Einrichten des SP-Adapters

für die Verwendung mit einem RADIUS-Server

Version 1.0
02.11.2016

Impressum

Akademie des Deutschen Kraftfahrzeuggewerbes GmbH (TAK)
Franz-Lohe-Str. 19
53129 Bonn

Kontakt

Kunden von SP Plus oder dem SP Vorgabenmodul können uns bei Fragen zur Einrichtung, der Konfiguration, bei Softwareupdates oder Hardwaredefekten unter folgenden Kanälen erreichen:

Web: www.sp-adapter.de www.spplus.de www.sp-vorgabenmodul.de
E-Mail: support@sp-adapter.de
Hotline: 0228/91 27 148 (Montag bis Freitag von 09:00 - 12:00 Uhr und 13:00 - 16:00 Uhr)

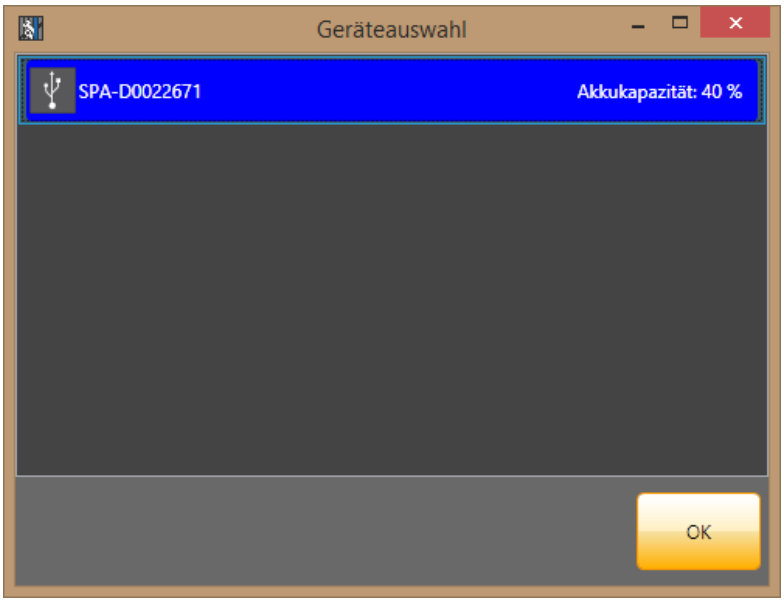
Konfiguration des SP-Adapters über HUAadmin

Die erweiterte Konfiguration für die Verbindung des SP-Adapters mit einem RADISU Server ist nur über das FSD-Tool HUAadmin und nicht über das vereinfachte WLAN-Konfigurationstool möglich.

Verbinden Sie für die Konfiguration den SP-Adapter zuerst über das Steckernetzteil mit der Stromversorgung. Danach verbinden Sie den SP-Adapter über das mitgelieferte USB-Kabel mit dem Bedienrechner.

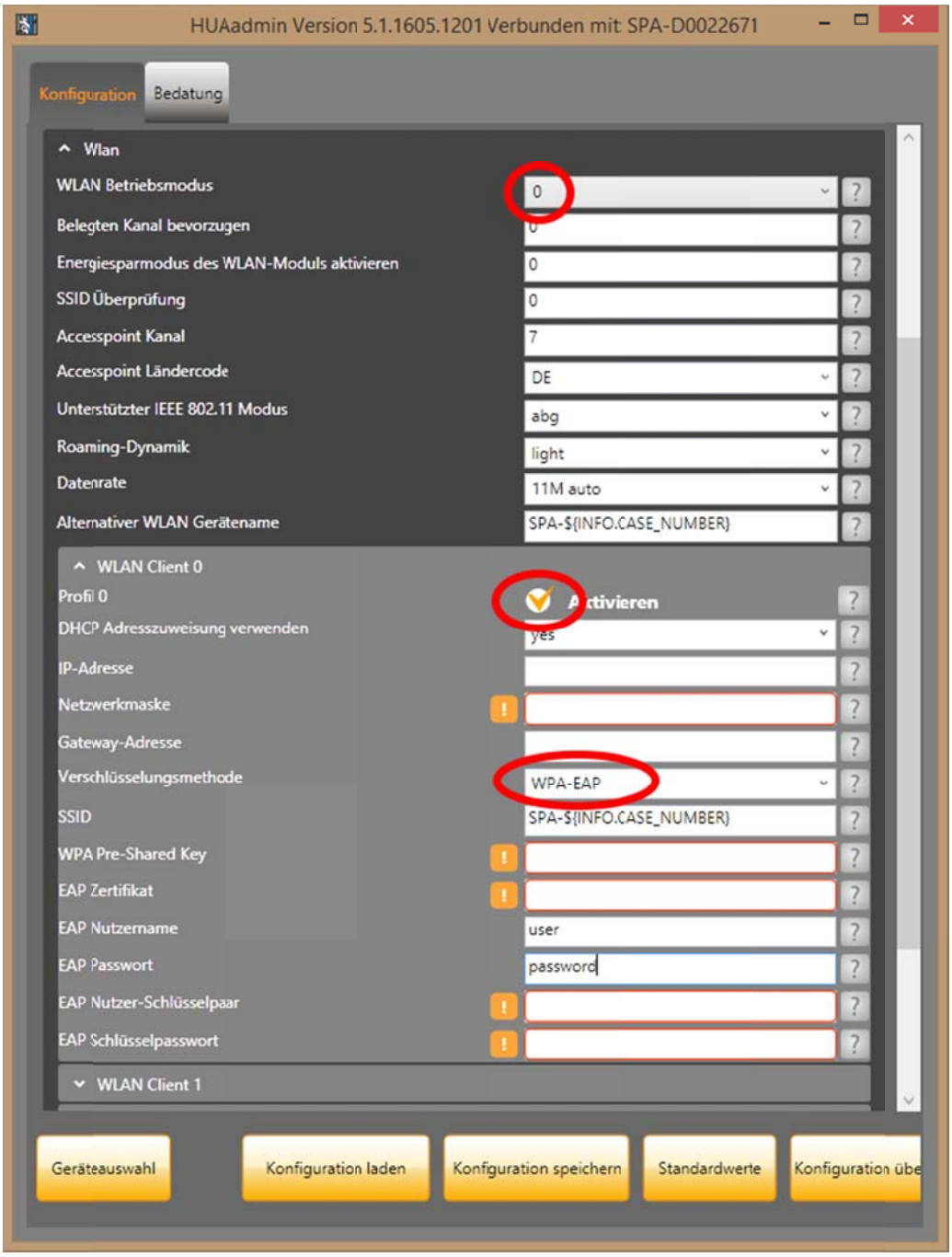
Starten Sie nun die HUAadmin.exe aus dem Unterverzeichnis

SPPlus\FSD.SP21\Interface\HUAadmin und verbinden Sie sich mit dem SP-Adapter.



Stellen Sie folgende Parameter ein:

- WLAN-Betriebsmodus auf 0 für 'Infrastruktur' stellen.
- WLAN Client 0
  - Profil 0 aktivieren
  - Verschlüsselungsmethode WPA-EAP
  - EAP Nutzername und Kennwort



Danach kann die Einstellung über die Schaltfläche 'Konfiguration übertragen' auf den SP-Adapter übertragen werden.

WPA2-verschlüsseltes Netzwerk mit Extensible Authentication Protocol (EAP)

Die Verwendung des Extensible Authentication Protocol (EAP) setzt voraus, dass im Netz ein Remote Authentication Dial-In User Service (RADIUS) Server vorhanden ist, der die Authentifizierung der Netzteilnehmer durchführt, bevor diese Zugang zum Netz erhalten. Diese erweiterte Sicherheit ist nur im Infrastruktur-Modus verfügbar. Der SP-Adapter kann selbst keine RADIUS-Authentifizierung bereitstellen.

Um die Identität des SP-Adapters als berechtigten Netzteilnehmer einzurichten, stehen die Optionen Protected EAP (PEAP) und EAP-Transport Layer Security (EAP-TLS) zur Verfügung. Bei PEAP wird der Netzteilnehmer durch eine Kombination aus Nutzername und Kennwort authentifiziert, bei EAP-TLS durch eine Kombination aus Nutzername und einem Zertifikat, welches mit einem Passwort geschützt sein kann. Der SP-Adapter unterscheidet den anzuwendenden Authentifizierungsmechanismus in Abhängigkeit der vorgenommenen Parametrierung.

Für ein Netz mit WPA2-Verschlüsselung und EAP muss die Verschlüsselungsmethode auf WPA-EAP gestellt werden.

Damit sichergestellt ist, dass sich der SP-Adapter nur mit dem richtigen RADIUS-Server verbindet, muss der öffentliche Schlüssel der Zertifizierungsstelle mit auf das Gerät übertragen werden. Dazu muss der Schlüssel als Datei im PEM oder DER Format vorliegen und über EAP Zertifikat referenziert werden. Der Benutzername für die Anmeldung am RADIUS-Server muss unabhängig von der verwendeten Authentifizierungsmethode über EAP Nutzername angegeben werden.

Der Ursprungspfad der verwendeten Zertifikate wird nicht auf dem SP-Adapter gespeichert, ein Auslesen der auf das Gerät gebrachten Zertifikate ist nicht möglich, so dass auch kein Abgleich der ggf. bereits installierten Zertifikate und der im Dateisystem referenzierten Zertifikate stattfindet. Zum Aufbringen neuer Zertifikate auf den SP-Adapter sollte deshalb die Gerätekonfiguration unter Verwendung von *HUAadmin* (Ändern der Gerätekonfiguration) neu geschrieben werden, die FSD Informationssysteme erneuern die Zertifikate nur, wenn sich neben den Zertifikatdateien auch andere Parameter der Gerätekonfiguration ändern.

WPA2-verschlüsseltes Netzwerk mit PEAP

Für die Authentifizierung mittels PEAP muss zusätzlich zum Nutzernamen das Passwort des Nutzers über den Parameter EAP Passwort angegeben werden. Durch das Setzen dieses Parameters erkennt der SP-Adapter automatisch den zu verwendenden Authentifizierungsmodus.

WPA2-verschlüsseltes Netzwerk mit EAP-TLS

Für die Authentifizierung mittels EAP-TLS muss zusätzlich zum Nutzernamen das Nutzerzertifikat über den Parameter EAP Nutzer-Schlüsselpaar referenziert werden. Dieses muss als Datei im PEM, DER oder PFX-Format vorliegen. Der private Schlüssel des Zertifikats kann dabei durch ein Passwort geschützt, dieses muss im Parameter EAP Schlüsselpasswort angegeben werden.