ネットワーク プラグアンドプレイ

この章は、次の項で構成されています。

ネットワーク プラグ アンド プレイについて

[Network Plug and Play] は、ネットワーク プラグ アンド プレイ対応デバイスと連動するサービスで、ファームウェアと設定を集中管理し、新しいネットワークデバイスをゼロタッチ展開することができます。デバイスは、ネットワーク プラグアンドプレイ プロトコルを使用して直接展開できます。Dashboard に関連付けられているプローブによって検出された場合は、間接的に展開されます。

ネットワーク プラグアンドプレイ対応デバイスが設置されると、そのデバイスは、手動設定、DHCP、DNS、またはプラグ アンド プレイ接続サービスのいずれかを通じてネットワーク プラグ アンドプレイ サーバを識別します。次のセクションでは、Cisco Business ダッシュボードでのネットワーク プラグアンドプレイ サービスの設定について詳しく説明します。

ネットワーク要件

ネットワーク プラグ アンドプレイ デバイスは、次のいずれかの方法を使用して、ネットワーク プラグ アンド プレイ サーバーのアドレスを自動的に見つけます。アドレスが見つかるまで、またはすべての方法が失敗するまで、各方法が順番に試行されます。これらの方法は以下の順番で使用されます。

- [Manual configuration]：管理インターフェイスを使用して、ネットワーク プラグ アンド プレイ対応デバイスにサーバーのアドレスを手動で設定できます
- [DHCP]：サーバーのアドレスは、ベンダー固有の情報オプションでデバイスに提供できます

- [DNS]：DHCP によるベンダー固有の情報オプションが提供されていない場合、デバイスは既知のホスト名を使用して、サーバについて DNS ルックアップを実行します。
- [Plug and Play Connect Service]：他のどの方法も成功しない場合、最終的にデバイスはプラグアンドプレイ接続サービスへの接続を試みます。このサービスにより、デバイスはサーバーにリダイレクトされます。

デバイスは、サーバを識別すると、そのサーバに接続し、サーバの指定に従いファームウェアと設定を更新します。

証明書の要件

ネットワーク プラグアンドプレイ サーバへの接続を確立する場合、クライアントは、サーバによって提示された証明書が有効であり、信頼できることを確認します。証明書が受け入れられ、接続が続行されるには、証明書が次の条件を満たしている必要があります。

- 証明書は信頼された証明機関（CA）によって署名されているか、または証明書自体がクライアントによって信頼されている必要があります。DHCP から学習した TrustpoolBundleURL か、またはプラグアンドプレイ接続サービスからダウンロードされた証明書は、クライアントによって信頼されます。
- サーバ ID が手動設定、DHCP、またはプラグアンドプレイ接続を使用して検出され、それが IP アドレスである場合は、[Common Name] フィールドまたは [Subject-Alt-Name] フィールドにその IP アドレスが含まれている必要があります
- サーバ ID が手動設定、DHCP、またはプラグアンドプレイ 接続を使用して検出され、それがホスト名である場合は、[Common Name] フィールドまたは [Subject-Alt-Name] フィールドにそのホスト名が含まれている必要があります。
- DNS 検出を使用してサーバ ID が検出された場合は、[Common Name] フィールドまたは [Subject-Alt-Name] フィールドに既知のホスト名である pnpserver.<*local domain*> に対応する IP アドレスが含まれている必要があります。

（注） 古いネットワーク プラグアンドプレイ クライアントの実装によっては、証明書内のサーバ ID の存在を確認しません。

DHCP を使用したディスカバリの設定

デバイスは、DHCP を使用してサーバ アドレスを検出するために、「ciscopnp」という文字列を含むオプション 60 を使用した DHCP discover メッセージを送信します。DHCP サーバは、ベンダー固有の情報オプション（オプション 43）を含む応答を送信する必要があります。デバイスは、このオプションからサーバアドレスを取得し、そのアドレスを使用してサーバに接続します。ネットワーク プラグアンドプレイ サーバのアドレスを含むオプション 43 の文字列は、たとえば「5A1N;B2;K4;I172.19.45.222;J80」などです。

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 プレイの DHCP サブオプション、アクティブ操作、バージョン 1、デバッグ情報なしを示します。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
- K4：Cisco プラグ アンド プレイ エージェントとサーバ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
- Ixxx.xxx.xxx.xxx：サーバの IP アドレスまたはホスト名（大文字の i に続く部分）。この例では、IP アドレスは 172.19.45.222 です。
- Jxxxx：サーバに接続するために使用するポート番号。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。
- T*trustpoolBundleURL*：トラストプール バンドルの外部 URL を指定するオプション パラメータ（サーバ以外の場所からトラストプール バンドルを取得する場合）。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「Ttftp://10.30.30.10/ca.p7b」と指定します。
- トラストプールセキュリティを使用し、T パラメータを指定しない場合、デバイスはサーバからトラストプール バンドルを取得します。
- Zxxx.xxx.xxx.xxx;：NTP サーバの IP アドレス。trustpool 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 オプションの設定方法について詳しくは、DHCP サーバのマニュアルを参照してください。

DNS を使用したディスカバリの設定

DHCP ディスカバリでサーバの IP アドレスを取得できない場合、デバイスは次に DNS ルックアップを方法として使用します。デバイスは、DHCP サーバによって返されるネットワーク ドメイン名に基づいて、プリセットのホスト名「pnpserver」を使用してサーバの完全修飾ドメイン名（FQDN）を生成します。

たとえば、DHCP サーバがドメイン名「example.com」を返した場合、デバイスは「pnpserver.example.com」という FQDN を生成します。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。

プラグ アンド プレイ接続を使用したディスカバリの設定

プラグ アンド プレイ接続は、シスコ提供のサービスで、ネットワーク プラグ アンド プレイ対応デバイスがサーバを検出するために使用する最後の手段です。プラグアンドプレイ接続を使

用してサーバを検出するには、最初にPnPサーバを表すコントローラプロファイルを作成し、次に各デバイスをプラグアンドプレイ接続サービスに登録する必要があります。

プラグ アンド プレイ接続サービスへのアクセス

プラグ アンド プレイ接続サービスにアクセスするには、以下を行います。

1. Web ブラウザで *https://software.cisco.com* を参照します。
2. 画面の右上にある [Log In] ボタンをクリックします。Cisco スマート アカウントに関連付けられている cisco.com ID でログインします。
3. [Network Plug and Play] という見出しの下の [Plug and Play Connect] リンクを選択します。**プラグ アンド プレイ接続**サービスのメイン ページが表示されます。

コントローラ プロファイルの作成

PnP サーバのコントローラプロファイルを作成するには、次の手順を実行します。

1. ブラウザでプラグ アンド プレイ接続の Web ページを開きます。必要に応じて、使用する正しい仮想アカウントを選択します。
2. [Controller Profiles] リンクを選択し、[Add Profile] ボタンをクリックします。
3. ドロップダウンリストからコントローラタイプとして [PNP SERVER] を選択します。その後、[Next] をクリックします。
4. プロファイルの名前を指定し、オプションで説明を指定します。
5. [Primary Controller] という見出しの下で、表示されているドロップダウンを使用して、名前とIPアドレスのどちらでサーバーを指定するか選択します。表示されるフィールドに、サーバの名前またはアドレスを入力します。
6. サーバとの通信時に使用するプロトコルを選択します。プロビジョニング プロセスを完全なものにするために、HTTPS を使用することを強くお勧めします。
7. 選択したプロトコルが HTTPS の場合、サーバが使用する証明書を表示されたコントロールを使用してアップロードする必要があります。Cisco Business ダッシュボード からの証明書のダウンロードに関する詳細については、証明書の管理 を参照してください。
8. オプションでセカンダリ コントローラを指定します。
9. [Next] をクリックし、設定を確認した後、[Submit] をクリックします。

デバイスの登録

シスコから直接購入した特定の製品は、注文の時点でCiscoスマート アカウントに関連付けることができ、それらの製品はプラグアンドプレイ接続に自動的に追加されます。ただし、Cisco Businessプラグアンドプレイ対応製品の大部分は、手動で登録する必要があります。デバイスをプラグ アンド プレイ接続に登録するには、以下を行います。

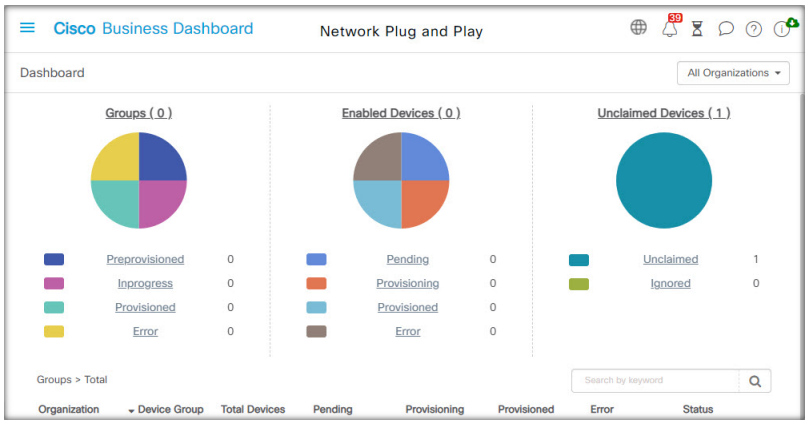
1. ブラウザでプラグ アンド プレイ接続の Web ページを開きます。必要に応じて、使用する正しい仮想アカウントを選択します。
2. [Devices] リンクを選択し、[Add Devices] をクリックします。アカウントにデバイスを手動で追加する場合、場合により承認を受ける必要があります。これは 1 回限りのプロセスであり、必要な場合は、承認が付与された後に電子メールで通知を受け取ることができます。
3. デバイスを手動で追加するか、またはCSV形式で詳細をアップロードすることで複数のデバイスを追加するか選択します。用意されているリンクをクリックすると、サンプルの CSV ファイルをダウンロードできます。CSV ファイルのアップロードを選択した場合、[Browse] ボタンをクリックしてファイルを選択します。
4. **[次へ (Next)]** をクリックします。
5. デバイスの手動追加を選択した場合、[Identify Device] をクリックします。追加するデバイスのシリアル番号と製品 ID を指定します。ドロップダウンからコントローラプロファイルを選択します。オプションで、このデバイスの説明を入力します。
6. すべてのデバイスを追加するまで手順 4 を繰り返し、[Next] をクリックします。
7. 追加したデバイスを確認し、[Submit] をクリックします。

ネットワーク プラグ アンド プレイ サービスの設定

ご使用の環境でネットワーク プラグ アンド プレイ サービスを設定する場合、実行する必要があるタスクがいくつかあります。これには、設定とイメージのアップロード、ネットワーク プラグアンドプレイを使用するためのデバイスの追加と設定、およびこれまでサービスに登録されたことがないサービスに接続するデバイスの管理が含まれます。次のセクションで、これらのタスクについて詳しく説明します。

ネットワーク プラグアンドプレイ ダッシュボードの使用方法

[Network Plug and Play] ダッシュボードにより、[Network Plug and Play] を使用して現在プロビジョニングされているデバイスの概要が提供されます。



デバイスのステータスを次のように分類した 3 つのグラフが表示されます。

- Device Group
- PnP 対応デバイス
- Cisco Business ダッシュボード インベントリで定義されていないデバイス（要求されていないデバイス）

各チャートには、一覧表示されたそれぞれの状態のデバイスまたはグループの数が表示されます。チャートの状態の見出しをクリックすると、そのカテゴリに分類されるデバイスまたはグループの詳細なリストを表示できます。次の表に、それぞれのステータスの内訳を示します。

表 *1:* ネットワーク プラグアンドプレイ ダッシュボード：ステータスの定義

ステータス	説明
グループ	
事前プロビジョニング済み	保留状態の PnP 対応デバイスのみが含まれるデバイスグループ。
進行中	一部の PnP 対応デバイスが保留状態で、一部がプロビジョニング中の状態またはプロビジョニング済みの状態のデバイスグループ。
プロビジョニング	すべての PnP 対応デバイスがプロビジョニング済み状態のデバイスグループ。
エラー	エラー状態の PnP 対応デバイスが 1 つ以上含まれるデバイスグループ。
有効なデバイス	
保留中	PnP が有効になっているものの、PnP サーバーにまだ接続していないインベントリ内のデバイス。
プロビジョニング	PnPサーバーに接続してプロビジョニングを開始したものの、プロビジョニングプロセスを完了していないデバイス。

ステータス	説明
プロビジョニング	PnP を使用して正常にプロビジョニングされたデバイス。
エラー	PnP プロビジョニングプロセスが失敗したデバイス。
要求されていないデバイス	
リクエスト元不明	PnP サーバーに接続したものの、インベントリで定義されていないデバイス。
無視	ユーザーによって明示的に無視された要求されていないデバイス。

ページの右上の組織のドロップダウンを使用して、特定の組織に対して表示されるデータを制限できます。テーブルに表示されるグループを制限するには、デバイス グループを表示するときに検索ボックスにグループ名全体または一部を入力します。または、個々のデバイスの現在のステータスを表示するには、プロビジョニングルールを表示するときにデバイス名、製品ID、またはシリアル番号を検索ボックスに入力します。

（注） 要求元不明デバイスのチャートは、[All Organizations] のデータを表示する [Administrators] にのみ表示されます。

対応デバイスの管理

対応デバイスとは、イメージファイルか設定ファイルを使用してプロビジョニングされるように設定されているか、または以前に Cisco Business ダッシュボード によって検出され、ネットワーク プラグアンドプレイ プロトコルを使用して接続しようとしたことがあるインベントリ内のデバイスのことです。イメージファイルまたは設定ファイルで設定された対応デバイスは、次の機会にそのイメージおよび/または設定がデバイスに適用されます。デバイスが Dashboard に接続されて管理されている場合、変更はすぐに適用されます。それ以外の場合は、次回デバイスが接続された時点で、プローブまたは直接管理を介して、またはネットワーク プラグアンドプレイ プロトコルを使用してチェックインするときに、変更が適用されます。対応デバイスは、次回の変更期間中に変更が適用されるように設定することもできます。その場合、変更は、デバイスがチェックインした後の次回の変更期間まで延期されます。

新しい有効なデバイスを作成するには、次の手順に従います。

1. [Network Plug and Play] > [Enabled Devices] に移動します。
2. [+]（プラス）アイコンをクリックして、新しい対応デバイスをインベントリに追加します。

（注） アップロードアイコンをクリックし、csv ファイルを使用して、デバイスを一括して追加することもできます。テンプレート csv ファイルは、[Network Plug and Play] > [Configurations] ページで、デバイスに使用する設定テンプレートを開き、[Actions] ドロップダウンから [Download CSV Template] を選択することにより、ダウンロードできます。

3. デバイスやそのデバイスが所属する組織、ネットワーク、およびデバイスグループの詳細の識別など、要求されたパラメータを [Add New Device] に入力し、[Next] をクリックします。
4. 必要に応じて、デバイスに適用するファームウェアイメージを選択します。イメージに [Default] を選択した場合、そのデバイスはサーバに接続するときにその製品の ID のデフォルトとして指定されたイメージを使用します。

（注） このページのチェックボックスを使用して、新しいデバイスのプロビジョニングを次回の変更期間まで遅らせることができます。ただし、新しいデバイスは、通常、プロビジョニングが完了するまでネットワークのアクティブな部分ではないため、これが新しいデバイスの作成時に適切になることはほとんどありません。

5. 必要に応じて、デバイスに適用する設定と、複数のバージョンがある場合はその設定のバージョンも選択します。設定がプレースホルダを含むテンプレートである場合は、このデバイスに使用する値の入力を求めるフォームが表示されます。必要に応じて、これらのフィールドに値を入力します。システムで定義されたパラメータがテンプレートに使用されている場合は、チェックボックスをクリックして、使用される値を表示することができます。
6. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

既存のデバイスを編集するには、以下の手順に従います。

1. [Network Plug and Play] > [Enabled Devices] に移動します。
2. 変更するデバイスのチェックボックスをオンにして、[Edit] をクリックします。または、デバイスの名前をクリックすることもできます。
3. [Next] をクリックして [Provision Device] 画面を表示します。必要に応じて、イメージや構成ファイルを変更し、その設定に関連付けられているパラメータ値に変更を加えます。必要に応じて、チェックボックスをオンにして、変更期間中に変更が適用されるようにします。
4. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

（注） すでにプロビジョニングされているデバイスのイメージファイルまたは設定ファイルの設定が変更されると、そのデバイスの状態は保留中にリセットされ、デバイスが再プロビジョニングされます。

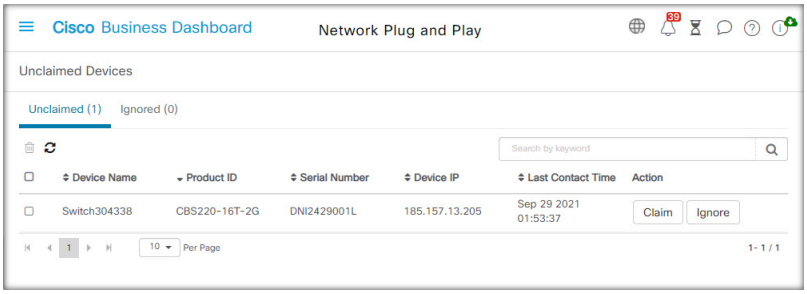
有効なデバイスを削除するには、次の手順に従います。

1. [Network Plug and Play] > [Enabled Devices] に移動します。
2. 削除するデバイスのチェックボックスを 1 つ以上オンにして、[Delete] アイコンをクリックします。

（注） 削除しなければそのデバイスが Dashboard に認識される場合に対応デバイスを削除し、そのデバイスがオンラインだった場合は、そのデバイスのイメージファイルまたは構成ファイルの設定のみが削除されます。他の管理対象デバイスと同様にそのデバイスはインベントリに残ります。その後、デバイスが PnP を使用して Dashboard に接続されると、新しいエントリが [Enabled Devices] テーブルに追加されます。

要求されていないデバイス

（注） [Unclaimed Devices] ページは、管理者のみが使用できます。



要求されていないデバイスとは、サービスに接続済みである一方で、そのデバイスに一致するデバイスレコードがインベントリにないデバイスです。要求されていないデバイスのリストを表示し、要求されていないデバイスをネットワーク プラグ アンド プレイを使用して管理できるように要求するには、以下の手順に従います。

1. [Network Plug and Play] > [Unclaimed Devices] に移動し、[Unclaimed] タブを選択します。
2. 管理するデバイスの要求ボタンをクリックします。
3. デバイスが所属する組織、ネットワーク、デバイスグループなど、要求されたパラメータを [Unclaimed Device] フォームに入力し、[Next] をクリックします。

4. 必要に応じて、デバイスに適用するファームウェアイメージを選択します。イメージに [Default] を選択した場合、そのデバイスはサーバに接続するときにその製品の ID のデフォルトとして指定されたイメージを使用します。
5. または、デバイスに適用する設定とともに、複数のバージョンがある場合はその設定のバージョンも選択します。設定がプレースホルダを含むテンプレートである場合は、このデバイスに使用する値の入力を求めるフォームが表示されます。必要に応じて、これらのフィールドに値を入力します。

   システムで定義されたパラメータがテンプレートに使用されている場合は、チェックボックスをオンにして、使用される値を表示することができます。
6. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

プロビジョニングせずに未要求リストからデバイスを削除するには、以下の手順に従います。

1. [Network Plug and Play] > [Unclaimed Devices] に移動し、[Unclaimed] タブを選択します。
2. リストから削除するデバイスに対して [Ignore] をクリックします。

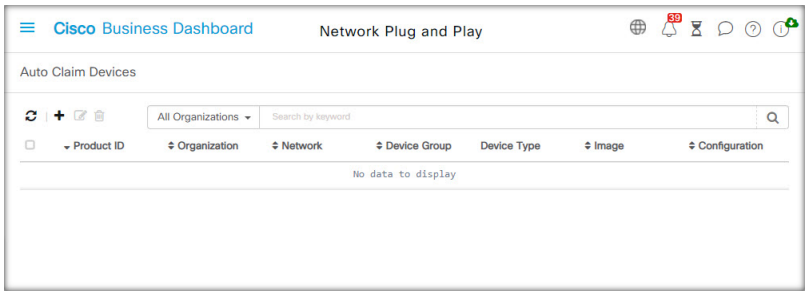
デバイスが [Ignored] リストに移動され、それ以上アクションは実行されません。無視されたデバイスを再利用するには、以下の手順に従います。

1. [Network Plug and Play] > [Unclaimed Devices] に移動し、[Ignored] タブを選択します。
2. 再要求するデバイスの[Unignore] ボタンをクリックします。

デバイスが [Unclaimed] リストに移動され、デバイスを上で説明したように要求できるようになります。

自動要求のデバイス

（注） [Auto Claim] ページは管理者のみが使用できます。



デバイスの製品 ID に対して自動要求ルールを作成することで、サーバーで要求されていないデバイスが自動的に要求され、プロビジョニングされるようにすることができます。自動要求ルールを作成するには、次の手順に従います。

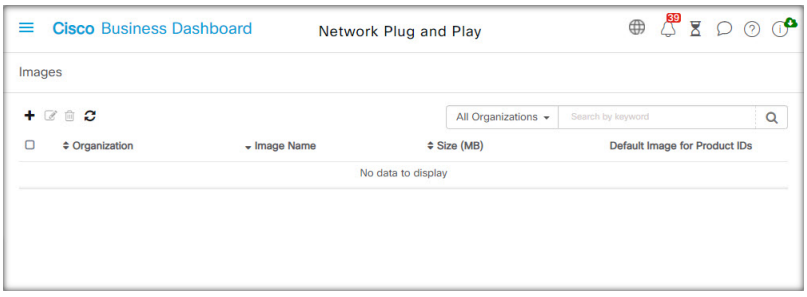
1. [Network Plug and Play] > [Auto Claim Devices] に移動します。
2. [+]（プラス）アイコンをクリックして、新しい**自動要求**ルールを作成します。
3. 照合する製品 ID（PID）と、新たに要求されたデバイスが所属する組織、ネットワーク、およびデバイスグループなど、要求されたパラメータを [Auto Claim Device] フォームに入力し、[Next] をクリックします。
4. 必要に応じて、デバイスに適用するファームウェアイメージを選択します。イメージに [Default] を選択した場合、そのデバイスはサーバに接続するときにその製品の ID のデフォルトとして指定されたイメージを使用します。
5. または、デバイスに適用する設定とともに、複数のバージョンがある場合はその設定のバージョンも選択します。設定がプレースホルダを含むテンプレートである場合は、このデバイスに使用する値の入力を求めるフォームが表示されます。必要に応じて、これらのフィールドに値を入力します。

   システムで定義されたパラメータがテンプレートに使用されている場合は、チェックボックスをオンにして、使用される値を表示することができます。
6. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

インベントリに存在しない新しいデバイスは、自動要求ルールのリストと比較照合されます。一致がある場合、**自動要求**ルールで定義されているイメージと構成ファイルで新しいデバイスレコードがインベントリ内に作成されます。その後、デバイスがそれに応じてプロビジョニングされます。デバイスが**自動要求**ルールに一致しない場合、そのデバイスは [Unclaimed] リストに追加され、以後アクションは実行されません。

デバイスのファームウェア イメージ

[Images] ページでは、ファームウェアイメージをアップロードできます。アップロード後、イメージをデバイスに展開できます。



ファームウェアイメージは、各プラットフォームのデフォルトイメージとして指定でき、それにより、デバイスファミリ全体に対してファームウェアを非常に簡単にアップデートできます。ファームウェアイメージは組織固有のものであり、同じ組織に関連付けられているプロビジョニングデバイスにのみ使用できます。

ファームウェアイメージをアップロードするには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Images]** に移動します。
2. ✚（プラス）アイコンをクリックします。
3. イメージの組織をドロップダウンから選択します。
4. ご使用の PC からファームウェア イメージをドラッグし、[Upload File] ウィンドウのターゲット領域にドロップします。または、ターゲット領域をクリックし、アップロードするファームウェア イメージを選択します。
5. [Upload] をクリックします。

ファイル名を変更するか、1 つ以上のデバイスタイプに対してイメージをデフォルトイメージとして指定することができます。ファイル名を変更するか、イメージをデフォルトイメージとして指定するには、以下の手順に従います。

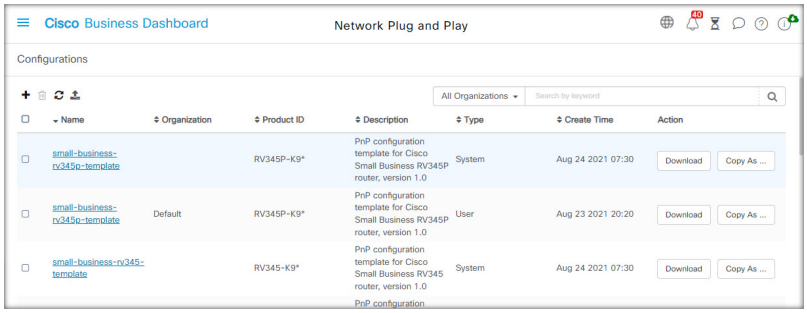
1. [Network Plug and Play] > [Images] に移動します。
2. [Images] テーブルでイメージのオプション ボタンを選択し、[edit] をクリックします。
3. 必要に応じて、提供されるテキストボックスを使用してイメージのファイル名を変更します。
4. 必要に応じて、[Default Image for Product IDs] フィールドに、製品 ID のカンマ区切りリストを入力します。製品 ID には、単一文字を表すワイルドカード文字の「?」、および文字列を表すワイルドカード文字の「*」を含めることができます。
5. [Save] をクリックします。

イメージを削除するには、以下の手順に従います。

1. [Network Plug and Play] > [Images] に移動します。
2. 削除するイメージのオプションボタンを選択し、[delete] をクリックします。

デバイスの設定ファイル

[Configurations] ページでは、構成ファイルをアップロードまたは作成できます。アップロード後、構成ファイルをデバイスに展開できます。構成ファイルは組織固有のものであり、同じ組織に関連付けられているプロビジョニングデバイスにのみ使用できます。



構成ファイルは、単純なテキストファイルの場合もあれば、複数のデバイスで同じ構成ファイルを使用できるようにするためのプレースホルダや関連付けられたメタデータが含まれている場合もありますが、デバイスごとに一意のパラメータを設定することができます。たとえば、1 つの設定テンプレートを複数のデバイスに適用できますが、デバイスごとにホスト名を個別に指定することもできます。

ダッシュボードアプリケーションには、いくつかの設定テンプレートがシステムテンプレートとして含まれており、すべての組織で使用できます。これらのテンプレートを使用すると、一般的に変更される設定を変更することもそのまま使用することもでき、新しいテンプレートのベースとしてコピーして使用することも可能です。設定テンプレートの構文の詳細については、「付録 *A*：設定テンプレートの管理」を参照してください。

新しい構成を手動で作成するには、以下の手順に従います。

1. [Network Plug and Play] > [Configurations] に移動します。
2. ✚（プラス）アイコンをクリックします。
3. テンプレートエディタが開くと、左側に設定用の空白の領域、右側にそのテンプレートに関連付けられたメタデータを管理するためのフォームが表示されます。

   左上のフィールドに設定の名前を入力します。組織を選択し、この設定をサポートする製品 ID のカンマ区切のリストを右側のフィールドに入力します。必要に応じて、説明を入力します。製品 ID には、単一文字を表すワイルドカード文字の「?」、および文字列を表すワイルドカード文字の「*」を含めることができます。
4. 左側のテキスト領域にテキストを入力するか、または貼り付けて、設定を作成します。必要に応じて、右側のコントロールを使用してメタデータに適切な変更を加えます。

   [Preview] ボタンを使用すると、デバイスに割り当てられたときに設定テンプレートがどのように表示されるかを確認できます。
5. 設定に問題なければ、[Save] をクリックします。

構成ファイルをアップロードするには、以下の手順に従います。

1. [Network Plug and Play] > [Configurations] に移動します。
2. [Upload] アイコンをクリックします。
3. ドロップダウンから設定に組織を選択します。設定の名前を指定し、必要に応じて説明を追加します。
4. ご使用の PC から設定ファイルをドラッグし、[Upload File] ウィンドウのターゲット領域にドロップします。または、ターゲット領域をクリックし、アップロードする設定ファイルを選択します。
5. [Upload] をクリックします。

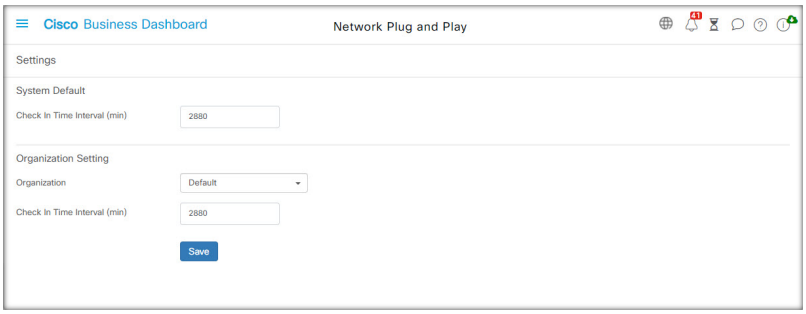
構成ファイルの内容を確認する必要がある場合、アップロードした構成ファイルのファイル名をクリックすると、テンプレートエディタに内容を表示できます。

構成を削除するには、次の手順に従います。

1. [Network Plug and Play] > [Configurations] に移動します。
2. 削除する設定のチェックボックスを 1 つ以上オンにして、[Delete] アイコンをクリックします。

設定の管理

[Network Plug and Play Settings] ページでは、ネットワーク プラグアンドプレイ プロトコルの動作を制御できます。



[Check In Time Interval] では、初回プロビジョニングの後にデバイスがネットワーク プラグアンドプレイ サービスに接続する頻度が制御されます。このパラメータを変更するには、以下の手順に従います。

1. [Network Plug and Play] > [Settings] に移動します。
2. 表示されるフィールドに、目的の接続間隔を入力します。時間は分単位で、デフォルトは 2880 分（2 日）です。
3. [Save] をクリックします。

[Check In Time Interval] はシステム全体に対して設定されますが、組織レベルでオーバーライドできます。組織に間隔が設定されていない場合は、システム値が使用されます。

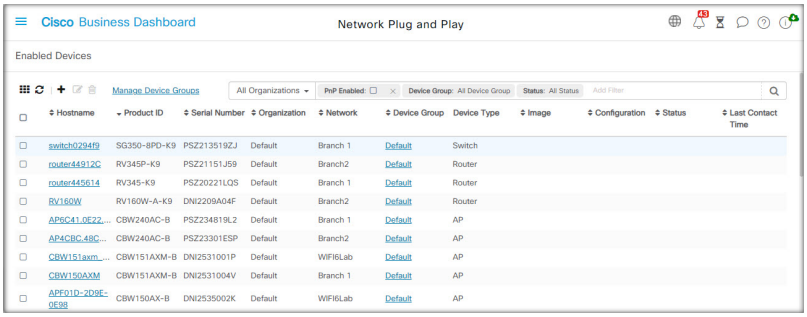
証明書の設定

最初の起動時に Cisco Business ダッシュボードによって自動的に生成された証明書は自己署名証明書です。ほとんどの場合、ネットワーク プラグアンドプレイ クライアントが証明書を受け入れるにはこれでは十分でなく、新しい証明書を生成する必要があります。新しい自己署名証明書または証明書署名要求（CSR）を生成する場合、Dashboard は、GUI の [Subject Alternative Name] フィールドに指定された値の他に、[Common Name] フィールドの内容を [Subject Alternative Name] フィールドに含めます。

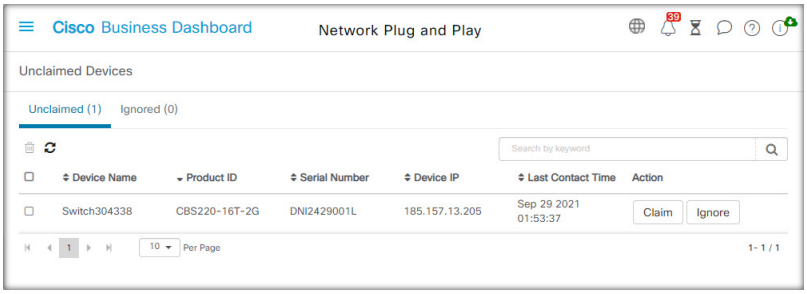
Dashboard の証明書の設定に関する詳細については、証明書の管理 を参照してください。

ネットワーク プラグ アンド プレイのモニタリング

ネットワーク プラグ アンドプレイ サービスで認識されている各デバイスは、[Enabled Devices] ページ



または [Unclaimed Devices] ページにステータス表示付きで表示されます。



また、このステータスは、[PnP Status] 列の表示を可能にすることで、[Inventory] ページに表示することもできます。ステータス フィールドには、デバイスの現在の状態が表示され、次の表にリストされている値のいずれかが含まれます。ステータス フィールドをクリックすると、そのデバイスの時間経過に伴う状態変化の履歴など、詳細を表示できます。

表 *2:* ネットワーク プラグ アンド プレイ：デバイス ステータス

ステータス	説明
Pending	デバイスが定義されている一方で、サービスには未接続。
Provisioning	デバイスがサービスに対して初回接続を実行済み。
Provisioning_Image	デバイスによってファームウェア イメージが適用中。
Provisioned _Image_Rebooting	新しいファームウェアを実行するためにデバイスがリブート中。
Provisioned_Image	新しいファームウェアの適用が正常に完了。
Provisioning_Config	デバイスに設定ファイルを適用中。

ステータス	説明
Provisioned_Config	デバイスへの設定ファイルの適用が正常に完了。デバイスの種類によっては、設定を適用するためにリブートする場合があります。
Error	エラーが発生しました。ログ ファイルで詳細を確認できます。
Provisioned	デバイスのプロビジョニング プロセスが完了。

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。