

デバイスの新しいPnP証明書を生成する方法

内容

外部のお客様/パートナー様専用：これらの手順は、お客様/パートナー様が問題を解決するための措置を自ら実行する際に役立ちます。お客様やパートナーが手順の問題に遭遇した場合は、ライセンスサポート(<https://www.cisco.com/go/scm>)でケースをオープンして解決してください。ライセンスサポートチーム以外の社内シスコリソースを使用している場合は、これらの操作を自分で行わないでください。

作業を開始する前に、次の点を確認してください。

- アクティブなCisco.comアカウント
- スマートアカウントとバーチャルアカウント
- 明示的なSA管理またはVA管理アクセスが必要です。

ステップ1:[Cisco Software Central](#)に移動し、Cisco.comクレデンシャルを使用してログインします

ステップ2：右上隅のスマートアカウントセレクトからスマートアカウントを選択します

ステップ3：ネットワークプラグアンドプレイの下にあるデバイスの管理をクリックします

ステップ4：バーチャルアカウントセレクトからバーチャルアカウントを選択します

ステップ5:[証明書]タブに移動します

ステップ6:+Generate Certificateをクリックします。

ステップ7：必要な情報（証明書名、署名機関、有効期間など）を入力し、Nextをクリックします

ステップ8：確認と送信



注：ダウンロードされるファイルは、証明書の有効性の詳細が記載された.cerファイルです。この有効期間は、証明書の作成時に入力した有効期間と一致します。



注：ユーザがスマートアカウント管理者ではない場合、仮想アカウントごとに1000の証明書を生成することに制限があります。

トラブルシューティング：

このプロセスで対処できない問題が発生した場合、ソフトウェアライセンスオプションを使用して[Support Case Manager\(SCM\)](#)（登録ユーザ専用）でケースをオープンしてください。

このドキュメントの内容についてのご意見は、[ここ](#)から送信してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。