LCOS LX 6.12

Addendum

07/2023

LANCOM
SYSTEMS

Inhalt

1 Addendum zur LCOS LX-Version 6.12....4
2 LED-Signalisierung bei unzureichender Stromversorgung....5
3 Client-Modus für flexible Einbindung von Ethernet-fähigen Geräten in WLAN-Netze....6
3.1 Verbindungen....6
3.2 RADIUS-Client....7
3.3 Roaming....8
3.4 WEBconfig: WDS (Wireless Distribution System) / Punkt-zu-Punkt-Verbindungen....9
3.4.1 Verbindungen....9
3.4.2 RADIUS-Clientprofile....10
3.4.3 Roamingprofile....11
3.4.4 Client-Zertifikat....11
3.5 Ergänzungen im Setup-Menü....11
3.5.1 Mode....11
3.5.2 Encryption-Profile....12
3.5.3 Encryption-Key....12
3.5.4 LCOS-Client-Bridge-Support....13
3.5.5 Roaming-Profile....13
3.5.6 RADIUS-Client-Profile....14
3.5.7 Roaming....14
3.5.8 Delete-WLAN-Supplicant-Certificates....15
3.5.9 WLAN-Supplicant....16

Copyright

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS LX) finden Sie über die Kommandozeile mit dem Befehl `show 3rd-party-licenses`. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Wenden Sie sich hierzu via E-Mail an *gpl@lancom.de*.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (*www.openssl.org*).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS LX-Version 6.12

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS LX-Version 6.12 gegenüber der vorherigen Version.

2 LED-Signalisierung bei unzureichender Stromversorgung

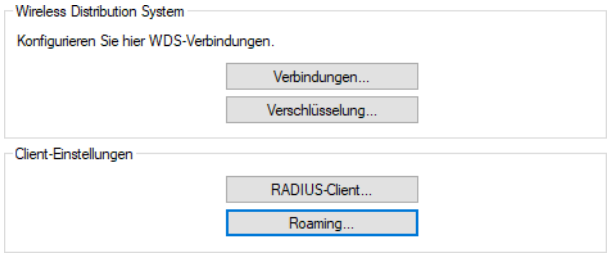
Ab LCOS LX 6.12 wird eine unzureichende Stromversorgung angezeigt.

Bei Geräten, die für volle Funktionalität (z. B. Aktivierung aller WLAN-Streams) PoE 802.3bt benötigen, wird über eine dauerhaft gelb leuchtende Power-LED signalisiert, dass eine unzureichende Stromversorgung vorliegt.

3 Client-Modus für flexible Einbindung von Ethernet-fähigen Geräten in WLAN-Netze

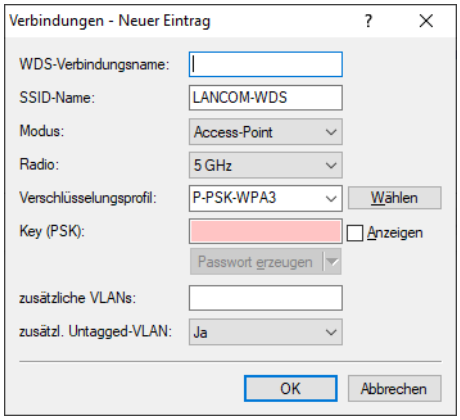
Ihre LCOS LX-basierten Access Points unterstützen ab sofort den Client-Modus. Verwenden Sie Ihre LCOS LX-basierten Access Points von nun an flexibel für die Einbindung vielfältiger Ethernet-fähiger Geräte in bestehende WLAN-Netzwerke – betriebssystem- und somit herstellerunabhängig. Für passgenaue Sicherheit wählen Sie zwischen zertifikatsbasiert verschlüsselter Kommunikation über IEEE 802.1X oder über WPA2/3-PSK.

WLAN-Client-Verbindungen sind technisch ähnlich zu WDS-Verbindungen und werden deshalb an der gleichen Stelle konfiguriert. Dazu gibt es in LANconfig die folgenden geänderten bzw. neuen Einstellungen unter **Wireless-LAN** > **WDS**.



3.1 Verbindungen

Konfigurieren Sie unter **Wireless-LAN** > **WDS** > **Verbindungen** alle generellen Einstellungen rund um die WDS-Verbindung. Fügen Sie je WDS-Verbindung eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.



Modus

Im Rahmen einer WDS-Verbindung gibt es drei Rollen: Access Point, Client, Legacy Client. Der als Client konfigurierte Partner sucht anhand der oben konfigurierten SSID einen als Access Point konfigurierten Partner und initiiert die Verbindung. Der als Legacy-Client konfigurierte Access Point kann sich in die SSID eines beliebigen Access Points einbuchen.

Im Rahmen eines Punkt-zu-Multipunkt-Szenarios können sich mehrere Clients zu einem Access Point verbinden.

Die Menge aus regulären konfigurierten SSIDs für die Client-Anbindung sowie konfigurierten WDS-Verbindungen kann die Menge an insgesamt durch das jeweilige Gerätemodell unterstützen SSIDs nicht überschreiten – es wird sozusagen dasselbe „SSID-Budget" verwendet.

Es können beliebig viele WDS-Verbindungen im Access Point-Modus betrieben werden (bis zur Ausschöpfung der o. g. Menge an technisch maximal möglichen SSIDs des Gerätemodells. Es kann jedoch nur eine WDS-Verbindung im Station-Modus je Gerät betrieben werden. Verbindungen im Access Point-Modus und Station-Modus (von letzterer nur eine) können gleichzeitig auf demselben Gerät betrieben werden.

Beachten Sie, dass für ein Punkt-zu-Multipunkt-Szenario in der Regel eine einzelne Verbindung im AP-Modus auf dem „Verteilerknoten" ausreichend ist.

Verschlüsselungsprofil

Das Verschlüsselungsprofil, welches für die WDS-Verbindung verwendet werden soll.

Key (PSK)

Der WPA-PSK, welcher für die WDS-Verbindung verwendet wird. Bei der Verwendung eines Verschlüsselungsprofils mit 802.1X, kann dieses Feld leer bleiben.

LCOS-Client-Bridge-Unterstützung

Wird der LCOS LX-Access Point im Client-Modus mit einem LCOS-Access Point im Basisstations-Modus verbunden, können hierfür weiterhin 4-Adress-Frames verwendet werden, was die Übertragung von VLANs oder MAC-Adressen ermöglicht. Dieser Modus kann nicht verwendet werden, wenn der LCOS LX-Access Point im Basisstations-Modus betrieben wird und ein LCOS-Access Point im Client-Modus an diesem eingebucht wird.

Roamingprofil

Hier können Sie ein Roaming-Profil eintragen, wenn der Access Point sich im Client- oder Legacy-Client-Modus befindet.

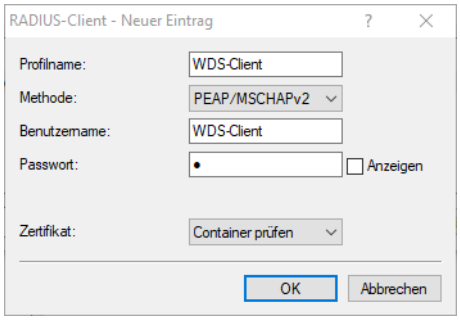
Konfigurieren Sie optional ein Verschlüsselungsprofil unter *Verschlüsselung*.

Möchten Sie eine Client-Verbindung mittels 802.1X aufbauen, konfigurieren Sie bitte zunächst ein RADIUS-Clientprofil. Siehe *RADIUS-Client* auf Seite 7.

Erstellen Sie bei Bedarf ein Roamingprofil. Siehe *Roaming* auf Seite 8.

3.2 RADIUS-Client

Die Einstellungen für ein Einbuchen mittels 802.1X werden unter **Wireless-LAN** > **WDS** > **Client-Einstellungen** > **RADIUS-Client** konfiguriert.



Profilname

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später im Verschlüsselungsprofil angeben.

Methode

Wählen Sie eine für Ihre Anforderung passende Methode aus. Bei der Verwendung von „TLS“ ist das Hochladen eines Zertifikates notwendig.

Benutzername

Tragen Sie hier den RADIUS-Benutzernamen ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Passwort

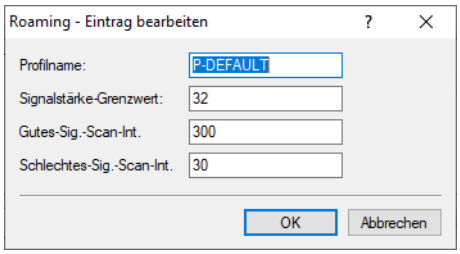
Tragen Sie hier das RADIUS-Passwort ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Zertifikat

Sie können das Zertifikat des RADIUS-Servers automatisch annehmen oder das hochgeladene Zertifikat prüfen lassen. Wir empfehlen immer, ein Zertifikat hochzuladen, um die Integrität des RADIUS-Servers zu verifizieren. Der Zertifikatupload ist nur in der WEBconfig möglich. Siehe *Client-Zertifikat* auf Seite 11.

3.3 Roaming

Die Einstellungen für das Roaming-Profil werden unter **Wireless-LAN** > **WDS** > **Client-Einstellungen** > **Roaming** konfiguriert.



Profilname

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später in der WDS-Verbindung angeben.

Signalstärke-Grenzwert

Tragen Sie hier den Schwellenwert ein, ab welchem sich das Scan-Intervall des Access Points verändern soll. Werte von 0 bis 100 geben einen Prozentwert an. Werte von -100 bis 0 sind in dbm.

Gutes-Signal-Scan-Intervall

Befindet sich die Signalstärke oberhalb des Grenzwertes, wird in dieser Zeit in Sekunden ein Scan durchgeführt, um zu prüfen, ob ein besserer Access Point zum Verbinden vorhanden wird.

Schlechtes-Signal-Scan-Intervall

Fällt die Signalstärke auf den angegebenen Grenzwert, wird direkt ein Scan ausgelöst, um nach einem besseren Access Point zu suchen. Ist kein besserer Access Point vorhanden, wird in der angegebenen Zeit in Sekunden weiter gesucht, bis eine Verbindung zu einem Access Point mit einer besseren Signalstärke verbunden werden konnte oder sich das Signal mit dem verbundenen Access Point wieder verbessert hat.

3.4 WEBconfig: WDS (Wireless Distribution System) / Punkt-zu-Punkt-Verbindungen

Sie erreichen diesen Bereich in der WEBconfig über den Punkt **WDS** in der Sidebar.

Mittels des WDS lassen sich Punkt-zu-Punkt-WLAN-Verbindungen zwischen Access Points aufbauen. Diese Verbindungen dienen als kabelloser Backhaul und ermöglichen so die Anbindung von abgesetzt betriebenen Access Points an den Rest des Netzwerks. So lässt sich beispielsweise die WLAN-Abdeckung auch in Bereichen sicher stellen, in denen keine Ethernet-Anbindung von Access Points möglich ist.

Die beteiligten Access Points können wahlweise ihrerseits SSIDs für die WLAN-Client-Anbindung anbieten („Repeater"-Betrieb) oder die kabellose Backhaul-Verbindung mit ihrem Ethernet-Port verbinden (Wireless Bridge).

3.4.1 Verbindungen

Konfigurieren Sie hier alle generellen Einstellungen rund um die WDS-Verbindung. Fügen Sie je WDS-Verbindung eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.

WDS-Verbindungsname

Der Name der Verbindung. Wird für die weitere Referenzierung in der Gerätekonfiguration verwendet.

SSID-Name

Der Name der speziellen SSID, die für die WDS-Verbindung verwendet wird. Dieser Name muss auf beiden Seiten der Verbindung übereinstimmen.

Modus

Im Rahmen einer WDS-Verbindung gibt es drei Rollen: Access Point, Client, Legacy Client. Der als Client konfigurierte Partner sucht anhand der oben konfigurierten SSID einen als Access Point konfigurierten Partner und initiiert die Verbindung. Der als Legacy-Client konfigurierte Access Point kann sich in die SSID eines beliebigen Access Points einbuchen.

Im Rahmen eines Punkt-zu-Multipunkt-Szenarios können sich mehrere Clients zu einem Access Point verbinden.

Die Menge aus regulären konfigurierten SSIDs für die Client-Anbindung sowie konfigurierten WDS-Verbindungen kann die Menge an insgesamt durch das jeweilige Gerätemodell unterstützen SSIDs nicht überschreiten – es wird sozusagen dasselbe „SSID-Budget" verwendet.

Es können beliebig viele WDS-Verbindungen im Access Point-Modus betrieben werden (bis zur Ausschöpfung der o. g. Menge an technisch maximal möglichen SSIDs des Gerätemodells. Es kann jedoch nur eine WDS-Verbindung im Station-Modus je Gerät betrieben werden. Verbindungen im Access Point-Modus und Station-Modus (von letzterer nur eine) können gleichzeitig auf demselben Gerät betrieben werden.

Beachten Sie, dass für ein Punkt-zu-Multipunkt-Szenario in der Regel eine einzelne Verbindung im AP-Modus auf dem „Verteilerknoten" ausreichend ist.

Radio

Das Frequenzband, welches für die WDS-Verbindung genutzt werden soll. Aus Kapazitätsgründen empfiehlt sich die Verwendung von 5 GHz oder 6 GHz (je nach Hardware-Fähigkeiten des verwendeten Gerätemodells).

Verschlüsselungsprofil

Das Verschlüsselungsprofil, welches für die WDS-Verbindung verwendet werden soll.

Key (PSK)

Der WPA-PSK, welcher für die WDS-Verbindung verwendet wird. Bei der Verwendung eines Verschlüsselungsprofils mit 802.1X, kann dieses Feld leer bleiben.

zusätzliche VLANs

Im Rahmen der WLAN-Konfiguration ist es möglich, einzelne SSIDs mit WDS-Verbindungen zu verknüpfen. Diese werden dann gebridget über die WDS-Verbindung zur Verfügung gestellt. Sollen zusätzliche, z. B. über Ethernet transportierte VLANs ebenfalls übertragen werden, können diese hier eingetragen werden (kommaseparierte Liste von VLAN-IDs [0-4095]).

zusätzl. untagged VLAN

Untagged-Pakete sollen übertragen werden.

LCOS-Client-Bridge-Unterstützung

Wird der LCOS LX-Access Point im Client-Modus mit einem LCOS-Access Point im Basisstations-Modus verbunden, können hierfür weiterhin 4-Adress-Frames verwendet werden, was die Übertragung von VLANs oder MAC-Adressen ermöglicht. Dieser Modus kann nicht verwendet werden, wenn der LCOS LX-Access Point im Basisstations-Modus betrieben wird und ein LCOS-Access Point im Client-Modus an diesem eingebucht wird.

Roamingprofil

Hier können Sie ein Roaming-Profil eintragen, wenn der Access Point sich im Client- oder Legacy-Client-Modus befindet.

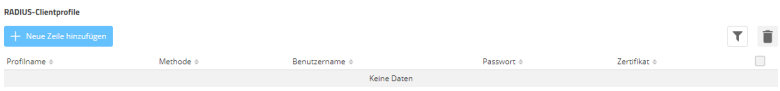
Konfigurieren Sie optional ein Verschlüsselungsprofil unter *Verschlüsselung*.

Möchten Sie eine Client-Verbindung mittels 802.1X aufbauen, konfigurieren Sie bitte zunächst ein RADIUS-Clientprofil unter *RADIUS-Clientprofile* auf Seite 10.

Erstellen Sie bei Bedarf ein Roamingprofil unter *Roamingprofile* auf Seite 11.

3.4.2 RADIUS-Clientprofile

Möchten Sie eine Client-Verbindung mittels 802.1X aufbauen, konfigurieren Sie bitte zunächst hier ein RADIUS-Clientprofil.



Profilname

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später im Verschlüsselungsprofil angeben.

Methode

Wählen Sie eine für Ihre Anforderung passende Methode aus. Bei der Verwendung von „TLS“ ist das Hochladen eines Zertifikates notwendig.

Benutzername

Tragen Sie hier den RADIUS-Benutzernamen ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Passwort

Tragen Sie hier das RADIUS-Passwort ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Zertifikat

Sie können das Zertifikat des RADIUS-Servers automatisch annehmen oder das hochgeladene Zertifikat prüfen lassen. Wir empfehlen immer, ein Zertifikat hochzuladen, um die Integrität des RADIUS-Servers zu verifizieren. Siehe *Client-Zertifikat* auf Seite 11 für den Zertifikatupload.

3.4.3 Roamingprofile

Erstellen Sie bei Bedarf hier ein Roamingprofil.

Profilname

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später in der WDS-Verbindung angeben.

Signalstärke-Grenzwert

Tragen Sie hier den Schwellenwert ein, ab welchem sich das Scan-Intervall des Access Points verändern soll.

Gutes-Signal-Scan-Intervall

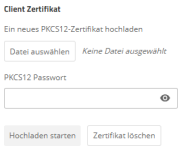
Befindet sich die Signalstärke oberhalb des Grenzwertes, wird in dieser Zeit in Sekunden ein Scan durchgeführt, um zu prüfen, ob ein besserer Access Point zum Verbinden vorhanden wird.

Schlechtes-Signal-Scan-Intervall

Fällt die Signalstärke auf den angegebenen Grenzwert, wird direkt ein Scan ausgelöst, um nach einem besseren Access Point zu suchen. Ist kein besserer Access Point vorhanden, wird in der angegebenen Zeit in Sekunden weiter gesucht, bis eine Verbindung zu einem Access Point mit einer besseren Signalstärke verbunden werden konnte oder sich das Signal mit dem verbundenen Access Point wieder verbessert hat.

3.4.4 Client-Zertifikat

Verwalten Sie hier die Client-Zertifikate für die WDS-Verbindungen.



Wählen Sie einen PKCS12-Container aus und geben das zugehörige Passwort an. Mittels **Hochladen starten** landen Sie das Zertifikat auf das Gerät. Über **Zertifikat löschen** können Sie ggf. vorhandene Zertifikate löschen.

3.5 Ergänzungen im Setup-Menü

3.5.1 Mode

Im Rahmen einer WDS-Verbindung gibt es drei Rollen: Access Point, Client, Legacy Client. Der als Client konfigurierte Partner sucht anhand der oben konfigurierten SSID einen als Access Point konfigurierten Partner und initiiert die

Verbindung. Der als Legacy-Client konfigurierte Access Point kann sich in die SSID eines beliebigen Access Points einbuchen.

Im Rahmen eines Punkt-zu-Multipunkt-Szenarios können sich mehrere Clients zu einem Access Point verbinden.

Die Menge aus regulären konfigurierten SSIDs für die Client-Anbindung sowie konfigurierten WDS-Verbindungen kann die Menge an insgesamt durch das jeweilige Gerätemodell unterstützen SSIDs nicht überschreiten – es wird sozusagen dasselbe „SSID-Budget" verwendet.

Es können beliebig viele WDS-Verbindungen im Access Point-Modus betrieben werden (bis zur Ausschöpfung der o. g. Menge an technisch maximal möglichen SSIDs des Gerätemodells. Es kann jedoch nur eine WDS-Verbindung im Station-Modus je Gerät betrieben werden. Verbindungen im Access Point-Modus und Station-Modus (von letzterer nur eine) können gleichzeitig auf demselben Gerät betrieben werden.

Beachten Sie, dass für ein Punkt-zu-Multipunkt-Szenario in der Regel eine einzelne Verbindung im AP-Modus auf dem „Verteilerknoten" ausreichend ist.

SNMP-ID:

2.20.13.1.3

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

Access-Point
Station

3.5.2 Encryption-Profile

Das Verschlüsselungsprofil, welches für die WDS-Verbindung verwendet werden soll.

SNMP-ID:

2.20.13.1.5

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.5.3 Encryption-Key

Der WPA-PSK, welcher für die WDS-Verbindung verwendet wird. Bei der Verwendung eines Verschlüsselungsprofils mit 802.1X, kann dieses Feld leer bleiben.

SNMP-ID:

2.20.13.1.6

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

3.5.4 LCOS-Client-Bridge-Support

Wird der LCOS LX-Access Point im Client-Modus mit einem LCOS-Access Point im Basisstations-Modus verbunden, können hierfür weiterhin 4-Adress-Frames verwendet werden, was die Übertragung von VLANs oder MAC-Adressen ermöglicht. Dieser Modus kann nicht verwendet werden, wenn der LCOS LX-Access Point im Basisstations-Modus betrieben wird und ein LCOS-Access Point im Client-Modus an diesem eingebucht wird.

SNMP-ID:

2.20.13.1.9

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

No
Yes

Default-Wert:

Yes

3.5.5 Roaming-Profile

Hier können Sie ein Roaming-Profil eintragen, wenn der Access Point sich im Client oder Legacy-Client Modus befindet.

Konfigurieren Sie optional ein Verschlüsselungsprofil.

Möchten Sie eine Client-Verbindung mittels 802.1X aufbauen, konfigurieren Sie bitte zunächst ein RADIUS-Clientprofil.

Erstellen Sie bei Bedarf ein Roamingprofil.

SNMP-ID:

2.20.13.1.11

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.5.6 RADIUS-Client-Profile

Geben Sie hier ggf. ein RADIUS-Clientprofil an.

SNMP-ID:

2.20.13.2.6

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Encryption**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.5.7 Roaming

Konfigurieren Sie hier die Einstellungen für das Roaming-Profil.

SNMP-ID:

2.20.13.3

Pfad Konsole:

Setup > **WLAN** > **WDS**

3.5.7.1 Profile-Name

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später in der WDS-Verbindung angeben.

SNMP-ID:

2.20.13.3.1

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.5.7.2 Signal-Strength-Threshold

Tragen Sie hier den Schwellenwert ein, ab welchem sich das Scan-Intervall des Access Points verändern soll. Werte von 0 bis 100 geben einen Prozentwert an. Werte von -100 bis 0 sind in dbm.

SNMP-ID:

2.20.13.3.2

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

max. 4 Zeichen aus `-[0-9]`

3.5.7.3 Good-Signal-Scan-Interval

Befindet sich die Signalstärke oberhalb des Grenzwertes, wird in dieser Zeit in Sekunden ein Scan durchgeführt, um zu prüfen, ob ein besserer Access Point zum Verbinden vorhanden wird.

SNMP-ID:

2.20.13.3.3

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

0 … 4.294.967.295 Sekunden

3.5.7.4 Bad-Signal-Scan-Interval

Fällt die Signalstärke auf den angegebenen Grenzwert, wird direkt ein Scan ausgelöst, um nach einem besseren Access Point zu suchen. Ist kein besserer Access Point vorhanden, wird in der angegebenen Zeit in Sekunden weiter gesucht, bis eine Verbindung zu einem Access Point mit einer besseren Signalstärke verbunden werden konnte oder sich das Signal mit dem verbundenen Access Point wieder verbessert hat.

SNMP-ID:

2.20.13.3.4

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

0 … 4.294.967.295 Sekunden

3.5.8 Delete-WLAN-Supplicant-Certificates

Mit dieser Aktion löschen Sie alle vorhandenen Zertifikate der WLAN-Supplicants.

SNMP-ID:

2.30.4

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Argumente:

keine

3.5.9 WLAN-Supplicant

Hier finden Sie die Einstellungen für die 802.1X-Supplicant-Funktionalität, um das Gerät WLAN-seitig an einer mit 802.1X gesicherten Infrastruktur zu authentifizieren.

SNMP-ID:

2.30.12

Pfad Konsole:

Setup > **RADIUS**

3.5.9.1 Profile-Name

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später im Verschlüsselungsprofil angeben.

SNMP-ID:

2.30.12.1

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.5.9.2 Method

Wählen Sie eine für Ihre Anforderung passende Methode aus. Bei der Verwendung von TLS ist das Hochladen eines Zertifikates notwendig.

SNMP-ID:

2.30.12.2

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

none
MD5
TLS
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

3.5.9.3 Username

Tragen Sie hier den RADIUS-Benutzernamen ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

SNMP-ID:

2.30.12.3

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.5.9.4 Password

Tragen Sie hier das RADIUS-Passwort ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

SNMP-ID:

2.30.12.4

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.5.9.5 Certificate

Sie können das RADIUS-Server Zertifikat automatisch annehmen oder das hochgeladene Zertifikat prüfen lassen. Wir empfehlen immer, ein Zertifikat hochzuladen, um die Integrität des RADIUS-Servers zu verifizieren.

SNMP-ID:

2.30.12.5

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

Auto-accept

Zertifikat automatisch annehmen.

Container

Hochgeladenes Zertifikat prüfen.