Cisco ネットワーク プラグ アンド プレイの設定

このドキュメントでは、Ciscoネットワーク プラグアンドプレイ ソリューションの概要を示し、プロジェクトを事前プロビジョニングしネットワーク内の未計画のデバイスを管理するプロセスについて説明します。

この章では、次の事項について説明します。

- Cisco ネットワーク プラグ アンド プレイの概要，2 ページ
- Cisco ネットワーク プラグ アンド プレイの編成，2 ページ
- プロジェクトの事前プロビジョニング ワークフロー，5 ページ
- 設定テンプレートの使用，9 ページ
- プロジェクトの複製，10 ページ
- デバイスのワークフロー，11 ページ
- シスコ デバイスのイメージ ファイルのアップロード，14 ページ
- デバイスへのデフォルト イメージの関連付け，14 ページ
- コンフィギュレーション ファイルのアップロード，16 ページ
- テンプレートのアップロード，16 ページ
- プロジェクトおよびデバイスの一括インポート，17 ページ
- シスコ スマート アカウントの設定，17 ページ
- イメージ プロビジョニングのタイムアウトの設定，19 ページ
- 設定プロビジョニングのタイムアウトの設定，20 ページ
- セキュリティのワークフロー，20 ページ
- デバイスでの AAA の設定，23 ページ
- Cisco 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，23 ページ

Cisco ネットワーク プラグ アンド プレイの概要

Cisco ネットワーク プラグ アンド プレイ ソリューションは、新しいブランチやキャンパスの展開を容易にする企業ネットワークのカスタマーのために、または既存ネットワークに更新のプロビジョニングを行うために、シンプルで、セキュアな、単一化された、統合サービスを提供します。ソリューションは、身近なゼロタッチ導入エクスペリエンスで Cisco ルータ、スイッチ、ワイヤレスデバイスを構成するプロビジョンのエンタープライズネットワークへの統合されたアプローチを提供します。Cisco ネットワーク プラグ アンド プレイ ソリューションの詳細については、『*Solution Guide for Cisco Network Plug and Play*』を参照してください。

Cisco ネットワーク プラグ アンド プレイ アプリケーションを使用すると、リモート プロジェクトを事前プロビジョニングしたり、未計画のデバイスを要求したりできます。大規模なプロジェクトをプロビジョニングする場合、Cisco ネットワーク プラグ アンド プレイ アプリケーションを使用してプロジェクトを事前プロビジョニングし、プロジェクトにデバイスを追加できます。これには、インストールする各デバイスのデバイス情報の入力と、ブートストラップ設定、全構成、およびシスコ デバイスのイメージのセットアップが含まれます。ブートストラップ設定では、プラグ アンド プレイ エージェントを有効にし、使用するデバイス インターフェイスを指定し、その静的 IP アドレスを設定します。

事前プロビジョニングが不要な小規模プロジェクトを作成する場合、デバイスは、Cisco ネットワーク プラグ アンド プレイ アプリケーションで事前設定せずに、そのまま展開し、要求できます。デバイス インストーラがシスコ ネットワーク デバイスをインストールし起動すると、デバイスは DHCP または DNS を使用して Cisco APIC-EM コントローラを自動検出します。自動検出プロセスが完了した後、デバイスは Cisco ネットワーク プラグ アンド プレイ アプリケーションで未計画のデバイスとしてリストされます。Cisco ネットワーク プラグ アンド プレイ アプリケーションを使用して、未計画のデバイスを要求し、新しい設定およびシスコ デバイスのイメージを使用して設定できます。

Cisco ネットワーク プラグ アンド プレイの編成

Cisco ネットワーク プラグ アンド プレイ Web インターフェイスは、次の表に示す高レベルのタスク エリアを含むワークフローに編成されます。Cisco ネットワーク プラグ アンド プレイ アプリケーションは、ネットワーク エンジニアがリモート サイトを事前プロビジョニングし、未計画のデバイスを要求するために使用します。このマニュアルでは、同じ一般構成に従います。

表 *1*：*Cisco* ネットワーク プラグ アンド プレイの編成

タスク エリア	説明
ダッシュボード	プロジェクトおよび未計画のデバイス情報のクイック ビューを提供するダッシュボードを表示できます。詳細については、Cisco ネットワーク プラグ アンド プレイ ダッシュボード, （4 ページ）を参照してください。

Projects（プロジェクトの事前プロビジョニング ワークフロー）	プロジェクトを作成および事前プロビジョニングできます。[Add Device] オプションを使用してプロジェクトに新しいデバイスを追加できます。詳細については、プロジェクトの事前プロビジョニング ワークフロー, （5 ページ）を参照してください。
Devices（未計画のデバイスのワークフロー）	未計画のデバイスを要求できます。未計画のデバイスを要求するか、無視するか、または削除できます。
イメージ	ローカルマシンからイメージをアップロードして、デバイスにデフォルトイメージを関連付けることができます。詳細はデバイスへのデフォルト イメージの関連付け, （14 ページ）を参照してください。
構成	コンフィギュレーションおよびブートストラップ ファイルをローカル マシンからアップロードできます。リストからコンフィギュレーション ファイルを表示したり、削除したりできます。
Templates	テンプレートをローカルマシンからアップロードできます。リストからテンプレートを表示したり、削除したりできます。
一括インポート	独自の一括インポート ファイルを作成するために使用できるテンプレートをダウンロードできます。テンプレートをダウンロードするには、ネットワーク プラグ アンド プレイ アプリケーションの [Bulk Import] セクションの [Sample] ボタンをクリックします。
Settings（シスコ スマート アカウント）	シスコ スマート アカウント機能により、APIC-EM コントローラのオンプレミスのシスコ プラグ アンド プレイ サーバとスマート アカウントが有効な PNP クラウド リダイレクション サービスを統合し、デバイスのプロビジョニングを自動化できます。詳細については、シスコ スマート アカウントの設定, （17 ページ）を参照してください。

Settings（APIC-EM でのグローバル設定）	[Settings] オプションは、Cisco APIC-EM グローバル ツールバーの右上端にあります。管理者およびオペレータ ロールを作成し、セキュリティ設定を管理できます。
ログ	[Logs] オプションは、固定グローバル ツールバーの右上端にあります。Cisco ネットワーク プラグ アンド プレイ アプリケーションに関するログを収集できます。詳細については、Cisco ネットワーク プラグアンドプレイ ログの収集, （24 ページ）を参照してください。

Cisco ネットワーク プラグ アンド プレイ ダッシュボード

Cisco ネットワーク プラグ アンド プレイ ダッシュボードには、ネットワークの最も重要なデータが一目でわかるように表示されます。ダッシュボードのグラフ表示には、事前プロビジョニング、進行中、プロビジョニング、およびプロジェクトのリストがエラー情報とともに表示されます。また、未請求デバイス、要求されたデバイス、および無視されたデバイスも表示されます。各円グラフの横にあるリンクをクリックして情報をすばやくスキャンし、関連プロジェクトまたはデバイスのリストにアクセスできます。特定のプロジェクトまたはデバイスの詳細を表示するには、最初のカラムのプロジェクトまたはデバイス名をクリックして、情報に基づいてアクションを実行します（図 1 を参照）。

[Dashboard] ページには、次のオプションがあります。

- Search Projects：プロジェクトのリストを検索し、プロジェクトをロードできます。
- Search Device：名前、シリアル番号、および MAC アドレスに基づいてデバイスを検索できます。

図 *1*：*Cisco* ネットワーク プラグ アンド プレイ ダッシュボード

プロジェクトの事前プロビジョニング ワークフロー

Cisco ネットワーク プラグ アンド プレイを使用して、新しいプロジェクトを事前プロビジョニングし、計画することができます。新しいプロジェクトを作成すると、Cisco ネットワーク プラグアンドプレイによって、選択したプラットフォームのコンフィギュレーションファイル、イメージ ファイル、およびデバイス ID 証明書を事前プロビジョニングできます。これは、サイトが完全に機能するためにかかる時間を簡素化および迅速化します。
ネットワークのプロジェクトを事前プロビジョニングするには、次の手順を実行します。

ステップ 1 新しいプロジェクトを作成します（プロジェクトの作成, （5 ページ） を参照）。
ステップ 2 プロジェクトにデバイスを追加します（デバイスの追加, （6 ページ） を参照）。

プロジェクトの作成

Cisco ネットワーク プラグ アンド プレイ（PnP）アプリケーションでは、プロジェクトの作成に必要なリソースのプロジェクトベース管理を行うことで、新しい IWAN サイトを容易に作成できます。これらのリソースには、コンフィギュレーションファイル、イメージファイル、およびデバイス ID 証明書が含まれます。Cisco ネットワーク PnP プロジェクトは、デバイス関連情報を収集し、Cisco APIC-EM IWAN アプリケーションで特定の IWAN サイトを事前プロビジョニングするために役立つ固有のエンティティです。別のプロジェクトをプロビジョニングするためにプロジェクト情報およびリソースを再利用するには、既存のプロジェクトを、固有のプロジェクト ID を持つ新しいプロジェクトに複製します。その後、必要に応じて [Projects] タブを使用して新しいプロジェクトを編集できます。

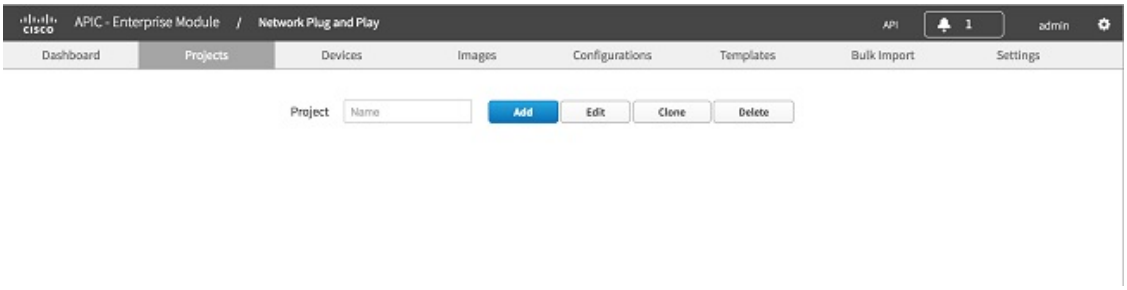
プロジェクトを作成するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Projects] を選択します。
ステップ 2 [Add] をクリックすると、[Add Project] ダイアログ ボックスが表示されます。
ステップ 3 [Add Project] テキスト ボックスに、新しいプロジェクトの名前を入力します。
ステップ 4 ファイルの完全なパス名を指定して TFTP サーバ オプションを使用するには、TFTP サーバの IP アドレスまたは URL を入力します。コンフィギュレーション ファイルまたはイメージ ファイルは、APIC-EM コントローラからではなく、指定された場所からデバイスにダウンロードされます。
Cisco APIC-EM サーバからコンフィギュレーション ファイルおよびイメージ ファイルをダウンロードするオプションがない場合は、外部 TFTP サーバからコンフィギュレーション ファイルおよびシスコ デバイスのイメージ ファイルを導入できます。
ステップ 5 [Installer Notes] アイコンをクリックし、参照ドキュメントについてのメモを追加します。テキスト ファイル、イメージ ファイル（GIF、ビットマップ、JPEG）、および Microsoft PowerPoint 形式がサポートされ

ています。これらのメモは、Cisco PnP モバイル アプリを使用してデバイスを展開するインストーラで使用できます。

ステップ 6 [Create] をクリックして、新しいプロジェクトを作成します（図 2 を参照）。

図 *2*：プロジェクトの作成



（注） 外部 TFTP サーバからコンフィギュレーション ファイルおよびシスコ デバイスのイメージ ファイルを導入する場合、設定およびイメージ リソースから入手できるコンフィギュレーション ファイルおよびシスコ デバイスのイメージ ファイルを使用することはできません。

デバイスの追加

デバイスを追加するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Projects] を選択します。

ステップ 2 既存のプロジェクトをロードするには、[Project] テキスト ボックスに、プロジェクトの名前を入力します。

ステップ 3 [Add] をクリックして、ポリシーを追加します。

ステップ 4 次の情報を入力します。

- Device Name：デバイス名（サイトごとに一意）
- Product ID：ドロップダウンリストからデバイスの製品識別番号を選択します。
- Serial Number：デバイスのシリアル番号（または）
- MAC Address：デバイスの MAC アドレス。これはアクセス ポイント デバイスにのみ適用可能です。

ステップ 5 次のいずれかのオプションを実行して、デバイスに適用する Cisco デバイス イメージ ファイルを選択します。

- Cisco APIC-EM コントローラにロード済みのデバイスに既存のシスコ デバイスのイメージをロードするには、イメージ フィールドをクリックし、ドロップダウンリストからイメージ ファイルを選択します。

- [Upload] アイコンをクリックし、デバイスに適用する Cisco デバイス イメージ ファイルを選択します。デバイスに新しいシスコ デバイスのイメージ ファイルをロードするには、サーバにシスコ デバイスのイメージ ファイルをアップロードし、リストからイメージ ファイルを選択する必要があります。シスコ デバイスのイメージ ファイルのアップロード, （14 ページ）を参照してください。このオプションは、アクセス ポイント デバイスではサポートされていません。

ステップ 6 次のいずれかのオプションを実行して、デバイスに適用するコンフィギュレーション ファイルまたはテンプレートのいずれかを選択します。

- Cisco APIC-EM コントローラにアップロード済みのデバイスにコンフィギュレーション ファイルまたはテンプレートのいずれかを適用するには、適切なオプション ボタンをクリックし、ドロップダウン リストからコンフィギュレーション ファイルまたはテンプレートを選択します。
- デバイスに適用するには [Upload] アイコンをクリックします。

Cisco ネットワーク プラグ アンド プレイでは、テンプレートを生成するために、バージョン 1.7 の Velocity エンジンを使用しています。Velocity エンジンの詳細については、http://velocity.apache.org/ を参照してください。複数のデバイスに同じ設定を導入する必要がある場合は、テンプレートを使用できます。テンプレートを使用する場合、デフォルト値を選択するか、指定したデバイスにカスタマイズされた値を指定できます。

注：ルータとスイッチに対しては、コンフィギュレーション ファイルはテキスト形式である必要があります。アクセス ポイント デバイスの場合、コンフィギュレーション ファイルは、JSON 形式にする必要があります。

ステップ 7 テンプレートを選択した場合は、次の手順を実行します。

a) 指定したデバイスにカスタマイズされた値を指定するには、テンプレートをクリックし、テンプレート エディタに値を入力します。

b) テンプレートの設定値をプレビューするには、[Preview] タブをクリックします。

ステップ 8 （任意）既存のブートストラップ設定をデバイスに適用するには、ドロップダウン リストからコンフィギュレーション ファイルを選択するか、または [Upload] アイコンをクリックし、デバイスに対してブートストラップ ファイルを選択します。WAN デバイスでブートストラップ設定を展開するには、Cisco ネットワーク プラグ アンド プレイ モバイル アプリケーションを使用できます。このオプションは、アクセス ポイント デバイスではサポートされていません。

ステップ 9 [Device Certificate] チェックボックスをオンにして、デバイスにデバイス証明書を適用します。Cisco ネットワーク プラグ アンド プレイによって、PKCS12 デバイス ID 証明書が自動的に生成されて展開されます。デバイス証明書は、アクセス ポイント デバイスではサポートされていません。

ステップ 10 [SUDI Required] チェックボックスをオンにして、SUDI 認証をサポートするデバイスに SUDI 認証を適用します。SUDI 認証をサポートしていないデバイスに対してこのチェックボックスをオンにすると、認証およびプロビジョニングに失敗して認証エラーが発生します。[SUDI Required] チェックボックスをオフにして、デバイスをリセットして再度プロビジョニングする必要があります。

注：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際には、シリアル番号フィールドに SUDI のシリアル番号を入力する必要があります。

ステップ 11 設定クレデンシャルを追加するには、クレデンシャル設定（プラス記号 [+]）ボタンをクリックして、必要な情報を指定します（デバイスでの AAA の設定, （23 ページ）を参照）。

ステップ 12 スタック スイッチを設定するには、スタック スイッチ設定（プラス記号 [+]）ボタンをクリックして、次の情報を指定します。

- Expected Member Count：ドロップダウン リストから、スタックの予想メンバー総数（マスターを含む）を選択します。
- License：ドロップダウン リストからライセンスを選択して、選択したライセンスをスタックのすべてのメンバーが確実に持てるようにします。
- Accept EULA：[Accept EULA] チェックボックスをオンにします。

ステップ 13 [Add] をクリックして、スタック スイッチを設定します。
注：スタックのメンバーであるデバイスを 1 つ追加すると、システムは他のメンバーを自動的に検出します。

スタック スイッチのメンバーを表示するには、デバイス リスト テーブルで、デバイスの横の [Stack View] アイコンの上にカーソルを移動します。

ステップ 14 デバイス テーブルにある 1 つ以上のデバイスを編集するには、編集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ます。
注：スタック デバイスと非スタック デバイスを一緒に編集することはできません。また、アクセス ポイントと他のデバイスを同時に編集することはできません。

ステップ 15 設定クレデンシャルを追加するには、クレデンシャル設定（プラス記号 [+]）ボタンをクリックして、次を指定します。

- Username：設定用のユーザ名を入力します。
- Password：設定用のパスワードを入力します。
- Confirm Password：確認のためにパスワードを再入力します。

ステップ 16 選択したデバイスを削除またはリセットするには、[Delete] または [Reset] をクリックします。

ステップ 17 [Save] をクリックして変更を保存します。

デバイスの配置

プロジェクトを作成したら、リモート サイトでプロビジョニング プロセスを開始できます。ラックにデバイスを設置し、電源ケーブルを接続する必要があります。デバイスの電源をオンにし、Cisco プラグ アンド プレイ モバイル アプリを使用してデバイスを配置し、デバイスにブートストラップ設定を配信します。

スタックのメンバー上に展開されるイメージのバージョンは、アクティブ スイッチのバージョンと同じである必要があります。両方が同一でない場合、スタックをプロビジョニングする前に、手動でスタックのバージョン不一致を訂正する必要があります。

注：Cisco APIC-EM を自動的に検出するためにネットワークで DHCP または DNS が設定されている場合、デバイスは電源がオンになると Cisco APIC-EM を自動的に検出し、すべての設定をダウンロードできます。ブートストラップ設定は、アクセスポイントデバイスではサポートされていません。ブートストラップ設定では、DHCP または DNS を使用して Cisco APIC-EM を検索します。デバイスでプロビジョニング プロセスを開始する方法の詳細については、『*Cisco Network Plug and Play Solution Guide*』を参照してください。

設定テンプレートの使用

Cisco ネットワーク プラグ アンド プレイの設定テンプレートを使用して、ブランチ内でデバイスを設定するために必要な一連のデバイス構成を設計できます。類似したデバイスと設定のセットを使用するサイト、オフィス、またはブランチがある場合は、設定テンプレートを使用して、ブランチ内の 1 台以上のデバイスに適用できる汎用設定を作成できます。新しいブランチがあり、ブランチ内のデバイスで共通の設定を迅速かつ正確にセットアップする場合にも、コンフィギュレーション テンプレートを使用できます。多数のデバイスにわたって設定を変更するには、時間と手間がかかることがあります。テンプレートで必要な設定を適用し、デバイス間で一貫性を保つことにより、時間を節約できます。設定テンプレートは、Velocity Template Language（VTL）をサポートしています。

設定テンプレートのサポートにより、管理者は複数のネットワーク デバイスを一貫して設定するのに使用する CLI コマンドの設定テンプレートを定義できるようになり、導入時間を短縮できます。テンプレートに含まれる変数により、デバイスごとの特定の設定のカスタマイズが可能で、テンプレートは #set、#if、#else、#foreach などの構造をサポートします。設定テンプレートは、オープン ソースの Velocity テンプレート エンジン、バージョン 1.7 に基づいています。

このリリースは、暗号化されたパスワードに含まれる $ の文字などの変数定義として解釈されないように、$の文字をエスケープする新しい機能を設定テンプレートに提供します。$の文字をエスケープするには、設定テンプレートの $ のすぐ後ろに {esc.d} を追加します。

たとえば、設定テンプレートに次の行がある場合、$ の文字が変数として解釈されないようにします。

```
enable secret 5 $1$cJX0$Cq6AtbQYt4owH2QTWmP4v/
Escape the $ characters as follows:
enable secret 5 ${esc.d}1${esd.d}cJX0${esc.d}Cq6AtbQYt4owH2QTWmP4v/
```

（注） **auto qos trust**、**auto qos voip trust**、**auto qos voip cisco-phone** などの自動 QoS マクロ コマンドは、Cisco PnP 設定テンプレートを介してコマンドがデバイスに展開される場合には、展開されません。

設定テンプレートを作成して使用するには、次の手順を実行します。

ステップ 1 設定テンプレートを作成し、テンプレートをマシンに保存します。

ステップ 2 Cisco ネットワーク プラグ アンド プレイ サーバに設定テンプレート ファイルをアップロードします。Cisco ネットワーク プラグ アンド プレイ サーバは、txt および .vm テンプレート ファイル形式をサポートします。テンプレートをアップロードする方法については、テンプレートのアップロード, （16 ページ）を参照してください。
Cisco PnP サーバは変数により設定テンプレート ファイルを自動的に検出し、次のビューにファイルを表示します。

- テキスト ビュー
- フォーム ビュー：変数にデフォルト値を割り当てます。
- プレビュー

ステップ 3 ユーザ作成変数またはシステム生成変数を定義します。

ステップ 4 次のいずれかのオプションを実行して、デバイスに適用する設定テンプレートを選択します。

- Cisco APIC-EM コントローラにアップロード済みのデバイスに設定テンプレートを適用するには、[Template] オプション ボタンをクリックし、ドロップダウン リストからテンプレートを選択します。
- [Upload] アイコンをクリックして、デバイスに適用するテンプレートを選択します。

Cisco ネットワーク プラグ アンド プレイでは、テンプレートを生成するために、バージョン 1.7 の Velocity エンジンを使用しています。Velocity エンジンの詳細については、http://velocity.apache.org/ を参照してください。複数のデバイスに同じ設定を導入する必要がある場合は、テンプレートを使用できます。テンプレートを使用する場合、デフォルト値を選択するか、指定したデバイスにカスタマイズされた値を指定できます。

ステップ 5 指定したデバイスにカスタマイズされた値を入力するには、[Form View] をクリックし、テンプレート エディタに値を入力します。

ステップ 6 テンプレートの設定値をプレビューするには、[Preview] タブをクリックします。

ステップ 7 [Save] をクリックして変更を保存します。

プロジェクトの複製

このオプションでは、プロジェクトを複製し、パラメータを使用して新しいプロジェクトを作成できます。プロジェクトを複製する場合、デバイスの設定やシリアル番号はコピーされません。プロジェクトを複製する場合、デバイス名および割り当てられている製品 ID のみが複製されます。

プロジェクトを複製するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Projects] を選択します。

ステップ 2 [Clone] をクリックして、選択したプロジェクトを複製します。

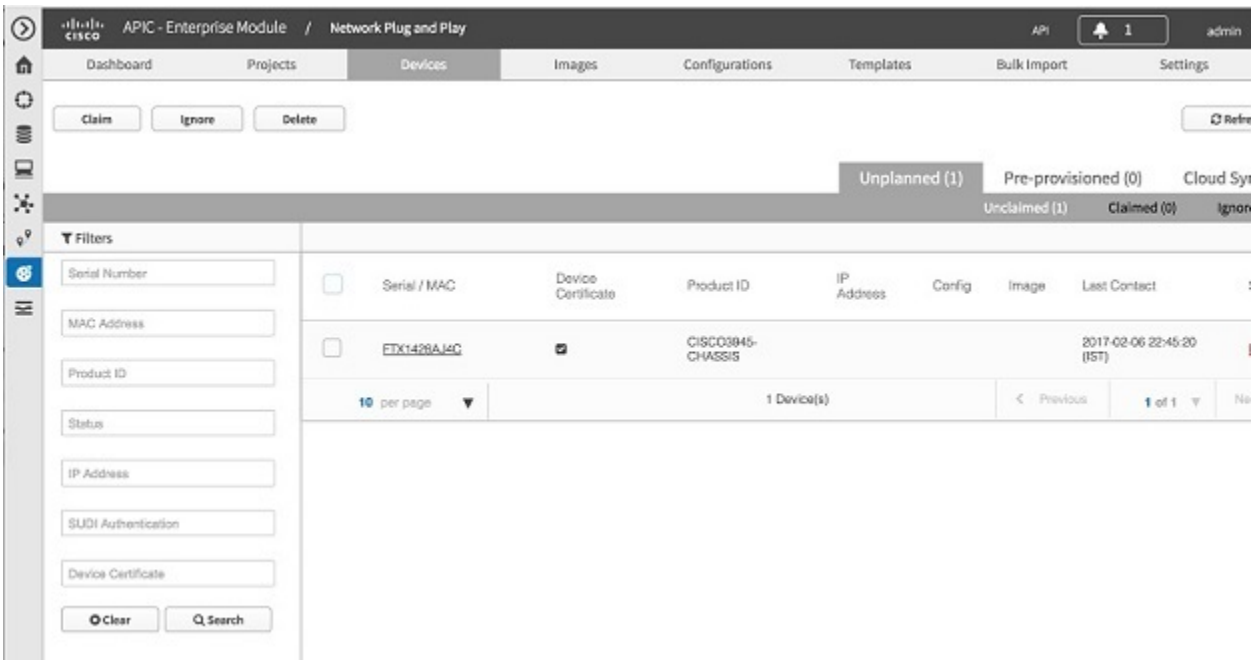
ステップ 3 [Clone Project] ダイアログボックスで、プロジェクトの名前を入力するか、またはドロップダウン リストからプロジェクトを選択します。

ステップ 4 プロジェクトを複製した後、複製したプロジェクトのデバイスごとに、シリアル番号/MAC アドレス、設定、イメージ、およびその他の設定を行う必要があります。

デバイスのワークフロー

事前プロビジョニングが不要な小規模プロジェクトの場合、デバイスは、Cisco ネットワーク プラグアンドプレイアプリケーションで事前設定せずに、そのまま展開し、要求できます。[Devices] ページには、未請求デバイス、要求されたデバイス、無視されたデバイスの詳細情報がそれぞれ示されています（図 3 を参照）。

図 *3* : **未計画のデバイス**



デバイスの要求

サーバに接続するためにデバイスが Call-Hone エージェント機能を用いた場合、シスコ APIC-EM でプロビジョニングされる前、もしくはシスコ APIC-EM が既存の設定に対してデバイスに一致しない場合は、未請求デバイス リストにデバイスが追加されます。

デバイスを要求するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Devices] を選択します。

ステップ 2 リストからデバイスを選択して、[Claim] をクリックします。[Claim Device] ダイアログボックスが表示されます。

ステップ 3 リストから既存のシスコ デバイスのイメージを再利用するか、新しいイメージ ファイルをデバイスに適用できます。

- デバイスに既存のシスコデバイスのイメージをロードするには、テキストボックスをクリックして、ドロップダウンリストからイメージ ファイルを選択します。
- [Upload] アイコンをクリックし、デバイスに適用する Cisco デバイス イメージ ファイルを選択します。
- ファイルの完全なパス名を指定して TFTP サーバ オプションを使用するには、TFTP サーバの IP アドレスを入力します。イメージ ファイルは、APIC-EM コントローラからではなく、指定された場所からデバイスにダウンロードされます

ステップ 4 リストから既存のコンフィギュレーション ファイルまたはテンプレートを再利用するか、または新規コンフィギュレーション ファイルまたはテンプレートをデバイスに適用することができます。

- Cisco APIC-EM コントローラにアップロード済みのデバイスにコンフィギュレーション ファイルまたはテンプレートのいずれかを適用するには、適切なオプション ボタンをクリックし、ドロップダウン リストからコンフィギュレーション ファイルまたはテンプレートを選択します。設定テンプレートの詳細については、設定テンプレートの使用, （9 ページ）を参照してください。

  （注） このコンフィギュレーション ファイルには、AAA 認証コマンドがあります。AAA 認証コマンドを使用するには、デバイス クレデンシャルを提供します。デバイスでは推奨される最低限の IOS バージョンが必要です。

- デバイスに適用するには [Upload] アイコンをクリックします。

- ファイルの完全なパス名を指定して TFTP サーバ オプションを使用するには、TFTP サーバの IP アドレスまたは URL を入力します。コンフィギュレーション ファイルは、APIC-EM コントローラからではなく、指定された場所からデバイスにダウンロードされます

ステップ 5 （任意）プロジェクト名を入力し、プロジェクトにデバイスを追加します。選択したプロジェクトにデバイスが追加されます。

ステップ 6 [Device Certificate] チェックボックスをオンにして、デバイスにデバイス証明書を適用します。Cisco ネットワーク プラグ アンド プレイによって、PKCS12 デバイス ID 証明書が自動的に生成されて展開されます。この設定は、アクセス ポイントには必要ありません。

ステップ 7 設定クレデンシャルを追加するには、クレデンシャル設定（プラス記号 [+]）ボタンをクリックして、必要な情報を指定します（デバイスでの AAA の設定, （23 ページ）を参照）。

ステップ 8 スタック スイッチの設定を有効にするには、プラス記号 [+] ボタンをクリックして、次の情報を指定します。

- License：ドロップダウン リストからライセンスを選択して、選択したライセンスをスタックのすべてのメンバーが確実に持てるようにします。
- Accept EULA：[Accept EULA] チェックボックスをオンにします。

ステップ 9 [Claim] をクリックしてデバイスを要求します。

ステップ 10 誤って追加したデバイスを削除するには、[Delete] をクリックします。これによりデバイスは工場出荷時の状態にリセットされ、再び追加できるようになります。

未請求デバイスの無視

デバイスを請求しない場合、無視ステータスにデバイスを移動できます。後でデバイスを再請求する場合は、デバイスを未請求デバイス リストに戻して請求できます。未請求デバイスを無視するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Devices] を選択します。

ステップ 2 デバイスを無視するには、リストからデバイスを選択し、[Ignore] をクリックします。
デバイスは [Ignored] ページに移動します。

ステップ 3 デバイスを未請求デバイス リストに戻す場合は、[Ignored] ページでデバイスを選択し、[Unignore] をクリックします。

シスコ デバイスのイメージ ファイルのアップロード

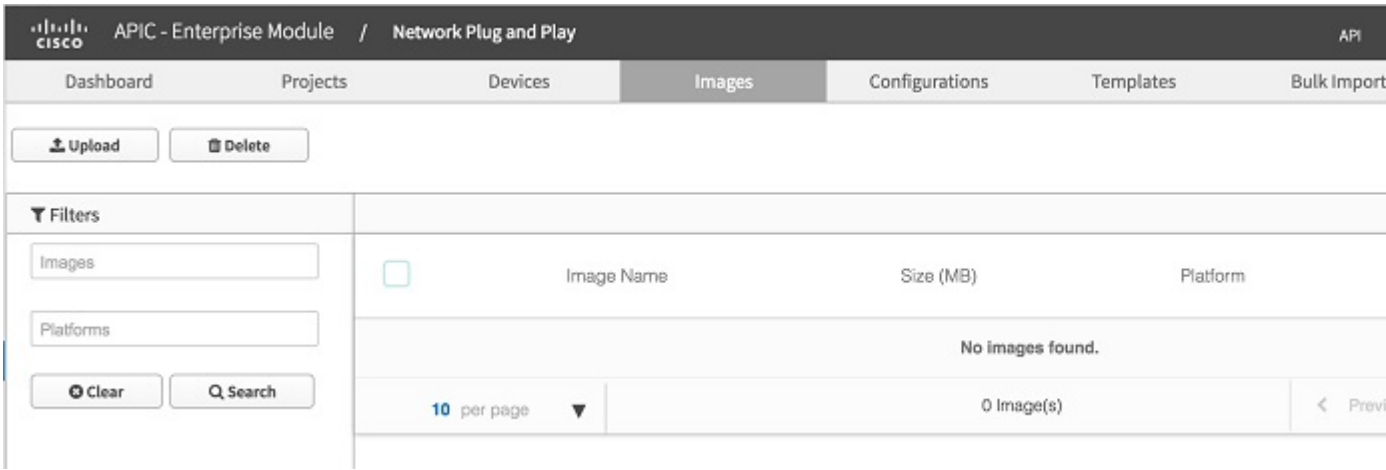
このオプションでは、ローカル マシンからシスコ デバイスのイメージ ファイルをアップロードできます。.tar、.bin、および.T 形式がサポートされています（図 4 を参照）。シスコ デバイスのイメージ ファイルをアップロードするには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Images] を選択します。

ステップ 2 [Upload] をクリックし、シスコ デバイスのイメージ ファイルを保存した場所を参照します。シスコ デバイスのイメージ ファイルを選択し、[Open] をクリックしてファイルをアップロードします。この画面にシスコ デバイスのイメージ ファイルをドラッグ アンド ドロップすることもできます。

ステップ 3 リストからイメージ ファイルを削除するには、ファイルを選択し、[Delete] をクリックします。

図 *4*：イメージ



（注） 同時進行する複数のイメージ ファイル アップロードを開始してネットワーク エラーが発生した場合は、ネットワークの輻輳またはパラレル アップロードが多すぎることが原因である可能性があります。この場合、一度に 1 つのイメージ ファイルをアップロードします。

デバイスへのデフォルト イメージの関連付け

Cisco ネットワーク プラグ アンド プレイでは、一連のプラットフォームにデフォルトのイメージとして、シスコ デバイスのイメージを関連付けることができます。一連のプラットフォームにデフォルトイメージとしてシスコデバイスのイメージを設定する場合、イメージはデバイスに自動

的に関連付けられます。このオプションを使用する場合、プロジェクトにデバイスを追加するときにプラットフォームにイメージを手動で割り当てる必要はありません。

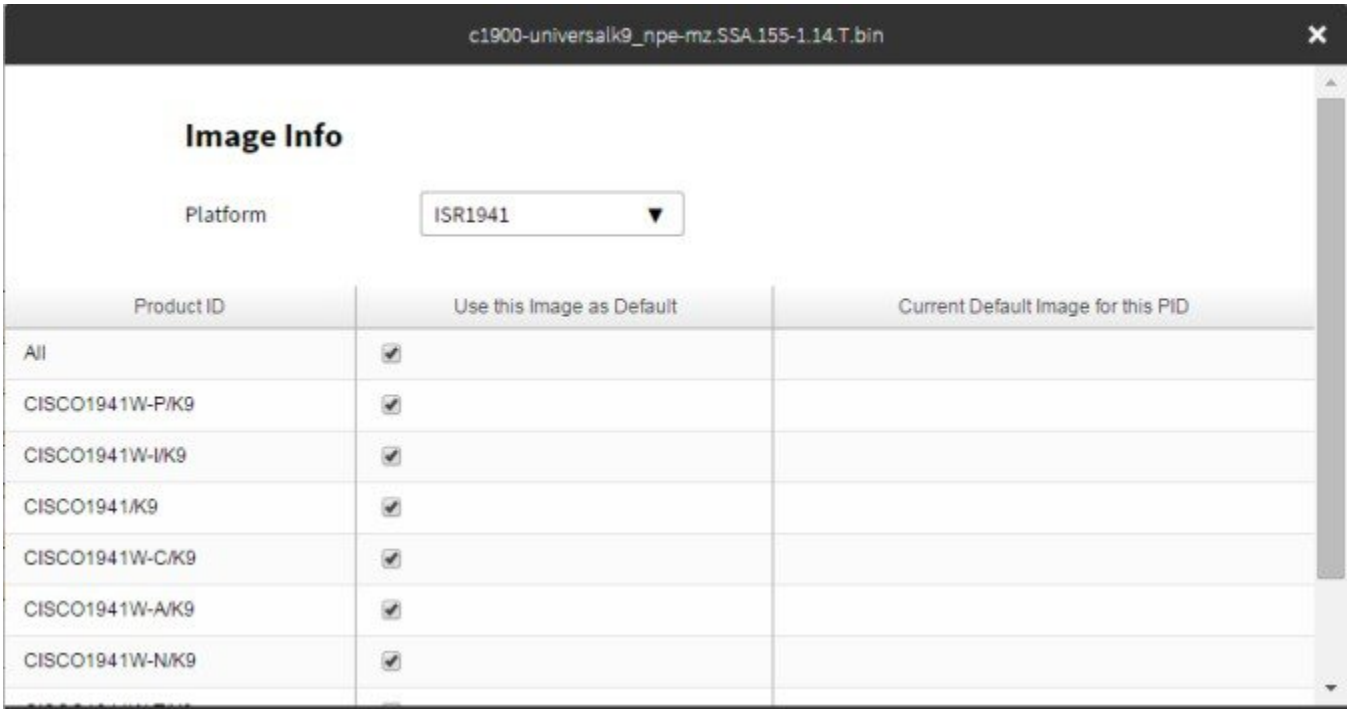
デフォルトのイメージとして Cisco IOS イメージを関連付けるには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Images] を選択します。

ステップ 2 [Images] リンクをクリックし、ドロップダウンリストから [Platform] を選択します。

ステップ 3 製品 ID をリストから選択し、[Use this image as Default Image] チェックボックスをオンにして、プラットフォームにイメージを関連付けます。
シスコ デバイスのイメージを特定のプラットフォーム、または同じプラットフォーム内の複数の製品 ID にデフォルト イメージとして関連付けることができます（図 5 を参照）。

図 *5*：イメージ情報



ステップ 4 プラットフォームでデフォルトイメージの設定を変更できます。デフォルト設定を変更するには、ステップ 1 からステップ 3 を繰り返します。

ステップ 5 [Yes] をクリックして変更を保存します。

コンフィギュレーション ファイルのアップロード

このオプションでは、ローカルマシンからコンフィギュレーションファイルをアップロードできます。テキスト形式がサポートされています。アクセス ポイント デバイスについては、*.json 拡張子を持つ JSON 形式のファイルがサポートされています。コンフィギュレーション ファイルをアップロードするには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Configurations] を選択します。

ステップ 2 [Upload] をクリックし、コンフィギュレーション ファイルを保存した場所を参照します。コンフィギュレーション ファイルを選択し、[Open] をクリックしてファイルをアップロードします。

ステップ 3 アップロードしたコンフィギュレーションファイルの内容を確認するには、コンフィギュレーションファイルの名前をクリックします。これにより、選択したコンフィギュレーションファイルの内容が表示されます。

ステップ 4 デバイスで使用されるコンフィギュレーション ファイルは削除できません。リストからコンフィギュレーション ファイルを削除するには、コンフィギュレーション ファイルを選択し、[Delete] をクリックします。

テンプレートのアップロード

このオプションでは、ローカル マシンから設定テンプレートをアップロードできます。テンプレートをアップロードするには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Templates] を選択します。

ステップ 2 [Upload] をクリックし、テンプレートを保存した場所を参照します。テンプレートを選択し、[Open] をクリックしてテンプレートをアップロードします。
テンプレートを使用する場合、デフォルト値を選択するか、指定したデバイスにカスタマイズされた値を指定できます。

ステップ 3 指定したデバイスにカスタマイズされた値を指定するには、テンプレートをクリックし、テンプレートのエディタに値を入力します。

ステップ 4 アップロードしたテンプレートの内容を確認するには、テンプレートの名前をクリックします。これにより、選択したテンプレート ファイルの内容が表示されます。

ステップ 5 デバイスで使用されているテンプレートは削除できません。リストからテンプレートを削除するには、テンプレートを選択し、[Delete] をクリックします。

プロジェクトおよびデバイスの一括インポート

一括インポート機能を使用して、プロジェクトおよびデバイス属性を含む CSV ファイルをインポートできます（図 6 を参照）。プロジェクトおよびプロビジョニングされたデバイスの一括インポートを実行するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Bulk Import] を選択します。

ステップ 2 [Sample] をクリックしてサンプルファイルをダウンロードし、プロジェクトおよびプロビジョニングされたデバイスの情報を追加します。

ステップ 3 [Import] をクリックして参照し、適切なファイルに移動します。

ステップ 4 ファイルを選択し、[Open] をクリックして CSV ファイルをインポートします。

ステップ 5 デバイス情報をエクスポートするには、[Export] をクリックします。デバイス情報が CSV 形式でエクスポートされます。デバイス ステータスを分析するには、この情報を使用します。

図 *6*：一括インポート

注：未請求リストにすでにあるデバイスを一括インポートすると、デバイスは請求され、指定されたプロジェクトに移動します。

シスコ スマート アカウントの設定

シスコ スマート アカウント機能により、APIC-EM コントローラ内のオンプレミス型シスコ プラグ アンド プレイ サーバと、スマート アカウントが有効な PnP Connect を統合して、デバイスのプロビジョニングを自動化できます。

シスコ スマート アカウントを使用することで、デフォルトのコントローラ プロファイルを作成できます。すべてのリダイレクション サービスに関する Cisco PnP Connect のデフォルト コントローラとして、APIC-EM コントローラのインスタンスを登録します。また、Cisco PnP Connect からこのオンプレミス コントローラにデバイス インベントリを同期し、導入を自動化します。組織にスマート アカウントがない場合、次のリンクから新しいスマート アカウントを要求できます。

シスコ スマート アカウントを登録するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Settings] > [Smart Account Settings] の順に選択します。

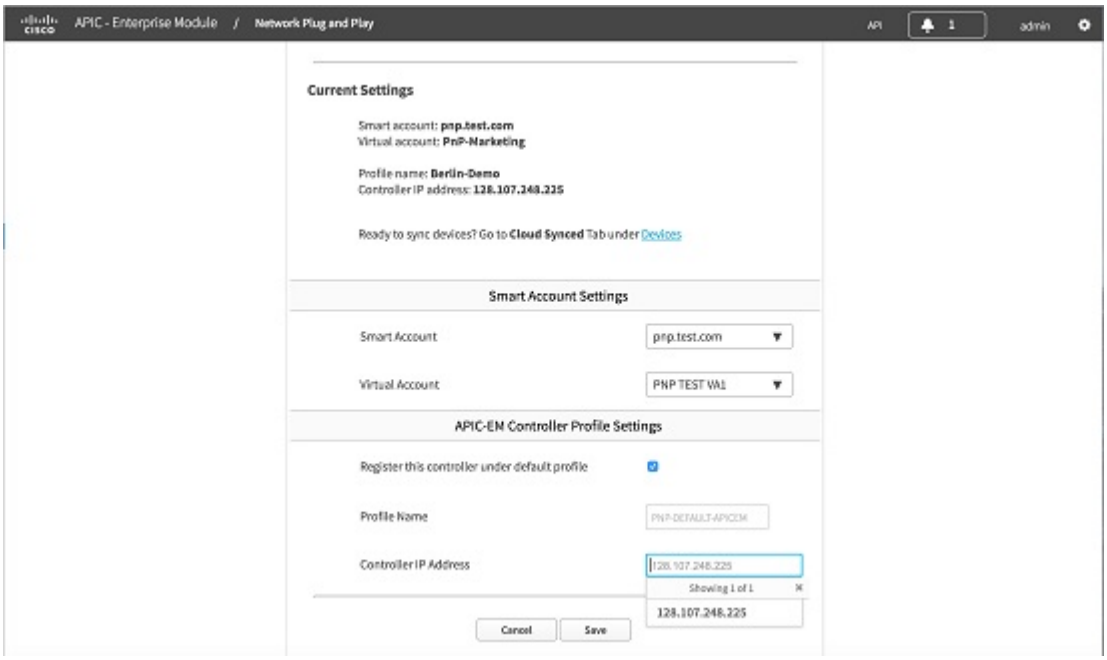
ステップ 2 ユーザ名とパスワードを入力して、[Authenticate] をクリックします。

ステップ 3 [Smart Account Settings] セクションで、ドロップダウン リストからスマート アカウントとバーチャル アカウントの名前を選択します。
そのスマート アカウントに複数のバーチャル アカウントがある場合、バーチャル アカウントのリストから使用するものを選択します。

ステップ 4 [APIC-EM Controller Profile Settings] セクションで、[Register this controller under default profile] チェックボックスをオンにします。

ステップ 5 [Controller IP Address] をドロップダウン リストから選択し、[Save] をクリックして情報を保存し、スマート アカウント ポータルに APIC-EM コントローラのプロファイルを登録します。

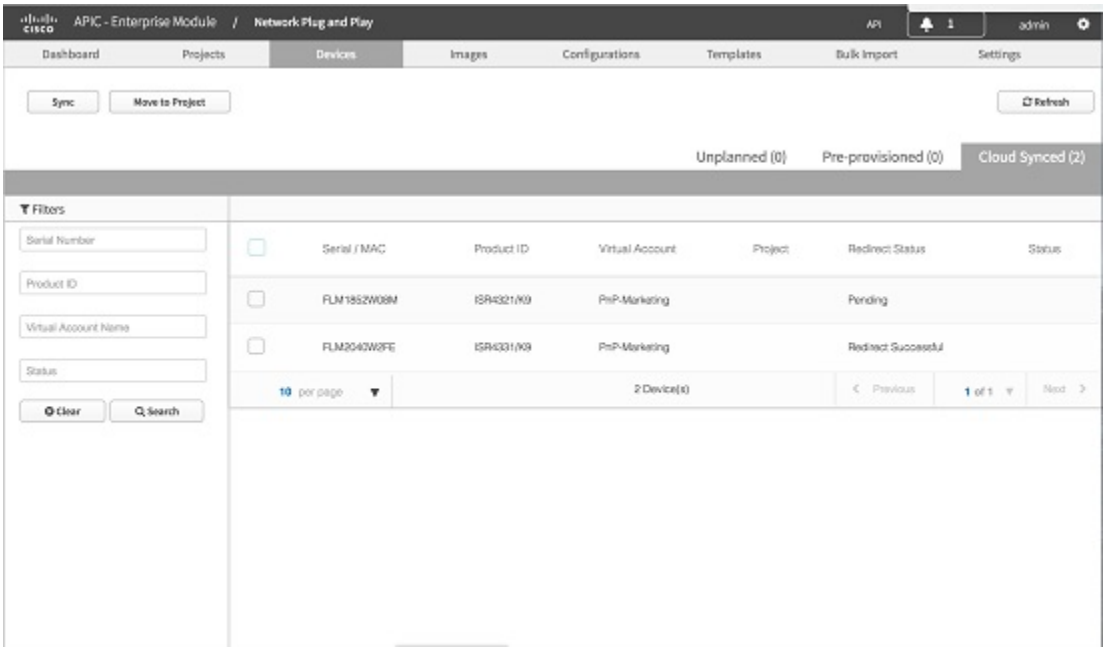
図 7: スマート アカウントの設定



ステップ 6 スマート アカウント ポータルに登録されたデバイスを同期して、シスコ プラグ アンド プレイ アプリケーションにダウンロードするには、[Devices] > [Cloud Synced] タブに移動します。[Sync] ボタンをクリック

し、スマート アカウントからデバイスのリストを取得します。スマート アカウント ポータルに登録されたデバイスのリストが表示されます。

図 *8*：クラウドからのデバイスの同期



ステップ 7 デバイスをプロビジョニングするには、デバイスをリストから選択し、[Projects] に移動します。

イメージ プロビジョニングのタイムアウトの設定

イメージ プロビジョニングのタイムアウト制限を設定すると、タイムアウトを超えたときにユーザ セッションが自動的に終了します。この設定はデフォルトで有効になっており、40 分に設定されています。

イメージ プロビジョニングのタイムアウトを設定するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Settings] > [Image Provisioning] の順に選択します。

ステップ 2 [Image Provisioning] ページで、ドロップダウン リストからタイムアウト制限を選択します。

ステップ 3 [Save] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

ステップ 4 デフォルトのタイムアウト設定にリセットするには、[Revert to Default] をクリックします。

設定プロビジョニングのタイムアウトの設定

設定プロビジョニングのタイムアウト制限を設定すると、タイムアウトを超えたときにユーザ セッションが自動的に終了します。この設定はデフォルトで有効になっており、40 分に設定されています。

設定プロビジョニングのタイムアウトを設定するには、次の手順を実行します。

ステップ 1 [Network Plug and Play] > [Settings] > [Config Provisioning] の順に選択します。

ステップ 2 [Config Provisioning] ページで、ドロップダウン リストからタイムアウト制限を選択します。

ステップ 3 [Save] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

ステップ 4 デフォルトのタイムアウト設定にリセットするには、[Revert to Default] をクリックします。

セキュリティのワークフロー

このセクションでは、PnP エージェント サーバ通信をさまざまなシナリオで保護するために使用する方法について説明します。PnP エージェントによって提供される、検出プロセスの完了後クライアント/サーバ通信を保護するために PnP サーバで使用できる方法について説明します。

Cisco APIC-EM 証明書の表示

Cisco APIC-EM 証明書を表示するには、次の手順を実行します。

ステップ 1 [Home] ページで、画面の右上隅にある [Settings] アイコンをクリックします。

ステップ 2 [Network Settings] ナビゲーション ウィンドウで、[Certificate] をクリックして現在の証明書を表示します。

ステップ 3 [Certificate] ページで、現在の証明書データを表示します。
表示された現在の証明書データは、コントローラの自己署名証明書です。自己署名証明書の有効期限は、協定世界時（UTC）値として表示されます。証明書の有効期限の 2 か月前にシステム通知が表示されます。

Cisco APIC-EM でのサードパーティ CA 署名付き証明書の配置

プロキシ証明書をインストールすることもできます。これは、APIC-EM コントローラと直接通信できないデバイスが対象です。Cisco APIC-EM で CA 署名付き証明書を配置するには、次の手順を実行します。

ステップ 1 [Home] ページで、画面の右上隅にある [Settings] アイコンをクリックします。

ステップ 2 [Network Settings] ナビゲーション ウィンドウで、[Certificate] をクリックして現在の証明書を表示します。ネットワーク設定ペインにアクセスするには、管理者ロールが必要です。

ステップ 3 [Certificate] ページで、[Replace Certificate] をクリックします。

ステップ 4 [Certificate] ページで、証明書のファイル形式タイプ [PEM] または [PKCS12] を選択します。

ステップ 5 [PEM] を選択した場合、次の手順を実行します。

- [Drag n' Drop a File Here] エリアにファイルをドラッグ アンド ドロップして、PEM ファイルをインポートします。
  ファイルには有効な PEM 形式の拡張子（.pem、.cert、.crt）が必要です。証明書の最大ファイル サイズは 10 KB です。
- [Drag n' Drop a File Here] エリアにファイルをドラッグ アンド ドロップして、秘密キーをインポートします。秘密キーの [Encrypted] ドロップダウン メニューから暗号化オプションを選択し、パスフレーズを入力します。
  ファイルには有効な秘密キー形式の拡張子（.pem、.cert）が必要です。

ステップ 6 [PKCS] を選択した場合、次の手順を実行します。

- [Drag n' Drop a File Here] エリアにファイルをドラッグ アンド ドロップして、PKCS ファイルをインポートします。
  ファイルには有効な PKCS 形式の拡張子（.pfx、.p12）が必要です。
- 秘密キーについては、秘密キーの [Encrypted] ドロップダウン メニューから暗号化オプションを選択し、パスフレーズを入力します。

ステップ 7 [Upload/Activate] をクリックして、現在の証明書を置換します。

ステップ 8 [Certificate] ページに戻り、更新された証明書データを表示します。
[Certificate] ページに表示される情報には、新しい証明書の名前、発行元、および認証局が反映されます。

trustpool バンドルの更新

Cisco APIC-EM で PKI trustpool バンドルをインポートし、更新できます。この PKI trustpool バンドルは、サポートされるシスコ ネットワーク デバイスで、Cisco APIC-EM とそのアプリケーショ

ン（Cisco ネットワーク プラグ アンド プレイなど）を認証するために使用されます。trustpool バンドルを更新するには、次の手順を実行します。

ステップ 1 [Home] ページで、画面の右上隅にある [Settings] アイコンをクリックします。

ステップ 2 [Network Settings] ナビゲーション ウィンドウで、[Trustpool] をクリックして trustpool バンドルを表示します。

ステップ 3 [Update] をクリックして、trustpool バンドルを更新します。
PKI trustpool バンドルによって、コントローラの既存の trustpool バンドルは上書きされます。

インストーラ ロールの作成

Cisco APIC-EM では、ロールベース アクセス コントロール（RBAC）がサポートされています。RBAC は、ユーザ ロールに基づいてユーザのコントローラ アクセスを制限または承認する方法です。ロールは、コントローラにおけるユーザの権限を定義します。ユーザを作成し、ユーザに適切なロールを割り当てることができます。ROLE_ADMIN ロールでは、インストーラで Cisco プラグ アンドプレイ モバイル アプリを使用して APIC-EM コントローラにアクセスし、デバイスの展開をトリガーし、デバイスのステータスを表示できます。ユーザ ロールの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。インストーラ ロールを作成するには、次の手順を実行します。

ステップ 1 [Home] ページで、画面の右上隅にある [Settings] アイコンをクリックします。

ステップ 2 [Settings] ナビゲーション ウィンドウで、[User Settings] > [Internal Users] > [Create User] をクリックします。

ステップ 3 [User] ダイアログボックスで、次のフィールドに値を入力します。

- Username：新しいユーザのユーザ名を入力します。
- Password：新しいユーザのパスワードを入力します。
- Confirm Password：確認のためにパスワードを再入力します。
- Scope：範囲はデフォルトで [ALL] に設定されます。
- Role：新規ユーザに対して ROLE_INSTALLER ロールを選択します。

ステップ 4 [Save] をクリックして、ROLE_INSTALLER ロールを持つ新規ユーザを作成します。

デバイスでの AAA の設定

Cisco APIC-EM は、AAA サーバからのユーザの外部認証および承認をサポートしています。外部認証と承認は、事前設定されたAAAサーバにすでに存在するユーザ名、パスワード、および属性に基づいています。外部認証および承認を使用して、AAAサーバにすでに存在するクレデンシャルを使用してコントローラにログインします。RADIUS プロトコルは、AAA サーバにコントローラを接続するために使用されます。ユーザ ロールの詳細については、『Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide, Release 1.3.x』を参照してください。設定クレデンシャルを追加するには、次の手順を実行します。

ステップ 1 既存デバイスの設定クレデンシャルをプロジェクトから追加するには、デバイスの横にあるボックスを選択して [Edit] をクリックします。[Edit Device] ダイアログボックスで、次を指定します。

- Username：設定用のユーザ名を入力します。
- Password：設定用のパスワードを入力します。
- Confirm Password：確認のためにパスワードを再入力します。

ステップ 2 未計画のデバイスの設定クレデンシャルを追加するには、[Network Plug and Play] > [Devices] を選択します。

ステップ 3 リストからデバイスを選択して、[Claim] をクリックします。[Claim Device] ダイアログボックスが表示されます。

ステップ 4 クレデンシャル設定（プラス記号 [+]）ボタンをクリックし、次を指定します。

- Username：設定用のユーザ名を入力します。
- Password：設定用のパスワードを入力します。
- Confirm Password：確認のためにパスワードを再入力します。

ステップ 5 [Claim] をクリックしてデバイスを要求します。

Cisco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

Cisco ネットワーク プラグ アンド プレイは、デバイスのモニタリングとトラブルシューティングのために次のトラブルシューティング情報を提供します。

Cisco ネットワーク プラグ アンド プレイ ログの収集

Cisco ネットワーク プラグ アンド プレイに関するログを収集するには、次の手順を実行します。

ステップ 1 [Home] ページで、画面の右上隅にある [Settings] アイコンをクリックします。

ステップ 2 [Settings] ナビゲーション ウィンドウで、[System Administration] > [Services] をクリックします。

ステップ 3 [Services] ダイアログボックスで、[Services] リストから PnP サービスを選択し、フィールドに適切な値を入力します。

ステップ 4 [tasks] をクリックして、タスクを表示します。

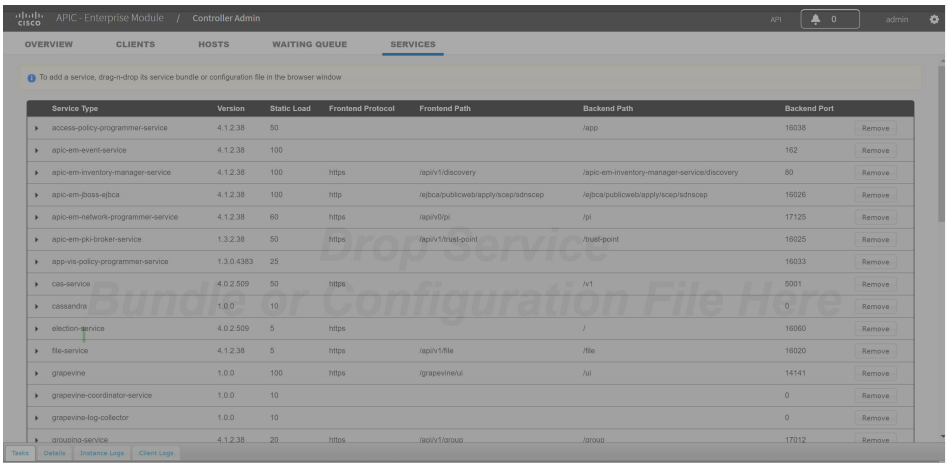
ステップ 5 [Details] をクリックして、ログの詳細を表示します。

ステップ 6 [Instance Logs] をクリックして、インスタンス ログを表示します。

ステップ 7 [Client Logs] をクリックして、クライアント ログを表示します。

ステップ 8 このログファイルを使用して Cisco ネットワーク プラグ アンド プレイ イベントを分析し、適切な処置を実行できます（図 9 を参照）。

図 *9*：*Cisco* ネットワーク プラグ アンド プレイ ログ



事前プロビジョニングされたプロジェクトのステータスの確認

事前プロビジョニングされたプロジェクトのステータスを確認するには、次の手順を実行します。

ステップ 1 ダッシュボードから [Network Plug and Play] を選択し、プロジェクト円グラフの横にある事前プロビジョニング済みリンクをクリックします。

ステップ 2 [Projects] カラムでプロジェクト名をクリックして、そのプロジェクトのデバイスのステータスを確認します。