HTTPS Based Remote Provisioning with the SPA2102, SPA3102, and SPA9000

Document ID: 108605

Contents

Introduction

This article is one in a series to assist in the setup, troubleshooting, and maintenance of Cisco Small Business products (formerly Linksys Business Series).

Q. I am unable to authenticate to an HTTPS server using the SPA2102, SPA3102, and SPA9000. What is the problem?

A.

The client certificates on some SPA2102, SPA3102, and SPA9000 devices manufactured between ***November 15, 2005*** and ***June 15, 2006*** were installed incorrectly. This defect affects the HTTPS provisioning feature.

The devices with incorrect certificates will fail ***client authentication*** with an HTTPS server.

This defect, however, does NOT affect proper functionality of the devices, including HTTPS server authentication, all telephony functions, remote firmware upgrades, and TFTP and HTTP based provisioning. Secure provisioning can be performed by transmitting encrypted provisioning files via TFTP or HTTP. The encrypted voice function is also not affected.

Some, but not all, of the devices in the following ranges of serial numbers have incorrect client certificates:

Product	***Range of Serial Numbers***
SPA2102	FM500F100000 − FM500F699999
?SPA3102	?FM600F100000 − FM600F699999
SPA9000	FM700F100000 − FM700F699999

If your device has this flaw, and the device needs to be remotely provisioned, you may take one of the following actions:

- Use HTTP or TFTP based provisioning with encrypted provisioning profiles.
- Use HTTPS provisioning with:
    - ♦ server authentication enabled,
    - ♦ client authentication disabled, or
    - ♦ encrypted provisioning profiles (encrypted via the Linksys SPC tool or openssl).

Devices with correctly installed client certificates are currently available.

Related Information

- **Technical Support &Documentation − Cisco Systems.**

Updated: Dec 12, 2008 Document ID: 108605