cisco.



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

Solution Overview 2 前提条件 3 ワイヤレスネットワークの定義 5 ワイヤレスネットワークの設計 12 ワイヤレスネットワークの展開 110 ワイヤレスネットワークの監視および操作 205 メッシュネットワーク 264 ハードウェアとソフトウェアの仕様 265 事前設定済みの各 RF プロファイルの設定 265 用語集 278 参照 280

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 $\ge \Im - \overrightarrow{x} \ \neg \cancel{z} \$

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
ー時エンドポイント (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。

- 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Floor2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	值
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	值
[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。

EQ. Search Settings	Settings / External Services			ISE server Integration \times
Clisco Accounts V Clisco com Credentialis PnP Connect SSM Connection Mode Smart Account Smart Licensing	Authentication and Use this form to specify the servers th Identity Services Engine (ISE) servers Settings have been updated.	Policy Servers at authenticate Cisco DNA Center users. Cisco can also supply policy and user information.		This is the first time Cisco DNA Center has seen this certificate from Gisco ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?
Device Settings	IP Address	Protocol	Type	less than a minute ago
Configuration Archive				This is the first time Class DNA Conter has seen this contificate from
Device Controllability	172.23.240.152	RADIUS_TACACS	ISE	Cisco ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?
Device EULA Acceptance	10.4.48.50	RADIUS	AAA	View certificate
Device Prompts				Accept Decline
Image Distribution Servers				
Network Resync Interval				 Establishing trust Reading, validating, and storing trusted certificates
PnP Device Authorization				
SNMP				Discovering nodes Discovering Cisco ISE primary and secondary admin nodes and pxGrid nodes
External Services				
Authentication and Policy Serv				Connecting to pxGrid Loading and validating pxGrid certificates, subscribing to pxGrid topics
CMX Servers/Cisco Spaces				
Cisco Al Analytics				
Cisco DNA - Cloud				
Cloud Access Login				
Cloud Authentication				
Destinations				
IP Address Manager				
Integrity Verification				
Machine Reasoning Engine				
Stealthwatch				
ThousandEyes Integration				Close
Webex Integration				

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。

Search Settings	Settings / External Services	Dolicy Servers		Edit ISE server	×
Cisco Accounts ~ Cisco.com Credentials PnP Connect	Use this form to specify the servers t Identity Services Engine (ISE) servers	hat authenticate Cisco DNA Center users. Cisco s can also supply policy and user information.		Sener IP Address 172.23.240.152	
SSM Connection Mode	⊕ Add ∨ Export				
Smart Account	IP Address	Protocol	Туре	Shared Secret	
Smart Licensing	172 22 240 152		ICC	Username* admin	
Device Settings 🗸 🗸	172.23.240.152	RADIUS_TAGAGS	ISE		
Configuration Archive	10.4.48.50	RADIUS	AAA	Depressed*	
Device Controllability				- 00399010	
Device EULA Acceptance				FQDN	
Device Prompts				cvdise31.cagelab.local	
ICMP Ping				Subscriber Name	
Image Distribution Servers				pxgrld_client_1683314602	
Network Resync Interval					
PnP Device Authorization				Virtual IP Address(es)	\sim
SNMP					Info
External Services					
Authentication and Policy Serv				Advanced Settings 🕕	
CMX Servers/Cisco Spaces				Connect to pxGrid 💿	
Cisco Al Analytics					
Cisco DNA - Cloud				Enable Multiple Cisco DNA Center operation	
Cloud Access Login				Use Cisco DNA Center Certificate for pxGrid	
Cloud Authentication				Protocol	
Destinations				RADIUS ZTACACS	
IP Address Manager				Enable KeyWrap	
Integrity Verification				Authentication Port 1812	
Machine Reasoning Engine					
Stealthwatch				Accountion Port	
or contractori					

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60m(200フィート)X約83m(274 フィート)X約3m(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60m(200フィート)X約83m(274 フィート)X約3m(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60m(200フィート)X約76m(250 フィート)X約3m(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60m(200フィート)X約76m(250 フィート)X約3m(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。

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。

Add Area	\times
Area contains other areas and/or buildings. Buildings contain floors and floor plans.	
Area Name*	
Daraat	
Global	\sim
Cancel Add	
Or	
Import Sites	

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。

contain flo	ors and floor plans.			
Building Name*				
Parent				
Milpitas Global/	US/ V			
Address (i)				
eg : 150 W Tasma	an Dr, San Jose			
Latitude*	Longitude*			
eg: 37.338 eg: -121.832				

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。

- 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	\times

Floor Name*	
Eg : Floor 1	
Site	
Global	\checkmark
Select Value	\checkmark
Type (RF Model)*	Floor Number*
Cubes And Walled Offices	1
	·
Floor Type*	Thickness (ft)*
Medium Floor (15dB/ft) 🛛 🗸	2
Medium Floor (15dB/ft) 🛛 🗸	2
Medium Floor (15dB/ft) ~	2
Medium Floor (15dB/ft) ∨	2
Medium Floor (15dB/ft) ~	2
Medium Floor (15dB/ft) ~	2
Medium Floor (15dB/ft) Floor Image Drag floor plan her or Upload file	2 re
Medium Floor (15dB/ft) Floor Image Drag floor plan her or Upload file	2
Medium Floor (15dB/ft) Floor Image Drag floor plan her or Upload file (Supported formats DXF, DWG , JPG,	2 re GIF, PNG, PDF)
Medium Floor (15dB/ft) Floor Image Drag floor plan her or Upload file (Supported formats DXF, DWG , JPG,	2 GIF, PNG, PDF)
Medium Floor (15dB/ft) Floor Image Drag floor plan her or Upload file (Supported formats DXF, DWG , JPG, Width (ft) * Length (ft) *	2 GIF, PNG, PDF) Height (ft) *

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

- 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。

- 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。

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。

Export Maps				
File to be saved to* DNAC_Map_Archive_172.23.240.221				
Export Format 💿 Ekahau Pro	ject (O Prime		
Do you still want to continue with data export?Click Export to proceed. The file will be automatically downloaded once export is complete.				
Can	cel	Export		

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。

 \times

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。

- **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	值
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

Network	Device Credentials	IP Address Pools SP Profil	es Wireless	Telemetry	Security and Trust		
Q Find Hie	erarchy V Search Help	Configure AAA, NTP, and Ir Servers" link. Once device these settings.	nage Distribution (S s are discovered, C	FTP) servers usin isco DNA Center	g the "Add will deploy using	đ	Add Servers
v 🕸 Global		i					
> 🕸 US		AAA Server 🛈					
		Network 🔽 Client/B	Endpoint				
		NETWORK					
		Servers	Protocol				
			⊖ RADIUS				
			O TACACS				
			Single Co	nnection i)			
		Network	IP Address (Prin	hary)			
		172.23.240.152	✓ 10.4.48.152 (Only device adm	inistration nodes)	+		
		Change Shared Secret					
		CLIENT/ENDPOINT					
		Servers	Protocol				
		O ISE 🔾 AAA	• RADIUS				
		Client/Endpoint	IP Address (Prin	nary)			
		172.23.240.152	× 10.4.48.152	~	+		
		Change Shared Secret					
						Reset	Save

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	值
DHCP	10.4.48.9

図 5: Cisco DNA Center の DHCP サーバーの設定

Network	Device Credentials	IP Address Pools SP Profiles	Wireless Telemetry Security and Trust	
Q Find Hier	rarchy ∇ Search Help	Configure AAA, NTP, and Image devices are discovered, Cisco I	ge Distribution (SFTP) servers using the *Add Servers" link. Once Add Servers o DNA Center will deploy using these settings.	
∨ 🕸 Global		CLIENT/ENDPOINT		
> 龅 US		Servers	Protocol	
		ISE 🔿 AAA	• RADIUS O TACACS	
		Client/Endpoint	IP Address (Primary)	
		172.23.240.152	✓ 10.4.48.152 +	
		Change Shared Secret		
		DHCP Server		
		DHCP		
		10.4.48.9	+	
			Reset Save	

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	值
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

Network Device Credentials	IP Address Pools SP Profiles Wireless Telemetry Security and Trust
Q Find Hierarchy V Search Help	Configure AAA, NTP, and Image Distribution (SFTP) servers using the *Add Servers* link. Once every devices are discovered, Cisco DNA Center will deploy using these settings.
∼ 🖓 Global	DNS Server ①
> 赩 US	Domain Name
	cagelab.local
	Primary +
	10.4.48.9 Supports both IPv4 and IPv6
	NTP Server
	S NTP
	10.4.48.17 +
	Supports both IPv4 and IPv6
	Reset Save

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	值
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

Network	Device Credentials	IP Address Pools SP Profiles Wireless Telemetry Security and Trust
⊇ Find Hier	rarchy \bigtriangledown Search Help	Configure AAA, NTP, and Image Distribution (SFTP) servers using the "Add Servers" link. Once et action of the Add Servers devices are discovered, Cisco DNA Center will deploy using these settings.
🖗 Global		NTP Server
> 🕸 US		S NTP
		10.4.48.17 + Supports both IPv4 and IPv6
		Time Zone ③ gwr
		Message of the day ()
		Reset

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	值
[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

Network Device Credentials II	Address Pools SP Profiles Wireless Telemetry Security and Trust
Q Find Hierarchy Search Help ✓ ₱ Global	Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned. Cisco DNA Center is your default SNMP collector. It polls network devices to gather telemetry data. View details on
> ൽ US	SNMP Traps Choose Cisco DNA Center to be your SNMP trap server, and/or add any external SNMP trap servers. These are the destination servers for SNMP traps and messages from network devices. Use Cisco DNA Center as SNMP trap server Add an external SNMP trap server
	 Syslogs Choose Cisco DNA Center to be your syslog server, and/or add any external syslog servers. Devices will be provisioned with syslog serverity level 6 (information messages) when they are assigned to a site and/or provisioned. Use Cisco DNA Center as syslog server Reset

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

Network Device Credentials	IP Address Pools SP Profiles Wireless Telemetry Security and Trust		
Q Find Hierarchy V	Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.		
〜 銫 Global	Cisco DNA Center is your default SNMP collector. It polls network devices to gather telemetry data. View details on the metrics gathered and the frequency with which they are collected.		
> 赩 US			
	 Syslogs Choose Cisco DNA Center to be your syslog server, and/or add any external syslog servers. Devices will be provisioned with syslog severity level 6 (information messages) when they are assigned to a site and/or provisioned. Use Cisco DNA Center as syslog server Add an external syslog server 		
	 NetFlow Choose the destination collector for Netflow records sent from network devices. To enable a network device sending Netflow, select the network device from the Provision/Inventory and choose *Action->Enable Application Telemetry* 		
	Reset		

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

E Clisco DNA Center	Design / Network Settings	0.000
Retwork Device Credentials I	P Address Pools SP Profiles Wreless Telemetry Security and Trust	
Find Herestry	SSID (0)	O Add
Search Hep	Q, Search have	V
De the first to add a new site from Network Henarchy	Em Deven 📾 5560 Scheduler 🕢 0 Serected	
	Network Name (ISSO) = WLAN Profile Name Policy Profile Name SSD Type L2 Security L3 Security Nitreless Profiles Postal Name	AAA Servers
	No data to display	
	Wireless Radio Frequency Profile	0 ***
	Basic M Profile Al IN Profile	
	RE Profile (3)	
	Q Seech tare	V
	Atters V Distance	
	Profile Name • Type 2.40Hz Data Rams 56Hz Data Rates 66Hz Data Rates Channel Web (3.45/5504) Profile Type
	HOH 2.4, 5, 6 8,12,18,24,36,48,54 12,18,24,36,48,54 8,8,12,18,24,36,48,54 20 MHz / Best / Best /	System
	LOW 2.4, 5, 6 1,2,5,5,6,5,11,12,16,24,36,48,54 6,5,12,16,24,36,48,54 8,5,12,16,24,36,48,54 20 MHz / Best / Best	System
	TYPECAL 2.4, 5, 6 8,12,18,24,38,48,54 8,912,18,24,38,48,54 8,9,12,18,24,38,48,54 20 MHz / Beat / Beat	System
	3 fecords Does Records: 10 🗸 1 = 3	
	Wireless Interfaces (1)	O A55
	Q. Search Tarre	7
	Fat Deare 0 Selected	
	Inseface Name + VLAN D	
	matagement NJA	

図 11 : [Wireless Interfaces] ウィンドウ

E Cisco DNA Center		Design / Network Settings	Q () () () () () () () () () () () () ()
Network Device Credentials	IP Address Pools SP Profiles Wireless	Telemetry Security and Trust	
Q. Find Herandry	Wireless Interfaces (6)		• AM
d' Clobal Be the first to add a new site from Natwork Herwichy	Adl Deem 0 Selected		
	Moerface Name + VLAN D		
	branchemployee 100		
	Clents 49		
	employee 160		
	guest-dm2 125		
	4 Aucorda	Show Record	× <u>10 v</u> 1+6 ⊂ 0 ⇒

- (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

Vetwork Device Credentials IF	Address Pools SP Profiles Wireless Telemetry Security and Trust	Construction lands
2, Find Hierarchy	Wireless Interfaces (6)	Create a Wireless Interface
Search Help	Q. Search Table	
ili Global		Interface Name*
Be the first to add a new site from Network Herarchy	Cdt Deline 0 Selected	Only 31 characters are allowed
	Interface Name - VLAN IO	VLAN ID range is 0-4094
	branchemployee 100	
	branchguest-dmz 110	
	Cilents 49	
	employee 160	
	guest-dmz 125	
	management N/A	
	6 Records	
	Antenna Radio Profile (0)	
	Q Search Table	
	Edit Delvie D Selected	
	Radio Profile Name Beam Steer Mode	
	No data to display	
	AP Authorization List (0)	
	Q. Search Table	
	Fill Colors 0 Salacted	
	and states a state and	

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

=	Cisco DNA Center	.∋w	ireless SSID		± Q © Δ Δ
	Basic Settings Fill the information like name, wireless options, st	tate and network to complete the basic setup of	SSID		
	Sensor	WLAN Profile Name*	Policy Profile Name		
	lab3employee	lab3employee_profile	lab3employee_profile	0	
	Wireless Option Multi band operation (2.4GHz, 5GHz, 6GHz)	Multi band operation with Band Select O 5GH	z only 🔿 2.4GHz only 🔿 6GHz Only		
	Prenary Traffic Type VolP (Platinum)				
	SSID STATE				
	Broadcast \$50				
<) Exit					Next

図 14:エンタープライズ SSIDのセキュリティ設定

■ Cisco DNA Center	Wireless SSID	\$ Q @ C	4
Security Settings			
Configure the security level and au	thentication, authorization, & accounting for SSID		
For 2.4GHz+ 5GHz only, et	nable WPA2 , WPA3 is optional. For 2.4GHz+ SGHz+6GHz to be operational on IOS devices version 17.7 and above, enable WPA3 and disable WPA2.	×	
SSID Name: lab3employee	(Enterprise)		
Level of Security			
O Enterprise O Personal (Open Secured Open		
WPA2 WPA3			
Most secure User Credentials are validated wit WPA3 feature is supported for Wi	n 802 1x Badius server to authenticate clients to the wireless natwork- reless Controller version 8.10 & above. For Catalyst 9800 Centrollers version 16.12 & above.		
Authentication, Authorization	on, and Accounting Configuration		
A Please associate one or m	ore AAA servers using Configure AAA link to ensure right configuration is pushed for the selected security setting.	×	
Configure AAA			
AAA Override	Fast Lane		
Mac Filtering	Deny RCM Clients 📀		
Enable Posture ()			
-) Duit		Back Next	

図 15:エンタープライズ SSIDの AAA サーバー

E Cisco DNA Ce	Nireless SSID	* < © < \$
Configure the se	curity level and authentication, authorization, & accounting for SSID	
For 2	Configure AAA Server for lab3employee	×
Lovel of S Cinterprin	Catalyst 9800 Controllers versions less than 17.9 support only upto 8 Accounting Method list configuration. Configuring more than that will result in X provisioning failure.	
Most secure User Creden WPA3 featur	Configure Authentication and Authorization Servers Server 10.4.48.152 v +	
Authentic AAA C	Copy same Servers for Accounting	
Mac File	5ever 10.4.48.152 V 0 +	
C table /	Cancel	Configure
€ Exe		Back

図 16:エンタープライズ SSID の詳細設定

Elsco DNA Center	Wireless SSID	* < @ & \$
Advanced Settings Configure the advanced fields to complete SSID setup.		
SSID Name: lab3employee (Enterprise)		
Fast Transition (802.11r)	MFP Client Protection ③	Protected Management Frame (802.11w)
Adaptive O Enable O Disable	Optional O Required O Disabled	Optional ORequired ODisabled
Over the DS		
11k		
Neighbor List		
in (secs)*	in (seci)*	
Session Timeout ()	Client Exclusion	
11v BSS Transition Support		
BSS Max Idle Service		
Client User Idle Timeout(Default: 300 secs)*		
Client User Idle Timeout	Unrected Multicast Service	
Radius Client Profiling		
-) twit		Back Next

図 17: エンタープライズ SSID の追加の詳細設定

Eisco DNA Center	Wireless SSID	\$ Q @ ∆ Q
Session Timeout O 1800	in (secs)*	
11v BSS Transition Support		
8SS Max Idle Service		
Client User Idle Timeout 200 Secol*	Directed Multicast Service	
Radius Client Profiling		
NAS-ID 💿		
NAS-ID Opt 1 - +		
Configure CCKM		
Configure Client Rate Limit 💿		
Client Rate Limit (in bits per second) Range is 8000.10000000000		
Coverage Hole Detection		
-) Dat		Back Next

(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

≡ Cisco	DNA Center	Wireless SSID	Q @ 🗗 🗘
As Selecto as	sociate SSID to F et a Profile on the left or Add f sociate the SSID to Profile.	Profile Profile and click 'Associate'	
	Add Profile Q Search Branch	0 profile(s) associated.	
€) Exit		Back	Next

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

■ Cisco DNA Center	Wireless SSID	Q @ 🛆 🗘
Associate SSID to I Select a Profile on the left or Add to associate the SSID to Profile.	Profile Profile and click 'Associate'	
SSID Name: lab3employee	e (Enterprise)	
Add Profile Q Search	Associate Profile Cancel Profile Name Image: Corporate WLAN Profile Name Image: Policy Profile Name Iab3employee_profile Image: Image: Policy Profile Name Image: Image: Image: Policy Profile Name Image: Image: Image: Policy Profile Name Image: Image	0
	Do you need Anchor for this SSID? Yes O No	
fox Exit		Back Next

- **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 \mathcal{O} 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。
		 [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。
		 [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 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 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。					
		• 仕息					
		 ・ ビタ ・ ディヤーブル 					
		[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認定です。 					
		• [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

E Cisco DNA Center	Design / Network Settings / Wireless						-	0000	
Q. Search Herarchy Search Heip v & Global v & US v & Milpitas	At / SSDs SSIDs Configure SSIDs for enterprise and Profiles.	d guest wireless networks. Y	bu can assign them to sites	i via Wireless Ne	twork				
 ✓ iiii Building 23 Ø Floor 1 Ø Floor 2 > iiii Building 24 > building 24 	SSID (5) Q Search Table								V
> el NewYork > el Sanjose	Network Name (SSID) +	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wreless Profiles	Portal Name	AAA Servers
	🔘 cagelabssid 🔻	cagelabssid_profile	cagelabssid_profile	Enterprise	wpa2_enter prise	open	CagelabProfile	N/A	Configure AAA
	🔘 lab3branch5 🍸	lab3branch5_profile	lab3branch5_profile	Enterprise	wpa2_enter prise	open	branch5	N/A	AAA Configured (1)
	🔘 lab3employee 💙	lab3employee_profile	lab3employee_profile	Enterprise	wpa2_enter prise	open	corporate	N/A	AAA Configured (1)
	🔘 lab3guest 🔻	lab3guest_profile	lab3guest_profile	Guest	open	web_auth	corporate	Lab3_Guest_ Portal	AAA Configured (1)
	🗍 lab3guest5 🔻	lab3guest5_profile	lab3guest5_profile	Guest	open	web_auth	branch5	N/A	AAA Configured

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

lasic Settings				
If the information like name, wireless optic	ns, state and network to complete the basic set	up of SSID		
A One (1) Warning Alert and One (1) I	nformation Alert on this page. Collapse to hide.			×
Cne (1) Warning Alert				
Updating the WLAN Profile Name is record	intended when making any site level overrides for the SSID. In	case the same WLAN Profile Name is already configured in the	WLC managing the selected sites, it will result in provisioning failure	
One (1) Information Alert				
Only L3 Security, AAA Configuration, NAS Please newlgate to Clobel level for Editing	I-ID, Mac Pittering, AP Impersonation, Radius Client Profiling, C other parameters.	CKM, MPSK, Protected Management Frame (802.11w), AAA D	vende and WLAN Profile Name can be overridden at Site level.	
Windows Network Network (SSID)	WAAN Profile Rame*	Policy Piolite Name		
lab3employee	lab3employee_profile	lab3employve_profile	0	
Wireless Option 📀				
Wireless Option ③ Multi band operation (2.4GHz, 5GHz, 6	SHz) () Multi band operation with Band Select (SCHellowy () 2.40Hz only () 60Hz Only		

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

Basic Settings				
ill the information like name, wireless o	ptions, state and network to complete the basic se	tup of SSID		
Winless Network Name (SSID)* Iab3guest	WLAN Profile Name* lab3guest_profile	Poicy Profile Name lab3guest_profile	o	
Wireless Option 0				
 Multi band operation (2.4GHz, 5GH 	z, 6GHz) O Multi band operation with Band Select	5GHz only 0 2.4GHz only 0 6GHz Only		
Primary Traffic Type Best Effort (Silver)	v			
SSID STATE				
Admin Status				
Broadcast SSID				

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

Eisco DNA Center		Wireless SSI)	\$ Q @ @ Q
SSID Name: lab3guest (Guest) O _o Associate Profile Cancel			
CagelabProfile	Profile Name corporate	Balay Brofile Manue		
	Fabric Vis No Enable SSD Scheduler	lab3guest_profile	O	
	Interface VLAN Group Interface Name* management Do you need Anchor for this SSID? Vie No.	~ •		
() tot	Fiex Connect Local Switching			Back Next

- **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

■ Cisco DNA Center		Wireless SS	SID	* < © △ 4
SSID Name: lab3guest (0	Guest)			
G Add Profile	🕒 Disassociate Profile 🛛 🔛 Save			
Q Search	Profile Name corporate			
CagelabProfile corporate	WLAN Profile Name lab3guest_profile	Policy Profile Name ab3guest_profile	Ø	
	Fabric O Yes O No			
	Enable SSID Scheduler ()			
	interface Name*	~ 🖨		
	Do you need Anchor for this SSID? Yes O No			
	Select Anchor Group Guest	~		

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。

E Cisco DNA Center	Wireless SSID	± < © < ¢
Portal Settings		
Configure the portal to complete the setup of S	SID for ISE. Please note that portal creation is optional	
SSID Name: lab3guest (Guest)		
	No Self Registration Portal Available	
	Use the create portal button to create a new portal	
	Create Portal	
) 6a		Back Next

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

		Portal Builder	\mathbf{X}
Lub3, Game, Portet	0	Login Page V Login Page S Registration Page	0000
> Color > Font >		Registration Success Success Page Sign In Writchers bit the Guest Portal. Sign on with the username and password provided to you USERNAME PASSWORD: Days regions up you agree to the terms and conditions Don't have an account?	

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。

SSIDs © Global Configure SSDs for enterprise and guest wireless networks. You can assign them to sites via Wireless Network > A US Profiles. SSID (3)									10%	All / 55		arch Hierarchy
b Cookel Configure SSDs for enterprise and guest wireless networks. You can assign them to sites via Wireless Network Profiles. SSID (3) C. Search Table SSD Context and SSD 5 Scheduler () 0 Selected To Texter and SSD 5 w WLAN Profile Name Price Profile Name SSD Type L2 Security L3 Security Wireless Profiles Profile Name AN Texter and SSD 5 w WLAN Profile Name Price Price Profile Name SSD Type L2 Security L3 Security Wireless Profiles Profiles AN									Ds	SSI	Search Help	
A US Profiles. SSID (3) C. Search Table LG1 Dense @ SSD Scheduler (3) 0 Selected					itwork	tes via Wireless N	You can assign them to si	quest wireless networks.	re SSIDs for enterprise and	Configu		obal
SSID (3) Q. Search Table Lot Device 2005 Scheduler () 0 Selected Image: Device 100 Scheduler () 0 Selected Image: Device 100 Scheduler () 10 S										Profiles.		US
Q. Search Table Edit: Owner @ S5D Scheduler ① 0 Selected INterpork Name (S5D) * WLAN Profile Name Pulicy Profile Name S5D Type L2 Security L3 Security Wireless Profiles Pursul Name AN Walk2-enter	🖨 Add) (3)	SSIC		
I SSD Scheduler 🕘 SSD Scheduler 🕢 0 Selected Network Name (SSD) • WKAN Profile Name Pulicy Profile Name SSD Type L2 Security L3 Security Wireless Profiles Portal Name Ad wsb2_enter	V								Search Table	Q		
Network Name (SSI0) * WLAN Profile Name Protocy Profile Name SSI0 Type L2 Security L3 Security Wireless Profiles Purtal Name A3 Work2_enter								ler 🕢 0 Selected	Delete 🛗 SSID Schedu	Edit		
wpa2.enter	UAA Servers	Portal Name	Wreless Profiles	L3 Security	L2 Security	SSID Type	Policy Profile Name	WLAN Profile Name	Network Name (SSID) *	0		
cagetabssid cagetabssi(1) cagetabssi(1) Enterprise prise open Cagetab9v0f/e N/A Co	onigure AAA	N/A	CagelabProfile	open	wpa2_enter prise	Enterprise	cagelabssi (1)	cagelabssi (1)	cagelabssid	0		
Lab3employee Lab3emplo(1) Lab3emplo(1) Enterprise wpi2_enter open corporate N/A	AAA Configurer (1)	N/A	corporate	open	wpa2_enter prise	Enterprise	lab3emplo (1)	lab3emplo (1)	lab3employee	0		
Lab3guest lab3guest (1) lab3guest (1) Guest open web_euth corporate N/A	AAA Configured	N/A	corporate	web_auth	open	Guest	lab3guest (1)	lab3guest., (1)	lab3guest	0		
Alexandream and a second	< 0 >	1 - 3	how Records: 10 🗸	5					ordia	3 Rec		
Alternative State Stat	< 0	1 - 3	how Records: 10 v	5					onfis	3 Rec		

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

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 O 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。

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
[Wireless Option]	オプションボタ ン(Radio	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。
	Button)	•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、2.4GHzチャネルでのプローブ応答を遅延させることで、 2.4GHzと5GHz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5GHz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]	オプション ボタ	
L2 セキュリティ	ン(Radio Button)	

機能	タイプ	説明	
		WLANのレイヤ クの暗号化およ およびフロアは ルディング、ま イドできます。	2 (L2) セキュリティ設定を決定します。ネットワー び認証タイプを選択します。サイト、ビルディング、 、グローバル階層から設定を継承します。サイト、ビ たはフロアレベルでセキュリティレベルをオーバーラ
		次のオプション	を利用できます。
		・[Enterprise] [WPA2] と [: それぞれのチェックボックスをオンにすることで、 WPA3] の両方のセキュリティ認証を設定できます。
		(注) 1	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] : [WPA2] と [デフォルト す。[Persona フレーズキ・ サーバーの] ます。	それぞれのチェックボックスをオンにすることで、 WPA3] の両方のセキュリティ認証を設定できます。 では、[WPA2] チェックボックスが有効になっていま al] を選択した場合は、[Passphrase] フィールドにパス ーを入力します。このキーは、クライアントと認証 間でペアワイズマスターキー(PMK)として使用され
		(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。
		 [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]	オプション ボタ	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
L3 セキュリティ	ン(Radio Button)	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。
		• [SelfRegistered]: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。
		 [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	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。
	フィールド	 [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NASID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

E Cisco ISE		Work Centers - Guest Access		Q 0 14 0
Overview Identities	Identity Groups Ext Id Source:	Administration Network Devic	es Portais & Components More ~	
Quest Portais	Guest Portals		×	
ionaor Groups ionaor Portala	Choose one of the three pre-	Rule Name	vize for guest access.	
	Create Edit Dup	Rule : Lab3_Guest_Portal_RedirectPolicy (v policy set : Default)	·	
	Hotspot Guest Portz		Self-Registe (default)	red Guest Portal
	password credentials to i network, but you can opti require an access code	_	Guests may cre and be assigne password, or un access the nets	ate their own accounts d a username and le their social logis to vork
	Authorization setup r		zation Used in 1 r policy	ules in the Authorization

図 30: ゲストポータルのプレビュー

≡ Cisco ISE			Work Centers	Guest Access			0 0 0 0
Overview Ident	ities Identity Groups	Ext Id Sources	Administration	Network Devices	Portals & Components	More ~	
Guest Portals	Pages	~	Page Customizat	ions		Preview	Settings
Guest Types Sponsor Groups	Login		Sign On				
Sponsor Portals	Reset Pass Reset Pass	word word Success	Optional Content 1 add button			ни	H-TECH
	Registration Self-Regist	n Form ration Success	Font ✓ 및 Ξ 등	$\frac{\circ}{\vartheta} \sim \frac{\text{Size}}{f_i} \frac{\circ}{\bigtriangledown}$	A ∽ B ⊡ II ∽		
	Acceptable	Use Policy				-11	
	Change Par Apple Mini Authenticat	ssword Browser Ion Success				Sign In Welcome to the Guest Pl username and password USERNAME:	ortal. Sign on with the provided to you.
	Error	~	(text or HTML) Click Pre Content Title	view to test HTML rendering.		PASSWORD:	Reset Pasaword
	Email		Sign In			Dy sipting up you pares	to the terms and conditions.
	SMS		Instructional Text			54	n On

- 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

	SE	Policy · Policy Sets					0 0	249	
0	Default		Default policy set	Default Net	a ~+	421239			
Authenticat	ion Policy (3)								
Authorizatio	on Policy - Local Exe	ceptions							
Authorizatio	en Policy - Global Ex	ceptions							
Authorizatio	on Policy (14)								
				Results					
• Statu:	s Rule Name		Conditions	Profiles		Security Groups		Hits	Action
Statur Q Sear	s Rule Name		Conditions	Profiles		Security Groups		Hits	Actions
Statur	s Rule Name		Conditions	Profiles		Security Groups		Hits	Actions
 Statur Q Searce O 	s Rule Name	AND	Conditions Wreless_MAB Ouest_Flow	Profiles PermitAccess ×	~+	Security Groups	a ~+	Hits	Actions
 Statut Q Search Search 	s Rule Name	AND	Conditions Wreless_MAB Ouss_Flow Redus-Called-Station-ID ENDS_WITH Jab3guest	Profiles PermitAccess ×	~ +	Security Groups	+	Hits	Actions
Statur Q Sear	s Rule Name	AND	Conditions Wireless_MAB Guest_Flow Radius_Called-Station-ID ENDS_WITH isb3guest Wireless_MAB	PermitAccess ×	×+	Security Groups	<u>@~</u> +	Hits	Actions

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

And Andrew Conductors 1		testers Testers	and Taxat			
twork Device Credentials	SSID (0)	Telemetry Security 1	nd trust.			O Add
Find Herarchy						-
Search Help Global	Q Search Table					V
De the first to add a new site from Network Manachy	(dt Deleter 🙆 550 Scheduler (0 Selected				
	Network Name (550) + WL	AN Profile Name Policy Profile Name	550 Type L2 Securit	y L3 Security Wrek	eus Profiles Portai Nome	AAA Servers
			No data to display			
	Wireless Radio Frequency Pro	ofile				O A60
	Basic RF Profile Al RF Profile					
	RF Profile (3)					
	Q. Search Table					V
	Actions 😒 0 Selected					
	Profile Name * Type	2.4GHz Data Rates	SGHz Data Rates	6GHz Data Rates	Channel Width (2.4/5/4GHz)	Profile Type
	HGH 2.4, 5, 6	9,12,18,24,36,48,54	12,18,24,36,48,54	8.9.12,18.24,38,48,54	20 MHz / Best / Best	System
	LOW 2.4, 5, 8	1,2,5,5,6,9,11,12,18,24,36,48,54	6,9,12,10,24,36,46,54	8.9,12,18,24,38,48,54	20 MHz / Best / Best	System
	TYPICAL 2.4, 5, 6	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System
	3 Records			Show Records: 10	1+3	0.0
	Wireless Interfaces (1)					O A04
	Q Search Table				_	Ÿ
	Edit Online O Selected					
	Diterface Name + VLAN (0					

- 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。

owork Device Credensals	IP Address Pools SP Profiles Wireless Telemetry Security and Trust	
Find Hierarchy	Wireless Interfaces (6)	Create a Wireless Interface
Global	Q, Search Table	Interface Name*
Be the first to add a new site from Network Hierarchy	Cott Delinie 0 Selected	Only 31 characters are allowed
	Interface Name - VLAN ID	VLAN ID range is 0-4054
	branchempioyee 100	
	branchquest-dmz 110	
	Clents 49	
	employee 160	
	gvest-dnz 125	
	management N/A	
	6 Records	
	Antenna Radio Profile (0)	
	Q. Search Tatrie	
	Cdt Determ 0 Selected	
	Radio Profile Name Beam Steer Mode	
	No data to display	
	AP Authorization List (0)	
	Q Search Toble	

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

E Cisco DNA Center		Design / Network Settings	0004
Network Device Credentials	IP Address Pools SP Profiles	Wireless Telemetry Security and Trust	
Q. Find Hierarchy	Wireless Interfaces (6)		Add
Search Harp sh Globel	Q. Search Table		V
Be the first to add a new site from Network Herarchy	Edit Delete 0 Selected		
	D Interface Name •	ND	
	D branchemployee		
	branchguest-dmz		
	Clients		
	employee		
	guest-dmz		
	management		
	6 Records	Show Record	ek 10 🗸 1 - 6 K 🔘 5

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

E Cisco DNA Center	Wireless SSD	\$ Q @ @ Q
Basic Settings Fit the information like name, wreter	is options, state and network to complete the basic setup of SSID	
Sonar 🕢	WLAS Florie Name" Paics Florie Name Ista Stream 5. profile Ist Stream 5. profile	
Wireless Option () Multi band operation (2.404c,)	Kinka, 46H4() 🔿 Multi band operation with Band Select 🔿 SOPE only 🔿 2,40PE only 🔿 60PE Only	
SSID STATE	<u> </u>	
Est		Next

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

Security Settings		
Configure the security level and authentication, a	uthorization, & accounting for SSID	
A For 2.4GHz+ SGHz only, enable WPA2 , V	IPA3 Is optional. For 2.6GHz+SGHz+SGHz+SGHz to be operational on IOS devices version 17.7 and above, enable WPA3 and disable WPA2.	×
SSID Name: lab3branch5 (Enterprise)		
Level of Security		
O Enterprise O Personal O Open Secur	ed O Quen	
C 10942		
Most secure User Credentals are validated with 802.1x Radiu WPA3 teature is supported for Wireless Controlik	s landrar 10 authenticate cileres to the universe network, r version 8,10 & adove, For Carsiyot 8800 Controllers version 16,12 & adove.	
Authentication, Authorization, and Acc	ounting Configuration	
AAA Configured (1)		
AAA Override	G Fast Lane	
G Mac Filtering	Deny RCM Clerres	
🗆 finable Posture 🧿		

図 37: エンタープライズ SSID の詳細設定

Advanced Settings		
Configure the advanced fields to complete SSID setup.		
SSID Name: Sab3branch5 (Enterprise)		
Fast Transition (802.11r)	MFP Client Protection ()	Protected Management Frame (802.11w)
Adaptive C Enable C Enable	Optional ORequired Obtaibled	O Optional O Required O Disabled
Over the DS		
11k		
Neighbor List		
in (anti)*	in junction	
Seasion Timeout 💿 1899	Client Exclusion 160	
11v BSS Transition Support		
B55 Max Idle Service		
Client User Idle Timeout Client User Idle Timeout	Directed Multicast Service	
Radius Client Profiling		
NAS-ID ()		

- **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

E Cisco DNA Center		Wireless SS6	•	* < @ \$ \$
SSID Name: lab3branch	5 (Enterprise)			
O Anter Providine	O _D Associate Profile Cancel			
Q, Swarch CagelabProfile	Profes Farme branch5			
corporate	WLAN Profile Name Nab3branch5_profile	Poles Polie Name (ab3branch5_profile	0	
	Palane O Yes O No Drushe SSD Scheever O Interface O VLAN Group			
	Insurface Name" management Do you need Anchor for this SSID? O Yes O Nes	~ 0		
	 First Connect Local Switching Logid to VLAN 100 			

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。

Cisco DNA Center

Cisco DNA Center</t

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] > [FlexConnect Settings]の順に選択します。

図 40 : [FlexConnect Settings] ページ

		Design / N	letwork Setsn	gs / Wireless		* 9 0 0 0
), Search Herarchy	Air / Finalization Sartings					
Search Holy	FlexConnect Settin	gs				
Global	Electonnect settings are inherited by a	Etildren stes. Ouenides done	at the child level	do not affact the perent.		
	ElevConnect M AN					
	Configure the VLAN for all PlanConnect	access points managed in the s	ite.			
	Nature 13, Mil E					
	90					
	VLAN ID range is 1.4	004				
		A REAL PROPERTY AND A REAL PROPERTY AND A				
	Fies deployments support a maximum o WLAN's VLAN and VLANs pushed by Ar	f 16 VLANa. For Catalyst 9808 5 AA.	Series Wireless C	unitsilets, this includes the	VLAU Tourse	
	First displayments support a maximum of WLAV's VLAV and VLAV's pushed by AV	f 16 VLANs. For Catalyor 9800 5 AL VLAN North Englishes Only 21 characters are alreed	Series Whelees C	orientians, this includes the NUME D 100 VLANID range is 1,4000	VLAN forms Duest Coty 21 charactery are adjusted	•
	Field deployments support a maximum of WLAN's VLAN and VLANs and VLANs pushed by A 40 100 100 100 100 100 100 100 100 100	1 16 VLANs. For Catalyst 9800 1 M. VLAN Norte Employee Only 21 physiolan are allowed	Sarina Witniana C	ontrolliers, this includes the 0.04 E 110 VLAN ID range to 1.4004	VLATI Turns Dural Chip 17 characters are allowed	•
	Her deployments support a maximum of WLAN's VLAN and VLANs pushed by Ar 	t 18 VLANa. For Catalyon 9800 f A. VLAN Nore Enginyse Orly 21 diverties an always	Series Windows C	entrahera, this includes the VLAV D 110 XLAND range to 1,4004	10,401 huma Durat Cely 27 characters are alterned	
	Files displayments support a machinum a WUAR's VLAN and VLANs pushed by AV 105 VLAN C runge a 1.4214	f 16 ULANa. For Catalyot 9808 5 M. <u>ULUI Torte</u> Enginyae Only 21 characters are divised	Series Windows C	entralisers, this includes, the ULAN C 110 VLAN C regis to 1.4008	MUM Norm Davat Chig 21 characters are allowed	•

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

E Cisco DNA Center		Tools / Model Config Editor	\$ Q @ @ A
Clesco DNA Center Netres Add Natura Atributes Center Add Natura Atributes Center Clesco DSD Center Clesco DNA Center Cle	Design Instances Fix Configuration - Model Configs There is Configuration the set takes - Default thes Configuration	Teols / Model Config Editor Add Flex Configuration The seventhilty is used for configuration of the Model Config Product of the managed AP location/lates. Except Numer Facility Config Config	Constraints of the second
	1 Jacobi		Canton Save

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

Cisco DNA Center	Design / Network Profiles / Wireless	* 9 0 0 4
naan Parline 1 Warren	Add Model Conf	ig
dit Network Profile		
Idening tasks must be completed before creating a Winness Network Profile. 1. Define SSDD, instrator, RF Profiles and AP Profiles under Network Setting 2. Define Model Configs (Spring) Media Config 12 2. Define Model Configs (Spring) Media Config 12	Is & Windows C ² Models CONTIGS Device Pyteric) Class Cemper 9993 Series V	Venkarg Controllars a
of le Name BranchS		
te 5 sites	Search	
who type: when		
SIDs AP Zones Model Configs Templates Advances	d Settings V	
	Progue General Cont	iguistice (C)
	2 CleanAir Configuration	on Q
Attach Model Configs	> RRM General Config	uration ©
	> RRM FRA Configurat	ion ()
	> Multicaer, Configurati	lon Q
	V Flex Configuration (D.
	Enderth	
	Default Flax Cor	rigunition
	> Advanced SSID Con	figuration ()
	> Dot11ax Configuration	on ©
	> Event Driven RRM C	ontguration ()
		Cancer Add

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

■ Cisco DNA Center		Wireless SSID		* Q @ C 4
Basic Settings Fill the information like name, wireless op	ptions, state and network to complete the basic setu	up of SSID		
Wireless Noteork Name (SSID)* fab3guest5	WLAN Profile Name* lab3guest5_profile	Policy Profile Name lab3guest5_profile	0	
Wireless Option () Multi band operation (2.40Hz, 50Hz)	. 6GHz) O Multi band operation with Band Select O) SGHz only 💫 2.4GHz only 📄 BGHz Only		
Primary Traffic Type Best Effort (Silver)	v			
Admin Status				
-) Exit				Next

図 44: ゲスト SSID のセキュリティ設定

=	Cisco DNA Center	w	ireless SSID	\$ Q @ @ \$
	SSID Name: lab3guest5 (Guest) Lavel of Socurity L3 SECURITY 6 Finançaise () Personal () Open Sec Least Socure () Any unit can associate to the network. L3 SECURITY 9 Web Raticy () Com Main secure	und Open		
	Authentication Server	What kind of portal are you creating today 7 Self Registered 🗸 🗸	Where will your quests redirect after successful authenticution ?	
	Authentication, Authorization, and Ac AAA Configured (1) AAA Overhite Max Filtering	Counting Configuration	0	
00				Bock Next

図 45: Flex ゲスト SSID の AAA 設定

E Cisco DNA Cer	itér Wireless SSID		\$ Q @ \$ \$
L2 SECURP	Configure AAA Server for lab3guest5		×
Any unor the	A Two (2) Warning Alerts and One (1) Information Alert on this page. Collapse to Note.	×	
Web Par Most secure Coast core	Tao (2) Warring Alerts Catalyst 0000 Controllers services loss than 17.8 subject only aptil 8 Accession Method Int configuration, Configuration man than the new result in providioning failure. To ensure the right strategiantees a powhed for this 2500, certigane are an envire AAA/HSN. Ore (3) Information Alert To one (3) Information Alert To one (3) Information of Servers. To one disc certificate an optimal particular of Servers. To support different and the certificate area of Servers. To support different and the certificate area of Servers. To support different and the certificate area of Servers. To one of Servers. To an area strategiate area one of Servers. To support different and support different area of Servers. To an area strategiate web antiversation.		
Central Web	Configure Authentication and Authorization Servers		
Authentic Atlant cou-	Server 172.23.240.152 v 17 + Copy same Servers for Accounting		
T) AAA Oo	Configure Accounting Server		
Pro-April A	50000 v 8 + 172.23.240.152 v 8 +		
E) Extr			Back Fred.

図 46: Flex ゲスト SSID の詳細設定

E Cisco DNA Center	Wireless SSID	\$ Q © A \$
Advanced Settings		
Configure the advanced fields to complete SSID setup.		
SSID Name: lab3guest5 (Guest)		
Past Transition (802.11r)	MFP Client Protection O	Protected Management Frame (802.11w)
Adaptive Constree Disable Divertifie Divertifie	Optional O Required O Disatiled	Optional Required Disabled
11k		
Neighbor List		
E Session Timeout	Client Exclusion 190	
11v BSS Transition Support		
BSS Max Idle Service		
Client User Idle Timeout Other User Idle Timeout 300	Directed Multicast Service	
Radius Client Profiling		
NAS-ID 💿		
Q 64		Back Next

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

E Cisco DNA Cent	er Wireless SSD	\$ Q @ \$ \$
SSID Name	lab3guest5 (Guest)	
Cagesian Cogesian Cogesian	vedea n Proteg faree Exactor N Proteg fare Vedea Proteg fare Pr	
θω.	Control Control Control Switching Local to MLAN Dee dath only MLMI througe to 1.4054	Tech Sect

- **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

E Cisco DNA Center	Wireless SSID	* 0 © 0 0
Portal Settings		
Configure the portal to complete the setup of SSID for	ISE. Please note that portal creation is optional	
SSID Name: lab3guest (Guest)		
	No Self Registration Portal Available	
	Use the create portal button to create a new portal	
	Create Portal	
		Back Next

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

≡ Cisco DNA	A Center		Wireless SSID	☆ C	004
Summ Review all o	ary changes				
 ✓ Ba SSI WL Poli Pvir Rad Adr Bro 	ISIC Settings ID Name AN Profile Name Icy Profile Name mary Traffic Type dio Policy min Status wadcast SSID	Edit Isb3guest5 Isb3guest5_profile Isb3guest5_profile Best Effort (Silver) ③ Multi band operation (2.4GHz, 5GHz, 6GHz) Yes			
✓ Se L2: AA Acc AA May Fas	curity Settings Security Security A Servers counting Servers A Override c Fittering it Lane	Edit open web_woth 172_23_240_152 172_32_240_152 Yes Yes No			
() Ext				lark	Caus

- **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

E Cisco DNA Center	Des	ign / Network Profiles	* 0 0 0 4
Cisco DNA Contor C. Search Table Porties Name - Israndi Corporate I Throndi	Des Type Miniess Winiess Winiess	Iden 2 Network Profiles Add Sites to Profile: branch5 Choose a ste Colored a ste Color	* Q © 0 Q ×
			Cancal Save

- **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

E Cisco DNA Center	Design / Network Settings / Wiveless 🏦 🔍 🗇 🔿 🖉				
Search Heranomy Search Heranomy who could be a could be a c	In Freedoment Instage Flex.Connect Settings Flex.Connect VLAN Rear Flex.Connect Flex.Con	n flore at the child leve in the site.	i do not affect the parent.		
	Visit Biological and VLANs purchase of VLANs to Classify WLAN's VLANs of VLANs purchase by AAA VLAN (C 100 VLAN (C) rungs is 1, 4014 VLAN (C) rungs is 1, 4014 Only 21 (detectors are a		ULAR D 10,010 100 10,010 trapp to 1,4000	0.00 have Good Orb 21 characters are allowed	•
					Center

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

E Cisco DNA Center	Tools	/ Model Config Editor	* Q @ C Q
Cisco DNA Centor Design Discovery Cannot America Americ	Tools Design Instances Flex Configuration - Model Configs ✓ Flex I terr Const 0 Sensitive Other Plax Configuration Other Plax Configuration	/ Model Carlig Editor Add Flex Configuration This consistent is used for configuration these Configuration if the Manager AP to statement with a the AP to s	
MMM FRA Configuration () MMM Exercise Configuration () Region Connect Configuration ()	1 Basers		Cancer Said

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

Cisce DNA Center	Design / Network Profiles / Wireless		* 0.004
ut Police / Workers	A	Add Model Config	
lit Network Profile			
amp tasks must be completed terteris creating a Tilmanos Hateoni Politie. . Define (500), interface, All Profiles and AP Profiles under Namonik Gettings I . Define Sterigibles in Templates Hub (common), Templates Hub (7) . Define Model Config. (Common) Model Config. (7)	& Windows CP	KOGEL CONFIGS Inves Turno Elass Celulysi Mill Series Minelos Consolers (*	
ie Name BranchS			
5 sites	1	Search .	
is 7gost when		Manager 1	
Is AP Zones Model Configs Templates Advanced	Settings v	Reque General Configuration	
) Clean Air Configuration (C)	
		> 199M Deneral Configuration C	
Attach Model Configs) RRM TRA Configuration (0)	
) Multicast Configuration (C	
		Y Fies Configuration O	
		E tranch	
		Default Res Configuration	
		> Advanced SSD Configuration (3)	
		2 Doll Tax Configuration (C)	
) Eveni Drivet RRV Configuration (C	
			Castal Add

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

Cisco DNA Center DE	SIGN POLICY PROVISIO	N ASSURANCE	PLATFORM		۹ 🕲	Ш	0	0	=
Network Hierarchy Network Se	ettings Image Repository	Network Profiles	Auth Template						
EQ. Find Herarchy	Wireless Radio Frequ	ency Profile						0	Add
 (b) Global 									
> 🕖 Milpitas	Ÿ Filter	w 📋 Damas 🗸 Mar	k Default 1 Selected						
	Profile Name -	Type	SGhz Data Rates	2.4Ghz Data Rates	Channel Width		Profile 1	Type	
	П НСН	2.4 GHz .5 GHz	12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz		System		
	LOW	2.4 GHz .5 GHz	6.9.11.12.18.24.36.48.54	1,2,5,5,6,9,11,12,18,24,36,48,54	20 MHz		System		
	TYPECAL (Default)	2.4 GHz .5 GHz	6.9,12,18,24,36,48,54	9,12.18,24,36,48.54	20 MHz		System		
			Show	ing 3 of 3					

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。

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

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
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

E Cisco DNA Center		Design / Ne	etwork Settings				0	004
Network Device Credentials	IP Address Pools SP Profiles	Wireless Teler	netry Security a	nd Trust				
Q Find Herarchy V	SSID (2)							🔁 Add
୍ ଶିଂ Global	Q Search Table							V
> dt Australia								
) 🗄 Austria	Edit Delete 💼 SSID Schedule	0 Selected						
> 🕸 Bermuda		an an Postin Name	Defen Desfie North	6640 T	10.0	1.0. Francisco	Martine Profiles	Destant Marries
> 🕀 China	Network Name (SSID) * 1	NLAN Profile Name	Policy Profile Name	SSID Type	L2 security	C3 security	Wireless Profiles	Portal Name
> db Cisco	0 405-0040	aws-0040 (1)	ant-oneo (1)	Enternrise	0040	0000	aws-open-	NIA
> db Egypt	O mit option	ana chair. (i) ana chair. (i	and observe (1)		again ag		profile	
> 🕸 England					wpa2_per	corpevent-	200	
> & France	C corpevent o	Jorbeveur" (J)	corpevent (1)	Encerprise	sonal	open	profile	NU/AL
> 🕸 India								
> da Japan	2 Records				Show Recon	58; 10 V	1 - 2	C O >

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

E Cisco DNA Center	E Cisco DNA Center Design / Network Settings	
Network Device Credentials	IP Address Pools SP Profiles Wireless Telemetry Security and Trust	
Q. Find Hierarchy	SSID (2)	4 Add
v & Global	Q. Search Table	Enterprise
> dh Australia		Guest
> el Austria > él Bermuda	The Decks at 250 Schedule () o selected	Dented Name

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。

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

表 **18**:エンタープライズ **SSID**の設定

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。

=	Cisco DNA Center	Wireless SSID	Q @ @ 4
	Associate SSID to Profile		
	Select a Profile on the left or Add Profile and click 'Associate' to associate to Profile.	the SSID	
	SSID Name: cornevent (Enterprise)		
	Add Profile		
	Q Search		

- **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。

図 *58*:ネットワークプロファイルへの *SSID*の関連付け

- (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VLAN16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

■ Cisco DNA Center	Wireless SSID	Q @ @ 4
SSID Name: corpev	ent (Enterprise)	
Add Profile	1 profile(a) essociated.	
Q Search aws-cl-profile aws-open-profile corpevent-profile		
() tea		Back Next

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

yes Settings Edit	corpevent							
settings Edit	corpavent						_	
Settings Eat	corpevent.							
me	corpevent							
the File Bittern o								
tone marrie	corpevent_profile							
rofile Name	corpevent_profile							
Traffic Type	VolP (Platinum) 💽							
stey	Multi band operation (2.4GHz,	5GHz, 6GHz)						
itatus	Ves							
st SSID	Yes							
ty Settings Edit								
ity:	wpa2_personal							
10y	open							
vers								
						Back		Saua
	offle Name fraffic Type ficy tatus at SSID y Settings Ede fy fy rers	offile Name corpevent_profile traffic Type VeIP (Plathum) () ficy Multi band operation (2,4GHz, tatus Yes t SSID Yes y Settings Edt try up92_personal try open ers	ofile Name corpevent_profile traffic Type VeIP (Platnum) () Ney Multi band operation (2,4GHz, 5GHz, 6GHz) tatus Yes at SSID Yes y Settings Ede try vpa2_personal try open ers	ofile Name corpevent_profile traffic Type ValP (Platnum) (3) Nov Multi band operation (2,4GHz, 5GHz, 6GHz) tatus Ves at SSID Ves y Settings Ede try wpa2_personal try open ers	ofile Name corpevent_profile traffic Type VoIP (Platnum) () top (Platnum) () top VoIP (P	ofile Neme corpevent_profile traftic Type VoIP (Platnum) () Not Vo	ofile Name coppevent_profile traffic Type VBP (Platinum) traffic Type VBP	ofile Neme corpevent_profile traffic Type VoIP (Platinum) top Nutri band operation (2,4GHz, 5GHz) tatus Ves ta SSID Ves y Settings Ede try wpa2_personal try open ers Dack

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

E Cisco DNA Center	Design / N	Design / Network Profiles		
				Add Profile
Q Search Table				
Profile Name *	Type	Sites	Action	
aws-cl-profile	Wireless	Assign Site	Edit Delete	
aws-open-profile	Wireless	2	Edit Delete	
corpevent-profile	Wireless	Assign Site	Edit Delete	

- 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

Cisco DNA Center	Discovery	</th
Discovery Dashboard		
Add Discovery View All Discoveries Device Controllability is Enabled.	Inventory Overview As of Jul 1, 2019 11:41 AM	Latest Discovery As of Jal 1, 2019 11:41 AM ② WLC-9800-2_2
Discovery Type As of Jul 1, 2019 11:41 AM 26 IP Address/Range : 26 LLDP : 0	Discovery Status As of Jul 1, 2019 11:41 AM 26 In Progress : 0 Completed : 26 Aborted : 0 Scheduled : 0	Recent 10 Discoveries As of Jul 1, 2019 11:41 AM

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

Cisco DNA Center	D	iscovery		(Q	=	0	0	1
 Search by Discovered Device P No Discoveries Added 	New Discovery								
	 ✓ IP Address/Range* Discovery Type ● CDP ● Range ○ LLDP From* ● 10.4.174.32 	To* 0 - 10.4.174.34	+						
	Preferred Management IP 0 None UseLoopBack								
	 Credentials* At least one CLI credential and one SI Netconf is mandatory for enabling Wir using port number 830. Do not use sta 	NMP credential are required. eless Services on Wireless capable devices : andard ports like 22, 80, 8080 etc.	such as C9800-	Switches	/Contr	ollers.	We rec	comme	nd
	 Credentials* At least one CLI credential and one SI Noteconf is mandatory for enabling Wir using port number 830. Do not use still global at task-specific CLI CiscoDNA No Description 	NMP credential are required. eless Services on Wireless capable devices r andard ports like 22, 80, 8080 etc. SNMPv2c Read	such as C9800-	Switches	i/Contr	ollers.	We rec	comme Credent	nd

- 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

Discovered devices will be added	to Inventory automatica	By after successful completio	n of each discovery, Vew	inventory							2
Catalyst_9800_WLCs 2 Peer					Y Filter					Histo	ry 🗸
			DEVICE STA	rus 🗸	P Address	Device Name	Status	1C809 +	INVP	CLI	1
		0			18.4.174.32	#5,0-9800- 2 class local					
			· Surress		12,4,174,24	MLC-1000-					
	Discovery D COP Level Protocol Order	Orvices Details None sah	E Discarded LLDP Level Retry Count	None 2	Show 20						
	Timeout	5 second(s)	IP Address/Range	10.4.174.32-10.4.174.34		_	~				
	IP Filter List	None	Preferred Management IP	None		tan @ series	. () Maria			PRODUCTION	
	CU Credentials	netadmin,CiscoDNA	SNMPv2c READ	Read							
	SNMPvzc WRITE	Write	SNMPv3	None							
	HTTP(S) READ	None	HTTP(S) WRITE	None							
	NETCONF	830									

- **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

III 🗘 Global		Design / Ima	ige Repository / Summary		* Q. @ @ A
		Romes (Sectors and Fills) (R	freites Controllers (Security and 1976	Senars (What Devices)	
SUMMARY	TOTAL REAGES	ADVISORIES			
4 7 3 Device Families Devices Families Mithout Dolder Image	6 3 1 Running Important Conden	2 73 Ortical High On Running Images On Ru	unsing lineque		
Image Families					Take is Tour (Occusion II) - Semapora (Not mer) - Sync Updames @
Q. Search Lans					7
Click or gol	den image			C Update	Onview of import image 2 lines fails as a subscription of
Family Name	Inter	Imagen	Cetterar O		Muger Warked Bolton
manual images @	-	1. N.	101	505	N/A
Cross Ceneyer \$300 Switch	3		3	72	0
Elece Catalyst 9300, Switch Stack	,		*		*
Class Calalyst 8000-60 Windows Cantrollar		1 C	.0		1
Class Catalyst MICO-CL Mindows Controller for Claud	1	10 A			

- **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。

Bengelunic 17.8.5 Aut In (KUR)

Coparting-17.8.3 And In Solid

Annual State of Land

10.11.01.0.1204 Mail Dr. Politi .

.

.

4

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。

E 7 Geov		Design / Image Repository / Imag	e Family	
Cisco Catal	yst 9800-40 Wireless Controller		-	
antennet > Molec & Tage (4) > Malar Western (5) > Datition Imagen (3)	Images (A)	download icon will downloading image fro Download Webs	start em Cisco ite	
 Meconimication 101 	maps faces		-	-
	Transal Mason (17.11.01.0.1004)	ALC: U.S. A. SHE		
	0000-unsesant, etc. 0114, 3, 00001, 17, 04, 00, 00001 8.	17.08.00.0.10		

_						
义	67:1	メー・	シの	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。

salet, als 17.06 05.8PH lan

1, ada, 17 / 1, (1, SPR.)au

All universalité, site 17.38.03.574.584

nel larest

.....

E Mare Rease - Discourse it - seringen (Normal) V

Danie from & Tage 🖷

٠

/

.

.

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1** 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

Cisco DNA Cent	ter DESIGN POLICY PROVISIO	ON ASSURAN	CE PLATFORM	
Network Hierarchy	Network Settings ~ Image Repos	itory Netwo	rk Profiles Au	Assign Device Family
😗 Import 🖞 Upda	ate Devices Show Tasks 0 Tak	ke a Tour		Assign C9800-40-universalk9_w/c.16.10.01e.SPA.bin to one or more supporting device series from the list below
Y Filter C Refrest	Last updated: 4:01 pm			✓ Device Series from CCO
Family	Image Name	Using Image	Version	
Assign	C9800-40-universalk9_wt Ø Verified	0	16.11.1c Add On (N/A)	1.Selected EQ, Find
				Device Series *
Assign	Werfied	0	16.3.3 Add On (N/A)	Cisco Catalyst 9800-40 Wireless Controller
Assign	cat9k_losxe.16.06.04.SPA Ø Verified	0	16.6.4 (Latest) Add Cin (N/A)	Show 10 entries Showing 1 - 1 of 1 Press
Assign	C9800-CL-universalk9.16 Ø Verified	0	16.11.1c Add On (N/A)	> All Device Series
Assign	isr4400-universalk9.16.06 Ø Verified	0	16.6.6 Add On (N/A)	
Assign	aar1002x-universalk9.16 Ø Verified	0	16.6.6 Add On (N/A)	
Assign	c3560e-universalit9-mz.1 Ø Verified	0	15.2(3)E1 Add On (N/A)	
Assign	C9800-40-universalk9_wt	0	16.10.1e	Please ensure that you select the right device series for the image. Wrong selection may cause issues during device upgrade. Cancel

- 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

E Color		Design / Image Repositor	y / Image Family				
Cisco Catal	yst 9800-40 Wireless Controller						
Enderson I Masse & Taga (5) J Magar Versions (5) I Goder Images (2)	Images 00	Clicking of against the image of the other of the clicking of the other ot	on the star s le of choice liden image	will mark it as)	i Dave Tank	 Descure it integers (for each) V An et al. (0, 000 million et al. (0)
 Recommendation (2) 	map form		\backslash		1004	nurse Mar	Denne Harre & Tage D
	Securit Made (17.11.01.8.1504)	12.111.01.0.1124 Ave: (n. 2010)		-			
	0000 alarahi, at. 199, 3, 0001, 9, 8, 81, 9940 k.	17.06.03.0.10 Autor (0.00)		~			
	C0001-4D universality, etc. 17.05.05.07% and Regional Labor	Bergelans-17.8.8 Aut (n. 909)	· \				•
	CHIEF of unservated, we 17 20 27 Min.com Register Control	Advantage 10.5.7 Augusta (0.0)		V.		1	•
	CHIEF 4D university as: 17.29 CL MH. Im	17.08.00.0.4111 Autor (Autor)		1			1
	Children of the second state of the second sta	17-11-01-01-0200 Aver-19-2000		•			/ 🚥

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

III O Global			Provisi	on / inventory				99.00	
			m Setutes C	Tanina Controllers	Access Points Serairs			8 II P	0
SEVEL WORK CENES	Devices (4) Focus tarbara images							Take a lose & Expert	0
() Livearians	Q. The desires								10
(1) Unavergened	S Searces @ Add Device Tag Actions	v 0						Acres 20124, 2022 11 202	
C Parled Provision	Dentes Tame	P Address	Dentro Family	humany 🔿	Sufferent trapp	01 Update Dianue	214	Provincency Datas	Marag
() Outlased Schware Image	C CHECK AD CVD respense town 10	164.503	Mineless Centralier	• Inschuter	Caeso((x,r,r,r) Needs Update	Activation Pending		Become See Details A Out of Spre-	• M1
C) Fallet Inage Prechectes	C 0000-0010 reprint local	10.4.46.153	Mireless Controller	· Reachable	Clease-CL(17, 11, 01, 0, 1304) Mark Golden S	-		Success See Despite A Out of Spre-	• 141
C Security Advances	D Ø 0000 040 teket %	10.4.48.707	Mireless Controller	· Reachable	C8800-serivematkit_wis.9176_3 Reads Update	Detribution Panding	Antige	Not Provisioned	• **
	C CHECO Place CVD capetals local	10.4.48.110	Wreiwes Controller	• Reachable	Caebo(17,11,1) Treads (Johns	Distribution Panding	NewNet/Brench 3	See Dealer A Out of Spre	• 10

- **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

Cooler		Provision / Inver	aby .		* 0 © B Q
		Image Update Readiness Check	r		×
provid wine, crown	Devices (4) Focus Bahaara Images	Concernant of the second secon			
C Unmertanne III	Q. The lease	Device Definis			
(1) Unansigned	distanted OAM Device has Arts	Denire CBR00-ChD-Applue1 (1	0.4.48.1011		
C False Processon	C Incus Name	Guiller mage CMOC-45-universality	un 12 de la SPA por		
() Non-Compilent		Related Required Tes			
Outstated Software Image No Souther Image	C 2000 40 CVD capabilities 1	Readiness Checks Results C No Co	cule Charles		di faquati 🖉 acut ar in 2001 il prime
C Faled Image Prechaster		Check Type	lossergeises	Status	Last Charinet
(*) Under Maintenance	U & case-of-one references	Part days	Part class, 500000 Organizati 1427 WE Analytic free score is 1600 ME	•	Ar 34, 38(311, 6) MR
C tecuty Admones	O CHEMO CALO Replace 1	beau Orbitation (Solis	Failed to liquid. Service contract economics Linkowskies Related Scholl to both Service contents wettendow strategical Relation Service Units COID-Destination (Service Service) 1005 contracted by to collarse Service	•	AN 28, 2010 11 00 MM
		Startug carefy chaos	foring configuration and for the dealers		AN DR. 2000 11:00 AM
		Corfig regions shock	Phone charge the Derfor separate ratio Parameter (PCPNI2,0000) Refere (Regarding to charge Config register to expected the set	•	AN 24, 2022 11-32 AM
	,	Pia Tanàn Diak	erritri) is ND* searcharp. YD* is submative Resemble Costs DM: Certer indiffusion has to its inspection accountify and provide and water is an in-maximal (1) at all (1) to an of the cost of the costs DMC (1) at all (1) costs of the costs of the costs DMC (1) and (1) costs of the costs of the costs DMC (1) and (1) costs of the costs of the costs of the means in analysis of the costs of the costs of the costs of the costs of the costs of the costs of the costs of the means in accessed action of the days detected during trages transfer.		Ar (94, 302). 11 dat MM

[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

Select Devices											
Salaci the devices for which shights devices are dealered multiple sites	con the 1	the special sector of the sect	dia aphasina shaga, Ort at admi(1.854536, al-loss								
the selecter totals I deta area	e t emi										
hermony 1		mium (1)									٠
factor that		factor of	-	-	104 \$155.0	0 010m					
al un		(woor he	Device Sales	17 NoTINA	Jacob Torda	Oncore Series	149.000	fations man	(C) artest france	(mour late	114
			And the last full fit	124.46.710	Northeast Contraction	Cites Camps MIC Inter Nation Contains	11.1.1pm#	Specify (1,11-2 fair), specify Republicants Report	Juniorizations Providing	MODER	interiored
								diving Second Sec			

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 Cisco DNA Center	Image Update	40004
New Custom Check	Name the custom check	×
To add a custom check, add commu- Xame* CustomCheck	Minard's before adding them. Use G+T to Minard's Peak x V	toggle the visibility of Command Ruiner.
Commundat(a) *	Add custom check CLI	
Try out the command(s) above by selecting Select x Test Series C9800-Flex-CVD (10.4.48.150)	a test device and stoking on Open Command Runner button.	
- Add Known Command-Patterns	to Ignore During Checks	on the shift from the
most commonly used patterns.	regen. These particulars are used to general mainting outputs for checks is pairs of the reg	
- Additional Criteria		
Daviduation x Authorities x	Chern Canalyst MMD Santes Windens C., x → →	
		Cansal

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。

IT : [Software Activation Checks]

E Clace DNA Center		Image Update		* 9 0 0 0
Software Activation Che	ecks			
You can enable prechecks and postchecks determine the check order. If you don't set	for your software as a check, you can a	tivation and 56 a custom check.		
Skip Activation				
2 PRE AND POST CHICKE	DITING INC.		_	
There carry cress	DISTON PAR	PORT	-	
				1
C EAR At charges seed				Back Next

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。

☑ 78 : [Device Activation Order]

Elisco DNA Cente	r			mage Update	<u> </u>		49.0	00
Device /	Activation	Order						
You can use fit sequentially. A	tais to sort devi for devices are	ces and order sorted, you ca	their activation in para in reorder them seque	fail or relatly.				
evice in Parallel(1) 🥜 bes (2man							
arafiel Sequential								
Q learn here								7
Selected In Manual In Series	ercel Quarte Cris	- 1989						
Desite Name -	W Address	Site .	Onatas Sarias	Device Name	Current Image	Updato Image 🛢	Connect	
C1000-Fax-C10	10.4.48.194	Unantigrad	Cisco Catalyst M	Access	C8000(17.87.81pmL	CHOO-AD-universal	Update Readines	a Report
haranda						Doe Receiptor 201	141	
East at starges seend						-	Back Disc	iest (

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

E Cisco DNA Center	image Update	0000
Schedule Task and Cle	an Up	
You can schedule software distribution, a memory.	choose, and cleanup of device	
O the set of Distribute schedul	on can be Now or set of for later time	tivation can be Now or cheduled for later time
C fore @ Later	After Southanne Caller	
Ami 12, 2003 🔛	ave 13, 2008	
tona dona Amarina Losa, Angarian v	Time Jose Angelesches_Angeles v	
INTER FLADY CLANNY INTER ACTIVITY	04	
Check	and writes all produce stager shart on the bortes.	
this box to delete th after activation to s space	e image ave disk	
() find an element of the		Ten Bei

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

Summary					
Review your scheduled task, the activation.	Click Edit to make changes o	Submit to sche	(),/ie		
1 1 Devices to Update Device Sec	1 Shee				
Task Nama Tun Name (1960)u					
- Selected Devices					
Q, teach tase					Ψ.
Bearing Name	Bassice Series	in.	formed trapp	Cantons Image	Galaxia Brater
08850-Pies-OVD (10	Choo Cetalysi MOI S.,	Duniped	04800(17.07.01/and.,	0800-10-000-04	Parallel Order
1 Macorda				Bhow Records: 28 -	101 - C O D

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。

🗵 81 : [Image Update Status]

E Cisco DNA Center	Image Update	\$ Q O O A
Done! Image update	scheduled.	
Successfully scheduled distribution	n	
What's Next?		
Image Update Status		
Image Repository	i i i i i i i i i i i i i i i i i i i	
 Workflows Home 		3

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

E Cisco DNA Center	Activities / Tasks		± Q (DCA
	Audit Logs Taxes Work Items			
SUMMARY V Status (4) Upcoming In Progress Success Failed	Q Search by description OS UPDATE A dmin c9800cpdate Starts: Jun 12, 2023 2:00 PM Status: ● In Progress	9	Sort by - Update Time: Most Recent to Oldest 🗸	Lest updated 2:05:12 PM

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

E Cisco DNA Center	()	Activities / Tasks	* 0 0 0 0
BUNNARY	Q. Search by description	os urpane c9800update Silves au 24, 2021 11.29 AM Status: I In Progress Last updated	×
 Status DO C Speciming C In Progress 	O os uroars A edmin c\$800.pdate	Devices (1) 6e s	o Image Codate Status
C Relect	Courts Alcours Suptem Wrekly backup of contg sofiections for	lapader Sanker 🚺 🔮 to Program (?) 🦹 Weiting (0) 💿 Alberhel (0) 🔍 Sances (0) 🔮 Falces (0) Sence Name Bence Name	
C 24 hours C 2 days	Starte: Feb 5, 2023 3:00 PM Law Ends: Neon/ Report: Every mont Becurrag	C8800-40-CVD capities.los d (10.4.60.2) Writeves Controller of 34,2023 17.08.03.0.4111 Activating C8801-40-Uni	vertal
1 Categories (H1) ~ Recurring C Show	PELD NOTICES Suptem Bcan network for Field Notices Starse Feb 24, 2013 9.31 PM Law		

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。



- ・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)。
 - Catalyst9800-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

Primary C9800		
WLC-9800-2.cisco.local		Redundancy Management IP*
Select Secondary C9800		
WLC-9800-1.cisco.local	~	Peer Redundancy Management IP*
Netmask*		

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	值
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

High Availability	∠ s q ⊞ ¢ ⊗ ⊯ ×
REDUNDANCY SUMMARY	
Primary C9800 Secondary C9800: Unit MAC: ① Redundancy State: Mobility MAC: ① Sync Status: ① Disable HA	WLC-9800-2.cisco.local WLC-9800-1.cisco.local d4:c9:3c:0a:e3:00 SSO d4:c9:3c:0a:e3:00 Complete

(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

E Cisco DNA Center	Provision / Ne	stwork Devices / Provision Devices	* 9 0 0
Network Devices / Provision Devices			
Asign Site (2) Configuration	(3) Motel Configuration (4) Advanced Configuration	5 Summery	
Bend Fairbor TTM243501KB, TTM234305MP	Develop C9800-40-CVD.cagehab.focal	🖓 Gronari 720 Millionau Banding 23	

 ・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。

Cancel Next

- 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	Provision / Network	Devices / Provision Devices	\$ Q @ @ Q
Nativent Devices / Provider Devices		Managed AP Location ①	×
1 Assign Site 2 Configs	ration 3 Model Configuration 4 Advanced Configuration 5) 51	
C9800-40-CVD.cagelab.local	Setal Number Devices TTM243505KB, TTM234305MY C0800-40-CVD.cagelab.local	Q. Search Herarchy	V Saaron Help
	Skip AP Provision Assign Interface rearries have Rearries Group have VLAV D		
	employee 🔇 - 160) # Tennox) ∰ Sanjose 7	
	Rolling AP Upgrade AP Recot Percentage C Enable 25 ~ 0		
			Gancel Save

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	值
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

with Devices / Provision Devices							
Assign Stee 2 Contigu	ration 3 Model Configuration	Advanced Configuration 5	lummery				
	TTM243505KB, TTM234305MK	C9800-40-CVD.cagelab.local	O Active 5	ain WLC 🔕	dt Managing 3 Prin	nary location(s)	
	Skip AP Provision ()		() Ancher		@ Select Secondar	y Managed AP Locations	
	Assign Interface						
	Interface None Enterface Group Non	VLANID R	* Address	Galennig (P.Add	Nots Baber	t Macaŭ+ tritoj	
	employee 💿 🛛 -	160	10.4.160.2 🕑	10.4.160.1	<u> </u>	B	
	1 Becorils		Stopa Rec	orde: <mark>24 v</mark>	1 - 1	< 0 >	
	Rolling AP Upgrade						
	AP Related Persentage	~ 0					

- (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。

E Cisco DNA Center		Provision / Network Devices / Provision Devices	* 0 0 4
Network Devices / Provision Devices			
1) Assign Site 2 Config	guration (3) Model Configuration (4 Advanced Configuration 5 Summary	
C9800-40-CVD.cagelab.l	(i) Default AP Profile (Default_AP_Profi	le_Akreos/default-ap-profile) will be applied to all Cisco DNA Center generated AP Groups/Site Tags	×
	Y Device Details		
	Device Name:	C9800-40-CVD.cagelab.local	
	Platform ld:	C9800-40-K9, C9800-40-K9	
	Device IP:	10.4.50.2	
	Device Location:	Global/US/Milpitas/Building 23	
	Device Role:	Active Main WLC	
	Associated Anchor device(s)	C9800-CL-CVD cagelab.local (10.4.48.153)	
	✓ Network Setting		
	NTP Server:	10.4.48.17	Network Setting
	AAA Client Server:	AAA client/endpoint settings are pushed as per the configuration added for each Managed AP location per WLAN.	
		MARANO, Do not use "admin" as the username for your device CU credentials, if you are using OE as your AAA server. If you do, this can result in you not being able to login to your devices.	
	DNS Domain Name:	cagelab.local	
	DNS Primary Server:	10.4.48.9	
	Cisco TrustSec (CTS) Credentials	No	
	Wireless Streaming Telemetry	Yes	
	Syslog Server	Cisco DNA Center	
	Netflow Collector	Cisco DNA Center	

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。

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

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

 ⁽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。

Cisco Cisco C	atalyst 9800-4	40 Wireless Controller	Welcome assurance	***	8 ¢ % Ø	C Search APs and C	ienta Q	eedback _w ^a ()
Q. Search Menu Items	Configuration	on • > Tags & Profiles • > 1	WLANs	Dirable WEAN				MI AN Mirard
Dashboard	Selected WL	ANs:0						
(C) Monitoring	> D Status	Name	T ID		Y SSID	Ŧ	Security	Ŧ
Configuration		cvduser lab3quest profile	1		cvduser lab3quest		[open] [open].MAC Filtering	
C Licensing		lab3employee_profile	▶ 18		lab3employee		[WPA2][802.1x][AES]	1 - 3 of 3 items
X Troubleshooting								
Walk Me Through 3								

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。

¢	cisco Ci	isco (Catalys	9800-4	0 Wireless Contr	roller Welcome assurance	* * A B ¢		Search APs and Clients Q	EFeedback 🖌
Q	Search Menu Items			onfiguration	Tags & Profile	es > Policy				
-	Dashboard			+ Add	× Delete	Clone				
\odot	Monitoring		>	Admin Status	Associated 0 T Policy Tags	Policy Profile Name	г	Description		т
				•		cvdopen		cvd open		
2			>	•		lab3guest_profile		lab3guest_pro	file	
ŝ	Administration			•		lab3employee_profile		lab3employee	_profile	
\$	Administration		1	•		default-policy-profile		default policy	profile	
C	Licensing			+ + 1	F F 10 V					1 - 4 of 4 items
×	Troubleshooting									
	Walk Me Through >									

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。

Clisco DNA Center Provisio Network Devices / Provision Devices		sion / Network Devices / Provision Devices	* Q © C Q ×	
		Managed AP Location ()		
1 Assign Site 2 Configu	uration (3) Model Configuration (4) Advance	ed Configuration		
C9800-CL-CVD.cagelab.local	Serial Number Device 9R106ZT7FLY C9800	s Q. Search Hierarchy o-CL-CVD.cagelab.locs	Search Help	
	In case of change in profile attributes, re-provisioni Skip AP Provision Assign Guest SSIDs to DMZ site	ng of respective Foreig		
	Interface Name - Interface Group Name Vu	> □ iii Building 24 AN ID > □ iii NewYork > □ iii Sanjose		
	1 Records			
	Rolling AP Upgrade			
	Enable 25 V 🕑		Cancel Save	

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

E Cisco DNA Center	Provision / Network Devices / Provision Devices			* Q @ C A		
Auron Da 2 Canton	natura (3) Manual Constructions (4)	Advanced Contraction (5) 1			
C9800-CL-CV0.cageius.boos	Serial Kanser Serial Kanser Serial Kanser I to case of change in profile attributes, re-pr Disp AP Provision ©	Bevices C9800-CL-CVO capetab.local	MAE Inve Active Marin Anchor controller is required to configur	Managet AP 8 WLC () & Managing In WLAN and VLAN Interface()	ustan)a) © 3 Anchor location(s) 0.	
	Assign Guest SSIDs to DMZ site	VLAND	Patron	Galman P Address	LAD Part Number	Robert Machine Level
	guest-dmz 🕥 🛛 -	125	10.4.125.2	10.4.125.1	N/A	24
	3 Records			Show Record	1 25 × 1-1	< 0 >
	Rolling AP Upgrade					
	🖹 faste 25 🗸	0				

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。

E Cisco DNA Cent	er	Provision / Network Devices / Provision Devices	\$ Q @ C Q
Nerwork Devices / Provision Dev	Ceefigurasian 3	Model Configuration (4) Advanced Configuration (5) Surrowy	
Device Select devices to IE Model Cord Pixt Q. Starch	S Ig parameters Draw <u>At</u> ~	Model Config not selected Salect any one of the Matel Config from " Devices" Panel.	
			Cancel Next

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。

Cisco Catal	lyst 9800-CL Wireless Con Welc	troller ome assurance 🐐 🕫 🧟 🖺 🌣 🔯 (C Search APs and Clerits Q EF	edback 🖌 🖗
Q. Search Menu Items	Configuration • > Tags & Profile	s* > Policy		
Dashboard	Admin T Associated O T		Developing	
Configuration	Catus Poincy Tags	lab3guest_profile	lab3guest_profile	T
Administration	· · · 1 · · · 10 ·	detaur-poicy-prome	detault boxcy brone	1 - 2 of 2 items
C Licensing				
Troubleshooting				
Walk Me Through)				

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。

	Sisco Cataly	yst 9800-40	Wireless Controller Weld	come assurance	* * & * *	000	Search APs and Clients Q	Feedback
Q. Search Menu Items		Configuration •	> Tags & Profiles * > Polic	SY				
Dashboard		+ Add	X Delete					
	,	Admin Y Status	Associated 0 T Policy Tags Policy Profil	le Name		T Description		т
	1921 - 1925 1930 - 1930 - 1930	0 0	lab3guest5	profile		lab3guest5_p	vofile	
Configuration	>	0 0	lab3branch5	5_profile		lab3branch5	profile	
Administration	,	00	default-poli	cy-profile		default policy	profile	1 - 3 of 3 items
Licensing								
Walk Mc Through 3								

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)

a Dashboard	Globa	I Configuration	Peer Config	uration								
Monitoring	, ~	Mobility Peer	Configurati	on								
	› [+ Add	Delete C									
Administration	>	MAC T Address	IP T Address	Public T	Group T Name	Multicast Y IPv4	Multicast T IPv6	Status	T P	мти 🔻	SSC Hash	Data
Licensing		3c13.cc95.30cb	10.4.50.2	N/A	default	0.0.0.0		N/A	N	A	4ca3029edad8d03c84d4d60312e63e594c2e15c	f N/A
	C	001e.bdee.d2ff	10.4.48.153	10.4.48.153	default	0.0.0.0	::	Up	■ 13	385		Disab
Troubleshooting		· · 1 ·	10 🗸								1 - 2 of 2 items	0
			10000000		120-240							

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)

Dashboard	Globa	I Configuration	Peer Config	guration									
) Monitoring	, ~	Mobility Peer	Configurat	ion									
	•	+ Add	Delate C										
Administration		MAC T Address	IP T Address	Public T IP	Group T Name	Multicast T IPv4	Multicast T IPv6	Status	Ŧ	PMTU 🝸	SSC Hash	Ŧ	Data Li Encrypt
Licensing		001e.bdee.d2ff	10.4.48.153	N/A	default	0.0.0.0		N/A	1	N/A	651185ed3f37489ecf26f0e05bd85d741a621	70	N/A
Licensing	(3c13.cc95.30cb	10.4.50.2 ==	10.4.50.2	default	0.0.0		Up	=	1385			Disable
Troubleshooting		· · 1 ·	10 🗸								1 - 2 of 2 it	ms	C

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

Q. Search Menu Items		Conf	iguration •	> Tags & Pro	Edit Policy Profile					
Dashboard				× Delete	General Access Policie	QOS and AVC	Mobility Adv	anced		
	,		Admin Y Status	Associated 0 Policy Tags	Mobility Anchors					
		0	۲	•	Export Anchor	0				
	,		0	<	Static IP Mobility	DISAB	ED			
Administration			0							
		0	0	•	Adding Mobility Anchors will ca and may result in loss of conne	use the enabled WLANs t ctivity for some clients.	o momentarily disable			
Licensing										
Licensing		- 14	1	F F 10						
Troubleshooting		н	< 1	P H 10	Drag and Drop/double click/c	lick on the arrow to add	/remove Anchors			
Troubleshooting		н	< 1	P P 10	Drag and Drop/double click/c Available (0)	lick on the arrow to add	/remove Anchors			
⁷ Troubleshooting		я	. 1	F F 10	Drag and Drop/double click/c Available (0) Anchor IP	Slick on the arrow to add	/remove Anchors elected (1) nchor IP	Anchor Priority		
* Troubleshooting		н	- 1	P P 10	Drag and Drop/double click/c Available (0) Anchor IP	Slick on the arrow to add	/remove Anchors elected (1) nchor IP 10.4.48.153	Anchor Priority Primary (1)	•	¢
Troubleshooting Walk Me Through 5		И	- 1	P P 10	Drag and Drop/double click/c Available (0) Anchor IP	click on the arrow to add	/remove Anchors alected (1) nchor IP 10.4.48.153	Anchor Priority Primary (1)	•	÷
Walk Me Through 1		н	< 1	F F 10	Drag and Drop/double click/c Available (0) Anchor IP No anchors availa	click on the arrow to add	/remove Anchors elected (1) nchor IP 10.4.48.153	Anchor Priority Primary (1)	•	¢
Troubleshooting		н	- 1	» # 10	Drag and Drop/double click/c Available (0) Anchor IP No anchors availa	click on the arrow to add	/remove Anchors elected (1) nchor IP 10.4.48.153	Anchor Priority Primary (1)	•	*

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

Cisco Catal Cisco Cat	vst 9800-CL Wireless Cor Configuration - > Tags & Prof - Add < Delete	ttroller Welcome admin Edit Policy Profile General Access Policies	QOS and AV	C Mobility	Search APs and Clients Q	X Feedback
Dashboard Image: Configuration Image: Configuration <td>Admin Y Associated Policy Tags O</td> <td>Mobility Anchors Export Anchor Static IP Mobility Adding Mobility Anchors will cause and may result in loss of connectiv Drag and Drop/double click/clich Available (1)</td> <td>the enabled WLAN ity for some clients.</td> <td>IBLED Is to momentarily dis dd/remove Anchor Selected (0)</td> <td>able</td> <td></td>	Admin Y Associated Policy Tags O	Mobility Anchors Export Anchor Static IP Mobility Adding Mobility Anchors will cause and may result in loss of connectiv Drag and Drop/double click/clich Available (1)	the enabled WLAN ity for some clients.	IBLED Is to momentarily dis dd/remove Anchor Selected (0)	able	
(Walk Me Through)		Anchor IP 10.4.50.2 Cancel	•	Anchor IP	Anchor Priority Anchors not assigned	Update & Apply to Device

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

E Cisco DNA Center		Provision / Network Devices / Provision Devices	\$ Q @ C 4
Network Courses / Provision Devices			
) Assign Site (2) Configuration (3 Surmary		
Betal Number RJC244117V2	Devices mi123+floor1-ap1	$\frac{1}{200}$ cal/05/Mioranibulising 23/Foor 1 \times	

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。

Cancel Next

図 *94 : AP*のプロビジョニングステップ 2 : 設定

	ar i por para						
Assign Site	2 Configuration (3) Summa	9					
Zones and SSIDs	are listed from Provisioned Wireless p	rofile(s) for each Access point.	For newly added Zones an	d SSIDs, Please provision	Controller prior to A	Access point provision.	×
Setal Number	Device Name	AP Zour Name	IF Posta	labiliguest, labil	lemployee		
FJC24411TV2	miQ3-8ppr1-ap1	Not Application	- TYPICAL	~ 2			

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

E Cisco DNA Con	tor	Provision / Network Device	es / Provision Devices		* 9 0 0 4
Network Devices / Provides Dev	Configuration 3 Summary				
miZ3-floor1-ap1	Device Details				
	Device Name: Sarial Namber: Mac Adorese: Device Location: Y AP Zone Details	mi23-fbor1-ap1 RiC244117V2 54:8xbam06xb0 Global/USIMIckas@unding 23/Floor 1			
	AP Zone Name V RF Profile Decails RF Profile Name TYPICAL Role Type	default-ooste 2.40es	stre	6046	
	Parent Profile Status	RF Profile Cetalls TVPICAL Enabled	TYPICAL Enabled	TVPICAL, Enabled	
	DCA Channels	7, 6, 11	36, 40, 44, 48, 52, 56, 60, 6 4, 149, 153, 157, 161	5, 21, 37, 53, 69, 85, 101, 117, 133, 1 49, 165, 181, 197, 213, 229	
	Channel Width	20 MHz	Best	Best	

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

Search Menu Items	Policy Site RF AP		
Dashboard Monitoring	+ Add × Delete		
	Policy Tag Name	▼ Description	
	C cvdopen	cvd open	
Administration >	default-policy-tag	default policy-tag	
	PT_Milpi_Build_Floor1_c9844	PolicyTagName PT_MIpi_Build_Floor1_c9	
Licensing	H H 1 H 10 V		1 - 3 of 3 item
Troubleshooting			

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

cisco Cisco Cisco Search Mercy Jerres	co Catalyst 9800-40 Wireless Controller	Welcome assurance A Tags Edit Policy Tag	C C C Search APs and Clients Q	E Feedback
Dashboard	Policy Site RF AP	Changes may result in loss of co	nnectivity for some clients that are associated to APs with this f	Policy Tag.
Configuration	Policy Tag Name cvdopen default-policy-tag PT Mini Build Eport c9844	Description PolicyTagName WLAN-POLICY Maps: 2	PT_Mipl	
C Licensing		+ Add X Delete	Y Policy Profile	Ŧ
		lab3guest_profile	lab3guest_profile lab3employee_profile	1 - 2 of 2 items
Walk Me Through 1		> RLAN-POLICY Maps: 0		, 1 - 6 yet & months
		D Cancel	B	Update & Apply to Device

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

Q. Search Menu Items	Configuration * > Tags & Profiles * > Tags	Edit RF Tag	×
Dashboard	Policy Site RF AP	A Changes may result in	loss of connectivity for clients that are associated to APs with this RF Tag.
	RF Tag Name	Name*	TYPICAL Show slot configuration
Administration	default-rf-tag	6 GHz Band RF Profile 5 GHz Band RF Profile	default-rf-profile v 22 Typical_Client_De v 22
C Licensing		2.4 GHz Band RF Profile	Typical_Client_De_ V
Walk Me Through >			
		Cancel	Update & Apply to Device

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

Cisco Cata	lyst 9800-40 Wireless	s Controller Welcome assura	nce 🖌 🏶 🗛 🛙		Search APs and Clients Q	Feedback x* 🗭
Q. Search Menu Items	Configuration • > Tags	Edit Site Tag				×
Dashboard	Policy Site RF	Name*	ST_Milpi_Building_e3b46			
(2) Monitoring >	+ Add 📔 🗆 Do	Description	Site Tag ST_Milpi_Buildin	-		
≪ Configuration →	Site Tag Name default-site-tag	AP Join Profile Fabric Control Plane Name	default-ap-profile 👻	8		
(Ô) Administration →	ST_Milpi_Building	Enable Local Site	Ø			
C Licensing		Load* (i)	0			
X Troubleshooting						
Walk Me Through >						
		Cancel				Update & Apply to Device

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

Q. Search Menu Items	Config	uration * > Tags 8	Profiles * > T	ags						
Dashboard	Policy	Site RF	AP							
) Monitoring	> Tag	Source Static	Location	Filter						
	> Nur	+ Add Del	ate gs selected : 0			C Select Fi	le	0 4	Upload File	
Administration	> C	AP MAC Address		Ŧ	Policy Tag Name	Ŧ	Site Tag Name	٦	RF Tag Name	т
Lissacina	0	1416.9d7c.13ec			PT_Mipi_Build_Floor1_c9844		ST_Milpi_Building_e3b46_0)	TYPICAL	
Licensing	C	34b8.8315.94ec			cvdopen		default-site-tag		default-rf-tag	
Troubleshooting	C	34b8.8319.5c88			cvdopen		default-site-tag		default-rf-tag	
	C	8411.4798.1118			cvdopen		default-site-tag		default-rf-tag	
		4 1 F F	10 🗸							1 - 4 of 4 items

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

Cisco DNA Center	Design / Network Hierarchy	* Q @ & A
Q. Search Hierarchy Search Help ∽ & Global	Devices Overlays APs Sensors	Show distances Close Save
 슈 US 슈 Mipitas H Builting 23 	Add APs Remove APs Assign Planned APs Step 2: Move cursor to desired position on	Edit AP ×
 Or Boar1 ** Or Floor 2 Jift Building 24 Jift Building 24 Jift NewYork Jift Sanjose 	Remove Planed AP Autoplace Planed AP	Position by 3 points 2 walls Remove AP Name mil23-floor1-ap1 AP Name distribution AP Name distribution AP Name distribution AA Monser AP Bloot AP Height (1) distribution AP Height (1) distribution AP Height (1) distribution A (1) 34.17 10.00 AP Height (1) distribution B02.11b/g 802.11a B02.11a Anternals Internal-B130-2.4.GHz V Height (1)300 omet interess (gain: 55bi) Ammution Ammution Develop V

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、APRSSI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、2.4GHzカバレッジ、5GHzカバレッジ、または2.4GHz と5GHz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

E Cisco DNA Center	Prov	sion / Network Devices / Provision Devices	\$ Q @ C A
Network Devices / Provision Devices		Choose a site	×
1 Assign Site 2 Configuration	3 Model Configuration 4 Advanced Con	nfguration 5 Su	
Server Number TTM-224801QK	Devcss C9800-Flex-CVD	Q. Search Herarchy	Seath No
			Cancel Save

(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。

E Cisco DNA Cent	er	Provision / Network D	evices / Provision Devices		* 0 0 0 4
Network Devices / Provision Dev 1 Assign Site 2	Configuration 3 Model Configuration	4 Advanced Configuration 5	Summary		
C9800-Flex-CVD	Serial Number TTM224801QX	Devices C9800-Flex-CVD	WLC Role Active Main WLC Active Main WLC Active	Managed AP location(s) () Managing & Primary location(s) Select Secondary Managed AP Locations	
	Assign Interface	Name VLAN ID IP - 100	Address Gateway IP Address Subne	e Mask(m bits)	
	branchguest- dmz O -	110	Show Records: 25 y 1 - 2	< 0 >	
	Rolling AP Upgrade			Cancel	Next

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。

フィールド	值
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

表 29:エンタープライズ ワイヤレスコントローラの設定

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

Assess the	Contraction (3) Market Contraction (A) Attacent Conference (5) a			
C9800-Flex-CVD	Serial Number TTM2248010X	Devices C3800-Fiex-CVD	WLC Role Active Main WLC Active Main WLC Active Main WLC	Managed AP location(s) A Managing 4 Primary location(s) A Select Secondary Managed AP Locations	
	Assign Interface				
	Interface Name Interface Group Na	ime VLAN ID IP /	Address Gateway IP Address S	ubnet Mask(in bits)	
	branchemployee _	100			
	branchguest- dmz 💽	110			
	2 Records		Show Records: 25 🗸 1 - 2	< 0 >	

- 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。

Cisco DNA Center				Provision / Network Devices / Provision Device	19	* 9 0 0 0
neort Devices / Provision Devices			~	~		
Assign Sas (2) Costig	22508 C	Mode	i Configuration 🗳 Advan	cel Contgaration 5 Summary		
Devices			Flex Configuration - M	odel Configs		
n devices to fill Model Config para	Show At		Cesign Name +	First Profile Name	Description	
C9800-Flax-CVD (1)		~	branch	FP_NewYn_Branc_5b486	-	Edt View
Flex Configuration				Showing 1	of 1	
						Cancel Next

- **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。

E Cisco DNA Cente	r	Provision / Netwo	rk Devices / Provision Device	\$		± Q ⊕ ∆	4
Network Devices / Provision Devic	**						
1 Assign Site 2	Configuration 3 Model Configuration (4 Advanced Configuration	Summary				
C9800-Flex-CVD	VAAN 00 Name: VLAN 00 Seme: VLAN 00 * Remote Teleworker Settings * Model Configs Cepating	Preview Flex Configuration IP Overap Flex Profile Name	Yes FP_NewYo_Branc_50486	×			
	Pex Configuration			Close	tane Iranc_50485		
	2 Records						

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

Cisco Cis	sco Cataly	/st 98	300-4	0 Wireless Controller	Welcome	assurance	* *	•	8	0000	Search APs and Cl		eedback 🖉 🕪
Q. Search Menu Items		Confi	iguratio	Tags & Profiles * > N	VLANs								
Dashboard		+	Add	X Delete 🔁 Cione	Ena	ble WLAN							WLAN Wizard
	>	Selec	ted WLA	Ns : 0									
20		0	Status	Name	т	ID			Ŧ	SSID	т	Security	т
~ Consiguration	2		0	lab3guest5_profile		17				lab3guest5		[open],MAC Filtering	
Administration	>		0	lab3branch5_profile		18				lab3branch5		[WPA2][802.1x][AES]	
C Licensing		14	- 1	н н 10 т									1 - 2 of 2 items
💥 Troubleshooting													
Walk Me Through >	8												

(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

	o Cataly	st 9	800-40 \	Wireless Con	troller Welcome assurance	 A 5 ¢	3	0 0	Search APs and Clients	C Feedback	~ 🕩
Q, Search Menu Items		Con	figuration •	> Tags & Prof	iles > Policy						
Dashboard		+	Add	Associated 0	Clone						
Monitoring	>		Status	Policy Tags	Policy Profile Name	Ŧ	Desc	cription			Ŧ
			0		lab3guest5_profile		lab3	guest5_prof	Se .		
Configuration	>		0		lab3branch5_profile		lab3i	branch5_pro	ofile		
O Administration	>	0	0	10	default-policy-profile		defa	uit policy pro	ofile	1 - 3 of	3 items
C Licensing											
X Troubleshooting											
Walk Me Through 3											

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

Cisco	Cisco Cata	yst 9800-40 Wireless Controller Welcome assurance	#	▲ ● ◆ ● ● ● ○ Search APs and Cleres Q	EFeedback 🖌
Q. Search Menu Iter	na	Configuration • > Tags & Profiles • > Flex			
Dashboard		+ Add × Delete	_	-	
Monitoring	>	Flex Profile Name FP_NewYo_Branc_5b486	Ť	Description	Ŧ
	,	default-flex-profile		default flex profile	
() Administration		10 -			1 - 2 of 2 items
C Licensing					
💥 Troubleshooti	ng				
	-01				
Walk Me Through	2				
Walk Me Through	D				

図 110: [Edit Flex Profile] ダイアログボックス

Q. Search Menu Items	Configuration • >	Edit Flex Profile				*
Dashboard Monitoring Configuration Administration Licensing Troubleshooting	Fiex Profile N Fiex Profile N FP_NewYo	General Local Ar Name* Description Native VLAN ID HTTP Praxy Port HTTP-Praxy IP Address CTS Policy	Policy ACL PP_NewYb_Branc_5b48 Enter Description 0 0.0.0.0	VLAN DNS Layer Security Faltback Radio Shut Flex Resilient ARP Caching Efficient image Upgrade OfficeExtend AP Join Minimum Latency IP Overlan		
Walk Me Through 2		Inline Tagging SGACL Enforcement CTS Profile Name	default-sxp-profile x v	mDNS Flex Profile PMK Propagation	Search or Select	o Device

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。

Cancel Next

図 112: ワイヤレスプロファイルに基づく N+1 AP SSID

	e Devices								
Assign Site	2 Configuration 3 Summa	~							
ones and SSIDs a	are lated from Provisioned Wireless p	esfla(x) for each Access point	For newly added	Zones and 55	Cs, Please provis	sion Controller prior	to Access point prov	sion.	×
or Number	Dovice Name	AP Zona Nami		18 Profile	lab3gvest5.	, lab3tranch5			
24411705	AP1416.907C.16F8	Not Applicable		TYPICAL	Ψ.	1			

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

- Oraco Drivi Certe	**	FIGHTING FIREWORK DEVICES FI	Contract Partners	¥ < 0 0 0
Network Deerges / Provision Dear				
1 Assign Site (2)	Configuration 3 Summary			
AP1416.9070.16F8	✓ Device Details			
	Device Name:	AP1416.9D7C.16F8		
	Senal Number:	FJC244117Q5		
	Mac Address	54.8x/ba #:1e:20		
	Device Location:	Global/US/NewYork/Branch S/Roor 2		
	Y AP Zone Details			
	AP Zone Name	default-zone		
	✓ RF Profile Details			
	RF Profile Name: TYPICAL			
	Radio Type	1.4040	50+0	
	Pwart Profile	TYPICAL	TYPICAL	
	Status	Enabled	Enabled	
	DCA Channels	1, 6, 11	36, 60, 44, 48, 52, 56, 60,	64, 149, 153, 157, 161
	Channel Width	20 MHz	Best	
				Concel Next

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

E Cisco DNA Center		Activities / Tasks dr Q	000
Clisco DNA Center Summune Su	C. Search by description Providiate Annin Providiate P	Acchildres / Tasks	C C C
Show	Provision Device Provisional Unifield APria) in Sin Stans Jul 25, 2023 2 53 P Provision Beneficial APria Provision Device Historianic (2600–CVD–Nation States) La 36, 3035 5 6 4 p		

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

E Cisco DNA Center		Ac	tivities / Tasks		\$ Q	000
SUMMARY	Q. Search by description	Provision Provision Device Stats: JA 25, 2023 3:43 PM	Completed: Jul 25, 2023 3:4	e PM Status: 🥥 Buccess	Last updated: 3.44.16 PM	C Refresh
 Status (4) Lipusming Is Program Statemen Falled Status Jatours Jatours Jatours Zathours Zathours Conteportes (41) Stouw 	Production Ar 25, 2023 3:43 P Provision Devide Provision Provision Provisione Pr		Conservation from numbers & interest to d + Jul 20, 2023 3:43 PM + Jul 25, 2023 3:43 PM + Jul 25, 2023 3:43 PM - Jul 25, 2023 3:43 PM Conservation from numbers & interest to d + Jul 25, 2023 3:43 PM + Jul 25, 2023 3:43 PM + Jul 25, 2023 3:43 PM	Instea Insex and duployment of configuration Successfully progared device lock in rts flaw Deploying configuration on the device C9800 - OVD ageletis local (16.6.48,150), Configured operation will be to Modify AP cont Instead operation will be to Modify AP cont Successfully arguined device configuration Deploying configuration on the device C9800- Nation Logarizatio Icoli (10.6.48,151),	Nos betals Success Paar Agunstons Success CVO	
Она	PROVISION & works Problem Device Research of the Total 3-54 in States	· Destroye	 An an, and 2.4.5 PM ent of Mediat Carefy 	Consignment operation like to its Modify of Coll No.11 MA, Modify AF Tag configurations, Add So occelligurations and Add Policy Tag configurato	SUCCESS	

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。

Dashboard All Access Points Monitoring Toul APs : 2 C Toul APs : 2 C Annie 1 APs AP Name 1 APs <li< th=""><th>Self-States in the self-</th><th></th><th>General Interface</th><th>High Availability</th><th>Inventory</th><th>ICap Advanced Support B</th><th>unde</th></li<>	Self-States in the self-		General Interface	High Availability	Inventory	ICap Advanced Support B	unde
Monitoring > Total APs : 2 > Primary Controller C9800-Plex-CVD 10.4.48.150 Administration > APrians 5000C16/6 Alia C94 Prianzy Controller C9800-CVD-Naka1 10.4.48.151 Licensing APrians 5000C16/6 Alia C94 APrians Controller C9800-CVD-Naka1 10.4.48.151 Troubleshooting > 6 GHz Radios > > > 2.4. GHz Radios > 2.4. GHz Radios	Deshboard	 All Access Points 		Nama		Management IP Address (IPv4/IPv6)	
Configuration > Administration > Administration > Licensing AP1416.9070.16F8 Troubleshoosing > > 6 GHz Radios > 5 GHz Radios > 2.4 GHz Radios	Monitoring	Total APs : 2	Primary Controller	C9800-Flex-CVD		10.4.48.150	
Administration Administratio Administration Administration Administration Adminis			Secondary Controller	C9800-CVD-Nolus1		10.4.48.151	
Licensing AP1418.507C.16FC_d_biat_OH AP1418.507C	Administration	AP1416.9D7C.16F8 duint C91	Tertiary Controller				
Troubleshooting Froubleshooting 6 GHz Radios 5 GHz Radios 5 2.4 GHz Radios	Licensing	AP1416.9D7C.16FC	AP failover priority	Low *			
Role Mo Towards 20 > 6 GHz Radios > 5 GHz Radios > 2.4 GHz Radios	Troubleshooting	H H 1 H H 10 V					
Kink Mit Through 3) > 5 GHz Radios > 2.4 GHz Radios		> 6 GHz Radios					
> 2.4 GHz Radios	Work Mr. Through 1	> 5 GHz Radios					
		> 2.4 GHz Radios					

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

Q, Search Monu Items	Configuration * > Wireless * > A	Edit AP				×
Deshboard Monitoring Configuration Administration Licensing Troubleshooting	All Access Points Totel APs : 2 AP Name AP A1416.507C.16F6 Alid C91 AP1416.507C.16F6 Alid C91 C91 AP1416.507C.16F6 Alid C91 D	General Interface Primary Controller Secondary Controller Tertiary Controller AP failower priority	High Availability Name C9800-Files-CVD O9800-CVD-Nplus1 C0800-CVD-Nplus1 C0800-CVD-Nplus1	Inventory	ICap Advanced Sup Management IP Address (IPv4/IPv6) 10.4.48.150 10.4.48.151	oort Bundle
	> 6 GHz Radios					1
Wak Me Through 3	> 5 GHz Radios					
	> 2.4 GHz Radios					
	> Dual-Band Radios	D Cancel				Update & Apply to Device

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

E Cisco DNA Center	Provision /	Network Devices / Provision	Devices	* Q © C A
Network Devices / Provision Devices		Choose a	site	×
Assign Size Configuration Serial Number TTM2224801MD	3 Model Configuration 4 Advanced Configuratio Devices C0800-CVID-Nplan1	ි 5 50 මී 201 ද මී 201 ර මී 000 ර මී 000 ර මී 000 ර මී 000	h Hierarchy al 5 Migotas NewYork 4 Benech 6	Search Hep
		> @	W Floor 1 W Floor 2 W Floor 3 Sanjose	
				Cancel Save

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

E Cisco DNA Center		Provision / Network Devi	ces / Provision Devices		* 0 0 0
Network Devices / Provision Device	nfiguration 3 Model Configuration	4 Advanced Configuration 5 Sur	nmary		
C9800-CVD-Nplus1	Serial Number TTM324801MD	Devices C9800-CVD-Aplus1	WLC flow Active Main WLC Active Anchor	Managed AP location(s) Select Primary Managed AP Locations Managing 4 Secondary location(s)	
	Assign Interface Interface Name Interface Name Interface Oroup Dranchemployee	Name VLANIO IPAdo - 100	tress Gateway IP Address 5	ubnert Mask(in bits)	
	branchguest- dmz 🕢	110			
	2 Records	Show Records	a <u>35 ∨</u> 1+2	< 0 >	
	Rolling AP Upgrade			Can	net Next

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

E Cisco DNA Cente	or	Provision / Network Dev	ices / Provision Devices	* Q @ C Q
Network Devices / Provision Devic	**		Managed AP Location ①	×
C9800-CVD-Hphus1	Assign Interface Interface Interface Interface Dranchamployee Dranchamployee 2 Records 2 Records	VLAN ID IP AC * 100 110 Show Record	 general Heararchy c) the Global (4) c) the US c) the Minches c) the NewYork c) the NewYork c) the Froor 1 c) the Froor 2 c) the Froor 3 c) the Samjose 	⊽ Search Neb
	Rolling AP Upgrade			Cancel Save

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

E Cisco DNA Center			Provision / Network Devices / Provision Devices		* Q @ @ 4
neork Devices / Provision Devices					
Assign Site 2 Configuration	3 Mor	del Configuration	ced Configuration 5 Summary		
Devices		Flex Configuration - M	odel Configs		
t devices to fill Model Config parameter Sho	5	V Filter			
Search At	~	Design Name +	Flex Profile Name	Description	
C9800-CVD-Nplus1 (1)	v	branch	FP_NewYo_Branc_5b486		Edit View
Flex Configuration			Showing 1 of 1		
					Cancel Next

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。

E Cisco DNA Cente	er	Provision / Network Devices / Provision Devices	* Q @ C A
Network Devices / Provision Devic	*1		
(1) Assign Site (2) (C9800-CVD-Nplus1	Configuration 3 Model Configuration Controller Certificates Netflow Application Telemetry	(4) Advanced Configuration 5 Summary Yes Disabled	
	 SSID (branch5) 		
	55ID Name	lab3guest5	
	WLAN Profile Name	lab3guest5_profile	
	Policy Profile Name	lab3guest5_profile	
	Sensor	No	
	Admin Status:	Enabled	
	Broadcast Enabled:	Yes	
	Type:	Guest	
	Securey:	open	
	Fast Transition:	Adaptive	
	Traffic Type:	Best Effort (Silver)	
	Fabric Enabled:	No 🛈	
	AAA Override	Yes	
	Fast Lane enabled:	No	
	Mac Filtering Enabled:	Yes	
	Flex Connect enabled:	Yes	
	Local to VLAN ID:	110	
	Paraul DPAH Prinate	Alte	

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

etwork Devices / Provision Device	15		Provision Device
Assign Size 2 C	ne mingurasion (3) Model Configuration Controller Certificates Nettiow Application Telemetry SSID (branch5) SSID Name WLNN Profile Name Policy Profile Name Seaso Admin Status: Broadcast Enabled: Type: Securit: East Transition: Traffic Type: Fast Transition: Traffic Type: Fast Cransition:	Advanced Configuration 5 Surreary Ves Disabled hab3guest5 hab3guest5_profile hab3guest5_profile hab3guest5_profile hab3guest5_profile babded Yes Guest open Adaptive Best Effort (Silver) No © Yes	Provision Device This workflow supports enhanced visibility into the generated configuration and incomposed on configuration. The settings for this can be viewed and modified in system + 3 settings + Configuration Visibility and Control Now Configuration Settings - Configuration Visibility and Control Now Configuration Provide the latter used to deploy on satisfied devices. View status in Work Items Tax Items Provision Device
	Fast Lane enabled: Mac Filtering Enabled:	No Yes	
	Flex Connect enabled: Local to VLAN ID:	Yes 110	

- 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

Operation	Policy Client Egress	Policy Profile	Policy Client Ingress	Auto
	· · · · · , · · · · · · · · · · · · · ·	,	· · · · · · · · · · · · · · · · · · ·	
UPDATE		lab3guest5_profile		ENM
UPDATE		lab3branch5_profile		ENM
	S	howing 2 of 2		
WLAN Configur	ration			
Operation	WLAN Name	WLAN Profile	WLAN Id	
CREATE	lab3guest5	lab3guest5_profile	17	
CREATE	lab3branch5	lab3branch5_profile	18	
	SI	howing 2 of 2		
Interface Confi	guration			
Operation	Interface IP Address	Interface Name	Interface VLAN Id	
CREATE	0.0.0.0	branchguest-dmz	110	

図 126 : N+1 プロビジョニングステータス:パート 3

Operation	Flex Profile Name	Native Vlanid	FlexProfileConfig.homeApEnab
CREATE	FP_NewYo_Branc_5b486	90	false
	Showing 1	of 1	
eWLC AAA Con	figurations		
Operation	Server Group Name		Protocol
CREATE	dnac-network-taca	ics-group	TACACS_PLUS
CREATE	dnac-rGrp-lab3bra c82a1739	nch-	RADIUS
CREATE	dnac-rGrp-lab3gue 2c41ebf1	est5-	RADIUS
CREATE	dnac-acct-lab3gue 2c41ebf1	est5~	RADIUS
	Showing 4	of 4	

図 127 : N+1 プロビジョニングステータス:パート 4

Operation	PreAuthGuestACLConfig.reapAclName	
CREATE	DNAC_ACL_WEBAUTH_REDIRECT	
	Showing 1 of 1	
Policy Tag Configurat	ion	
Operation	Policy Tag Name	
CREATE	PT_NewYo_Branc_Floor1_64cf5	
	Showing 1 of 1	
Policy Profile Configu	ration	
Operation	WLAN Policy Name	
CREATE	lab3guest5_profile	
CREATE	lab3branch5_profile	
	Showing 2 of 2	
	Operation CREATE Policy Tag Configurat Operation CREATE Policy Profile Configurat Operation CREATE CREATE CREATE CREATE	Operation PreAuthGuestACLConfig.reapAcIName CREATE DNAC_ACL_WEBAUTH_REDIRECT Showing 1 of 1 Policy Tag Configuration Operation Policy Tag Configuration CREATE PT_NewYo_Branc_Floor1_64cf5 Showing 1 of 1 Policy Profile Configuration Operation Operation VLAN Policy Name CREATE Iab3guest5_profile CREATE Iab3branch5_profile Showing 2 of 2

図 128: N+1 プロビジョニングのステータス:パート5

operation	to reg tonic		10 11000 (1000)	
CREATE	TYPICAL	Typical_Client_Density_	rf_5gh Typical_Client	_Density
		Showing 1 of 1		
Policy Profile	UDN Properties			
Operation	Unicast Stat	us UDN Status	WLAN Policy Name	
CREATE	false	false	lab3guest5_profile	
CREATE	false	false	lab3branch5_profile	
		Showing 2 of 2		
Advanced WI	AN Configuration			
Provanceu vit.	Neighbor List	Directed Multicast Service	Client User Idle timeout	BSS I
Operation				and the second sec
Operation	true	true	300	true

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

SUCCESS View Details	Deployment of network intent
SUCCESS Hide Details	Deployment of Model Config
SUCCESS guration: Deployed configuration on the device.	Deployment of Model Config • Jul 25, 2023 2:25 PM
SUCCESS	Deployment of network intent(templates) Click on view details for the deployment of

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

Cisco DNA Center	Design /	Network Profiles		* Q @ C A
				🕒 Add Profile
Q Search Table				
Profile Name +	Type	Sites	Action	
branch5	Wireless	6	Edit Delete	
CagelabProfile	Wireless	Assign Site	Edit Delete	
corporate	Wireless	2	Edit Delete	

 [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

E Cisco DNA Center		De	sign / Network Profiles / Wireless	* 2 0 0 0
Network Profiles / Wireless 2. Define Templates in Templates Hub (optiona 3. Define Model Configurational Model Configuration)	() Templates Hub C			
Profile Name branch5				
lite:5 sites				
rofile Type: wian				
SSIDs AP Zones Model Configs	Templates Advanced Settin	as V		
the network profile will be applied to AP and yo AP zones will not be applicable to AP in Plug and AP zones will not be applicable to AP in Plug and the second	ou will need to manually select RF Profi nd Play flow.	le.		
AP Zone Name* sjcfloor1zone2		Ŷ	۲	
Device Tags				
Device Tags				
RF Profile*	Isb3branch5 (Flex) x			

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

rk Profiles / Wireless					
AP Zone Name* sjcfloor1zone2			v	۲	
Device Tags					
Contra lage	~				
HIGH	~	lab3branch5 (Flex) ×	~		
AP Zone Name*			v	0 💿	
aperiora recine r					
Device Tags					
Device Tags	~				
		55i0+			
RF Profile*	~	teo3guests (rilex) ×	~		
LOW					
LOW					
LOW .					

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.

E Cisco DNA Ce	nter	Provision / Network Devices / Provision Devices	\$ Q @ C
nwork Devices / Provision D	Devices		
Assign Site	Configuration (3) Summary		
and Biomber	Deste	-	
JC24411TQ5	AP10	16.5D7C.16F8 @bbaUUS/NewYork/Branch 5/Floor 2 ×	
			Cancel Next
Cisco DNA Ce	inter	Provision / Network Devices / Provision Devices	☆ Q © C
twork Devices / Provision D	Devices		
Assistan 2	Continuention (3) Summer		
-			
Zones and SSIDs are	listed from Provisioned Wireless pro	file(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.	×
Serial Number	Device Name	AP Zone Name IIF Profile SSIDs	
FJC24411TQS	AP1416.9D7C.16F8	sjcfloor1zone1 V LOW V lab3guest5	
FJC24411TQS	AP1416.9D7C.16F8	sjcfloortzene1 V LOW V tab3guest5	
FJC24411TQS	AP1416.9D7C.16F8	sjeffoortzene 1 V LOW V Lub3guest5	
FJC24411TQS	AP1416.9D7C.16F8	sjefloorizene1 v LOW v lub3guest5	
FJC24411TQ5	AP1416.9D7C.16F8	sgcfloor1zone1 v LOW V Lub3guest5	
FJC24411TQ5	AP1416.9D7C.16F8	sgefloorfzone1 v LOW V Lub3guest5	
FJC24411TQS	AP1416.907C.16F8	sgefloorfzone1 v LOW V Lub3guest5	
FJC24411TQ5	AP1416.907C.16F8	sgefloorfzone1 v LOW V Lub3guest5	
FJC24411TQ5	AP1416.907C.16F8	sgefloorfzone1 v LOW V Lub3guest5	
FUC24411TQS	AP1416.907C.16F8	sgefleorfzene1 v LOW V Lub3guest5	
FJC24411TQ5	AP1416.907C.16F8	sgefleorfzene1 👻 LOW 🗡 Lub3guest5	
FJC24411TQS	AP1416.907C.16F8	sgefleorfzene1 👻 LOW 🗡 lub3guest5	

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

vork Devices / Provision Devic	ces				
Assign Site 2	Configuration 3 Summary				
AP1416.9D7C.16F8	✓ Device Details				
	Device Name:	AP1416.9D7C.16F8			
	Serial Number:	FJC24411TQS			
	Mac Address:	54:8a:ba:ff:1e:20			
	Device Location:	Global/US/NewYork/Branch 5/Floor 2			
	✓ AP Zone Details				
	AP Zone Name	sjcfloor1zone1			
	✓ RF Profile Details				
	RF Profile Name: LOW				
	Radio Type:	2.4GHz	SGHz	6GHz	
	Parent Profile	LOW	LOW	LOW	
	Status	Enabled	Enabled	Enabled	
	DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 6 4, 149, 153, 157, 161	5, 21, 37, 53, 69, 85, 101, 117, 133, 1 49, 165, 181, 197, 213, 229	

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

	PROV	sion Vision Device	×
SUMMARY	Q Search by description Starts:	Jul 26, 2023 12:02 AM Completed: Jul 26, 2023 12:02 AM St	tatus: 🥥 Success Last updated: 12:02:28 AM 📿 Refresh
✓ Status (4)	PROVISION	Conversion of business intent to network intent	SUCCESS
O Upcoming	A admin		
O In Progress	Provision Device	Deployment of network intent	SUCCESS
O Success	Provisioned Unified AP(s) in Site		Hide Details
O Failed	starts: Jul 26, 2023 12:02	Conversion from network intent to device intent an	nd deployment of configuration SUCCESS
	PROVISION	Jul 26, 2023 12:02 AM Success	fully acquired device lock in rfs flow
 Last Updated 	<u>A</u> admin		
O 3 hours	Provision Device	Jul 26, 2023 12:02 AM Deployin	g configuration on the device CS800-Flex-
O 24 hours	Provisioned Unified AP(s) in Site	CVD.cag	elab.local (10.4.48.150).
O I due	Starts: Jul 25, 2023 11:51	Jul 26, 2023 12:02 AM Configure	ed operation will be to Modify AP configurations, Modify
O / days	- PROVIDION	AP Tag o	configurations, Add RF Tag configurations, Add Site Tag
Categories (41)		configura	ations and Add Policy Tag configurations.
Recurring	E admin		
O Show	Hostname: C9800-Flex-CVD.cc		
0.000	Starts: Jul 25, 2023 11:46	Conversion from natwork intent to device intent as	ind deployment of configuration CLIPACCO
O Hide			a separation and a separation and a separation and a separation of the second
	PROVISION	Jul 26, 2023 12:02 AM Success	fully acquired device lock in rts flow
	& admin	Jul 26, 2023 12:02 AM Deployin	g configuration on the device C9800-CVD-
	Provision Device	Nplus1.c	agelab.local (10.4.48.151).
	Provisioned Unified AP(s) in Site		

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。

Cisco Catalyst 9800-40 Wireless Controller Welcome assurance 🛛 🛠 📽 🏝 🕸 🔞 🛛 🎜 Search APs and Cleres Q Configuration · > Wireless · > A Edit AP General Interfaces High Availability Inventory ICap Advanced Support Bundle All Access Points Dashboard General Tags Monitoring Total APs : 2 AP Name* PT_NewYo_Branc... + AP1416.9D7C.16F8 Policy ST_NewYo_Branc... • Site Location* default location AP Name : AP M LOW • 🖬 RF 548a.baff.1e20 Base Radio MAC Write Tag Config to AP 80 C Licensing 1416.9d7c.16f8 Ethernet MAC н. н. 1. н. н. 10 🗸 Admin Status ENABLED Version K Troubleshooting Flex . AP Mode Primary Software Version 17.11.0.155 > 6 GHz Radios Operation Status Registered Predownloaded Status N/A Fabric Status Disabled Predownloaded Version N/A Walk Me Through > > 5 GHz Radios CleanAir NSI Key Next Retry Time N/A > 2.4 GHz Radios LED Settings Boot Version 1.1.2.4 I ED State > Dual-Band Radios D Cancel Update & Apply to Device

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

CISCO CISCO Cataly	Vst 9800-40 Wireless Controller Welco Configuration * > Tags & Profiles * > Tags	Edit Policy Tag	Connectivity for some clients that are associated to APs with this Policy Tan.
Deshboard Configuration Confi	Policy Site RF AP	Name* PT_NewYo, Description PolicyTagNa V WLAN-POLICY Maps: 1 + Add > Delete	Branc, Floor
Troubleshooting		WLAN Profile Usb3guest5_profile K I I I I I I I K RLAN-POLICY Maps: 0	Policy Profile T Isb3guest5_profile 1 - 1 of 1 items

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

Q. Search Menu Items	Configuration • > Tags	Edit Site Tag		×
Dechboard	Policy Site RF	Name*	ST_NewYo_Branch5_5b	
	+ Add × De	Description	Site Tag ST_NewYo_Bran	
Monitoring >	Cito Tao Mamo No omula	AP Join Profile	default-ap-profile 🗸 💈	
% Configuration >	Site Tag Name	Flex Profile	FP_NewYo_Branc 🗸 🖸	
کې Administration کې	ST_NewYo_Brank	Fabric Control Plane Name	• •	
C Licensing	8 4 1 F F	Enable Local Site	0	
X Troubleshooting		Load* 🛈	0	
Walk Me Through >				
		Cancel		Indate & Apply to Davice

- 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

 Search Menu Items 	Configuration * > Wireless * > /	Edit AP			
Dashboard	 All Access Points 	General Interfaces General	High Availability Inventory	ICap Advanced : Tags	Support Bundle
Monitoring	> Total APs : 2	AP Name*	AP1416.9D7C.16FC	Policy	PT_NewYo_Branc ¥
	AP Name AP	Location*	default location	Site	ST_NewYo_Branc 🔻 💋
Administration	> AP1416.9D7C.16F8 4	Base Radio MAC	548a.baff.1e40	RF	HIGH 🗸 🖉
Licensing	AP1416.9D7C.16FC 4. 141 C9	Ethernet MAC	1416.9d7c.16fc	Write Tag Config to AP	0
Troubleshooting	R 4 1 P R 10	Admin Status		Version	
		AP Mode	Flex	Primary Software Version	17.11.0.155
	6 GHz Radios	Operation Status	Registered	Predownloaded Status	N/A
Walk Me Through >	> 5 GHz Radios	Fabric Status	Disabled	Predownloaded Version	N/A
	> 2.4 GHz Radios	LED Settings		Next Retry Time Boot Version	N/A 1.1.2.4
	> Dual-Band Radios	D Cancel	ENADI ES		E Lindate & Apply to D
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

Cisco Cisco C	atalyst 9800-40 Wireless Controller Welco	ome assurance 🛪 🕫 🛕 🖺 🌣 🐚	Search APs and Clients Q	Feedback 🖌 🖌
Q. Search Menu Items	Configuration * > Tags & Profiles * > Tags Policy Site RF AP	Edit Policy Tag A Changes may result in loss of connectivity for	r some clients that are associated to APs with this P	volicy Tag.
Dashboard	Add X Delote Cione Policy Tag Name "Is equal to" PT_NewYo_Branc_F	Name* PT_NewYo_Branc_Floor		
Configuration	Policy Tag Name PT_NewYo_Branc_Floor1_64cf5_1	WLAN-POLICY Maps: 1		
C Licensing		+ Add × Delete WLAN Profile Isb3branch5_profile	Policy Profile Iab3branch5_profile	Ŧ
Walk Me Through >		RLAN-POLICY Maps: 0		1 - 1 of 1 items
		Cancel	一 門 0	pdate & Apply to Device

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

Cisco Catal	vst 9800-40 Wireless	Controller Welcome assur	ance 🛛 🌴 🐔 🛕 🖹 🗘 🔯 😡 🎜 Search APs and C	tients Q
Cashboard Image: Dashboard Image: Dashboard	Policy Site RF Add Ov Site Tag Name "Is equal t Site Tag Name Site Tag Name SI_NewYo_Brank II = 1 = II	Name* Description AP Join Profile Fiex Profile Fabric Control Plane Name Enable Local Site Load* ①	ST_NewYo_Branch5_5b Site Tag ST_NewYo_Bran default-ap-profile FP_NewYo_Branc 0	
Walk Me Through 1		Cancel		🗄 Update & Apply to Device

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HASSO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。

- 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

E Cisco DNA Center	Pro	vision / Network Devices / Provision Devices	* 0 © 4
Network Devices / Provinian Devices			
1 Annage Sites 2 Configuration	3 Simmary		
Denial Number KUC24411TIM	Devices AP1415.907C.16FC	gB) notari/US/NewYork/Branch Siftwort \times	

- **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。

Cancel

図 144: APのプロビジョニングステップ 2: 設定

E Cisco DNA C	enter		Provision	/ Network Devi	es / Provision Devices	\$ Q @ C Q
Servert Devices / Provider	Devroes					
1 Assign the	Configuration 3 Summer	Y				
A Zones and SSIDs a	re Ested from Provisioned Winieus pr	otle(x) for each Access point. I	for newly as	Ided Zones and 55	3s, Please provision Controller prior to Azcess point provision.	×
Seriel Natiber	Device hearse	AP Zone Name		BE Profile	weaguests, weathances	
FJC24411TRM	AP1416.907C.16FC	Not Applicable	4	TYPICAL	· 2	

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

E Cisco DNA Cente	er	Provision / Network Devices	/ Provision Devices		\$ Q @ C L
Network Devices / Provision Devic	ces				
1 Assign Site 2	Configuration 3 Summary				
AP1416.9D7C.16FC	Y Device Details				
	Device Name:	AP1416.9D7C.16FC			
	Serial Number:	FJC24411TRM			
	Mac Address:	54:8a/ba/#:1e:40			
	Device Location:	Global/US/NewYork/Branch 5/Floor1			
	✓ AP Zone Details				
	AP Zone Name	default-zone			
	~ RF Profile Details				
	RF Profile Name: TYPICAL				
	Radio Type:	2.4GHz	SGHz	6GHz	
	Parent Profile	TYPICAL	TYPICAL	TYPICAL	
	Status	Enabled	Enabled	Enabled	
	DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 6 4, 149, 153, 157, 161	5, 21, 37, 53, 69, 85, 101, 117, 133, 1 49, 165, 181, 197, 213, 229	
	Channel Width	20 MHz	Best	Best	
				Cancel	Next

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。

Cancel Next

- (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

Cisco Cisco	Catalyst 98	00-40 Wireless Controller	Velcome assurance	* A	* * • 2	Search APs and Clients Q	EFeedback e^* 🗭
Q. Search Menu Items	Confi	guration • > Tags & Profiles • > Ta	ags				
Dashboard	Policy	Site RF AP					
Monitoring	· ·	+ Add Clevelo Clov			econtration		
	· 0	default-policy-tag		4 D	efault policy-tag		,
O Administration	· · · ·	PT_NewYo_Branc_Floor1_64cf5		P	olicyTagName PT_NewYo	_Branc_Floor1_64	
C Licensing	1	4 1 ≥ ≥ 10 ¥					1 - 2 of 2 items
X Troubleshooting							
Walk Me Through 3							

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

Cisco Cisco	o Catalyst 98	800-40 Wireless Control	ler Welcome assurance	* * 4 8 * 8	Search APs and Clients Q	Feedback x ^A (+
Q. Search Menu Items	Confi	iguration • > Tags & Profiles •	 Tags Edit Policy Tag 			×
Dashboard	Polic	ay Site RF AP	A Changes	may result in loss of connectivity for s	some clients that are associated to APs with thi	s Policy Tag.
Monitoring		+ Add × Delete	Name*	PT_NewYo_Branc_Floor		
	· .	Policy Tag Name default-policy-tag	Description	PolicyTagName PT_New		
O Administration	, 🖸	PT_NewYo_Branc_Floor1_64cf5	V WLAN-POI	LICY Maps: 2		
C Licensing		10 •	+ Add	Delete		
💥 Troubleshooting			WLAN Profile		▼ Policy Profile	т
			lab3guest5_pro	ofile	lab3guest5_profile	
			lab3branch5_pr	rofile	lab3branch5_profile	
			14 4 1 4	H 10 ¥		1 - 2 of 2 items
Walk Me Through F			> RLAN-POL	ICY Maps: 0		
			Dému			
			U Cancel		G	Update & Apply to Device

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。

Cisco Cataly Cataly Cisco Cataly Catal	est 9800-40 Wireless Controller Welcome assurance Configuration - > Tags & Profiles - > Tags Policy Site RF AP	Edit RF Tag	Search APs and Clients Q Search APs and Clients Q Search APs and Clients Q Search APs with this RF Tag.
	Add X Delets Cone RF Tag Name TYPRCAL default-rf-tag 4 1 P K 10 V	Name* Description 6 GHz Band RF Profile 5 GHz Band RF Profile 2.4 GHz Band RF Profile	TYPICAL Show slot configuration Enter Description Image: Classical Clas

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。

Cisco Cata	lyst 9800-40 Wireles	s Controller Welcome assur	ance 🗌 🏶 🗞 🕲 🌣 🐧 🕢 🎜 Search A	Ps and Clients Q
Q, Search Menu Items	Configuration • > Tags	Edit Site Tag		×
Dashboard Monitoring Configuration Configur	Policy Site RF Add X Dev Site Tag Name Gefault-site-tag ST_NewYo_Brank X 1	Name* Description AP Join Profile Flex Profile Fabric Control Plane Name Enable Local Site Load* (i)	ST_NewYo_Branch5_5bi Site Tag ST_NewYo_Bran default-ap-profile \$ FP_NewYo_Branc	
(Walt Me Through)		Cancel		🗊 Update & Apply to Device

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。

Q. Search Menu Items	Co	onfiguration * >	Edit Flex Profile				×
		+ Add	General Local At	thentication Policy ACL VL/	AN DNS Layer Security		
Dashboard		Flex Profile N	Name*	FP_NewYo_Branc_5b48	Fallback Radio Shut	0	
Monitoring	· · C	FP_NewYo_	Description	Enter Description	Flex Resilient	0	
	, C	default-flex-p	Native VLAN ID	90	ARP Caching		
C Administration			HTTP Draw Part	0	Efficient Image Upgrade		
			in the second		OfficeExtend AP	0	
			HTTP-Proxy IP Address	0.0.0.0	Join Minimum Latency	0	
X Troubleshooting			CTS Policy	-	IP Overlap		
			Inline Tagging	0	mDNS Flex Profile	Search or Select 👻	
			SGACL Enforcement	U	PMK Propagation		
Walk Me Through >			CTS Profile Name	default-sxp-profile × 👻			

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。

Q. Search Menu Items	Confi	guration • >	Edit	Flex Profile								×
and the second s		Add		General	Loca	I Authe	ntication	Po	licy ACL	VLAN	DNS Layer Security	
Dashboard		Eley Profile N	+	Add		to						
Monitoring >	0	FP_NewYo		VI AN Name		ID .	Ingress	Ŧ	Egress	т		
Configuration	0	default-flex-p	0	Guest	1	110	AUL		MUL			
	.01	← 1 →	0	Employee		100						
205 Administration \$			0	branchemploy	ee	100						
C Licensing			U	branchguest-	dimz	110			t - A of A ite	-		
💥 Troubleshooting						10	•		1 - 4 01 4 100	n th		
Walk Me Through 1												
		1	2	Cancel							78.	

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

Q. Search Menu Items	Configuration • > Tags & Profiles • > Tags	Edit Tags ×
Dashboard	Policy Site RF AP Tag Source Static Location Filter	▲ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.
Configuration	Add Evelote Number of AP Tag mappings selected : 0	AP MAC Address* 1416.9d7c.16fc Policy Tag Name PT_NewYo_Branc
 (c) Administration → (c) Licensing 	AP MAC Address ▼ Polic 1416.9d7c.16fc PT≦ 1	Site Tag Name ST_NewYo_Branc_
X Troubleshooting		
Walk Me Through >		
		Cancel

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

Ver categorie - Maraton Macoing Assistant	Your Seved List			
	elisite cisco	Cisco Cataly	st 9800-CL Wire	eless Controller for Clo
	Overv	riew	Pricing	Usage
	Cisco Cat CloudForm Cisco® Catalyst® 980 • View Template Co • View Usage Instru • Close CloudForma Cisco CloudForma Download CloudFor View Template in Ch End User Licens By subscribing to thi	alyst C9800-CL Wirel ation Template IO-CL - Cloud Formation imponents ctions tion Template AWS Private subnet mation Template (2 oudformation Designer e Agreement s product you agree to to	ess Controller Template GE 1	tlined in the product End

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

cisco	Cisco Catalyst 980 Cloud	00-CL Wireless Controller for
< Product Detail	Subscribe Configure	
Configur	e this software	
Choose a fulfillm required to confi	nent option below to select how igure the deployment.	you wish to deploy the software, then enter the informatio
Fulfillment O	ption	
✓ Select a fulfill	ment option	Amazon Machine Image Deoloy a vendor-orovided Amazon Machine Image
Amazon Mach CloudFormati	nne image on	(AMI) on Amazon EC2

CloudFormation

Deploy a complete solution configuration using a

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

cisco Cloud	00-CL Wireless Controller for	Continue to Launch
Futifillment option CloudFormation Template Cloco Catalyst C9800-CL Wireless Controller Software version 17.9.1 (Nov 28, 2022) Whats in This Westion Close Catalyst 9800-CA Westion Controller for Or convergence Subger Learn more	ChoodFermation Template Deploy a complete solution configuration using a CoudFormation template	ach statement period may differ from this estimate. Software Pricing Close Catalyst 960-CL Wisters Candular for Close Catalyst Ca
Select a region US East (N. Vrojnic) US East (N. California) US West (N. California) US West (Oregon) Canada (Central) EU (Frankfurt) EU (Ireland) EU (Inden) EU (Inden)	nent may alter your final pricing.	
EU (Stockholm) EU (Mian) Asia Pacific (Hong Kong) Asia Pacific (Singapore) Asia Pacific (Sydney)	Nace Blog Bi RSS Feed Data Products Resources AWS Marke Financial Services Data Analyst Reports Americanov W	rtplace is histogl ds Services (1969) is a dynamic, growing ds winthis dualance may ble low generativ

- 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

cisco	Cisco Catalyst 9800-CL Wireless Controller for Cloud
< Product Detail	Subsorbe Configure Laurch
Launch	this software
Review the lau	nch configuration details and follow the instructions to launch this software.
Configurati	on details
Fulfillment o	tion Cisco Catalyst C9800-CL Wireless Controller Cisco Catalyst 8000-CL Wireless Controller for Cloud
Software ver	ion 17.9.1
Region	US West (Oregon)
Usage i	structions
Choose Act	on
Launch Clo	dFormation Choose this action to launch your configuration through the AWS CloudFormation console.
	Laurch

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

ite stack	Create stack		
2 cify stack details	Prerequisite - Prepare template		
p 3	Prepare template Every stack is based on a template. A template is a JSON or VAM, 10	e that contains configuration information about the A	WS resources you want to include in the stack.
imgure stack options	 Template is ready 	 Use a sample template 	Create template in Designer
	Specify template A template is a JSON or VXML file that describes your stack's resource	ies and properties.	
	Specify template A template is a JSON or YAM, Rie that describes your stack's resource Selecting a template gamerates an Amazon S3 URL where it will be a Amazon S3 URL Amazon S3 URL	es and properties.	mplate file
	Specify template A template is a SON or VAM. Rie that describes your stacks resource Selecting a template gammates an Amazon S3 URL where it will be a Manazon S3 URL Amazon S3 URL Matps://s3.amazonaws.com/awsmp-fulfillment-cf-template Amazon S3 semplate LRL S3 URE: S3 URE:	as and properties. tored. Upload a te tes-prod/36aaa0b8-cf25-45aa-9fcc-16915f2 Ftemplates-prod/36aaa0b8-cf25-45aa-9fcc-	mplate file 4cc71.bcfca1f9-e47e-41b7-a86c-5644ef777b7a.template 16915f24ce71.bcfca1f9-e47e-41b7-a86c-

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

Specify a stack name and para	meter values. You can use or change t	he default	parameter values, which are defined in the AW
Stack name	c9800-stack-name		
Parameters			
Instance Details			
Hostname	myC9800-CL		Specify the hostname of C9800-CL instance
Instance Key Pair	c9800-demo1	•	
	Pem file for access to created instance		

- 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

Network Details		
Management Network	subnet-087bf7c0a83ci45a1 (10.10.20.0 • Subnet for Wireless Management Interface	
Management Security Group	C9800-CL_security_group (sg-ObecRe5 • Choose the security group to be attached to the interfe	cm.
Management IP address	10.10.20.8	(Optional) Provide the desired IP for the instance in the selected subnet. Note: Make sure the IP in not already taken.

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

User Details					
Username	admin	Specify the usersame			
Enter Password		Specify the parameter			
Confirm Password		Retyte the parameters			
Other parameters					
C9800InstanceType	✓ c5.deps c5.2xiege c5.4xiege	3 Specify Instance type for Class-Categor OBSIG-CL Weekes Complete			
			Carcol	Previous	Next

- **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

itep 1 Create stack	Review c9800-stack-name	
Step 2 Specify stack details	Step 1: Specify template	Edit
Step 3 Configure stack options	Template	
tep 4 Review c9800-stack-name	Template URL. https://s3.amazonaws.com/awsmp-fulfiliment-cf-templates-prod/36aaa0b8-cf25-45aa-9fcc-16915f24ce71.bcfca1 Stack description	f9-e47e-41b7-a86c-5644ef777b7a.template
	AWS CloudFormation Template for Cisco Catalyst 9800-CL Wireless Controller for CloudAWSMP::36aaa0b8-cf25-4 439f521f4376	45aa-9fcc-16915f24ce71::fca11194-78c0-43ed-debf-

図 166:設定の確認:パート2

Stack creation options	
Timeout -	
Termination protection Deactivated	
Quick-create link	
Create change set	Cancel Previous Submit

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。

oudFormation > Stacks > c9800-stack-name	c9800-stack-name ©
🖸 Stacks (1)	Delete Update Stack actions V Create stack
Q. c9800 X	Stack Info Events Resources Outputs Parameters Template Change sets
Active View nested	Resources (1)
Stacks	Q. Search resources < 1 > @
c9800-stack-name	Logical ID 🔺 Physical ID 🔍 Type 🖤 Status 🔍
2025-05-18 11:39:47 UTC-0700 ⓒ CREATE_COMPLETE	 EC2Instance I-07b2dbf21b2ca99e2 AWS:EC2:Instance OCREATE_COMPLETE

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

.,			G	Connect		Instance state V	Actions V		Launch instances		•
nce by attribute or tag (cas	se-sensitive)								< 1	>	۲
Instance state = running	Clear filters]									
▼ 1	Instance ID	Instance state	⊽	Instance type	▼	Status check	Alarm statu	s	Availability Zone		Pub
stack-name	i-014b3b2cb8750c6db	⊘ Running	QQ	c5.xlarge		Ø 2/2 checks passed	No alarms	+	us-west-2a		-
	nce by attribute or tag (ca Instance state = running v -stack-name	nce by attribute or tag (case-sensitive) Instance state = running X Clear filters v Instance ID -stack-name i-014b3b2cb8750c6db	nce by attribute or tag (case-sensitive) Instance state = running X Clear filters v Instance ID Instance state -stack-name i-014b3b2cb8750c6db Ø Running	nce by attribute or tag (case-sensitive) Instance state = running X Clear filters ▼ Instance ID Instance state ▼ -stack-name i-014b3b2cb8750c6db ⊘Running @Q	nnce by attribute or tag (case-sensitive) Instance state = running X Clear filters ▼ Instance ID Instance state ▼ Instance type -stack-name i-014b3b2cb8750c6db ⊘ Running @Q c5.xlarge	nce by attribute or tag (case-sensitive) Instance state = running X Clear filters ▼ Instance ID Instance state ▼ Instance type ▼ -stack-name i-014b3b2cb8750c6db ② Running @ c.5.xlarge	nce by attribute or tag (case-sensitive) Instance state = running X Clear filters ✓ Instance ID Instance state ▼ Instance type ▼ Status check -stack-name i-014b3b2cb8750c6db ⊘ Running @Q c5.xlarge ⊘ 2/2 checks passed	nnce by attribute or tag (case-sensitive) Instance state = running X Clear filters ✓ Instance ID Instance state ▼ Instance type ▼ Status check Alarm statu -stack-name i-014b3b2cb8750c6db ⊘ Running @, c5.xlarge ⊘ 2/2 checks passed No alarms	nce by attribute or tag (case-sensitive) Instance state = running X Clear filters	nnce by attribute or tag (case-sensitive) < 1 Instance state = running X Clear filters ▼ Instance ID Instance state ▼ Instance type ▼ Status check Alarm status Availability Zone -stack-name i-014b3b2cb8750c6db ⊘ Running @Q c5.xlarge ⊘ 2/2 checks passed No alarms + us-west-2a	nce by attribute or tag (case-sensitive) < 1 > Instance state = running X Clear filters ▼ Instance ID Instance state ▼ Instance type ▼ Status check Alarm status Availability Zone ▼ -stack-name i-014b3b2cb8750c6db ⊘ Running @Q c5.xlarge ⊘ 2/2 checks passed No alarms + us-west-2a

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#

1

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

aws Services Q Search		[Option+S]	\$ Ø	N. California 🔻	
🛃 EC2 🔞 S3 🧣 VPC 👩 CloudFor	mation				
New EC2 Experience ×	Resources	EC2	Global view 🖄 🖸 💿	Account a	
EC2 Dashboard EC2 Global View	You are using the following Amazon EC	2 resources in the US West (N. California	i) Region:	Supported p	
Events	Instances (running) 9	Auto Scaling Groups 0	Dedicated Hosts 0	• VPC	
Limits	Elastic IPs 4	Instances 14	Key pairs 2	Default VPC vpc-09e0fa	
▼ Instances	Load balancers 0	Placement groups 0	Security groups 11	Settings	
Instance Types	Snapshots 0	Volumes 14		EBS encrypt Zones	
Launch Templates Spot Requests Savings Plans	③ Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the X AWS Launch Wizard for SQL Server. Learn more				
Reserved Instances Dedicated Hosts Capacity Reservations	Launch instance To get started, launch an Amazon EC2 instan	ce, which is a	alth	Additiona	

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

ect to your instance i-0	3f235ba2d68fd0e9 (AW	5-9800-Controlle	r) using any of these optic	ons	
	1				
2 Instance Connect	Session Manager	SSH client	EC2 serial console		
stance ID		Ser	ial port		
i-03f235ba2d68fd0e9	(AWS-9800-Controller)	0	ttvS0		

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

	co Catalyst 9800-CL Wirele	ess Controller We	icome lab 🛛 🕷 🐔 🐧		learch Afs and Charits Q	B Feedback 🖌 Թ
Q. Search Menu Itema	Configuration * > Ta	gs & Profiles * > WLANs				
Dashboard	+ Add > Del	ete 📄 🖸 Clone 🛛 Erable WLAN	Disable WLAN			WLAN Wizard
Monitoring	Selected WLANS : 0					
	Status Name O corpever	▼ © 17	Ť	SSID corpevent	▼ Security [WPA2[[PSK][AES]	Ŧ
C Administration		10 •				1 - 1 of 1 items
C Licensing						
💥 Troubleshooting						

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

Con	figuration *	> Tags & Profile	es > Policy			
-+	Add	× Delete	C Clone			
	Admin T Status	Associated 0 7 Policy Tags	Policy Profile Name	Ŧ	Description	Ŧ
0	0		corpevent_profile		corpevent_profile	
-					the second second second	

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。

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	С9124АХД-В	Building 24、Floor 1
mil24-floor2-ap1	С9124АХД-В	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

E Cisco DNA Center	Assurance / Dashboards / Health	* Q @ @ @
Overall Network Client Network Services - Applications SD-A	kcess Al Analytics \lor	
🛇 Graber 🚦 🛞 34 Hours 🗸		May 7, 2023 1 15 PM - May 8, 2023 1 15 PM 0
		Actions
Network Devices	Arrent Point United Clients	ν ·
un U	No No.	View Client Health

サイトレベルのネットワークの正常性

^{⑦ 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

E Cisco DNA Center	Assurance / Dashboards / Health	± Q © ₫ 4
Overall Network Client Network Services O Global/US/Milpitas I 0 24 Hours	Applications SD-Access Al Analytics V	May 7, 2023 1.15 PM - May 8, 2023 1.15 PM 0
Q. Search H voty V Site	Level Network Health	Action
A Gobal Add Angela Add		19
visibility by clicking on Global	View Remark House	View Client Insulty

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。

2	176 ·	[Noviro	3601 -	いいだけ
	1/0.	DEVICE	JUUI / 1	~ ~ /

ork / Decks 202												
LC C98	00-40-CVD.	cagelab.	local									
A Nours 🗸												Ran Commands
ing.												2400
												-
/10 ⁰ DEVI	e privila	44		in .	104	14				AN 23, 2023	140 2 00 PW - Ad 24, 202	2 100 MM ()
V10 ⁰ DEVI 1 CONSE 40 43	A CE DETALS 1. Biologomer (* 18.4382	Na Lonamen Gladead	N) (1.01.) Witprise (Studiety biture	19 20 Series 113.3 No 9 Physics Reighbor To	ACCESS Face-for	an - Frank Star of Frank	martenens ni	No. Data an Optime 21 articles Exert View	12 miles 🕤 1	tar Jar 25, 2625 Secondarily Taxon Readings	100 2 00 PW - Ar 34, 202	2 100 IM S
),10 ⁰ DEVI 10 CHIER 41 43 SSUES (1)	AR CE DETALLS Miningeneric (* 18.4.98.2	ka Lunaiten Okolad	N. (1,8) / Wepter / Hubbing Rose	19 23 Software 118.3 No. 6 Physica Neighbor To	ACCESS Farm for pology Path Two	aur - Farra Sau 1 Ia - Application Depart	inter Roberts rel Inter Device Int	in Universities Control 21	10 10 m 13 m 44 0 1	Ar 23, 2629	1 00 PW - 34 24, 202	2103 MA 5
0/10 ⁹ DEVI 10 COMB 40 40 25SUES (1)	in CE DE DALS 1 Minisperses (* 18.4.98.3 AM (4.202) 2-08 PM Availability	No.	Ni (1,8) (1994) in (Subley Jacut	ing 23 Software 11 8.3 No 6 Physical Relightor To	ACCESE Term for policy Path Theo	auro Paro Sauro - 1 a Application Dapar	N Intel Recentle 14 Intel Device III	n Data ne Upter 2 effects Event View	а того, 13 техника 🕞 — 1 т	Ad 23, 2023	105 PW - 34 34, 102	1 100 m 5
0,10 ⁰ 0000 	IP CE DCMUS I Ministerium III III 4383 Art 34, 2022 3 48 MM Availability Helenin davida "Citta Helenin Care, 1	No Constitute Obdawal 100-40-CVO conge	in LOE / Werken / Solding Isour	119 23 Serieure 11 5.3 Noi 5 Physical Neighbor 5 91 Nik publichever 🗃	ACCESS Trans for actingy Fach Trans	in Farm Sau 1 in Application Experi	n muthemen - vit	to Touto ees Lysten 21 arfaces. Event View	ар 1909, 13 менала С. — 3 1	Ar 23, 2023	100 2 00 PW - Ad 34, 202 0 1 West Ad Datab	1.46 PM

[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

Cisco DNA Center		4 9 0 0 0
WLC C9800-	Network Device C9800-40-CVD.cagelab.local is unreachable from Cisco DNA Center	2
© 24 Hours ~	New V 🖄 Insue Profile	r. picturi (5 Eat Innue Settings
The second	Jescripth	1
1.	his network dev	
1	Issue could be lanored or This	5
10	Resolved disabled from Issue Solution	ettings
more California All Maria	Suggested Actions (3) page	
Contrar 2 days, 7 hours, 14 m		
	 From the Cloce DNA Center, verify whether the last hop is machable. 	
Issues (1) ways	2 Verify that the physical port(s) on the network device associated with the network device discovery(P) is UR.	
Availabet		
P1 Antest	3 Verify access to the device.	
1 Records		
	Clicking on Issue opens a side	
Ci	par with details about the issue	
Physical Ne		
20 C		

[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

	4 APs			×
	Device	Health Score +	IP Address	Schear
	♥ miD4-foor1-ap1	10	10.4.60.102	17.8.4.
const. Jose	T mill3-foor1-ep1	10	10.4.60.101	17.8.4.
I	T mil/3-foor2-ap2	10	10.4.60.100	17.8.4
54ey 6, 2023 10:52 AM	P mil/4-foor2-ap1	10	10.4.60.103	17.8.4.
View Device List				
6.0%		Show Records:	10 V C O	

[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

Berles Interfaces				
Assolutions		Al Rebuilderry		
Cyline # hours, 42 minutes (Reductory Mode	880	
Last Renet Research Reliand Conversed		Reductionry Unit	hat.	
Primary Preser Supply Balas Presert, Dr		Local State	HEADY (ACTIVE)	
Sacurdary Power Supply Status NA		Page State	ABADY (STANDER HOT)	
mana Tenansian and register O				
		Davit		
	Mar 9, 2020 10,21 Aw • Sound 1 • Local 0	C • text		
1	Anne 1 Anne 1	🗹 🔹 Famiga		
ting tink tink tink tink tink technologiet *Takin tink tink	100a 1200a	🕼 🖷 Ancher		

図 180: デバイスインターフェイスの詳細

Detail Information							
reice Interfaces							
Interfaces (12) Kost of 13 Mar	face(c) are down						
Tong A Physical Village							
Q. Inust here							v
Puthate	Operational Status *	Autor Datas	Tan .	Speed	Description		
C Longitude1			Virtual	Vitual			
Lingback100			Virtual.	Viter			
Terdigatetharved/did			Physical	10 Okpe	-		
Terdigulationared/5/3			Physical	10 Okpe	-		
12 Records						Dow Records 21	
anat SightChenet			Traffic a	of Packet Summery			
			Tere 1	-		1.000	1.00
			- 100	acters.		870307	121
Equilitanet			Unive	wn Protocol Packets			
			1000	C Packets		441,223	121
1.010 0.070 0	10 k/w 1.01e	1.00x 1.00x 11.00p	Mutte	at Packets		322544	
	new (Secure)		(real)	unt Parkets		105524	
			Farmer	el Packets O			
			firme f	Sectors.			
			Data	d Packets			

[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

mil24-floor2-ap	1								
Hours 🗸								Intelligent Capture	88
2a				13					11:5
									_
1 1	40 60	80 10	7/18	28	40	64	1		
DEVICE DETAILS DEVICE CREATING DEVICE CREATING DEVICE CREATING DEVICE CREATING DEVICE CREATING DEVICE CREATING DEVICE CREATING	Model: C9124AXD-B Soft Negotiated Power Level: 60.0	ware: 17.11.0.155 Management IP: 10. W PoE Status: ON Power Save Mode	4.60.103 Location: Global / US Cspability: Not Supported View	Alipitas / Building 24 /	Floor 2 Mode: Local	Uptime: 18 days, 1	Jul 17, 2023	10a 11:52 AM - Jul 18, 2023 Sapability: Wi-Fi 6	3 11:52 /
DEVICE DETAILS DEVICE DETAILS end To W.C. CRED-49-CVD capability.or oral Status: Up O EFE Class: EEE	ad Model: C9124AXD-B Sof	ware: 17.11.0.155 Management IP. 10. W PoE Status: ON Power Save Mode	4.60.103 Location: Global / US Copubliny: Not Supported View	vilpitas / Building 24 / Il Details	Floor 2 Mode: Local	Uptime: 18 days, 1	Jul 17, 2023 :	10a 11:52 AM - Jul 18, 2023 Capability: Wi-Fi 6	3 11:52 A
O DEVICE DETAILS DEVICE OFFAILS ted To W.C. COMOD-40-CVD capabilities ted To W.C. COMOD-40-CVD capabilities ted To W.C. COMOD-40-CVD capabilities Toools	Model: C9124AXD-8 Soft	ware: 17.11.0.155 Management IP: 10. W Poli Status: ON Power Save Mode	4.60.103 Location Global / US Capability: Not Supported View	Mipitas / Building 24 /	Floor 2 Mode: Local	Uptime: 18 days, 1	Jul 17, 2023	10a 11;52 AM - Jul 18, 2023 2apability: Wi-Fi 6	8 11:52 A
O DEVICE DETAILS DEVICE DETAILS Test To W.C.: CREDIN-40-CVD capability.io consil Status: Up O EEE Class: EEE TOOOIS Ping Discussion	al Model: C9124AXD-B Soft I Negotiated Power Level: 60.0	were 17.11.0.155 Management IP-10. W Pold Status: ON Power Save Mode * Trace Routs	4.60.103 Location Global (US) Copublity: Not Supported View	Mipitas / Building 24 / Il Details	Floor 2 Mode: Local	Uptime: 18 days, 1	Jul 17, 2023 : Jul 17, 2023 :	104 11:52 AM - Jul 16, 2023 2apability: Wi-Fi 6	8 11:52 A

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 184 : AP 360 : PoE 情報

Detail Information

vice RF Ethernet	Pot			
IEEE PD Class	IEEE4	Allocated Power	39.5W	
Power Level	60.0W	Consumed Power	11.6W	
PoE Admin Status	AUTO	Max Power Drawn	12.3W	
PoE Oper Status	ON	PoE Priority	LOW	
PoE Policing Status	Disabled	Fast PoE	Disabled	
Four Pair	Disabled	Perpetual PoE	Disabled	
Switch Name	C9300-STACK2-CVD	UPOE+	Disabled	
Interface Name	GigabitEthernet2/0/1	Last Seen	May 10, 2:50 PM	
Power Distribution				
80				
60				
40				

0 3.00p 6.00p 9.00p 5.110 2.00p 8.00p 9.00p • Alocated Power • Consumed Power

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

20

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

≡ Cisco	DNA Center												\$	9000
Intelligent	Capture:	P Abbus	loor1-ap	2 Chichael I	105 / Wigitan J ave Denies: 13	Building 23 //	Noor 1 Meter La		Uptime: 1 days	1 hr 27 min	Core	ected to WLC C	NREE-40-0V0 II	X and here
RF Statistics	Spectrum An	alysis												
⊙1 hour ∨	Handra	1.4%	2.454	1540	1 He	1.14.0	1150	1.16	1.54	1.25g	1.2%	I No	2.54e	(I) NE O
						0	7.6							
							No Dat	а						
					No Spe	ectrum Analy	nis data in th	e selected to	me range.					
						Star	1 Spectrum A	unalysis						

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。

elligent Captur	e: DES	KTOP-P6	6HKGR				1 Download	Stop Live Capture	Run Pa	cket Capture
12 I hour	12	12-20p	12.25e	12.000 12.00	12.469	12409 1240	12.1%	198a 1.95a	1120 1 1.120	
boarding Events			+LWI	2	1 3 8 8	3 3 8 3 8		esta destructions		*
Al Anonaly Ne Event		đ Time	Event PGAP			88	and die			000
May 12, 2023				V RF Statistics						+LIVE
DHCP	(1)	1:05:52 PM		RSSI, SNR, TA Data	Rate, Ra/Ta Packet, Ra I	Betry Court				
Onboarding	(6)	1:05:52 PM	3 ms	50						40
Delete	610	1:05:52 PM		· · · · · · · · · · · · · · · · · · ·						-29 -
DHCP	(1)	1:05:52 PM	_	• #552 (dbm)	12:30y	12-31g	12:40#	\$2,50	1-01#	1:11:20 pm
1-7				1,000 1,	12:31g a Kate From Clent	LE Sta Last Data Rate Fr	12-4br	12-519	Lity	410 410 410 410 410 410 410 410 410 410
				Lass Cont						z
				0	12-29a Sient Packets I	12:39e From Client	32-60p	12-50y	3-00#	10 110 20 pm

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-ap	517	AP serviceal	oility
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 pa	acket-trace stats			
AP times	stamp	:	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 de	etection event stats			
AP times	stamp	:	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 de	etection packet stats			
AP times	stamp	:	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	s stats			
AP times	stamp	:	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
                    : Enabled
Stats
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

Intelligent Capture	e: DESKTOP-P66H	IKGR 🗘 Full Packet Ca	pture in Progress (26KB/1	100MB) Stop	<u>↓</u> Download	Run Packet Ca	pture
) 1 hour V PCAP I Jul 20	0 3:20p 3:25p	Data Packet Captures	Last Packet Time	Туре	Duration (h:m:s)	Size	X
Onboarding Events		Jul 20, 2023 4:14:44 PM	Jul 20, 2023 4:15:34 PM	Wireless	00:00:50	26 KB	¥
Al Anomaly 🚧	đ۵				DCAD He see he down	~~	_
Jul 20, 2023	Time Du				Download	I symbol	
> OHCP	4:08:50 PM						
Onboarding	4:08:50 PM						
DHCP	4:08:49 PM						
> Onboarding	4:08:49 PM						
DHCP	4:00:40 PM						
> Onboarding	4:00:40 PM						
> o Delete	4:00:40 PM	Showing 1 - 1 of 1					
> • DHCP	3:30:39 PM	-90 dBm	000000000000000000000000000000000000000			000000	0
> Onboarding	3:30:39 PM	6 ms		10 010 <u>2</u>	ab <u>c</u> alla alla B ana a	(ellip) (ell <u>*</u>	Q
> • Delete	3:30:38 PM						0
> Oelete	3:29:32 PM	✓ RF Statistic	:5				0 LIVE
> Onboarding	3:29:32 PM	2 ms	TX Data Kate, HX/TX Packet, RX I	Retry Count			

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 ツーセンド)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-75dBm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-75dBm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

Al Endpoint Analytics	Application Hosting	Group-Based Policy Analytics
Endpoint Analytics delivers automated and ustom classification for both wired and wireless indoo few Details	Application Husting lets you manage the life cycle of third party applications on devices managed by View Details	Segmentation Policy Analytics drastically reduces your time to value for segmentation policy by ends View Denaits
Rogue and aWIPS	Support Services	()) Wide Area Bonjour
te Rogue Monagement and the Cisco Advanced Indexs Intrusion Prevention System (JWIPS) to elect w lee Details	Cisco Support personnel assigned to your open support cases can interact with and troubleshoot your	The White Area Borgiour application provides an end-to-and enterprise-class Apple Borgiour solution in View Details

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

E Clace DNA Center	Assurance / Cashboards / Polt	• 0 0 0 4
() Basenandi Milyana, Rushing Sa 👔 🛞 20 Maam 🚽		$m_{\rm H}$ =5, and n =0.0 m $_{\rm H}$ =0, and n =0
		Atten
Pol. Telementy is available on Oxco Catal	vi \$206, \$206,5, \$306, \$306,5, \$400, 3856, \$1300, \$3400, \$2200, and \$553300 pix	forms with minimum 105-KE 18,12.3s and 17.3 software ventions.
AP Power Santigs () Power (conursed bid black ((co. cons. (co. box))	AP Power Save Mode Distribution .:	Poli Operational State Distribution
1 1 1 1 1 1 1 1 1 1 1 1 1 1	2 2 2 2 2 2 2 2 2 2 2 2 2 2	E la de la de la delasticación
Pot Powered Device Distribution	Pol: maights	Power Alsocation Load Distribution
And	eer Propose hel 340 3985 of universid device als of matter to Propose Fed.	Landar D11 370 p1 peluhas lake HD11 had
11 1010 1010 1010 1010 1010	anter a for former	
	team, New York	Nu hait
Power Usage ()	Pol Port Availability :	Pof AP Power Mode Datribution
960W There is an a function	Name and Name	2
 All has basics (M) = take the dense (A) = take 51 has been all has been been been been been been been bee	ne	Frag hardelit Physics Sector 11 Sector 2

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

E Cisco DNA Center	System / Settings		\$ Q @ C Q
59. Search Settings	Settings / Central Services	Add CMX Server	×
Class Accounts ~ Class com Oredentials PoP Connect SSM Connection Mode Smart Account Smart Ucensing Device Settings ~ Configuration Archive	CINIX Servers/CISCO Spaces To integrate Disco DNA Center with Class Spaces, please provide the Class Spaces tenant token. To integrate Cisco DNA Center with CMX Servers, please provide the CMX Server credential. Cisco Spaces Actives Struts Onto Registered Tenant None CMX Servers	P Addess* 10.4.48.228 Over Torne* admin Passnorf* 	2-04
Device Controllability Device EULA Acceptance Device Prompts ICMP Ping	As of Jun 1 O Selected IP Address - User Name	SSR Patracet*	1-01
Image Distribution Servers Network Resync Internal PriP Device Authorization SNMP	No data to display		
External Services \checkmark Authentication and Policy Ser			8
CMX Servers/Cloco Spaces Cloco Al Analytics Cloco DNA - Cloud			
Cloud Access Login Cloud Authentication Destinations		Cano	

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 1	198:サイ	トへの	СМХ Ф.	割り	当て
-----	--------	-----	---------------	----	----

■ Cisco DNA Center	Design / Network Settings	Q @ C 4
Network Device Credentials	IP Address Pools SP Profiles Wireless Telemetry Security and Trust	
Q Find Hierarchy Search Help	Cisco Spaces/CMX Servers 🛛 Save 🕕 Remove 🗁 Reset	
 එ Global එ US එ Milpitas 	Location Services Step 2 Select the CMX Q [Search	
 > I Building 23 > I Building 24 > I NewYork 	10.4.48.228 Seset	
> & Sanjose Step 1 Select Site	Native VLAN ID VLAN ID range is 14094	

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

■ Cisco DNA Center	Design / Network Settings / Wireless
Q Search Hierarchy Search Help	All / Cisco Spaces Cisco Spaces/CMX Servers
◇ 命 Global ◇ 命 US	Cisco Spaces settings are inherited by all children sites. Overrides done at the child level do not affect the parent.
ບ ທີ່ Milpitas	Location Services
> Ell Building 23	10.4.48.228 Clear
> Ell Building 24	
V 🗟 NewYork	
> Bl Branch 5	
✓ d₀ Sanjose	
> Bill Eventcenter	

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。



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

cisco 10.6.3-146	Last Successful Login - 2023-06-15 16:32:02 1 Faled Attempt since last successful login Click here for imere details	DETECT ANALY	rics manage	SYSTEM	👘 admin -
≡					Map Troubleshooting
(III)(II) cax cisco 1083346 tanĝ cisto 1083346 tanĝ cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto Cisto 1083346 tanĝ Cisto Cis	Activity Map		Click here	to add WLC to CMX	1 Campus, 2 Buildings, 4 Floors, 0 Zone
	Colored Periodicity Bateria		n (jal 22,240) 4 Mah Nager Nagera		

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

IIII CMX ISCO 10.6.3-1	Last Succ 46 1 Failed / Click here	cessful Login - 20 Altempt since las e for more details	123-06-15 16:32:02 t successful login				DE & L	♥ TECT OCATE	ANALYTICS M		SYSTEM) ••	min •
	12.5%	an an a tha tha tha tha tha tha tha tha tha t											Dashboard	Alerts P	itterns	Met
Coverage D	Details															
Access Point				Map Eleme	ents				Active Devices							
Placed AP	Missing AP	Active AP	Inactive AP	Campus	Building	Floor	Zone	Total	Associated Client	Probing C	lient RFID Ta	g Interferer	Rogue AP	Rogue Clie	t Tota	1
5	0	0	0	1	2	4	0	7	0	0	0	0	0	0	0	
ontrollers											\langle	Click "+" to add	WLC to CMX			+
P Address		Versio	n		Byte	is In			Bytes Out First Hea	ard	La	st Heard		Action		
								No Cont	rollers.							
						Act	ive 📒	Missing (Details 📕 Inactive							

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

SETTINGS	Lool Susseenful Looin 2022 66 16 18 64 60	** 0	668	
ETTINGS				
Fracking				
Filtering	Import from Cisco Prime			
ocation Setup	Please provide Cisco Prime credentials below:			
Data Privacy	Username	Password		
	Enter Username	Enter Password		
Data Retention	IP Address -			
Mail Server	Enter IP Address			
✓ Controllers and Maps Setup	Save Cisco Prime Credentials			
Import	Delete & replace existing maps & analytics data			
Advanced	Delete & replace existing zones		C Import Contro	ollers and Maps
Upgrade	*P tring after import.			
High Availability	Click on Advanced to add individual WLC			
Smart Liconso	▶ Controllers			
Smart License	Last Synced: N/A			
	▶ Maps			
	Last Synced: N/A			
			C	Close Sa
	Active Missing Details	nactive		

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

Mail Server	Delete & replace existin	g zones
✓ Controllers and Maps Setup	Upload	
Import	Controlloro	
Advanced	Controllers	
Uporade	Please add controllers by	providing the information below:
00.000	Controller Type	Catalyst (IOS-XE) WLC 👻
High Availability	ID Address	10.4.50.2
Smart License	IF Addiess	10.4.50.2
	Controller Version [Optional]	17.11.1
	Username	assurance
	Password	
	Enable Password	
	Add Controller	
		Close Save

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

Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
0.4.50.2	17.11.01	4 KB	469 Bytes	06/15/23, 5:02 pm	12s ago	Edit Delete

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

← → C a dnaspaces.io/home				
CISCO SPACES				
Home		(([NA	Ð
Integrations	>		No access points data available	
Admin Management				
IoT Services	>			
{ộ} Setup	>	erience usir	ng these Apps available in your SEE s	ubscription



図 206:新しいトークンの作成

Create new 1	oken	~
	Enter the Cisco DNA Center Instance name	
	Instance Name	
	CVDDNAC	
Oreste Takan		

- 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

System / Settings Q (© C	5 0
Settings / External Services	
DNA Spaces/CMX Servers	
Provide the credentials to enable CMX server connectivity by Cisco DNA Center and Provide the token to active DNA Spaces	
DNA Spaces Activate	
Status O Not Registered	
Pasta X	
Integrate DN the Token from	
dnaspaces.io into this	
space	
X	
Terror Teller	
Cancel Connect	
	<page-header></page-header>

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

etup > Connectors >	DNACConn	ector		1	D:7403841577	684727000 Last Mo	dified : Jun 21, 2023, 10:07:40 AN
S	UMMAR	Y					
) Istances	0 Active	0 Inactive	2 Services enabled	0 Controller	0 Switches	
Configuration	Instance	s Metrics			0	C Generate Token	Troubleshoot Connector
Services							GAdd Services
Service Nam	e	Version	Last	t Updated	Actions		
O Service M	lanager	3.1.0.104	Jun 10:0	21, 2023, 07:40 AM			
O Location		3.1.0.66	Jun 10:0	21, 2023, 07:40 AM			
Controllers					≣Q,	Find Controllers	Add Controller

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

S	PACES Connect	tor 3.1
6	Dashboard	
6	Configure Connector	
0	Configure HTTP proxy	
â	Privacy Settings	Configure the token below to activate your connector
P	Manage API Keys	Note: If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.
	Troubleshoot	Token
		Configure
		Don't have the token? Click Here for the Step by Step Guide V

- **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] > [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

E Cisco DNA Center	System / Settings		0000
59. Search Settings	Settings / External Services	Add CMX Server	×
Ciaco Accounta	CMX Servers/Cisco Spaces	P Aldests"	
Cisco.com Credentials PriP Connect	To integrate Cisco DNA Center with CMX Servers, please provide the CMX Server oredential.	10.4.48.328	
SSM Connection Mode	Cisco Spaces Actuate	User Nome* admin	
Smart Account	Status O Not Registered Tenant None	Personal*	
Device Settings			5-QW
Configuration Archive	CMX Servers	STOL User Name* cmxadmin	
Device EULA Acceptance	-	An of Jun 1 Still Pantword*	1-010
Device Prompts	D Selected		
Image Distribution Servers	No data to display		
Network Resync Interval			
SNMP			
External Services			
CMX Servers/Cisco Spaces			
Cisco Al Analytics			
Cisco DNA - Cloud Cloud Access Login		Cance	Att
Cloud Authentication			
Destinations			

- **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

■ Cisco DNA Center	Design / Network Settings	$Q \odot C \varphi$
Network Device Credentials	IP Address Pools SP Profiles Wireless Telemetry Security and Trust	
Q Find Hierarchy	Cisco Spaces/CMX Servers Save CRemove Step 3 Cick Save	
∨ ສີ Global ∨ ສີ US ∨ ສີ Miloitas	Location Services Step 2 Select the CMX	
> Building 23 > Building 24 > ➾ NewYork	amove ← Reset 10.4.48.228 VLAN for all FlexConnect Access Points managed in the site ♀	
> & Sanjose Step 1 Select Site	Native VLAN ID VLAN ID range is 14094	

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

≡ Cisco DNA Center	Design / Network Settings / Wireless
Q Search Hierarchy	All / Cisco Spaces
Search Help v ଜି Global v ଜି US	Cisco Spaces/CMX Servers Cisco Spaces settings are inherited by all children sites. Overrides done at the child level do not affect the parent.
 ◇ Ø Mipitas > Ø Mipitas > Ø Building 23 > Ø NewYork > Ø Branch 5 ◇ Ø Sanjose > Ø Eventcenter 	Location Services 10.4.48.228 Clear

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

Last Successful Login - 2023-06-15 16:32:02 CISCO 10.6:3-146 Cisk here for more details					ANALYTICS	ANALYTICS MANAGE SYSTEM		тем				👔 admin -					
														Dashboard			
Coverage [Details																
Access Point	8			Map Eleme	ents				Active Devices								
Placed AP	Missing AP	Active AP	Inactive AP	Campus	Building	Floor	Zone	Total	Associated Clie	nt Probing	Client	RFID Tag	Interferer	Rogue AP	Rogue Clie	nt Tota	6
5	0	0	0	1	2	4	0	7	0	0		0	0	0	0	0	
Controllers							Healthy	Warr	ning Critical			Cli	ck "+" to add	WLC to CMX	>	_	+
IP Address		Versk	n		Byte	is In			Bytes Out First H	leard		Last	Heard		Action		
								No Cont	rollers.								
						Act	tive <mark>–</mark>	Missing [Details 📕 Inactive								

3. [Controllers and Maps Setup] で [Advanced] をクリックします。

☑ 217 : [Controllers and Maps Setup] : [Advanced]

ullully ow	Lost Sussessibilit poin - 2022 DE 15 16 51 50	B	¢\$	å	•
SETTINGS					
Tracking					
Filtering	Import from Cisco Prime				
Location Setup	Please provide Cisco Prime credentials below:		Password		
Data Privacy	Enter Username		Enter Password	1	
Data Retention	IP Address 🔹				
Mail Server	Enter IP Address				
✓ Controllers and Maps Setup	Save Cisco Prime Credentials				
Import	Delete & replace existing maps & analytics of	data			
Advanced	Delete & replace existing zones			C Import Co	ontrollers and Maps
Upgrade	*P> tring after	r import.			
High Availability	Click on Advanced to add individual WLC				
Smart License	 Controllers 				£
	Last Synced: N/A				
	▶ Maps				£
	Last Synced: N/A				
					Close Save
	Active Missing Det	ails 📕 Ind	active	_	

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。

Mail Server	U Delete & replace existi	ng zones	
✓ Controllers and Maps Setup	Upload		
Import	0		
Advanced	Controllers		
Upgrade	Please add controllers by	providing the information below:	
	Controller Type	Catalyst (IOS-XE) WLC -	
Smart License	IP Address -	10.4.50.2	
	Controller Version [Optional]	17.11.1	
	Usemame	assurance	
	Password		
	Enable Password		
	Add Controller		
			Close Save

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

	Last Heard Action
10.4.50.2 17.11.01 4 KB 469 Bytes 06/15/23, 5:02 pm	12s ago Edit D

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。 **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。

☑ 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。

🗵 224 : [Choose Faulty Device]

■ Cisco DNA Center	Replac	e Device	☆ Q @ 凸 Q
Choose Faulty Choose the device you wa	Device nt to replace in order to proceed with	the device replacement.	
AP (1)			٢
Q Search Table			∇
Reachability All Re	IP Address Serial Number	Reachability Device Family	Platform
mil23-floor2-ap1	10.4.60.100 FJC26361HAD	Unified AP Unified AP	C9130AXI-B
1 Records		Show Records: 25 🗡 1 - 1	< 0 >
Exit All changes saved		Review	Back Next

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。

☑ 226 : [Choose Replacement Device]

⊟ Cisc	o DNA Center			Replace Device	9		\$ Q @ ₫ ₽	
Choose Replacement Device								
	You have selected to replace mil23-floor2-ap1. Now, it is time to choose your replacement device.							
	Replacing mil23-floor2-ap1							
	IP Address Platform Serial Number Software Version Available Repla Below is the suitt and Play and Mai Source Unclaim	10.4.60.100 C9130AXI-B FJC26361HAD 17.11.0.155 accement Device able replacement naged devices an managed	es (2) s for your device. U e the ones that are	nclaimed devices ar onboarded through I	e ones that are onboard nventory or Discovery.	ed through Plug		
	Q Search Table	2					∇	
	Device Name	-	IP Address	Status	Serial Number	Platform		
	• AP1416.	9D7C.1750	10.4.60.109	Managed	FJC24411TRJ	C9130AXI-B		
	O mil23-flc	oor1-ap2	10.4.60.104	Managed	FJC242615XS	C9130AXI-B		
	2 Records			Sh	ow Records: 25 🗸	1 - 2	< 0 >	
🕣 Exit 🛛 All c	hanges saved					Review Bac	k Next	

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。
🗵 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

≡	Cisco DNA Center	Replace Device 🖈	Q	0 0	4
	Summary We are almost t now is the time	/ here. Review the summary below to be sure we have got everything covered. If you need to update anything, to do it.			
	 Device Typ Type AP 	e Edit			
	 Faulty Devi Name Serial Number 	C0 Edit mil23-floor2-ap1 FJC26361HAD			
	 Replaceme Name Serial Number Replacement of OS Image 	nt Device Edit AP1416.9D7C.1750 FJC24411TRJ Ievice will be configured with the following settings 7.11.0.155			
	 Schedule R Schedule Date Schedule Option 	eplacement Edit 2023-06-22 16:00 (America/Los_Angeles) on Now			Ĩ
Ex.	it All changes saved	Back		Repla	ce

- **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

twork / Device 360					
P mil23-floor2	-ap1			L Dawel	Run OTA Capture
				+ Down	
3 Hours 🗸					Intelligent Capture
10:06p					4:06
5	\frown	$\wedge \wedge \land$			
•					
1:30p	2p Jun 22, 2023 4:00 PM	2:30p System Resources	3p Events	3:30p	4:00 pm - 4:05 pm
	Device Health: 6	Memory Utilization 10 0%	AP RMA	4:02:51 PI	
	Device Health is the minimum of all KPI Health Score.	CPU Utilization 10 0%		e 4:02:31 Pl	
	* - The KPI is not included for Health Score	Data Plane	 AP is connected to WLC. 		
		Link Errors 10 0%	AP is disconnected from	WL 4:01:35 PI	
		Radio 0 Ri (2.4GHz) (5	See Full List (3 Events)		
		Noise 6 -47 dBm -8			
		Interference 10 0% 0!			
		Radio 10 0% 0!			
<i>I:</i> イベント ビューフ Cisco DNA Center	7				☆ Q ⊘
D:イベントビューフ Cisco DNA Center work / Device 360	7				☆ Q ⑦
D:イベントビュー: Cisco DNA Center work / Device 360 ・ Event Viewer Go to Global Event	₽ Viewer		€ f_ Export		★ Q @
D:イベントビュー: Cisco DNA Center Noork / Device 360 ・ Event Viewer Go to Global Event	Viewer		t Export		☆ Q ③
D:イベントビュー: Cisco DNA Center work / Device 360 * Event Viewer Go to Global Event Q Search Table	Viewer		t Export ▽	• AP RMA	☆ Q ⑦
D:イベントビュー: Cisco DNA Center work / Device 360 ・ Event Viewer Go to Global Event Q Search Table Details	Viewer	Event Time	t Export ▽	AP RMA Detailed Infor	☆ Q ③
D:イベントビュー: Cisco DNA Center work / Device 360 Cisco Event Viewer Go to Global Event Q Search Table Details	Viewer	Event Time	t Export ↓	AP RMAN Detailed Infor WLC Name	
D:イベントビュー: Cisco DNA Center work / Device 360 Cisco DNA Center Go to Global Event Q Search Table Details	7 Viewer	Event Time 4:02:51.863	t Export √ PM	AP RMAN Detailed Infor WLC Name AP Mac	
D:イベントビュー: Cisco DNA Center work / Device 360 Cevent Viewer Go to Global Event Q Search Table Details	Γ Viewer	Event Time 4:02:51.863 4:02:31.079	Export ✓ PM PM	AP RMA Detailed Infor WLC Name AP Mac Eventype Benlared AP	
D:イベントビュー: Cisco DNA Center work / Device 360 Cevent Viewer Go to Global Event Q Search Table Details Configuration Changes AP Operational Discon	Viewer s nect - Tag Modified	Event Time 4:02:51.863 4:02:31.079 4:01:35.292	Export ✓ PM PM PM PM	AP RMAA Detailed Infor WLC Name AP Mac EventType Replaced AP Mac	
D:イベントビュー: Cisco DNA Center work / Device 360 Cevent Viewer Go to Global Event Q Search Table Details Configuration Changes AP Operational Discon	Viewer	Event Time 4:02:51.863 4:02:31.079 4:01:35.292	▲ Export PM PM PM PM	AP RMAA Detailed Infor WLC Name AP Mac EventType Replaced AP Mac Replaced AP Serial Number	

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

2	Access Point Refresh
	Replace Your Access Points with New
	ones
Wirel	ess
	000

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。

233 : [Select Access Points]

■ Cisco DNA Center	-	le l	Access Point Refr	esh		\$ Q @ ₫ ₽
Select Ac Select the Acces so please make t	CCESS Points Is Points you want to replace. Yo sure the locations of selected Ac	ou can select upto 250 Acces ccess Points in this workflow	is Points in a workflo are provisioned with	w. This workflow does provision of new Access Poir Wireless Controller from Cisco DNA Center.	nts,	
Q, Search Hierarchy Search Help ✓ ■ & Global (1) ✓ ■ & US	ACCESS POINTS (2) Q Search Table 1 Selected Reachability:	Al Reschable Unreachab	te			V
V S Milpitas	Device Name • Plat	tform Serial Number	Mac Address	Series	IP Address	Site
Ploor 1 Ploor 2	mil23-floor1-ap1 C9	130AXI-B FJC24411TV2	54:8a:ba:ff:05:c0	Cisco Catalyst 9130AXI Series Unified Access Points	10.4.60.101	Global/US/Milpitas/Building
_ ⊕ Floor 2 > _ ∰ Building 24 > _ ⊛ NewYork > _ ⊕ Sanjose	2 Bernrifs	130AXI-8 FJC242615XS	14:16:9d:e1:b1:40	Cisco Catalyst 9130AXI Series Unified Access Points	10.4.60.104	Giobal/US/Milpitas/Building
€] Exit	x neuros			anow Records. 20	iew B	ack Next
Exit				Rev	iew B	ack Next

- 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

	Cisco DNA Center		Access Point Ref	íresh				
	Assian New APs t	o Old APs						
	You have selected 1 Old APs fo will be detected in Cisco DNA (r refresh. Assign Nev Center either through	w AP for each Old one. If New AP(s) is alr WLC inventory or PnP based on the existi	eady connected, it ng configuration. If				
	New AP is not yet connected, p You can also download the Old Upload it.	New AP is not yet connected, provide the sensi Number of those New AP's against each Uid AP. You can also download the Old APs list in CSV format, provide the details of the New AP against each Old AP and Upload It.						
	ACCESS POINTS (1)	ACCESS POINTS (1)						
	Q. Search Table	For bulk refresh of AP	's download the template and till the AP details and upload				∇	
	▼ Upload CSV ± Download CS	v						
	Old Devices	201		New Devices	5-200			
	mil23-floor1-ap1	Platform C9130AXI-B	Site Global/US/Milpitas/Building 23/Floor 1	mil23-floor1-ap1	Platform	Serial Number* ()	Edit	
	10.4.60.101 FJC24411TV2	Cisco Catalyst 913.	-					
			C	If only one device need	to be refreshed the	en click on the pencil		
						uparted man		
								- 1
€ Exe	(i)					Review	Back	Next
× 23	5:計神の編集							
≡	Cisco DNA Center		Access Point Ref	fresh			\$ Q @	000
	Assign New APs t	o Old APs						
	You have selected 1 Old APs fo will be detected in Cisco DNA (r refresh. Assign Ner Center either throu puide the Serial N	w AP for each Old one. If New AP(s) is all	ready connected, it	×			
	You can also download the Old	APs list in CSV fo	Edit details					
	Upload it.							
	ACCESS POINTS (1)		Old Device mil23-floor1-ap1(FJC24-	411TV2)				
	Q Search Table		New AP Name*				Q	
	TUpload CSV ± Download CS	v	Choose Platform ID					
	Old Devices		C9124AXD-B		<u>×</u>			
	Device Name	Platform	Choose Serial Number* FJC27101QME (Managed)		, m	Serial Number* 🕕	Edit	
	10.4.60.101 FJC24411TV2	Cisco Catalyst S	Note: Serial Number validation is relaxed her	e to help user to clear th	is .		0	
			field on wrong entry.					
			Cancel	Save				

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。

€ Exit

Back

Review

図 236: 古い AP から新しい AP への設定のコピー

Configuration to be	
	e copied from Old APs to New
now configuration will be copi	ied from Old AP to New AP as applicable. User can change the an AP provisioning or "Configure Access Points" workflow.
bu have 1 Old APs to be refresh	ed with New APs
of 1 Old APs are 'Provisione	d' using Cisco DNA Center
ocation Configuration	
P Location, Position on Floor Map, A	ntenna Angle Parameters (Azimuth and Elevation as applicable) will be copied from Old APs.
/LC/AP Configuration	
ireOS WLCs - AP Name, AP Mod ontroller	le, AP Groups including RF Profiles, FlexConnect Groups, Primary/Secondary
isco Catalyst 9800 Series WLCs rimary/Secondary Controller	- AP Name, AP Mode, Policy Tags, Site Tags, RF Tags, Fiex Profiles,
review Configurations	
ote : The following AP attributes are vel, Radio level attributes. These car	not copied from the old AP to the new AP : AP Failover Priority, AP Admin status, AP Modes - Monitor, Sniffer, Bridge, Flex+Bridge, AP LED Status & Brightness to configured on the APs using the 'Configure Access Points' workflow once the AP Refresh is done.
	Review Back
存関係の解決	
字関係の解決	
字関係の解決 DNA Center	Access Point Refresh
字関係の解決 DNA Center	Access Point Refresh 対
字関係の解決 DNA Center Resolve Depender	Access Point Refresh 🛪
存関係の解決 DNA Center Resolve Depender	Access Point Refresh 🖈
字関係の解決 DNA Center Resolve Depender lependencies are met. Proceed v	Access Point Refresh 🖈
字関係の解決 DNA Center Resolve Depender Rependencies are met. Proceed to Device EULA Acceptance	Access Point Refresh * Incies with provisioning of New Access Points
字関係の解決 DNA Center Resolve Depender Pependencies are met. Proceed v Device EULA Acceptance ⊘ Accepted	Access Point Refresh * ICIES with provisioning of New Access Points
字関係の解決 DNA Center Resolve Depender Pependencies are met. Proceed to Device EULA Acceptance ⊘ Accepted	Access Point Refresh *
字関係の解決 DNA Center Resolve Depender Rependencies are met. Proceed to Device EULA Acceptance ⊘ Accepted	Access Point Refresh
字関係の解決 DNA Center Resolve Depender Rependencies are met. Proceed to Device EULA Acceptance ⊘ Accepted AP Connected SwitchPort ○ R to detected that New AP is not con	Access Point Refresh 🖈 Icies with provisioning of New Access Points rected to the same switch port of the Oid AP. If different port is to be used for New AP, ensure that reachability through the port has been established already.
字関係の解決 DNA Center Resolve Depender Rependencies are met. Proceed in Device EULA Acceptance ⊘ Accepted AP Connected SwitchPort © R is detected that New AP is not con v Access Points Detaits:	Access Point Refresh 🔅
字関係の解決 DNA Center Resolve Depender Rependencies are met. Proceed to Device EULA Acceptance ⊘ Accepted AP Connected SwitchPort © R is detected that New AP is not con v Access Points Details: DE AP Name:	Access Point Refresh * Incies with provisioning of New Access Points rected to the same switch port of the Oid AP If different port is to be used for New AP, ensure that reachability through the port has been established already. mi22-froor1-ap1
字関係の解決 DNA Center Resolve Depender Pependencies are met. Proceed Device EULA Acceptance ⊘ Accepted Accepted AP Connected SwitchPort © It is detected that New AP is not con ~ Access Points Details: Oid AP Sarial No:	Access Point Refresh
字関係の解決 DNA Center Resolve Depender Rependencies are met. Proceed Device EULA Acceptance ◇ Accepted Accepted AP Connected SwitchPort ○ R is detected that New AP is not con ◇ Accepted Otal AP Name: Otal AP Samati No Otal Port	Access Point Refresh
字関係の解決 DNA Center Cessolve Depender Resolve Depender Pependencies are met. Proceed = Device EULA Acceptance ② Accessed AP Connected SwitchPort ③ It is detected that New AP is not con ③ Access Peints Detais: Old AP Serial No.: Old AP Serial No.: Old AP Serial No.: Old port: New AP Serial No.: New Not:	Access Point Refresh
存関係の解決 DNA Center Resolve Depender Device EULA Acceptance ○ Accepted AP Connected SwitchPort ○ It is detected that New AP is not con ◇ Accepted Cold AP Sarrial No.: Cold AP Sarrial No.: Cold Spiral No.: Cold Spiral No.: New AP Sarial	Access Point Refresh 🖈
存関係の解決 DNA Center Resolve Depender Dependencies are met. Proceed 1 Device EULA Acceptance ② Accepted Accepted New AP Serial No.: Old AP Serial No.: Old AP Serial No.: New AP Se	Access Point Refresh 🖈 Incies with provisioning of New Access Points rected to the same witch port of the Oid AP. If different port is to be used for New AP, ensure that reachability through the port has been established already. mi23-fbort1-ap1 KIC234111V2 GigabetThermet2701 KIC231010ME GigabetThermet2701 KIC231010ME GigabetThermet2701 KIC231010ME
存関係の解決 DNA Center Resolve Depender Device EULA Acceptance ② Accepted Accepted AP Connected SwitchPort ③ It is detected that New AP is not con ◆ Access Points Details: Old AP Name: Old AP Sarial No.: Old Point: New AP Sarial No.: New Sort: New	Access Point Refresh
存関係の解決 DNA Center Resolve Depender Dependencies are met. Proceed Device EULA Acceptance ② Accepted Accepted SwitchPort OI til & detected SwitchPort OI til & detected SwitchPort OI til & detected SwitchPort Cold AP Serval No.: Oid AP Serval	Access Point Refresh
存関係の解決 DNA Center Resolve Depender Device EULA Acceptance ② Accepted Accepted New port: New port: New port: New port: New port: New port:	Access Point Refresh
存関係の解決 DNA Center Resolve Depender Pependencies are met. Proceed * Device EULA Acceptance ② Acceptad AP Connected SwitchPort ③ It is detected that New AP is not con ③ Access Points Detais: ① Of AP Serial No.: ① Of port: New AP Serial No.: New Dort: New AP Serial No.: New Dort: Location:	Access Point Refresh

Exit

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。

Review Back Next

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

Cisco DNA Center			Access Point Refresh		\$ Q	004
	Summary Review details before submitting the	ə taşk.				
	~ Task Name APrefresh					
	 Access Points Edit 					
	Q Search Table					
	Old Devices			New Devices		
	Device Name	Platform	Site	Device Name	Platform	Serial Numb
	mil23-floor1-ap1 10.4.60.101 FJC24411TV2	C9130AXI-B Cisco Catalyst 913	Global/US/Milpitas/Building 23/Floor 1	mil23-floor1-ap1	C9124AXD-B	FJC27101
	1 Records			Show Re	cords: 10 🗸	1-1
	 Configuration to be copied from Old APs to New View 					
	Location Configuration					
	AP Location, Position on Floor Map Old APs.	o, Antenna Angle Paramete	rs (Azimuth and Elevation as applicable) will t	be copied from		
Exit				Review	Back	Provision

- **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

The replacement Check the table b If there is any error	of each old AP will beg elow for the status of in or occurred during repla	in when the correspondindividual AP replacement acement then use 'Retry	ing new AP is conne it and cause for any ' option to retrigger	cted and the old AP is failure. replacement.	unreachable.		
Note: If the new A 'PNP Claim proce	AP is not timely discove ss in progress', please r	red in inventory and cor resync the WLC ()	Provision rep	port could be downloaded y clicking here	og for new	device to be co	nnected' or
1 Sites 1 Dev	vices	🔔 Download R	Report	© 01 PROVISIONED	S 00 FAILED	DO PENDING	© 00 IN PROGRESS
ACCESS PC	DINTS						
BU	LDINGS & FLOORS	ACCESS POINTS	PROGRESS		STATUS		
e (Global/US/Milpitas/Building 23						
		1			• • 1 P	rovisioned	

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。

E Cisco DNA Center * 2 0 0 4 Network / Device 360 AP mil23-floor1-ap1 Run OTA Captur 1 Dov load () 3 Hours 🗸 18 5. o o 9:30a 11:50 am - 11:55 am Jun 22, 2023 11:50 AM Device Health: 1 Events Events • AP is connected to WLC. C., • AP Refresh • AP Refresh • AP is disconnected from WL, • Tx Power Change 11:54:06 AM 11:53:41 AM 11:53:41 AM 11:53:15 AM 11:52:11 AM CPU L Device Health is the mini of all KPI Health Score. Data Pia Link Errors Radie 0 Radie 1 (2.40Hz) (50Hz) -61 dBm -74 dBm 100% 95% 82% 44% See Full List (6 Events) 1 10 1 Air Quality Interference Radio Utilization 6 85% 45%

図 241:デバイス 360

図 242:イベント ビューア

/ Device 360			
Event Viewer			
Go to Global Event Viewer	🕁 Export		
Q. Search Table	∇	AP Refreshium	22, 2023 11:53:41 AM
Details	Event Time	Detailed Informat	ion
Configuration Changes	11:54:06.802 AM	WLC Name	C9800-40-CVD cavalab local
AP Refresh - AP has been updated	11:53:41.839 AM	AP Mac	54:8A:8A:FF:05:00
AP Refresh - AP has been updated	11:53:41.839 AM	EventType	AP Refresh
		Reason	AP Refresh - AP has been updated
AP Operational Disconnect - Tag Modified	11:53:15.794 AM	Replacing AP Mac	C8:28:E5:40:50:C0
Radio Slot : 1 (5.0GHz) Power: 4 dBm -> 1 dBm System Driven	11:52:11.869 AM	Replacing AP Serial Number	FUC27101QME
Radio Slot : 0 (2.4GHz) Power: 9 dBm -> 6 dBm System Driven	11:52:02.451 AM		
22 records Show Re	cords: 25 V 1 - 24 ()		

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 Al 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 Al 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PF プロファイルの提合、このチェックボックフロナンになります。
		BANF ノドノナイルの物白、このナエツク かツク へはオ イになります。

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] >	[Multiple Choice]	5GHz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。
	オプションボタ ン	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] >	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。
[KX SOP]		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 フロファイルの場合、ナヤネル幅は 20 MHz に設定され ます。
[PROFILE TYPE] > [5 GHz] >	[Multiple Choice]	5GHz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。
[DCA Channel]	オブションボタ ン 	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5GHz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] >	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 フ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] >	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。
		向 KF ノロノアイルの場合、アヤイル幅は 20 MHZ に設正されます。

機能	タイプ	説明
[PROFILE TYPE] > [5 GHz] >	[Multiple Choice]	5GHz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。
	スノンヨンホタ ン	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5GHz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5GHz 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-10~30dBmで、増分単位は1dBm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] >	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5GHz 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] >	海粉の設定があ	「TDC Dower Threshold」はADのセル倍界にたける日的の電力レベルの
[TX Power Configuration] > [TPC Power Threshold]	る複数方向のス ライダ	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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

【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。

©2008 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, およびCisco Systems ロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。 本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。 「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R) 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。

cisco.

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。