



## 構築と展開のワークフロー

- [Cisco DNA Center ワークフローナビゲーション \(1 ページ\)](#)
- [デバイスの検出 \(2 ページ\)](#)
- [AP 更新ワークフロー \(3 ページ\)](#)
- [ユーザー定義ネットワークの設定ワークフロー \(6 ページ\)](#)
- [スイッチでのアプリケーションホスティングの有効化 \(9 ページ\)](#)
- [IoT サービスの有効化ワークフロー \(11 ページ\)](#)
- [Cisco DNA Center での AP 設定 \(12 ページ\)](#)
- [デバイスと既存のインフラストラクチャからデバイス構成を学習する \(22 ページ\)](#)
- [デバイスの交換ワークフロー \(27 ページ\)](#)
- [リモートサポート許可の作成 \(30 ページ\)](#)
- [イベント通知の作成 \(31 ページ\)](#)
- [リモート LAN の設定 \(35 ページ\)](#)
- [IP ベースおよび URL ベースのアクセスコントロールポリシー作成のワークフロー \(37 ページ\)](#)

## Cisco DNA Center ワークフローナビゲーション

Cisco DNA Center ワークフローはウィザードに似ています。ワークフローは GUI に組み込まれており、複雑すぎたり完了するには高度すぎるような多段階のタスクをガイドします。それらの多くには、さまざまなメニューオプションから、または [Workflows] メニューオプションから直接アクセスできます。

次のガイドラインを使用すると、ワークフローのナビゲートに役立ちます。

- ワークフローの手順に従い、[Next] をクリックして次のページに進みます。
- ワークフローの各ページの上部近くにカーソルを合わせると、進行状況バーが表示され、プロセスを完了するためのステップと現在実行中のステップが示されます。
- 一部のワークフローではダイアログボックスが開き、クリックすることでタスクの概要を視覚的に表示できます。タスクの概要の任意の時点で、[Let's Do it] をクリックして、ワークフローの最初に直接ジャンプできます。

今後タスクの概要をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

## デバイスの検出

このワークフローは、デバイス検出からネットワークの正常性までをガイドします。

### 始める前に

- [ディスカバリの前提条件](#)で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。
- シスコ検出プロトコル（CDP）を使用する場合は、ネットワークデバイスで CDP を有効にします。
- リンク層検出プロトコル（LLDP）を使用する場合は、ネットワークデバイスで LLDP を有効にします。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。（ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。）

- 
- ステップ 1** メニューアイコン（☰）をクリックして、[Workflows] > [Discover Devices] の順に選択します。
- ステップ 2** タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。
- ステップ 3** [Let's Get Ready] ウィンドウで、[Next] をクリックします。
- ステップ 4** [Discover Devices] ウィンドウで、次のフィールドに入力します。
- a) 検出ジョブの名前を入力します。
  - b) [Discovery Type] で、デバイスの検出に使用するプロトコルを選択し、次のように対応するフィールドを全て入力します。
    - [CDP] : [IP Address]、[CDP Level]、および [Subnet Filter] を入力します。
    - [IP Address Range] : [Starting IP Address] および終了 [Ending IP Address] を入力します。
    - [LLDP] : [IP Address]、[LLDP Level]、および [Subnet Filter] を入力します。
  - c) [Preferred Management IP Address] を選択します。
- ステップ 5** [Provide Credentials] ウィンドウで、少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Cisco DNA Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、[ディスカバリ クレデンシャル](#)を参照してください。
- ステップ 6** [Advanced Settings] ウィンドウで、次の手順を実行します。
- a) [Protocol Order] : [SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。

- b) [SNMP Polling Properties] を構成します。[Network Settings]> [Device Credentials] ウィンドウで定義されたグローバルSNMPポーリングプロパティを使用するか、この検出インスタンス用に変更します。

**ステップ 7** [Assign Devices to Site] ウィンドウで、次のいずれかを実行します。

- [Assign devices to an existing site] : [Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、[ネットワーク階層の検索](#)を参照してください。
- [Assign devices to a new site] : [Already have an area] オプションボタンまたは [Create a new area] ラジオボタンをクリックし、必須フィールドに入力します。
- [Skip site assignment for now] : 後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

**ステップ 8** [Schedule Task] ウィンドウで、次の手順を実行します。

- a) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。
- b) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

**ステップ 9** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

**ステップ 10** [Start Discovery and Telemetry] をクリックします。

[Activity] ページでタスクのステータスを確認できます。

## AP 更新ワークフロー

AP リフレッシュ機能を使用すると、アクセスポイントリフレッシュワークフローを使用して、プロビジョニングされた古い AP モデルとプロビジョニングされていない古い AP モデルの両方を新しい AP モデルに置き換えることができます。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。

デバイスの互換性については、「[Cisco DNA Center Compatibility Matrix](#)」を参照してください。

### 始める前に

- 古い AP が到達不能状態であり、サイトに割り当てられていることを確認します。
- 古い AP サイトは、新しい AP が関連付けられるワイヤレスコントローラの管理対象 AP の場所としてプロビジョニングする必要があります。
- 新しい AP は、どのサイトにも割り当てることはできません。

- 新しい AP をシスコワイヤレスコントローラに接続する必要があります。新しい AP は、Cisco DNA Center インベントリに登録されているか、プラグアンドプレイ (PnP) を介して Cisco DNA Center に接続できる必要があります。到達可能状態である必要があります。

**ステップ 1** 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。

(注) [Overview] ウィンドウが開いたら、[Let's Do it] をクリックしてワークフローを開始します。

**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。

**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。

**ステップ 4** [Assign New APs to Old APs] ウィンドウで、新しい AP の詳細を提供する方法を選択します。

- GUI を使用して新しい AP の詳細を追加するには、AP の編集アイコン (📎) をクリックし、[Edit details] ウィンドウで次の手順を実行します。

1. (オプション) 新しい AP 名を更新します。
2. (オプション) [Choose Platform ID] ドロップダウンリストから、新しい AP のプラットフォームを選択します。
3. [Choose Serial Number] ドロップダウンリストから、新しい AP のシリアル番号を選択します。

新しい AP がすでにワイヤレスコントローラに関連付けられ、インベントリに登録されている場合、Cisco DNA Center ではその AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Managed] として表示されます。

新しい AP が PnP で Cisco DNA Center に接続されている場合、Cisco DNA Center ではその AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Unclaimed] として表示されます。

新しい AP のシリアル番号がインベントリに登録されていない場合、そのシリアル番号は [Serial Number] ドロップダウンリストに表示されません。インベントリに登録されていない新しいシリアル番号を追加するには、[Choose Serial Number] ドロップダウンリストでシリアル番号を入力して [+] をクリックします。

4. [Save] をクリックします。

- コンマ区切り値 (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。

3. [Upload CSV] ウィンドウで、CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[Choose a file] をクリックして CSV ファイルの場所を参照し、[Open] をクリックします。

Cisco DNA Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。[View Details] をクリックすると、エラーメッセージの詳細が表示されます。

4. [Upload] をクリックします。

**ステップ 5** [Configuration Copied from Old Access Point to New] ウィンドウで、古い AP から新しい AP にコピーされる設定を表示します。

**ステップ 6** Cisco DNA Center でエラーまたは未解決の依存関係が検出されると、[Resolve Dependencies] ウィンドウが表示されます。続行する前に、次のようにエラーと依存関係を解決する必要があります。

- **デバイスの EULA への同意** : Cisco.com のログイン情報を指定して、デバイスのエンドユーザーライセンス契約 (EULA) に同意します。
- **シスコ ワイヤレス コントローラ ソフトウェア イメージ バージョンの更新** : AP の更新を続行できなくても、この依存関係を解決する必要があります。
- **AP が接続するスイッチポート** : AP の更新を続行できなくても、この依存関係を解決する必要があります。

**ステップ 7** [Schedule Access Point Refresh Task] ウィンドウで、[Now] をクリックします。または [Run Later] をクリックして AP 更新タスクを後の日時にスケジュールします。

**ステップ 8** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

**ステップ 9** [Track Replacement Status] ウィンドウで AP 交換ステータスをモニターします。

- AP の交換に成功した場合、[Replacement Status] に [REPLACED] と表示されます。
- AP の交換に失敗した場合、[Replacement Status] に [Error] と表示されます。

(注) 新しい AP がインベントリでまだ検出されておらず、対応する AP 更新エントリが新しいデバイスの接続を待機している場合、または PnP 要求プロセスが進行中の場合は、シスコ ワイヤレス コントローラを再同期します。

**ステップ 10** (任意) [Track Replacement Status] ウィンドウで、次のいずれかを実行します。

- AP 交換ステータスの詳細を確認するには、[View Details] をクリックします。
- 交換エントリを削除するには、[Actions] 列で青色の 3 つのドットをクリックし、[Delete] をクリックします。[Warning] ダイアログボックスで、[Yes] をクリックします。
- プロビジョニングの概要を CSV ファイルにダウンロードしてローカルに保存するには、[Export] をクリックします。
- プロビジョニング ステータス レポートをダウンロードするには、[Download Report] をクリックします。

**ステップ 11** [Next] をクリックして、更新の概要を表示します。

交換が正常に完了すると、Cisco DNA アシユアランス で古い AP と新しい AP についての AP 更新イベントが生成されます。

**ステップ 12** (任意) AP 更新イベントは、[AP View 360] ウィンドウの [Event Viewer] で確認します。

Cisco DNA Center では、[Network Hierarchy] ウィンドウの対応するフロアマップで、新しい AP が自動的に更新されます。

## ユーザー定義ネットワークの設定ワークフロー

ここでは、Cisco DNA Center でワークフローを使用して Cisco ユーザー定義のネットワークサービスを設定する方法を示します。

### ユーザー定義のネットワークサービスの概要

プリンタ、スピーカー、Apple TV、Google Chromecast、リングドアベル、スマート電球など、ネットワーク上のホームデバイス、コンシューマデバイス、IoT デバイスは、デバイスの検出と使用が簡単になるように、Apple Bonjour などの Simple Service Discovery Protocol (SSDP)、マルチキャスト DNS (mDNS)、ユニバーサルプラグアンドプレイ (UPnP) に依存しています。

シスコのユーザー定義ネットワークサービスは、寮の部屋、学生寮、教室、講堂などの共有環境において、クライアントデバイスのセキュアでリモートのオンボーディングを提供します。ユーザー定義のネットワークサービスを使用すると、SSDP (Apple Bonjour など)、mDNS プロトコル (AirPlay、AirPrint、画面ミラーリング、印刷など)、UPnP プロトコルのセキュアな使用が可能になり、共有環境におけるやり取りや共有を登録されたデバイスのみで行えるようになります。

ユーザー定義のネットワークサービスは、次のソリューションを提供します。

- クライアントデバイスの簡単でセキュアなオンボーディング。
- 特定のユーザーに属するクライアントデバイスの自動セグメンテーション。
- 他のユーザーを招待してデバイスを共有する機能。

### ユーザー定義のネットワークサービスを設定するための前提条件

Cisco ユーザー定義のネットワークサービスを設定する前に、次の前提条件を満たしている必要があります。

- AP がシスコ ワイヤレス コントローラ に参加していることを確認します。

- 検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内の シスコ ワイヤレス コントローラと AP を検出します。
- AAA サーバー クライアント エンドポイントを Cisco Identity Services Engine にマッピングします。
- 認証トークンを Cisco DNA Center に追加します。
- 非ファブリック エンタープライズ SSID またはゲストワイヤレス SSID を任意のセキュリティで作成し、ネットワークプロファイルにマッピングします。
- SSID をプロビジョニングします。

## Cisco ユーザー定義のネットワークの設定

この手順は、ワークフローを使用して Cisco User Defined Network (UDN) を構成する方法を示しています。

**ステップ 1** メニューアイコン (☰) をクリックして、[Workflows] > [Configure Cisco UDN] の順に選択します。

Cisco UDN は、[Provision] > [Services] > [Cisco User Defined Network] から設定できます。

**ステップ 2** タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

a) [Click here] をクリックします。

[Cloud Authentication] ウィンドウが開きます。

b) [Where did I get my token encryption key?] をクリックし、ダイアログボックスで [Go to the Portal] をクリックします。

[Cisco DNA - Cloud] アプリケーションが新しいタブで開きます。

c) Cisco.com アカウントの ID とパスワードを使用して [Cisco DNA - Cloud] にログインします。

[Cisco DNA - Cloud] ホームウィンドウが表示され、自身のリージョンのサブスクライブしているオフナーがカードとして示されます。

**ステップ 3** Cisco DNA Center が Cisco DNA Cloud に接続できるようにするには、Cisco DNA Cloud ポータルを使用して認証トークンを生成します。

a) [Cisco DNA - Cloud] GUI で [On-Prem Connections] を選択して、メニューアイコン (☰) をクリックして、クラウドサブスクリプションに Cisco DNA Center を登録します。

デフォルトでは、[ALL] タブが開き、青いチェックマークで強調表示されます。[ALL] タブまたは [Cisco DNA Center] タブから登録できます。

(注) Cisco DNA - Cloud ポータルで Cisco DNA Center の登録が断続的に失敗する。これは、すべてのリージョンで Cisco DNA - Cloud から Cisco DNA Center への通信障害が原因で、1 回おきの登録解除で発生する断続的な問題です。

b) [ALL] タブから登録するには、次の手順を実行します。

- [Register Product] をクリックします。  
[Register Product] スライドインペインが表示されます。
  - [Product Name] フィールドに、名前を入力します。
  - [Product Type] ドロップダウンリストから、[Cisco DNA Center] を選択します。
  - [Region] ドロップダウンリストから、オンプレミスの Cisco DNA Center の場所を選択します。
  - [Register] をクリックします。
  - Cisco DNA Center が正常に登録されると、[OTP Generated] ダイアログボックスが表示されます。OTP をコピーするには、[Copy] をクリックし、[close] をクリックします。
- c) または、次の手順に従って [Cisco DNA Center] タブから登録することもできます。
- [Register Cisco DNA Center] をクリックして、シスコとそのパートナーが提供する関連クラウドアプリケーションとサービスに製品を安全に接続します。  
[Register Cisco DNA Center] スライドインペインが表示されます。
  - [Cisco DNA Center Name] フィールドに、オンプレミスの Cisco DNA Center の名前を入力します。
  - [Region] ドロップダウンリストから、Cisco DNA Center の場所を選択します。
  - [OTP Generated] ダイアログボックスで、[Copy] をクリックして OTP をコピーし、[close] をクリックします。

**ステップ 4** [Cloud Authentication] ウィンドウに戻り、接続を確立します。

- a) Cisco DNA Center GUI でメニューアイコン (☰) をクリックして、[System] > [Settings] > [External Services] > [Cloud Authentication] の順に選択します。
- b) [Cloud Authentication] で、[Add OTP Key] をクリックします。
- c) [OTP Code] フィールドに、Cisco DNA - Cloud アプリケーションで生成してコピーした OTP を貼り付け、[Done] をクリックします。
- d) [Success] ダイアログボックスが表示されます。[OK] をクリックします。

**ステップ 5** Cisco DNA Center と Cisco DNA - Cloud 間の接続が確立されたかどうかを、[Cisco DNA - Cloud] > [On-Prem Connections] ウィンドウで確認します。

登録が成功すると、[Registration Status] 列にステータスが [Registered] と表示されます。

**ステップ 6** サイトを有効にし、ネットワーク上で Cisco UDN サービスをプロビジョニングします。

- a) Cisco DNA Center の [Welcome to Cisco User Defined Network] ウィンドウに戻ります。
- b) [Next] をクリックします。
- c) [Select Sites] ウィンドウで、次を実行します。
  - [Select Sites] ドロップダウンリストから、Cisco UDN サービスを有効にするサイトを選択します。
- d) [SSID] ウィンドウで、次の手順を実行します。
  - [SSID] ドロップダウンリストから、Cisco UDN サービスを有効にする SSID を選択します。



- 選択した SSID のユニキャストトラフィックを制限するには、[Unicast Traffic Containment] をオンにします。
- ユニキャストトラフィックの封じ込めを特定のサイトに適用するには、[Apply Individually] をクリックします。
- ユニキャストトラフィックの封じ込めをすべてのサイトに適用するには、[Apply to all] をクリックします。
- [次へ (Next) ] をクリックします。

**ステップ 7** [Scheduling] ウィンドウで、[Now] または [Later] をクリックして、Cisco UDN サービスをいつプロビジョニングするかを指定します。

[Next] をクリックします。

**ステップ 8** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

- a) [Connection Status] エリアを展開して、Cisco DNA Center と Cisco UDN Cloud 間の接続ステータスを表示します。

Cisco DNA Center と Cisco UDN Cloud 間の接続が確立されると、「Paired with Cisco DNA - Cloud」という成功メッセージが表示されます。

- b) [Configure] をクリックします。

次のウィンドウでは、完了した順に各ステップの横にチェックマークが表示されます。

---

## スイッチでのアプリケーションホスティングの有効化

次の手順は、ThousandEyes Enterprise Agent、iPerf などの Docker アプリケーションを特定のサイトの選択したスイッチで有効にする方法を示します。

### 始める前に

- 前提条件を満たします。詳細については、「[アプリケーションホスティングの前提条件](#)」を参照してください。
- アプリケーションを Cisco DNA Center に追加します。詳細については、「[アプリケーションの追加](#)」を参照してください。
- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、「[アプリケーションをホストするデバイスの準備状況の表示](#)」を参照してください。

---

**ステップ 1** メニューアイコン (☰) をクリックして、[Provision] > [App Hosting for Switches] の順に選択します。

**ステップ 2** アプリケーションを選択し、ウィンドウの下部にある [Install] をクリックします。

または、[Workflows] > [Enable Apps on Switches] > [Let's Do it] を選択してワークフローを起動することもできます。

(注) ウィンドウの上部にある青色の進捗状況バーにカーソルを合わせると、一覧表示される前の手順に戻ることができます。

**ステップ 3** [Select Site] ウィンドウで、アプリケーションを有効にするビルディングに移動します。

**ステップ 4** [Select App] ウィンドウで、選択するアプリケーションをクリックします。

(注) [+New App] リンクにアクセスして、Cisco DNA Center に存在しないアプリケーションを追加できます。

**ステップ 5** [Select Switches] ウィンドウで、アプリケーションを有効に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。

(注) [Select Switches] ダイアログボックスで指定したテンプレートに詳細を入力することにより、デバイスを一括でインポートまたはエクスポートできます。

**ステップ 6** [Configuration App] ウィンドウで、以降の設定を実行します。

- **App Networking**

- [Device Network] : [Select Network] ドロップダウンリストから、アプリケーションを設定する VLAN を選択します。

- [App IP address] : [Address Type] ドロップダウンリストから [Static] または [Dynamic] を選択します。[Static] を選択した場合は、サムネイルアイコンをクリックして、アプリケーションの [IP Address]、[Gateway]、[Prefix/Mask]、および [DNS] を入力します。

- [Resource Allocation] : [Allocate resources as asked by the app] または [Allocate all resources available on a device] チェックボックスをオンにします。

- [Custom Settings] : (Cisco パッケージアプリケーションにのみ適用) アプリケーションによって指定された属性の設定の詳細を入力します。

- [App Data] : アプリケーション固有のファイルを参照してアップロードします。必要なアプリケーション固有のファイルを特定するには、関連するアプリケーションのドキュメントを参照してください。

- [Docker Runtime Options] : アプリケーションに必要な Docker ランタイムオプションを入力します。

**ステップ 7** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

[Provisioning Task] ウィンドウに、スイッチでのアプリケーションの展開を追跡するタスク名が表示されます。

**ステップ 8** 自動生成されたタスク名を確認し、[Provision] をクリックします。

**ステップ 9** [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。

**ステップ 10** [View Details] をクリックして、個々のデバイスのプロビジョニングステータスと障害を確認し（ある場合）、[Next] をクリックします。

アプリケーションが正常に有効化されました。

タスクの結果の概要と成功/失敗の回数が表示されます。

**ステップ 11** [Manage App] をクリックします。ここで、アプリケーションのライフサイクル動作を管理して、N 日目のタスクを実行することができます。

## IoT サービスの有効化ワークフロー

ここでは、Cisco DNA Center の [Workflows] を使用して、Cisco Catalyst 9100 シリーズ アクセスポイントで Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効にする方法について説明します。

### Cisco Catalyst 9100 シリーズ アクセスポイントでの IoT サービスの有効化

この手順では、選択した Catalyst 9100 シリーズ アクセスポイントで、Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効にする方法を説明します。

**ステップ 1** メニューアイコン (☰) をクリックして、[Workflows] > [Enable IOT Services] の順に選択します。

**ステップ 2** タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

**ステップ 3** [Select Site] ウィンドウで、IoT サービスを有効にするフロアまで移動し、[Next] をクリックします。

**ステップ 4** [Select the Application] ウィンドウで、ネットワークで IoT を有効にするための SES-imagotag ESL Connector アプリケーションを選択し、[Next] をクリックします。

(注) Cisco DNA Center に存在しないアプリケーションを追加するには、「[アプリケーションの追加](#)」を参照してください。

[Select Access Points] ウィンドウには、特定のフロアで使用可能なすべての AP が表示されます。

**ステップ 5** [Select Access Points] ウィンドウで、IoT コネクタアプリケーションをインストールするデバイスの [Device Name] の横にあるチェックボックスをオンにして、[Next] をクリックします。

**ステップ 6** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

**ステップ 7** [Provisioning Task] ウィンドウが表示され、AP への任意のアプリケーションの展開を追跡するために作成されたタスク名が表示されます。自動生成されたタスク名を確認し、[Provision] をクリックします。

**ステップ 8** [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。[View Details] をクリックして、プロビジョニングステータスを確認し、[Next] をクリックします。

**ステップ 9** タスク完了 [Done! Task Completed] ウィンドウが表示されます。[Manage IoT Application] をクリックして、Day N タスクを実行します。

## IoT アプリケーションの管理

この手順では、IoT アプリケーションを管理する方法を示します。

### 始める前に

Cisco Catalyst 9000 シリーズ アクセス ポイントで IoT サービスを有効にしておく必要があります。

**ステップ 1** IoT サービスを有効にした後、[Done! Task Completed] ウィンドウで **[Manage IoT Application]** をクリックします。

**ステップ 2** [Hostname] の横にあるチェックボックスをオンにして、次のタスクを実行します。

- アプリケーションを起動するには、[Actions] ドロップダウンリストから **[Start App]** を選択します。
- アプリケーションを停止するには、[Actions] ドロップダウンリストから **[Stop App]** を選択します。
- アプリケーション設定を編集するには、[Actions] ドロップダウンリストから **[Edit App Config]** を選択します。
- アプリケーションをアップグレードするには、[Actions] ドロップダウンリストから **[Upgrade App]** を選択します。
- 選択した AP からアプリケーションをアンインストールするには、[Actions] ドロップダウンリストから **[Uninstall App]** を選択します。

**ステップ 3** AP 名をクリックして、AP 名、ステータス、IP アドレス、正常性などの詳細を表示します。

**ステップ 4** [Tech Support logs] をクリックして、アプリケーション ホスティング ログを収集します。

## Cisco DNA Center での AP 設定

[Configure Access Points] ワークフローを使用すると、AP の場所、管理ステータス、モードなど、AP レベルのパラメータを設定および展開できます。無線電力レベル、チャンネル設定、方位角、仰角などの無線レベルのパラメータを設定することもできます。

### AP ワークフローの設定

この手順では、Cisco DNA Center で AP および無線パラメータを設定する方法を示します。

[Configure Access Points] ワークフローを使用して設定された無線の管理ステータス、AP プライマリコントローラ、および AP セカンダリコントローラ情報などの設定は、ワイヤレスコントローラ または AP が再プロビジョニングされても上書きされません。

- ステップ 1** メニューアイコン (☰) をクリックして、**[Workflows] > [Configure Access Points]** の順に選択します。  
[Overview] ウィンドウが表示されたら、**[Let's Do It]** をクリックして、ワークフローに直接移動します。
- ステップ 2** [Get Started] ウィンドウで、[Task Name] フィールドにワークフローの一意の名前を入力し、[Next] をクリックします。
- ステップ 3** [How do you want to configure APs?] ウィンドウで、次の操作を行います。
- [Configure AP And Radio Parameters] オプションボタンをクリックします。
  - 実行するタスクの横にあるチェックボックスをオンにします。
    - **[Modify AP Name]**
    - [Configure AP Parameters]
    - [Configure 5 GHz Radio Parameters]
    - [Configure 2.4 GHz Radio Parameters]
    - [Configure 6 GHz Radio Parameters]
    - [Configure Dual-Band (XOR) Radio Parameters]
    - [Configure Tri-Radio Parameters]
- (注) オンにしたチェックボックスに基づいて、Cisco DNA Center では対応する後続の構成手順が表示されます。
- [Next] をクリックします。
- ステップ 4** [Select Access Points] ウィンドウで、次の手順を実行します。
- AP 関連の設定を適用するサイトに移動します。  
右側のペインに、選択したサイトで使用可能なすべての AP が一覧表示されます。
  - 設定する AP 名の横にあるチェックボックスをオンにします。
  - [Next] をクリックします。
- ステップ 5** (オプション) [Modify AP Name] ウィンドウで、次のいずれかの方法を使用して 1 つ以上の AP 名を変更します。
- **[Create a New Naming Convention]** : このオプションボタンをクリックして、命名規則に基づいて名前を入力し、**[Apply Pattern]** をクリックします。**[Access Points]** テーブルには、入力した命名パターンに基づいて新しい AP 名が表示されます。
  - **[Upload a CSV file]** : このオプションボタンをクリックして、サンプル CSV テンプレートファイルをダウンロードし、そのファイルに AP 名を追加します。次に、CSV ファイルをドラッグしてドロップエリアにドロップすることにより、または **[Choose a file]** をクリックし、CSV ファイルを参照して選択することにより、ファイルをアップロードします。
- ステップ 6** (オプション) [Configure AP Parameters] ウィンドウで、AP パラメータを設定します。

- [Admin Status] : 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [AP Mode] : このチェックボックスをオンにして、[Select AP Mode] ドロップダウンリストから AP モードを選択します。有効なモードは、[Local/Flexconnect]、[Monitor]、[Sniffer]、および [Bridge/Flex+Bridge] です。
  - (注) AP モードを [Monitor] または [Sniffer] から [Local/Flexconnect] に変更すると、Cisco DNA Center では次の設定が使用されます。

関連付けられた SSID で [FlexConnect Local Switching] が有効になっている場合は、Cisco DNA Center では AP に [FlexConnect] モードが設定されます。それ以外の場合は、AP に [Local] モードが設定されます。

割り当てられていない AP または割り当てられているがプロビジョニングされていない AP の場合、Cisco DNA Center では次のように AP に [FlexConnect] モードが設定されます。

    - Cisco AireOS ワイヤレスコントローラ : AP が存在する AP グループ内の関連付けられた SSID で [FlexConnect Local Switching] が有効になっている場合。
    - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ : AP の現在関連付けられている サイトタグで [Local site] が無効になっている場合。
- [AP Location] : このチェックボックスをオンにして、ロケーションの詳細を入力します。
- [AP LED Status] : AP LED ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [LED Brightness Level] : このチェックボックスをオンにして、[LED Brightness Level] から明るさのレベルを選択します。
- [AP Height] : このチェックボックスをオンにして、AP の高さをフィートで入力します。Cisco DNA Center での最小の高さは 3 フィートです。
  - (注) Cisco DNA Center で AP がフロアに割り当てられたときに、AP の高さが AP に適用されます。AP の高さがフロアの高さを超えないようにしてください。
- [AP Failover Priority] : このチェックボックスをオンにして、[AP Failover Priority] ドロップダウンリストから次のフェールオーバー優先順位のいずれかを選択します。
  - [Low] (デフォルト) : レベル 1 の優先順位。これは最も低い優先度レベルです。
  - [Medium] : レベル 2 の優先順位。
  - [High] : レベル 3 の優先順位。
  - [Critical] : レベル 4 の優先順位。これは最も高い優先度レベルです。
- [High Availability] : このチェックボックスをオンにして、AP のプライマリ、セカンダリ、およびターシャリコントローラの名前と IP アドレスを設定します。

プライマリコントローラとセカンダリコントローラに対して [Inherit from site / Clear] を選択した場合：

- プロビジョニングされた状態の AP の場合、AP が割り当てられているフロアのプライマリおよびセカンダリとして設定されたコントローラが、AP のプライマリおよびセカンダリコントローラとして設定されます。
- プロビジョニングされた状態にない AP の場合、現在のプライマリ、セカンダリコントローラの設定が AP から消去されます。

ターシャリコントローラの場合、[Clear] オプションのみが使用可能です。

- (注)
- コントローラで AP フォールバックが無効になっている場合、AP は新しく設定されたプライマリ、セカンダリ、およびターシャリコントローラに参加しません。
  - AP が ROW AP の場合は、コントローラの国のリストに、運用国のサポートが追加されていることを確認してください。コントローラの管理対象 AP ロケーションとして、運用国の少なくとも 1 つのサイトを設定する必要があります。

**ステップ 7** (オプション) [Configure 5 GHz Radio Parameters] ウィンドウで、5 GHz 無線パラメータを設定します。

- a) 5 GHz 無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

Cisco DNA Center では、5 GHz 無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。

- b) 次の 802.11 a/n/ac/ax パラメータを設定します。

- [Admin Status] : 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Power Assignment] : カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment] : カスタムチャンネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャンネル番号を選択します。
- [Channel Width] : チャンネル幅を選択するには、このチェックボックスをオンにし、チャンネル帯域幅を選択します。
- [CleanAir / Spectrum Intelligence] : CleanAir スペクトルインテリジェンスを無効にするには、このチェックボックスをオンにして [Disable] をクリックします。
- [Antenna Name] : アンテナ名を選択するには、このチェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。アンテナ名として [Other] を選択した場合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲインアンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ~ 40 です。

- [Antenna Cable] : アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ~ 40 です。
- [Azimuth] : 方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ~ 360 です。
- [Elevation] : 仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ~ 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

**ステップ 8** (オプション) [Configure 2.4 GHz Radio Parameters] ウィンドウで、2.4 GHz 無線パラメータを設定します。

- a) 2.4 GHz 無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

Cisco DNA Center では、2.4 GHz 無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。

- b) 次の 802.11 b/g/n パラメータを設定します。
- [Admin Status] : 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
  - [Power Assignment] : カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
  - [Channel Assignment] : カスタムチャンネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャンネル番号を選択します。
  - [CleanAir/Spectrum Intelligence] : CleanAir スペクトルインテリジェンスを無効にするには、このチェックボックスをオンにして [Disable] をクリックします。
  - [Antenna Name] : アンテナ名を選択するには、このチェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。アンテナ名として [Other] を選択した場合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲインアンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ~ 40 です。
  - [Antenna Cable] : アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ~ 40 です。



- [Azimuth] : 方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 – 360 です。
- [Elevation] : 仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 – 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

**ステップ 9** (オプション) [Configure 6 GHz Radio Parameters] ウィンドウで、6 GHz 無線パラメータを設定します。

- a) 6 GHz 無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

Cisco DNA Center では、6 GHz 無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。

- b) 次のパラメータを設定します。

- [Admin Status] : 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Radio Role Assignment] : 無線の役割を選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] ボタンをクリックします。
- [Power Assignment] : カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment] : カスタムチャンネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャンネル番号を選択します。
- [Channel Width] : チャンネル幅を選択するには、このチェックボックスをオンにし、チャンネル帯域幅を選択します。
- [Azimuth] : 方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 – 360 です。
- [Elevation] : 仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 – 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

**ステップ 10** (オプション) [Configure Dual-Band (XOR) Radio Parameters] ウィンドウで、デュアルバンド (XOR) 無線パラメータを設定します。

- a) デュアルバンド (XOR) 無線パラメータ設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

Cisco DNA Center では、デュアルバンド (XOR) パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。

次の AP でデュアルバンド (XOR) 無線パラメータを設定できます。

- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント
- Cisco Catalyst 9120 シリーズ アクセスポイント
- Cisco Catalyst 9166 シリーズ アクセスポイント

(注) Cisco Catalyst 9166 シリーズ アクセスポイントは、5 GHz と 6 GHz の無線モード間のデュアルバンド (XOR) をサポートします。他の AP は、2.4 GHz と 5 GHz の無線モード間のデュアルバンド (XOR) をサポートします。

b) 次のパラメータを設定します。

- [Admin Status] : 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Radio Role Assignment] : 無線の役割を選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] ボタンをクリックします。無線帯域の必要なオプションをクリックします。
- [Power Assignment] : カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment] : カスタムチャンネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャンネル番号を選択します。
- [Channel Width] : チャンネル幅を選択するには、このチェックボックスをオンにし、チャンネル帯域幅を選択します。
- [CleanAir] : CleanAir スペクトルインテリジェンスを無効にするには、このチェックボックスをオンにして [Disable] をクリックします。
- [Antenna Name] : アンテナ名を選択するには、このチェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。アンテナ名として [Other] を選択した場合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲインアンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ~ 40 です。
- [Antenna Cable] : アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ~ 40 です。
- [Azimuth] : 方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ~ 360 です。

- [Elevation] : 仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 - 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

**ステップ 11** (オプション) [Configure Tri-Radio Parameters] ウィンドウで、トライ無線パラメータを設定します。

- a) トライ無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。
- (注)
- Cisco DNA Center では、トライ無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。
  - Cisco DNA Center では、[Monitor] モードまたは [Sniffer] モードの AP のトライ無線パラメータ設定をサポートしていません。

次の AP にトライ無線パラメータを設定できます。

- Cisco Catalyst 9124AXE シリーズ アクセスポイント
- Cisco Catalyst 9130AXI シリーズ アクセスポイント
- Cisco Catalyst 9130AXE シリーズ アクセスポイント

b) 次のパラメータを設定します。

- [Dual Radio Mode] : デュアル無線モードを選択するには、このチェックボックスをオンにして、[Auto]、[Enable]、または [Disable] をクリックします。

(注) デュアル無線モードを有効にすると、対応するワイヤレスコントローラでグローバルトライ無線モードが有効になります。
- [Radio Role Assignment] : 無線の役割を選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] をクリックします。
- [Admin Status] : 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Power Assignment] : カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment] : カスタムチャンネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャンネル番号を選択します。
- [Channel Width] : チャンネル幅を選択するには、このチェックボックスをオンにし、チャンネル幅を選択します。

(注) [Channel Assignment] の [Custom] オプションを選択すると、Cisco DNA Center でこのパラメータが有効になります。

- **[CleanAir / Spectrum Intelligence]** : CleanAir スペクトルインテリジェンスを無効にするには、このチェックボックスをオンにして **[Disable]** をクリックします。  
(注) CleanAir スペクトルインテリジェンスを設定できるのは、**[Local/FlexConnect]** モードおよび **[Monitor]** モードの CleanAir スペクトルインテリジェンス対応 AP だけです。802.11a ネットワークで CleanAir スペクトルインテリジェンスが無効になっている場合、AP の動作状態はダウンしています。
- **[Antenna Name]** : アンテナ名を選択するには、このチェックボックスをオンにして、**[Select Antenna Name]** ドロップダウンリストからアンテナ名を選択します。アンテナ名として **[Other]** を選択した場合は、**[Antenna Gain(in dBi) (for Antenna-Other)]** フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲインアンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ~ 40 です。
- **[Antenna Cable]** : アンテナケーブルを選択するには、このチェックボックスをオンにして、**[Select Antenna Cable]** ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして **[Other]** を選択した場合は、**[Cable Loss (in dBi) (for Cable-Other)]** フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ~ 40 です。
- **[Azimuth]** : 方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ~ 360 です。
- **[Elevation]** : 仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ~ 90 です。**[Up]** および **[Down]** トグルボタンを使用して、方向を指定します。

**ステップ 12** **[Schedule Task]** ウィンドウで、**[Now]** または **[Later]** をクリックして、AP をいつプロビジョニングするかを指定します。

**ステップ 13** **[Summary]** ウィンドウで、設定を確認します。変更するには、**[Edit]** をクリックします。

**ステップ 14** **[構成]** をクリックします。

**ステップ 15** **[Track Provision Status]** ウィンドウで、**[AP Configuration Provision]** ステータスを確認できます。

---

## AP ワークフローの定期的なイベントのスケジュール

この手順は、Cisco DNA Center で AP および無線パラメータの定期的なイベントをスケジュールする方法を示しています。

---

**ステップ 1** メニューアイコン (☰) をクリックして、**[Workflows]** > **[Configure Access Points]** の順に選択します。

**ステップ 2** **[Overview]** ウィンドウが開いたら、**[Let's Do it]** をクリックしてワークフローを開始します。

**ステップ 3** **[Get Started]** ウィンドウで、**[Task Name]** フィールドにタスクの一意の名前を入力します。

**ステップ 4** [How do you want to configure APs?] ウィンドウで、[Schedule Recurring Events For AP And Radio Parameters] オプションボタンをクリックします。

**ステップ 5** [Select Access Points] ウィンドウで、次の手順を実行します。

a) AP 関連の設定を適用するサイトに移動します。

右側のペインに、選択したサイトで使用可能なすべての AP が一覧表示されます。

b) 設定する AP 名の横にあるチェックボックスをオンにします。

**ステップ 6** [Select AP and Radio Parameters] ウィンドウで、設定する AP および無線パラメータを選択します。

Cisco DNA Center は、次のように特定の設定を 1 つの AP スロットのみに適用します。

- [5 GHz Admin Status] : AP のスロット 1 に適用されます。
- [2.4 GHz Admin Status] : AP のスロット 0 に適用されます。
- [6 GHz Admin Status] : 6 GHz 対応 Cisco Catalyst 9136 シリーズ AP のスロット 3 および 6 GHz 対応 Cisco Catalyst 9164 シリーズ AP のスロット 2 に適用されます。
- [Dual-Band (XOR) Admin Status] : 次のデュアルバンド (XOR) 対応 AP のスロット 0 に適用されます。
  - Cisco Aironet 2800 シリーズ アクセス ポイント
  - Cisco Aironet 3800 シリーズ アクセス ポイント
  - Cisco Aironet 4800 シリーズ アクセス ポイント
  - Cisco Catalyst 9120 シリーズ アクセス ポイント

デュアルバンド (XOR) 対応 Cisco Catalyst 9166 シリーズ AP のスロット 2 に適用されます。

- [Tri-Radio Admin Status] : デュアル無線モードが有効になっているトライ無線対応 AP のスロット 2 に適用されます。

パラメータの構成を無効にするには、対応するチェックボックスをオンにして、[Disable] をクリックします。

**ステップ 7** [Schedule Provision] ウィンドウで、次のように構成します。

1. 開始日時を指定します。
2. タイムゾーンを選択します。
3. [Recurrence] 設定では、次のトグルボタンのいずれかをクリックして、Cisco DNA Center での AP 設定タスクの実行タイミングを指定します。
  - [None] : 1 回実行し、繰り返しません。
  - [Hourly] : Cisco DNA Center は指定した時間間隔ごとに AP 設定タスクを実行します。[Run at Interval (Hours)] フィールドで、タスクを繰り返す間隔を時間数で指定します。有効な範囲は 1 ~ 48 です。
  - [Daily] : 指定した日間隔ごとに AP 設定タスクを実行します。[Run at Interval (Days)] フィールドで、タスクを繰り返す間隔を日数で指定します。有効な範囲は 1 ~ 14 です。

- [Weekly] : 指定した週間隔ごとに AP 設定タスクを実行します。[Run at Interval (Weeks)] フィールドで、タスクを繰り返す間隔を週単位で指定します。有効な範囲は 1 ~ 52 です。
4. (オプション) [Hourly]、[Daily]、または [Weekly] の繰り返し間隔を選択する場合は、[Set Schedule End] チェックボックスをオンにして、繰り返しの終了設定を完了します。
- 終了日を指定するには、[End Date] オプションボタンをクリックして終了日を指定します。
 

(注) Cisco DNA Center では、開始日から最長 3 年の終了日を設定できます。
  - 指定した回数の後に定期的なイベントを終了するには、[End After] オプションボタンをクリックして、回数を指定します。
 

(注) Cisco DNA Center では、最小値 2、および開始日から最長 3 年の終了日を設定できません。

ステップ 8 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 9 [設定 (Configure) ] をクリックします。

## デバイスと既存のインフラストラクチャからデバイス構成を学習する

次の手順は、Cisco DNA Center を使用してデバイスと既存のインフラストラクチャから構成を学習する方法を示しています。

- ステップ 1 メニューアイコン (☰) をクリックして、[Workflows] > [Learn Device Configuration] > [Let's Do it] の順に選択してワークフローを起動します。
- (注) [workflow] ウィンドウの上部で、青い進行状況バーにカーソルを合わせると、現在の手順を確認したり、前の手順のいずれかに戻ることができます。
- ステップ 2 [Select a WLC to Learn Configuration] ウィンドウで、Cisco DNA Center により構成が学習されていないワイヤレスコントローラをクリックし、[Next] をクリックします。
- ステップ 3 [Site Assignment] ウィンドウで、ワイヤレスコントローラと AP の既存のワイヤレス ネットワーク プロファイルに関連付けられていないサイトを選択します。
- (注) サイトを割り当てなくてもデバイス構成を学習できますが、Cisco DNA Center から同じワイヤレスコントローラを管理するために必要なサイトを割り当てることをお勧めします。
- a) ワイヤレスコントローラにサイトを割り当てるには、[Device Name] の横にある [Assign Site] をクリックします。
- [Assign Site] ウィンドウで、関連付ける建物に移動して [Save] をクリックします。

b) APにサイトを割り当てるには、[Unified AP] テーブルの AP 名の隣にあるチェックボックスをオンにして、[Assign Site] をクリックします。

- [Assign Site] ウィンドウで、フロアに移動して [Save] をクリックします。

c) [Next] をクリックします。

**ステップ 4** [Learned Network Settings] ウィンドウで、次の学習済みネットワーク設定を確認します。

これらの設定はそのデバイスが物理的に存在する場所に保存されます。このウィンドウに表示されるネットワークサーバーは、サイトレベルで保存されます。

- AAA サーバーの [Shared Secret] を入力します。

#### • システム設定

- AAA サーバーを Cisco ISE サーバーとして保存するには、[Cisco ISE Server] トグルボタンをクリックし、[Username]、[Password]、および [FQDN] に詳細情報を入力します。

(注) Cisco DNA Center に Cisco ISE サーバーがすでに存在する場合は、AAA サーバーを Cisco ISE サーバーとして保存できません。

AAA サーバーを Cisco ISE サーバーとして設定すると、Cisco ISE サーバーからの証明書が自動的に受け入れられ、信頼が確立されます。

- [Virtual IP Address(es)] トグルボタンをクリックして、ロードバランサの IP アドレスを入力します。
- [AAA Server] : Cisco DNA Center で設定されたネットワークサーバーが表示されます。これらのネットワークサーバーは事前入力されます。
  - AAA サーバーの [Network] または [Client/Endpoint] をカスタマイズできます。サーバーとプロトコルはデフォルトで選択されます。
  - ドロップダウンリストから [IP Address (Primary)] と [IP Address (Secondary)] を選択します。これらのサーバーはグローバルレベルで保存されます。
    - [DHCP Server] : デバイスで使用可能なすべての DHCP サーバーが表示されます。
    - [NTP Server] : デバイスで使用可能なすべての NTP サーバーが表示されます。
- [Next] をクリックします。

**ステップ 5** [Assign Sites to Configurations Learned] ウィンドウでは、構成がデバイス上で使用可能な場合、学習した次の設定を表示できます。サイトに割り当てられていない構成は無視されます。

- Flex オーバーライド
- AAA Server
- VLAN エントリ
- メッシュ設定

- リモートテレワーカーの有効化

**ステップ 6** [Learned Wireless Configuration] ウィンドウでワイヤレスコントローラから学習された設定を確認します。このウィンドウに表示されるワイヤレス設定は、グローバルレベルで保存されます。

- [Supported] タブには、[SSID]、[RF Profiles]、[Interfaces]、[Interface Groups]、[aWIPS and Forensic Capture Enablement]、[Pre Auth ACLs]、[VLAN] などの学習された構成のリストが表示されます。
  - デフォルトでは、NAC 設定が有効になっている SSID はゲスト SSID として学習されます。[SSID] テーブルの [SSID Type] の横にある [Edit] アイコンをクリックして、[SSID Type] を [Guest] から [Enterprise] に変更します。
  - 設定を無視するには、学習した設定の横にあるチェックボックスをオンにして、対応するテーブルで [Ignore Config] をクリックします。
  - 無視された SSID、RF プロファイル、インターフェイス、またはインターフェイスグループを再学習するには、再学習する対象を選択し、対応するテーブルで [Relearn Config] をクリックします。
- [Unsupported] タブには、[SSID]、[RF profile]、[interface]、[Pre Auth ACLs]、[Interface Groups] など、学習されていない設定が表示されます。これらのサポートされていない設定または不明な設定に対処し、CLI テンプレートを使用できます。

**ステップ 7** [Assign Sites to Learned SSIDs] ウィンドウで、複数の WLAN プロファイルの競合を確認して解決します。

- グローバルレベルで保存され、複数の WLAN プロファイルで学習されている SSID がリストされません。競合を解決するには、WLAN プロファイルを SSID からグローバルに割り当て、別のプロファイルを特定のサイトに割り当てます。
- (オプション) WLAN プロファイルをサイトに割り当てるには、対応する SSID 行の [Assign Site] をクリックします。
  - [Assign Site] ウィンドウで、サイトを選択して [Save] をクリックします。

(注) 上書きできるのは、ワイヤレス設定またはプロファイルが関連付けられていないサイトだけです。関連付けられていないサイトがない場合は、現在のワークフローを終了し、新しいサイトを作成してからワークフローを再開してください。

**ステップ 8** [Resolve Configuration Conflicts] ウィンドウで、表示される競合を確認して解決します。

デバイスから学習された設定と、グローバルレベルで保存されている設定が表示されます。競合を解決する設定セットを選択します。

- [Use DNAC Configuration] : グローバルレベルで設定を保存する場合。
- [Use Device Configuration] : デバイスから設定を学習する場合。
  - デバイス設定を選択すると、グローバルレベルで保存されている設定が上書きされます。



- [Use Custom Configuration] : 必要な [Wireless Interface] を選択することによって設定をカスタマイズする場合。

### ステップ 9 [Model Configs Learned] ウィンドウで、モデル設定を確認します。

モデル設定とは、ネットワークデバイスに展開できる、モデルベースの、検出可能でカスタマイズ可能な一連の設定機能です。モデル設定は、さまざまなハードウェア プラットフォームおよびソフトウェア タイプに展開できます。Cisco DNA Center は、CLI などのデバイス固有の設定からモデル設定を検出して学習します。学習されたモデル設定は、ネットワークプロファイルに関連付けることができる設計に保存されます。

次のワイヤレスモデル設定設計タイプを展開して確認します。

- AAA Radius 属性の設定
- 高度な SSID 設定
- CleanAir の設定
- Dot11ax 設定
- イベント駆動型 RRM の設定
- グローバル IPv6 設定
- マルチキャストの設定
- RRM の一般設定

各モデル設定設計タイプからの設定を対象外にする場合は、対応するテーブルで設定を選択し、[Ignore Config] をクリックします。対象外の設定を再学習するには、対象外の設定を選択し、[Relearn Config] をクリックします。

### ステップ 10 [CLI Templates Learned] ウィンドウで、CLI テンプレートを確認し、これらのテンプレートを使用して、不明の設定またはサポートされていない設定に対処します。

- 対象外になっているすべての WLAN 設定がデフォルトで選択されています。[Ignore Template] をクリックして、テンプレートによる設定への対処を制限します。[Relearn Template] をクリックして設定に対処します。
- すべての不明な設定またはサポートされていない設定がデフォルトで選択されています。[Ignore Template] をクリックして、テンプレートによる設定への対処を制限します。[Relearn Template] をクリックして設定に対処します。

### ステップ 11 [Network Profiles] ウィンドウで、学習したネットワークプロファイル設定を確認します。学習した設定に基づいて、Cisco DNA Center によってネットワークプロファイルが作成されます。学習したネットワークプロファイルを使用することも、新しいネットワークプロファイルを作成することもできます。SSID は、ネットワークプロファイルの作成中に学習され、グループ化されます。

Cisco AireOS ワイヤレスコントローラでは、Flex グループと AP グループはネットワークプロファイルにマッピングされます。AP サイトの割り当てに応じて、ネットワークプロファイルは適切なサイトに割り当てられます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、サイトタグ、ポリシータグ、ネットワークプロファイルにマッピングされているサイト階層が表示されます。

- APサイトの割り当て設定に基づいて、ネットワークプロファイルが適切なサイトに割り当てられます。[Sites Assigned] をクリックして、ネットワークプロファイルに割り当てられたサイトの詳細を表示します。
- 新しいネットワークプロファイルを作成するには、[Create New Profile] をクリックします。

[New Profile] ウィンドウが表示されます。

- [Network Profile Name] フィールドに、ネットワークプロファイルの名前を入力します。
- [SSID] テーブルで、[Network Name] の横にあるチェックボックスをオンにして SSID を選択します。
- [Save] をクリックします。
- (オプション) テンプレートの詳細を確認し、変更が必要な場合は編集します。
  - ネットワークプロファイルにサイトを割り当てるには、[Assign Site] をクリックします。[Assign Site] ウィンドウで、サイトを選択して [Save] をクリックします。

[Sites Assigned] をクリックして、このプロファイルに割り当てられたサイトを確認します。
  - ネットワークプロファイルにテンプレートを関連付けるには、[Assign Template] をクリックします。[Assign Template] ウィンドウで、既存の展開の各デバイスに対して [Select Templates] ドロップダウンリストからテンプレートを選択し、[Save] をクリックします。

[View Templates] をクリックして、プロファイルに割り当てられているテンプレートを確認します。
  - ネットワークプロファイルを対象外にするには、[Ignore Profile] をクリックし、[Continue] をクリックします。

プロファイルが対象外としてマークされている場合、そのプロファイルのすべてのプロファイル属性が削除されます。これは、プロファイルを再学習することによって元に戻すことはできません。対象外のプロファイルを再学習するには、[Relearn Profile] をクリックします。
  - ネットワークプロファイルにサイトタグを追加するには、[Site Tag] テーブルで [Add] をクリックします。[Add Site Tag] ウィンドウで、[Select Site Tag] ドロップダウンリストからサイトタグを選択し、階層からサイトを選択して、[Save] をクリックします。

**ステップ 12** (オプション) [Network Profile - Model Configurations] ウィンドウで、Cisco DNA Center によって学習されたモデル設定をネットワークプロファイルに関連付けます。

- [追加 (Add) ] をクリックします。
- [Add Model Configs to Network Profile] ウィンドウで、次の手順を実行します。
  - 追加するモデル設定設計を展開します。

- 設計を選択します。[Advanced SSID Configuration] の場合は、設計ごとに [Applicable SSID] 列のドロップダウンリストから SSID を選択します。
- [Apply] をクリックします。
- ネットワークプロファイルに追加されたモデル設定を削除するには、モデル設定を選択して、[Delete] をクリックします。
- [Next] をクリックします。

**ステップ 13** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

**ステップ 14** [Save] をクリックします。

ネットワーク設定は、グローバルレベルおよびサイトレベルで適切に作成されます。

**ステップ 15** メニューアイコン (☰) をクリックして、[Design] > [Network settings]。

- [Network] タブでは、デバイスから学習されたすべてのネットワーク設定を確認できます。
- [Wireless] タブでは、デバイスから学習されたすべてのワイヤレス設定を確認できます。

学習された設定は、デバイスのプロビジョニング時にデバイスにプッシュされます。

## デバイスの交換ワークフロー

このワークフローでは、故障したデバイスを交換するための詳細な手順が示されます。

シスコのスイッチスタック（ハードウェアスタッキング）の場合、メンバースイッチの交換のために Cisco DNA Center で別の手順に従う必要はありません。これはアクティブスイッチにより処理されます。メンバースイッチは、ソフトウェアイメージと設定を提供することで、アクティブスイッチにより交換されます。フルスタック交換は Cisco DNA Center によって処理されます。



- (注) [Inventory] ウィンドウから故障したデバイスを交換することもできます。詳細については、[故障したデバイスの交換](#)を参照してください。

### 始める前に

- 故障したデバイスのソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換するデバイスにマークを付ける必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。

- RMA ワークフローのトリガー中は、交換用デバイスがプロビジョニング状態ではありません。
- スイッチスタックの交換の場合、故障したデバイスと交換用デバイスのスタックの数が同一である必要があります。

- 
- ステップ 1** 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。
- ステップ 2** タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。
- ステップ 3** [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。
- ステップ 4** [Choose Device Type] 画面で、交換する故障したデバイスのタイプを選択します。
- ステップ 5** [Choose Site] 画面で、故障したデバイスがあるサイトを選択します。
- ステップ 6** [Choose Faulty Device] ウィンドウで、交換する故障したデバイスを選択します。
- ステップ 7** [Choose Faulty Device] ウィンドウで故障したデバイスが見つからない場合は、次の手順を実行します。
- [Add Faulty Device] をクリックします。
  - 故障したデバイスを選択し、[Next] をクリックします。
  - [Mark For Replacement] ウィンドウで、[Mark] をクリックします。
- ステップ 8** [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のいずれかによってオンボードされたデバイスが表示されます。
- ステップ 9** (任意) 交換用デバイスがまだオンボードされていない場合は、次の手順を実行します。
- [Choose Replace Device] ウィンドウで、[Add Device] をクリックします。
  - [Add New Device] ウィンドウで、デバイスのシリアル番号を入力し、[Add New Device] をクリックします。
- または
- [Choose Replace Device] ウィンドウで、[Sync with Smart Account] をクリックします。
  - [Sync with Smart Account] ウィンドウで、[Sync] をクリックします。
- ステップ 10** [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] をクリックして特定時刻でのデバイスの交換をスケジュールします。
- 交換用デバイスがまだオンボードされていない場合、[Now] オプションは無効になります。[Later] をクリックして特定時刻でのデバイスの交換をスケジュールすることは可能です。
- ステップ 11** [Review] をクリックして、選択したデバイスタイプ、故障したデバイスの詳細情報、および交換用デバイスの詳細情報を確認します。
- ステップ 12** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。
- (任意) [Replacement Device] で、[View] をクリックして、交換用デバイスの設定を確認します。
  - [置換 (Replace)] をクリックします。

**ステップ 13** [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 14** [Replace Status] をクリックすると、次のように RMA ワークフローの進捗状況が表示されます。

- デバイス交換の準備状況チェックを実行します。
- (PnP) 交換用デバイスを請求します。
- 交換用デバイスにソフトウェアイメージを配信してアクティブ化します。
- ライセンスを展開する。
- VLAN 構成をプロビジョニングします。
- スタートアップ構成をプロビジョニングします。
- 交換用デバイスをリロードします。
- 交換用デバイスの到達可能性を確認します。
- 交換用デバイスに SNMPv3 ログイン情報を展開します。
- 交換用デバイスを同期します。
- 故障したデバイスを CSSM から削除します。
- 交換用デバイスを CSSM に追加します。
- PKI 証明書を失効化して作成します。
- Cisco ISE を更新します。
- 障害のあるデバイスを削除します。

ワークフローが完了すると、[Replace Status] が [Replaced] に更新されます。

**ステップ 15** エラーメッセージが表示された場合は、エラーリンクをクリックします。[Retry] をクリックして、故障したデバイスと交換用デバイスの同じ組み合わせを使用してワークフローを再トリガーします。

(注) [Main Inventory] ウィンドウには、故障したデバイスと交換した新しいデバイスの詳細情報が表示されます。

**ステップ 16** (任意) どの段階でもワークフローを終了し、後で再開することができます。[Exit] オプションは、すべてのウィンドウの左下隅に表示されます。ワークフローを終了して後で再開するには、次の手順を実行します。

- a) [終了 (Exit) ] をクリックします。  
[Exiting Workflow] 確認ウィンドウが表示されます。
- b) 確認ウィンドウで、[Exit] をクリックします。  
タスク名の付いたワークフローの [In Progress] カードが作成されます。
- c) 終了した位置からワークフローを再開するには、[In Progress] カードをクリックします。

- デバイスに [In progress] カードがあり、[Inventory] > [Marked for Replacement] ウィンドウから同じデバイスを交換しようとする、シリアル番号と [In progress] カードのタスク名を含む確認メッセージが表示されます。[Yes] をクリックしてワークフローを再開するか、[Cancel] をクリックして新しいワークフローを開始します。
- 交換対象としてマークされていないデバイスの [In progress] カードをクリックすると、警告メッセージが表示されます。[Yes] をクリックし、障害のある別のデバイスを選択して、新しいワークフローを開始します。[Cancel] をクリックすると、ワークフローがキャンセルされます。

## リモートサポート許可の作成

次の手順では、リモートサポートの許可を作成する方法について説明します。



(注) Cisco DNA Center のリモートサポート許可は、RADKit バージョン 1.2.1 以降でのみサポートされます。

**ステップ 1** メニューアイコン (☰) をクリックして、[Workflows] > [Create a Remote Support Authorization] の順に選択します。

**ステップ 2** タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

**ステップ 3** [Set up the Authorization] ウィンドウで、次を入力します。

- シスコスペシャリストの電子メールアドレス
- 既存のサービスリクエスト番号
- アクセスを許可する理由

**ステップ 4** [Schedule the Access] ウィンドウで、[Now] または [Later] をクリックして、シスコスペシャリストによる Cisco DNA Center へのアクセスをいつ許可するかを指定します。

**ステップ 5** [Access Permission Agreement] ウィンドウで、次の手順を実行します。

- [I agree to provide access to network devices] チェックボックスをオンにして、ネットワークデバイスへのアクセスを承認します。
- [I agree to provide access to our Cisco DNA Center setup] チェックボックスをオンにして、シスコスペシャリストが SSH ログイン情報を使用して Cisco DNA Center セットアップにアクセスできるよう承認します。

- (注)
- リモートサポート認証を完了する前に、SSH 認証情報を作成する必要があります。SSH ログイン情報を作成するには、「[SSH ログイン情報の設定](#)」を参照してください。
  - この許可は、アクセス前であればいつでもキャンセルまたは取り消しできます。許可をキャンセルするには、[リモートサポート許可の表示に関するトピック](#)を参照してください。

ステップ6 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ7 [作成 (Create) ] をクリックします。

タスク完了[Done! Authorization is created] ウィンドウが表示されます。

ステップ8 [View All Authorizations] をクリックして、[Remote Support Authorization] ウィンドウに移動します。詳細については、[リモートサポート許可の表示に関するトピック](#)を参照してください。

## イベント通知の作成

Cisco DNA Center イベント通知を使用すると、複数のポイントで発生する選択したイベントの詳細を配信する1つの通知内に複数のチャンネルを関連付けることができます。

ステップ1 メニューアイコン (☰) をクリックして、[Workflows] > [Create a New Notification]の順に選択します。

ステップ2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ3 [Select Channels] ウィンドウで、通知チャンネルを選択します。

サポートされているチャンネルは、[REST]、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、[EMAIL]、およびカスタムチャンネルです。

ステップ4 [Select Site and Events] ウィンドウで、[Select a site] ドロップダウンリストから、選択したイベントの通知を受け取る特定のサイトを選択します。

(注) 複数のサイトを同時に選択できます。

ステップ5 イベントの横にあるプラスアイコンをクリックするか、[Add All] をクリックしてすべてのイベントをそれぞれの通知に追加します。

ステップ6 通知からイベントを削除するには、削除するイベントの横にあるXアイコンをクリックするか、[Remove All] をクリックしてイベントリストからすべてのイベントを削除します。

- (注)
- 通知チャンネルを選択すると、[Select Site and Events] ウィンドウのテーブルに、選択した通知チャンネルでサポートされるイベントの数が一覧表示されます。
  - 複数の通知チャンネルを選択すると、[Select Site and Events] ウィンドウのテーブルに、選択した通知チャンネルに共通のサポートされているイベントの数が一覧表示されます。

ステップ7 [Configure Notification] ウィンドウで、次の値を設定します。

1. [EMAIL] 通知チャンネルを選択した場合は、[Email Settings] ウィンドウで次のように設定します。

1. リンクをクリックして [Email] GUI ウィンドウにアクセスし、新しいメールサーバーを設定します。

- (注) • 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[EMAIL] を選択した場合に電子メール設定が完了していないと、該当する GUI ウィンドウにアクセスして設定作業を行うよう求められます。電子メール設定は、[Email] タブで設定します。

(オプション) [Email] タブにアクセスするには、メニューアイコン (☰) をクリックし、[System] > [Settings] > [External Services] を選択します。

[External Services] を展開し、[Destinations] を選択して、[Email] タブをクリックします。

- 電子メール通知を受信する電子メールアドレスは、エンドポイントごとに最大 20 個まで設定できます。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Cisco DNA Center により電子メールアドレスが検証され、構文が正しくない場合は通知されます。
  - エンドポイントごとに 20 を超える電子メールアドレスを設定する必要がある場合は、グループ電子メールエイリアスを使用できます。
  - イベント サブスクリプションに電子メールの宛先を使用している場合、送信される電子メールには UTC タイムスタンプ付きのイベントが表示されます。
2. [Select Existing Instance] をクリックして既存の電子メールインスタンスを使用するか、[Create New Instance] をクリックして新しい電子メールインスタンスを作成します。
  3. [Select Existing Instance] をクリックした場合は、[Select Instance] ドロップダウンリストから電子メールインスタンスを選択します。
  4. [From] および [To] フィールドに電子メールアドレスを入力し、電子メールの [Subject] ヘッダーに件名を入力します。
2. [SYSLOG] 通知を選択した場合は、[Syslog Settings] ウィンドウで次の値を設定します。
    1. リンクをクリックして [Syslog] GUI ウィンドウにアクセスし、新しい syslog エンドポイント (Syslog サーバーのホスト名とポート番号) を設定します。

- (注) 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[SYSLOG] を選択したが、Syslog サーバーの設定を行っていない場合、GUI ウィンドウにアクセスして設定作業を行うよう求められます。Syslog サーバーの設定は、[Syslog] タブで行います。

(オプション) [Syslog] タブにアクセスするには、メニューアイコン (☰) をクリックし、[System] > [Settings] > [External Services] を選択します。

[External Services] を展開し、[Destinations] を選択して、[Syslog] タブをクリックします。



2. [Protocol] フィールドに、TCP または UDP のいずれかを入力します。
  3. [Port] フィールドに、syslog サーバーのポート番号を入力します。
  4. [Hostname/IP] フィールドで、syslog サーバーのホスト名または IP アドレスを入力します。
  5. [Select Instance] ドロップダウンリストで syslog インスタンスを選択します。
3. [REST] 通知を選択した場合は、[REST Settings] ウィンドウで次の値を設定します。
- リンクをクリックして [REST Webhook] GUI ウィンドウにアクセスし、新しいウェブフックエンドポイントを設定します。
    - (注) 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[REST] を選択したが、ウェブフックの設定を行っていない場合、GUI ウィンドウにアクセスして設定作業を行うよう求められます。ウェブフックの設定は [Webhook] タブで行います。
      - (オプション) [Webhook] タブにアクセスするには、[System] > [Settings] > [External Services] を選択します。
- [External Services] を展開し、[Destinations] を選択して、[Webhook] タブをクリックします。
- [Webhook Instance] ドロップダウンリストから、通知エンドポイントと URL を選択します。
  - [URL] フィールドにイベント送信先の REST API エンドポイントの URL アドレスを入力します。
    - [Trust certificate] : REST API エンドポイント通知に信頼できる証明書が必要かどうか。
    - [Method] : PUT メソッドまたは POST メソッド。
  - [Basic] : クライアントが HTTP 要求を送信することで認証を行います。認証ヘッダーには「Basic」という単語が含まれ、後にスペース、「username:password」の形式の base64 でエンコードされた文字列が続きます。GUI で [Basic] を選択すると、[Headers] フィールドに「Authorization」という値が自動的に入力されます。
  - [Token] : サーバーから提供されたセキュリティトークンを使用してユーザーが認証されます。[Token] を選択すると、[Headers] フィールドに「X-Auth-Token」という値が自動的に入力されます。
  - [No Authentication] : 認証が不要になります。
  - [Headers] : [Header Name] と [Header Value]。
    - (注) [Headers] フィールドは、認証の選択内容に応じて自動的に値が入力される場合があります。
4. [SNMP] 通知チャンネルを選択した場合は、[SNMP Settings] ウィンドウで次のように値を設定します。
1. リンクをクリックして [SNMP] GUI ウィンドウにアクセスし、新しい SNMP エンドポイントを設定します。

(注) 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または[EMAIL]のいずれかに設定できます。[SNMP]を選択した場合に SNMP 設定が完了していないと、該当する GUI ウィンドウにアクセスして設定作業を行うよう求められます。SNMP の設定は [SNMP] タブで行います。

(オプション) [SNMP] タブにアクセスするには、メニューアイコン (☰) をクリックし、[System] > [Settings] > [External Services]を選択します。

[External Services] を展開し、[Destinations]を選択して、[SNMP] タブをクリックします。

SNMP トラップ通知は、システムハードウェアイベントに対してのみ使用できます。ハードウェアコンポーネントの正常性状態が変化した場合、システムハードウェアイベントによってサブスクリバへの通知がトリガーされます。変更がモニターされるハードウェアコンポーネントには、CPU、メモリ、ディスク、NIC、ファン、電源、RAID コントローラなどがあります。

2. [SNMP Instance] ドロップダウンリストから、通知エンドポイントを選択します。
3. [Create a new endpoint] : 新しいエンドポイント名と説明を入力します。
4. [Hostname/IP Address] フィールドに SNMP トラップレシーバ（サーバー）のホスト名または IP アドレスを入力します。
5. [Port] フィールドに SNMP トラップレシーバ（サーバー）のポート番号を入力します。
5. [PAGERDUTY] 通知チャンネルを選択した場合は、[PAGERDUTY Settings] ウィンドウで次のように設定します。
  1. [SERVICE CONFIGURATION] エリアで、[Select Existing Instance] をクリックして既存の PagerDuty インスタンスを使用するか、[Create New Instance] をクリックして新しい PagerDuty インスタンスを作成します。
  2. [Select Instance] ドロップダウンリストで PagerDuty インスタンスを選択します。
  3. [PagerDuty Events API URL] フィールドに、PagerDuty イベント API URL を入力します。
  4. [PagerDuty Integration Key] フィールドに、PagerDuty 統合キーを入力します。
6. [WEBEX] 通知チャンネルを選択した場合は、[WEBEX Settings] ウィンドウで次のように値を設定します。
  1. [Select Instance] ドロップダウンリストで Webex インスタンスを選択します。
  2. [Webex URL] フィールドに、Webex URL を入力します。
  3. [Webex Room ID] フィールドに、Webex ルーム ID を入力します。
  4. [Webex Bot Access Token] フィールドに、Webex ボットアクセストークンを入力します。

ステップ 8 [Save] をクリックします。

[Name and Description] ウィンドウで、次の手順を実行します。

- a) [Name] フィールドに、通知の一意の名前を入力します。
- b) [Description] ボックスに、通知の説明を入力します。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 [完了 (Finish) ] をクリックします。

タスク完了 Done! Your new notification is complete] ウィンドウが表示されます。

## リモート LAN の設定

リモート LAN (RLAN) を使用すると、シスコワイヤレスコントローラの AP に RLAN ポートを構成できます。ワイヤレスコントローラは有線クライアントを認証し、ネットワークへの接続を許可します。

Cisco DNA Center は Cisco Catalyst 9800 シリーズワイヤレスコントローラでのみ RLAN 構成をサポートします。Cisco IOS XE リリース 16.12 以降を実行するワイヤレスコントローラでは非ファブリックサイトに RLAN を設定できます。Cisco IOS XE リリース 17.7 以降を実行するワイヤレスコントローラではファブリックサイトに RLAN を設定できます。



(注) Cisco DNA Center は Cisco AireOS ワイヤレスコントローラでの RLAN 設定をサポートしていません。

このセクションでは、RLAN ポートを設定する方法について説明します。

### 始める前に

- サイトにシスコワイヤレスコントローラおよび 1 つ以上の AP がプロビジョニングされていることを確認します。

ファブリックサイトに RLAN ポートを構成するには、次の手順を実行します。

- 必要なファブリックサイトがプロビジョニングされていることを確認します。
- IP プールとセキュリティグループタグ (SGT) が作成されていることを確認します。

ステップ 1 メニューアイコン (☰) をクリックして、[Workflows] > [Configure RLAN] の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Get Started] ウィンドウで、タスクの一意の名前を入力します。

ステップ 4 [Select Floor] ウィンドウで、RLAN ポートを設定するフロアに移動します。

右側のペインには、選択したフロアの概要が表示されます。Cisco DNA Center は選択したフロアでプロビジョニングされたすべての AP の RLAN を設定します。

**ステップ 5** [Remote LAN Configuration] ウィンドウで、次の手順を実行します。

a) [Port 1]、[Port 2]、および [Port 3] オプションから必要な RLAN ポートを選択します。

AP に単一の RLAN ポートがある場合、Cisco DNA Center では AP の [Port 2]、および [Port 3] の設定は無視されます。

b) [Enable RLAN] トグルボタンをクリックして、RLAN を有効または無効にします。

c) [Connectivity Settings] 領域で、[Fabric] トグルボタンをクリックして、ファブリックサイトまたは非ファブリックサイトに RLAN ポートを設定します。

(注) ファブリックまたは非ファブリックの接続設定を行った後、このオプションを後で変更することはできません。

[Fabric] トグルボタンを有効にする場合は、次の手順を実行します。

- [IP Address Pool] フィールドに、IP アドレスを入力します。
- (オプション) [Scalable Group Tag] ドロップダウンリストから必要なオプションを選択します。

[Fabric] トグルボタンを無効にする場合は、次の手順を実行します。

- [Select Switching] ドロップダウンリストから必要なオプションを選択します。
- [VLAN] フィールドに、VLAN 番号を入力します。VLAN の有効な範囲は 1 ~ 4096 です。

d) [Security Settings] 領域で、次の手順を実行します。

- [Maximum End Points] フィールドに、エンドポイントの数を入力します。有効な範囲は 0 ~ 10000 です。

(注) このフィールドでは、RLAN ごとのクライアント接続数を設定します。0 は無制限のクライアント接続を示します。

- [Timeout Period (in seconds)] フィールドに、タイムアウト期間を秒単位で入力します。タイムアウトの有効範囲は 0 ~ 86400 です。
- (オプション) [Layer 2] ドロップダウンリストから必要なオプションを選択します。
- (オプション) MAC フィルタリングを有効にするには、[MAC Filtering] チェックボックスをオンにします。
- (オプション) [Fallback Authentication] ドロップダウンリストから必要なオプションを選択します。

(注) フォールバックメカニズムは、Cisco IOS XE リリース 17.8 以降が動作する Cisco Catalyst 9800 シリーズワイヤレスコントローラのファブリックサイトと非ファブリックサイトの両方でサポートされます。

- (オプション) [Layer 3] ドロップダウンリストから必要なオプションを選択します。

- (オプション) [Select a AAA Server Group] ドロップダウンリストから、AAA サーバグループを選択します。

このドロップダウンリストには、プライマリコントローラでの WLAN プロビジョニングの一部として設定された AAA サーバグループのリストが表示されます。AAA サーバグループを選択しない場合、Cisco DNA Center では選択したセキュリティ設定の RLAN プロファイルでデフォルトの方式が設定されます。

- e) (任意) [Point over Ethernet Settings] エリアで、[PoE] トグルボタンを使用して、Point over Ethernet (PoE) を有効または無効にします。

(注) Cisco DNA Center は、PoE 対応ポートを備えた AP でのみ PoE を有効にします。

**ステップ 6** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

**ステップ 7** [Schedule Task] ウィンドウで、次のいずれかを実行します。

- [Now] または [Later] をクリックして、プロビジョニングを行うタイミングを指定します。
- 選択したデバイスに設定を展開するために後で使用できるプレビューを作成するには、[Generate Preview] をクリックします。

**ステップ 8** [Apply] をクリックします。

#### 次のタスク

[Activities] > [Tasks] ウィンドウで RLAN 設定のステータスを表示できます。

セカンダリワイヤレスコントローラをプロビジョニングした場合は、[Provision] > [Inventory] ウィンドウからセカンダリワイヤレスコントローラを再プロビジョニングします。

## IP ベースおよび URL ベースのアクセスコントロールポリシー作成のワークフロー

ネットワークの認証後アクセスコントロールリスト (ACL) を作成できます。ACL は、IP、URL、またはその両方に基づくことができます。

#### 始める前に

[IP ベースのアクセスコントロール契約の作成](#)

**ステップ 1** メニューアイコン (☰) をクリックして、[Workflows] > [Create IP & URL-Based Access Control Policy] の順に選択します。

(注) [Overview] ウィンドウが開いたら、[Let's Do it] をクリックしてワークフローを開始します。

**ステップ 2** [Policy Name and Details] ウィンドウで、次の手順を実行します。

- a) ポリシーの名前と説明を入力します。
- b) [Select ACL Type] で、[IP] チェックボックス、[URL] チェックボックスをオンにするか、または [IP] チェックボックスと [URL] チェックボックスの両方をオンにします。

**ステップ 3** [Select Site and SSID] ウィンドウで、ポリシーを適用するサイトを選択します。

サイトが非ファブリック SSID ですすでにプロビジョニングされていることを確認してください。

**ステップ 4** [Policy Name and Details] ウィンドウで [IP] チェックボックスをオンにした場合は、[IP Access Control List] ウィンドウで次の手順を実行します。

- a) [Add New Row] をクリックし、[Source]、[Destination]、[Contracts]、または [Direction] を選択します。
- b) [Add] をクリックします。

**ステップ 5** [Policy Name and Details] ウィンドウで [URL] チェックボックスをオンにした場合は、[URL Access Control List] ウィンドウで次の手順を実行します。

1. URL を入力します。
2. [Action] ドロップダウンリストをクリックして [Permit] または [Deny] を選択します。

**ステップ 6** [Schedule Task] ウィンドウで、次のいずれかを実行します。

- 展開を続行するには、[Now] または [Later] オプションボタンのいずれかを選択します。
- 選択したデバイスに後で展開できるプレビューを作成するには、[Generate Preview] オプションボタンをクリックします。

**ステップ 7** [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

**ステップ 8** [展開 (Deploy) ] をクリックします。

---

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。