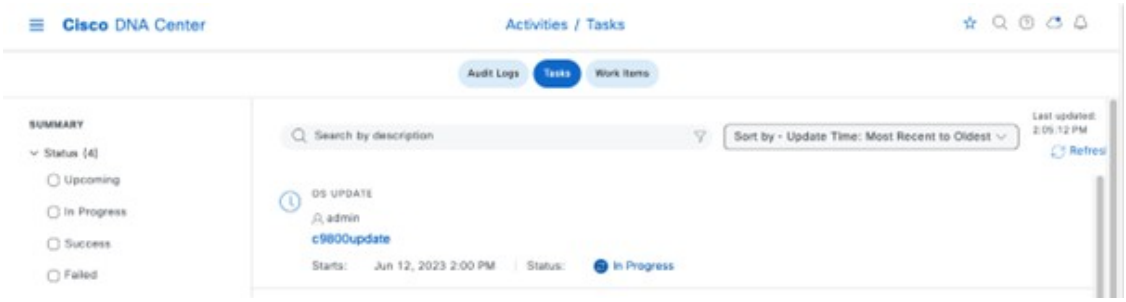
図 *81 : [Image Update Status]*



ステップ 11 [Image Update Status] をクリックすると、更新の進行状況ウィンドウが表示されます。

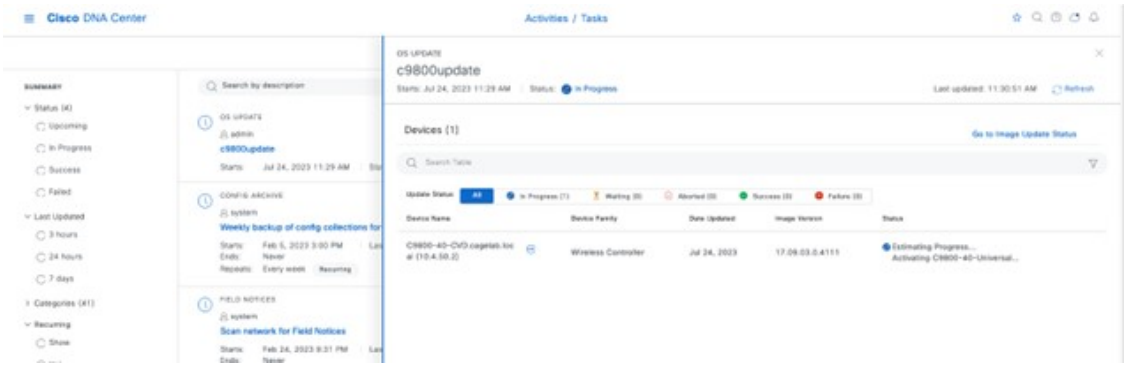
または、メニューアイコンをクリックして、 **[Activities]** > **[Tasks]**を選択します。[Scheduled Task] ウィンドウが表示されます。

図 *82 : [Scheduled Task]* ウィンドウ



タスクを展開して、イメージの配布とアクティベーションに関する詳細を表示できます。

図 *83 :* オペレーティングシステムの更新が進行中



タスクが正常に完了すると、タスクの横にアイコンが表示され、更新が成功したことが示されます。この場合も、タスクを展開して、イメージの配布とアクティベーションに関する詳細を表示できます。

ステップ 12 [Scheduled Task] slide-in paneを閉じます。

ステップ 13 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]**の順に選択して、メインの [Provisioning] ウィンドウのインベントリリストに戻ります。

Catalyst 9800-40 ワイヤレスコントローラのイメージは、選択した IOS バージョンに更新されたことを示しています。

Catalyst 9800-CL ゲスト ワイヤレスコントローラ（Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ -CL）に対して手順全体を繰り返します。

Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラでの HA SSO の設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、アクティブまたはスタンバイの高可用性（HA）ステートフル スイッチオーバー（SSO）ペアで設定する機能がサポートされています。Cisco DNA Center では、同じオペレー

ティング システム バージョンを実行している同じモデルの 2 つのコントローラを取得し、HA SSO ペアとして設定する機能がサポートされています。

（注）

- HA SSO を有効にする前に、RP ポートは直接または専用 L2 ネットワークを介して接続されます。光ファイバ SFP またはイーサネット RJ-45 ポートに接続できます。光ファイバ SFP HA 接続は、RJ-45 よりも優先されます。RJ-45 HA の稼働中に SFP が接続されると、HA ペアがリロードされます。
- RP ポートをバックツーバックで直接接続する場合は、長さが 30 m（100 フィート）未満の銅ケーブルを使用することを推奨します。30 m（100 フィート）を超える距離に設置する必要がある場合は、光ファイバケーブルを使用して RP ポートを接続することを推奨します。
- 両方のボックスで同じソフトウェアが実行されており、同じブートモードになっています（インストールモードが推奨のブートモードです）。
- 物理アプライアンスの場合は、同じハードウェアタイプを使用します（たとえば、C9800-LC と C9800-LF はペアリングできません）。
- Catalyst 9800-CL ワイヤレスコントローラの場合、両方の仮想マシンで同じスケールテンプレート（大、中、または小）を選択します。
- HA ペアを形成する前に、以前にスタンドアロンとして展開されていた各 Catalyst 9800 シリーズ ワイヤレスコントローラ内の既存の証明書とキーを削除することを推奨します。削除することで、異なるキーがある両方の ワイヤレスコントローラに同じトラストポイントが存在し、スイッチオーバー後に問題が発生するリスクを回避できます。
- キープアライブ再試行回数を 5 回（リリース 17.1 のデフォルト）に設定します。
- アクティブ ワイヤレスコントローラにするシャーシで高い優先順位（2）を設定します。

次の手順では、Catalyst 9800-40 ワイヤレスコントローラ（WLC-9800-1 および WLC-9800-2）を HA SSO ペアとして設定する方法について説明します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

メインの [Provisioning] ウィンドウにデバイスが表示されます。デフォルトでは、[Focus] は [Inventory] に設定されます。

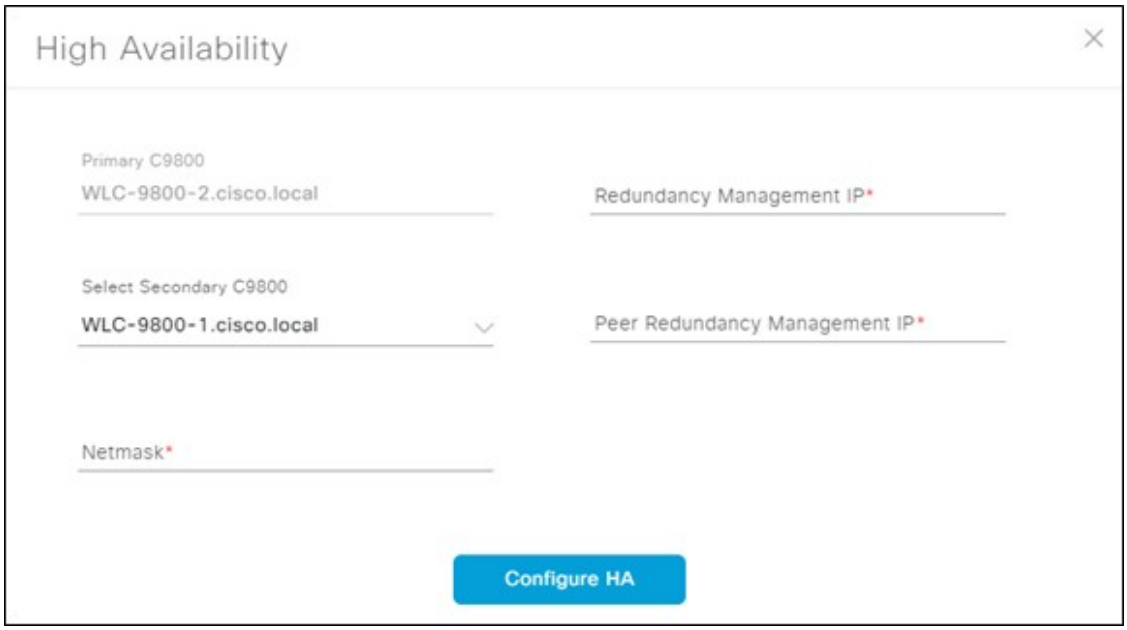
ステップ 2 HA SSO ワイヤレスコントローラ ペアのプライマリ ワイヤレスコントローラとなる Catalyst 9800-40 ワイヤレスコントローラのチェックボックスを見つけてオンにします。

この設計および導入ガイドでは、**WLC-9800-2** がプライマリ ワイヤレスコントローラとして選択されています。

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

[High Availability] slide-in paneが表示されます。

図 *84 : [High Availability]* ウィンドウ



ステップ 4 それぞれのフィールドに必要な情報を入力し、[Configure HA] をクリックします。

次の表に、この導入ガイドの高可用性情報を示します。

表 *21 :* 高可用性の設定

フィールド	値
Primary Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	WLC-9800-1.cisco.local
冗長性管理 IP	10.4.174.132
セカンダリ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの選択	WLC-9800-2.cisco.local
ピア冗長性管理 IP	10.4.174.134
ネットマスク（Netmask）	24

（注） [Redundancy Management IP] および [Peer Redundancy Management IP] アドレスは、ワイヤレス管理インターフェイスと同じ IP 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が高可用性モードになると再起動されることを通知するダイアログボックスが表示されます。

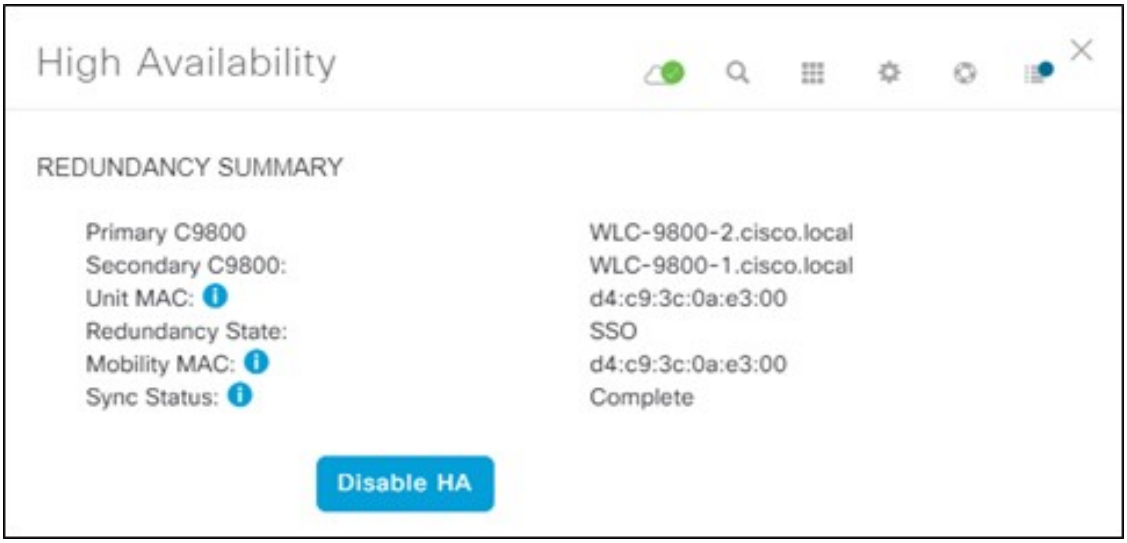
ステップ 5 [OK] をクリックして承認し、2 台の Catalyst 9800-40 ワイヤレスコントローラを HA SSO モードにします。

ワイヤレスコントローラが再起動して HA SSO モードで表示されるまでに数分かかります。管理インターフェイスの IP アドレスを含む、プライマリ Catalyst 9800-40 ワイヤレスコントローラのすべての設定がセカンダリ Catalyst 9800-40 ワイヤレスコントローラにコピーされます。Cisco DNA Center ではインベントリ内の 2 つのワイヤレスコントローラは表示されなくなります。代わりに、2 つのシリアル番号がある単一のワイヤレスコントローラ HA SSO ペアのみがインベントリに表示されます。

この導入ガイドでは、ワイヤレスコントローラ HA SSO ペアは WLC-9800-2 です。

ステップ 6 ワイヤレスコントローラ（WLC-9800-2）を選択し、[Actions] ドロップダウンリストから**[Provision]** > **[Configure WLC HA]**の順に選択すると、Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペアに関する追加情報を確認できます。

図 *85 : Catalyst 9800-40* ワイヤレスコントローラ *HA SSO* ペアの詳細



（注） [Disable HA] をクリックすると、両方の Catalyst 9800-40 ワイヤレスコントローラがスタンドアロンモードに戻り、セカンダリ ワイヤレスコントローラが工場出荷時の設定にリセットされます。HA を無効にする前に、ワイヤレスコントローラへのコンソールアクセスを確立することを推奨します。HA を無効にした後、Cisco DNA Center のコントローラを再検出するには、いずれかのワイヤレスコントローラの IP アドレスとホスト名を変更する必要があります。

Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペアのプロビジョニング

次の手順では、Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（Cisco Catalyst 9800-40-CVD.cagelab.local）に企業のワイヤレスプロファイルをプロビジョニングする方法について説明します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

メインの [Provisioning] ウィンドウにインベントリ内のデバイスが表示されます。デフォルトでは、[Inventory] は [Focus] ドロップダウンリストから選択されます。

ステップ 2 **C9800-40-CVD.cagelab.local** のチェックボックスを見つけてオンにします。

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。

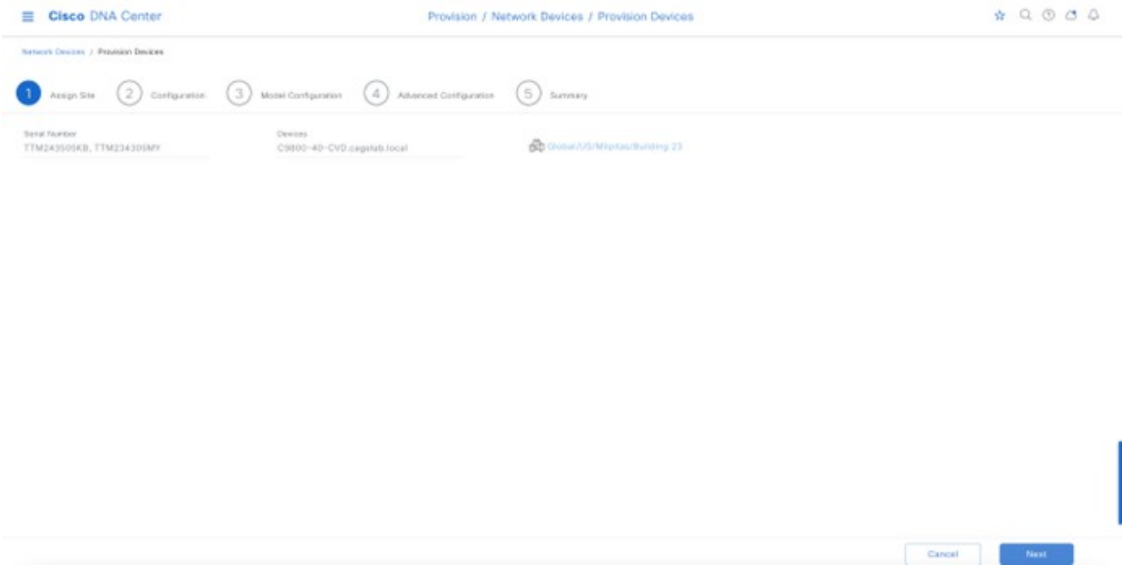
エンタープライズ ワイヤレスコントローラ HA SSO ペア（C9800-40-CVD.cagelab.local）をプロビジョニングするための 4 つのステップから成るワークフローが表示されるので、[Assign Site] から開始します。

ステップ 4 [Assign Site] ウィンドウで [Choose a Site] をクリックします。Cisco DNA Center に設定されたサイト階層を示すスライドインペインが表示されます。

この導入ガイドでは、エンタープライズ ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）がビルディングレベルに割り当てられます。

ステップ 5 [Milpitas] のサイト階層を展開し、[Building 23] を選択します。

図 *86* : ビルディングレベルへのサイトの割り当て



（注）

- エンタープライズ ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）は、Cisco DNA Center サイト階層内のビルディングまたはフロアに割り当てる必要があります。この導入ガイドでは、**C9800-40-CVD.cagelab.local** が **Building 23** に割り当てられていますが、Milpitas エリアまたはサイト階層のグローバルレベルに割り当てることはできません。他のビルディングのフロアにある AP は、ワイヤレスコントローラによってサポートされています。
- ワイヤレスコントローラがサイトに割り当てられると、ワイヤレスコントローラがデバイスとして Cisco ISE に追加されます。

ステップ 6 [Save] をクリックして、**C9800-40-CVD.cagelab.local** を **Building 23** に割り当てます。

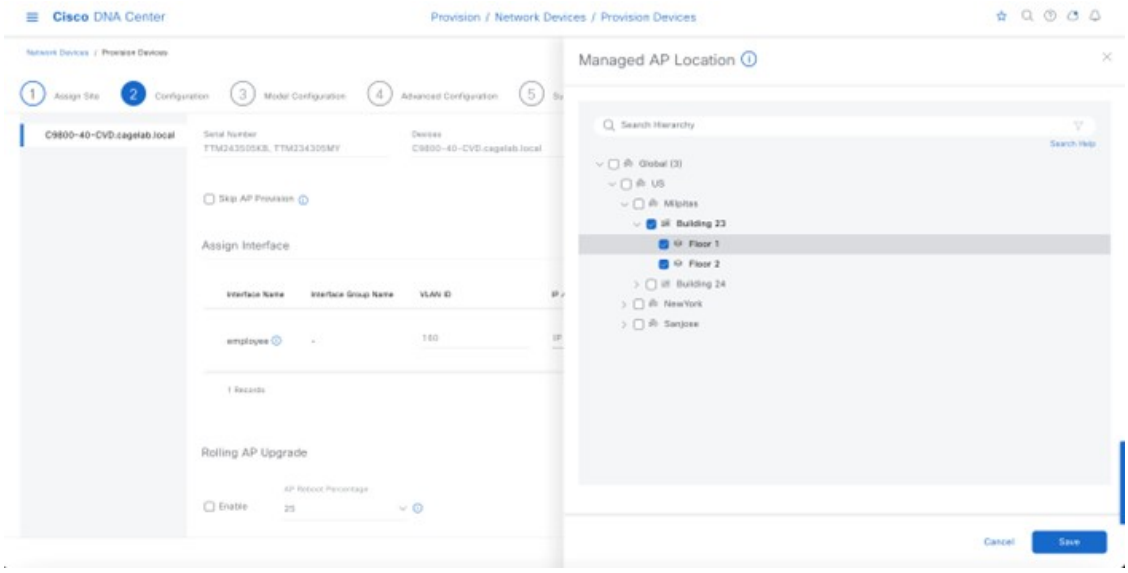
ステップ 7 **[次へ (Next)]** をクリックします。

[Configuration] ウィンドウが表示されます。

ステップ 8 [Configuration] ウィンドウで、ワイヤレスコントローラ [Role] の [Active Main] を選択します。

ステップ 9 [Select Primary Managed AP locations] をクリックします。

Cisco DNA Center のサイト階層を示す [Managed AP Location] slide-in paneが表示されます。



Cisco DNA Center は、AP の N+1 冗長性とワイヤレスコントローラの HA SSO を設定する機能をサポートしているため、プライマリとセカンダリの両方の管理対象 AP の場所を設定できます。プライマリ管理対象 AP の場所は、ビルディングやフロアを含むサイトで、ワイヤレスコントローラは AP の高可用性設定内でプライマリワイヤレスコントローラとして機能します。セカンダリ管理対象 AP の場所は、ワイヤレスコントローラが AP の高可用性設定内でセカンダリワイヤレスコントローラとして機能するサイトです。プライマリワイヤレスコントローラまたはワイヤレスコントローラの HA SSO ペアに障害が発生した場合、AP はワイヤレスコントローラへの CAPWAP 接続を再確立します。

このガイドでは、Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）がプライマリワイヤレスコントローラになり、 **Building 23** と **Building 24** の **Floor 1** と **Floor 2** の AP を管理します。ワイヤレスコントローラ HA SSO ペアは、すべての AP が集中型モード展開で動作しているキャンパスネットワークですでに冗長性を提供しているため、セカンダリ管理対象 AP の場所は設定されません。

ステップ 10 サイト階層を展開し、**Building 23** の場合は **Floors 1** と **Floor 2** を、**Building 24** の場合は **Floors 1** と **Floor 2** を選択します。

ステップ 11 [Save] をクリックします。

このワイヤレスコントローラをアクティブなメイン ワイヤレスコントローラとして選択したため、追加のフィールドが表示されます。企業のワイヤレスプロファイルでは、エンタープライズ SSID を **lab3employee** として定義し、SSID が **VLAN ID 160 の従業員**として終端するワイヤレスインターフェイスを定義しているため、このエンタープライズSSIDとワイヤレスインターフェイスは自動的に表示されます。同様に、企業のワイヤレスプロファイルではゲスト SSID が **lab3guest** として定義され、SSID が

VLAN ID 125 の guest-dmz として終端するワイヤレスインターフェイスが定義されているため、この情報も自動的に表示されます。

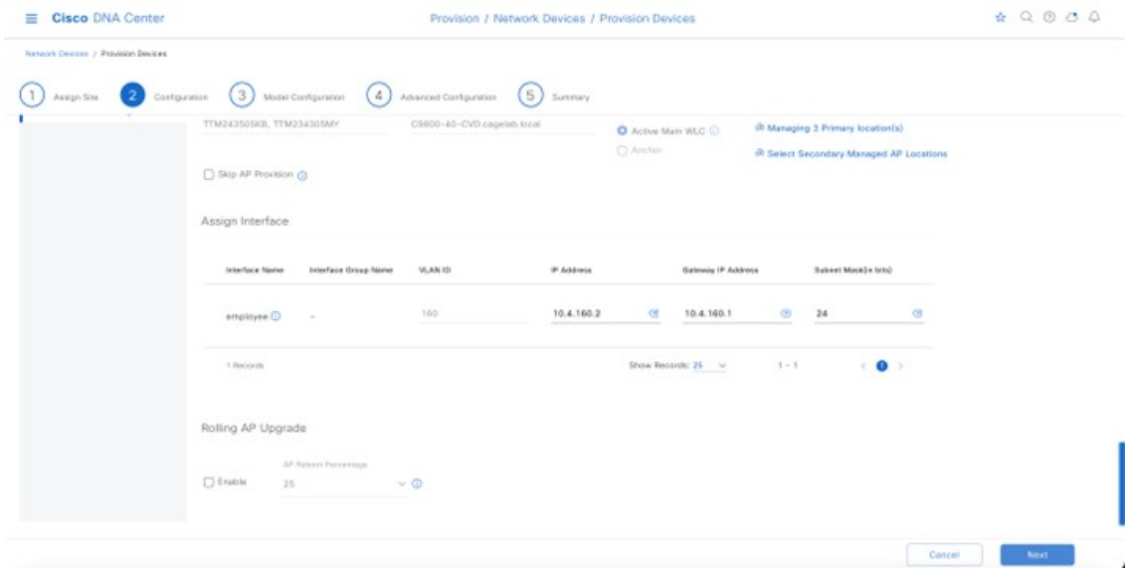
ステップ 12 各 SSID の IP アドレス、ゲートウェイ IP アドレス、LAG/ポート番号、およびサブネットマスク（ビット単位）の値を入力します。

次の表に、この導入ガイドで入力した値を示します。

表 *22*：エンタープライズ ワイヤレスコントローラの設定

フィールド	値
SSID 名	lab3employee
Interface Name	employee
VLAN ID	160
IPアドレス	10.4.160.2
Gateway IP Address	10.4.160.1
LAG/ポート番号	1
サブネットマスク（ビット単位）	24
SSID 名	lab3guest
Interface Name	Guest-dmz
VLAN ID	125
IPアドレス	10.4.125.2
Gateway IP Address	10.4.125.1
LAG/ポート番号	1
サブネットマスク（ビット単位）	24

図 *87 : Cisco DNA Center* のエンタープライズワイヤレスコントローラの設定



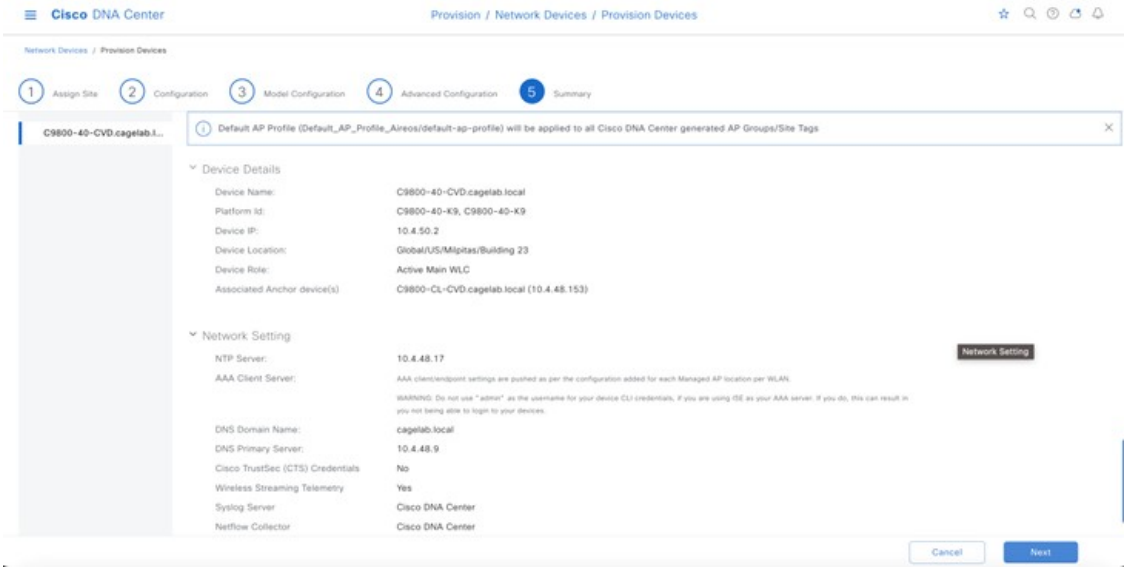
（注） guest-dmzインターフェイスは、エンタープライズフォーリンワイヤレスコントローラで定義されます。エンタープライズフォーリンワイヤレスコントローラとゲストアンカーワイヤレスコントローラの間でアンカートンネルが稼働している場合、ゲストワイヤレストラフィックはゲストアンカーワイヤレスコントローラのguest-dmzインターフェイスで自動的に終端します。ただし、アンカートンネルがダウンしている場合、ゲストワイヤレストラフィックはエンタープライズフォーリンワイヤレスコントローラのguest-dmzインターフェイスで終端します。ゲストワイヤレスデバイスにIPアドレスを提供するDHCPサーバーを使用せずに、エンタープライズ フォーリン ワイヤレスコントローラの guest-dmz インターフェイスに独立したレイヤ 2 VLAN を指定することを推奨します。指定することで、アンカートンネルがダウンしている場合、ゲストワイヤレスデバイスはネットワークアクセスのないレイヤ2サブネットに分離されます。

ステップ 13 [Next] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。デバイスタイプとサイトの [Template Editor] 内でテンプレートを設定している場合は、ここでテンプレートを適用できます。この導入ガイドでは、Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）の詳細な設定に関するテンプレートの使用については取り上げていません。

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。このウィンドウに、Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）にプロビジョニングされる設定の概要が表示されます。各セクションを展開すると、この導入ガイドの「ワイヤレスネットワークの設計」で作成された企業のワイヤレスプロファイルに基づいた設定の詳細を確認できます。



ステップ 15 [Deploy] をクリックして、Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）に設定を展開します。スライドインペインが表示され、今すぐ設定を展開するか、後で設定をスケジュールするかの確認を求められます。

（注） ベストプラクティスは、スケジュールされたネットワーク運用の変更時間帯にのみネットワークで設定を変更し、新しいデバイスをプロビジョニングすることです。

ステップ 16 [Now] オプションボタンをクリックし、[Apply] をクリックして設定を適用します。[Provisioning] 内の [Inventory] ウィンドウにリダイレクトされます。デバイスのプロビジョニングステータスは一時的に [Provisioning] と表示されますが、数分後に [Success] に変わります。詳細については、デバイスのプロビジョニングステータスの下にある [See Details] をクリックして確認してください。

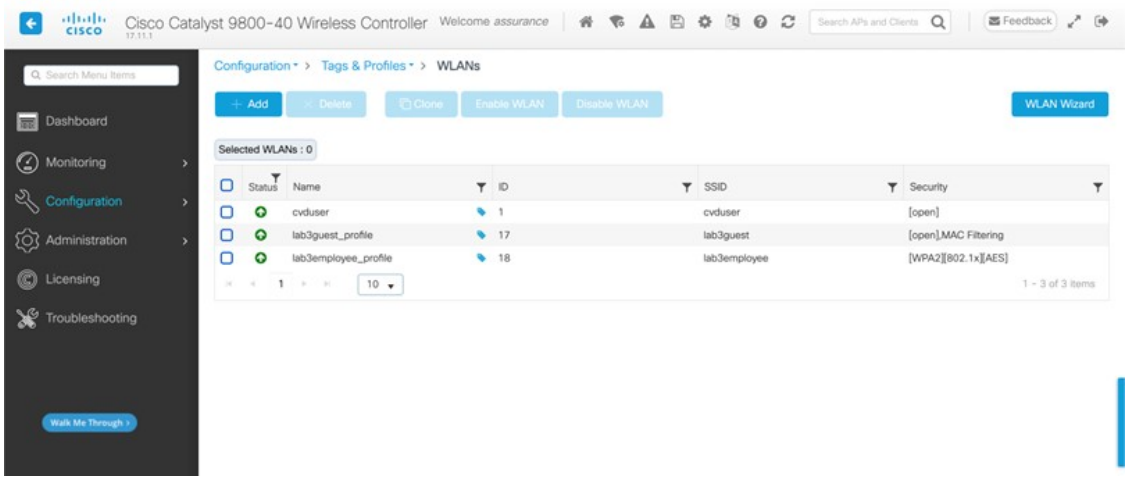
Cisco DNA Center では、Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）内に 2 つの新しい WLAN プロファイルが動的に作成されます。各 WLAN プロファイルには、企業のワイヤレスプロファイルで指定された SSID 名に基づいて動的に生成された名前があります。次の表に、この導入ガイドの **C9800-40-CVD.cagelab.local** のプロビジョニング中に Cisco DNA Center によって自動的に生成される WLAN プロファイルの名前と各プロファイルの SSID を示します。

表 *23 : Cisco DNA Center* によって動的に生成される *WLAN* プロファイル

WLAN Profile Name	SSID	WLAN ID
lab3guest_profile	lab3guest	17
lab3employee_profile	lab3employee	18

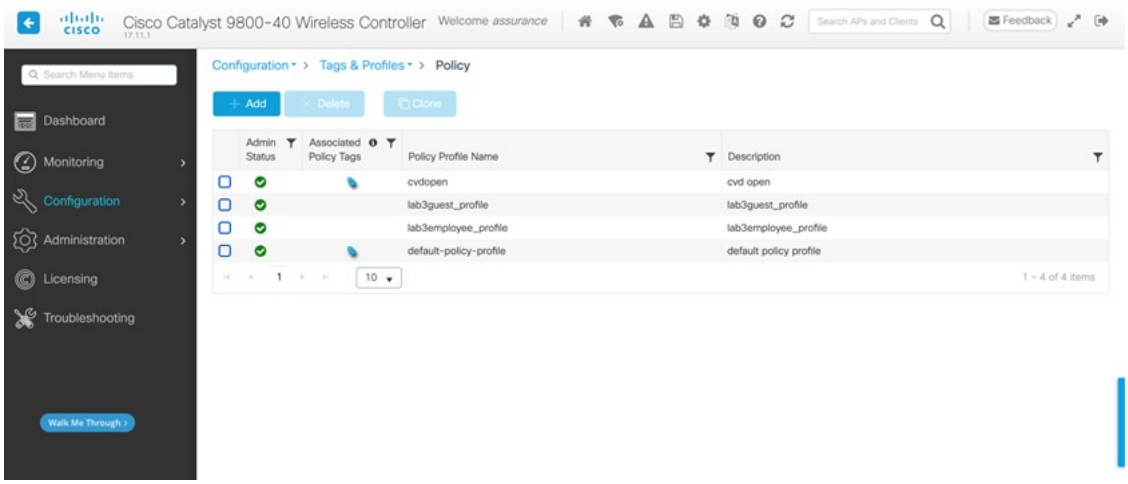
（注） ベストプラクティスは、ワイヤレスコントローラでの相互検証プロセスを容易にするために、サイトのカスタムプロファイルを作成し、ユーザーが設定したプロファイル名でポリシータグを作成することです。デフォルトのプロファイルを使用する場合、Cisco DNA Center では名前の前に SSID が付加されます。

次の図に、**C9800-40-CVD.cagelab.local** の Web ベースの GUI に表示される WLAN 設定の例を示します。



2 つの SSID（**lab3guest** と **lab3employee**）に対応する WLAN ID は、それぞれ 17 と 18 です。AP にポリシータグ **default-policy-tag** が割り当てられている場合、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに参加している AP は、ID が 1 ～ 16 の WLAN の SSID をブロードキャストします。**default-policy-tag** でブロードキャストされる WLAN ID の作成を回避するために、Cisco DNA Center では WLAN ID が 17 以上で始まる WLAN と SSID が作成されます。

Cisco DNA Center では、プロビジョニング中に **C9800-40-CVD.cagelab.local** 内に新しい 2 つのポリシープロファイルも作成されます。新しいポリシープロファイルの名前は、作成された WLAN プロファイルの名前と一致します。次の図に、**C9800-40-CVD.cagelab.local** の Web ベースの GUI に表示される設定の例を示します。



プロビジョニングプロセスのこの時点では、ポリシープロファイルと WLAN プロファイルは、AP に適用されているポリシータグにマッピングされていません。

Cisco Catalyst 9800-CL ゲストアンカー ワイヤレスコントローラのプロビジョニング

次の手順を使用して、企業のワイヤレスプロファイルを Cisco Catalyst 9800-CL ゲストアンカー ワイヤレスコントローラ（**C9800-CL-CVD.cagelab.local** と呼ばれる）にプロビジョニングします。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

メインの [Provisioning] 画面にインベントリ内のデバイスが表示されます。デフォルトでは、[Inventory] は [Focus] ドロップダウンリストから選択されます。

ステップ 2 **C9800-CL-CVD.cagelab.local** のチェックボックスを見つけてオンにします。

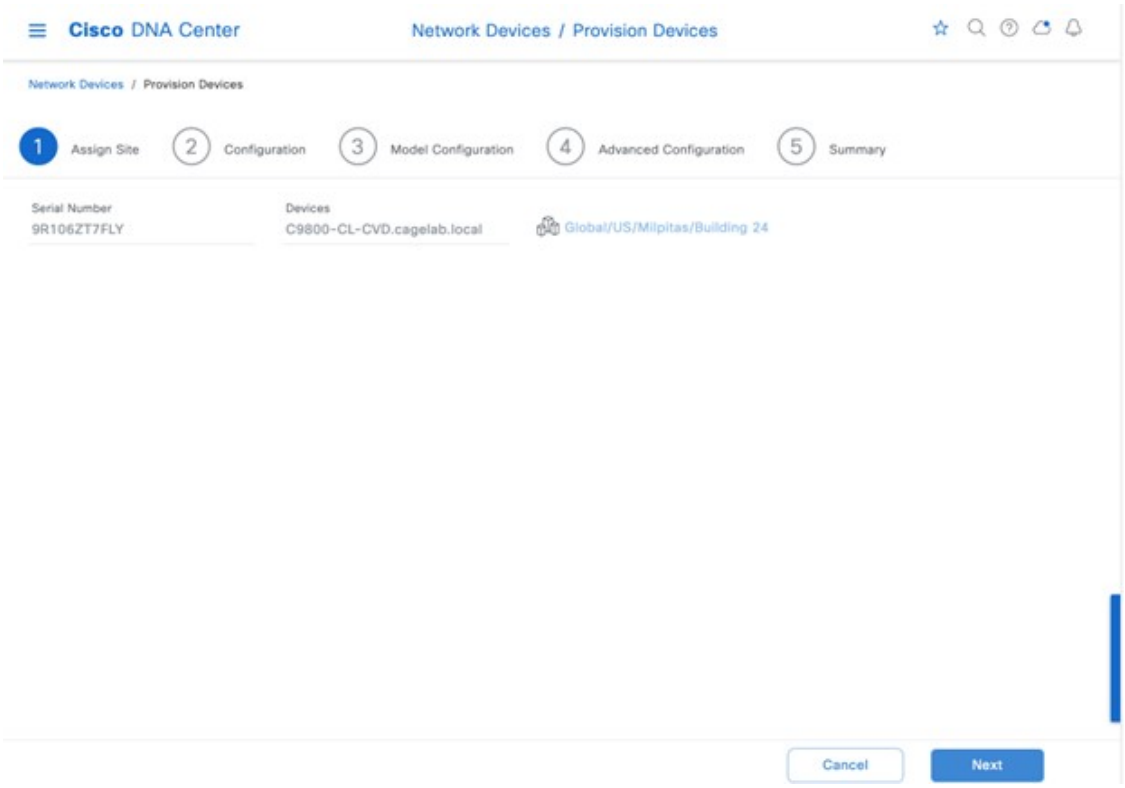
ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ゲスト ワイヤレスコントローラ（C9800-CL-CVD）をプロビジョニングするための 4 つのステップから成るワークフローが表示されるので、[Assign Site] から開始します。

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

slide-in paneが表示され、Cisco DNA Center に設定されたサイト階層が示されます。この導入ガイドでは、ゲストアンカー ワイヤレスコントローラ（**C9800-CL-CVD.cagelab.local**）がビルディングレベルに割り当てられます。

ステップ 5 [Milpitas] のサイト階層を展開し、[Building 23] を選択します。



（注）　ゲスト ワイヤレスコントローラ（**C9800-CL-CVD.cagelab.local**）は、Cisco DNA Center サイト階層のビルディングまたはフロアに割り当てる必要があります。この導入ガイドでは、**C9800-CL-CVD.cagelab.local** が **Building 23** に割り当てられていますが、コントローラを Milpitas やサイト階層のグローバルレベルに割り当てることはできません。他のビルディングのフロアにある AP は、ワイヤレスコントローラによってサポートされています。

ステップ 6　[Save] をクリックして、**C9800-CL-CVD.cagelab.local** を **Building 23** に割り当てます。

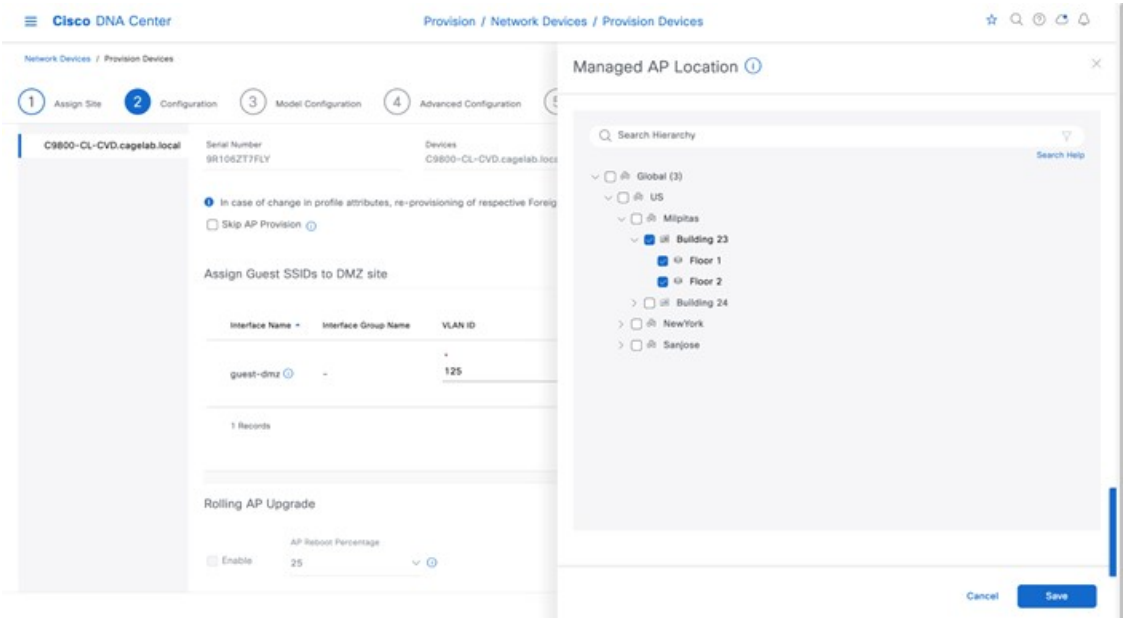
ステップ 7　**[次へ (Next)]** をクリックします。

[Configuration] ウィンドウが表示されます。

ステップ 8　[Configuration] ウィンドウで、ワイヤレスコントローラ [Role] の [Guest Anchor] を選択します。

ステップ 9　[Select Primary Managed AP locations] をクリックします。

Cisco DNA Center のサイト階層を示す [Managed AP Location] slide-in paneが表示されます。



この導入ガイドでは、ゲストアンカー ワイヤレスコントローラ（**C9800-Flex-CVD.cagelab.local**）がビルディング **branch5** の **Floor 1**、**Floor 2**、および **Floor 3** の AP を管理します。

ステップ 10　サイト階層を展開し、サイト階層内にある目的のサイトを選択します。

ステップ 11　[Save] をクリックします。

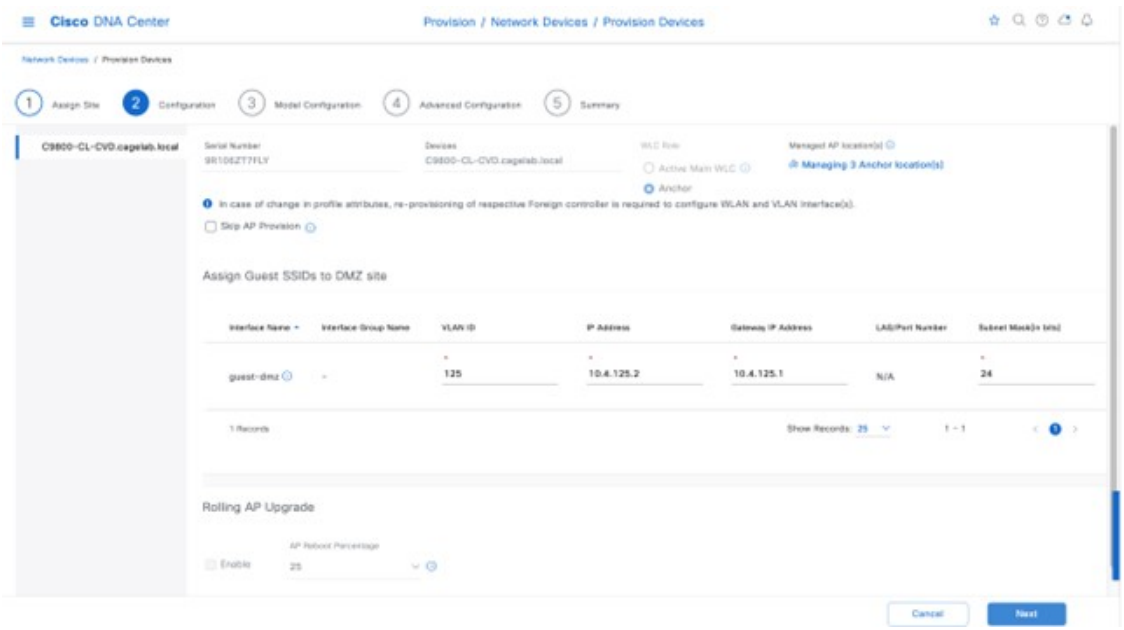
[Managed AP Location] slide-in paneが閉じます。このワイヤレスコントローラをゲスト ワイヤレスコントローラ として選択したため、追加のフィールドが表示されます。企業のワイヤレスプロファイルでは、エンタープライズ SSID が **lab3guest** として定義され、SSID が **VLAN ID 110 の branchguest-dmz** として終端するワイヤレスインターフェイスが定義されているため、このエンタープライズ SSID とワイヤレスインターフェイスは自動的に表示されます。

ステップ 12　SSID の IP アドレス、ゲートウェイ IP アドレス、LAG/ポート番号、およびサブネットマスク（ビット単位）の値を入力します。次の表に、この導入ガイドで入力した値を示します。

表 *24* : ゲスト ワイヤレスコントローラ の設定

フィールド	値
SSID 名	lab3guest
Interface Name	guest-dmz
VLAN ID	125
IPアドレス	10.4.125.2
Gateway IP Address	10.4.125.1
LAG/ポート番号	1
サブネットマスク（ビット単位）	24

図 *88* : *Cisco DNA Center* のゲスト ワイヤレスコントローラ の設定

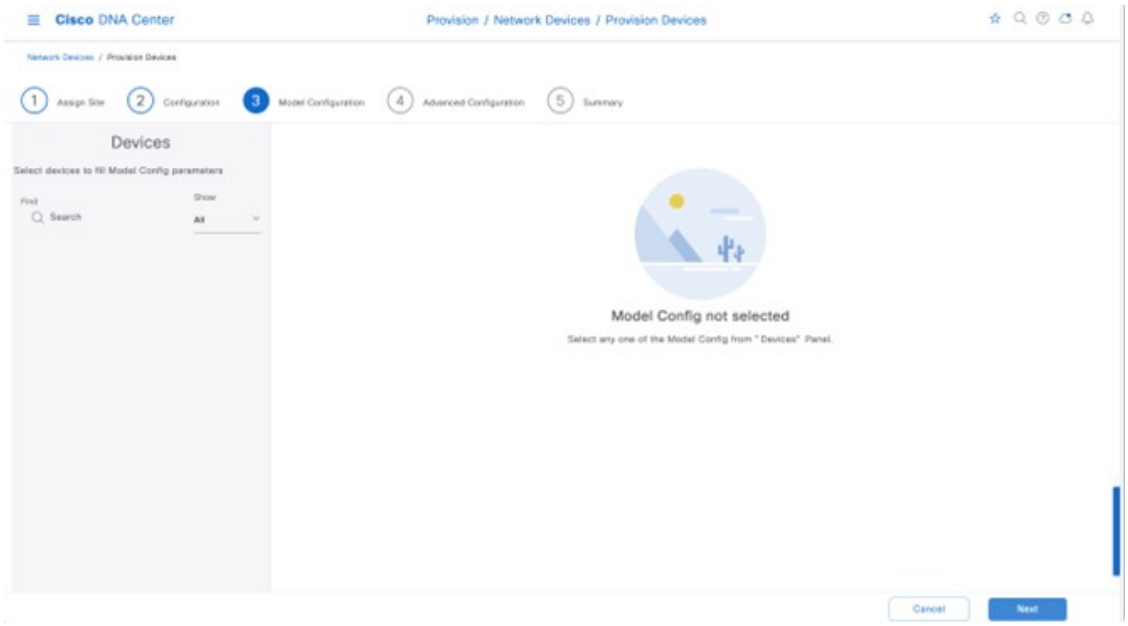


ステップ 13 [Next] をクリックします。

[Model Configuration] ウィンドウが表示されます。デバイスタイプとサイトの [Model Configs] 内でテンプレートを設定している場合は、ここでテンプレートを適用し、モデル設定を編集および表示できます。キャンパスのワイヤレス展開では、モデル設定は使用されません。

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。

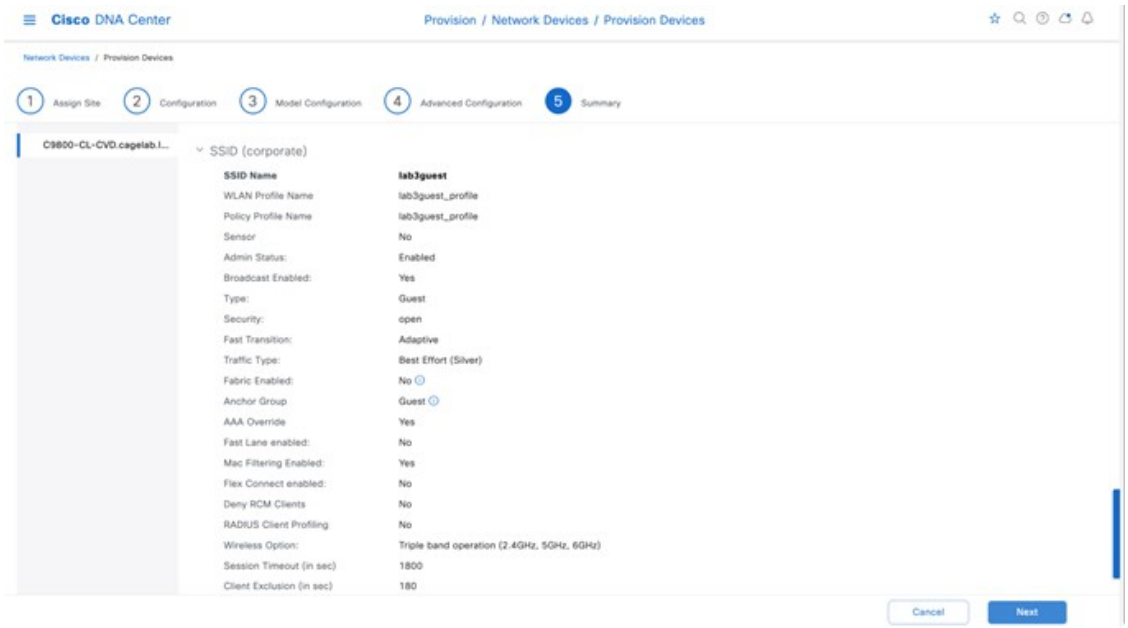


ステップ 15 デバイス プロビジョニング ワークフローで [Next] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。デバイスタイプとサイトの [Template Editor] 内でテンプレートを設定している場合は、ここでテンプレートを適用できます。この導入ガイドでは、Catalyst 9800-CL ゲスト ワイヤレスコントローラ の詳細な設定に関するテンプレートの使用については取り上げていません。

ステップ 16 デバイス プロビジョニング ワークフローで [Next] をクリックします。

[Summary] ウィンドウが表示されます。この画面には、C9800-CL-CVD にプロビジョニングされた設定の概要が表示されます。



ステップ 17 各セクションを展開すると、この導入ガイドの「ワイヤレスネットワークの設計」で作成された企業のワイヤレスプロファイルに基づいた設定の詳細を確認できます。

ステップ 18 [Next] をクリックして、設定を C9800-CL-CVD に展開します。slide-in pane が表示され、今すぐ設定を展開するか、後で設定をスケジュールするかの確認を求められます。

（注） ベストプラクティスは、スケジュールされたネットワーク運用の変更時間帯にのみネットワークで設定を変更し、新しいデバイスをプロビジョニングすることです。

ステップ 19 [Now] オプションボタンをクリックし、[Apply] をクリックして設定を適用します。[Provisioning] 内の [Inventory] ウィンドウに再度リダイレクトされます。デバイスのプロビジョニングステータスは一時的に [Provisioning] と表示されますが、数分後に [Success] に変わります。詳細については、デバイスのプロビジョニングステータスの下にある [See Details] をクリックして確認してください。

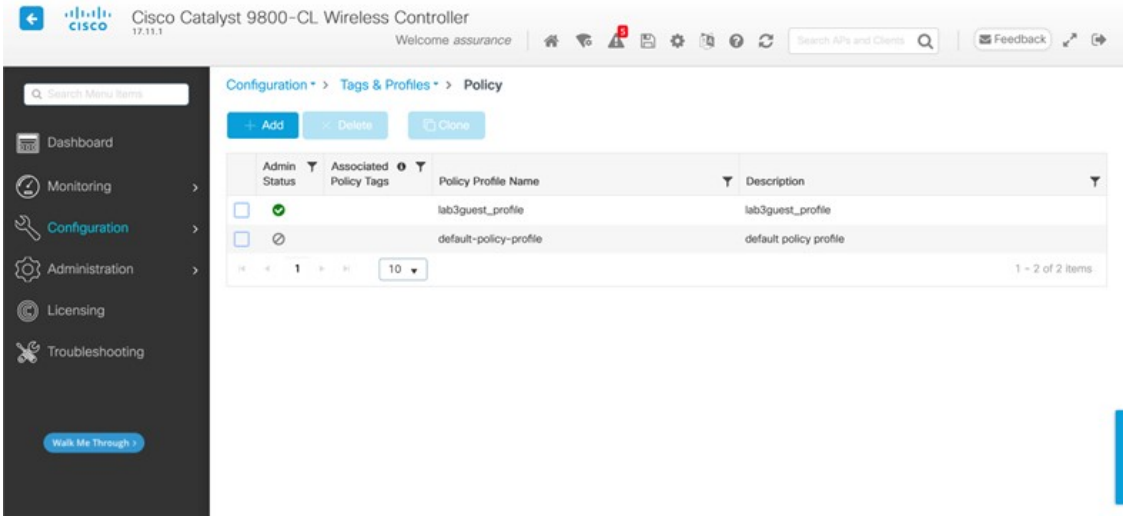
Cisco DNA Center では、Catalyst 9800-CL ゲストワイヤレスコントローラ（**C9800-CL-CVD.cagelab.local**）内に新しい WLAN プロファイルが動的に作成されます。次の表に、この導入ガイドの **C9800-CL-CVD.cagelab.local** のプロビジョニング中に Cisco DNA Center によって生成された WLAN プロファイルの名前と各プロファイルの SSID を示します。

表 *25* : ゲストアンカー ワイヤレスコントローラ の *WLAN* プロファイル

WLAN Profile Name	SSID	WLAN ID
lab3guest5_profile	lab3guest	17

WLAN プロファイル名は、企業のワイヤレスプロファイル内で指定され、この導入ガイドの「ワイヤレスネットワークの設計」で作成された SSID 名に基づいています。

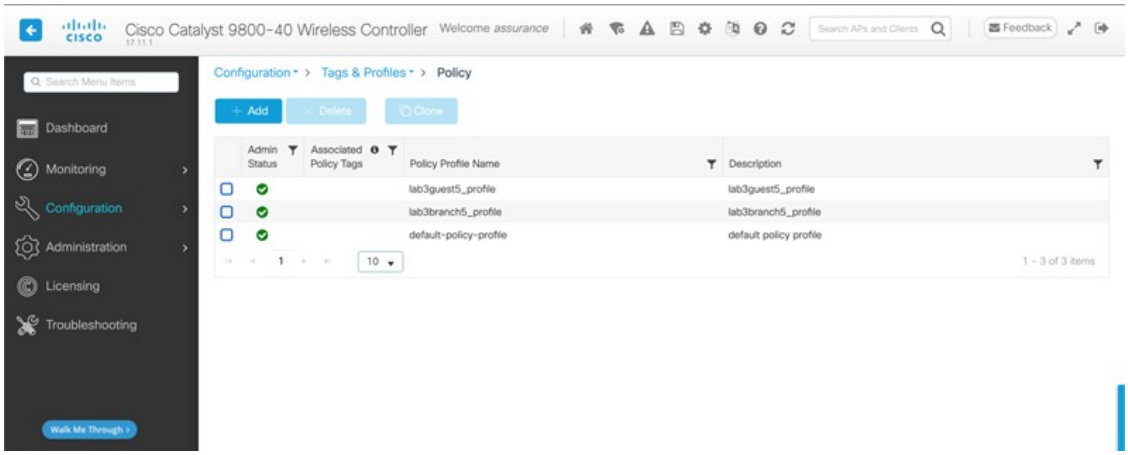
次の図に、**C9800-CL-CVD.cagelab.local** の Web ベースの GUI から表示した WLAN 設定の例を示します。



lab3guest SSID に対応する WLAN ID は 17 です。AP にポリシータグ **default-policy-tag** が割り当てられている場合、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに参加している AP は、ID が 1 ～ 16 の WLAN の SSID をブロードキャストします。**default-policy-tag** でブロードキャストされる WLAN ID の作

成を回避するために、Cisco DNA Center では WLAN ID が 17 以上で始まる WLAN または SSID が作成されます。

Cisco DNA Center では、プロビジョニング中に **C9800-40-CVD.cagelab.local** 内に新しいポリシープロファイルも作成されます。新しいポリシープロファイルの名前は、作成された WLAN プロファイルの名前と一致します。次の図に、**C9800-40-CVD.cagelab.local** の Web ベースの GUI に表示される設定の例を示します。



Cisco DNA Center では、フォーリンコントローラとして機能するエンタープライズ ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）と、アンカーコントローラとして機能するゲスト ワイヤレスコントローラ（C9800-CL-CVD.cagelab.local）の間にモビリティトンネルがプロビジョニングされます。次の図に、モビリティトンネルを示します。

図 *89 :* フォーリンコントローラのモビリティトンネル（*C9800-40-CVD.cagelab.local*）

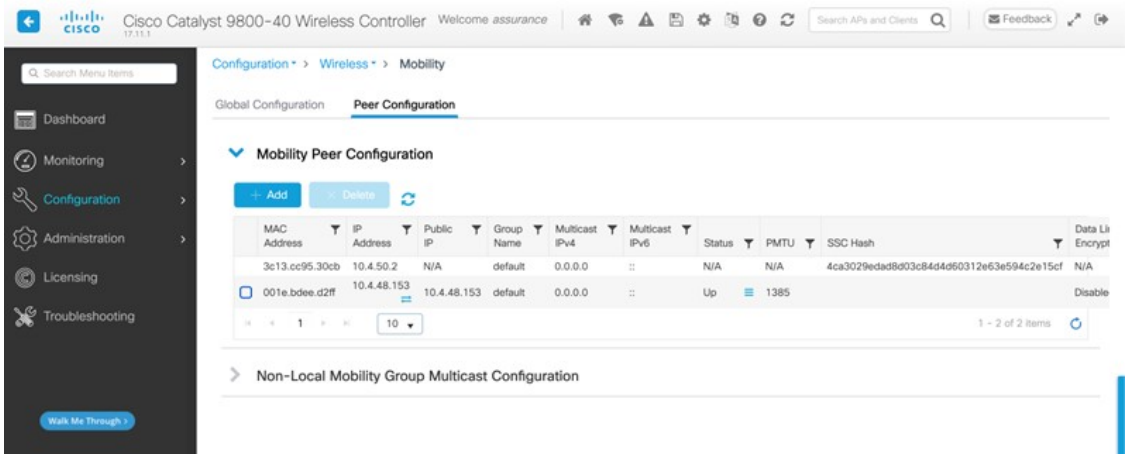
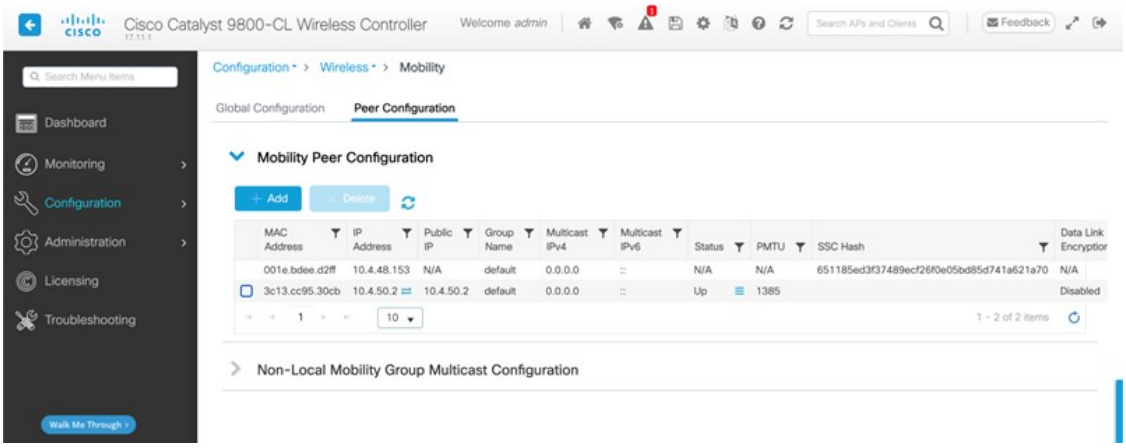


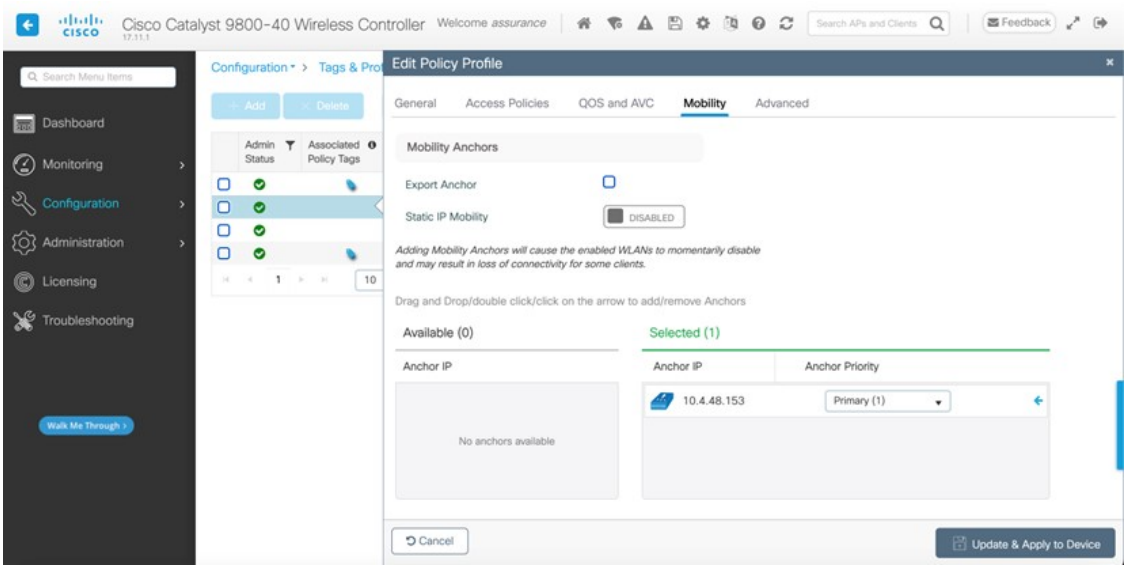
図 *90* : アンカーコントローラのモビリティトンネル（*C9800-CL-CVD.cagelab.local*）



ステップ 20 フォーリンコントローラ（**C9800-40-CVD.cagelab.local**）の [lab3guest_Profile] ポリシープロファイルをクリックし、[Mobility] ウィンドウに移動します。このウィンドウに、アンカーコントローラからポリシープロファイルへのマッピングが表示されます。

各設定は、プロビジョニング時に Cisco DNA Center によって自動的に設定されます。

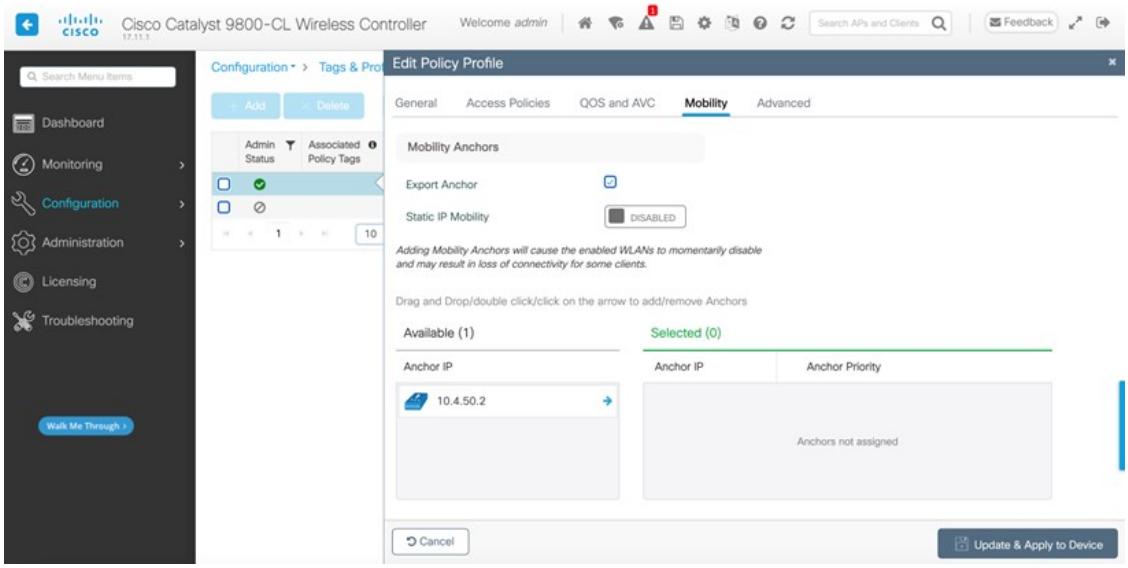
図 *91* : フォーリンコントローラ（*C9800-40-CVD.cagelab.local*）ゲストポリシープロファイルとモビリティ設定



ステップ 21 アンカーコントローラ（**C9800-CL-CVD.cagelab.local**）の [lab3guest_profile] ポリシープロファイルをクリックし、[Mobility] ウィンドウに移動します。このウィンドウに、ポリシープロファイル内のアンカーコントローラのエクスポートが表示されます（Cisco AireOS ワイヤレスコントローラ内のアンカーコントローラとフォーリンコントローラの設定と類似）。

各設定は、プロビジョニング時に Cisco DNA Center によって自動的に設定されます。

図 *92 :* モビリティ設定を含むアンカーコントローラ（***WLC-9800-CL***）ポリシープロファイル



エンタープライズ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの新しい AP の参加

次の手順では、AP を検出してエンタープライズCatalyst 9800 シリーズ ワイヤレス コントローラに参加させる方法について説明します。

始める前に

導入ガイドのこの手順では、新しい AP が IP DHCP 検出を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出し、新しい AP はまだプライミングされていないことを前提としています。以前ワイヤレスコントローラに参加（CAPWAP トンネルを確立）し、ワイヤレスコントローラ の IP アドレスを NVRAM にキャッシュしている場合、あるいは、プライマリ、セカンダリ、またはターシャリ ワイヤレスコントローラ管理 IP アドレスが AP 内で設定されている場合、その Cisco AP はプライミングされています。そのようなシナリオの AP では、IP DHCP 検出よりもプライマリ、セカンダリ、またはターシャリ ワイヤレスコントローラの設定が優先されます。

IP DHCP 検出では、DHCP サーバーはオプション 43 を使用して、1 つ以上のワイヤレスコントローラ 管理 IP アドレスを AP に提供します。AP が Catalyst 9800 シリーズ ワイヤレス コントローラの管理 IP アドレスを学習すると、ワイヤレスコントローラに CAPWAP 参加要求メッセージが送信されます。ワイヤレスコントローラが参加すると、AP の設定、ファームウェア、制御トランザクション、およびデータトランザクションが管理されます。

手順

ステップ 1 Catalyst 9800 シリーズ ワイヤレス コントローラに参加する Cisco AP をサポートするレイヤ 2 アクセススイッチで必要な VLAN を設定します。

この導入ガイドでは、APがレイヤ2アクセススイッチに接続されていることを前提としています。専用の VLAN は、PC や IP フォンなどのエンドユーザーデバイスとは別の AP 用のスイッチ上にあります。AP お

よびスイッチ管理に専用の VLAN を使用することは、一般に設計上のベストプラクティスと見なされますが、この方法ではスイッチに追加の VLAN が展開されます。

管理 VLAN（VLAN 64）は、ブランチ AP への CAPWAP トンネルを確立し、ブランチスイッチへの接続を管理するために使用されます。ブランチ従業員 VLAN（VLAN 16）は、ブランチスイッチの企業イベント SSID からのワイヤレストラフィックをローカルで終端するために使用されます。

ステップ 2 ブランチスイッチで VLAN 64 と VLAN 16 を設定します。

ステップ 3 AP が接続されているスイッチポートをトランクポートに設定し、許可されている VLAN 64 と 16 を使用して、VLAN 16 をネイティブ VLAN として設定します。スイッチポートがシャットダウンされていないことを確認します。次に設定の例を示します。

```
interface GigabitEthernet1/0/1
switchport trunk native vlan 64
switchport trunk allowed vlan 16,64
switchport mode trunk logging event trunk-status load-interval 30
no shutdown
spanning-tree portfast trunk
ip dhcp snooping trust
```

この導入ガイドでは、IP アドレス `10.4.48.9` の Microsoft Active Directory（AD）サーバーが IP DHCP サーバーとして機能します。DHCP オプション 43 内で設定された Catalyst 9800 シリーズ ワイヤレス コントローラ（AWS に展開された C9800-CL）の IPv4 アドレスは `172.38.0.10`です。Microsoft AD サーバー内の DHCP の設定は、このマニュアルの範囲外です。

次に、VLAN スイッチ仮想インターフェイス（SVI）を使用したレイヤ 3 スイッチの設定例を示します。

```
interface Vlan64
ip address 10.5.64.1
255.255.255.0
ip helper-address 10.4.48.10

interface Vlan16
ip address 10.5.16.1
255.255.255.0
ip helper-address 10.4.48.10
```

ステップ 4 Cisco AP をレイヤ 2 アクセススイッチのスイッチポートに接続します。

AP は IP アドレスを取得し、Catalyst 9800 シリーズ ワイヤレス コントローラに自動的に参加する必要があります。新しい AP がワイヤレスコントローラに登録されると、Cisco DNA Center での再同期が自動的にトリガーされます。再同期が完了すると、新しい AP がインベントリに表示されます。あるいは、次の手順を使用して、ワイヤレスコントローラのインベントリを手動で再同期できます。

1. 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。
2. デバイス名のチェックボックスをオンにします。
3. [Actions] ドロップダウンリストから [Inventory] > [Resync Device] の順に選択します。
4. 警告ウィンドウで [OK] をクリックして、再同期を確認します。

Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）を再同期すると、ワイヤレスコントローラに参加している AP がインベントリ内に表示されます。

新しい AP のプロビジョニング

アクセスポイント（AP）が Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）に参加したら、その AP をプロビジョニングする必要があります。AP が正しい設定を受信して **lab3employee** および **lab3guest** SSID をアドバタイズするためには、Cisco DNA Center を使用してプロビジョニングする必要があります。

次の表に、この導入ガイドでプロビジョニングされている AP と各 AP の場所を示します。

AP 名	AP Model	ロケーション
mil23-floor1-ap1	C9130AXI-B	Building 23、Floor 1
mil23-floor1-ap2	C9130AXI-B	Building 23、Floor 1
mil23-floor2-ap1	C9130AXI-B	Building 23、Floor 2
mil24-floor1-ap1	C9124AXD-B	Building 24、Floor 1
mil24-floor2-ap1	C9124AXD-B	Building 24、Floor 2
AP1416.9D7C.16FC	C9130AXI-B	Branch 5、Floor 1
AP1416.9D7C.16F8	C9130AXI-B	Branch 5、Floor 2

（注） この導入ガイドでは、ビルディングとフロア全体に展開された AP の組み合わせは、別の場所にある異なる AP モデルのプロビジョニングを示しており、すべて同じ Catalyst 9800 シリーズ HA SSO ワイヤレスコントローラペアによって制御されます。一般的な展開では、同じ AP モデルがフロアと展開全体に展開されます。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

メインの [Provisioning] 画面にインベントリ内のデバイスが表示されます。デフォルトでは、[Focus] は [Inventory] に設定されます。

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

ステップ 3 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

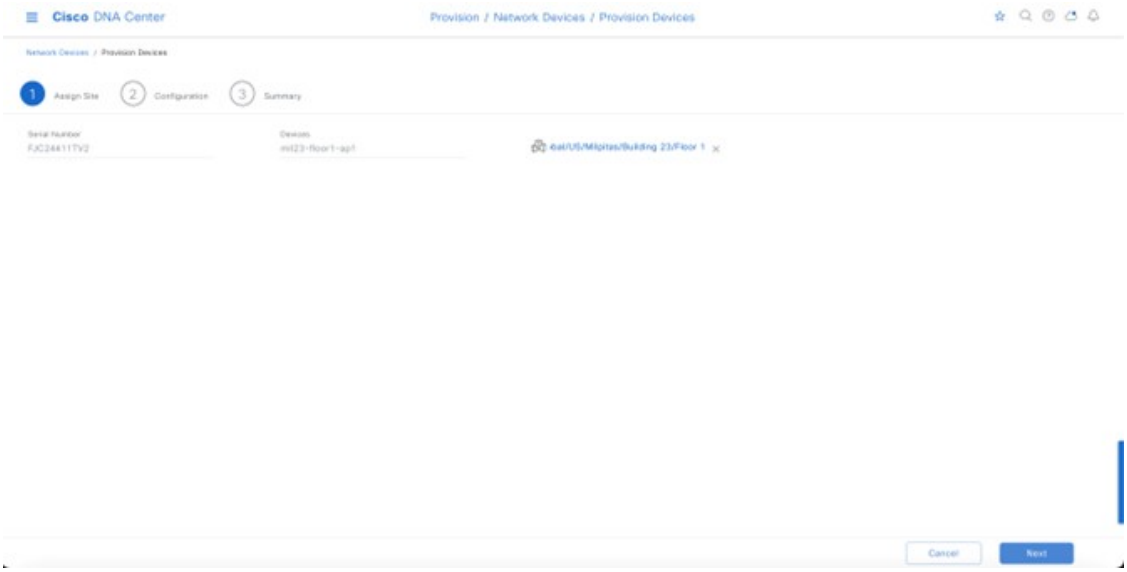
AP をプロビジョニングするためのワークフローが表示され、[Assign Site] が開始されます。

ステップ 4 AP ごとに、[Choose a Site] をクリックします。

サイドパネルが表示され、Cisco DNA Center に設定されたサイト階層が表示されます。

Milpitas のサイト階層を展開し、各 AP のビルディング（**Building 23** または **Building 24**）とフロア（**Floor 1** または **Floor 2**）を選択します。

図 *93 : AP* のプロビジョニングステップ *1* : サイトの割り当て



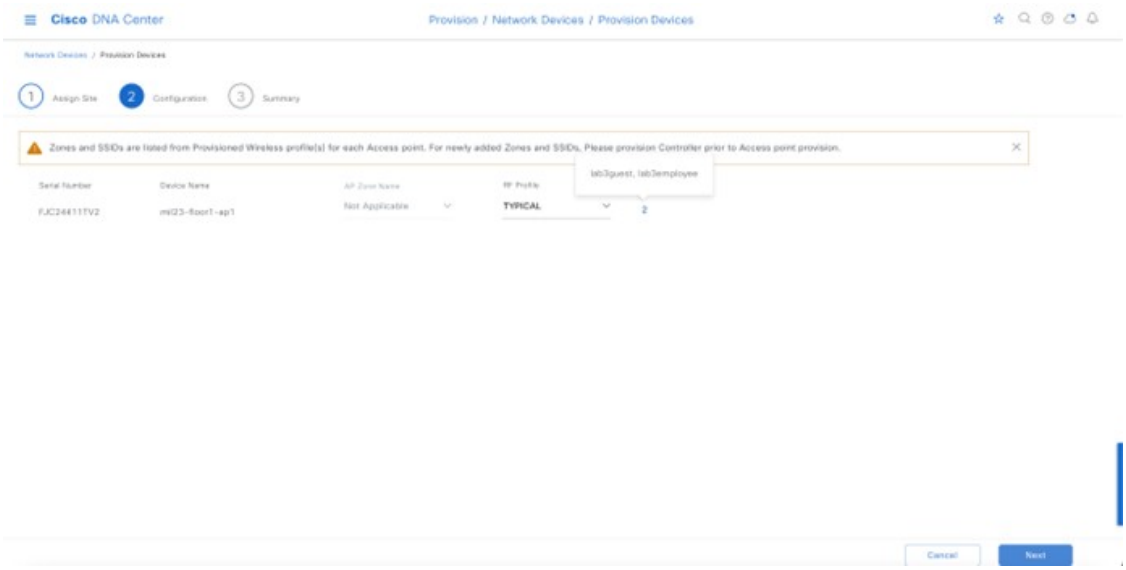
ステップ 5 [Save] をクリックします。

ステップ 6 [Next] をクリックして、設定をセットアップします。

ステップ 7 [RF Profile] のドロップダウンメニューから、各 AP に割り当てる RF プロファイルを選択します。

この導入ガイドでは、TYPICAL RF プロファイルが選択されています。TYPICAL RF プロファイルは 、「ワイヤレスネットワークの設計」でもデフォルトの RF プロファイルとして選択されています。

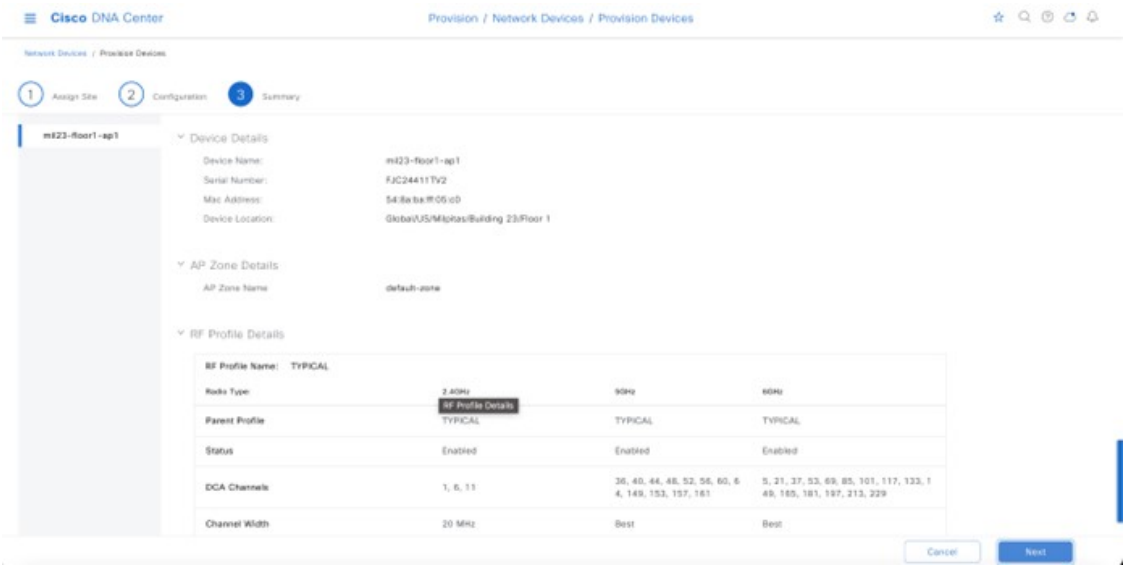
図 *94 : AP* のプロビジョニングステップ *2* : 設定



ステップ 8 [Next] をクリックします。

[Summary] 画面が表示され、各 AP にプロビジョニングされる設定の詳細が示されます。

図 *95 : AP* のプロビジョニングステップ *3* : 概要



ステップ 9 [Deploy] をクリックして、AP をプロビジョニングします。

slide-in pane が表示されます。設定を今すぐ展開することも、後で設定をスケジュールすることもできます。

ベストプラクティスは、スケジュールされたネットワーク運用の変更時間帯にのみネットワークで設定を変更し、新しいデバイスをプロビジョニングすることです。

次のメトリックは、推奨されるスケール制限を示しています。推奨値以外の場合、ワイヤレスコントローラは機能しますが、コントローラは最適なパフォーマンスを下回って動作します。

表 *26 :* ローカルモードでサイトタグごとに推奨される *AP* の最大数

プラットフォーム	AP の数
C9800-90	1,600 AP/タグ
C980040	800 AP/タグ
C9800-CL（中規模および大規模）	1,600 AP/タグ
その他の C9800 プラットフォーム	500 AP/タグ

表 *27 : Flex* モードでサイトタグごとに推奨される *AP* の最大数

プラットフォーム	AP の数
すべて	100 AP/タグ

表 *28* : サイトタグの推奨数

プラットフォーム	サイトタグの数
C9800-80	8
C980040	5
C9800-CL（中規模）	3
C9800-CL（大規模）	7

ステップ 10 [Now] を選択し、[Apply] をクリックして設定を適用します。

[Success] ダイアログボックスが表示され、プロビジョニング後に AP が再起動することが示されます。

ステップ 11 [OK] をクリックします。

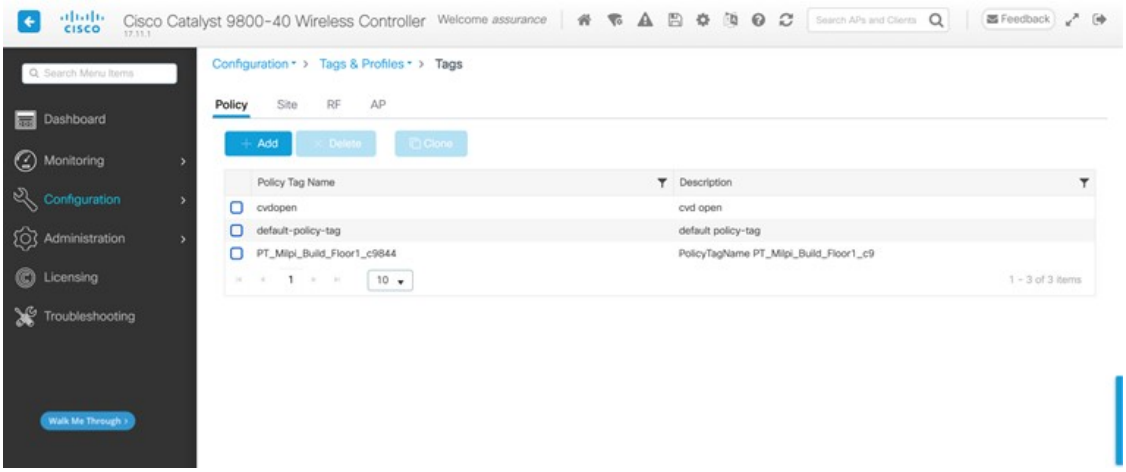
メインの [Provisioning] ウィンドウに、インベントリのリストが表示されます。

AP のプロビジョニングステータスは一時的に [Provisioning] と表示されますが、数分後に [Success] に移行します。詳細については、各 AP のプロビジョニングステータスのすぐ下にある [See Details] をクリックして確認してください。

Cisco DNA Center では、プロビジョニングされた AP を含む各フロアの Catalyst 9800-40 エンタープライズ ワイヤレス コントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）内に新しいポリシータグが作成されます。

たとえば、次の図では、**Building 23** の**Floor 1** にプロビジョニングされた AP に対応する 3 つの新しいポリシータグが作成されています。各ポリシータグはサイトに固有であり、ビルディング内の特定のフロアを示します。フロアのポリシータグは、AP がフロアにプロビジョニングされるときに Cisco DNA Center によって作成されます。

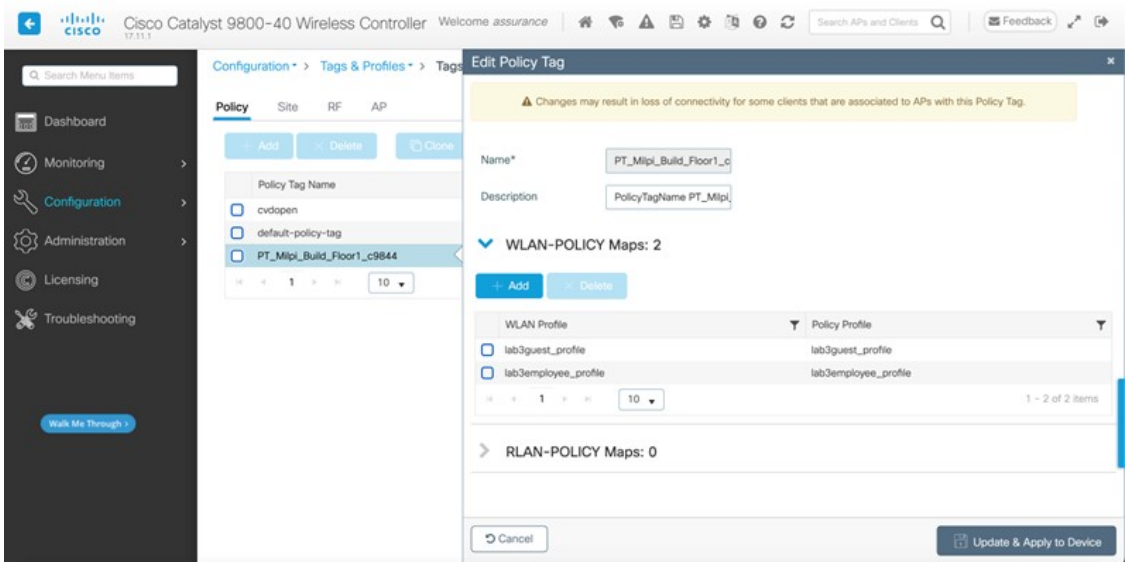
図 *96 : Catalyst 9800-40* エンタープライズ ワイヤレスコントローラで *Cisco DNA Center* によって作成されたポリシータグ



いずれかのポリシータグをクリックすると、Cisco DNA Center によって新しいポリシータグに追加されたポリシープロファイルと WLAN プロファイルが表示されます。

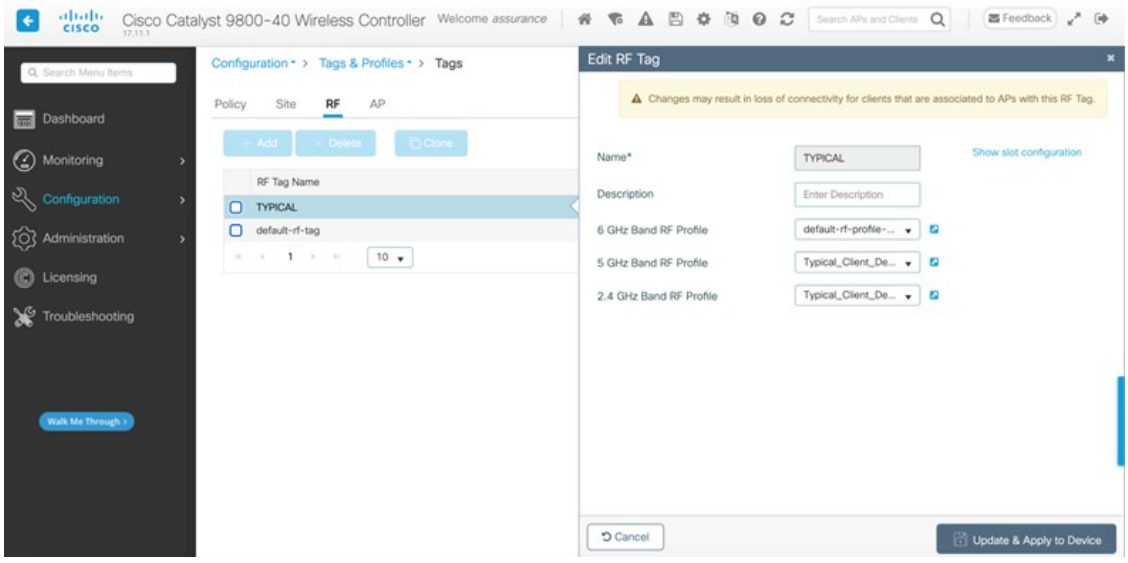
Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペアのプロビジョニング中に作成された WLAN プロファイルとポリシープロファイルが、各ポリシータグに追加されています。ポリシータグは、Cisco DNA Center で作成された企業 WLAN プロファイルによって制御されます（「ワイヤレスネットワークの設計」を参照）。企業 WLAN プロファイルでは、**lab3employee** および **lab3guest** SSID が Milpitas エリア（**Building 23** の **Floor 1**）全体にブロードキャストされるように指定されています。

図 *97 :* ポリシータグの詳細



AP のプロビジョニングプロセス中に、TYPICAL RF プロファイルが選択され、Cisco DNA Center により、Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）内に TYPICAL という名前の新しい RF タグが作成されます。

図 *98 : Cisco DNA Center* によって作成された *TYPICAL RF* タグ



最後に、Cisco DNA Center により、ポリシータグ（各フロアに固有）、RF タグ（AP のプロビジョニング中に指定された唯一の RF プロファイルであるため、TYPICAL という名前）、およびサイトタグ（ST_Milpi_Building_e3b46_0 という名前）が Catalyst 9800 エンタープライズ ワイヤレスコントローラ HA SSO ペア（C9800-40-CVD.cagelab.local）内の各 AP に静的に割り当てられます。サイトタグ ST_Milpi_Building_e3b46_0 には、default-ap-profile という名前のデフォルトの AP 参加プロファイルが含まれています。

図 *99 : Cisco DNA Center* によって作成されたサイトタグ

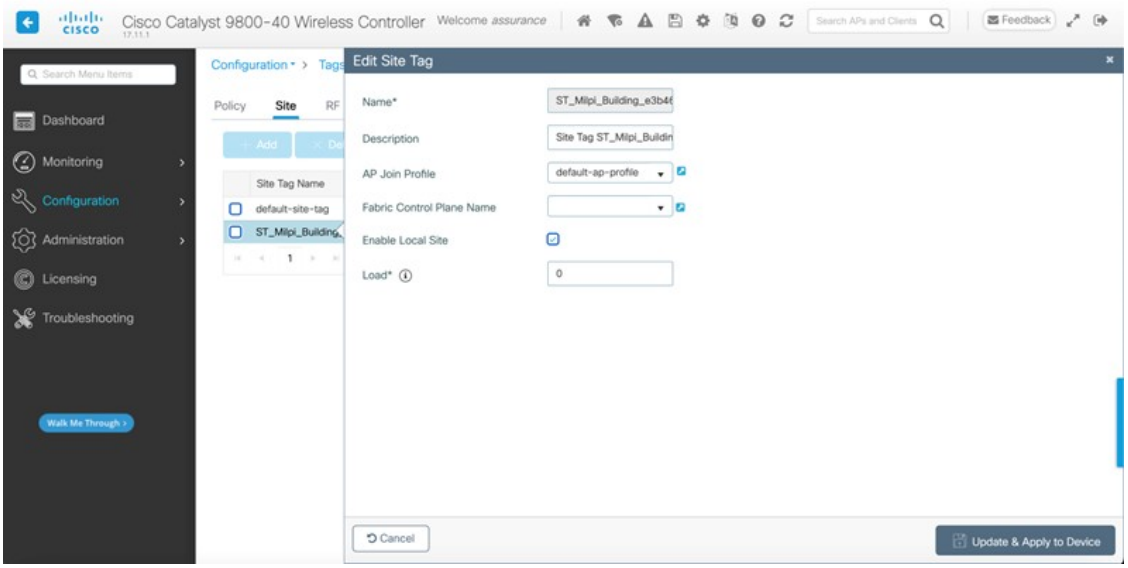
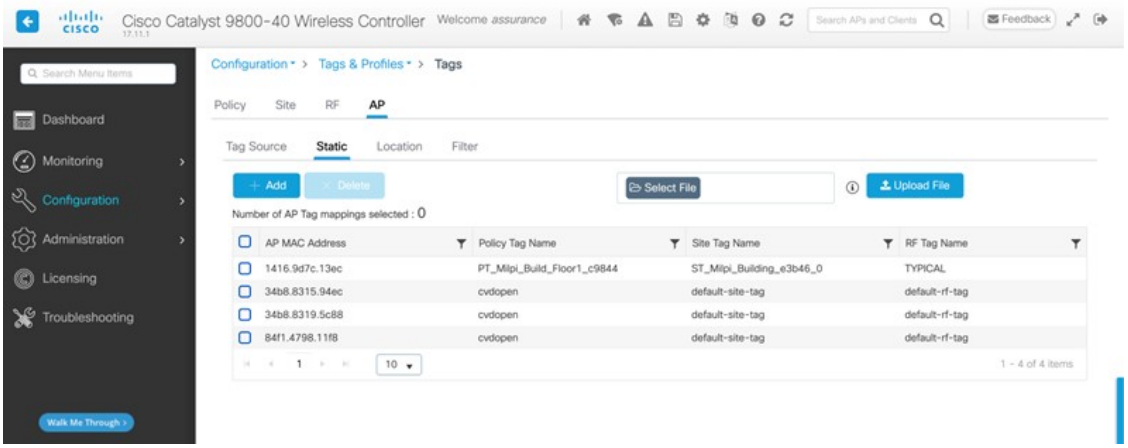


図 *100 : Cisco DNA Center* による *AP* へのタグの静的割り当て



AP にポリシータグを割り当てると、フロアにプロビジョニングされた AP によって、**lab3employee** および **lab3guest** SSID がブロードキャストされます。この時点で、ワイヤレスクライアントは **lab3employee** や **lab3guest** SSID に関連付けられ、ネットワークに認証される必要があります。

計画済み AP が無いフロアマップでの新しい AP の配置

Cisco DNA Center 内の各ビルディングとフロアに対応する計画済み AP が存在しない場合は、新たに検出された AP をフロアマップに配置する必要があります。計画済み AP が新しい AP のホスト名と一致する場合、新しい AP は計画済み AP と自動的に照合され、計画済み AP に従って配置されます。

（注） 自動照合は、ネットワーク階層内のフロアを参照する場合にのみ実行されます。

展開のこの時点で、ローカルモードの AP は、Milpitas、Building 23 のフロアで SSID をブロードキャストする必要があります。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

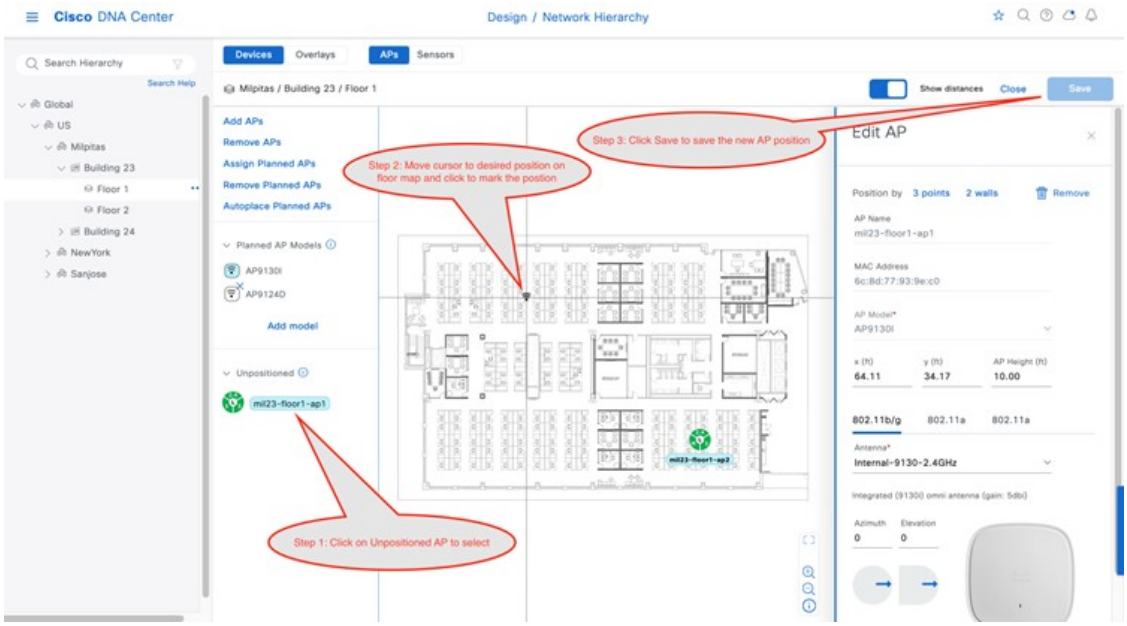
ステップ 2 左側の階層ツリーでネットワーク階層を展開し、[Milpitas] > [Building 23] > [Floor 1] の順に選択します。

Floor 1 のフロアプランが表示されます。

ステップ 3 [Add/Edit] をクリックしてフロアプランを編集します。

配置されていない AP が表示され、フロアプランのさまざまな側面を編集できます。

図 *101* : フロアプランの編集



ステップ 4 配置されていない AP を選択し、フロアマップ上の正しい位置にカーソルを移動し、クリックして目的の位置を選択します。

フロアマップが変更され、フロアマップ上の AP の位置に関する詳細が表示されます。配置する AP のモデルによっては、AP のアンテナを選択する必要があります。アンテナを選択する必要がある場合、赤色の警告が表示されます。

ステップ 5 （任意）[802.11a/b/g/n] タブをクリックして、アンテナ、方位角、および仰角の設定を表示します。

ステップ 6 [Antenna] ドロップダウンリストから、配置している AP のアンテナタイプを選択します。

この設計および導入ガイドでは、すべての AP で内部アンテナが使用されています。

ステップ 7 [802.11a] タブに対してステップ 1 ～ 6 を繰り返します。

AP をフロアマップに配置したら、位置を微調整し、AP の高さを調整できます。デフォルトの AP の高さは、フロアマップのインポート時に指定したフロアの高さに基づきます。アンテナの方位角と仰角の設定は調整できます。また、集積アンテナを使用した AP の場合は、AP の方位角と仰角を調整できます。

ステップ 8 フロア上の残りの配置されていない AP について、ステップ 1 ～ 7 を繰り返します。

ステップ 9 [Save] をクリックします。

フロアマップ上の AP の位置が保存されます。フロアマップに AP を配置すると、ヒートマップが表示されます。ヒートマップのデフォルトでは、AP RSSI 値が表示され、フロア上の各 AP のカバレッジエリアに関する概算値を得られます。ヒートマップは、2.4 GHz カバレッジ、5 GHz カバレッジ、または 2.4 GHz と 5 GHz の両方のカバレッジに対して表示できます。

ステップ 10 （任意）[Add/Edit] を再度クリックしてフロアプランを編集します。

ステップ 11 [Overlays] セクションでは、カバレッジエリア、開口部、ロケーションリージョン、壁、棚ユニット、マーカー、GPS マーカーを追加し、実際のフロアの RF 特性がより正確にフロアプランに反映されるようにポイントを調整できます。

展開のこの時点で、ローカルモードの AP は、Milpitas、Building 23 のフロアで SSID をブロードキャストする必要があります。

リモートオフィスのワイヤレス展開用エンタープライズ WLAN

ここでは、**New York** のサイトに Flex モードで AP をプロビジョニングする方法について説明します。

次の手順を使用して、**branch5** ワイヤレスプロファイルを Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ（**C9800-Flex-CVD**）にプロビジョニングします。**branch5** ワイヤレスプロファイルの詳細については、ワイヤレスネットワークの定義 （5 ページ）を参照してください。

始める前に

ワイヤレスコントローラが検出され、ソフトウェアイメージが更新されていて、高可用性（HA）ワイヤレスコントローラが設定されていることを確認します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

メインの [Provisioning] ウィンドウにデバイスが表示されます。デフォルトでは、[Focus] は [Inventory] に設定されます。

ステップ 2 Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ（**C9800-Flex-CVD**）のチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

エンタープライズ ワイヤレスコントローラ（**C9800-Flex-CVD**）をプロビジョニングするためのワークフローが表示されるので、[Assign Site] から開始します。

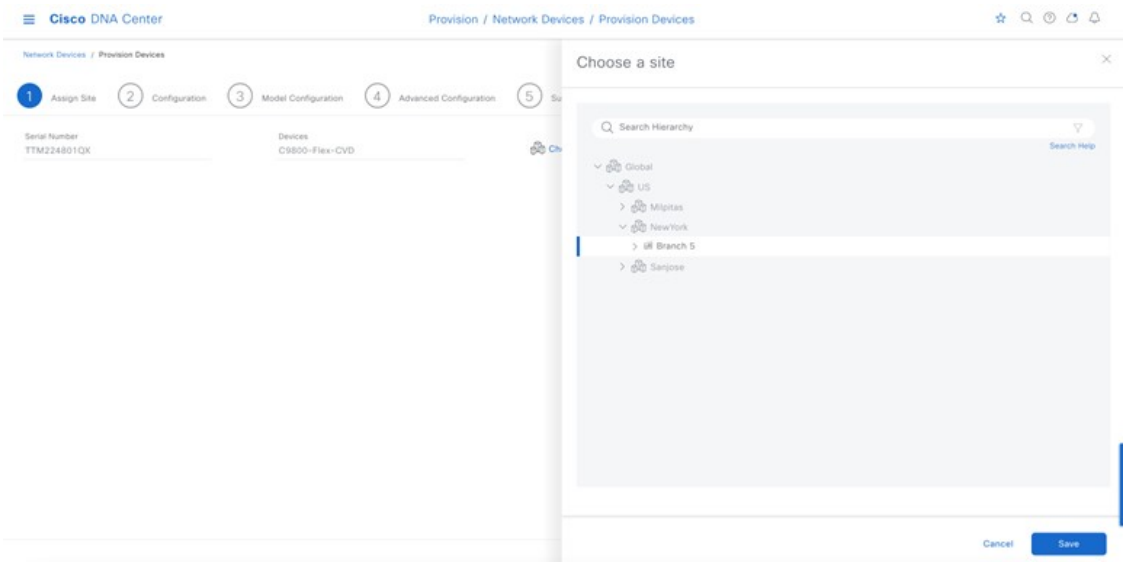
ステップ 4 [Assign Site] ウィンドウで [Choose a Site] をクリックします。slide-in paneが表示され、Cisco DNA Center に設定されたサイト階層が示されます。

エンタープライズ ワイヤレスコントローラ（**C9800-Flex-CVD**）はビルディングレベルで割り当てる必要があります。

[Choose a Site] slide-in paneで次の手順を実行します。

a) **New York** のサイト階層を展開し、[Branch 5] を選択します。

図 *102*：エンタープライズ ワイヤレスコントローラのプロビジョニング：サイトの割り当て



（注） エンタープライズ ワイヤレスコントローラ（**C9800-Flex-CVD**）は、Cisco DNA Center サイト階層内のビルディングまたはフロアに割り当てる必要があります。エリア（**New York** など）やサイト階層のグローバルレベルに割り当てることはできません。**C9800-Flex-CVD** はビルディング（このガイドでは**Branch 5**）に割り当てられますが、他のビルディングのフロアにある AP はワイヤレスコントローラによってサポートされます。

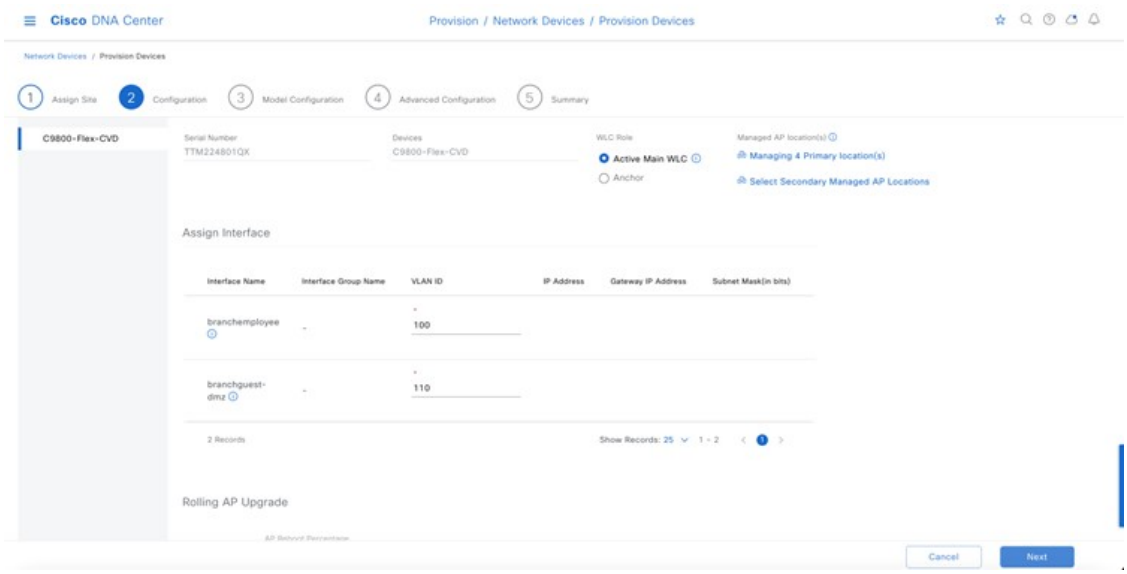
b) [Save] をクリックして、**C9800-Flex-CVD** をビルディング **Branch 5** に割り当てます。

ステップ 5 [Next] をクリックします。

ステップ 6 [Configuration] ウィンドウで、次の手順を実行します。

a) [WLC Role] の場合は [Active Main WLC] を選択します。
b) [Select Primary Managed AP locations] をクリックします。Cisco DNA Center のサイト階層を示す [Managed AP Location] slide-in paneが表示されます。

図 *103 :* エンタープライズ ワイヤレスコントローラのプロビジョニング：設定



Cisco DNA Center 2.3.5.5 リリースでは、ワイヤレスコントローラの AP および HA SSO の N+1 冗長性を設定する機能がサポートされているため、プライマリとセカンダリの両方の管理対象 AP の場所を設定できます。プライマリ管理対象 AP の場所は、AP の高可用性設定内でワイヤレスコントローラがプライマリ ワイヤレスコントローラとして機能するサイト（ビルディングやフロア）です。セカンダリ管理対象 AP の場所は、AP の高可用性設定内でワイヤレスコントローラがセカンダリ ワイヤレスコントローラとして機能するサイトです。プライマリ ワイヤレスコントローラまたはワイヤレスコントローラの HA SSO ペアに障害が発生した場合、AP はワイヤレスコントローラへの CAPWAP 接続を再確立します。

この導入ガイドでは、Catalyst 9800-40 シリーズ ワイヤレスコントローラ（**C9800-Flex-CVD**）が、**Branch 5** の **Floor 1**、**Floor 2**、および **Floor 3** 内の AP を管理するプライマリ ワイヤレスコントローラになります。ワイヤレスコントローラ HA SSO ペアは、すべての AP が集中型（ローカル）モード展開で動作しているキャンパスネットワークですでに冗長性を提供しているため、セカンダリ管理対象 AP の場所は設定されません。

c) サイト階層を展開し、**Branch 5** の **Floor 1**、**Floor 2**、**Floor 3**、および **Floor 1**、**Floor 2**、**Floor 3** を選択します。
d) [Save] をクリックします。

[Managed AP Location] slide-in paneが閉じます。ワイヤレスコントローラ を [Active Main WLC] として選択したため、ウィンドウ内に追加のフィールドが表示されます。**branch5** ワイヤレスプロファイルでは、エンタープライズ SSID が **lab3branch5** として定義され、SSID が VLAN ID 100 の **branchemployee** として終端するワイヤレスインターフェイスが定義されているため、SSID とワイヤレスインターフェイスの両方が自動的に表示されます。同様に、**corporate** のワイヤレスプロファイ

ルではゲスト SSID を **lab3guest** として定義し、SSID が VLAN ID 125 の **guest-dmz** として終端するワイヤレスインターフェイスを定義しているため、これらも自動的に表示されます。

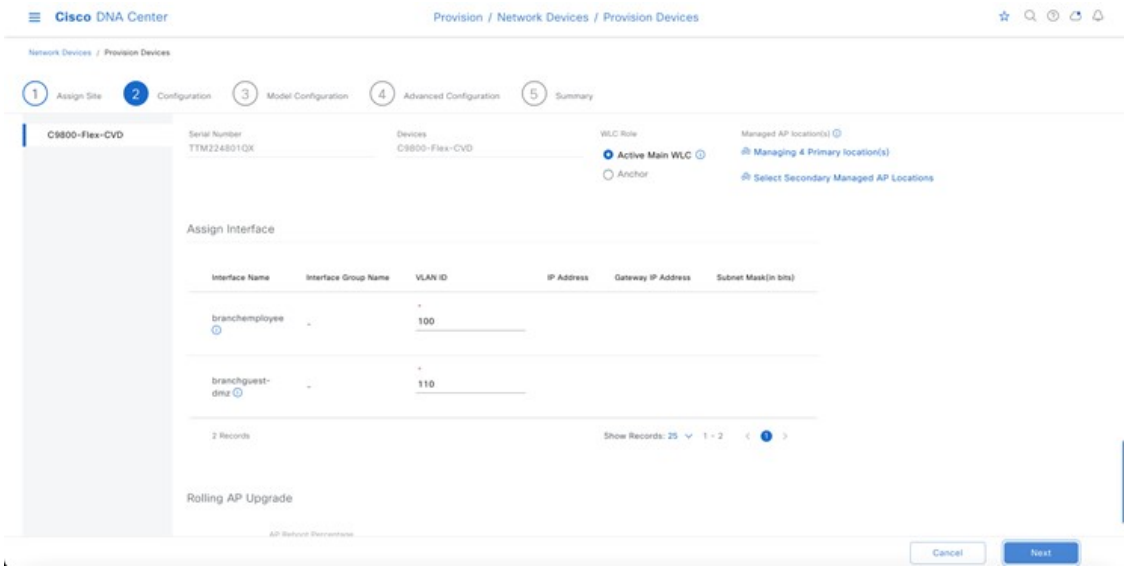
e) 各 SSID の IP アドレス、ゲートウェイ IP アドレス、LAG/ポート番号、およびサブネットマスク（ビット単位）の値を入力します。

次の表に、この導入ガイドで入力した値を示します。

表 *29 :* エンタープライズ ワイヤレスコントローラの設定

フィールド	値
SSID 名	lab3branch5
Interface Name	branchemployee
VLAN ID	100
IPアドレス	**10.4.160.2**
Gateway IP Address	**10.4.160.1**
LAG/ポート番号	1
サブネットマスク（ビット単位）	24
SSID 名	lab3guest5
Interface Name	branchguest-dmz
VLAN ID	110
IPアドレス	**10.4.125.2**
Gateway IP Address	**10.4.125.1**
LAG/ポート番号	1
サブネットマスク（ビット単位）	24

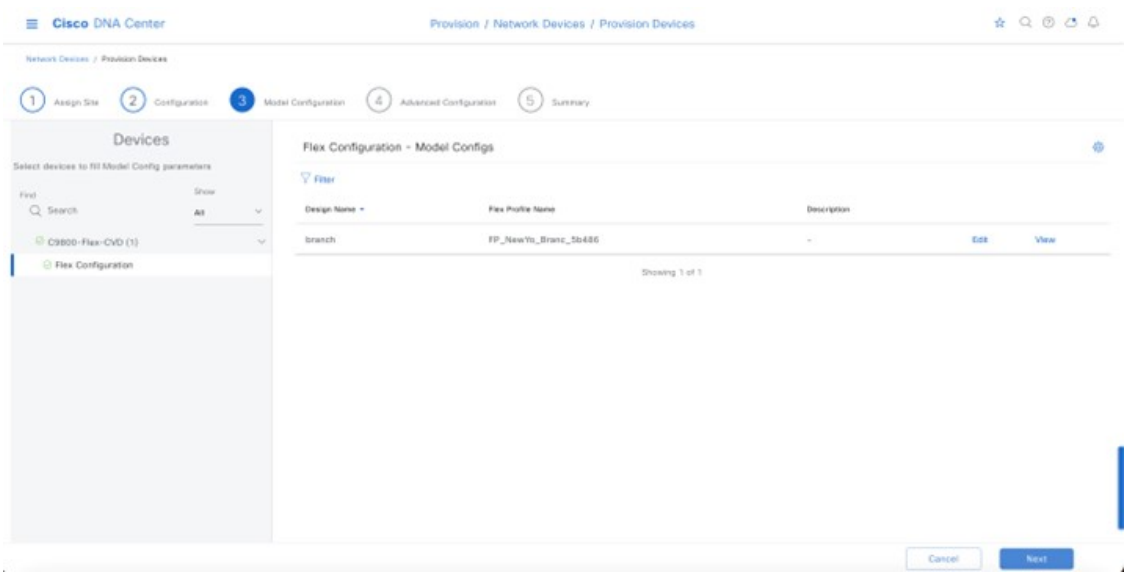
図 *104 : Cisco DNA Center* のエンタープライズ ワイヤレスコントローラの設定



f) [Next] をクリックします。

ステップ 7 [Model Configuration] ウィンドウが表示されます。デバイスタイプとサイトの [Model Configs] 内でテンプレートを設定している場合は、ここでモデル設定を適用し、Flex 設定のモデル設定を編集および表示できます。

図 *105 : Flex* モードのモデル設定



ステップ 8 [Next] をクリックします。

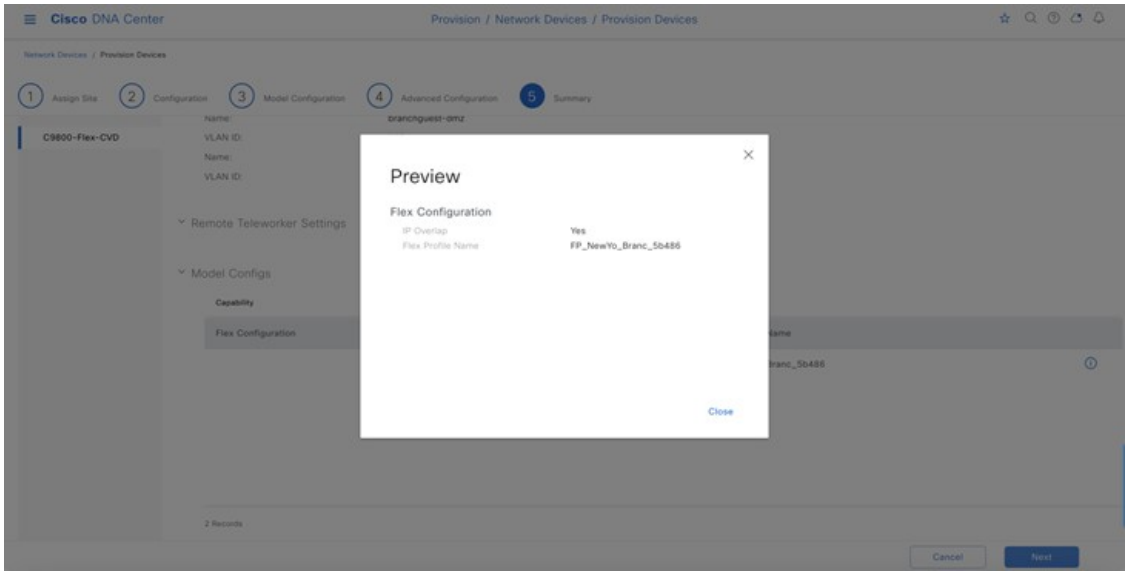
ステップ 9 [Advanced Configuration] ウィンドウが表示されます。デバイスタイプとサイトの**[Tools]** > **[Template Hub]** ウィンドウでテンプレートを設定している場合は、ここでテンプレートを適用できます。この導入ガイ

ドでは、Catalyst 9800-40 シリーズ ワイヤレスコントローラ（**C9800-Flex-CVD**）の詳細な設定に関するテンプレートの使用については取り上げていません。

ステップ 10 [Next] をクリックします。

ステップ 11 [Summary] ウィンドウが表示されます。このウィンドウに、Catalyst 9800-40 シリーズ ワイヤレスコントローラ（**C9800-Flex-CVD**）にプロビジョニングされる設定の概要が表示されます。

図 *106 : Flex* モードのデバイスプロビジョニングの概要



各領域を展開すると、設定の詳細を確認できます。設定は、このガイドの「ワイヤレスネットワークの設計」セクションで作成された **branch5** ワイヤレスプロファイルに基づいています。

ステップ 12 [Deploy] をクリックして、Catalyst 9800-40 シリーズ ワイヤレスコントローラ HA SSO ペア（**C9800-40-CVD.cagelab.local**）に設定を展開します。

（注） ベストプラクティスは、スケジュールされたネットワーク運用の変更時間帯にのみネットワークで設定を変更し、新しいデバイスをプロビジョニングすることです。また、デバイスに展開する前に設定をプレビューすることも推奨します。

ステップ 13 [Now] をクリックして設定をただちに展開するか、[Later] をクリックして後で展開をスケジュールします。

ステップ 14 [Apply] をクリックします。

[Provisioning] 内の [Inventory] ウィンドウに戻ります。

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

ステップ 15 詳細については、デバイスのプロビジョニングステータスの下にある [See Details] をクリックして確認してください。

Cisco DNA Center では、Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（**C9800-Flex-CVD**）内に 2 つの新しい WLAN プロファイルが動的に作成されます。各 WLAN プロファイルの名前は、**branch5** ワイヤレスプロファイル内で指定され、この導入ガイドの「ワイヤレスネット

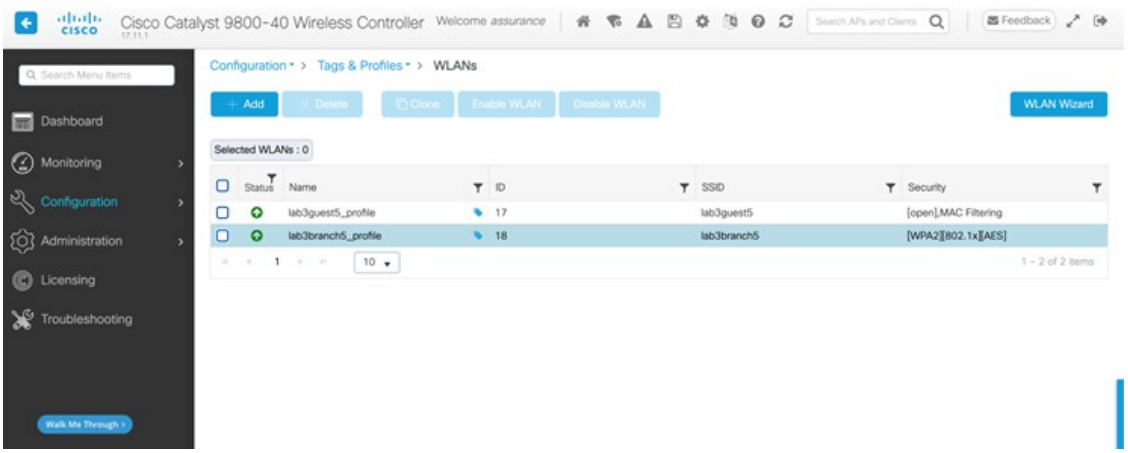
ワークの設計」で作成された SSID 名に基づいて動的に生成されます。次の表に、この導入ガイドの **C9800-40-CVD.cagelab.local** のプロビジョニング中に Cisco DNA Center によって自動的に生成される WLAN プロファイルの名前と各プロファイルの SSID を示します。

表 *30 : Cisco DNA Center* によって生成された *WLAN* プロファイル

WLAN Profile Name	SSID	WLAN ID
lab3guest5_profile	lab3guest5	17
lab3branch5_profile	lab3branch5	18

次の図に、**C9800-Flex-CVD.cagelab.local** の Web ベースの GUI における WLAN 設定の例を示します。

図 *107 : Cisco DNA Center* によって作成された *Flex WLAN/SSID*

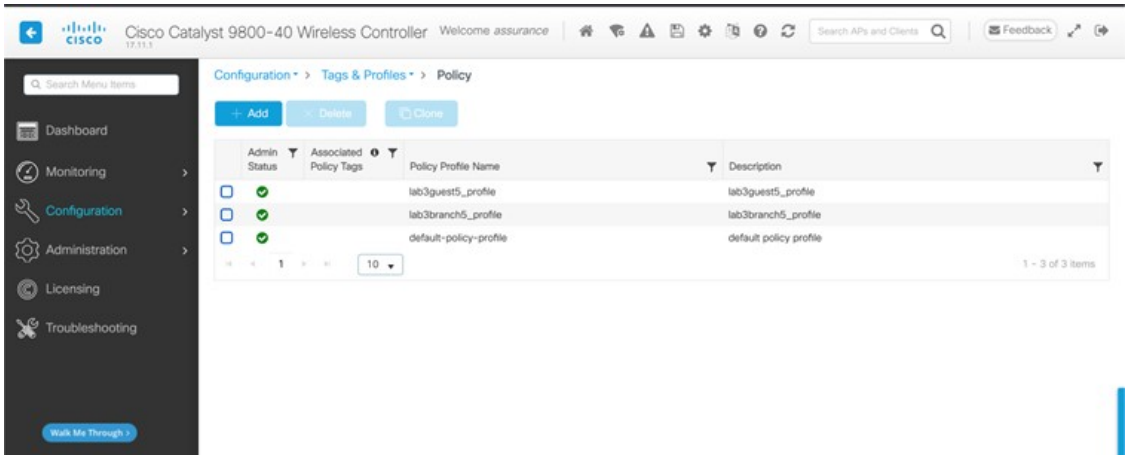


（注） 2 つの SSID（lab3guest5 と lab3branch5）に対応する WLAN ID は、それぞれ 17 と 18 です。AP に **default-policy-tag** という名前のポリシータグが割り当てられている場合、Catalyst 9800 シリーズ ワイヤレス コントローラは ID が 1 ～ 16 の WLAN の SSID をブロードキャストします。**default-policy-tag** でブロードキャストされる WLAN ID の作成を回避するために、Cisco DNA Center では WLAN ID が 17 以上で始まる WLAN/SSID が作成されます。

Cisco DNA Center では、プロビジョニング中に **C9800-Flex-CVD** 内に 2 つの新しいポリシープロファイルも作成されます。新しいポリシープロファイルの名前は、作成された WLAN プロファイルの名前と一致します。

次の図に、**C9800-Flex-CVD** の Web ベースの GUI における設定の例を示します。

図 *108 : Cisco DNA Center* によって *Flex* 用に作成された *Catalyst 9800* ワイヤレスコントローラのポリシープロファイル



プロビジョニングプロセスのこの時点では、ポリシープロファイルと WLAN プロファイルは、AP に適用されているポリシータグにマッピングされていません。コントローラでは、Cisco DNA Center は Cisco DNA Center によって生成された名前で Flex プロファイルを作成します。

図 *109 : [Flex Profile]* ウィンドウ

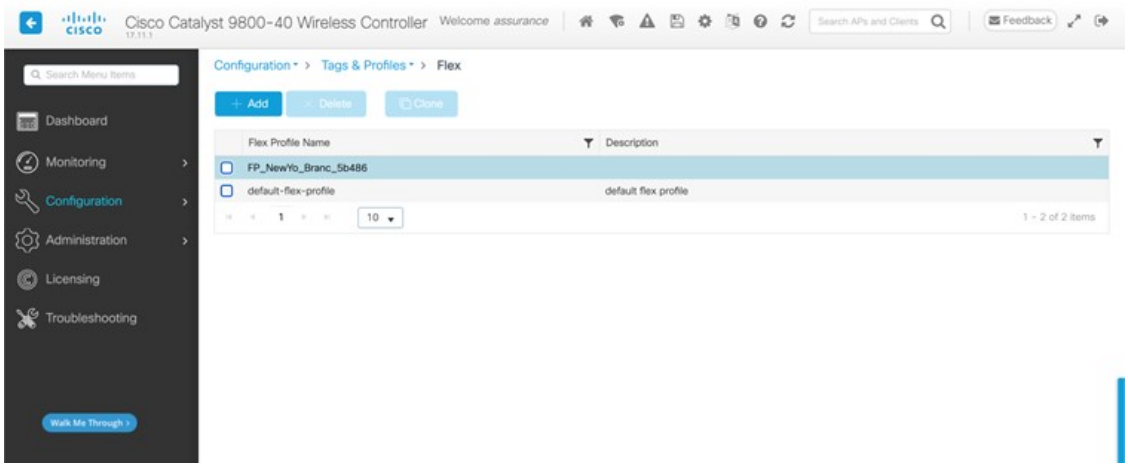
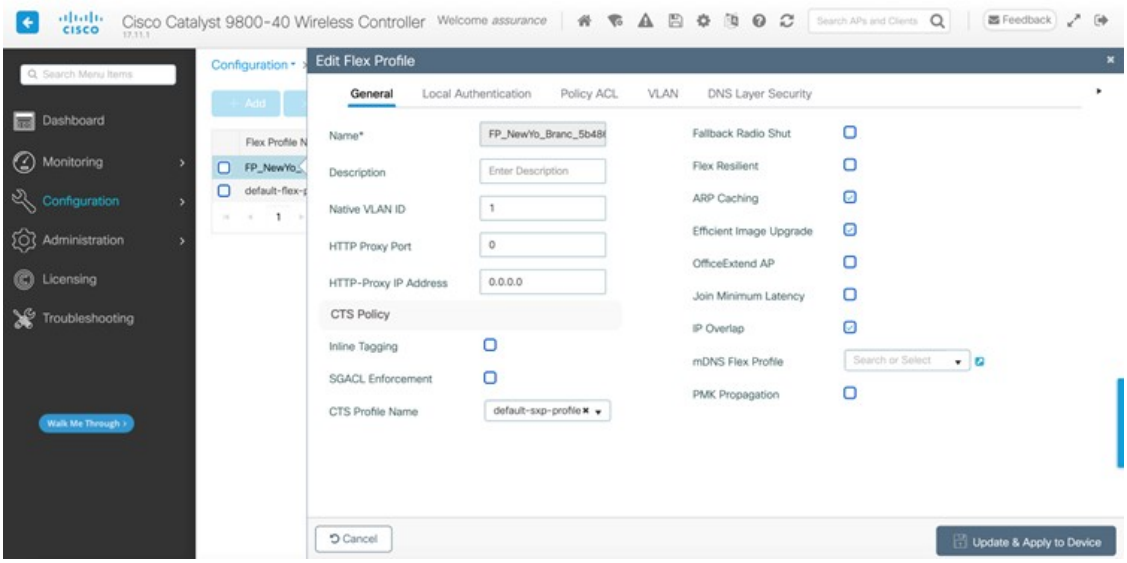


図 *110 : [Edit Flex Profile]* ダイアログボックス



N+1 ワイヤレスコントローラの AP のプロビジョニング

次の手順では、N+1 ワイヤレスコントローラに関連付けられた AP をプロビジョニングする方法について説明します。

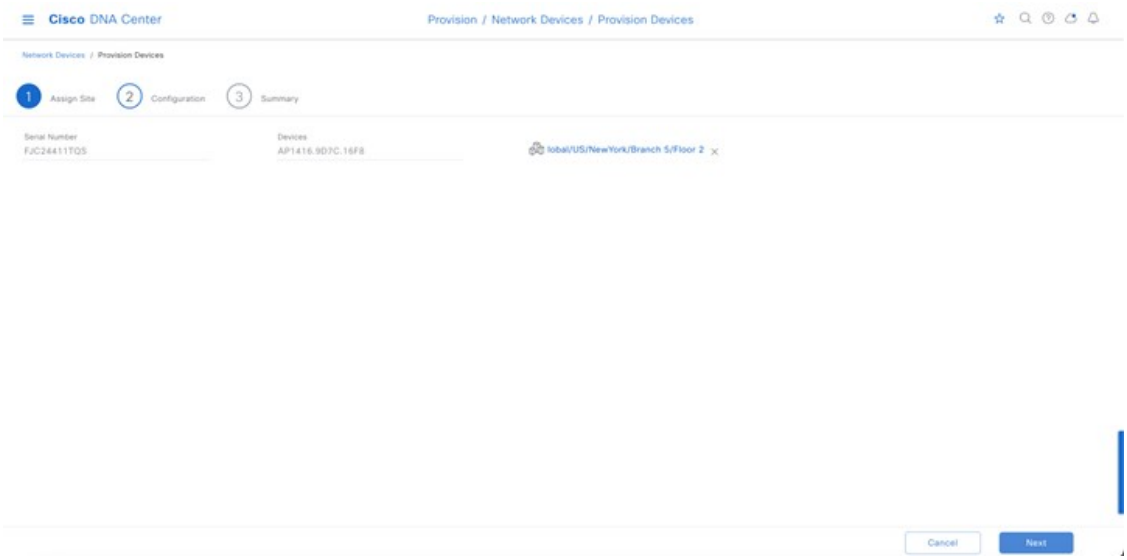
手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 目的の AP を選択し、[Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]**の順に選択します。

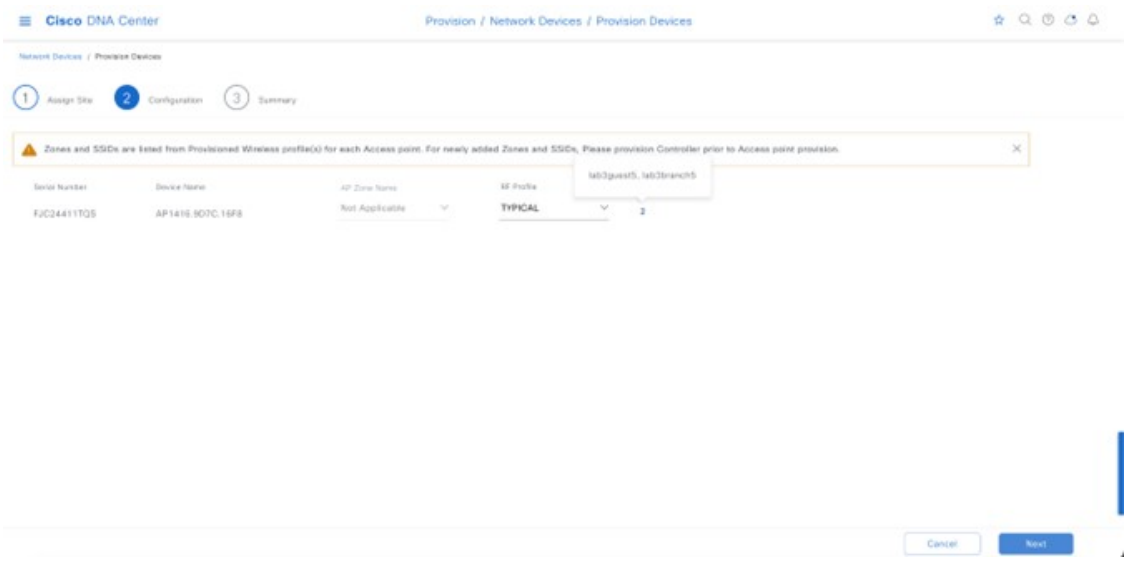
ステップ 3 AP の [Assign Site] を選択します。

図 *111 : N+1 AP* フロア割り当て



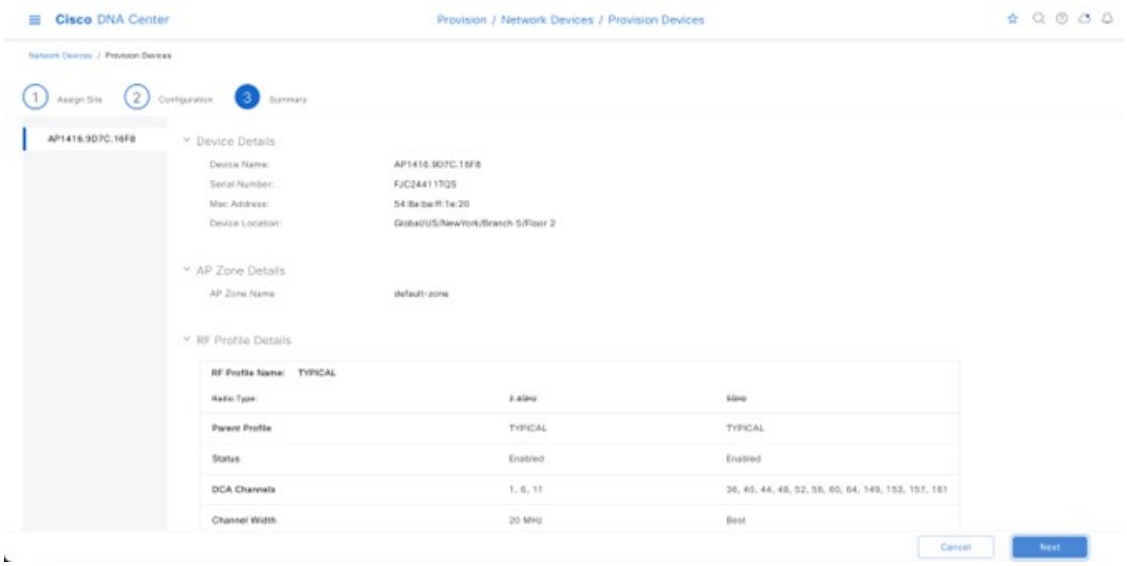
[Configuration] ウィンドウに、AP にプロビジョニングされる SSID が表示されます。

図 *112 :* ワイヤレスプロファイルに基づく *N+1 AP SSID*



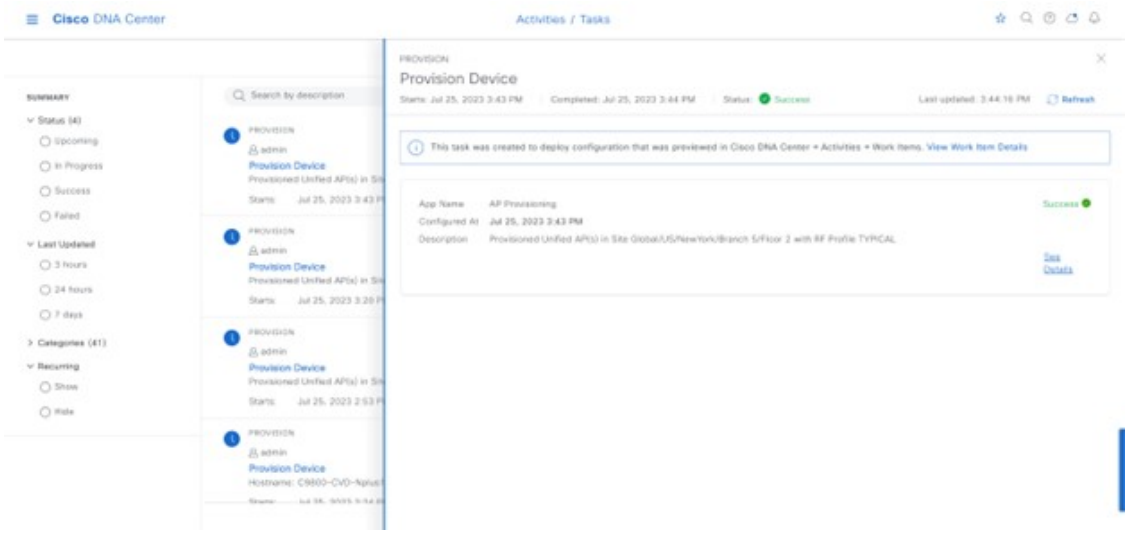
Cisco DNA Center に、プロビジョニング前の AP の概要に関する詳細が表示されます。

図 *113 : N+1 AP* のプロビジョニングの概要



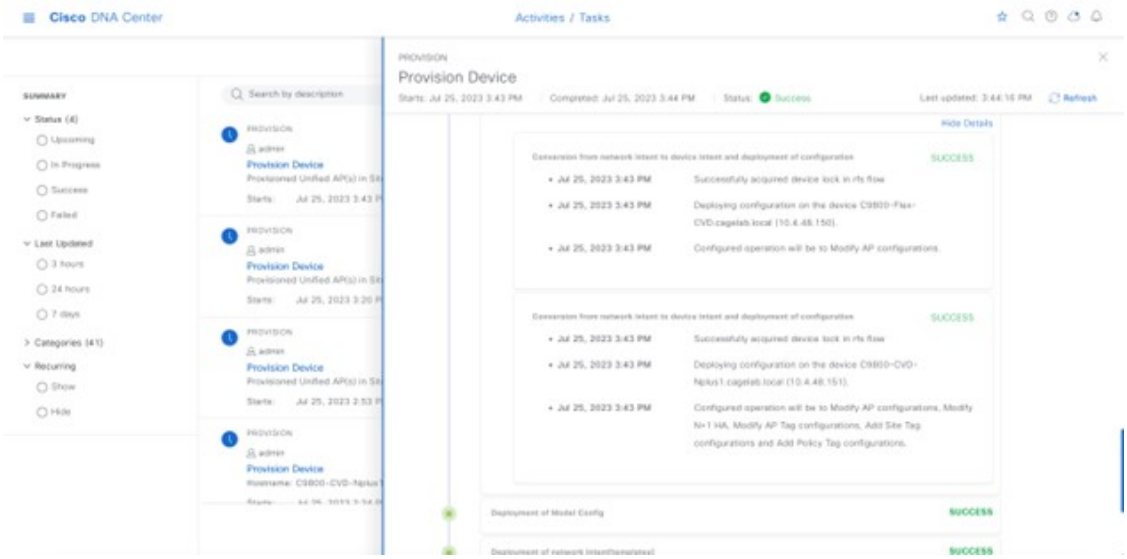
ステップ 4 **[Activities]** > **[Tasks]**に移動して、AP のプロビジョニングステータスを確認します。

図 *114 : N+1 AP* のプロビジョニングステータス



ステップ 5 プロビジョニング後、AP 設定の詳細を確認します。

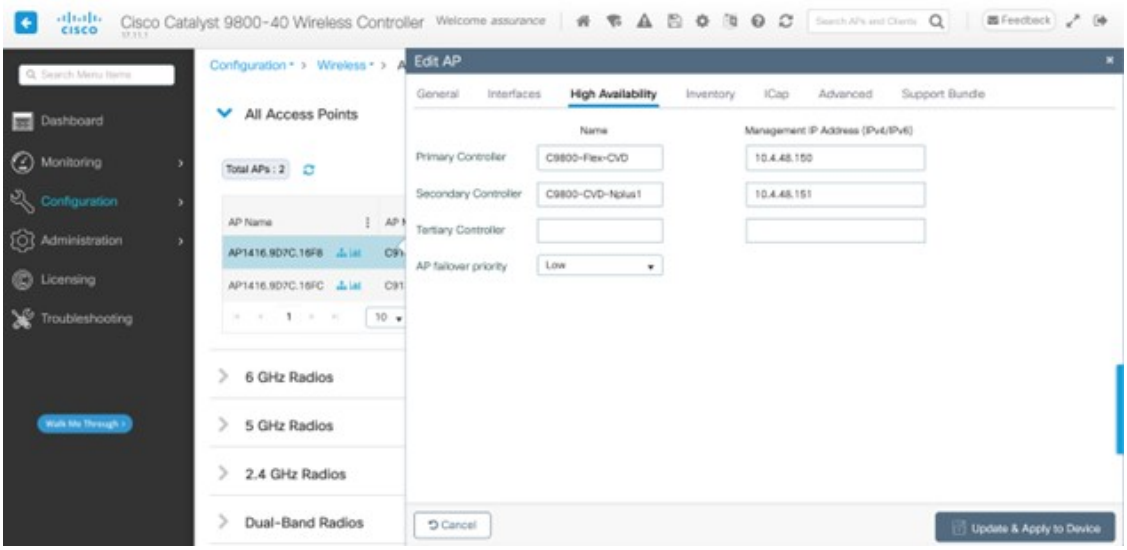
図 *115 : N+1 AP* のプロビジョニングの詳細



ステップ 6 ワイヤレスコントローラで AP の設定を確認します。AP には、プライマリコントローラとセカンダリコントローラの高可用性が正しく表示される必要があります。

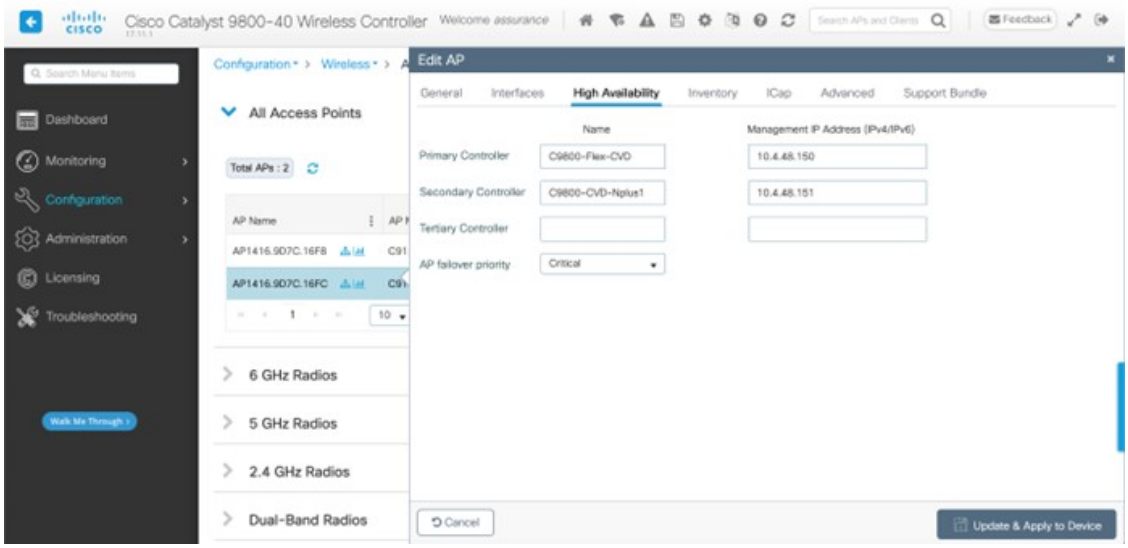
AP は再起動後にプライマリコントローラに参加し、プライマリコントローラが到達不能な場合はセカンダリコントローラに参加できるようになります。N+1 コントローラのプロビジョニングと AP に参加したプライマリコントローラを含む、プライマリコントローラとセカンダリコントローラの詳細は AP の高可用性で変更されています。

図 *116 : プライマリとセカンダリ ワイヤレスコントローラを示す N+1 AP*



ステップ 7 次の図に示されているように、この手順を繰り返して **Branch 5** の **Floor 2** に 2 番目の AP をプロビジョニングし、プライマリとセカンダリ ワイヤレスコントローラが正しく設定されていることを確認します。

図 *117 : N+1 AP* でのセカンダリ *AP* 用のプライマリおよびセカンダリ ワイヤレスコントローラの割り当て



FlexConnect の N+1 ワイヤレスコントローラの設定

このガイドでは、Cisco Catalyst 9800-40 ワイヤレスコントローラの名前は Cisco Catalyst 9800-CVD-Nplus1.cagelab.local で、Cisco Catalyst 9800-Flex-CVD.cagelab.local（プライマリコントローラ）の N+1 コントローラ（セカンダリコントローラ）として機能します。

次の手順を実行して N+1 コントローラを展開します（N+1 コントローラがプライマリコントローラと同じサイトに存在することが前提）。

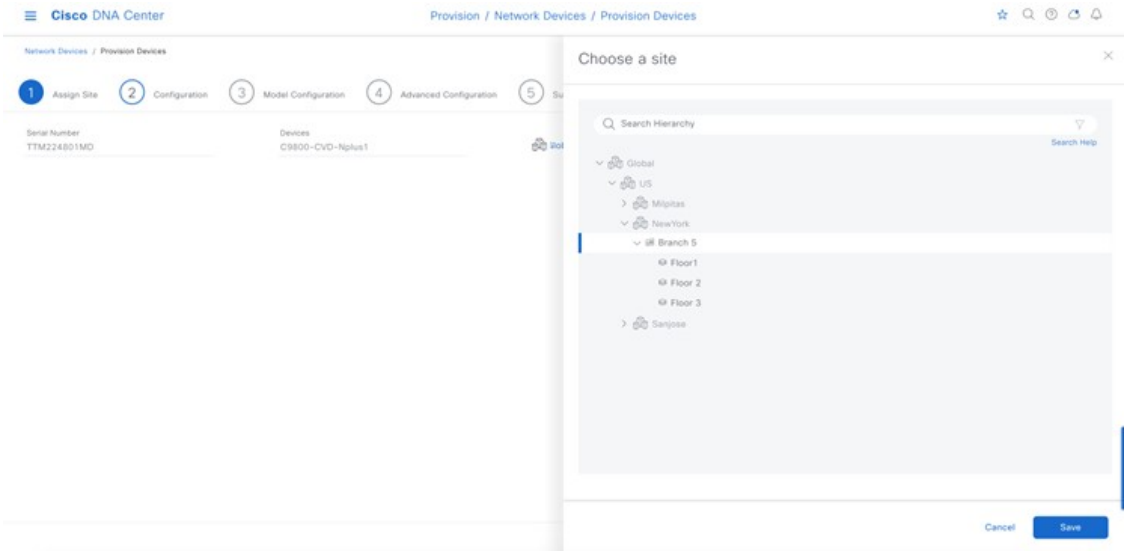
手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]**の順に選択し、N+1 コントローラを選択します。

ステップ 2 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

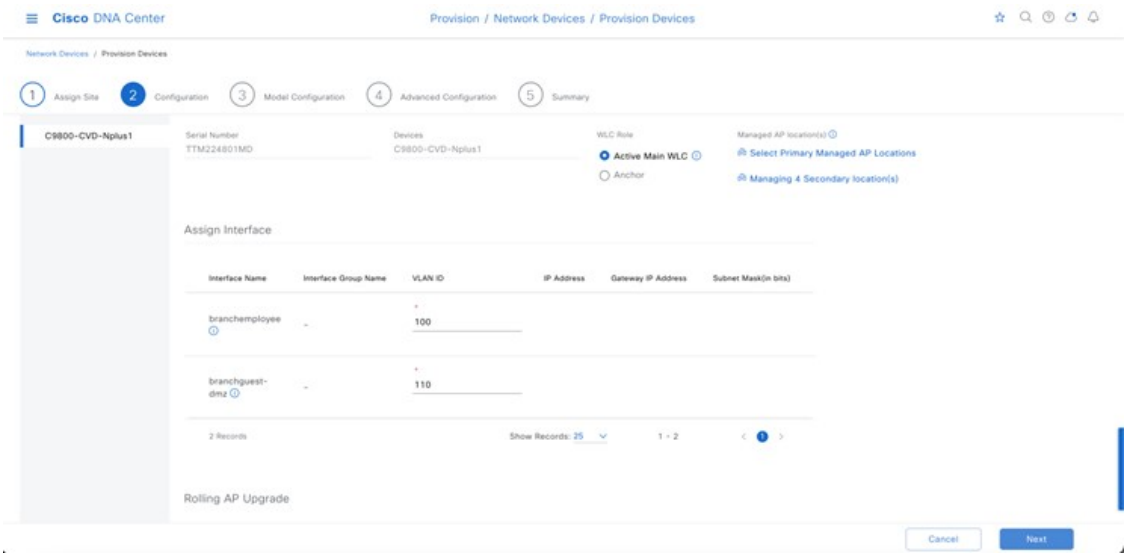
ステップ 3 次の図に示されているように、[Assign Site] ウィンドウで、サイトを N+1 コントローラと **Branch 5** のビルディングの場所に割り当てます。

図 *118 : N+1* コントローラへのサイトの割り当て



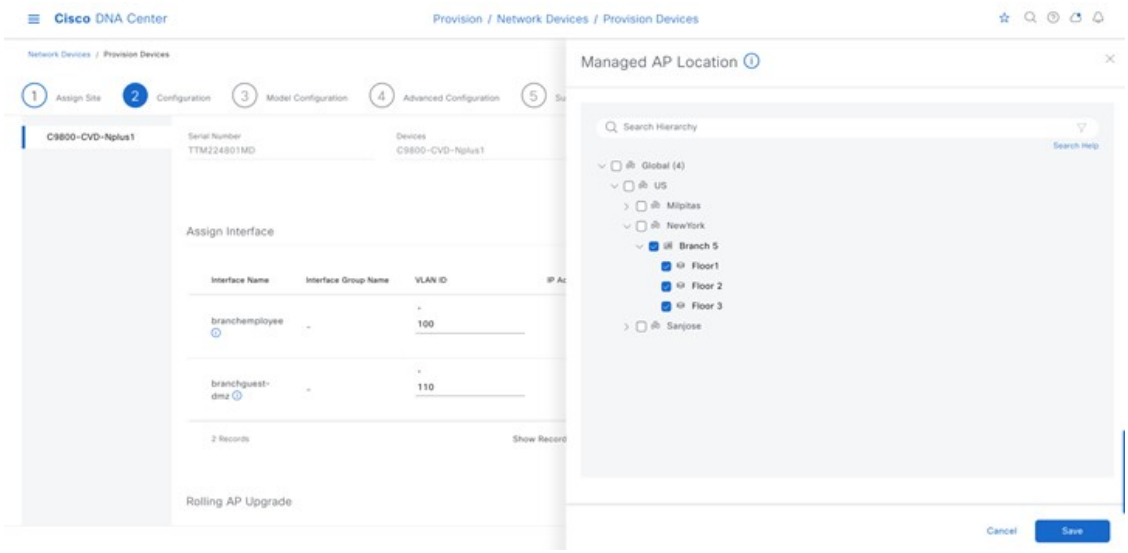
ステップ 4 [Configuration] ウィンドウで、プライマリコントローラ AP を管理する [Managing Secondary Locations] をクリックします。

図 *119 : N+1* コントローラの設定



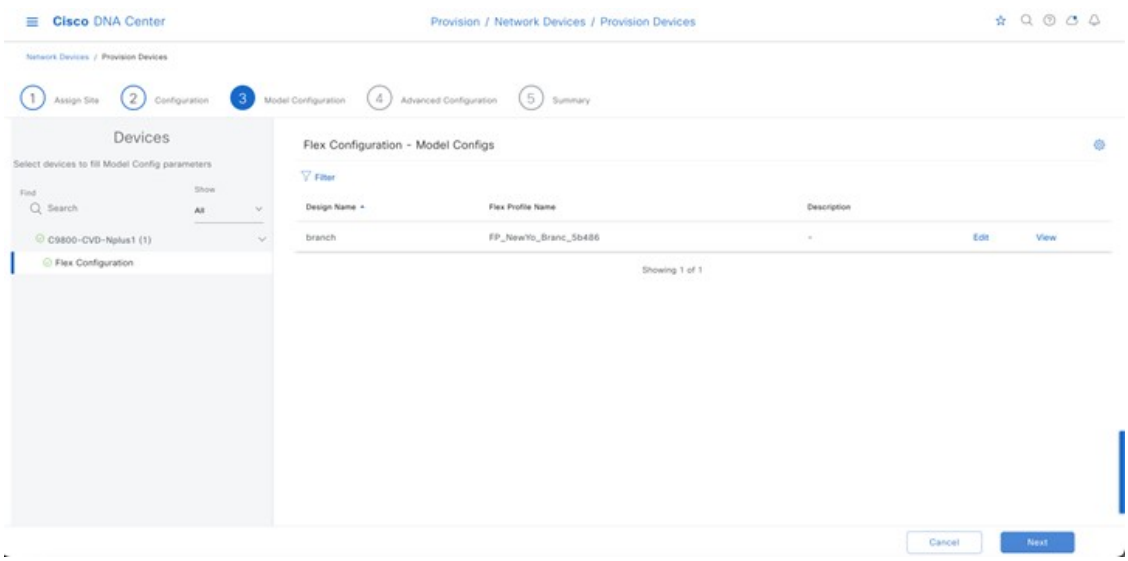
ステップ 5 プライマリコントローラによって管理されるフロアを選択します。

図 *120* : 管理対象 *AP* の場所の選択



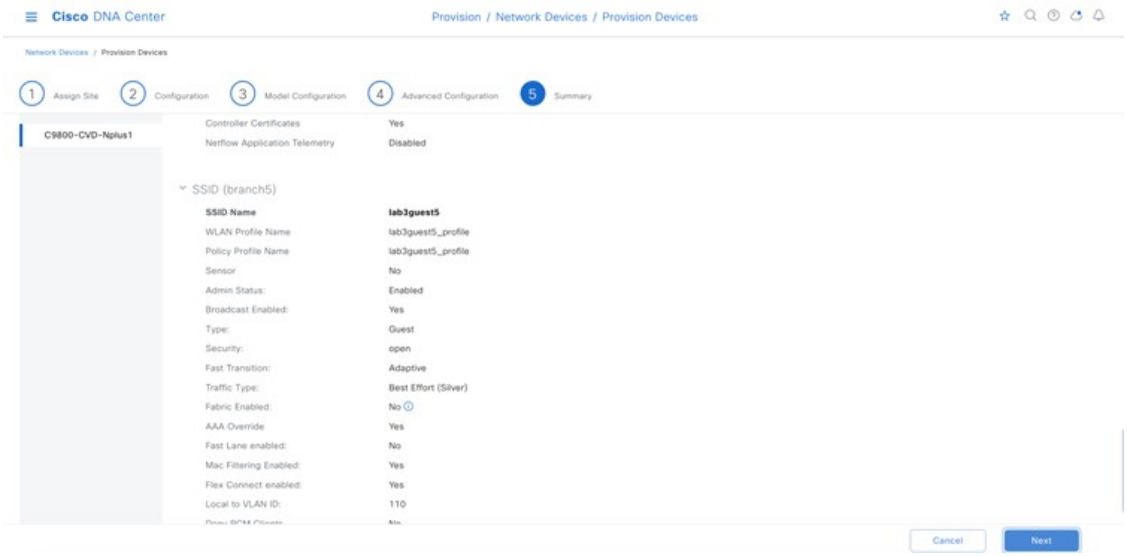
Cisco DNA Center は、Flex 設定があるモデル設定をプライマリコントローラの一部として自動的に認識します。

図 *121* : *N+1* ワイヤレスコントローラ、*Flex* モデル設定あり



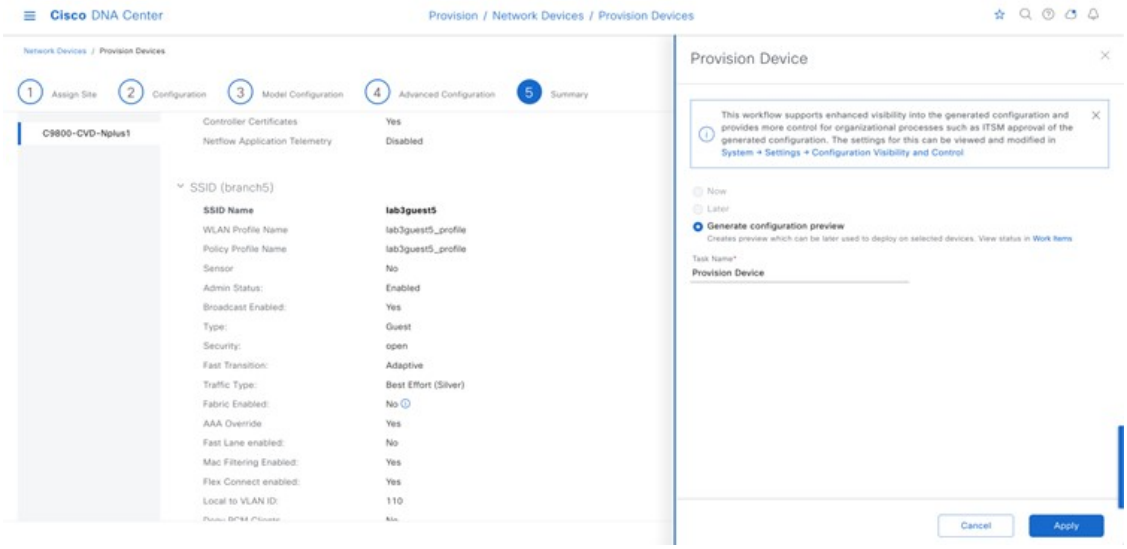
ステップ 6 [Summary] ウィンドウでは、展開前に SSID、サイト、およびネットワーク設定の構成の詳細を確認できます。

図 *122 : [N+1* ワイヤレスコントローラ *Provision Summary]* ウィンドウ



ステップ 7 展開前に [Generate Configuration Preview] オプションボタンを選択して、設定を確認します。

図 *123 : N+1* ワイヤレスコントローラの設定プレビュー



ステップ 8 [Apply] をクリックします。

ステップ 9 **[Activities]** > **[Task]**の順に選択します。

Cisco DNA Center により、コントローラが正常にプロビジョニングされる必要があります。

Cisco DNA Center により、プライマリコントローラから N+1 コントローラに同じ設定が適用されます。次の図に、プロビジョニングの概要を示します。

図 *124 : N+1* プロビジョニングステータス：パート *1*

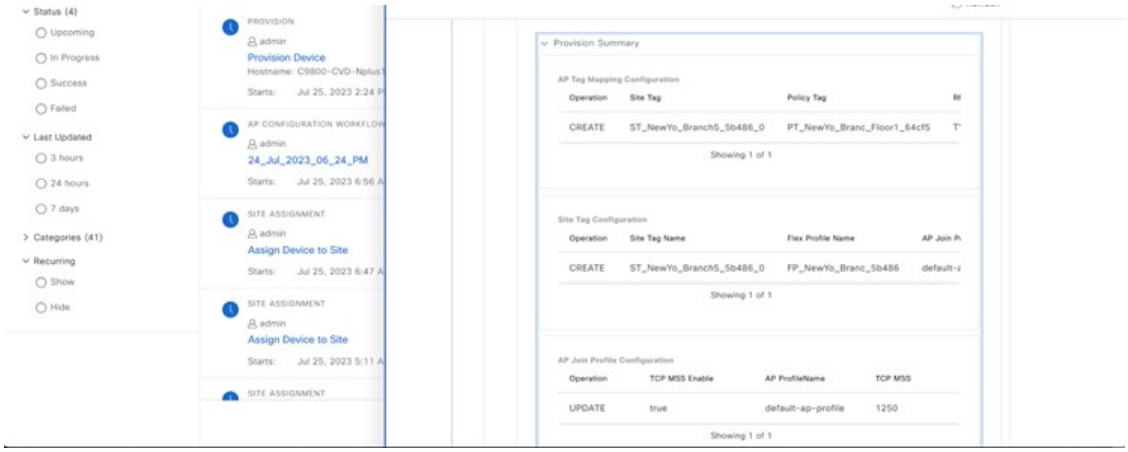


図 *125 : N+1* プロビジョニングステータス：パート *2*

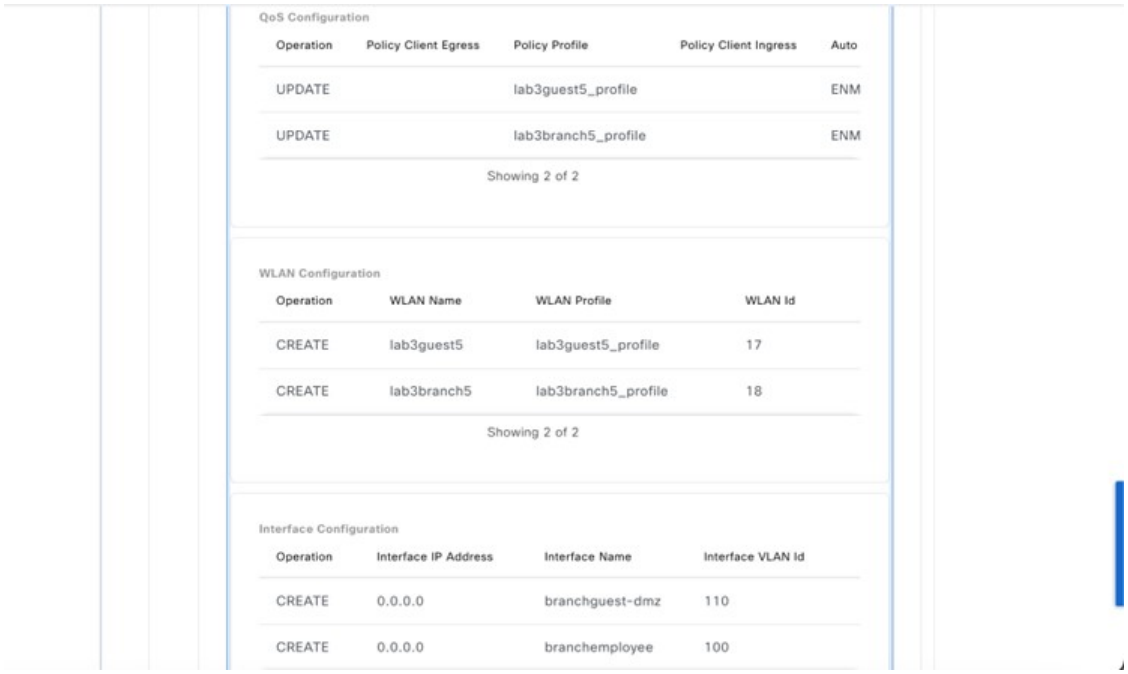


図 *126 : N+1* プロビジョニングステータス：パート *3*

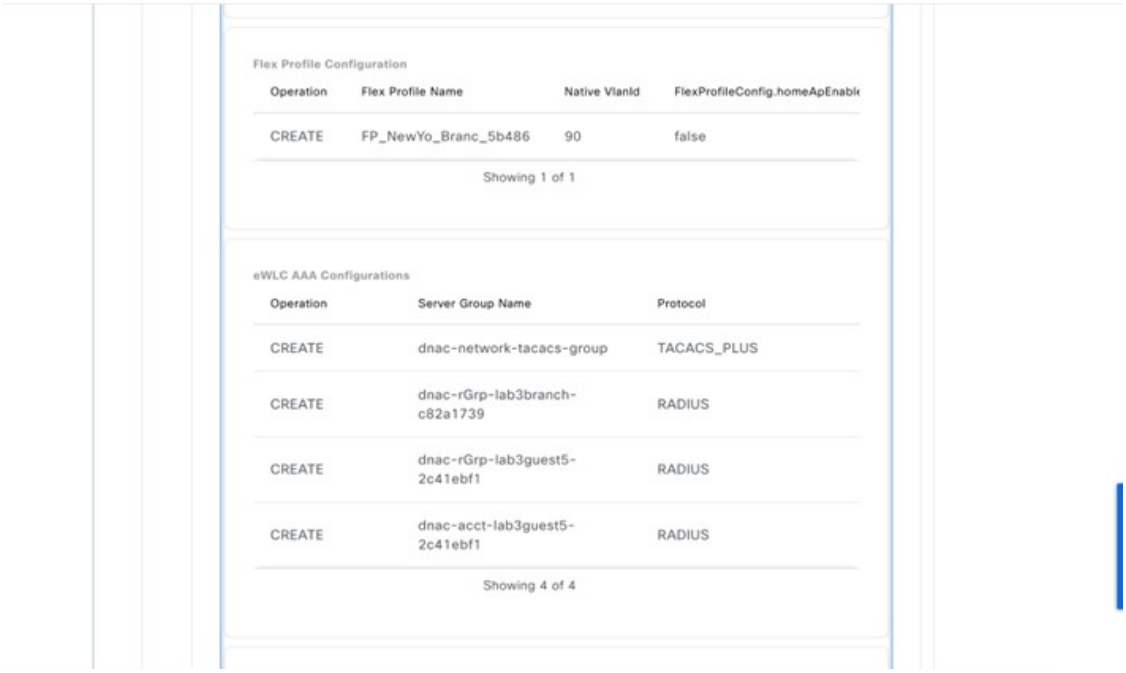
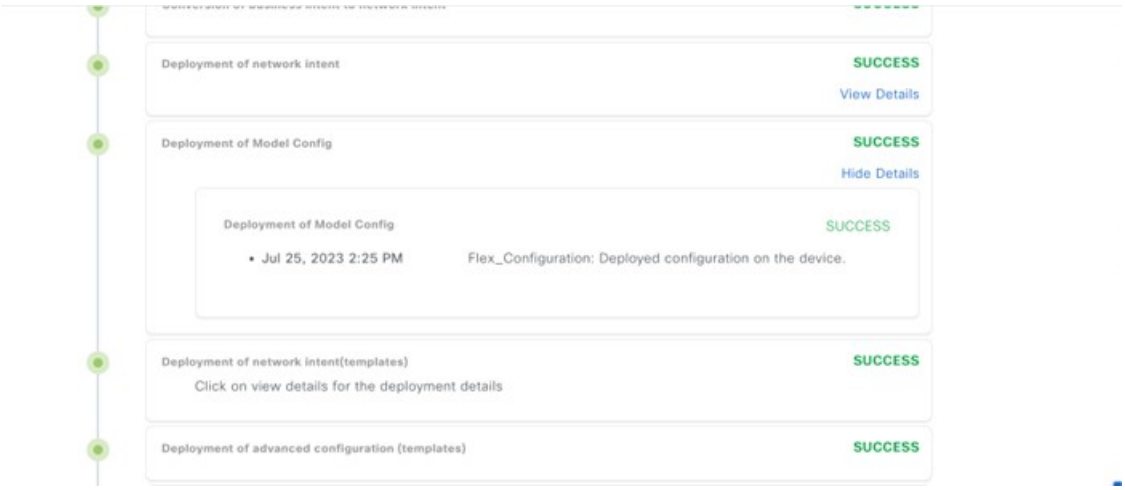


図 *127 : N+1* プロビジョニングステータス：パート *4*

図 *128 : N+1* プロビジョニングのステータス：パート *5*

次の図は、モデル設定を使用した Flex 設定を示しています。

図 *129 : N+1* モデルのプロビジョニングステータス



同じフロアの異なる AP セットを使用して 2 つの SSID をオンボーディングするための AP ゾーンの作成

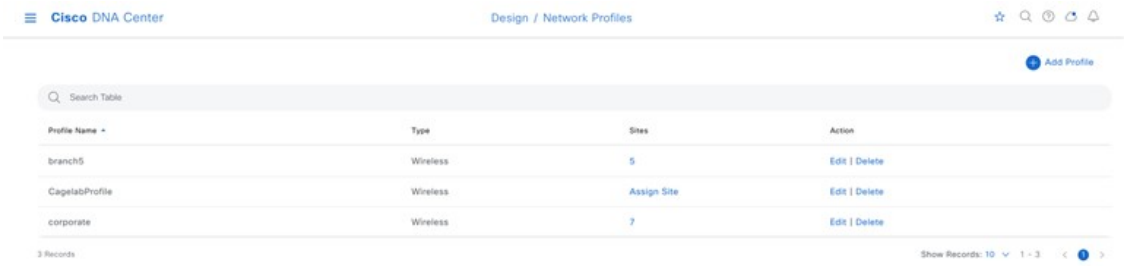
AP ゾーンを使用すると、同じサイト上の一連の AP に異なる SSID と RF プロファイルを関連付けることができます。デバイスタグを使用して、AP ゾーンを適用する AP を識別できます。ワイヤレスプロファイル内の [AP Zones] タブから、デバイスタグのネットワークプロファイルで設定された SSID のサブセットを使用して個別の AP ゾーンを作成できます。Cisco DNA Center は、AP プロビジョニング中に AP ゾーン設定を AP に適用します。

このガイドでは、New York に 2 つのゾーンを作成し、Branch 5、Floor 1 を構築します。フロアには 2 つの AP があります。1 つの AP はゾーン 1 で企業 SSID をブロードキャストし、もう 1 つの AP はゾーン 2 でゲスト SSID をブロードキャストします。

次の手順では、2 つの AP ゾーンを作成し、作成したゾーンで設定する AP をプロビジョニングする方法について説明します。

1. 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Profiles]**の順に選択し、[Corporate] ネットワークプロファイルの [Edit] をクリックします。

   図 ***130 : AP*** ゾーン：***[Network Profile]*** ウィンドウ



2. [AP Zones] タブをクリックし、2 つの AP ゾーンを作成します。RF プロファイル：High の lab3branch5 SSID に対する最初のゾーン sjcfloor1zone2 に名前を付け、RF プロファイル：Low の lab3guest5 SSID に対するその他の AP ゾーン sjcfloor1zone1 に名前を付けます。

   図 ***131 :*** ネットワークプロファイルで作成された ***AP*** ゾーン ***1***

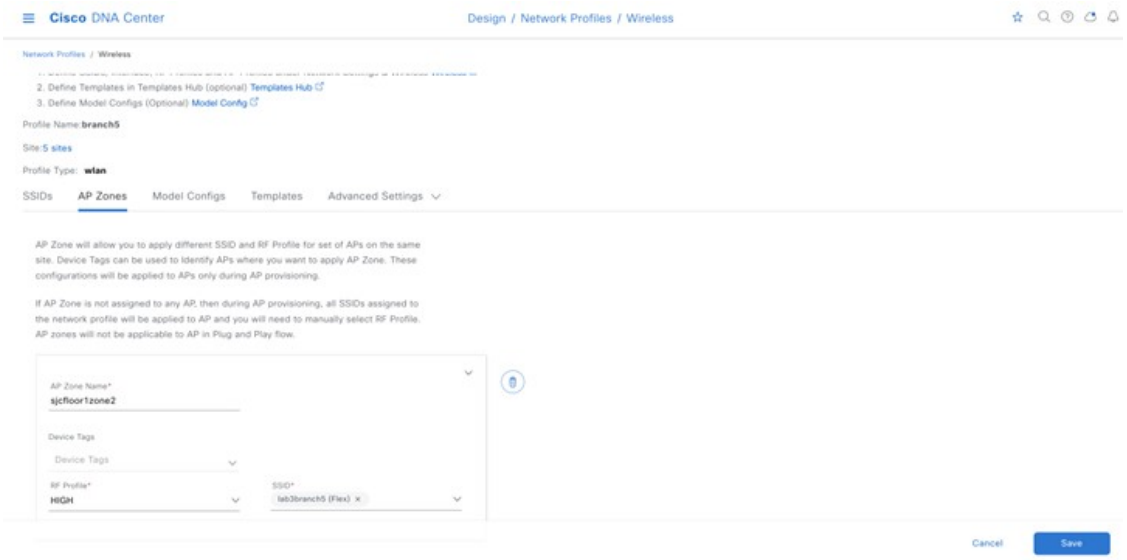
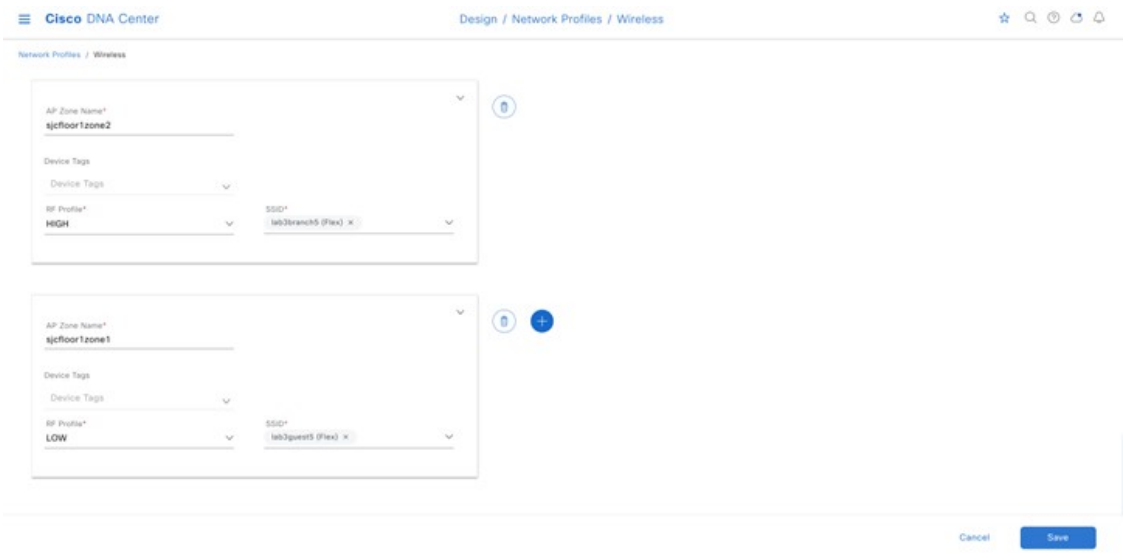


図 *132 :* ネットワークプロファイルで作成された *AP* ゾーン *2*



3. [Save] をクリックします。

（注） Cisco DNA Center は、プラグアンドプレイ（PnP）プロセスから要求された AP に AP ゾーン設定を適用しません。

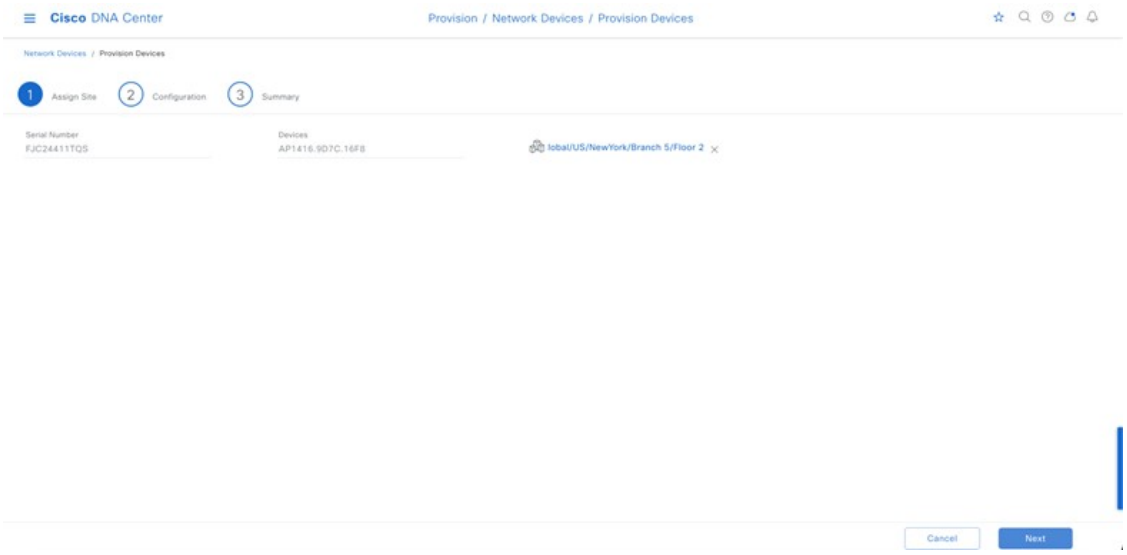
AP ゾーンが AP ですでにプロビジョニングされている場合、および AP ゾーン設定を後で更新する場合は、更新を適用するためにワイヤレスコントローラを再プロビジョニングする必要があります。AP を再プロビジョニングする必要はありません。

AP のプロビジョニング中、AP のデバイスタグとサイトに基づいて、Cisco DNA Center は対応する AP ゾーンを選択し、RF プロファイルを自動的に割り当てます。AP に 2 つの AP ゾーンが設定されている場合、必要な AP ゾーンを選択できます。AP の AP ゾーンがない場合は、必要な RF プロファイルを選択できます。AP ゾーンを作成する前に、**[Design]** > **[Network Settings]** > **[Wireless]**タブでワイヤレス SSID を作成していることを確認します。AP ゾーン設定を AP に適用するには、ワイヤレスコントローラを再プロビジョニングします。

RF プロファイル： Low の lab3guest5 SSID に対するゾーン sjcfloor1zone1 への 1 つの AP のプロビジョニング

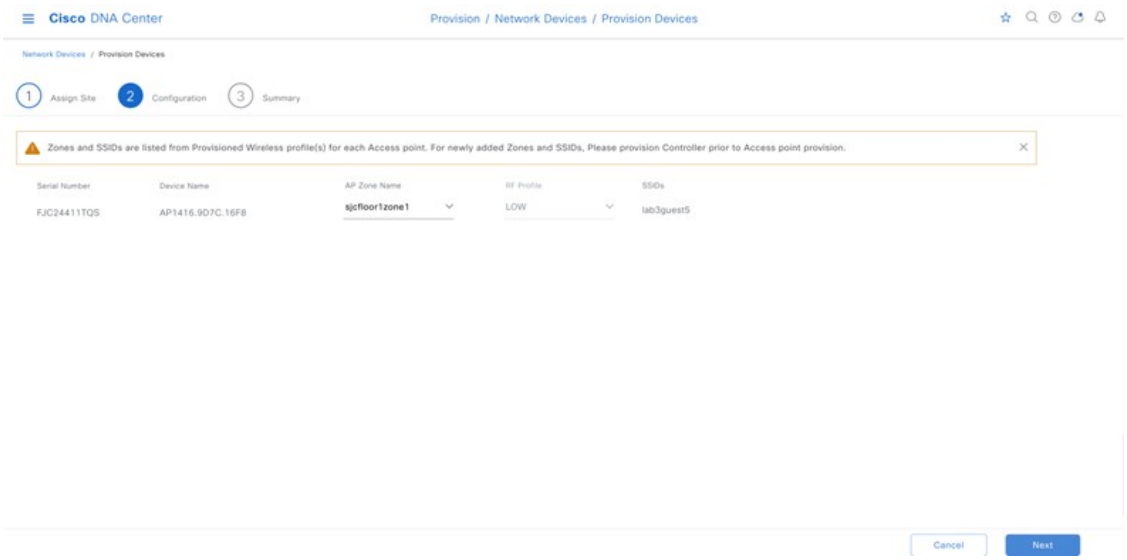
1. 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。
2. [Actions] ドロップダウンメニューから AP を選択し、**[Provision]** > **[Provision Devices]**の順に選択します。
3. AP のサイトを選択し、[Next] をクリックします。

図 *133 : AP* ゾーンのプロビジョニング：サイトの選択



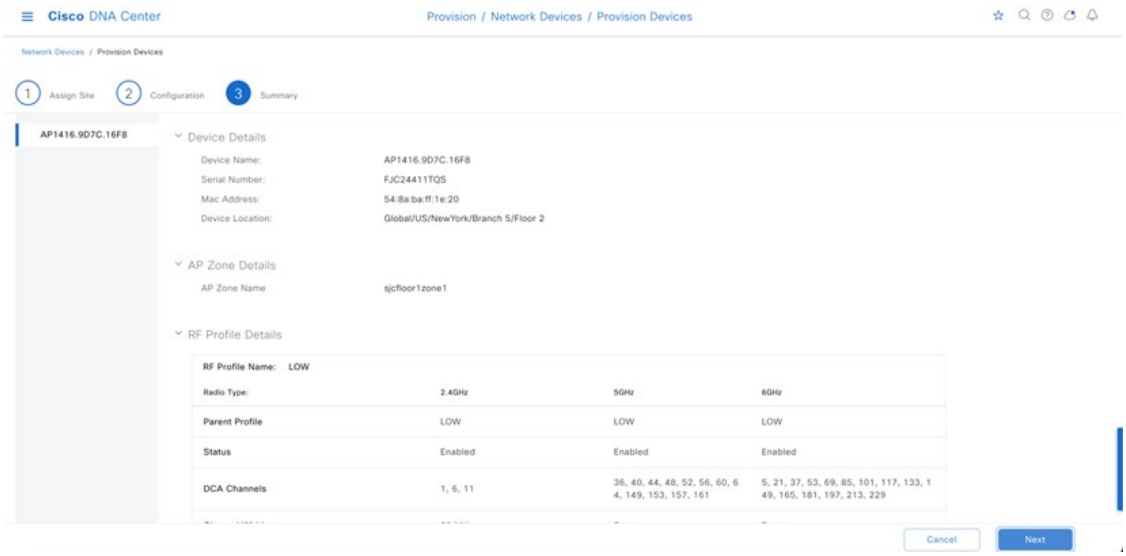
4. ドロップダウンリストから AP ゾーンを選択します。

図 *134 : AP* ゾーンのプロビジョニング：ゾーンの選択



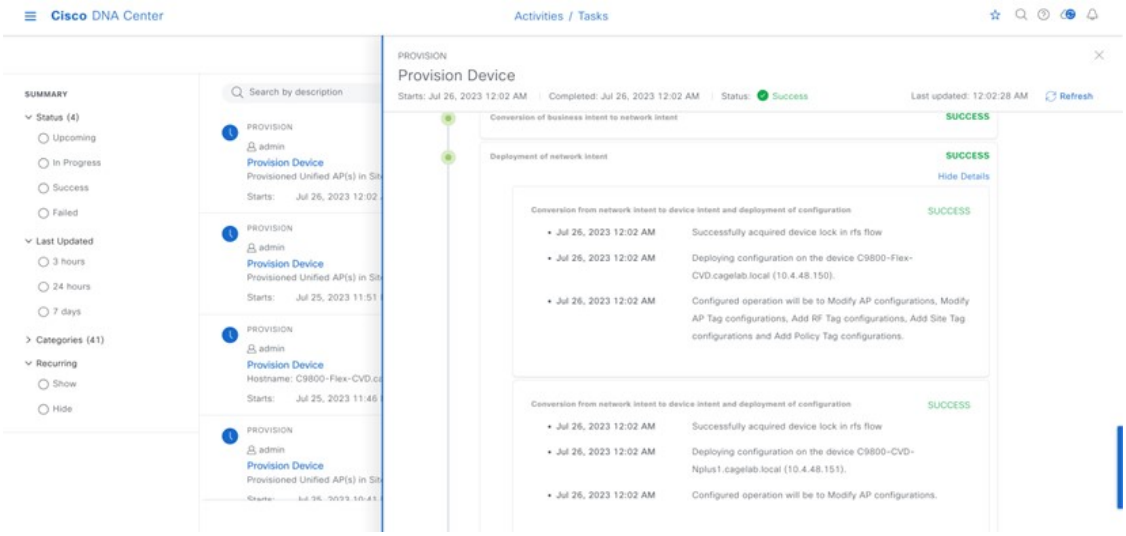
5. [Summary] ウィンドウで詳細を確認し、[Next] をクリックします。

図 *135 : AP* ゾーンのプロビジョニングの概要



6. **[Activities]** > **[Tasks]**に移動し、AP ゾーンが AP に正常にプロビジョニングされていることを確認します。

図 *136 : AP* ゾーンのプロビジョニングステータス



7. シスコ ワイヤレス コントローラ GUI で AP の設定を確認します。AP 設定には、ワイヤレスコントローラの RF タグ、サイトタグ、およびポリシータグが正しく表示されます。

図 *137 : Cisco DNA Center* を使用してプロビジョニングされた *AP1 SSID*

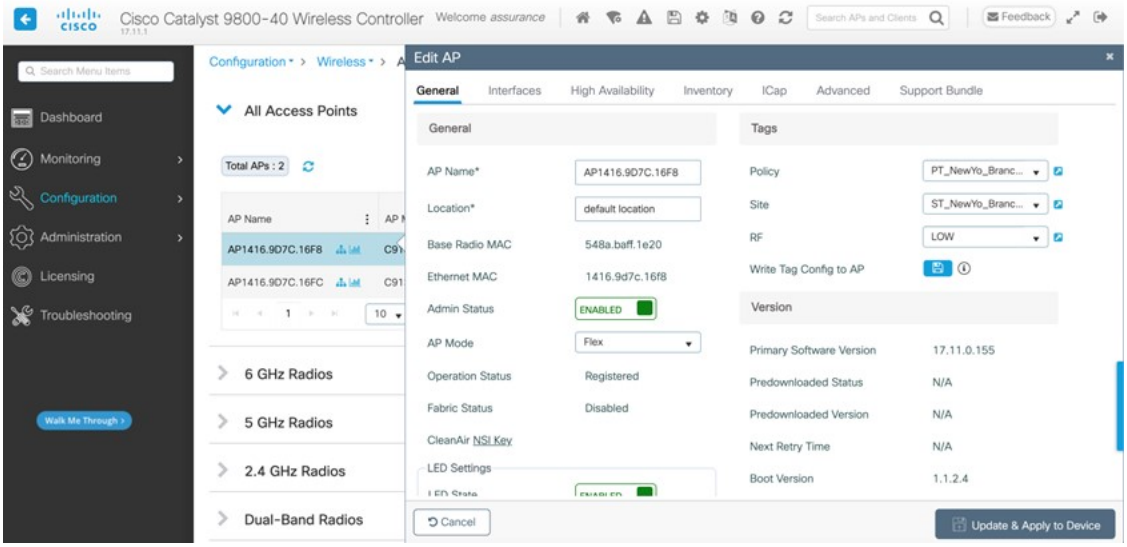


図 *138 : Cisco DNA Center* を使用してプロビジョニングされたポリシータグ *1*

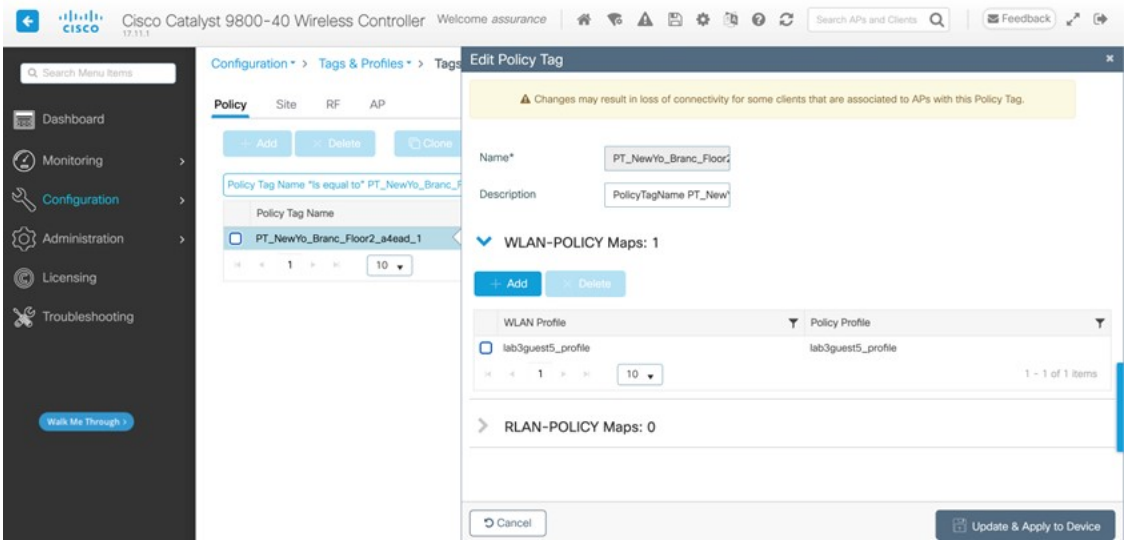
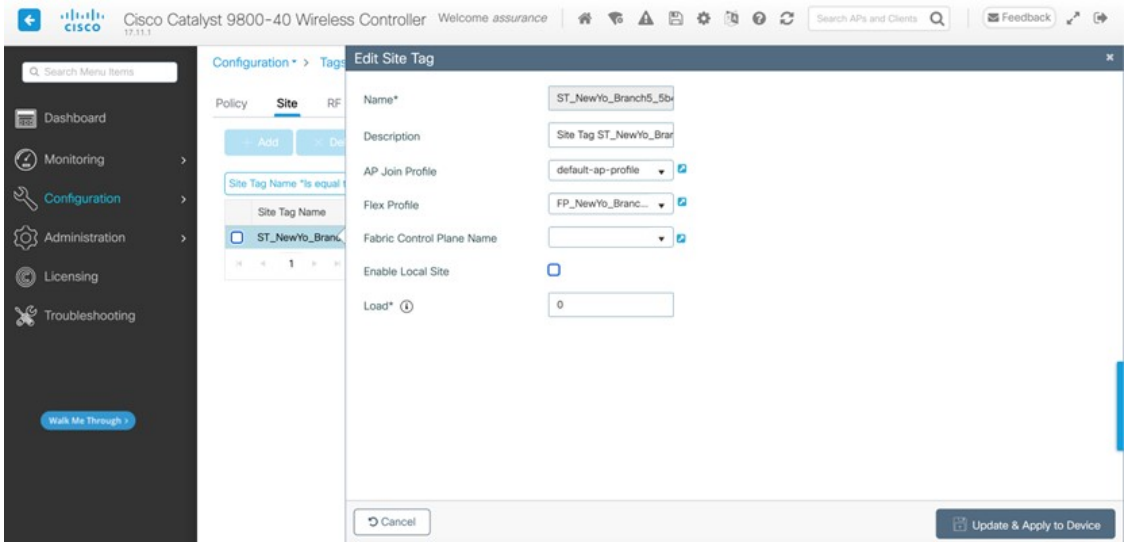


図 *139 : Cisco DNA Center* を使用してプロビジョニングされたサイトタグ *1*



8. ステップ 1 ～ 7 を繰り返して、RF プロファイル：High の lab3branch5 SSID に sjcfloor1zone2 という名前の AP をプロビジョニングします。

9. ワイヤレスコントローラ GUI で 2 番目の AP の AP 設定を確認します。AP 設定には、コントローラの RF タグ、サイトタグ、およびポリシータグが正しく表示されます。

図 *140 : Cisco DNA Center* を使用してプロビジョニングされた *AP2 SSID*

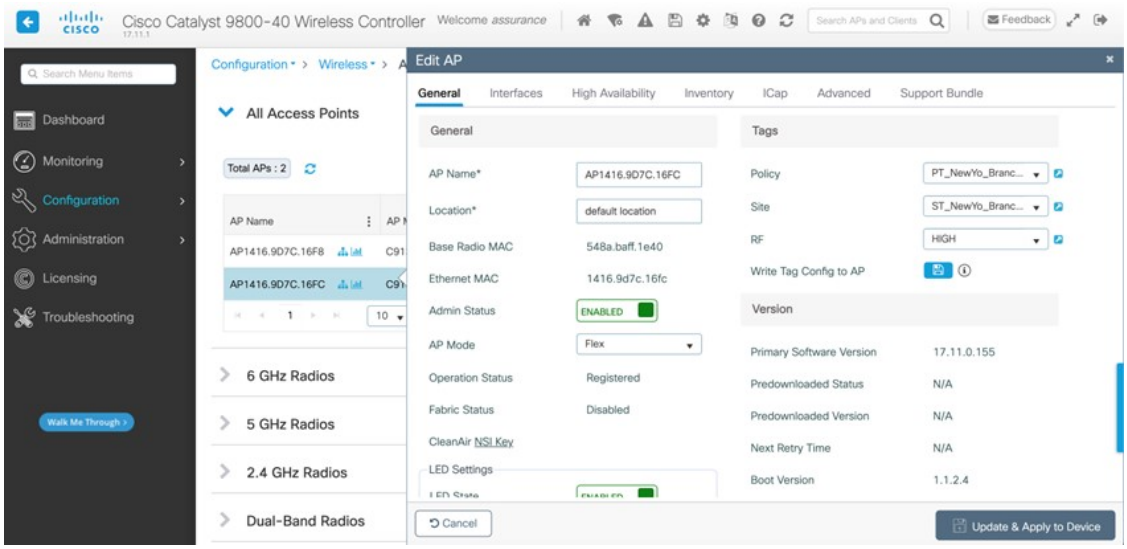


図 *141 : Cisco DNA Center* を使用してプロビジョニングされたポリシータグ *2*

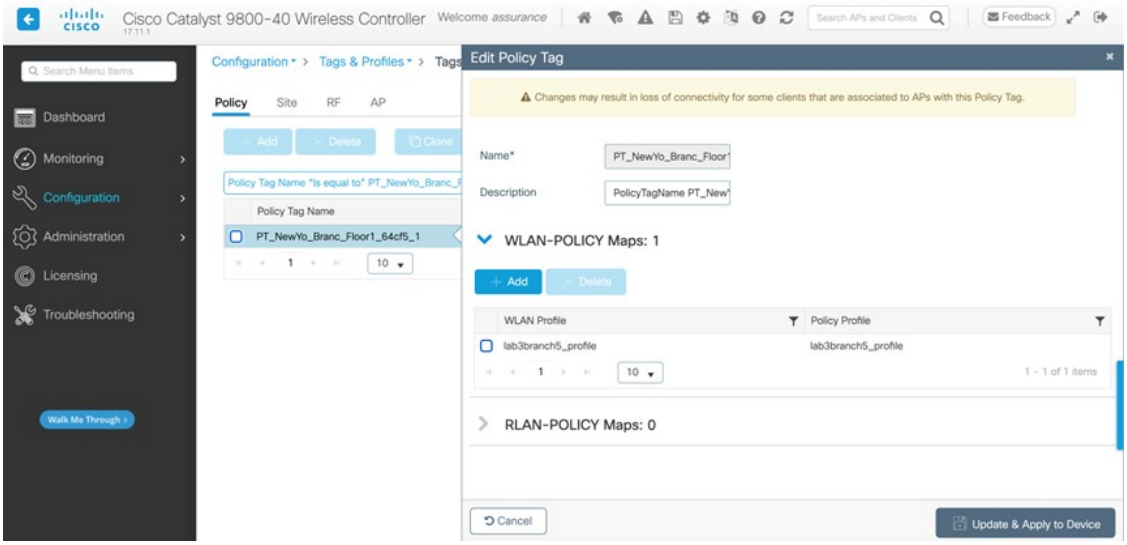
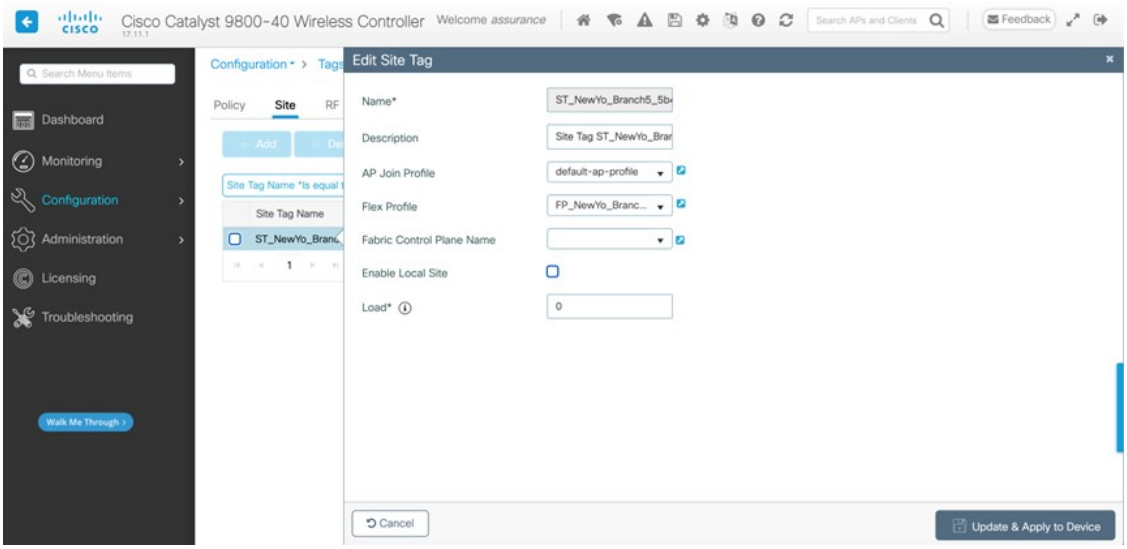


図 *142 : Cisco DNA Center* を使用してプロビジョニングされたサイトタグ *2*



エンタープライズ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ HA SSO ペアへの新しい AP の参加（WLC-9800-2）

この導入ガイドでは、新しい AP で IP DHCP 検出を使用して Cisco Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）が検出され、新しい AP がプライミングされていないことを前提としています。以前ワイヤレスコントローラに参加（CAPWAP トンネルを確立）し、ワイヤレスコントローラ の IP アドレスを NVRAM にキャッシュしている場合、あるいは、プライマリ、セカンダリ、またはターシャリ ワイヤレスコントローラ管理IPアドレスがAP内で設定されている場合、その Cisco AP はプライミングされています。そのようなシナリオの AP では、IP DHCP 検出よりもプライマリ、セカンダリ、またはターシャリ ワイヤレスコントローラの設定が優先されます。

IP DHCP 検出では、DHCP サーバーはオプション 43 を使用して、1 つ以上のワイヤレスコントローラ 管理 IP アドレスを AP に提供します。AP が Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）の管理 IP アドレスを学習すると、ワイヤレスコントローラに CAPWAP 参加要求メッセージが送信されます。ワイヤレスコントローラが参加すると、AP の設定、ファームウェア、制御トランザクション、およびデータトランザクションが管理されます。

次の手順では、AP を検出してエンタープライズ ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）に参加させる方法について説明します。

手順

ステップ 1 Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）に参加する Cisco AP をサポートするレイヤ 2 アクセススイッチで、必要な VLAN を設定します。

この導入ガイドでは、APがレイヤ2アクセススイッチに接続されていることを前提としています。専用の VLAN は、PC や IP フォンなどのエンドユーザーデバイスとは別の AP 用のスイッチ上にあります。AP に専用の VLAN を使用することは、一般に設計上のベストプラクティスと見なされますが、この方法ではスイッチに追加の VLAN が展開されます。

次に、レイヤ 2 アクセススイッチの設定例を示します。

```
vlan 102
name AP_management
```

ステップ 2 APが接続されるスイッチポートを、設定されたVLANの一部として設定します。スイッチポートがシャットダウンされていないことを確認します。

次に、インターフェイス構成の例を示します。

```
interface TenGigabitEthernet1/0/45
description AIR-AP2802I-B-K9 AP00F6.6313.B796
switchport access vlan 102
switchport mode access
no shutdown
```

レイヤ 2 アクセススイッチを使用する展開シナリオでは、AP に接続された VLAN に関連付けられているアップストリームレイヤ 3 デバイス（スイッチまたはルータ）は、DHCP 要求を中央の DHCP サーバーにリレーするように設定する必要があります。リレー機能を有効にするには、**ip helper-address** インターフェイスレベル コマンドを使用します。

ステップ 3 Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）に参加する AP をサポートするアップストリームレイヤ 3 デバイスで、必要な DHCP リレーコマンドを設定します。

次に、VLAN スイッチ仮想インターフェイス（SVI）を使用したレイヤ 3 スイッチの設定例を示します。

```
interface Vlan102
ip address 10.4.2.1 255.255.255.0
ip helper-address 10.4.48.10
```

ステップ 4 オプション 43 で Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）の管理 IP アドレスを返すように、IP DHCP サーバー内の DHCP スコープを設定します。

この導入ガイドでは、IP アドレス **10.4.48.10** の Microsoft Active Directory（AD）サーバーが IP DHCP サーバーとして機能します。DHCP オプション 43 内で設定されたエンタープライズ ワイヤレスコントローラ

HA SSO ペア（WLC-9800-2）の IPv4 アドレスは **10.4.74.32** です。Microsoft AD サーバー内の DHCP の設定は、このマニュアルの範囲外です。

ステップ 5 Cisco AP をレイヤ 2 アクセススイッチのスイッチポートに接続します。

AP は IP アドレスを取得し、Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）に自動的に参加する必要があります。WLC-9800-2 のインベントリ再同期間隔が経過すると、新しい AP が Cisco DNA Center インベントリに表示されます。あるいは、次の手順を使用して、ワイヤレスコントローラのインベントリを手動で再同期できます。

1. 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

   メインの [Provisioning] ウィンドウにインベントリ内のデバイスが表示されます。デフォルトでは、[Focus] は [Inventory] に設定されます。

2. **WLC-9800-2** のチェックボックスをオンにします。

3. [Actions] ドロップダウンメニューから **[Inventory]** > **[Resync Device]** の順に選択します。再同期の確認を求める警告ダイアログボックスが表示されます。

4. [OK] をクリックして再同期を確認し、ダイアログボックスを閉じます。

Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）を再同期すると、ワイヤレスコントローラに参加している AP が [Inventory] ウィンドウに表示されます。

新しい AP のプロビジョニング

AP が Cisco Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（C9800-40-CVD.cagelab.local）に参加したら、プロビジョニングする必要があります。AP が正しい設定を受信して **lab3employee** および **lab3guest** SSID をアドバタイズするためには、Cisco DNA Center を使用してプロビジョニングする必要があります。次の表に、この導入ガイド用にプロビジョニングされた AP と各 AP の場所を示します。

表 31 : Cisco DNA Center でプロビジョニングされた AP

AP 名	AP Model	ロケーション
AP1416.9D7C.16FC	C9130AXI-B	Branch 5、Floor 1

（注） この設計および導入ガイド内のビルディングとフロア全体に展開された AP の組み合わせは、別の場所にある異なる AP モデルの Cisco DNA Center を介したプロビジョニングを示しており、すべて同じ Catalyst 9800 シリーズ HA SSO ワイヤレスコントローラ ペアによって制御されます。一般的な展開では、同じ AP モデルがフロア内に展開される傾向があり、多くの場合、展開全体に展開されます。

Cisco DNA Center 内で AP をプロビジョニングする手順は次のとおりです。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Inventory]** > **[Provision]**の順に選択します。

メインの [Provisioning] ウィンドウにデバイスが表示されます。デフォルトでは、[Focus] は [Inventory] に設定されます。

ステップ 2 プロビジョニングする各 AP のチェックボックスを見つけてオンにします。

ステップ 3 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

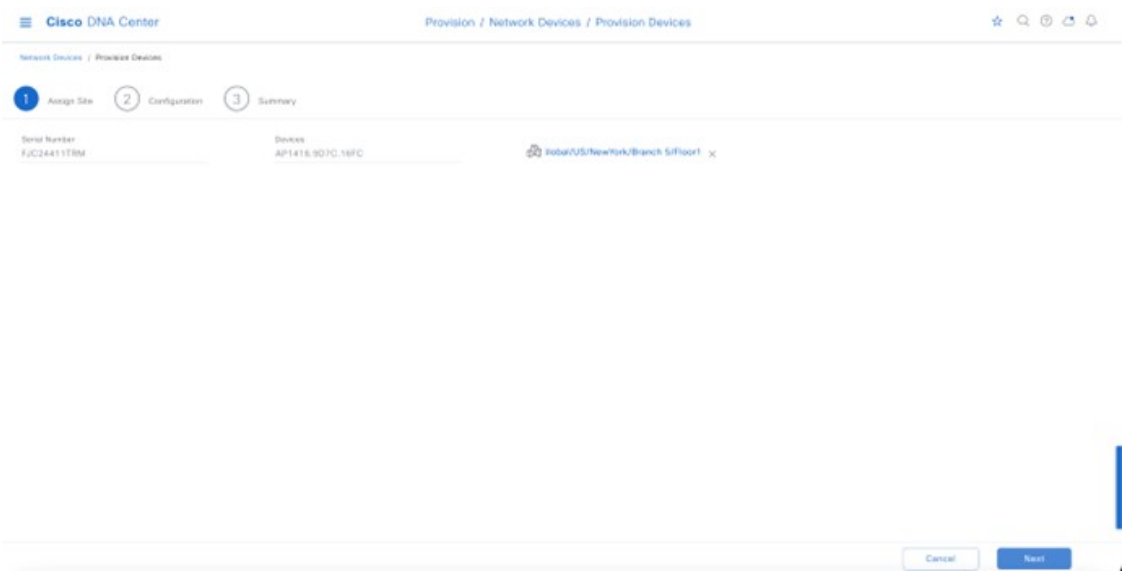
AP をプロビジョニングするためのワークフローが表示されるので、[Assign Site] から開始します。

ステップ 4 リストされた AP ごとに、[Choose a Site] をクリックします。

slide-in paneが表示され、Cisco DNA Center に設定されたサイト階層が示されます。

ステップ 5 **New York** のサイト階層を展開し、各 AP のビルディング（**Branch 5**）とフロア（**Floor 1**）を選択します。

図 *143 : AP* のプロビジョニングステップ *1*：サイトの割り当て



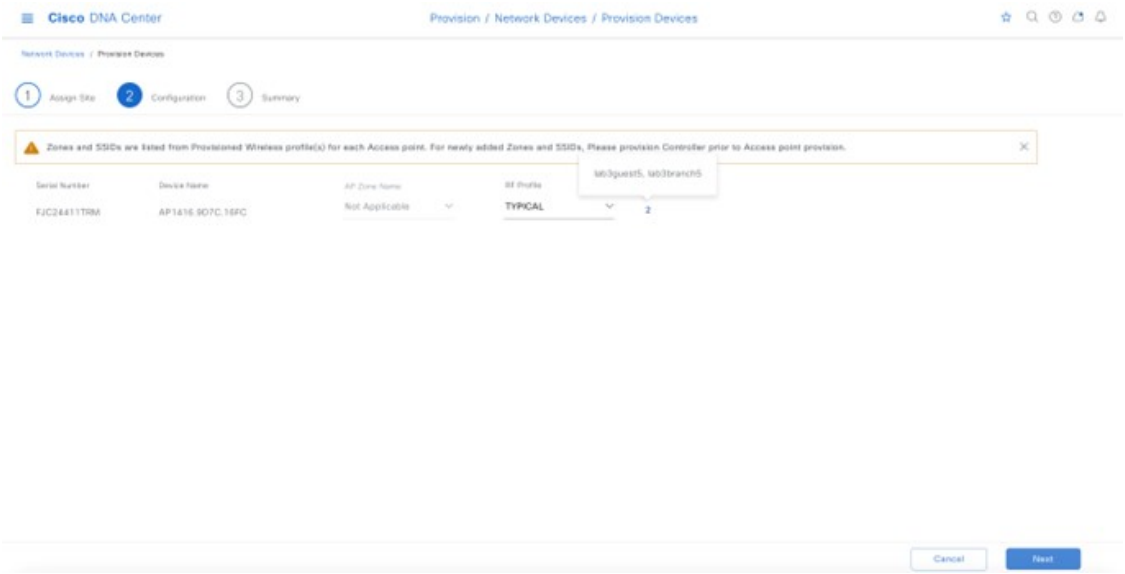
ステップ 6 [Save] をクリックし、AP のサイトの割り当てを保存します。

ステップ 7 [Next] をクリックして、プロビジョニング ワークフローの次の [Configuration] に進みます。

ステップ 8 [RF Profile] ドロップダウンリストから、各 AP に割り当てる RF プロファイルを選択します。

この導入ガイドでは、TYPICAL RF プロファイルが選択されています。TYPICAL RF プロファイルは 、「ワイヤレスネットワークの設計」でもデフォルトの RF プロファイルとして選択されています。

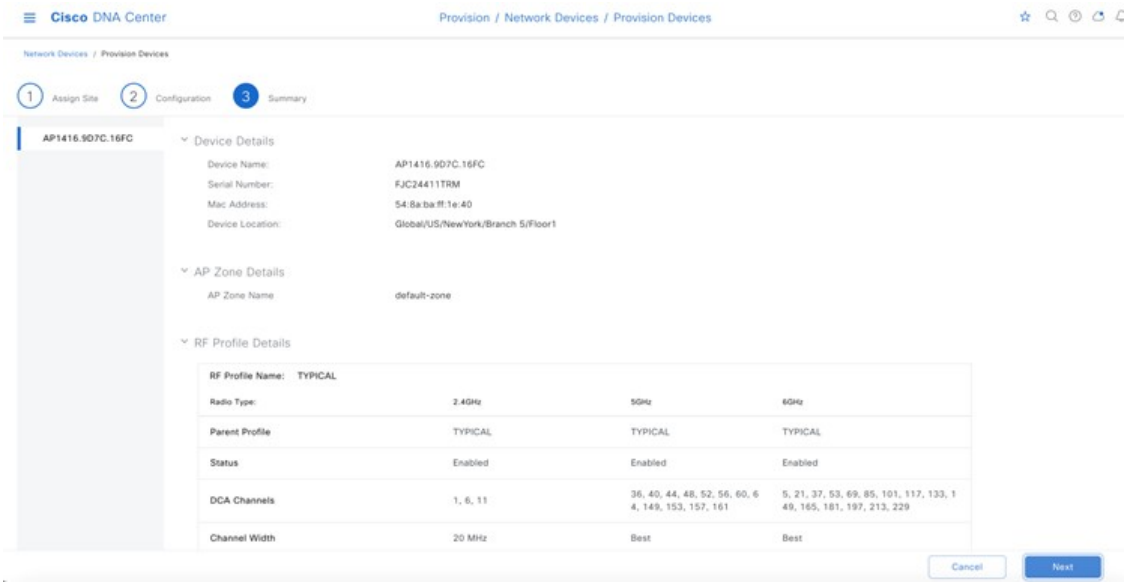
図 *144 : AP* のプロビジョニングステップ *2* : 設定



ステップ 9 [Next] をクリックして、プロビジョニング ワークフローの次のステップ [Summary] に進みます。

[Summary] ウィンドウに、各 AP にプロビジョニングされる設定の概要が表示されます。

図 *145 : AP* のプロビジョニングステップ *3* : 概要



ステップ 10 [Deploy] をクリックして、AP をプロビジョニングします。slide-in paneが表示されます。設定は今すぐ展開できます。あるいは、後で展開するようにスケジュールできます。

（注）　ベストプラクティスは、スケジュールされたネットワーク運用の変更時間帯にのみネットワークで設定を変更し、新しいデバイスをプロビジョニングすることです。

このシナリオでは、Flex プロファイルが AP にプロビジョニングされ、AP モードがローカルから Flex に変更されます。その結果、AP の再起動が必要になり、ワイヤレスクライアントのサービスが中断されます。

ステップ 11　[Now] オプションボタンをクリックします。

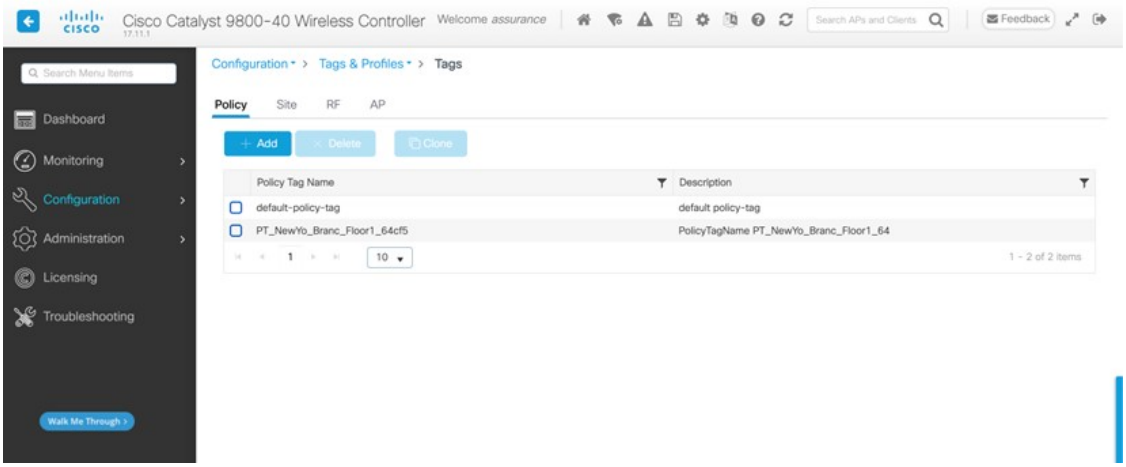
ステップ 12　[Apply] をクリックして設定を適用します。

[Success] ダイアログボックスが表示され、プロビジョニング後に AP が再起動し、AP モードがローカルから Flex に変更されることを示すメッセージが表示されます。

ステップ 13　[OK] をクリックして確定します。メインの [Provisioning] ウィンドウにインベントリのリストが表示されます。AP のプロビジョニングステータスは一時的に [Provisioning] と表示されますが、数分後に [Success] に変わります。詳細については、各 AP のプロビジョニングステータスの下にある [See Details] をクリックして確認してください。

Cisco DNA Center では、プロビジョニングされた AP を含むフロアごとに、Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（C9800-Flex-CVD）に新しいポリシータグが作成されます。

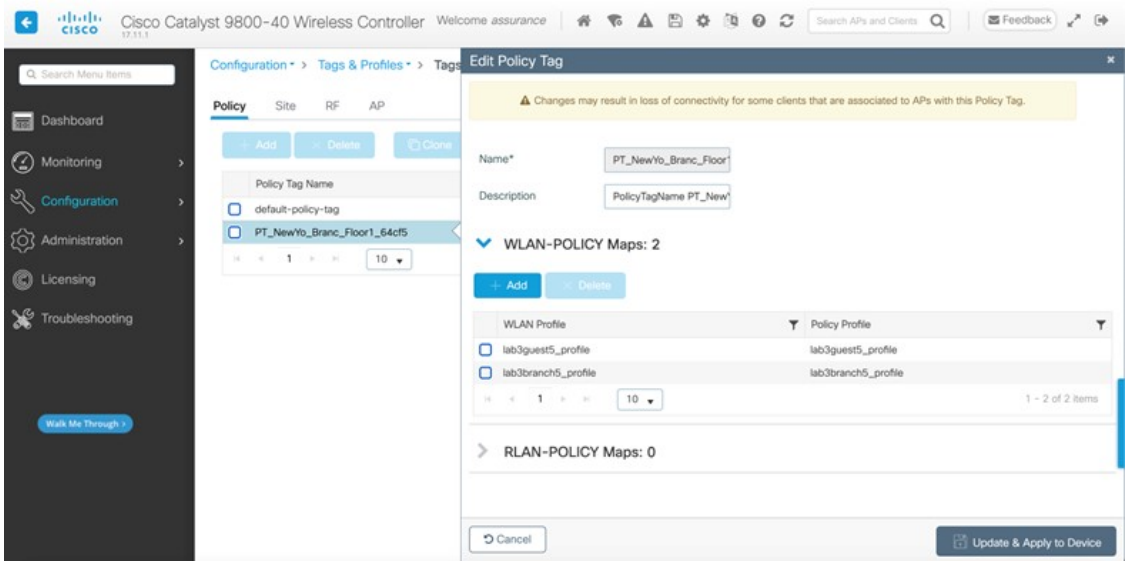
図 *146 : Catalyst 9800-40* エンタープライズ ワイヤレスコントローラで *Cisco DNA Center* によって作成されたポリシータグ



Branch 5 ビルディングの **Floor 1** にプロビジョニングされた AP に対応する 3 つの新しいポリシータグが作成されました。各ポリシータグはサイトに固有であり、ビルディング内の特定のフロアを示します。フロアのポリシータグは、AP がフロアにプロビジョニングされている場合にのみ Cisco DNA Center によって作成されます。

いずれかのポリシータグをクリックすると、Cisco DNA Center によって新しいポリシータグに追加されたポリシープロファイルと WLAN プロファイルを表示できます。

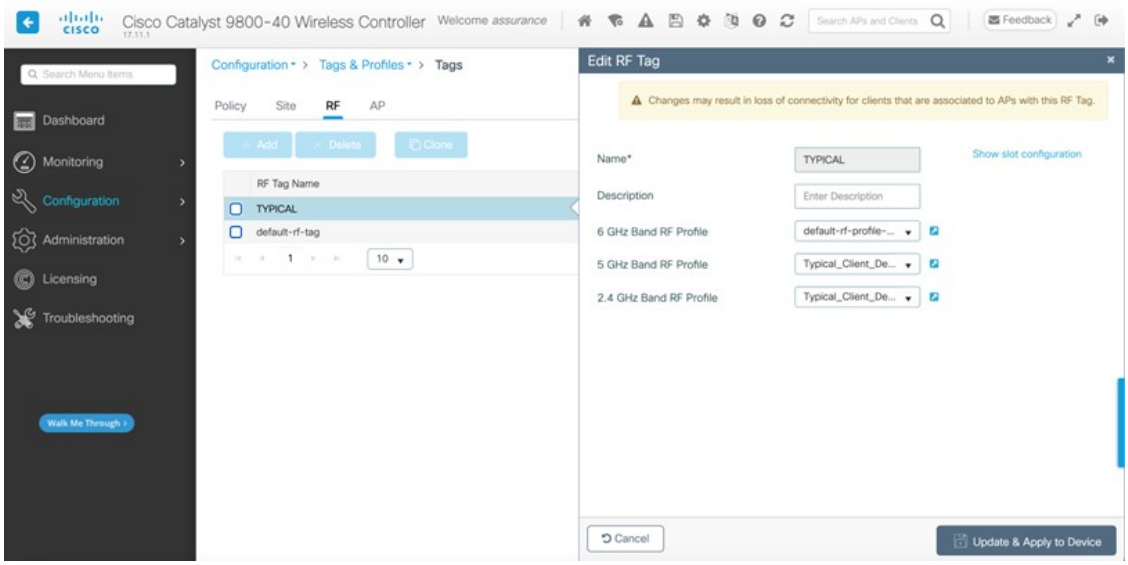
図 *147* : ポリシータグの詳細



Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペアのプロビジョニング中に作成された WLAN プロファイルとポリシープロファイルが、各ポリシータグに追加されています。このプロセスは、「ワイヤレスネットワークの設計」で Cisco DNA Center で作成された **branch5** WLAN プロファイルによって制御されます。**branch5** WLAN プロファイルでは、**lab3branch5** および **lab3guest5** SSID が **New York** エリア全体（**Branch 5** ビルディングの **Floor 1**）にブロードキャストされるように指定されています。

AP のプロビジョニングプロセス中に、TYPICAL RF プロファイルが選択され、Cisco DNA Center により、Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（C9800-Flex-CVD）内に TYPICAL という名前の新しい RF タグが作成されます。

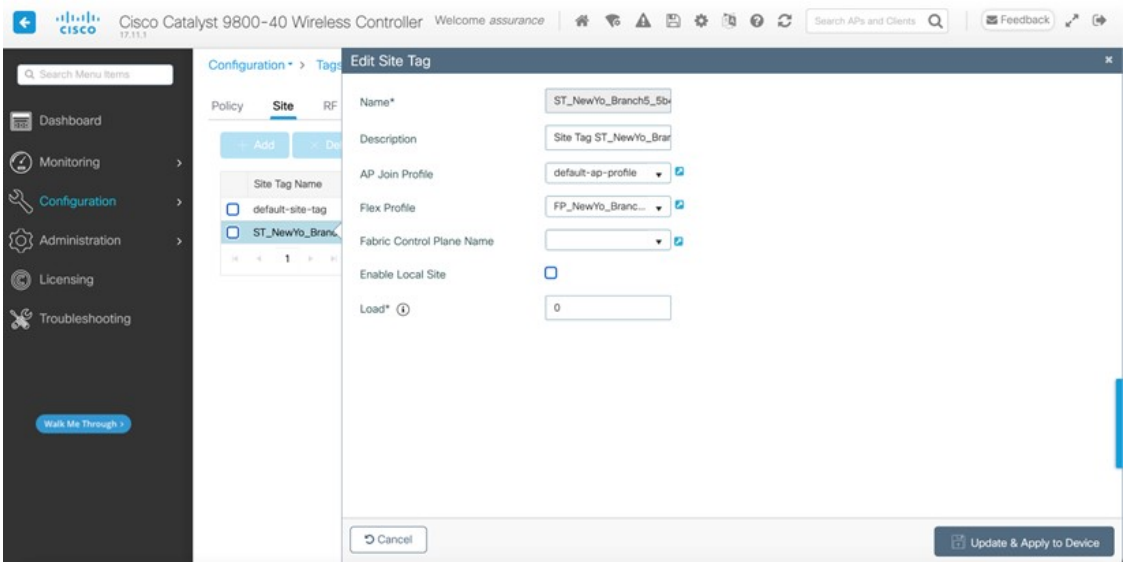
図 *148 : Cisco DNA Center* によって作成された *TYPICAL RF* タグ



最後に、Cisco DNA Center により、ポリシータグ（各フロアに固有）、RF タグ（TYPICAL という名前）、およびサイトタグ（ST_NewYo_Branch5_5b486_0 という名前）が Catalyst 9800-40 エンタープライズ ワイヤレスコントローラ HA SSO ペア（C9800- Flex-CVD）の各 AP に割り当てられます。サイトタグ ST_NewYo_Branch5_5b486_0 には、**default-ap-profile** という名前のデフォルトの AP 参加プロファイルが含まれています。

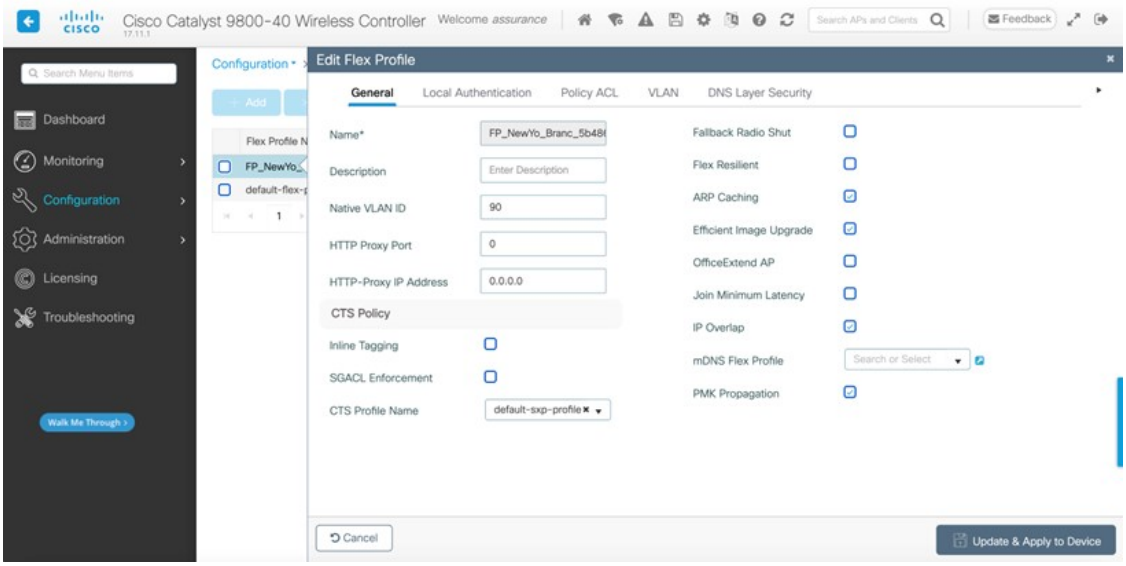
次の図に、各 AP へのポリシータグ、サイトタグ、および RF タグの静的割り当ての例を示します。

図 *149 :* ワイヤレスコントローラ *GUI* に表示されているサイトタグの割り当て



Flexプロファイルがサイトタグにマッピングされていて、ローカルサイトが無効になっています。VLAN 90 で AP をプロビジョニング後、Flex プロファイルがネイティブ VLAN ID で正しく更新されています。

図 *150 :* ワイヤレスコントローラ *GUI* に表示されている *Flex* プロファイル



Flex プロファイルにマッピングされた Flex プロファイルのローカル VLAN を表示するには、Flex プロファイルの [VLAN] タブをクリックします。

図 *151 :* ワイヤレスコントローラ *GUI* に表示されている *Flex* プロファイル

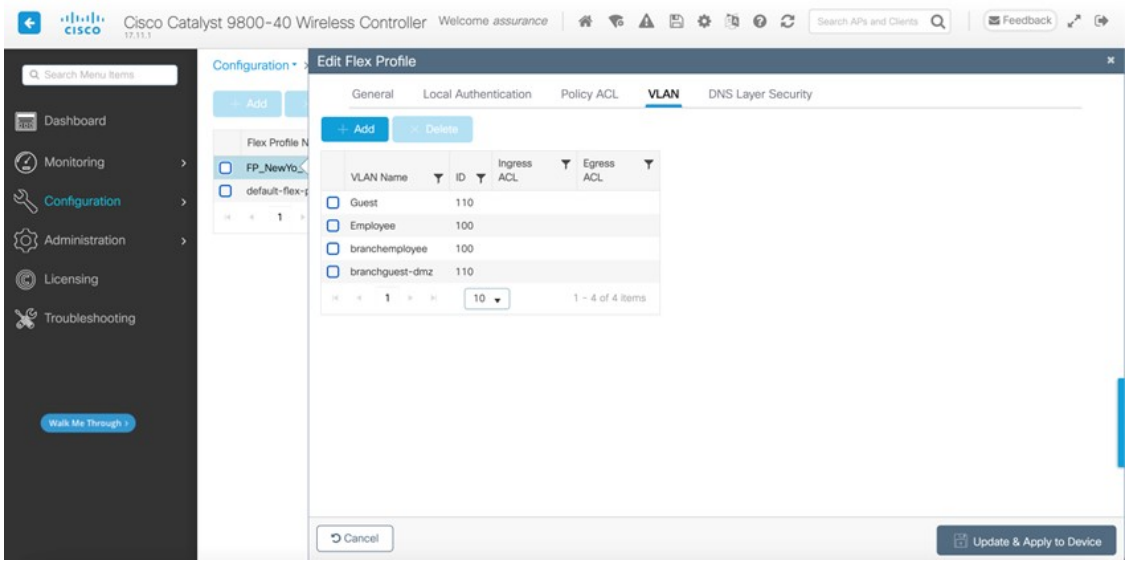
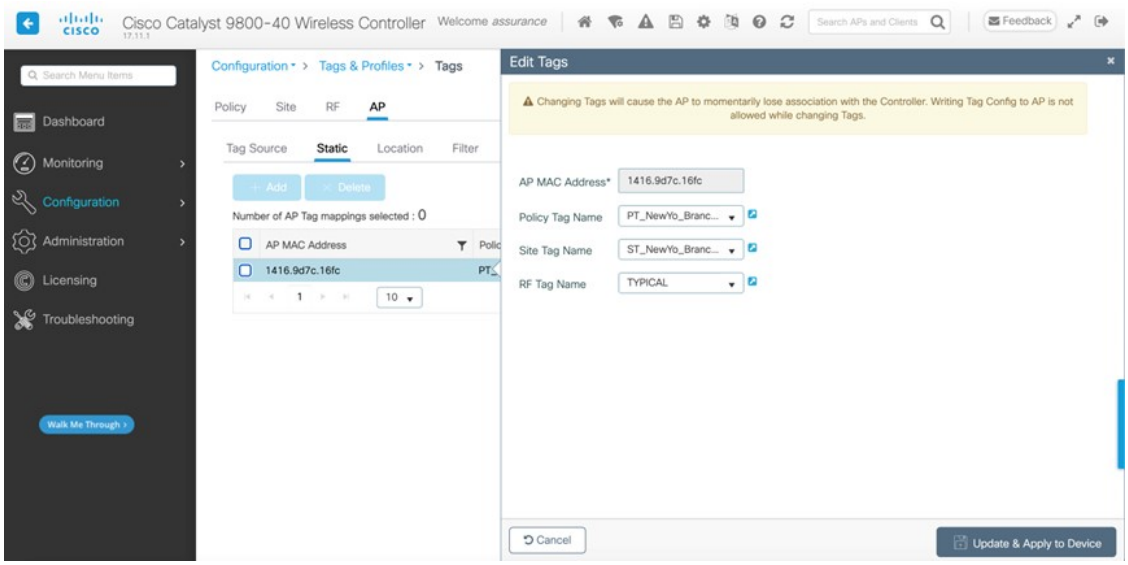


図 *152 : Cisco DNA Center* による *AP* へのタグの静的割り当て



AP にポリシータグを割り当てると、フロアにプロビジョニングされた AP によって、**lab3branch5** および **lab3guest5** SSID がブロードキャストされます。この時点で、ワイヤレスクライアントは **lab3branch5** や **lab3guest5** SSID に関連付けられ、ネットワークに認証される必要があります。

（注） ワイヤレスコントローラをプロビジョニングせずに AP がプロビジョニングされている場合のベストプラクティスは、[Inventory] ウィンドウに移動し、フォーカスを [Provision] に変更することです。[Provisioning Status] 列をモニターして、[Out of Sync] と表示されているワイヤレスコントローラを確認します。表示されている場合は、ワイヤレスコントローラをプロビジョニングして同期状態に戻します。

Cisco DNA Center の新しいリリースでは、追加のワイヤレス機能のサポートが追加され続けます。追加のワイヤレス機能は Cisco DNA Center を使用してプロビジョニングできます。新しい機能がテンプレートプログラマまたは他のツールを使用してプロビジョニングされている場合のベストプラクティスは、ワイヤレスコントローラと AP を Cisco DNA Center からプロビジョニングする前に、設定をプレビューして競合を解決することです。

Cisco DNA Center を新しいリリースにアップグレードする場合は、新しい Cisco DNA Center リリースと互換性のある推奨バージョンにワイヤレスコントローラをアップグレードすることを推奨します。

AWS 展開でホストされるワイヤレスコントローラの WLAN

次の手順では、CloudFormation テンプレートを使用して AWS Marketplace から Cisco Catalyst 9800-CL ワイヤレスコントローラ（C9800-CL）を起動する方法について説明します。

手順

ステップ 1 AWS Marketplace にログインします。

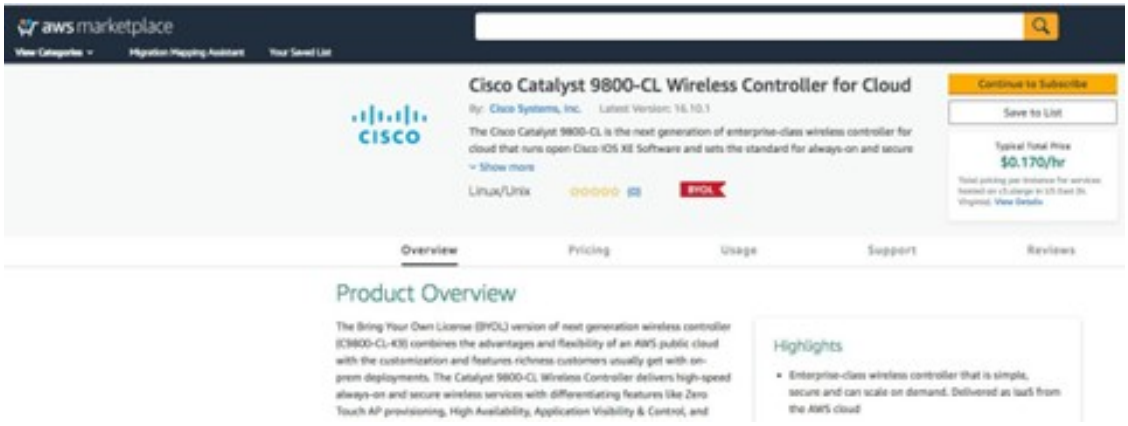
図 *153 : [AWS Marketplace]* ウィンドウ

ステップ 2 Catalyst 9800 または C9800-CL を検索し、検索結果から [Cisco Catalyst 9800-CL ワイヤレスコントローラ for Cloud] ウィンドウをクリックします。

図 *154 : C9800-CL* の検索

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

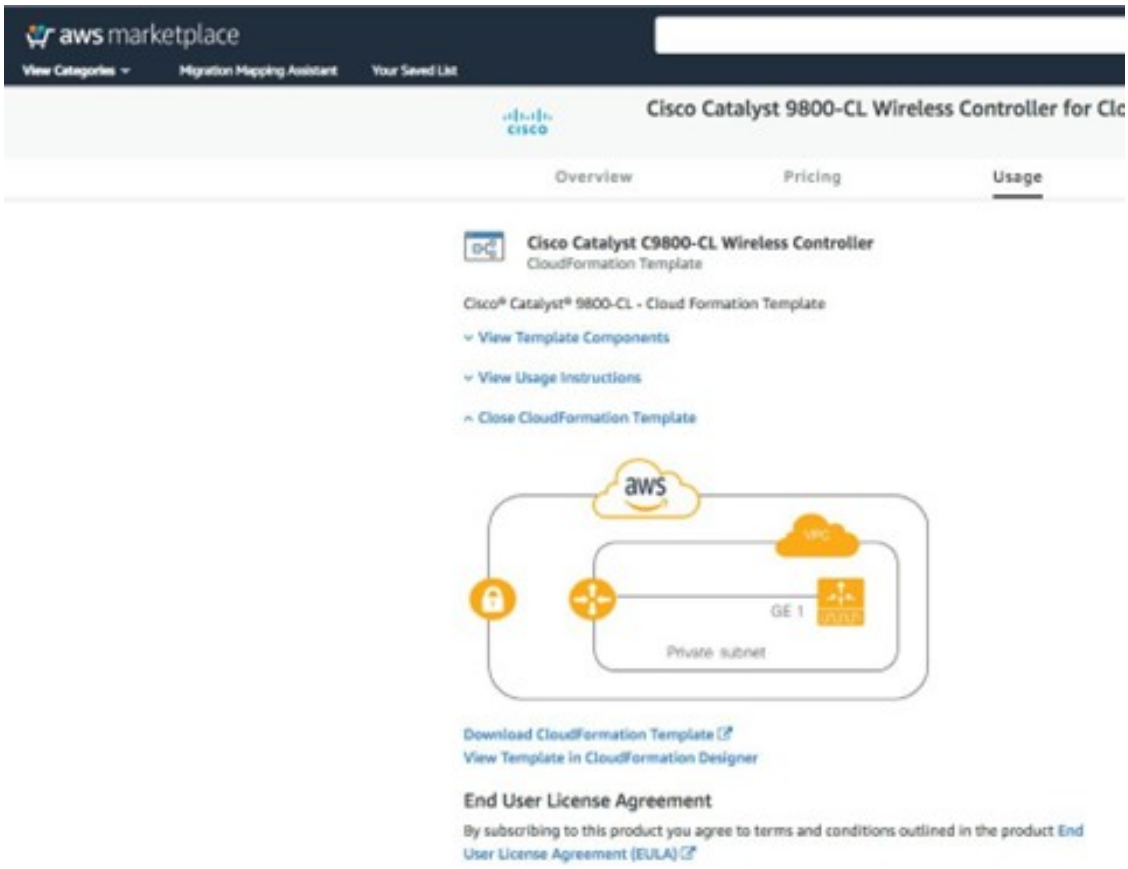
図 *155 :* 製品概要



このウィンドウで製品、サポート、ライセンスに関するすべての情報を確認し、さまざまな AWS リージョンで C9800-CL を導入する場合のコストを見積もれます。

このウィンドウを下にスクロールすると、次の図に示されているようにトポロジと CloudFormation テンプレートに関する情報が表示されます。

図 *156 : CloudFormation* テンプレート



ステップ 4　右上隅にある [Continue to Subscribe] をクリックします。

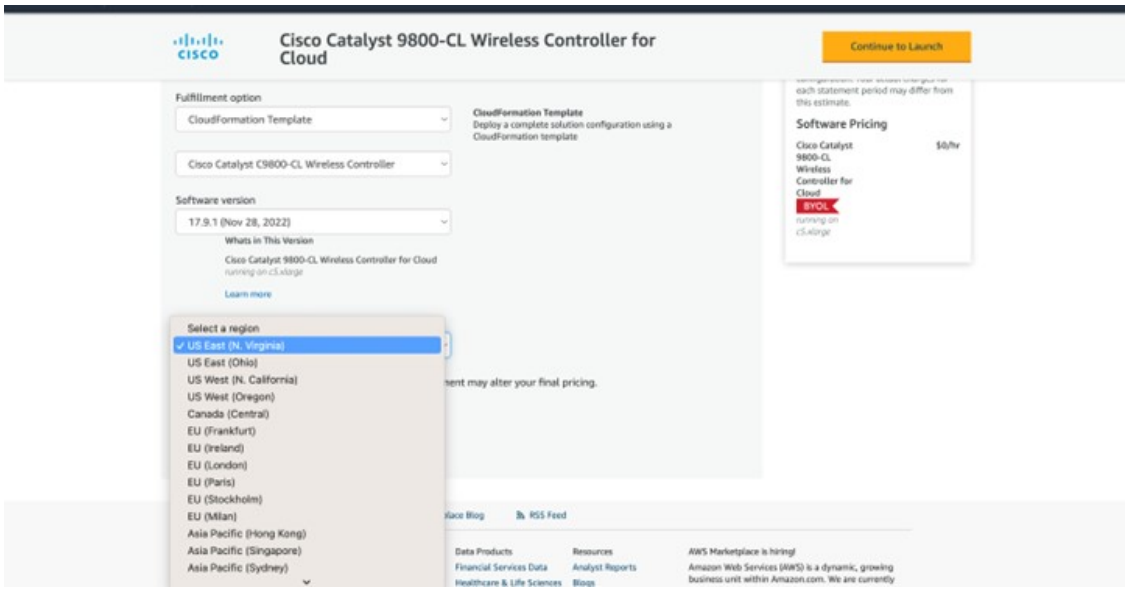
図 *157 : [Subscription]* ウィンドウ

ステップ 5　[Fulfillment Option] として [CloudFormation] を選択します。

図 *158 :* ソフトウェアの設定

ステップ 6　下にスクロールして、C9800-CL インスタンスを作成する [Region] を選択します。

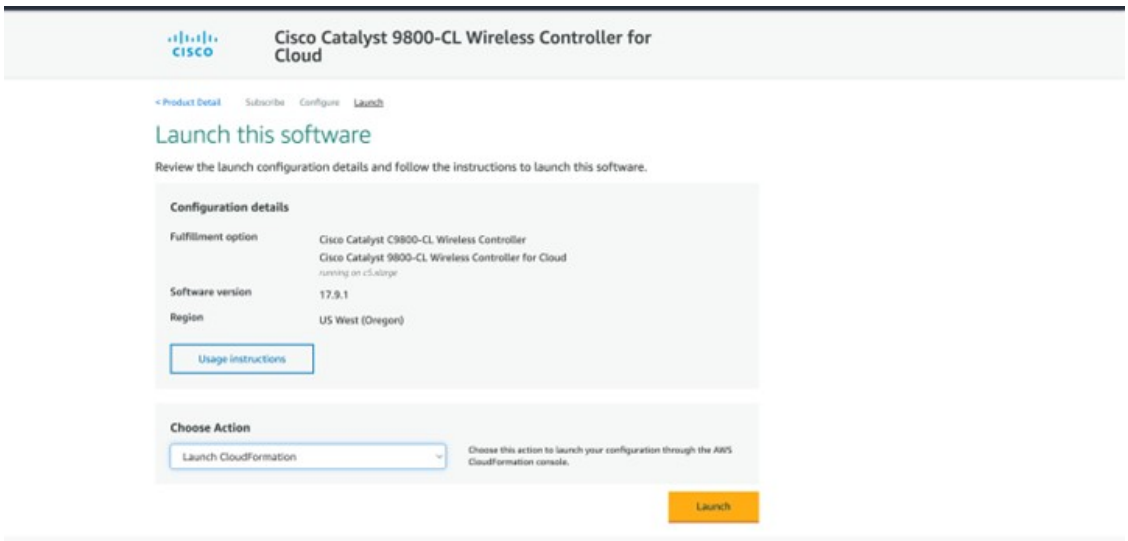
図 *159* : リージョンの選択



ステップ 7 [続行して起動する（Continue to Launch）] をクリックします

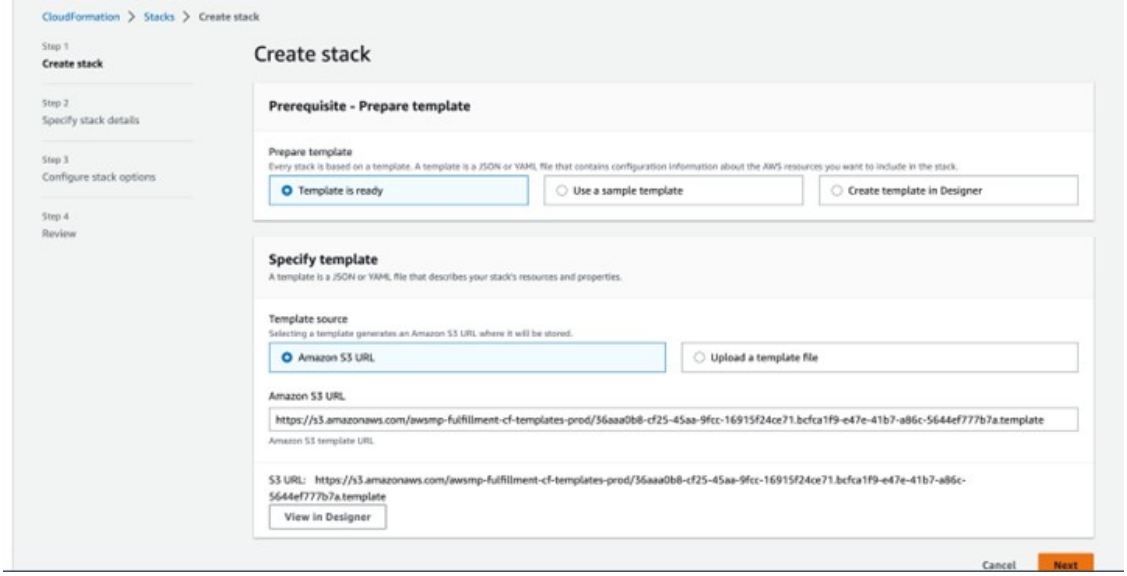
ステップ 8 [作成（Launch）] をクリックします。

図 *160* : ソフトウェアの起動



自動的に AWS コンソールの CloudFormation サービスにリダイレクトされ、次のウィンドウが表示されます。

図 *161 : [Create Stack]* ウィンドウ



ステップ 9 [Next] をクリックします。

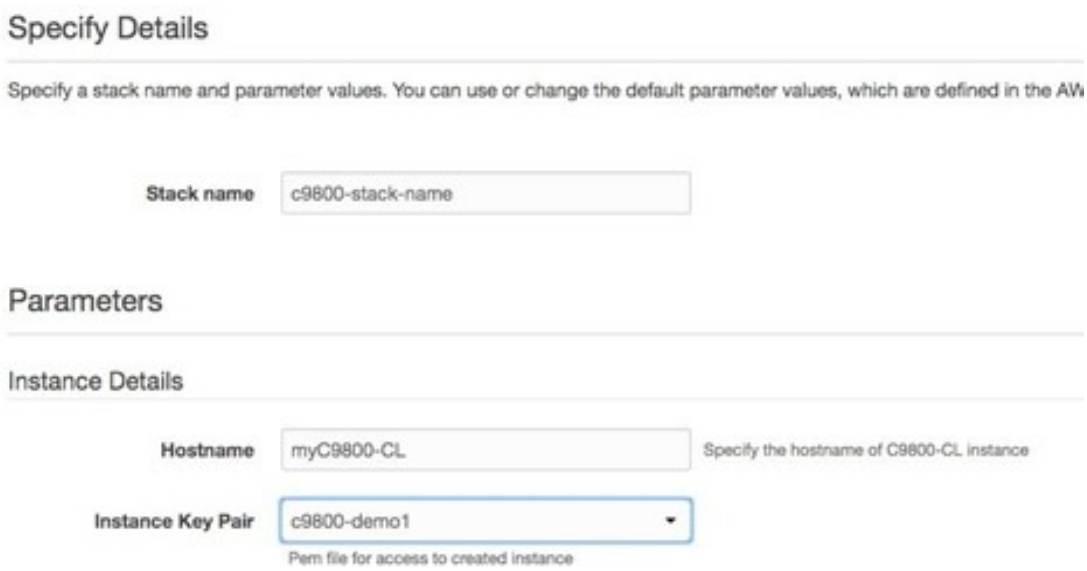
テンプレートは自動的に選択されています。

（注） 仕様上、デフォルトのテンプレートを変更する必要がある場合は、[Upload a template to Amazon S3]オプションボタンをクリックし、関連するファイルを選択することで、別のテンプレートをアップロードできます。

ステップ 10 [Stack name] と [Instance Details] に入力します。

ステップ 11 C9800 の [Hostname] を入力し、以前に作成したキーペアを選択します。

図 *162* : 詳細の指定



ステップ 12 [Network Details] に入力します。

1. ドロップダウンリストから、ワイヤレス管理インターフェイスに割り当てるサブネットとセキュリティグループを選択します。

   （注） 選択したサブネットとセキュリティグループが同じ VPC に属していることを確認してください。

2. 選択したサブネット内で、C9800 インスタンスに割り当てる IP アドレスを入力できます。選択したサブネットに特定の IP が属していること、およびその IP がまだ使用されていないことを確認してください。使用されている場合、スタックの作成は失敗します。

図 *163* : ネットワークの詳細

ステップ 13 （任意）インスタンスにリモート接続するためのユーザー名とパスワードを入力します。

ユーザー名とパスワードを設定しなくても、デフォルトの AWS ユーザー（ec2-user）とインスタンスのキーペアを使用して SSH 経由でログインできます。スケールに合わせてインスタンスタイプを選択します。シスコでは、サポート対象のスケール（1,000 の AP、10,000 のクライアント）に対応する c5.xlarge（デフォルト値）のみサポートしています。

図 *164 :* ユーザーの詳細

ステップ 14 [Next] をクリックします。

ステップ 15 オプションウィンドウでは、デフォルト設定を使用し、[Next] をクリックします。

ステップ 16 設定を確認して [Submit] をクリックします。

図 *165 :* 設定の確認：パート *1*

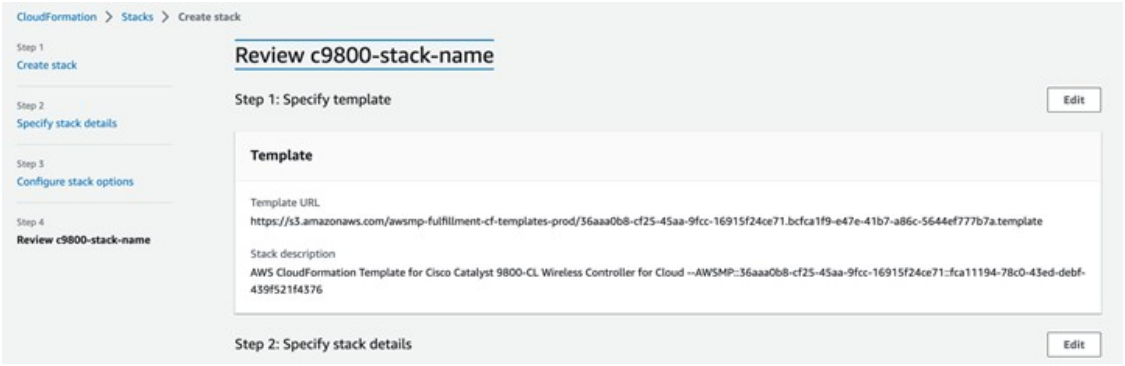
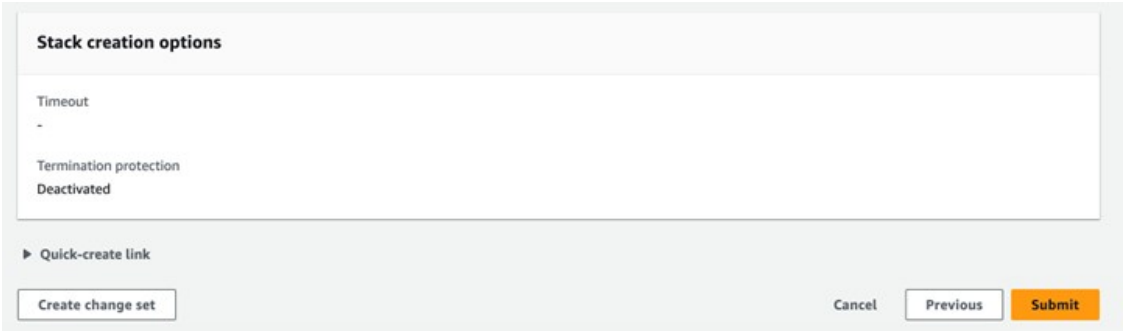
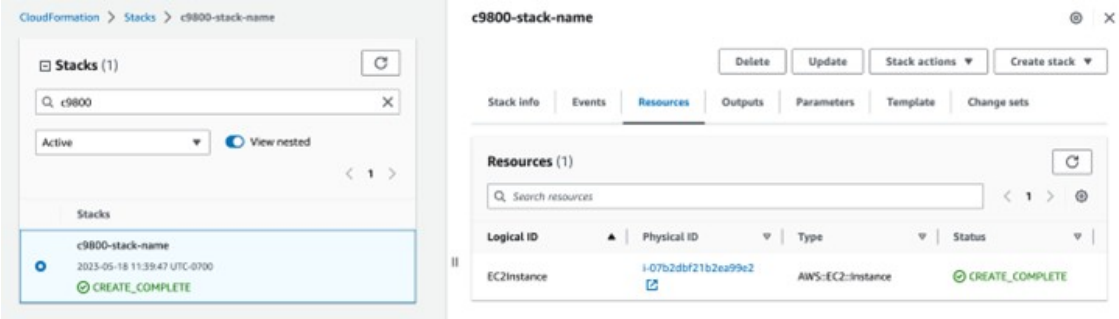


図 *166 :* 設定の確認：パート *2*



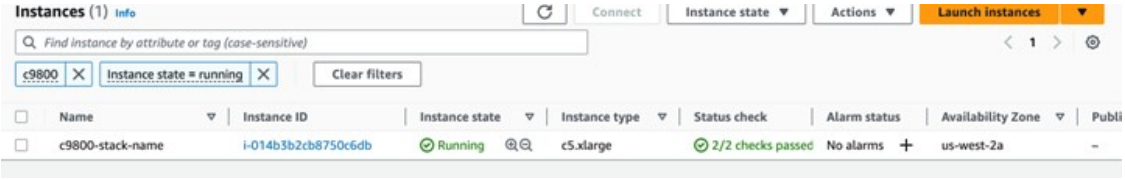
ステップ 17 ステータスが **CREATE_IN_PROGRESS** から **CREATE_CMPLETE** に変わるまで数秒待ちます。

図 *167 :* 設定の完了ステータス



ステップ 18 [EC2] ダッシュボードに移動して [Running Instances] をクリックします。

図 *168 : [EC2]* ダッシュボード



CLI コマンドを使用した Cisco Catalyst 9800-CL ワイヤレスコントローラの設定

Day 0 Web ベースのガイド付きワークフローは、基本設定の CLI コマンドを設定するときにスキップできます。次の手順を実行すると、DAY 1 設定用の GUI にアクセスできます。AWS クラウド上の Cisco Catalyst C9800-CL ワイヤレスコントローラ（C9800-C）の場合、使用できるインターフェイスは GigabitEthernet 1 のみで、次の特性があります。

- レイヤ 3 インターフェイスを使用します（AWS はこのタイプのインターフェイスのみをサポートしています）。
- DHCP を使用して IP アドレスを取得します。
- Catalyst 9800-CL ワイヤレスコントローラ用のワイヤレス CLI ウィザードはありません。

手順

ステップ 1 SSH を介して CLI コマンドにアクセスします。.pem ファイルを使用して、証明書の使用を認証します。

```
chmod 400 <file>.pem
ssh -i “file name.pem” ec2-user@<c9800-CL IP>
```

ステップ 2 （任意）ホスト名を次のように設定します。

```
WLC(config)#hostname C9800
```

ステップ 3 コンフィギュレーション モードを開始し、次のコマンドを使用してログイン情報を追加します。

```
C9800(config)#username <name> privilege 15 password <yourpwd>
```

ステップ 4 GigabitEthernet 1 の設定と IP アドレスを確認します。次のインターフェイスが DHCP 用に設定されています。

```
c9800#sh run int gig 1
Building configuration...
Current configuration : 99 bytes
!
interface GigabitEthernet1
ip address dhcp
negotiation auto
no mop enabled
no mop sysid
end

C9800#show ip int brief

Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet1       172.38.0.10     YES DHCP   up                    up

Vlan1                  unassigned      YES unset  administratively down down

C9800#
```

ステップ 5 ワイヤレスネットワークを無効にして国コードを設定します。

```
C9800(config)#ap dot11 5ghz shutdown
Disabling the 802.11a network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
C9800(config)#ap dot11 24ghz shutdown
Disabling the 802.11b network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
```

ステップ 6 AP の国ドメインを設定します。Catalyst 9800 シリーズ ワイヤレス コントローラが動作するには国コードが必要なため、この設定によって GUI がトリガーされて DAY 0 ワークフローがスキップされます。

```
C9800(config)# c9800-10-30(config)#ap country ?
WORD Enter the country code (e.g. US,MX,IN) upto a maximum of 20 countries

C9800(config)#ap country US
```

国コードを変更すると、チャネルと RRM グループの設定がリセットされる場合があります。このコマンドを実装したら、カスタマイズされた AP で有効なチャネル値を確認し、ワイヤレスコントローラが RRM ワンタイムモードで実行されている場合は、チャネルを再割り当てします。

```
Are you sure you want to continue? (y/n)[y]: y

C9800(config)#
```

ステップ 7 AP が仮想 Catalyst 9800 シリーズ ワイヤレス コントローラ に参加するには、証明書が必要です。この証明書は DAY 0 ワークフローで自動作成するか、次のコマンドを使用して手動で作成できます。

ワイヤレス管理インターフェイスにするインターフェイスを指定します。

```
C9800(config)#wireless management interface gig 1In exec mode, issue the following command:
C9800#wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 <pwd>
Configuring vWLC-SSC…
Script is completed
This is a script the automates the whole certificate creation:Verifying Certificate
Installation:C9800#show wireless management trustpoint
Trustpoint Name : ewlc-default-tp
Certificate Info : Available
Certificate Type : SSC
```

```
Certificate Hash : e55e61b683181ff0999ef317bb5ec7950ab86c9e
Private key Info : Available
```

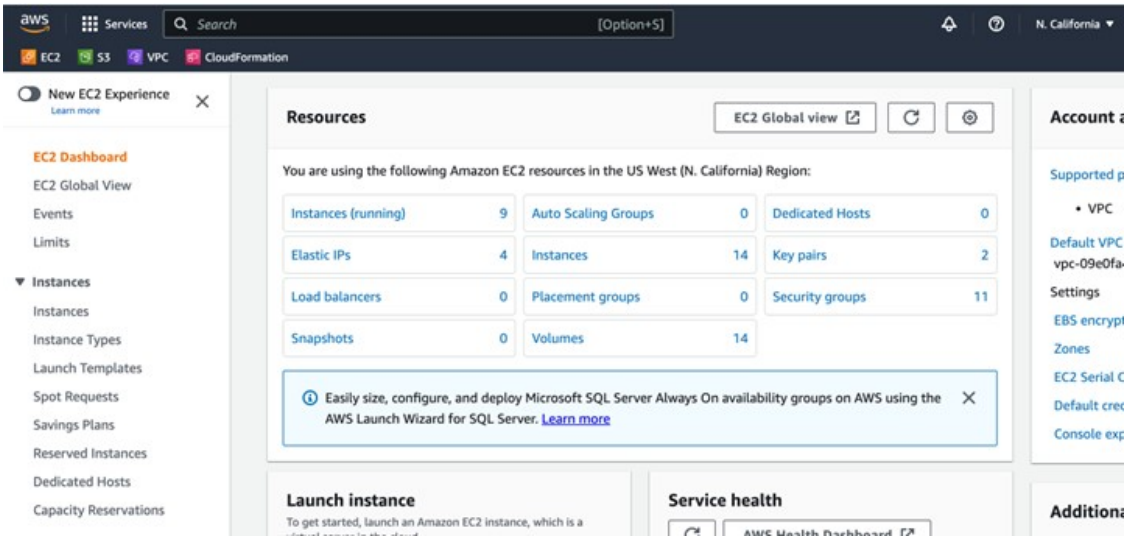
（注） 証明書やトラストポイントの設定は省略できますが、省略すると AP が参加できなくなり、代わりに、目的の証明書をインポートして、GUI から証明書を設定する必要があります。

ステップ 8 メインのダッシュボードにアクセスするには、https://<IP of the wireless management interface> および以前に入力したログイン情報を使用します。ボックスには国コードが設定されているため、GUI では DAY 0 ワークフローがスキップされ、DAY 1 設定用のメインのダッシュボードにアクセスできます。

ステップ 9 Cisco DNA Center から Catalyst 9800-CL ワイヤレスコントローラをプロビジョニングするには、次の手順を使用して管理インターフェイスを DHCP から静的に変更します。

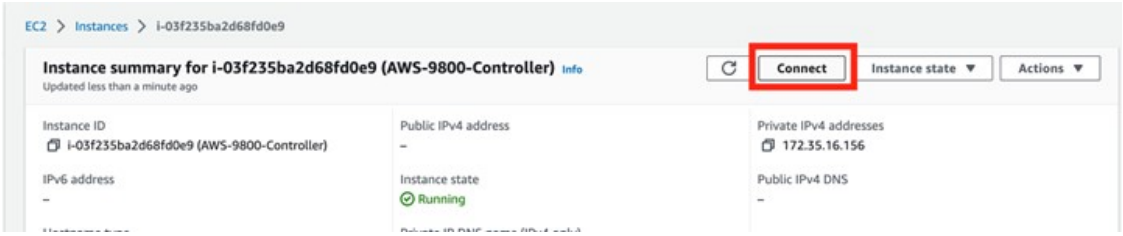
a) AWS コンソールに移動し [EC2] ダッシュボードを見つけます。

図 *169 : [EC2]* ダッシュボード



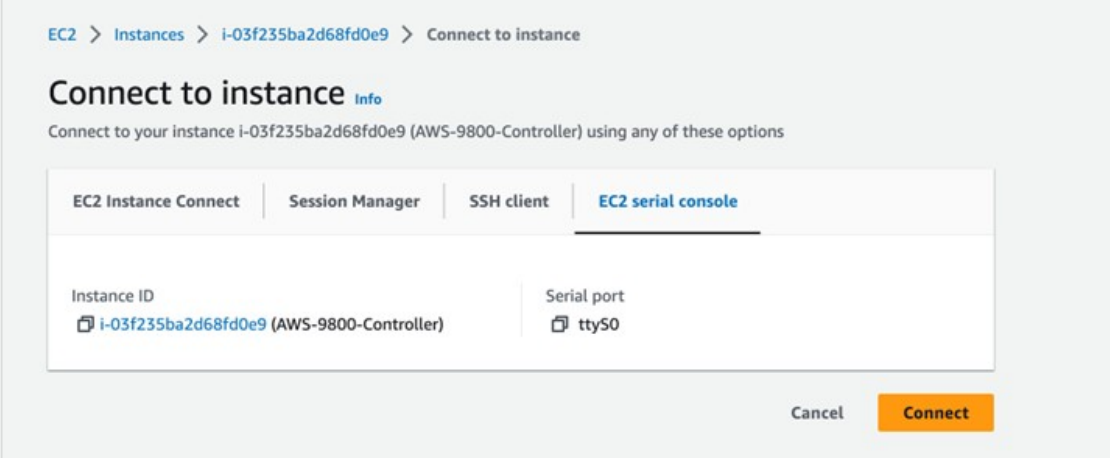
b) [Instances] をクリックし、Catalyst 9800-CL ワイヤレスコントローラ インスタンスを選択します。

図 *170 : EC2* インスタンス



ステップ 10 [接続（Connect）] をクリックします。

図 *171 : [Connect to Instance]* ウィンドウ



ステップ 11 `interface gig 1` で `ip address dhcp` の設定を解除し、静的 IP アドレス `ip address 172.38.0.10` を設定します。

AWS に展開された Cisco Catalyst 9800-CL ワイヤレスコントローラの検出と管理

検出プロセスは、他の Cisco Catalyst 9800-CL ワイヤレスコントローラと同じです。

AWS に展開された Cisco Catalyst 9800-CL ワイヤレスコントローラのプロビジョニング

San Jose エリアがワイヤレスコントローラのプライマリ管理対象 AP の場所になるように、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。

次の手順では、**corpevent-profile** ワイヤレスプロファイル（「ワイヤレスネットワークの定義」で定義）を Catalyst 9800-CL ワイヤレスコントローラにプロビジョニングする方法について説明します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウにデバイスが表示されます。 デフォルトでは、[Focus] は [Default] に設定されています。

ステップ 2 Catalyst 9800 シリーズ ワイヤレス コントローラのチェックボックスを見つけてオンにします。

ステップ 3 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 4 [Choose a Site] をクリックします。

slide-in paneが表示され、Cisco DNA Center に設定されたサイト階層が示されます。この導入ガイドでは、Catalyst 9800 シリーズ ワイヤレス コントローラはビルディングレベルに割り当てられます。

ステップ 5 San Jose のサイト階層を展開し、[Eventcenter] を選択します。

ステップ 6 [Save] をクリックして、Catalyst 9800 シリーズ ワイヤレス コントローラを San Jose/Eventcenter に割り当てます。

ステップ 7 [Next] をクリックして、デバイス プロビジョニング ワークフローの次のステップに進みます。

ステップ 8 [Configuration] ウィンドウで、[WLC Role] の [Active Main WLC] を選択します。

ステップ 9 [Summary] ウィンドウが表示されるまで、[Next] をクリックし続けます。

[Summary] ウィンドウに、Catalyst 9800 シリーズ ワイヤレス コントローラにプロビジョニングされる設定の概要が表示されます。

各セクションを展開すると、設定の詳細を確認できます。設定は、この導入ガイドの「ワイヤレスネットワークの設計」で作成された **branch5** ワイヤレスプロファイルに基づいています。

ステップ 10 [Deploy] をクリックして、設定を Catalyst 9800-40 ワイヤレスコントローラに展開します。slide-in paneが表示されます。設定は今すぐ展開できます。あるいは、後で展開するようにスケジュールでき、設定のプレビューも生成できます。プレビューの生成を選択した場合、作成されたプレビューは選択したデバイスに後で展開できます。設定のプレビュー中にサイトの割り当てが呼び出されると、デバイスの可制御性設定が対応するデバイスにプッシュされます。[Work Items] でステータスを確認できます。

（注） ベストプラクティスは、スケジュールされたネットワーク運用の変更時間帯にのみネットワークで設定を変更し、新しいデバイスをプロビジョニングすることです。

ステップ 11 [Now] オプションボタンをクリックし、[Apply] をクリックして設定を適用します。

[Provisioning] ダッシュボード内の [Inventory] ウィンドウに戻ります。デバイスののプロビジョニングステータスは一時的に [Configuring] に設定されますが、数分後に [Success] に変わります。プロビジョニングの詳細については、デバイスのプロビジョニングステータスのすぐ下にある [See Details] をクリックして確認してください。

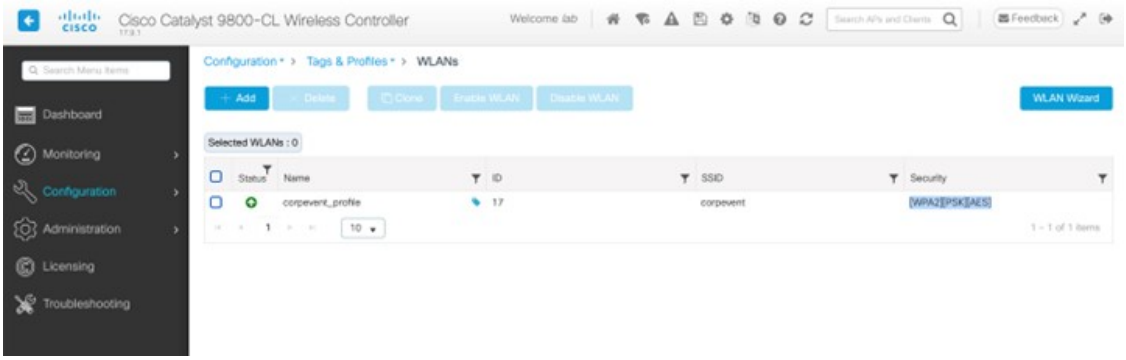
次の表に、この導入ガイドの Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング中に Cisco DNA Center によって自動的に生成される WLAN プロファイルの名前と各プロファイルの SSID を示します。

表 *32 : Cisco DNA Center* によって動的に生成される *WLAN* プロファイル

WLAN Profile Name	SSID	WLAN ID	セキュリティ
corpevent_profile	corpevent	17	[WPA2][PSK][AES]

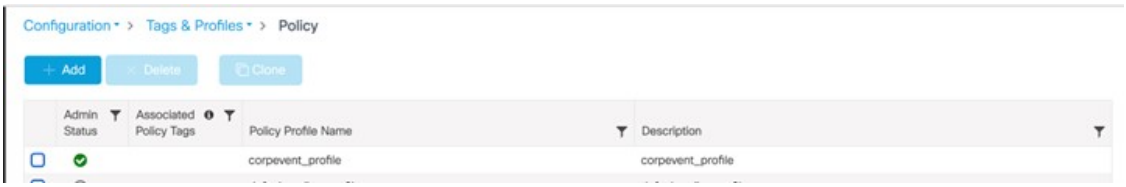
次の図に、Catalyst 9800 シリーズ ワイヤレス コントローラ-1 の Web ベースの GUI から見た WLAN 設定の例を示します。

図 *172 : Cisco DNA Center* によって動的に作成された *WLAN/SSID*



プロビジョニング中に、Cisco DNA Center によって Catalyst 9800 シリーズ ワイヤレス コントローラ に新しいポリシープロファイルが作成されます。新しいポリシープロファイルの名前は、作成された WLAN プロファイルの名前と一致します。次の図に、Catalyst 9800 シリーズ ワイヤレス コントローラ の Web ベースの GUI から見た設定の例を示します。

図 *173 : Cisco DNA Center* によって作成されたポリシータグ



プロビジョニングプロセスのこの時点では、ポリシープロファイルと WLAN プロファイルは、AP に適用されるポリシータグにはマッピングされません。同様に、Flex プロファイルは作成されていません。

エンタープライズ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの新しい AP の参加

次の手順では、AP を検出してエンタープライズCatalyst 9800 シリーズ ワイヤレス コントローラに参加させる方法について説明します。

始める前に

導入ガイドのこの手順では、新しい AP が IP DHCP 検出を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出し、新しい APはまだプライミングされていないことを前提としています。以前ワイヤレスコントローラに参加（CAPWAP トンネルを確立）し、ワイヤレスコントローラ の IP アドレスを NVRAM にキャッシュしている場合、あるいは、プライマリ、セカンダリ、またはターシャリ ワイヤレスコントローラ管理 IP アドレスが AP 内で設定されている場合、その Cisco AP はプライミングされています。そのようなシナリオの AP では、IP DHCP 検出よりもプライマリ、セカンダリ、またはターシャリ ワイヤレスコントローラの設定が優先されます。

IP DHCP 検出では、DHCP サーバーはオプション 43 を使用して、1 つ以上のワイヤレスコントローラ 管理 IP アドレスを AP に提供します。AP が Catalyst 9800 シリーズ ワイヤレス コントローラの管理 IP アドレスを学習すると、ワイヤレスコントローラに CAPWAP 参加要求メッセージが送信されます。ワイヤレスコントローラが参加すると、AP の設定、ファームウェア、制御トランザクション、およびデータトランザクションが管理されます。

手順

ステップ 1 Catalyst 9800 シリーズ ワイヤレス コントローラに参加する Cisco AP をサポートするレイヤ 2 アクセススイッチで必要な VLAN を設定します。

この導入ガイドでは、APがレイヤ2アクセススイッチに接続されていることを前提としています。専用の VLAN は、PC や IP フォンなどのエンドユーザーデバイスとは別の AP 用のスイッチ上にあります。AP およびスイッチ管理に専用の VLAN を使用することは、一般に設計上のベストプラクティスと見なされますが、この方法ではスイッチに追加の VLAN が展開されます。

管理 VLAN（VLAN 64）は、ブランチ AP への CAPWAP トンネルを確立し、ブランチスイッチへの接続を管理するために使用されます。ブランチ従業員 VLAN（VLAN 16）は、ブランチスイッチの企業イベント SSID からのワイヤレストラフィックをローカルで終端するために使用されます。

ステップ 2 ブランチスイッチで VLAN 64 と VLAN 16 を設定します。

ステップ 3 APが接続されているスイッチポートをトランクポートに設定し、許可されている VLAN 64 と 16 を使用して、VLAN 16 をネイティブ VLAN として設定します。スイッチポートがシャットダウンされていないことを確認します。次に設定の例を示します。

```
interface GigabitEthernet1/0/1
switchport trunk native vlan 64
switchport trunk allowed vlan 16,64
switchport mode trunk logging event trunk-status load-interval 30
no shutdown
spanning-tree portfast trunk
ip dhcp snooping trust
```

この導入ガイドでは、IP アドレス `10.4.48.9` の Microsoft Active Directory（AD）サーバーが IP DHCP サーバーとして機能します。DHCP オプション 43 内で設定された Catalyst 9800 シリーズ ワイヤレス コントローラ（AWS に展開された C9800-CL）の IPv4 アドレスは `172.38.0.10`です。Microsoft AD サーバー内の DHCP の設定は、このマニュアルの範囲外です。

次に、VLAN スイッチ仮想インターフェイス（SVI）を使用したレイヤ 3 スイッチの設定例を示します。

```
interface Vlan64
ip address 10.5.64.1
255.255.255.0
ip helper-address 10.4.48.10

interface Vlan16
ip address 10.5.16.1
255.255.255.0
ip helper-address 10.4.48.10
```

ステップ 4 Cisco AP をレイヤ 2 アクセススイッチのスイッチポートに接続します。

AP は IP アドレスを取得し、Catalyst 9800 シリーズ ワイヤレス コントローラに自動的に参加する必要があります。新しい AP がワイヤレスコントローラに登録されると、Cisco DNA Center での再同期が自動的にトリガーされます。再同期が完了すると、新しい AP がインベントリに表示されます。あるいは、次の手順を使用して、ワイヤレスコントローラのインベントリを手動で再同期できます。

1. 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。
2. デバイス名のチェックボックスをオンにします。

3. [Actions] ドロップダウンリストから [Inventory] > [Resync Device] の順に選択します。
4. 警告ウィンドウで [OK] をクリックして、再同期を確認します。

Catalyst 9800-40 ワイヤレスコントローラ HA SSO ペア（WLC-9800-2）を再同期すると、ワイヤレスコントローラに参加している AP がインベントリ内に表示されます。

新しい AP のプロビジョニング

AP が Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに参加したら、参加した AP をプロビジョニングする必要があります。AP が正しい設定を受信して **corpevent** SSID をアドバタイズするためには、Cisco DNA Center を使用してプロビジョニングする必要があります。

Cisco DNA Center 内で AP をプロビジョニングするには、次の手順を使用します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Provision]** > **[Inventory]** の順に選択します。

メインの [Provisioning] ウィンドウにデバイスが表示されます。デフォルトでは、[Focus] は [Inventory] に設定されます。

ステップ 2 プロビジョニングする各 AP のチェックボックスを見つけてオンにします。

ステップ 3 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

AP をプロビジョニングするためのワークフローが表示されるので、[Assign Site] から開始します。

ステップ 4 AP ごとに、[Choose a Site] をクリックします。

slide-in paneが表示され、Cisco DNA Center に設定されたサイト階層が示されます。Milpitas のサイト階層を展開し、各 AP のビルディング（**Branch 5**）とフロア（**Floor 1** または **Floor 2**）を選択します。

次の表に、この導入ガイドでプロビジョニングされている AP と各 AP の場所を示します。

AP 名	AP Model	ロケーション
mil23-floor1-ap1	C9130AXI-B	Building 23、Floor 1
mil23-floor1-ap2	C9130AXI-B	Building 23、Floor 1
mil23-floor2-ap1	C9130AXI-B	Building 23、Floor 2
mil24-floor1-ap1	C9124AXD-B	Building 24、Floor 1
mil24-floor2-ap1	C9124AXD-B	Building 24、Floor 2
AP1416.9D7C.16FC	C9130AXI-B	Branch 5、Floor 1
AP1416.9D7C.16F8	C9130AXI-B	Branch 5、Floor 2

ステップ 5 [Save] をクリックし、AP のサイトの割り当てを保存します。

ステップ 6 [Next] をクリックして、プロビジョニング ワークフローの次のステップ [Configuration] に進みます。

ステップ 7 [RF Profile] ドロップダウンリストから、各 AP に割り当てる RF プロファイルを選択します。

この導入ガイドでは、TYPICAL RF プロファイルが選択されています。この RF プロファイルは 、「ワイヤレスネットワークの設計」でもデフォルトの RF プロファイルとして選択されています。

ステップ 8 [Next] をクリックして、プロビジョニング ワークフローの次のステップ [Summary] に進みます。

[Summary] ウィンドウに、各 AP にプロビジョニングされる設定の概要が表示されます。

ステップ 9 [Deploy] をクリックして、AP をプロビジョニングします。

slide-in paneが表示されます。設定を今すぐ展開することも、後で設定をスケジュールすることもできます。

（注） ベストプラクティスは、スケジュールされたネットワーク運用の変更時間帯にのみネットワークで設定を変更し、新しいデバイスをプロビジョニングすることです。

ステップ 10 [Now] オプションボタンをクリックし、[Apply] をクリックして設定を適用します。

[Success] ダイアログボックスが表示され、プロビジョニング後に AP が再起動することが示されます。

ステップ 11 [OK] をクリックして確定します。

Cisco DNA Center を使用してプロビジョニングされたポリシー、サイト、および RF タグは、ワイヤレスコントローラ GUI で確認できます。

この時点で、ワイヤレスクライアントは **corpevent** SSID に関連付けられ、ネットワークを認証できる必要があります。

ワイヤレスネットワークの監視および操作

ここでは、すでにネットワークを展開している Cisco DNA Center を介したワイヤレスネットワークの日常的なモニタリングと操作について説明します。

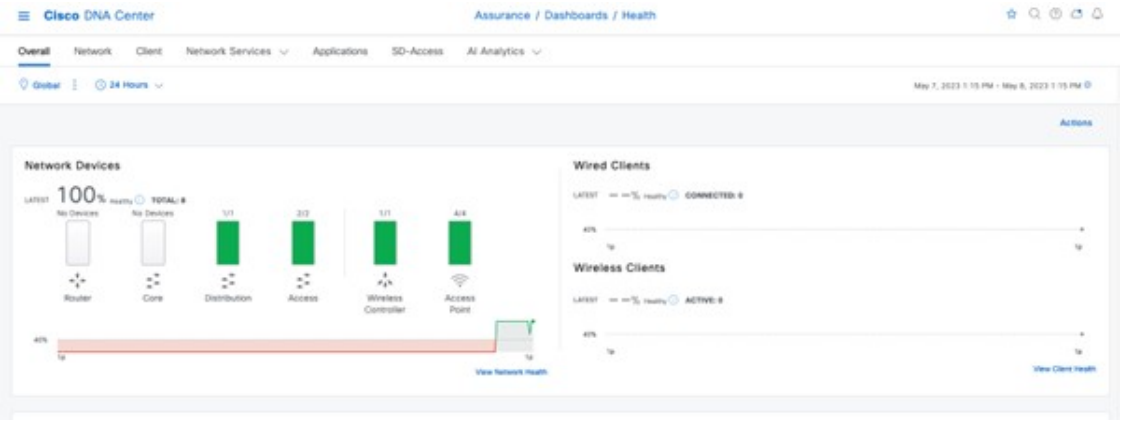
ワイヤレスネットワークの正常性の監視

Cisco DNA Center は、重要な重要業績評価指標（KPI）を使用してスコアを計算することで、ネットワークの正常性を監視します。デバイスの正常性は、デバイスごとに収集された KPI を使用して計算されます。デバイスタイプごとに、異なる KPI を使用して正常性が計算されます。たとえば、AP では干渉、使用率、電波品質、ノイズなどの RF パラメータが使用され、ワイヤレスコントローラ ではリンクエラー、空き Mbuf、パケットプール、空きタイマー、WQE プールが使用されます。デバイスの正常性は、[Global] サイトの Cisco DNA Center に表示され、個々のデバイスレベルは [Assurance] セクションに表示されます。

グローバルレベルのネットワークの正常性

[Health]左上隅にあるメニューアイコンをクリックして、**アシュアランス** > 。[Overall Health] ウィンドウが表示され、デバイスの総数に対する正常なデバイスの比率によって定義されるグローバルレベルのネットワークの正常性が示されます。

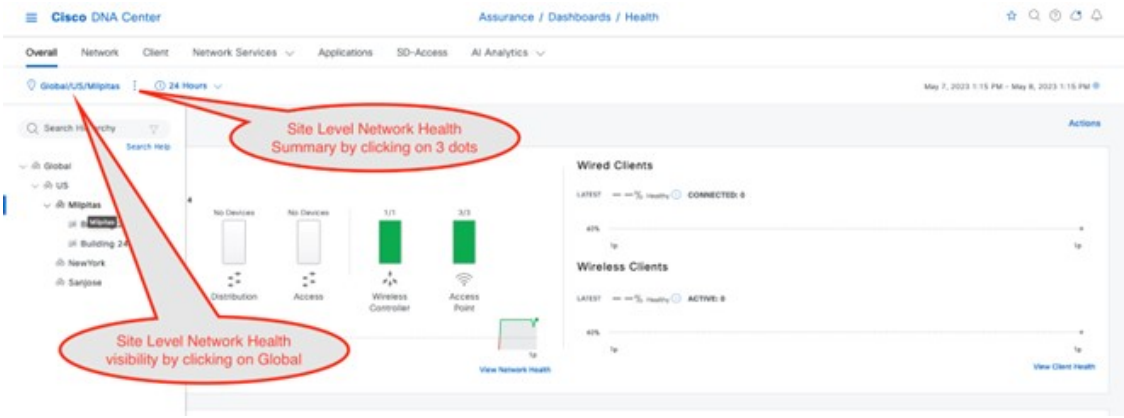
図 *174 : [Overall]* ウィンドウ



サイトレベルのネットワークの正常性

Global をクリックしてサイトレベルのネットワークの正常性を表示するか、 をクリックしてサイトレベルのネットワークの正常性の概要を表示します。

図 *175 :* サイトレベルのネットワークの正常性



デバイスレベルの正常性

[Network] タブをクリックします。[Network Devices] ダッシュボードの [Device Name] 列で、デバイス名をクリックします。

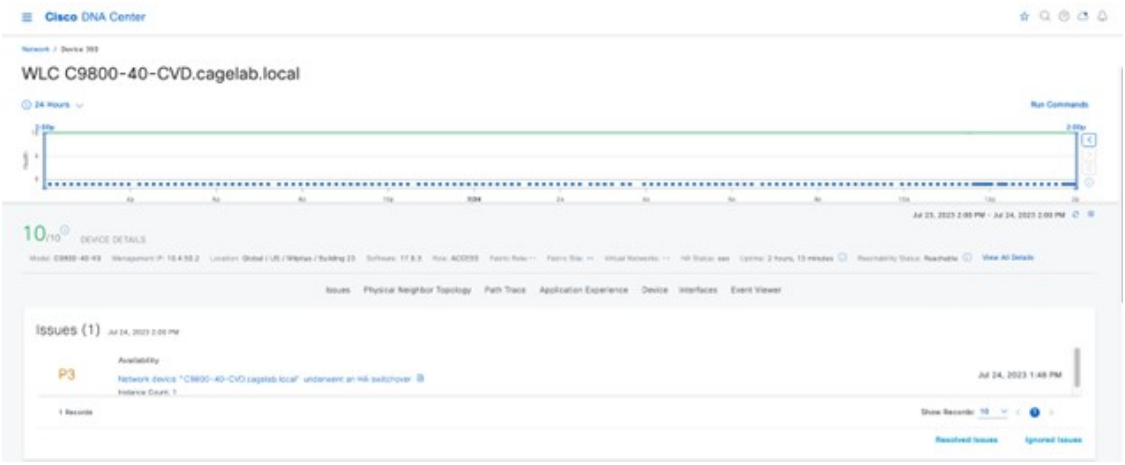
[Device 360] ウィンドウに、ネットワークデバイスの 360 度ビューが表示され、一定期間の正常性の変化が示されます。タイムラインスライダにカーソルを合わせ、一定期間のネットワークデバイスに関する正常性およびイベント情報を表示できます。

ワイヤレスコントローラ 360

正常性タイムラインは、[Device 360] ウィンドウの上部に表示されます。モデル、管理 IP、場所、現在のソフトウェアバージョン、高可用性ステータスなどのデバイスレベルの詳細が [Device Details] エリアに表示されます。タイムラインにカーソルを合わせると、詳細が表示されます。左上隅にあるドロップダウンリストから目的の時間を選択して、過去 3 時間、24 時間、または 7 日間の統計情報を確認できます。正常性プロットは最大 30 日間使用できます。

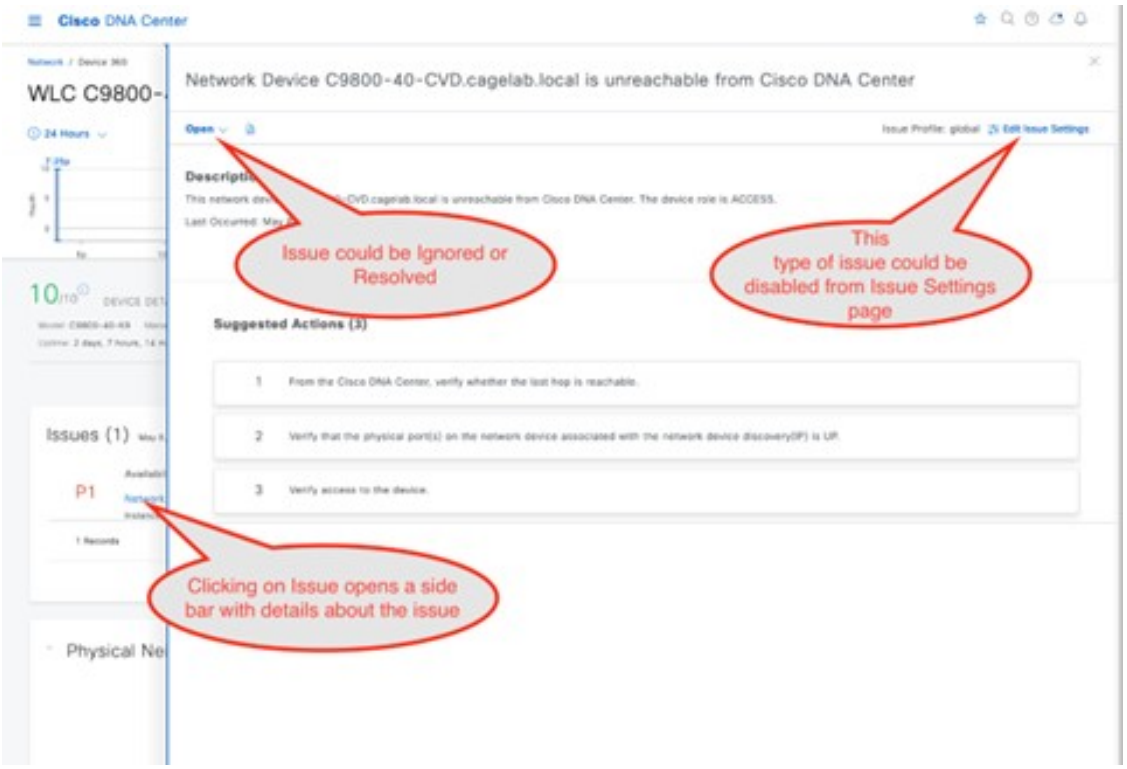
（注） ワイヤレスコントローラの正常性を表示するには、サイトにワイヤレスコントローラを割り当ててください。

図 *176 : [Device 360]* ウィンドウ



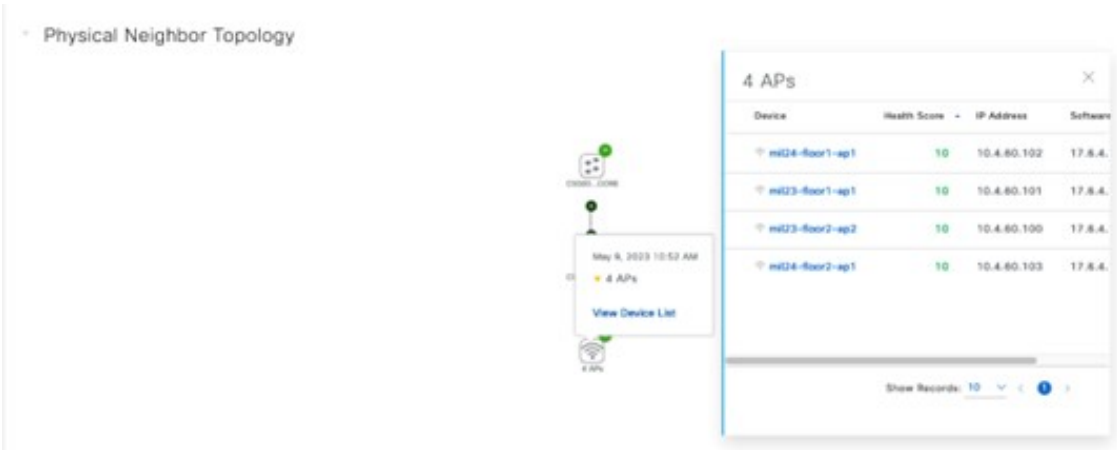
[Issues] セクションには、重大な問題（存在する場合）とその問題の簡単なタイトルが表示されます。対応する問題のタイトルをクリックすると、その問題に関する詳細が表示されます。**[Assurance]** > **[Issue Settings]**の順に選択し、問題に固有のカテゴリとそのしきい値を有効または無効にできます。

図 *177* : ワイヤレスコントローラの問題の例



[Physical Neighbor Topology] セクションでは、ネクストホップデバイスとの接続が可視化されます。デバイスにカーソルを合わせるか、デバイスをクリックして詳細を表示します。このチャートには、ワイヤレスコントローラに関連付けられている AP とクライアントの総数が表示されます。

図 *178* : 物理ネイバートポロジ



[Event Viewer] セクションには、ワイヤレスコントローラのイベントが統合されて表形式で表示されます。syslog メッセージに関連付けられたイベントは、生成された問題に対して作成され、[Issues] セクションに表示されます。このカスタム問題を作成するには、**[Assurance]** > **[Issue Settings]** > **[User Defined]**の順に選択して、[Create an Issue] をクリックします。

[Path Trace] セクションは、ワイヤレスコントローラと接続先デバイス間のルーティングの問題を特定するのに役立ちます。パストレースは、接続先デバイスに至るすべてのデバイスが Cisco DNA Center で検出された場合にのみ機能します。

（注） [Live Traffic] を使用するには、**[Design]** > **[Network Settings]** > **[Telemetry]**から有線エンドポイントのデータ収集を有効にする必要があります。また、関連付けられているすべてのデバイスを [Inventory] ページからプロビジョニングする必要があります。

[Application Experience] セクションには、ワイヤレスコントローラによって認識されるワイヤレスクライアントからのアプリケーション トラフィックが表示されます。APがローカルモードの場合、ワイヤレスコントローラはアプリケーション トラフィック エクスポータになります。AP が Flex モードの場合、トラフィックを伝送するいずれかのスイッチやルータから、Cisco DNA Center にアプリケーション トラフィック情報がエクスポートされる必要があります。ワイヤレスコントローラの 17.10.1 以降でも、Flex モードの AP は、ワイヤレスコントローラ経由で Cisco DNA Center にアプリケーション トラフィックを送信できます。

[Detail Information] セクションには、[Device] および [Interfaces] サブセクションがあります。[Device] セクションには、ワイヤレスコントローラの稼働時間、温度、HA、および最後のリロード理由に関する情報が表示されます。チャートには、一定期間の CPU、メモリ、温度、および AP 数が表示されます。クライアント数チャートには、ローカル、外部、アンカー、およびアイドル情報が表示されます。

図 *179* : デバイスの詳細

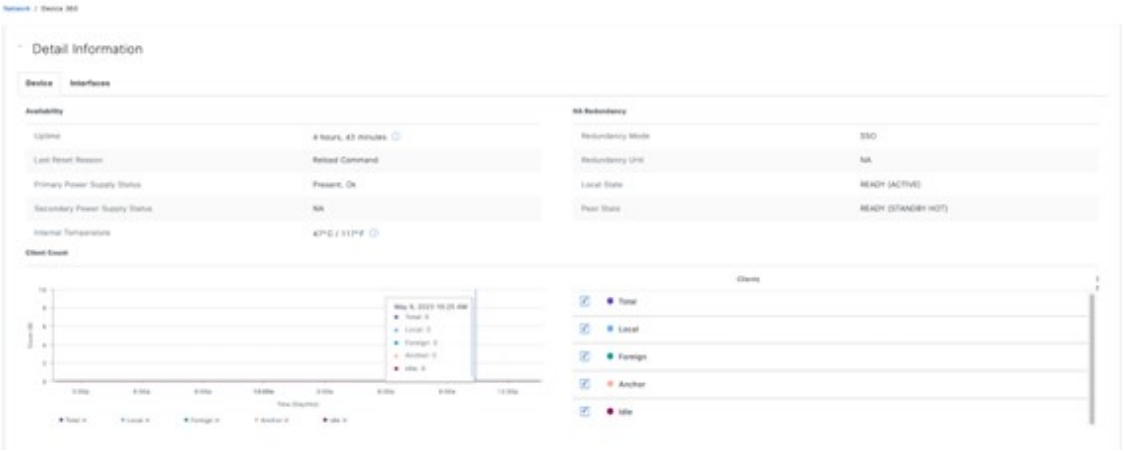
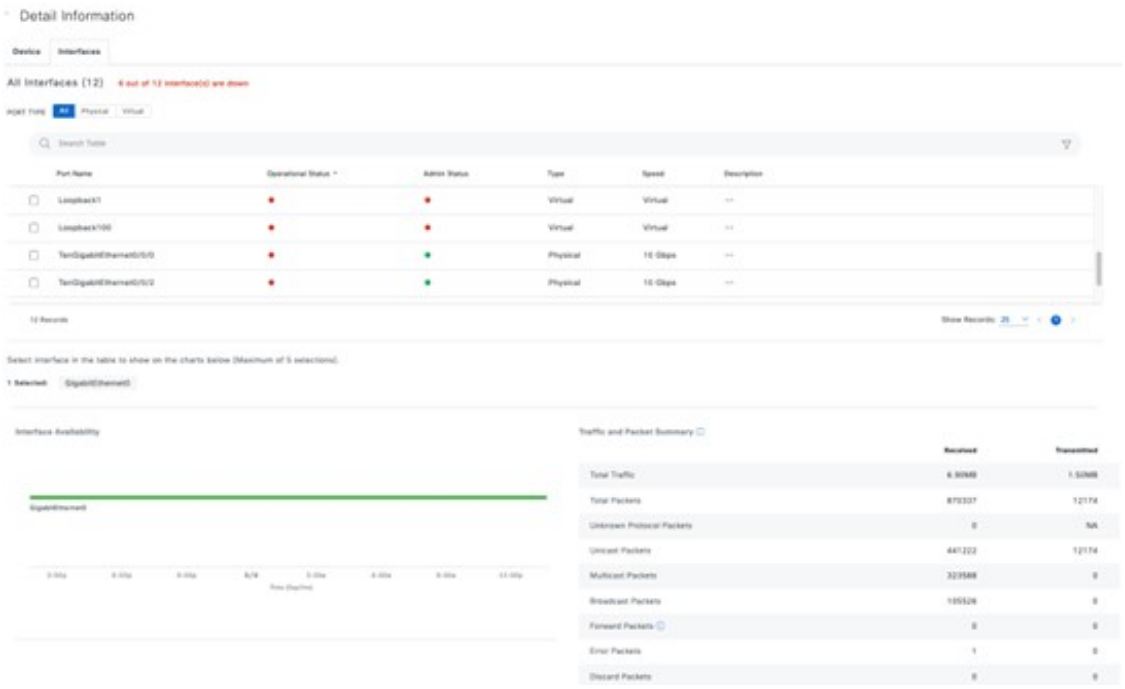
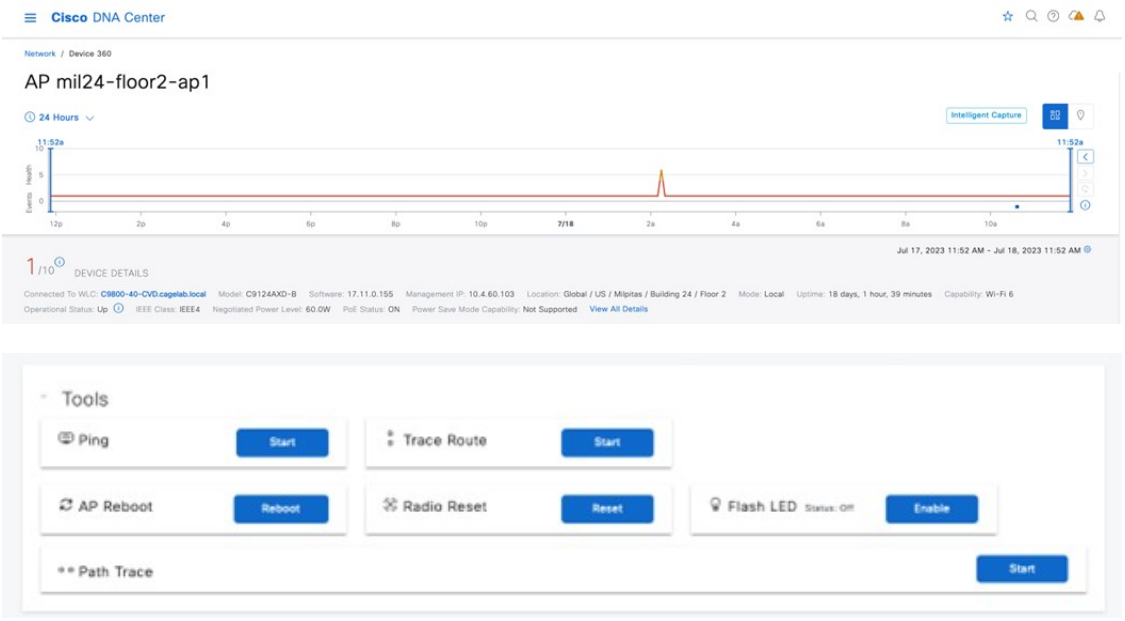


図 *180* : デバイスインターフェイスの詳細



[AP 360] ウィンドウには、正常性タイムライン、問題、物理ネイバートポロジ、イベントビューア、詳細情報セクションなど、ワイヤレスコントローラにあるほとんどのチャートがあります。[AP 360] ウィンドウには、接続の確認、APのリロード、無線のリセット、フラッシュ LED の制御など、AP 固有のセクションもあります。[Detail] セクションには、AP 360 に固有の RF および PoE に関する追加のサブセクションがあります。

図 *181* : *AP 360* 正常性タイムライン



次の図は、SSIDがAPからブロードキャストを開始できる、有効なポリシープロファイルに割り当てられたAPの例を示しています。APがSSIDのブロードキャストを開始すると、次のトレンドチャートに示されているように、メモリ使用率の干渉とチャネル使用率が増加します。

図 ***182 : AP 360*** : ***CPU*** およびメモリのチャート

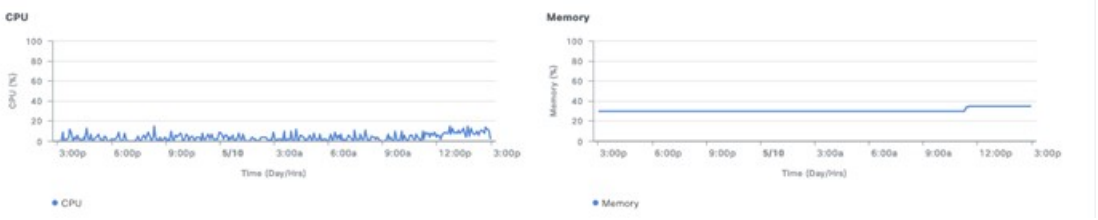
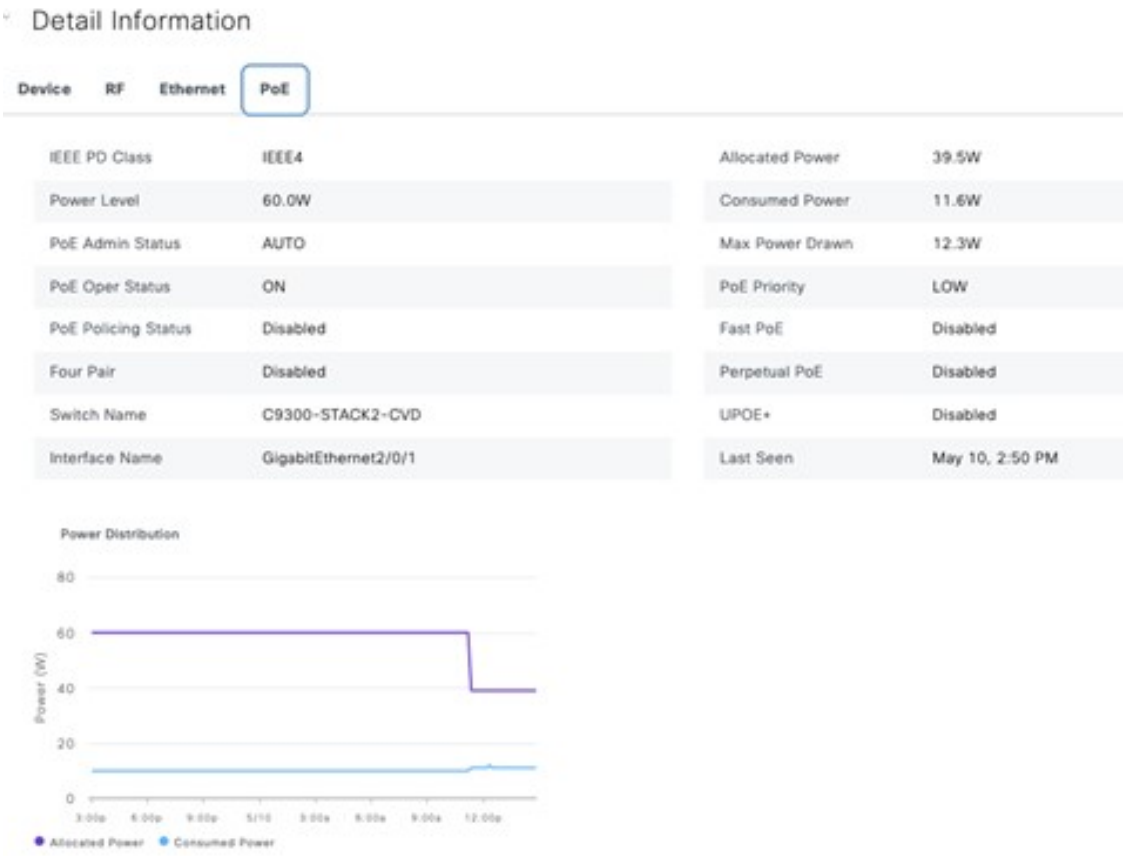


図 ***183 : AP 360*** : チャネル使用率の推移

図 *184 : AP 360* : *PoE* 情報

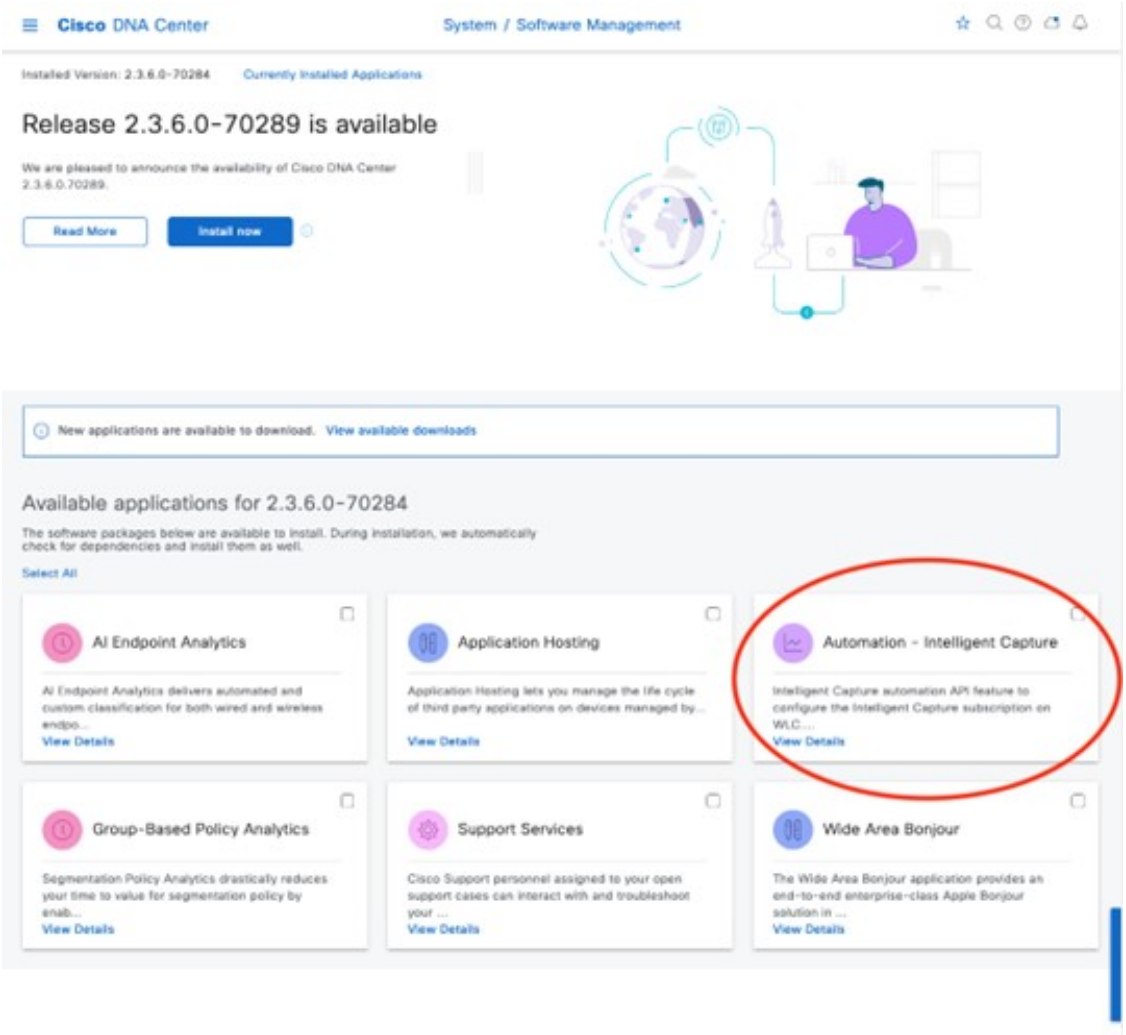


インテリジェントキャプチャ

インテリジェントキャプチャと AP

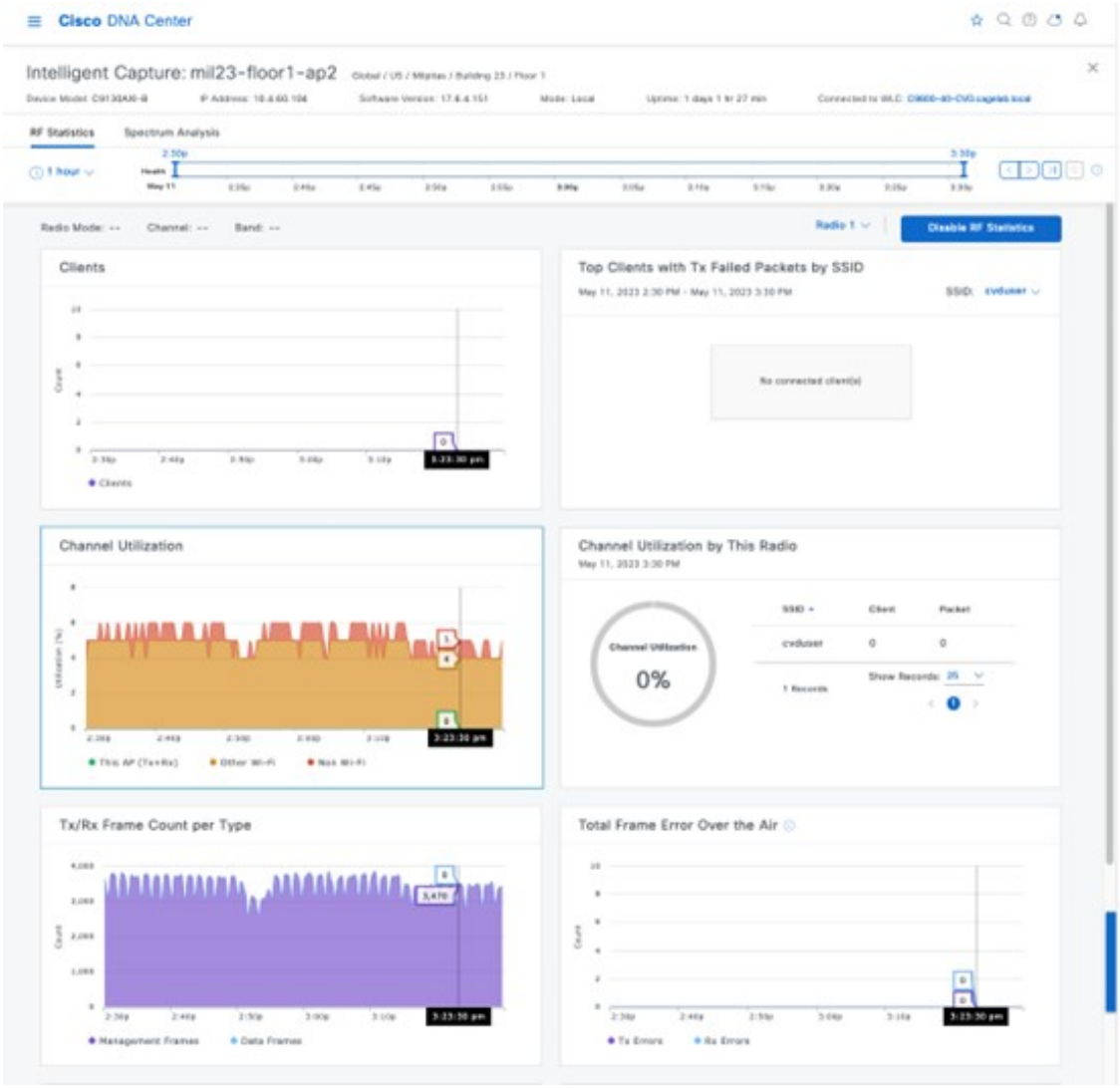
インテリジェントキャプチャ（ICAP）を使用すると、gRPC トンネル経由で AP から Cisco DNA Center に送信されるパケットとストリーム統計情報を AP が直接キャプチャできます。この機能を使用するには、AP がポート 32626 経由で Cisco DNA Center に直接到達できる必要があります。AP と Cisco DNA Center の間にファイアウォールがある場合、このトラフィックは 32626 ポート経由で許可される必要があります。Cisco DNA Center の最新リリースの 2.3.5.0 までは、統計情報に対して有効にできる AP のスケール制限は 1,000 です。デフォルトでは、ICAP アプリケーションは工場出荷時にインストールされていないため、[Software Management] ウィンドウからパッケージをインストールする必要があります。次の図は、工場出荷時にインテリジェント パケット キャプチャ パッケージがインストールされていないことを示しています。

図 *185 :* インテリジェント パケット キャプチャ パッケージのインストール



[Automation - Intelligent Capture] パッケージを選択し、[Install] をクリックしてアプリケーションをインストールします。インストールすると、[AP 360] ページの右上に [Intelligent Capture] ボタンが表示されます。[Intelligent Capture] ボタンをクリックしてサイドバーを開きます。ページの右上隅にある [Enable RF Statistics] をクリックして、RF 統計情報を有効にします。または、[Intelligent Capture Settings] ページから**[Assurance]** > **[Settings]** > **[Intelligent Capture Settings]** > **[Access Points]**の順に選択して、RF 統計情報を有効にできます。Cisco DNA Center のスケールに基づいて、RF 統計情報を有効にするには数分かかります。有効にすると、次の図に示されているように、[Intelligent Capture] ウィンドウのチャートに、クライアント、チャネル使用率、Tx/RX フレーム数、フレームエラー、Tx 電力、マルチキャスト数またはブロードキャスト数の統計情報が表示されます。統計情報は 30 秒ごとに更新されます。[Enable RF Statistics] または [Disable RF Statistics] をクリックして、AP の帯域を変更します。

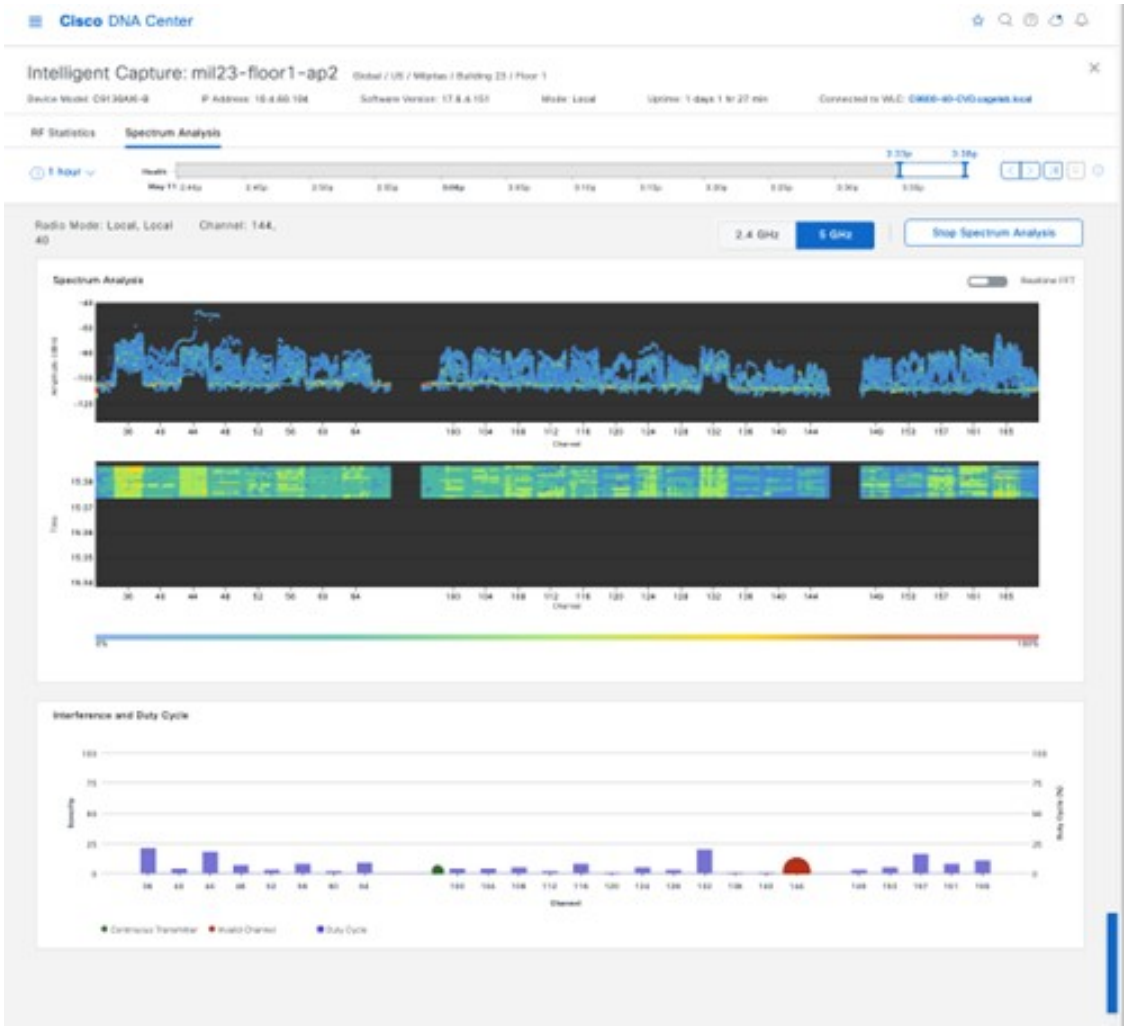
図 *186 : RF* 統計情報が有効になった後の *AP* のインテリジェントキャプチャ



[Spectrum Analysis] タブをクリックして、AP を有効にします。次の図に示されているように、[Start Spectrum Analysis] をクリックして、スペクトル解析データのキャプチャを開始し、Cisco DNA Center にストリーミングするように AP を設定します。スペクトル解析は、一度に 10 分間のみ実行できます。

図 ***187 : [Intelligent Capture Spectrum Analysis]*** ウィンドウ

図 ***188 : 5G*** 帯域の ***AP*** スペクトル解析

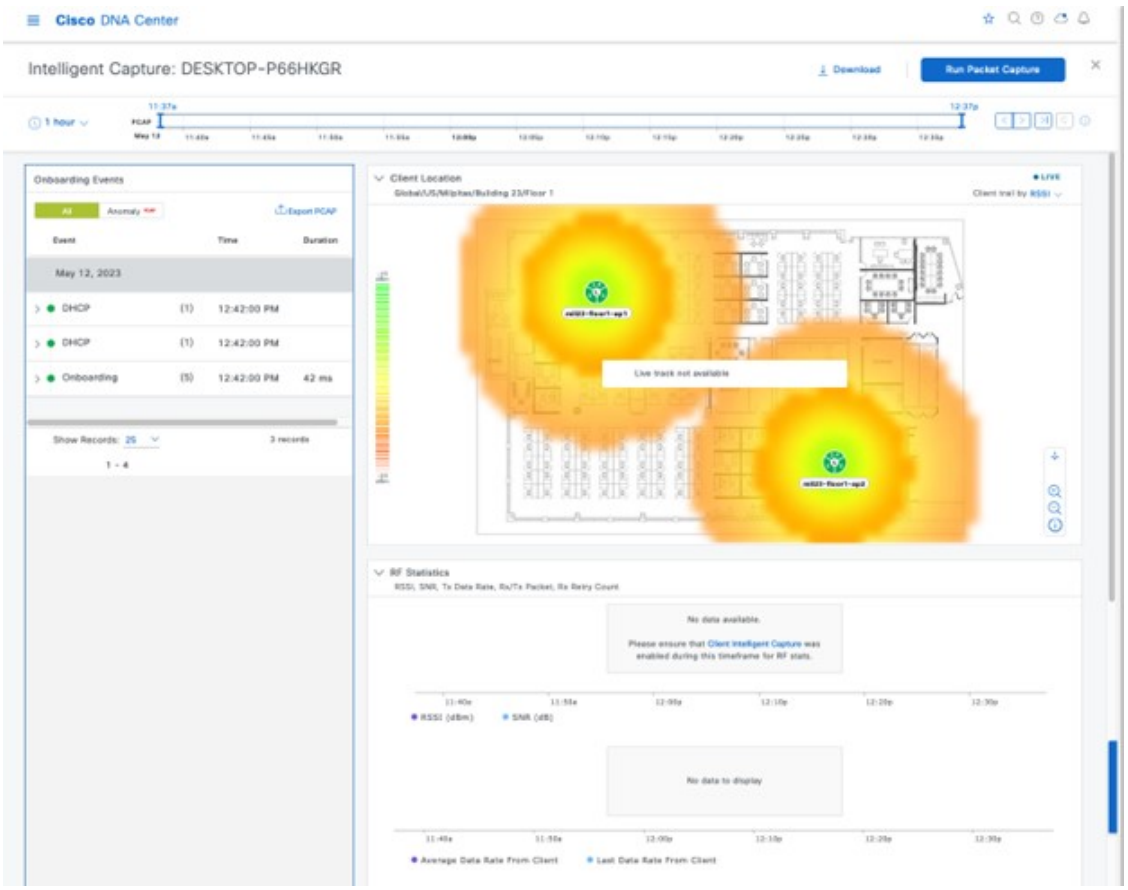


[Spectrum Analysis] が有効になって Cisco DNA Center に表示されると、30 日間保持され、左または右の矢印ボタンを使用してその時間枠と期間（1、3、または 5 時間）を選択することで再表示できます。この機能は、干渉イベントが発生しているときに RF 状態をキャプチャするために、ライブで短期間使用するように設計されています。

インテリジェントキャプチャとワイヤレスクライアント

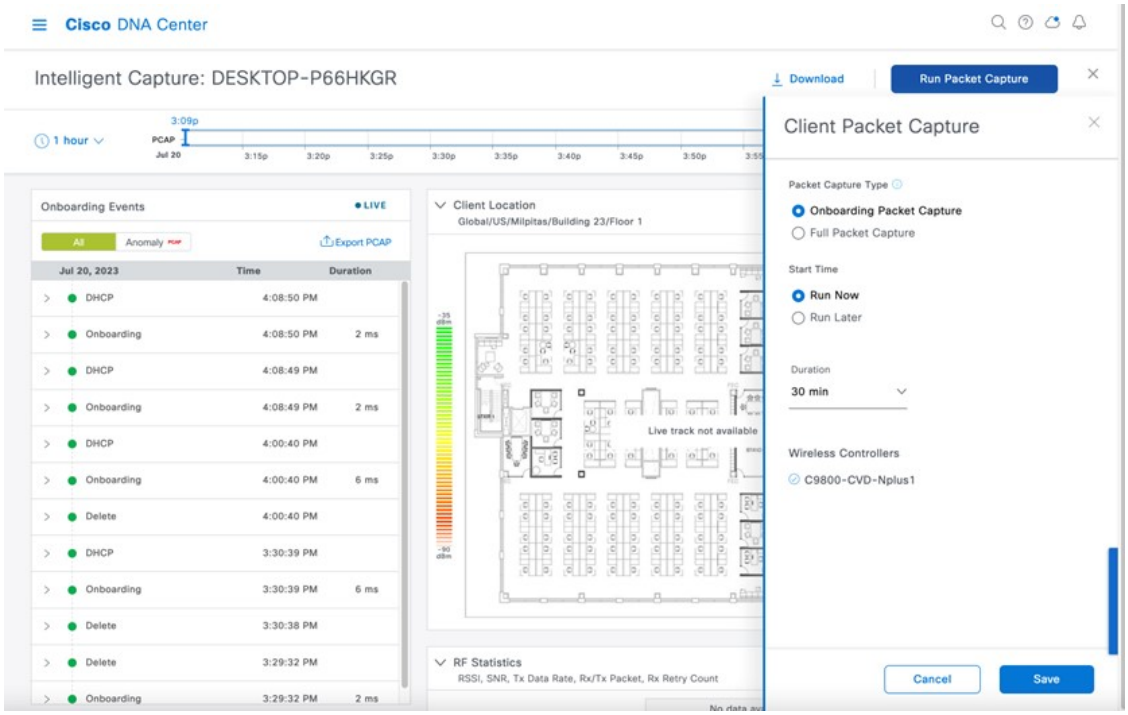
ICAP は、Cisco DNA Center によって検出された AP に関連付けるワイヤレスクライアントのライブパケットキャプチャまたはスケジュールされたパケットキャプチャを有効にします。[Client 360] ウィンドウの [ICAP] ページには、一定期間の RF 統計情報、平均データレート、パケット数など、クライアントに関する追加のライブ統計情報も表示されます。このウィンドウに、クライアントのオンボーディングに関連付けられているイベントと、フロアマップ上のクライアントの場所を示すマップセクション（CMX/Cisco Spaces が Cisco DNA Center に統合されている場合）も表示されます。次の図は、オンボーディング パケット キャプチャを有効にする前のワイヤレスクライアントの [ICAP] ページを示しています。

図 *189 : ICAP* を有効にする前のワイヤレスクライアントのインテリジェントキャプチャ



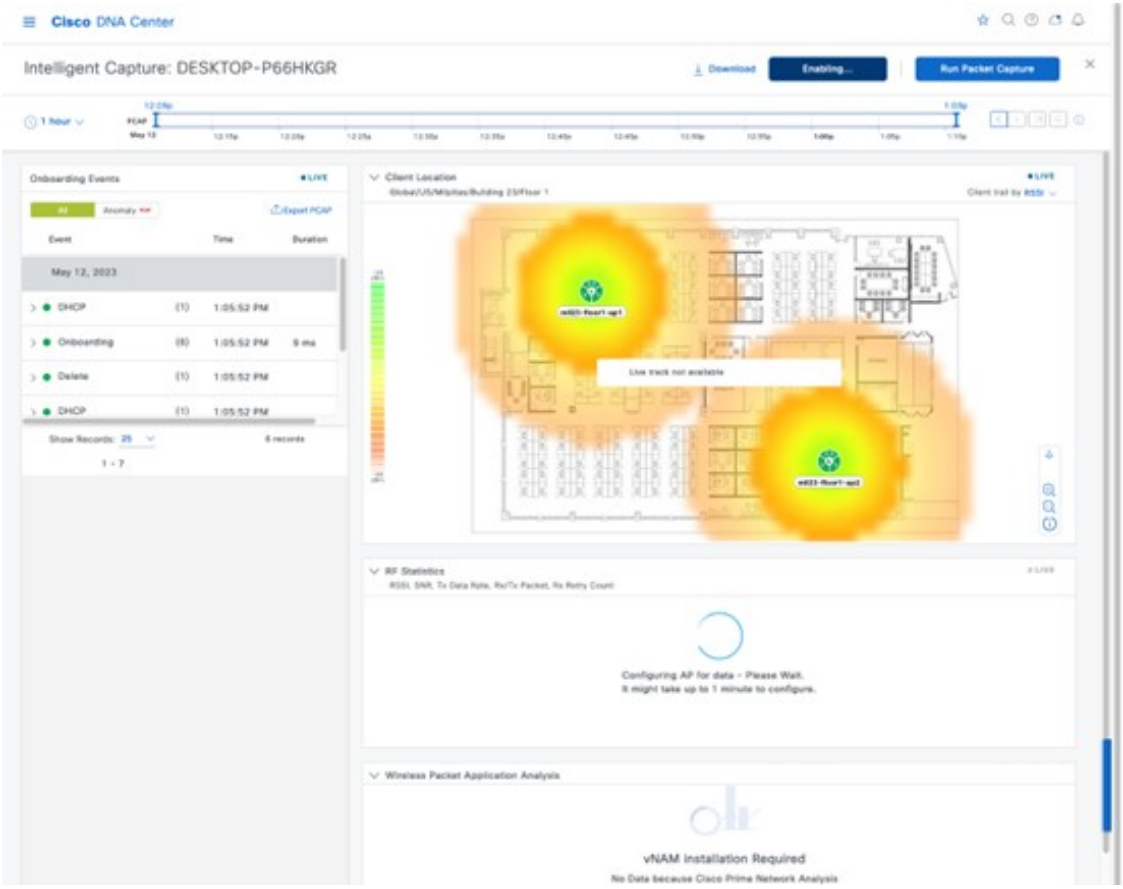
ウィンドウの右上隅にある [Run Packet Capture] をクリックして、オンボーディング パケット キャプチャを有効にします。[Client Intelligent Capture] をクリックすると [ICAP Settings] ページが表示され、このキャプチャをスケジュールできます。オンボーディング パケット キャプチャを有効にするときに、必要なワイヤレスコントローラを選択できます。選択したワイヤレスコントローラの場合、ワイヤレスコントローラ名の左側に緑色のチェックマークが表示されます。デフォルトでは、次の図に示されているように、クライアントが現在関連付けられているワイヤレスコントローラが選択されます。

図 *190* : ワイヤレスクライアントのオンボーディングイベントのパケットキャプチャ



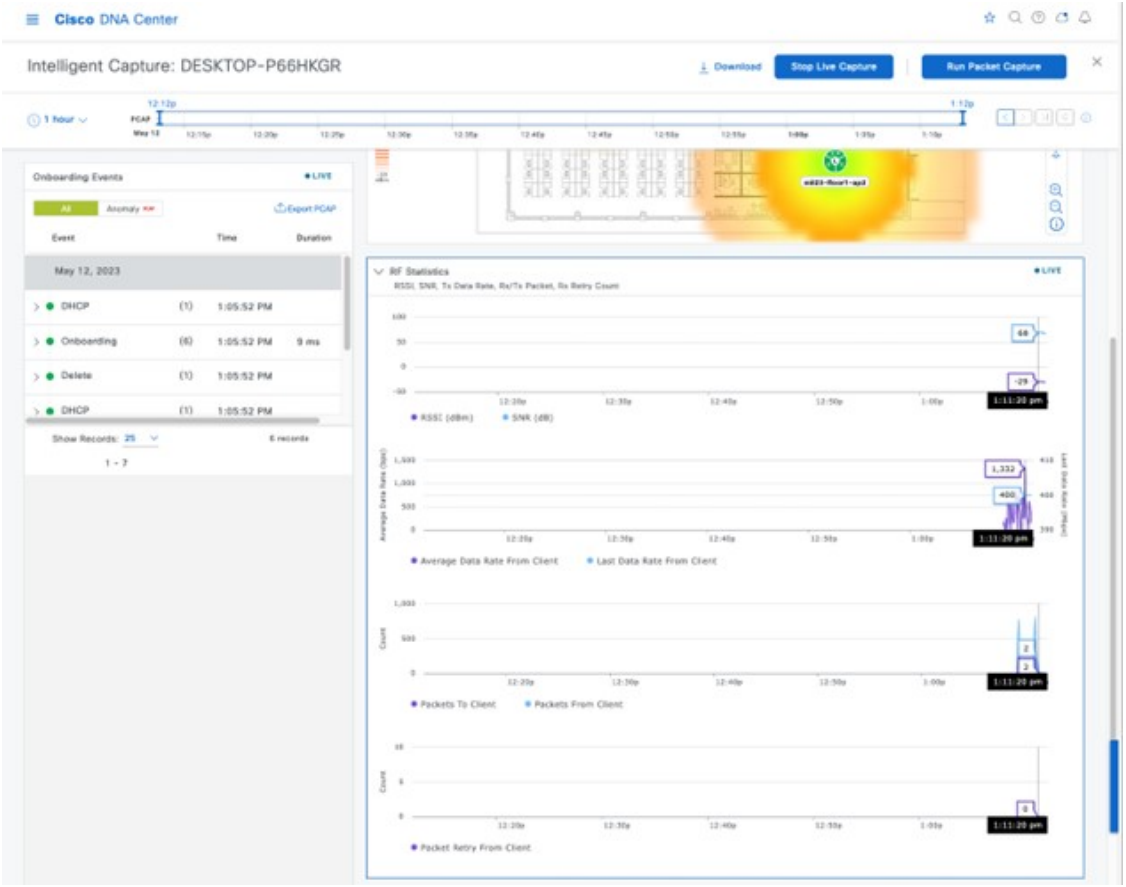
[Save] をクリックすると、次の図に示されているように、ワイヤレスクライアントのライブパケットキャプチャを送信するためのワイヤレスコントローラと AP の設定に数分かかります。

図 *191* : ワイヤレスクライアントの *ICAP* の設定



ワイヤレスコントローラと AP を設定すると、次の図に示されているように、クライアントに関するライブ統計情報がチャートに表示されます。

図 *192 : [Intelligent Capture]* ウィンドウに表示されるライブ オンボーディング イベントと統計情報



ワイヤレスコントローラおよび AP では、次の CLI を使用して設定を確認できます。

- **C9800-40-CVD#show ap icap serviceability detail**

```
AP name         : mil23-floor1-ap1AP serviceability
gRPC server status
  WLC timestamp                  : 05/12/2023 13:29:55
  AP timestamp                   : 05/12/2023 13:29:54
  Status                         : ready
  Last success timestamp         : 05/12/2023 13:29:54
  Last failure timestamp         : 12/31/1969 16:00:00
  Last failure status            : idle
  Last JWT success timestamp     : 05/12/2023 13:27:35
  Last JWT failure timestamp     : 12/31/1969 16:00:00
  Last JWT failure reason        : Unknown
  Packet transmit attempts       : 53
  Packet transmit failures       : 0
  Packet receive count           : 1061
  Packet receive failures        : 0
Full packet-trace stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 0
  Packets sent                   : 0
  Packets filtered               : 0
  Packets dropped                : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 0
```

```
Partial packet-trace stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 1061
  Packets sent                   : 262
  Packets filtered               : 799
  Packets dropped                : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 0
Anomaly detection event stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 0
  Packets sent                   : 0
  Packets filtered               : 0
  Packets dropped                : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 0
Anomaly detection packet stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 0
  Packets sent                   : 0
  Packets filtered               : 0
  Packets dropped                : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 0
Statistics stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 0
  Packets sent                   : 15165
  Packets filtered               : 0
  Packets dropped                : 2
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 2
```

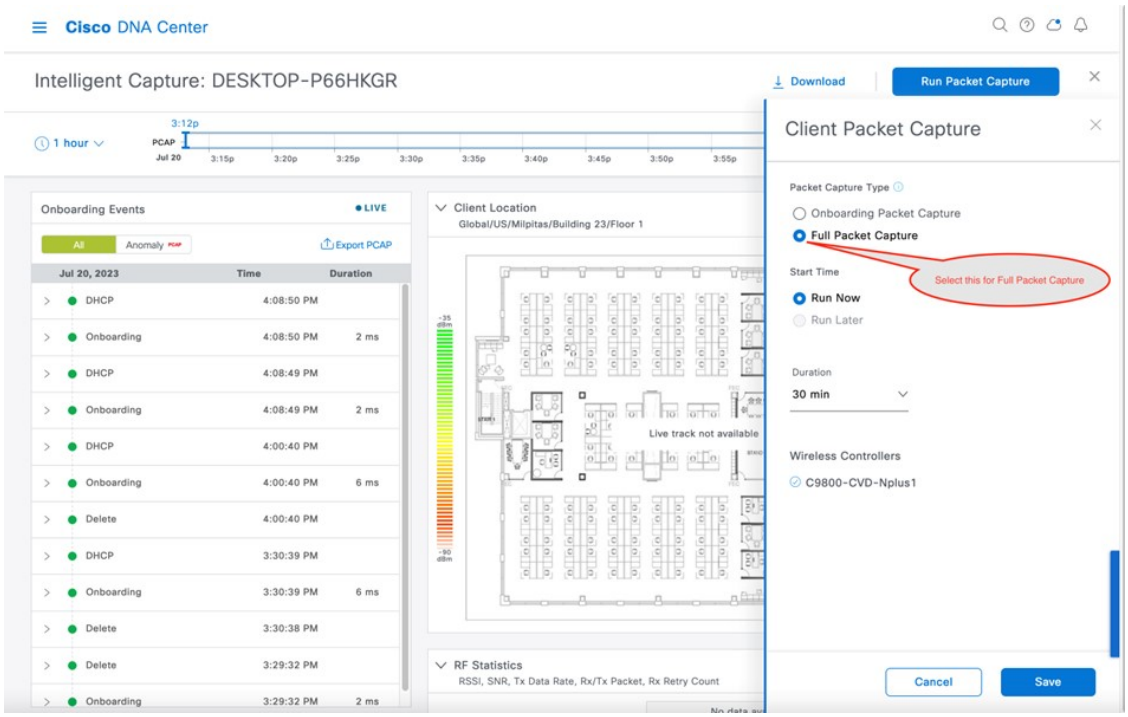
- **mil23-floor1-ap1#show ap icap subscription**

```
Subscription list
-----------------
 Full Pkt Capture      : Disabled
 Partial Pkt Capture   : Enabled
 Anomaly Event         : Disabled
 Debug                 : Disabled
 Stats                 : Enabled
 Ap Operational Data   : Disabled
       Sensor Message        : Disabled
 RRM Operational Data  : Disabled
 Client Events         : Disabled
 MMAP Packets          : Disabled
 aWIPS Forensic Pkts   : Disabled
MAC and Filters subscription list
---------------------------------
Full-packet-trace: None
Partial-packet-trace: 1C:1B:B5:1F:C0:F7
 Filters: assoc auth probe arp dhcp eap icmp dhcpv6 icmpv6 dns ndp
Anomaly Detection: None

Client Stats
------------
MAC Address Table:
  1C:1B:B5:1F:C0:F7

RF Spectrum
-----------
Radio Slot(s): NONE
mil23-floor1-ap1#
```

オンボーディングイベントのICAPが有効になり、クライアントが認証解除されて再認証されると、オンボーディングイベント中にパケットがキャプチャされ、 Cisco DNA Center に送信されます。パケットがキャプチャされたイベントには、オンボーディング イベント セクションのイベント名の右側に [PCAP] アイコンが表示されます。イベントを選択すると、キャプチャされたパケットの分析が視覚的な形式で表示されます。キャプチャされたパケットは、[Auto Packet Analyzer] セクションの右上隅にある [Download Packets] をクリックすると、PCAP ファイルとしてダウンロードできます。イベントグループのキャプチャされたパケットは、[Onboarding Events] セクションの [Export PCAP] をクリックしてダウンロードできます。[Export PCAP] はイベントのフルセットを対象としており、[Download Packets] はサブイベントに使用する必要があります。

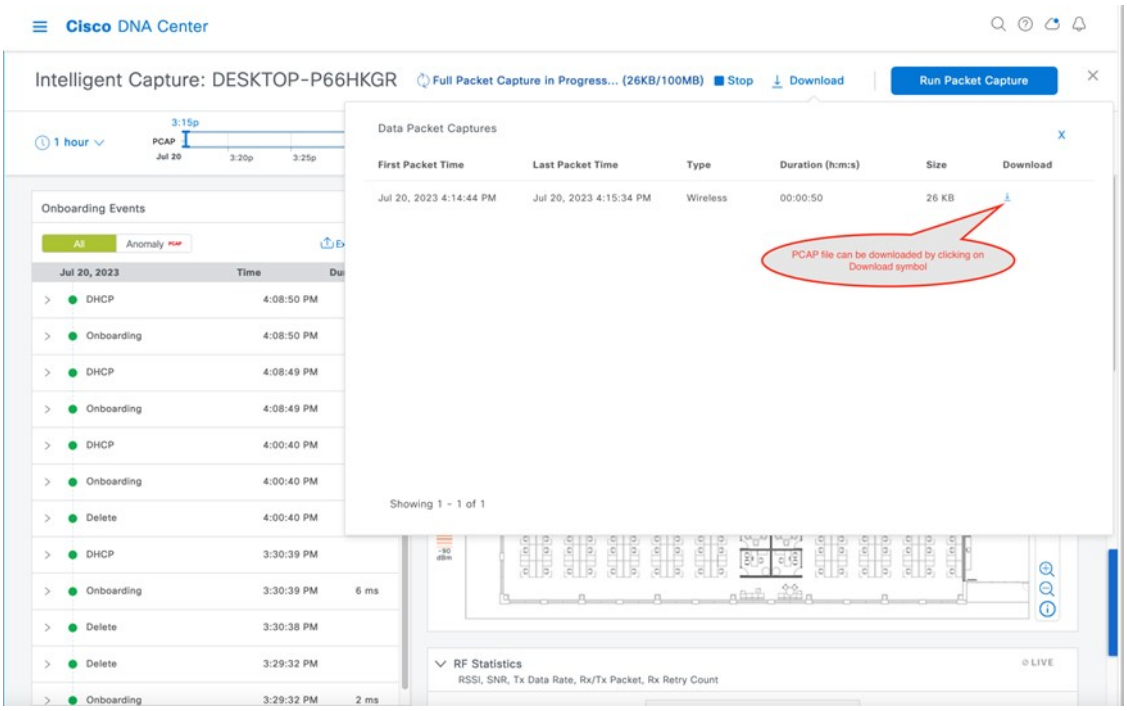
クライアントからのデータパケットをキャプチャするには、次の図に示されているように、フルパケットキャプチャを有効にする必要があります。

図 *193 :* フルパケットキャプチャの設定



[Save] をクリックして、フルパケットキャプチャを有効にします。次の図に示されているように、[Download] アイコンをクリックして、パケットを PCAP ファイルとしてダウンロードします。

図 *194 :* フルパケットキャプチャのダウンロード



不正管理および適応型ワイヤレス侵入防御

不正アクセス ポイントの管理

Cisco DNA Center の不正管理アプリケーションは、脅威を検出して分類し、ネットワーク管理者、ネットワークオペレータ、およびセキュリティオペレータがネットワークの脅威を監視できるようにします。Cisco DNA Center を使用すると、最も優先順位の高い脅威を迅速に特定し、Cisco DNA アシュアランス 内の [Rogue and aWIPS] ダッシュボードで特定した脅威を監視できます。

不正なデバイスとは、ネットワーク内で管理対象の AP によって検出される、未知（管理対象外）のアクセスポイントまたはクライアントのことです。不正 AP は、正規のクライアントをハイジャックすることによって、無線 LAN の動作を妨害する可能性があります。ハッカーは不正 AP を使用して、ユーザ名やパスワードなどの機密情報を取得できます。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー セント）フレームを送信できるようになります。この AP のなりすましアクションにより、特定のクライアントは送信を許可され、他のクライアントはすべて待機させられるため、正規のクライアントはネットワークリソースに接続できなります。したがって、無線 LAN サービスプロバイダーは、空間からの不正な AP の締め出しに強い関心を持っています。

Cisco DNA Center は、すべての近隣の AP を継続的にモニタし、不正 AP に関する情報を自動的に検出して収集します。

Cisco DNA Center は 、管理対象 AP から不正なイベントを受信すると、次のように反応します。

- 不明な AP が Cisco DNA Center によって管理されていない場合は、Cisco DNA Center によって不正分類ルールが適用されます。
- 不明な AP がネットワークと同じ SSID を使用していない場合は、Cisco DNA Centerが、AP が企業の有線ネットワークに接続され、有線ネットワークに通じているかどうかを確認します。不正 AP が企業ネットワークのスイッ

チポートに物理的に接続されている場合、Cisco DNA Center は AP を**有線ネットワーク上の不正**として分類します。

有線ネットワーク上の不正を検出するには、Cisco DNA Center で管理されているシスコスイッチが必要です。

- AP が Cisco DNA Center に対して不明で、ネットワークと同じ SSID を使用している場合、Cisco DNA Center は AP を**ハニーポット**として分類します。
- 不明な AP がネットワークと同じ SSID を使用しておらず、社内ネットワークに接続されていない場合、Cisco DNA Centerは、干渉が発生しているかどうかを確認します。存在する場合は、Cisco DNA CenterはAPを**干渉源**として分類し、不正な状態を**潜在的な脅威**としてマークします。この分類のしきい値レベルは-75 dBm で、それを超える場合にネットワーク上の干渉源として分類されます。
- 不明な AP がネットワークと同じ SSID を使用しておらず、社内ネットワークに接続されていない場合、Cisco DNA Center はその AP がネイバーであるかどうかを確認します。ネイバーである場合、 Cisco DNA Centerは AP を**ネイバー**として分類し、不正状態を**情報**としてマークします。この分類のしきい値レベルは-75 dBm で、それ以下の場合に不正 AP がネイバー AP として分類されます。

適応型ワイヤレス侵入防御

Cisco Advanced Wireless Intrusion Prevention System（aWIPS）は、ワイヤレス侵入の脅威を検出して軽減するメカニズムです。ワイヤレスの脅威検出およびパフォーマンスの管理のための高度な手法を使用します。APは脅威を検出し、アラームを生成します。この手法では、ネットワークトラフィック分析、ネットワークデバイスとトポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的なワイヤレス侵入防御を実現できます。

インフラストラクチャに完全に統合されたソリューションを使用すると、有線ネットワークと無線ネットワークの両方で無線トラフィックを継続的に監視し、ネットワーク インテリジェンスを使用して多くのソースからの攻撃を分析できます。また、損害や漏洩が発生するまで待たずに、攻撃を正確に特定しプロアクティブに防止できます。

Cisco DNA Center には aWIPS の機能が統合されているため、aWIPS のポリシーとアラームを設定および監視して、脅威を報告できます。

aWIPS は次の機能をサポートしています。

- スタティックシグニチャ
- スタンドアロンシグニチャ検出
- アラーム
- コントローラおよび AP イメージに付属のスタティック シグニチャ ファイル

Cisco DNA Center では、さまざまなサービス妨害（DoS）攻撃を検出する次のシグニチャがサポートされています。

- **認証フラッド**：多数のクライアントステーションを偽装（MAC アドレススプーフィング）して AP に認証要求を送信し、APのクライアントステートテーブル（アソシエーションテーブル）のフラッディングを引き起こすDoS攻撃の形式。ターゲット AP では、個々の認証要求を受け取るたびにアソシエーションテーブルに状態 1 のクライアント項目が作成されます。オープンシステム認証が使用されているAPは、認証成功フレームを戻し、クライアントを状態 2 にします。共有キー認証（SHA）が AP に使用されている場合、AP は攻撃者の模倣クライアントに認証チャレンジを送信しますが、これは応答せず、AP はクライアントを状態 1 に保ちます。これらのシナリオの

いずれにおいても、APには、状態1または状態2のいずれかの状態にある複数のクライアントが含まれ、APアソシエーションテーブルがいっぱいになります。テーブルが上限に達すると、正規のクライアントがこのAPに対して認証およびアソシエートできなくなります。

- **アソシエーションフラッド**：APに大量のスプーフィングされたクライアントアソシエーションを送り付け、APのリソース（特にクライアントアソシエーションテーブル）を枯渇させます。攻撃者はこの脆弱性を利用して大量のクライアントをエミュレートし、多数のクライアントを作成して、ターゲットAPのクライアントアソシエーションテーブルのフラッディングを発生させます。クライアントアソシエーションテーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなります。

- **CTS フラッド**：特定のデバイスが同じ無線周波数（RF）メディアを共有するワイヤレスデバイスにバルク Clear To Send（CTS）制御パケットを送信する DoS 攻撃の形式この種の攻撃は、CTS フラッドが停止するまで、ワイヤレスデバイスによる RF メディアの使用をブロックします。

- **RTS フラッド**：特定のデバイスが AP にバルク RTS 制御パケットを送信してワイヤレス帯域幅をブロックし、その AP 上のクライアントのパフォーマンス障害を引き起こします。

- **ブロードキャストプローブ**：特定のデバイスがブロードキャストプローブ要求を使用して、管理対象APをフラッディングしようとします。

- **ディスアソシエーションフラッド**：APからクライアントへのディスアソシエーションフレームをスプーフィングして AP を状態 2（未アソシエートまたは未認証）にします。クライアントアダプタ実装では、この攻撃はこのクライアントに対してワイヤレスサービスを妨害する点で効果的かつ即効性があります。通常、クライアントステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、クライアントを使用不能な状態にします。

- **ディスアソシエーション ブロードキャスト**：特定のデバイスが関連付け解除ブロードキャストをトリガーして、すべてのクライアントを切断しようとすることです。

  この攻撃では、APからブロードキャストアドレス（すべてのクライアント）へのディスアソシエーション フレームをスプーフィングして AP のクライアントを状態 2（未アソシエートまたは未認証）にします。現在のクライアントアダプタの実装では、この形式の攻撃は、複数のクライアントに対するワイヤレスサービスを即座に中断します。通常、クライアントステーションは攻撃者が新たなディスアソシエーションフレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

- **認証解除フラッド**：APからクライアントユニキャストアドレスへの認証解除フレームをスプーフィングしてAPのクライアントを状態1（未アソシエートまたは未認証）にします。現在のクライアントアダプタの実装では、この形式の攻撃はクライアントに対するワイヤレスサービスを即座に中断します。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返し認証解除フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

- **認証解除ブロードキャスト**：この DoS 攻撃では、AP からブロードキャストアドレスへの認証解除フレームをスプーフィングして AP のすべてのクライアントを状態 1（未アソシエートまたは未認証）にします。クライアントアダプタの実装では、この形式の攻撃は、複数のクライアントに対するワイヤレスサービスを即座に中断します。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。

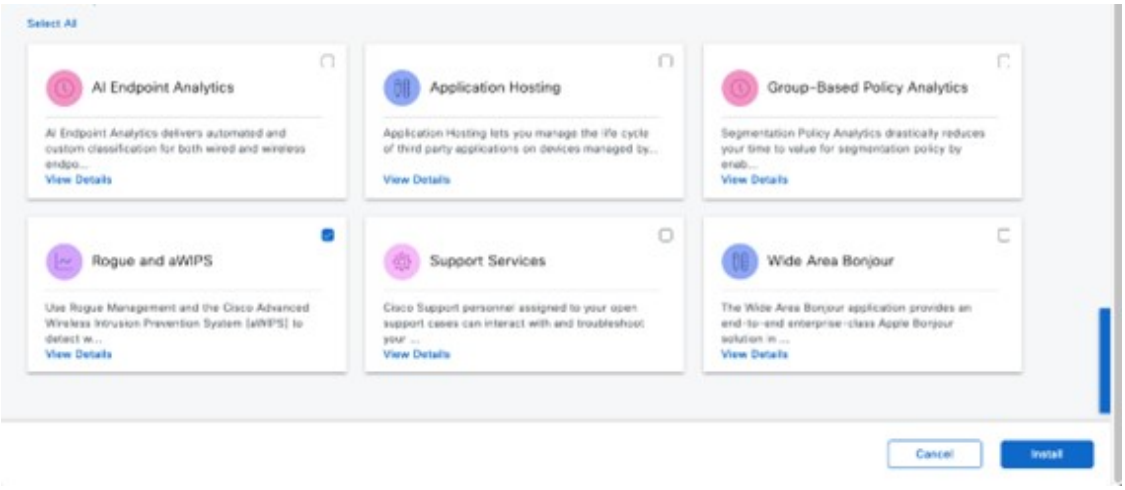
- **EAPOL ログオフフラッド**：特定のデバイスが、LAN 上で動作する拡張可能な認証プロトコル（EAPOL）ログオフパケットを送信しようとすることです。このパケットが WPA および WPA2 認証で使用され、サービス妨害が引き起こされます。

  EAPOL ログオフフレームは認証されないため、攻撃者はこのフレームをスプーフィングし、ユーザを AP からログオフさせることができます。これにより DoS 攻撃が成立します。クライアントが AP からログオフしたことは、クライアントが WLAN 経由で通信を試行するまでは明らかではありません。通常この妨害が検出されると、クライアントはワイヤレス接続を回復するため自動的に再アソシエートと認証を行います。攻撃者は、スプーフィングされた EAPOL-Logoff フレームを継続的に送信できます。

基本的な設定のワークフロー

Cisco DNA Center に不正管理および aWIPS アプリケーションをインストールするには、メニューアイコンをクリックして、 **[System]** > **[Software Management]**の順に選択します。次の図に示されているように、[Rogue and aWIPS] パッケージを選択し、右下隅にある [Install] をクリックします。

図 *195*：不正管理および *aWIPS* アプリケーションのインストール

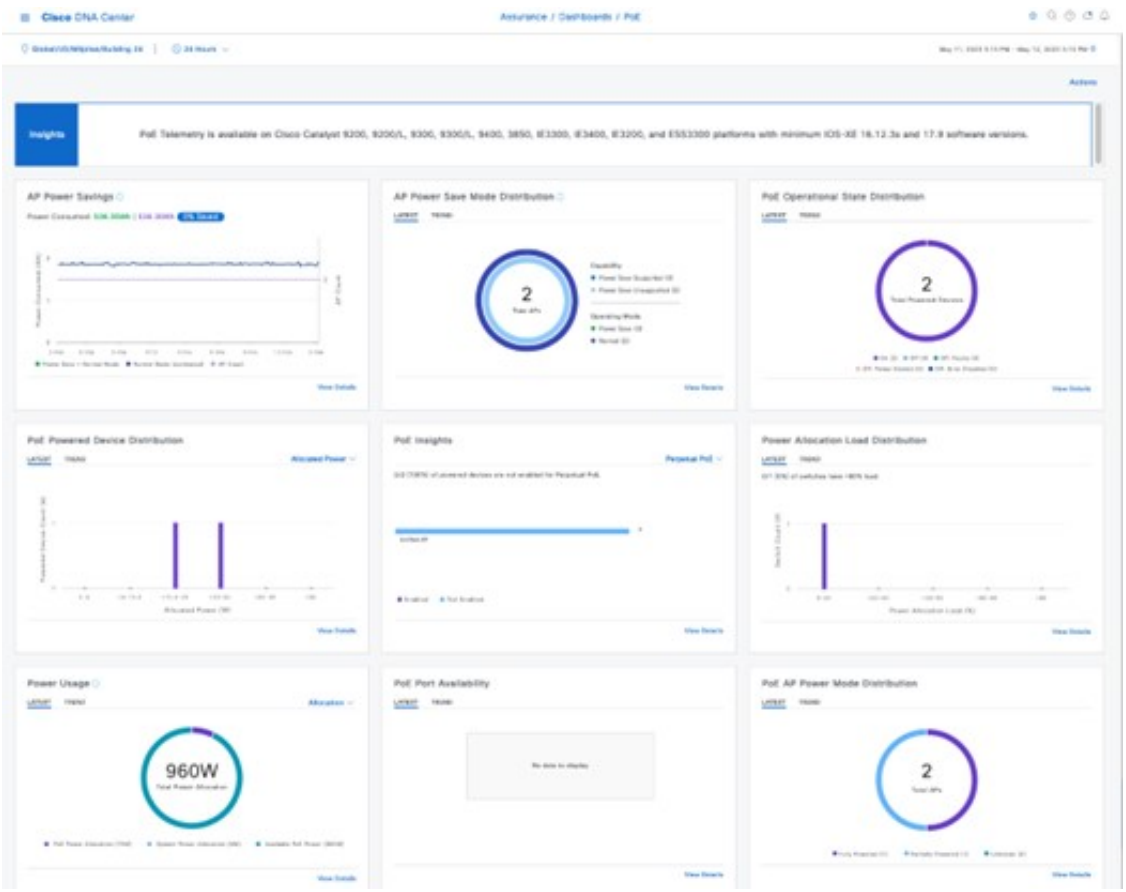


パッケージをインストールしたら、**[Assurance]** > **[Rogue and aWIPS]**の順に選択します。

Cisco DNA Center での不正管理および aWIPS アプリケーションの設定方法の詳細については、Cisco DNA Center 不正管理および aWIPS アプリケーション クイック スタート ガイド [英語] を参照してください。

PoE チャート

図 *196 : Cisco DNA Center* の *PoE* チャート



PoE チャートは [AP 360] ウィンドウにあり、選択した期間に AP によって消費される電力のタイムラインビューが表示されます。

Cisco Aironet 1800S ネットワークセンサー

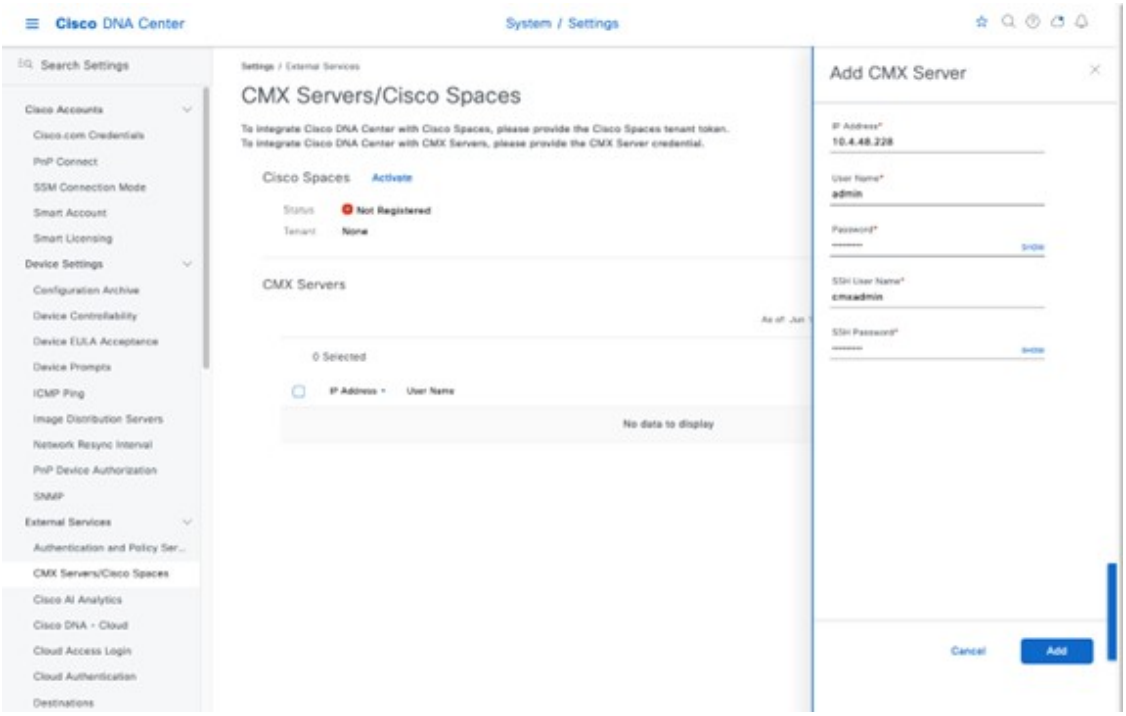
ワイヤレスネットワークが拡大するにつれて、ワイヤレスの問題をプロアクティブに特定して解決することが不可欠になっています。ネットワークセンサーは、ワイヤレスカバレッジは重要だが、オンサイトの IT 技術者を必要としない会議室や作業エリアなどのオフィススペースに導入できる小型フォームファクタデバイスです。ネットワークセンサーは、オンデマンドまたはスケジュールされた模擬テストを実行できるワイヤレスクライアントとして機能します。詳細については、Cisco Aironet アクティブセンサー導入ガイド [英語] を参照してください。

Cisco Spaces と CMX の統合

CMX オンプレミス統合

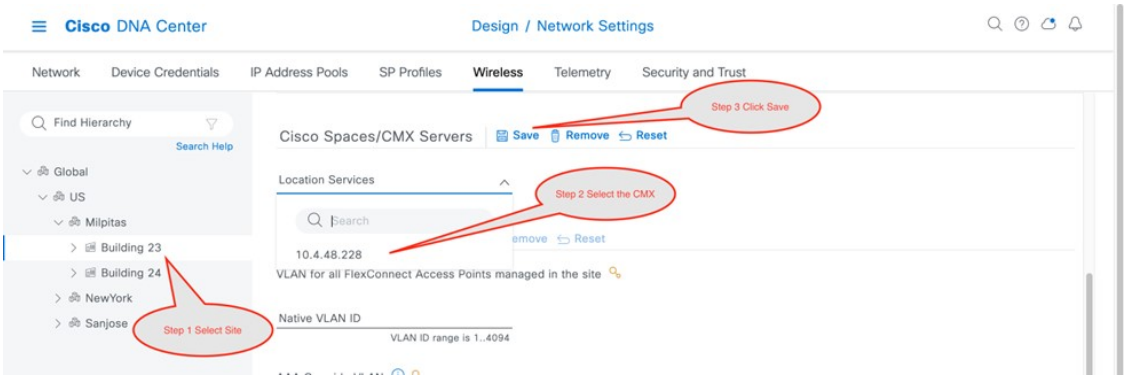
オンプレミスの CMX を統合するには、メニューアイコンをクリックして、**[System]** > **[Settings]** > **[CMX Servers/Cisco Spaces]**の順に選択します。次の図に示されているように、[CMX Servers] の下にある [Add] をクリックし、[Add CMX Server] slide-in paneに要求された値を入力します。値を入力したら、[Add] をクリックします。

図 *197 : Cisco DNA Center* へのオンプレミス *CMX* の統合



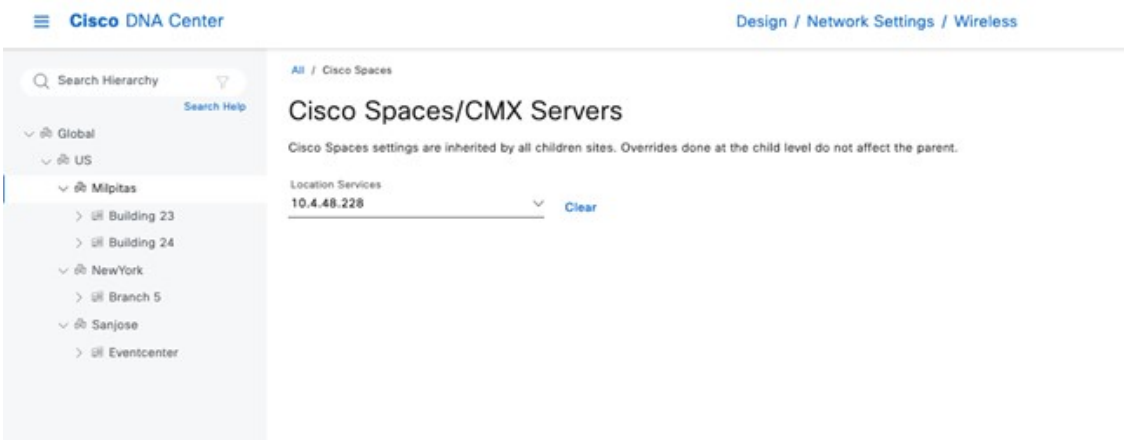
CMX をサイトに割り当てるには、**[Design]** > **[Network Settings]**の順に選択して、[Wireless] タブをクリックします。次の図に示されているように、[Cisco Spaces/CMX Servers] タブをクリックします。

図 *198 :* サイトへの *CMX* の割り当て



左側の階層ツリーから目的のサイトを選択します。[Location Services] ドロップダウンリストから、CMX サーバーを選択します。次の図は、選択した Milpitas サイトの CMX サーバーの例を示しています。

図 *199 : Cisco DNA Center* を介した *CMX* サイトの割り当て



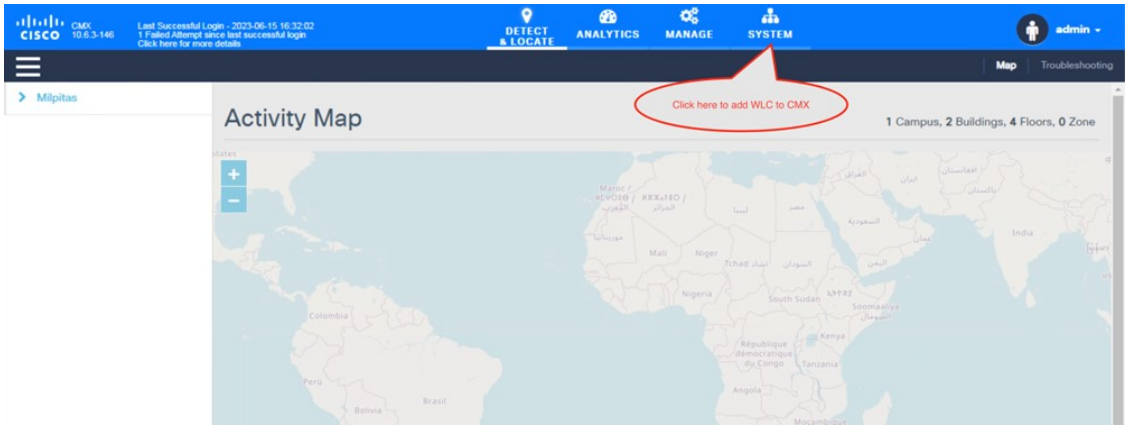
CMX に場所が割り当てられると、そのサイトに関連するサイト階層、そのサイト内の AP、および AP 位置情報が CMX と同期されます。

（注） CMX と Cisco DNA Center を統合しても、ワイヤレスコントローラは CMX に自動的に追加されません。CMX GUI インターフェイスを使用して、CMX にワイヤレスコントローラを手動で追加する必要があります。

次の手順を使用して、ワイヤレスコントローラを CMX に追加します。

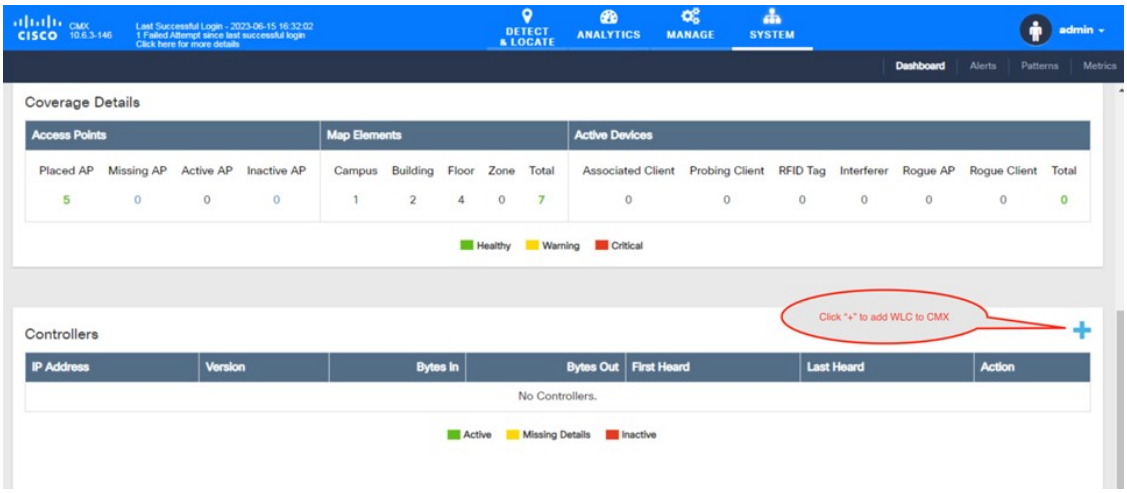
1. 次の図に示されているように、CMX GUI インターフェイスにログインし、[SYSTEM] に移動します。

図 *200 :* ワイヤレスコントローラを追加する *CMX GUI*



2. [+] をクリックして、ワイヤレスコントローラを CMX に追加します。

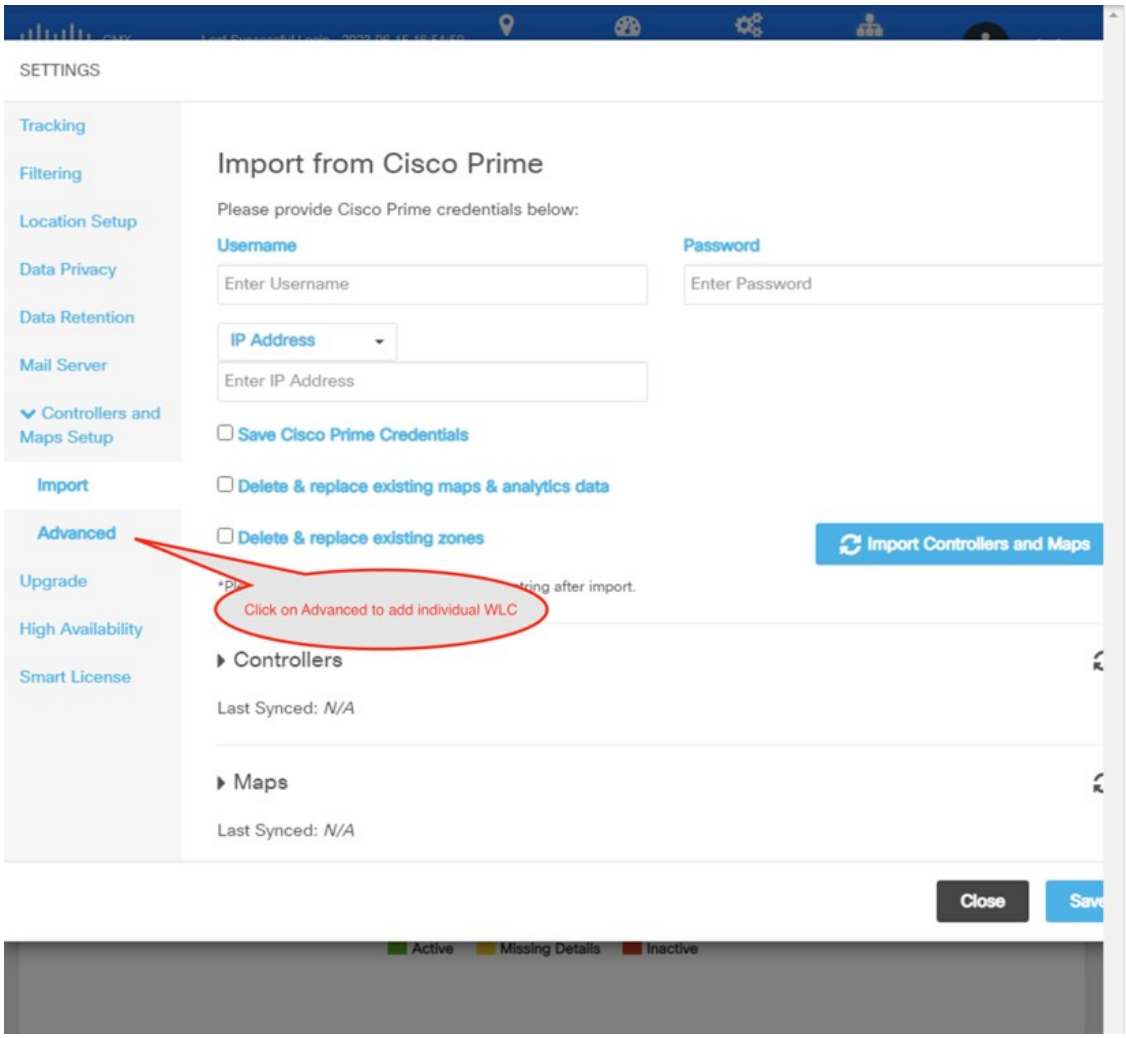
図 *201 : CMX* の *SYSTEM* 内でのワイヤレスコントローラの追加



3. **[Settings]** > **[Controllers and Map Setup]**から [Advanced] をクリックして、個々のワイヤレスコントローラを追加します。

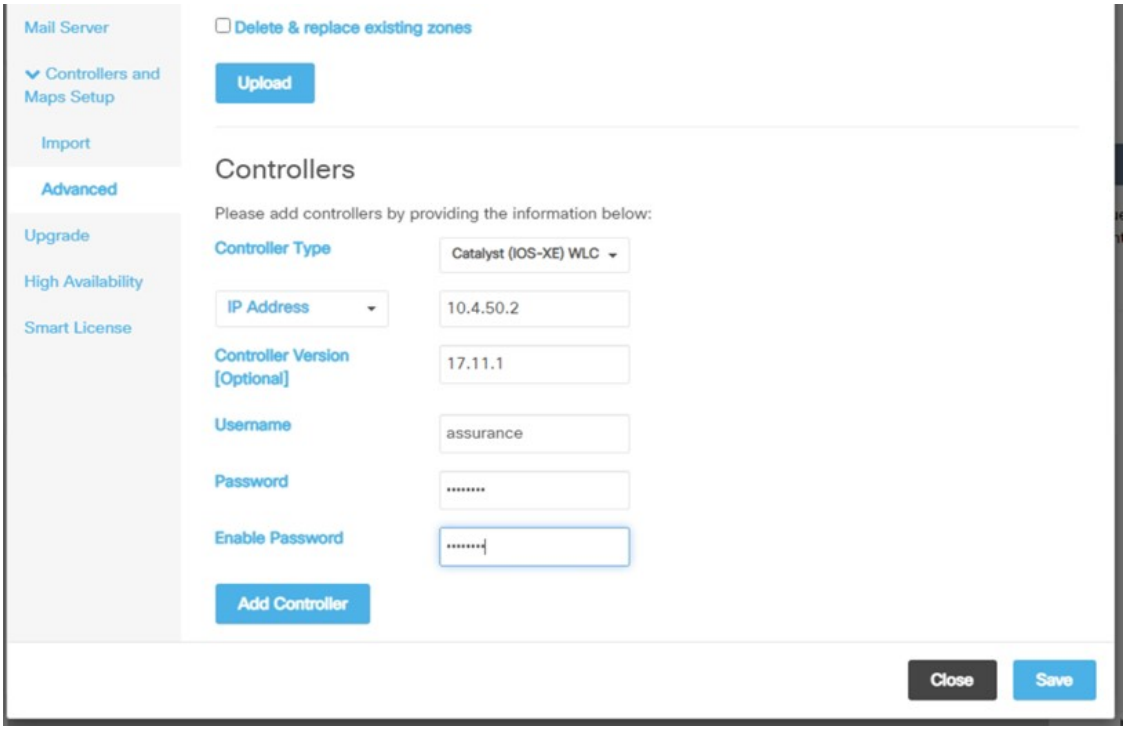
   [Import from Cisco Prime] ダイアログボックスが表示されます。

図 *202 : CMX* への個々のワイヤレスコントローラの追加



4. 次の図に示されているように、下にスクロールして [Add Controller] をクリックし、ワイヤレスコントローラを CMX に追加します。

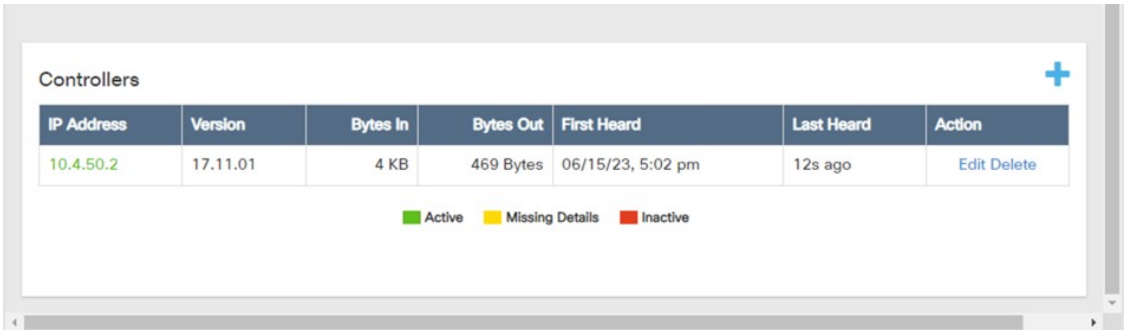
図 *203* : 個々のワイヤレスコントローラ情報の追加



5. [Save] をクリックします。

   ワイヤレスコントローラのリストが表示されます。

図 *204* : ワイヤレスコントローラのリスト



Cisco Spaces と Cisco DNA Center の統合

Cisco Spaces アカウントをアクティブ化し、Cisco DNA Center と統合するには、次の手順を使用します。詳細については、Cisco Spaces コンフィギュレーション ガイド [英語] を参照してください。

始める前に

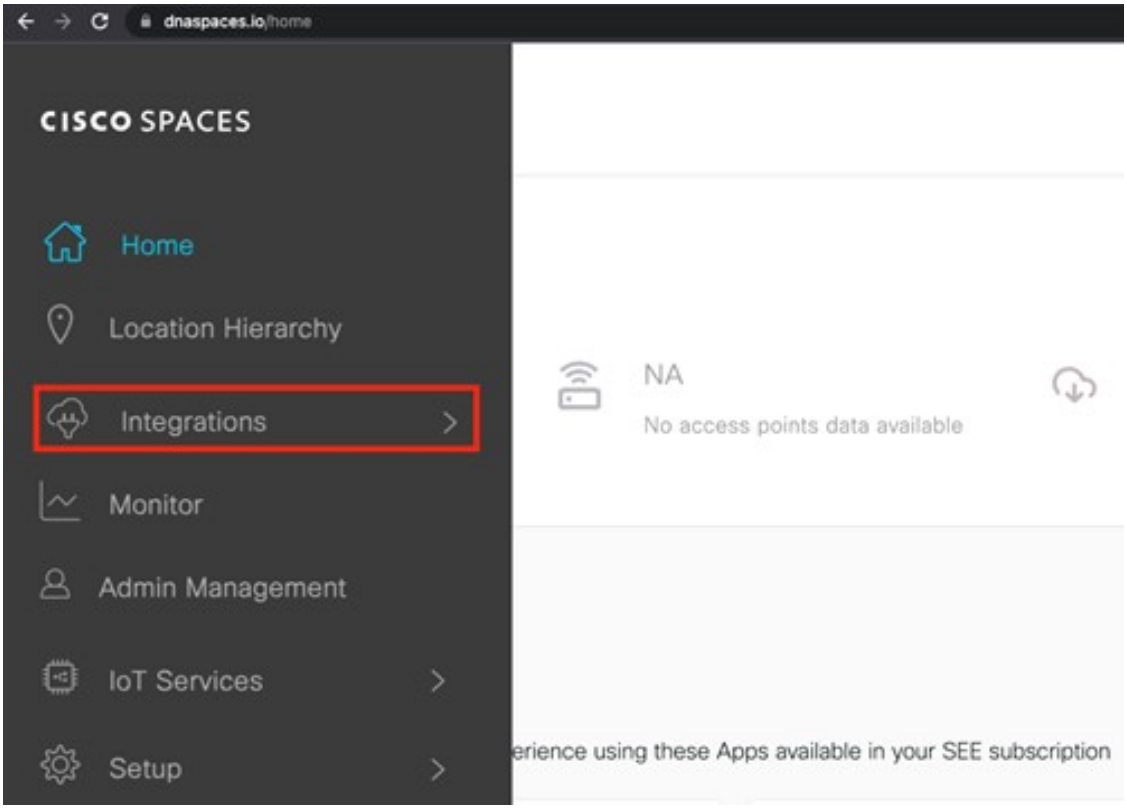
Cisco Spaces と Cisco DNA Center を統合するには、 Cisco Spaces アカウントが必要です。

手順

ステップ 1 dnaspace.io でアカウントをアクティブ化するには、cisco-dnaspace-support@external.cisco.com に電子メールを送信します。アクティベーションの要求に使用した電子メールアドレスにアクティベーションリンクが送信されます。

ステップ 2 Cisco DNA Center 統合用の dnaspaces.io からトークンを生成してコピーします。

図 *205 : dnaspaces.io* での *Cisco DNA Center* 統合用のトークン生成



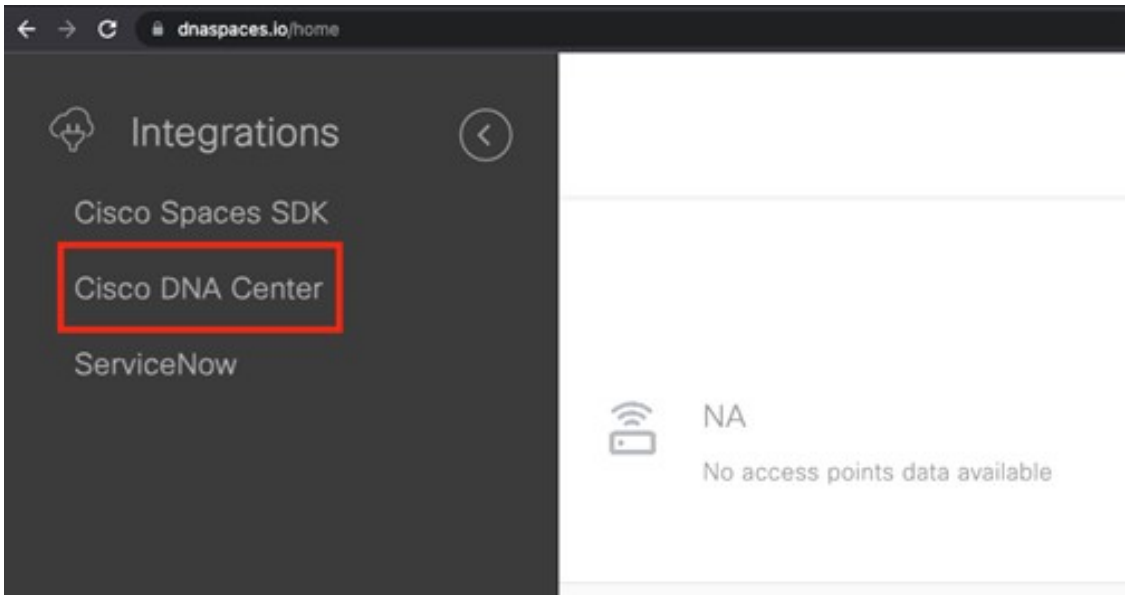
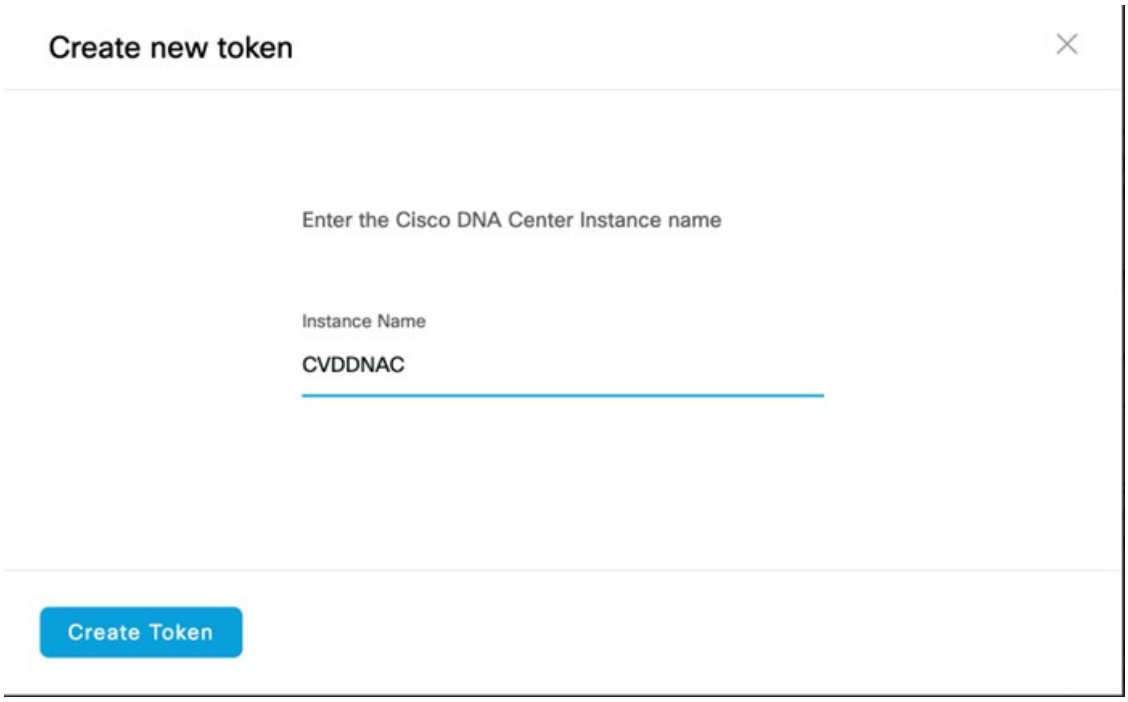


図 *206* : 新しいトークンの作成



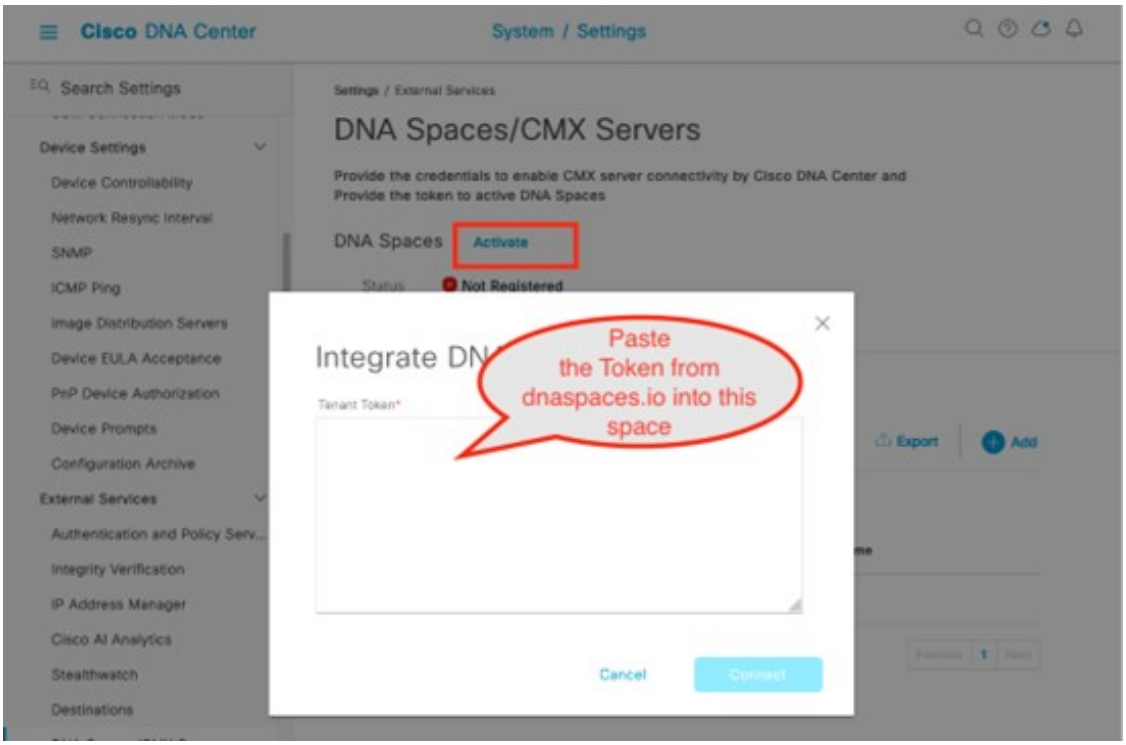
ステップ 3 Cisco DNA Center UI にログインします。

ステップ 4 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[CMX Servers/Cisco Spaces]**の順に選択します。

ステップ 5 Cisco Spaces の横にある [Activate] をクリックします。

ステップ 6 ダイアログボックスで、dnaspaces.io からコピーしたトークンを貼り付けます。

図 *207 : Cisco Spaces* テナントトークンを入力します



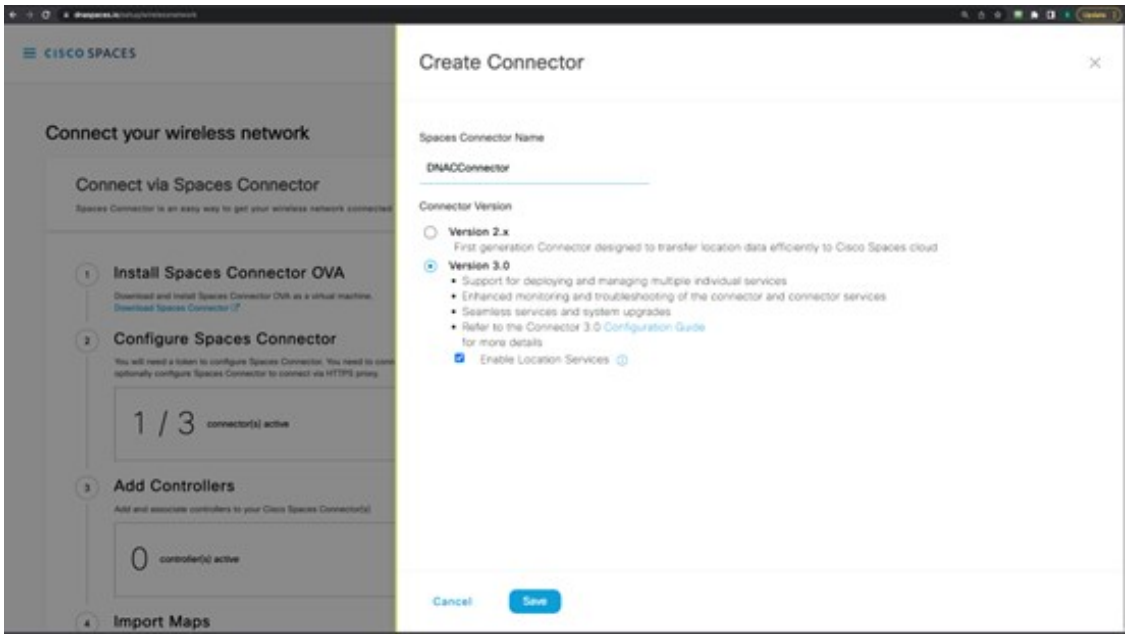
ステップ 7 ワイヤレスコントローラが dnaspaces.io に到達できない場合は、Cisco Spaces コネクタをダウンロードし、ワイヤレスコントローラと dnaspaces.io の両方に到達できるオンプレミスに展開します。このプロセスには、Cisco Spaces コネクタのデュアル インターフェイス バージョンが必要です。詳細については、Cisco Spaces：コネクタ コンフィギュレーション ガイド [英語] の「Retrieving a Token for a Connector from Cisco Spaces (Wireless)」のトピックを参照してください。

プライマリインターフェイス情報は、コネクタの電源を初めて投入したときに要求されます。マニュアルの記載に従い、CLI を使用してセカンダリインターフェイスの値を入力する必要があります。コネクタが dnaspaces.io に到達するためにプロキシが必要な場合は、コネクタ UI インターフェイスを介してプロキシを追加する必要があります。

ステップ 8 dnaspaces.io にログインし、メニューアイコンをクリックして、 **[Setup]** > **[Wireless Networks]** > **[Connect via Spaces]**の順に選択します。

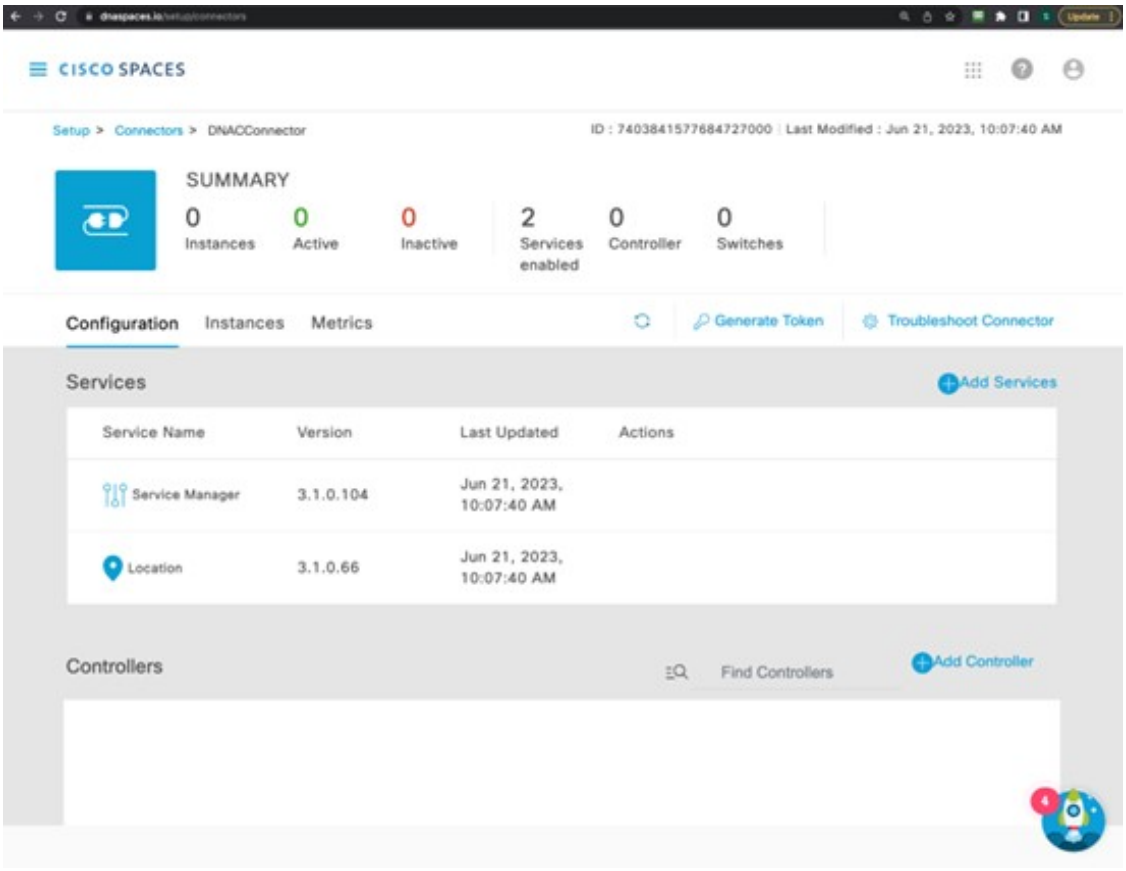
ステップ 9 [Create Connector] をクリックし、コネクタの名前を入力します。

図 *208* : コネクタの作成



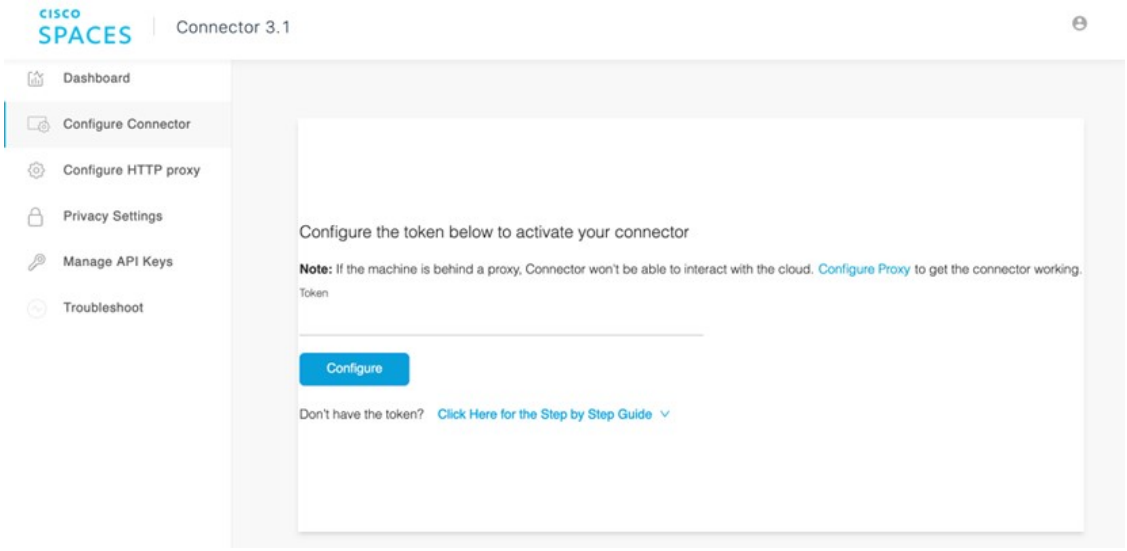
ステップ 10 最近作成されたコネクタを選択し、[Generate Token] をクリックします。

図 *209 : [Summary]* ウィンドウ



ステップ 11 Cisco Spaces コネクタ GUI にログインし、トークンを入力して、この展開されたコネクタを dnaspaces.io に登録します。

図 *210* : コネクタのアクティブ化



ステップ 12 コネクタが dnaspaces.io に正常に登録されたら、dnaspace.io のコネクタインスタンスからワイヤレスコントローラを追加できます。

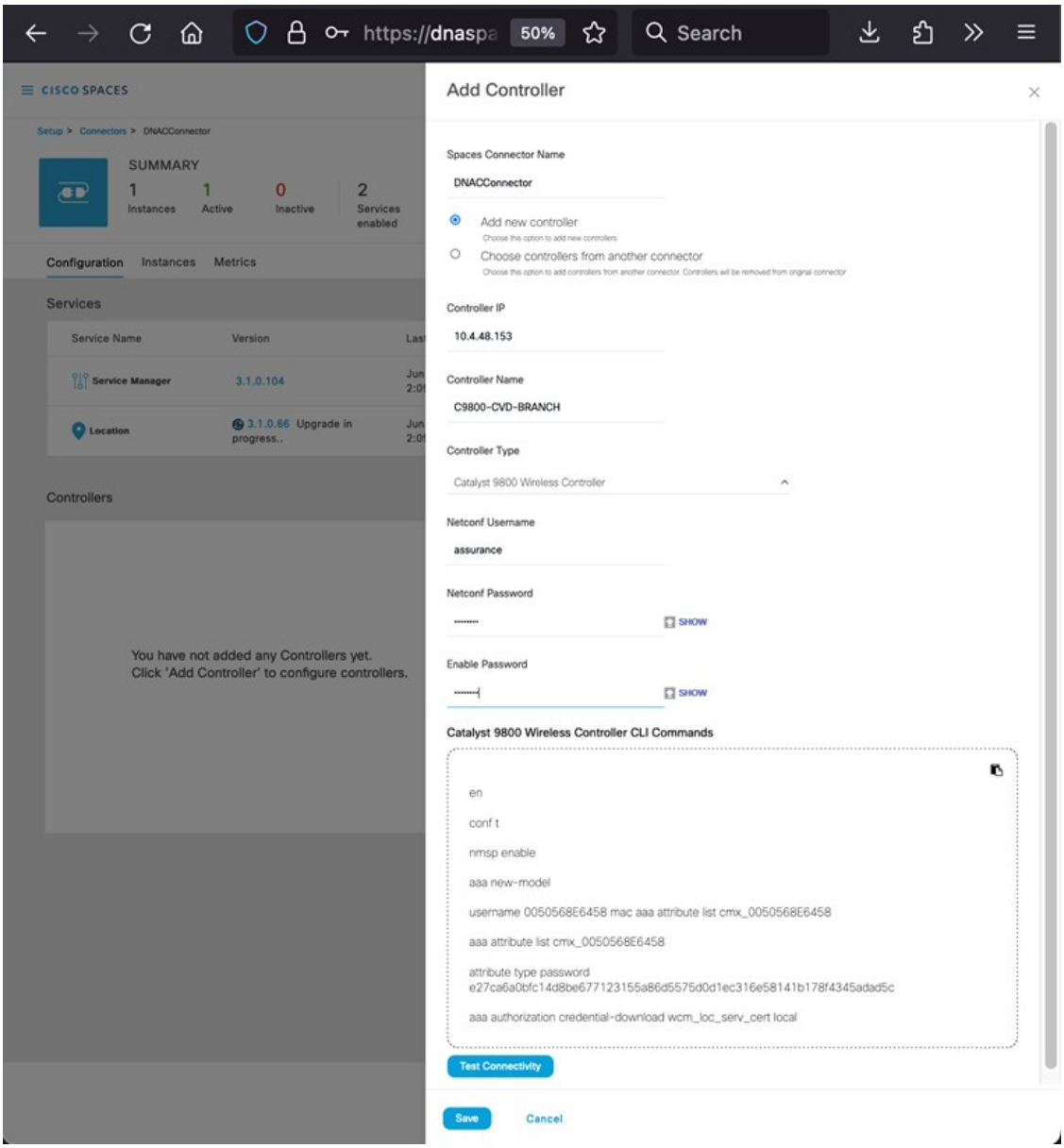
ステップ 13 dnaspaces.io にログインし、メニューアイコンをクリックして、 **[Setup]** > **[Wireless Networks]** > **[View Connectors]**の順に選択します。

ステップ 14 [Add Controller] をクリックします。

ステップ 15 [Controller Type] として [Catalyst 9800 Wireless Controller] を選択します。

ステップ 16 ユーザー名とパスワードを入力し、[Save] をクリックします。

図 *211* : コネクタの追加



ステップ 17 dnaspace.io で ワイヤレスコントローラ が [Active] と表示されるまで数分待ちます。

ステップ 18 Cisco DNA Center UI に移動します。

ステップ 19 左上隅にあるメニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 20 [Cisco Spaces/CMX Servers] をクリックします。

ステップ 21 [Location Services] ドロップダウンリストから自分のアカウントを選択します。

ステップ 22 左側の階層ツリーから [Global] を展開し、Cisco Spaces を使用してクライアントの場所を追跡するサイトを選択します。

ステップ 23 [Save] をクリックします。

（注） Cisco Spaces に割り当てられたサイトに変更を加えると、再同期が必要になる場合があります。再同期を実行するには、メニューアイコンをクリックして、**[Design]** > **[Network Settings]** > **[Wireless]**の順に選択します。サイトまたはフロアの 3 つのドットをクリックし、[Sync CMX Server/Cisco Spaces] を選択します。

オンプレミスの Cisco CMX と Cisco DNA Center の統合

オンプレミスの Cisco コネクテッド モバイル エクスペリエンス（CMX）を Cisco DNA Center と統合するには、次の手順を使用します。

手順

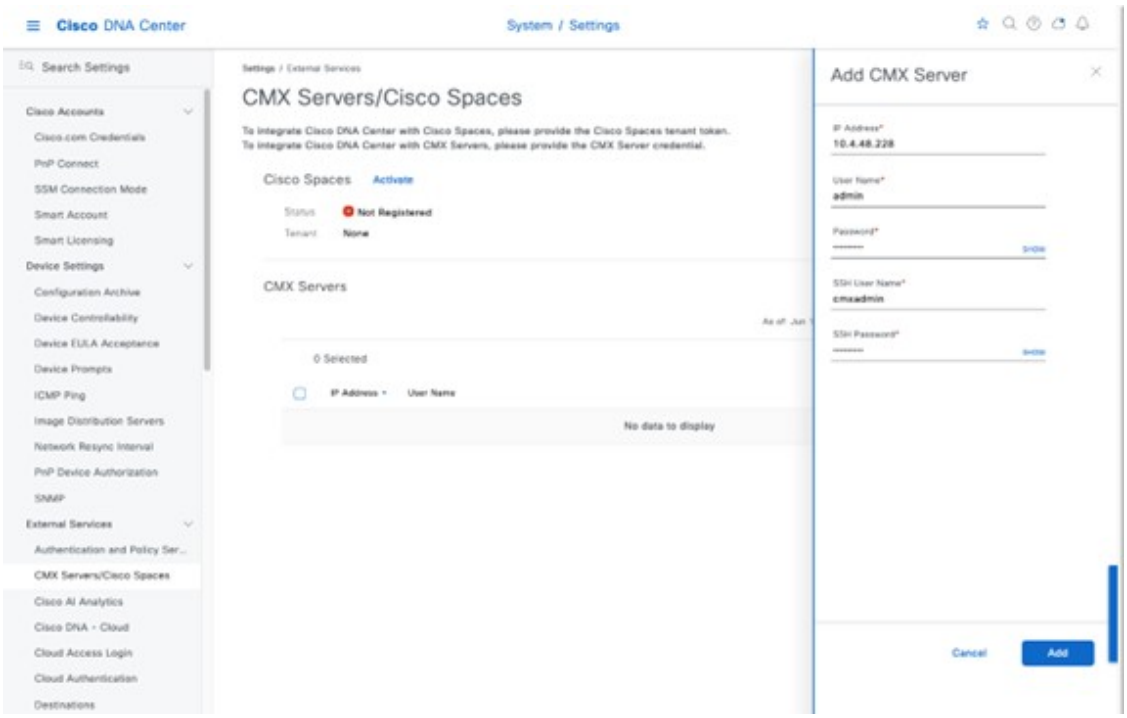
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[CMX Servers/Cisco Spaces]**の順に選択します。

ステップ 2 [CMX Servers] から、[Add] をクリックします。

[Add CMX Server] スライドインペインが表示されます。

ステップ 3 関連フィールドに必要な情報を入力します。

図 *212 :* オンプレミスの *CMX* と *Cisco DNA Center* の統合

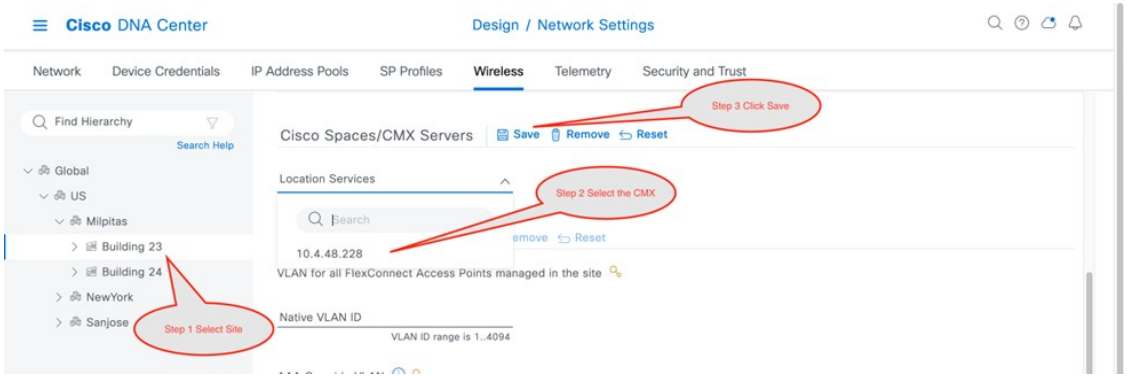


ステップ 4 [追加（Add）] をクリックします。

ステップ 5 CMX をサイトに割り当てるには、メニューアイコンをクリックして、 **[Design]** > **[Network Settings]** > **[Wireless]**の順に選択します。

ステップ 6 [Cisco Spaces/CMX Servers] をクリックします。

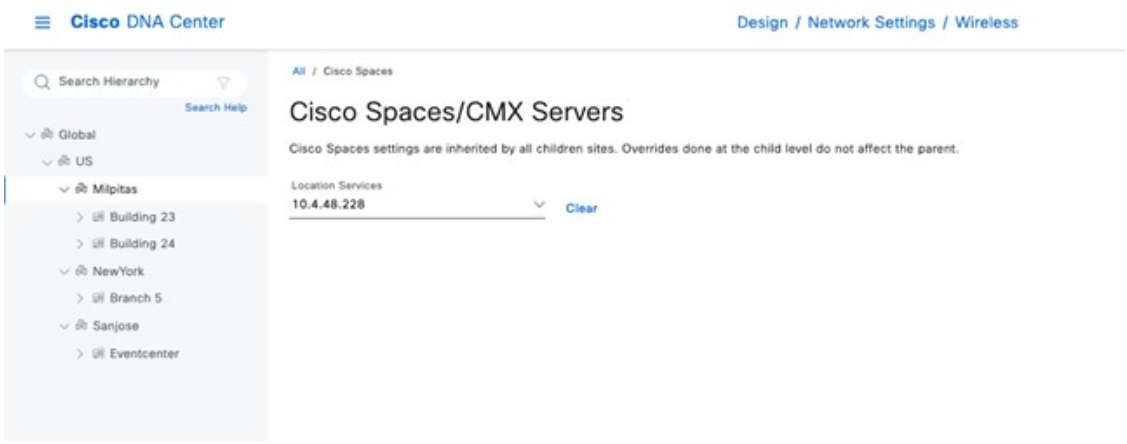
図 *213 : サイトへの CMX の割り当て*



ステップ 7 [Location Services] ドロップダウンリストから、CMX サーバーを選択します。

次の図は、Milpitas サイトの CMX サーバー（10.4.48.228）の例を示しています。

図 *214 : Cisco DNA Center* を介した *CMX* サイトの割り当て



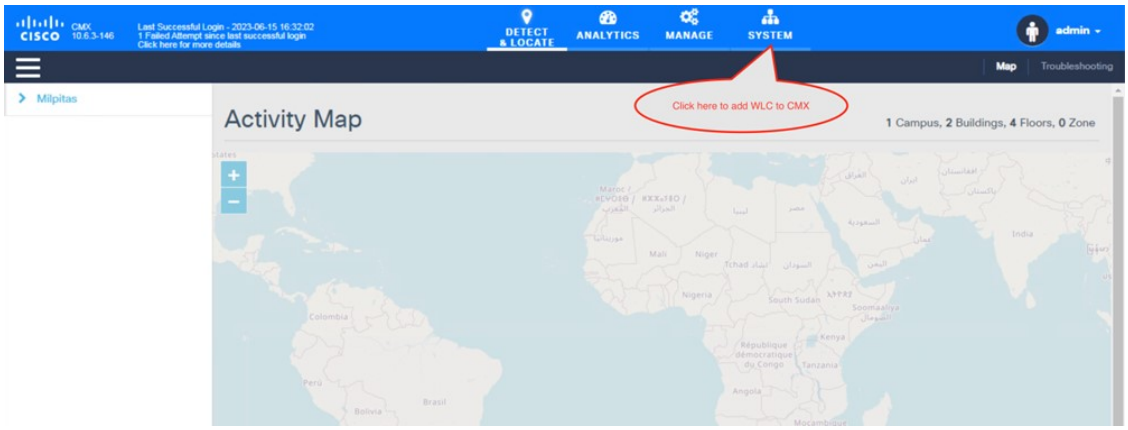
CMX サーバーに場所が割り当てられると、そのサイトに関連するサイト階層、そのサイト内の AP、および AP 位置情報が CMX サーバーと同期されます。

（注）

CMX を Cisco DNA Center と統合しても、ワイヤレスコントローラは CMX サーバーに自動的に追加されません。CMX GUI インターフェイスを使用して CMX にワイヤレスコントローラを手動で追加するには、次の手順を実行します。

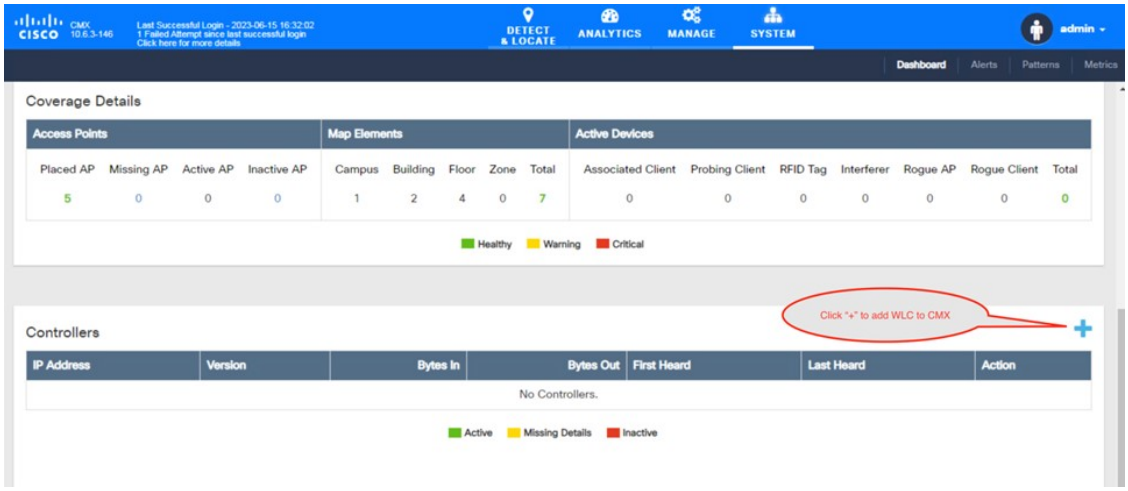
1. CMX GUI インターフェイスにログインし、[SYSTEM] に移動します。

図 *215 :* ワイヤレスコントローラ を追加する *CMX GUI*



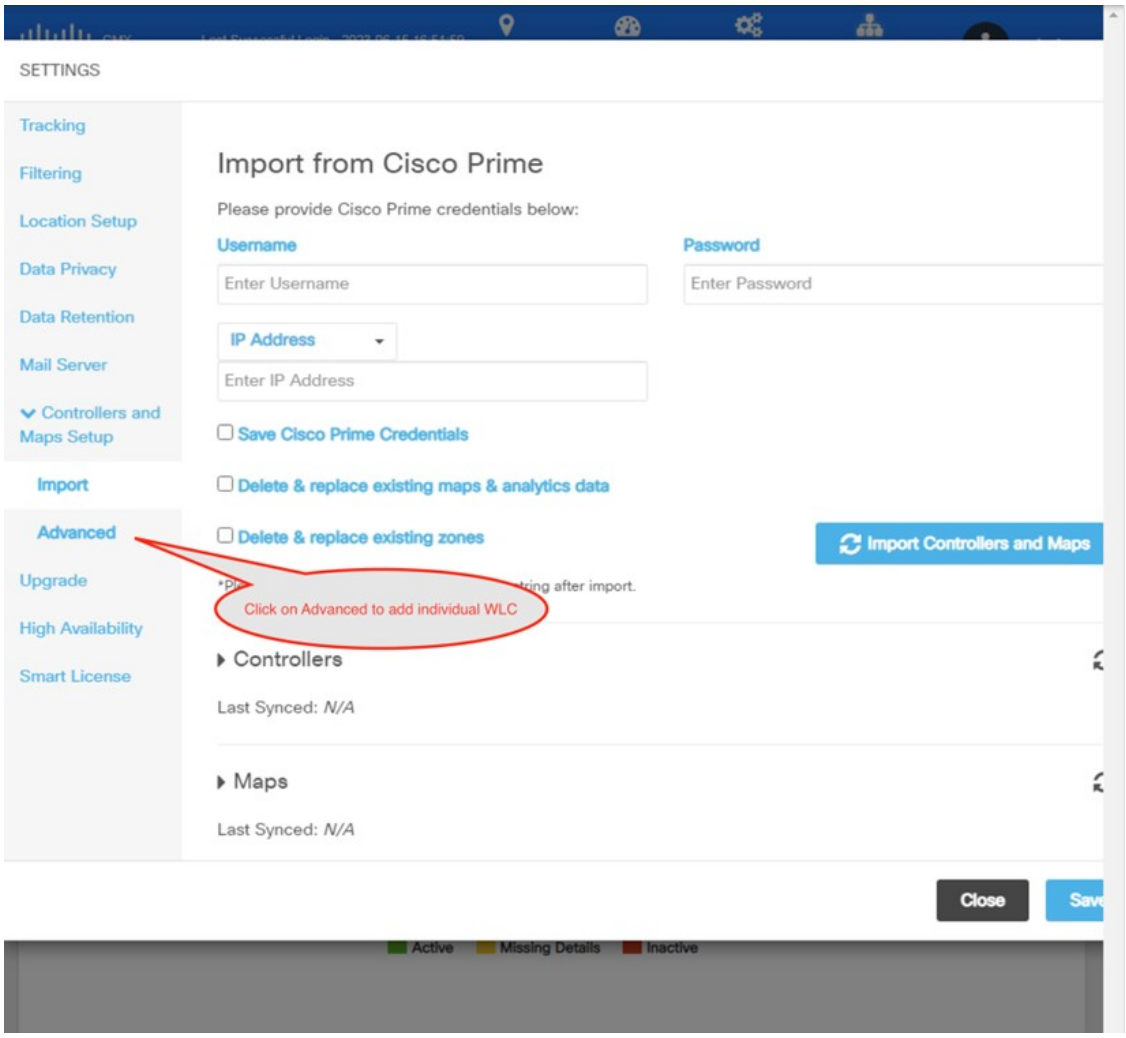
2. [+] をクリックして、ワイヤレスコントローラを CMX に追加します。

図 *216 : CMX*へのワイヤレスコントローラの追加



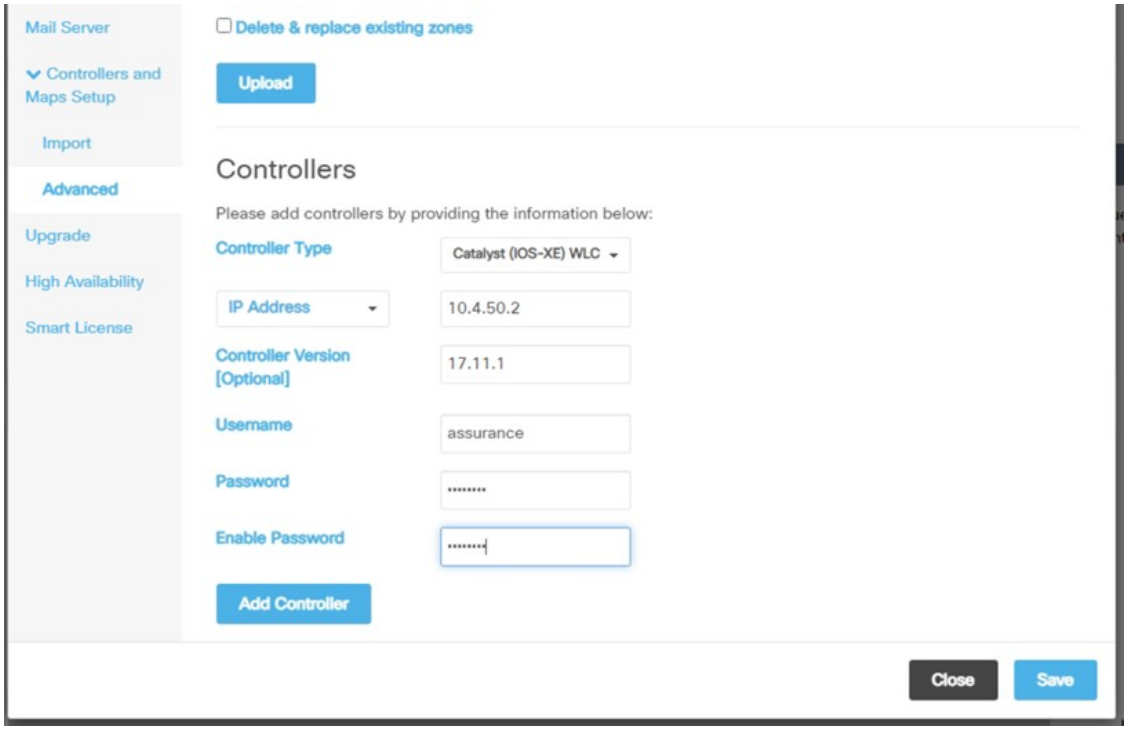
3. [Controllers and Maps Setup] で [Advanced] をクリックします。

図 *217 : [Controllers and Maps Setup]* : *[Advanced]*


SETTINGS
Tracking
Filtering
Location Setup
Data Privacy
Data Retention
Mail Server
Controllers and Maps Setup
Import
Advanced
Upgrade
High Availability
Smart License
Import from Cisco Prime
Please provide Cisco Prime credentials below:
Username
Enter Username
Password
Enter Password
IP Address
Enter IP Address
Save Cisco Prime Credentials
Delete & replace existing maps & analytics data
Delete & replace existing zones
Import Controllers and Maps
Click on Advanced to add individual WLC
Controllers
Last Synced: N/A
Maps
Last Synced: N/A
Close
Active
Missing Details
Inactive

4. 次の図に示されているように、[Controllers] から [Add Controller] をクリックして、ワイヤレスコントローラを CMX に追加します。

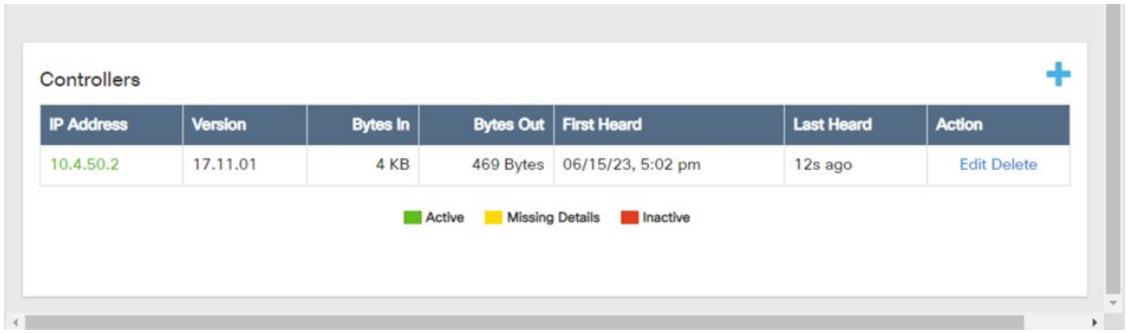
図 *218 :* 個々のワイヤレスコントローラ情報



5. [Save] をクリックします。

   ワイヤレスコントローラのリストが表示されます。

図 *219 :* ワイヤレスコントローラのリスト



ハードウェアのアップグレード、更新、および交換

シスコ ワイヤレス コントローラの交換

Cisco DNA Center では、ワイヤレスコントローラの交換ワークフローはサポートされていないため、ワイヤレスコントローラで直接交換を実行する必要があります。SSO ペアのいずれかのボックスに障害が発生し、交換する必要がある場合は、ワイヤレスネットワークの中断を回避しながら、この手順に従ってデバイスをクラスタに戻すことを推奨します。

手順

ステップ 1 障害が発生したボックスを物理的に切断し、返品許可（RMA）のためにボックスを送ります。

ステップ 2 アクティブなワイヤレスコントローラがより優先順位が高いシャーシ（=2）で設定されていることを確認します。

ステップ 3 新しいボックスを受け取ったら、ネットワークおよび既存の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続する前に、基本パラメータ（ログイン情報、IP 接続、および RMI を含む冗長構成（該当する場合））をオフラインで設定します。シャーシの優先順位は必ず 1 に設定してください。1 にすることで、SSO ペアが形成されると、このボックスがスタンバイになり、既存のアクティブ ワイヤレスコントローラが中断されなくなります。

ステップ 4 新しいボックスに設定を保存し、電源をオフにします。

ステップ 5 新しい Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをネットワーク（アップリンクおよび RP ポート）に物理的に接続します。

ステップ 6 新しいボックスの電源をオンにします。

ステップ 7 ボックスが起動し、SSO ペアが再度形成され、新しいボックスがスタンバイホット状態になります。

AP の交換

AP ハードウェアを交換するには、次の手順を実行します。Cisco DNA Center には、ハードウェア障害などの理由による AP ハードウェア交換のガイド付きワークフローがあります。

始める前に

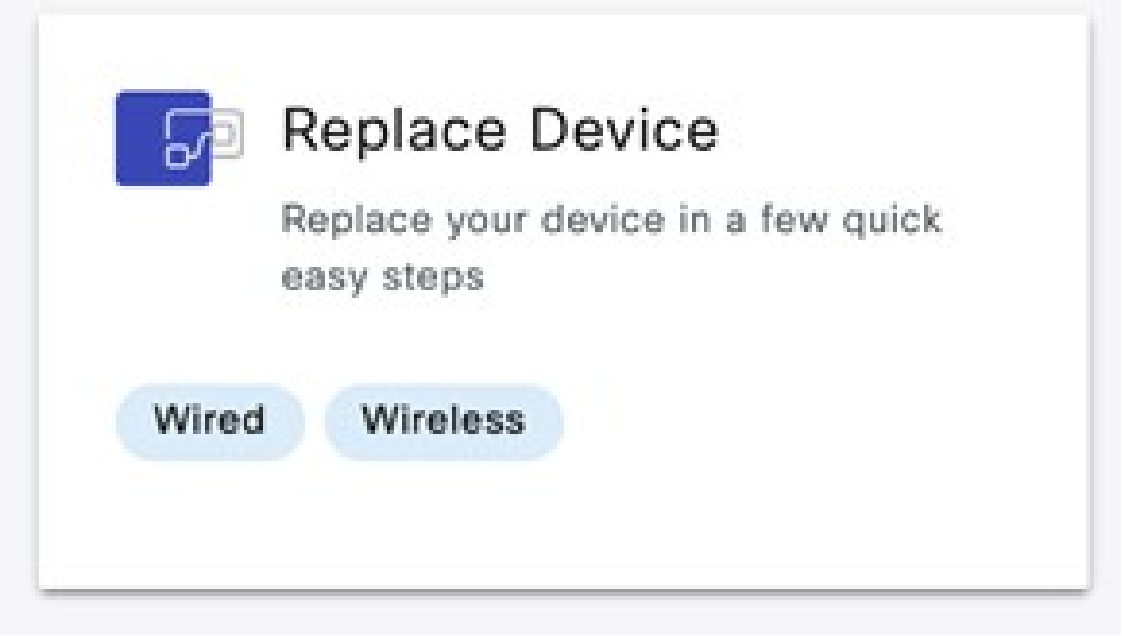
- 交換する AP を Cisco DNA Center でプロビジョニングしている必要があります。
- 交換する AP は到達不能状態である必要があります。
- 新しい AP は、古い AP が登録されていたワイヤレスコントローラに登録されます。
- 新しい AP は Cisco DNA Center インベントリウィンドウに表示されます。

AP を交換する場合、古い AP と新しい AP は同じモデルである必要があります。古い AP を別のモデルと交換する場合は、次のサブセクションで説明されている**アクセスポイントの更新**ワークフローを使用します。

手順

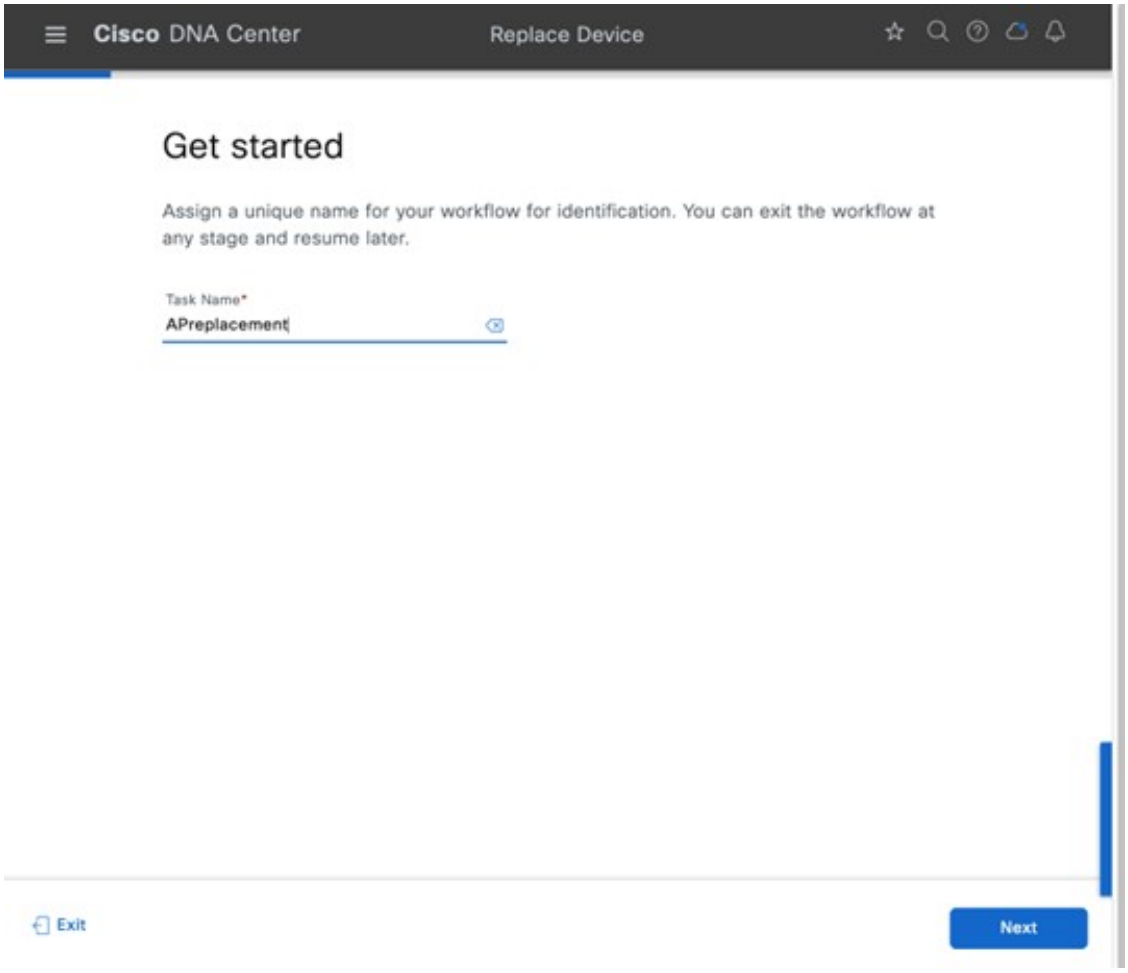
ステップ 1　左上隅にあるメニューアイコンをクリックして、**[Workflows]** > **[Replace Device]** の順に選択します。

図 *220 :* デバイスの交換



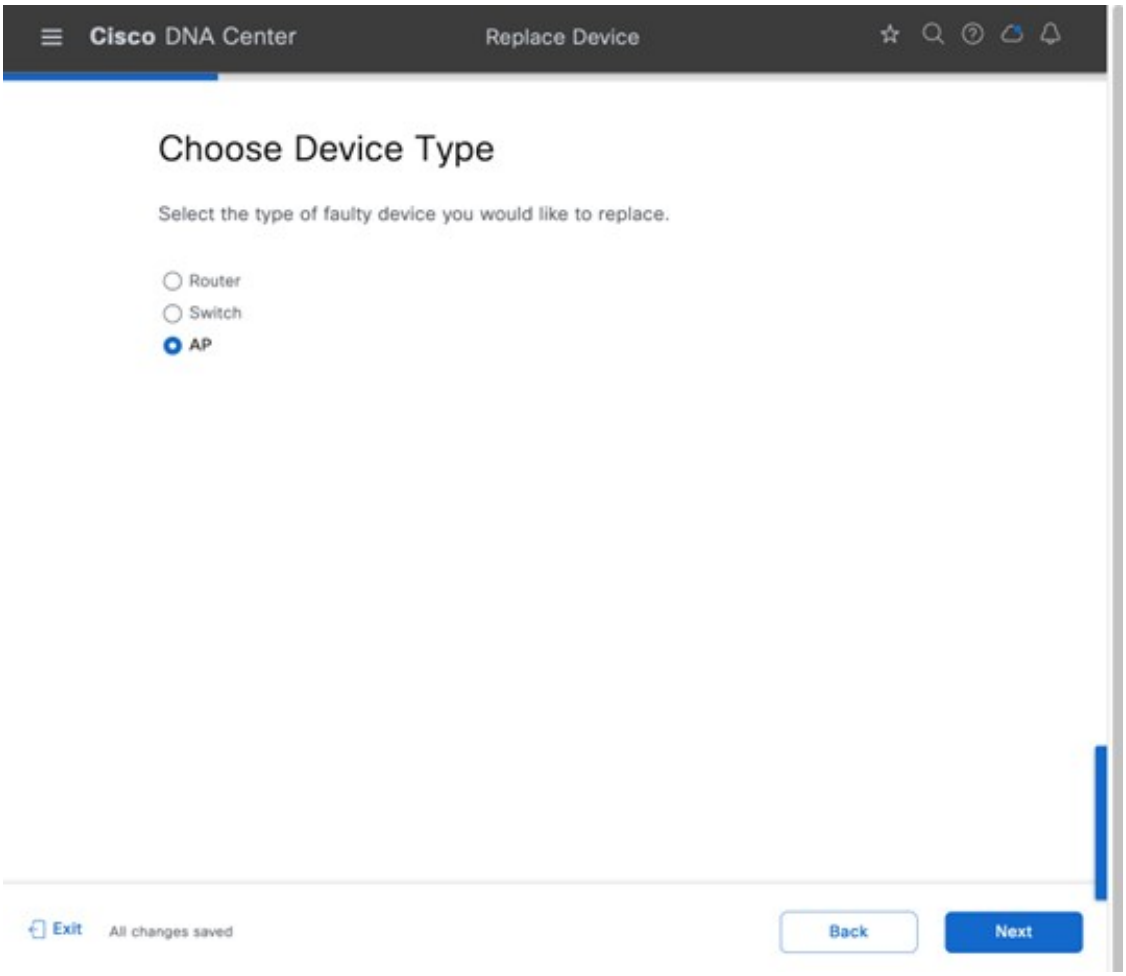
ステップ 2　[Get Started] ウィンドウで、ワークフローの一意の [Task Name] を入力します。

図 *221 :* はじめに



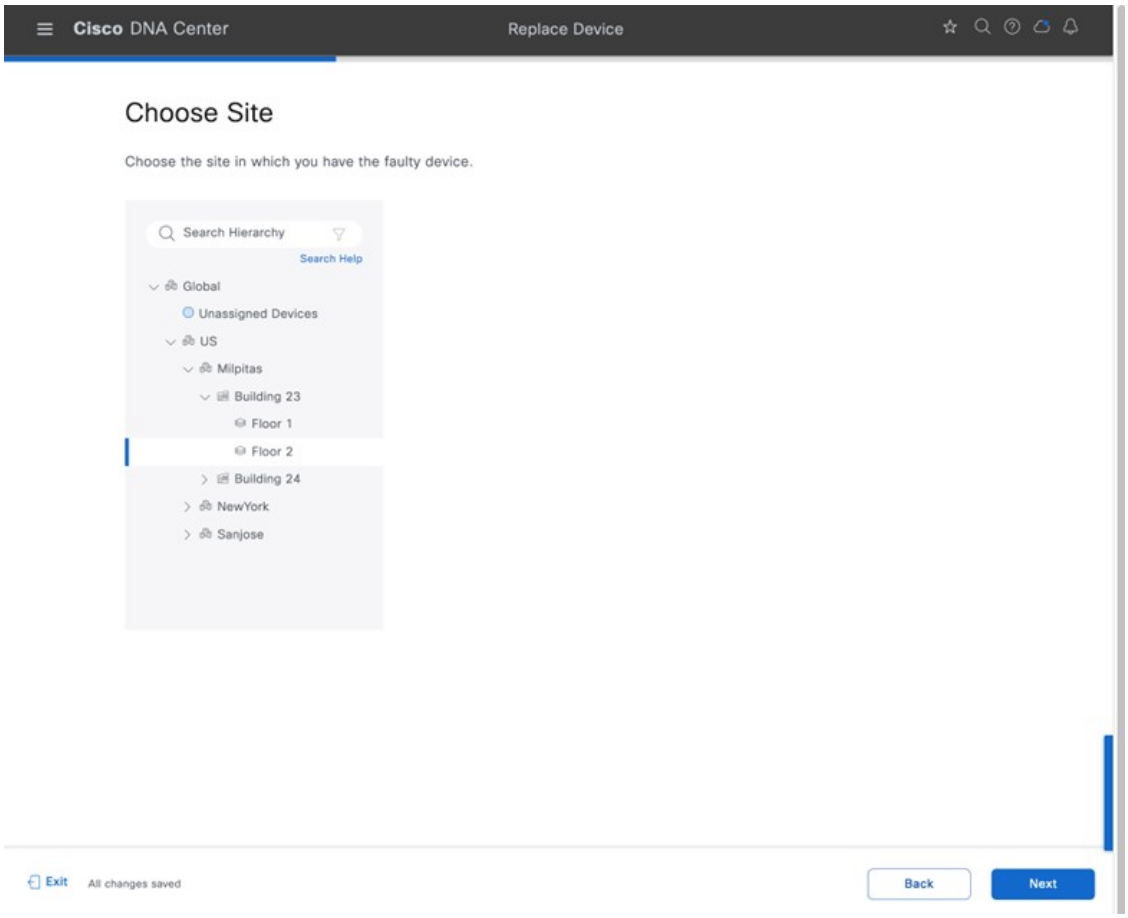
ステップ 3 [Choose Device Type] ウィンドウで、[AP] を選択します。

図 *222 : [Choose Device Type]*



ステップ 4 [Choose Site] ウィンドウで、AP を交換する必要があるサイトを選択します。

図 *223 : [Choose Site]*



ステップ 5 [Choose Faulty Device] ウィンドウで AP が見つからない場合は、次の手順を実行します。

a) [Add Faulty Device] をクリックします。

b) 故障したデバイスを選択し、[Next] をクリックします。

c) [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

図 *224 : [Choose Faulty Device]*

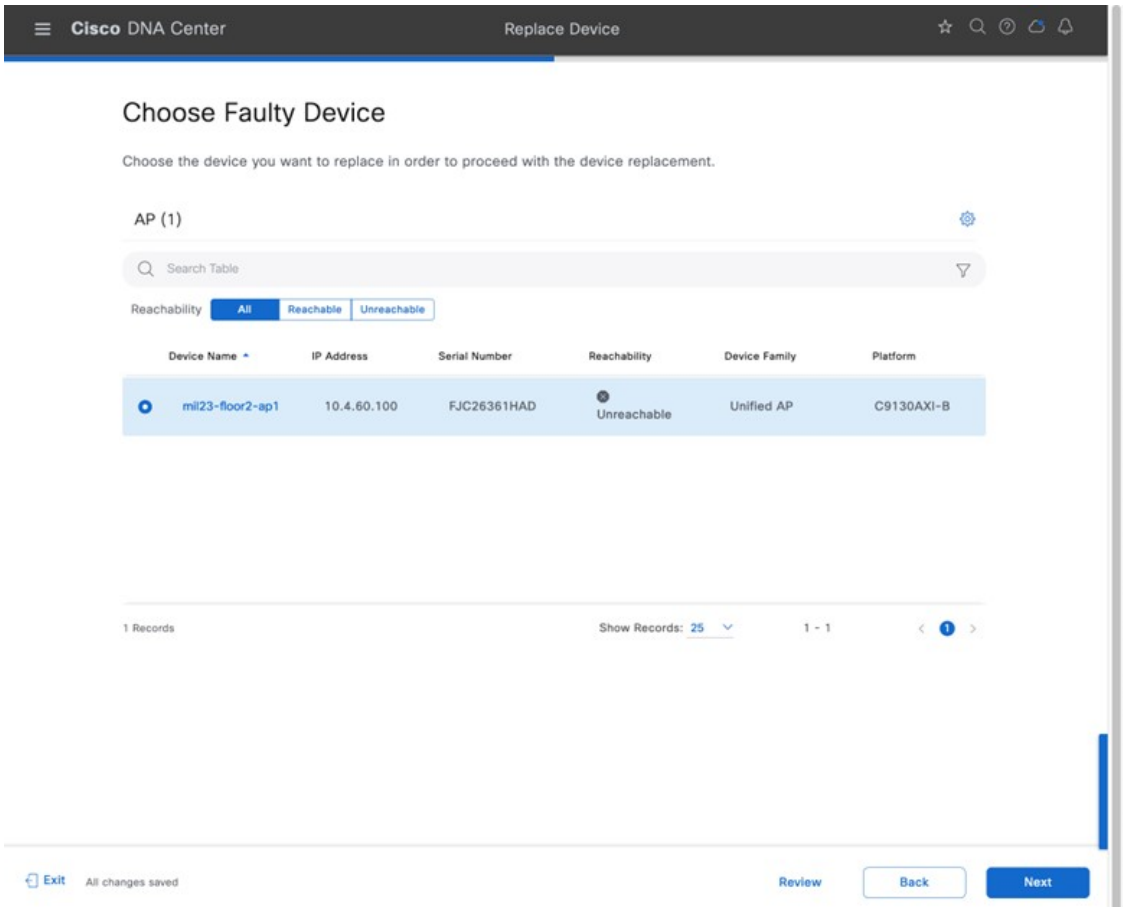
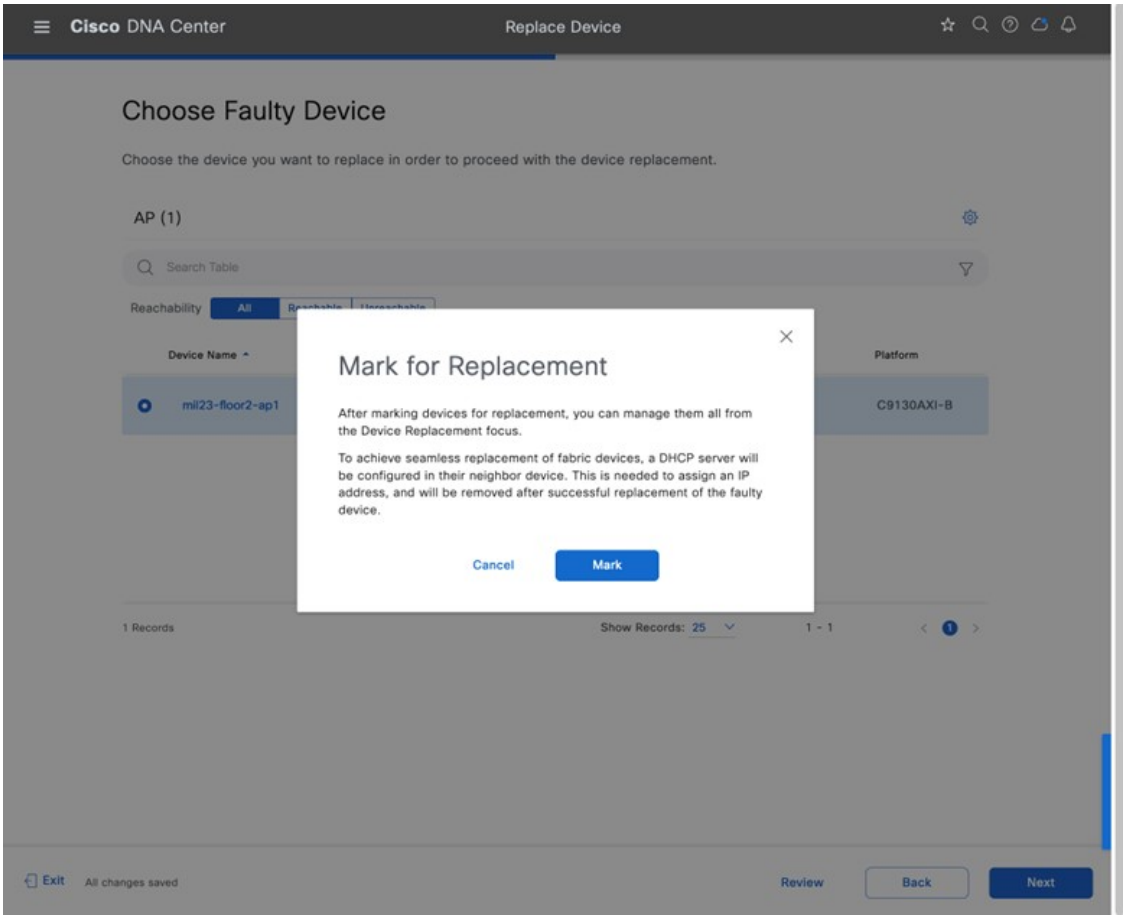


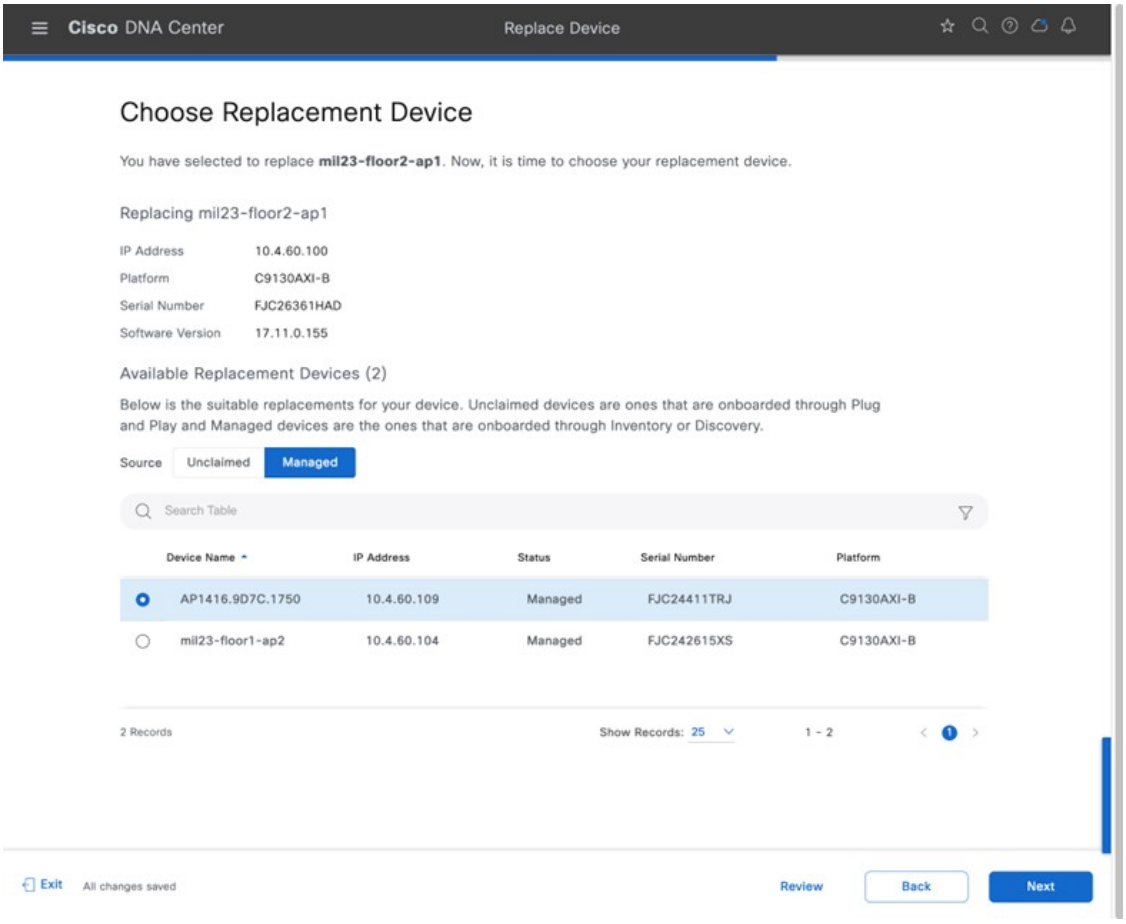
図 *225 : [Mark for Replacement]*



ステップ 6 [Choose Replace Device] ウィンドウで、[Unclaimed] タブまたは [Managed] タブから交換用デバイスを選択します。

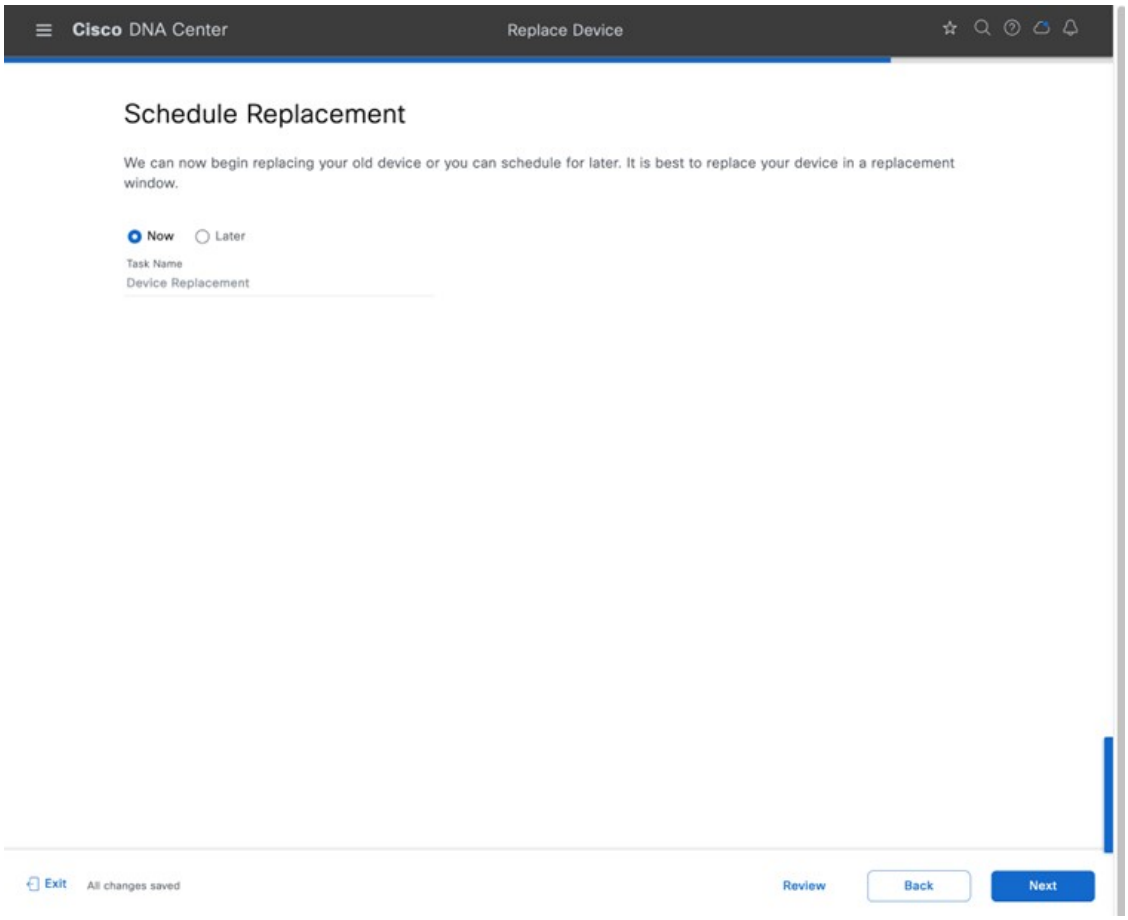
[Unclaimed] タブには、PnP によってオンボードされたデバイスが表示されます。[Managed] タブには、インベントリまたは検出プロセスによってオンボードされたデバイスが表示されます。

図 *226 : [Choose Replacement Device]*



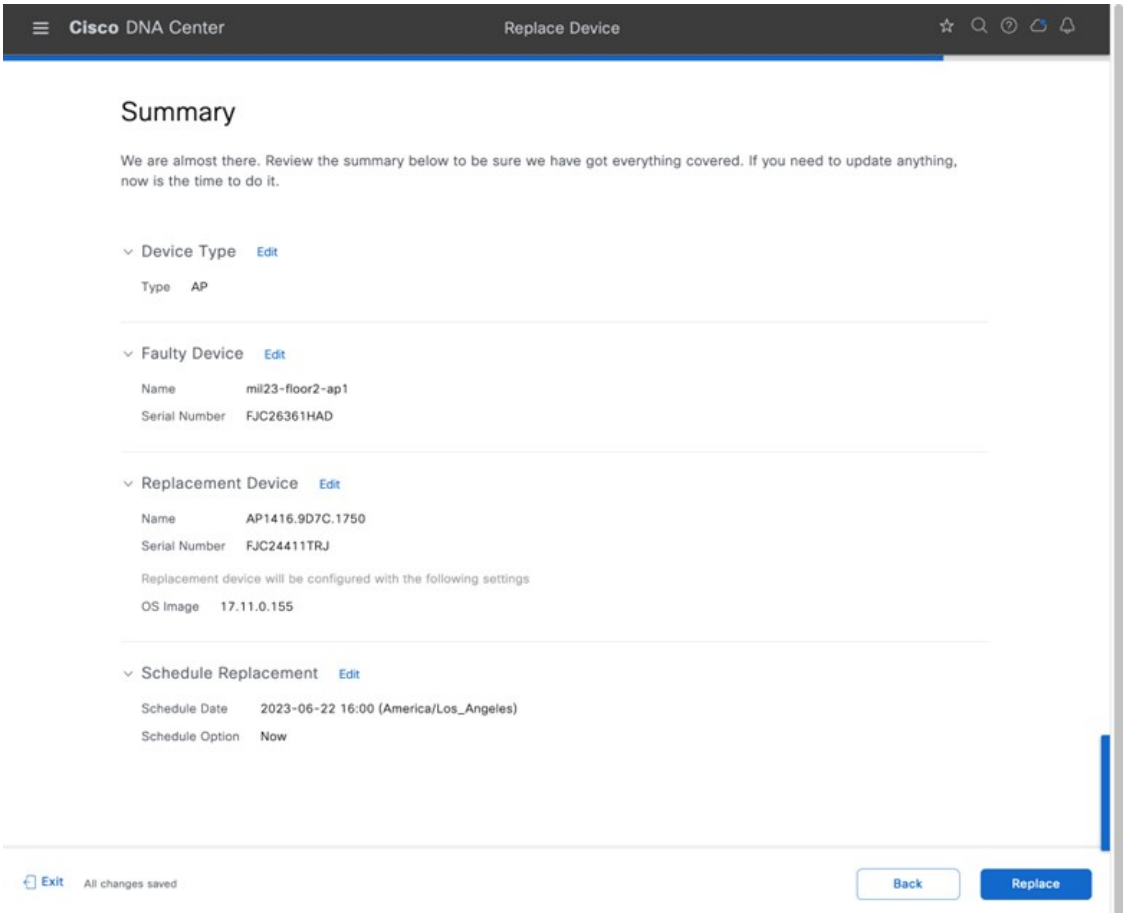
ステップ 7 [Schedule Replacement] ウィンドウで、[Now] をクリックしてデバイスの交換をただちに開始するか、[Later] をクリックしてデバイスの交換を特定の時間にスケジュールします。

図 *227 : [Schedule Replacement]*



ステップ 8 [Summary] ウィンドウで、設定を確認します。

図 *228 : [Summary]* ウィンドウ



ステップ 9 [Click Monitor Replacement Status] をクリックして [Provision] ウィンドウの [Mark for Replacement] ビューに移動します。

ステップ 10 [Device 360] ウィンドウのタイムラインと [Event] テーブルに RMA が表示されます。

図 *229 : [Device 360]* ウィンドウ

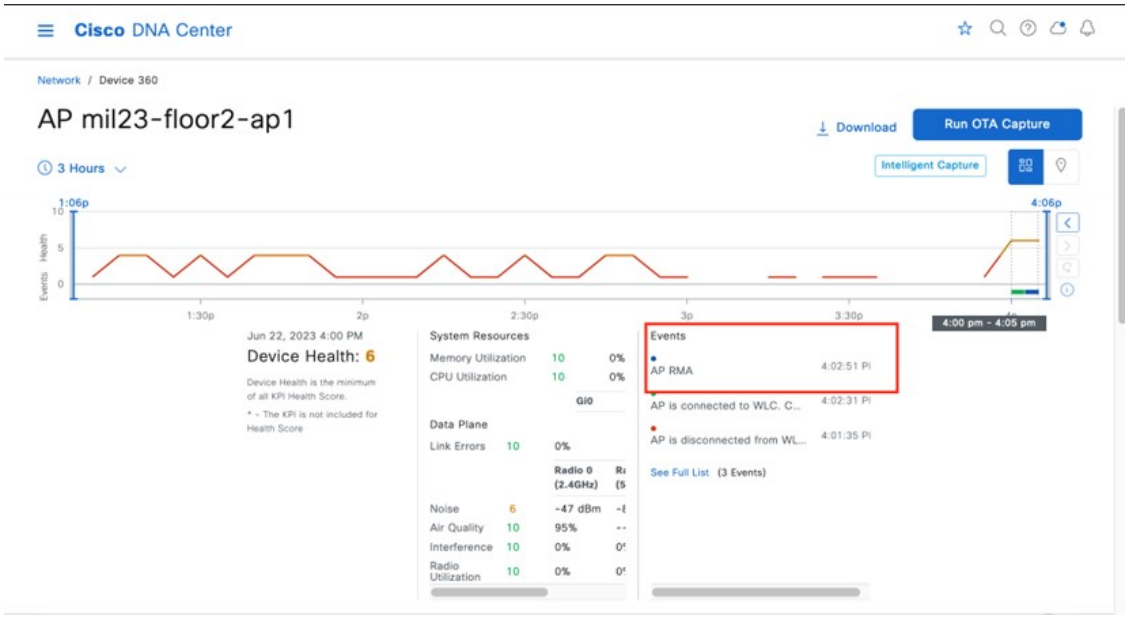
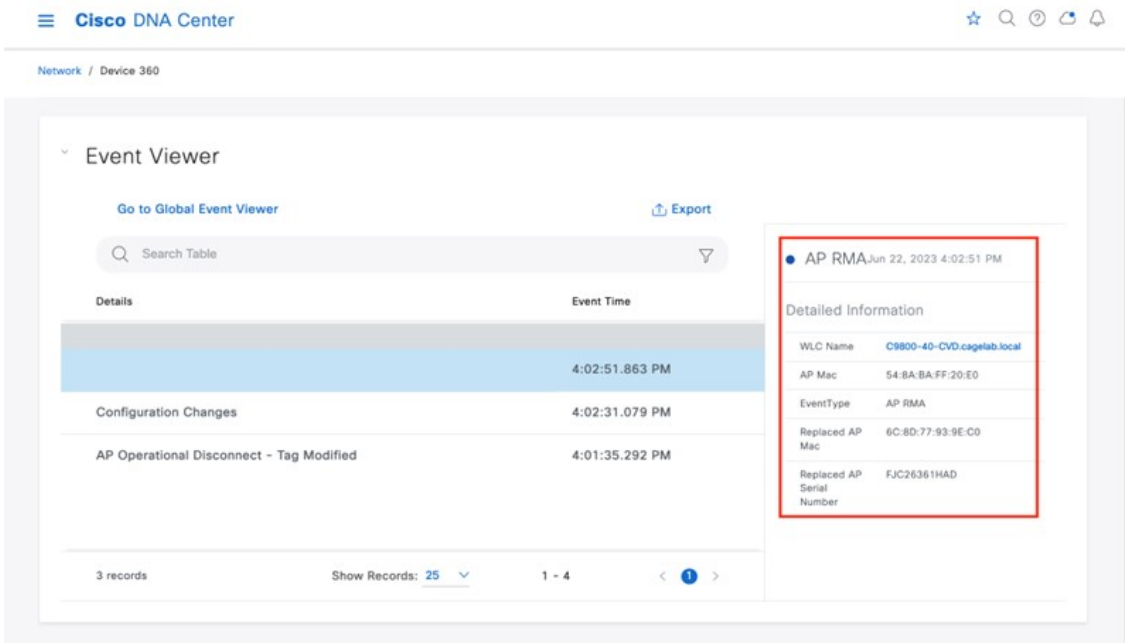


図 *230 :* イベント ビューア



AP の更新

Cisco DNA Center には、AP ハードウェアの更新に関するガイド付きワークフローがあります。次の手順を使用して、Cisco DNA Center で古い AP を新しい AP に置き換えることができます。

始める前に

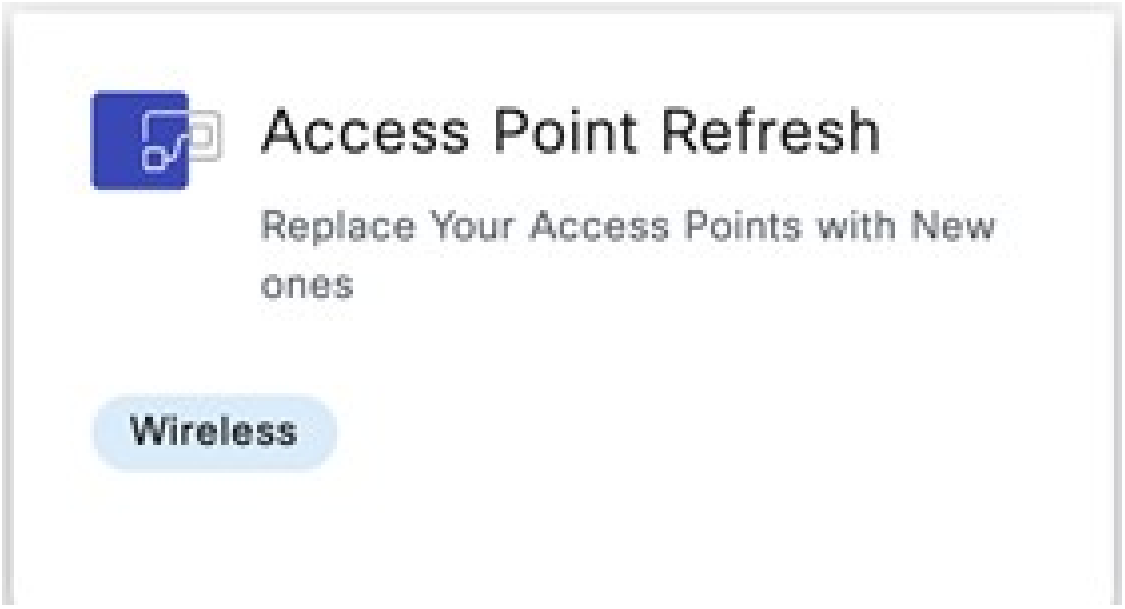
- 古い AP サイトはプロビジョニングする必要があります。
- 古い AP が到達不能状態であることを確認します。
- 新しい AP は、古い AP が登録されているワイヤレスコントローラに登録する必要があります。
- 新しい AP は、Cisco DNA Center インベントリで使用可能である必要があります。

内部アンテナを備えた AP を外部アンテナを備えた AP に置き換える場合は、外部アンテナの角度を手動で設定する必要があります。その逆も同様です。

手順

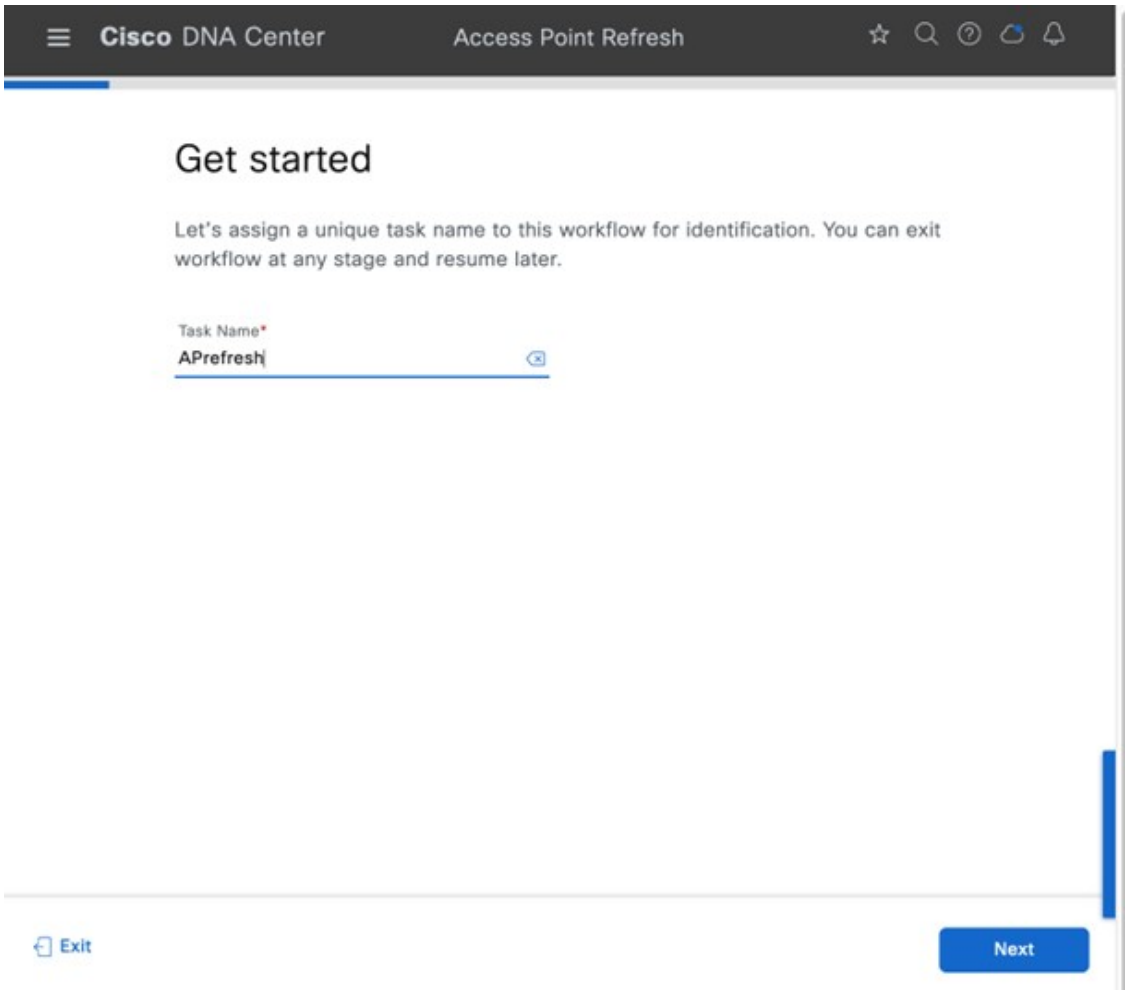
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Workflows]** > **[Access Point Refresh]** の順に選択します。

図 *231* : アクセスポイントの更新



ステップ 2 [Get Started] ウィンドウで、タスクの一意の名前を入力し、[Next] をクリックします。

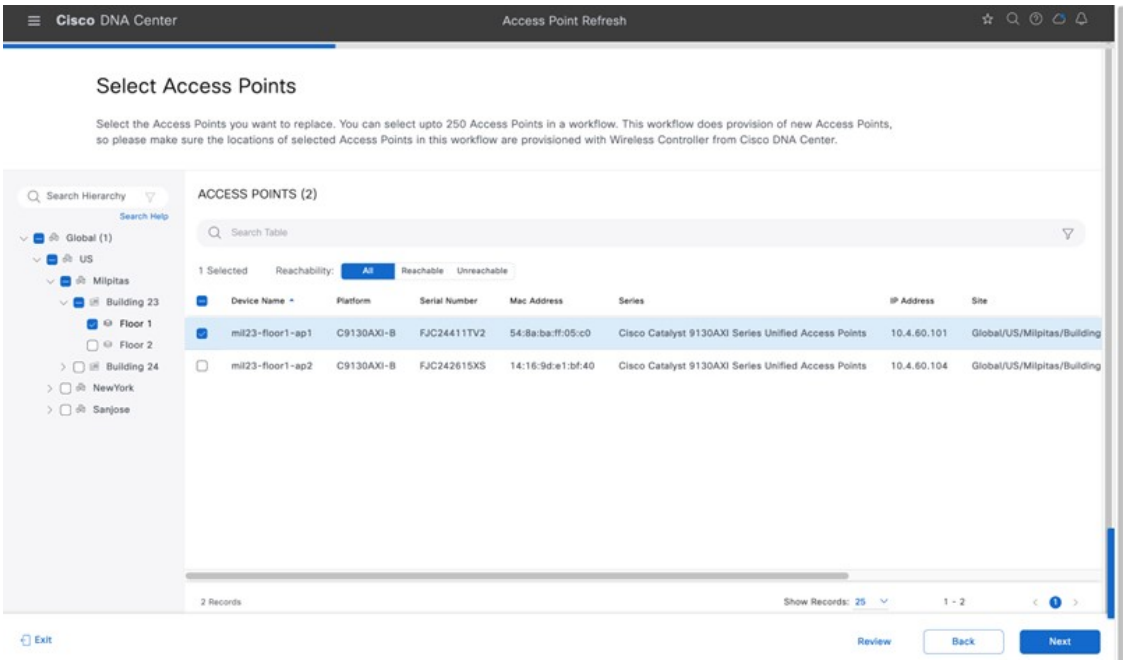
図 *232 :* はじめに



ステップ 3 [Select Access Points] ウィンドウで、次の手順を実行します。

1. 左側のペインで、AP を更新するフロアの横にあるチェックボックスをオンにします。
2. 右側のペインで、置き換える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。

図 *233 : [Select Access Points]*



ステップ 4 [Assign New APs to Old APs] ウィンドウで、カンマ区切り値（CSV）ファイルを使用して新しい AP の詳細を追加するには、次の手順を実行します。

1. [Download CSV] をクリックします。ダウンロードした CSV テンプレートファイルには、古い AP の詳細が含まれています。デバイス名を更新し、新しい AP のシリアル番号を追加します。
2. CSV ファイルをインポートするには、[Upload CSV] をクリックします。

ステップ 5 GUI を使用して新しい AP の詳細を追加するには、その AP の [Edit] アイコン（ ）をクリックし、[Edit details] で次の図に示されているように必要な変更を加えます。

図 *234* : 古い *AP* への新しい *AP* の割り当て

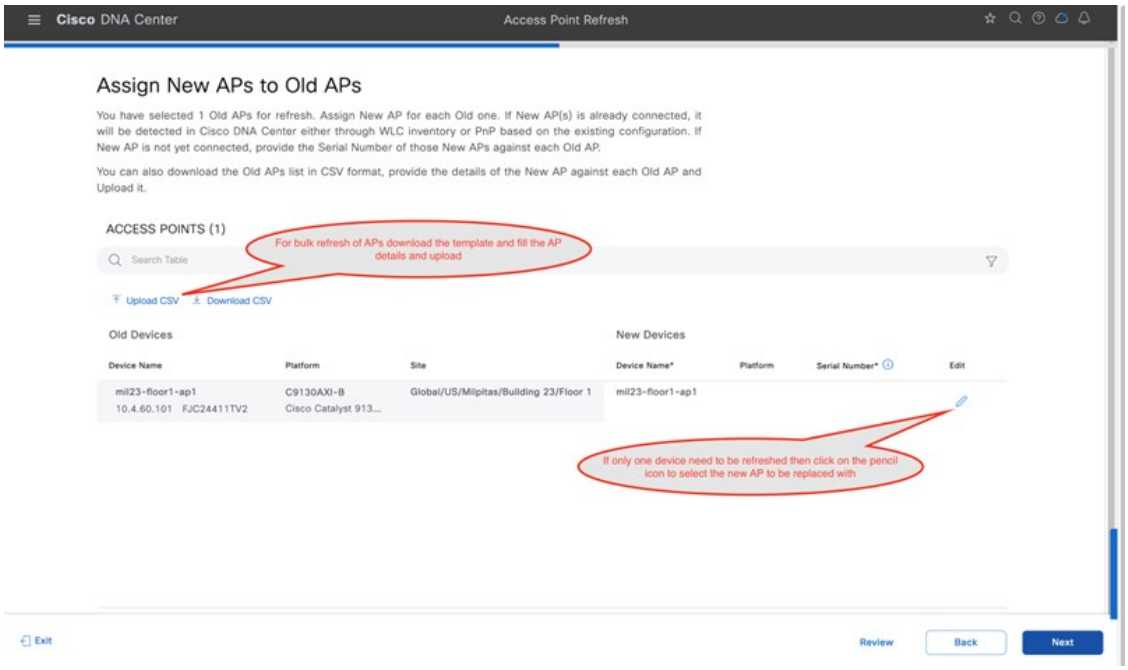
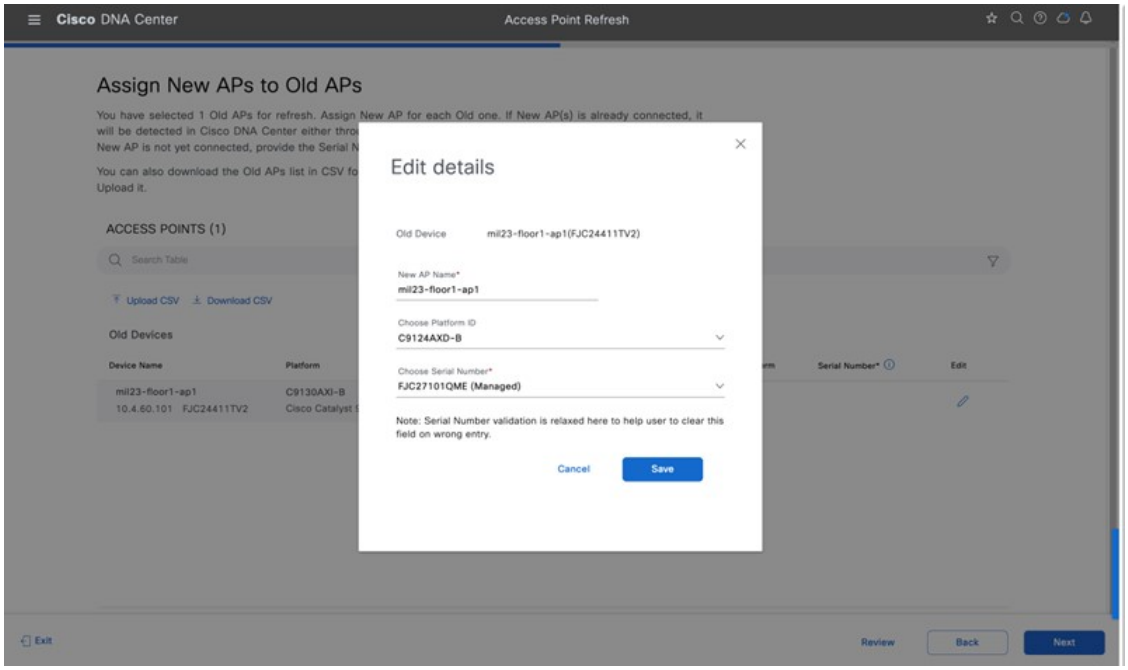


図 *235* : 詳細の編集



ステップ 6 [Save]、[Next] の順にクリックして、更新の概要を表示します。

図 *236* : 古い *AP* から新しい *AP* への設定のコピー

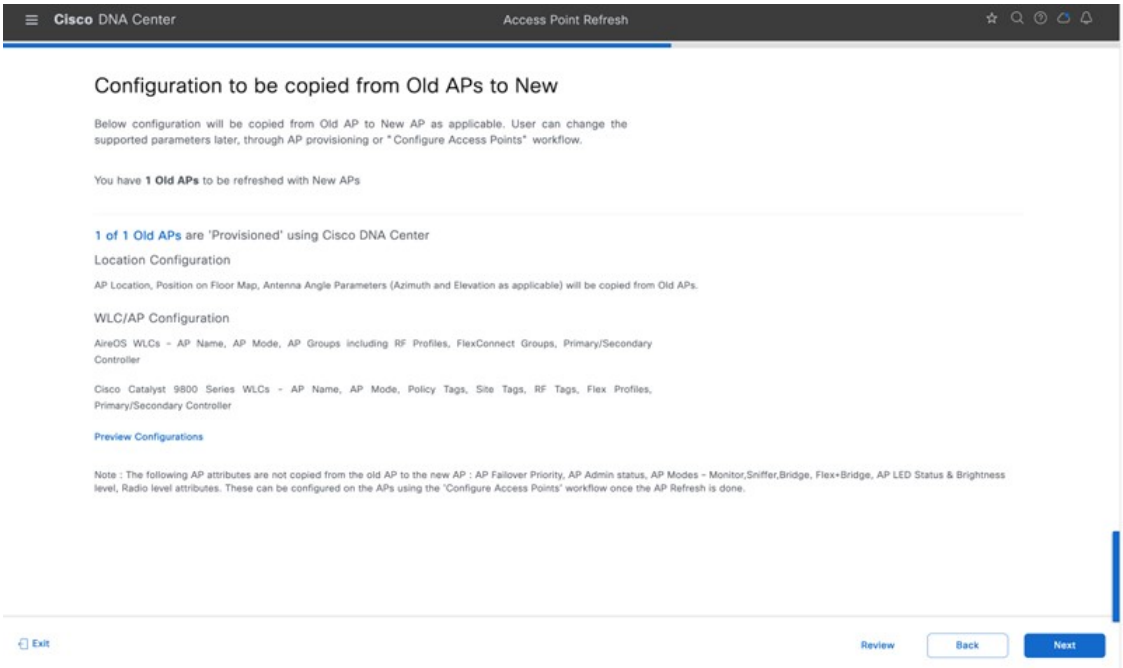
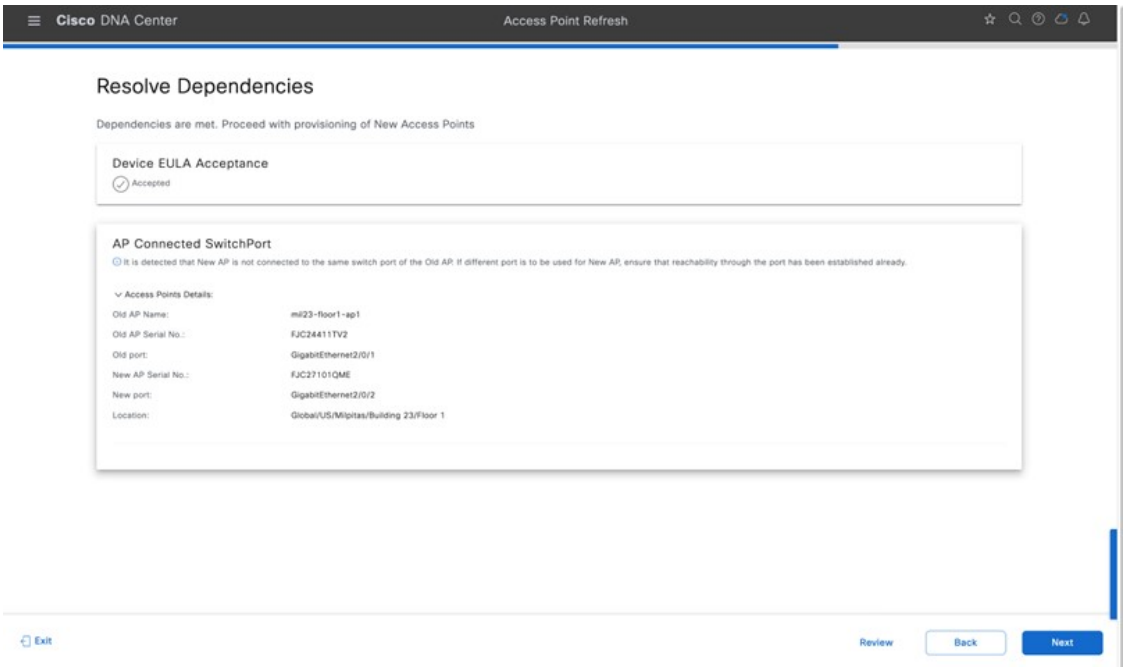
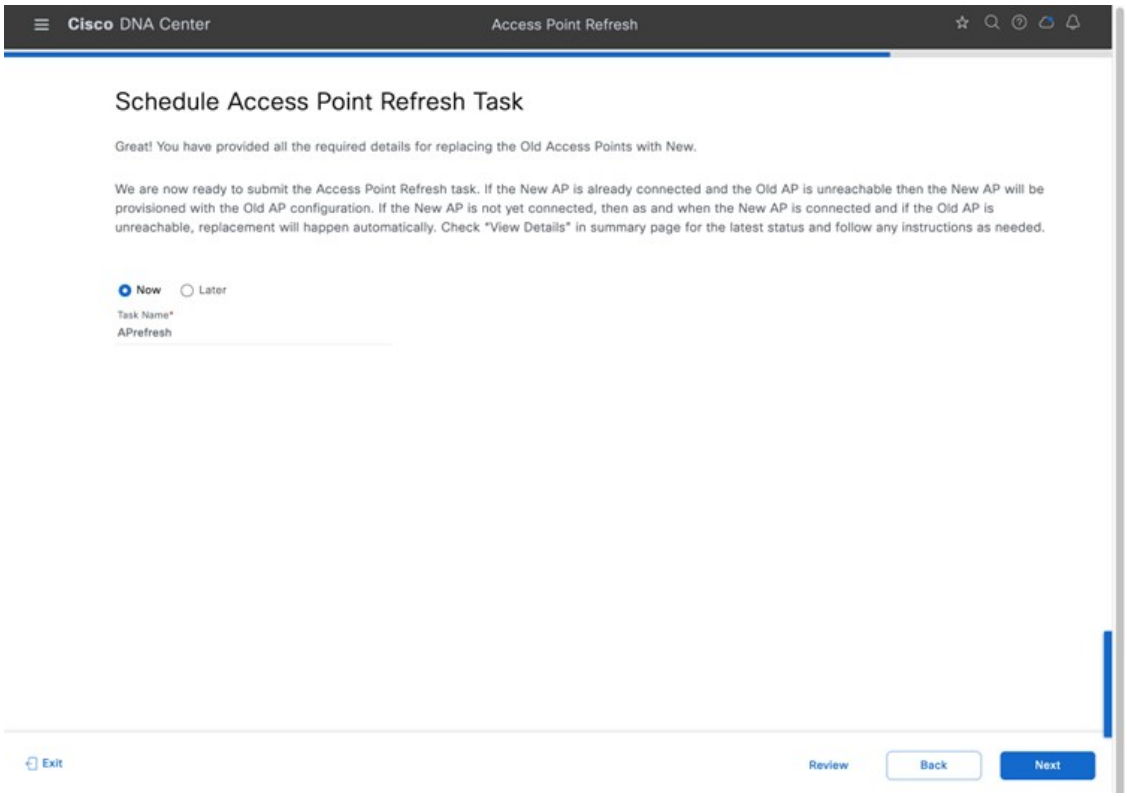


図 *237* : 依存関係の解決



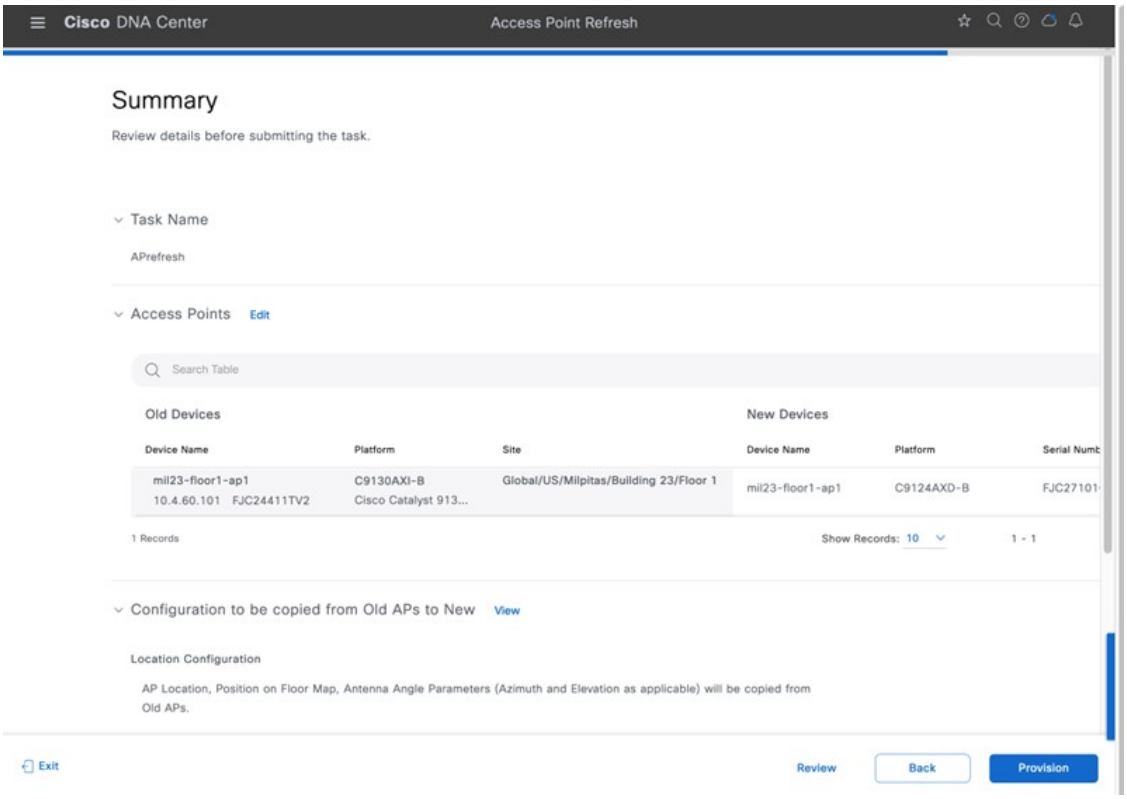
ステップ 7 [Schedule Access Point Refresh Task] ウィンドウで、[Now] をクリックして AP の交換をただちに開始するか、[Later] をクリックして AP の交換を特定の時間にスケジュールします。

図 ***238 : AP*** 更新タスクのスケジュール



ステップ 8 [Summary] ウィンドウで、設定を確認します。

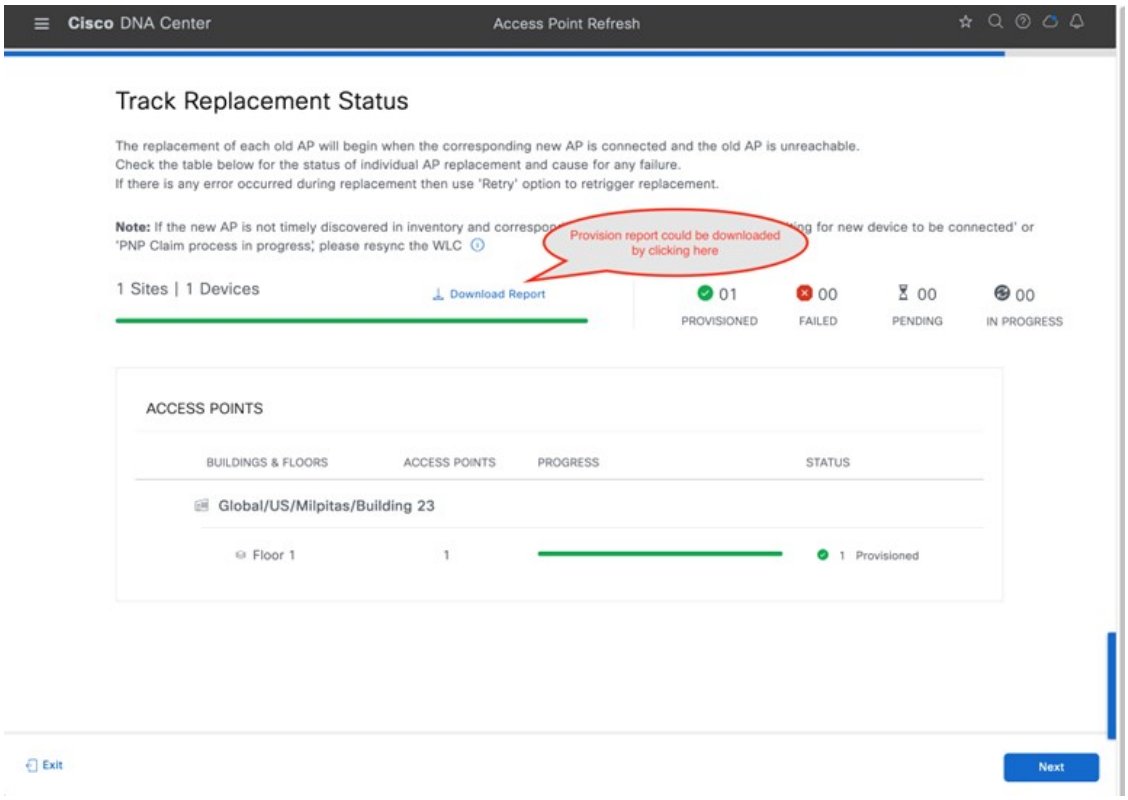
図 *239 : [Summary]* ウィンドウ



ステップ 9 [Provision] をクリックして、プロビジョニングを開始します。

ステップ 10 [Track Replacement Status] ウィンドウで、[Download Report] をクリックして、プロビジョニング ステータス レポートをダウンロードします。

図 *240* : 交換ステータスの追跡



ステップ 11 [Assurance AP 360] ページには、次の図に示されているように、タイムトラベルと [Events] テーブルの AP 更新タイムラインが表示されます。

図 *241* : デバイス *360*

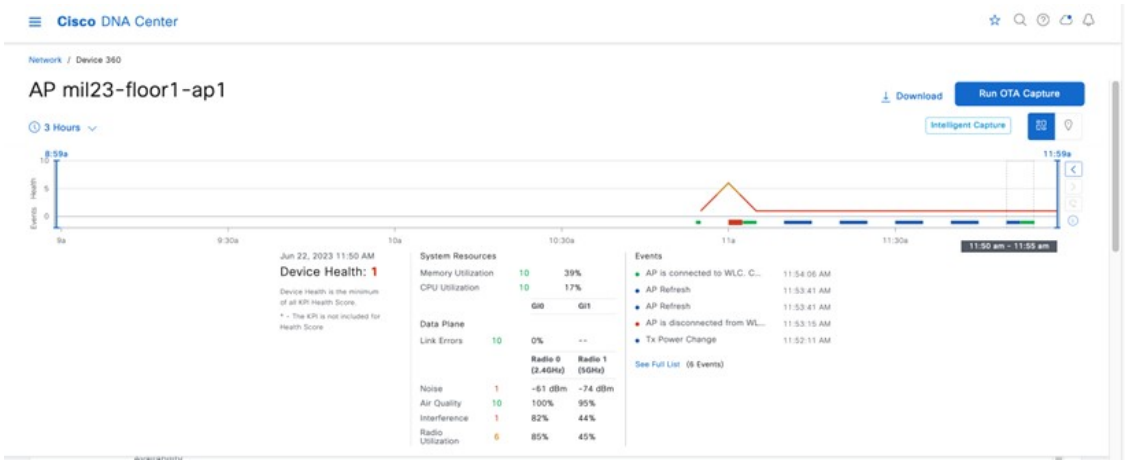
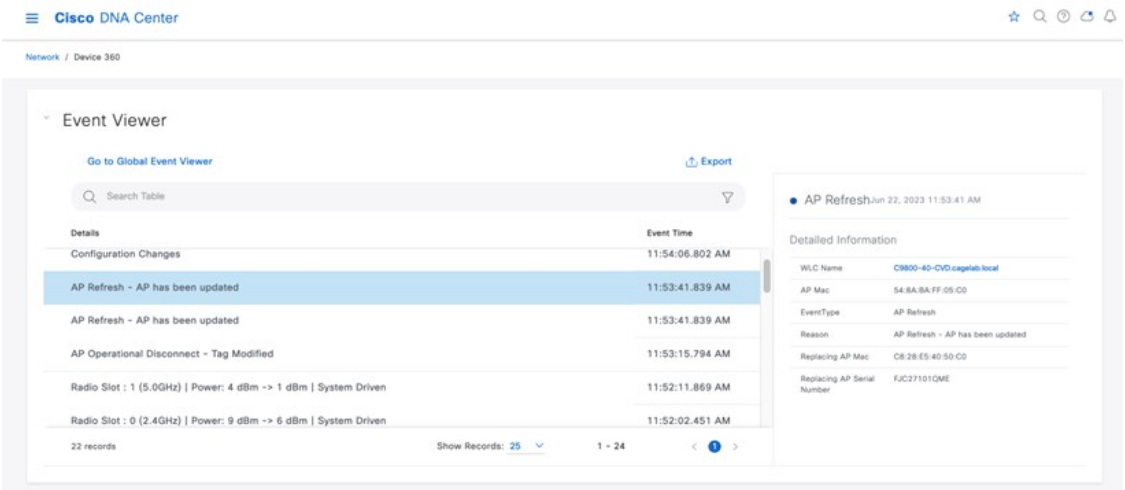


図 *242 :* イベント ビューア



クラウドベースの AI 拡張機能

Cisco DNA Center には、機械学習（ML）と機械推論（MR）の機能を活用して、ネットワーク展開に固有の正確なインサイトを提供する AI ベースの拡張機能があります。AI ベースの機能には、Radio Resource Management（RRM; 無線リソース管理）と、ネットワークのインサイトとベースラインからの逸脱を提供する広範な AI ベースの分析が含まれます。

Cisco AI RRM

AI 拡張 RRM は、人工知能（AI）と ML の機能を、クラウド内の信頼性の高い Cisco RRM 製品ファミリアルゴリズムに統合します。AI 拡張 RRM は、Cisco DNA Center（オンプレミスアプライアンス）を介してサービスとして調整されます。既存の Cisco Catalyst 9800 RRM サイトは、インテリジェントな一元化されたサービスにシームレスに移行できます。AI 拡張 RRM は、他の Cisco DNA Center サービスとして多数の新機能を提供します。詳細はこちらで確認してください。

Cisco AI Analytics

Cisco AI Analytics は、ネットワーク管理者がネットワークの問題をトラブルシューティングし、長期的なキャパシティプランニングを実施するのに役立つインサイトとチャートを提供します。詳細はこちらで確認してください。

メッシュネットワーク

Cisco 屋外 AP は、バックホール用の有線ネットワーク、または 5 GHz や 2.4 GHz 無線をバックホールとして使用するメッシュネットワークで運用できます。シスコ ワイヤレス メッシュ ネットワークでは、複数のメッシュ AP によって、安全でスケーラブルなワイヤレス LAN を提供するネットワークが構成されます。メッシュネットワーク内の AP は、ルートアクセスポイント（RAP）またはメッシュアクセスポイント（MAP）を介して動作します。RAP は、それぞれの場所で有線ネットワークに接続します。すべてのダウンストリーム AP は、MAP として動作し、ワイヤレスリンク

を使用して通信します。すべての AP はメッシュ AP として設定され、出荷されています。AP を RAP として使用するには、MAP を RAP として再設定する必要があります。すべてのメッシュネットワークに、少なくとも 1 つの RAP が含まれている必要があります。

Cisco DNA Center を使用してメッシュネットワークを設定する方法の詳細については、こちらを参照してください。Cisco DNA Center 2.3.6 以降、[Wireless Settings] ウィンドウでは、さまざまなタイルの下にワークフローが整理されています。[Security Settings] で AP 認証リストを作成し、[AP Authorization List] をクリックします。[AP Profiles] タイルでメッシュ AP プロファイルを作成し、[Add] をクリックします。IOS XE の AP プロファイルになるワイヤレスコントローラ タイプを選択します。[Profile] ウィンドウで、[Mesh] をクリックしてメッシュパラメータを設定します。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアでテストされています。

機能エリア	製品	ソフトウェアバージョン
エンタープライズ 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	17.09.04a
ゲスト ワイヤレスコントローラ	Cisco Catalyst 9800-CL クラウドコントローラ	17.09.04a
エンタープライズ SDN コントローラ	Cisco DNA Center	2.3.5.5
AAA Server	Cisco Identity Services Engine	3.2

事前設定済みの各 RF プロファイルの設定

次の表に、Cisco DNA Center のデフォルトの各ワイヤレス RF プロファイル（低、標準、高）の設定を示します。

デフォルトの RF プロファイル設定は変更できません。設定を変更するには、カスタムプロファイルを作成し、デフォルトの RF プロファイルとして割り当てる必要があります。

表 *33* : 低ワイヤレス *RF* プロファイルの設定

機能	タイプ	説明
プロファイル名	テキストフィールド	LOW
[PROFILE TYPE] > [2.4 GHz]	[On/Off] トグルボタン	RF プロファイルの 2.4 GHz 帯域を有効または無効にします。[On] に設定します。

機能	タイプ	説明
[PROFILE TYPE] > [2.4 GHz] > [Parent Profile]	オプション ボタン	これは、この RF プロファイルの派生元である親プロファイルです。カスタム RF プロファイルは事前設定済み RF プロファイルに基づいて作成できるため、このフィールドはカスタム RF プロファイルの作成時にのみ適用されます。低 RF プロファイルの場合は [Low] に設定されます。 使用可能なオプション： • [High]：高密度クライアント RF プロファイル。 • [Medium (Typical)]：中密度クライアント RF プロファイル。 • [Low]：低密度クライアント RF プロファイル。 • [Custom]：カスタム RF プロファイル。
[PROFILE TYPE] > [2.4 GHz] > [DCA Channel]	[Multiple Choice] オプションボタン	2.4 GHz 帯域内で動的チャネル割り当て（DCA）が自動モードで動作するチャネルを選択します。チャネル 1 ～ 14 を選択できます。デフォルト設定は、チャネル 1、6、および 11 です。 このフィールドは、事前設定済みプロファイル（LOW、TYPICAL、HIGH）のいずれかを編集する場合は 2.4 GHz 帯域では表示されず、2.4 GHz 帯域で新しい RF プロファイルを作成する場合にのみ表示されます。通常、2.4 GHz 帯域では 1、6、および 11 以外のチャネルの実装は推奨されません。
[PROFILE TYPE] > [2.4 GHz] > [Supported Data Rates]	複数の位置がある単一方向のスライダ	2.4 GHz 帯域でサポートされるデータレートの範囲を示す複数の位置があるスライダ。レートは、低いものから順に、1、2、5.5、6、9、11、12、18、24、36、48、および 54 Mbps です。 低 RF プロファイルの場合、すべてのデータレートに設定され、デバイスの互換性が最大限に向上します。 低 RF プロファイルは、低密度クライアントのワイヤレス環境向けに設計されています。そのような環境では、ワイヤレスクライアントから AP への接続距離が長くなり、データレートが低くなる可能性があります。
[PROFILE TYPE] > [2.4 GHz] > [Supported Data Rates] > [Enable 802.11b Data Rates]	Check box	このチェックボックスは、前述のスライダと連動します。このチェックボックスをオンにすると、スライダで 802.11b データレート 1、2、5.5、6、9、および 11 Mbps が有効になります。 低RFプロファイルの場合、このチェックボックスはオンになります。

機能	タイプ	説明
[PROFILE TYPE] > [2.4 GHz] > [Mandatory Data Rates]	[Multiple Choice] オプションボタン	このオプションボタンは、2.4 GHz 帯域のワイヤレスネットワークとの関連付けを可能にするために、ワイヤレスクライアントがサポートする必要があるデータレートを選択するために使用されます。選択肢は 1、2、5.5、6、9、11、12、18、24、36、48、および 54 Mbps です。 低 RF プロファイルの場合、必須のデータレートは 1、2、5.5、および 11 Mbps です。
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [Power Level]	複数の設定がある複数方向のスライダ	このスライダで、この RF プロファイルに関連付けられた AP の 2.4 GHz 無線において伝送パワーコントロール（TPC）で設定できる最小および最大電力レベルを決めます。スライダの全範囲は -10 ～ 30 dBm で、増分単位は 1 dBm です。TPC により、隣接する AP からの RSSI に基づいて各無線の送信電力が自動的に調整されます。 低 RF プロファイルの場合、全範囲の電力レベル（-10 ～ 30 dBm）を TPC で使用できるようにスライダが設定されます。 低密度クライアントの環境では、AP の間隔が広くなる可能性があるため、完全なカバレッジを得るには、より高い電力レベルで送信する必要があります。この設定により、TPC は全範囲の電力レベルで 2.4 GHz 無線を調整できます。
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [RX SOP]	ドロップダウンメニュー	RX-SOP（Receiver Start of Packet Detection Threshold）は、2.4 GHz 無線でワイヤレスパケットを復調および復号する RF 信号レベルを決定します。 RX-SOP レベルが低いほど、ワイヤレスクライアントに対する 2.4 GHz 無線の感度が高くなります。受信信号強度表示（RSSI）値が低いワイヤレス クライアント トラフィックは、AP によって復号されます。RSSI が低下するのは、多くの場合、ワイヤレスクライアントが AP から離れているためなので、結果として AP のセルサイズ（カバレッジ）が増えます。これは、AP がより離れた場所にある可能性がある、低密度クライアントの環境に役立ちます。 低 RF プロファイルの場合は [Low]（-80 dBm）に設定されます。
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [TPC Power Threshold]	複数の設定がある複数方向のスライダ	[TPC Power Threshold] は AP のセル境界における目的の電力レベルの制御に使用されるため、システムのカバレッジ動作の制御にも使用されます。 [TPC Power Threshold] の範囲は -80 ～ -50 dBm です。低密度クライアントのワイヤレス展開では、通常、AP の数が少なくなります。[TPC Power Threshold] の値を大きくすると、個々の AP における無線の送信電力レベルが高くなり、各 AP の全体的なカバレッジが増加します。 低 RF プロファイルの場合、2.4 GHz 無線は -65 dBm に設定されます。

機能	タイプ	説明
[PROFILE TYPE] > [5 GHz]	[On/Off] トグルボタン	RF プロファイルの 5 GHz 帯域を有効または無効にします。[On] に設定します。
[PROFILE TYPE] > [5 GHz] > [Parent Profile]	オプション ボタン	これは、この RF プロファイルの派生元である親プロファイルです。カスタム RF プロファイルは事前設定済み RF プロファイルに基づいて作成できるため、このフィールドはカスタム RF プロファイルの作成時にのみ適用されます。低 RF プロファイルの場合は [Low] に設定されます。 使用可能なオプション： • [High]：高密度クライアント RF プロファイル。 • [Medium (Typical)]：中密度クライアント RF プロファイル。 • [Low]：低密度クライアント RF プロファイル。 • [Custom]：カスタム RF プロファイル。
[PROFILE TYPE] > [5 GHz] > [Channel Width]	ドロップダウンメニュー	5 GHz 帯域のチャネル幅を選択します。[20]、[40]、[80]、および [160] MHz または [Best] を選択できます。[Best] を選択すると、DCA により環境に最適なチャネル幅が選択されます。 低 RF プロファイルの場合、チャネル幅は 20 MHz に設定されます。
[PROFILE TYPE] > [5 GHz] > [DCA Channel]	[Multiple Choice] オプションボタン	5 GHz 帯域内で DCA が自動モードで動作するチャネルを選択します。 選択肢は規制ドメインによって異なります（UNII-1 チャネル 36 ～ 48、UNII-2 チャネル 52 ～ 144、UNII-3 チャネル 149 ～ 165）。 このフィールドは、事前設定済みプロファイル（LOW、TYPICAL、HIGH）のいずれかを編集する場合は 5 GHz 帯域では表示されず、5 GHz 帯域で新しい RF プロファイルを作成する場合にのみ表示されます。
[PROFILE TYPE] > [5 GHz] > [Supported Data Rates]	複数の位置がある単一方向のスライダ	5 GHz 帯域でサポートされるデータレートの範囲を示す複数の位置があるスライダ。レートは、低いものから順に、6、9、12、18、24、36、48、および 54 Mbps です。 低 RF プロファイルの場合はすべてのデータレートに設定されます。 低 RF プロファイルは、低密度クライアントのワイヤレス環境向けに設計されています。そのような環境では、ワイヤレスクライアントから AP への接続距離が長くなり、データレートが低くなる可能性があります。

機能	タイプ	説明
[PROFILE TYPE] > [5 GHz] > [Mandatory Data Rates]	[Multiple Choice] オプションボタン	このオプションボタンは、5 GHz 帯域のワイヤレスネットワークとの関連付けを可能にするために、ワイヤレスクライアントがサポートする必要があるデータレートを選択するために使用されます。選択肢は 6、9、11、12、18、24、36、48、および 54 Mbps です。 低 RF プロファイルの場合、必須のデータレートは 6、12、および 24 Mbps です。
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [Power Level]	複数の設定がある複数方向のスライダ	このスライダで、この RF プロファイルに関連付けられた AP の 5 GHz 無線で TPC が設定できる最小および最大電力レベルを決めます。スライダの全範囲は -10 ～ 30 dBm で、増分単位は 1 dBm です。TPC により、隣接する AP からの RSSI に基づいて各無線の送信電力が自動的に調整されます。 低 RF プロファイルの場合、全範囲の電力レベル（-10 ～ 30 dBm）を TPC で使用できるようにスライダが設定されます。 低密度クライアントの環境では、AP の間隔が広くなる可能性があるため、完全なカバレッジを得るには、より高い電力レベルで送信する必要があります。この設定により、TPC は全範囲の電力レベルで 5 GHz 無線を調整できます。
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [RX SOP]	ドロップダウンメニュー	RX-SOP は、5 GHz 無線がワイヤレスパケットを復調および復号する RF 信号レベルを決定します。 RX-SOP レベルが低いほど、ワイヤレスクライアントに対する 5 GHz 無線の感度が高くなります。RSSI 値が低いワイヤレス クライアント トラフィックは、AP によって復号されます。RSSI が低下するのは、多くの場合、ワイヤレスクライアントが AP から離れているためなので、結果として AP のセルサイズ（カバレッジ）が増えます。これは、AP がより離れた場所にある可能性がある、低密度クライアントの環境に役立ちます。 低 RF プロファイルの場合は [Low]（-80 dBm）に設定されます。
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [TPC Power Threshold]	複数の設定がある複数方向のスライダ	[TPC Power Threshold] は AP のセル境界における目的の電力レベルの制御に使用されるため、システムのカバレッジ動作の制御にも使用されます。 [TPC Power Threshold] の範囲は -80 ～ -50 dBm です。低密度クライアントのワイヤレス展開では、通常、AP の数が少なくなります。[TPC Power Threshold] の値を大きくすると、個々の AP における無線の送信電力レベルが高くなり、各 AP の全体的なカバレッジが増加します。 低 RF プロファイルの場合、5 GHz 無線は -60 dBm に設定されます。

表 *34* : 一般的なワイヤレス *RF* プロファイルの設定

機能	タイプ	説明
プロファイル名	テキストフィールド	TYPICAL
[PROFILE TYPE] > [2.4 GHz]	[On/Off] トグルボタン	RF プロファイルの 2.4 GHz 帯域を有効または無効にします。[On] に設定します。
[PROFILE TYPE] > [2.4 GHz] > [Parent Profile]	オプション ボタン	これは、この RF プロファイルの派生元である親プロファイルです。カスタム RF プロファイルは事前設定済み RF プロファイルに基づいて作成できるため、このフィールドはカスタム RF プロファイルの作成時にのみ適用されます。TYPICAL RF プロファイルの場合は [Medium (Typical)] に設定されます。 使用可能なオプション： • [High]：高密度クライアント RF プロファイル。 • [Medium (Typical)]：中密度クライアント RF プロファイル。 • [Low]：低密度クライアント RF プロファイル。 • [Custom]：カスタム RF プロファイル。
[PROFILE TYPE] > [2.4 GHz] > [DCA Channel]	[Multiple Choice] オプションボタン	2.4 GHz 帯域内で DCA が自動モードで動作するチャネルを選択します。チャネル 1 ～ 14 を選択できます。デフォルト設定は、チャネル 1、6、および 11 です。 このフィールドは、事前設定済みプロファイル（LOW、TYPICAL、HIGH）のいずれかを編集する場合は 2.4 GHz 帯域では表示されず、2.4 GHz 帯域で新しい RF プロファイルを作成する場合にのみ表示されます。通常、2.4 GHz 帯域では 1、6、および 11 以外のチャネルの実装は推奨されません。
[PROFILE TYPE] > [2.4 GHz] > [Supported Data Rates]	複数の位置がある単一方向のスライダ	2.4 GHz 帯域でサポートされるデータレートの範囲を示す複数の位置があるスライダ。レートは、低いものから順に、1、2、5.5、6、9、11、12、18、24、36、48、および 54 Mbps です。 TYPICAL RF プロファイルの場合は 9 Mbps 以上のレートに設定されます。 TYPICAL RF プロファイルは、中密度クライアントのワイヤレス環境向けに設計されています。そのような環境では、ワイヤレスクライアントが AP に低速で接続すると、ワイヤレスネットワークの全体的なスループットが低下します。クライアントがより高いレートで接続および送信できるように、十分な AP 密度を展開する必要があります。

機能	タイプ	説明
[PROFILE TYPE] > [2.4 GHz] > [Supported Data Rates] > [Enable 802.11b Data Rates]	Check box	このチェックボックスは、前述のスライダと連動します。このチェックボックスをオンにすると、スライダで 802.11b データレート 1、2、5.5、6、9、および 11 Mbps が有効になります。 TYPICAL RF 展開の場合、このチェックボックスはオフになっています。
[PROFILE TYPE] > [2.4 GHz] > [Mandatory Data Rates]	[Multiple Choice] オプションボタン	このオプションボタンは、2.4 GHz 帯域のワイヤレスネットワークとの関連付けを可能にするために、ワイヤレスクライアントがサポートする必要があるデータレートを選択するために使用されます。選択肢は 1、2、5.5、6、9、11、12、18、24、36、48、および 54 Mbps です。 TYPICAL RF プロファイルの場合、必須のデータレートは 12 Mbps のみです。
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [Power Level]	複数の設定がある複数方向のスライダ	このスライダで、この RF プロファイルに関連付けられた AP の 2.4 GHz 無線で TPC が設定できる最小および最大電力レベルを決めます。スライダの全範囲は -10 ～ 30 dBm で、増分単位は 1 dBm です。TPC により、隣接する AP からの RSSI に基づいて各無線の送信電力が自動的に調整されます。 TYPICAL RF プロファイルの場合、全範囲の電力レベル（-10 ～ 30 dBm）を TPC で使用できるようにスライダが設定されます。 中密度クライアントの環境では、AP の間隔が広くなる可能性があるため、完全なカバレッジを得るには、より高い電力レベルで送信する必要があります。この設定により、TPC は全範囲の電力レベルで 2.4 GHz 無線を調整できます。
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [RX SOP]	ドロップダウンメニュー	RX-SOP は、2.4 GHz 無線がワイヤレスパケットを復調および復号する RF 信号レベルを決定します。 RX-SOP レベルが低いほど、ワイヤレスクライアントに対する 2.4 GHz 無線の感度が高くなります。RSSI 値が低いワイヤレス クライアント トラフィックは、AP によって復号されます。RSSI が低下するのは、多くの場合、ワイヤレスクライアントが AP から離れているためなので、結果として AP のセルサイズ（カバレッジ）が増えます。これは、AP がより離れた場所にある可能性がある、低密度クライアントの環境に役立ちます。 TYPICAL RF プロファイルの場合は [Auto] に設定されます。

機能	タイプ	説明
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [TPC Power Threshold]	複数の設定がある複数方向のスライダ	[TPC Power Threshold] は AP のセル境界における目的の電力レベルの制御に使用されるため、システムのカバレッジ動作の制御にも使用されます。 [TPC Power Threshold] の範囲は -80 ～ -50 dBm です。中密度クライアントのワイヤレス展開では、通常、AP の数が多くなります。[TPC Power Threshold] の値を小さくすると、個々の AP における無線の送信電力レベルが低下し、各 AP の全体的なカバレッジが減少しますが、同一チャネル干渉（CCI）も最小限に抑えられます。 TYPICAL RF プロファイルの場合、2.4 GHz 無線は -70 dBm に設定されます。
[PROFILE TYPE] > [5 GHz]	[On/Off] トグルボタン	RF プロファイルの 5 GHz 帯域を有効または無効にします。[On] に設定します。
[PROFILE TYPE] > [5 GHz] > [Parent Profile]	オプション ボタン	これは、この RF プロファイルの派生元である親プロファイルです。カスタム RF プロファイルは事前設定済み RF プロファイルに基づいて作成できるため、このフィールドはカスタム RF プロファイルの作成時にのみ適用されます。TYPICAL RF プロファイルの場合は [Medium (Typical)] に設定されます。 使用可能なオプション： • [High]：高密度クライアント RF プロファイル。 • [Medium (Typical)]：中密度クライアント RF プロファイル。 • [Low]：低密度クライアント RF プロファイル。 • [Custom]：カスタム RF プロファイル。
[PROFILE TYPE] > [5 GHz] > [Channel Width]	ドロップダウンメニュー	5 GHz 帯域のチャネル幅を選択します。[20]、[40]、[80]、および [160] MHz または [Best] を選択できます。[Best] を選択すると、DCA により環境に最適なチャネル幅が選択されます。 TYPICAL RF プロファイルの場合、チャネル幅は 20 MHz に設定されます。
[PROFILE TYPE] > [5 GHz] > [DCA Channel]	[Multiple Choice] オプションボタン	5 GHz 帯域内で DCA が自動モードで動作するチャネルを選択します。 選択肢は規制ドメインによって異なります（UNII-1 チャネル 36 ～ 48、UNII-2 チャネル 52 ～ 144、UNII-3 チャネル 149 ～ 165）。 このフィールドは、事前設定済みプロファイル（LOW、TYPICAL、HIGH）のいずれかを編集する場合は 5 GHz 帯域では表示されず、5 GHz 帯域で新しい RF プロファイルを作成する場合にのみ表示されます。

機能	タイプ	説明
[PROFILE TYPE] > [5 GHz] > [Supported Data Rates]	複数の位置がある単一方向のスライダ	5 GHz 帯域でサポートされるデータレートの範囲を示す複数の位置があるスライダ。レートは、低いものから順に、6、9、12、18、24、36、48、および 54 Mbps です。 TYPICAL RF プロファイルの場合はすべてのデータレートに設定されます。
[PROFILE TYPE] > [5 GHz] > [Mandatory Data Rates]	[Multiple Choice] オプションボタン	このオプションボタンは、5 GHz 帯域のワイヤレスネットワークとの関連付けを可能にするために、ワイヤレスクライアントがサポートする必要があるデータレートを選択するために使用されます。選択肢は 6、9、11、12、18、24、36、48、および 54 Mbps です。 TYPICAL RF プロファイルの場合、必須のデータレートは 6、12、および 24 Mbps です。
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [Power Level]	複数の設定がある複数方向のスライダ	このスライダで、この RF プロファイルに関連付けられた AP の 5 GHz 無線で TPC が設定できる最小および最大電力レベルを決めます。スライダの全範囲は -10 ～ 30 dBm で、増分単位は 1 dBm です。TPC により、隣接する AP からの RSSI に基づいて各無線の送信電力が自動的に調整されます。 TYPICAL RF プロファイルの場合、全範囲の電力レベル（-10 ～ 30 dBm）を TPC で使用できるようにスライダが設定されます。 中密度クライアントの環境では、AP の間隔が広くなる可能性があるため、完全なカバレッジを得るには、より高い電力レベルで送信する必要があります。この設定により、TPC は全範囲の電力レベルで 5 GHz 無線を調整できます。
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [RX SOP]	ドロップダウンメニュー	RX-SOP は、5 GHz 無線がワイヤレスパケットを復調および復号する RF 信号レベルを決定します。 RX-SOP レベルが低いほど、ワイヤレスクライアントに対する 5 GHz 無線の感度が高くなります。RSSI 値が低いワイヤレス クライアント トラフィックは、AP によって復号されます。RSSI が低下するのは、多くの場合、ワイヤレスクライアントが AP から離れているためなので、結果として AP のセルサイズ（カバレッジ）が増えます。これは、AP がより離れた場所にある可能性がある、低密度クライアントの環境に役立ちます。 TYPICAL RF プロファイルの場合は [Auto] に設定されます。

機能	タイプ	説明
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [TPC Power Threshold]	複数の設定がある複数方向のスライダ	[TPC Power Threshold] は AP のセル境界における目的の電力レベルの制御に使用されるため、システムのカバレッジ動作の制御にも使用されます。 [TPC Power Threshold] の範囲は -80 ～ -50 dBm です。中密度クライアントのワイヤレス展開では、通常、AP の数が多くなります。[TPC Power Threshold] の値を小さくすると、個々の AP における無線の送信電力レベルが低下し、各 AP の全体的なカバレッジが減少しますが、CCI も最小限に抑えられます。 TYPICAL RF プロファイルの場合、5 GHz 無線は -70 dBm に設定されます。

表 *35* : 高ワイヤレス *RF* プロファイルの設定

機能	タイプ	説明
プロファイル名	テキストフィールド	HIGH
[PROFILE TYPE] > [2.4 GHz]	[On/Off] トグルボタン	RF プロファイルの 2.4 GHz 帯域を有効または無効にします。[On] に設定します。
[PROFILE TYPE] > [2.4 GHz] > [Parent Profile]	オプション ボタン	これは、この RF プロファイルの派生元である親プロファイルです。カスタム RF プロファイルは事前設定済み RF プロファイルに基づいて作成できるため、このフィールドはカスタム RF プロファイルの作成時にのみ適用されます。高 RF プロファイルの場合は [High] に設定されます。 使用可能なオプション： • [High]：高密度クライアント RF プロファイル。 • [Medium (Typical)]：中密度クライアント RF プロファイル。 • [Low]：低密度クライアント RF プロファイル。 • [Custom]：カスタム RF プロファイル。
[PROFILE TYPE] > [2.4 GHz] > [DCA Channel]	[Multiple Choice] オプションボタン	2.4 GHz 帯域内で DCA が自動モードで動作するチャネルを選択します。チャネル 1 ～ 14 を選択できます。デフォルト設定は、チャネル 1、6、および 11 です。 このフィールドは、事前設定済みプロファイル（LOW、TYPICAL、HIGH）のいずれかを編集する場合は 2.4 GHz 帯域では表示されず、2.4 GHz 帯域で新しい RF プロファイルを作成する場合にのみ表示されます。通常、2.4 GHz 帯域では 1、6、および 11 以外のチャネルの実装は推奨されません。

機能	タイプ	説明
[PROFILE TYPE] > [2.4 GHz] > [Supported Data Rates]	複数の位置がある単一方向のスライダ	2.4 GHz 帯域でサポートされるデータレートの範囲を示す複数の位置があるスライダ。レートは、低いものから順に、1、2、5.5、6、9、11、12、18、24、36、48、および 54 Mbps です。 高 RF プロファイルの場合は 9 Mbps 以上のレートに設定されます。 高 RF プロファイルは、高密度クライアントのワイヤレス環境向けに設計されています。そのような環境では、ワイヤレスクライアントが AP に低速で接続すると、ワイヤレスネットワークの全体的なスループットが低下します。クライアントがより高いレートで接続および送信できるように、十分な AP 密度を展開する必要があります。
[PROFILE TYPE] > [2.4 GHz] > [Supported Data Rates] > [Enable 802.11b Data Rates]	Check box	このチェックボックスは、前のスライダと連動します。このチェックボックスをオンにすると、スライダで 802.11b データレート 1、2、5.5、6、9、および 11 Mbps が有効になります。 高 RF 展開の場合、このチェックボックスはオフになっています。
[PROFILE TYPE] > [2.4 GHz] > [Mandatory Data Rates]	[Multiple Choice] オプションボタン	このオプションボタンは、2.4 GHz 帯域のワイヤレスネットワークとの関連付けを可能にするために、ワイヤレスクライアントがサポートする必要があるデータレートを選択するために使用されます。選択肢は 1、2、5.5、6、9、11、12、18、24、36、48、および 54 Mbps です。 高 RF プロファイルの場合、必須のデータレートは 12 Mbps のみです。
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [Power Level]	複数の設定がある複数方向のスライダ	このスライダで、この RF プロファイルに関連付けられた AP の 2.4 GHz 無線で TPC が設定できる最小および最大電力レベルを決めます。スライダの全範囲は -10 ～ 30 dBm で、増分単位は 1 dBm です。TPC により、隣接する AP からの RSSI に基づいて各無線の送信電力が自動的に調整されます。 高 RF プロファイルの場合、全範囲の電力レベル（7 ～ 30 dBm）を TPC で使用できるようにスライダが設定されます。 講堂のような高密度クライアント環境では、部屋がいっぱいになると、室内の人数によってフロアに到達する RF エネルギーの量が大幅に減衰する可能性があります。TPC を使用すると、追加の減衰を考慮して、室内の AP の送信電力が段階的に増えますが、時間の経過とともに電力も徐々に増えます。TPC の最小電力レベルを高く設定すると、最初（レクチャーの開始時）に十分な RF エネルギーがフロアに到達するようになります。

機能	タイプ	説明
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [RX SOP]	ドロップダウン メニュー	RX-SOP は、2.4 GHz 無線がワイヤレスパケットを復調および復号する RF 信号レベルを決定します。 RX-SOP レベルが高くなると、ワイヤレスクライアントに対する 2.4 GHz 無線の感度が低下します。RSSI 値が低いワイヤレス クライアント トラフィックは、AP によって復号されません。RSSI が低下するのは、多くの場合、ワイヤレスクライアントが AP から離れているためなので、結果として AP のセルサイズ（カバレッジ）が減ります。これは、AP がより高密度に展開される可能性がある、クライアント密度の高い環境に役立ちます。 高 RF プロファイルの場合は [Medium] に設定されます。
[PROFILE TYPE] > [2.4 GHz] > [TX Power Configuration] > [TPC Power Threshold]	複数の設定がある複数方向のスライダ	[TPC Power Threshold] は AP のセル境界における目的の電力レベルの制御に使用されるため、システムのカバレッジ動作の制御にも使用されます。 [TPC Power Threshold] の範囲は -80 ～ -50 dBm です。高密度クライアントのワイヤレス展開では、通常、AP の数が多くなります。[TPC Power Threshold] の値を小さくすると、個々の AP における無線の送信電力レベルが低下し、各 AP の全体的なカバレッジが減少しますが、CCI も最小限に抑えられます。 高 RF プロファイルの場合、2.4 GHz 無線は -70 dBm に設定されます。
[PROFILE TYPE] > [5 GHz]	[On/Off] トグル ボタン	RF プロファイルの 5 GHz 帯域を有効または無効にします。[On] に設定します。
[PROFILE TYPE] > [5 GHz] > [Parent Profile]	オプション ボタン	これは、この RF プロファイルの派生元である親プロファイルです。カスタム RF プロファイルは事前設定済み RF プロファイルに基づいて作成できるため、このフィールドはカスタム RF プロファイルの作成時にのみ適用されます。高 RF プロファイルの場合は [High] に設定されます。 使用可能なオプション： • [High]：高密度クライアント RF プロファイル。 • [Medium (Typical)]：中密度クライアント RF プロファイル。 • [Low]：低密度クライアント RF プロファイル。 • [Custom]：カスタム RF プロファイル。
[PROFILE TYPE] > [5 GHz] > [Channel Width]	ドロップダウン メニュー	5 GHz 帯域のチャネル幅を選択します。[20]、[40]、[80]、および [160] MHz または [Best] を選択できます。[Best] を選択すると、DCA により環境に最適なチャネル幅が選択されます。 高 RF プロファイルの場合、チャネル幅は 20 MHz に設定されます。

機能	タイプ	説明
[PROFILE TYPE] > [5 GHz] > [DCA Channel]	[Multiple Choice] オプションボタン	5 GHz 帯域内で DCA が自動モードで動作するチャネルを選択します。 選択肢は規制ドメインによって異なります（UNII-1 チャネル 36 ～ 48、UNII-2 チャネル 52 ～ 144、UNII-3 チャネル 149 ～ 165）。 このフィールドは、事前設定済みプロファイル（LOW、TYPICAL、HIGH）のいずれかを編集する場合は 5 GHz 帯域では表示されず、5 GHz 帯域で新しい RF プロファイルを作成する場合にのみ表示されます。
[PROFILE TYPE] > [5 GHz] > [Supported Data Rates]	複数の位置がある単一方向のスライダ	5 GHz 帯域でサポートされるデータレートの範囲を示す複数の位置があるスライダ。レートは、低いものから順に、6、9、12、18、24、36、48、および 54 Mbps です。 高 RF プロファイルの場合は 12 Mbps 以上のレートに設定されます。
[PROFILE TYPE] > [5 GHz] > [Mandatory Data Rates]	[Multiple Choice] オプションボタン	このオプションボタンは、5 GHz 帯域のワイヤレスネットワークとの関連付けを可能にするために、ワイヤレスクライアントがサポートする必要があるデータレートを選択するために使用されます。選択肢は 6、9、11、12、18、24、36、48、および 54 Mbps です。 高 RF プロファイルの場合、必須のデータレートは 12 および 24 Mbps です。
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [Power Level]	複数の設定がある複数方向のスライダ	このスライダで、この RF プロファイルに関連付けられた AP の 5 GHz 無線で TPC が設定できる最小および最大電力レベルを決めます。スライダの全範囲は -10 ～ 30 dBm で、増分単位は 1 dBm です。TPC により、隣接する AP からの RSSI に基づいて各無線の送信電力が自動的に調整されます。 高 RF プロファイルの場合、全範囲の電力レベル（7 ～ 30 dBm）を TPC で使用できるようにスライダが設定されます。 講堂のような高密度クライアント環境では、部屋がいっぱいになると、室内の人数によってフロアに到達する RF エネルギーの量が大幅に減衰する可能性があります。TPC を使用すると、追加の減衰を考慮して、室内の AP の送信電力が段階的に増えますが、時間の経過とともに電力も徐々に増えます。TPC の最小電力レベルを高く設定すると、最初（レクチャーの開始時）に十分な RF エネルギーがフロアに到達するようになります。

機能	タイプ	説明
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [RX SOP]	ドロップダウンメニュー	RX-SOP は、5 GHz 無線がワイヤレスパケットを復調および復号する RF 信号レベルを決定します。 RX-SOP レベルが高くなると、ワイヤレスクライアントに対する 5 GHz 無線の感度が低下します。RSSI 値が低いワイヤレス クライアント トラフィックは、AP によって復号されません。RSSI が低下するのは、多くの場合、ワイヤレスクライアントが AP から離れているためなので、結果として AP のセルサイズ（カバレッジ）が減ります。これは、AP がより高密度に展開される可能性がある、クライアント密度の高い環境に役立ちます。 高 RF プロファイルの場合は [Medium] に設定されます。
[PROFILE TYPE] > [5 GHz] > [TX Power Configuration] > [TPC Power Threshold]	複数の設定がある複数方向のスライダ	[TPC Power Threshold] は AP のセル境界における目的の電力レベルの制御に使用されるため、システムのカバレッジ動作の制御にも使用されます。 [TPC Power Threshold] の範囲は -80 ～ -50 dBm です。高密度クライアントのワイヤレス展開では、通常、AP の数が多くなります。[TPC Power Threshold] の値を小さくすると、個々の AP における無線の送信電力レベルが低下し、各 AP の全体的なカバレッジが減少しますが、CCI も最小限に抑えられます。 高 RF プロファイルの場合、5 GHz 無線は -65 dBm に設定されます。

用語集

AP

アクセス ポイント

Cisco ISE

Cisco Identity Services Engine

Cisco SDA

Cisco Software-Defined Access

CDP

Cisco Discovery Protocol

CWA

Central Web Authentication（中央 Web 認証）

DS

distribution system(分散システム、配布システム、配信システム)

FT

Fast Transition

HA

ハイ アベイラビリティ

IBN

インテントベース ネットワーク

L2

レイヤ 2

LWA

ローカル Web 認証

Microsoft AD

Microsoft Active Directory

PSK

事前共有キー

PSN

ポリシーサービスノード

RF

無線周波数

RSSI

受信信号強度表示

RX-SOP

Receiver Start of Packet Detection Threshold

SSID

サービスセット識別子

SSO

ステートフル スイッチオーバー

SVI

スイッチ仮想インターフェイス

SWIM

ソフトウェアイメージ管理

TPC

伝送パワー コントロール

VLAN

仮想ローカルエリアネットワーク

WLAN

ワイヤレス ローカル エリア ネットワーク

WNM

ワイヤレスネットワーク管理

WPA

Wi-Fi Protected Alliance

参照

- *Amazon Web Services* でのクラウド版 *Cisco Catalyst 9800* ワイヤレスコントローラのための導入ガイド
- *Cisco Aironet* アクティブセンサー導入ガイド [英語]
- *Cisco Catalyst 9800 Series Configuration Best Practices*

シスコのガイドに関するご意見やご提案がある場合は、シスココミュニティのディスカッションにご参加ください。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。