SPA2102、SPA3102 および SPA9000 によるリモート プロビジョニングに基づく HTTPS

目次

概要

この記事は、Cisco Small Business 製品（以前の Linksys Business シリーズ）のセットアップ、トラブルシューティング、およびメンテナンスを支援するドキュメントの 1 つです。

Q. SPA2102、SPA3102、および SPA9000 を使用して HTTPS サーバに認証できません。 この問題の原因は何ですか?

A.

2005 年 11 月 15 日から 2006 年 6 月 15 日までに製造された一部の SPA2102、SPA3102、および SPA9000 デバイスでは、クライアント証明書が正しくインストールされていません。 この問題により HTTPS プロビジョニング機能が影響を受けます。

誤った証明書がインストールされているデバイスでは、HTTPS サーバとの ***クライアント認証*** が失敗します。

ただし、この問題によりデバイスの適切な機能（HTTPS サーバ認証、すべての電話機能、リモート ファームウェア アップグレード、TFTP および HTTP ベースのプロビジョニングなど）に影響が及ぶことはありません。 TFTP または HTTP を介して暗号化プロビジョニング ファイルを伝送することにより、セキュア プロビジョニングを実行できます。 さらに、暗号化された音声機能も影響を受けません。

次のシリアル番号範囲に含まれる一部（全部ではない）のデバイスに、誤ったクライアント証明書がインストールされています。

製品	シリアル番号の範囲
SPA2102	FM500F100000 ~ FM500F699999
?SPA3102	?FM600F100000 ~ FM600F699999
SPA9000	FM700F100000 ~ FM700F699999

ご使用のデバイスにこの欠陥があり、デバイスをリモート プロビジョニングする必要がある場合には、次の選択肢のいずれかを実行できます。

暗号化されたプロビジョニング プロファイルで HTTP または TFTP ベースのプロビジョニングを使用します。
以下の設定で HTTPS プロビジョニングを使用します。
サーバ認証を有効化、
クライアント認証を無効化、または
暗号化されたプロビジョニング プロファイル（Linksys SPC ツールまたは openssl を介して暗号化される）。

現在では、正しいクライアント証明書がインストールされているデバイスをご利用いただけます。

関連情報

- テクニカル サポートとドキュメント：Cisco Systems