

プラグアンドプレイを使用したデバイスのオンボーディングとプロビジョニング

- プラグアンドプレイ プロビジョニングの概要 （1 ページ）
- プラグ アンド プレイ プロビジョニングの前提条件 （4 ページ）
- プラグアンドプレイ展開のガイドライン （11 ページ）
- デバイスの表示 （12 ページ）
- デバイスの追加または編集 （16 ページ）
- デバイスの一括追加 （17 ページ）
- バーチャル アカウント プロファイルの登録または編集 （18 ページ）
- スマートアカウントからのデバイスの追加 （20 ページ）
- プラグアンドプレイ対応デバイスのプロビジョニング （22 ページ）
- デバイスの削除 （38 ページ）
- デバイスのリセット （38 ページ）

プラグアンドプレイ プロビジョニングの概要

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

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

- サイトの割り当て、サイト設定の展開、デバイス ソフトウェア イメージのインストール、およびカスタム オンボード設定の適用によって、デバイスをプロビジョニングする。
- インストールの前に、デバイス情報を入力し、プロビジョニング操作を選択してデバイスを計画します。デバイスはオンラインになると Catalyst Center に接続します。次に、デバイスのプロビジョニングとオンボーディングが自動で実行されます。
- 事前の計画なしにネットワーク上に表示される新しいデバイスである、要求されていないネットワーク デバイスをプロビジョニングします。

- Cisco スマート アカウントの Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリをプラグ アンド プレイに同期して、すべてのデバイスが Catalyst Center に表示されるようにします。
- ネットワーク デバイスの詳細なオンボーディング ステータスを表示します。

ここでは、プラグ アンド プレイ プロビジョニングの一般的なユースケースとワークフローについて説明します。

計画的なプロビジョニング

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

（注） AP の計画済みステータスは、AP がプラグアンドプレイを介して Catalyst Center に接続したときに、ゼロタッチプロビジョニング（ZTP）のみを使用して AP を要求するための状態です。この計画は、AP がワイヤレスコントローラに直接関連付けられている場合、**[プロビジョニング（Provision）]** > **[インベントリ（Inventory）]** オプションを介した AP のプロビジョニングには適用されません。

計画的なプロビジョニングの手順は、次のとおりです。

1. ネットワーク階層内のサイトを定義することをお勧めします。ネットワーク階層を参照してください。
2. デバイスに適用する [オンボーディング設定（Onboarding Configuration）] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。多くの場合、Day-0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。デバイス設定の変更を自動化するテンプレートの作成を参照してください。

（注） Day-0 テンプレートは、対話型コマンドをサポートしていません。

3. 展開するデバイスのタイプについて、ネットワークプロファイルを定義します。ネットワークプロファイルの概要を参照してください。
4. 展開するデバイスのデバイスログイン情報（CLI および SNMPv2c/SNMPv3）を定義することをお勧めします。SNMPv2c を使用している場合は、読み取りと書き込み両方のログイン情報を指定する必要があります。

（注） ログイン情報が不足していると、プロビジョニング後にデバイスをインベントリに追加できなくなります。

5. プロビジョニングするデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェアイメージのインポートを参照してください。
6. CSV ファイルを使用して一度にまたは一括で、計画したデバイスに関する詳細を追加します。デバイスの追加または編集 （16 ページ）またはデバイスの一括追加 （17 ページ）を参照してください。
7. デバイスが起動し、自動的にプロビジョニングされます。

要求されていないプロビジョニング

計画前に新しいネットワークデバイスをネットワークに追加すると、そのネットワークデバイスは要求されていないデバイスとしてラベル付けされます。要求のないデバイスは、管理者が手動で追加することも、プラグ アンド プレイ プロビジョニングの前提条件 （4 ページ）で説明されているいずれかの検出方法を使用して自動的に追加することもできます。

管理者がデバイスをプロビジョニングする手順は、次のとおりです。

1. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （12 ページ）」を参照してください。
2. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （22 ページ）」を参照してください。サイトを割り当てずにデバイスを要求することもできます。

（注） サイトが割り当てられていないデバイスの場合、グローバルデバイスログイン情報が必要です。サイトが割り当てられているデバイスの場合、サイトレベルのグローバルデバイスログイン情報が必要です。

Cisco スマートアカウントの同期とプロビジョニング

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

1. スマートアカウントと同期するバーチャルアカウントを登録して同期します。「バーチャル アカウント プロファイルの登録または編集 （18 ページ）」を参照してください。
2. スマート アカウントからデバイス インベントリを同期します。スマートアカウントからのデバイスの追加 （20 ページ）を参照してください。
3. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （12 ページ）」を参照してください。

4. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （22 ページ）」を参照してください。
5. デバイスが起動し、自動的にプロビジョニングされます。

デバイスの要求と管理のシナリオ

- **要求されているデバイス**
  - デバイスが要求されて管理されると、PnP プロファイルがデバイスから削除されます。
  - デバイスは、工場出荷時設定へのリセット後にのみ PnP に再度接続しません。
- **インベントリ内の要求されていないデバイス**
  - ユーザーがすでにインベントリにあるデバイスを PnP を介して要求しようとすると、その要求はブロックされます。
  - Catalyst Center は、インベントリ通知を読み取って PnP を更新し、重複要求を防止します。
- **デバイスの工場出荷時設定へのリセット**
  - 管理対象デバイスが工場出荷時設定にリセットされると、要求されていない状態になります。
  - Catalyst Center はインベントリの存在をチェックし、デバイスがまだインベントリにある場合は新しい要求をブロックします。

プラグ アンド プレイ プロビジョニングの前提条件

プラグ アンド プレイ プロビジョニングを使用する前に、プロビジョニングするサイトとデバイスにアクセスできること、およびプラグ アンド プレイ プロビジョニングを実行するために必要な権限があることを確認してください。詳細については、ユーザープロファイルのロールおよび権限を参照してください。

すべてのデバイスタイプが必要な前提条件を満たしていることを確認します。さらに、ワイヤレスデバイスまたはセンサーデバイスを展開している場合は、それらの前提条件が満たされていることも確認してください。その他の前提条件はオプションですが、それらを実装することを選択した場合は、プラグアンドプレイを使用してデバイスをプロビジョニングする前に実行する必要があります。

すべてのデバイスの前提条件

すべてのデバイスタイプが次の前提条件を満たしていることを確認します。

- デバイスが、次のいずれかの方法で Catalyst Center コントローラを自動的に検出できることを確認します。
  - DHCP：DHCP コントローラディスカバリ （7 ページ）を参照してください。
  - DNS：DNS コントローラディスカバリ （9 ページ）を参照してください。
  - Cisco Plug and Play Connect クラウドサービス：Plug and Play Connect コントローラディスカバリ （10 ページ）を参照してください。
- **[System]** > **[Settings]** > **[Cisco.com Credentials]** を使用して、メインのCatalyst Center設定で cisco.com ログイン情報を設定します。

  必要に応じて、**[System]** > **[Settings]** > **[Smart Account]** で、Cisco スマートアカウントのログイン情報を設定します。
- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、*Cisco Catalyst Center* のネットワーク プラグアンドプレイのトラブルシューティング ガイド [英語] で、デバイスのクリーンアップとリセットの詳細を確認してください。

ワイヤレスデバイスまたはセンサーデバイスの前提条件

前述の前提条件に加えて、すべてのワイヤレスデバイスまたはセンサーデバイスが次の要件を満たしていることを確認してください。

- ワイヤレス AP デバイスの場合は、ワイヤレス AP を管理している シスコ ワイヤレス コントローラ がインベントリに追加され、プロビジョニングされ、ワイヤレス AP が割り当てられるサイトに割り当てられていることを確認します。この要件は、Mobility Express AP では必要ありません。
- ワイヤレス AP デバイスの場合は、ワイヤレス無線周波数プロファイルを定義します。ワイヤレス無線周波数プロファイルの作成を参照してください。この要件は、Mobility Express AP では必要ありません。
- Mobility Express AP の場合は、IP アドレスプールと管理インターフェイスを定義します。IP アドレスプールを設定するを参照してください。
- ROW AP の場合は、必要な国コードを使用して AP プロファイルを作成し、カスタムサイトタグを設定することを推奨します。Cisco IOS XE デバイスの AP プロファイルの追加設定を行うを参照してください。
- インテント AP の場合は、[**PnP AP Location**] ウィンドウで [**Configure AP Location**] チェックボックスを使用して、PnP オンボーディングのための AP の場所を設定できます。このチェックボックスは、デフォルトでオフになっています。必要に応じて、このチェックボックスをオンにして、PnP オンボーディング中の AP の場所として PnP 要求中に割り当てられるサイトを設定します。詳細については、『*Catalyst Center Administrator Guide*』の「Configure AP location for PnP onboarding」を参照してください。

- センサーの場合は、センサーが Catalyst Center エンタープライズ IP アドレス（private/enp9s0）を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが Catalyst Center の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス enp9s0 IP アドレスから到達可能である必要があります。DHCP サーバーで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80;」を使用して、NTP サーバー（DHCP オプション 42）とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は enp9s0 インターフェイスに関連付けられた Catalyst Center の仮想 IP アドレスです。
- PnP は、AP 検出の DHCP オプション 43、DNS オプション、または devicehelper メソッドをサポートしています。AP が DNS オプションを使用してワイヤレスコントローラに参加しているが、PnP 検出に DHCP オプション 43 が使用されている場合、競合が発生します。

ワイヤレスコントローラ のオプションの前提条件

プラグ アンド プレイ プロビジョニング プロセスを自動化するのに役立つオプションの前提条件には、次のようなものがあります。

- ネットワーク階層内のサイトを定義します。ネットワーク階層を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。「グローバル デバイス クレデンシャルの設定」を参照してください。

（注） CLI、SNMPv2c、または SNMPv3 ログイン情報を使用して Cisco IOS XE コントローラを要求できます。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定します。

- イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージをアップロードし、イメージリポジトリ内でゴールデンとしてマークされるようにします。ソフトウェアイメージのインポートを参照してください。

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

- デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基

本的なネットワーク設定コマンドが含まれています。デバイス設定の変更を自動化するテンプレートの作成を参照してください。

（注） [Onboarding Configuration] テンプレートで `ip http client source-interface` CLI コマンドを使用すると、Catalyst Center はその IP アドレスをデバイスの管理 IP アドレスとして使用でき、特に複数の IP または VRF のシナリオにおいて有用です。

- デバイスのネットワークプロファイルを定義します。ネットワークプロファイルの概要を参照してください。

プラグアンドプレイのシステム証明書の要件

HTTP から HTTPS への安全な移行を容易にするために、PnP 検出プロセスには、有効なシステム証明書が必要です。システム証明書が正しく設定されていない場合、PnP 検出は失敗します。デバイスを正常に検出するには、次の要件を確認してください。

- システム証明書に、SAN IP および SAN FQDN を含む必要なすべての情報カテゴリ代替名（SAN）フィールドが含まれていることを確認します。
- DHCP オプション 43 文字列で設定された FQDN は、システム証明書に存在する FQDN と一致する必要があります。
- システム証明書で定義されているすべてのホスト名が、DNS インフラストラクチャ経由で解決可能であることを確認します。

証明書の設定と検出時に入力されたアドレスに不一致がある場合、デバイスはセキュアな接続を確立できず、検出に失敗します。

DHCP コントローラディスカバリ

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

DHCP による検出方法の前提条件には、次が含まれます。

- 新しいデバイスが DHCP サーバにアクセスできる。
- DHCP サーバが Cisco Plug and Play のオプション 43 を使用して設定されている。DHCP オプション 43 を設定する場合は、Catalyst Center 企業 IP、企業仮想 IP（VIP）、または完全修飾ドメイン名（FQDN）を使用できます。FQDN を使用している場合は、ホスト名を正しい Catalyst Center クラスタアドレスに解決するように DNS サーバーが設定されていることを確認します。

  DHCP サーバが文字列「ciscopnp」を含むオプション 60 を使用してデバイスから DHCP の検出メッセージを受信すると、オプション 43 の情報を含む応答をデバイスに返します。

デバイスの Cisco Plug and Play IOS エージェントは、応答から Catalyst Center コントローラの IP アドレスを抽出し、このアドレスを使用してコントローラと通信します。

（注） Lightweight AP の場合、オプション 60 には文字列 `ciscopnp` は含まれません。代わりに、Lightweight AP のベンダークラス識別子（VCI）が含まれています。プラグアンドプレイが Lightweight AP を検出できるように、必要に応じて DHCP サーバールールを設定します。詳細については、「Configure DHCP OPTION 43 for Lightweight Access Points」 [英語] を参照してください。

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

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

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

- 5A1N;（プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし）。文字列のこの部分は変更する必要がありません。
- B2;（IP アドレスのタイプ）：
  - B1 = ホスト名
  - B2 = IPv4（デフォルト）
- I*xxx.xxx.xxx.xxx*：Catalyst Center コントローラのエンタープライズ IP またはエンタープライズ VIP アドレスまたはホスト名（大文字の i の後）。エンタープライズ VIP の設定は単一ノードの展開では任意ですが、3 ノードのクラスタでは必須です。この例では、IP アドレスは 172.19.45.222 です。
- J*xxxx*：Catalyst Center コントローラへの接続に使用するポート番号。HTTP にはポート 80 を使用する必要があります。

（注） PnP 検出中に信頼できる証明書をインストールした後、デバイスは自動的に HTTPS にポート 443 を使用するように切り替わります。

- K4; : デバイスとコントローラの間で使用されるトランスポート プロトコル。
  - K4 = HTTP（デフォルト）

• K5 = HTTPS

• T*TrustedCertificateBundleURL*：デフォルト（Catalyst Center コントローラ）以外の別の場所から信頼できる証明書のバンドルを取得する場合は、このオプションパラメータを使用して信頼できる証明書のバンドルの外部 URL を指定します。APIC-EM コントローラは、Cisco InfoSec Cloud（http://www.cisco.com/security/pki/）からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Tftp://10.30.30.10/ios.p7b」と指定します。

  信頼できる証明書のセキュリティを使用していて、T パラメータを指定しない場合、デバイスは Catalyst Center コントローラから信頼できる証明書のバンドルを取得します。

• Z*xxx.xxx.xxx.xxx*;（NTP サーバの IP アドレス）。信頼できる証明書のセキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

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

DHCP オプション 43 が設定されていない場合、デバイスが DHCP サーバに接続できない場合、またはこの方法が別の理由で失敗する場合は、ネットワークデバイスは DNS を使用して検出を試行します。詳細については、DNS コントローラディスカバリ （9 ページ）を参照してください。

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

DHCP プールがシスコスイッチまたはルータに依存している場合、次の設定例のようになります。

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

DNS コントローラディスカバリ

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

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

DNS による検出方法の前提条件には、次が含まれます。

• 新しいデバイスが DHCP サーバにアクセスできる。

- Catalyst Center コントローラがホスト名「pnpserver」を使用して展開されている。
- NTP のサーバ名はホスト名「pnpserver」で展開される。

Plug and Play Connect コントローラディスカバリ

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

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

始める前に

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

手順

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

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

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

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

ステップ 4 Catalyst Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマート アカウントに登録します。バーチャル アカウント プロファイルの登録または編集 （18 ページ）を参照してください。

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

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

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

ステップ 6 新しく同期されたデバイスを要求します。プラグアンドプレイ対応デバイスのプロビジョニング（22 ページ）を参照してください。

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

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

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

プラグアンドプレイ展開のガイドライン

ルータ、スイッチ、ワイヤレスコントローラにプラグアンドプレイを使用する場合は、次の推奨事項に従ってください。

- デバイスの起動順序：一般に、ルーティングとアップストリームデバイスは最初に展開する必要があります。ルータおよびすべてのアップストリームデバイスがアップされてプロビジョニングされると、スイッチとダウンストリームデバイスを展開できます。デバイスのプラグ アンド プレイ エージェントは最初のデバイスの起動時のみ、Catalyst Center コントローラの自動検出を試みます。現時点で、デバイスがコントローラに接続できない場合、デバイス プロビジョニングは失敗するため、アップストリーム デバイスは最初にプロビジョニングする必要があります。
- シスコのルータトランク/アクセスポートの構成：一般的なブランチネットワークには、ルータとスイッチが含まれます。1 つ以上のスイッチは WAN ルータに接続され、IP フォンやアクセス ポイントなどの他のエンドポイントはスイッチに接続します。スイッチがアップストリームルータに接続されると、次の展開モデルはプラグアンドプレイでサポートされます。
  - ダウンストリーム スイッチはルータのスイッチ ポートを使用してルータに接続されます。このタイプの接続では、ルータのスイッチ ポートをトランクまたはアクセス ポートとして設定できます。
  - ルータのルーテッド ポートを使用してダウンストリーム スイッチをルータに接続する。この場合、ルーテッド ポートはサブインターフェイスを使用して複数の VLAN をサポートできます。プラグアンドプレイのプロセス中、スイッチはそのポートを自

動的にトランクポートとして設定します。大規模ブランチの場合は、ルータとダウンストリーム スイッチ間に複数の VLAN を設置する必要があります。このような使用例をサポートするには、スイッチをルーテッド ポートに接続する必要があります。

- 非 VLAN 1 構成：プラグアンドプレイは、VLAN 1 を使用して、デフォルトでデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリームデバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリームデバイスに「**pnp startup-vlan** *x*」グローバル CLI コマンドを設定して、以降のプラグアンドプレイデバイスにこの CLI をプッシュする必要があります。隣接するアップストリーム デバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、アップストリームに接続された、以降のプラグアンドプレイデバイス上のアクティブインターフェイスは、指定された VLAN に変更されます。このガイドラインは、ルータとスイッチの両方に適用され、アクセスモードではなくトランクモードのシナリオでのみ使用する必要があります。

デバイスの表示

[Plug and Play] ウィンドウでデバイスに関する情報を表示できます。

さらに、このウィンドウからいくつかのタスクを実行できます。詳細は、次のトピックを参照してください。

- デバイスの追加または編集 （16 ページ）
- デバイスの一括追加 （17 ページ）
- スマートアカウントからのデバイスの追加 （20 ページ）
- プラグアンドプレイ対応デバイスのプロビジョニング （22 ページ）
- デバイスのリセット （38 ページ）
- デバイスの削除 （38 ページ）

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]** を選択します。

[プラグアンドプレイ（Plug and Play）] ウィンドウには、次のデバイス情報を含むテーブルが表示されます。

表 *1*: デバイス情報

カラム	説明
#	行番号。

カラム	説明
Device Name	デバイスのホスト名。このリンクをクリックすると、デバイスの詳細ウィンドウが開きます。スタック アイコンはスイッチ スタックを示します。
Serial Number	デバイスのシリアル番号。
Product ID	デバイスの製品 ID。
IP Address	デバイスの IP アドレス。
Source	デバイスエントリの送信元： • [User]：ユーザーが GUI または API を介してデバイスを追加しました。 • [Network]：コントローラに接続されたデバイスが要求解除されました。 • [SmartAccount]：デバイスはスマートアカウントから同期されました。
State	• [Unclaimed]：デバイスは正常に初期化が完了し、要求される準備ができているか、または [Planned] 状態になっています。 • [Planned]：ユーザーがデバイス構成またはプロビジョニングパラメータを指定し、デバイスをプロビジョニングする準備ができています。 • [Onboarding]：デバイスオンボーディングが進行中です。 • [Provisioned]：デバイスは正常にオンボーディングされ、インベントリに追加されています。AP とセンサーの場合、デバイスが ワイヤレスコントローラに正常に割り当てられると、状態が [Provisioned] に変わります。 • [Error]：デバイスにエラーがあり、プロビジョニングできませんでした。

カラム	説明
Onboarding State	デバイスのオンボーディング状態： • [Not Contacted]：デバイスが呼び出されていません。ユーザーがデバイスを追加またはリセットした可能性があります。 • [Connecting]：デバイスが呼び出されました。 • [Initializing]：システムワークフローを実行しています。基本的なデバイス情報が収集されます。スタックライセンスとバージョンの不一致が修正されます。 • [Initialized]：システムワークフローが完了しました。 • [Executing Workflow]：要求中に選択されたタスクは、この状態で適用されます。スタックは、製品およびイメージのバージョンに基づく番号の再割り当てとライセンスの更新をサポートしています。 • [Executed Workflow]：ユーザーワークフローが完了しました。 • [Connection Error]：接続を保護するための証明書をインストールできませんでした。 • [Authentication Error]：SUDI 証明書を検証できませんでした。 • [Authorization Error]: ユーザーが指定した SUDI シリアル番号を確認できませんでした。 • [Initialization Error]：システムワークフローの実行中にエラーが発生しました。 • [Workflow Execution Error]：ユーザーワークフローの実行中にエラーが発生しました。 • [Executing Reset]：リセットワークフローを実行しています。エラーが発生したデバイスを手動でリセットする必要があります。リセットすると、デバイスがリロードされます。 • [Reset Execution Error]：リセットワークフローの実行中にエラーが発生しました。 デバイスの履歴に移動するには、経過表示バーをクリックします。
サイト	デバイスが関連付けられているサイト。
Last Contact	デバイスが最後にプラグ アンド プレイに接続した日時。
Smart Account	デバイスが関連付けられている Cisco スマート アカウント。
Virtual Account	デバイスが関連付けられている（Cisco スマート アカウント内の）バーチャル アカウント。
Created	デバイスがプラグ アンド プレイに追加された日時。

デバイステーブルには、各デバイスについて、以下の表に示した情報が表示されます。一部の列はソートに対応しています。

（注）
- [Device Name] や [Serial Number] などの特定の列は、[Default] フォーカスビューに表示されます。
- [Devices]テーブルをカスタマイズして、列の表示と非表示を切り替えることができます。設定アイコン（⚙）をクリックして [Table Settings] スライドインペインを表示し、[Edit Table Columns] タブで表示する列や非表示にする列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 2 [プラグアンドプレイ（Plug and Play）] ウィンドウから、次の方法でデバイス情報の表示を制御できます。

- 行を昇順または降順に並べ替えるには、キャロット矢印アイコン ▲ が付いている列ヘッダーをクリックします。
- 特定の状態のデバイスを表示するには、[Device Status] フィルタから、[Unclaimed]、[Error]、[Provisioned]、または [All] を選択します。
- ビューをフォーカスするには、[Focus] ドロップダウンリストから [Default] または [All] を選択します。
- テーブル情報の更新のタイミングを変更するには、[Auto-Refresh] ドロップダウンリストをクリックして、望ましい更新間隔を選択します。デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。
- 特定のデバイスを見つけるには、[Filter] または [Find] オプションを使用します。
- デバイスの詳細を表示するには、デバイス名をクリックします。

  その他の詳細を表示するには、開いたウィンドウで、[Details]、[History]、または [Configuration] タブをクリックします。スイッチスタックの場合は、[Stack] タブをクリックすることもできます。一部のタブには、クリックしてさらに詳細を表示できる追加のリンクがあります。

（注） スイッチスタックからスタックメンバーを削除するには、[Stack] タブで、削除するメンバーの横にあるチェックボックスをオンにして、[Delete Member] をクリックします。

デバイスの追加または編集

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

表 *2:* デバイスフィールド

フィールド	説明
[Serial Number]	デバイス シリアル番号（デバイスを編集している場合は読み取り専用）。
Product ID	デバイス製品 ID（デバイスを編集している場合は読み取り専用）。
[Device Name]	デバイス名
Enable SUDI Authorization	セキュアな固有デバイス識別子（SUDI）認証をサポートするデバイスで有効にします。有効にすると、デバイスがプラグアンドプレイサーバーに接続しようとしたときに、サーバーによって、SUDI 証明書のシリアル番号とユーザーが提供するシリアル番号が比較されます。シリアル番号が一致すると、デバイスが検証され、プラグアンドプレイサーバーに接続されます。
SUDI Serial Numbers	SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号（デバイス ラベルのライセンス SN と呼ばれる）の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加するときは、このフィールドに 1 つまたは複数の SUDI シリアル番号をカンマで区切って入力します。このフィールドは、[SUDI 認証の有効化（Enable SUDI Authorization）] がチェックされている場合にのみ表示されます。
This Device Represents a Stack	デバイスがスタックを表します（デバイスを編集している場合、この項目は読み取り専用です）。サポート対象のスタッカブルスイッチにのみ適用されます。

始める前に

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

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

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

ステップ 3 デバイスを追加または編集するには、次の手順を実行します。

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

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

ステップ 5 次のいずれかのタスクを実行して、設定を保存します。

- デバイスを追加し、後で要求するには、[デバイスの追加（Add Device）] をクリックします。
- デバイスを追加し、すぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細については、プラグアンドプレイ対応デバイスのプロビジョニング （22 ページ）を参照してください。
- デバイスを編集する場合は、[デバイスの編集（Edit Device）] をクリックします。

デバイスの一括追加

この手順では、CSV ファイルからデバイスを一括で追加する方法を示します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

ステップ 2 [Add Devices] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Bulk Devices] をクリックします。

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

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

ステップ 5 各デバイスの情報をファイルに追加し、ファイルを保存します。

デバイスタイプに基づいて、必須フィールドにデータを入力します。

（注） ファイルテンプレートを使用して追加されたサイトがネットワーク階層に存在しない場合、そのデバイスは削除されます。

ワイヤレスコントローラ の場合、Catalyst Center は IP アドレスタイプ（IPv4 アドレス、IPv6 アドレス、またはその両方）に基づいてデータを処理します。

ステップ 6 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

- ドラッグ アンド ドロップ エリアにファイルをドラッグアンドドロップします。
- [ファイルの選択（Choose a file）] をクリックし、CSV ファイルの保存場所を参照して [開く（Open）] をクリックします。

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

CSV ファイル内のデバイスがテーブルにリストされます。

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

ステップ 9 次のいずれかのタスクを実行して、デバイスを追加します。

- デバイスを追加し、それらを後で要求するには、**[デバイスの追加（Add Devices）]** をクリックします。
- デバイスを追加し、それらをすぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細については、プラグアンドプレイ対応デバイスのプロビジョニング （22 ページ）を参照してください。

バーチャル アカウント プロファイルの登録または編集

リダイレクトサービスの場合、Cisco スマートアカウントで、Catalyst Centerを Cisco Plug and Play Connect のコントローラとして登録します。これにより、Cisco Plug and Play Connect クラウドポータルから Catalyst Centerの Cisco Plug and Play にデバイスインベントリを追加できます。

スマートアカウント、バーチャルアカウント、および関連するサーバーのプロファイル情報を、Plug and Play システムとデータベースに登録できます。登録された仮想アカウントのデバイスは、プラグ アンド プレイ データベースと同期されます。

表 *3:* バーチャルアカウント フィールド

オプション	説明
スマートアカウントの選択	Cisco スマート アカウント名

オプション	説明
バーチャルアカウントの選択	バーチャルアカウント名バーチャルアカウントは、Cisco スマートアカウント内のサブアカウントです。
IP または **FQDN**	[IP]：この Catalyst Center コントローラの IPv4 アドレス、IPv6 アドレス、または両方のタイプの IP アドレス。 [FQDN]：この Catalyst Center コントローラの完全修飾ドメイン名。
プロファイル名	コントローラのプロファイル名
デフォルト コントローラ プロファイルとして使用	*[Default controller profile]* とは、仮想アカウントに追加された新しいデバイス、またはデフォルトのコントローラが割り当てられていない既存のデバイスは、このリダイレクトプロファイルに割り当てられることを意味します。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[PnP Connect]**の順に選択します。

ステップ 2 テーブル内のバーチャルアカウントを表示します。

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

ステップ 3 バーチャル アカウント プロファイルを登録または編集します。

- バーチャルアカウントを登録するには、[Register] をクリックします。[Register Virtual Account] ペインが表示されます。
- 登録済みのバーチャルアカウントプロファイルを編集するには、編集するプロファイル名の横にあるオプションボタンをクリックし、[Edit Profile] をクリックします。[Edit Profile] ペインが表示されます。

ステップ 4 必要に応じてフィールドを設定します。

ステップ 5 次のいずれかのタスクを実行して、設定を保存します。

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

次のタスク

Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリを Catalyst Center プラグ アンド プレイに同期します。詳細については、スマートアカウントからのデバイスの追加 （20 ページ）を参照してください。

スマートアカウントからのデバイスの追加

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

バーチャル アカウント テーブルには、各プロファイルに関する次のような情報が表示されます。

表 *4:* バーチャルアカウント情報

カラム	説明
バーチャル アカウント	バーチャルアカウント名
スマート アカウント	バーチャルアカウントが関連付けられているスマートアカウント
プロファイル	プロファイル名
コントローラ	コントローラ IP アドレス

始める前に

Cisco プラグアンドプレイ接続クラウド ポータルからデバイスインベントリを同期する前に、バーチャルアカウントを登録する必要があります。バーチャル アカウント プロファイルの登録または編集 （18 ページ）を参照してください。**[Add Devices]** > **[Smart Account Devices]** ダイアログの **[PnP Connect]** リンクをクリックすると、[PnP Connect] 設定ページに直接移動できます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]** を選択します。

ステップ 2 [Add Devices] をクリックします。

ステップ 3 [Smart Account Add] をクリックし、[Add Devices from a Smart Account] スライドインペインを開きます。

ステップ 4 cisco.com ユーザーを設定済みの場合は、ステップ 5 に進みます。設定していない場合は、次の手順を実行します。

a) ブラウザでシークレット/プライベートウィンドウを開きます（以前にキャッシュされたログイン情報の使用を避けるため）。

b) 別の Catalyst Center GUI インスタンスを開いてログインします。

c) [Add Devices from a Smart Account] スライドインペインの別のインスタンスを開きます。

d) 次のいずれかのタスクを完了します。

次の場合は...	次の操作...
Catalyst Center 2.3.7.9 の新規インストールを完了します。	[Cisco.com ID] フィールドの [Add] リンクをクリックして、新しい cisco.com ユーザーを設定します。
Catalyst Center 2.3.7.9 にアップグレードし、以前に設定されたユーザーと同じcisco.com ユーザーを使用する場合：	[Cisco.com ID] フィールドの [Re-Authenticate] リンクをクリックして該当ユーザーを再認証します。
Catalyst Center 2.3.7.9 にアップグレードし、以前に設定されたユーザーと同じ cisco.com ユーザーを使用しない場合：	古い cisco.com ユーザーを削除してから、新しいユーザーを設定します。 **1.** [Cisco.com ID] フィールドの [Delete] リンクをクリックします。 **2.** 表示されたダイアログボックスで、[Delete] をクリックして操作を確定します。 **3.** [Cisco.com ID] フィールドの [Add] リンクをクリックします。

e) [Information] ポップアップウィンドウで、次のチェックボックスの一方または両方をオンにして、[Authenticate] をクリックします。

- （必須）[I am in private or incognito mode]
- （オプション）[Save Credentials]

f) [Activate your device] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[Next] をクリックします。

g) [Log in] ポップアップウィンドウで、cisco.com ユーザの電子メールアドレスを入力し、[Next] をクリックします。

h) [Verify with your password] ポップアップウィンドウで、cisco.com ユーザーのパスワードを入力し、[Verify] をクリックします。

[Device Activated] ポップアップウィンドウが表示されます。

i) [Device Activated] ポップアップウィンドウを閉じます。

j) [Plug and Play] ウィンドウを更新し、**[Add Devices]** > **[Smart Account Add]**をクリックし、[Add Devices from a Smart Account] スライドインペインを再度開きます。

k) [Cisco.com ID] フィールドに、ユーザーに対して入力した電子メールアドレスが表示されていることを確認します。また、[Change] リンクが表示されていることを確認します。

ステップ 5 プラグアンドプレイに登録するスマートアカウントとバーチャルアカウントを選択します。

PnP Connect バーチャル アカウント プロファイルを登録する必要がある場合は、[PnP Connect] リンクをクリックします。Cisco ID を変更する場合は、[Not me?] リンクをクリックします。

ステップ 6 [Devices] テーブルから、追加するデバイスを選択し、[Add Devices] をクリックします。

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

次のタスク

新しく追加されたデバイスを請求処理します。デバイスの要求の詳細については、プラグアンドプレイ対応デバイスのプロビジョニング （22 ページ）を参照してください。

プラグアンドプレイ対応デバイスのプロビジョニング

デバイスを要求すると、デバイスをプロビジョニングするプロセスが開始されます。デバイスがプロビジョニングされると、Catalyst Center は次のアクションを実行します。

1. イメージをデバイスに展開します。
2. 次の設定を構成するシステム構成 CLI コマンドを展開します。
   - デバイスのログイン情報（CLI および SNMP）
   - SSH v2 および SCP サーバの有効化
   - HTTP および HTTPS サーバの無効化
   - スイッチでは、vtp モードの透過が有効になっています
3. デバイスのタイプに対応するデバイスオンボーディング構成テンプレートを展開します。
   - 有線デバイスの場合、Catalyst Center は定義したオンボーディング設定（Day-0）テンプレートを展開します。
   - ワイヤレスデバイスの場合、Catalyst Center はサイトに割り当てられたネットワークプロファイルに基づいて構成を展開します。

   オンボーディング構成テンプレートに同じシステム構成 CLI コマンドのいずれかが含まれている場合、オンボーディング構成テンプレートはシステム構成 CLI コマンドの後にデバイスに適用されるため、システム構成 CLI コマンドはオーバーライドされます。
4. デバイスのプロビジョニング先のサイトで QoS ポリシーを設定した場合は、有線デバイスに Application Quality of Service（QoS）ポリシーを展開します。詳細については、アプリケーションポリシーの作成を参照してください。
5. デバイスのオンボーディング中に、ポート 830 で NETCONF 設定をプッシュします。NETCONF ポート情報は、グローバルログイン情報とネットワーク設定に保存されます。

（注）
- 標準ポート 830 ではなく誤ったポートを通じて NETCONF がプッシュされた場合、デバイスはオンボーディングを正常に完了しますが、インベントリに追加することはできません。
- 要求プロセス時にデバイスがサイトに割り当てられていない場合、NETCONF はそのデバイスでは設定されません。
- 自動 NETCONF 有効化のサポートは、次でのみ使用できます。
  - Cisco IOS XE 17.3 以降のリリースを実行している Cisco Catalyst 9000 シリーズ スイッチ、および
  - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ。

6. アプリケーションテレメトリおよびコントローラベースのアプリケーション認識（CBAR）が、該当するネットワークデバイスで有効になっています。
7. デバイスをインベントリに追加します。
8. PnP ラベルトラストポイントは、デバイスが Day-0 オンボーディングを正常に完了し、一覧で管理状態になり、サイトに割り当てられると、自動的に削除されます。

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

まだ起動していないデバイスを初めて要求する場合、デバイスは起動時に自動的にプロビジョニングされます。このプロセスは、デバイスのプランニングと呼ばれます。

デバイスをプロビジョニングするための手順は、デバイスのタイプによって異なります。

- スイッチとルータの参照資料： スイッチまたはルータデバイスのプロビジョニング （23 ページ）
- シスコ ワイヤレス コントローラ、AP、およびセンサー： ワイヤレスコントローラ のプロビジョニング （28 ページ）

スイッチまたはルータデバイスのプロビジョニング

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

始める前に

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、プラグ アンド プレイ プロビジョニングの前提条件 （4 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

デバイスを表示するには、[Focus] ドロップダウンリストから [Default] または [All] を選択します。

デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。[Auto-Refresh] ドロップダウンリストをクリックして、更新間隔を選択します。

[Filter] または [Find] オプションを使用して、特定のデバイスを見つけます。

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

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

ステップ 5 （任意） [Assign Site] ウィンドウで、次の手順を実行します。

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかのタスクを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、[Assign] をクリックし、[Select a Site] ドロップダウンリストからサイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Site to All] を選択します。
- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

（注） デバイスをサイトに割り当てていない場合は、ステップ 6 （24 ページ） でデバイスのテンプレートを選択する必要があります。

c) [Next] をクリックします。

ステップ 6 [Assign Configuration] ウィンドウで、次の手順を実行します。

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次のステップに進みます。それ以外の場合は、次のいずれかの設定を変更または設定します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Image]：このドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。

（注） デバイスのソフトウェア イメージ バージョンまたはゴールデンタグ付きバージョンが 17.14.1 以降の場合、選択したサイトで SNMP ログイン情報に MD5 認証が設定されていると、デバイス要求がブロックされます。

ゴールデンイメージが利用できず、イメージがイメージリポジトリ内で、このデバイスタイプの特定のデバイスロール（Border、Core など）でタグ付けされている場合、ドロップダウンリストに利用可能なイメージが表示されます。

デバイスを要求するには、SNMP ログイン情報に SHA 認証も設定する必要があります。あるいは、ソフトウェア イメージ バージョンが 17.14.1 より前である必要があります。SHA 認証の設定方法については、「グローバル デバイス クレデンシャルの編集」を参照してください。

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

（注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択する必要があります。選択するテンプレートには、デバイスにグローバル デバイス ログイン情報を設定するために必要な CLI コマンドを含める必要があります。それ以外の場合、デバイスは管理対象外の状態で一覧に追加されます。

- [Apply the PKCS12 device certificate on the device]：PKCS12 証明書をデバイスに展開するには、このチェックボックスをオンにします。このオプションは、ルータの場合にのみ使用可能です。
- [RTU License Level]：このドロップダウンリストから、[Lanbase] または [IP Services] を選択します。このオプションは、Cisco Industrial Ethernet（IE）4000 シリーズおよび 5000 シリーズ スイッチでのみ使用できます。
- [Select a Cabling Scheme]：スタックの番号を付け直す場合は、このドロップダウンリストで、スタックのケーブル配線スキームを選択します。

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

図 *1:* ケーブル配線スキーム



- [Select a Top of Stack Serial Number]：スタックスイッチの先頭のシリアル番号は、ユーザが入力したスタックメンバーのシリアル番号が自動入力されます。自動入力されたシリアル番号を使用しない場合は、シリアル番号をクリックし、[Select a Top of Stack Serial Number] で、ドロップダウンリストをクリックします。[X] アイコンをクリックして、シリアル番号の選択を解除します。

  このオプションは、スタック構成をサポートしているスイッチがケーブル配線図に示すように接続されている場合にのみ表示されます。

  計画されているデバイスの場合、スタックスイッチの先頭のシリアル番号がデフォルトとして設定されています。必要に応じて、別のシリアル番号を指定できます。

  要求されていないデバイスの場合、スタックスイッチの先頭のシリアル番号はデフォルトとして設定されません。ドロップダウンリストからスタックスイッチの先頭のシリアル番号を選択します。

- [Select a License Level]：このドロップダウンリストで、スタックのライセンスレベルを選択します。[X] アイコンをクリックして、ライセンス レベルの選択を解除します。

  この項目は、スタック構成をサポートしているスイッチにのみ表示されます。

c) [Save] をクリックします。

d) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Images]：このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

e) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。

スタック構成のデバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

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

g) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 7 すべてのデバイスのテンプレートパラメータ値をまとめて設定するには、次のステップに進みます。デバイスのテンプレートパラメータ値を 1 つずつ設定するには、[Provision Templates] ウィンドウから、次の手順を実行します。

a) 設定するデバイスの名前をクリックします。

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

各デバイスのフィールドに各パラメータの値を入力します。レッド アスタリスクは必須フィールドを表します。

c) 選択したデバイスの起動構成に実行中の構成をコピーする場合、[Copy running config to startup config] チェックボックスをオンにします。

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

e) [Next] をクリックします。

ステップ 8 すべてのデバイスのパラメータ値を一括で指定するには、[Provision Templates] ウィンドウで次の手順を実行します。

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

b) 各パラメータの値をファイルに追加して、ファイルを保存します。

c) [Import] をクリックします。

d) ドラッグアンドドロップ エリアにファイルをドラッグアンドドロップするか、[click to select] をクリックしてファイルを選択します。

e) [Import] をクリックします。

f) [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで、デバイスに関する詳細や構成プレビューステータスを確認できます。

ステップ 10 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列を確認します。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。

プロビジョニングエラーを回避するには、デバイスを要求する前に問題がある場合は解決します。必要に応じて、[Provision Templates] のステップに戻ってパラメータ値やテンプレートを変更したり、[Design] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題があれば解決します。

問題を解決したら、[Day-0 Config] 列に戻り、[Retrying get Day-0 configuration Preview for failed device(s)] をクリックし、[OK] をクリックします。

ステップ 11 [Day-0 Config] 列のリンクをクリックして、デバイス、その構成、構成プレビューエラーの詳細を確認します。

ステップ 12 [Claim] をクリックします。

ステップ 13 確認のダイアログボックスで [Yes] をクリックしてデバイスを要求します。

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了 （36 ページ）を参照してください。

ワイヤレスコントローラ のプロビジョニング

この手順では、[Plug And Play Devices] リストからワイヤレスコントローラを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの [Details] ウィンドウからデバイスを要求することもできます。

始める前に

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、プラグ アンド プレイ プロビジョニングの前提条件 （4 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

検索バーを使用して、特定のデバイスを検索できます。

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

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

ステップ 5 （任意） [Assign Site] ウィンドウで、次の手順を実行します。

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかのタスクを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、[Assign] をクリックし、[Select a Site] ドロップダウンリストからサイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Site to All] を選択します。

- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

割り当てられたサイトに関連付けられているワイヤレス ネットワーク プロファイルにオンボーディング テンプレートがある場合、Catalyst Center はこのテンプレートを PnP オンボーディングに使用します。詳細については、ネットワークプロファイルへのテンプレートの追加を参照してください。

c) [Next] をクリックします。

ステップ 6 [Assign Configuration] ウィンドウで、次の手順を実行します。

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次の手順に進みます。それ以外の場合は、次のいずれかの設定を変更または設定します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Image]：このドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。

（注） デバイスのソフトウェア イメージ バージョンまたはゴールデンタグ付きバージョンが 17.14.1 以降の場合、選択したサイトで SNMP ログイン情報に MD5 認証が設定されていると、デバイス要求がブロックされます。

デバイスを要求するには、SNMP ログイン情報に SHA 認証も設定する必要があります。あるいは、ソフトウェア イメージ バージョンが 17.14.1 より前である必要があります。SHA 認証の設定方法については、グローバル デバイス クレデンシャルの編集を参照してください。

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

（注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択する必要があります。選択するテンプレートには、デバイスにグローバル デバイスログイン情報を設定するために必要な CLI コマンドを含める必要があります。それ以外の場合、デバイスは管理対象外の状態で一覧に追加されます。

アシュアランスの使用例とデバイスごとの設定を含む、非インテントベースのネットワーク展開での AP のオンボーディングについては、非インテントベースの展開に PnP を使用する AP のオンボーディング を参照してください。

- [Catalystワイヤレス LANコントローラ設定（Catalyst Wireless LAN Controller Settings）]：Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、必須フィールドである [ワイヤレス管理IP（Wireless Management IP）]、[サブネットマスク（Subnet Mask）]、[ゲートウェイ（Gateway）]、[ワイヤレス管理IP（IPv6）（Wireless Management IP (IPv6)）]、[プレフィックス（Prefix）]、[ゲートウェイ（IPv6）（Gateway (IPv6)）]、[IPインターフェイス名（IP Interface Name）] 、およびオプションで [VLAN ID] のフィールドにデータを入力します。

（注） 使用可能なフィールドは ワイヤレスコントローラ の IP アドレスタイプによって異なります。ワイヤレスコントローラに IPv4 アドレスタイプのみが含まれている場合、Catalyst Center には IPv4 アドレスのフィールドが表示されます。IPv6 アドレスタイプのみが含まれている場合、Catalyst Center には IPv6 アドレスのフィールドが表示されます。IPv4 と IPv6 の両方のアドレスタイプがある場合、Catalyst Center には IPv4 アドレスと IPv6 アドレスの両方のフィールドが表示されます。

- Mobility Express デバイスの場合は、[Wireless management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。
- 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

c) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Images]：このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

d) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。

[ライセンスレベルを他のデバイスに適用（Apply License Level to Other Devices）] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

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

f) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 7 [Provision Templates] ウィンドウで、[Devices] エリアからテンプレートを選択し、[Domain] フィールドにドメイン名を入力して、[Next] をクリックします。

ステップ 8 [Summary] ウィンドウで、デバイスに関する詳細や構成プレビューを確認できます。

ステップ 9 設定プレビューが成功したかどうかを確認するには、各デバイスの [Device Configuration] 列をチェックします。

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

ステップ 10 [Device Configuration] 列で、[Preview Configuration] をクリックして設定を確認します。

ステップ 11 [要求（Claim）] をクリックします。

ステップ 12 確認ダイアログボックスで [Yes] をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

（注） 選択したサイトに競合する操作がある場合、現在の設定を続行するには、既存、スケジュール済み、またはレビュー保留の操作が完了するまで待つか、この操作を破棄する必要があります。

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了 （36 ページ）を参照してください。

AP またはセンサーデバイスのプロビジョニング

[プラグアンドプレイデバイス（Plug and Play Devices）] リストから AP またはセンサーデバイスを要求するには、次の手順を実行します。代わりに、[Claim] をクリックしてデバイスの [Details] ウィンドウからデバイスを要求することもできます。

Before you begin

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、「プラグ アンド プレイ プロビジョニングの前提条件 （4 ページ）」を参照してください。

手順

ステップ 1 **[プラグアンドプレイ（Plug and Play）]** に移動して、必要なデバイスを選択します。

a) メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

b) テーブル内のデバイスを表示します。

検索バーを使用して、特定のデバイスを検索できます。

c) 要求するデバイスの横にあるチェックボックスをオンにします。

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

ステップ 2 （任意） [Assign Site] ウィンドウで、次の手順を実行します。

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかのタスクを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、[Assign] をクリックし、[Select a Site] ドロップダウンリストからサイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Site to All] を選択します。
- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

割り当てられたサイトに関連付けられているワイヤレス ネットワーク プロファイルにオンボーディング テンプレートがある場合、Catalyst Center はこのテンプレートを PnP オンボーディングに使用します。詳細については、「ネットワークプロファイルへのテンプレートの追加」を参照してください。

（注） **[System]** > **[Settings]** > **[Device Settings]** > **[PnP AP Location]** ウィンドウでは、次のようになります。

- [Configure AP Location] チェックボックスがオンの場合、AP の設定 は PnP オンボーディング中にこのサイトを AP ロケーションとして割り当てます。
- [Configure AP Location] チェックボックスがオフの場合、Catalyst Center は PnP オンボーディング中にこのサイトを AP ロケーションとして設定しません。[Configure Access Points] ワークフローを使用して AP の場所を設定できます。詳細については、「AP の設定」を参照してください。

詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Configure AP location for PnP onboarding」を参照してください。

c) [Next] をクリックします。

ステップ 3 [Assign Configuration] ウィンドウで、次の手順を実行します。

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次の手順に進みます。それ以外の場合は、次のいずれかの設定を変更または設定します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Template]：このドロップダウンリストで、デバイスに適用するオンボーディング設定テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

（注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択する必要があります。選択するテンプレートには、デバイスにグローバル デバイスログイン情報を設定するために必要な CLI コマンドを含める必要があります。それ以外の場合、デバイスは管理対象外の状態で一覧に追加されます。

アシュアランスのユースケースと デバイスごとの設定 を含む、非インテントベースのネットワーク展開での AP のオンボーディングについての詳細は、「非インテントベースの展開に PnP を使用する AP のオンボーディング」を参照してください。

- AP の場合、[APゾーン（AP Zone）] ドロップダウンリストから AP ゾーンを選択します。[RFプロファイル（RF Profile）] は自動的に入力され、SSID 数は選択した AP ゾーンに基づいて表示されます。デフォルトの AP ゾーンを選択する場合は、RF プロファイルを選択します。

- AP の場合、[無線周波数プロファイル（Radio Frequency Profile）] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1つのプロファイルをデフォルトとして指定した場合に設定できます。
- センサーの場合、[センサー設定（Sensor Settings）] ドロップダウンリストで、デバイスに適用するセンサー デバイス プロファイル（バックホール）を選択します。

（注） 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサー デバイス プロファイル **CiscoProvisioningSSID** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。

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

c) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。
- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Images]：このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

d) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。
e) プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。
f) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 4 [Provision Templates] ウィンドウで、[Devices] エリアからテンプレートを選択し、[Domain] フィールドにドメイン名を入力して、[Next] をクリックします。

（注） デバイスがサイトに割り当てられている場合は、[次へ（Next）] をクリックします。

ステップ 5 [Summary] ウィンドウで、デバイスに関する詳細や構成プレビューを確認できます。

ステップ 6 設定プレビューが成功したかどうかを確認するには、各デバイスの [デバイス設定（Device Configuration）] 列をチェックします。

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

ステップ 7 [Device Configuration] 列で、[Preview Configuration] をクリックして設定を確認します。

ステップ 8 [要求（Claim）] をクリックします。

ステップ 9 確認ダイアログボックスで [Yes] をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

（注） 選択したサイトに競合する操作がある場合、現在の設定を続行するには、既存、スケジュール済み、またはレビュー保留の操作が完了するまで待つか、この操作を破棄する必要があります。

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了 （36 ページ） を参照してください。

StackWise Virtual Link スイッチのプロビジョニング

PnP のオンボーディング中に、StackWise Virtual Link（SVL）を使用して、接続されたスイッチのペアを単一の論理デバイスとしてオンボーディングできます。現在、SVL PnP オンボーディングは、Catalyst 9500 シリーズ スイッチでのみサポートされています。

Before you begin

- 両方のスイッチが直接接続されていることを確認します。
- 最小速度 1 Gbps のリンクを使用してスイッチを接続し、インターフェイス速度が一致していることを確認します。
- スイッチが初期化状態にあることを確認します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]** を選択します。

ステップ 2 [SVL スイッチの要求（Claim a SVL switch）] をクリックします。

ステップ 3 [SVL スイッチとして要求（Claim as an SVL switch）] ポップアップウィンドウで、SVL オンボーディング設定に必要な値を入力します。

1. [アクティブスイッチ（Active Switch）]：スイッチの 1 つをアクティブスイッチとして選択します。
2. [スタンバイスイッチ（Standby Switch）]：スタンバイスイッチとして別のスイッチを選択します。
3. [StackWise Virtual Link]：SVLリンクを選択します。最大 8 つの SVL リンクを選択できます。
4. [デュアルアクティブ検出リンク（Dual-Active Detection Link）]：使用可能な場合、デュアルアクティブ検出リンクを選択します。
5. [ドメイン（Domain）]：ドメインに一意の値を割り当てます。

ステップ 4 [サイトの選択（Select Site）] を クリックし、SVL スイッチの目的のサイトを選択します。

ステップ 5 [テンプレートの管理（Manage Template）] をクリックし、SVL スイッチにプロビジョニングするテンプレートを選択します。

ステップ 6 （任意） SVL 作成後に適用する標準イメージを選択します。

デバイス上のイメージバージョンが異なる場合、PnP では標準イメージが強制的に選択され、SVL 生成の前に両方のデバイスに適用されます。

ステップ 7 [Claim] をクリックします。

PnP サーバーは SVL を作成し、デバイスをプロビジョニングします。

プロビジョニングプロセスの完了

プラグアンドプレイのプロビジョニング中に、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。他のネットワーク設定はプッシュされません。プラグアンドプレイのプロビジョニングが完了したら、[Design] 領域で構成されているネットワーク設定をプッシュすることで、プロビジョニングプロセスを完了できます。

ネットワーク設定には AAA サーバー設定が含まれます（設定されている場合）。Cisco ISE の場合、Catalyst Center は Cisco ISE のデバイスを RADIUS または TACACS の AAA クライアントとして設定します。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラおよびCisco Catalyst 9000 シリーズ スイッチでは、デイゼロ設定中に NETCONF が有効になると、ローカル AAA 設定がデバイスにプッシュされます。

ワイヤレスおよびセンサーデバイスの場合、ネットワーク設定には、RF プロファイルやアンテナ無線プロファイルなどのワイヤレス設定が含まれます（設定されている場合）。詳細については、「ワイヤレスデバイスのプロビジョニングの概要」を参照してください。

始める前に

- 次のいずれかの手順を使用して、デバイスがプロビジョニング（オンボード）されていることを確認します。
  - スイッチまたはルータデバイスのプロビジョニング （23 ページ）
  - ワイヤレスコントローラ のプロビジョニング （28 ページ）
- ネットワークの設定値を設定します。詳細については、ネットワークの設定を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 デバイスを選択し、**[Actions]** > **[Provision]** > **[Provision Device]** を選択します。

ステップ 3 ワークフローの手順を進めます。

ステップ 4 [Summary] ウィンドウで、残りのネットワーク設定を確認します。変更を加えるには、関連するカテゴリの横にある [Edit] をクリックします。それ以外の場合は、[Deploy] をクリックします。

（注） デバイスのソフトウェア イメージ バージョンまたはゴールデンタグ付きバージョンが 17.14.1 以降の場合、選択したサイトで SNMP ログイン情報に MD5 認証が設定されていると、デバイス要求がブロックされます。

デバイスを要求するには、SNMP ログイン情報に SHA 認証も設定する必要があります。あるいは、ソフトウェア イメージバージョンが 17.14.1 より前である必要があります。SHA 認証の設定方法については、「グローバル デバイス クレデンシャルの編集」を参照してください。

ステップ 5 （任意） デバイスで構成を展開すると、[Task Progress] バーに、**[Activities]** > **[Tasks]** で進行中のプロビジョニングタスクの進行状況が表示されます（タスク名をクリックすると表示されます）。

デバイスの削除

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

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

（注）
- デバイスがプロビジョニングの状態の場合は、[Inventory] タブからのみ削除できます。
- デバイスが一時的な状態（接続中や実行中など）の場合、そのデバイスは [プラグアンドプレイ デバイス（Plug and Play Devices）] リストから削除できません。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

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

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

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

ステップ 5 （任意）要求元不明デバイスの場合は、[インベントリ内のこのデバイスのプラグアンドプレイ機能を削除（Delete Plug and Play capabilities for this device in inventory）] チェックボックスをオンにします。

このオプションを選択すると、Catalyst Center はデバイスプロファイルを削除し、デバイスは PnP に再表示されません。

デバイスはインベントリに残り、引き続き管理できます。PnP 機能は後で再度有効にできます。

ステップ 6 [OK] をクリックします。

デバイスのリセット

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

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

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

（注） デバイスが一時的な状態（接続中や実行中など）の場合、リセットすることはできません。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

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

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

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

確認ダイアログボックスが表示されます。

ステップ 5 次のオプションのいずれかを選択します。

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

ステップ 6 [**リセット（Reset）**] をクリックします。

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。

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。

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。

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。

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。

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。

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。

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。