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。

この章は、次の項で構成されています。

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、エンタープライズ ネットワーク カスタマーが新しいブランチまたはキャンパスの展開を迅速化するため、または既存のネットワークへの更新をプロビジョニングするための、シンプルでセキュアな統合されたオファリングを提供します。 このソリューションは、Cisco ルータ、スイッチ、およびワイヤレス デバイスで構成されるエンタープライズ ネットワークをプロビジョニングするための統合されたアプローチにほ

ぼゼロ タッチ導入のエクスペリエンスを提供します。 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 サイ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。 大規模なサイ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サイトを事前プロビジョニングし、サイ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 プレイの組織

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、同じ一般組織に従います。

表 *1*：*Cisco* ネットワーク プラグ アンド プレイの組織

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、シスコのネットワーク プラグ アンド プレイ ダッシュボード，（3 ページ）を参照してください。
プロジェクト（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。 [デバイスの追加（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、サイトの事前プロビジョニング ワークフローを参照してください。

未計画のデバイス（Unplanned 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（Images）	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。 詳細については、デバイスへのデフォルトイメージの関連付け，（13 ページ）を参照してください。
コンフィギュレーション（Configurations）	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。
一括インポート（Bulk Import）	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 [一括インポート（Bulk Import）] セクションの [サンプル（Sample）] ボタンをクリックします。
設定	[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	[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，（20 ページ）を参照してください。

シスコのネットワーク プラグ アンド プレイ ダッシュボード

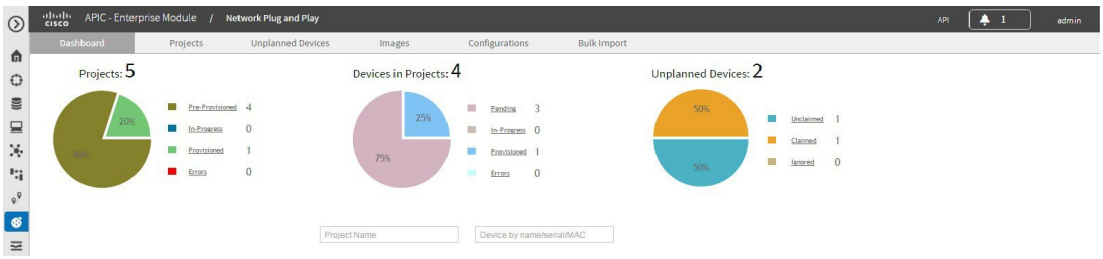
シスコのネットワーク プラグアンドプレイ ダッシュボードには、ネットワークの最も重要なデータが一目でわかるように表示されます。 ダッシュボードのグラフ表示には、事前プロビジョニング、進行中、プロビジョニング、およびプロジェクトのリストがエラー情報とともに表示されます。 また、要求元不明デバイス、要求されたデバイス、および無視されたデバイスも表示されま

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）。

[ダッシュボード（Dashboard）] ページには、次のオプションがあります。

- プロジェクトの検索（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。
- デバイスの検索（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*：シスコのネットワーク 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、PKI 証明書、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。 これにより、サイトが完全に機能するためにかかる時間が短縮され迅速化されます。
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, （4 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, （7 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、PKI 証明書、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一意のエンティティです。 異なる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、固有のプロジェクト ID を持つ新しいプロジェクトに既存のプロジェクトを複製します。 その後、必要に応じて [プロジェクト（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 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [プロジェクト（Projects）] を選択します。

ステップ 2 新しいプロジェクトの名前を入力します。

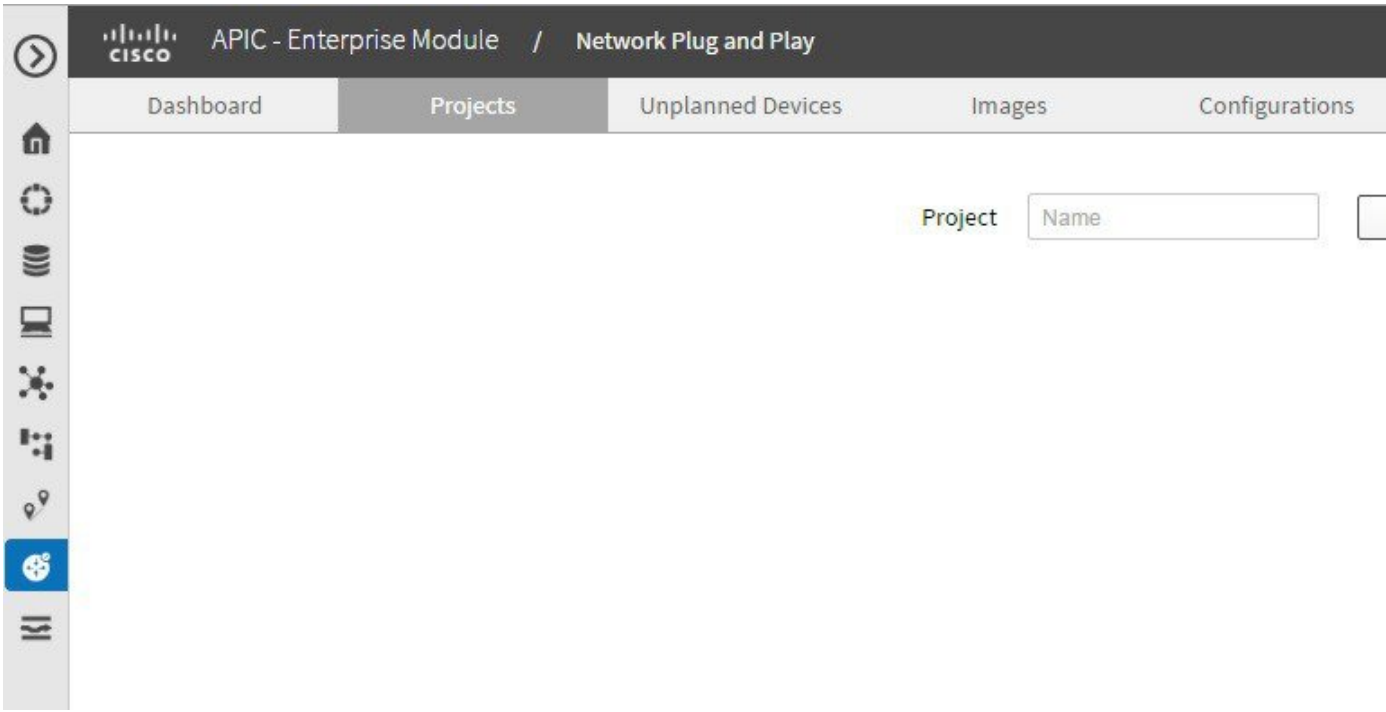
ステップ 3 [作成（Create）] をクリックして新しいプロジェクトを作成します。

ステップ 4 プロジェクトを作成した後、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 ファイルをデバイス テーブルから選択するか、[外部 TFTP サーバからコンフィギュレーション/イメージ ファイルを導入（Deploy configuration/ image files from an external TFTP server）] オプションを使用してデバイスを設定します。

プロジェクトを作成した後、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 ファイルをデバイス テーブルから選択するか、[外部 TFTP サーバからコンフィギュレーション/イメージ ファイルを導入（Deploy configuration/ image files from an external TFTP server）] オプションを使用してデバイスを設定します。 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 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（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、デバイス テーブルで使用可能な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。

ステップ 5 [外部 TFTP サーバからコンフィギュレーション/イメージ ファイルを導入（Deploy configuration or Image files from an external TFTP Sever）] チェックボックスを選択し、TFTP サーバのホスト名または IP アドレス、および TFTP サーバのパスを入力します。

ステップ 6 [メモ（Notes）] をクリックしてメモを追加するか、参照ドキュメントをドラッグアンドドロップします。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されます。

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 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [プロジェクト（Projects）] を選択します。

ステップ 2 次の情報を入力します。

- デバイス名（Device Name）：デバイス名（サイトごとに一意）
- 製品 ID（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。
- シリアル番号（Serial Number）：デバイスのシリアル番号（または）
- MAC アドレス（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 3 [デバイスの追加（Add Device）] をクリックしてデバイスを追加します。

ステップ 4 デバイスに適用するコンフィギュレーション ファイルを選択します。

注：コンフィギュレーション ファイルはテキスト形式にする必要があります。 ルータとスイッチのコンフィギュレーション ファイルは、*.txt 形式にする必要があります。 アクセス ポイント デバイスの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。

a) 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を適用するには、[設定（Configuration）] フィールドをクリックし、リストからコンフィギュレーション ファイルを選択します。

b) デバイスに新しい設定を適用するには、サーバにコンフィギュレーションファイルをアップロードし、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必要があります。 コンフィギュレーション ファイルのアップロード, （14 ページ）を参照してください。

c) （オプション）デバイスに既存のブートストラップ設定を適用するには、リストからコンフィギュレーション ファイルを選択します。 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して、WAN デバイスでブートストラップ設定を展開できます。 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 5 デバイスに適用するシスコ デバイスのイメージ ファイルを選択します。

a) 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。

b) 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, （12 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 [デバイス証明書（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 7 [SUDI が必要（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 認証をサポートしないデバイスに対してこのボックスをオンにした場合、認証およびプロビジョニングは認証エラーで失敗し、デバイスを追加するにはボックスをオフにする必要があります。

デバイスの展開

プロジェクトを作成した後、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展開し、デバイスにブートストラップ設定を配信します。

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。

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 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [プロジェクト（Projects）] を選択します。

ステップ 2 プロジェクトの名前を入力するか、ドロップダウンリストからプロジェクトを選択します。

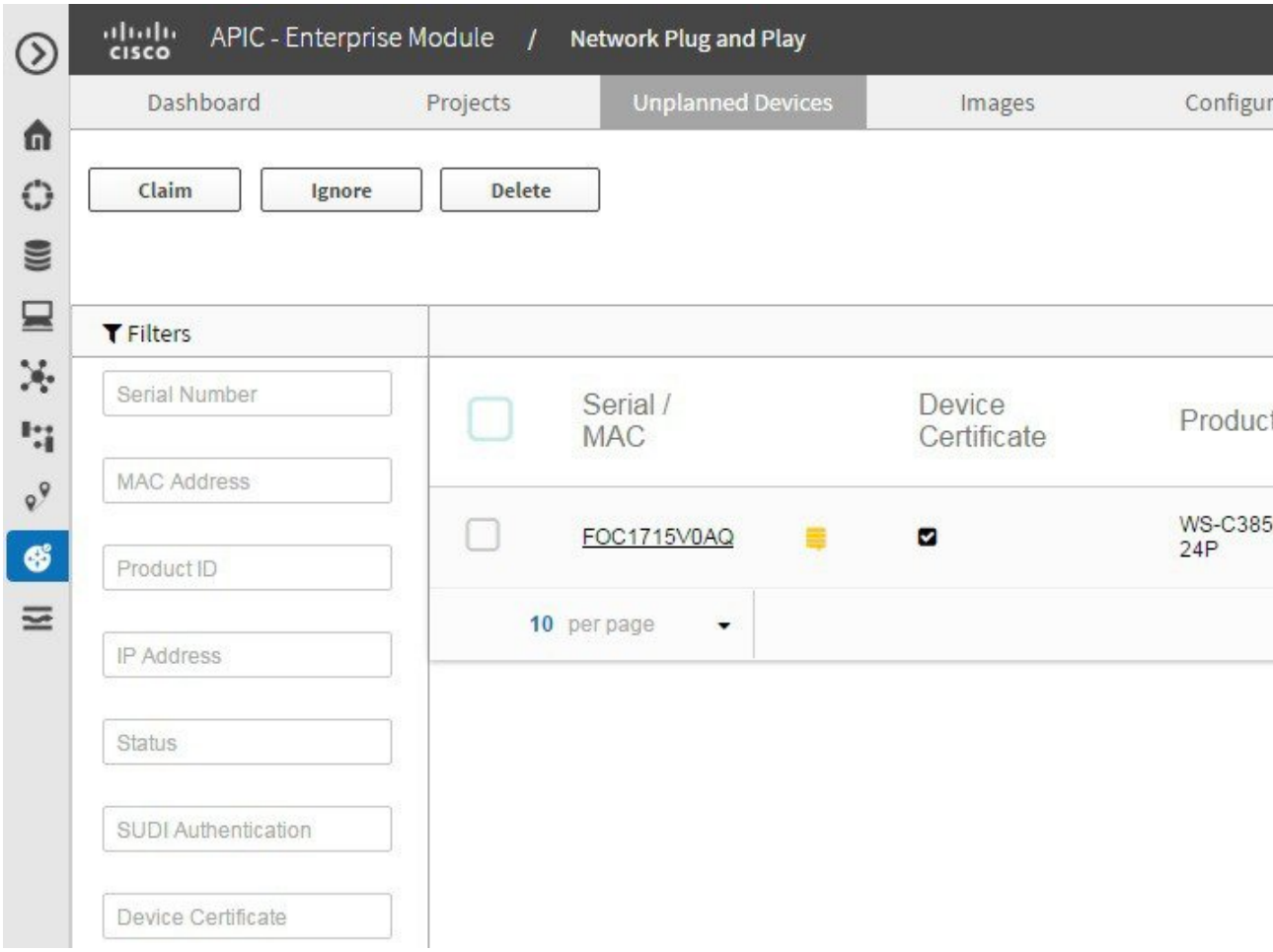
ステップ 3 [複製（Clone）] をクリックして、選択したプロジェクトを複製します。 プロジェクトを複製した後、複製したプロジェクトのデバイスごとにシリアル番号/MAC アドレス、設定、イメージ、およびその他の設定を行う必要があります。

未計画の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サイトの場合、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。 [未計画のデ

バイス（Unplanned Devices）]ページには、要求元不明デバイス、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

デバイスが Cisco APIC-EM によってプロビジョニングされる前に Call Home Agent 機能を使用してサーバに接続した場合、または Cisco APIC-EM が既存の設定に対してデバイスを照合できない場合、デバイスは未請求デバイス リストに追加されます。

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 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [未計画のデバイス（Unplanned 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、コンフィギュレーション ファイルおよびイメージ ファイルを関連付けます。

ステップ 3 リストから既存の設定を再利用するか、新しい設定をデバイスに適用できます。

注：コンフィギュレーション ファイルはテキスト形式にする必要があります。 ルータとスイッチのコンフィギュレーション ファイルは、*.txt 形式にする必要があります。 アクセス ポイント デバイスの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。

a) デバイスに既存の設定を適用するには、リストからコンフィギュレーション ファイルを選択します。

b) デバイスに新しい設定を適用するには、Cisco APIC-EM にコンフィギュレーション ファイルをアップロードし、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必要があります。 コンフィギュレーション ファイルのアップロード, （14 ページ）を参照してください。

c) （オプション）デバイスに既存のブートストラップ設定を適用するには、リストからコンフィギュレーション ファイルを選択します。 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して、WAN デバイスでブートストラップ設定を展開できます。

ステップ 4 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。

a) 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、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。

b) 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, （12 ページ）を参照してください。 この設定は、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。

a) プロジェクト名を設定し、プロジェクトにデバイスを追加します。

ステップ 5 [デバイス証明書（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 6 [要求（Claim）] をクリックして、デバイスを要求します。

ステップ 7 デバイスのシリアル番号をクリックしてデバイス情報を表示します。

要求されていないデバイスの無視

デバイスを要求しない場合、無視ステータスにデバイスを移動できます。 後でデバイスを再要求する場合は、デバイスを未請求デバイス リストに戻して要求できます。 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 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [未計画のデバイス（Unplanned 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、[無視（Ignore）] をクリックします。
デバイスは [無視済み（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、[無視済み（Ignored）] ページでデバイスを選択し、[無視の解除（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。

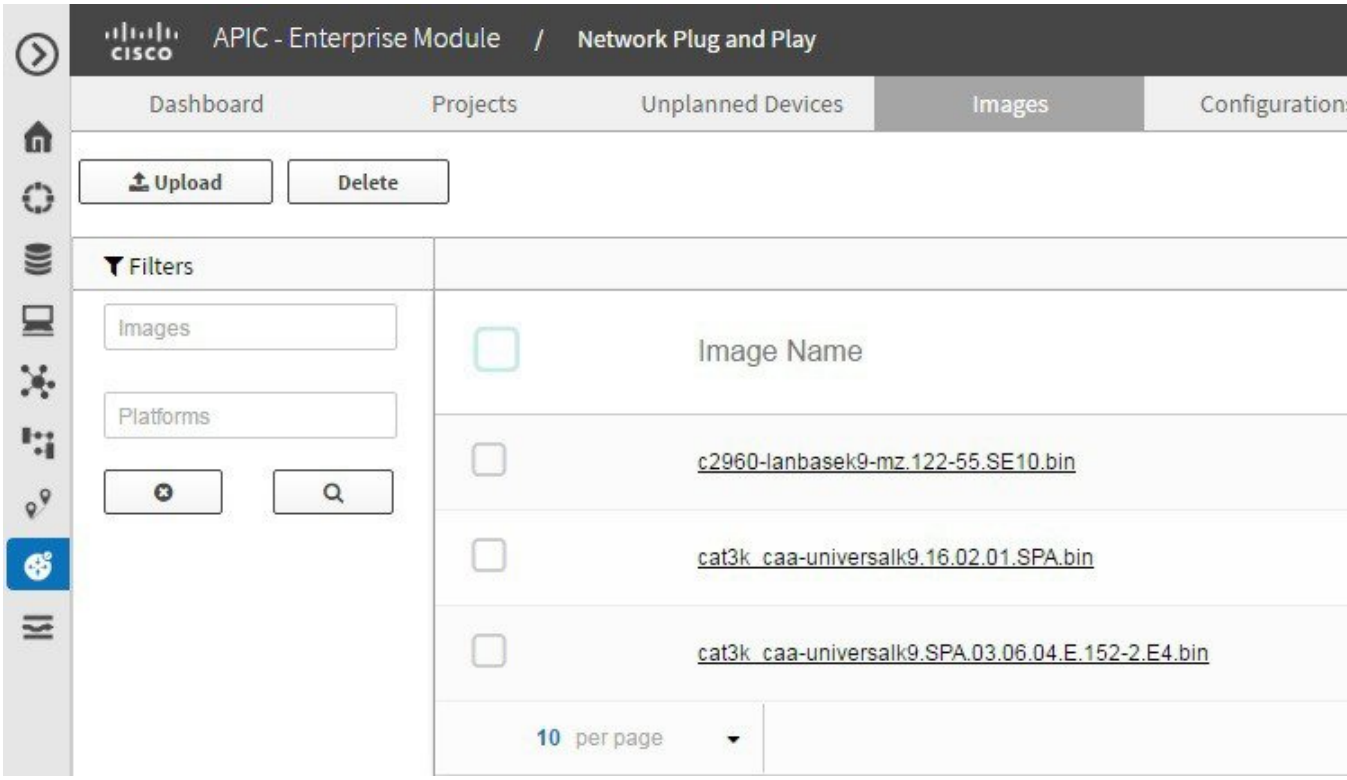
ステップ 1 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [イメージ（Images）] を選択します。

ステップ 2 [アップロード（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、[開く（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、[削除（Delete）] をクリックします。

図 *4*：イメージ（*Images*）



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。

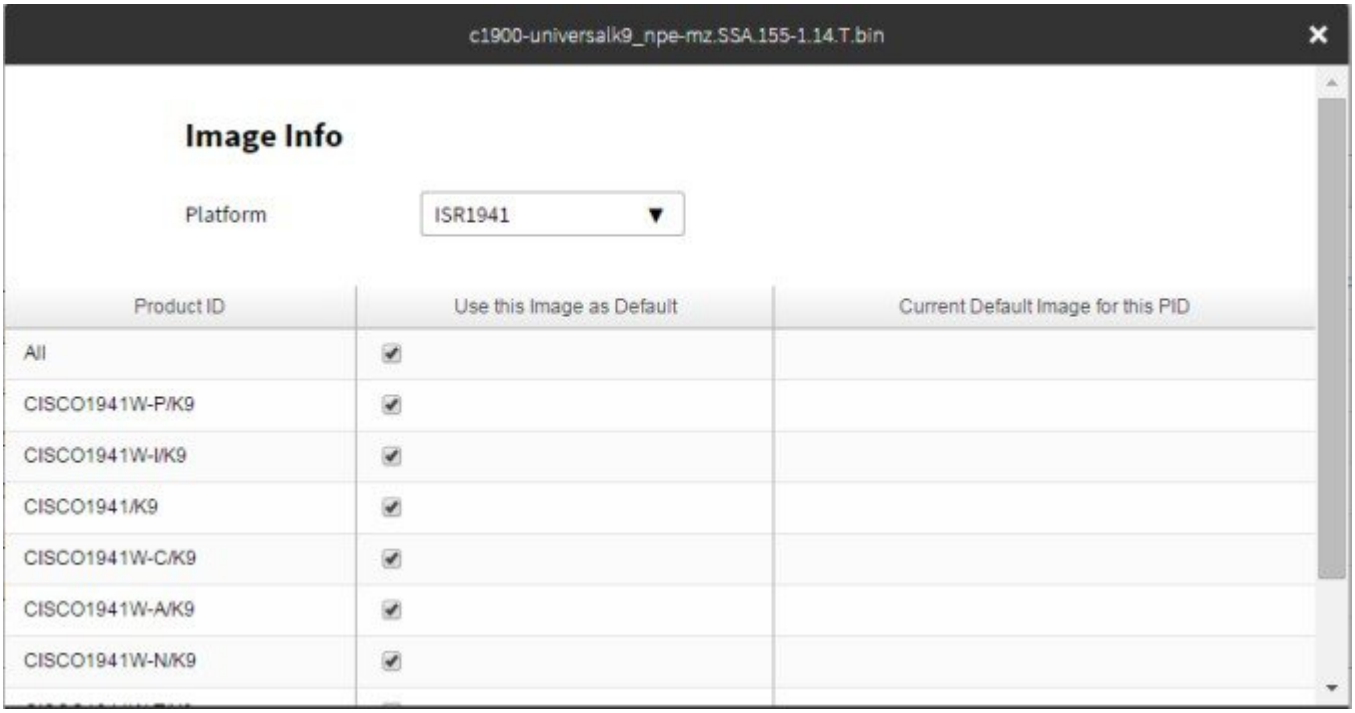
デフォルトのイメージとして Cisco IOS イメージを関連付けるには、次の手順を実行します。

ステップ 1 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [イメージ（Images）] を選択します。

ステップ 2 [イメージ（Images）] リンクをクリックし、ドロップダウンリストから [プラットフォーム（Platform）] を選択します。

ステップ 3 製品 ID をリストから選択し、[このイメージをデフォルト イメージとして使用する（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 [はい（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 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [設定（Configuration）] を選択します。

ステップ 2 [アップロード（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、[開く（Open）] をクリックしてファイルをアップロードします。この画面にコンフィギュレーション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 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てい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、[削除（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 [ネットワーク プラグ アンド プレイ（Network Plug and Play）] > [一括インポート（Bulk Import）] を選択します。

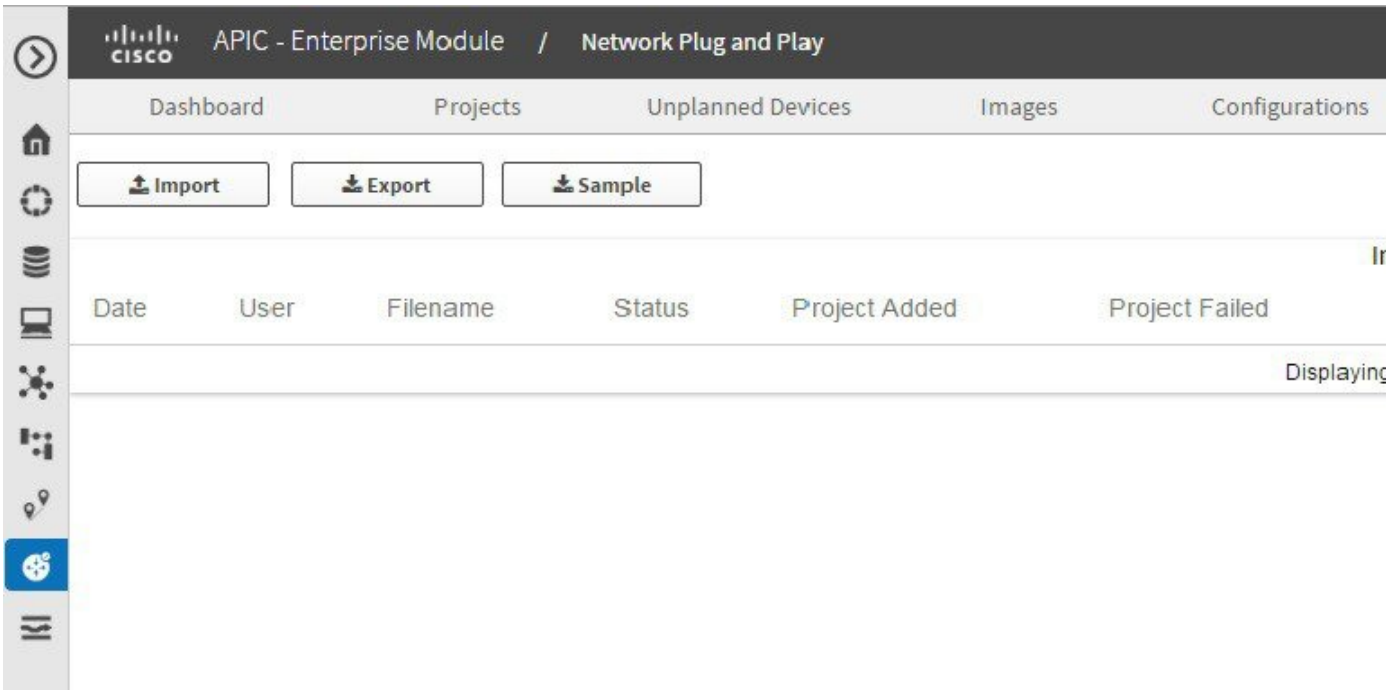
ステップ 2 [サンプル（Sample）] をクリックしてサンプル ファイルをダウンロードし、プロジェクトおよびプロビジョニングされたデバイスの情報を追加します。

ステップ 3 [インポート（Import）] をクリックし、該当するファイルを参照して移動します。

ステップ 4 ファイルを選択し、[開く（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、[エクスポート（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。 この情報を使用してデバイスのステータスを分析します。

図 *6*：一括インポート



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 [ホーム（Home）] ページで、画面の右上隅にある [設定（Settings）] アイコンをクリックします。

ステップ 2 [設定（Settings）] ナビゲーション ウィンドウで、[証明書（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 [証明書（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 [ホーム（Home）] ページで、画面の右上隅にある [設定（Settings）] アイコンをクリックします。

ステップ 2 [ネットワーク設定（Network Settings）] ナビゲーション ウィンドウで、[証明書（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 [証明書（Certificate）] ページで、[証明書の置換（Replace Certificate）] をクリックします。

ステップ 4 [証明書（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。

- [ここにファイルをドラッグアンドドロップ（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。

- [ここにファイルをドラッグアンドドロップ（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 [暗号化（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。

- [ここにファイルをドラッグアンドドロップ（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 [暗号化（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 [アップロード/有効化（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 [証明書（Certificate）] ページに戻り、更新された証明書データを表示します。
[証明書（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 [ホーム（Home）] ページで、画面の右上隅にある [設定（Settings）] アイコンをクリックします。

ステップ 2 [設定（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 [更新（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 バンドルが上書きされます。

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。 ロールでは、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 [ホーム（Home）] ページで、画面の右上隅にある [設定（Settings）] アイコンをクリックします。

ステップ 2 [設定（Settings）] ナビゲーション ウィンドウで、[ユーザ設定（User Settings）] > [ユーザ（User）] をクリックします。

ステップ 3 [ユーザ（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。

- ユーザ名（Username）：新しいユーザのユーザ名を入力します。
- パスワード（Password）：新しいユーザのパスワードを入力します。
- パスワードの確認（Confirm Password）：確認のためにパスワードを再入力します。
- 範囲（Scope）：範囲はデフォルトで [すべて（ALL）] に設定されます。
- ロール（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 [追加（Add）] 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。

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 プレイでは、デバイスを監視およびトラブルシューティングするための次のトラブルシューティング情報が提供されます。

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 [ホーム（Home）] ページで、画面の右上隅にある [設定（Settings）] アイコンをクリックします。

ステップ 2 [設定（Settings）] ナビゲーション ウィンドウで、[ログ（Logs）] をクリックします。

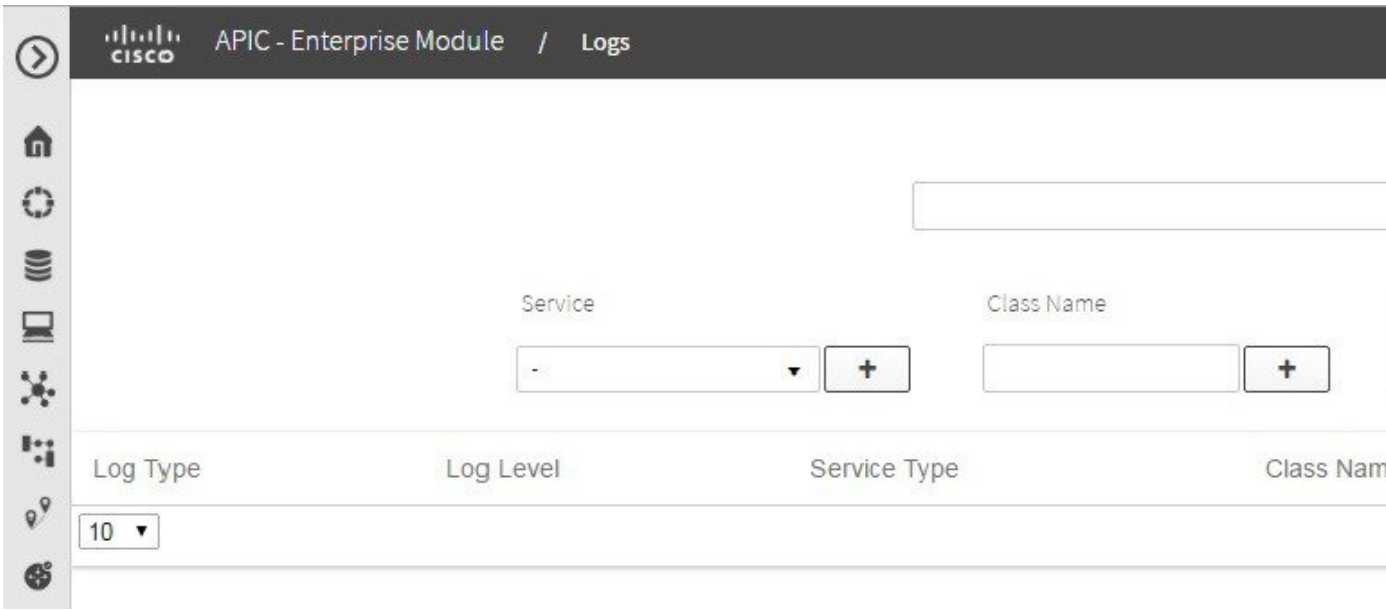
ステップ 3 [ログ（Logs）] ダイアログボックスで、[サービス（Services）] ドロップダウンリストから PnP サービスを選択します。

ステップ 4 プラス記号アイコンをクリックします。

ステップ 5 [検索（Search）] をクリックしてログを検索します。

ステップ 6 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 7 を参照）。

図 *7*：*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サイトのステータスの確認

事前プロビジョニングし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 [ネットワーク プラグ アンド プレイ（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 [プロジェクト（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。