Cisco プラグ アンド プレイ アプリケーション ソリューション ガイド

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目次

このマニュアルについて 5
目的 5
対象読者 5
問題 5
Cisco プラグ アンド プレイ ソリューション 6
コンポーネント 6
Cisco ISR 上の Cisco プラグ アンド プレイ導入の導入 6
Cisco プラグ アンド プレイ導入の概要 7
Cisco プラグ アンド プレイ サーバ コンポーネントのインストール 8
Cisco Prime Infrastructure のインストールおよびセットアップ 8
Cisco プラグ アンド プレイ ゲートウェイのインストールおよびセットアップ 9
事前プロビジョニング タスク 11
第 0 日のブートストラップ設定の定義 11
第 1 日の設定テンプレートの定義 15
IOS イメージ ファイルのインポート（任意） 15
Cisco プラグ アンド プレイ導入プロファイルの定義 16
Cisco プラグ アンド プレイ プロファイルの導入 17
ISR のブートストラップおよび登録 20
Cisco Prime Infrastructure からのブートストラップ 20
エクスポート 21
TFTP を介した配布方法 21
ブートストラップ設定のメール送信 22
PIN の電子メールによる送信 22
Cisco Integrated Customization Service（CICS）を使用したブートストラップ 25
USB フラッシュを使用するブートストラップ（主導オプション） 27
自動インストールを使用したブートストラップ 28
Cisco コンフィギュレーション プロフェッショナル エクスプレス（CCP Express）を使用するブートストラップ 30
Smart Install を使用するブートストラップ 30
Cisco プラグ アンド プレイのアプリケーション 31
Cisco プラグ アンド プレイ アプリケーションを使用するブートストラップ フロー 33
トラブルシューティング情報 43

推奨バージョン 43
インストールとセットアップの問題 43
接続性の問題 44
サーバの状態の確認 45
ログの収集 46
Cisco CNS エージェントを搭載した Cisco ルータ/スイッチ 52
すでに導入済みのデバイスの再導入 53
参照 53

図のリスト

図 1 ブランチでの ISR の Cisco プラグ アンド プレイ導入 8
図 2 サンプル テンプレート「acme-branch-day0-bootstrap」、事前定義された Cisco プラグ アンド プレイ ブートストラップ テンプレートのインスタンス 13
図 3 ブートストラップおよび設定テンプレートを使用した Cisco プラグ アンド プレイ導入プロファイルのサンプル 17
図 4 ブートストラップ設定テンプレートのプロパティ 18
図 5 事前プロビジョニングのためのデバイスおよびそのパラメータの追加 20
図 6 ブートストラップ配信オプション 21
図 7 Cisco プラグ アンド プレイ ゲートウェイからのブートストラップ設定のダウンロード 23
図 8 Cisco Prime Infrastructure での Cisco プラグ アンド プレイ導入の状態の表示 24
図 9 詳細な状態メッセージの表示 25
図 10 ブートストラップ設定と共に ISR を発注する Cisco CICS オプション 26
図 11 CICS ベースの事前プロビジョニングの手順 27
図 12 USB ベースのプロビジョニング 28
図 13 自動インストールを使用するブートストラップ 29
図 14 Cisco プラグ アンド プレイの設定 30
図 15 Cisco プラグ アンド プレイ アプリケーション ベースのプロビジョニング 31
図 16 Redpark コンソール ケーブル（C2- RJ45V） 32
図 17 USB タイプ A からミニ USB タイプ B への変換ケーブルのサンプル 33
図 18 USB/シリアル アダプタのサンプル 33
図 19 Cisco プラグ アンド プレイ アプリケーションの起動ページ 35
図 20 Cisco プラグ アンド プレイ アプリケーションの [Settings] ページ 36
図 21 Cisco プラグ アンド プレイ アプリケーションでの PIN の指定 38
図 22 Cisco プラグ アンド プレイ アプリケーションの導入の状態 40
図 23 Cisco プラグ アンド プレイ アプリケーション：[Downloads] ページからのデバイス導入の開始 42
図 24 Cisco プラグ アンド プレイ アプリケーション：サポート ログの電子メール送信 47
図 25 Cisco プラグ アンド プレイ アプリケーション上での導入状態のモニタリング 51

このマニュアルについて

目的

このマニュアルでは Cisco プラグ アンド プレイ導入ソリューションのビジネス ニーズとメリットを提供するほか、このソリューションのソリューション コンポーネント、導入シナリオ、実装、および設定手順に関る詳細情報を示します。

対象読者

このガイドは、特定のプラグ アンド プレイ ベースのネットワーク導入ソリューションの仕様、設計、実装に携わる技術スタッフを対象としています。たとえば、以下の役割の方が対象です。

- ネットワーク管理者
- シスコ アカウント チーム
- Cisco SE
- シスコ テクニカル マーケティング エンジニア（TME）

問題

企業は、データセンターとブランチ ネットワークに多数のデバイスを設置し導入するために大きなコストが発生します。通常、すべてのデバイスは熟練した設置技術者によって前もって設定され、コンソール接続を介して、ネットワークの他の部分に接続可能にする CLI 設定を使用してロードしなければなりません。このプロセスは、コストと時間がかかり、エラーが生じやすい作業です。

カスタマーが使用しているネットワークの現在の導入手法は、組織間での大量の調整および多くの手動手順が必要なため、コストと時間がかかりエラーが生じやすくなります。企業は運用コストの削減に注視しているため、ネットワークの導入および継続的な変更の容易さが購入を決定する重要な要因になりつつあります。導入の簡略化のためにシスコの機器全体にスケーラブルで、使いやすく、安全で、一般的なソリューションを提供する機能は、購入の意思決定における差別化要因となると同時に、先進のシスコ テクノロジーとサービスの導入を可能にするものです。

さらに、カスタマーはシスコのボーダレス ネットワークのソリューションとシステムを購入し導入するので、コンポーネントごとにまったく異なる導入手法を必要としないことを望む可能性があります。カスタマーのサイトに導入されているシスコ デバイス全体に広げる共通の方法についての問い合わせがすでにあることはカスタマーとの対話から明らかです。

現在、新しいサイトを「立ち上げる」ために、ほとんどのカスタマーで次の手順が実施されています。

- ステージング実施場所にシスコの機器を配送します。
- 熟練した IOS に精通した技術者を使って、ルータ、スイッチ、アクセス ポイントなどを開梱します。
- 正しいイメージ、コンフィギュレーション ファイル、およびその他の必要な起動ファイルをロードします。
- 機器を再梱包します。
- 機器を再度配送します。
- サイトで装置を開梱します。
- 機器をラックに搭載しスタックに設置してケーブルを接続します。
- 最後に、サイトを NOC に引継ぎます。

そして、カスタマーが自身で機器をステージングしない場合、機器のステージング費用をサードパーティに支払うか、またはサイトに IOS に精通した技術者を派遣します。いずれの選択肢も、非常に費用がかかります。

Cisco プラグ アンド プレイ ソリューション

Cisco プラグ アンド プレイ ソリューションは、新しいデバイスの導入プロセスを劇的に簡略化する仕組みを提供することによって企業の負担を軽減します。Cisco プラグ アンド プレイ ソリューションを使用することで、新しいデバイスは、IOS CLI の予備知識がなくてもサイトの任意の設置者によって、導入できます。このガイドでは、ブランチ サイトとリモート サイトでのサービス統合型ルータ(ISR)のプラグ アンド プレイ導入について説明します。

コンポーネント

Cisco プラグ アンド プレイ ソリューションは、次のコンポーネントで構成されます。

- Cisco Prime Infrastructure
- Cisco プラグ アンド プレイ ゲートウェイ
- Cisco プラグ アンド プレイ アプリケーション(iOS アプリ、PC ベースのアプリケーション)
- シスコ デバイス上の Cisco CNS エージェント

Cisco ISR 上の Cisco プラグ アンド プレイ導入の導入

ISR に Cisco プラグ アンド プレイを導入するには、次のコンポーネントが必要です。

- **Cisco Prime Infrastructure** は、シスコ デバイス用の統合型有線およびワイヤレス管理ツールです。Cisco Prime Infrastructure では、ネットワーク管理者がネットワーク インフラストラクチャを構成、管理、モニタする単一のツールがあります。
  Prime Infrastructure はライセンスを次の 3 レベルで使用可能です。
  - ライフサイクル:ライフ サイクル全体のネットワーク管理およびモニタリングのライセンス
  - コンプライアンス:Payment Card Industry(PCI)などの標準を使用するネットワーク コンプライアンスを確認するライセンス
  - 保証:ネットワーク上のアプリケーションおよびそのパフォーマンスを詳細に見ることを可能にするライセンス

  Cisco Prime Infrastructure および各種のライセンスに関する詳細情報については、『Cisco Prime Prime Infrastructure』ページを参照してください。

  Cisco Prime Infrastructure はプラグ アンド プレイ導入の設定とイメージ ファイルをセットアップするために使用され、これを実現するには、**ライフサイクル**のライセンスが必要です。

  望ましいバージョンは、Cisco Prime Infrastructure 2.0 です。

- **Cisco プラグ アンド プレイ ゲートウェイ**は Cisco Prime Infrastructure のサービスの一部です。これは非武装地帯(DMZ)で機能し、Cisco Prime Infrastructure からのプラグ アンド

プレイ導入ジョブのホストとなり、ネットワークに加わる新しいデバイス（ISR など）からの接続を受け付けます。

- **プラグ アンド プレイ アプリケーション**はスタンドアロン アプリケーション（iPhone/iPad および PC）で、ブートストラップ設定を使用して ISR の導入を助け、プラグ アンド プレイ導入をトリガーします。これらのアプリケーションは Cisco Prime Infrastructure バージョン 1.3 以降で動作します。
- **Cisco CNS エージェント**はシスコ デバイスで実行される組み込み IOS エージェントです。

Cisco プラグ アンド プレイ導入の概要

Cisco プラグ アンド プレイを使用している ISR ブランチ WAN ルータを導入するには、次の手順を実行してください。

1. Cisco プラグ アンド プレイ サーバのコンポーネントをインストールし、セットアップします。
2. Cisco Prime Infrastructure のバージョンおよび導入要件に基づいて、Cisco プラグ アンド プレイ ゲートウェイをインストールおよびセットアップする必要があります（インストール情報については以下の表を参照してください）。
3. Cisco Prime Infrastructure でプラグ アンド プレイ プロファイルを設計します。
4. Cisco Prime Infrastructure に ISR を追加および事前プロビジョニングします。
5. Cisco Prime Infrastructure を使用して ISR をブートストラップして登録します。
6. オプションで、2 日目以降の管理のために Cisco Prime Infrastructure でこのデバイスを管理します。

ISR ルータがブートストラップしたあと、設置者はルータのケーブルを接続し電源投入して、リモートサイトにブートストラップ設定を提供します。ルータは、Cisco プラグ アンド プレイ ゲートウェイに接続し、自分自身を認識します（シリアル番号を使用）。そしてすべてのコンフィギュレーション、および任意選択で IOS イメージをダウンロードします。図は、ブランチ サイトでのプラグ アンド プレイ導入について説明しています。

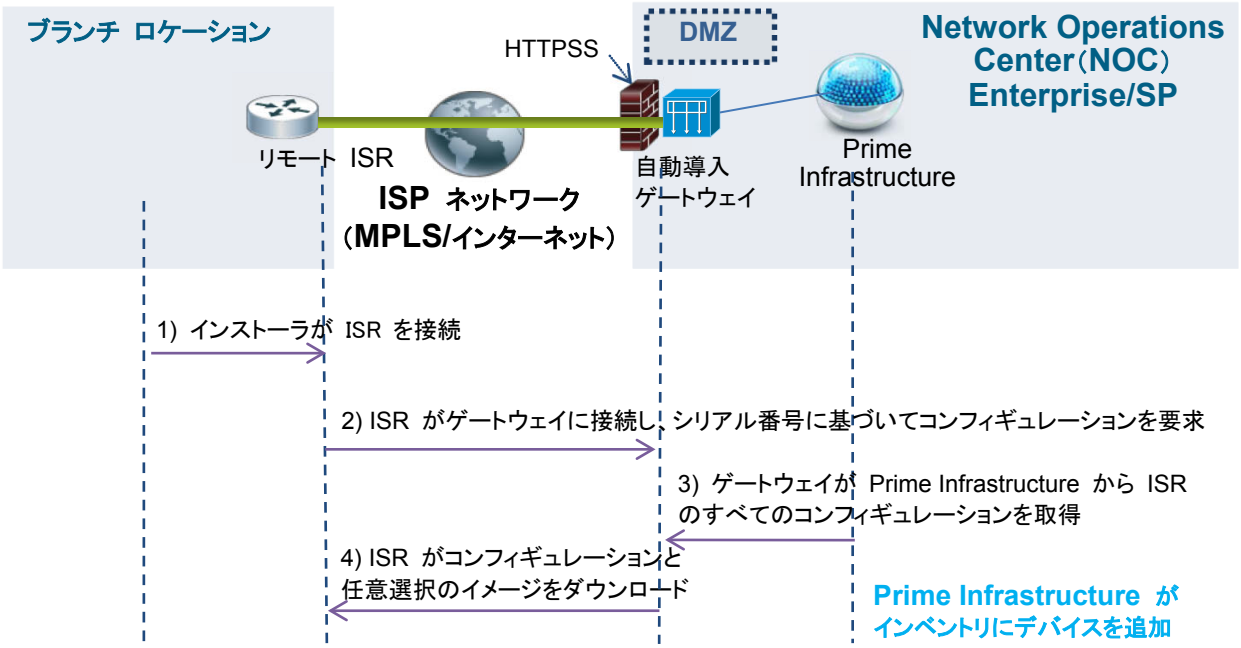


図 1 ブランチでの ISR の Cisco プラグ アンド プレイ導入

Cisco プラグ アンド プレイ サーバ コンポーネントのインストール

Cisco Prime Infrastructure 2.0 は統合されたプラグ アンド プレイ ソリューションを単一ボックスに提供します。Cisco プラグ アンド プレイ ゲートウェイを分けてインストールすることは、非 DMZ 導入では必要ありません。DMZ 導入での Cisco プラグ アンド プレイ ゲートウェイのインストールは、以前のバージョン（Cisco Prime Infrastructure 1.2）よりも簡単になります。

必要なインストール手順を特定するには、以下の表を使用して、サーバ側コンポーネントをインストールするためのこのマニュアルの項に進みます。

ネットワーク導入	Prime Infrastructure のバージョン	インストール作業
非 DMZ	PI 2.0 以降 **注**：Prime Infrastructure のインストールにはプラグ アンド プレイ ゲートウェイが含まれます。	「Prime Infrastructure のインストールおよびセットアップ」の項に進みます。（プラグ アンド プレイ ゲートウェイのインストールを分けて行う必要はありません）
非 DMZ	PI 1.2 **注**：Prime サーバとプラグ アンド プレイ ゲートウェイを別にインストールする必要があります。	1. 「Prime Infrastructure サーバのインストールおよびセットアップ」の項に進みます。 2. 「プラグ アンド プレイ ゲートウェイのインストールおよびセットアップ」の項に進みます。
DMZ	PI 2.0 以降 **注**：この導入では Prime サーバとプラグ アンド プレイ ゲートウェイを分けてインストールする必要があります。	1. 「Prime Infrastructure サーバのインストールおよびセットアップ」の項に進みます。 2. 「プラグ アンド プレイ ゲートウェイのインストールおよびセットアップ」の項に進みます。
DMZ	PI 1.2 **注**：この導入では Prime サーバとプラグ アンド プレイ ゲートウェイを分けてインストールする必要があります。	1. 「Prime Infrastructure のインストールおよびセットアップ」の項に進みます。 2. 「プラグ アンド プレイ ゲートウェイのインストールおよびセットアップ」の項に進みます。

Cisco Prime Infrastructure のインストールおよびセットアップ

Cisco プラグ アンド プレイ ゲートウェイは Cisco Prime Infrastructure 2.0 に統合されています。Cisco Prime Infrastructure サーバのインストールにも同様に Cisco プラグ アンド プレイ ゲート

ウェイのインストールが含まれます。Cisco プラグ アンド プレイ ソリューションには Prime Infrastructure 2.0 を使用することを推奨します。

ネットワークに Prime Infrastructure 2.0 をインストールするには、『Cisco Prime Infrastructure Quick Start Guide』で説明されている手順に従ってください。

Cisco プラグ アンド プレイ ゲートウェイのインストールおよびセットアップ

注:Cisco プラグ アンド プレイ ゲートウェイ サーバをインストールする前に Cisco Prime Infrastructure サーバをインストールする必要があります。

Cisco Prime Infrastructure のサーバがインストールされ起動されて実行中になったあと、Cisco プラグ アンド プレイ ゲートウェイは他の仮想マシンまたはアプライアンスにインストールできます。この手順は、DMZ 導入シナリオまたは Cisco Prime Infrastructure バージョン 1.2 または 1.3 の早い時期のリリースを使用している場合にのみ必要です。

ISR から導入されている接続を受信し、Cisco プラグ アンド プレイ導入ジョブのホストになるためには、Cisco プラグ アンド プレイ ゲートウェイは DMZ にインストールされる必要があります。Cisco プラグ アンド プレイ ゲートウェイと Cisco Prime Infrastructure サーバ間の通信もセットアップする必要があります。Cisco Prime Infrastructure は Cisco プラグ アンド プレイ ゲートウェイにジョブ(新しいデバイスのための)を追加します。ゲートウェイは Prime Infrastructure と通信して Cisco プラグ アンド プレイ導入を実行しているデバイスの設定を配信します。

Cisco Prime Infrastructure 2.0 での非 DMZ 導入では、Cisco プラグ アンド プレイ ゲートウェイを別にインストールする必要はありません。

ネットワークに Cisco プラグ アンド プレイ ゲートウェイをインストールおよびセットアップするには『Cisco Prime Infrastructure Quick Start Guide』の第 9 章に記載されている手順に従ってください。

Cisco プラグ アンド プレイ ゲートウェイ 2.0 を使用した「**pnp setup**」CLI コマンドの使用例

手順 1 ログイン管理ユーザ名とパスワードを使用して Cisco プラグ アンド プレイ ゲートウェイにログインします。

手順 2 コマンド プロンプトで「***pnp setup***」コマンドを入力し Enter を押します。

手順 3 以下のパラメータ入力のためのコンソール プロンプトが表示されます。

- Prime Infrastructure サーバの IP アドレス
- 自己署名サーバ証明書の使用
- Prime Infrastructure サーバ証明書の自動ダウンロード
- プレーン テキストと暗号化処理を使用して開始するためのイベント ゲートウェイの数
- 管理対象デバイスをこのゲートウェイに接続する方法を指定する CNS イベント コマンド
- 変更を確定します。
- Prime サーバ証明書をダウンロードするための Prime Infrastructure 管理ユーザ名とパスワード

手順 4　以下はコンソール出力です。

bgl-pnp-dev1-ovf/admin# ***pnp setup***

##
Enter Plug and Play Gateway Setup (setup log /var/KickStart/install/setup.log)
For detail information about the parameters in this setup,
refer to Plug and Play Gateway Admin Guide.
##

Enter Prime Infrastructure IP Address: [] primeserver.acme.com
Enable self certificate for server bgl-pnp-dev1-ovf (y/n) [y]
Self Signed Certificate already available do you want to recreate (y/n)?[n] y
Generated Self Signed Certificate for 5 Years (1825 Days)

Automatic download of SSL Certificate is possible if
Prime Infrastructure Server is up and running.

Automatically download the certificate for server primedev-01.cisco.com (y/n) [n] y
Enter number of Event Gateways that will be started with crypto operation: [5]
Enter number of Event Gateways that will be started with plaintext operation: [5]

The CNS Event command configures how the managed devices should
connect to this particular Plug and Play Gateway. The command entered in the following
line should match what's configured on the devices WITHOUT the port
number and keyword 'encrypt' if cryptographic is enabled.

For example, if the following CLI is configured on devices
"cns event bgl-pnp-dev1-ovf encrypt 11012 keepalive 120 2 reconnect 10",
then `encrypt 11012` should be removed and the below line should be entered :
"cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10"

Another example, if this is a backup Plug and Play Gateway and the following CLI is
configured on devices
"cns event bgl-pnp-dev1-ovf 11011 source Vlan1 backup", then `11011`
should be removed and the below line should be entered :
"cns event bgl-pnp-dev1-ovf source Vlan1 backup"

Unable to enter a correct CLI could cause the managed devices not
be able to connect to this Plug and Play Gateway. For details, please refer to
Installation and Configuration Guide.

Enter CNS Event command: [cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10]

Commit changes (y/n): y
Attempting to disable the local Plug and Play Gateway in Prime Infrastructure Machine
primeserver.acme.com
Enter the username to login to the Prime Infrastructure Machine: [admin]
Enter the password to login to the Prime Infrastructure Machine:
Setup is in progress.....
Stop Plug and Play Gateway server

Done. Plug and Play Gateway setup completed
Start Plug and Play Gateway server....
Done. Plug and Play Gateway server started!

これで、Cisco プラグ アンド プレイ ゲートウェイが無事にインストール、セットアップされ、実行されています。

注:プラグ アンド プレイ ゲートウェイの Cisco Prime Infrastructure サーバ証明書のインストールは、バージョン 2.0 のセットアップ処理を使って自動化されます。

事前プロビジョニング タスク

次の事前プロビジョニング タスクは Cisco プラグ アンド プレイのデバイスに対して実施する必要があります。

- Cisco Prime Infrastructure に事前に準備されたシステム テンプレート「*プラグ アンド プレイ ブートストラップ*」を使用して第 0 日のブートストラップ設定を定義します。
- Cisco Prime Infrastructure の CLI テンプレート、UI ベースのテンプレート、または構成テンプレートを使用して、第 1 日の設定テンプレートを定義します。
- Cisco Prime Infrastructure のソフトウェア イメージ管理機能を使用して Cisco プラグ アンド プレイのデバイス用に更新されたイメージを、任意で追加します。
- 「プラグ アンド プレイ プロファイル」を作成し、第 0 日のブートストラップ設定テンプレート(上記で指定済)、第 1 日の設定テンプレート、および任意で適用するイメージを追加します。
- 新しく作成した Cisco プラグ アンド プレイ プロファイルをパブリッシュします。
- 新しく作成した Cisco プラグ アンド プレイ プロファイルを導入します。
- 導入処理で、Cisco プラグ アンド プレイのデバイスをプロファイルに追加し、任意でシリアル番号を登録します。シスコ デバイスのシリアル番号を指定しなかった場合は、導入処理中に Cisco プラグ アンド プレイ ソリューションによって自動的に検出され、プロファイルに追加されます。
- デバイスの Call Home によって導入がトリガーされるとすぐに、導入の状態は [Plag and Play Status] 画面から Cisco Prime Infrastructure に戻って確認できます。導入が成功すると、状態は成功を示し、デバイスのシリアル番号が Cisco Prime Infrastructure に登録され表示されます。デバイスが Cisco Prime Infrastructure のインベントリに追加され、日常的なデバイス管理に使用できます。

第 0 日のブートストラップ設定の定義

ネットワーク管理者は、ISR が Cisco プラグ アンド プレイのゲートウェイと通信できるようにブートストラップ設定を定義するために Cisco Prime Infrastructure の設定テンプレートを使用できます。このブートストラップ設定は、設置者に電子メールで送信されコンソールを介してルータにロードすることも、または設置者が Cisco Prime Infrastructure から直接ダウンロードすることもできます。Cisco Prime Infrastructure のブートストラップ設定テンプレートは ISR の Cisco Networking Service(CNS)のエージェントを設定します。CNS エージェントは ISR から Cisco プラグ アンド プレイのゲートウェイへの接続を確立するために使用されます。さらに、WAN がリモート サイトにまだ設定されていない

（すなわち、リモート サイトが WAN で DHCP を使用していない）場合は、ブートストラップ テンプレートに任意に ISR の WAN インターフェイス用の設定を含むことが可能です。

Cisco Prime Infrastructure 2.0 には Cisco プラグ アンド プレイ第 0 日のブートストラップ設定用の定義済みシステム テンプレートがあります。管理者はブートストラップ設定テンプレートのインスタンスを作成するために、このテンプレートを使用できます。

Cisco Prime Infrastructure で事前定義された Cisco プラグ アンド プレイ ブートストラップ テンプレートのインスタンスを作成する手順の詳細を以下に示します。

手順 1 [Feature] > [Design] を選択します。

手順 2 左側のメニューから、[CLI Templates] ツリー ノードを展開します。

手順 3 [CLI Templates] >[System Templates – CLI] を選択します。

手順 4 [Plug and Play Bootstrap] テンプレートを選択します。

手順 5 テンプレートに名前を付けます。例：acme-branch-bootstrap

手順 6 （任意）このテンプレートを適用するデバイス タイプを選択します。

手順 7 （任意）テンプレートに表示される値を必要に応じて編集します。表示される値がデフォルトです。

手順 8 [Save as New Template] をクリックします。

[My Templates] ノードの下に指定した名前の付いたテンプレートが表示されます。

図 2 に、事前定義された Cisco プラグ アンド プレイ ブートストラップ システム テンプレートを示します。

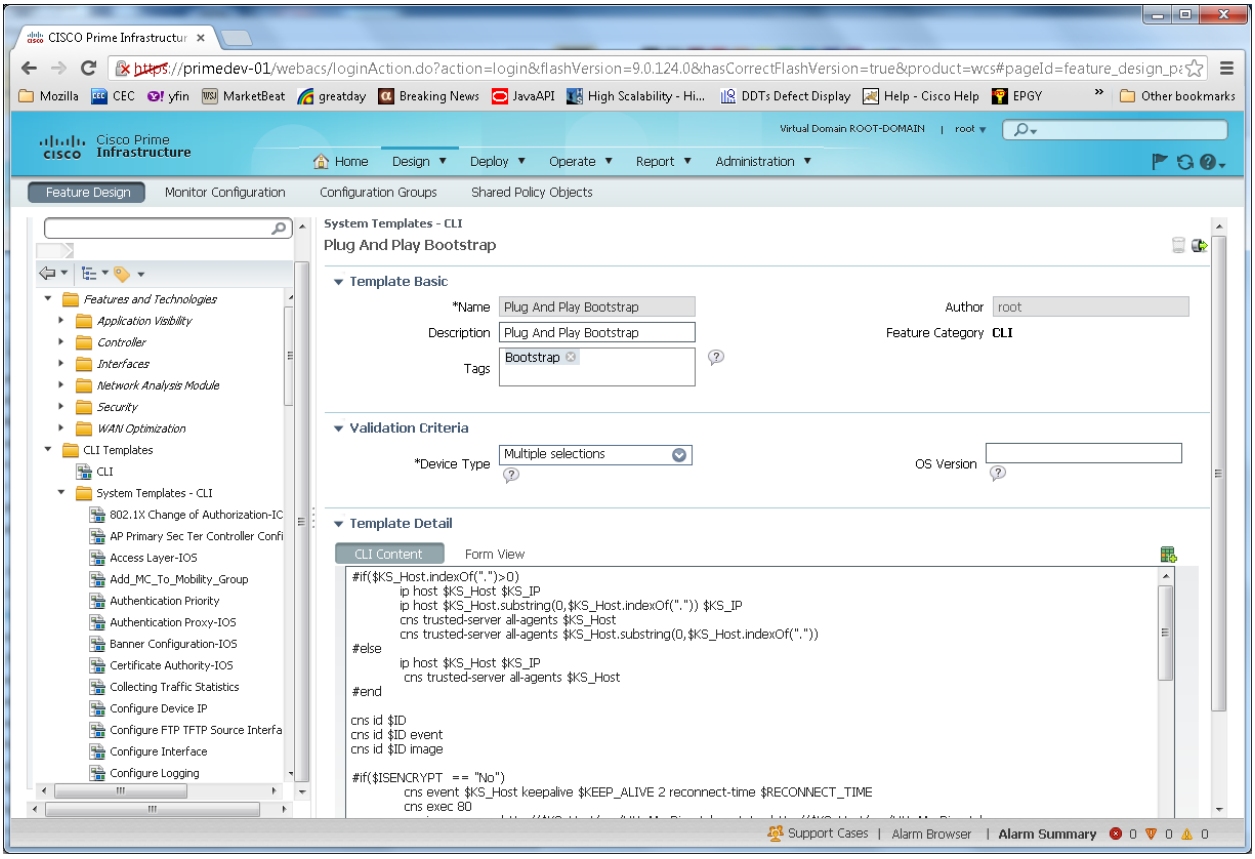
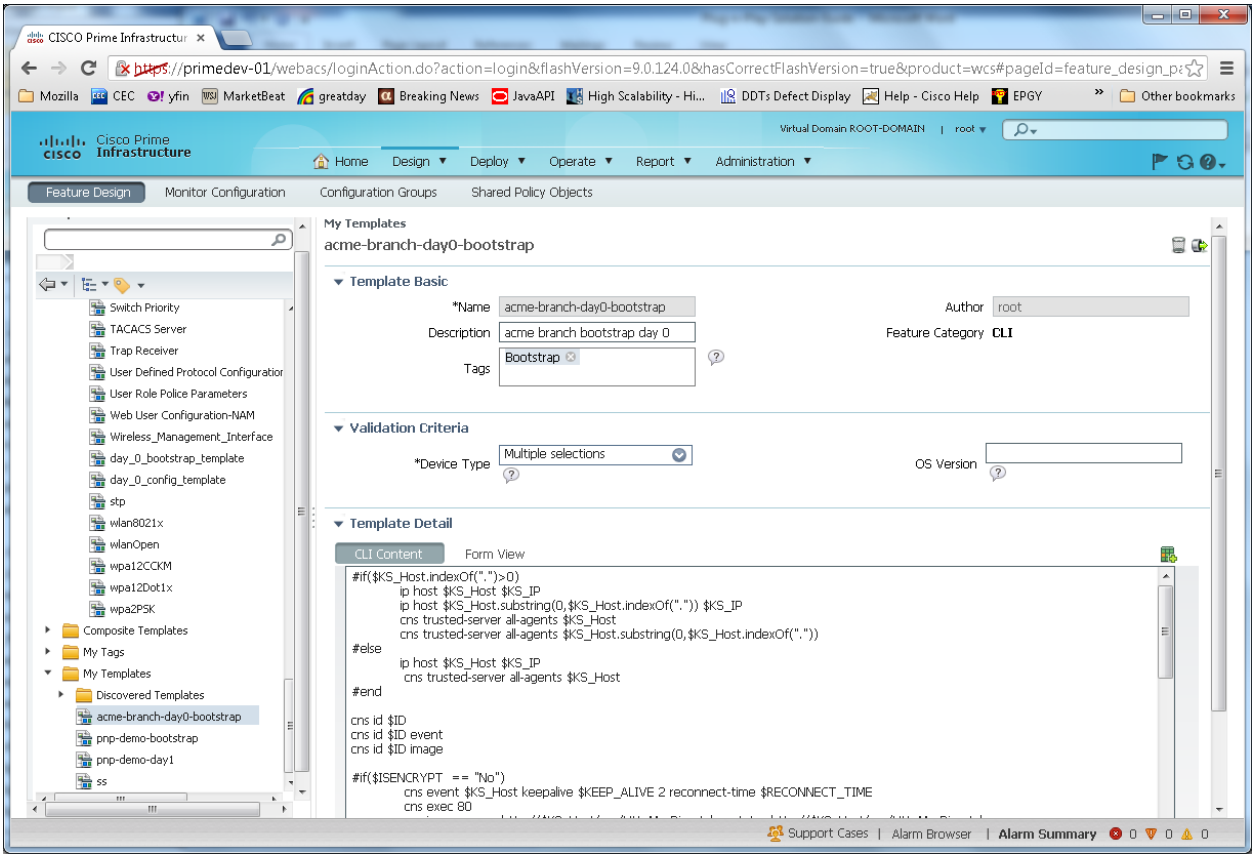


図 2 サンプル テンプレート「acme-branch-day0-bootstrap」、事前定義された Cisco プラグ アンド プレイ ブートストラップ テンプレートのインスタンス



次は、**ISR をシリアル番号で**識別する ISR CNS ブートストラップ設定のサンプルです（ゲートウェイは Cisco プラグ アンド プレイ ゲートウェイを示します）。太字で示されたすべてのフィールドは、実際のネットワーク上の対応する値に置き換える必要があります。

```
ip host <Gateway FQDN> <Gateway IP address>
ip host <Gateway hostname> <Gateway IP address>
cns trusted-server all-agents <Gateway FQDN>
cns trusted-server all-agents <Gateway hostname>
cns trusted-server all-agents <Gateway IP address>
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns event <Gateway FQDN> 11011 keepalive 120 2 reconnect-time 60
cns exec 80
cns image server http://<Gateway FQDN>/cns/HttpMsgDispatcher status http://<Gateway FQDN>/cns/HttpMsgDispatcher
cns config partial <Gateway FQDN> 80
cns config initial <Gateway FQDN> 80
```

もう 1 つの選択肢は、Unique Device Identifier（UDI）を使用して同じデバイス タイプのすべての ISR を特定することです。この選択肢は、これらの ISR をすべて同じ設定にし同じイメージを入れる場合にのみ使用する必要があります。ISR によってきめ細かい本来のセキュリティを提供するために、シリアル番号（ID）で ISR を識別することを強く推奨します。

次は、**ISR をデバイス タイプ**で識別する ISR CNS ブートストラップ設定のサンプルです（ゲートウェイは Cisco プラグ アンド プレイ ゲートウェイを示します）。太字で示されたすべてのフィールドは、実際のネットワーク上の対応する値に置き換える必要があります。

```
ip host <Gateway FQDN> <Gateway IP address>
ip host <Gateway hostname> <Gateway IP address>
cns trusted-server all-agents <Gateway FQDN>
cns trusted-server all-agents <Gateway hostname>
cns trusted-server all-agents <Gateway IP address>
cns id udi
cns id udi event
cns id udi image
cns event <Gateway FQDN> 11011 keepalive 120 2 reconnect-time 60
cns exec 80
cns image server http://<Gateway FQDN>/cns/HttpMsgDispatcher status http://<Gateway
FQDN>/cns/HttpMsgDispatcher
cns config partial <Gateway FQDN> 80
cns config initial <Gateway FQDN> 80 inventory
```

注：Cisco プラグ アンド プレイ アプリケーションでは UDI またはタイプ ベースの導入はまだサポートしていません。そのため、これらは使用できません。基盤となる CNS 組み込みエージェントによってサポートされる UDI は、すべての ISR プラットフォームで利用不可能で、問題が生じる可能性があります。

別の ISR ブートストラップ オプションの詳細についてはこのマニュアルの「Bootstrap and Register the ISR」の項を参照してください。

注：Cisco Prime Infrastructure バージョン 1.3 以前では、Cisco プラグ アンド プレイ ブートストラップ設定用の定義済みシステムのテンプレートがありません。管理者は、上記のサンプル テンプレートを使用し、Cisco Prime Infrastructure でのブートストラップ設定用 *CLI テンプレート*としてこれを定義します。

第 1 日の設定テンプレートの定義

Cisco プラグ アンド プレイ導入処理の際に、リモート サイトの ISR WAN ルータは、このサイトをネットワークの他の部分に接続するためのルータ上で機能とサービスをイネーブルにする設定ファイルをダウンロードします。この設定ファイルは Cisco Prime Infrastructure 上の単一テンプレートまたは構成テンプレートを使用して生成されます。Cisco Prime Infrastructure 上のテンプレートの使用方法の詳細については、『Cisco Prime Infrastructure User Guide』の「Designing the Network」の項を参照してください。

IOS イメージ ファイルのインポート（任意）

多くの場合、企業は ISR ルータに対して特定の IOS イメージのバージョンを検証しそこで標準化します。そのため、Cisco プラグ アンド プレイ導入では ISR で実行する目的の IOS イメージのバージョンを指定することができます。この機能を使用する場合は、『Cisco Prime Infrastracture User Guide』の「Operating the Network」セクションに説明されている「*Software Image Management (SWIM)*」手順を使用して Cisco Prime Infrastructure に IOS イメージをインポートします。

Cisco プラグ アンド プレイ導入プロファイルの定義

Cisco プラグ アンド プレイ導入プロファイルを設計する手順の詳細を以下に示します。

手順 1	[Design] > [Plug and Play Profiles] を選択します。
手順 2	[Plug and Play Profile Quick View] アイコンの上にマウスを移動し、[New] をクリックします。
手順 3	このプロファイルに使用できる新しいデバイスの [Device Type] を選択します。
注	一括導入では、イメージと設定の同じセットを使う同じ導入プロファイルを複数デバイスで使用します。デバイス ID を指定して導入プロファイルを使用するには、[Device Type] は選択しないでください。

手順 4 （任意）ブートストラップ CLI テンプレートを関連付けます。

手順 5 （任意）ソフトウェア イメージを関連付け、イメージを配信する必要のあるデバイス上のフラッシュの場所を指定します。

手順 6 （任意）設定テンプレートを関連付けます。

注：上記のうちの 1 つを指定する必要があります（すなわち、イメージ ファイルのブートストラップ テンプレートまたは第 1 日の設定テンプレート）

手順 7 （任意）フラッシュ イメージの場所。

手順 8 [Save as New Plug and Play Profile] をクリックします。保存されたプロファイルは左側のツリー [Node] の [Plug and Play Profile] の下に表示されます。

手順 9 プロファイルをパブリッシュして今後の導入に利用できようにするには [Publish] をクリックします。

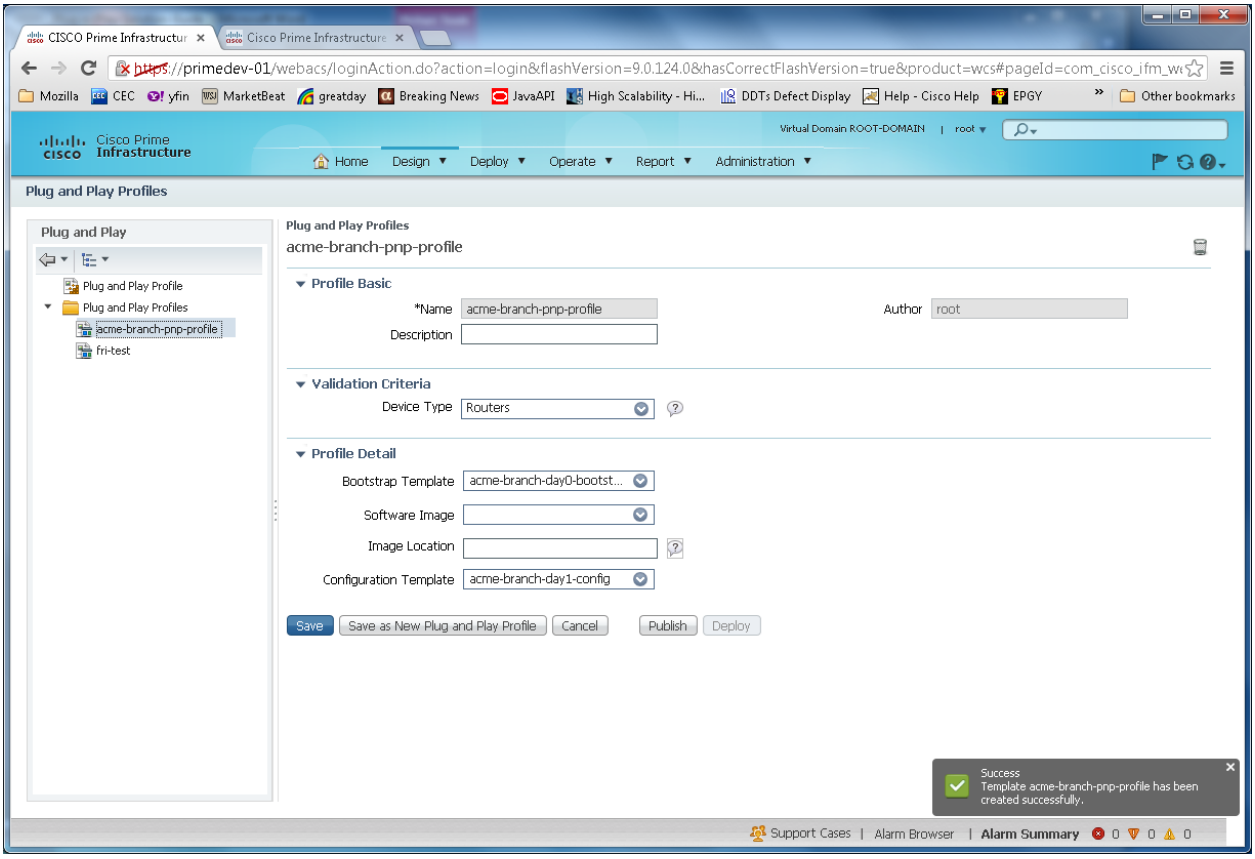


図 3 ブートストラップおよび設定テンプレートを使用した Cisco プラグ アンド プレイ導入プロファイルのサンプル

Cisco プラグ アンド プレイ プロファイルの導入

Cisco プラグ アンド プレイ導入プロファイルの設計が終わったので、次に ISR WAN ルータをプラグ アンド プレイ導入用に準備するためにこれを追加してプロビジョニングします。

手順 1 [Deploy] > [Plug and Play Deployment Profiles] を選択します。

手順 2 [Plug and Play Deployment Profiles] ページからプロファイルを選択し、次に [Deploy] をクリックします。

手順 3 [Device Provisioning Profiles] ページから、新しいデバイスを導入するために [Add] をクリックします。

注 単一プロファイルに異なるデバイスに対して適用される複数のプロビジョニング定義がある場合があります。

手順 4 （任意）デバイスのハードウェア シリアル番号または UDI を指定します。

手順 5 次のプロファイル パラメータを指定し [Apply] をクリックします。

➢ **ブートストラップ テンプレートのプロパティ**

- [PnP-Gateway Hostname]：Cisco プラグ アンド プレイ ゲートウェイのホスト名を指定します。単一ボックス インストールの場合、Cisco Prime Infrastructure のサーバ名と同じです。
- [PnP-Gateway IP]：Cisco プラグ アンド プレイ ゲートウェイの IP アドレスの IP アドレスを指定します。

- 注: ***この IP アドレスは、ISR WAN ルータから到達可能でなければなりません。***
- 残りのパラメータについてはデフォルト値を使用するのか、必要に応じて変更するのかを選択できます。Cisco Prime Infrastructure でのデフォルトのデバイス登録ではデバイスのシリアル番号（ハードウェアのシリアル番号）を使用します。デバイスのこのシリアル ID は、[show inventry] CLI を使用して表示できます。

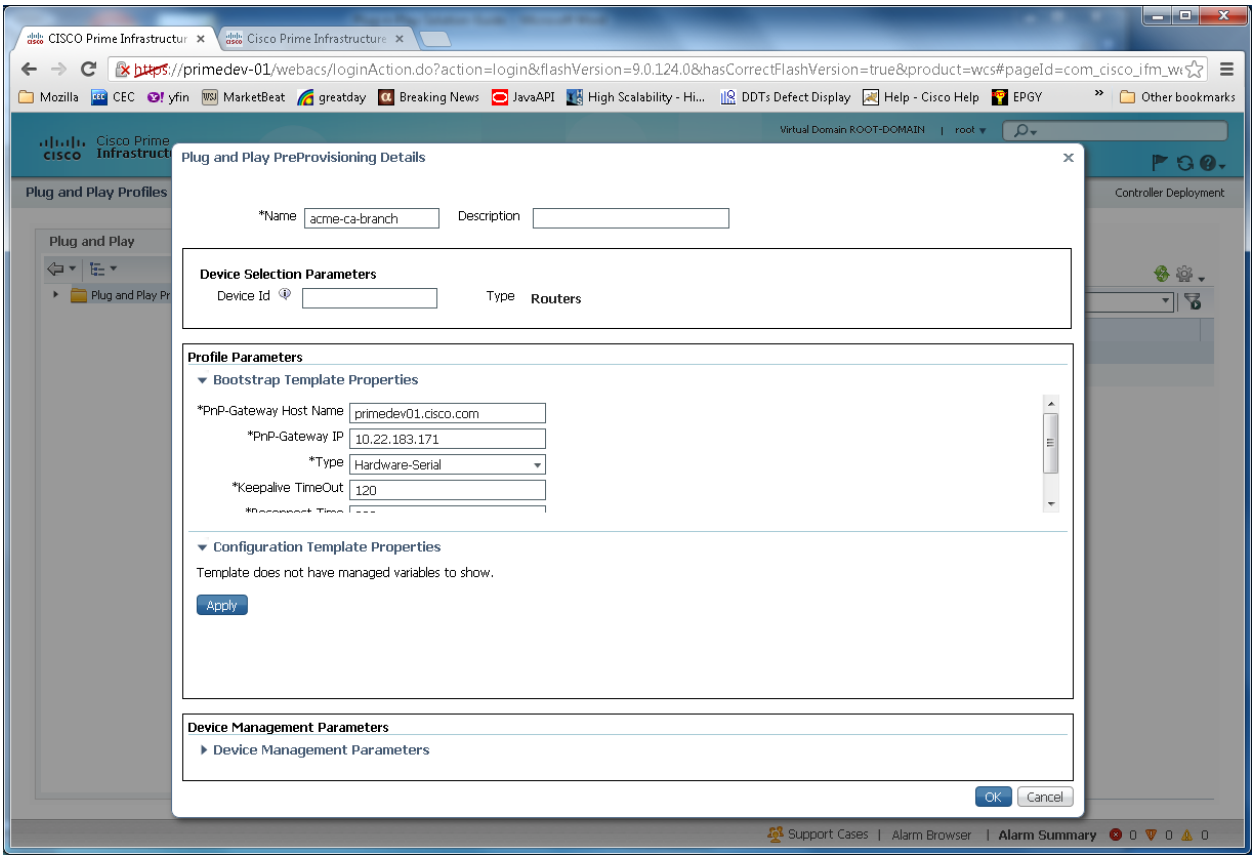


図 4 ブートストラップ設定テンプレートのプロパティ

- **イメージのプロパティ**
  - [Image location]：デフォルトでは、設計段階で指定したロケーションがターゲットロケーションとして表示されます。必要に応じて、このロケーションを変更できます。
  - [Continue on Image Failure]：イメージの導入がうまくいかなかった場合も、設定導入を継続します。
  - [Erase Flash]：イメージを配信する前にフラッシュ メモリを消去できます（つまり、フラッシュの内容全部を消去します）。
  - [Activate Image]：そのデバイスで新しいイメージを有効化することができます。
- **設定テンプレートのプロパティ**
  - 第 1 日の設定テンプレートに展開中にデバイスごとに必要なパラメータがある場合は、値を指定してください。

[Apply] をクリックしテンプレートまたはイメージ パラメータを保存します。

手順 6 Cisco Prime Infrastructure がルータを管理できるように以下のデバイス管理パラメータを指定します。Cisco Prime Infrastructure では、デバイス通信プロトコル（SNMP、Telnet、HTTP、SSH）の少なくとも 1 つを日常的な管理でこのデバイスを管理するために指定しおく必要があります。

- [IP address]：Cisco Prime Infrastructure デバイス インベントリへのデバイスの追加に使用される管理 IP アドレス。
- [SNMP Parameters]
- [SSH/Telnet Parameters]

注 Cisco Prime Infrastructure はデバイスにデバイス管理パラメータを配信しません。Cisco プラグ アンド プレイ導入の完了後、日常の管理ニーズのために Cisco Prime Infrastructure でこのデバイスを管理するために、Cisco Prime Infrastructure インベントリによってデバイス管理パラメータが使用されます。すべての設定は、Cisco プラグ アンド プレイ導入中にプロファイル内の設定テンプレートを介してのみ実行できます。

手順 7 [OK] をクリックします。

手順 8 [Close] をクリックし [Device Provisioning Profiles] ページを閉じます。

このタスクの最後で、デバイスは Cisco Prime Infrastructure 上で準備が整い、対応するジョブが Cisco プラグ アンド プレイ導入のゲートウェイに追加され、実行するために ISR からの接続を待っています。

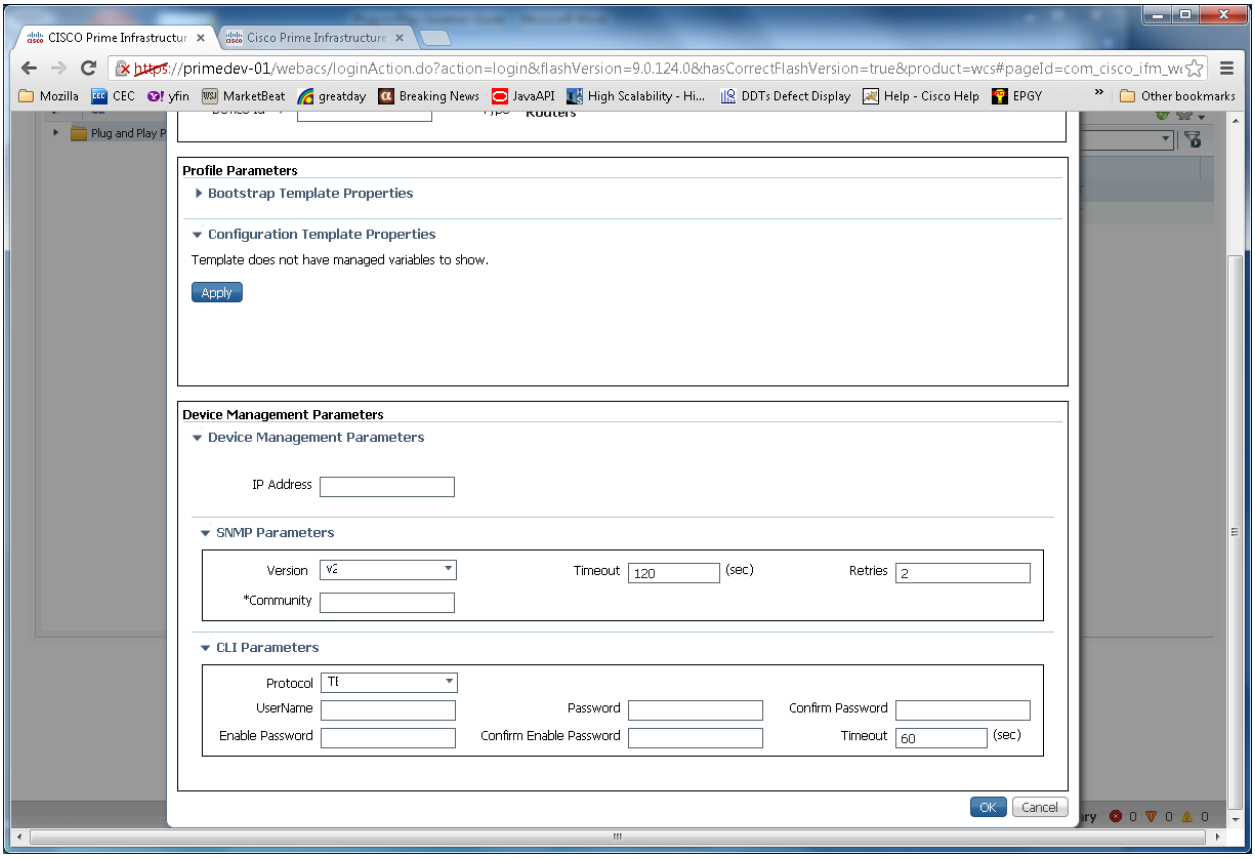


図 5 事前プロビジョニングのためのデバイスおよびそのパラメータの追加

ISR のブートストラップおよび登録

これでプラグ アンド プレイ導入ジョブの準備が整ったので、設置者はリモート サイトに ISR を導入できます。Cisco プラグ アンド プレイ導入のゲートウェイに接続するには、ISR をブートストラップする必要があります。ISR をブートストラップするにはいくつかの方法があります。

Cisco Prime Infrastructure からのブートストラップ

Cisco Prime Infrastructure からのブートストラップは、各 ISR に個別のブートストラップ設定がある場合に使用します。ブートストラップ テンプレートは Cisco プラグ アンド プレイ導入プロファイルの一部として定義され、ISR にそのブートストラップを配信するために使用されることができる次の方法の 1 つです。

- Exporting
- Delivering through Trivial File Transfer Protocol（TFTP）
- E-mailing
- E-mailing the PIN

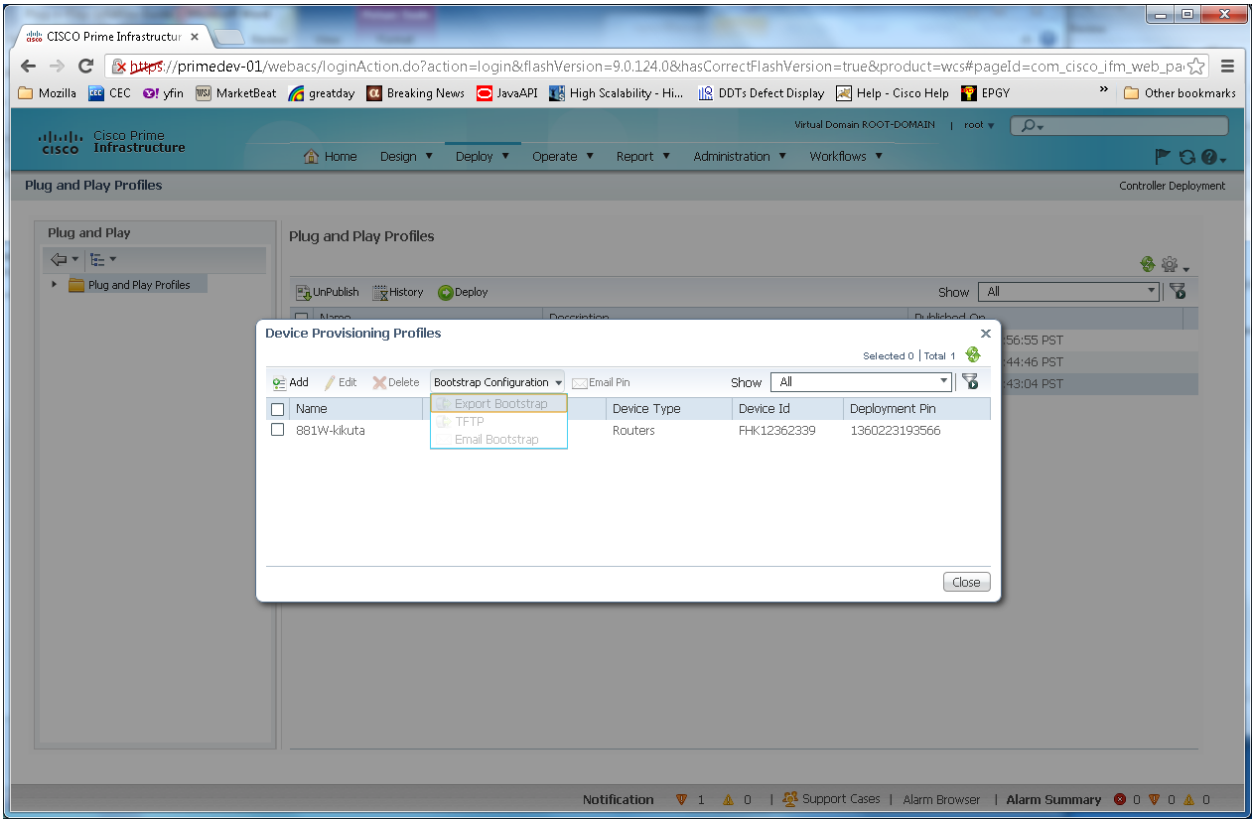


図 6 ブートストラップ配信オプション

エクスポート

Cisco Prime Infrastructure からブートストラップ設定をエクスポートするには、次の手順を実行します。

手順 1 [Deploy] > [Plug and Play Deployment Profile] を選択します。

手順 2 [Plug and Play Deployment Profiles] ページで、プロファイルを選択し、[Deploy] をクリックします。

手順 3 [Device Provisioning Profiles] ページで、リストからデバイス プロファイルを選択し、次に [Export Bootstrap] をクリックします。

手順 4 [OK] をクリックします。

設置者は手動でブートストラップをデバイスに適用できます（つまり、コンソールまたは USB フラッシュを使用）。ブートストラップ設定が適用された後、プラグ アンド プレイ導入が開始され、管理者は Cisco Prime Infrastructure 上の設定ステータスを表示できます。

TFTP を介した配布方法

TFTP を介してブートストラップ設定を配信するには、次の手順を実行します。

手順 1 [Deploy] > [Plug and Play Deployment Profile] を選択します。

手順 2 [Plug and Play Deployment Profiles] ページで、プロファイルを選択し、[Deploy] をクリックします。

手順 3 [Device Provisioning Profiles] ページで、リストから [Device Profile] を選択し、次に [TFTP] をクリックします。

手順 4 [OK] をクリックします。

注	TFTP はブートストラップ設定を配信するために使用できます。Cisco Prime Infrastructure が TFTP サーバとして機能できます。TFTP サーバで作成する必要のあるファイルの名前を指定できます。このファイルは DHCP 経由で IP アドレスと TFTP サーバ詳細を取得する自動インストール対応デバイスによって使用されます。DHCP サーバでは、TFTP サーバは Cisco Prime Infrastructure TFTP サーバとして設定する必要があります。

ブートストラップ設定のメール送信

ブートストラップ設定を電子メールで設置者へ送るには、次の手順を実行します。

手順 1	[Deploy] > [Plug and Play Deployment Profile] を選択します。
手順 2	[Plug and Play Deployment Profiles] ページで、プロファイルを選択し、[Deploy] をクリックします。
手順 3	[Device Provisioning Profiles] ページで、リストから [Device Profile] を選択し [Email Bootstra] をクリックします。
手順 4	ブートストラップ設定の送信先となる電子メール アドレスを入力します。
注	ブートストラップ設定を電子メールで送信するには、[Administration] > [System Settings] > [Mail Server Configuration] の下で設定されている電子メール設定を確認します。
手順 5	[OK] をクリックします。

設置者は手動でブートストラップをデバイスに適用できます（つまり、コンソールまたは USB フラッシュを使用）。ブートストラップ設定が適用された後、自動導入が開始されます。管理者は Cisco Prime Infrastructure 上で設定ステータスを表示できます。

PIN の電子メールによる送信

ブートストラップ設定用の PIN を配信するには、次の手順を実行します。

手順 1	[Deploy] > [Plug and Play Deployment Profile] を選択します。
手順 2	[Plug and Play Deployment Profiles] ページで、プロファイルを選択し、[Deploy] をクリックします。
手順 3	[Device Provisioning Profiles] ページで、リストからデバイス プロファイルを選択し、次に [Email PIN] をクリックします。
手順 4	PIN が送信される電子メール アドレスを指定し、[OK] をクリックします。
手順 5	設置者が PIN を使用して手動でブートストラップ設定を適用した場合は、以下を実行してください。
a.	Cisco プラグ アンド プレイ導入のゲートウェイからブートストラップ設定をダウンロードするには、次のように PIN を使用します。 https://<PnP-Gateway-Hostname>/cns/PnpBootstrap.html このプロセス中に ISR のシリアル番号も登録できます。
b.	ブートストラップ設定を手動でデバイスに適用します（つまり、コンソールまたは USB フラッシュを使用）。

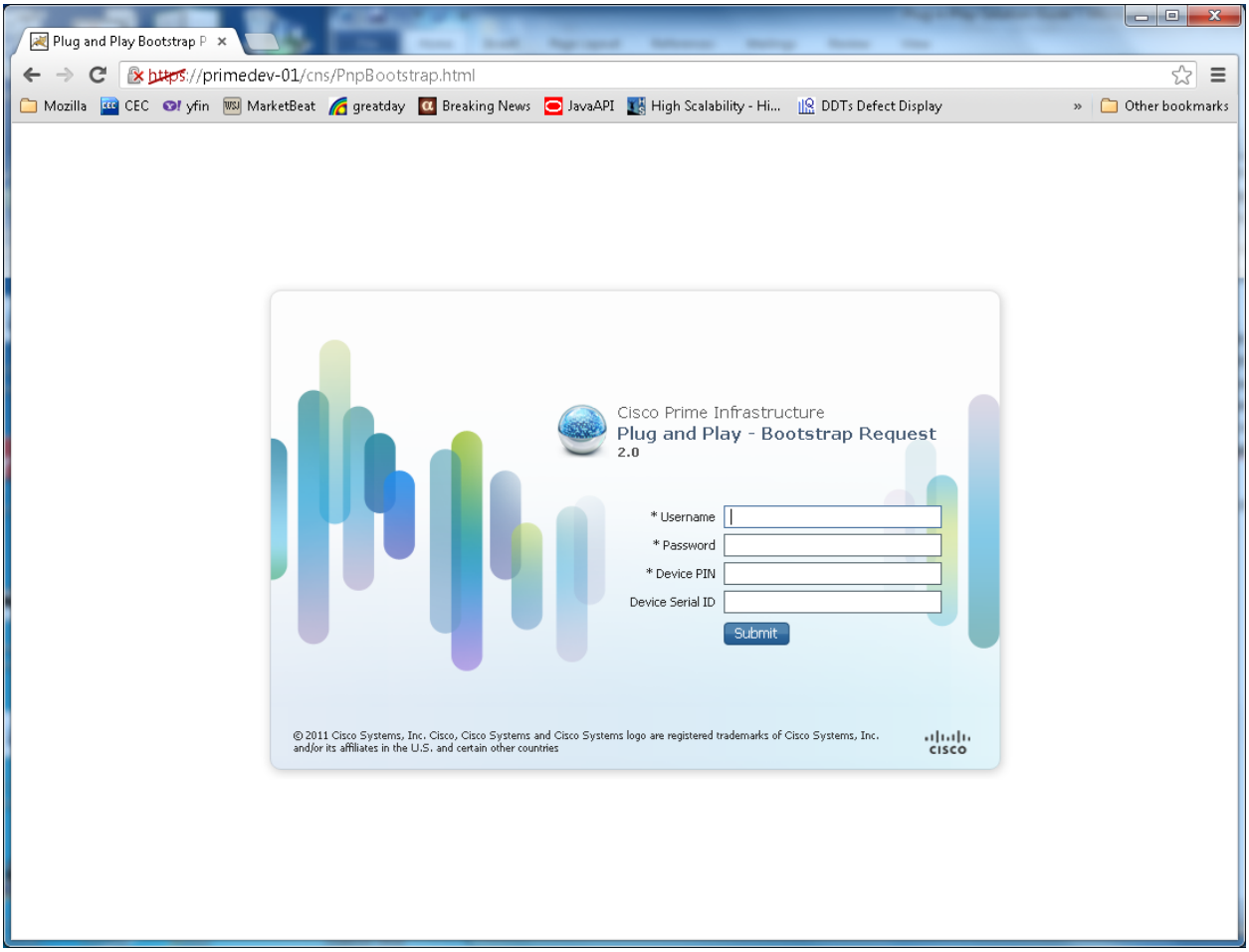


図 7 Cisco プラグ アンド プレイ ゲートウェイからのブートストラップ設定のダウンロード

手順 5　代わりに、設置者は Cisco Prime Infrastructure 導入アプリケーション（App）を使用して、ブートストラップ設定をダウンロードし適用できます。設置者はノート PC のアプリケーションに PIN を入力します。アプリケーションは Cisco プラグ アンド プレイ導入ゲートウェイからブートストラップ設定をダウンロードし、USB コンソール ケーブルを使用してノート PC に接続されているルータに適用します。詳細についての参照のリストにある『Deployment Application User Guide』を参照してください。

ブートストラップ設定が適用された後、プラグ アンド プレイ導入が開始されます。管理者は Cisco Prime Infrastructure 上で設定ステータスを表示できます。

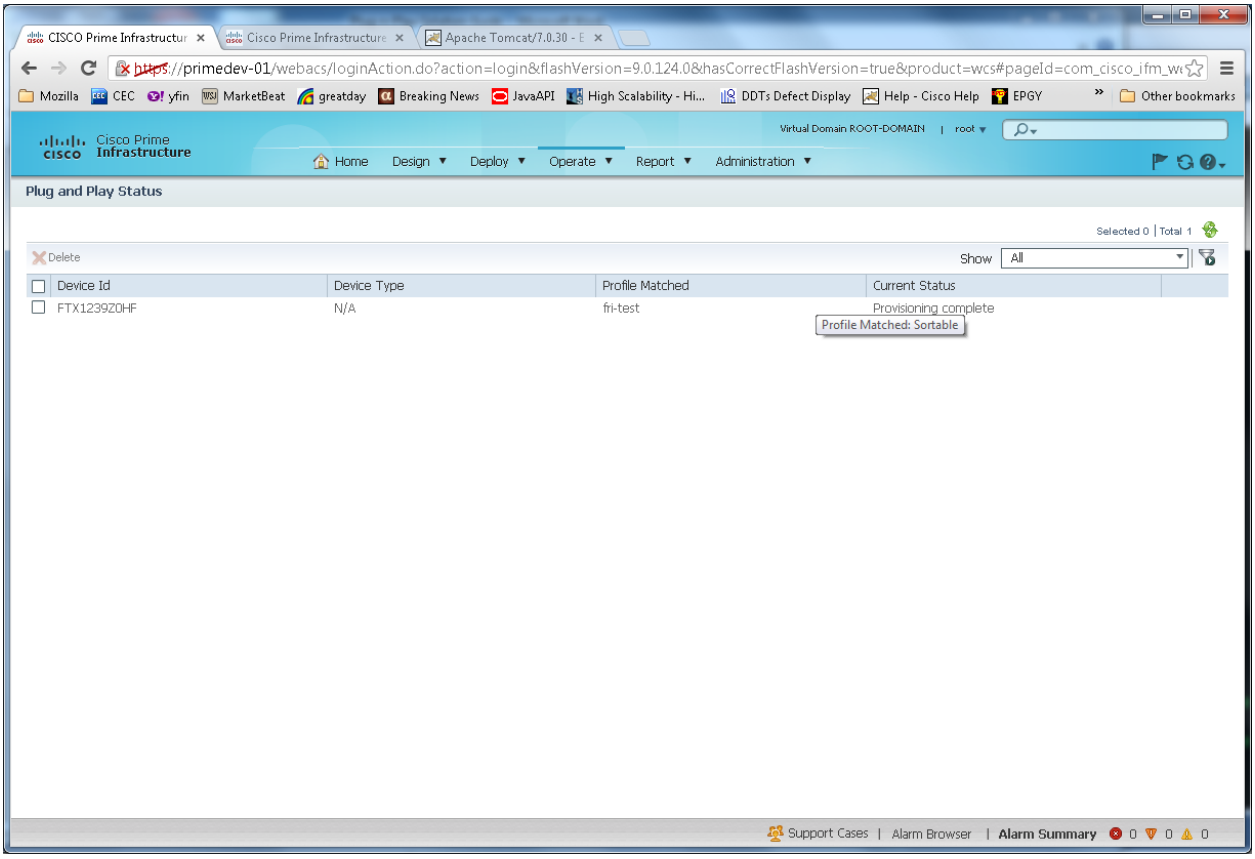


図 8 Cisco Prime Infrastructure での Cisco プラグ アンド プレイ導入の状態の表示

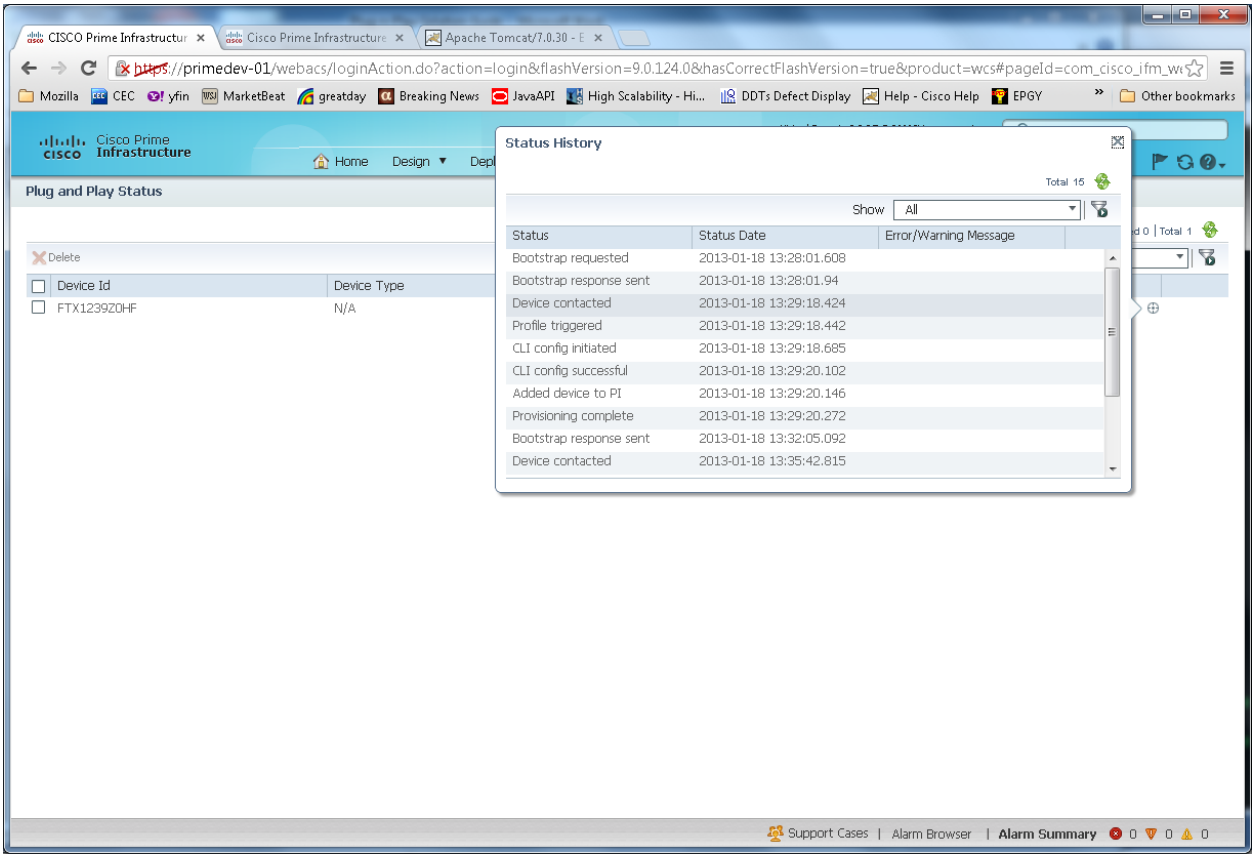


図 9 詳細な状態メッセージの表示

プラグ アンド プレイ プロファイルが正常にプロビジョニングされると、デバイスのシリアル番号が Cisco Prime Infrastructure（上図を参照）に登録され、デバイスが Cisco Prime Infrastructure のインベントリに追加されます。プロファイル導入の状態は [Added device to the PI] でも表示できます。このデバイスは、これで Cisco Prime Infrastructure の他のデバイス同様、Cisco Prime Infrastructure Device Work Center (DWC) からもアクセスできます。

注: デバイスがファイアウォールの背後にあり、Cisco Prime Infrastructure で管理されていない場合、デバイスに通信プロトコル（SNMP/Telnet/HTTP/SSH）パラメータを設定する必要はありません。ただし、このデバイスを Cisco Prime Infrastructure によって管理されるようにする場合は、対応するプロトコル パラメータを第 0 日または第 1 日の設定テンプレートに追加する必要があります。

Cisco Integrated Customization Service（CICS）を使用したブートストラップ

すべての ISR（つまり、その WAN でイーサネットを介して DHCP を使用するすべてのリモート サイト）が同じブートストラップ設定を共有している場合、共通ブートストラップ設定を製造段階からすべての ISR にロードするには Cisco Integrated Customization Services（CICS）を使用できます。CICS は Cisco Commerce Workspace（CCW）での発注プロセスの際に使用され、ISR の発注後出荷前に特定のコンフィギュレーション ファイルをロードするようにシスコへ通知します。これは、Cisco ISR G2 ルータの大量のゼロ タッチ導入に役立ちます。

図 10 ブートストラップ設定と共に ISR を発注する Cisco CICS オプション

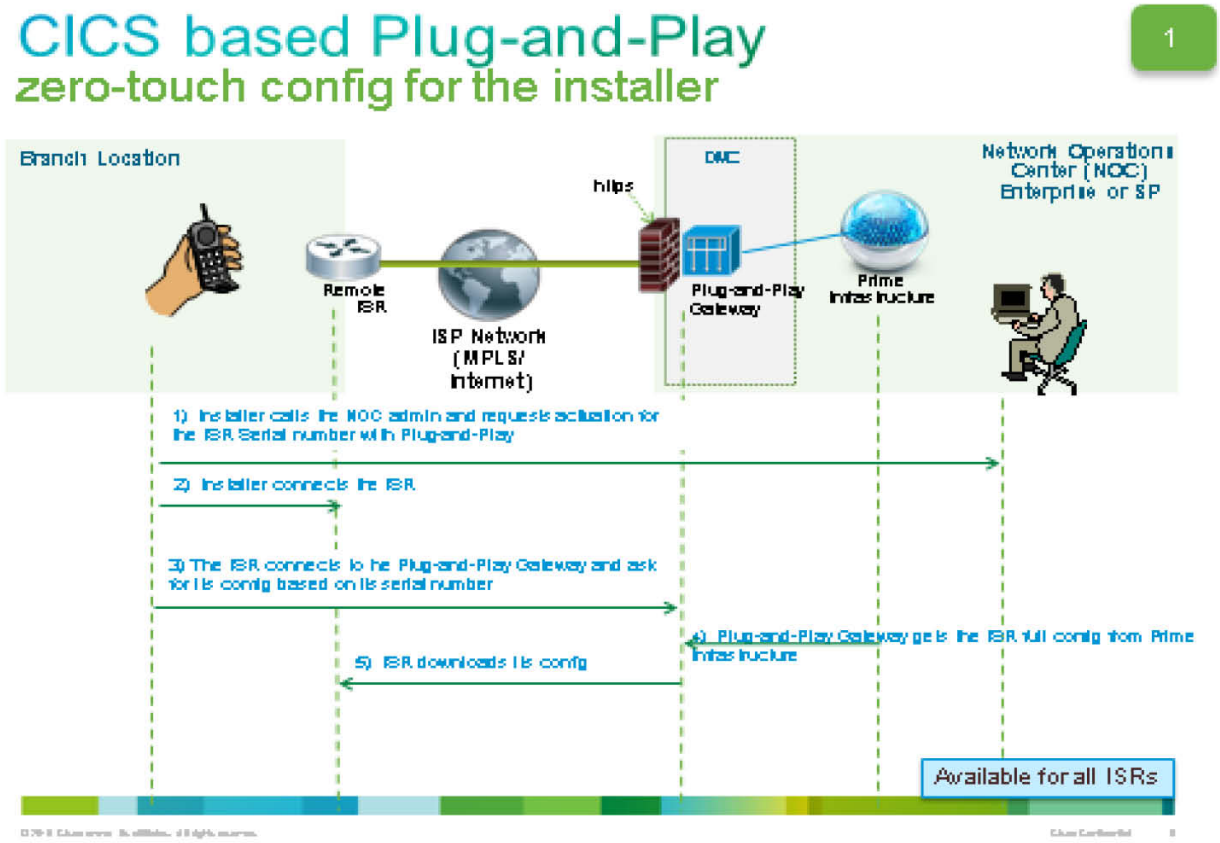


図 11 CICS ベースの事前プロビジョニングの手順

USB フラッシュを使用するブートストラップ（主導オプション）

設置者が電子メールまたはその他の手段でネットワーク管理者から実際のブートストラップ設定を入手した場合、USB フラッシュにこの設定をコピーし、USB フラッシュスロットが使用できるシスコのデバイスに挿入できます。これは、ブートストラップ設定を適用するための手動のオプションです。

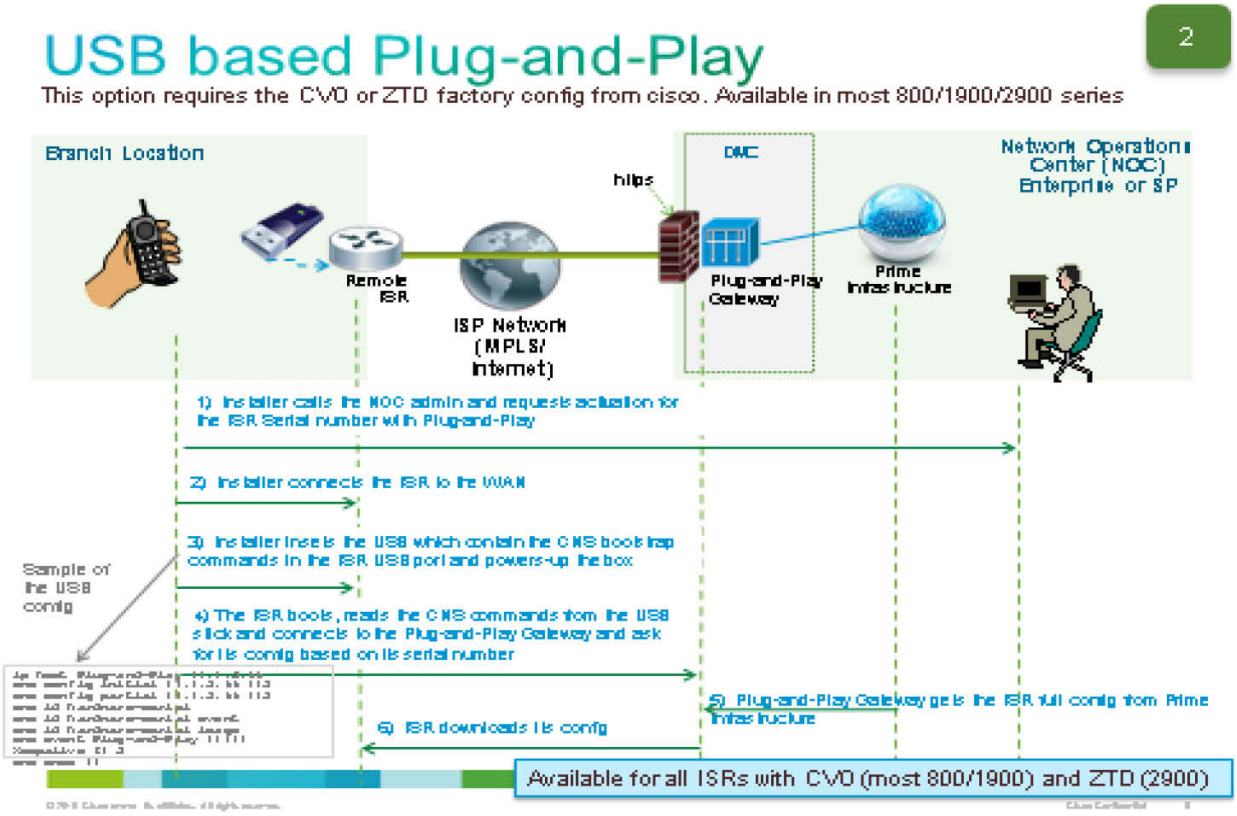


図 12 USB ベースのプロビジョニング

自動インストールを使用したブートストラップ

Cisco IOS ソフトウェアの機能には、*自動インストール*があり、シスコのデバイスの導入を簡略化し、自動化できます。自動インストールではネットワーク管理者が TFTP サーバから自動で新しいシスコ デバイス コンフィギュレーション ファイルをロードできます。これは、ネットワーク内の DHCP サーバと連携して動作します。

Cisco IOS 自動インストール機能の使用の詳細については、『Cisco IOS AutoInstall feature』を参照してください。

一般的に、自動インストール機能が搭載されている新しいルータは、TFTP サーバの IP アドレスおよびそれ自身の IP アドレスを取得するために DHCP サーバに DHCP 要求を送信します。デバイスはこれで、TFTP サーバからコンフィギュレーション ファイルを取得します。Cisco Prime Infrastructure は TFTP サーバとしてここで機能できます。ルータがコンフィギュレーション ファイルを取得すると、これを使用してロードしブートします。デバイスのブート後、Cisco プラグ アンド プレイ プロファイルで指定されている先の第 1 日の設定およびイメージ ファイルを取得するために Cisco プラグ アンド プレイ ゲートウェイに接続します。

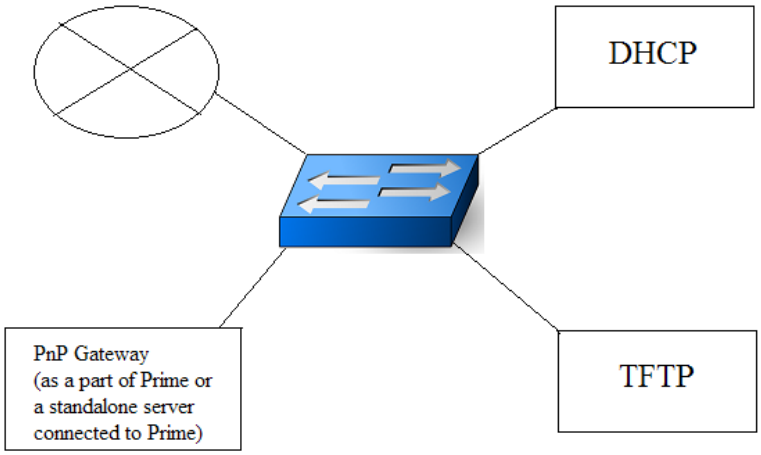


図 13 自動インストールを使用するブートストラップ

前提条件:

- Cisco Prime Infrastructure および Cisco プラグ アンド プレイ サーバが実行中であること。
- DHCP サーバが、カスタマー ネットワーク上に設定され、TFTP サーバとして指定された Cisco Prime Infrastructure があること。
- 新しいシスコ デバイスに自動インストール機能があること。
- Cisco Prime(TFTP サーバ)の「***network-confg.cfgtpl***」と呼ぶファイルにブートストラップ設定があること。上記の「TFTP を介したブートストラップの送信」の項を参照してください。
- 注:ファイル名は「***network-confg.cfgtpl***」*である必要があり、ほかの名前には変更できません。*
- DHCP プールには十分な IP アドレスがある必要があります。
- セットアップ コンポーネントは同じサブネット上にあります。

自動インストールを使用するブートストラップの手順

手順 1: Cisco Prime Infrastructure 上にプラグ アンド プレイ プロファイルを作成する手順に従います。

手順 2:「TFTP を介したブートストラップの送信」の項の手順に従って、ブートストラップ設定をファイル名 ***network-confg.cfgtpl*** で生成します。

手順 3: TFTP サーバの IP アドレスに対してオプション 150 で DHCP サーバを設定します。

ルータでスタートアップ コンフィギュレーションをなにも検出しない場合、ルータ内のインストール スクリプトが自動的に実行されます。自動インストール スクリプトは自動的に DHCP ブロードキャストを送信し、DHCP プールから IP アドレスを取得します。DHCP サーバに指定したオプション 150 は、TFTP サーバの IP アドレスを使って DHCP サーバがデバイスに応答することを可能にします。これで、デバイスは TFTP サーバに接続し、初期ブートストラップ設定を取得します。このブートストラップ

設定を使用してデバイスがロードおよび起動後に、Cisco プラグ アンド プレイ プロファイルに従って、第 1 日設定とイメージ ファイル用の Cisco プラグ アンド プレイ サーバとの接続を確立します。

Cisco コンフィギュレーション プロフェッショナル エクスプレス（CCP Express）を使用するブートストラップ

Cisco コンフィギュレーション プロフェッショナル エクスプレス（CCP Express）は、Cisco コンフィギュレーション プロフェッショナル（CCP）の簡易バージョンで、ルータのフラッシュ メモリで使用可能な組み込みデバイス マネージャです。これは、ルータの LAN および WAN インターフェイスおよび基本設定の一部を設定するために使用し、ルータをブートストラップするために使用します。デフォルトでは、CCP Express はルータのフラッシュ メモリで使用可能になります。

CCP Express バージョン 2.7 には、Cisco プラグ アンド プレイのブートストラップ設定のサポートが追加されました。これはプラグ アンド プレイ ゲートウェイ IP アドレス/ホスト名と省略可能なイメージのアップグレード コマンドを指定できるようにします。CCP Express が設定された後に、CCP Express によって基本的な CNS ブートストラップ接続コマンドがデバイス上に置かれ、Call Home 機能がイネーブルになります。デバイスに CNS ブートストラップ コマンドがある場合は、Cisco プラグ アンド プレイ ゲートウェイに接続し、第 1 日の設定および任意でイメージのダウンロード処理を開始します。

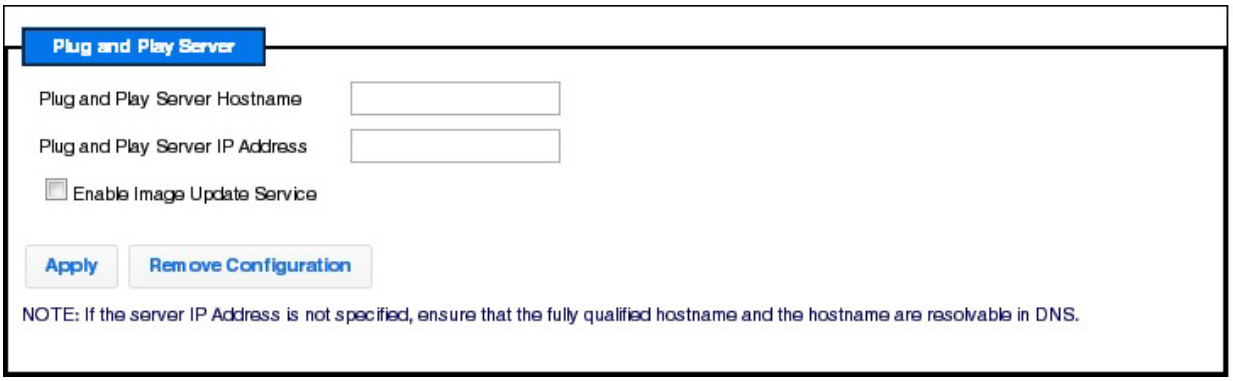


図 14 Cisco プラグ アンド プレイの設定

詳細については、CCP Express のマニュアルを参照してください。

Smart Install を使用するブートストラップ

このオプションは「***Smart Install***」機能をサポートしている Cisco スイッチに適用されます。通常、シスコ スイッチの設定は似ていて、これをすべてのスイッチに適用する必要があります。このオプションによって、Cisco Prime Infrastructure は TFTP サーバとして機能します。Cisco プラグ アンド プレイ導入プロファイルは、[Deploy] > [Add Device] > [Bootstrap Configuration] > [TFTP] オプションを使用して Cisco Prime Infrastructure TFTP ディレクトリに保存できます。Smart Install では、ディレクタ Cisco スイッチ設定が TFTP サーバとしての Cisco Prime Infrastructure を指定することを可能にします。ディレクタ スイッチがブートストラップ設定を Cisco Prime Infrastructure から取得すると、これはブートストラップ設定となり、このディレクタに接続されている集約スイッチがこのブートストラップ設定を取得して、今後導入する第 1 日の設定またはイメージ ファイルに対する Cisco Prime Infrastructure に Call Home できようになります。

Cisco プラグ アンド プレイのアプリケーション

上記のブートストラップ オプションで説明したように、デバイスにブートストラップ設定を適用する方法はいくつかあります。ブートストラップ設定を適用するために使用できるスタンドアロンのプラグ アンド プレイ導入アプリケーションがあります。これらのアプリケーションは、自動インストールまたは他のどんな仕組みもブートストラップに使用できない場合で、カスタマーがブートストラップ設定を適用する自動方式を使用することに関心がある場合に有用です。

Cisco プラグ アンド プレイ ソリューションは、iTunes からダウンロードできる iPhone/iPad ベースのモバイル スタンドアロン アプリケーション（iOS ベース）を提供します。Cisco プラグ アンド プレイ ソリューションは、これもまた iTunes Apple App Store から入手できる Cisco Prime モバイル アプリケーションとも統合されます。

Cisco プラグ アンド プレイ ソリューションは、CCO ログインを使用してシスコからダウンロードできるデスクトップ/ラップトップ ベースのスタンドアロン アプリケーション提供します（Windows ベース）。

リモート ブランチ サイトのリソースの可用性によって、設置者はデバイスをブートストラップするためにこれらのアプリケーションの 1 つを使用できます。これらのどれでもアプリケーションで提供される機能とフローは同じです。ただし、オペレーティング システムの基本的な違いがあるため、表示や感じにわずかな違いが見られることがあります。

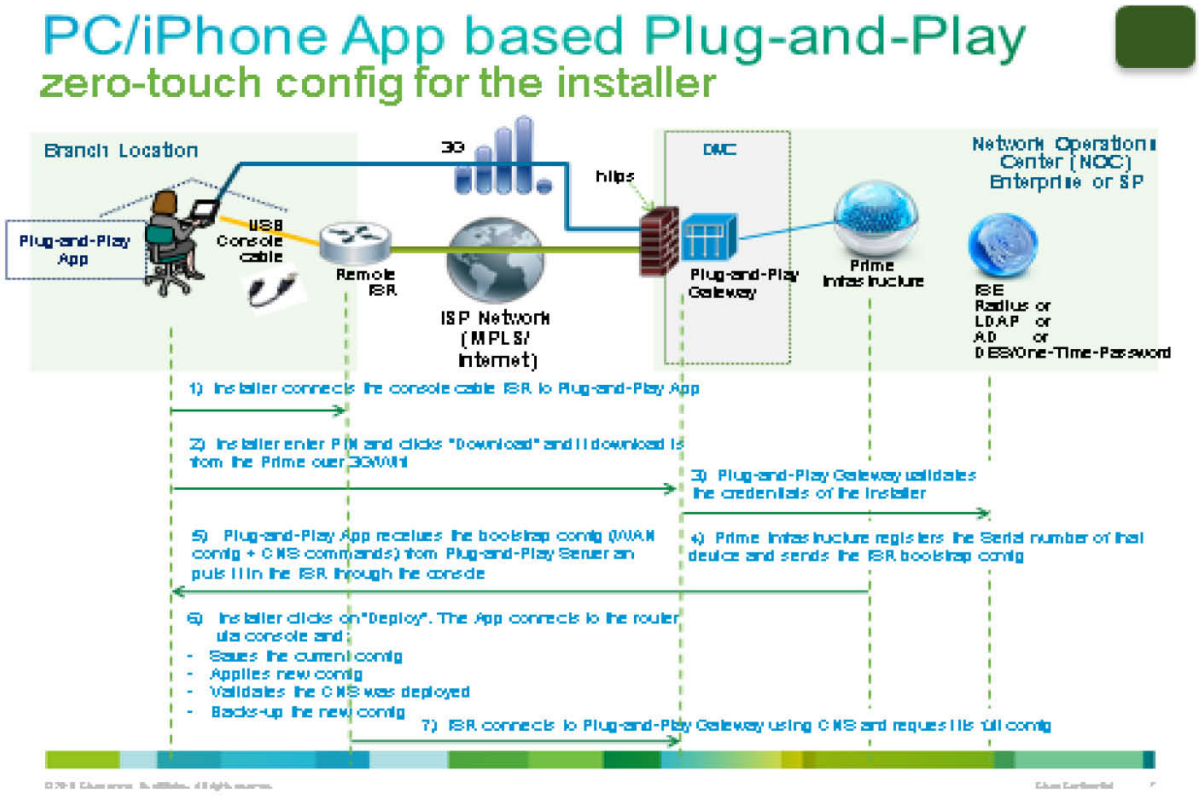


図 15 Cisco プラグ アンド プレイ アプリケーション ベースのプロビジョニング

iPhone/iPad 導入アプリケーションを使用するための前提条件

インストーラは「Redpark」ベンダーの特殊なケーブル（C2-RJ45V）を購入する必要があります。このケーブルの一方の端を iPhone/iPad の USB ケーブルに接続しもう一方の端をシスコ デバイスの青いコンソール ポートに接続します。C2-RJ45V ケーブルの詳細については、http://www.redpark.com/c2rj45.html を参照してください。

Redpark コンソール ケーブル C2-RJ45V

ケーブルの一方の端を iPhone/iPad の USB ポートに接続しもう一方の端をシスコ デバイスの青いコンソール ポートに接続します。

図 16 Redpark コンソール ケーブル（C2- RJ45V）

デスクトップ/ラップトップ PC ベースの導入アプリケーションを使用するための前提条件

設置者は、USB タイプ A からミニ USB タイプ B への変換器またはシスコ デバイスに接続するために使用可能な USB/シリアル アダプタのいずれかを持っている必要があります。Cisco ISR G2 シリーズ ルータには、導入に使用できるミニ USB コンソール ポートがあります。Cisco 8xx シリーズ ISR ルータにはミニ USB コンソール ポートがありませんが、導入のために USB/シリアル アダプタを使用できます。

図 17 USB タイプ A からミニ USB タイプ B への変換ケーブルのサンプル

図 18 USB/シリアル アダプタのサンプル

Cisco プラグ アンド プレイ アプリケーションを使用するブートストラップ フロー

Cisco プラグ アンド プレイ アプリケーションは 2 種類のモードで動作します。

- Cisco プラグ アンド プレイ アプリケーションがインストールされたデバイス(iPhone またはデスクトップ)に Cisco プラグ アンド プレイ ゲートウェイに接続する 3G 接続がある場合、導入はリモート ブランチ サイトですぐに実施できます。
- Cisco プラグ アンド プレイ アプリケーションがインストールされたデバイス(iPhone またはデスクトップ)に Cisco プラグ アンド プレイ ゲートウェイに接続する 3G 接続がない場合、ブートストラップ設定はサーバと接続可能な場所から事前にダウンロードすることができます。ブートストラップ設定のダウンロード後、この設定はデバイス(iPhone/ラップトップ/iPad)でローカルに保存されます。その後で設置者は、リモート サイトに移動し、この事前ダウンロードされたブートストラップを使用して導入を開始できます。

必要なケーブルがシスコ デバイスに接続され、ケーブルのもう一方の端がユーザ デバイス（iPhone/iPad/デスクトップ/ラップトップ）に接続された後、導入を開始できます。

デバイスが Cisco Prime プラグ アンド プレイ ゲートウェイとネットワーク接続している場合（3G またはイーサネット）に導入を開始するには、次の手順を実行します。

手順 1 Cisco プラグ アンド プレイ アプリケーションを起動します。

手順 2 最初の起動画面で、[Settings] をクリックします。

手順 3 Cisco Prime プラグ アンド プレイ ゲートウェイのアドレスを指定します。

手順 4 Cisco Prime Infrastructure のユーザ名およびパスワードを指定します。

Cisco Prime Infrastructure に適切な特権を**所有**する**非 root** ユーザを作成することを推奨します。ユーザの作成および特権の割り当ての詳細については、『Cisco Prime Infrastructure User Guide』を参照してください。

手順 5 [Test Connection] をクリックして、デバイスがサーバに接続できること確認します。サーバ エントリの定義が必要なのは Cisco プラグ アンド プレイ アプリケーションを初めて使用するときだけで、その後はサーバ情報を保存しています。

手順 6 [Deploy] アイコンをクリックして導入を開始します。

手順 7 事前にダウンロードしたブートストラップ設定が見つかった場合は、それを導入に使用できるかまたはブートストラップ設定を再度ダウンロードするのかを確認するために質問が表示されます。事前にロードした設定が見つからない場合は、PIN（手順 8 で指定するものと同じ）を指定するように促されます。

手順 8 導入を開始すると、PIN を導入するように促されます。管理者が提供する PIN 情報を入力して、[OK] をクリックします。

手順 9 導入がV完了したら、成功または失敗を示す状態メッセージが表示されます。緑色は「**導入完了**」を示し、赤色は「**導入失敗**」を示します。

手順 10（任意）ネットワーク管理者は導入が進行中のすべてのデバイスの導入の状態を、Cisco Prime Infrastructure の [Operate] > [Plug and Play] 状態メニュー オプションを使用して表示できます。

図 19 Cisco プラグ アンド プレイ アプリケーションの起動ページ

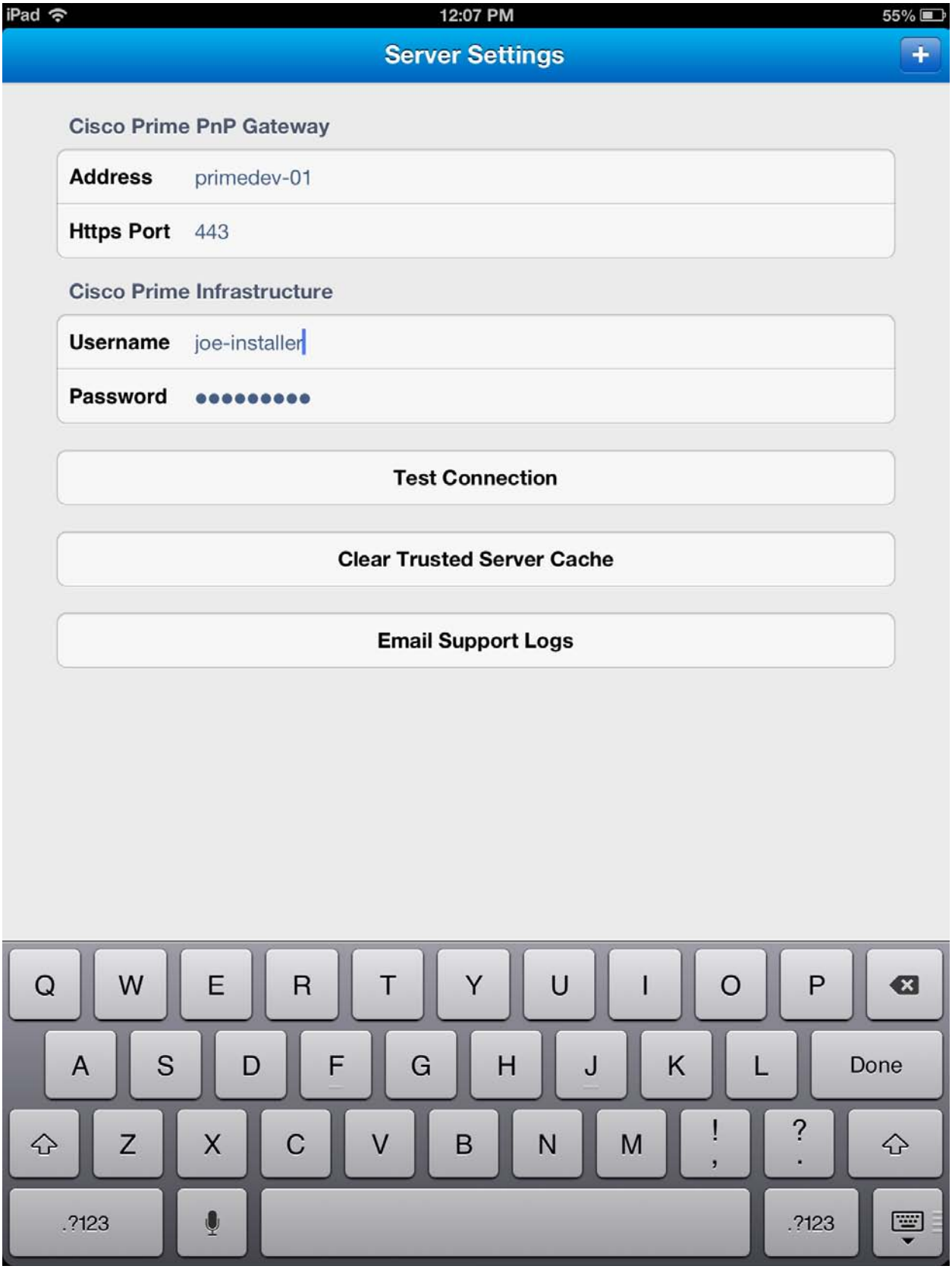


図 20 Cisco プラグ アンド プレイ アプリケーションの [Settings] ページ

導入が開始した後に、Cisco プラグ アンド プレイ アプリケーションからデバイスの PIN 番号の入力を求められます。この PIN 番号は、電子メールの [PIN] オプションを使用するか手動でネットワーク管理者から取得します。

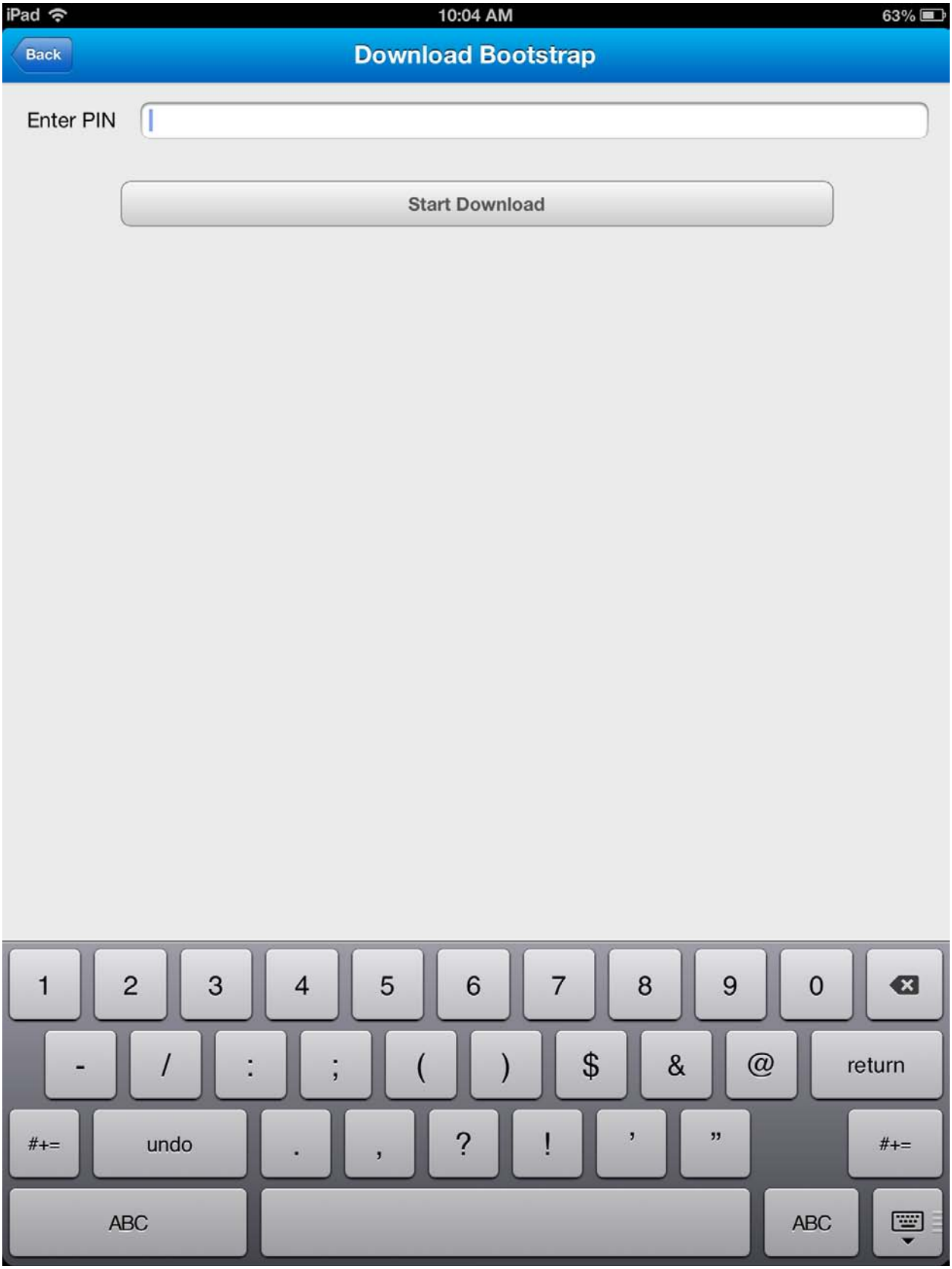


図 21 Cisco プラグ アンド プレイ アプリケーションでの PIN の指定

導入が完了したら、Cisco プラグ アンド プレイ アプリケーションは、次のように導入の状態を表示します。

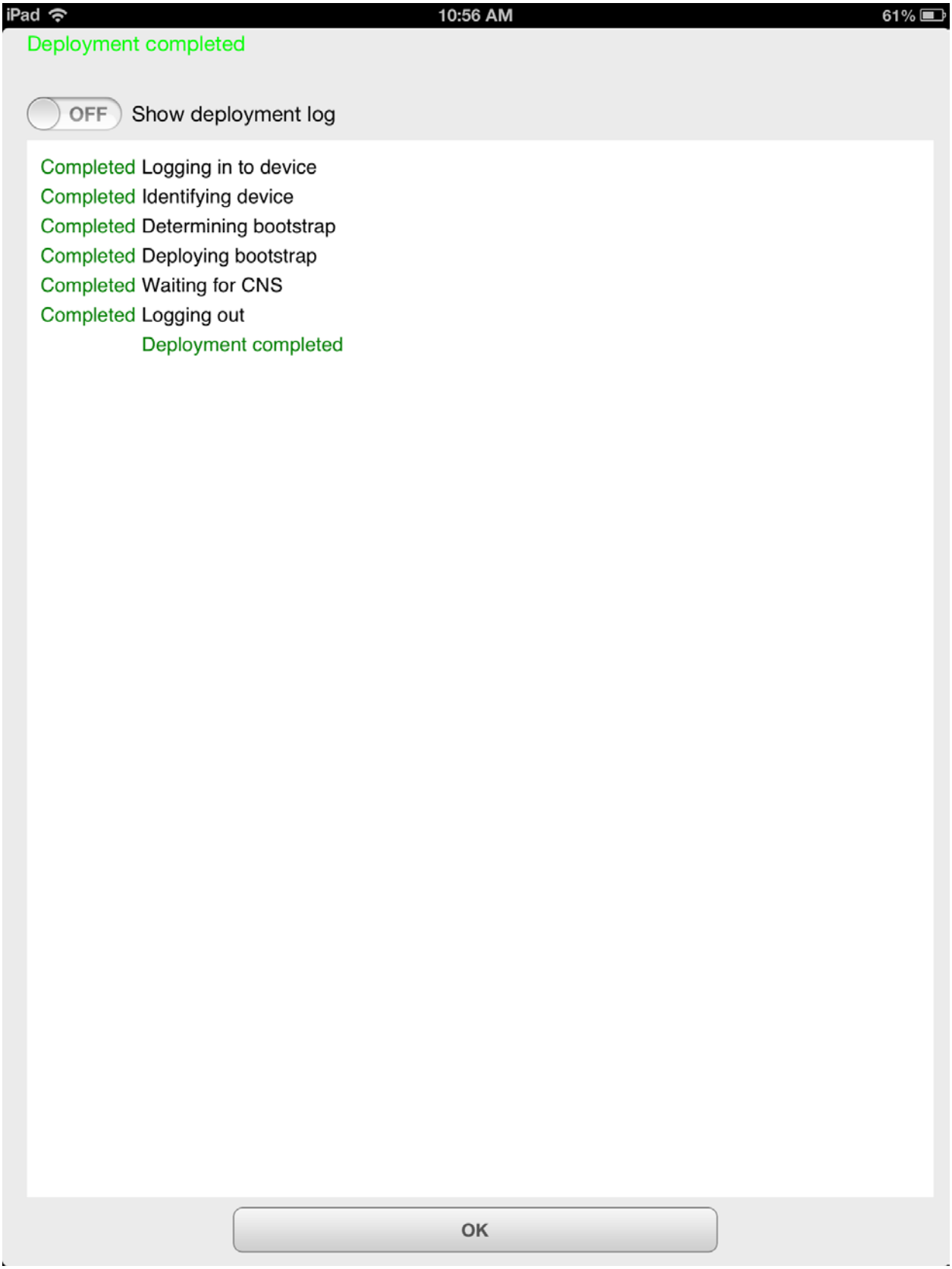


図 22 Cisco プラグ アンド プレイ アプリケーションの導入の状態

注:画面上部左角の [Show Deployment Logs] の [ON]/[OFF] スライダーを使用して、導入が進行中でもログを参照できます。

設定をダウンロードし、導入を後で実行するには、次に示す手順に従います。そのリモート ブランチ自体から Cisco Prime プラグ アンド プレイ ゲートウェイに対するネットワーク接続がデバイスにまったくない場合は、この手順を使用します。

手順 1 導入アプリケーションを開始します。

手順 2 最初の起動画面で、[Settings] をクリックします。

手順 3 Cisco Prime プラグ アンド プレイ ゲートウェイのアドレスを指定します。

手順 4 Cisco Prime Infrastructure のユーザ名およびパスワードを指定します。

Cisco Prime Infrastructure に適切な特権を**所有**する**非 root** ユーザを作成することを推奨します。ユーザの作成および特権の割り当ての詳細については、『Cisco Prime Infrastructure User Guide』を参照してください。

手順 5 [Test Connection] をクリックして、デバイスがサーバに接続できること確認します。サーバ エントリの定義が必要なのは Cisco プラグ アンド プレイ アプリケーションを初めて使用するときだけで、その後はサーバ情報を保存しています。

手順 6 [Download] アイコンをクリックして導入を開始します。

手順 7 入力を促された場合は、**PIN 番号**を入力します。ブートストラップ設定がダウンロードされデバイスにローカルに保存されます。

手順 8 導入を開始する準備ができている場合 [Deply] アイコンをクリックするか [Start Deployment] をクリックします(および、サーバへの接続が使用できる場合は上に概要を示した手順に従ってください)。

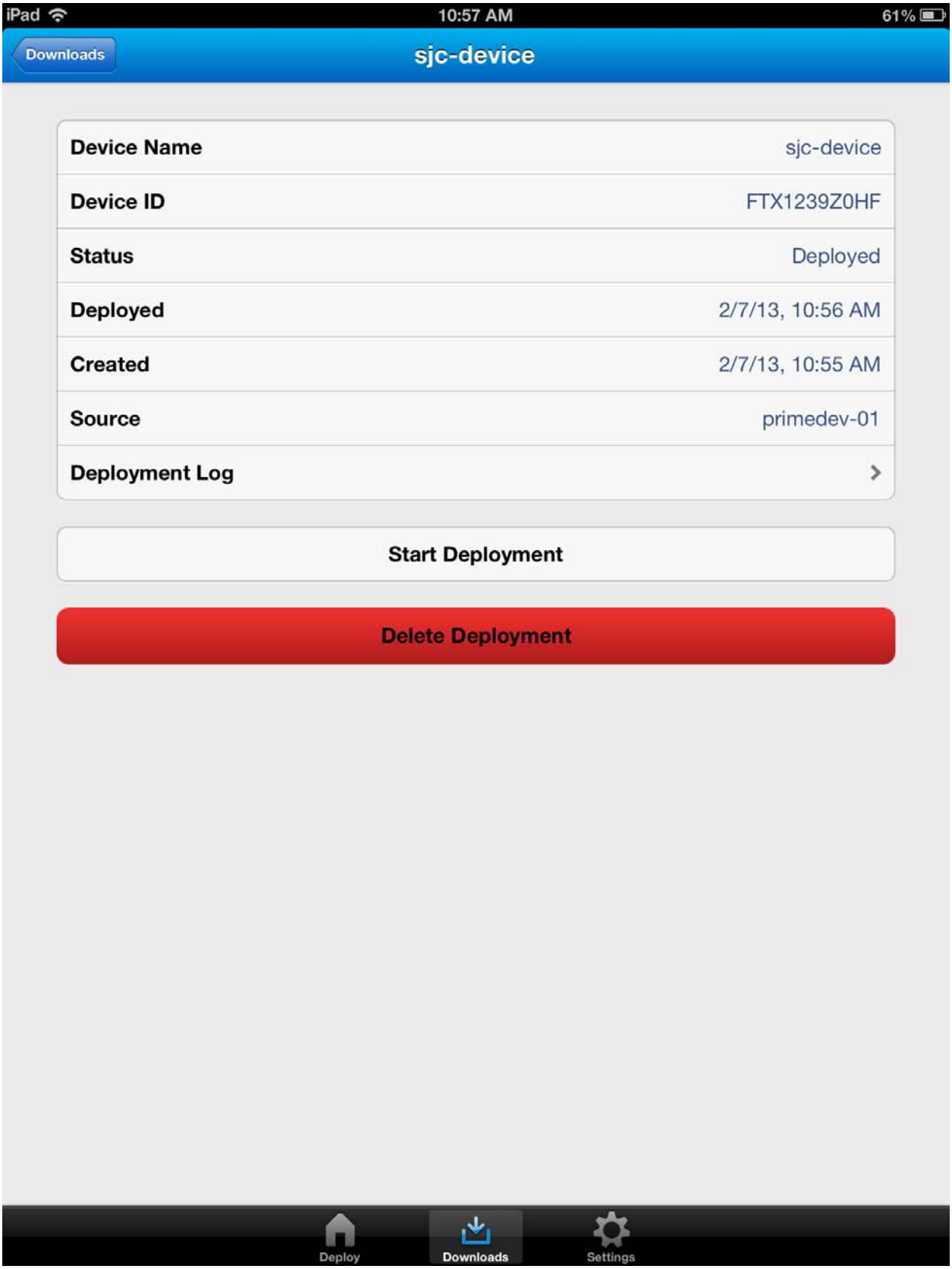


図 23 Cisco プラグ アンド プレイ アプリケーション：[Downloads] ページからのデバイス導入の開始

トラブルシューティング情報

この項では、導入時に発生する可能性のある共通のセルフ ヘルプ トピックまたは問題を扱います。さらに援助が必要な場合は、Cisco TAC にご連絡ください。

推奨バージョン

すべての問題の解決の重要な最初のステップとしてこのバージョンの推奨事項に従ってください。

- 通常、統合された Cisco プラグ アンド プレイ ソリューション向けには Cisco Prime Infrastructure のバージョン 2.0 以降を推奨します。
- Cisco プラグ アンド プレイ アプリケーションは Cisco Prime Infrastructure のバージョン 1.3 以降をサポートします。Cisco プラグ アンド プレイ アプリケーションは Cisco Prime Infrastructure のバージョン 1.2 とは機能しません。ただし、Cisco Prime Infrastructure 1.2 のカスタマー向けには、ブートストラップを適用する他の仕組み（例：エクスポート、TFTP、電子メール、USB フラッシュなど）がまだ使用可能です。Cisco プラグ アンド プレイ モバイル アプリケーションは、iOS バージョン 6.0 以上の下で動作する必要があります。
- Cisco プラグ アンド プレイ Windows PC アプリケーションは、Windows XP または Windows 7. にインストールする必要があります。
- デバイスに組み込まれた CNS エージェントと優れた互換性を確保するためシスコ デバイスの IOS のバージョンは 12.3 以上である必要があります。

インストールとセットアップの問題

Cisco プラグ アンド プレイ ソリューション コンポーネントを使用するときの、インストール上のヒントまたはセットアップに関する問題については、このセクションを使用してください。

- **Cisco Prime Infrastructure バージョン 1.2**：
  - Cisco Prime Infrastructure 1.2 にはサーバ証明書を外部の VM にエクスポートする CLI はありません。
    - **オプション 1**：
      Cisco Prime Infrastructure VM から証明書を取得するには Cisco プラグ アンド プレイ ゲートウェイ VM から次のコマンドを使用します。

      手順 1： 管理者証明書を使用して Cisco プラグ アンド プレイ ゲートウェイ VM にログインします。

      手順 2： 次のコマンドを実行します。次のコマンドを実行する前に Cisco Prime Infrastructure サーバが起動し実行していることを確認します。

      “*openssl s_client -connect "PI_MOM_HOST_NAME:61617" 2>&1 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > ncsserver.crt*”

      注：PI_MOM_HOST_NAME を Cisco Prime Infrastructure サーバの IP アドレスまたはホスト名に置き換えます。このコマンドは、Prime Infrastructure 証明書を「ncsserver.crt」と呼ばれるファイルに保存します。「pnp setup」コマンドで証明書をインポートする際にこのファイルを使用します。

- **オプション 2:**
  Internet Exporter、Mozilla Firefox などなんらかの Web ブラウザを使用して、Cisco Prime Infrastructure のセキュア Web URL にアクセスしてください（例: https://prime-server）。サーバ証明書を受け入れる警告ダイアログが表示されます。この時点で、証明書を表示してファイルにエクスポートするためにクリックします。Cisco プラグ アンド プレイ ゲートウェイ VM を使用し、「copy」CLI を使ってこの証明書を取得します。「pnp setup」コマンドで証明書をインポートする際にこの CLI を使用します。

  このセットアップ手順は、Prime Infrastructure 2.0 バージョンでは必要ありません。Cisco プラグ アンド プレイ ゲートウェイは、セットアップ コマンドの実行中にサーバ証明書のエクスポートを処理します。

- Cisco Prime Infrastructure サーバは常にインストールされている必要があり、Cisco プラグ アンド プレイのゲートウェイの個別の DMZ インストールの実施前に必ず起動して動作している必要があります。
- サーバのインストールの詳細については『Cisco Prime Infrastructure Quick Start Guide』および『Cisco Prime Infrastructure User Guide』を参照してください。
- Cisco プラグ アンド プレイ コマンドまたは CLI の詳細については、『Cisco Prime Infrastructure Command Reference Guide』を参照してください。

接続性の問題

Cisco Prime Infrastructure および Cisco プラグ アンド プレイ ゲートウェイが別のマシンにインストールされている場合は、これらのサーバ間で IP 接続されていることを確認します。

- Cisco Prime Infrastructure と Cisco プラグ アンド プレイ ゲートウェイ間で IP 接続が存在することを確認します。次のコマンドを実行して接続を確認します。
  "netstat -an | grep EST | grep 61617"
  出力がない場合、確立された接続がないことを意味します。Cisco プラグ アンド プレイ ゲートウェイまたは Cisco Prime Infrastructure サーバのいずれかが機能していないか起動していません。次のリストされている順序でサーバを再起動します。
- サーバを始動および再起動するための正しい順序に従います。Cisco Prime Infrastructure が常に最初に起動され、Cisco プラグ アンド プレイ ゲートウェイより前に始動する必要があります。Cisco Prime Infrastructure が何らかの理由で再起動すると、Cisco プラグ アンド プレイ ゲートウェイ サーバもまた再起動する必要があります。両方のサーバは常に同期させる必要があります。
- Cisco プラグ アンド プレイ ゲートウェイが DMZ ゾーンにインストールされている場合は、ファイアウォー上に必要なポートを確実に開くようにする必要があります。これらのポートが開くと、Cisco プラグ アンド プレイ ゲートウェイはシスコ デバイスからイベントを受信できます。Cisco プラグ アンド プレイ ゲートウェイでは、次のポートがファイアウォールで開いている必要があります。

    - 11011 ～ 11022（Cisco プラグ アンド プレイ ゲートウェイでの「*pnp status*」の出力ですべてのポートが表示される）
    - 8080
    - 8443
    - 8045
    - FTP ポート/データ ポート（FTP のメッセージ交換の一部）
- シスコ デバイスが Cisco プラグ アンド プレイ ゲートウェイに ping を送信できるか、そしてこれらの間に IP 接続が存在するのかを確認します。

サーバの状態の確認

Cisco プラグ アンド プレイ サーバが動作していることを確認するには、次のコマンドを使用します。

Cisco **プラグ アンド プレイ ゲートウェイ サーバ**:（個別のインストールのみ）

"PNP {status|start|stop|restart|reload|enable|disable}"

すべてが OK の場合、コマンド出力は、「Plug and Play Gateway is running」と表示されます。出力に問題が表示された場合、問題が発生した場合は、Cisco プラグ アンド プレイのゲートウェイを再起動します。

出力例:

Plug and Play Gateway is running.

Prime Infrastructure サーバ:

Cisco Prime Infrastructure サーバの状態を確認するには、次のコマンドを使用します。また、Cisco プラグ アンド プレイ ゲートウェイと単一ボックスにインストールされている場合、または非 DMZ 導入の場合、Cisco プラグ アンド プレイ ゲートウェイの状態も含まれます。

「ncs status」

出力例:

Health Monitor Server is running.

Compliance engine is running.

Ftp Server is running

Database server is running

Tftp Server is running

Matlab Server is running

NMS Server is running.

Plug and Play Gateway is running.

SAM Daemon is running ...

DA Daemon is running ...

Syslog Daemon is running ...

ログの収集

ログは、すべての問題の詳細なトラブルシューティングおよび Cisco TAC への連絡で役に立ちます。

Cisco プラグ アンド プレイ ゲートウェイ:（分けてインストールされている場合のみ）

Cisco プラグ アンド プレイ ゲートウェイが分けてインストールされている VM では次のコマンドを使用します。VM からログ ファイルを取得するために「*Copy*」コマンドを使用します。

admin# pnp tech log

The System Status file created: /localdisk/20121003032209.pnp_systemmonitor.tar.gz

Cisco Prime Infrastructure サーバ:

[Administration] > [Log Setting] に移動し、ログ ファイルをダウンロードします。

Cisco プラグ アンド プレイ iOS アプリケーション（iPhone/iPad モバイル アプリ）

ログを送信できるようにする前に、iPhone/iPad で電子メール設定を設定しておく必要があります。アプリで [Settings] アイコンをクリックし、サポート ログを電子メールで送信するために [Email Support Logs] オプションを使用します。アプリケーションは、汎用アプリケーションの問題に関して Cisco TAC にログを送信するように設定した電子メール アカウントを使用します。

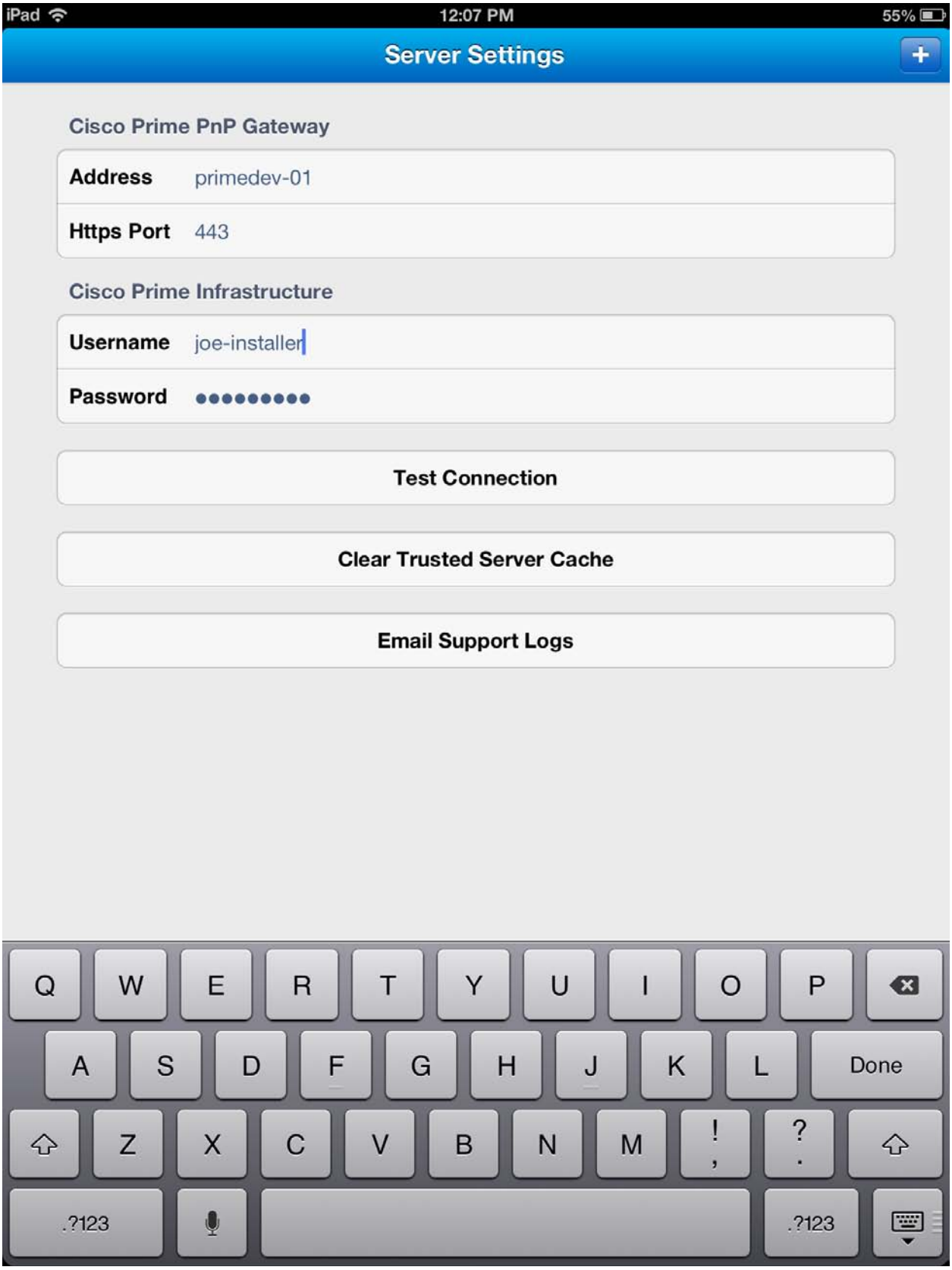
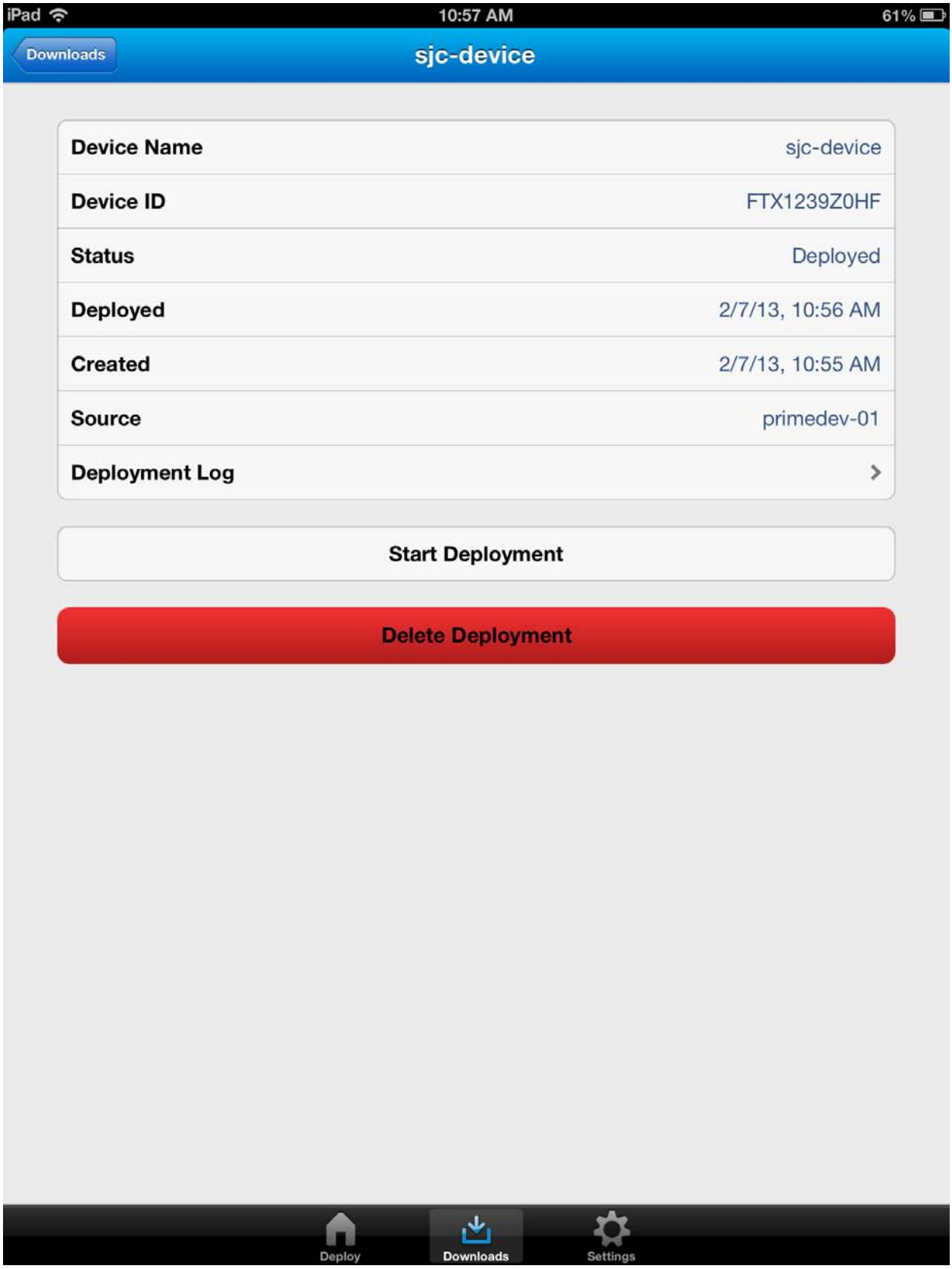


図 24 Cisco プラグ アンド プレイ アプリケーション：サポート ログの電子メール送信

また、任意の一般的なアプリの問題でデバイス導入ログをネットワーク管理者または Cisco TAC に送信できます。

下のスクリーン ショットで、デバイス導入ログごとのアクセスについて説明します。[Deployment Logs] オプションをスワイプして電子メールのオプションを表示する必要があります。


iPad
10:57 AM
61%
Downloads
sjc-device
Device Name
sjc-device
Device ID
FTX1239Z0HF
Status
Deployed
Deployed
2/7/13, 10:56 AM
Created
2/7/13, 10:55 AM
Source
primedev-01
Deployment Log
Start Deployment
Delete Deployment
Deploy
Downloads
Settings

ログ表示をイネーブル/ディセーブルにするオプションを使用して進行中の導入の状態をモニタすることができます。

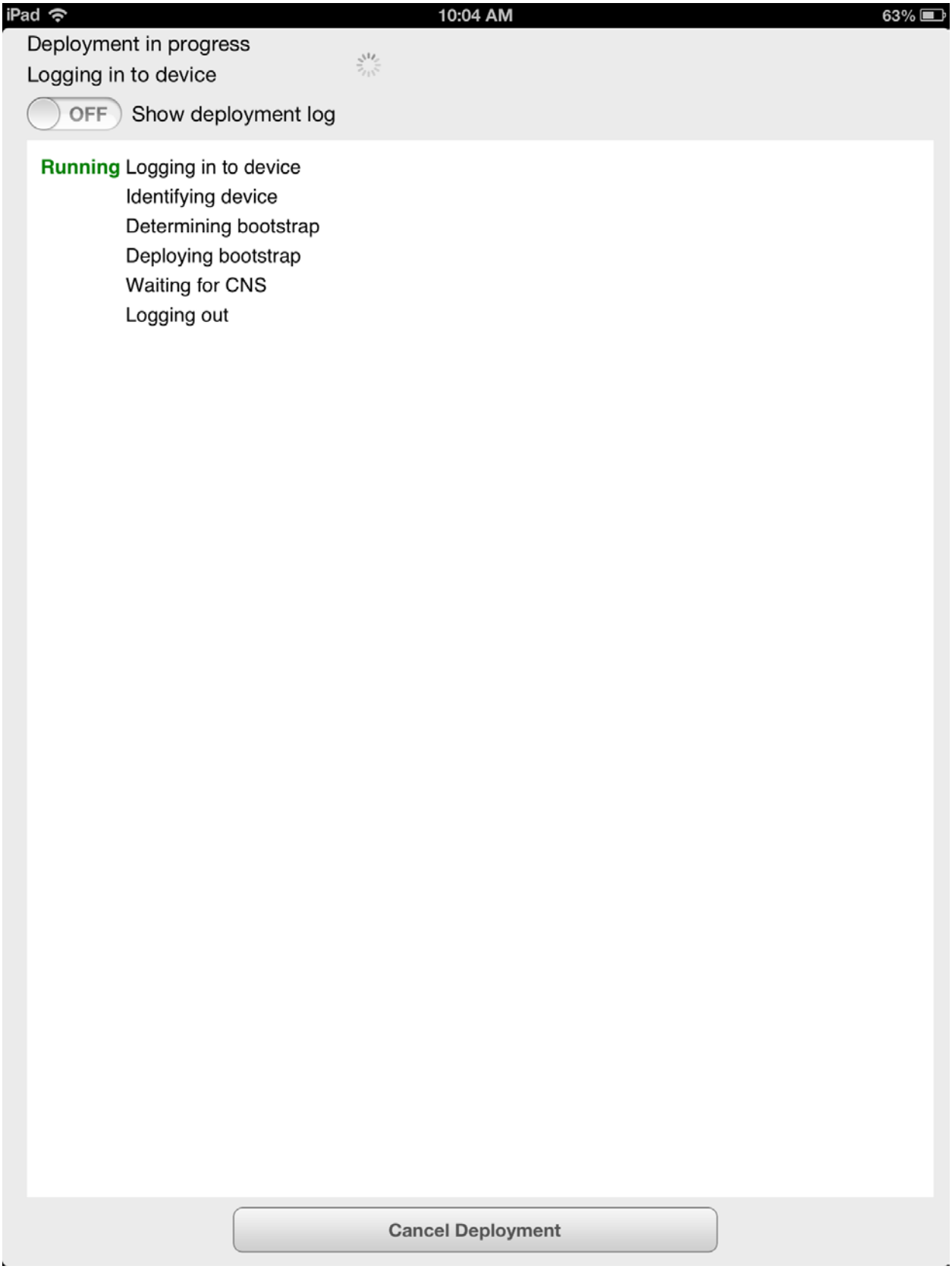


図 25 Cisco プラグ アンド プレイ アプリケーション上での導入状態のモニタリング

Cisco プラグ アンド プレイ PC アプリケーション（Windows アプリケーション）

Windows の Cisco プラグ アンド プレイ アプリケーションには、電子メール オプションが組み込まれていません。ログを収集するにはメニュー オプションを使用する必要があります。ログは、圧縮された ZIP ファイル形式であり、汎用アプリケーションの問題に関して、ネットワーク管理者または Cisco TAC に電子メールを送信できます。デバイス導入ログはアプリケーション上の [Deploy] または [Download] オプションで収集して、ネットワーク管理者に送信できます。

Cisco CNS エージェントを搭載した Cisco ルータ/スイッチ

この項では、Cisco CNS エージェントがそのデバイスで実行されているシスコ デバイスでの問題のトラブルシューティングについて説明します。

ここにリストされているすべてのコマンドの詳細なヘルプについては、『Cisco CNS Documentation』を参照してください。

- CNS ログの有効化およびデバッグ出力のキャプチャ
  Router> config t
  Router> enable
  Router> debug cns all
  Router> ter mon

- [*show cns event*] CLI を使用してアクティブな接続を表示します。
  Router#show cns event connections
  The currently configured primary event gateway:
  hostname is ciscoprimepnp.
  port number is 11013.
  encryption is disabled.
  Event-Id is FTX14068095
  Keepalive setting:
  keepalive timeout is 120.
  keepalive retry count is 2.
  Connection status:
  Connection Established.
- Cisco プラグ アンド プレイ アプリケーションが「Waiting for CNS initial CLI to be removed」の状態に陥った場合、このシスコ デバイスにログインし、[*cns event*] コマンドの no 形式を適用し、再度追加し直します。これによって、デバイスの CNS エージェントに問題がある場合に、Cisco プラグ アンド プレイ サーバに再度 Call Home がトリガーされることになります。
- プラグ アンド プレイ導入の状態は *[Operate] > [Plug and Play Status]* を使用して Cisco Prime Infrastructure サーバからリアルタイムでモニタできます。詳細な導入の状態が表示されます。稼働中のシスコ デバイスのエントリがない場合、ブートストラップがこのデバイスにまだ適用されていないことを示します。このマニュアルで前述したブートストラップ オプションの 1 つを使用して、導入をトリガーします。

すでに導入済みのデバイスの再導入

すでに導入済みのデバイスを再度導入するために、Cisco Prime Infrastructure 内の導入済みプロファイルをクリーン アップします。これを行わない場合、すでに導入されたデバイスを再導入することはできません。

Cisco Prime Infrastructure サーバからデバイスおよびプロファイルをクリーン アップするには、次の手順に従います。

手順 1: [operate] > [Plug and Play Status] に移動し、再展開するデバイスを削除(シリアル ID でデバイスを識別)します。

手順 2: [Deploy] > [Plug and Play Profiles] に移動し、プロファイルを選択します。

手順 3: [Unpublish] をクリックして、このプロファイルをアンパブリッシュします。

手順 4: [Deploy] をクリックし、プロファイルにリストされたデバイスを選択します。

手順 5: [Delete] をクリックして、デバイスを削除します。

手順 6: [Feature] > [Plug and Play Profiles] > に移動し、プロファイルを選択し、マウスをその上に移動します。プロファイルを削除するには [Delete] をクリックします。

参照

- 『Cisco Prime Infrastructure Quick Start Guide』
- 『Cisco Prime Infrastructure User Guide』
- 『Cisco Prime Infrastructure Command/CLI Reference Guide』(プラグ アンド プレイ関連コマンド/CLI を含む)
- 『Cisco Plug and Play Application Deployment User Guide』
- 『Cisco Auto Install Guide』
- 『Cisco Smart Install Guide』
- 『Cisco IOS CNS Documentation』
- 『Cisco IOS CNS CLI』
- 『Cisco IOS Auto Install Feature』
- 『Cisco Commerce Workplace (CCW) integrated, Cisco Integrated Customization Services (CICS) for ISR G2』
- 『Cisco Configuration Professional Quick Start Guide』
- 『Cisco Configuration Professional Express (CCP Express) version 2.7 Plug and Play Settings』

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/